PCI Express® Protocol Analysis
Summit™ M5x Gen4
Analyzer / Jammer
User Manual



For PCIe Protocol Analysis Software Version 13.26

Generated: January 8, 2026 5:09pm

Teledyne LeCroy Protocol Solutions Group

Trademarks and Servicemarks

Teledyne LeCroy, CATC Trace, PETracer, PETracer Summit, Summit M5x, Summit T416, Summit T48, Summit T24, Summit T28, Summit T34, Summit T3-8, Summit T3-16, Summit Z3-16, Summit Z416, PCIe Protocol Suite, PCIe Protocol Analysis, Universal Protocol Analyzer System, UPAS, and BusEngine are trademarks of Teledyne LeCroy.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Intel and Pentium are registered trademarks of Intel Corporation.

All other trademarks and registered trademarks are property of their respective owners.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL INFORMATION, EXAMPLES AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE REPRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS ARE FULLY RESPONSIBLE FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN INFORMATION THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT Teledyne LeCroy FOR A COPY.

© 2024 Teledyne LeCroy, Inc. All rights reserved.

This document may be printed and reproduced without additional permission, but all copies should contain this copyright notice.

WEEE Program



Teledyne LeCroy
teledynelecroy.com

Contents

Chapter 1: Overview 25

1.1 PCIe Protocol Analysis™ Analyzer Hardware and Software 25

1.1.1 CATC Trace Software 27

1.1.2 Summit M5x Analyzer 28

1.1.3 Features 29

1.1.4 Other Documents 29

Chapter 2: Hardware Description 31

2.1 System Components 31

2.2 Host Machine Requirements 31

2.3 Summit M5x Operation in AJ Mode and AJA Mode vs. Analyzer Only Mode 32

2.4 Summit M5x Front Panel Description 33

2.5 Status and Config Display (Summit M5x) 34

2.5.1 LCD Display and Button Functions for Analyzer Host Connection Setup 34

Press the Up Ý and Down ß buttons to navigate through the following menu items: 34

Set IP Configuration 35

Changing from Dynamic to Static IP Mode 35

Changing from Static to Dynamic IP Mode 36

Setting the Gateway and Subnet Mask 37

2.6 Summit M5x Rear Panel Description 38

2.7 Gen4 Host and Device Probe Cards (Analyzer/Jammer Mode) 39

2.7.1 Using Gen4 Host and Device Probe Cards 39

2.8 Interposers (Analyzer Mode only) 40

2.8.1 Gen5 Slot Interposer (passive) 40

2.8.2 Gen5 x8 Interposer 42

2.8.3 Gen5 x16 Interposer 43

2.8.4 Gen4 x8 Interposer 44

Chapter 3: Installation and Setup 47

3.1 Installing the PCIe Protocol Analysis software 47

3.1.1 Downloading the PCIe Protocol Analysis software 47

3.1.2 Windows Server 2016/2019 48

3.1.3 Launching the PCIe Protocol Analysis 57

3.2 Setting Up the Summit M5x Analyzer/Jammer using a USB Connection 58

3.3 Setting Up the Summit M5x Analyzer/Jammer using an Ethernet Connection 59

3.3.1 TCP Port Connections for Different Modes 59

3.4 Adding Devices Manually 63

3.4.1 Adding a Summit M5x to an Ethernet Network 65

Chapter 4: Software Overview 71

4.1 The PCIe Protocol Analysis software 71

4.2 Application Layout 72

4.3 Using the Toolbar 72

4.3.1 Frequently Used Toolbars 72

Quick Search Feature 74

4.3.2 Multi-Segment Toolbar 77

4.3.3 Toolbar Hide Buttons 77

4.4 Using the Menus 80

4.4.1 File Menu 80

File Dialog 81

Clean Up Decoder Temp Files 82

4.4.2 Setup Menu 86

Display Options: Level Hiding -> Direction 86

4.4.3 Record Menu 87

4.4.4 Report Menu 88

4.4.5 Search Menu 89

Find Feature 90

4.4.6 ..... View Menu 96

4.4.7 Tools Menu 98

4.4.8 Window Menu 98

Windows... Feature 99

4.4.9 Help Menu 100

4.5 Dashboard View 101

4.5.1 Launching and Setting Recording Option from Dashboard View 103

4.6 Jammer Log View 103
4.7 Tool Tips 104
4.8 Keyboard Shortcuts 104
4.9 Status Bar 105
4.9.1 Recording Progress Bar 105
4.9.2 Recording Status 105
4.9.3 Recording Activity 107
4.9.4 Search Direction Indicator 107
4.10 Making a PCI Express Recording 107
4.10.1 Stopping a Recording 110
4.10.2 Saving a Recording 110
4.11 PCIe Protocol Analysis Files 111
4.11.1 CATC Trace Files 111
4.11.2 Recording Options Files 111
4.11.3 Display Options Files 111
4.12 Saving CATC Trace Files 111
4.12.1 Using the Save As Function 111
4.12.2 Saving a Portion of a CATC Trace 113
4.12.3 Save Copy As Function 113
4.12.4 Trace File Structure 115
4.13 Exporting a CATC Trace File 116
4.13.1 Export: To Text 117
4.13.2 Export: Packets to CSV Text 119
4.13.3 Export: To Generator File Format 121
Exporting a CATC Trace to a Traffic Generation File 121
4.13.4 Export From Data Flow View 124
Data Flow CSV File: Legacy Format 125
Data Flow CSV File: New Format 126
4.14 Printing Data Files 127
4.15 Analyzer Chat Window 127
4.15.1 CrossSyncTM Control Panel 129
Launching the CrossSyncTM Control Panel 129

Chapter 5: Recording Options: AJ Mode 131
5.1 Recording Overview 131
5.1.1 Analyzer/Jammer (AJ) 131

5.2 Recording Option Dialog 131
5.3 Recording Type: Select Analyzer 131
5.4 Recording Type: Summit M5x Jammer (AJ) Analyzer 133
5.4.1 Recording Options: Simple Mode Summit M5x Jammer (AJ) 133
5.4.2 Recording Options: Advanced Mode Summit M5x Jammer (AJ) 134
Options in Advanced Mode: Disable Auto Channel Swap 135
Options in Advanced Mode: TC to VC mapping 137
5.5 Recording Type: Triggering Options 138
5.5.1 Snapshot 138
5.5.2 Manual Trigger 138
5.5.3 Event Trigger 138
Events: Triggering On (Simple Mode) 139
5.6 Trigger Mode 140
5.7 Recording Mode 143
5.7.1 Protocol Recording 143
Recording the CCIX Protocol 143
5.8 Buffer Size 145
5.9 Trigger Position 146
5.10 Filter Out 146
5.11 Jammer Action 146
5.12 Advanced Trace File Settings 147
5.13 Trace Filename and Path 148
5.14 Saving and Loading Previously Saved Recording Options 149
5.14.1 Saving Recording Options 149
Buttons 149
Steps 149
5.14.2 Loading Recording Options 150
Buttons 150
Steps 150
5.15 Transceiver Preset Settings 151
5.16 Viewing Legacy Multi-Segmented CATC Traces 152
5.17 Link Settings 153
5.17.1 Speed 154
5.17.2 Link Width 154
5.17.3 Upstream and Downstream 155
5.17.4 Reference Clock 156
Reference Clock: Cable A 158
Reference Clock: Cable B 158

5.17.5 Set Reference Clocks Independently 159
5.17.6 Disable Descambling 159
5.17.7 Auto-Configure Lane Polarity 160
5.17.8 Ignore Idle Errors 160
5.17.9 Swizzling Config... 160
Manual Configure Lane Swizzle 160
Example: Move Highest Source Lane First 163
Example: Move Lowest Source Lane First 163
Working with Less Than Sixteen Lanes 163
Auto-Configure Lane Swizzle 166
5.17.10 Decode Optimized Buffer Flush/Fill (OBFF) 167
5.18 Triggering 168
5.18.1 Triggering On (Advanced Mode) 168
5.19 Navigating Recording Rules 169
5.19.1 Toolbar 169
5.19.2 Available Events Area 169
5.19.3 Main Display Area 170
5.19.4 Recording Rules Buttons 170
5.20 Recording Rules Overview 170
5.20.1 Defining Recording Rules 170
Steps to Create a Recording Rule 171
5.20.2 Resources 173
Basic Matcher (x8) 174
5.20.3 Ordered Set (OS) Matcher (x8) 175
Trigger on Control Skip 176
5.20.4 Data Link Layer Packets (DLLPs) Matcher (x8) 178
5.20.5 Transaction Layer Packets (TLPs) Matcher (x8) 179
5.20.6 Global State and Sequence States 180
Global State 180
Sequence State 182
5.20.7 Recording Rules Events 183
5.20.8 Properties Dialog Boxes for Events 186
Accessing the Properties Dialog 186
Event Properties Dialog Box Features 186
Link State Dialog 187
Ordered Sets 190
Framing Token 192
Error Properties Dialog 196
DLLP Packet Properties Dialog 197
TLP Header Properties Dialog 199
TLP Prefix Properties Dialog 200
NVME Register Properties Dialog 203

PQI Register Properties Dialog 206
5.20.9 Actions Properties Dialog 207
Filter Out 208
Filter-Out In Simple Mode 209
Filter-Out in Advanced Mode 210
5.20.10 Filter In 210
5.20.11 Valid Configuration 211
5.20.12 Invalid Configuration 213
5.20.13 Filtering Events: (Electrical Idle, CLKREQ#, WAKE#) 214
Example of CLKREQ# Filtering Enabled 214
Example of CLKREQ# Filtering Not Enabled 215
5.20.14 Filtering Out NVMe CSTS, DLLP Ack and TLP Completions 216
5.20.15 Triggering Configuration on a per Lane Basis 227
DLLP/TLP Packets Category 228
Errors Category 228
Ordered Sets Category 229
5.20.16 Lane Trigger Configuration 230
Example 1: 230
Lane Trigger Configuration Example 2: 230
Lane Trigger Configuration Example 3: 231
5.20.17 Counter 233
How to Set a Counter 234
How to Increment or Reset a Counter 235
Changing the Value of the Counter 237
Deleting a Counter 237
5.20.18 Timer 237
How to Set a Timer 238
How to Start or Reset a Timer 239
Changing the Value of the Timer 240
Deleting a Timer 241
5.20.19 Channel 241
5.20.20 Lane Margining 242
5.21 Triggering On (Advanced Mode) 244
5.21.1 Triggering On (Advanced Mode) 246
Selecting Triggers/Filters to be Active 246
Selected Items Settings 247
Direction 247
5.22 Recording Options for Compute Express Link (CXL) Mode 248
5.22.1 Triggering On (Simple Mode): PCIe Phy & CXL.io 249
5.22.2 Trigger On CXL.cache/mem 250
5.22.3 Trigger On CXL Flits 251
5.22.4 CXL: Filter Out for PCIe Phy and CXL.io 252

5.22.5 CXL: Filter Out for CXL.cache/mem....253
5.22.6 CXL: Filter Out for CXL Flits....253

Chapter 6: Recording Options: AJA Mode....255
6.1 Jammer Mode Overview....255
6.1.1 Jammer Mode (AJ)....255
6.1.2 Jammer Mode (AJA)....255
6.1.3 PCIe Protocol Analysis Software....255
6.1.4 Recording Options....256
6.1.5 Recording Options: Recording Rules (AJ)....258
6.1.6 Recording Rules AJ: New Events....259
6.2 Converting Recording Rules and Jammer Actions from GUI to Script File (AJ)....260
6.2.1 Complex Recording Rules....260
6.2.2 Jammer Options....262
Example: Jammer Replace....263
6.3 Script Mode....267
6.3.1 Script Parsing....271
6.4 Commands....272
6.5 Events....273
6.6 Jammer Actions....274
6.7 Scripting Jammer Functionality....275
6.7.1 Example: Select Jammer Action: Delete....275
6.8 Recording Options and Jammer Action Script....280
6.9 Updating Jammer Action Script....282
6.10 Warning Message if Mistake in Jammer Script....287
6.11 Updated GUI After Scripting Mistake Corrected....289
6.12 Saving a Jammer Actions Script File....290
6.13 Loading a Jammer Script File....291
6.14 Examples of Scripting for Common Events with Jammer Actions....295
6.14.1 Link State: Speed Change....296
6.14.2 Ordered Set: TS2....300
Ordered Set: TS1....301
6.14.3 Framing Token: EDS....304
6.14.4 Errors: Symbol Error....306
6.14.5 DLLP: Any....308
6.14.6 TLP: Any....310
6.14.7 NVMe....312
NVMe Register....312
NVMe Command Submission: Any....313

NVMe Command Completion: Any 316
6.15 Jammer Mode Overview (AJA) 318
6.15.1 Examples of AJA Traces (Jammer Actions and Results) 320
Delete: UpdateFC_P DLLP Packet 320
Insert Error: DROP_STP_SDP for UpdateFC_P Packet 323
Insert TLP After UpdateFC_NP Packet 326
Modify: UpdateFC_P Packet to UpdateFC_NP Packet 329
Replace: UpdateFC_CP with TS1_PAD_PAD 332

Chapter 7: Recording Options: Analyzer Only Mode 335
7.1 Recording Overview 335
7.1 Recording Option Dialog 335
7.2 Select Summit M5x Analyzer for Recording 335
7.3 Recording Options M5x Analyzer: Simple Mode 336
7.4 Recording Options M5x Analyzer: Event Trigger Mode 337
7.5 Recording Options M5x Analyzer: Advanced Mode 338
7.6 Recording Type 340
7.6.1 Snapshot 340
7.6.2 Manual Trigger 340
7.6.3 Event Trigger 341
..... Triggering On (Simple Mode) 342
Filter Out (Simple Mode) 343
7.7 Recording Mode 344
7.7.1 Protocol Recording 344
7.7.2 Bit Tracer Recording 345
7.8 Buffer Size 345
7.9 Trigger Position 345
7.10 Advanced Trace File Settings 346
7.11 Analyzer & Probe Settings 347
7.11.1 Library 347
7.11.2 Search Filter 348
7.11.3 Saving a Selected Preset 350
7.11.4 Library Operations 352
Buttons & Functions 354
7.12 Trace Filename and Path 355
7.13 Saving and Loading Previously Saved Recording Options 355
7.13.1 Saving Recording Options 355
7.13.2 Loading Recording Options 356

7.13.3 Loading Recording Options 356
7.13.4 Saving Recording Options 357
7.14 Viewing Legacy Multi-Segmented CATC Traces 357
7.15 Link Settings 357
7.15.1 Speed 358
7.15.2 Link Width 360
7.15.3 Upstream and Downstream 362
7.15.4 Reference Clock 362
Internal 363
External 363
SMA 364
7.15.5 Set Reference Clock Independently 365
7.15.6 Auto-Configure Lane Polarity 366
7.15.7 Ignore Idle Errors 366
7.15.8 Swizzling Config... 366
Manual Configure Lane Swizzle 366
Example: Move Highest Source Lane First 369
Example: Move Lowest Source Lane First 369
Working with Less Than Eight Lanes 370
Auto-Configure Lane Swizzle 371
7.15.9 Decode Optimized Buffer Flush/Fill (OBFF) 373
7.15.10 Disable Descrambling 373
7.15.11 Ignore EDS 373
7.16 General guidelines to do the Calibration and AutoTuning 373
7.16.1 Interposer Host to DUT Path 375
Interposer Host to DUT CTLE and DCGain Settings 375
Interposer Host to DUT Autotune 380
Using Z516 or Z58 as a DUT 382
Auto-tuning Algorithms 383
Host is on Linux OS: 399
Write to Interposer 406
Write to RAM 406
Write to Flash + RAM 406
Write Default to Flash + RAM 406
Configurations: U2 x2, U2 x4 406
Read from Interposer 406
Set All Lanes 407
Log 407
Save to File 407
Load from File or Predefined Values 407
7.16.2 Interposer to Analyzer Path 409
Calibration Sequence 411

7.16.3 Analyzer Calibration 412
Analyzer Calibration: Auto Option 413
Analyzer Calibration: Manual Option 414
7.16.4 Using the Autotune and Probe Calibration Wizard 416
7.16.5 Interposer Settings for Bifurcated Multiport Link 427
7.16.6 Saving Auto-Tune and Calibration Results 429
7.17 Analysis Options 429
7.17.1 Example: Gen5 Trace 429
7.18 BitTracer Recording 431
7.18.1 Enabling BitTracer Recording 431
7.18.2 Triggering in Simple Mode 432
7.18.3 Views Available for Captured Data 432
7.18.4 De-skewing Data 433
7.18.5 Data Display Formats 434
7.18.6 Color-Coding of BitTracer Contents 434
7.18.7 Report and Analysis Windows 435
7.18.8 Timing Measurements Bar 435
Markers/Speed Bar 435
Defining a Marker 436
7.18.9 Errors Bar 438
7.18.10 Symbols Bar 440
7.18.11 Events Bar 440
7.18.12 Packets Bar 441
7.18.13 Decoding Bar 442
7.18.14 Search 443
7.18.15 Link Configuration 444
7.18.16 Export of BitTracer Capture to CATC Trace Format 446
Exports Involving Multiple Logical Links on One Physical Link 446
Export To CSV Text 446
Exporting Data from Bit Tracer to a Trace File 448
7.18.17 Compressing and Expanding the Data View 453
7.18.18 Opening and Saving BitTracer Captures 453

Chapter 8: Jammer Options 455
8.1 Jammer Mode Overview 455
8.1.1 Jammer Mode (AJ) 455
8.1.2 Jammer Mode (AJA) 455
8.1.3 PCIe Protocol Analysis Software 455
8.1.4 Recording Options 456
8.1.5 Recording Options: Recording Rules (AJ) 458
8.1.6 Recording Rules AJ: New Events 459

8.2 Converting Recording Rules and Jammer Actions from GUI to Script File (AJ)..... 460
8.2.1 Complex Recording Rules....460
8.2.2 Jammer Options....462
8.3 Script Mode..... 463
8.3.1 Script Parsing....467
8.4 Commands..... 468
8.5 Events..... 469
8.6 Jammer Actions..... 469
8.7 Scripting Jammer Functionality..... 470
8.7.1 Example: Select Jammer Action: Delete....471
8.8 Recording Options and Jammer Action Script..... 475
8.9 Updating Jammer Action Script..... 477
8.10 Warning Message if Mistake in Jammer Script..... 482
8.11 Updated GUI After Scripting Mistake Corrected..... 484
8.12 Saving a Jammer Actions Script File..... 484
8.13 Loading a Jammer Script File..... 486
8.14 Examples of Scripting for Common Events with Jammer Actions..... 490
8.14.1 Link State: Speed Change....491
8.14.2 Ordered Set: TS2....495
Ordered Set: TS1..... 496
8.14.3 Framing Token: EDS....499
8.14.4 Errors: Symbol Error....501
8.14.5 DLLP: Any....503
8.14.6 TLP: Any....505
8.14.7 NVMe....507
NVMe Register..... 507
NVMe Command Submission: Any..... 509
NVMe Command Completion: Any..... 511
8.15 Jammer Mode Overview (AJA)..... 513
8.15.1 Examples of AJA Traces (Jammer Actions and Results)....515
Delete: UpdateFC_P DLLP Packet..... 515
Insert Error: DROP_STP_SDP for UpdateFC_P Packet..... 518
Insert TLP After UpdateFC_NP Packet..... 521
Modify: UpdateFC_P Packet to UpdateFC_NP Packet..... 524
Replace: UpdateFC_CP with TS1_PAD_PAD..... 527

Chapter 9: Reading CATC Traces 531
9.1 Viewing PCI Express CATC Traces 531
9.2 Expand and Collapse Data Fields 531
9.3 Resizing Cells 532
9.4 Context Menus 532
9.4.1 Address Context Menu 532
9.5 View Data Block 534
9.5.1 Save Data Block 535
9.6 Show Raw 10b Codes 537
9.7 Show Header Fields 537
9.8 Packet Cell Context Menus 539
9.8.1 Show/Hide Link Tracker 540
9.8.2 Show Raw 10b Codes 541
9.8.3 Time From Trigger 542
9.8.4 Time From Marker 543
9.8.5 Copy for PETrainer 'packet' command 544
9.8.6 Set Start Quick Timing Marker 545
9.8.7 Set End Quick Timing Marker 545
9.8.8 Tag Context Menu 546
Quick Timing Bar 548
9.8.9 Delete All Quick Timing Markers 548
9.8.10 Set Marker 548
9.8.11 Edit or Clear Marker 550
9.8.12 Format 551
9.8.13 Color 552
9.8.14 Other Packet Cell Context Menus 553
Packet Header R-> Cell Popup Menu 553
Packet Header Speed Cell Popup Menu 553
9.9 Compressed CATC Trace View 554
9.10 Spreadsheet View 555
9.10.1 Columns 557
9.10.2 Detail View and Spreadsheet View 561
9.11 Decoding Traffic 561
9.11.1 Packet 561
9.11.2 Link 564
9.11.3 Split 564
9.11.4 Lane Margining Decoding 565
Typical Lane Margining Commands and Responses 565
Lane Margining Command: Step Margin to Timing Offset 567
Lane Margining Errors 568

9.11.5 NVMe Decoding 569
NVMe: Device ID and Model Name Decoded 571
NVMe: Data Field on Packets 572
NVMe: Trusted Computing Group Decode 574
The Opal Storage Specification 575
Opalite Version 0.1: Decoded 577
NVMe: Command IOPS and Doorbell Statistical Information 579
NVMe: Decode for Doorbells 583
Time Stamp from Implicit Start 585
NVMe Commands and Transactions: Data Throughput 586
NVMe Decoding vs. NVMe Specification 587
NVMe Controller Register 590
Decoding Multiple NVMe Commands for a Single MemRead or MemWrite 594
9.11.6 NVMe 1.2 Specification Decoding 597
9.11.7 Support for Physical Region Page (PRP) and Scatter Gather List (SGL) in Controller Memory Buffer (CMB) 601
9.11.8 NVMe Decoding for Host Memory Buffer FID 604
9.11.9 AHCI 605
9.11.10 ATA 605
ATA IO: Pending Transactions Statistical Report 606
9.11.11 PQI 609
9.11.12 SOP 609
9.11.13 SCSI 610
9.11.14 Decoding MCTP (Management Component Transport Protocol) 611
MCTP Levels in Floating Transactions Bar Window 611
Decoding MCTP Commands 612
Expanding MCTP Commands 616
Decoding MCTP Messages 617
MCTP Commands with SMBus Traffic 618
MCTP Commands: Request from Host, Response from Device 619
Decoding MCTP Messages and Transactions 620
MCTP Messages 621
MCTP Transactions 621
MCTP Errors Reported 622
MCTP Trace In Spreadsheet View 623
Decoding MCTP Messages with PLDM Message Types 624
Decoding MCTP Messages with NC-SI Message Types 625
MCTP Command with NVMe-MI Errors Decoded 626
MCTP Message Type and IC Cells 627
9.11.15 Decoding MCTP Messages with SMBus Traffic 629
Sideband Traffic: Displayed or Hidden 631
SMBus Errors 633

SMBus Error Tooltip 634
Traffic Summary Report: SMBus Errors 635
9.11.16 Decoding SMBus with Address Resolution Protocol (ARP) 637
9.11.17 Decoding MCTP Traffic with Vendor Defined Messages (VDM) 638
9.11.18 Decoding Side Band Signals 639
9.11.19 PMUX Channel ID Found and PMUX Packet Error Decoded in Trace 640
9.11.20 Decoding Traces with Different Class Codes 641
Example: Loading an NVMe Trace and Decoding for ATA 641
Example: Loading a PQI Trace and Decoding for NVMe 642
9.11.21 Data Link Features 643
9.11.22 Decode for NVMe 1.3c Specification 644
9.11.23 NVMe Warning Messages 648
Trace View 648
Traffic Summary View 650
Find NVMe Commands and Transactions 653
Hiding NVMe Warning Messages 655
9.11.24 Decoding Lightweight Notification (LN) Protocol 656
Lightweight Notification Protocol Errors 657
Lightweight Notification Protocol in Trace Expert 658
Lightweight Notification Transaction Analysis Errors: Trace Expert 660
Find: Lightweight Notification Transactions 661
9.11.25 Decoding CCIX Protocol 662
9.11.26 Decoding TCG Support of Pyrite 663
9.11.27 MCTP: Simple Hiding 664
MCTP: Hide VDM Traffic 664
MCTP: Hide SMBus Traffic 666
MCTP Message Type and IC Cells 668
9.11.28 Decoding NVME-MI Version 1.1 670
9.11.29 Swapping Direction of Recorded Traffic Data 671
9.11.30 Decoding Traces Exported from USB4 Traces with Tunneled PCIe Traffic 674
9.11.31 Decoding CXL Traffic 676

Chapter 10: Searching CATC Traces 679
10.1 CATC Trace Search Overview 679
10.2 Go to Trigger 680
10.3 Go to Selected Packet 680
10.4 Go to Packet 680
10.5 Go to Time 681
10.6 Go To Marker 681
10.6.1 Markers 682
Markers Overview 682

Functionality of Markers 683
Set New Marker 683
10.6.2 Attaching Markers 684
10.6.3 Adding an Attachment 685
10.6.4 Recording an Audio File 685
10.6.5 Video Files Supported 686
10.6.6 Attachment Types and Visualization 686
10.6.7 Embedded Attachments to a Marker 686
10.6.8 Viewing Attachments of a Marker 687
Text 687
Audio 688
Video 689
File Attachment 689
URL Link 689
YouTube Video 691
Images 691
Other Attachments 692
10.6.9 Edit Marker 693
10.6.10 All Markers Dialog 694
10.6.11 CATC Walk Playlist 696
10.6.12 Playlist Functionality 696
10.6.13 Playback Window 697
Playlist Playback Controls 698
10.7 Go to NVMe Transactions and Commands 699
10.7.1 NVMe Transaction 699
10.7.2 NVMe Command 700
10.8 Go To SCSI Menu 701
10.9 Go To Menu 702
10.9.1 Example: Search -> Go to -> Link Event -> Link Up/Link Down 703
10.9.2 Example: Go To CXL 704
10.10 Find 705
10.10.1 Event Groups for Packets 709
Example: TS1 and TS2 Event Groups 710
Example: Search for PMUX Channel ID 719
10.10.2 Find Function and CXL Packets 721
10.10.3 Event Groups for Link Transactions: 722
10.10.4 Event Groups for Split Transactions: 722
10.10.5 Event Groups for LM Commands 722
10.10.6 Event Groups for NVMe transactions: 723
10.10.7 Event Groups for PQI Transactions: 724
10.10.8 Event Groups for AHCI Transactions: 724
10.10.9 Event Groups for ATA transactions: 724

10.10.10 Event Groups for SOP Transactions: 724
10.10.11 Event Groups for SCSI Transactions: 724
10.10.12 Event Groups for NVMe Commands: 725
Example: Search for NVMe Command 725
Example: Search for NVMe Command: NVM Payload Portion.... 728
10.10.13 Example: Search for DLLP Header -> Flow Control Feature....730
10.11 Find Next Packet Type 732
10.11.1 Quick Search Feature....732
10.12 Toggle Search Direction 735

Chapter 11: Display Options 737
11.1 Display Options: General Tab 737
11.1.1 Collapsing Data Fields....739
11.2 Display Options: BitTracer General 739
11.3 Display Options: Color/Format/Hiding 739
11.3.1 Setting Colors....740
11.3.2 Changing Formats and Bit Order....741
11.3.3 Hiding Fields....742
11.4 Display Options: Level Hiding.... 742
11.4.1 Hiding Levels 743
11.4.2 PCIe Trace Event Groups 744
11.4.3 CXL Trace Event Groups 744
11.5 Display Options: Error Hiding 745
11.5.1 Transaction Types....745
11.6 Display Options: Warning Hiding.... 745
Transaction Types.... 746
11.7 Load a Previously Saved Display Options File.... 746
11.8 Saving Display Options.... 746
11.9 Save as Default 747
11.10 Load Default.... 747

Chapter 12: Reports and Tools 749
12.1 Trace Expert.... 752
12.1.1 Performance Analysis....755
12.1.2 Trace Analysis Statistics 756
12.1.3 Error Reports 757
12.1.4 Trace Information 758

12.2 Trace Information 759
12.3 Error Summary 762
12.3.1 Error Summary for Storage Protocols 762
12.3.2 Error Summary for Storage Protocols -- NVMe 765
Types of NVMe Errors: 765
12.3.3 NVMe Queue Errors 765
Types of NVMe Queue Errors 766
12.3.4 NVMe CMD Errors 767
Types of NVMe CMD Errors 767
12.4 Traffic Summary 770
12.4.1 Traffic Summary for Storage Protocols 770
12.4.2 Using the Traffic Summary Window to Search the CATC Trace 771
12.4.3 NVMe Queue Time Metrics 771
NVMe Queue Time Metrics Defined (Commands/Transactions) 773
NVME Command Example 773
NVME Transaction Example 774
12.4.4 Traffic Summary Buttons 774
12.4.5 Traffic Summary for Flow Control 775
12.4.6 Example: CXL in Traffic Summary 776
12.4.7 Example: CXL Errors Shown in Traffic Summary Report 777
12.4.8 CXL Flit Data View 778
12.5 Bus Utilization 783
12.5.1 Bus Utilization Pop-up Menu 784
12.5.2 Bus Utilization Buttons 785
Graph Area Options 787
Example: NVMe Queue Load Graph Feature 789
Graph Legend 790
Graph Properties 790
12.6 Link Tracker 791
12.6.1 Using the Link Tracker Window 791
12.6.2 Zooming In and Out 792
12.6.3 Collapsing Idle Time, Enabling Tool tips, and Resetting Column Widths 792
12.6.4 Docking and Undocking the Window 793
12.6.5 Setting Markers 793
12.6.6 Calculating Time between DWORDs 793
12.6.7 Hiding Traffic 794
12.6.8 Link Tracker Buttons 794
Exporting to CSV File 796

12.7 Data Flow Window 797
12.8 Flow Control Tracking 799
12.9 Using the CATC Trace Navigator 800
12.9.1 Displaying the Navigator 800
12.9.2 Navigator Toolbar 800
12.9.3 Navigator Ranges 801
12.9.4 To Determine Current Position 801
12.9.5 To Reset Navigator Range 802
12.9.6 Navigator Panes 802
12.9.7 To Show/Hide Nav55igator Panes 803
12.9.8 Navigator Slider 803
12.9.9 CATC Trace Navigator Legend 803
12.9.10 Using the Legend to Show/Hide Navigator Panes 804
12.9.11 Using the Legend to Set the Priority of Information Display 804
12.10 Detail View 806
12.11 LTSSM Flow Graph 807
12.11.1 LTSSM Dynamic Equalization 808
12.12 TCG Security View 811
12.13 Get Log Page View 813
12.14 Lane Margining: Eye Diagram 814
12.15 Packet Header Bar 817
12.16 Packet Data Window 818
12.17 Configuration Space View 819
12.18 Using Unit Metrics 824
12.19 Metrics Defined for Link Transactions 824
12.19.1 Metrics Defined for Split Transactions 824
12.20 Show Metrics in the CATC Trace Display 825
12.20.1 Collapsed Metrics Header Display 825
12.20.2 Metrics Tool Tip Display 825
12.20.3 Expanded Metrics Header Display 825
12.21 Show Metrics in the Traffic Summary Window 827
12.21.1 Reports at Split Transaction Level 827
12.21.2 Reports at the Link Transaction Level 827
12.22 Show Metrics in the Bus Utilization Window 829
12.22.1 Unit-Based Averaging 829
12.22.2 Bus Utilization Window Features 830
12.22.3 Split Transaction Level Graphs 830
12.22.4 Link Transaction Level Graphs 831

12.23 Real-Time Statistics Window 833
12.23.1 Real-Time Statistics Buttons 834
12.23.2 Real-Time Statistical Monitor Pop-up Menu 835
12.23.3 Real-Time Statistics Graph Areas 836
Data Packet Count 836
12.24 Tools -> Import Configuration Space File 839
12.25 Tools -> Configuration Space Editor 841
12.26 Tools -> Memory I/O Space Editor 843
12.27 Tools -> Interposer Programmer 844
12.27.1 Installing the FTDI Serial Cable 844
12.27.2 Installing USB Type-C Serial Cable 845
12.27.3 Running the PCIe Interposer ASIC Programmer Utility 847
12.27.4 PCIe Interposer ASIC Programmer Utility Functionality 849
Equalization Settings 850
Write to Flash 850
Write to Interposer 850
Read from Interposer 850
Set All Lanes 850
Log 850
Save to File 850
Load from File/Preset 851
12.28 Tools -> Probe Calibration 853
12.29 Tools -> TC to VC Mapping 854
12.30 Tools -> Timing and Bus Usage Calculations 855
12.30.1 Timing Calculator 855
PCIe Timing Information: Entire Trace 855
Bus Utilization 856
Split Transaction Performance 856
Memory Writes Performance 856
Queue Utilization 857
Total Input/Output 858
Timing Calculator Display units 859
12.30.2 Details of Timing Calculations 860
Timing From Beginning of Event to Beginning of Event or to End of Event 860
Types of Events 860
Displaying Time 861
Markers 861
Timing To Beginning of NVMe Command 862
Timing To End of NVMe Command 863
Results from Timing Calculator 863

Timing to Beginning and End of Events: Effect on Queue Utilization 864
Timing to Beginning and End of Events: Effect on Total Input / Output..... 865
12.31 Tools -> PCIe SSD Base Address Mapping..... 866
12.31.1 Base Address Not Recorded in Trace 866
12.31.2 Base Address Recorded in Trace 867
12.31.3 NVMe PCIe SSD Device Configuration 868
Interrupts..... 871
12.31.4 AHCI PCIe SSD Device Configuration 871
12.31.5 PQI PCIe SSD Device Configuration.....873
12.31.6 SCSI PCIe SSD Device Configuration.....875
12.32 Tools -> Running Verification Scripts 877
12.32.1 NVMe Performance: Doorbell Timing 880

Chapter 13: Updates and Licensing 881
13.1 Updating the Analyzer..... 881
13.2 License Keys..... 881
13.3 License Information..... 881

Appendix A: How to Contact Teledyne LeCroy.....883

Appendix B: China Restriction of Hazardous Substances Table.....885

Appendix C: Quick Search Feature 887
C.1 Quick Search Feature: Pre-Defined Terms..... 887

Appendix D: Configuration Space Decoding 891
D.1 Mandatory Definitions 891
D.2 Mandatory Module Functions 891
D.2.1 DecodeRegister(offset) 892
D.2.2 GetSize() 892
D.3 Configuration Register Types..... 892
D.4 Primitives..... 893
D.4.1 GetRegisterField 893
D.4.2 AddField.....893
D.4.3 AddSubField.....894

D.5 Helper File 894

Appendix E: Example of XML File Format for SSD Decodes 895

Appendix F: Expandability 897

F.1 Expandability 897

F.1.1 Removal of Expansion Cards 898

F.1.2 Installation of Expansion Cards 902

F.1.3 Daisy-Chaining with CATC SYNC Expansion Cards 905

Chapter 1

Overview

Designed for developers and validators, the Teledyne LeCroy Summit M5x™ is a PCI Express 4.0 compliant advanced verification system supporting 2.5/5.0/8.0/16.0 GT/s speeds.

By leveraging years of experience in protocol analysis tools for emerging markets, the Summit M5x blends sophisticated functionality with practical features to speed the development of PCI Express™ IP cores, semiconductors, bridges, switches, add-in boards, and systems.

For Gen5 analysis capabilities see Chapter 7, “Recording Options: Analyzer Only Mode,” on page 333.

1.1 PCIe Protocol Analysis™ Analyzer Hardware and Software

Summit M5x Analyzer/Jammer has these features and benefits:

TABLE 1.1: Summit M5x Analyzer/Jammer Features & Benefits (Sheet 1 of 2)

Features	Benefits
Powerful and Intuitive CATC Trace™ Analysis Software	Faster interpretation and debug of PCI Express traffic with color-coded, clearly labeled protocol elements in a graphical display.
Extensive Decoding	Complete, accurate and reliable decoding of TLPs (Transaction Layer Packets), DLLPs (Data Link Layer Packets), NVMe, PQI, AHCI, ATA, SOP and SCSI command transactions and all PCI Express Primitives.
Intelligent Reporting	Quickly identify and track error rates and abnormal link or timing conditions. Display configuration space and protocol specification details.
Jamming Capability	With the addition of the jammer capability the Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior. The Summit M5x also introduces for the first time NVMe and NVMe-MI protocol jamming as well.

TABLE 1.1: Summit M5x Analyzer/Jammer Features & Benefits (Sheet 2 of 2)

Features	Benefits
Sophisticated Viewing	View Packet, Link, Split, NVMe, PQI, AHCI ATA, SOP and SCSI command transaction levels of the PCI Express protocol. Collapsible/expandable headers with Tool tip explanations make it easy to navigate and interpret packet contents, headers, and commands. View packets, transactions of TLPs and DLLPs in classic CATC Trace™ format or in raw bit stream for deeper analysis.
Summit M5x 128 GB Recording Capacity, 64 GB in each direction	Capture long recording sessions for analysis and problem solving.
Flexible Host Interface	USB and GIGE.
Downloadable CATC Trace Viewer	Share and annotate CATC Trace recordings within a development team. Freely distributable PCIe Protocol Analysis enables collaborative analysis across sites and time zones.
Summit M5x Bidirectional x1-x16, 2.5 GT/s to 16.0 GT/s recording support	Accurate and non-intrusive collection of PCI Express CATC Trace data.
Field-upgradeable firmware and recording engine	Upgrades available for download direct from the Teledyne LeCroy website.
Flexible probing options	Gen4 Host and Device Probe Cards.
External interface	Enables cross triggering between other test instruments.
Dword to Transaction Level Viewer	View Dwords, Packet, Link, Split, NVMe, PQI, AHCI ATA, SOP and SCSI command transaction levels of the PCI Express protocol.
Support for Gen1/Gen2/Gen3/ Gen4/Gen5 Compliance Patterns	Gen1/Gen2/Gen3/Gen4/Gen5 Compliance Patterns can be decoded as well as filtered out of the traffic stream.

1.1.1 CATC Trace Software

The Summit M5x utilizes the CATC Trace™ to assist users in analyzing how PCI Express components work together, diagnose problems, and test for interoperability and standards compliance.

The CATC Trace is a powerful and intuitive expert software system embedding detailed knowledge of the protocol hierarchy and intricacies, as defined in the protocol specification. The software allows the user to control the Analyzer and set specific real-time triggering and filtering conditions. The CATC Trace utilizes a Windows-based graphical display that has been optimized for fast and easy navigation through a captured traffic session. Users are alerted as violations are detected at all levels of the protocol layering and can easily drill down on areas of interest or collapse and hide fields that are not relevant.

1.1.2 Summit M5x Analyzer

The Teledyne LeCroy Summit M5x is Teledyne LeCroy's high performance PCI Express analyzer/jammer for customers in server, workstation, desktop, graphics, storage and network card markets.

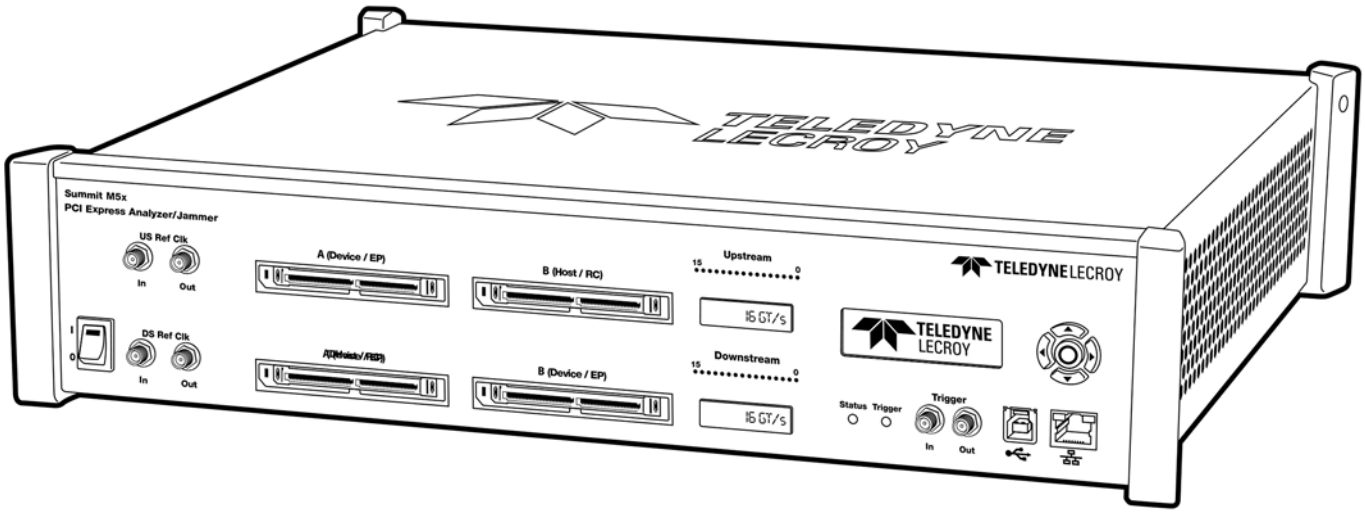


Figure 1.1: Summit M5x Analyzer/Jammer

With advanced features such as support for PCI Express Spec 4.0, data rates from 2.5 to 16.0 GT/s, lane widths from x1 to x16, and a full 128 GB of memory, the Summit M5x provides unmatched capability and flexibility for developers and users of advanced PCI Express products. The Summit M5x is the most advanced and sophisticated PCI Express Analyzer available in the market today.

With the addition of the jammer capability the Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to the PCIe 4.0 design specifications and identify potential errors in protocol behavior. The Summit M5x also introduces for the first time NVMe and NVMe-MI protocol jamming as well.

As with other Teledyne LeCroy PCI Express analyzers, the Summit M5x leverages the intuitive and powerful CATC Trace analysis software system, embedding a deep understanding of the PCI Express protocol hierarchy and intricacies. The colorful, intuitive and easy-to-use graphical display allows you to quickly capture and validate PCI Express product designs.

In addition to a full suite of advanced hardware and software features, the Summit M5x has user-convenience and analysis features, such as support for "lane swizzling," which allows a board developer to lay out a mid-bus probe pad with lanes in non-standard order, simplifying the design of the board. Internally, the Summit M5x maps the lanes back into their correct order and accurately displays the embedded bus traffic. An optional BitTracer™ mode allows bytes to be recorded as they come across the link, allowing debugging of PHY layer problems and combining the features of a logic analyzer format with a protocol analyzer format.

The Summit M5x supports USB and GIGE host interfaces. By connecting over GIGE, engineers can operate the system remotely (for example, install the client software on their desktop systems to control an analyzer operating in a remote lab). Also, multiple engineers working collaboratively can time-share use of a single analyzer, reducing the need for an additional analyzer for each engineer and increasing the cost effectiveness of the product.

1.1.3 Features

- **Powerful and Intuitive CATC Trace Analysis Software System**: The CATC Trace embeds deep understanding of the PCI Express protocol hierarchy and intricacies. This knowledge is presented in a colorful, intuitive and easy-to-use graphical display, allowing you to quickly capture and validate PCI Express product designs.
- **Protocol Hierarchical Viewing**: Displays Packet, Transaction, Split, NVMe, PQI, AHCI, ATA, SOP and SCSI command transactions levels of the PCI Express protocol, with increased drill-down detail for PCI Express primitives, errors, payloads or individual packets.
- **Jammer Capability**: Can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior.
- **Lane-Reversal Compatible**: Triggers, records, and displays PCI Express traffic logically, regardless of the physical configuration of the lanes.
- **Statistical and Error Reporting**: Provides a quick summary of the CATC Trace file to identify and track error rates and abnormal link or timing conditions.
- **BitTracer™ Recording Mode (optional)**: Records the bytes exactly as they come across the link, allowing debugging of PHY layer problems.
- **Auto Speed detection**: Follows link transitions through speed changes.
- **Lane Swizzling Support**: Allows board developers to lay out lanes in a non-standard order, simplifying board design.
- **Field-upgradeable Firmware and Engine**: Positions you to receive the latest PCIe Protocol Analysis enhancements and future additional capabilities. Allows field upgrades of all system types.
- **M5x has up to 128-GB Data Buffer**: Capture long time windows for in-depth analysis and identification of erratic problems.
- **GIGE Ethernet Connectivity**: Allows connection to an Ethernet network and sharing of analyzer resources by multiple engineers.
- **USB connectivity**: Allows connection by USB cable.
- **CrossSync™ Application:** The CrossSync™ application allows you to select analyzers for synchronization and manage the recording process.

1.1.4 Other Documents

For more information, refer to the following documents:

- Teledyne LeCroy Analyzers File-based Decoding Manual
- PCIe Protocol Analysis/Trainer Automation Manual
- PCIe Protocol Analysis VSE Manual
- CrossSync™ Control Panel User Manual
- Scripting and Automation API Reference Manual

Chapter 2

Hardware Description

The PCI Express™ system features Summit Analyzers.

2.1 System Components

The system components are different for the Summit M5x when used in Analyzer/Jammer (AJ) or Analyzer/Jammer/Analyzer (AJA) Mode or in Analyzer Only Mode.

System Components	
Summit M5x Analyzer/Jammer or Analyzer/ Jammer/Analyzer Mode	**Summit M5x Analyzer Only Mode**
Summit M5x™ analyzer box	Summit M5x™ analyzer box
Gen4 x16 (or x8) Host Probe Card (see “Gen4 Host and Device Probe Cards (Analyzer/Jammer Mode)” on page 37	Gen5 x8 Slot Interposer (or other see “Interposers (Analyzer Mode only)” on page 38)
Gen4 x16 (or x8) Probe Card Cables (PE018UCA-X) (2 required) when used with Gen4 x16 (or x8) Device Probe Cards Host (PE177UIA-X) or Device (PE173UIA-X)	Gen4 x16 (or x8) Probe Card Cables (PE018UCA-X) (2 required) when used with Gen4 x8 interposer (PE182UIA-X) or other Gen4 interposers
	Gen4 to Gen5 Conversion cables (PE031UCA-X) when used with Gen5 x8 (PE202UIA-X) or x16 interposers (PE207UIA-X)

2.2 Host Machine Requirements

The Summit M5x Analyzer/Jammer connects to a host machine. Please consult the **readme** file within the software installation for the latest host machine requirements.

2.3 Summit M5x Operation in AJ Mode and AJA Mode vs. Analyzer Only Mode

When the Summit M5x Jammer capability is used in Analyzer /Jammer (AJ) Mode or Analyzer/ Jammer/Analyzer (AJA) Mode you are using Host and Device Probe Cards to test the robustness of your system.

In these modes you can analyze and jam at up to Gen4 speeds (16 GT/sec) and up to x16 lanes.

- **AJ Mode**: In this mode you can analyze, then introduce jamming actions.
- **AJA Mode**: In this mode you can analyze, then introduce jamming actions and then analyze again after the jamming actions have been introduced.

When the Summit M5x Analyzer is used in Analyzer only mode you can analyze DUTs at up to Gen5 speeds (32 GT/sec) and up to x8 lanes.

Analyzer Only: Up to Gen5 speed and x8 lanes.

2.4 Summit M5x Front Panel Description

When powered on, the Summit M5x activates the user-accessible controls and LEDs on the front panel. See Figure 2.1.

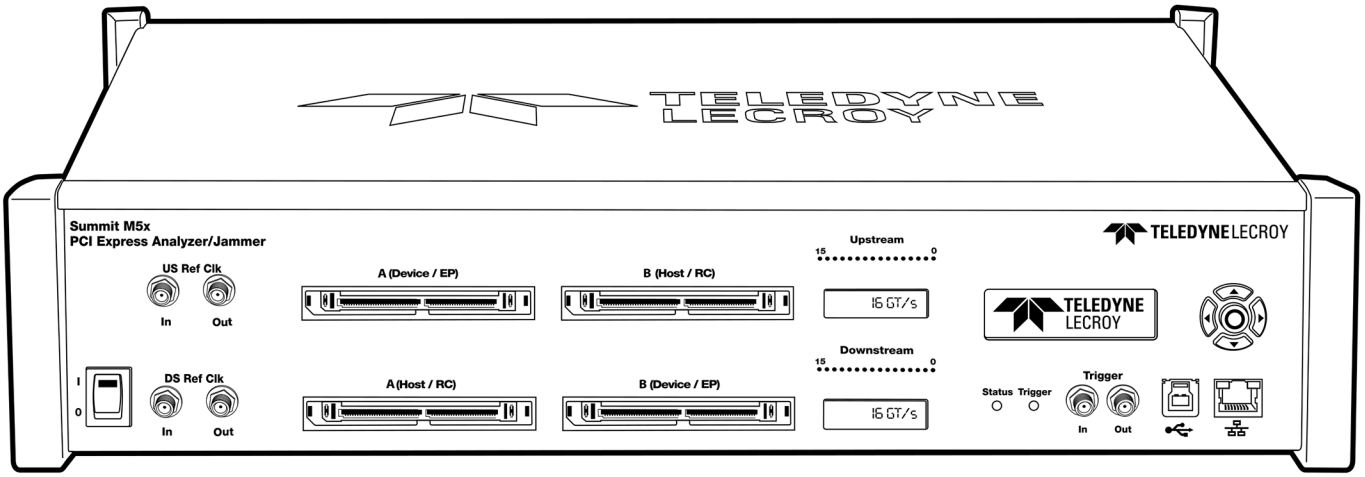


Figure 2.1: Summit M5x: Front Panel

WARNING: Do not open the enclosure. There are no operator serviceable parts inside. Refer servicing to Teledyne LeCroy.

The controls and LEDs are:

- **Power Switch (black)**: 1 = On and 0 = Off. Once the analyzer is powered off you need to wait at least 10 seconds before you power it back on, otherwise the analyzer may not initialize properly.
- **LCD Menus**: Allow you to set up the Summit M5x and view status.
- **LCD Menu Navigation Buttons**: Allow you to navigate through the LCD menu.
- **Speed Display**: Indicate the current speed for the Upstream and Downstream link.
- **Upstream LEDs**: Indicates the activity of the Upstream lanes.
- **Downstream LEDs**: Indicates the activity of the Downstream lanes.
- **UPSTREAM [15:0] Host and Device connectors**: Connection to the probe cards for the capture of upstream direction of the link.
- **US Ref Clk In:** Upstream Reference Clock Input SMA.
- **DOWNSTREAM [15:0] Host and Device connectors**: Connection to the probe cards for the capture of downstream direction of the link.
- **DS Ref Clk In:** Downstream Reference Clock Input SMA.
- **Trigger**:
  - **In** for SMA external trigger input.
    - Trigger Input has a 1.5 kohm pullup resistor to 3.3 volts and a 50 ohm RC termination.
    - Threshold voltage for Trigger Input is 0.55 volts.

- Voltages below 0.4 volts will be detected as low, voltages above 0.7 volts will be detected as high.
- The minimal pulse width is 70ns for rising pulses and 20us for falling pulses.
- When Internal Triggering option is selected in the recording options, any edge of this signal will cause the analyzer to trigger.

■ **Out** for SMA external trigger output.

- Output buffer is 3.3 volts. The buffer can drive up to 32 mA of current and meet VOH (2.5 V) and VOL (0.5 V) thresholds.
- Output buffer can drive a 50 ohm DC load (such as scope input).

❑ **USB**: USB Type B connector for connection to host machine.

❑ **ETHERNET**: Gigabit Ethernet connector for connection to a host machine.

2.5 Status and Config Display (Summit M5x)

The Summit M5x Analyzer/Jammer has a front panel LCD display which indicate the configuration and status of the device. For example, during initialization, the LCD panel displays boot status messages. See Figure 2.1.

2.5.1 LCD Display and Button Functions for Analyzer Host Connection Setup

The host connection settings of the Summit M5x can be configured from the unit itself. Five buttons are provided to navigate menus and input settings presented on the LCD display. When you first turn on the Analyzer, after initialization, the LCD displays **Summit M5x Available** with two arrows pointing up and down as shown in the illustration below.

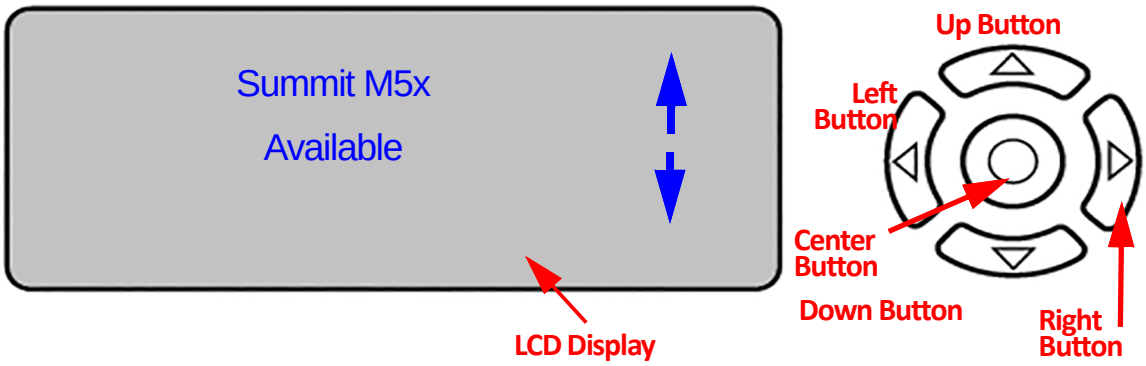


Figure 2.1: LCD Display and Button on the Front Panel

2.5.1.1 Press the Up ⇑ and Down ⇓ buttons to navigate through the following menu items:

❑ Displays current Static or Dynamic IP Address

❑ Summit M5x (serial number)

❑ Connection

❑ Unit Name

❑ Set IP Configuration

- IP Mode Dynamic, or
- IP Mode Static

The **Left** ⟸ and **Right** ⟹ buttons are used to change the configuration properties.

The LCD will display **Button Inactive In This Menu Item** if the button does not serve any purpose for that selection.

Perform the following steps to set IP Configuration, Static on Dynamic IP using the buttons and the LCD display on the Analyzer:

2.5.1.1 Set IP Configuration

After powering on your unit (with the **TELEDYNE** LECROY logo being displayed (TELEDYNELECROY) and after waiting for it to initialize (**Initializing.....**), you can scroll through the LCD Menu display by pressing the **Down Button**:

- Main menu -> IP Address -> **Available** (Unit not in use by other user)

Scroll through the other menus by pressing the **Down Button:**

- Main Menu -> Product Name -> **Serial Number**
- Main Menu -> IP Mode -> **Dynamic**
  - The display will show you which IP Configuration mode your product is currently in: Dynamic or Static. In this case it is in Dynamic IP Address Mode
- Main Menu -> **Set IP Configuration**
  - From this menu you can change the IP Configuration from Dynamic to Static or from Static to Dynamic
- Main menu -> IP Address -> **Available** (Unit not in use by other user)

2.1.4.1 Changing from Dynamic to Static IP Mode

If your unit is in Dynamic IP Mode (factory default) you can change it to Static IP Mode and manually set the IP Address by following the steps below:

To set a Static IP Address:

1. After initialization, press the **Down Button** to ensure your unit is in **Dynamic IP Mode**.
2. Press the **Down Button** until you see the **Set IP Configuration.**
3. Press the **Center Button** once to select **Set IP Configuration.**

   Set IP Mode -> Static is displayed in the LCD display.
4. Press the **Center Button** once to select **Set IP Mode Static.**

   The **Static IP** address (for example: 188.168.040.036) is displayed in the LCD display.
5. Press the **Center Button** once to set the **Static IP address.**

   The first numeral of the IP address will have a arrow below it pointing to it.
6. Use the **Up Button** or **Down Button** to change the IP Address.

7. Press the **Right Button** or **Left Button** to move to the right or left to change each component of the static or dynamic IP address and change it using step 6.
8. Once the IP Address is selected, press the **Center Button** to set the new **Static IP Address**.
9. The new **Static IP Address** will be displayed.
10. Press the **Up Button** once and "**Accept and Reboot"** will be displayed.
11. Press the **Center Button** and "**Center Button to Confirm Reboot"** will be displayed.
12. If you want the new **Static IP Address** to be stored and your unit to **Reboot** press the **Center Button: Rebooting ..... will be displayed.**

    a. Press any other button and your changes will be cancelled.

12. After **Rebooting** has completed, to check that you are in **Static IP Mode**, just scroll through the Main Menu using the **Down Button.**

2.1.4.2 Changing from Static to Dynamic IP Mode

If your unit is in Static IP Mode you can change it to Dynamic IP Mode, the IP Address will be set automatically by the network using DHCP.

To change from a Static IP address to a Dynamic IP address follow the steps below:

1. Ensure your unit is in Static IP Mode by scrolling through the Menus displayed on the LCD by pressing the down button. Main Menu -> IP Mode -> **Static.**
2. Press the **Down Button** one more time and **Set IP Configuration** should be displayed.
3. Press the **Center Button** once to select **Set IP Configuration.**
   Set IP Mode -> Dynamic should be displayed.
4. Press the **Center Button** once to select **Set IP Mode Dynamic.**
5. "**Accept and Reboot**" should be displayed. Press the **Center Button** once.
6. **"Center Button to Confirm Reboot"** should be displayed.
7. If you want the new Dynamic IP Address to be stored and your unit to Reboot press the **Center Button: Rebooting ..... will be displayed.**

   Press any other button and your changes will be canceled.
8. To check that you are in Dynamic IP Mode, just scroll through the Main Menu using the **Down Button**.

Note: In case the device is often moved from one subnet to the other, it is recommended to set the IP Mode to Dynamic and to configure the DHCP server so that the device always receives the same (known) IP address. Many DHCP servers allow this type of static allocation based on the device's MAC address.

2.1.4.3 Setting the Gateway and Subnet Mask

Note: Setting the Gateway and Subnet Mask require a detailed knowledge of your network.

1. Ensure that you are in Static IP Mode by following the steps in "Set IP Configuration" on page 33 and "Changing from Dynamic to Static IP Mode" on page 33 if necessary.
2. Press the **Down Button** to get to the **Set IP Configuration** Menu.
3. Press the **Center Button** and then the **Down Button** to get to the **Set IP Mode Static** Menu.
4. Press the **Center Button** once and then press the **Down Button** to get to the **Subnet Mask** Menu.
5. To set the **Subnet Mask**: Press the **Center Button** and the first numeral of the **Subnet Mask** will have a arrow below it pointing to it.
6. Use the **Up Button** or **Down Button** to change the **Subnet Mask**.
7. Press the **Right Button** or **Left Button** to move to the right or left to change each component of the **Subnet Mask** and change it using step 6.
8. Once the **Subnet Mask** is selected, press the **Center Button** to set and display the new **Subnet Mask**.
9. The press the **Down Button** to get to the **Gateway Address** Menu.
10. To set the **Gateway Address**: Press the **Center Button** and the first numeral of the **Gateway Address** will have a arrow below it pointing to it.
11. Use the **Up Button** or **Down Button** to change the **Gateway Address**.
12. Press the **Right Button** or **Left Button** to move to the right or left to change each component of the **Gateway Address** and change it using step 11.
13. Once the **Gateway Address** is selected, press the **Center Button** to set and display the new **Gateway Address**.
14. Press the **Up Button** to confirm the **Subnet Mask** and then press the **Up Button** to confirm the **Static IP Address.**
15. Press the **Up Button** one more time to display **"Accept and Reboot".**
16. Press the **Center Button** once and the LCD display will read "**Center Button to Confirm Reboot".**
17. If you want the new **Subnet Mask, Gateway Address** and **Static IP Address** to be stored and your unit to Reboot press the **Center Button: Rebooting ..... will be displayed.**
18. Press any other button and your changes will be canceled.

2.6 Summit M5x Rear Panel Description

The Summit M5x rear panel contains the following connectors:

- Wide-range **AC Connector** Module
  - Power socket
  - Enclosed 5.0 A 250 V fuse
- **Sync In and Sync Out** connectors which are used to send synchronization and control messages to other Teledyne LeCroy Analyzers. See Figure 2.1.

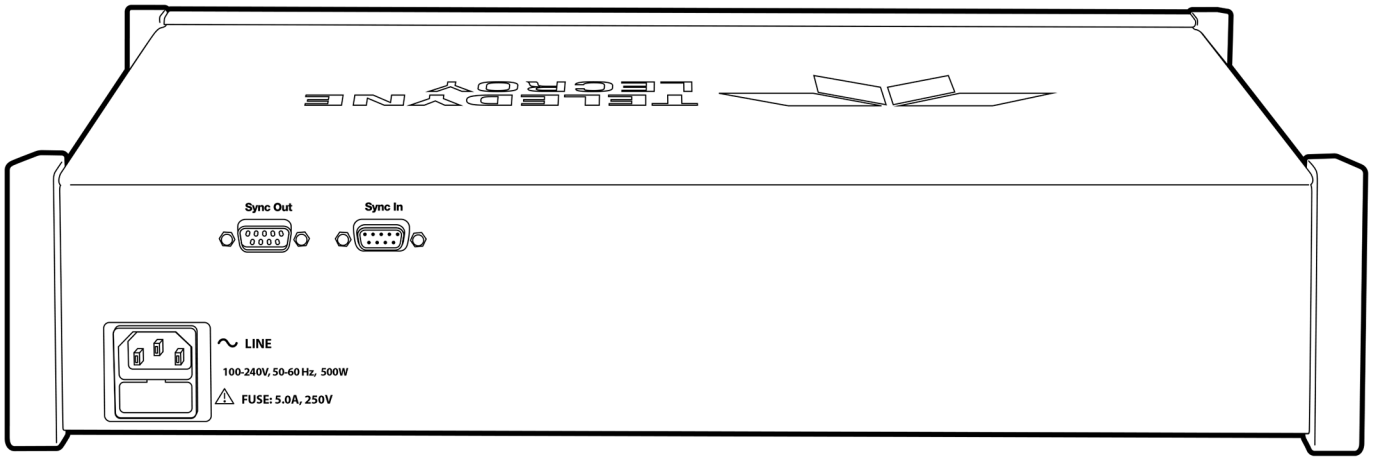


Figure 2.1: Summit M5x: Rear Panel

2.7 Gen4 Host and Device Probe Cards (Analyzer/Jammer Mode)

The Summit M5x works with the PCI Express Gen4 Host and Device Probe Cards.

- **Gen4 Host and Device Probe Cards (x16 or x8)**:
  The Teledyne LeCroy PCI Express 4.0 Host and Device Probe Cards plug in to a PCIe Host CEM Connector and allows you to probe PCI Express traffic between a host and a PCIe expansion card. The Gen4 Host and Device cards support data rates of 2.5 GT/s, 5.0 GT/s, 8.0 GT/s and 16.0 GT/s, and depending on the version purchased link widths up to x16.

2.7.1 Using Gen4 Host and Device Probe Cards

The Gen4 Host Probe Card and Gen4 Device Probe Card connecting to a Summit M5x analyzer is discussed in more detail in the M5x PCIe Gen4 Host and Device Probe Cards Quick Start Guide. See interconnect diagram below (see Figure 2.1).

Gen4 Host and Device Probe Card Interconnection Overview with Summit M5x Analyzer

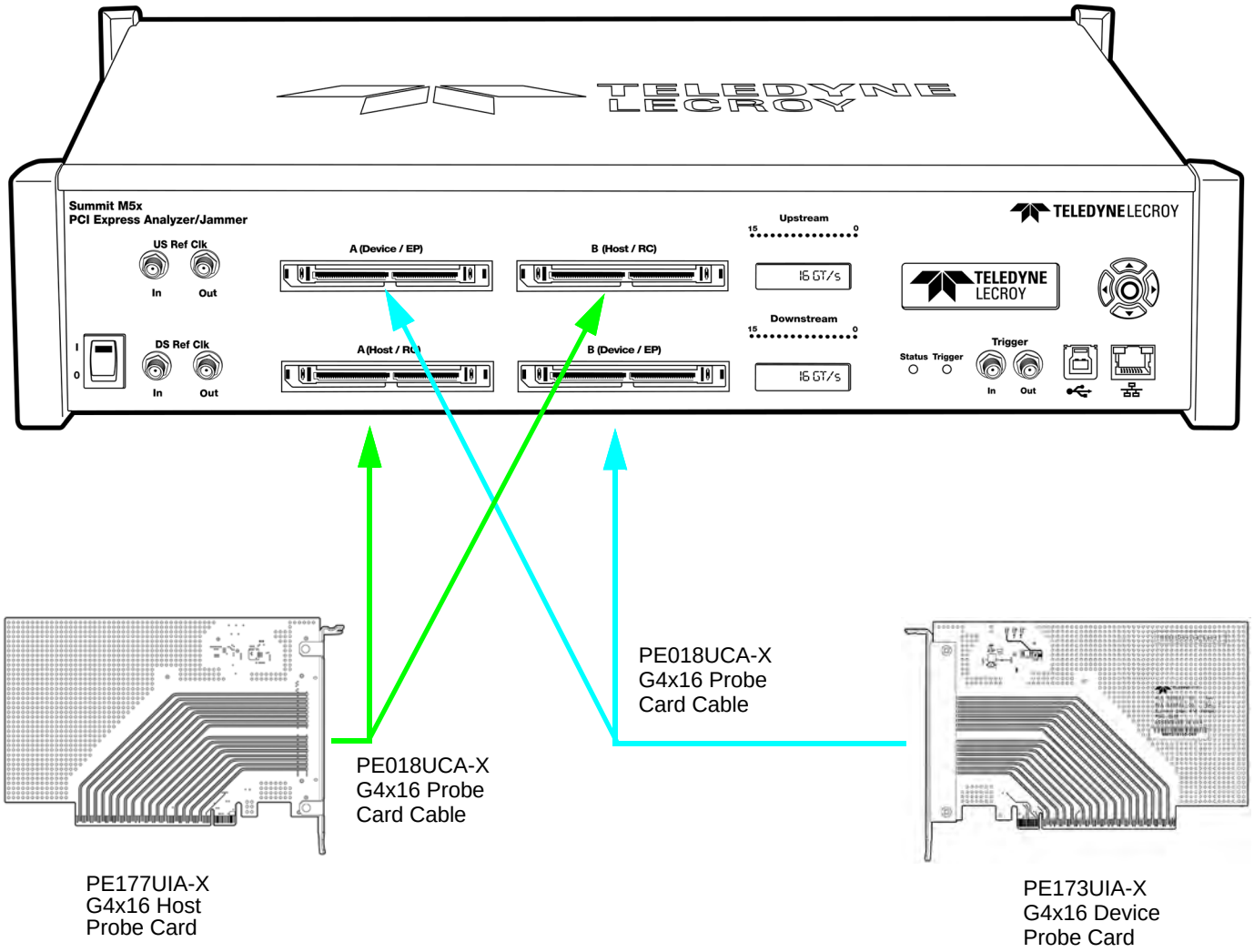


Figure 2.1: Summit M5x Connected to Gen4 Host and Device Probe Cards

2.8 Interposers (Analyzer Mode only)

The Summit M5x works with the PCI Express Gen5 x8 Slot Interposer Card.

- **Gen5 Slot Interposer**:
  The Teledyne LeCroy PCI Express 5.0 Slot Interposer for Summit M5x plugs in to a PCIe® CEM Connector and allows you to probe PCI Express 5.0 traffic between a host and a PCIe expansion card. The Gen5 Interposer supports data rates of 2.5 GT/s, 5.0 GT/s, 8.0 GT/s, 16.0 GT/s and 32.0 GT/s and link widths up to x8. The PCIe connector on the top of the card will support PCIe expansion cards up to x16. A x16 DUT card can be inserted on the top connector and the connection will automatically negotiate to the lesser link width.

2.8.1 Gen5 Slot Interposer (passive)

The Gen5 Slot Interposer (passive) connecting to a Summit M5x analyzer is discussed in more detail in the PCIe Gen5 Slot Interposer Quick Start Guide. See interconnect diagram below (see Figure 2.1 on page 39).

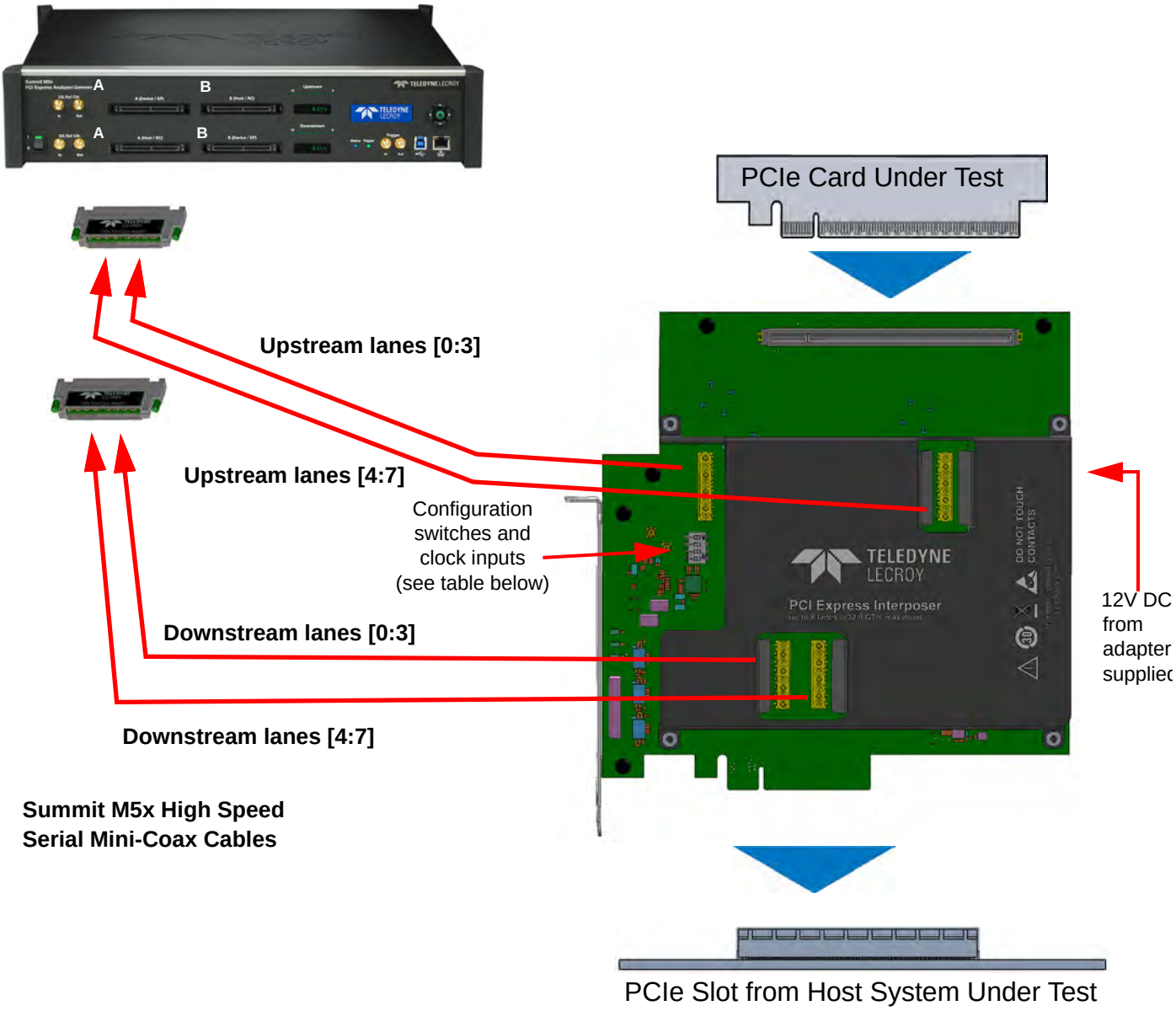


Figure 2.1: Summit M5x Connected to Gen5 Slot Interposer (passive)

2.8.2 Gen5 x8 Interposer

The Gen5 x8 Interposer can be connected to a Summit M5x analyzer. See interconnect diagram below (see Figure 2.1).

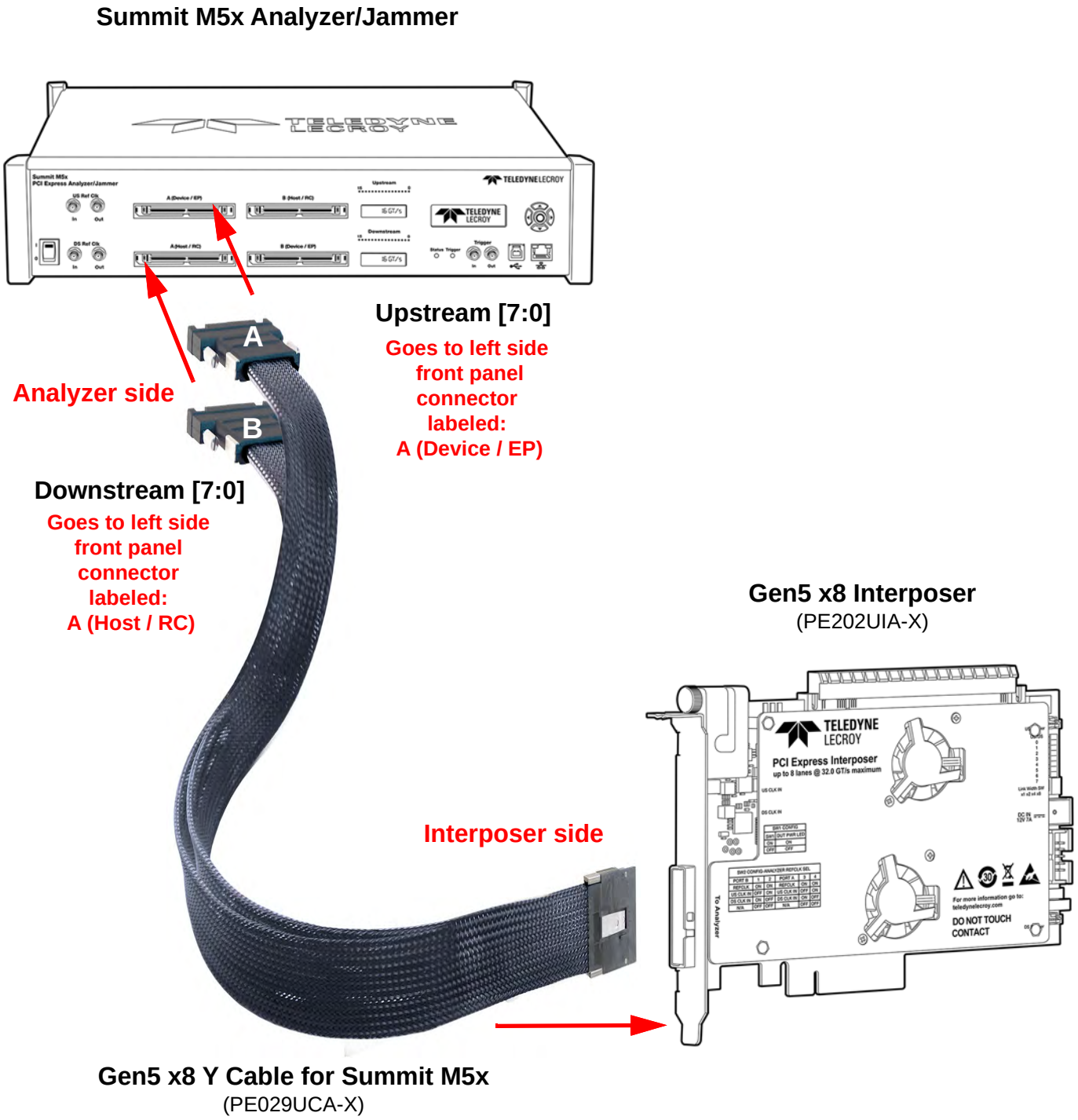


Figure 2.1: Connection diagram for single port up to x8 to Summit M5x

2.8.3 Gen5 x16 Interposer

Connect the Summit M5x Analyzer to the Gen5 x16 Interposer as shown in Figure 2.1 below.

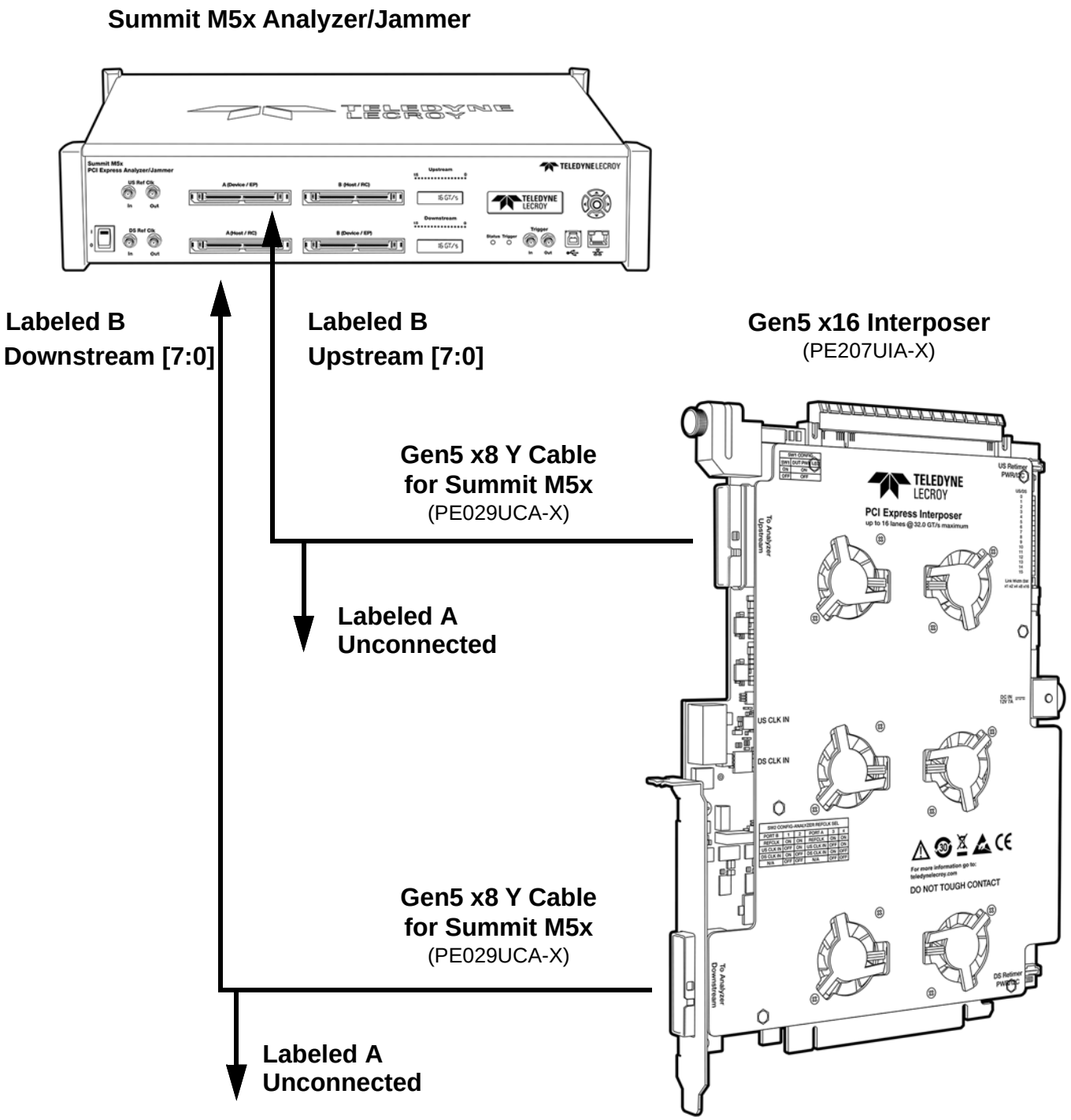


Figure 2.1: Connection diagram for single port up to x8 to Summit M5x with Gen5 x16 Slot Interposer

2.8.4 Gen4 x8 Interposer

Connect the Summit M5x Analyzer to the Gen4 x8 Interposer as shown in Figure 2.1 below.

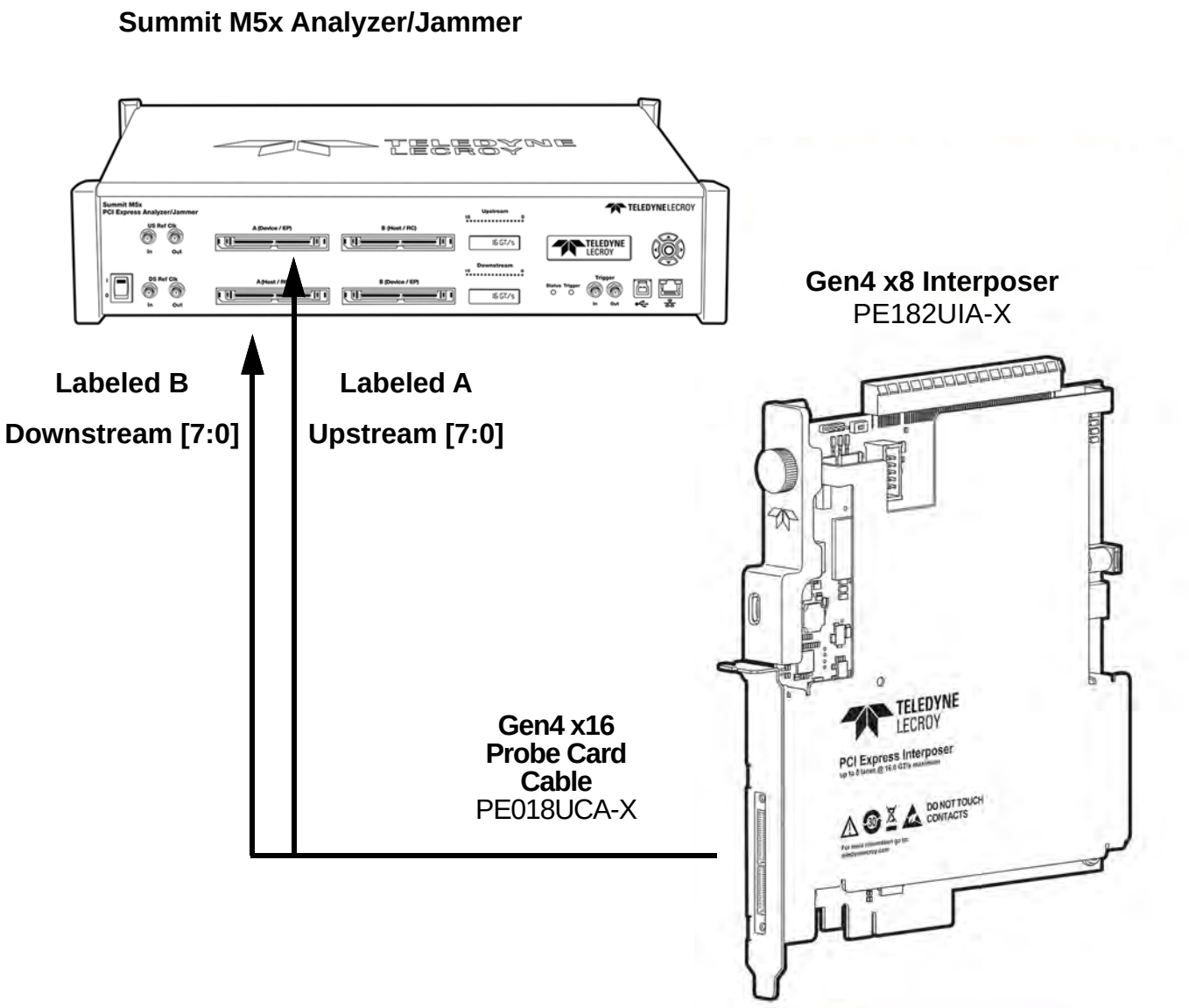


Figure 2.1: Summit M5x connect to Gen4 x8 Interposer using Gen4 x16 Probe Card Cable

The same general interconnection diagram utilizing the Gen4 x16 Probe Card Cable can be used with the following interposers:

- ❑ Gen4 x16 Slot Interposer
- ❑ 90 Deg Server Interposer
- ❑ M.2 MKey Interposer
- ❑ OCP NIC3.0 Interposer

- OCuLink Interposer
- U.2/U.3 Interposer
- RSSD Interposer

Chapter 3

Installation and Setup

The Summit M5x™ is a standalone system.

You can begin PCI Express™ recordings after following the steps in this chapter.

3.1 Installing the PCIe Protocol Analysis software

PCIe Protocol Analysis software operates all of Teledyne LeCroy's PCI Express protocol Analyzer and Exerciser products:

The PCIe Protocol Analysis software is supported on systems using a Microsoft® Windows®-based host machine running Windows Server 2016, Windows Server 2019 and Windows 10 64-bit operating systems and serves as the interface for the Exerciser and/or Analyzer.

3.1.1 Downloading the PCIe Protocol Analysis software

You can download the latest version of the PCIe Protocol Analysis software from the following site:

https://teledynelecroy.com/sw/pciexpress/

Note: First-time user registration is required.

3.1.2 Windows Server 2016/2019

If you are using Windows Server 2016/2019, the Teledyne LeCroy PCIe Protocol Suite needs to be added to the firewall exceptions to ensure that the application can find the analyzers over your Ethernet network.

To add the PCIe Protocol Suite application to the firewall exceptions perform the following steps.

1. Open the Control Panel. See Figure 3.1 on page 46.

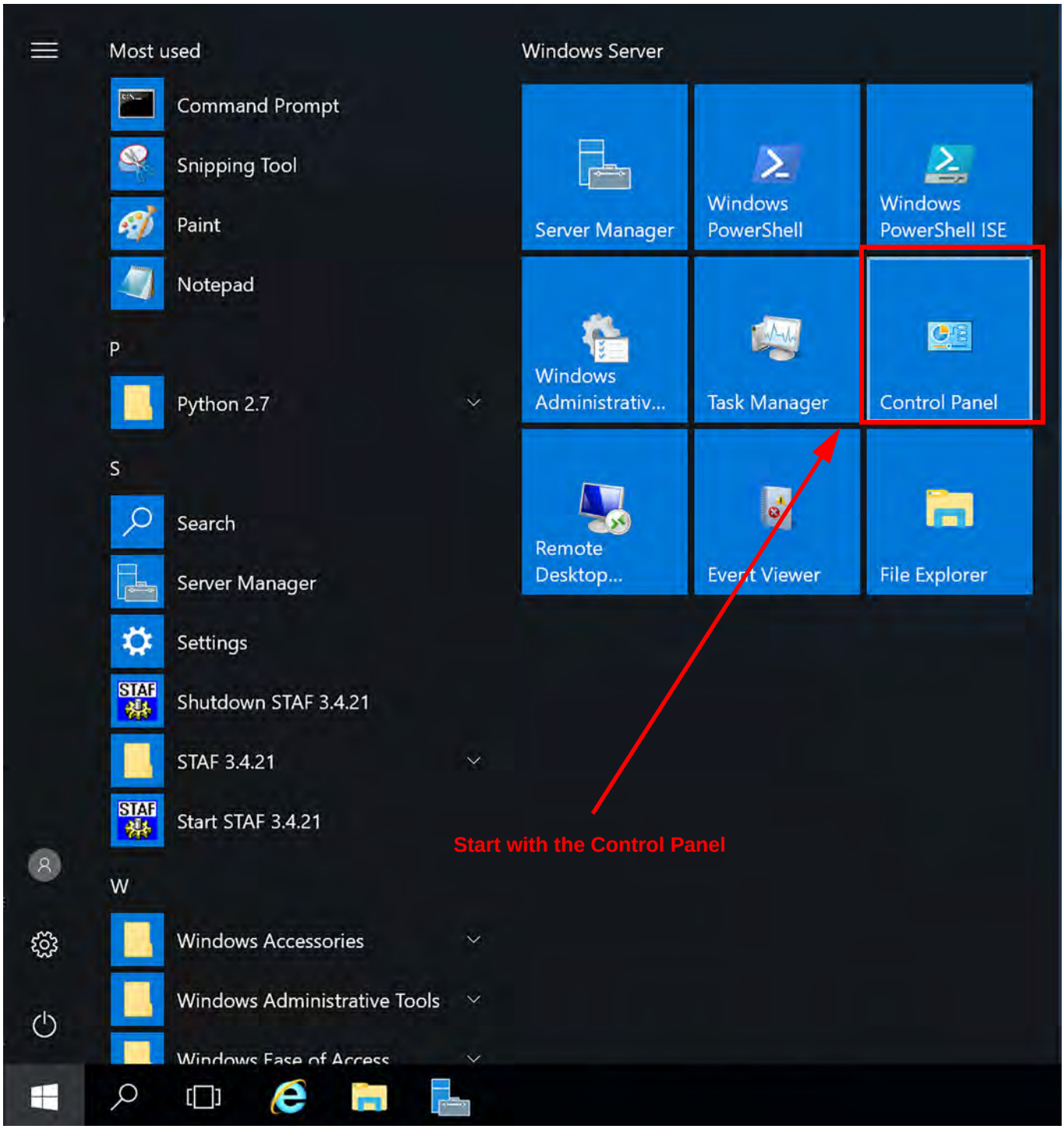


Figure 3.1: Windows Server 2016/2019: Start Menu -> Control Panel

2. From the Control Panel. select the “Systems and Security” screen. See Figure 3.2.

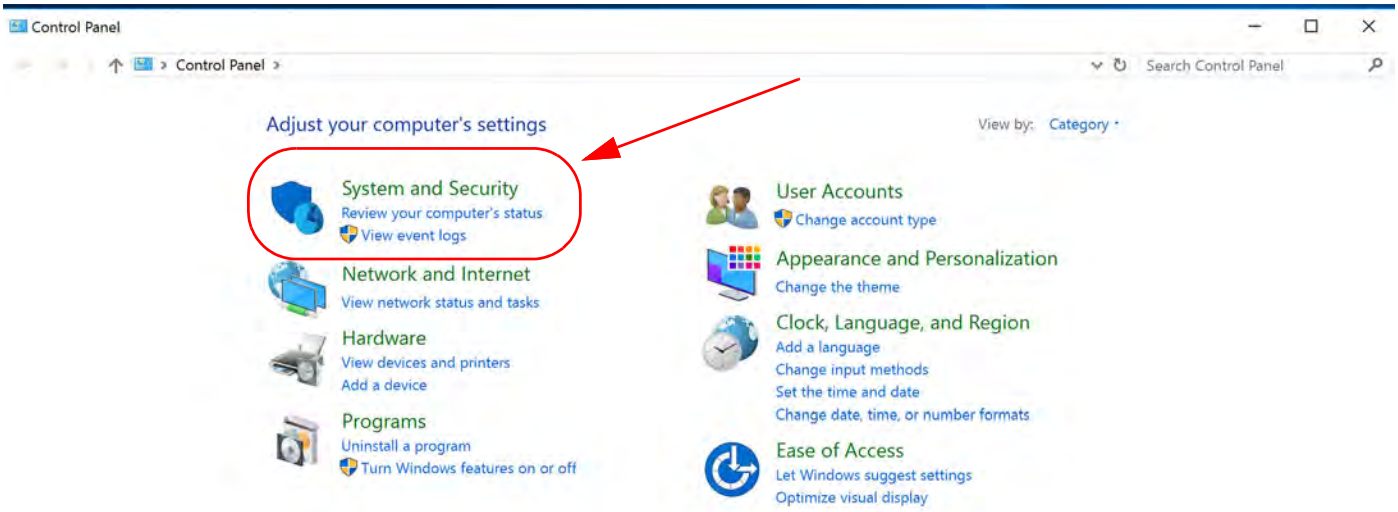


Figure 3.2: Windows Server 2016/2019: Control Panel -> System and Security Screen

3. From the Control Panel -> System and Security Screen, select “Allow an App through Windows Firewall”. See Figure 3.3.

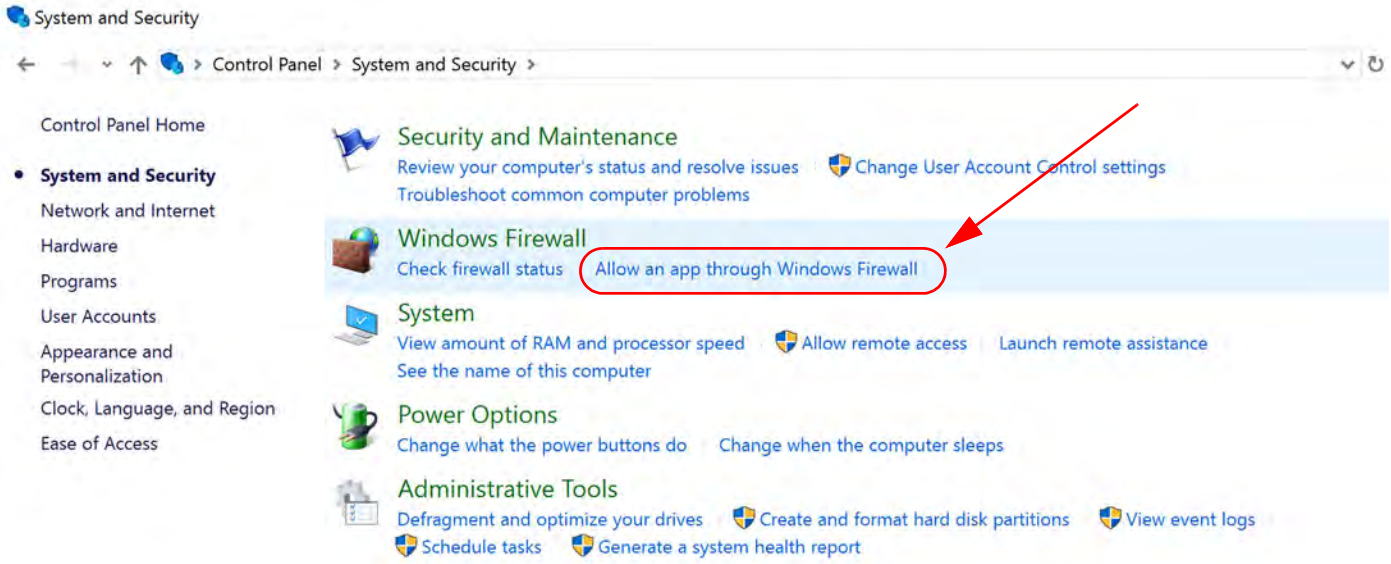


Figure 3.3: Windows Server 2016/2019: Allow an App Through Windows Firewall

4. From the Windows Firewall screen -> Allow apps to communicate through Windows Firewall, select “Change settings”, then select “Allow another program”. See Figure 3.4.

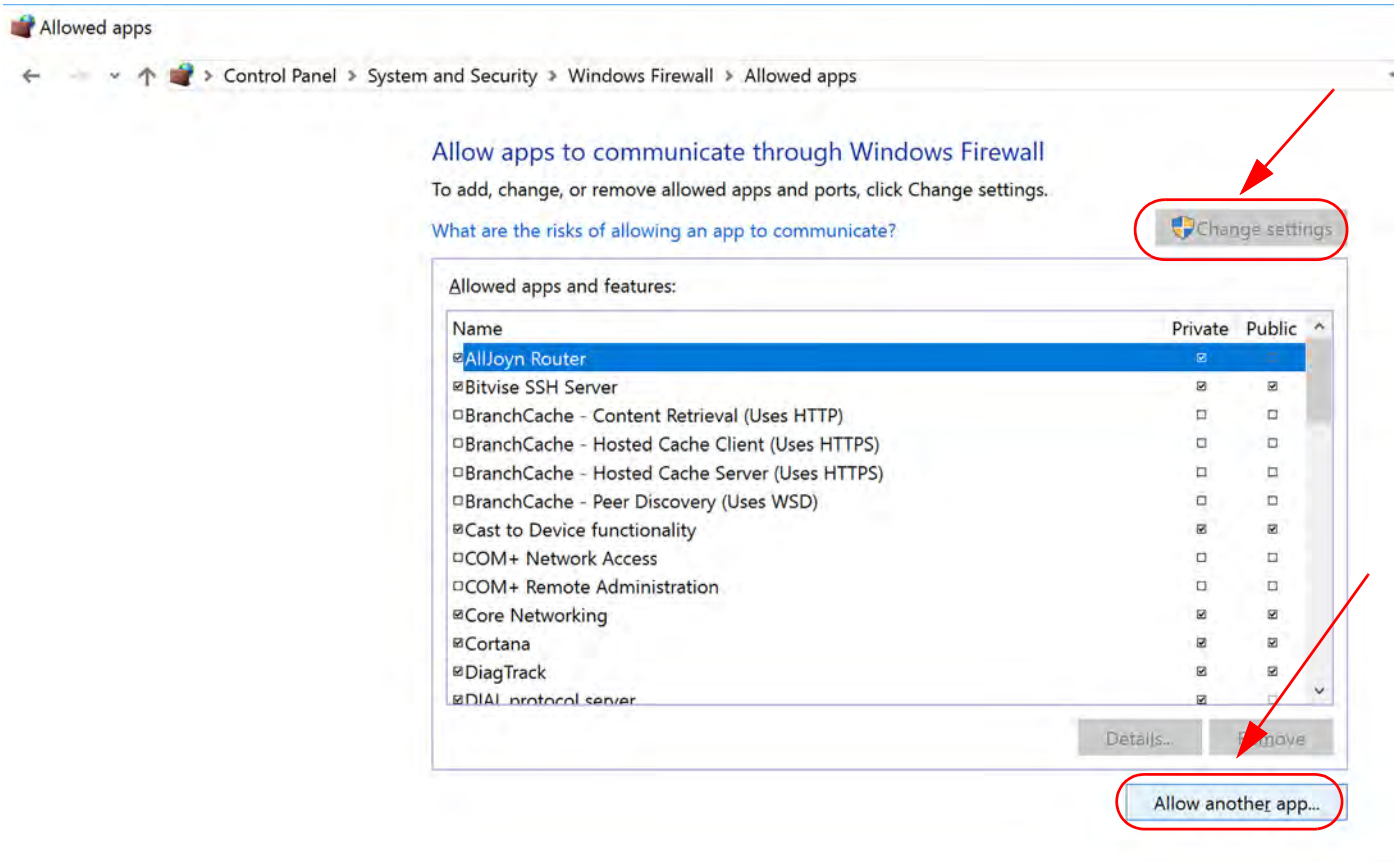


Figure 3.4: Windows Server 2016/2019: Change Settings -> Allowed Another app

5. From the User Account Control screen, select “Yes”. Figure 3.5.

Note: This screen may be optional if you have already allowed Microsoft Windows to make changes to your computer.

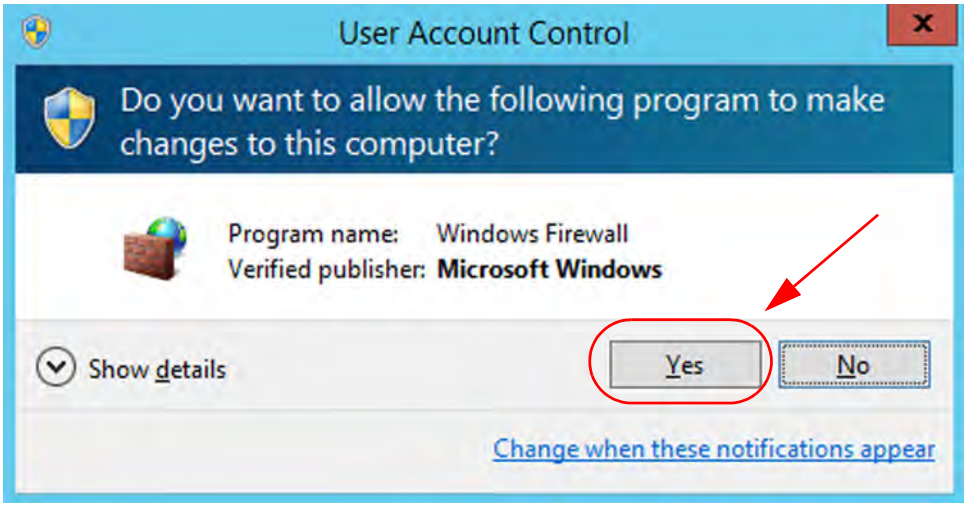


Figure 3.5: Windows Server 2016/2019: User Account Control

6. From the “Add an app” screen, select the Browse button. See Figure 3.6.

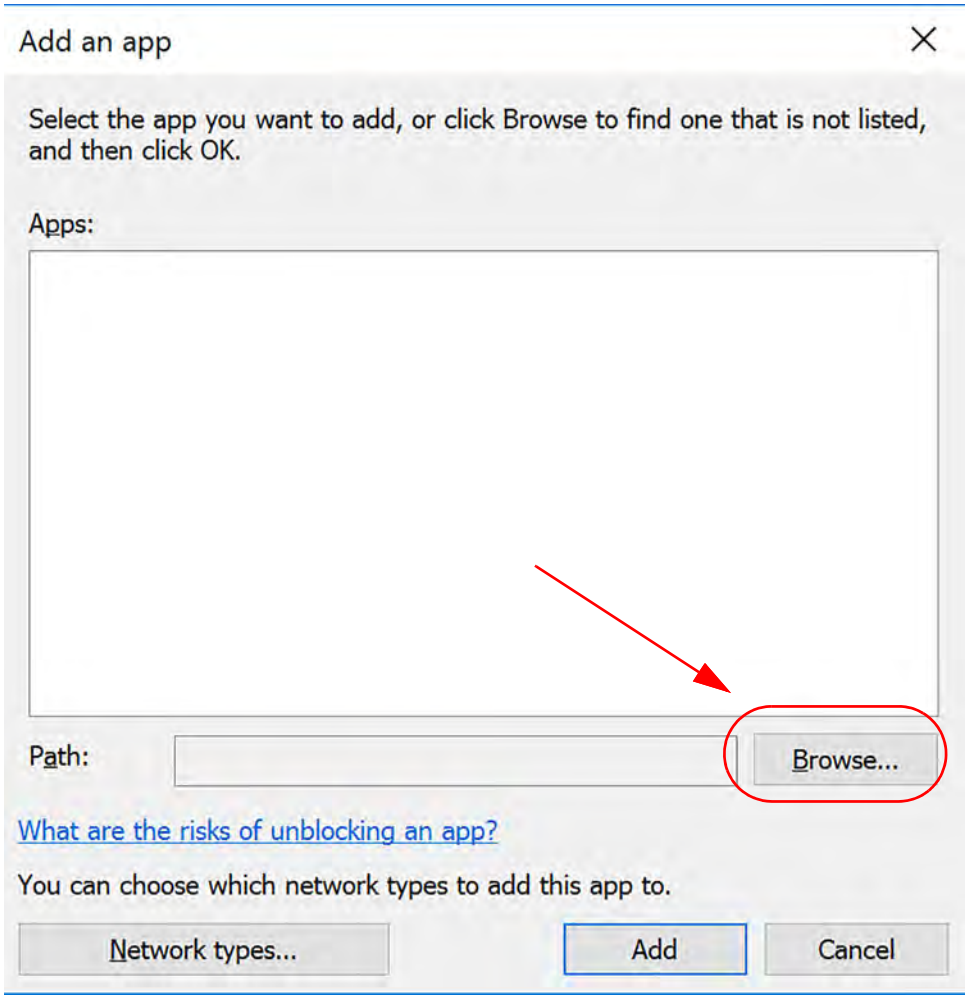


Figure 3.6: Windows Server 2016/2019: Add an App

7. In the Browse window navigate to the location of the installation directory for the PCIe Protocol Suite you are installing. The Teledyne LeCroy PCIe Protocol Suite is typically installed on your machine in the C:\Program Files\LeCroy\PCIe Protocol Suite directory. See Figure 3.7.

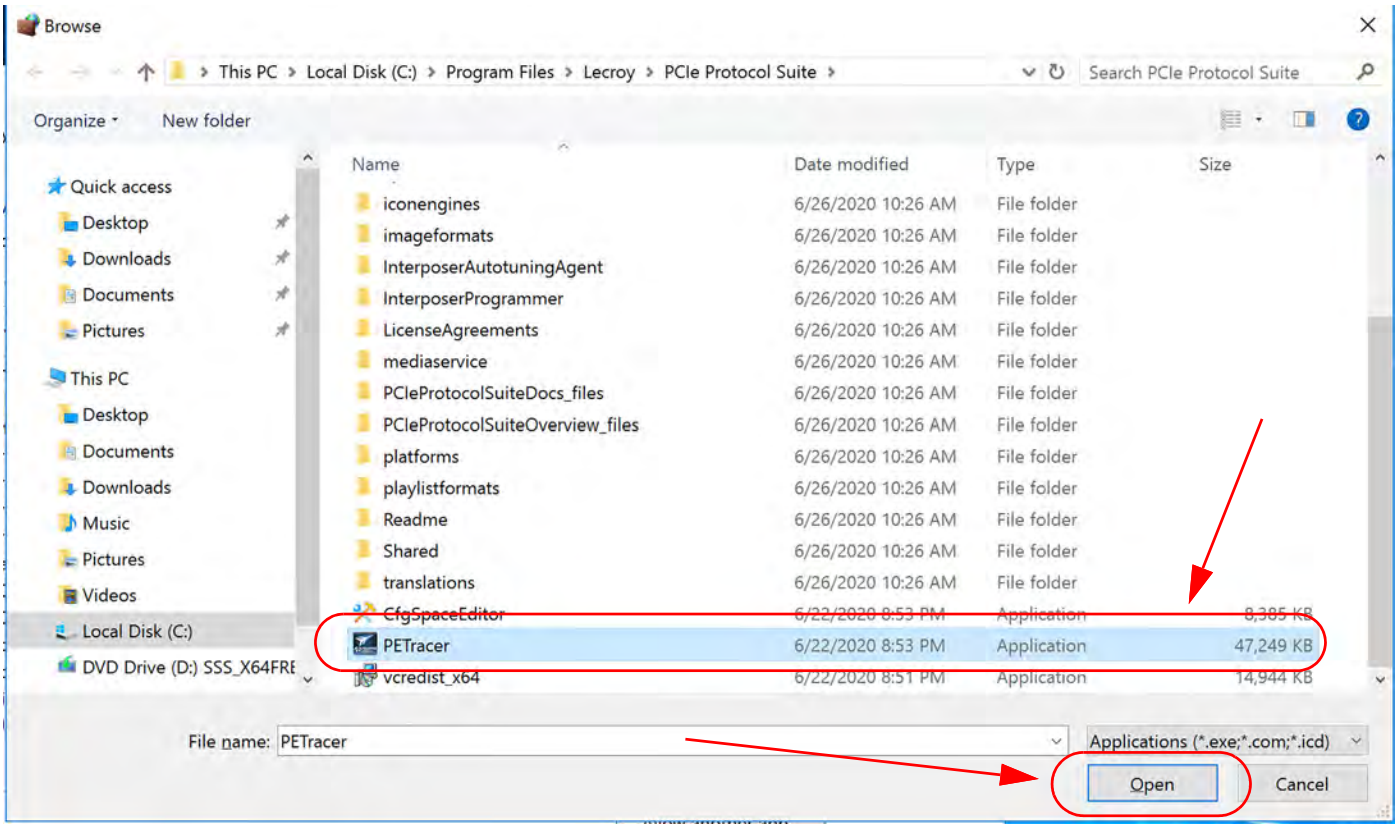


Figure 3.7: Windows Server 2016/2019: Browse to Find Application -> PCIe Protocol Analysis Application

8. Select the PCIe Protocol Analysis executable file (with the .exe extension) and click on “Open”.

9. If necessary, select the Teledyne LeCroy PCIe Protocol Suite you want to add. Then click on “ADD”, this will add the Teledyne LeCroy PCIe Protocol Suite to the Apps allowed through the Firewall. See Figure 3.8.

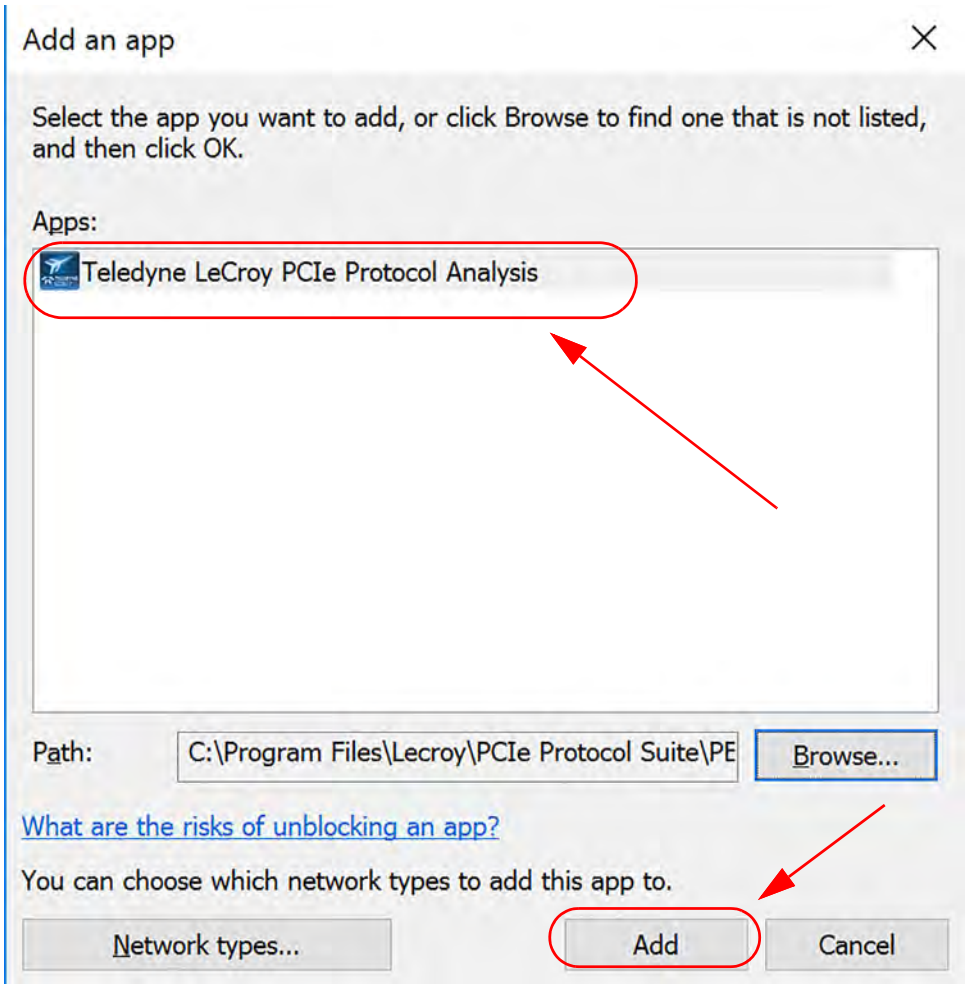


Figure 3.8: Windows Server 2016/2019: Add an Application to the Firewall Exceptions

10. After the Application has been added, you can see it in the “Allow apps to communicate through Windows Firewall” screen. See Figure 3.9.

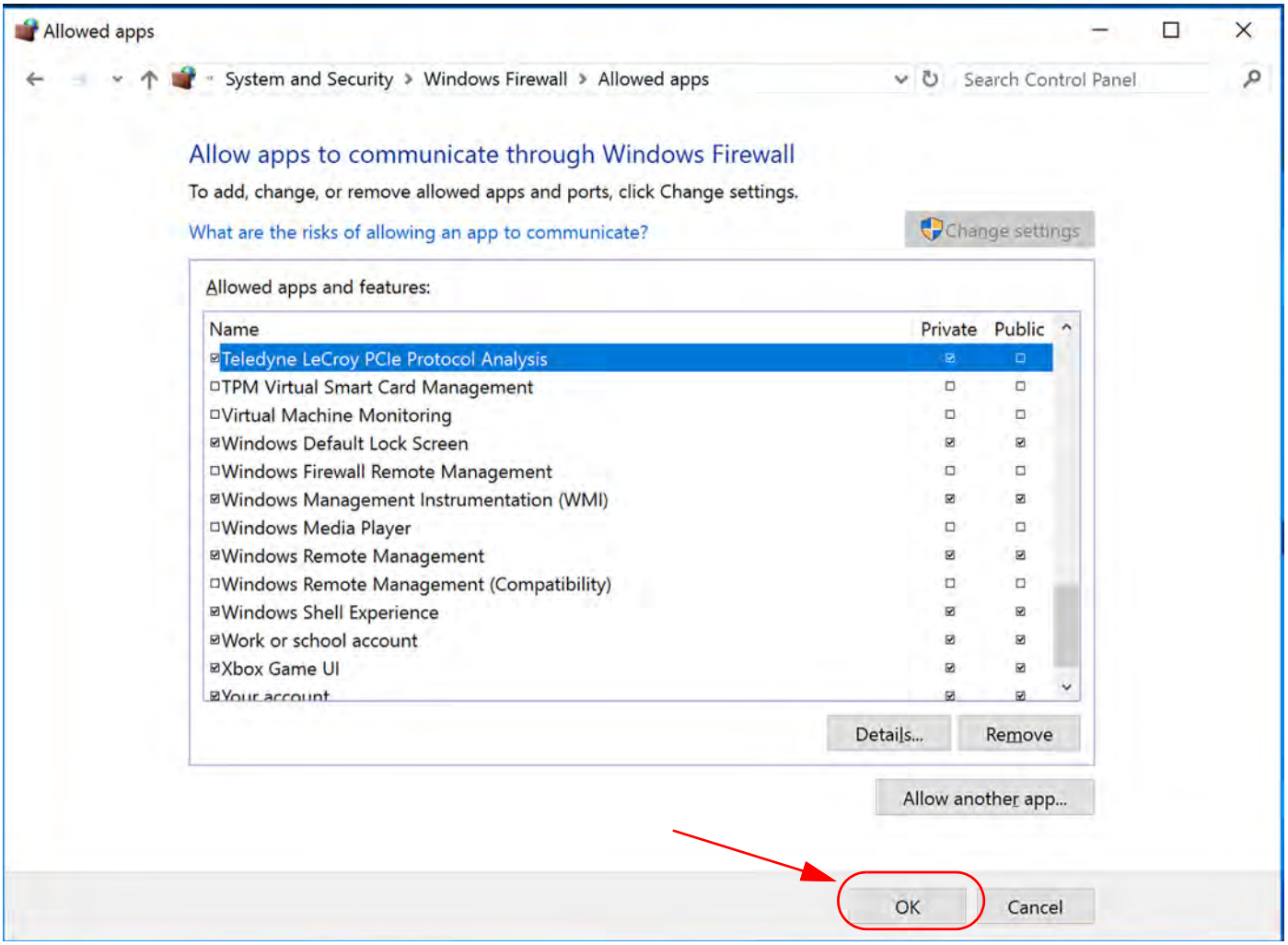


Figure 3.9: Windows Server 2016/2019: Add Teledyne LeCroy PCIe Protocol Suite to Allowed Applications

Click “**OK**” and you’re done with updating the Firewall.

3.1.3 Launching the PCIe Protocol Analysis

To start the application, launch the PCIe Protocol Analysis program from the Start menu:
Start > All Apps > LeCroy > PCIe Protocol Suite

Note: The above path is for Windows 10, the path may be different for other versions of Wndows.

The PCIe Protocol Analysis program displays, as seen below. See Figure 3.10.

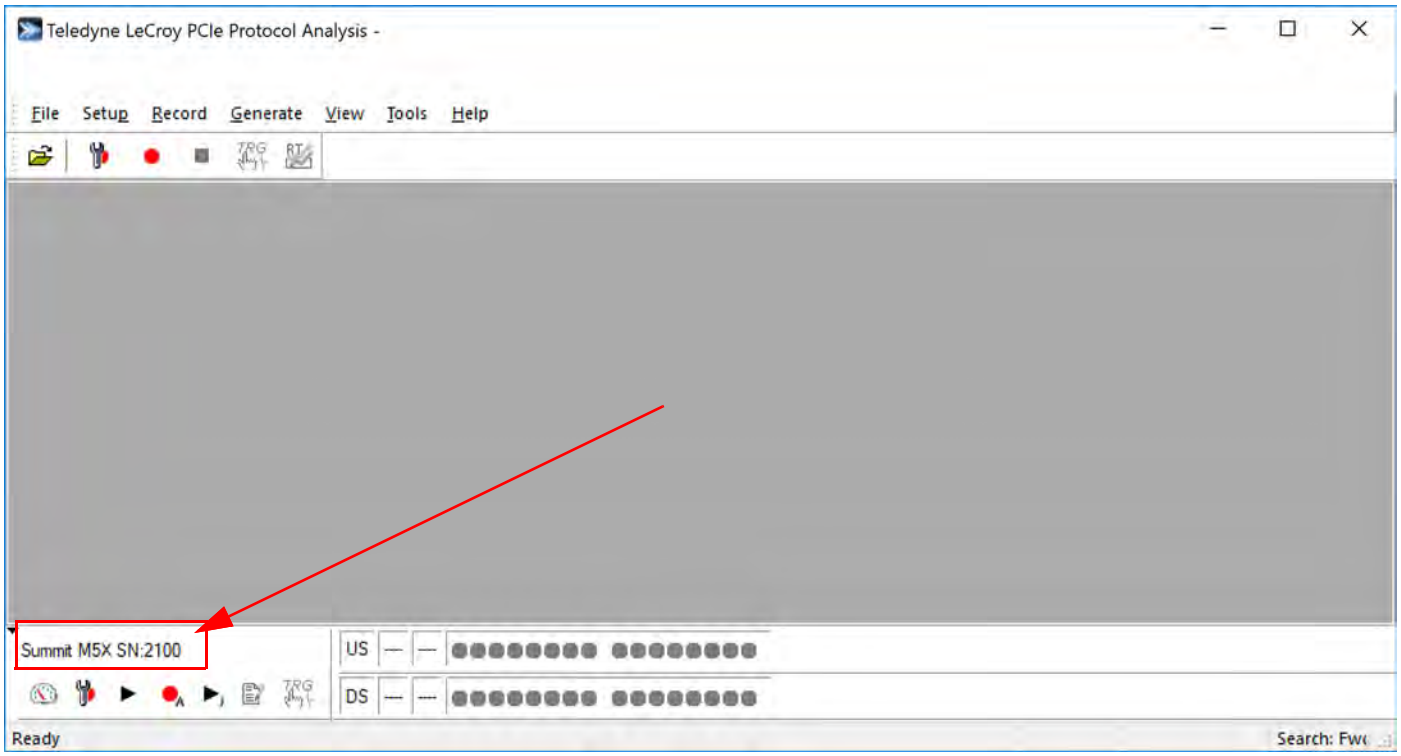


Figure 3.10: Teledyne LeCroy PCIe Protocol Analysis Application

Note: The image above shows the application with a Summit M5x attached. The software may be used with or without the Analyzer. When used without an Analyzer attached to the computer, the program functions as a CATC Trace Viewer to view, analyze and print captured traffic.

3.2 Setting Up the Summit M5x Analyzer/Jammer using a USB Connection

To set up the Analyzer using a USB connection:

1. Connect the Analyzer to a 100-volt to 240-volt, 50 Hz to 60 Hz, 120 W power outlet using the provided power cord.
2. Connect the USB port to a USB port on the host machine using a USB cable.

Note: To connect using Ethernet, see "Setting Up the Summit M5x Analyzer/Jammer using an Ethernet Connection" on page 57.

3. Turn on the front power switch.

Note: At power-on, the Analyzer initializes itself in approximately five seconds and performs an exhaustive self-diagnostic that lasts about forty seconds. The results are reflected by messages on the Summit M5x LCD display. If the LCD display indicates failure, call Teledyne LeCroy Customer Support for assistance.

4. Follow the Microsoft® Windows® on-screen Plug-and-Play instructions for the automatic installation of the Analyzer as a USB device on your analyzing host machine. (The required USB drivers are installed on your system by the PCIe Protocol Analysis installation.)

   Click **Finish** when you see the message that says "Windows has finished installing the software that your new hardware requires" and the file has been installed in your host machine.

3.3 Setting Up the Summit M5x Analyzer/Jammer using an Ethernet Connection

3.3.1 TCP Port Connections for Different Modes

In AJA Mode, AJ Mode and Gen5 Mode the Summit M5x Analyzer/Jammer uses different TCP ports for different configurations. Typical port assignments are shown below.

TABLE 3.1: TCP Port Configurations

Logical Unit	M5x: AJA Mode	M5x: AJ Mode	M5x: Gen5 Mode
Unit 0	4000 – 4003	4000 – 4003	4000 – 4003
Unit 1	N/A	N/A	N/A
Unit 2	4020 – 4023	N/A	N/A
Unit 3	N/A	N/A	N/A

Note: If your PC and the analyzer are both on the same subnet you should have no problem making a DHCP connection. If they are not, you may have to set appropriate subnet and gateway settings. Also, it is best if TCP ports 4000 to 4003 and UDP ports 4012, 4013 and 4014 are available on the network, but even if they are not you may be able to force a connection by checking the "Force add/connect attempt" box.

1. Connect the Analyzer to a 100-volt to 240-volt, 50 Hz to 60 Hz, 120 W power outlet using the provided power cord.
2. Connect the Summit M5x Analyzer/Jammer to the network. The Ethernet port is on the front of the Analyzer.

Note: To connect using USB, see “Setting Up the Summit M5x Analyzer/Jammer using a USB Connection” on page 56.

3. Turn on the front power switch.

Note: At power-on, the Analyzer initializes itself in approximately five seconds and performs an exhaustive self-diagnostic that lasts about forty seconds. The results are reflected by messages on the Summit M5x LCD display. If the LCD display indicates failure, call Teledyne LeCroy Customer Support for assistance.

4. After you have installed the PCIe Protocol Analysis application software, perform the following procedure to connect to a Summit M5x analyzer/jammer in the local network.

   Select the **Setup > All connected devices…** menu in the PCIe Protocol Analysis application to display the Analyzer Devices dialog.

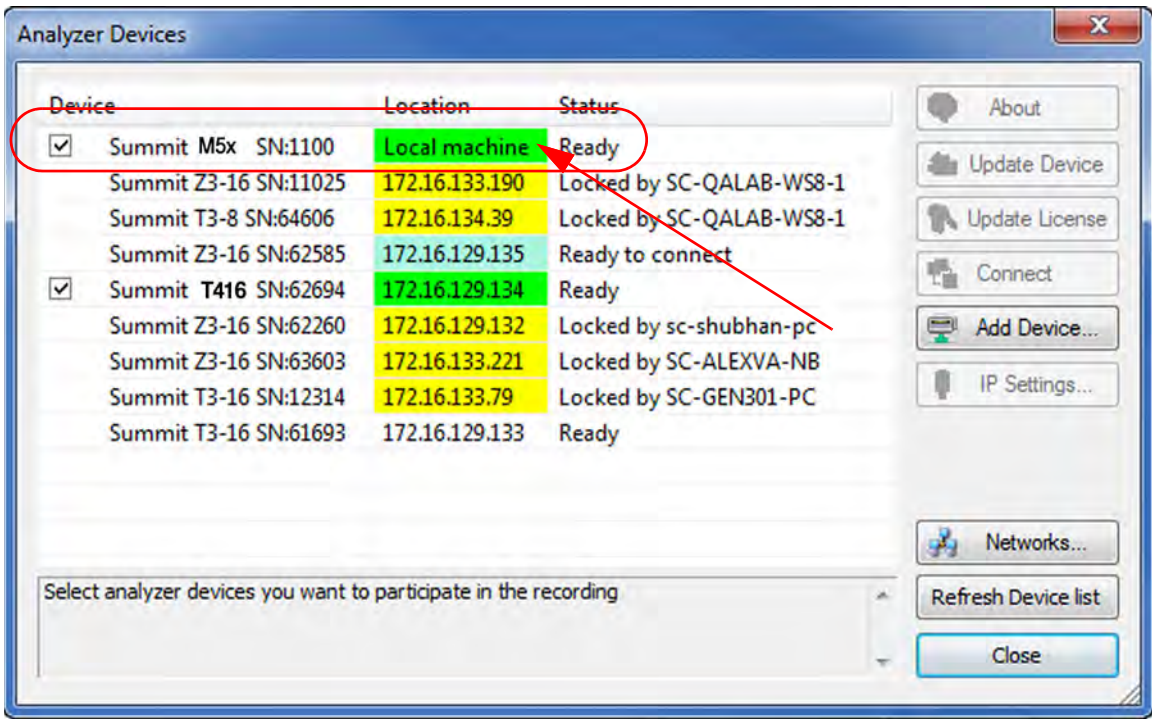


Figure 3.11: Analyzer Devices Dialog

The PCIe Protocol Analysis fills the list with devices that are connected over USB or discovered on the Ethernet network. The discovery mechanism works only within one network subnet. If a Summit is connected to the network on a different subnet, you can manually add the subnet to the list by clicking the **Add Device** button and specifying the IP address.

The Summit devices in the list are marked:

- **Locked**: Some other client on the network is already connected to that device
- **Ready to connect**: Available for connection

1. If a Summit device is marked Ready To Connect, you can select that device and press the **Connect** button to execute the connection procedure.

   After the connection is established, the application displays the Connection Properties dialog.

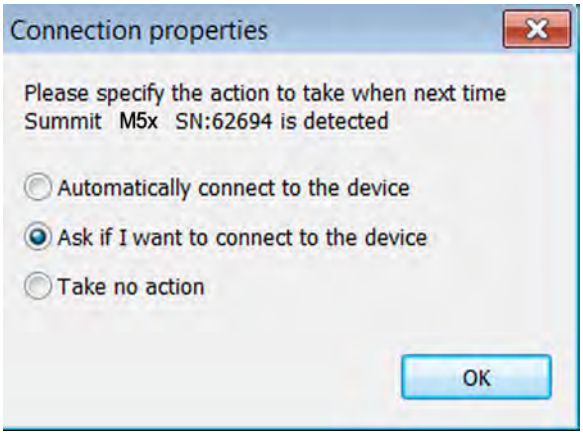


Figure 3.12: Connection Properties Dialog (Summit M5x)

Note: The Connection Properties dialog will show either the Summit M5x detected.

2. Select an option:
   - **Automatically connect to the device**: When the application is started or when the named device is added to the network while the PCIe Protocol Analysis application is running on this computer, the PCIe Protocol Analysis application will try to connect to the named device.
   - **Ask if I want to connect to the device**: When the application is started or when the named device is added to the network while the PCIe Protocol Analysis application is running on this computer, the PCIe Protocol Analysis application will display a message box allowing you to connect to the named device.
   - **Take no action**: When you start the application or when you want to add the named device to the network while the PCIe Protocol Analysis application is running on this computer, you must connect manually to use the named device.

Note: When you close the application on this computer (or you perform a manual disconnect), the application disconnects from the device.

3. Press **OK** in the Connection Properties dialog.

   After you finish the connect procedure, the Summit device to which you have connected is marked as **Ready** and you can use it for recording (see Figure 3.13 and Figure 3.14 on page 61).

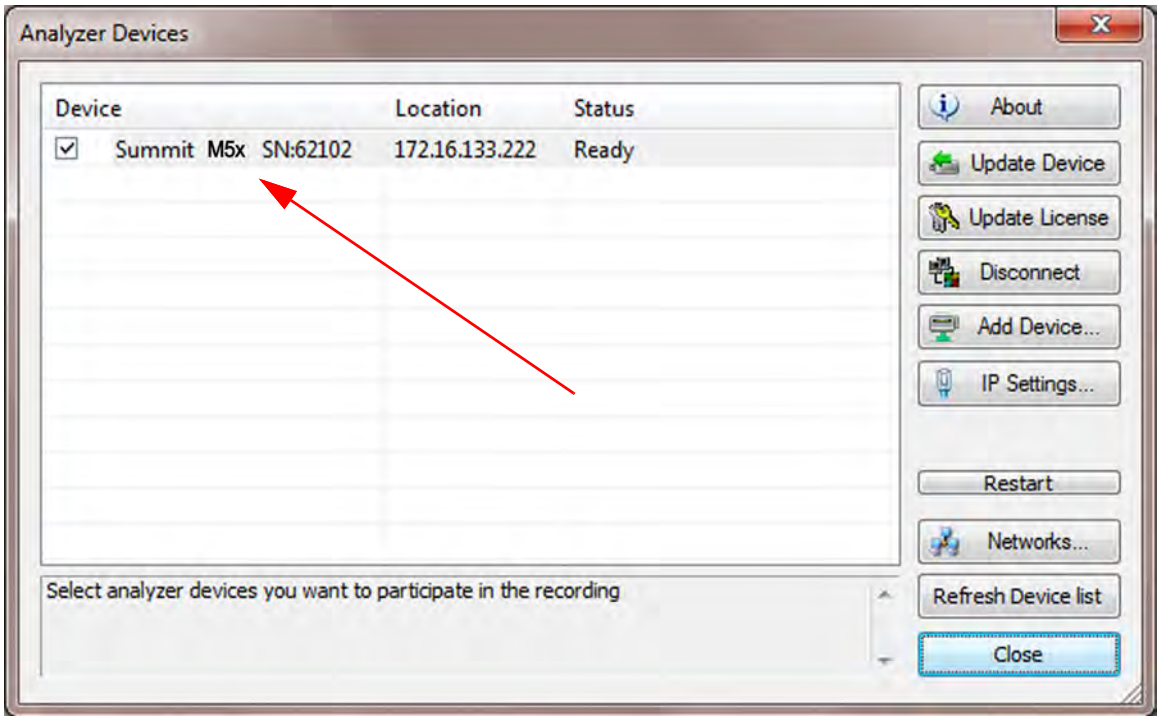


Figure 3.13: Analyzer Devices Dialog (Summit M5x)

Note: To disconnect from a device, display this dialog, select the device, and click the **Disconnect** button.

Note: As of version PCIe Protocol Analysis version 7.34, the software is able to access a Summit analyzer via VPN solutions that require explicit bindings to PPP adapters that they create.

3.4 Adding Devices Manually

You can locate and add a Summit M5x analyzer/jammer located in a Ethernet subnet using the Add Device button. Perform the following steps:

Click **Setup -> All Connected Devices -> Add Device ->** to display the Add Ethernet Attached Device dialog.

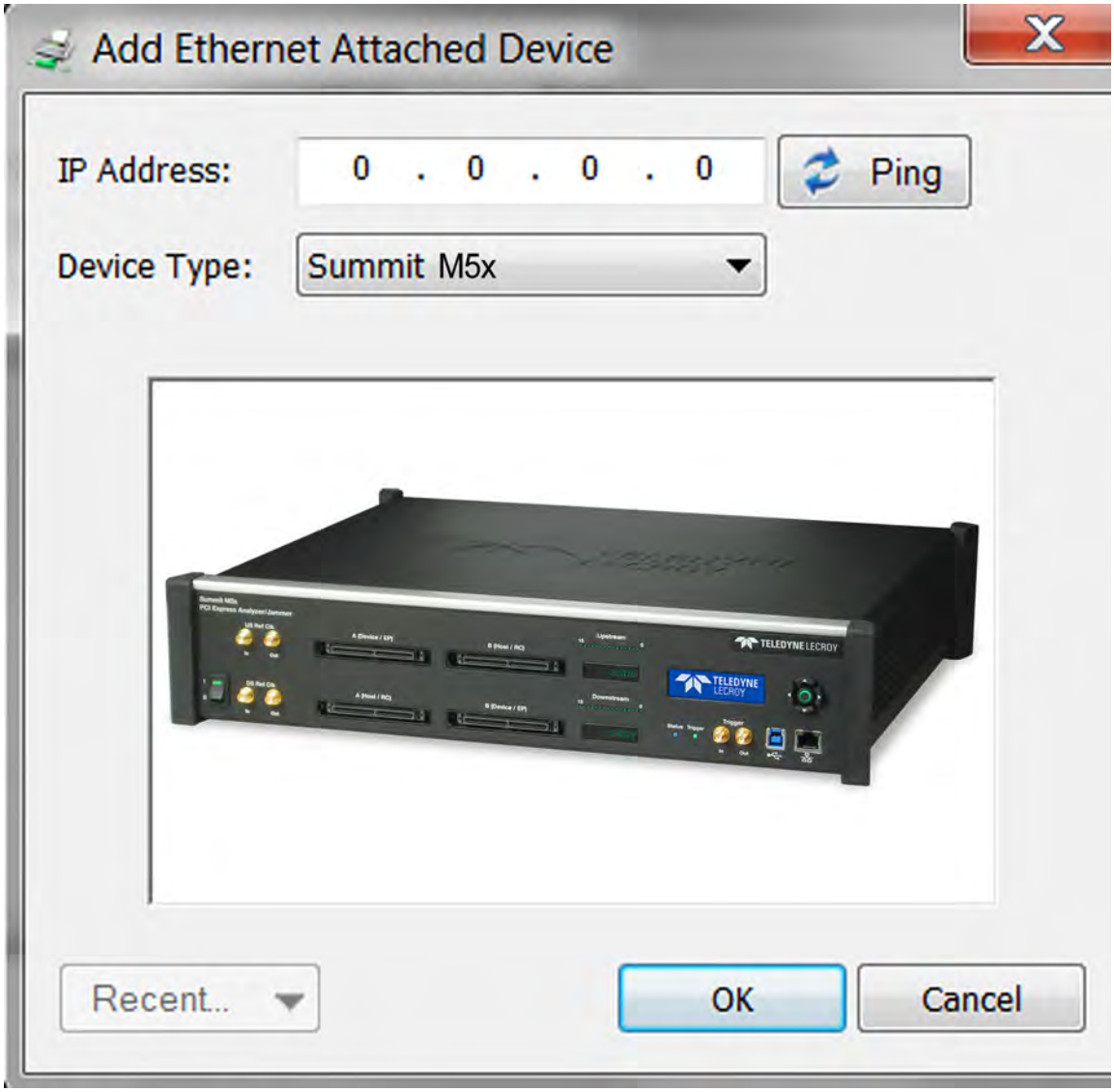


Figure 3.14: Add Ethernet Attached Devices Dialog (Summit M5x)

Click the **Recent** button to display a list of recently added devices (up to 15) and quickly add a recently used device.

Click the **Ping** button to ping a device as a network node (prompting an error message if no response). Ping also allows PCIe Protocol Analysis to detect a device type before actually connecting to the device.

If the "Ping" feature discovers that the device is already connected and "locked" then it will inform the user and provide information about who locked the device.

Click **Setup -> All Connected Devices** to display the Analyzer Devices dialog.

If software fails to connect to a manually added device, a message displays notifying the user about the connection failure. The user is given the option to keep the failed device in the device list, in this case PCIe Protocol Analysis displays a "Failed to connect" status message in gray.

Square brackets for IP addresses are used for manually added devices to easily distinguish them from auto-discovered devices.

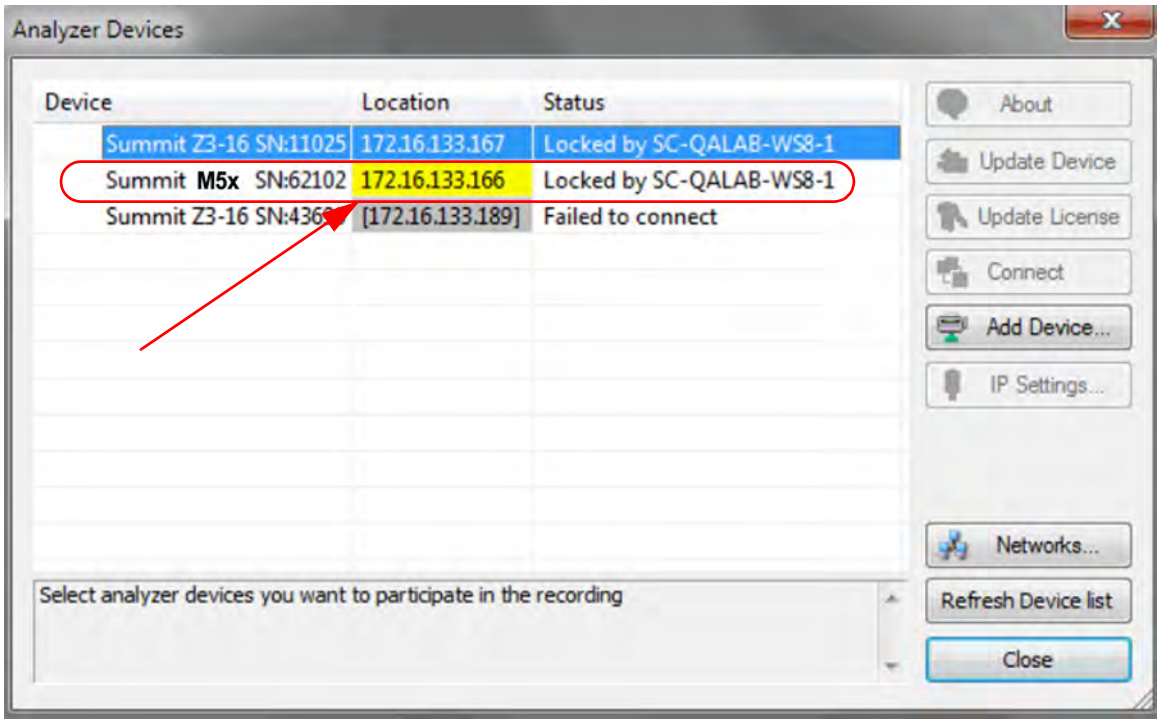


Figure 3.15: Add Ethernet Attached Devices Dialog (Summit M5x)

3.4.1 Adding a Summit M5x to an Ethernet Network

If you have a Summit M5x and want to add it to an Ethernet Network but don't know it's IP address you can find out the IP address and add it to the Ethernet Network using the USB connection.

With the USB cable installed, start up the PCIe Protocol Analysis and select **Setup > All connected Devices.**

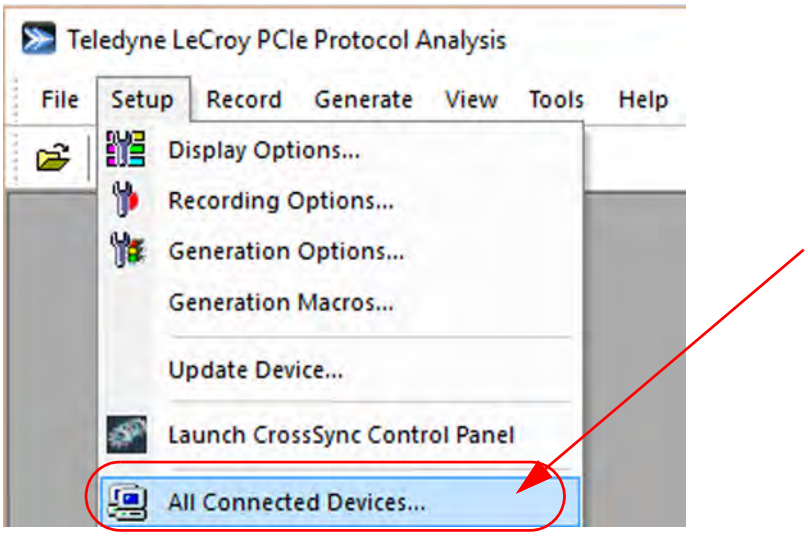


Figure 3.16: Setup > All Connected Devices

This will popup a dialog box showing all the connected devices on your network. See Figure 3.17 on page 64.

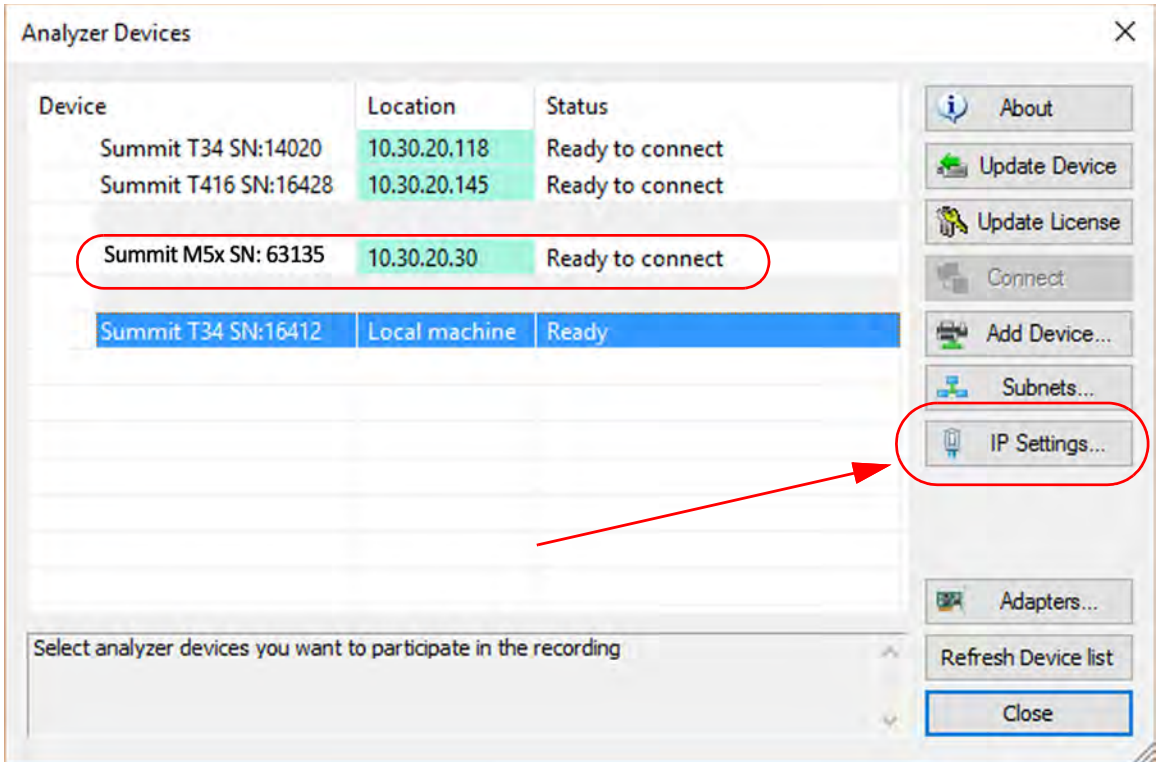


Figure 3.17: All Devices Connected on Your Network

To discover the IP address of the local Summit M5x (attached via the USB cable to your Summit M5x), select the IP Settings tab. This will popup the Device Settings dialog box. See Figure 3.18.

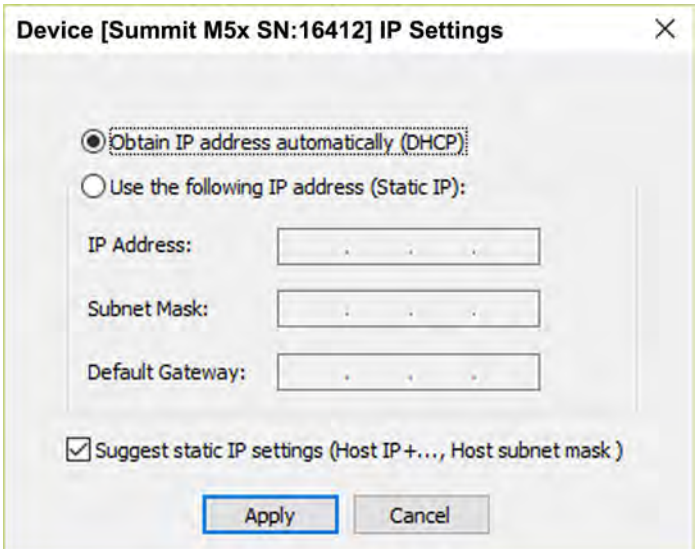


Figure 3.18: Device IP Settings (Summit M5x)

From this dialog box you can either:

- Obtain an IP address automatically (DCHP)
- Use the following IP address (Static IP)
- Suggest Static IP Settings

If you choose the DCHP option the following dialog box will popup (see Figure 3.19).

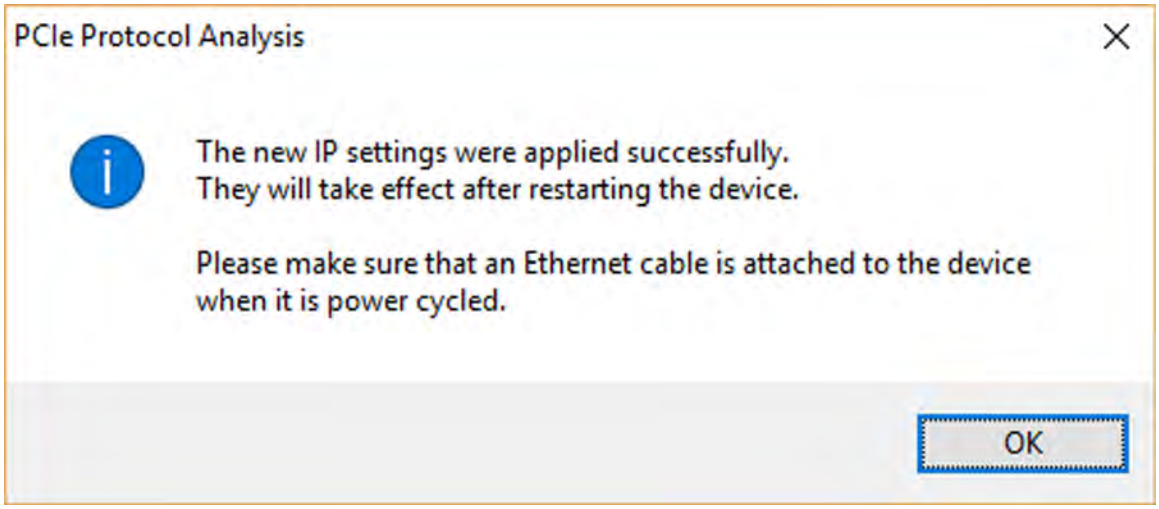


Figure 3.19: Use DCHP to Set IP Address

If you had chosen to use the Static IP address the following Dialog Box would popup (see Figure 3.20. You can either

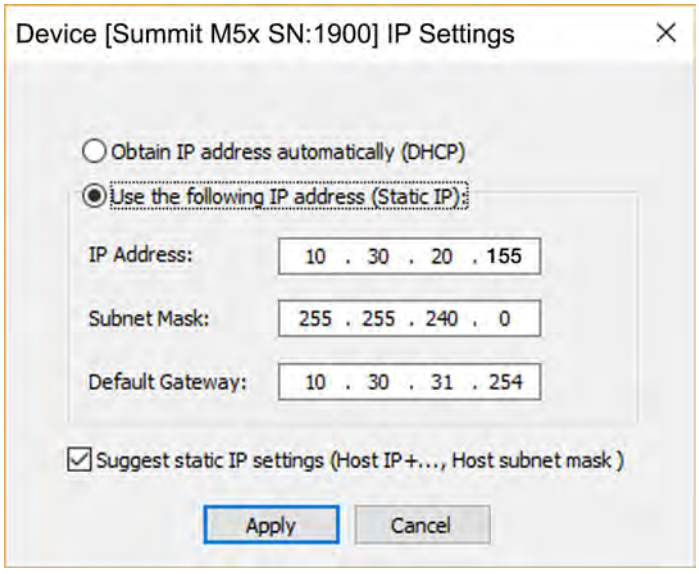


Figure 3.20: Use Static IP Address Summit M5x

If you had chosen the Suggest static IP settings the following dialog box would popup (see Figure 3.21).

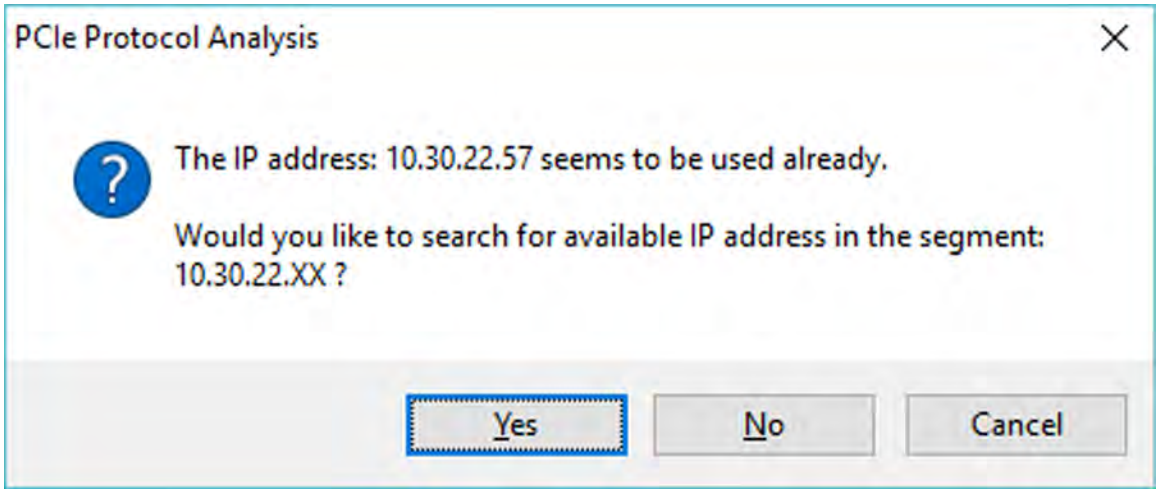


Figure 3.21: Suggest Static IP Settings

Select "Yes" and the system will select an unused IP address.

The the following dialog box will popup. See Figure 3.22.

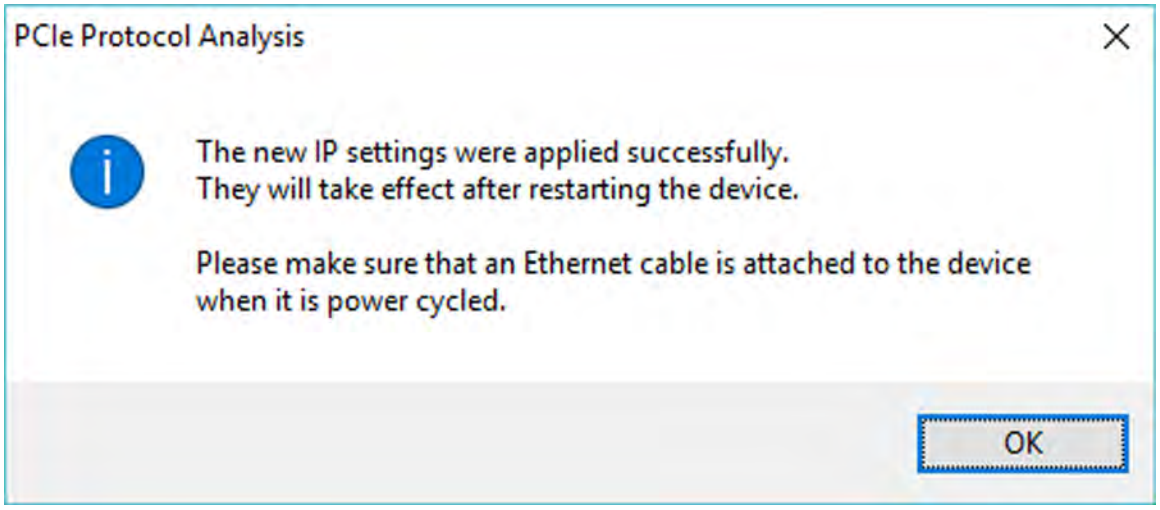


Figure 3.22: New IP Settings Applied

Now you should attach the Ethernet cable, disconnect the USB cable and cycle the power on the Summit M5x .

After the Summit M5x re-initializes and the Status LED goes from OFF to Green to Blue, restart the PCIe Protocol Analysis and select **Setup > All Connected Devices.**

Now the Summit M5x has an IP address and is Ready to Connect.

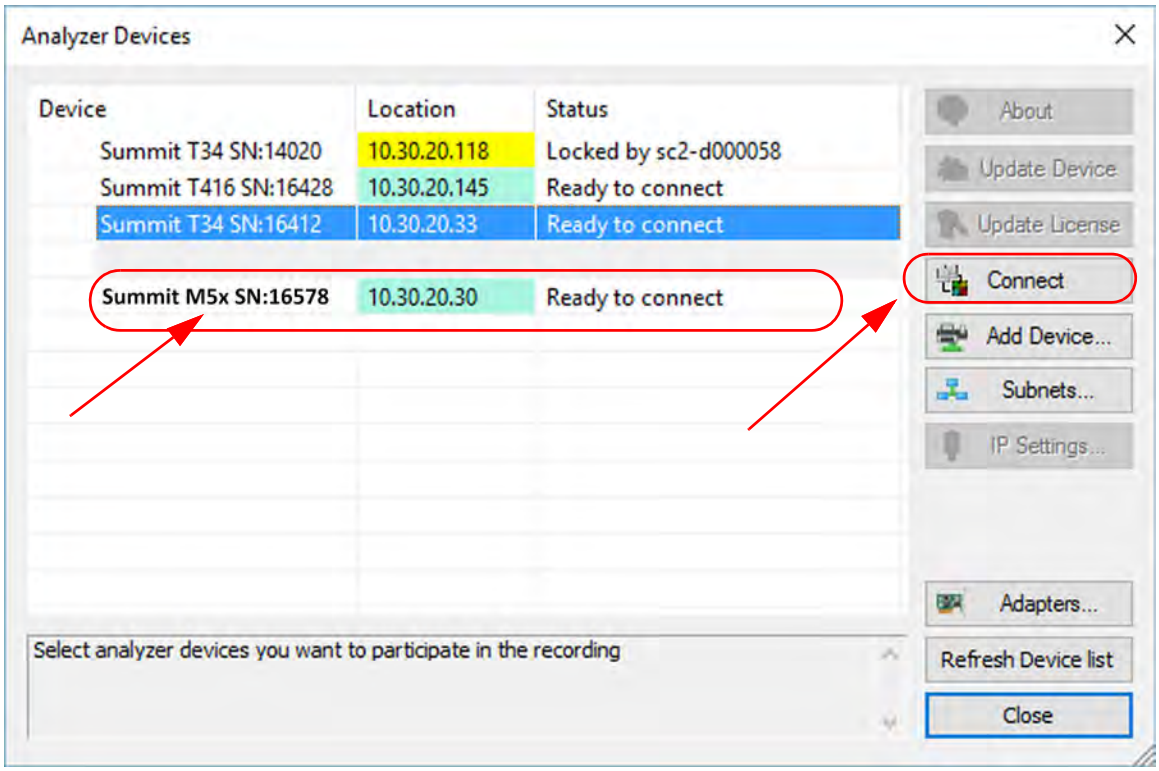


Figure 3.23: Analyzer Devices: Summit M5x Showing IP Address

Select the Connect tab and you are ready to start capturing data traffic with the Summit M5x.

Chapter 4

Software Overview

4.1 The PCIe Protocol Analysis software

The PCIe Protocol Analysis™ software administers Analyzer platforms and handles all CATC Trace analysis and display. The core software is thus the same for all of Teledyne LeCroy's PCI Express products.

The software runs on a Windows® based host machine that is attached to the Analyzer via an Ethernet or USB 2.0 connection (USB 1.0 is also supported). PCIe Protocol Analysis can be used without the Analyzer as a CATC Trace viewer for viewing, analyzing and printing traces.

The PCIe Protocol Analysis software operates on systems using Windows Server 2019 (x64), Windows Server 2016 (x64) and Windows 10 64-bit. The latest Service Pack available for the Windows OS in use is required. It is recommended that you use one of the supported 64-bit Windows versions listed above.

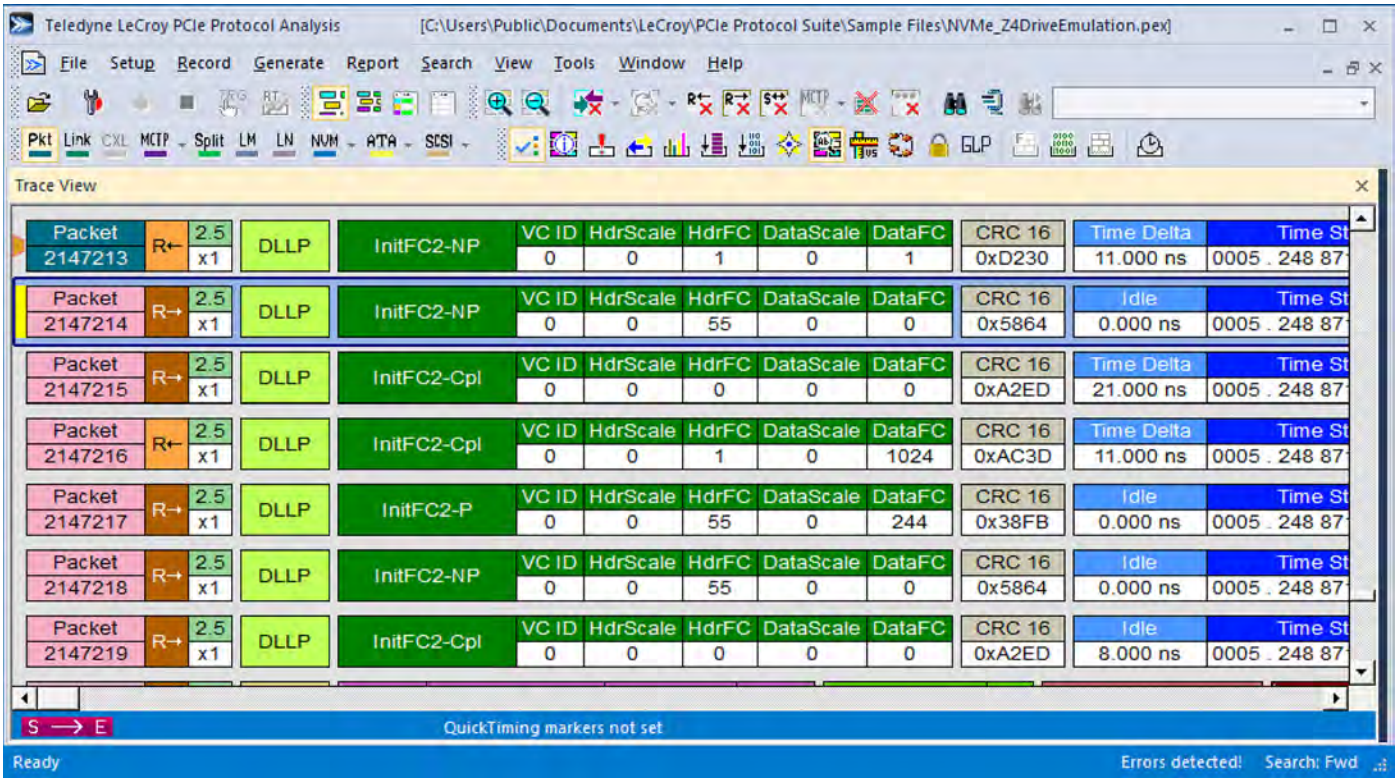


Figure 4.1: Sample of a CATC Trace

4.2 Application Layout

The PCIe Protocol Analysis application contains the following components:

Title bar: The title bar is at the top of the application window and displays the CATC Trace file name or generation script name.

Menu bar: The menu bar is located below the title bar, by default. The menu bar can be moved by clicking a blank area of the bar and then dragging the menu to a new position. It can be docked in another part of the application window or moved outside of the window to become a floating menu.

Toolbar: The toolbar is composed of buttons that represent the commonly used commands. The toolbar divides into smaller toolbars that can be moved and docked in a new position or made to float outside of the window.

Display area: The display area is the main part of the application window in which CATC Traces are displayed.

Status bar: The status bar is located at the bottom of the application window. The left end of the status bar displays descriptions of buttons and menu items when the mouse is positioned over them. The right end of the bar shows the search direction.

4.3 Using the Toolbar

You can use the PCIe Protocol Analysis application Toolbar as a shortcut to most of the operations supplied by the menus.

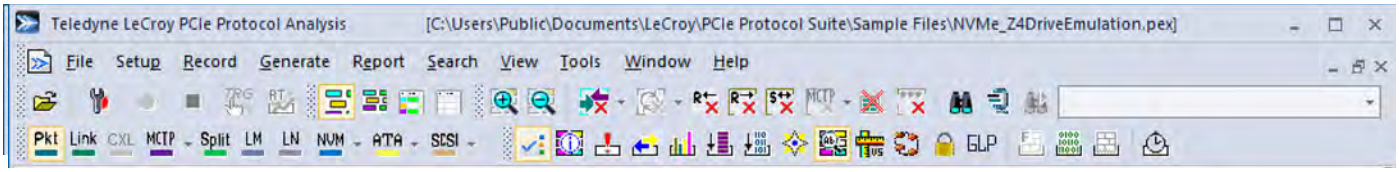


Figure 4.2: Summit M5xToolbar Set

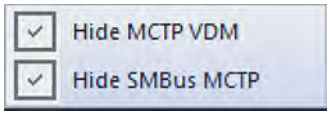
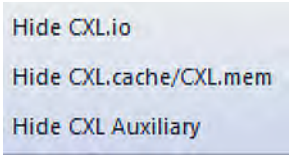
4.3.1Frequently Used Toolbars

	Opens a previously recorded CATC Trace file.		Stop Recording.
	Setup Recording Options Opens the Recording Options dialog.		Real Time Statistics monitor Opens a window that displays real-time information.
	Start Recording.		

	Displays CATC Trace view.		Displays color spreadsheet view.
	Displays compressed CATC Trace view.		Displays black and white spreadsheet view.

	Zoom in display.		Advanced Hiding Options Opens a dialog box that allows you to select items to hide from view.
	Zoom out display.		Hide Unassociated Traffic Hides the lower-level transaction packets. Example: Link Transactions and Packets are considered “unassociated” when using Split Transaction Level view.

	Hide Training Sequence.		Compact View Toggles compacting of training sequences to analyze CATC Trace data faster, or no compacting to display more data. Compact View also compacts CXL NULL Flit Packets.
	Hide SKIP and Update FC packets.		Find Opens a dialog box that allows you to select one or more items to find in the recording, then searches to that point.
	Hide Upstream recording/ traffic.		Find Next. Repeats last Find or Search action.
	Hide Downstream traffic/ recording.		Hide Sideband traffic.
	Hide MCTP VDM and Hide SMBus MCTP		Hide CXL traffic

			
		Quick Search window: Allows user to search for pre-defined terms or type in their own term to search for. See “Quick Search Feature” on page 72.	

Quick Search Feature

The Quick Search feature allows you to either search for a pre-defined term (see Figure 4.3) within a loaded Trace by clicking on the down arrow  or by typing your own term into the search window  and then moving the cursor into the window and hitting the Enter key. This feature will scroll through the entire Trace searching for the requested term and either stop at a highlighted Packet within the Trace or not move to a new position in the Trace if the term was not found. For more details see “Quick Search Feature” on page 730.

For a list of all possible terms, refer to “Quick Search Feature” on page 895.

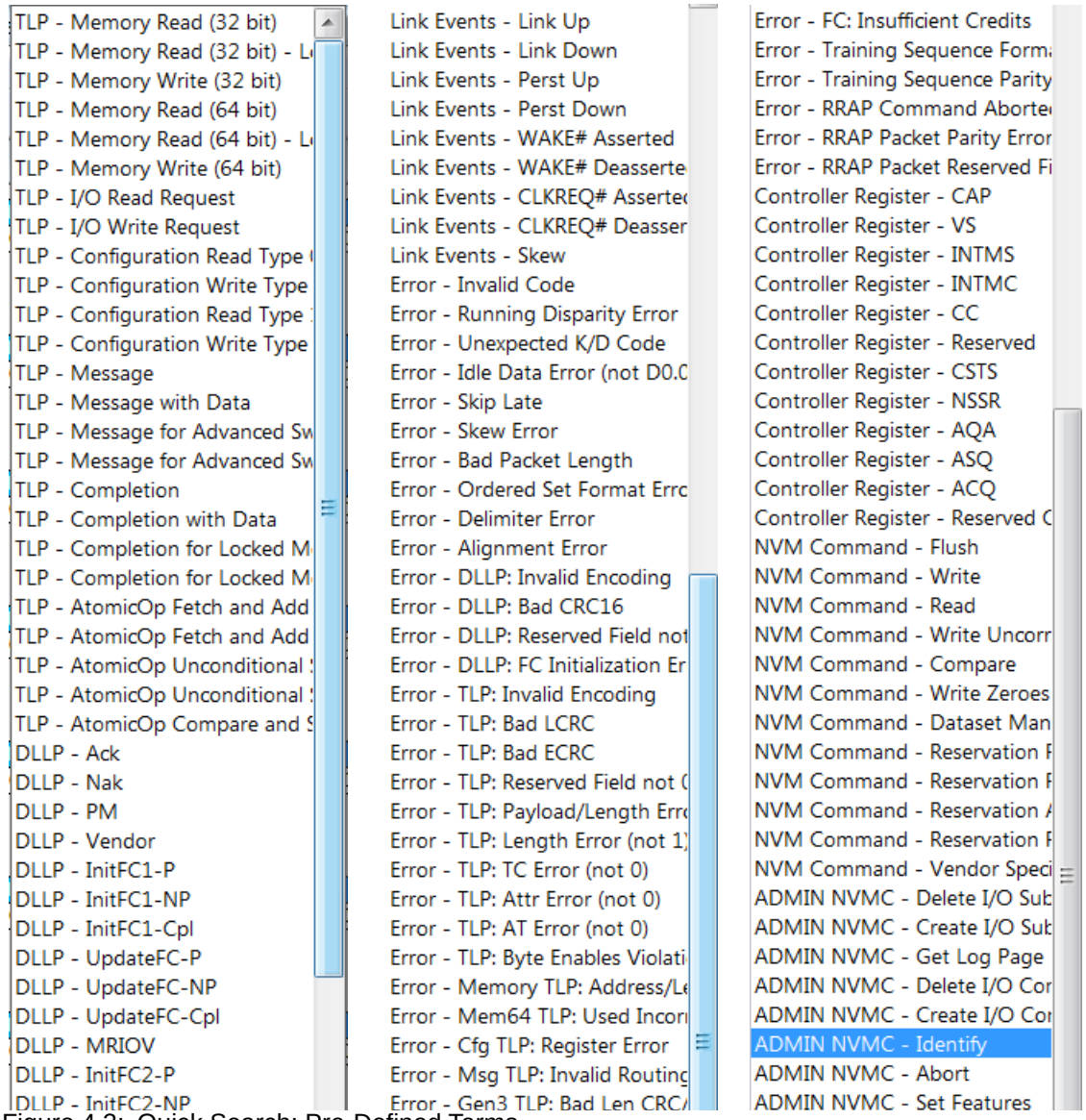
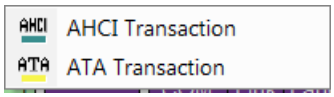


Figure 4.3: Quick Search: Pre-Defined Terms

Pkt	View Packet Level data.	Link	View Link Transaction Level data.
Split	View Split Transaction Level data		View PQI, SOP and SCSI Transaction Level data pull down menus.
NVM	View NVME Transaction Level and Command data pull down menus	SCSI	PQI Transaction SOP Transaction SCSI Transaction
	NVM NVME Transaction NVM NVME Command	MCTP	View MCTP Transaction Level data

	View AHCI and ATA Transaction Level data pull down menus		Lane Margining Commands/Responses
			Lightweight Notification Transaction Level data
	Trace Expert Generates data on Performance Analysis, Trace Analysis Statistics, Error Reports and Trace Information.		Opens the Data Flow window. Shows recorded data in a compressed tabular format.
	Trace Information Lists the conditions under which the recording was made.		Navigator. Shows/hides the Navigator bar - a utility that lets you easily navigate the CATC Trace
	Error Report Opens a window that lists all errors identified in the recording.		Detail View Shows the Detail view of the selected packet.
	Traffic Summary Opens a window that lists all events that occurred during the recording		Running Verification Scripts Runs selected Verification Scripts
	Bus Utilization Opens a window that graphically represents various information about the recording.		LTSSM Flow Graph Shows a state diagram of the Link Training and Status State machine.
	Link Tracker Opens a window that displays symbol information per lane.		Opens view for TCG Security Codes. TCG decoding is performed using NVMe Command Level option.
	Get Log Page View Opens Log Page View		

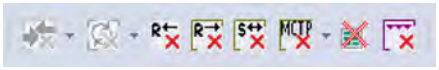
	CXL Flit Data View Opens window showing detailed view of CXL Flit Data		Displays the Data/Payload window for the current packet.
	Displays the Packet Header bar. Opens a window that displays the header information in the current packet, as it would be viewed in the specification.		Opens the Timing and Bus Usage Calculations window.

4.3.2Multi-Segment Toolbar

	First Segment. Open first segment in the multisegment CATC Trace.		Index file. This button becomes active if a multisegment CATC Trace file is open and displays the index file for the recording.
	Previous segment. Open previous segment in the multisegment CATC Trace.		Next Segment. Open next segment in multisegment CATC Trace.
			Last segment. Open last segment in multisegment CATC Trace.

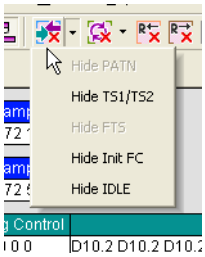
4.3.3 Toolbar Hide Buttons

The PCIe Protocol Analysis application toolbar has seven buttons related to show/hide of CATC Trace file contents. The buttons allow you to quickly adjust the display to your needs.



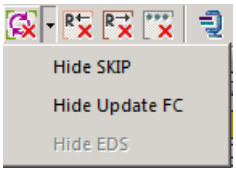


Hide Training: Brings up a drop-down menu that lets you to hide all or a portion of the packets in the training portion of the CATC Trace.





Hide SKIP, Update FC and Hide EDS: Brings up a drop-down menu that lets you hide SKIP, Update FC and hide EDS packets in a CATC Trace.



Hide Upstream: Hide all traffic from endpoint devices to the root complex.



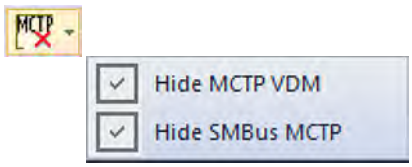
Hide Downstream: Hide all traffic from the root complex to endpoint devices.



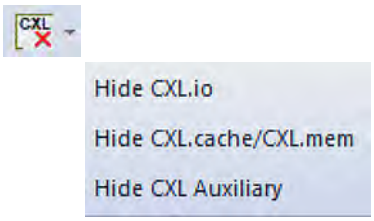
Hide Sideband: Hide all sideband traffic (includes SMBus traffic).



Hide MCTP: Hide MCTP VDM traffic (and/or) Hide SMBus MCTP traffic.



Hide CXL: Hide CXL traffic (io, cache/mem or Auxiliary).



Advanced Hiding Options: Brings up the Level Hiding pane of the Display Options window. Use this pane to tune the show/hide options within the CATC Trace display.



Hide Unassociated Traffic: Hides the lower-level transaction packets. Example: Link Transactions and Packets are considered "unassociated" when using Split Transaction Level view.



4.4 Using the Menus

The PCIe Protocol Analysis application main display includes the following set of pull-down menus:

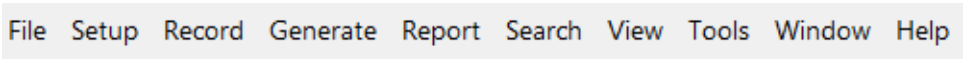


Figure 4.4: Menus

4.4.1 File Menu

New PETrainer Script	Creates a new Traffic Generation file.
Open	Opens a file.
Close	Closes the current file.
Save as	Saves all or a specified range of packets to a uniquely named file. Overwrites existing file name. See “Using the Save As Function” on page 109.
Save Copy As	Saves all or a specified range of packets to a uniquely named file. Original file remains the same and new file is created with the new file name. See “Save Copy As Function” on page 111.
Convert Old Files	Convert CATC Trace files made in previous versions of PE*Tracer* to the new format for PE*Tracer* version 5.0 and higher.
Print	Prints part or all of the current traffic data file.
Print Preview	Produces an on-screen preview before printing.
Print Setup	Setup your current or new printer.
Clean Up Decoder Temp Files	Let’s you selectively delete decoder temp files (see “Clean Up Decoder Temp Files” on page 80).
Edit Comment	Create or edit the comment field in a CATC Trace file.
Export >> to Text >> Packets to CSV Text >> to Generator File Format	Saves all or part of a CATC Trace to a text file or traffic generation file. This text file summarizes the traffic in the CATC Trace. Saves the CATC Trace to a text file in Comma Separated Value (CSV) format. Saves the CATC Trace to a generation file, which can be used Summit Exerciser (Z3-16 or Z416).
Exit	Exit the PCIe Protocol Analysis application.

File Dialog

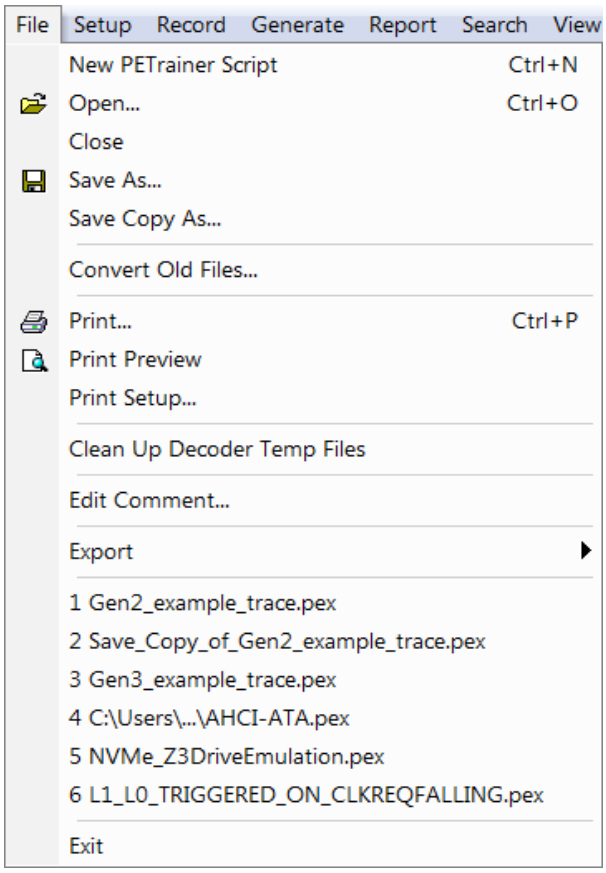


Figure 4.5: File Dialog

Clean Up Decoder Temp Files

This command deletes selected decoder temp files from the selected folder.

The file types effected by this command are:

- *.pem
- *.pex
- *.peraw
- *.mpex
- *.peg

To use this command follow the steps below:

1. The Sample File Folder has Temp files for every trace that has been opened: See Figure 4.6.

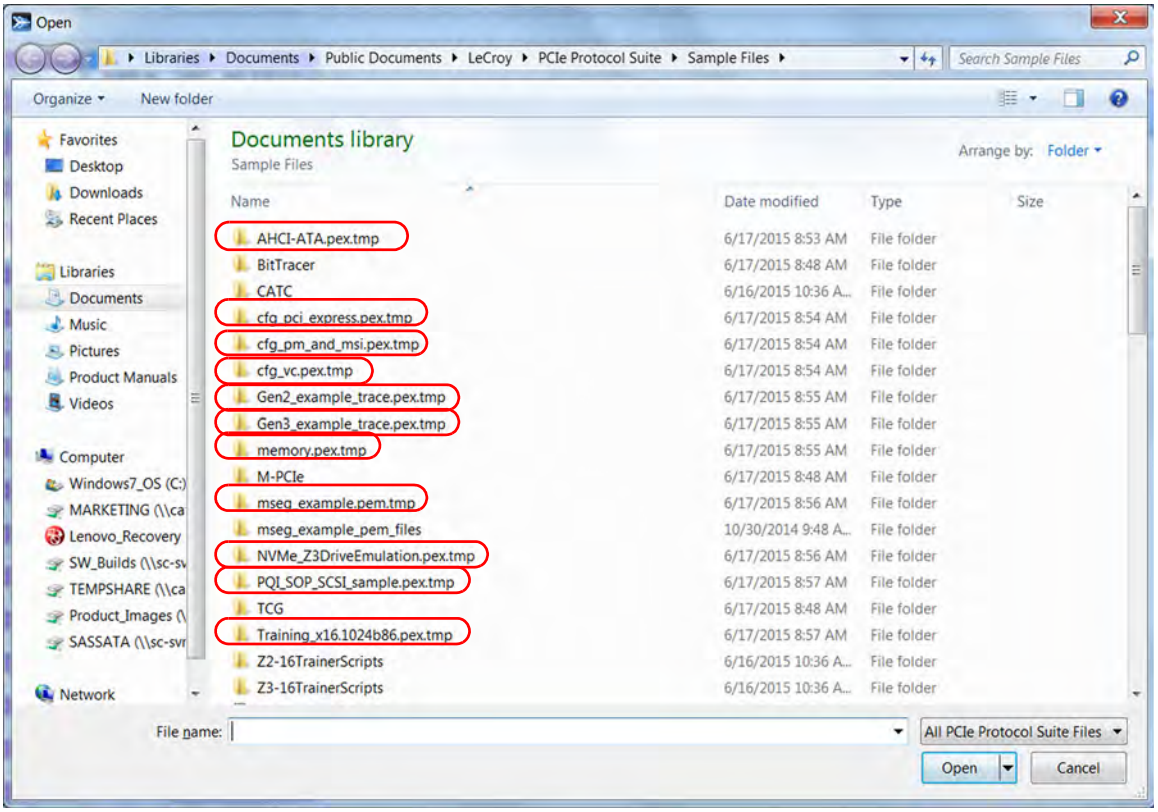


Figure 4.6: Sample Files Folder After Opening a Variety of Traces

2. Now select the File -> Clean Up Decoder Temp Files (see Figure 4.5 on page 79).
3. The following Dialog will pop up: See Figure 4.7 on page 81.

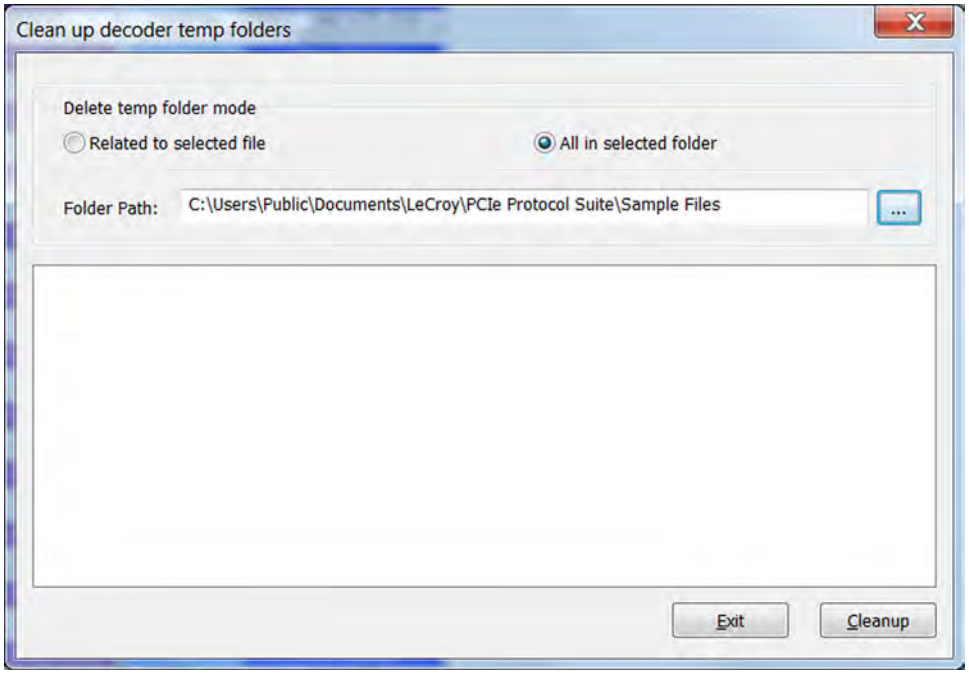


Figure 4.7: Clean Up Decoder Temp Files Dialog

4. Select C:\Users\Public\Documents\LeCroy\PCIe Protocol Site\Sample Files folder.
5. Select Cleanup and a Warning Dialog will pop up. See Figure 4.8.

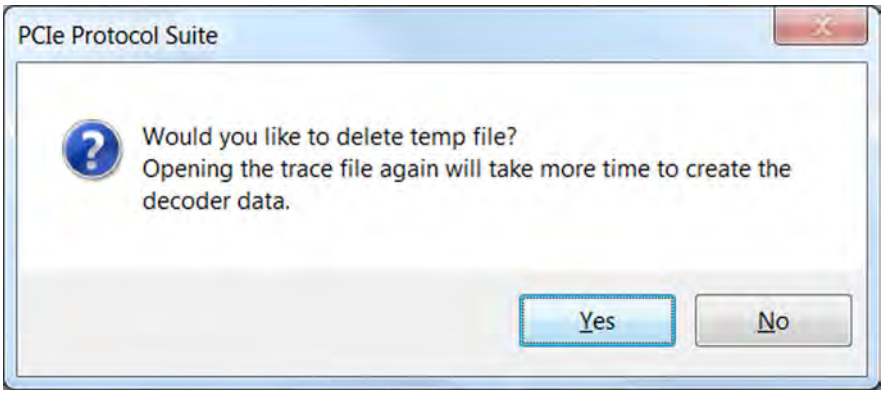


Figure 4.8: Clean Up Decoder Temp Files Warning Dialog

6. Click on Yes, (if files are still in use the Clean Up will Fail, see Figure 4.9 on page 82).

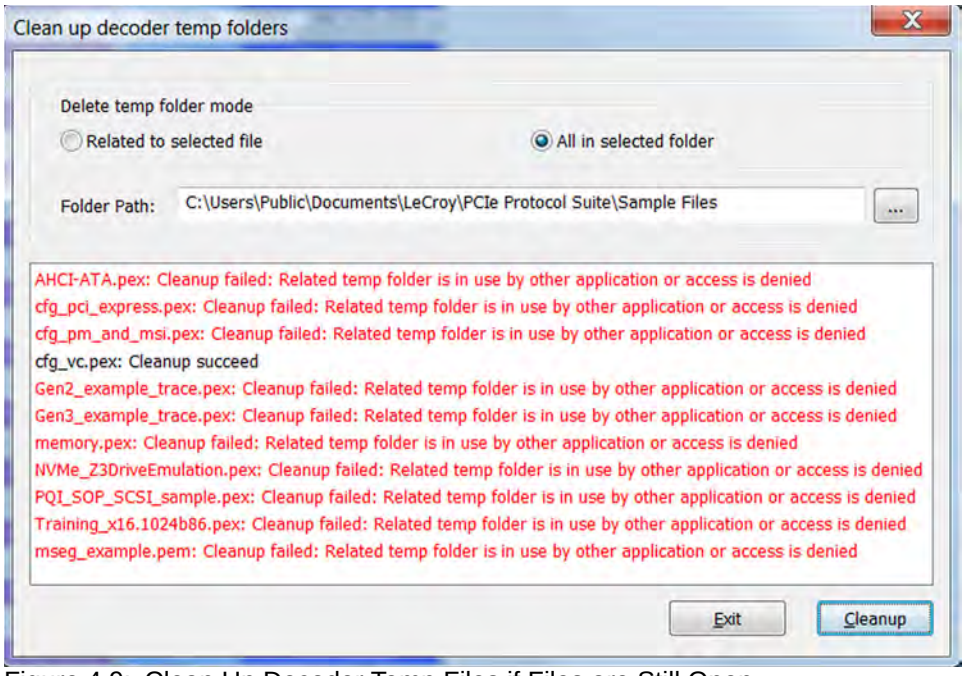


Figure 4.9: Clean Up Decoder Temp Files if Files are Still Open

7. Close Files you're not working with.
8. Select Clean Up Decoder Temp Files again.
9. Select Yes on the Warning Dialog.
10. With the files closed, the Clean Up Dialog will respond as shown below (see Figure 4.10).

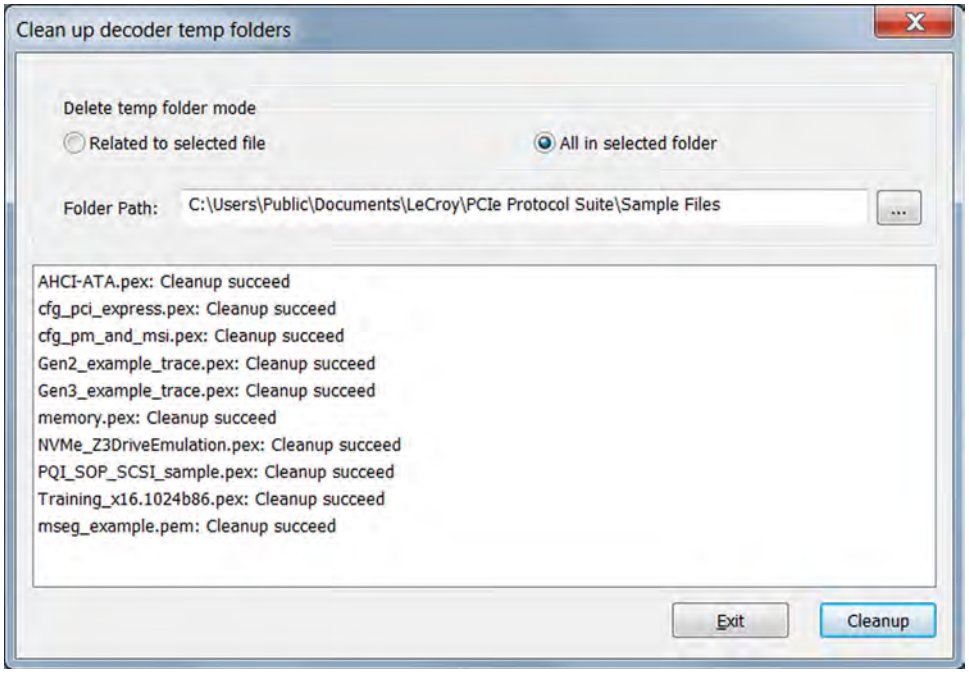


Figure 4.10: Results of Running Clean Up Command

11. Confirm that the Clean Up Command was successful by viewing the C:\Users\Public\Documents\LeCroy\PCIe Protocol Site\Sample Files folder contents, (see Figure 4.11).

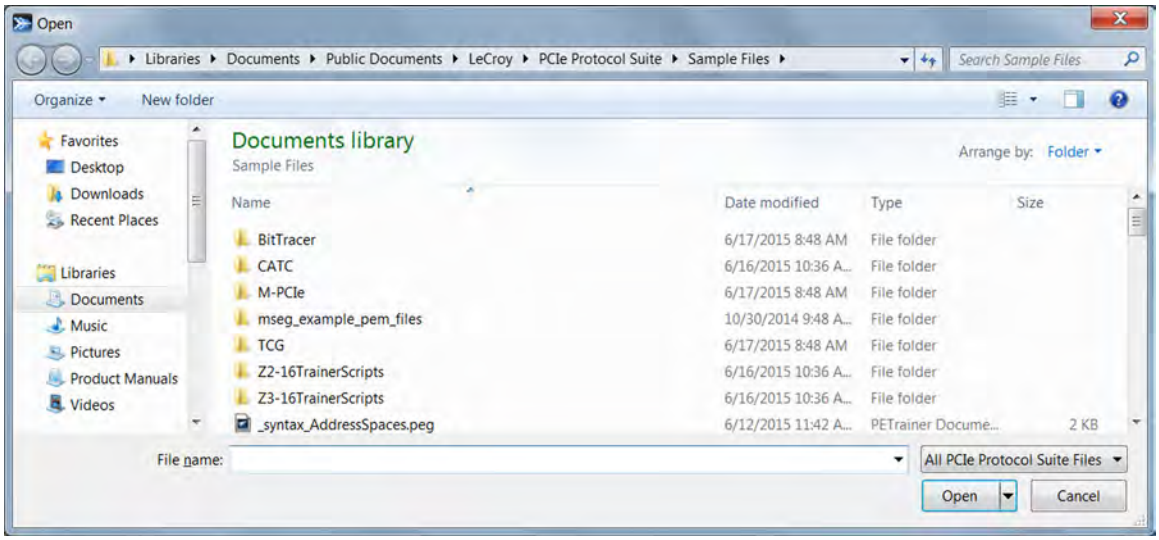


Figure 4.11: Sample File Folder After Temp File Clean Up

12. Compare Figure 4.6 on page 80 with Figure 4.11 to ensure that the .tmp files have been deleted.

4.4.2 Setup Menu

Display Options	Allows you to customize display options such as field colors, field formats and level hiding.
Recording Options	Allows you to customize control and setup features associated with recording, triggering, and filtering recorded events.
Generation Options	The Generation Options dialog is used to set configuration settings in a traffic generation script (*.peg). This dialog provides a convenient alternative means of editing a traffic generation file.
Generation Macros	Opens a dialog for creating buttons on the status bar that can be used to run traffic generation macros.
Update Device	Opens a dialog box that lets you update the BusEngine™ and Firmware.
Launch CrossSync™ Control Panel	Launches the CrossSync™ application. The CrossSync™ Control Panel allows you to select analyzers for synchronization and manage the recording process. See “CrossSyncTM Control Panel” on page 127.
All Connected Devices	Opens a dialog box with a list of locally or remotely connected devices. Allows you to update the BusEngine™, Firmware, and your licensing information.

Display Options: Level Hiding -> Direction

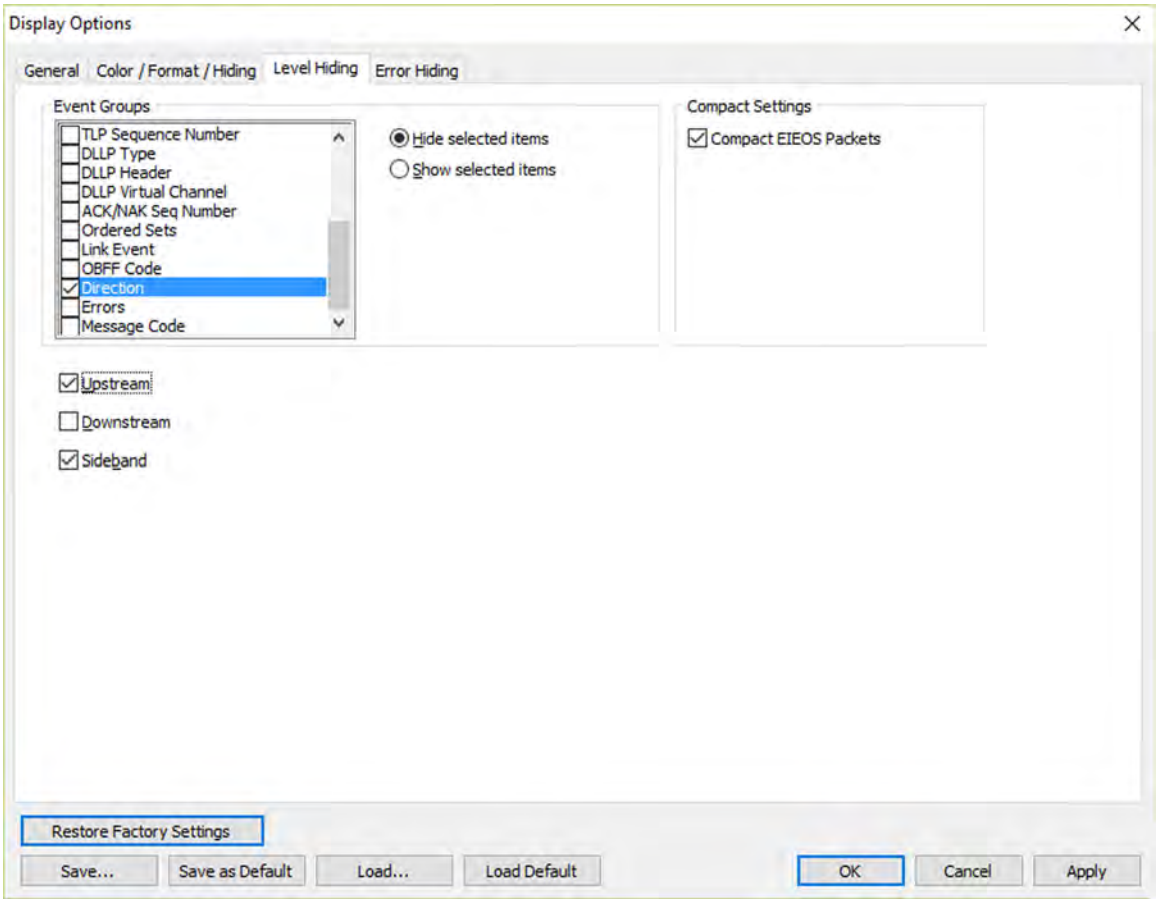


Figure 4.12: Display Options: Level Hiding -> Direction

You can select the Direction of traffic to Hide:

- Upstream
- Downstream
- Sideband (includes SMBus traffic)

4.4.3 Record Menu

Start	Causes the Analyzer to begin recording traffic.
Stop	Causes the Analyzer to stop recording traffic.
Reupload	Causes the Analyzer to re-send all, or selected portions, of the CATC Trace from the Analyzer buffer to the host machine.
Manual Trigger	Trigger command for Analyzer is generated upon clicking this button.

4.4.4 Report Menu

Report Menu operations are only available when you are working with a CATC Trace file.

Trace Expert Report	Generates Reports for the currently loaded trace: Performance Analysis, Trace Analysis, Errors, File Information.
Trace Information	Displays information about the file contents and describes the conditions of the file's recording (Recording Options, hardware information, and so on).
Error Summary	Displays an error summary of the current CATC Trace file and allows you to go to a specific packet, and save the error file to a uniquely named file.
Traffic Summary	Details the number and types of packets that were transferred during the recording. You can hide, save, send, text, print, and view.
Bus Utilization	Opens a window with graphs of bus usage for the open CATC Trace.
Link Tracker	Opens a window for displaying a detailed chronological view of traffic. The window provides view and navigation options.
Data Flow	Opens the Data Flow Window, providing a tabular view of transactions and their payload.
Trace Navigator	Shows the Navigator bar for navigating a CATC Trace. Shows a snapshot of the recording and allows you to adjust the memory area for the view.
LTSSM Flow Graph	Shows a state diagram of bus activity. Also allows you to navigate through the LTSSM, based on the current recording.
TCG Security View	Shows Trusted Computing Group (TCG) Security View. Opens the Security View window to display security data fields decoded.
Get Log Page View	Opens Log Page View window when selected.
LM Eye Diagram	Opens Lane Margining Eye Diagram when selected.
Packet Header	Opens the Packet Header bar, showing the Packet Header information as it would be viewed in the specification.
Packet Data	Opens the Data Window for the current packet or transaction, with the options: Hide, Save, Hexadecimal, ASCII, Decimal, Binary, MSB Format, LSB Format, Big Endian, and Little Endian. Format Line allows you to enter the number of bytes, words, or dwords per line.
Configuration Space	Presents a list of Configuration Spaces. Clicking an item displays the selected Configuration Space in a Configuration Table format.

4.4.5 Search Menu

Search Menu operations are only available when you are working with a CATC Trace file.

Go to Trigger	Repositions the display to show the first packet following the trigger event.
Go to Selected Packet	Repositions the display to a specific packet, Link or Split transaction of PCI Express protocol or NVME, PQI, AHCI, ATA, SOP and SCSI command transaction levels.
Go to Segment/ Packet	Allows searching for specific link events packets or time.
Go to Time	Repositions the display to specific timestamp.
Go to Marker	Repositions the display to a previously marked packet, Link, Split, NVME, PQI, AHCI, ATA, SOP or SCSI command transactions.
Go to NVMe Transaction	Allows searching for Controller Registers, Other NVMe Entities, Doorbell Registers, Admin Submission Command Set, NVM Submission Command Set, Completion Queue Entry and NVMe Errors.
Go to NVMe Command	Allows searching for Admin Command Set NVM Command Set, Status, Errors, TCG Types, TCG Method, TCG Invoker, TCG Com ID and TCG Ext Com ID.
Go to SCSI	Allows searching for SCSI commands and sub-commands: SCSI Operation, Command Status, Task Management, Task Management Response, Error, SCSI Logical Unit Number.
Go to	Allows searching for specific link events: TLP Type, DLLP Type, Ordered Set, Link Event, Traffic Class, DLLP Virtual Channel, TLP Virtual Channel, Direction, Speed, Link Width, Requester ID, Completer ID, Data Lengths, Errors.
Find	Allows searching for various events within a CATC Trace. See “Find Feature” on page 88 for more information.
Find Next	Repeats the previous Find or Search operation.
Toggle Search Direction	Changes the current search direction from Forward to Backward or from Backward to Forward. Current search direction shown in lower right hand corner of main PCIe Protocol Analysis Menu.

Find Feature

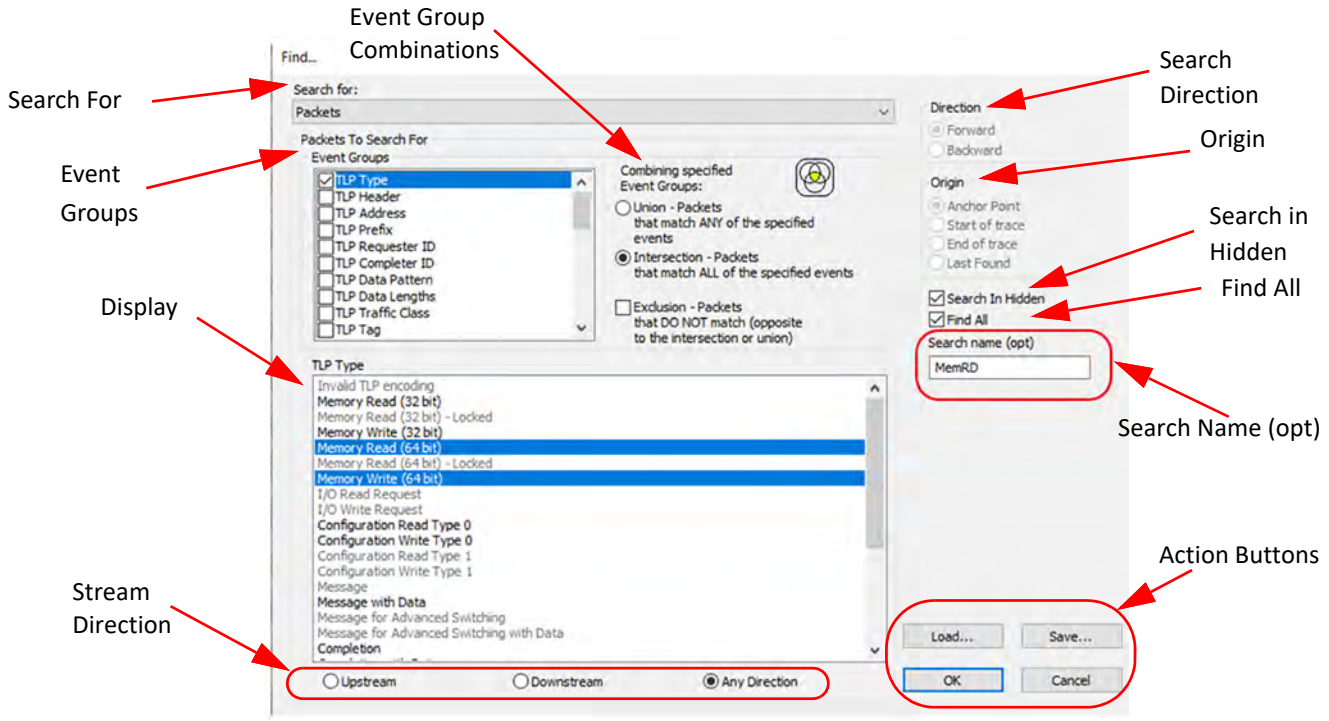


Figure 4.13: Find Menu Features

Find Criteria	Description
Search For	Use the drop down menu to select the search event. See for the type of events you can search. See “Search For” on page 89 for more information
Event Groups	Click the type(s) of Event Groups related to the Search For criteria. These change to match the Search For selection, i.e., if you search for Packets, the Event Group listing changes to types of packets. See “Search For” on page 89for more information.
Display	Further refines the Event Group selection(s). See “Search For” on page 89.
Stream Direction	Choose Upstream, Downstream, or Any Direction to search the streams.
Event Group Combinations	Refine the search by different combinations: Union or Intersection. Click the Exclusion button to search for the opposite combination.
Search Direction	Search through traces forward or backward.
Origin	Choose where to start the search: Anchor Point, Start of Trace, End of Trace, or Last Found.

Find Criteria	Description
Search in Hidden	Searches in hidden locations.
Find All	Finds all trace data that matches the search criteria.
Search Name (opt)	Allows you to enter a search name to label your search. You must click **Find All** to use this feature. See "Search Name (opt)" on page 91 for more information.
Action Buttons	Load: Opens the folder dialog to Load a previous search. Save: Opens the folder dialog to Save the current search. OK: Start the search and displays the results. Cancel: Exits the search and closes the Find dialog.

Search For

In the Find Dialog, the Search For, Event Group, and the display area are interrelated. Choosing a Search For item from the drop down list will change the Event Group settings and the display area, showing selections related to that Search For choice.

The following table shows the search for criteria and its coordinating Event Group choices:

Search For Criteria	Event Group Choices
Packets	TLP Type, TLP Header, TLP Requester ID, TLP Completer ID, TLP Data Pattern, TLP Data Lengths, TLP Tag, TLP Sequence Number, DLLP Type, DLLP Header, DLLP Virtual Channel, ACK/NAK Seq Number, Ordered Sets, Link Event, Direction, Errors, TS1 Data, TS2 Data.
Link Transactions	TLP Type, Traffic Class, Virtual Channel, Direction, Requester ID, Completer ID, Status, Tag.
Split Transactions	TLP Type, Traffic Class, Virtual Channel, Direction, Requester ID, Completer ID, Status, Tag.
Link Margining (LM) Transactions	Margin Command, Margin Type, Receiver Number or Errors.
LN Transactions	Notification Reason, Cacheline Size, Cachelines, Completion Status, Read/Write, Directed/Broadcast and Errors.
NVME Transactions	Controller Registers, Queue IDs, Command IDs, Doorbell Registers, Admin Submission Command Set, NVMe Submission Command Set, Completion Queue Entry, and PRP.
PQI Transactions	TLP Type, Traffic Class, Virtual Channel, Direction, Requester ID, Completer ID, Status, Tag, Address.
AHCI Transactions	AHCI Register ID, AHCI Port Number, AHCI Slot Number, AHCI Port Multiplier Port, Raw Address, AHCI Direction, AHCI Errors
ATA Transactions	ATA Register Type, ATA Port Number, ATA Slot Number, ATA Raw Address, ATA Port Multiplier, ATA Interruption Reason, ATA Error Type, ATA Input/ Output, ATA Payload Portion, ATA CFS Fields, ATA RFIS Device to Host Fields, ATA DSFIS Fields, ATA PSFIS Fields, ATA SDBFIS Fields.

Search For Criteria	Event Group Choices
SOP Transactions	SOP Information Unit ID, SOP Errors.
SCSI Transaction	SCSI Operation, Command Status, Task Management, Task Management Response, Errors, SCSI Logical Unit Numbers. Find allows you to create complex searches based on numerous criteria.
NVME Commands	Admin Command Set, NVM Command Set, Submission QID, Completion QID, Status, Errors, LBA, NVM Command, NVM Payload Portion, TCG Types, TCG Method, TCG Invoker, TCG Com ID, TCG Ext Com ID and RPMB.
MCTP Messages	MCTP Message Type, MCTP Source EID, MCTP Destination EID, MCTP Control Command Code, MCTP Control Completion Code, MCTP Control Instance ID, MCTP Error, PLDM Type, PLDM Command Code, PLDM Completion Code.
MCTP Commands	MCTP Message Type, MCTP Control Command Code, MCTP Control Completion Code, MCTP Source EID, MCTP Destination EID, PLDM Type, PLDM Command Code, PLDM Completion Code, NC-SI Command, NC-SI Response, NC-SI AEN Type, MCTP Cmd Errors.
DOE Transactions	DOE Type Name, DOE Error, DOE Warning.
SPDM Messages	SPDM Code, SPDM Error
Search by mask/ match	Opens a new search to search by TLP and DLLP packets.
Search by address	Search for a specific packet by its address. Use the Address field and click Add to add addresses to the Addresses list. Delete addresses from the Addresses list by using the Delete key on the keyboard.

The Find options dynamically change depending on the Search For criteria. Refer to the following screens for examples.

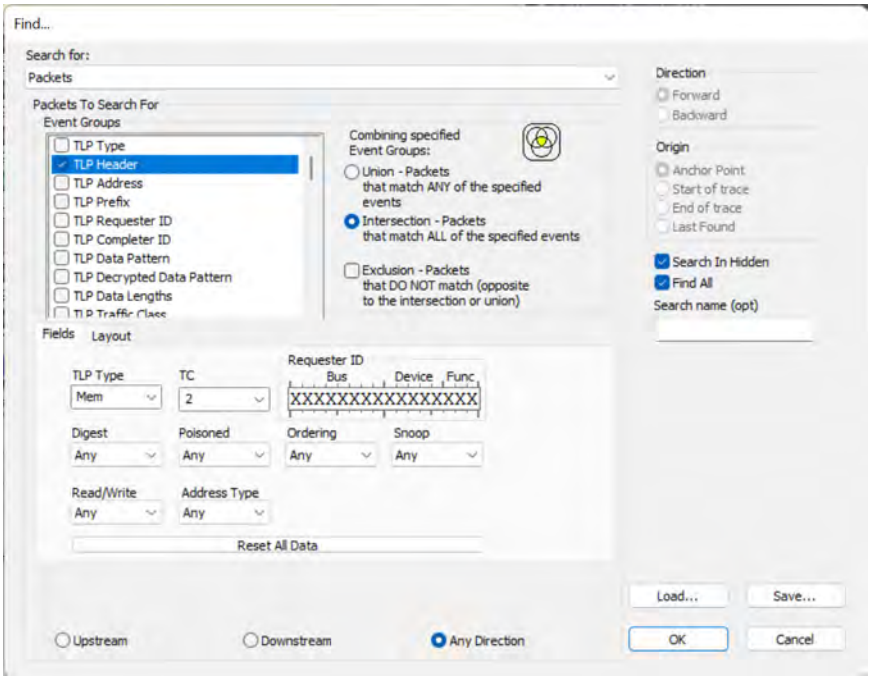


Figure 4.14: Find example: Search for Packets by TLP Address

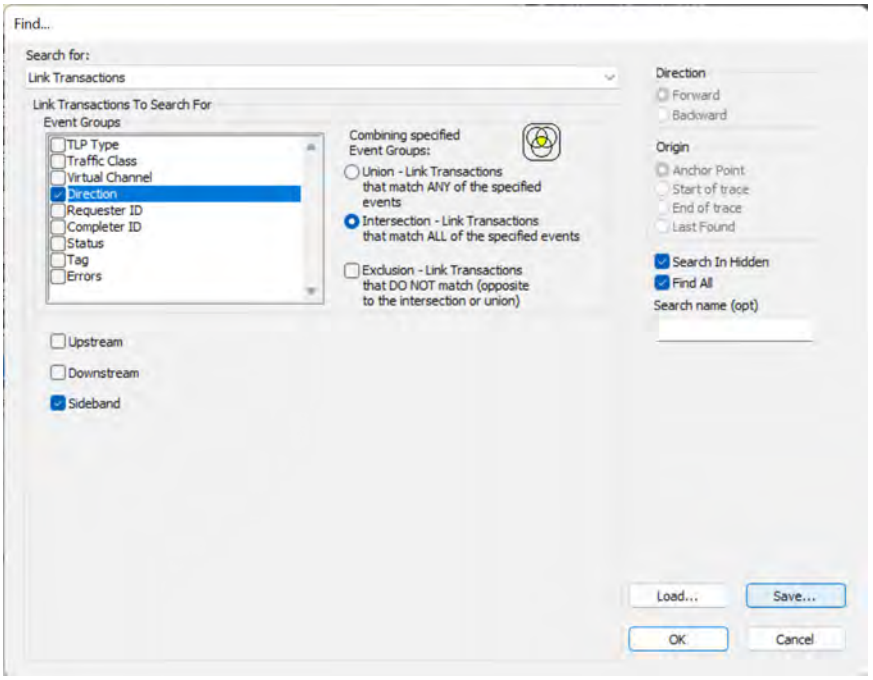


Figure 4.15: Find example: Search for Link Transactions by Direction

Search Name (opt)

The optional Search Name field allows you to set a specific name for your search. See Figure 4.16.

Note: You must have **Find All** checked to use the Search Name (opt) feature.

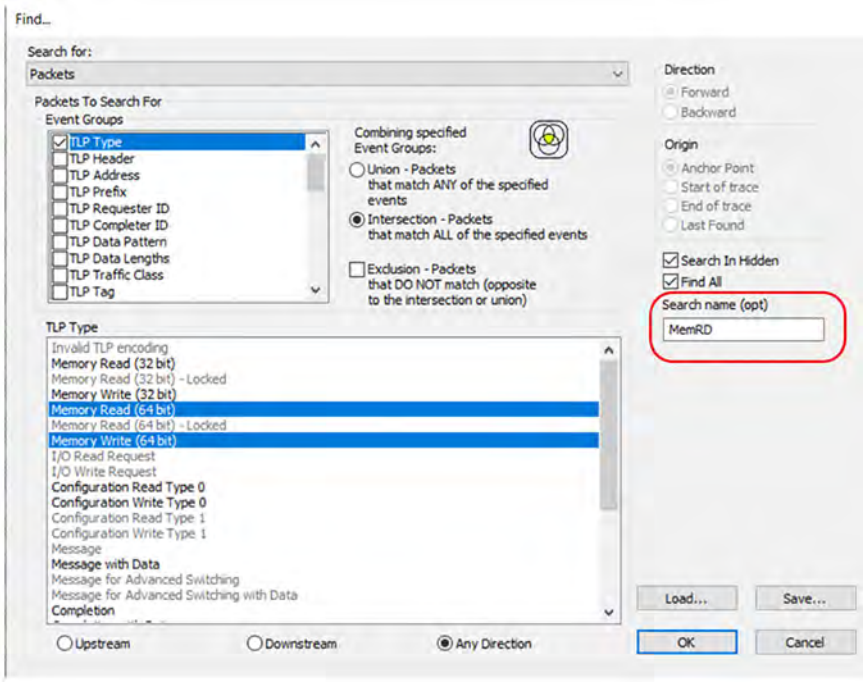


Figure 4.16: Search Name (opt) in the Find Dialog

The search name also displays on the main screen as the name of the trace. See Figure 4.17.

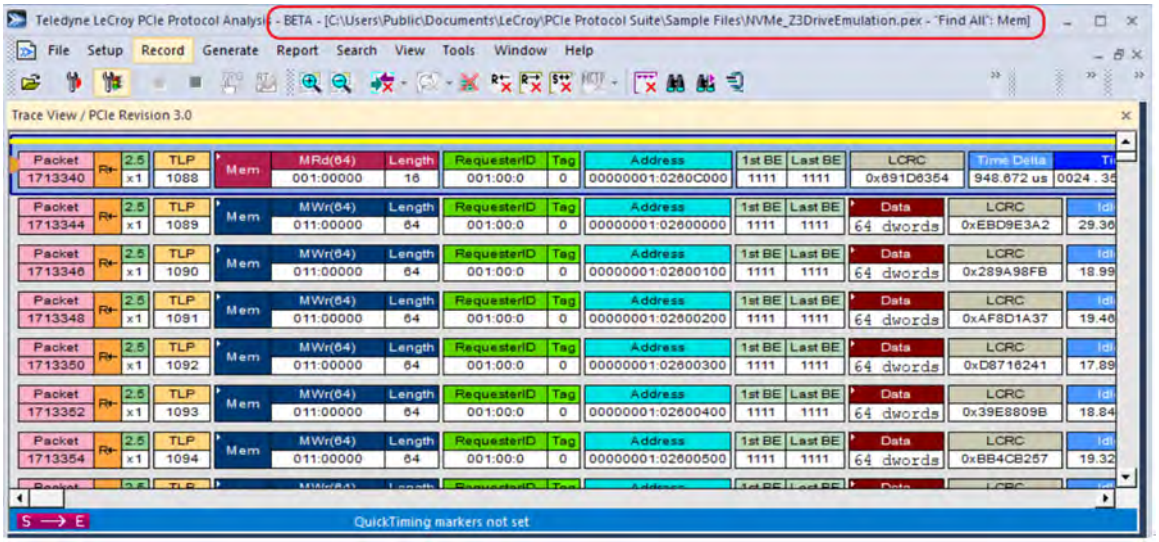


Figure 4.17: Name of Trace with Search Name

Byte Position

There are two ways to search by Byte Position: **Sliding** or **Fixed**.

Sliding searches for entered values everywhere without a specific Dword position. For the TLP Data Pattern search category, Use the "+" and "-" buttons to add more (up to 1024 Dwords) or remove extra (minimum 1 Dword present) Dwords. See Figure 4.18.

I

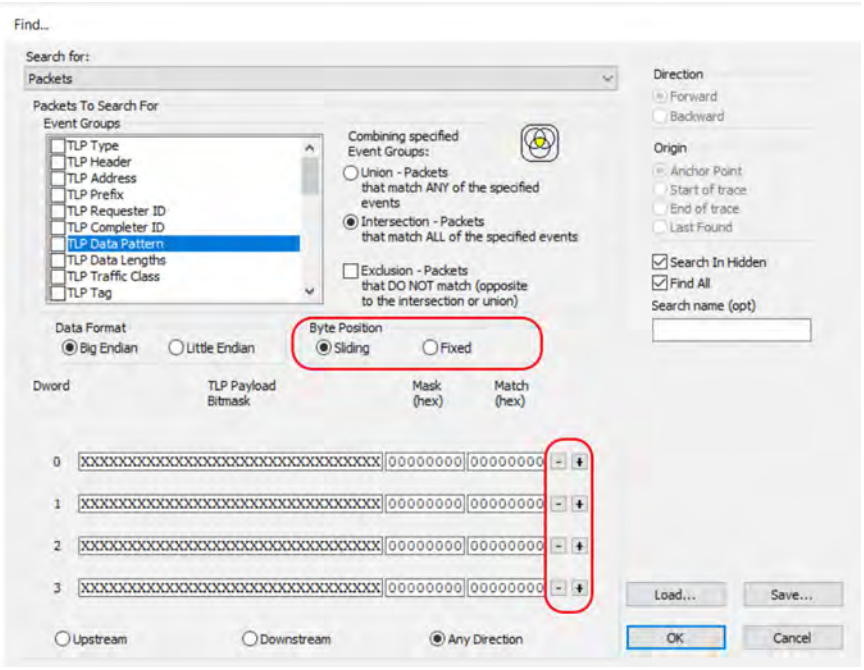


Figure 4.18: Find by Byte Position - Sliding

Fixed byte position searches for entered values in a specific Dword position. To select the specific Dword position, enter a Dword index number in the input field before the Bitmask. See Figure 4.19.

Note: The Dword index only allows numerical values. The maximum value allowed is 1023.

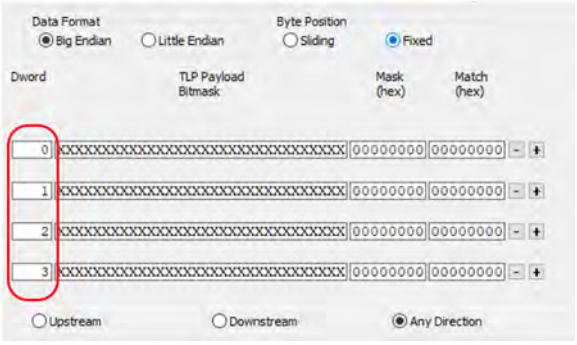


Figure 4.19: Find by Byte Position - Fixed

4.4.6 View Menu

Toolbars>>	Displays available toolbars: Standard, View Type, Frequently Used, Analysis, and Transaction Level. Use Customize to display the Windows Customize window.
Analyzer Network Chat Bar	Opens a chat window for communicating with persons working with networked Analyzers. This command requires that your host machine be attached to a LAN. The Chat window broadcasts messages to whatever host machines have been connected.
Status Bar	Switches display of the Status Bar on or off.
QuickTiming Bar	Switches display of the QuickTiming Bar on or off.
CATC Walk	Lets you play a playlist or manage Playlists (see “CATC Walk Playlist” on page 694).
Real Time Statistics	Opens the Real Time Statistics monitor dialog and displays a real-time graph of link activity.
Unhide Cells	Unhides PQI Reserved, PQI SGL Reserved and SOP reserved cells. You can also select Unhide all.
Script Editor	Displays the Script Editor (only appears if a **.peg** file is open).
Zoom In	Zoom in increases the size of the displayed elements.
Zoom Out	Zoom out decreases the size of the displayed elements.
Wrap	Wraps displayed packets within the window.
Synchronize Trace View With Other Views	Synchronizes the Trace view with other views.
FC Credits	Toggles a display for tracking Flow Control Credit update and consumption on a PCI Express link.
FC Credits Setup	Allows you to customize the display for tracking Flow Control Credits.
Compact View	Toggles compacting of the Link Training sequence to analyze CATC Trace data faster or no compacting to display more data.
Packet Level	View the current recording at the Packet Level.
Link Transaction Level	View the current recording at the Link Transaction Level.

Split Transaction Level	View the current recording at the Split Transaction Level.
Lane Margining Commands/ Responses Level	View the current recording with Lane Margining Commands and Responses.
Lightweight Notification Commands and Responses	View the current recording of Lightweight Notification Commands and Responses.
NVMe Transaction Level	View the current recording at the NVMe Transaction Level.
PQI Transaction Level	View the current recording at the PQI Transaction Level.
ACHI Transaction Level	View the current recording at the ACHI Transaction Level.
ATA Transaction Level	View the current recording at the ATA Transaction Level.
SOP Transaction Level	View the current recording at the SOP Transaction Level.
SCSI Transaction Level	View the current recording at the SCSI Transaction Level.
Restore views to default positions	Restores views to the default positions after you click **Yes** on the prompt.

4.4.7 Tools Menu

Configuration Space Editor	Displays the Configuration Space Editor dialog which allows you to either create a new Configuration Space File or open an existing Configuration Space File.
Memory/IO Space Editor	Displays the Memory/IO Space Editor dialog which allows you to either create a new Address Space File or open an existing Address Space File. Select the memory size from the drop-down menu.
Interposer Programmer	This utility allows you to program the Continuous Time Linear Equalizer (CTLE) and DCGain between the host (root complex) and device (end-point) on the interposer connected to your analyzer to achieve optimum link performance.
Probe Calibration	Opens Autotune and Calibration Wizard.
RDE Dictionary Management	Displays RDE Dictionary.
TC to VC Mapping	Allows Traffic Classes to be mapped to Virtual Channels for purposes of simplifying navigation (for example, Search > Go to > TLP Virtual Channel) and changing the way the CATC Trace is displayed (for example, in Split Transactions).
Timing Calculations	Starts the mode-less calculator dialog for calculating various timing and bandwidth parameters in the recording file.
PCIe SSD Base Address Mapping	Displays the PCIe SSD Base Address Mapping dialog.
NVMe MI Configuration	Displays NVMe MI Configuration.
Import PCIe Configuration Space	Imports PCIe Configuration Space.
Run Verification Scripts	Displays a list of verification scripts, from which you can run a verification script.

4.4.8 Window Menu

This menu helps display the loaded traces.

New Window	Opens a copy of the current CATC Trace window.
Cascade	Displays all open CATC Trace windows in an overlapping arrangement.

Tile	Displays all open CATC Trace windows as a series of strips across the display.
Arrange Icons	Arranges minimized CATC Trace windows at the bottom of the display.
Synchronize Traces	Synchronizes the CATC Trace View windows so that a move in one window repositions the other window of the same recording.
Windows	Displays all open windows. Select to display. See Figure 4.20 on page 97 and Figure 4.21 on page 98 as well as "Trace Display Options" on page 98.

For a more detailed explanation of the Window Menu options see Figure 4.20 and Figure 4.21 as well as "Trace Display Options" on page 98.

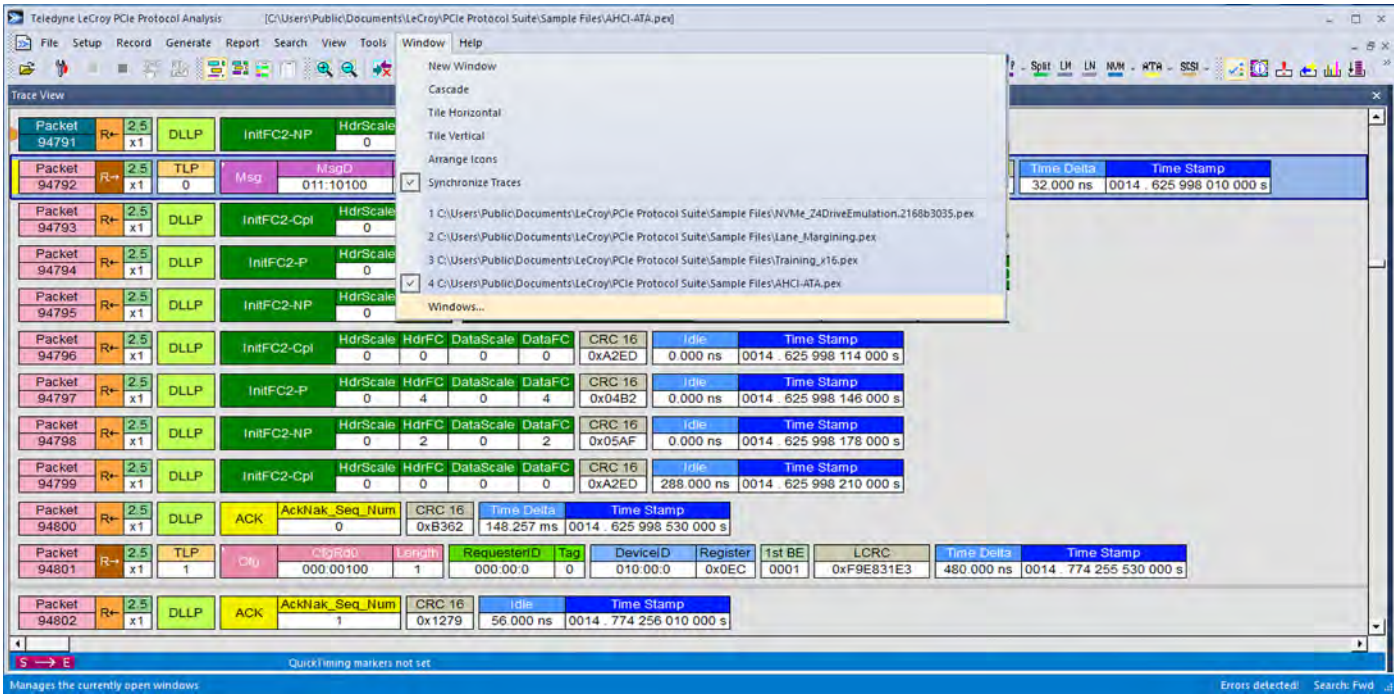


Figure 4.20: Window: Windows Menu with four traces loaded

Windows... Feature

Selecting **Windows...** from the Window menu, the Windows dialog displays with the list of loaded traces. See Figure 4.21.

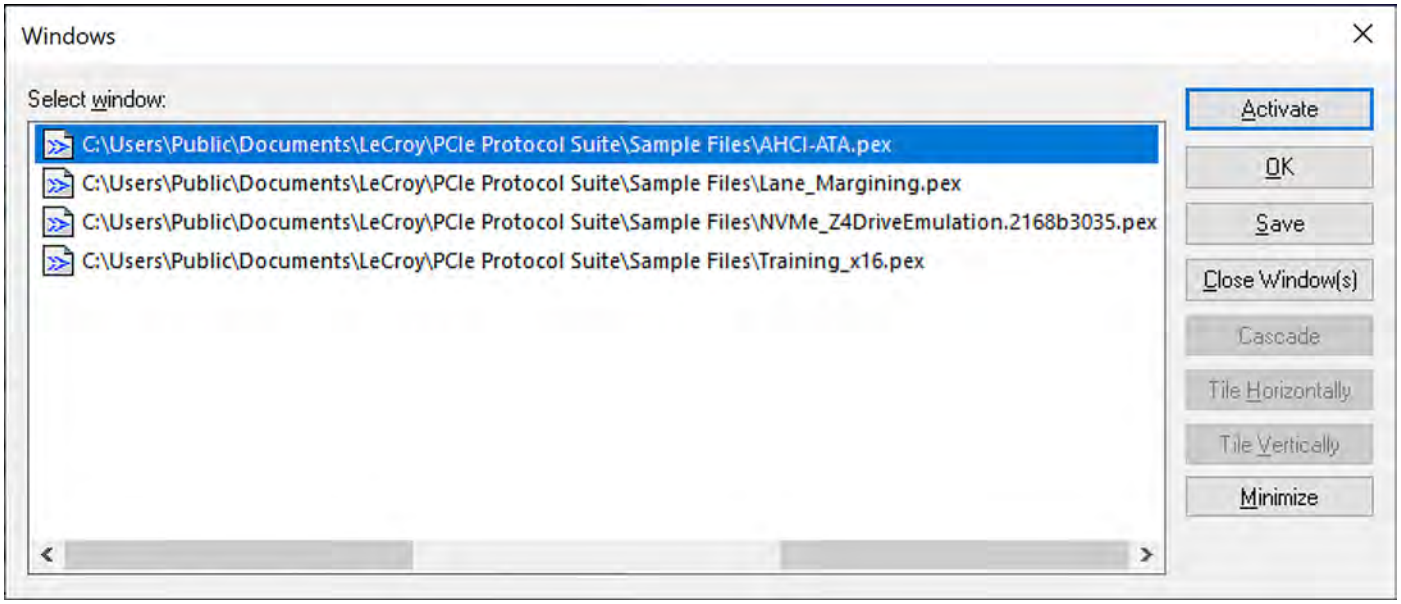


Figure 4.21: Window: Windows menu with four traces loaded

Trace Display Options

The following options are available:

- Activate - makes selected trace active in the Trace View.
- OK - closes dialog.
- Save - This is useful for Generation Scripts, it brings up save dialog to save changes in generation script, for opened trace it does nothing.
- Close - closes selected window(s).
- Cascade, Tile Horizontally and Tile Vertically - enabled only when multiple windows are selected. Cascades or tiles selected windows.
- Minimize - minimizes selected window.

4.4.9 Help Menu

User Manuals F1	Click User Manuals or press F1 to access the documentation guide for all Teledyne LeCroy PCIe products.
Display License Information	Opens an information box describing the current license information.
Register Product Online	Register at the Teledyne LeCroy website registration page.
Check for Updates	Check whether a new software version is available. If so, you can download from the Teledyne LeCroy web site. https://teledynelecroy.com/sw/pciexpress/ You can select to **Check for updates at application startup**

Tell Teledyne LeCroy	Report a problem to Teledyne LeCroy Support via e-mail. This requires that an e-mail client be installed and configured on the computer.
Shortcut List	Displays a list of Keyboard shortcuts.
About PCIe Protocol Analysis	Displays version information about the attached Analyzer and its Firmware and BusEngine™.

4.5 Dashboard View

Dashboard View shows the state that the link that analyzer is tracking. Click the Dashboard View  icon to view the Dashboard View window for the selected device at the bottom left of the application.

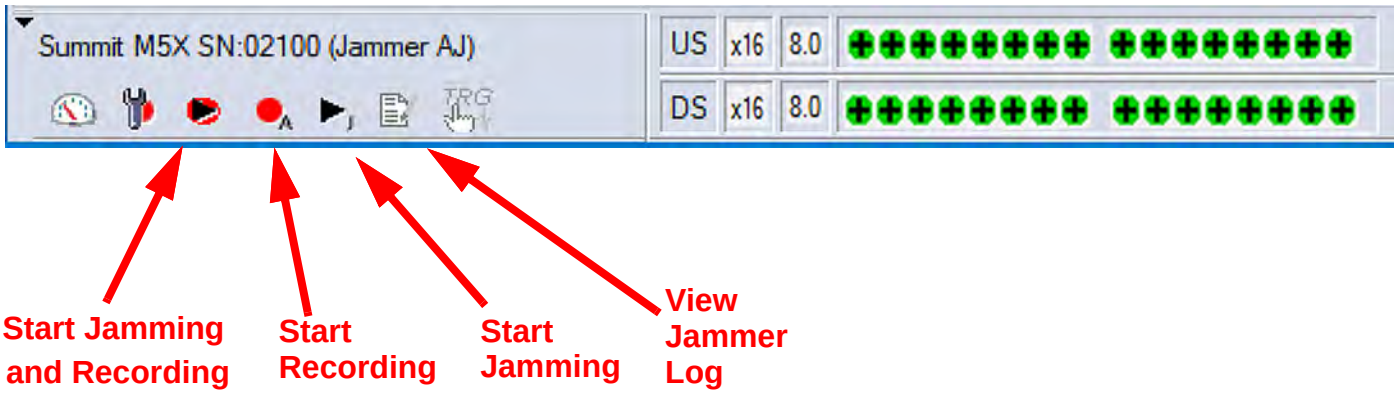


Figure 4.22: Dashboard View Icon Displaying Device

Dashboard (see Figure 4.23 on page 100) displays the following information for Upstream and Downstream:

- Link Width
- Link speed
- Per lane activity indication
  - Green - lane is active, analyzer does not detect any signal errors on this lane
  - Orange - lane is active, analyzer detects signal errors on this lane
  - Grey - lane is inactive
- Logical to physical lane mapping
- Lane polarity
- Link Number
- NFTS - The number of FTS advertised by the device for each speed

Note: The dashboard display depends on the Recording Options configuration and may not match the current actual link state. For example, if the analyzer is configured to track 2.5 GT/s speed only, the Dashboard View will display 2.5GT/s speed as a current tracking speed regardless of the actual speed of the link.

Note: The update to the status bar requires reading the current state of the analyzer. This happens at the end of the recording. In case the analyzer is power cycled, perform at-least one recording to have the updated status bar with current analyzer link information.

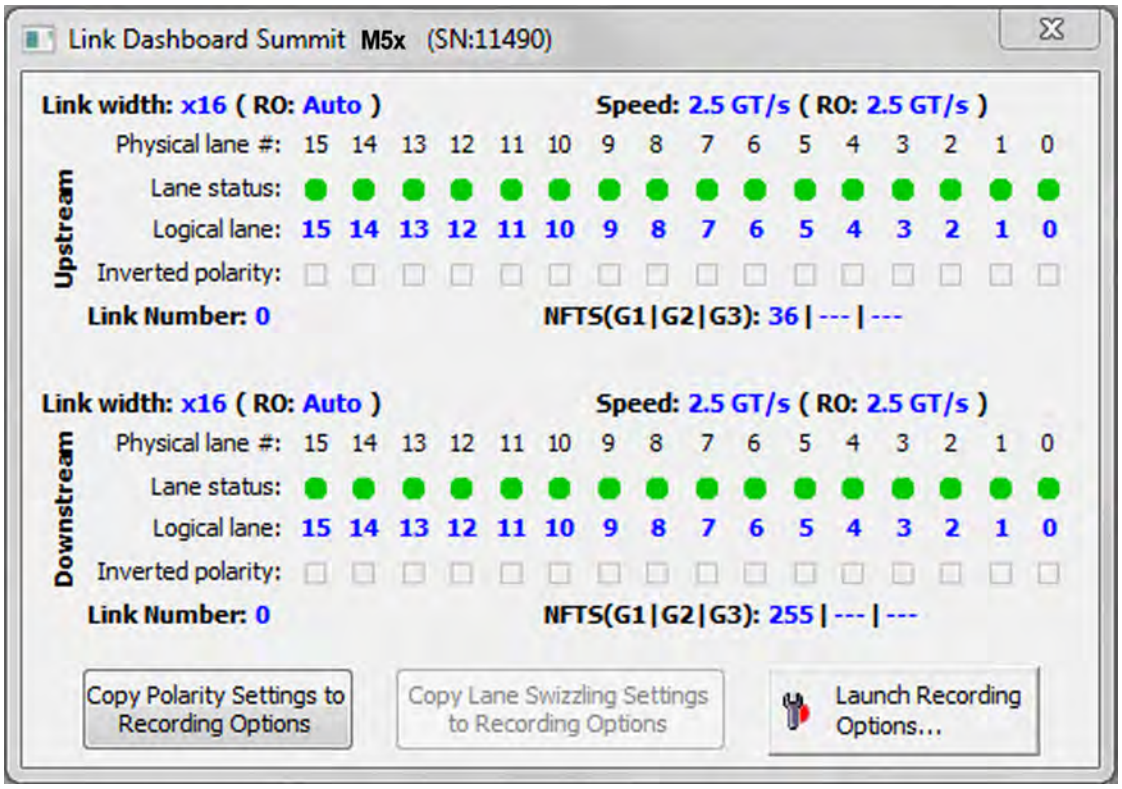


Figure 4.23: Dashboard View Dialog

You can launch Recording Options for the analyzer from the Dashboard View and adjust recording settings to match the current link configuration. The **Copy Polarity Settings to Recording Options** button allows you to copy the detected polarity into Recording Options. The **Copy Lane Swizzling Settings to Recording Options** button allows you to copy the detected Lane Swizzling Settings into Recording Options.

Note: Polarity auto detection and lane swizzling detection requires the link to go through link retraining at Gen1 or Gen2 speed. The analyzer has to be configured correctly to track this link retraining. For example, if the analyzer is configured to track only 8.0 GT/s speed, auto polarity detection will not work even if the link goes through the appropriate retrain.

4.5.1 Launching and Setting Recording Option from Dashboard View

You can select a device and click the **Launch Recording Options as shown in** Figure 4.23 on page 100 button to go to **Recording Options**. In the Recording Options window the Upstream and Downstream channels can be set manually by unchecking the **Auto-Configure Lane Polarity** checkbox, refer to Figure 5.2 on page 134 (3G). Click on the **Port Polarity Settings to Recording Options** to save the settings.

Note: The lane polarity values are dynamic so this feature allows the user to make the settings and save them for future use.

In the default setting the **Auto-Configure Lane Polarity** checkbox is selected, refer to Figure 5.2 on page 134 (3G).

4.6 Jammer Log View

The Jammer Log View shows you lists of performed Jammer Actions. Clicking the View Jammer Log icon  opens the Jammer Log View window for the selected device, at the bottom left of the application.

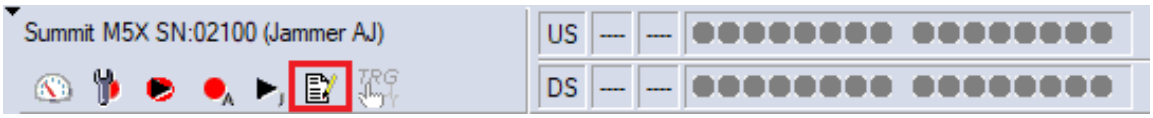


Figure 4.24: Jammer Log View Icon

Jammer Log View can be opened only after starting **Jamming** or **Jamming and Recording** and it displays the following information for Upstream and Downstream:

- Timestamp
- Jammer Action
- Status

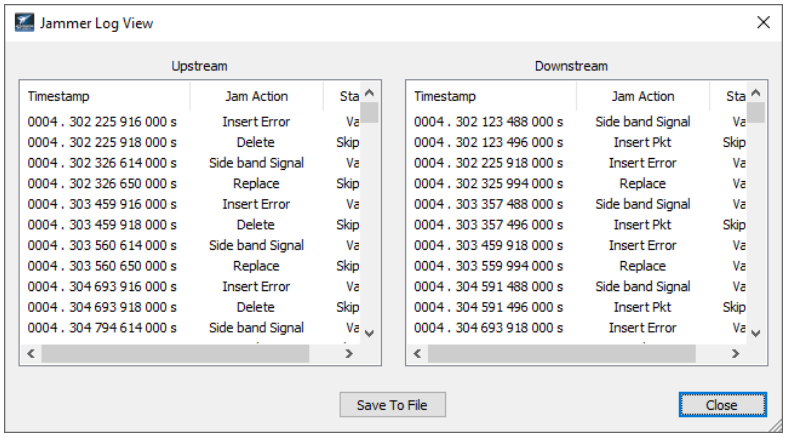


Figure 4.25: Jammer Log View Showing Performed Jammer Actions

The **Save To File** button allows you to save the information from Jammer Log View to a text file.

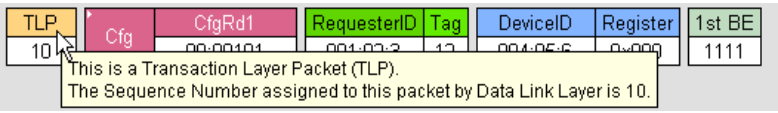
Also you can navigate to the corresponding Jammer Log Packet in the recorded trace by clicking on the cell in Timestamp column.

Note: Jammer Log View shows the performed Jammer Actions only for the last recording session. After starting new **Jamming** or **Jamming and Recording** the lists will be updated. So navigation will work only for the last recorded trace.

If the option **Synchronize Trace View With Other Views** is enabled, then after opening Jammer Log View the lists for Upstream and Downstream will synchronize the position with Trace View.

4.7 Tool Tips

Tool tips provide details about fields within the CATC Trace. To see a tool tip, position your mouse pointer over a field within the CATC Trace.



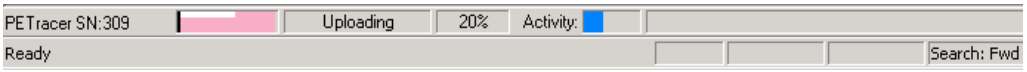
You can turn off this capability in the Display Options menu.

4.8 Keyboard Shortcuts

Keystrokes	Operation
Ctrl+N	New PCIe Protocol Analysis script
Ctrl+O	Open file
Ctrl+P	Print
Ctrl+S	Save file
Ctrl+R	Start Analyzer recording
Ctrl+T	Stop Analyzer recording
Ctrl+Home	Jump to first packet
Ctrl+End	Jump to last packet
Ctrl+G	Go to packet...
Ctrl+F	Open Find dialog
Ctrl+1	Access documentation
F3	Find next
F6	Next pane
Shift+F6	Previous pane
Ctrl+B	Search backward

4.9 Status Bar

The Status Bar is a gray bar that runs along the bottom of the application window.



From left to right:

PCIe Protocol Analysis SN:309: Analyzer Serial Number

Ready: Analyzer Status

Recording Progress Bar: The colored bar to the right of the serial number represents how much traffic has been recorded. The trigger point is indicated by the black line at the left side of the bar. In this example, the trigger occurred at the very beginning of the CATC Trace. If the trigger is set in the middle of the CATC Trace, the line is positioned in the middle of the bar. Additionally, the color of the bar is different on each side of the trigger point. For examples, see “Recording Progress Bar” on page 103. The white strip along the top edge of the color bar indicates how much traffic has been uploaded from the Analyzer buffer to the host machine.

Uploading and 20%: Indicates the Analyzer's recording status, what part of the recording process the Analyzer is now in. In this example, the Analyzer is in the upload stage and has completed 20% of the upload from the Analyzer to the host machine. See “Recording Status” on page 103 for details on other status messages.

Activity: The colored bar moves to indicate that the Analyzer is currently recording.

Search: Fwd: Indicates search direction. The direction can be toggled to **Search: Bwd** by double-clicking the search direction or by selecting **Toggle Search Direction** from the Search menu.

4.9.1 Recording Progress Bar

This indicator bar changes color to reflect the recording progress.

- Black vertical line is at the location of Trigger position.
- Black vertical line wiggles when Trigger Position is nearly reached.
- Field to right of Trigger Position changes color to indicate post-trigger activity.
- Upper half of progress indicator turns white when recording is complete.

4.9.2 Recording Status

The second segment from the left in the Status Bar indicates recording status.

During recording, the current Recording Status is in a segment. When you activate the **Record** function, this segment flashes a message depending on the selected Recording Options, such as **Waiting for Trigger**, **Uploading** or **Triggered**.

- The status bar displays **Waiting for Trigger** while waiting for trigger to occur based on the settings defined in the Recording Options.



Figure 4.26: Status Bar - Waiting For Trigger

The status bar displays **Uploading** when recording is complete and is being uploaded (see Figure 4.27 on page 104).

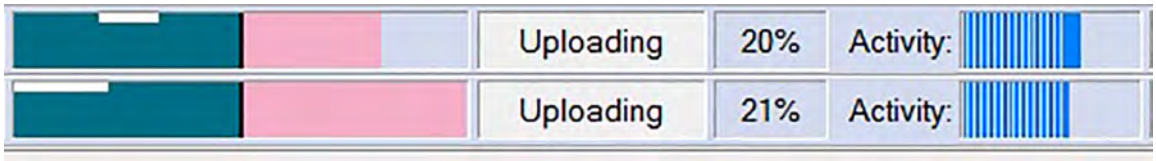


Figure 4.27: Status Bar - Uploading

The status bar displays **Triggered** when the trigger condition has occurred, but uploading has not commenced yet.

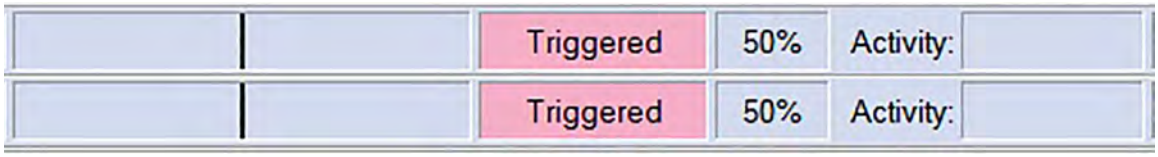


Figure 4.28: Status Bar - Triggered

As uploading progresses, the percent increases to 100. You can abort this upload if you wish by pressing the **ESC** button on your keyboard or

clicking  in the Tool Bar.

4.9.3 Recording Activity

The third segment displays recorded activity as a series of blue vertical bars. The more vertical bars that display, the greater the amount of activity recording. If there are no vertical bars, there is no recording activity.

During uploading, the percent of the completed upload displays.

4.9.4 Search Direction Indicator

The fourth segment in the status bar indicates search direction. The direction can be changed by selecting Toggle Search Direction from the Search menu.

4.10 Making a PCI Express Recording

When the analyzer is not yet detected, you can choose the analyzer from the drop-down menu which displays the following:

- **Summit M5x Gen5:** Displays the options for the Summit M5x Gen5 Analyzer.
- **Summit M5x AJ:** Displays the options for the Summit M5x Analyzer/Jammer. (See Chapter 5, “Recording Options: AJ Mode,” on page 131).
- **Summit T416 Standard:** Displays the options for the Summit T416 Analyzer.
- **Summit T416 4 Ports:** Displays the options for the Summit T416 Analyzer used in Multiport mode.
- **Summit T416 2 Ports:** Displays the options for the Summit T416 Analyzer used in Multiport mode.
- **Summit T48 Standard:** Displays the options for the Summit T48 Analyzer.
- **Summit T48 2 Ports:** Displays the options for the Summit T48 Analyzer used in Multiport mode.
- **Summit T48** (2 Units): Displays the same options as Summit T3-8 but lists **Unit 1** and **Unit 2** in the Link Section on the right. In a two-unit setup, **Unit 1** and **Unit 2** are two separate Analyzers linked together.
-
- **Summit T3-16**: Displays the options for the Summit T3-16 Analyzer.
- **Summit T3-8** (2 Units): Displays the same options as Summit T3-8 but lists **Unit 1** and **Unit 2** in the Link Section on the right. In a two-unit setup, **Unit 1** and **Unit 2** are two separate Analyzers linked together.
- **Summit T3-8**: Displays the options for the Summit T3-8 Analyzer.
- **Summit T34** (2 Units): Displays the same options as Summit T34 but lists **Unit 1** and **Unit 2** in the Link Section on the right. In a two-unit setup, **Unit 1** and **Unit 2** are two separate Analyzers linked together.
- **Summit T34:** Displays the options for the Summit T34 Analyzer.
- **Summit Z416:** Displays the options for the analyzer portion of the Z416.
- **Summit T28**: Displays the options for the Summit T28 Analyzer.
- **Summit T24**: Displays the options for the Summit T24 Analyzer.

After connecting the Analyzer to the device(s), you must select Standard Mode (see “PCIe Protocol Analysis Files” on page 109). The default mode is usually Standard Mode.

To make this recording, follow these steps:

1. From the **Setup** menu, select **Recording Options** and click the **Switch to Simple Mode** button.
2. Select the **Simple Mode** tab (see Figure 4.29 on page 106).

   The following window displays the factory default settings in **Simple Mode**, such as Snapshot and 32-MB buffer size. For your first recording, select the proper speed and link width.

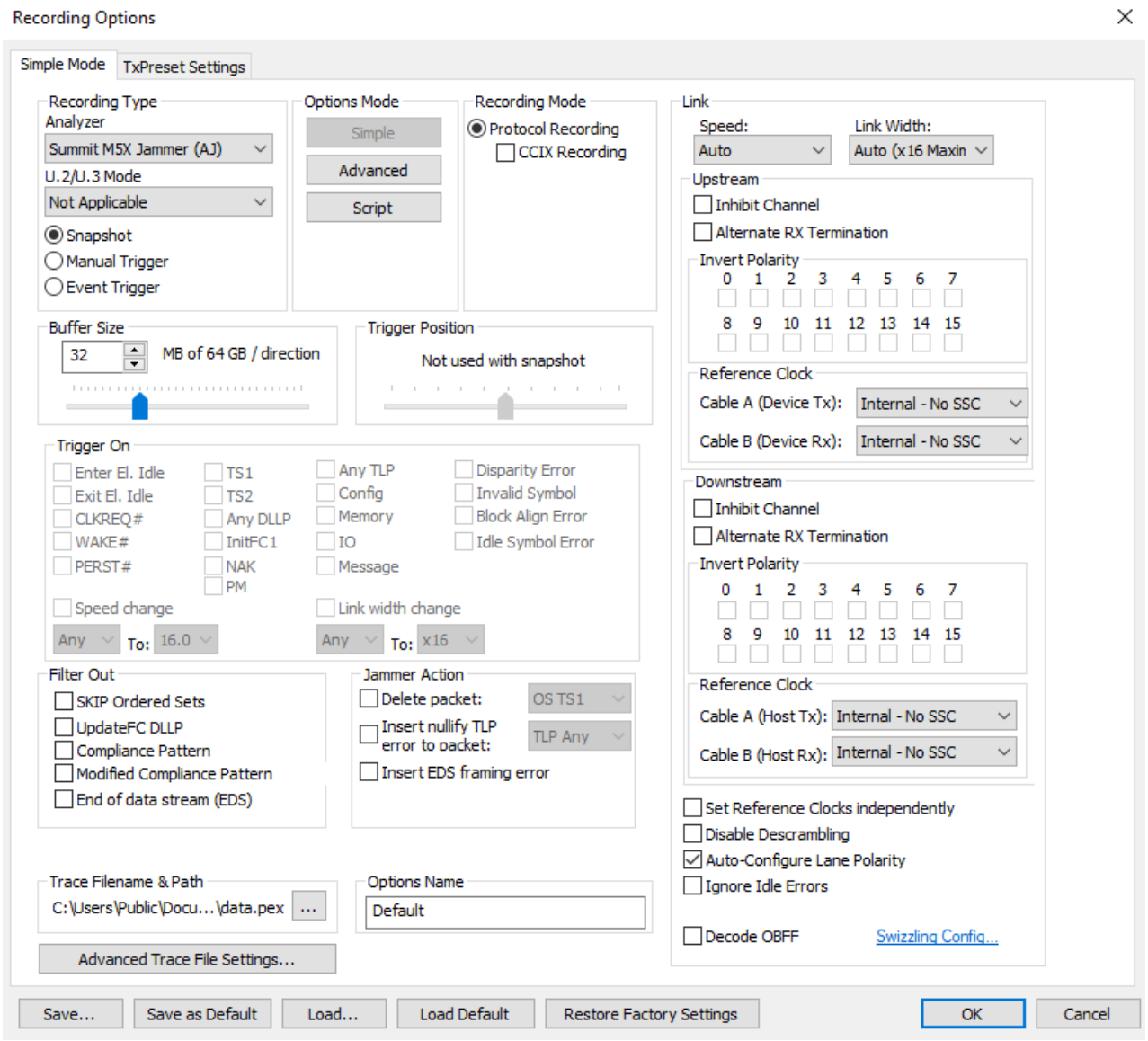


Figure 4.29: Summit M5x in Simple Recording Mode

3. In the **Link** section, specify the lane width of the PCI Express link to be analyzed. The rest of the settings in this section can be left at the factory defaults for most PCI Express systems.

4. For multi-lane PCI Express links when using Auto options, the Analyzer needs to observe link training in order to record link traffic correctly.
5. Click **OK** at the bottom of the Recording Options dialog to apply the Analyzer recording settings specified.
6. Click the **Record**  button.

4.10.1 Stopping a Recording

You can stop the recording process at any time by pressing the **Stop** button ■. This causes the Analyzer to stop the recording and upload the CATC Trace to the host machine. If you press the **Stop** button again, the Analyzer temporarily halts the upload process and opens the following dialog box.

Note: If the uploading process is stopped manually, the resulting trace may have significant periods of time where the traffic from upstream and downstream will seem like they are not interleaved. Teledyne recommends to always let the analyzer complete the upload process.

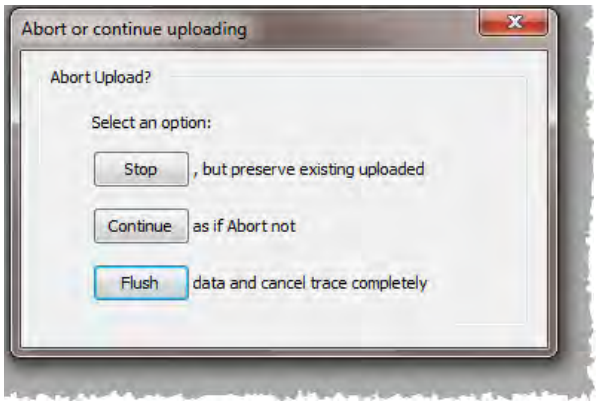


Figure 4.30: Abort Upload

This dialog presents options for stopping, continuing, or aborting the upload:

- **Stop**: Aborts further CATC Trace upload and displays whatever data that has already been uploaded.
- **Continue**: Resumes the upload. This command tells the Analyzer to finish uploading whatever CATC Trace data is still in its buffer.
- **Flush**: Flushes the CATC Trace without saving or displaying it.

If you allow the traffic data to be uploaded, it is automatically saved on the host machine's hard drive as a file named **data.pex** or the name you assign as the default filename in the recording options.

4.10.2 Saving a Recording

1. To save a current recording for future reference, select **Save As** from the File menu.
2. Give the recording a unique name, then save it to the appropriate directory.

4.11 PCIe Protocol Analysis Files

The PCIe Protocol Analysis creates and uses different kinds of files:

- **CATC Trace Files**: Recorded traffic
- **Recording Options Files**: Configuration file that contains the various options selected in the Recording Options dialog to configure the recording
- **Display Options Files**: Configuration file that contains the options selected in the Display Options dialog to configure how traffic is displayed

4.11.1 CATC Trace Files

PCIe Protocol Analysis records PCI Express traffic into a CATC Trace file with the default name **data.pex** or any other that you specified in the Recording Options. This file is overwritten with new data each time PCI Express traffic is recorded.

If you want to save a CATC Trace, use the **File > Save As** function. This option allows you to save the current CATC Trace to a unique file name, thereby ensuring that it is not overwritten. This option also allows you to save a range of packets in a CATC Trace file.

You can pre-define the name of the recorded CATC Trace file using the Trace Filename and Path option in Recording Options.

4.11.2 Recording Options Files

Recording Options files are created when you set recording options. These files use the **.rec** or the **.crec** extension and contain recording option information. See "Saving and Loading Previously Saved Recording Options" on page 149.

4.11.3 Display Options Files

Display Options files are created when you set display options. These files use the **.opt** extension and contain the display options information.

4.12 Saving CATC Trace Files

4.12.1 Using the Save As Function

When you record a CATC Trace file, the Analyzer software provides a pre-defined name to the CATC Trace file (**data.pex** or any other that you specified in the Recording Options). If you do consecutive recordings, each time the previous recording is overwritten. If you see a recording you want to analyze later, you need to give a unique name to the CATC Trace file, so it is not overwritten with the next recording.

Also, when you analyze a recorded CATC Trace file, you might be interested in preserving just a part of the PCI Express traffic that was recorded. If you save a portion of a CATC Trace file, it can get significantly smaller, allowing you to attach it to an e-mail.

To save a portion of a CATC Trace file or the whole file to a unique name, select **Save As** from the File menu (see Figure 4.31 on page 110).

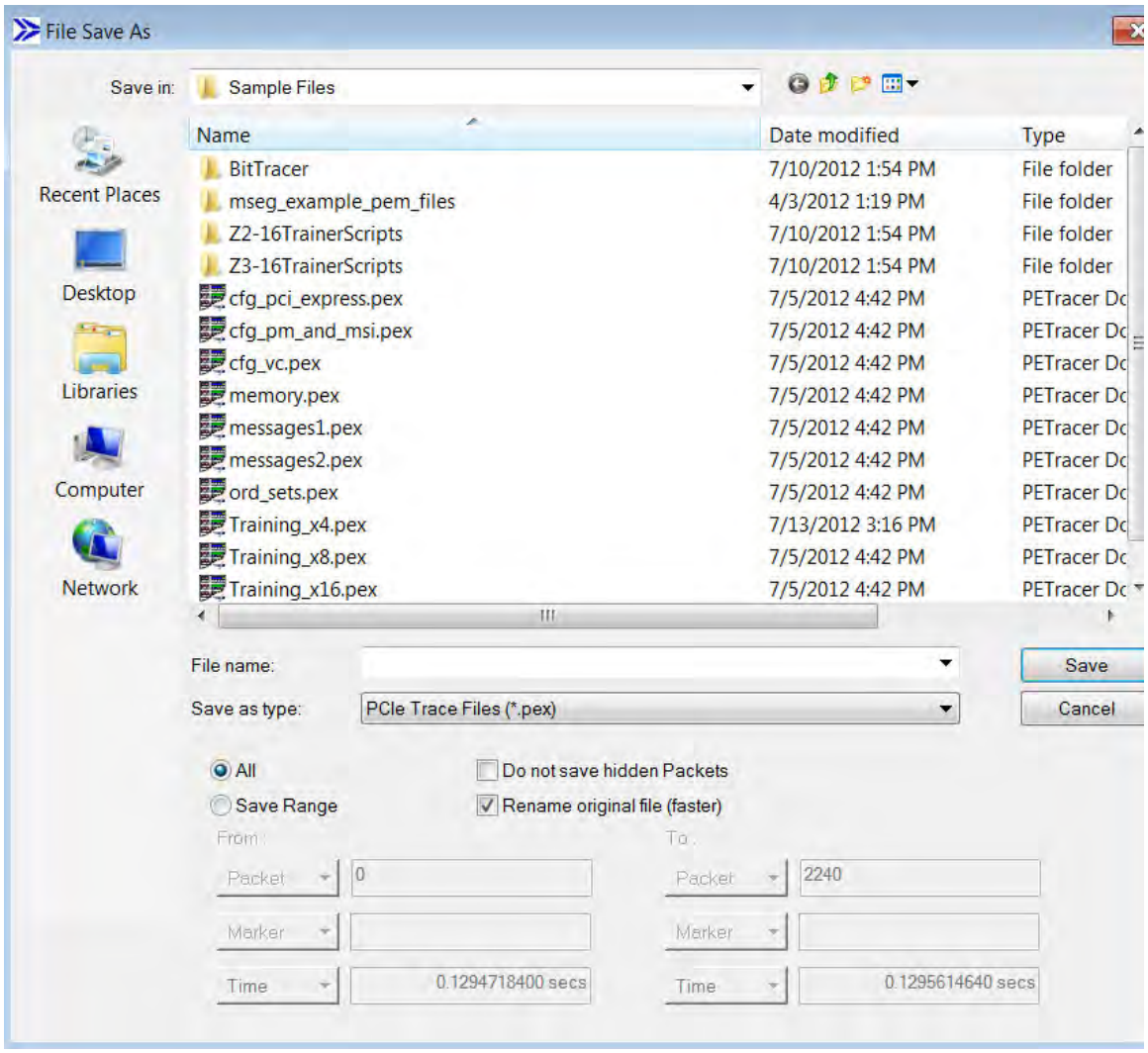


Figure 4.31: File Save As Dialog

If you want to give a unique name to the CATC Trace file, select the **All** option and keep **Rename original file** checked. This is the default setting for the dialog. The existing file will be overwritten with the new file name.

4.12.2 Saving a Portion of a CATC Trace

If you want to save a portion of a CATC Trace file, select **Save packet range**. Enter starting and ending packet numbers in the **From Packet** and **To Packet** fields. By default, it has the numbers of the first and the last packets in the file. The software is going to save all the packets in specified range to the new file, unless you have **Do not save hidden packets** checked. In this case it is going to save all packets in the range, EXCLUDING the currently hidden packets.

4.12.3 Save Copy As Function

If you want to Save a trace (or a portion of a trace) to a new file name but keep the existing file name select Save Copy As. See Figure 4.32.

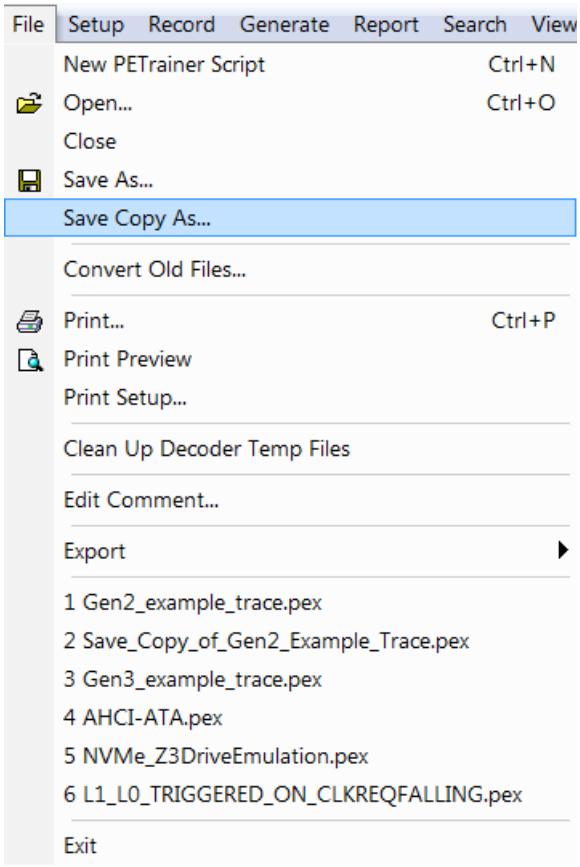


Figure 4.32: File -> Save Copy As Function

Select Save Copy As and the following dialog will pop up and you can enter a unique file name (see Figure 4.33 on page 112).

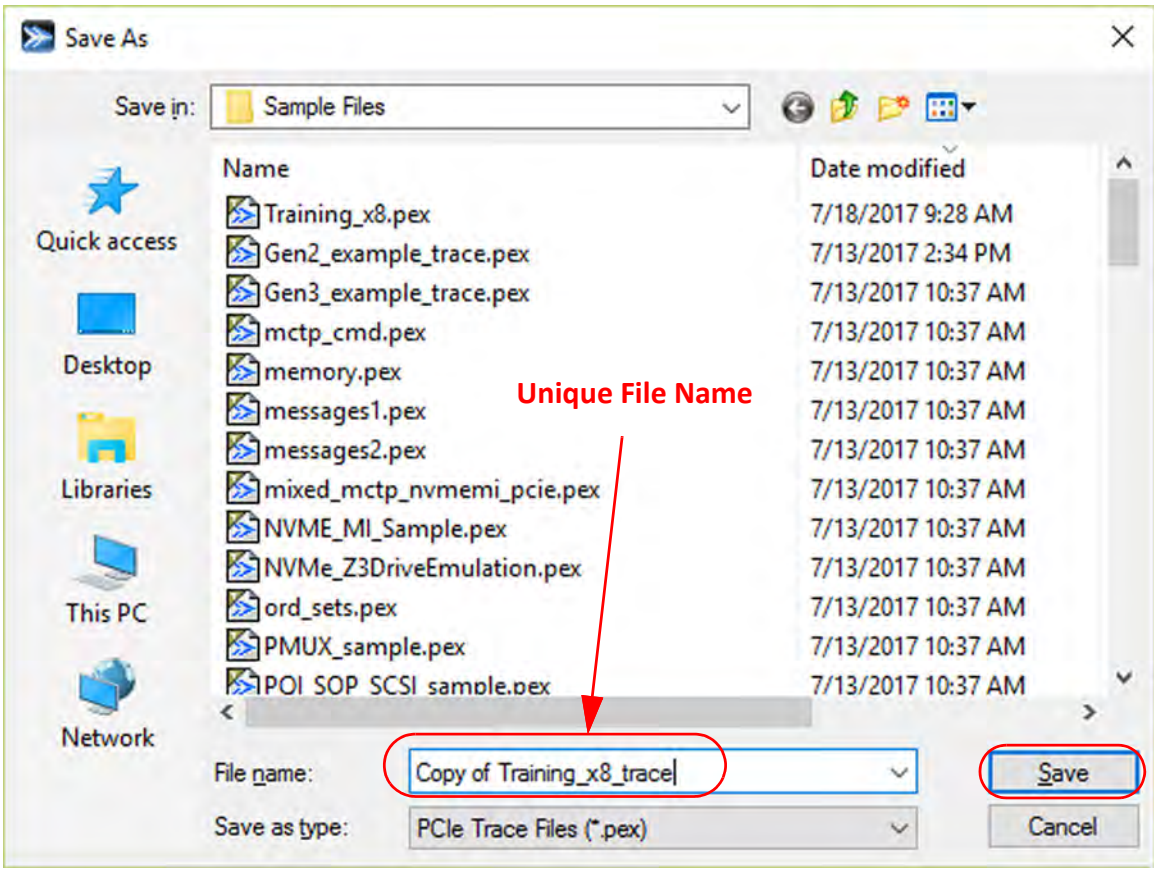


Figure 4.33: Save As Copy Dialog (Sample File Directory Before Save)

Click on the Save button and the trace will be saved with the new file name. This file can be loaded by Selecting File -> Open and selecting the new file and selecting the Open button. See Figure 4.34.

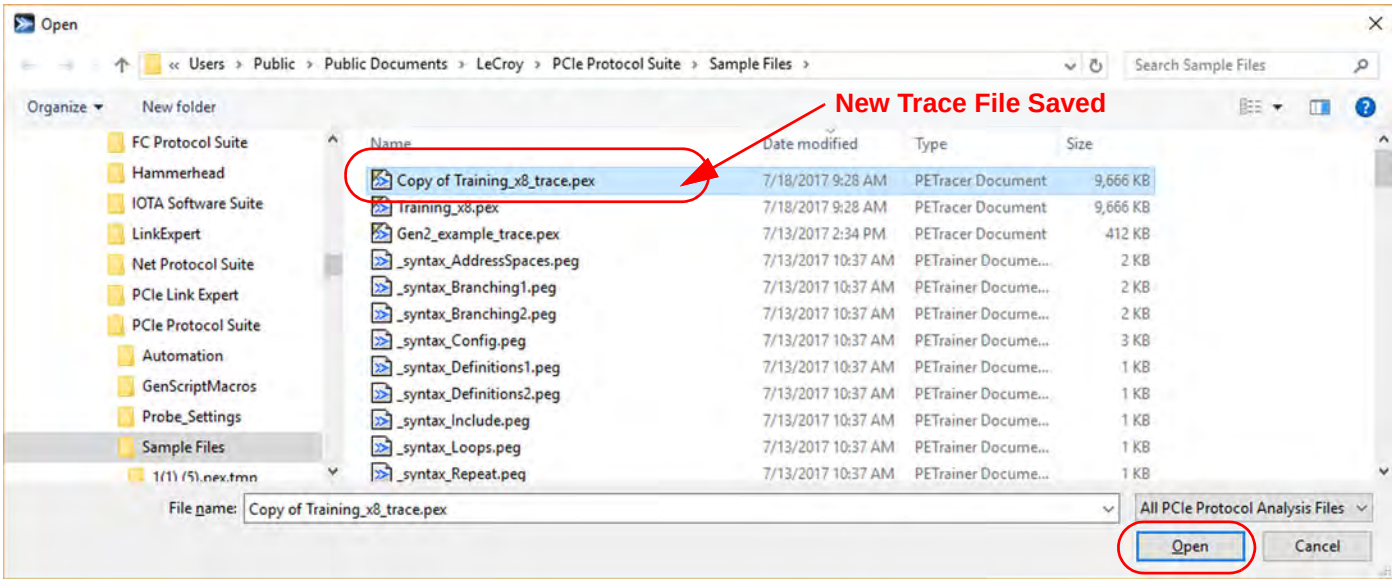


Figure 4.34: File -> Open: New Trace File Available

4.12.4 Trace File Structure

The captured trace file has an extension of ".pex". When the trace file is loaded, additional decoding and data reduction is done which results in additional files of data which are placed in a folder of the same name as the trace file (with the extension ".tmp"). This allows the trace file to be loaded and displayed quickly during subsequent viewings.

When copying a trace file, or sending it to someone, you can chose to send just the .pex file. In that case, the software re-generates the additional folder and files when the trace is first opened. The other choice is to send the additional folder with contents along with the .pex file, which will save the rebuilding effort when the file is opened again. The choice is up to the user. If you do NOT want these files kept, and don't mind the extra time it takes to re-build these every time you load a trace file, then you can select this in the Recording Options.

If the additional files ever become out of date (newer software structures from a new release, etc.) or if any of the files are lost or damaged, the software will rebuild a fresh version of the information.

4.13 Exporting a CATC Trace File

By default, PCIe Protocol Analysis saves CATC Trace files in the **.pex** format. However, you can export a CATC Trace to a file in any of the following other formats:

- Text
- Comma Separated Value (CSV)
- Generator file format

Exporting to Generator file format is a simple way to create a script file from your CATC Trace. Only PCI Express packets will be exported to a script. All transaction levels, including supported SSD decodes, can be exported to Text or CSV Text.

To export a CATC Trace file, select **File > Export**.

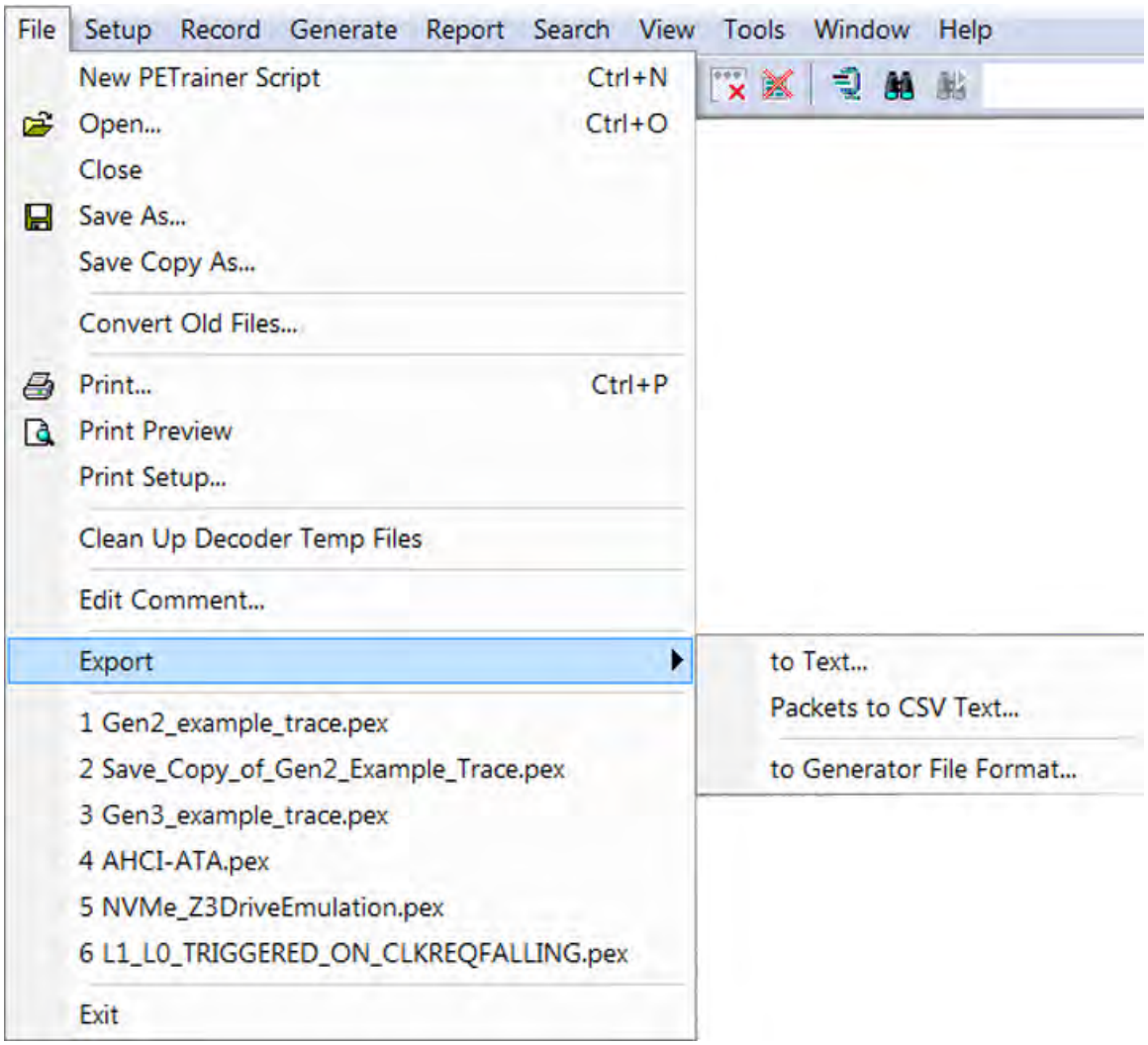


Figure 4.35: Exporting a File

4.13.1 Export: To Text

Select Export => To Text, a window pops up that has a button to select legacy format, which would not effect older scripts (see Figure 4.36) or to use the newer default format. See Figure 4.38 on page 116.

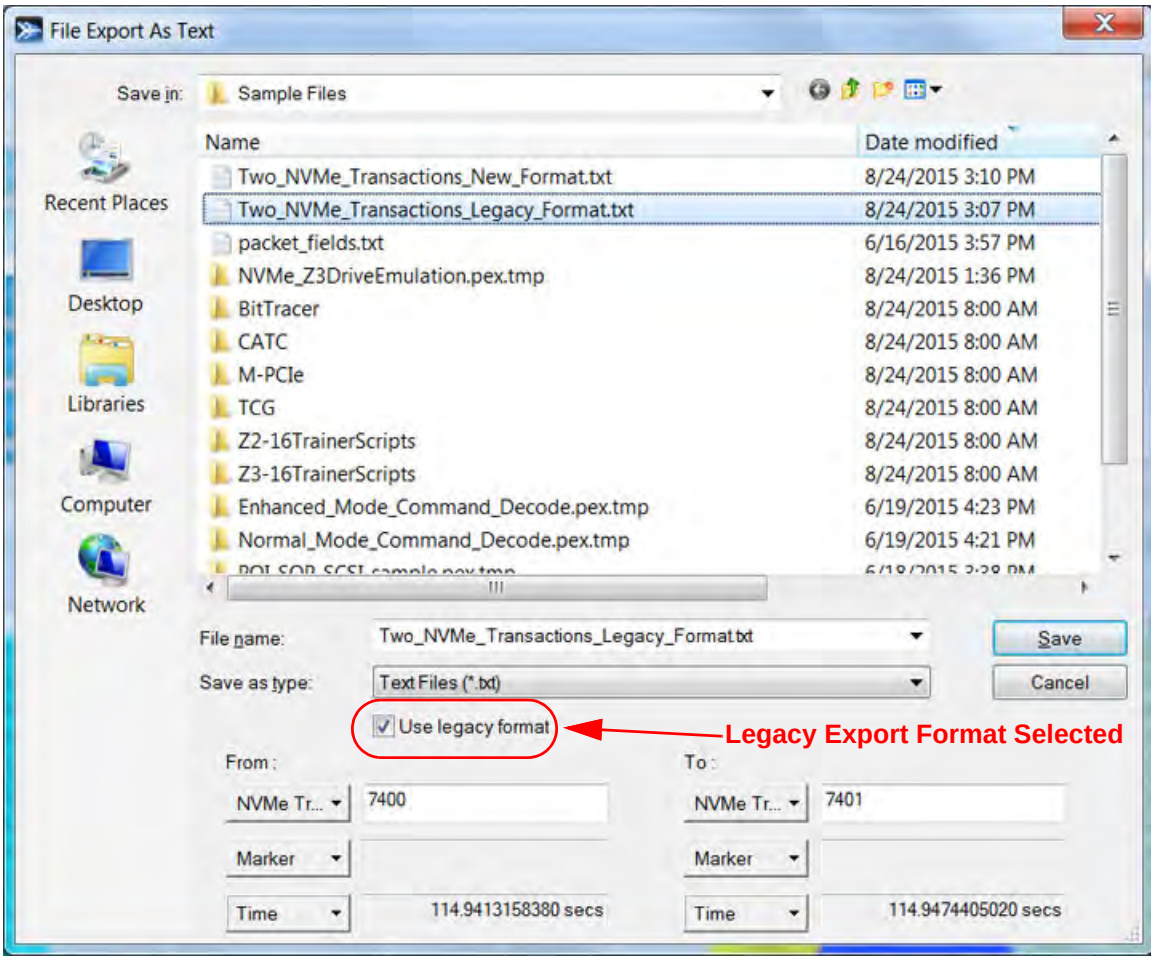


Figure 4.36: Export Two NVMe Transactions to Text File, Legacy Format

You can also select to Export only a portion of the Trace by setting the “From” and “To” menu items at the bottom of the dialog. You can select from Packets (or decoded Items see Figure 4.37) , Markers or Time see Figure 4.38 on page 116.

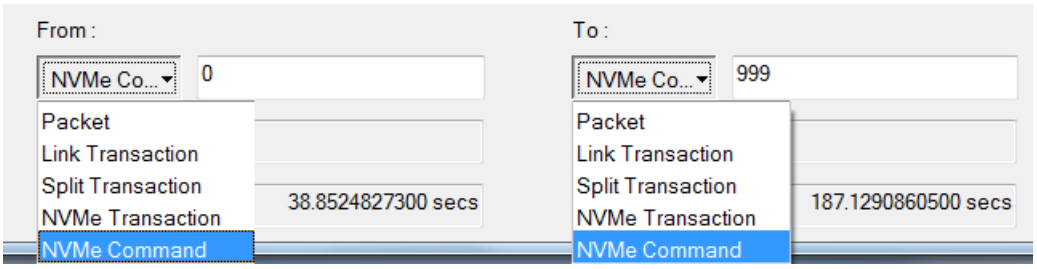


Figure 4.37: From and To Delimiters

The newer default format has the following characteristics:

- Removes spaces from time stamp format, i.e. "0002 . 742 651 908" -> 2.742651908
- Adds time delta value to the export
- Modifies 'Data' field to show '4 B' or 1 KB instead of '1 dword'
- QID / CID fields will be in decimal format rather than hexadecimal, i.e. 0x0007 -> 7

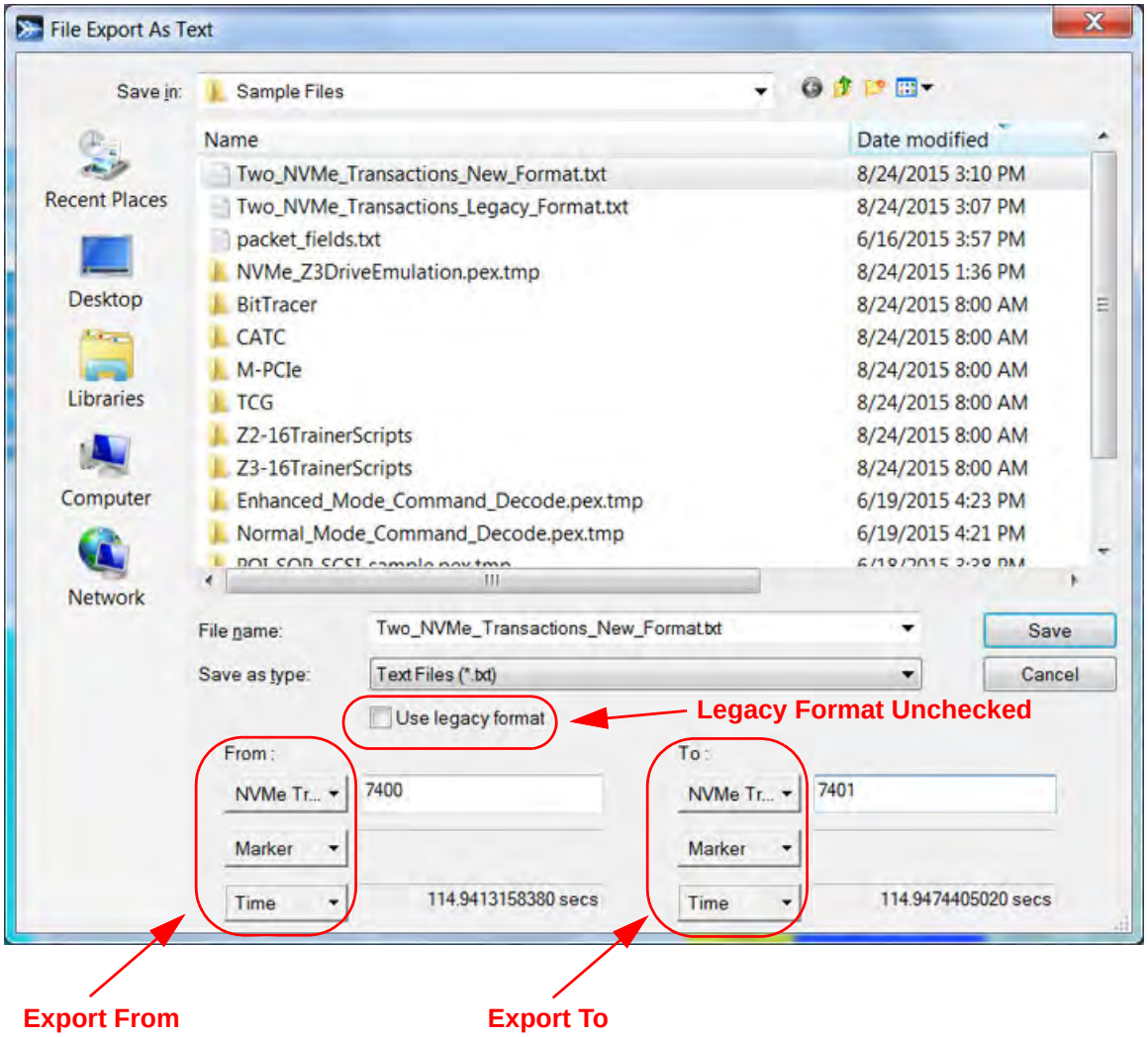


Figure 4.38: Export Two NVMe Transactions to Text File, New Format

You can see the differences in the two file formats below:

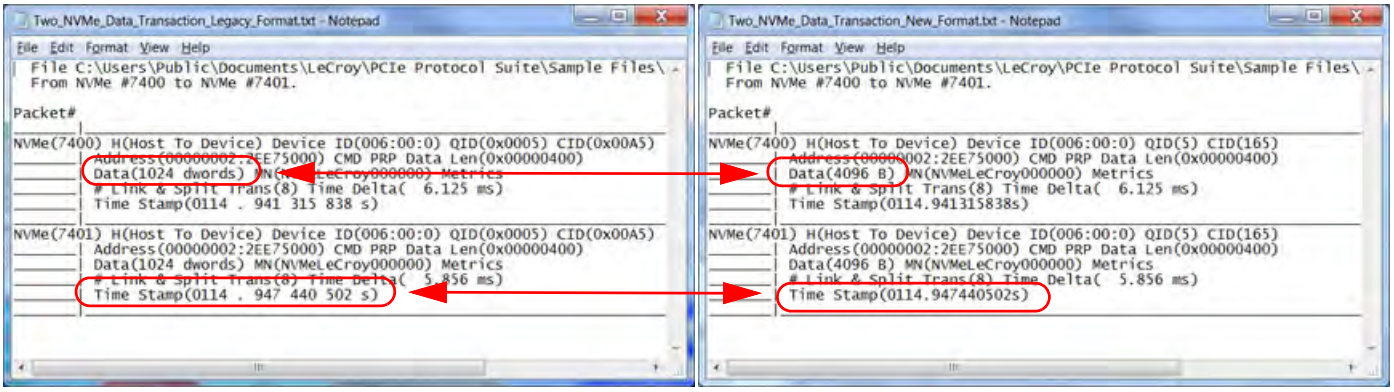


Figure 4.39: Export Trace Data to Text: Legacy vs New Format

4.13.2 Export: Packets to CSV Text

Now we'll Export Packets to CSV text using the legacy format, see Figure 4.40.

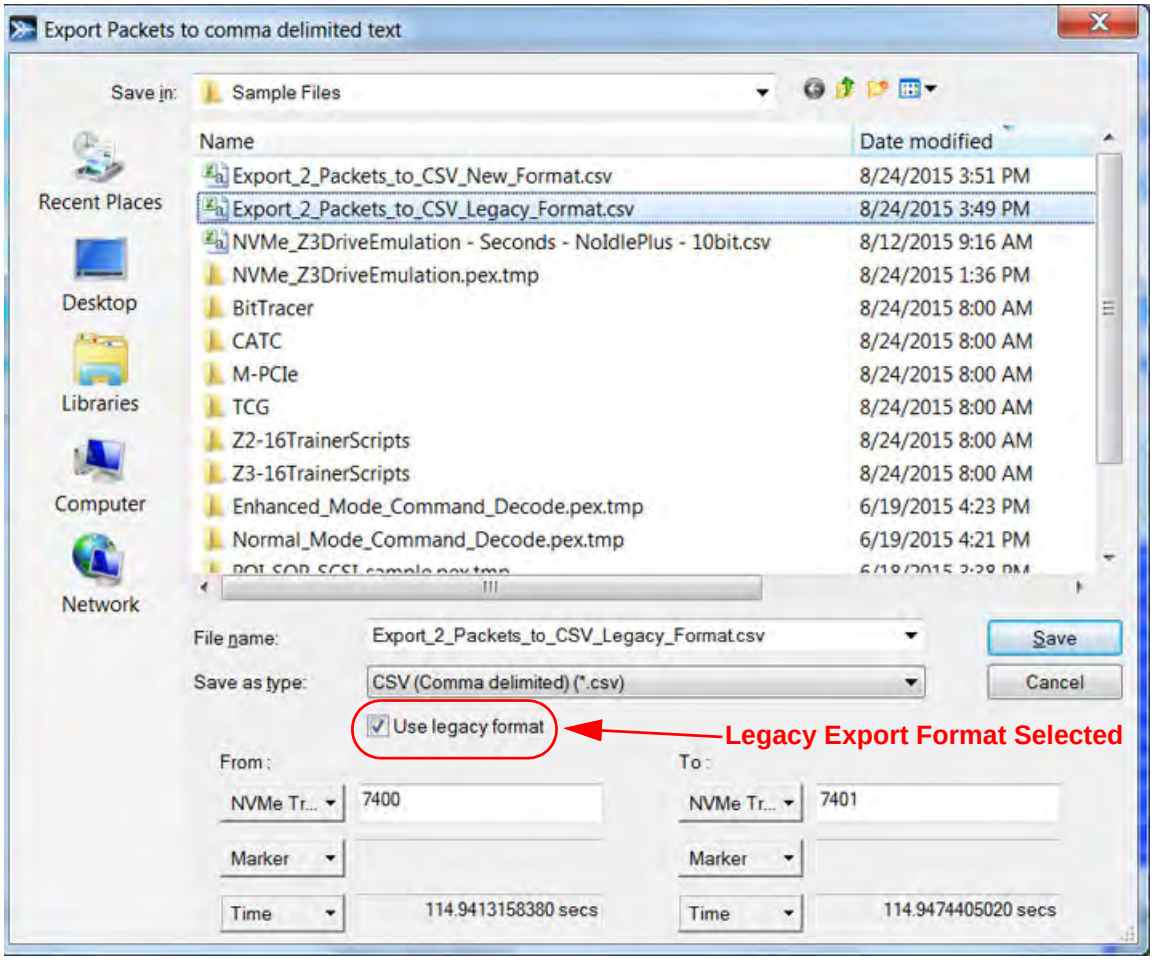


Figure 4.40: Export Packets to Comma Delimited Text: Legacy Format

Or we can export Packets to CSV text using the new format, see Figure 4.41.

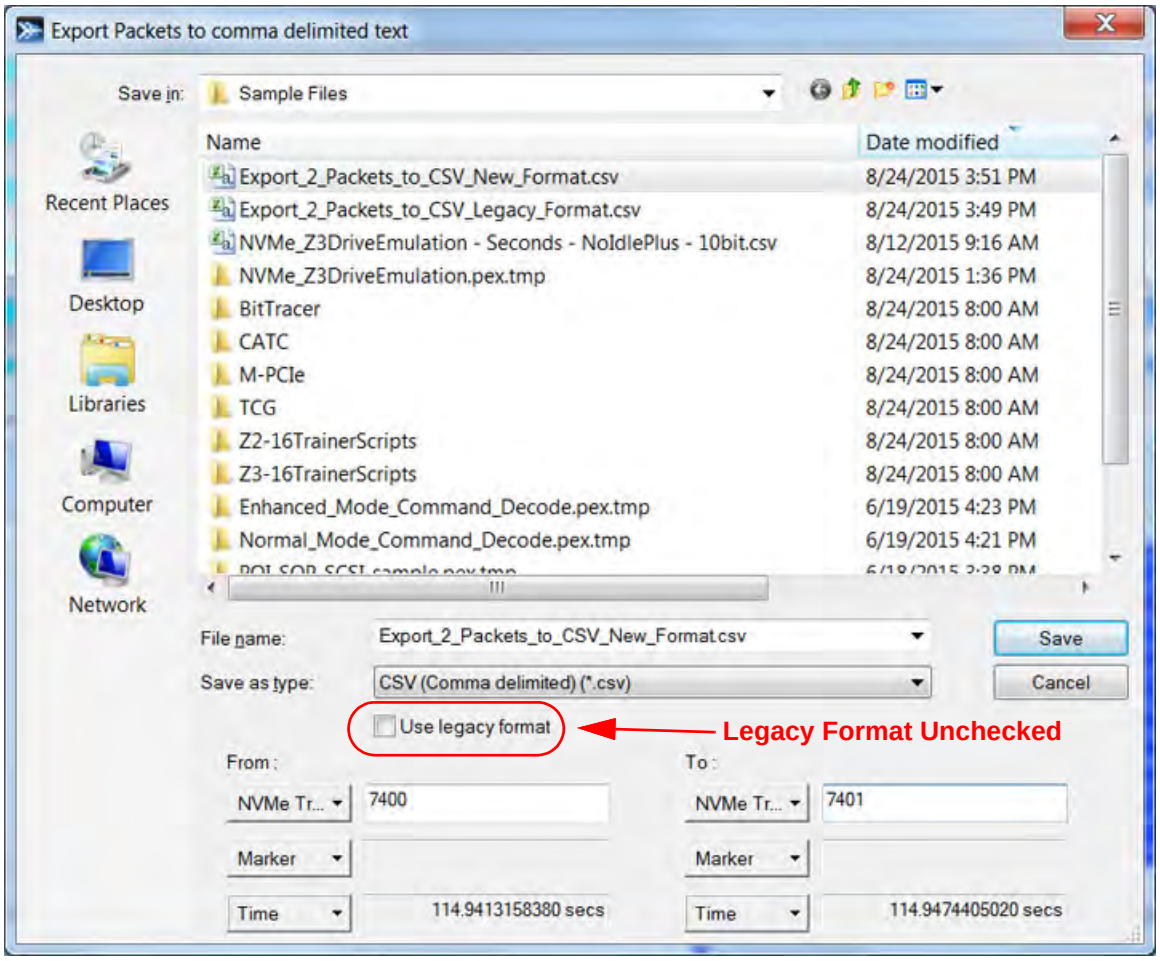


Figure 4.41: Export Packets to Comma Delimited Text: New Format

The differences in the two files can be seen in Figure 4.42.

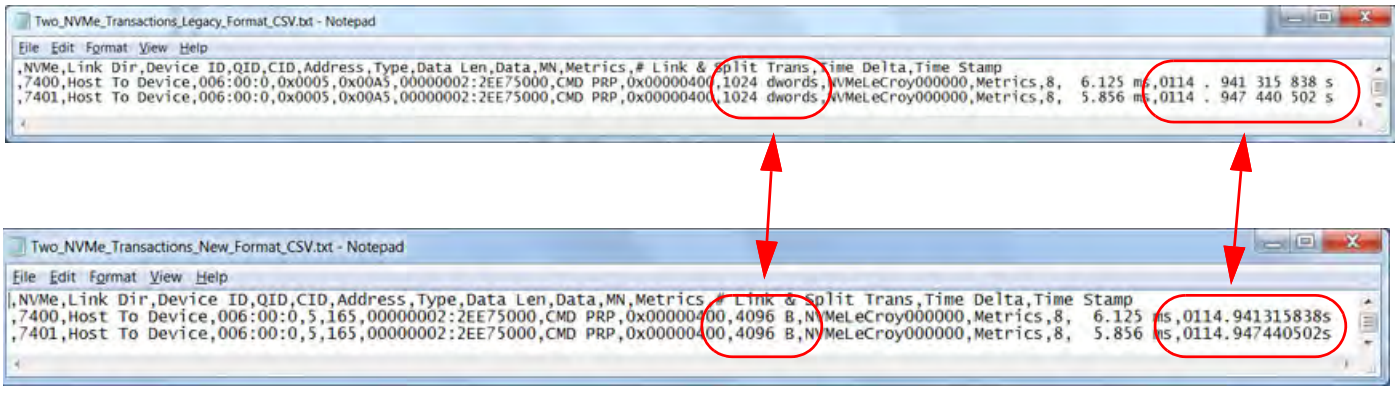


Figure 4.42: Export Packets to CSV Text: Legacy vs New Format

4.13.3 Export: To Generator File Format

To export a Trace File to Generator File format, choose that option. See Figure 4.43

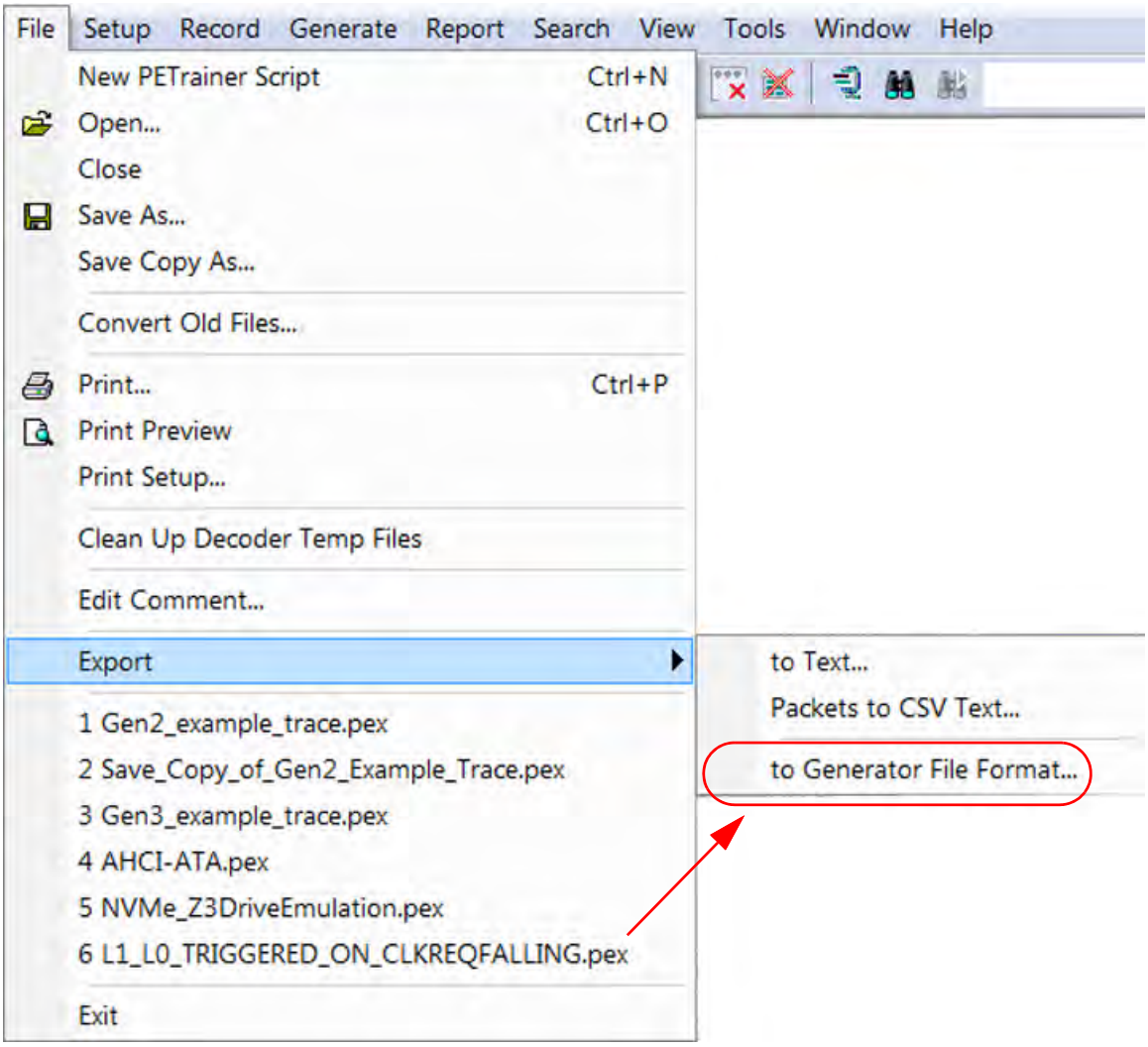


Figure 4.43: Export to Generator File Format

The purpose of Exporting a Trace file to Generator File Format is so that you can load that Generator file into a Teledyne LeCroy Exerciser (i.e. Z3-16 or Z416) to generate data traffic to test a device.

Exporting a CATC Trace to a Traffic Generation File

A simple way to create a script file is to open a CATC Trace and then to export the CATC Trace data to a generation file:

1. Open a CATC Trace file.
2. Select **File > Export > to Generator File Format**.
3. Select the desired options from the File Export dialog box as shown below. See Figure 4.44 on page 120.

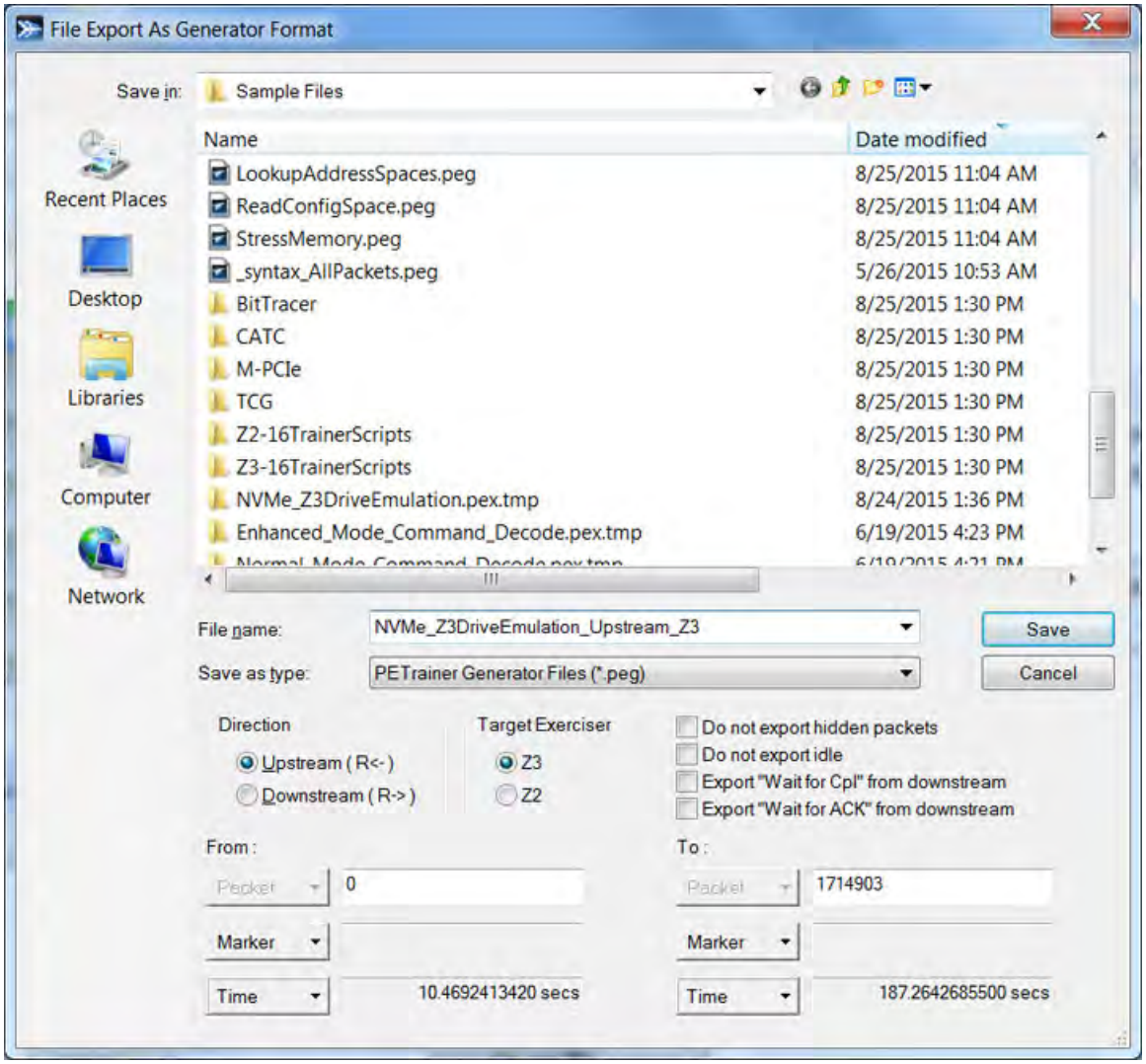


Figure 4.44: File Export As Generator Format Dialog.

Direction

Selects the direction of the traffic to be exported (Upstream or Downstream). In this case we chose Upstream. This will affect the Export “Wait for Cpl” and “Wait for ACK” options.

Target Exerciser

Select the type of Exerciser you plan to use (Z416, Z3-16 or Z2).

From and To

Selects a range for exporting. You can export all or part of the CATC Trace. You can select a range of Packets, Markers or Time.

Do not export hidden packets

Ignores any packets hidden through the various hide options.

Do not export Idle packets

Excludes Idles from the export.

Export “Wait for Cpl” from downstream

Exports all **Wait for Completions** from the opposite direction. **Wait = TLP** is a script command.

Export “Wait for ACK” from downstream

Exports all **Wait for ACK DLLPs** from the opposite direction.

4.13.4 Export From Data Flow View

You can also Export Trace Data from the Data Flow view (see Figure 4.45, Figure 4.46 on page 123 and Figure 4.47 on page 124) in either the Legacy or New data format.

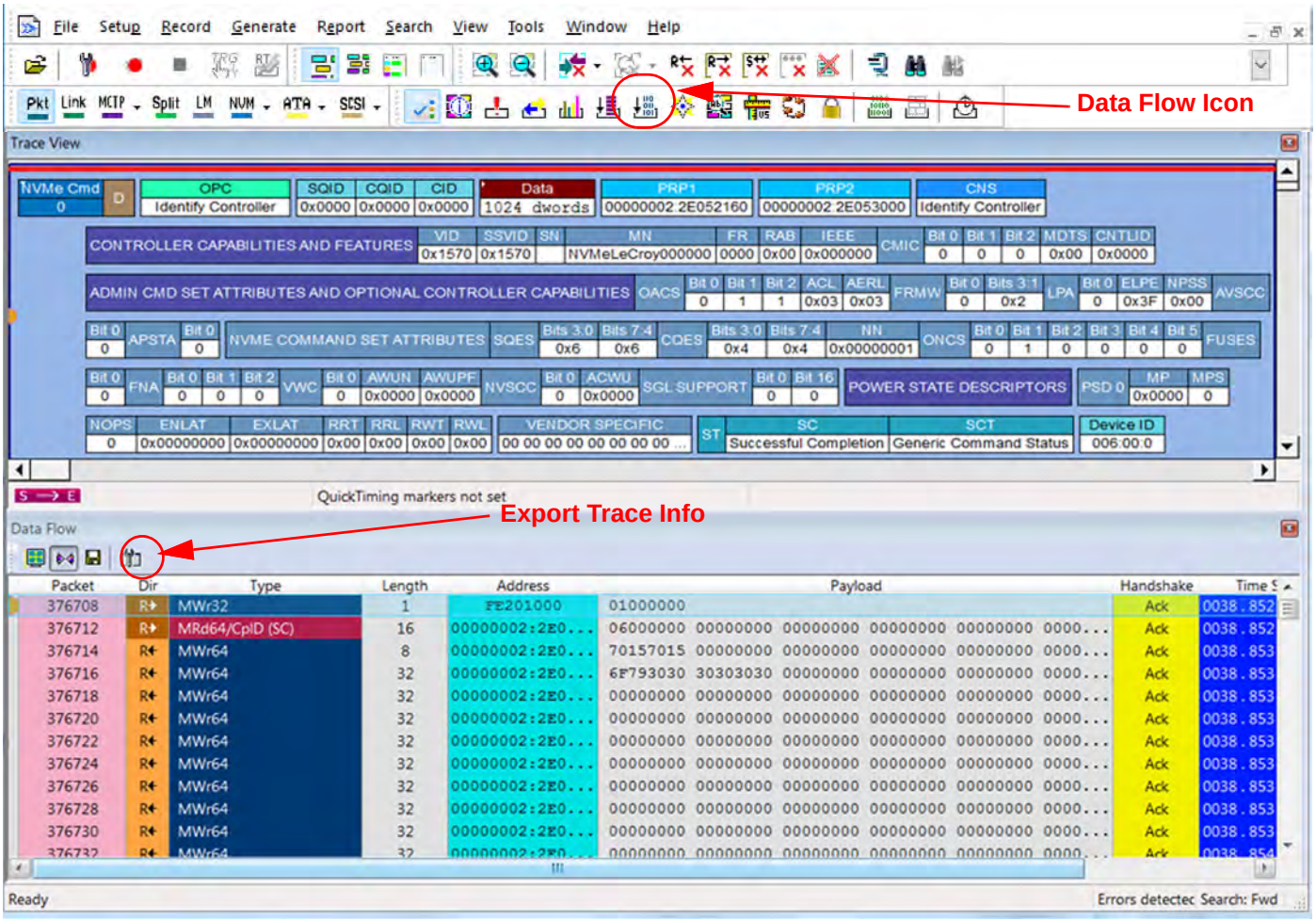


Figure 4.45: Data Flow View: Export by Selecting Save Icon

Export the Data Flow View information by selecting the Save icon. A new window will pop up where you can decide on the file name and path as well as whether the New data file format or the Legacy data file format is used. In this first example, we've chosen the Legacy format. See Figure 4.46.

Data Flow CSV File: Legacy Format

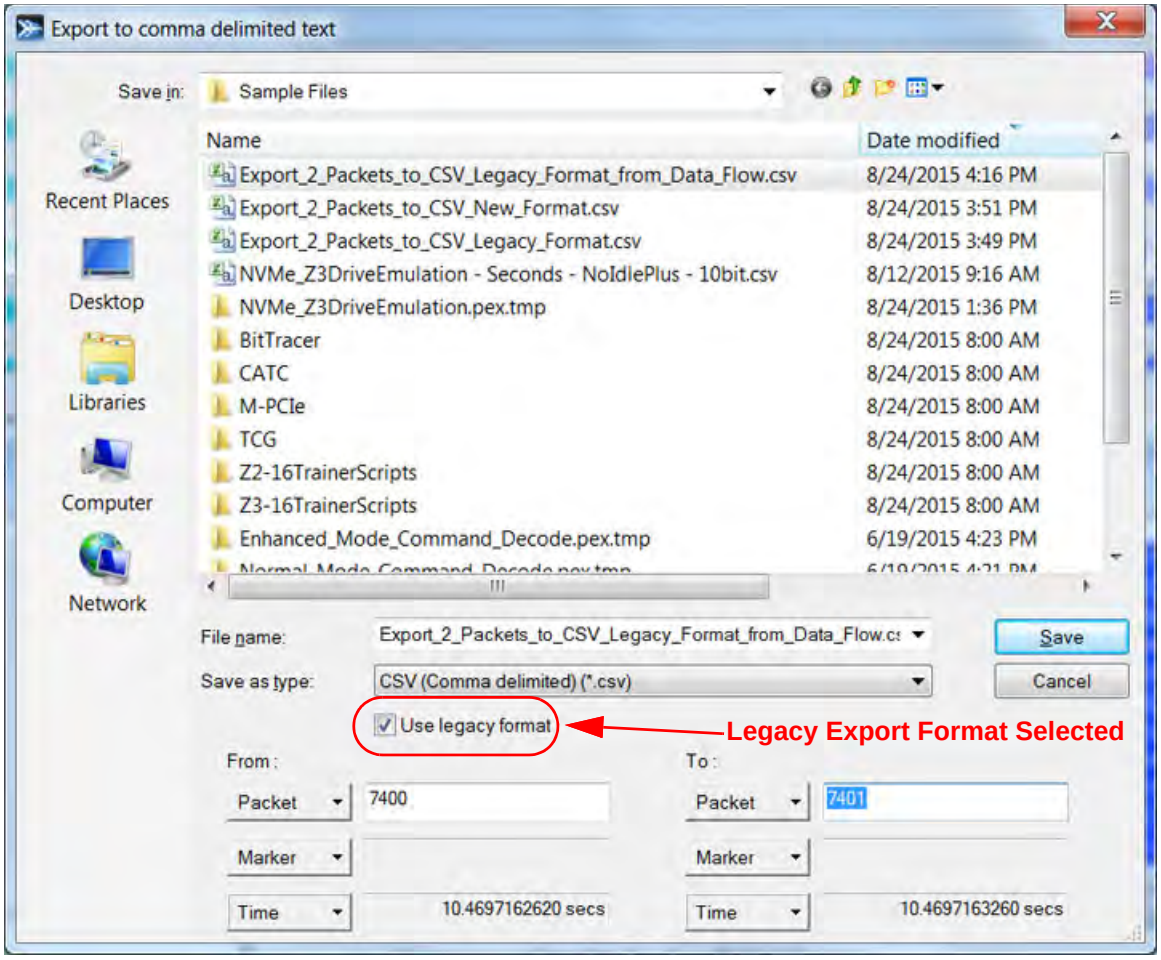


Figure 4.46: Data Flow View: Export Packets to Comma Delimited Text: Legacy Format

Data Flow CSV File: New Format

Next we'll chose the New Data format for the CSV file. See Figure 4.47.

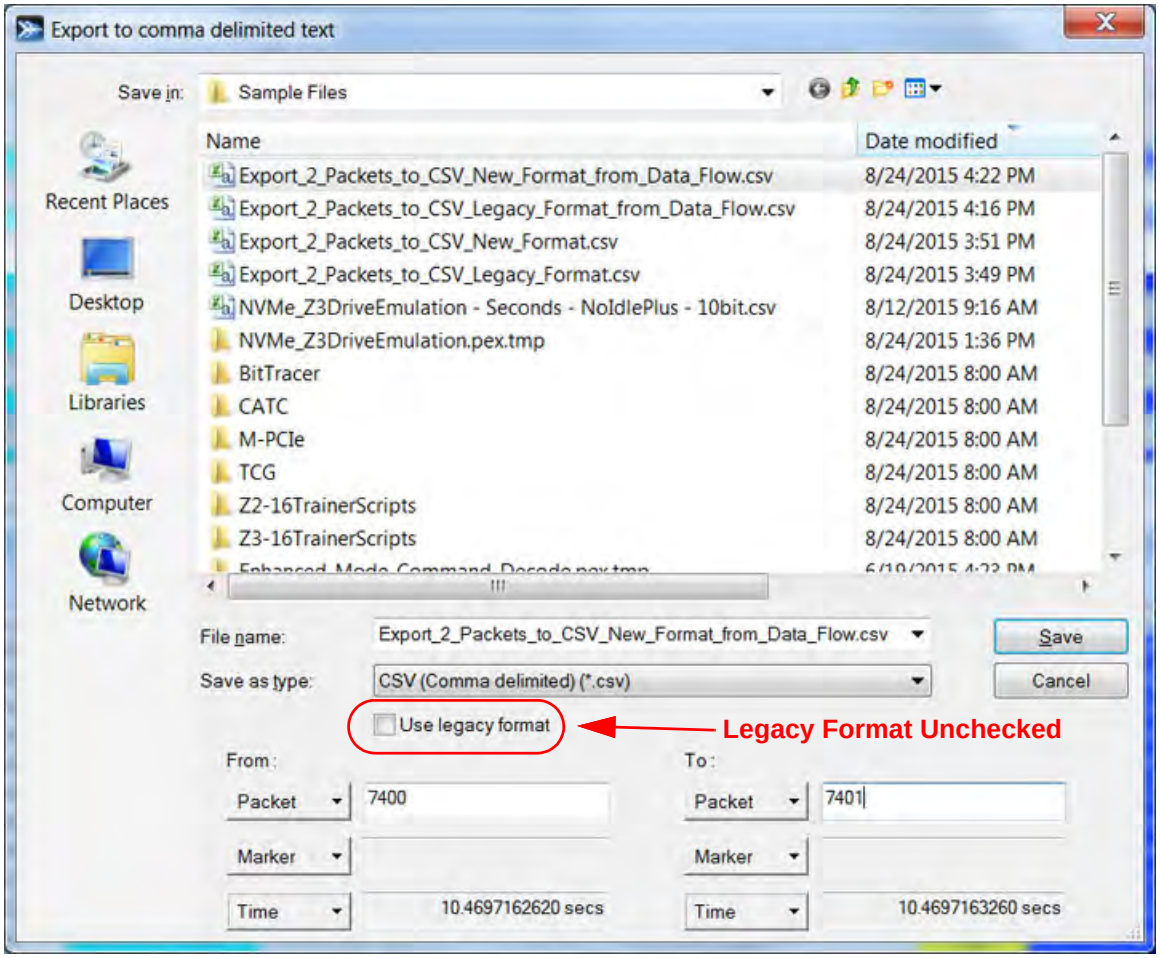


Figure 4.47: Data Flow View: Export Packets to Comma Delimited Text: New Format

4.14 Printing Data Files

To print all or part of the open CATC Trace:

1. Select **File > Print** from the menu or

   click the **Printer**  button on the toolbar.
   The Print Packets dialog displays (see Figure 4.48 on page 125).

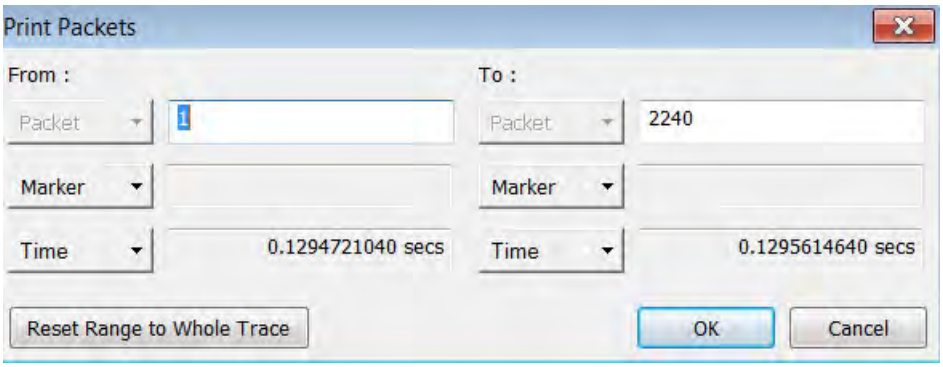


Figure 4.48: Print Packets Dialog

2. To select a range of packets, enter values in the **From packet #** and **To packet #** fields and click **Print**.
3. To print an entire file, leave the From and To fields empty and click **Print**.

The specified traffic information is printed as currently displayed, in color or gray scale as supported by your printer. Any CATC Trace File comments you entered are printed following the current document name at the top of each page.

Note: CATC Trace File comments can be created by using **Edit Comment** on the File menu.

4.15 Analyzer Chat Window

PCIe Protocol Analysis has a Chat window that allows you to communicate with users on remote host machines. For Chat to work, two conditions must be met:

- The host machines must have PCIe Protocol Analysis installed and running.
- The host machines must be listed in each other's All Connected Devices list. This means that your host machine must have the remote host machine listed in its Analyzer Devices window and the remote host machine must have your host machine listed in its Network Browse window. See Figure 4.49 on page 126.

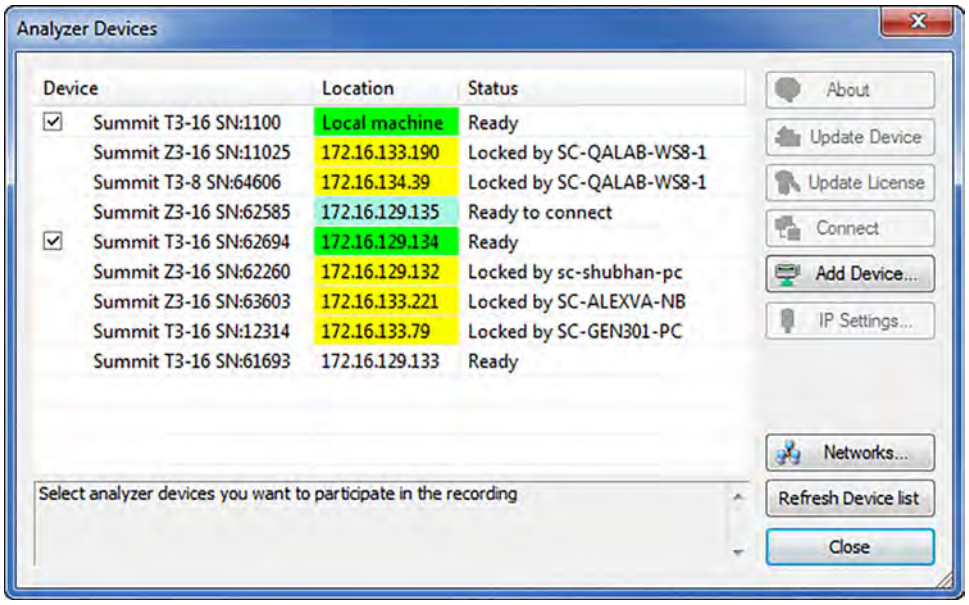


Figure 4.49: Analyzer Network Dialog

If the above conditions are met, a Chat session is initiated by running the command: **View > Analyzer Network Chat Bar**. The following dialog box opens.

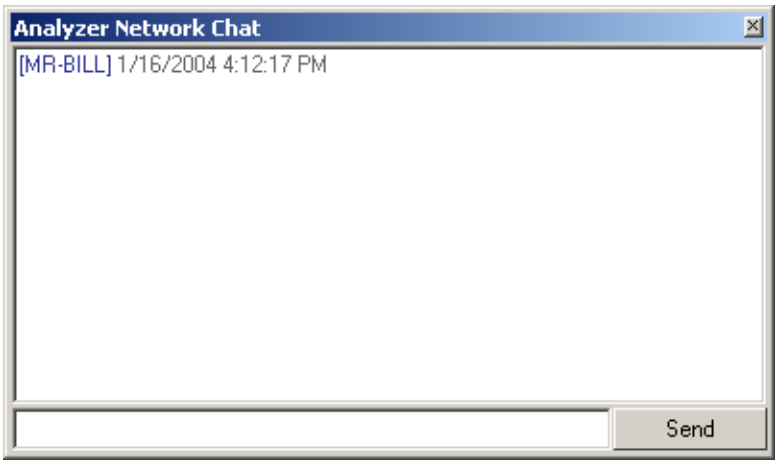


Figure 4.50: Analyzer Network Chat Dialog

Enter some text, then press **Send**. The message is then broadcast to all host machines listed in your network browse window. If a target host machine also lists your host machine in its Network Browse window, then it can receive your message. When the message arrives, the Chat window automatically opens.

4.15.1 CrossSync™ Control Panel

The CrossSync™ Control Panel allows you to select analyzers for synchronization and manage the recording process. It supports a wide combination of Teledyne LeCroy's flagship analyzers including PCI Express, USB, DDR, Serial ATA (SATA), Serial Attached SCSI (SAS), Fibre Channel (FC) and Ethernet.

CrossSync™ is Teledyne LeCroy's analyzer synchronization solution that enables time-aligned display of protocol traffic from multiple daisy-chained analyzers showing packet traffic from multiple high-speed serial busses. A lightweight software control panel allows users to select analyzers for synchronization and manage the recording process. Captured traffic is displayed using the latest analyzer software (in separate windows) with all the protocol specific search and reporting features.

Captured packets are displayed in separate windows that share a common time scale. Navigating the traffic in either direction will scroll to the same timestamp in a synchronized window. When using the CrossSync™ option, users can access the full complement of analysis capabilities available within the individual Teledyne LeCroy software. Search, reporting, and decoding all operate normally.

This feature is available with the Teledyne LeCroy PCIe Protocol Analysis application.

Launching the CrossSync™ Control Panel

To launch CrossSync™ from the PCIe Protocol Analysis application, select the '**Launch CrossSync™ Control Panel**' entry in the 'Setup' menu (see the screen below). Or, you can launch CrossSync™ from the '**Start**' menu.

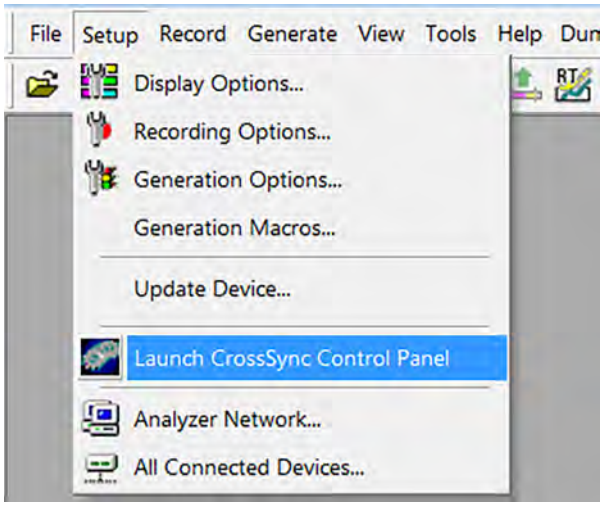


Figure 4.51: Launching CrossSync™ from the PCIe Protocol Analysis Application

Please refer to the *CrossSync™ Control Panel User Manual* for more information.

Chapter 5

Recording Options: AJ Mode

5.1 Recording Overview

After installing the software, recording options should be set prior to recording. The recording options define the behavior of the Summit M5x Analyzer/Jammer (AJ) during recording. The Recording Options dialog displays options that affect all recordings. You can create, save and load previously saved recordings. This section explains how to define recording options on the Summit M5x (AJ).

5.1.1 Analyzer/Jammer (AJ)

The Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior. The Summit M5x also provides NVMe and NVMe-MI protocol jamming as well. The analyzer and jammer combination features on the Summit M5x make this a powerful testing tool for PCIe validation and development labs. This Jammer and Scripting capability is built into the PCIe Protocol Analysis software.

5.2 Recording Option Dialog

The Recording Options dialog is used to configure a recording.

To open the Recording Options window, from the main screen click  or select **Setup → Recording Options**.

Note: There are separate sets of Recording Options for each Analyzer type. To set the Analyzer type, select the appropriate platform from the Target Analyzer menu in the General tab of the Recording Options.

5.3 Recording Type: Select Analyzer

The Recording Type options available on each analyzer are different. As shown in Figure 5.2 on page 134 the Summit M5x Analyzer is detected and the recording options available for it are displayed (See Figure 5.2 on page 134: 2) or see the more detailed drop down menu below in Figure 5.1.

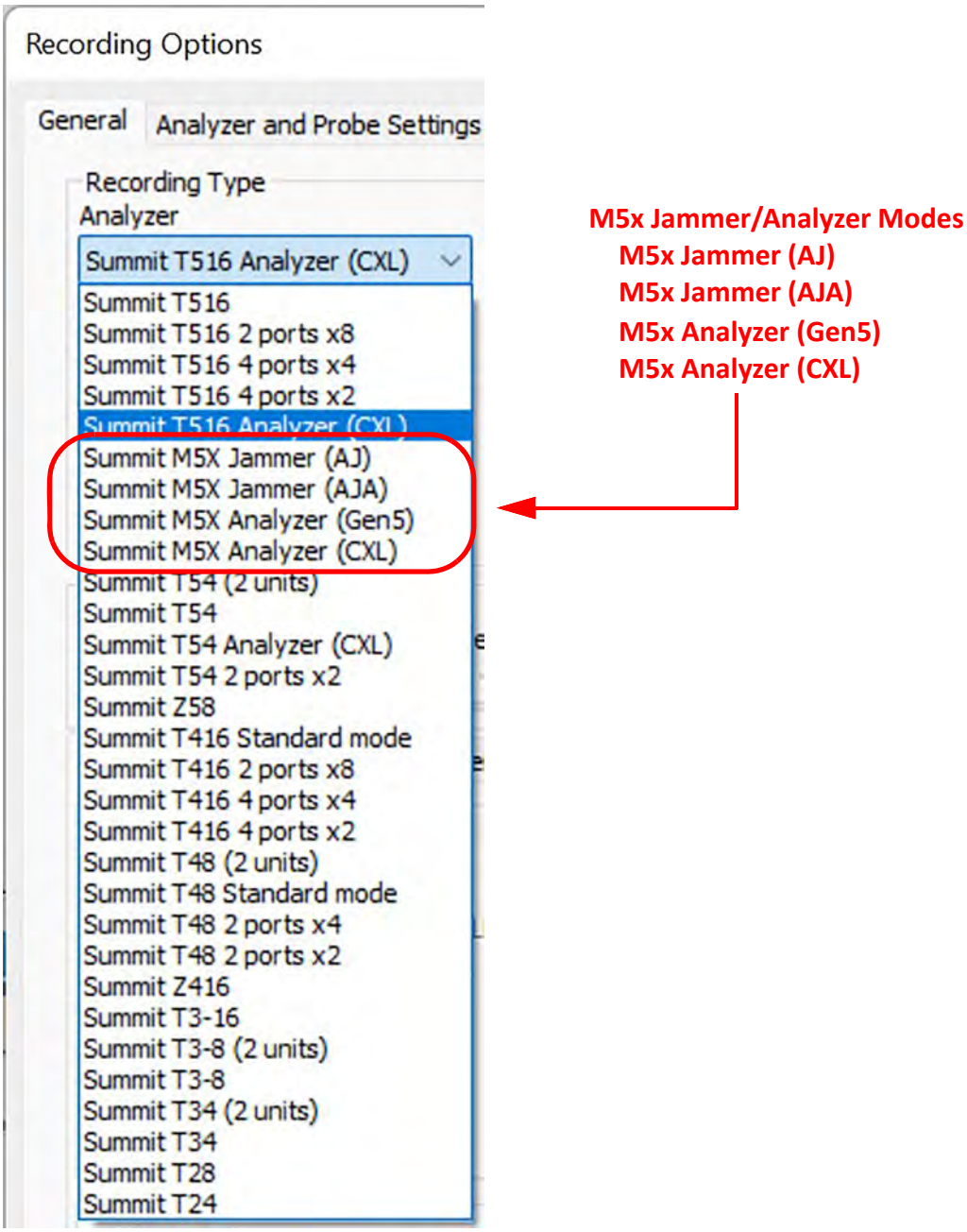


Figure 5.1: Analyzer Types

When the analyzer is not yet detected, choose the analyzer from the Analyzer drop-down menu in the Recording Type zone. The choices are:

- **Summit M5x Analyzer/Jammer/Analyzer (AJA):** Displays the options for the Summit M5x Analyzer/Jammer/Analyzer.
- **Summit M5x Jammer (AJ):** Displays the options for the Summit M5x Analyzer/Jammer.
- **Summit M5x Analyzer (Gen5):** Displays the options for the Summit M5x Gen5 Analyzer. (See Chapter 7, “Recording Options: Analyzer Only Mode,” on page 335).

- **Summit M5x Analyzer (CXL):** Displays the options for the Summit M5x Analyzer in CXL mode. See “Recording Options for Compute Express Link (CXL) Mode” on page 248).
- **Summit T54 (2 Units):** Displays the same options as Summit T54 but lists Unit 1 and Unit 2 in the Link Section on the right. In a two-unit setup, Unit 1 and Unit 2 are two separate Analyzers linked together with a combined link width of x8.
- **Summit T54:** Displays the options for the Summit T54 Analyzer.
- **Summit T54 Analyzer (CXL):** Displays the options for the Summit T54 Analyzer with CXL recording options.
- **Summit T54 2 ports x2:** Displays the options for the Summit T54 Analyzer used in Multiport mode.
- **Summit T416 Standard:** Displays the options for the Summit T416 Analyzer.
- **Summit T416 4 Ports:** Displays the options for the Summit T416 Analyzer used in Multiport mode.
- **Summit T416 2 Ports:** Displays the options for the Summit T416 Analyzer used in Multiport mode.
- **Summit T48 Standard:** Displays the options for the Summit T48 Analyzer.
- **Summit T48 2 Ports:** Displays the options for the Summit T48 Analyzer used in Multiport mode.
- **Summit T48 (2 Units):** Displays the same options as Summit T3-8 but lists Unit 1 and Unit 2 in the Link Section on the right. In a two-unit setup, Unit 1 and Unit 2 are two separate Analyzers linked together.
- **Summit T3-16:** Displays the options for the Summit T3-16 Analyzer.
- Summit T3-8 (2 Units): Displays the same options as Summit T3-8 but lists Unit 1 and Unit 2 in the Link Section on the right. In a two-unit setup, Unit 1 and Unit 2 are two separate Analyzers linked together.
- **Summit T3-8:** Displays the options for the Summit T3-8 Analyzer.
- Summit T34 (2 Units): Displays the same options as Summit T34 but lists Unit 1 and Unit 2 in the Link Section on the right. In a two-unit setup, Unit 1 and Unit 2 are two separate Analyzers linked together.
- **Summit T34:** Displays the options for the Summit T34 Analyzer.
- **Summit Z416:** Displays the options for the analyzer portion of the Z416.
- **Summit T28:** Displays the options for the Summit T28 Analyzer.
- **Summit T24:** Displays the options for the Summit T24 Analyzer.

5.4 Recording Type: Summit M5x Jammer (AJ) Analyzer

This section describes the recording options when selecting the Summit M5x (AJ) analyzer.

5.4.1 Recording Options: Simple Mode Summit M5x Jammer (AJ)

The Simple Mode recording options are shown in Figure 5.2 on page 134.

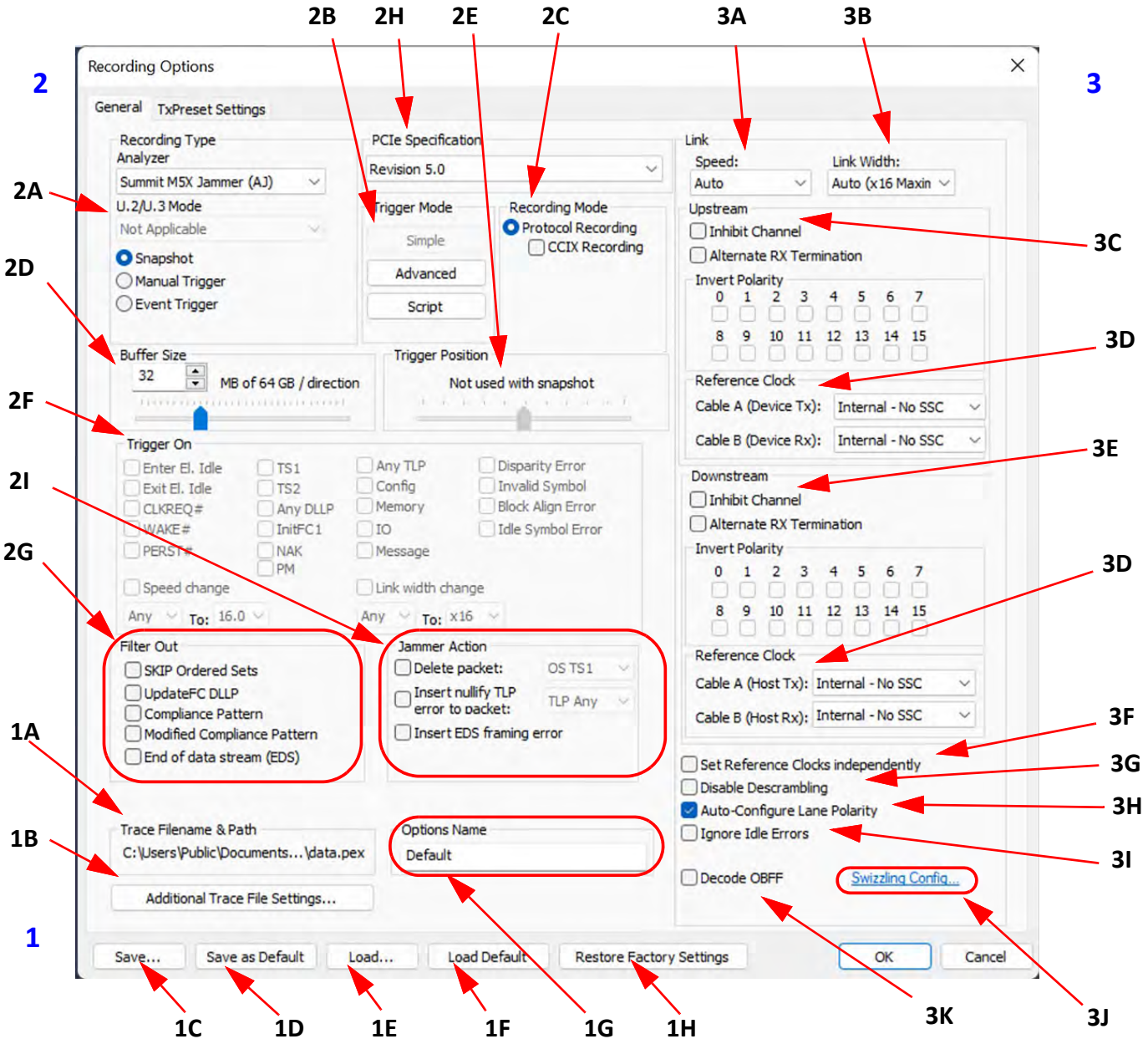


Figure 5.2: Summit M5x Jammer (AJ) in Simple Recording Options

Note:
- Please refer to the figure callout numbers in each of the sections below to correlate to Figure 5.1 shown above. For instance, for Simple and Advanced Mode, see Figure 5.1: 2B.
- For the Summit M5x Recording Options refer to Figure 5.3. In the following section with detailed explanations always refer to Figure 5.3 for the Summit M5x.

5.4.2 Recording Options: Advanced Mode Summit M5x Jammer (AJ)

The advanced Trigger Mode options are shown in Figure 5.3.

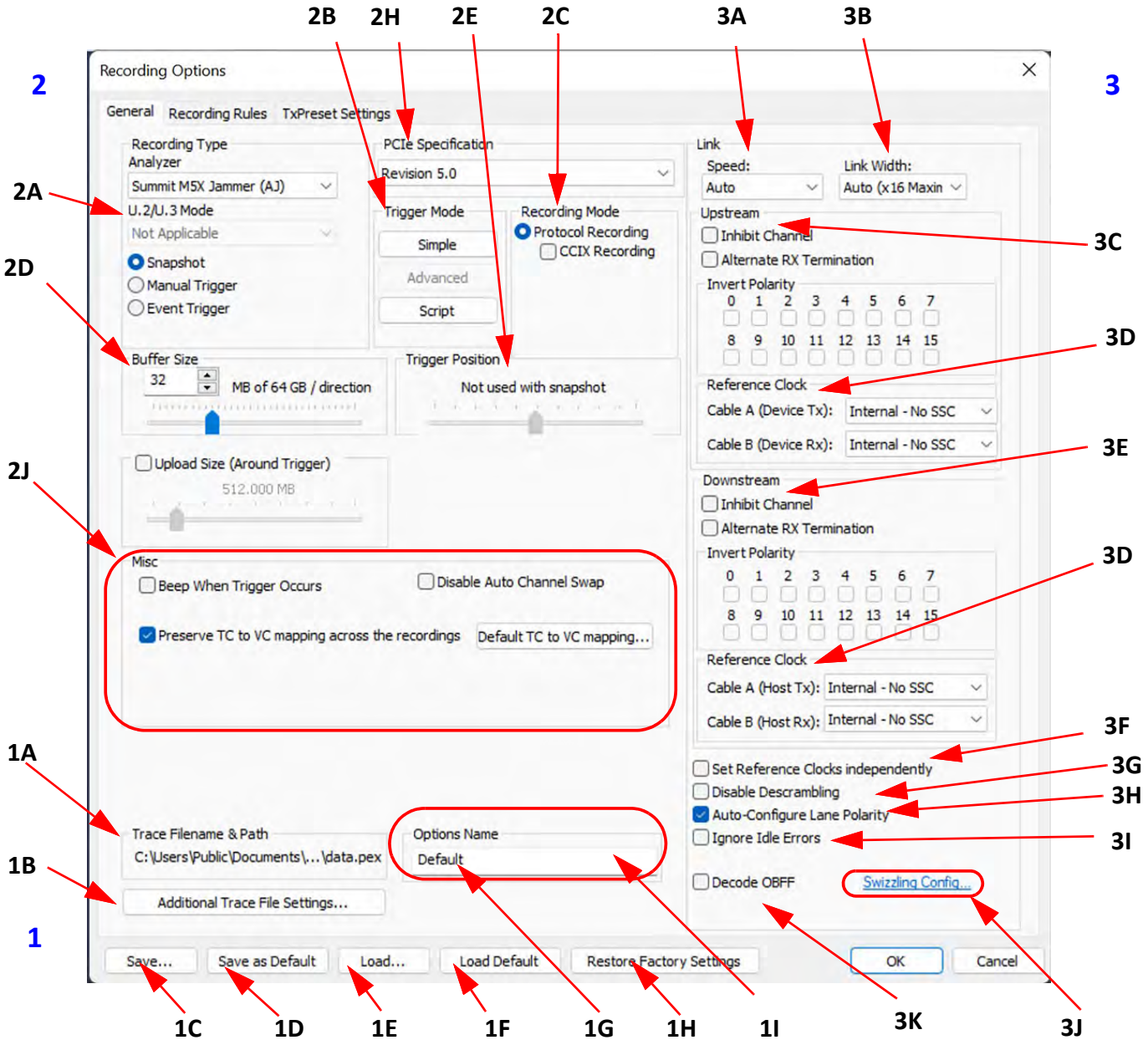


Figure 5.3: Recording Options: Summit M5x Jammer (AJ) → Advanced Mode (Snapshot)

5.4.2.1 Options in Advanced Mode: Disable Auto Channel Swap

One Recording Option that becomes available in Advanced Mode is Disable Auto Channel Swap. See Figure 5.6.

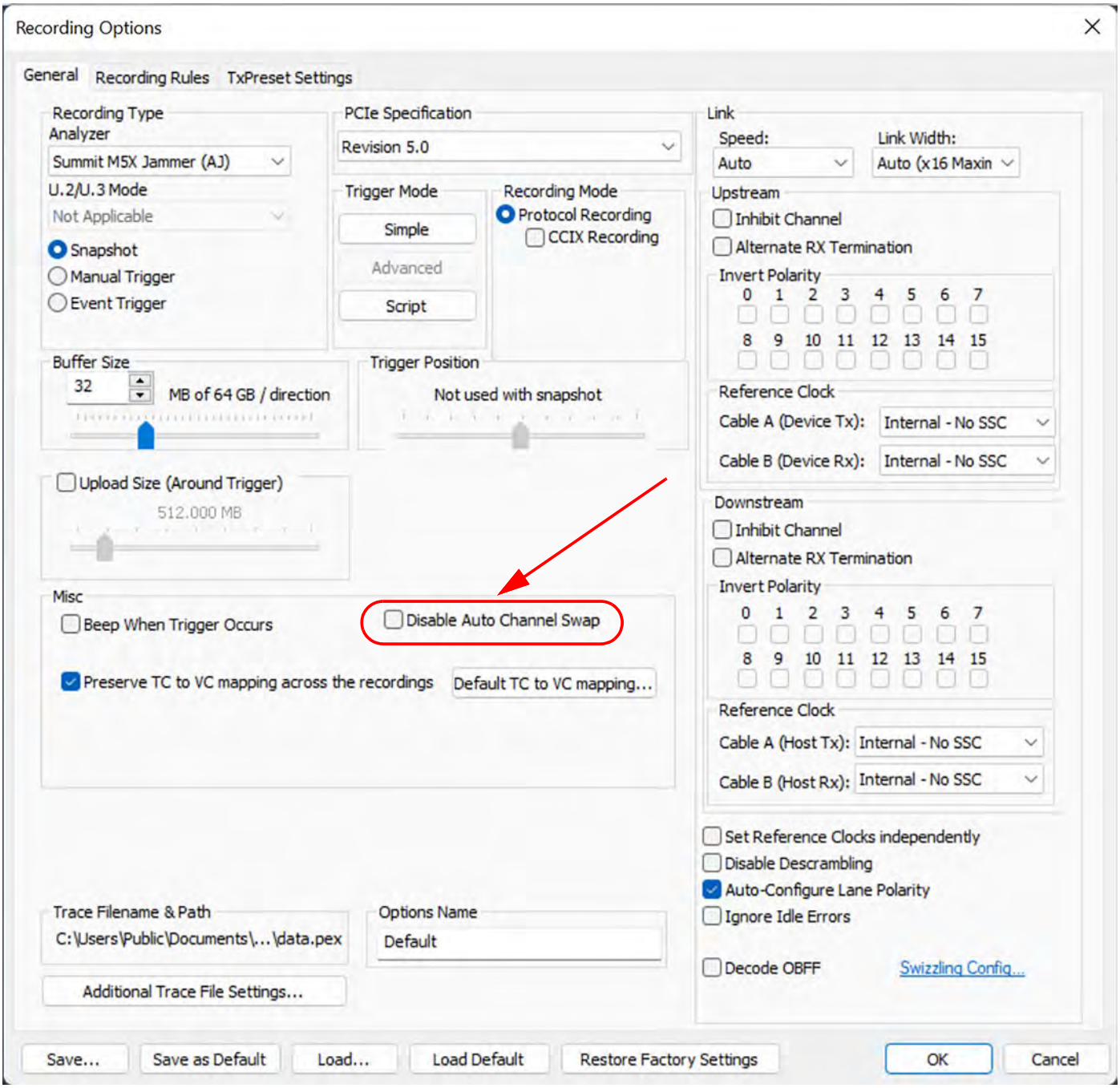


Figure 5.4: Recording Options: Advance → Disable Auto Channel Swap

If Disable Auto Channel Swap **is not selected** the PCIe Analysis software will swap the direction of the traffic data based on it's internal analysis of the traffic on the bus (channel direction swapping is enabled).

If Disable Auto Channel Swap **is selected** the PCIe Analysis software will record the traffic data as the Summit analyzer sees it and this depends on the way the connections were made to probe the bus (channel direction swapping is disabled).

5.4.2.2 Options in Advanced Mode: TC to VC mapping

One Recording Option that becomes available in Advanced Mode is TC to VC mapping. See Figure 5.10.

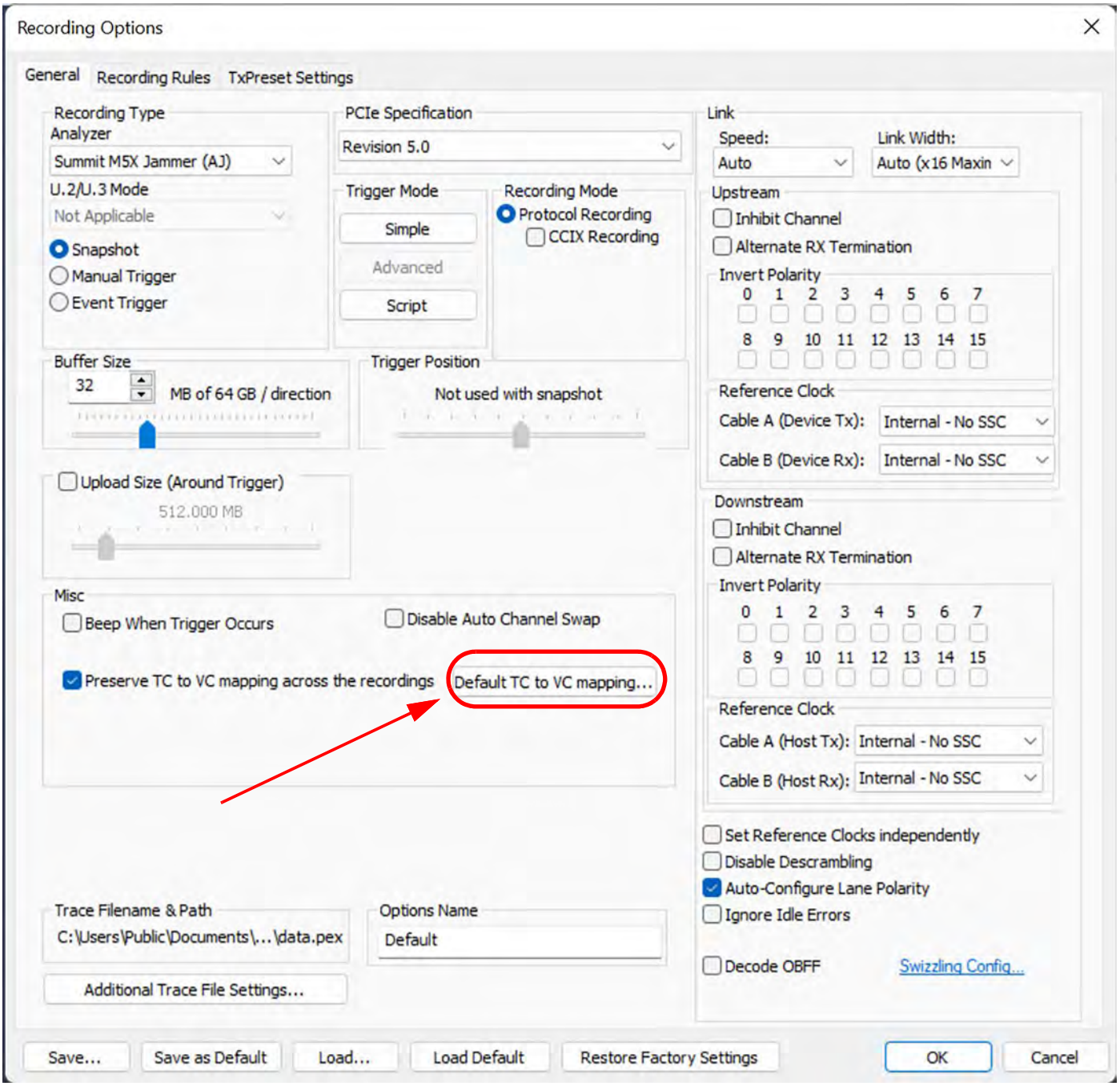


Figure 5.5: M5x Advanced Recording Mode: Default TC to VC mapping

If you select Default TC to VC mapping, the following dialog box pops up and you can manipulate the TC to VC mapping. See Figure 5.11 on page 143.

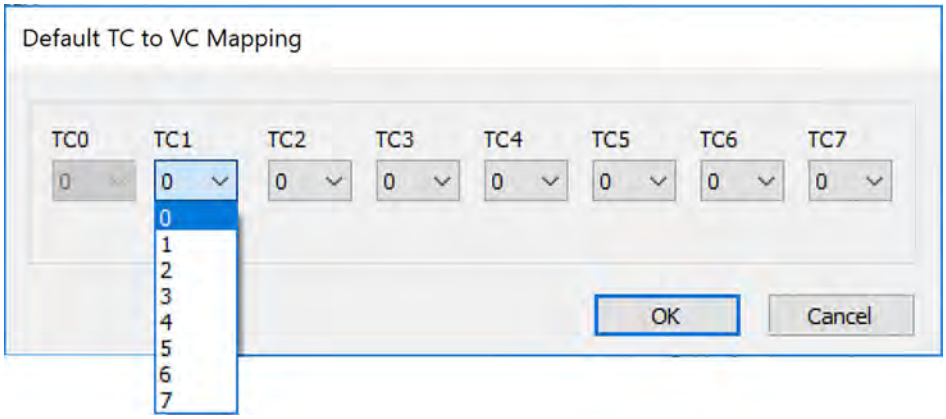


Figure 5.6: TC to VC Mapping

5.5 Recording Type: Triggering Options

See Figure 5.2 on page 134: 2A.

5.5.1 Snapshot

Snapshot is a recording of a pre-determined length. You set the recording length in the Buffer Size box. Recording begins when you click the **Rec** button on the toolbar and ends when the selected buffer size is filled or when you press the **Stop** button.

5.5.2 Manual Trigger

Recording begins when you select **Start** in the application. Pressing the **Trigger** button allows the Analyzer to finish recording by switching between the pre-trigger buffer and the post-trigger buffer. Recording continues until the post-trigger buffer has been filled. You can also end the recording immediately by pressing the **Stop** button in the application.

Note: Consider that when filtering is enabled, pressing the Trigger button will not necessarily cause the post-trigger buffer to fill automatically, due to packets being filtered and not stored. In this case you will have to use the Stop button to immediately end the recording.

5.5.3 Event Trigger

A recording that switches between the pre-trigger buffer and the post-trigger buffer when it is triggered by an event in the CATC Trace. An Event Trigger begins when you select **Start** in the application and ends when the specified triggering event occurs in the CATC Trace or you press **Stop**. If an event triggers the end of the recording, the Analyzer records a predefined amount of post-trigger data (specified by Trigger Position and Buffer Size.)

You can also terminate an Event Trigger recording by pressing the Manual Trigger button on the front of the Analyzer. When the Manual Trigger button is pressed, the Analyzer continues to record until the specified post-trigger buffer has been filled. See Figure 5.7 on page 139.

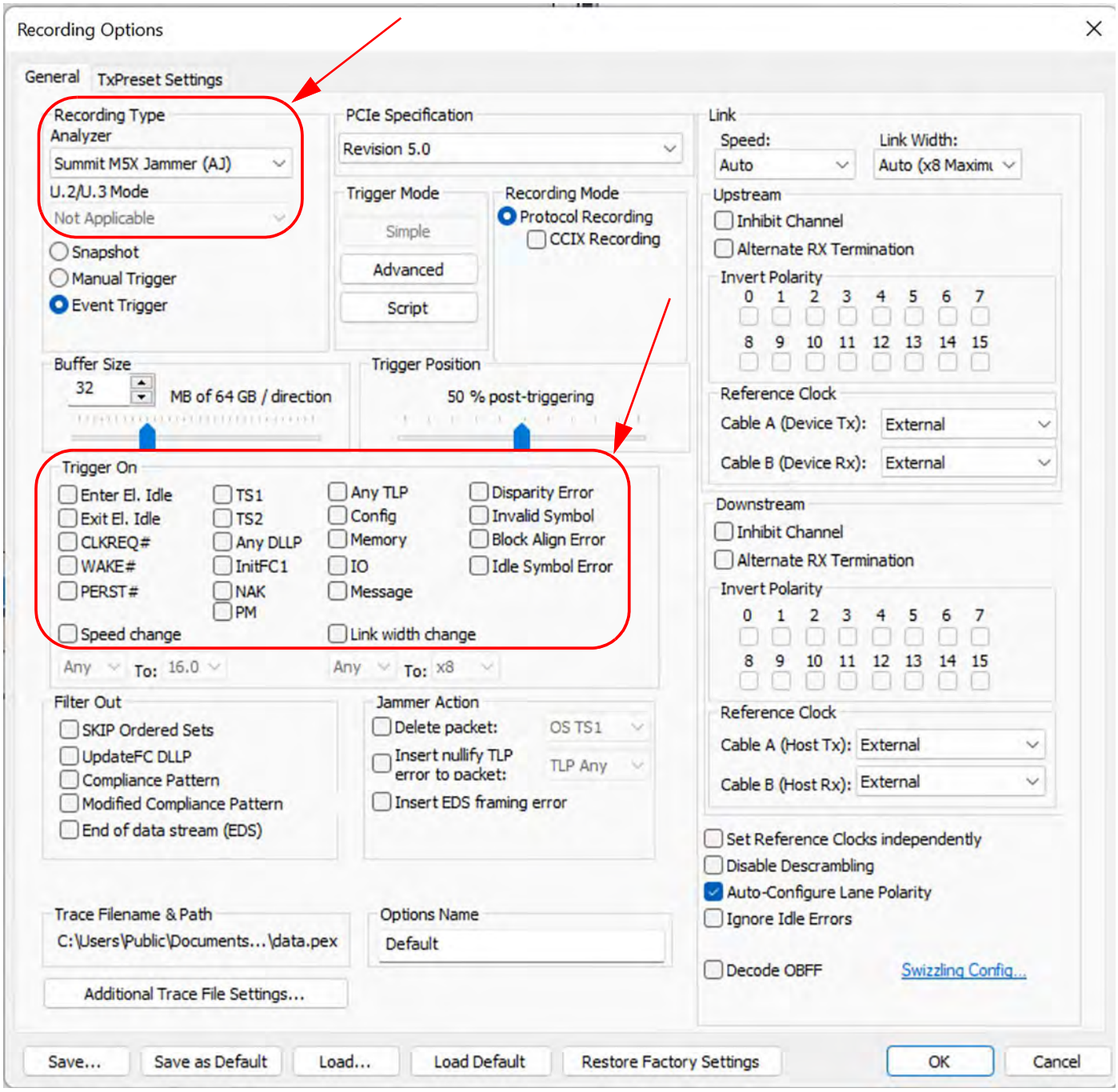


Figure 5.7: Simple Recording Options: Triggered Events

5.5.3.1 Events: Triggering On (Simple Mode)

You can check any of the boxes shown in Table 5.2 for Trigger On in Simple Mode (see Figure 5.7 on page 139 or Figure 5.2 on page 134: 2F).

TABLE 5.2: Simple Mode Trigger on Events (Upstream or Downstream)

Enter Elec Idle	Any TLP
Exit Elec Idle	Config
CLKREQ#	Memory

TABLE 5.2: Simple Mode Trigger on Events (Upstream or Downstream)

WAKE#	IO
PERST#	Message
TS1	RD Error
TS2	Invalid Symbol
Any DLLP	Block Align Error
InitFC1	Idle Symbol Error
NAK	
PM	
Speed Change: Any, 2.5, 5.0. 8.0, 16.0 To: Any, 2.5, 5.0, 8.0, 16.0	Link Width Change: Any, x1, x2, x4, x8 or x16 To: Any, x1, x2, x4, x8 or x16

Note:
- Trigger Position slider becomes enabled only when Recording Type is set to Manual Trigger or Event Trigger.
- If you check 2 or more boxes the triggering will occur based on an OR condition, not AND condition.
- External Input Trigger is not configurable, it will always cause the analyzer to trigger on a toggle when using manual trigger or triggering on any event.

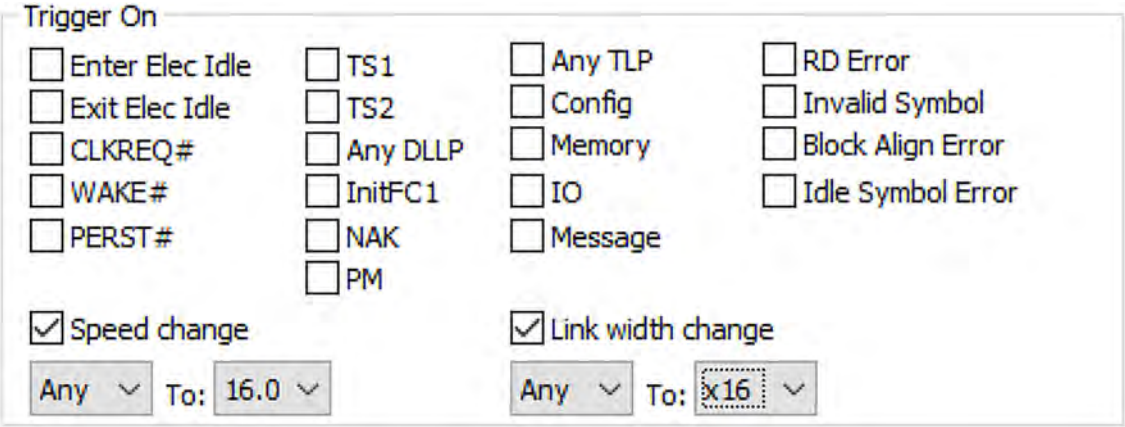


Figure 5.8: Simple Mode Triggering Options

5.6 Trigger Mode

The recording options are: Simple, Advanced or Script modes. The Simple Recording and Advanced Recording options are the same in functionality, only the interface displayed is different. The Simple Mode allows quick access to commonly used options. The recording options are the same in both modes (See Figure 5.2 on page 134: 2B).

In Advanced Mode, you can set complex recording rules.

In Script Mode, you can see the script converted from the complex recording rules you set in the Advanced Mode GUI. See Figure 5.9.

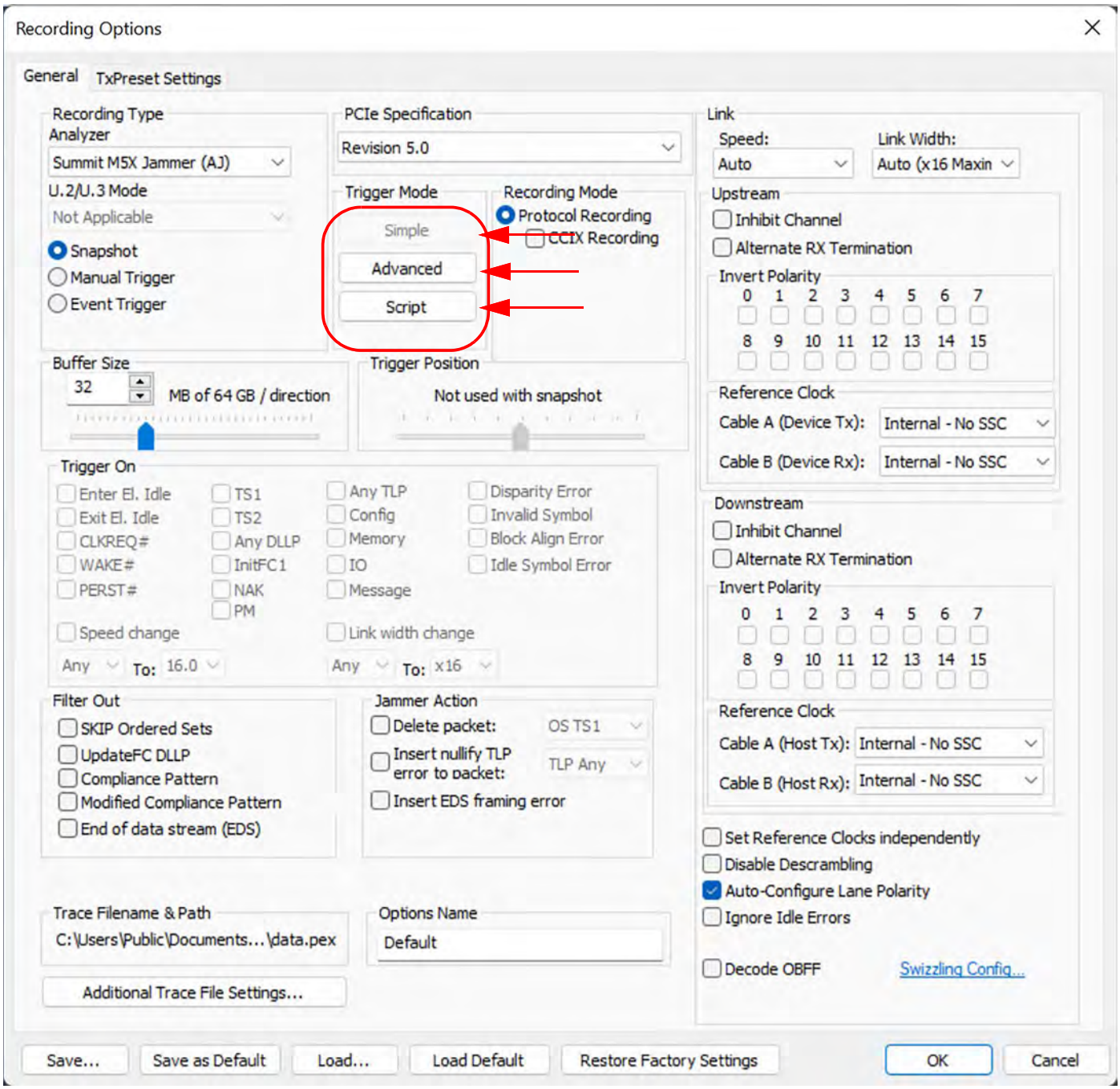


Figure 5.9: Switch to Simple, Advanced or Script Mode Buttons Summit M5x

One option that becomes available in Advanced Mode is CCIX. See Figure 5.10.

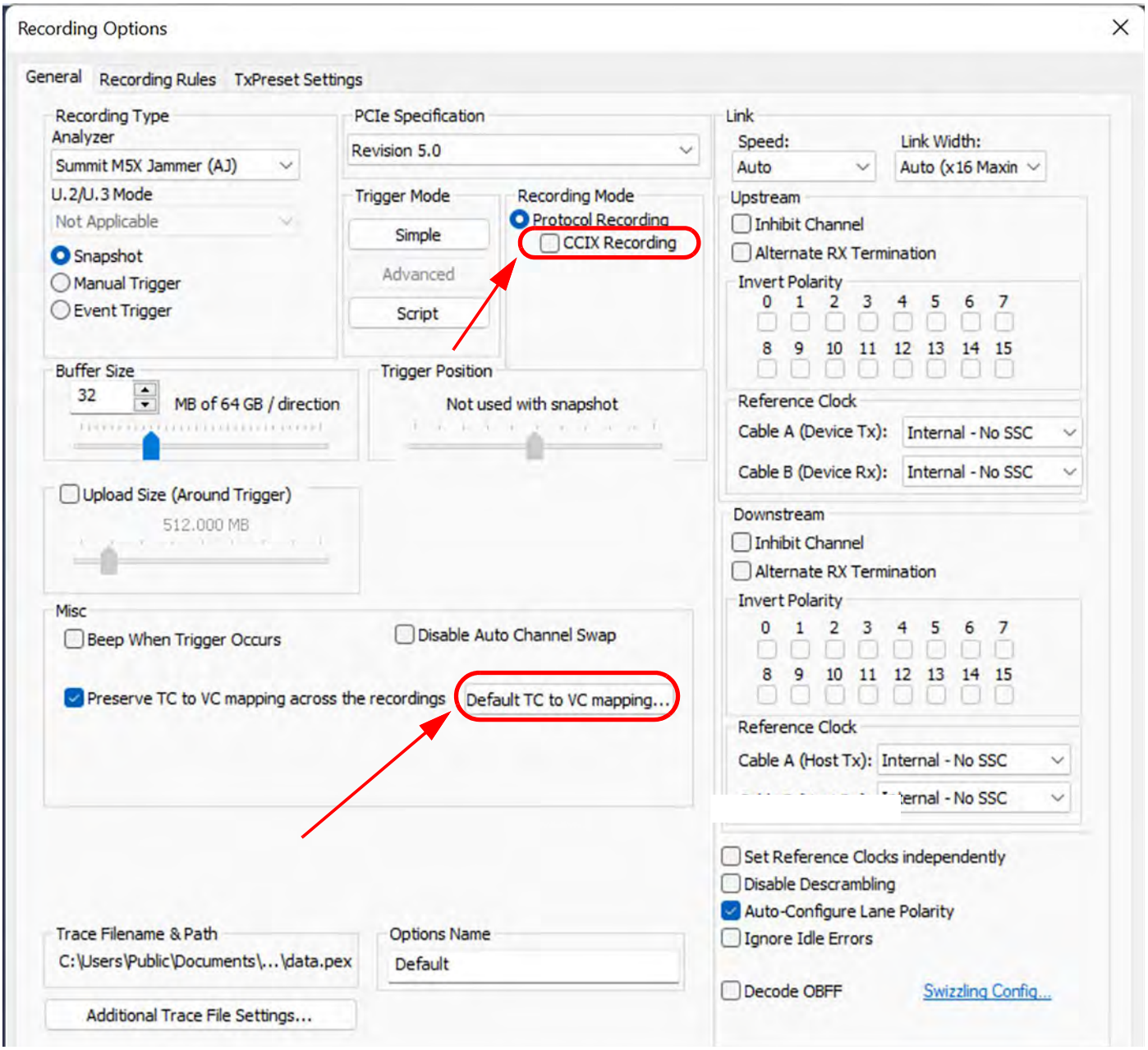


Figure 5.10: M5xAdvanced Recording Mode: Default TC to VC mapping

If you select Default TC to VC mapping, the following dialog box pops up and you can enable CCIX to be decoded. See Figure 5.11 on page 143.

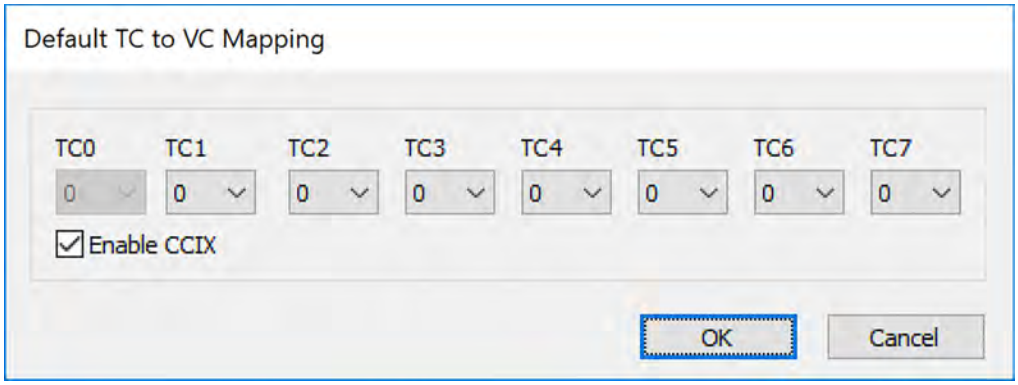


Figure 5.11: CCIX Enabled

For more details about CCIX refer to “Decoding CCIX Protocol” on page 662.

5.7 Recording Mode

There is one recording mode option for Recording Mode with the Summit M5x (see Figure 5.2 on page 134: 2C): Protocol Recording → CCIX recording



Figure 5.12: Recording Mode Options

5.7.1 Protocol Recording

The Protocol Recording mode is an intelligent mode that understands the protocol and displays the recorded data according to the specification. By default it uses the CATC Trace View to show the traffic happening on the wire.

You can use most of the triggering, filtering and sequencing features.

5.7.1.1 Recording the CCIX Protocol

PCIe Protocol Analysis software can record the Cache Coherent Interconnect for Accelerators (CCIX) transaction protocol.

CCIX is a high-performance, low latency, chip-to-chip interconnect architecture that provides a cache coherent framework for heterogeneous system architectures. Cache coherency is automatically maintained at all time between the central processing unit and the various other accelerators in the system. Operating over standard PCIe, CCIX supports signaling rates between 16 GT/s and 25 GT/s per link with support for port aggregation for higher performance.

CCIX is largely an extension of the PCI Express architecture, consists of a number of stacked protocol layers.

- CCIX Protocol Layer – coherency protocol that manages memory reads and writes, provides a mapping for the on-chip architecture-dependent coherency protocols (e.g., AMBA CHI/ACE). This layer also defines the cache state (e.g. shared/unique, clean/dirty).
- CCIX Link Layer – formatting protocol for transport (e.g., PCIe). This layer also manages link aggregation.
- CCIX Transport Specification
- PCIe Transaction Layer – Handles PCIe transactions. The layer also supports virtual channels, permitting transmission for different data streams across a single shared link.
- CCIX Transaction Layer – Handles CCIX transactions. This layer optimizes out superfluous PCIe packet fields, reducing overhead.
- PCIe Data Link Layer – Handles standard data link layer (e.g., CRC, ACK).
- CCIX/PCIe Physical Layer – Handles standard PCIe physical layer. This layer also supports 25 GT/s ESM mode.

CCIX decoding relies on Traffic Class (TC) to Virtual Channel (VC) mapping to be configured. If not configured you'll get the warning message below. See Figure 5.13 on page 144.

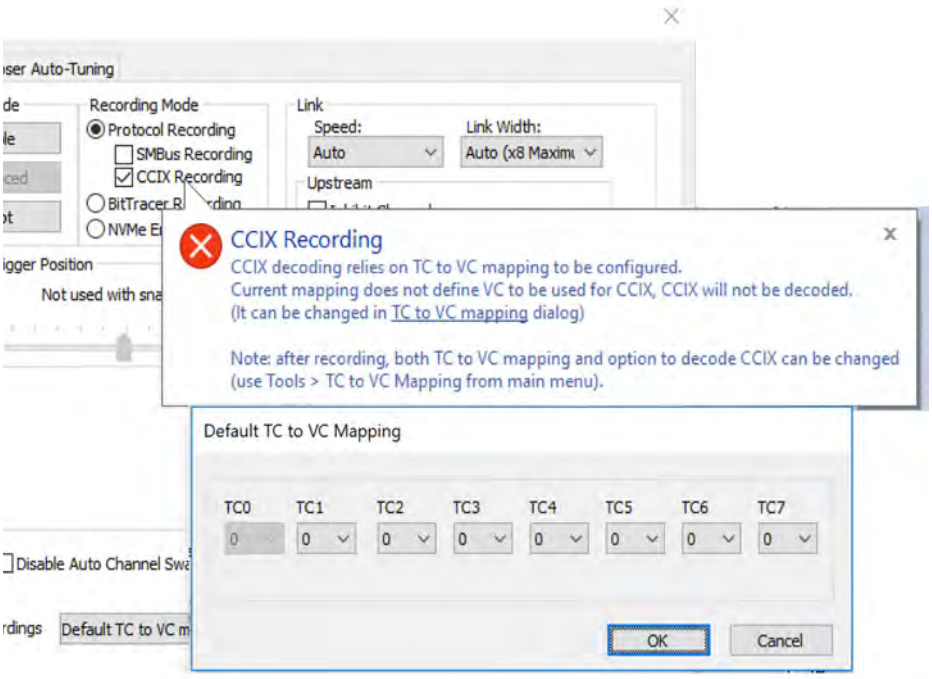


Figure 5.13: Selecting CCIX Recording Before Mapping from TC to VC

After mapping TC to VC the warning message goes away, as shown in Figure 5.14

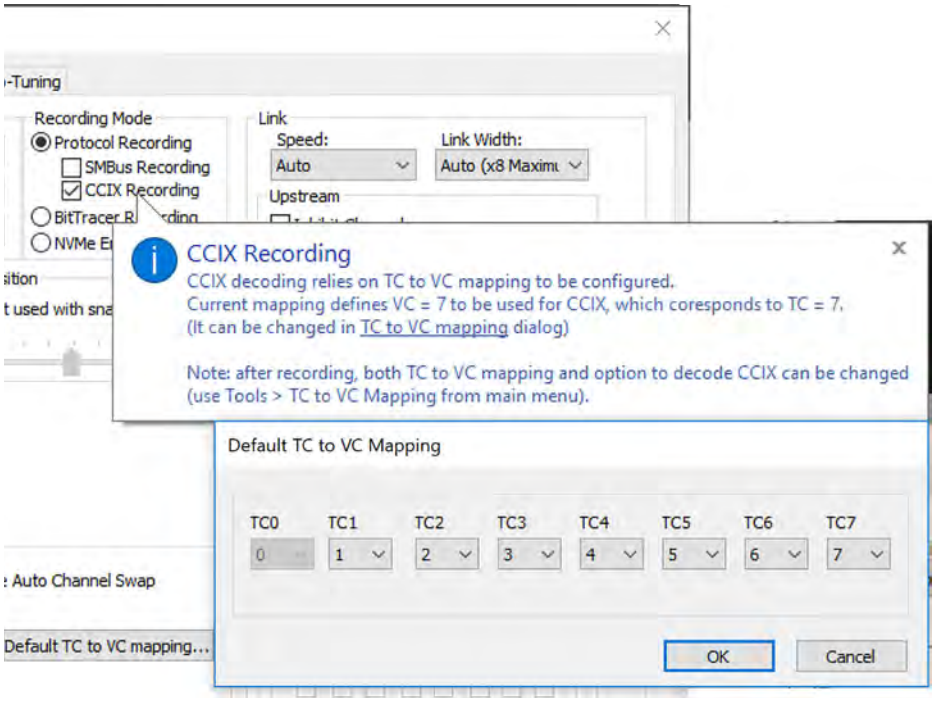


Figure 5.14: Selecting CCIX Recording after Mapping from TC to VC

See “Decoding CCIX Protocol” on page 662 for more details.

5.8 Buffer Size

The Buffer Size allows the Analyzer to record traffic to its buffer and then upload the CATC Trace to the host machine. Recordings are limited in size to the size of the Analyzer's buffer, see Figure 5.2 on page 134: 2D (64 GB per direction for the Summit M5x). The Buffer Size slide-bar allows you to set the size of the recording buffer (see Figure 5.15).



Figure 5.15: Buffer Size Slide Bar (Summit M5x)

The size selection is per direction. For example, selecting 32 MB creates two memory areas of that size.

After you have set the Buffer Size, you must set the Recording type and Trigger position options. These options determine how the buffer is used.

Note: The Buffer Size slide-bar does not precisely portray the buffer size because of the way the packets are stored in the Analyzer’s memory.

5.9 Trigger Position

This Trigger Position slide-bar lets you adjust the amount of recording buffer allocated to recording pre-trigger and post-trigger traffic (See Figure 5.2 on page 134: 2E).

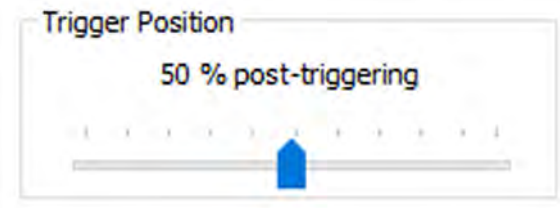


Figure 5.16: Trigger Position Slide Bar

For example, if you set the Trigger Position to 90% Post-Triggering Traffic, the Analyzer records 10% pre-trigger traffic and 90% post-trigger traffic.

Trigger Position is only available when Manual Trigger or Event Trigger is selected.

5.10 Filter Out

Filter Out allows you to filter out the following types of events (see Figure 5.2 on page 134: 2G):

- SKIP Ordered Sets
  - Training Sequence 1 (TS1)
  - Training Sequence 2 (TS2)
  - Electrical Idle (EI)
  - Fast Training Sequence (FTS)
  - SKIP
- Update Flow Control (FC) Data Link Layer Packets (DLLP): UpdateFC DLLP
  - Posted Requests
  - Non-Posted Requests
  - Completion

5.11 Jammer Action

Jammer Actions (see Figure 5.2 on page 134: 2I) allows you to Delete specific Packets (see Figure 5.17), Insert an EDS framing error to packet (see Figure 5.18 on page 147) or Insert nullify TLP errors to packets (see Figure 5.19 on page 147).

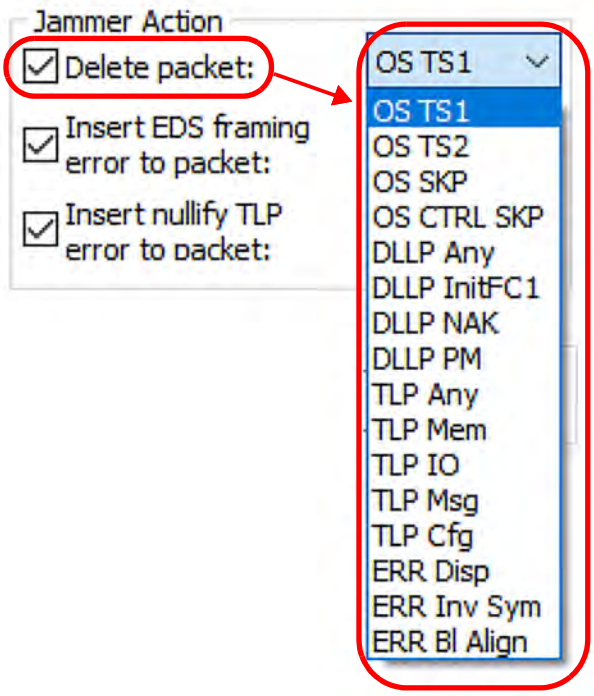


Figure 5.17: Jammer Action: Delete Packets

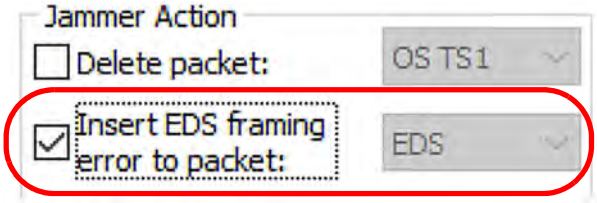


Figure 5.18: Jammer Actions: Insert EDS Framing Error to Packet

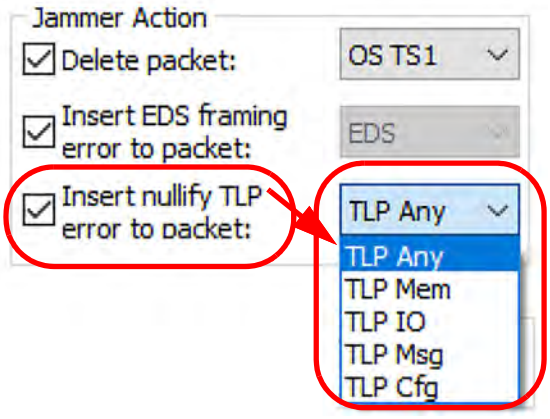


Figure 5.19: Jammer Action: Insert Nullify TLP Error to Packet

5.12 Advanced Trace File Settings

You can set the maximum number of traces that can be opened at one time when recording (from 1 to 10). You can also auto-delete traces if your recording session goes beyond the limit set (from 1 to 10). See Figure 5.2 on page 134: 1B or Figure 5.20 and Figure 5.21.

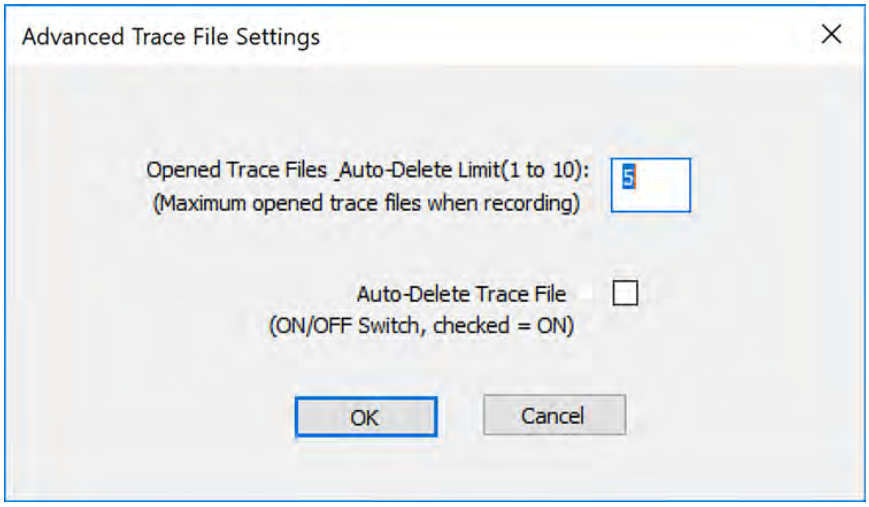


Figure 5.20: Advanced Trace File Settings: 5 Open Traces at a Time

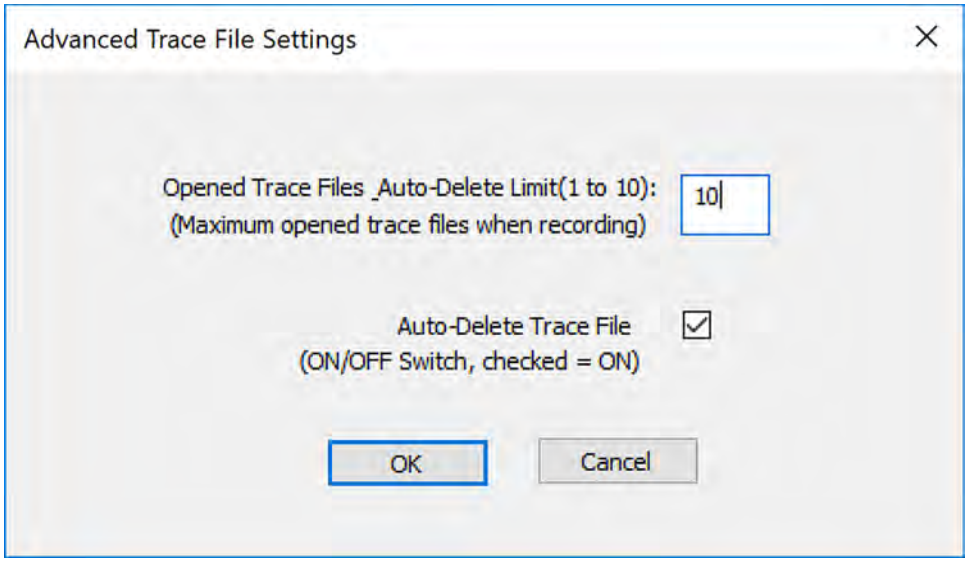


Figure 5.21: Advanced Trace File Settings: 10 Open Traces at a time, Auto-Delete when maximum number reached (10)

5.13 Trace Filename and Path

The Trace Filename and Path button sets the path and CATC Trace name for the recording. It allows you to change the default file name and path for the recorded CATC Trace file. The pre-defined name is **data.pex**. See Figure 5.2 on page 134: 1A.

1. Select the **Recording File Name** button.
2. The Specify Trace File Name dialog opens to navigate to the directory you want.
3. Enter the new file name in the File name field.
4. Click the **Save** button.

   This action does not do any immediate save operation. It just changes the default name and uses it in subsequent recordings.

5.14 Saving and Loading Previously Saved Recording Options

You can save a recording or load previously saved recordings. In the Recording Options dialog the following Save options are available (see Figure 5.2 on page 134: 1C and 1D).

Recording Options settings can be saved and later reused by loading previously saved files. Recording options settings are stored in ***.rec** or ***.crec** files. File options are:

- General Recording (**.rec** extension): A general recording options file which contains settings from the 'General(Tab)', 'Recording Rules' and 'Analyzer Calibration' tabs
- Combined Recording (**.crec** extension): An extended recording options file containing everything in the **.rec** extension but also presets for an interposer ('Interposer to Analyzer Path', 'Interposer Host to DUT Path').
- Recording Rules (**.rr** extension): See Chapter 5, "Recording Rules Overview," on page 170.
- PCIe Trace Files (**.pex** extension). See Chapter 4, "Saving CATC Trace Files," on page 111.

5.14.1 Saving Recording Options

5.14.1.1 Buttons

Table 5.1: Buttons for Saving Recording Options

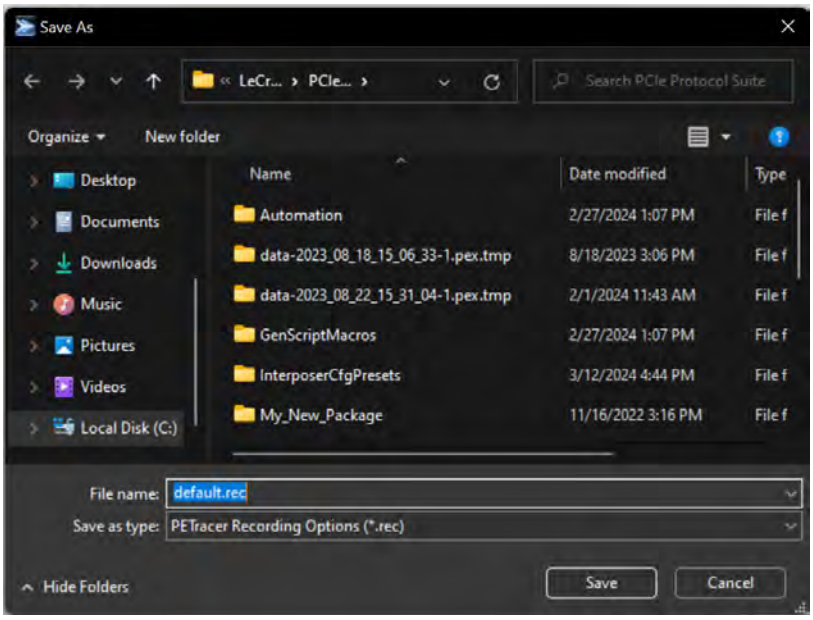
Button	Description
Save	Saves the current options to whatever file name you provide. Figure 5.2 on page 134: 1C
Save As Default	Saves the current options into the default options file. This file is called **default.rec** or any other name you have assigned to the default options file. Whenever the Teledyne LeCroy PCIe Protocol Analysis begins execution, it automatically loads the default file, if one exists. Figure 5.2 on page 134: 1D

5.14.1.2 Steps

To save recording options:

1. Open the Recording Options dialog by clicking  or selecting the menu **Setup → Recording Options**.

2. Set your options, then click **Save** (see Figure 5.2 on page 134 1C). The **Save As..** dialog displays.



3. Enter a unique file name.
4. Choose the **.rec** or **.crec** extension from the drop down menu.
5. (optional) To add a descriptive label to this file to help you remember what options were set, use the **Options Name** box(Figure 5.2 on page 134 1G).
   - For example: If your Recording Options file were named **StandardSettings.rec**, your Options Name could be a long descriptive label such as **Standard Record Options used for all normal Recordings**.

5.14.2 Loading Recording Options

5.14.2.1 Buttons

Table 5.2: Buttons for Loading Recording Options

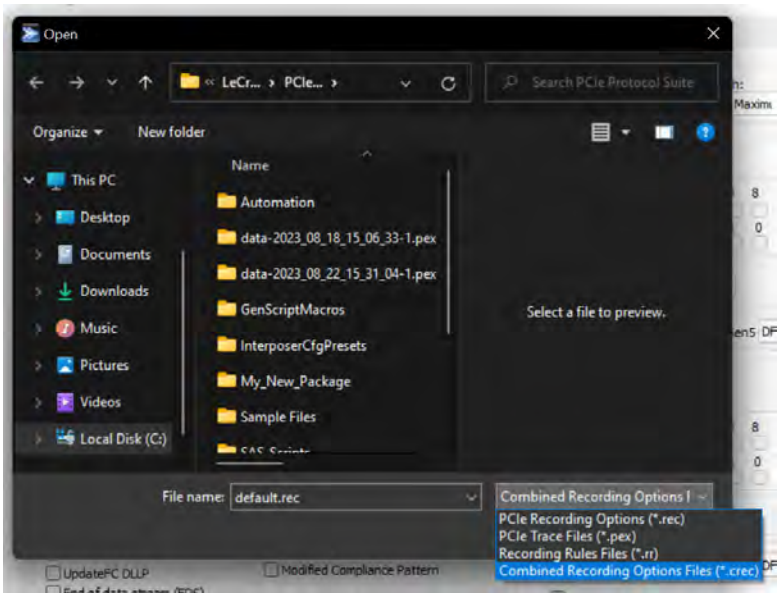
Button	Description
Load	Loads a previously saved set of recording options. Figure 5.2 on page 134: 1E
Load Default	Loads the default set of recording options. Figure 5.2 on page 134: 1F
Restore Factory Settings	Select this tab to Restore the Factory Settings for Recording Options. Figure 5.2 on page 134: 1H

5.14.2.2 Steps

To load Recording Options:

1. Click  or select the menu **Setup** → **Recording Options**.

2. Click the **Load** button from the Recording Options dialog (see Figure 5.2 on page 134 1E). The Load dialog opens and lists previously saved options files:



3. Select a file and click **OK**. The options file loads.

5.15 Transceiver Preset Settings

Next to the General tab is the TxPreset Settings tab - Transceiver Preset settings. See Figure 5.22.

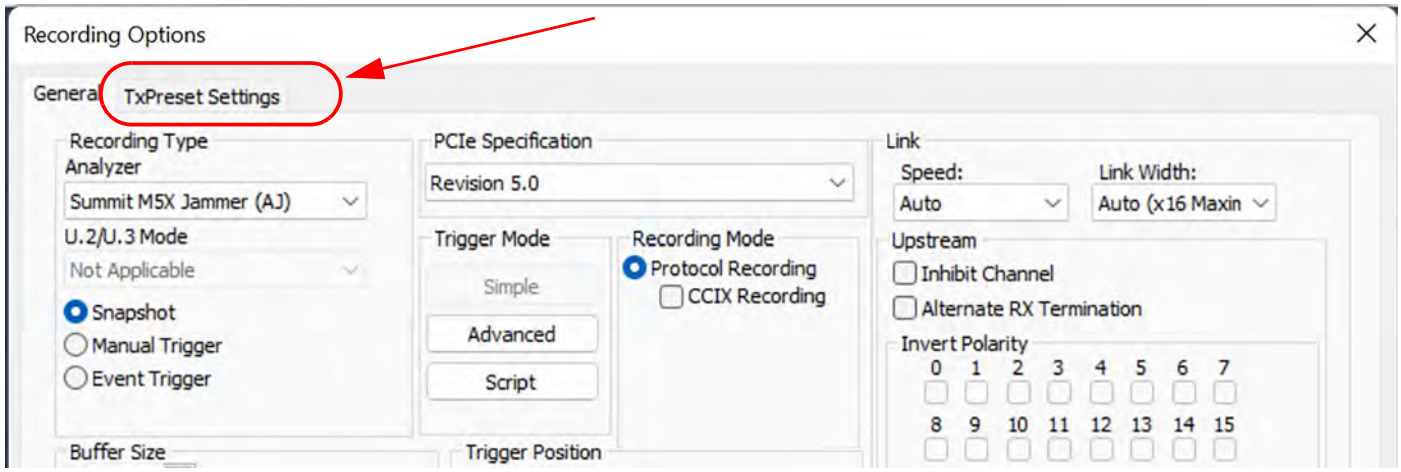


Figure 5.22: Transceiver Preset Settings tab

When you select the “TxPreset Settings” tab, you can adjust the characteristics on the transceiver to get the highest quality signal for both Upstream and Downstream signals. There are ten settings to choose from (P0 to P9) and for each setting you can set the voltage swing from 390 mv to 1040 mv. See Figure 5.23 on page 152.

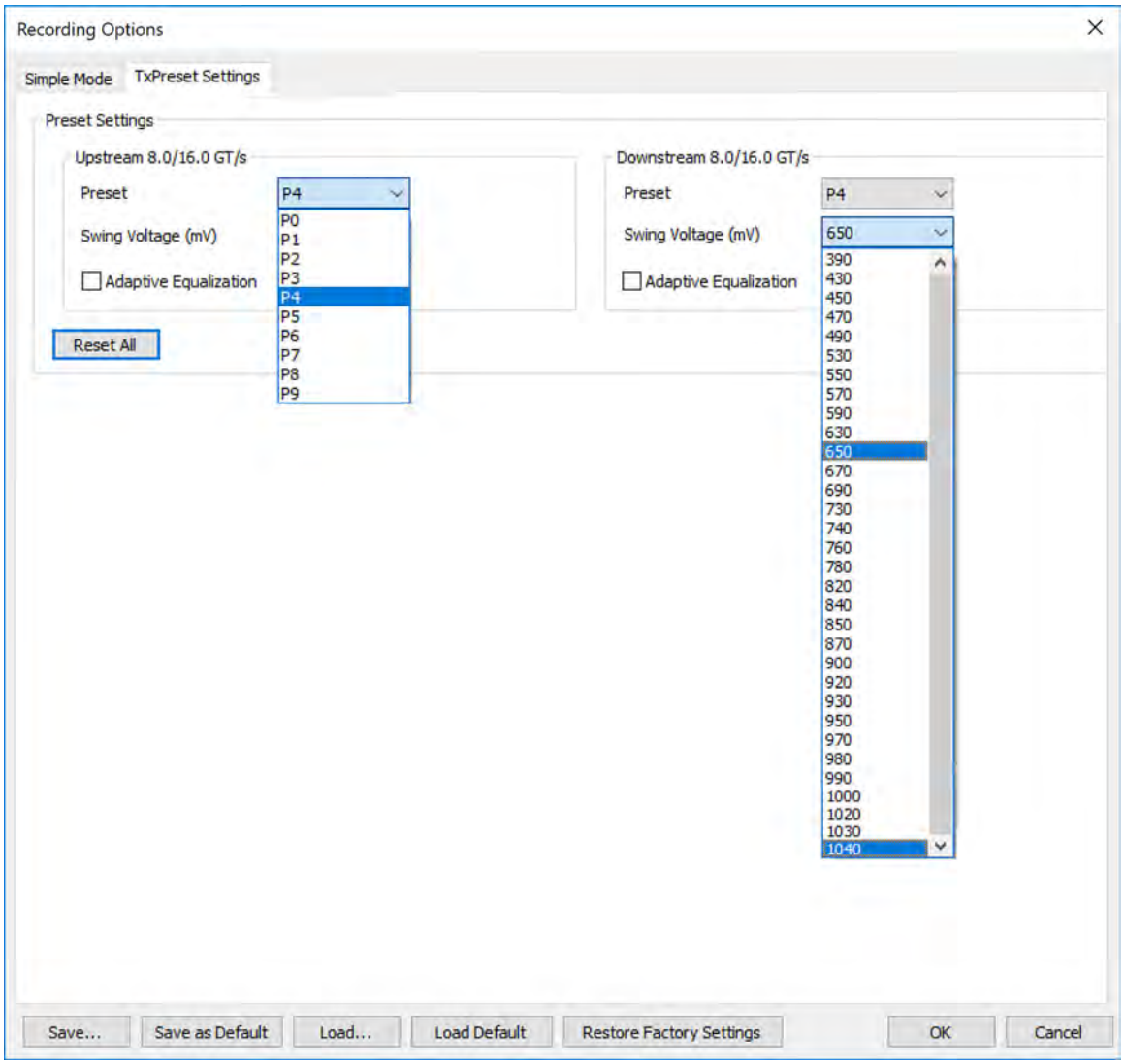


Figure 5.23: Turn Off Adaptive Equalization: Manually Setting each Point and Voltage Swing

There are also buttons to:

- Save your settings
- Save your settings as the Defaults
- Load Settings from a file
- Load the Default Settings
- Restore Factory Settings
- OK
- Cancel

5.16 Viewing Legacy Multi-Segmented CATC Traces

Current PCIe Protocol Analysis handles traces as large as the maximum buffer size selected. It does not need to generate segmented traces, but is able to open segmented traces generated with older software versions. Simply open the *.pem extension file and

the trace will be converted to a new format single trace. If opening a *.pex file part of a segmented trace make sure not to update the file in order for the original segmented index to work properly.

5.17 Link Settings

The Link options panel allows you to manage links (see Figure 5.24 for the Summit M5x). You can define the basic link parameters or leave it on Auto detect. The various link settings are described in this section (See Figure 5.2 on page 134: 3).

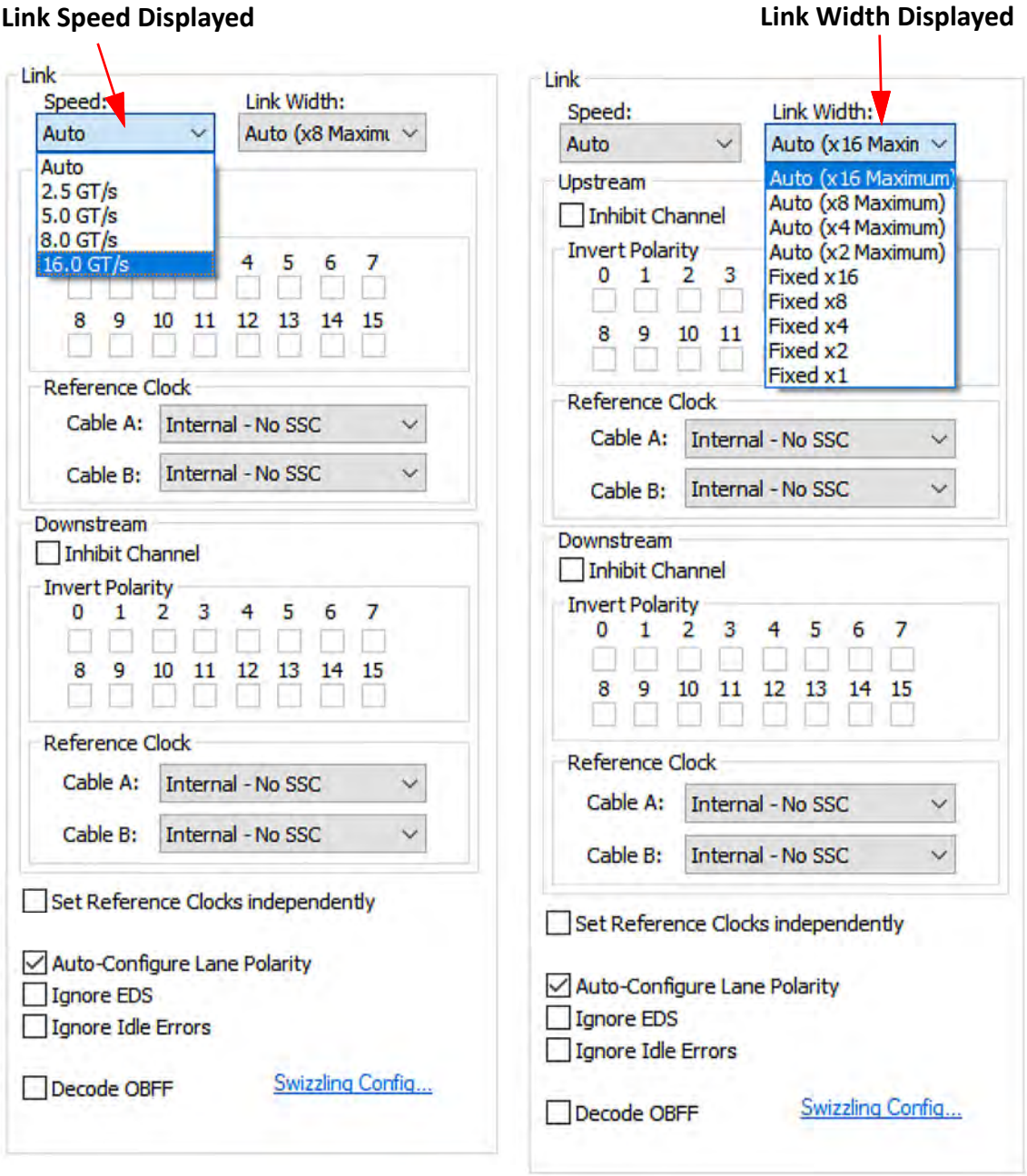


Figure 5.24: Link Options for Summit M5x

5.17.1 Speed

The Speed can be set at Auto, 16.0 GT/s, 8.0 GT/s, 5.0 GT/s, or 2.5 GT/s for the Summit M5x from the drop-down menu. The default is Auto (see Figure 5.2 on page 134: 3A or Figure 5.24 on page 153 above left side).

Note: Auto: When set to Auto, Teledyne LeCroy's embedded software auto-determines the speed. Disable Descrambling is also enabled.

When set to a specific speed (16.0 GT/s, 8.0 GT/s, 5.0 GT/s, or 2.5 GT/s) Teledyne LeCroy's software forces the hardware to record at that speed.

Note: When set to a specific speed, (End of Data Stream) EDS detection is disabled.

For Auto speed setting to work the polarity setting of lane 0 has to be correct. The polarity can be set manually if the link is already in L0 state, or, for automatic polarity detection, the bus has to go through a training sequence so the analyzer can track the polarity.

Note: When selecting Auto in the Speed drop-down list the embedded software is able to find the correct speed even if the link does not go through a training sequence.

5.17.2 Link Width

The Link Width sets the physical width of the link. Select the Link Width from the drop-down menu (see Figure 5.2 on page 134: 3B or Figure 5.24 on page 153 right side for the Summit M5x). The available options (and the default) will be shown according to the detected product.

Auto Max X16: Calculates link width automatically up X16

Auto Max X8: Calculates link width automatically up X8

Auto Max X4: Calculates link width automatically up X4

Auto Max X2: Calculates link width automatically up X2

Fixed X1 Link is assumed to be always X1

Fixed X2 Link is assumed to be always X2

Fixed X4 Link is assumed to be always X4

Fixed X8 Link is assumed to be always X8

Fixed X16 Link is assumed to be always X16

Note:
- If the bus goes to a link width different from the one selected as fixed option, the trace will be full of errors. The appropriate Auto option needs to be selected in this case.
- When selecting Auto in the Link Width drop-down list the embedded software is able to find the correct link width even if the link does not go through a training sequence.
- If an Auto Link Width is selected, there is no Lane Reversal. If a Fixed Link Width is selected, the Reverse Lanes checkbox is enabled. See Figure 5.26 on page 155 for the Summit M5x.

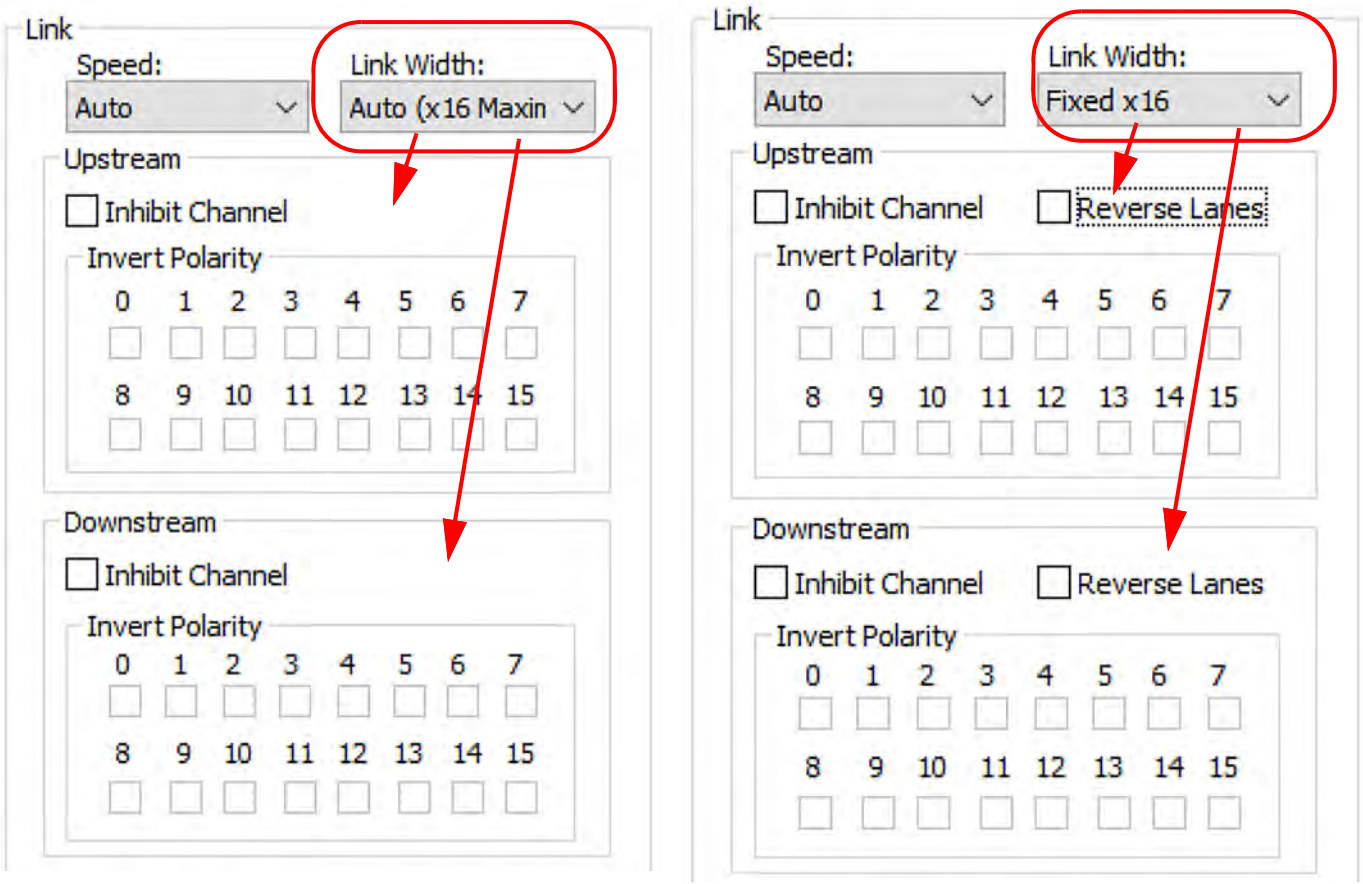


Figure 5.25: Summit M5x Link Width: Auto -> No Lane Reversal, Fixed Lane Width -> Lane Reversal Check Box is Enabled

5.17.3 Upstream and Downstream

Gives you low-level control over each link direction. The heading for these boxes indicates the port and/or unit to which the following options are applied based on the current Analyzer configuration (see Figure 5.2 on page 134: 3C and 3E for the Summit M5x).

- ❑ Inhibit Channel: Do not record/upload this channel.
- ❑ Reverse Lanes: Manual lane reversal. If Auto-Configure Lane Swizzle is set, the Reverse Lanes option will be ignored.

- ❑ Invert Polarity.
- ❑ Alternate RX Termination: When selected and saved you will get a Warning Message that the RX termination has changed and you will need to retrain (examples below). See Figure 5.26.

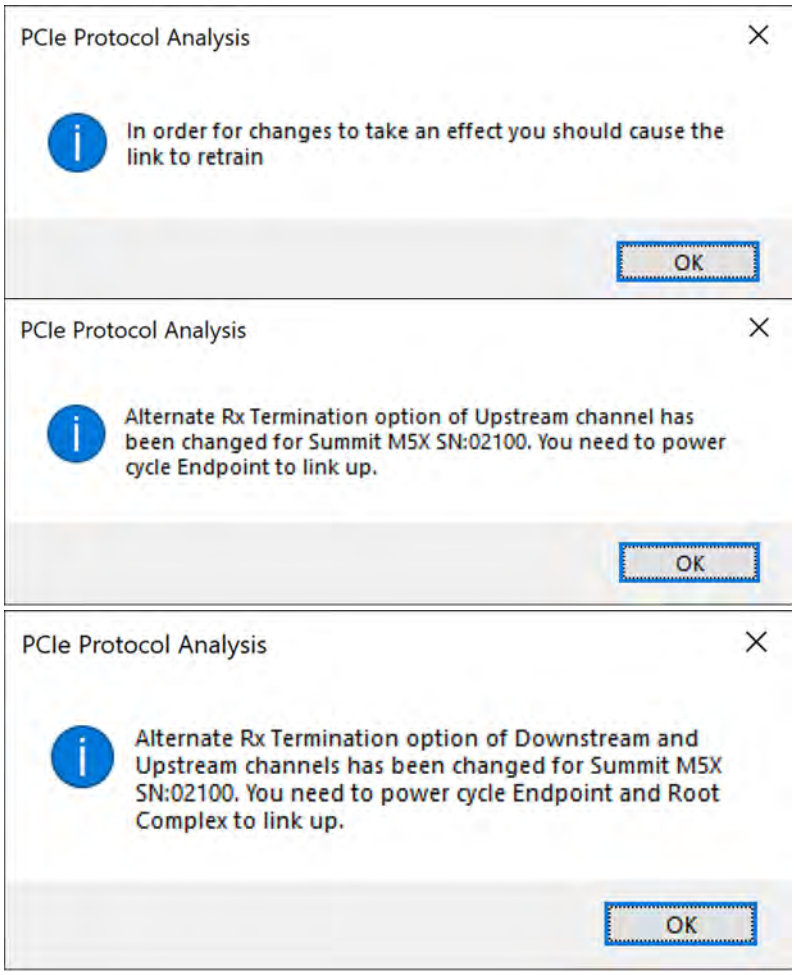


Figure 5.26: Warning Messages After Setting Upstream or Downstream or Both Alternate Rx Termination option

5.17.4 Reference Clock

See Figure 5.2 on page 134: 3D for the Summit M5x Jammer (AJ).

Usually, both Upstream and Downstream directions use the same clock option, this is why the recording option Reference Clock Independently is set by default.

In cases when you have to use different clocks for the different traffic directions you must select the “Set Reference Clock Independently” option (see Figure 5.2 on page 134: 3F) and set the upstream and downstream clock to come from different sources. See “Set Reference Clocks Independently” on page 159.

In both the Upstream and Downstream directions, Cable A and Cable B can have the following sources for the Reference Clock:

- ❑ The Internal Clock (100MHz +/-300ppm No SSC clock generated in the analyzer)

- An External Source (Reference clock from the PCIe bus routed through the interposer cable)
- The SMA connector on the front panel
- Internal — SSC (Spread Spectrum Clock)
- FROM Cable B CLK or if defining the clock for Cable B the source can be FROM Cable A CLK

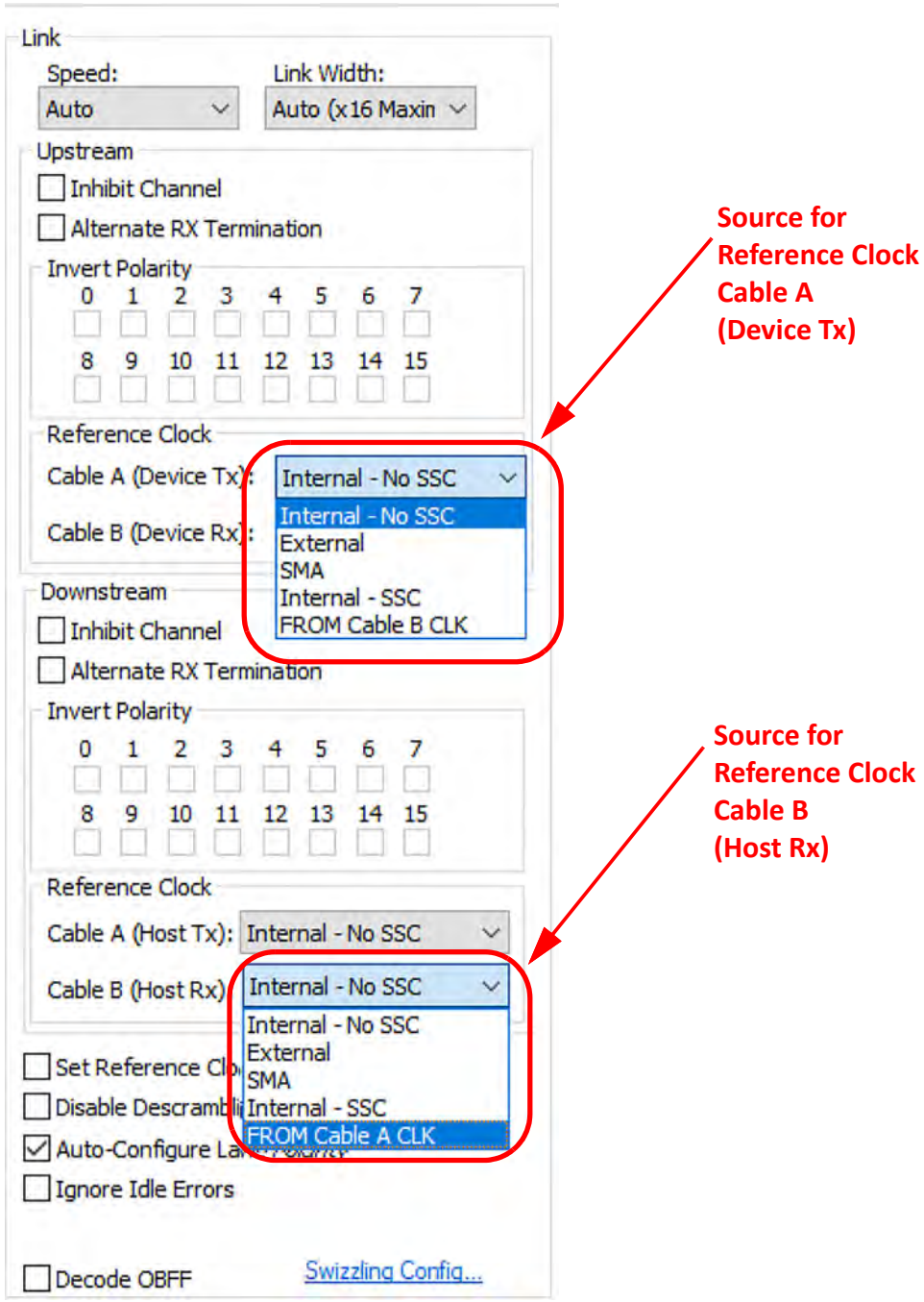


Figure 5.27: Reference Clock: Upstream and Downstream

5.17.4.1 Reference Clock: Cable A

Internal – No SSC

The analyzer has an internal clock generator that can be used for recording when the Device Under Test does not supply a reference clock. In this case, you select the Internal option. If you select this option the Internal clock will not have Spread Spectrum capability.

Note: Due to long exit latency from low power sub states some loss of traffic has been observed when analyzer latency exceeds DUT latency using the common reference clock. Teledyne recommends the use of the internal reference clock setting for low power sub-states testing.

External

For the Summit M5x , External Clock means to use the clock that is supplied through the cable from the Probe card. The Probe card cable gets its clock from the specific Host of Device being used with the analyzer/jammer. You need to select the External Reference Clock option.

Teledyne LeCroy's Summit M5x Probe cards support separate clocks for SRIS applications.

Note: If the PCI Express link under analysis uses spread-spectrum clocking, then the Analyzer must use an external reference clock from the system. Select the External Reference Clock option.

SMA

The SMA clock recording option refers to the **Ref Clk In** SMA input connectors on the front panel of the analyzer/jammer. Both the Upstream data and the Downstream data support using a clock from the SMA input connectors. When using the SMA option both clock cables must be connected and the clock must be supplied by the system in order for the recording to happen correctly. The standard PCI Express compliant reference clock is supported. You also need to select the SMA Reference Clock option.

Internal — SSC

The analyzer has an internal clock generator that can be used for recording when the Device Under Test does not supply a reference clock. In this case, you select the Internal option. If you select this option the Internal clock will have Spread Spectrum capability.

From Cable B Clock

If you chose this Reference Clock option, the clock for Cable A will come from Cable B. So both clocks (Cable A and Cable B will be the same).

5.17.4.2 Reference Clock: Cable B

All options same as Reference Clock: Cable A except From Clock A

If you chose this Reference Clock option, the clock for Cable B will come from Cable A. So both clocks (Cable B and Cable A will be the same).

5.17.5 Set Reference Clocks Independently

If you select this option the source of the Upstream clock and the Downstream clock can be independent of each other. See Figure 5.2 on page 134: 3F and Figure 5.28 on page 159.

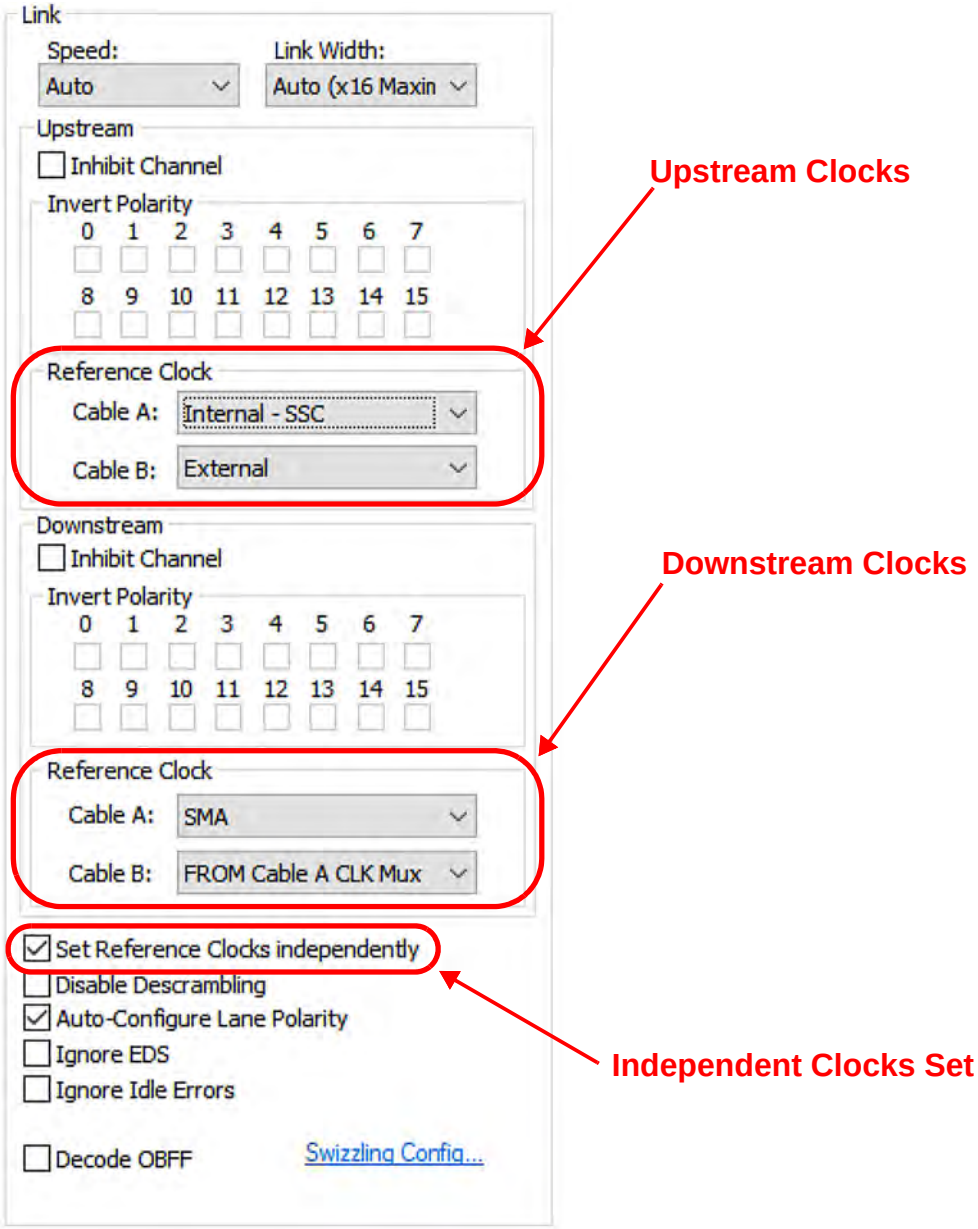


Figure 5.28: Setting Up Independent Reference Clocks

5.17.6 Disable Descambling

If checked, causes the Analyzer to assume that none of the PCI Express traffic is scrambled. By default, the Analyzer determines the scrambling state of the devices under test (see Figure 5.2 on page 134: 3G).

5.17.7 Auto-Configure Lane Polarity

Lets the Analyzer determine lane polarity (see Figure 5.2 on page 134: 3H for the Summit M5x). Auto functions such as Auto Configure polarity rely on Gen1 or Gen2 training sequences to properly discover their values. If the speed option is set to fixed Gen3, the analyzer will never see these sequences and the polarity discovery will not be reported properly in the dashboard dialog.

5.17.8 Ignore Idle Errors

When set, the analyzer will not store errors in between packets into memory. This option helps to preserve analyzer memory to store more packets in cases where memory efficiency is critical. This option filters out Compliance Pattern as well. See Figure 5.2 on page 134: 3I for the Summit M5x.

5.17.9 Swizzling Config...

The Swizzling Config dialog allows you to reconfigure the logical order of the lanes in a link separately for Upstream and Downstream PCIe directions. You can perform the logical to physical assignment manually or let the analyzer detect this on its own (Auto-Configure Lane Swizzle option checked). See Figure 5.2 on page 134: 3J for the Summit M5x.

Note: Autoswizzle works only when the analyzer sees the LTSSM Configuration state link training sequence.

5.17.9.1 Manual Configure Lane Swizzle

If you know how your physical link is connected and the lane numbers advertised for each lane, then you can use the manual swizzle option (Auto-Configure Lane Swizzle option unchecked). On the Swizzling Configuration dialog, drag the number of the logical lane (in blue) to the desired lane physical position.

In the case shown below the Link Width is set to Auto (x16 Maximum) for the Summit M5x , so all 16 lanes are available to be manually configured. See Figure 5.29 on page 161 for the Summit M5x.

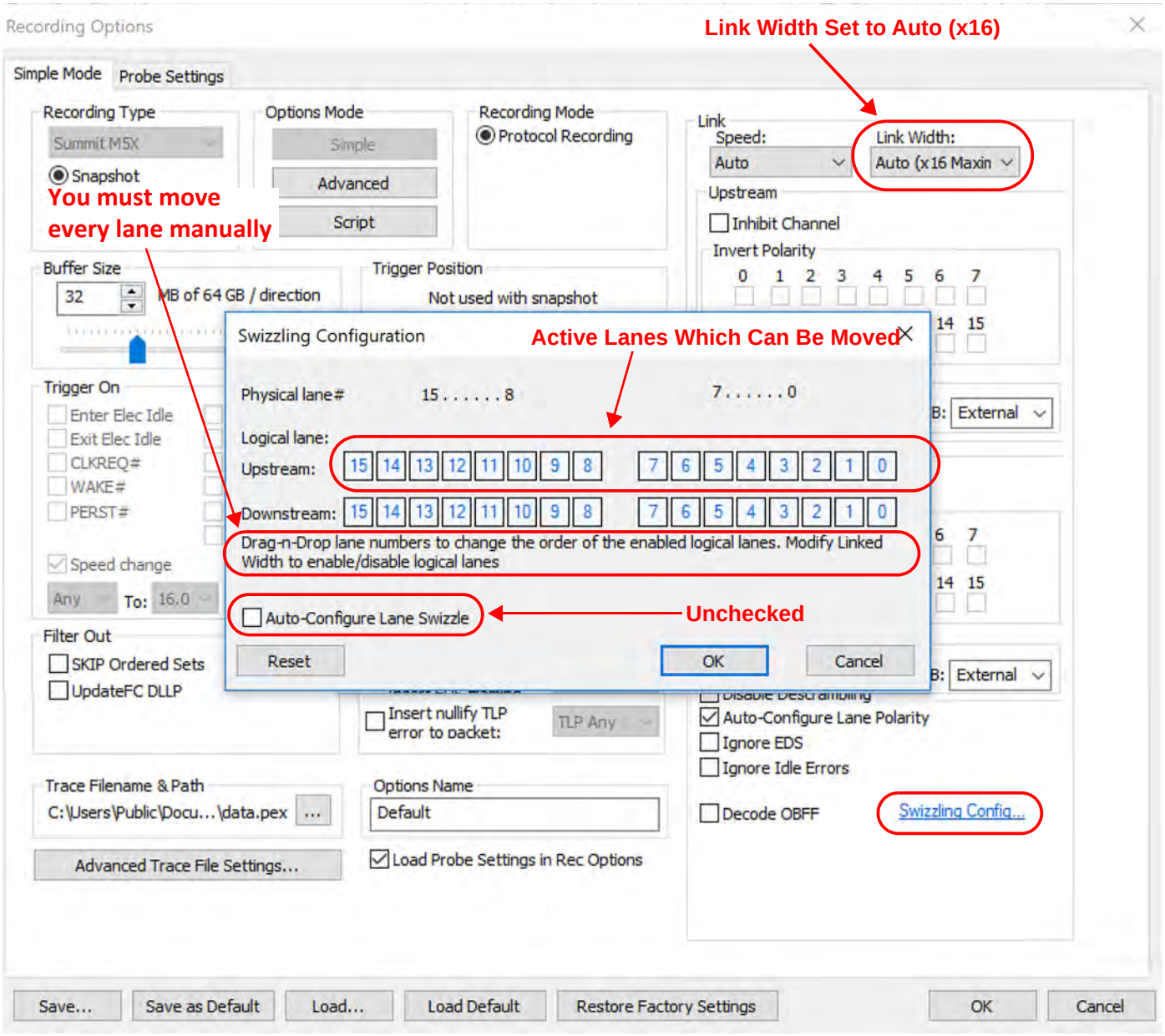


Figure 5.29: Manual Swizzle: Link Width Set to Auto (x16)

In the example shown below, we re-assigned the Upstream Physical lanes as follows:

- Lane 7 to Lane 15
- Lane 6 to Lane 14
- Lane 5 to Lane 13
- Lane 4 to Lane 12
- Lane 3 to Lane 11
- Lane 2 to Lane 10
- Lane 1 to Lane 9
- Lane 0 to Lane 8

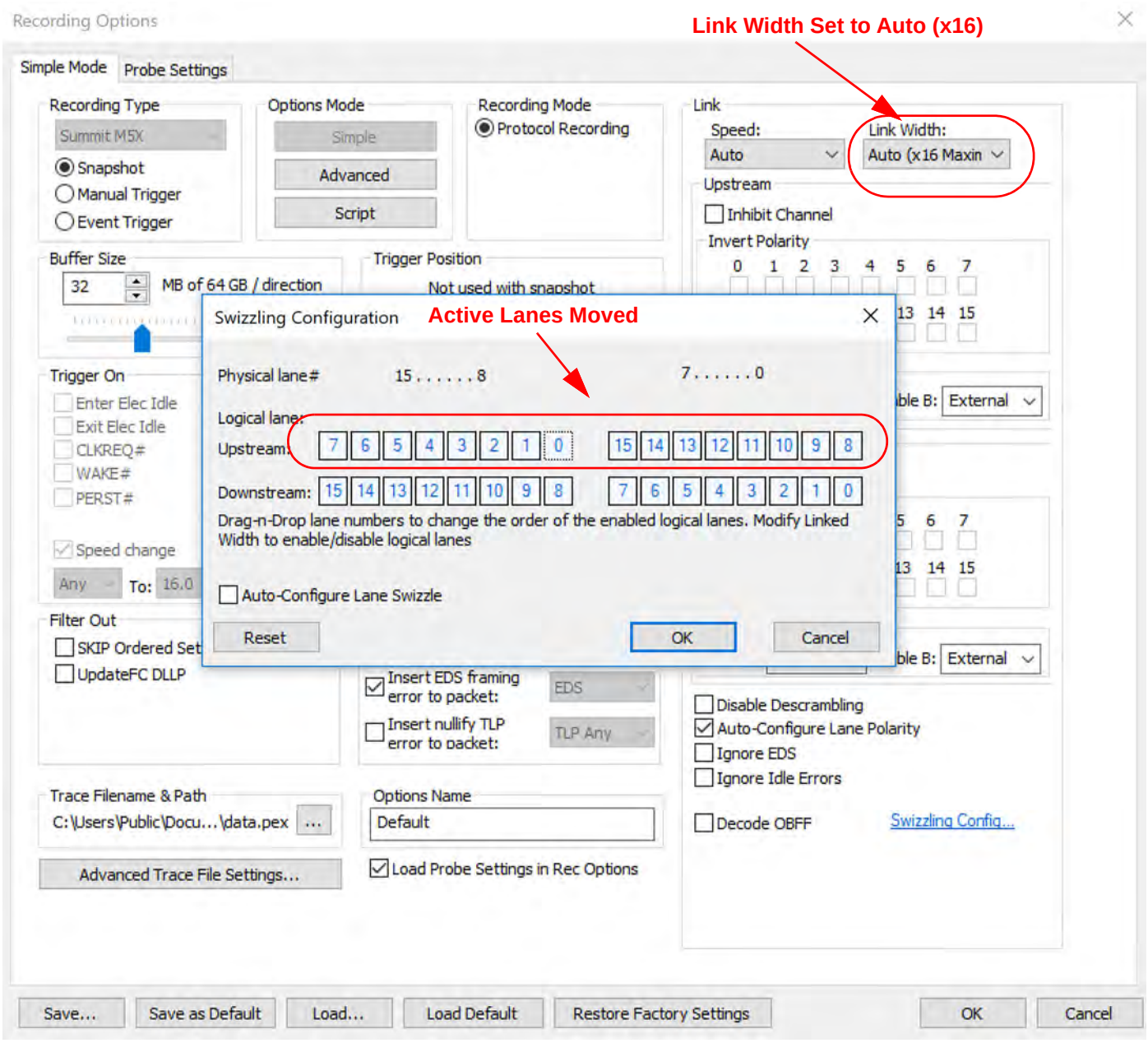


Figure 5.30: Manual Swizzle Configuration

Note:
- The simplest way to make new lane assignments is to always move the highest source lane number to the highest destination lane number.
- If the source lane has a lower number than the lane it is replacing, then the software performs a right shift to the higher numbered replaced lane. If the source lane has a higher number than the lane it is replacing the software performs a left shift to the lower numbered replaced lane.

5.17.9.2 Example: Move Highest Source Lane First

In the example below we replaced Lane 7 with Lane 3 and Lanes 7 through 4 were shifted to the right. Then Lane 7 was replaced with Lane 2 and Lanes 7 through 4 were shifted to the right. Then Lane 7 was replaced with Lane 1 and Lanes 7 through 4 were shifted to the right. Finally Lane 7 was replaced with Lane 0 and Lanes 7 through 4 were shifted to the right.

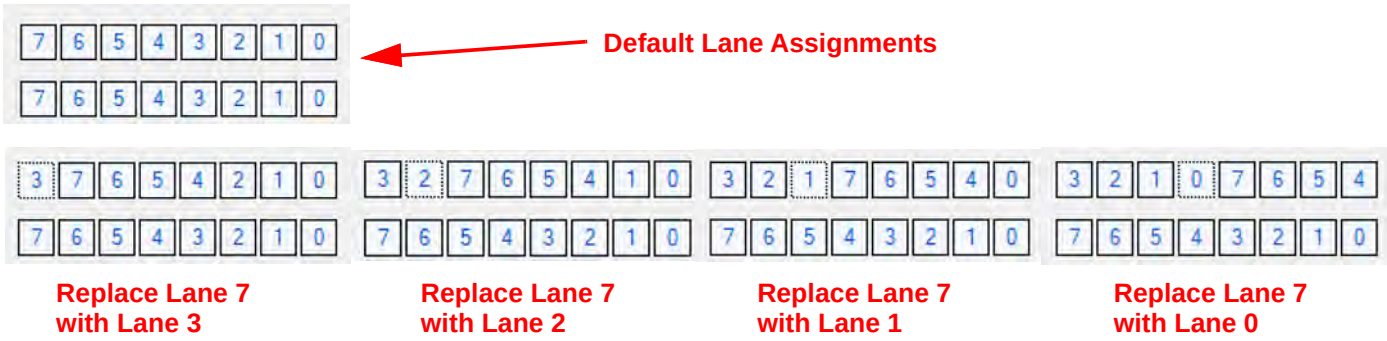


Figure 5.31: Manually Moving Lane Assignments: Highest Numbered Lane First

5.17.9.3 Example: Move Lowest Source Lane First

If you start with the lowest numbered lane you will get completely different results.

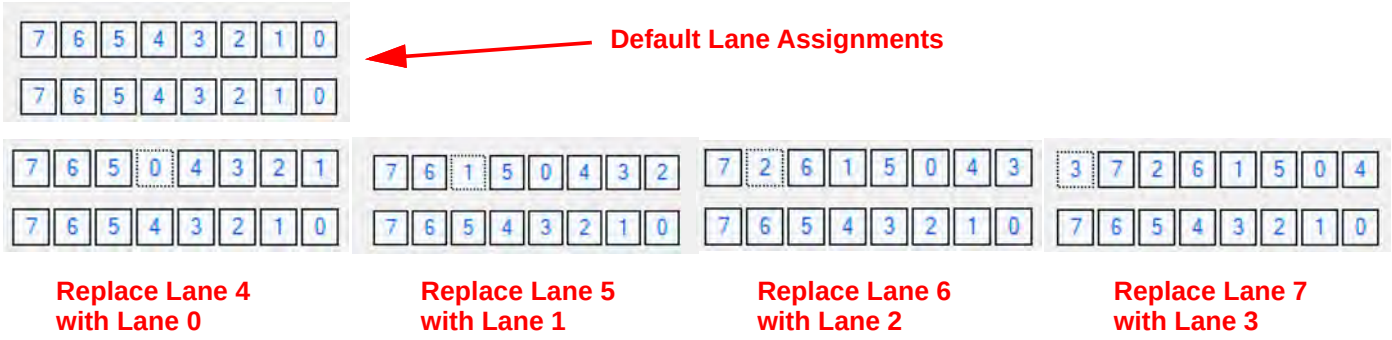


Figure 5.32: Manually Moving Lane Assignments: Lowest Numbered Lane First

5.17.9.4 Working with Less Than Sixteen Lanes

If the lane number in the box is not in blue this means that the lane is not participating in the link from the Summit analyzer's point of view. This may happen because the Link Width selected is less than x16. See Figure 5.33.

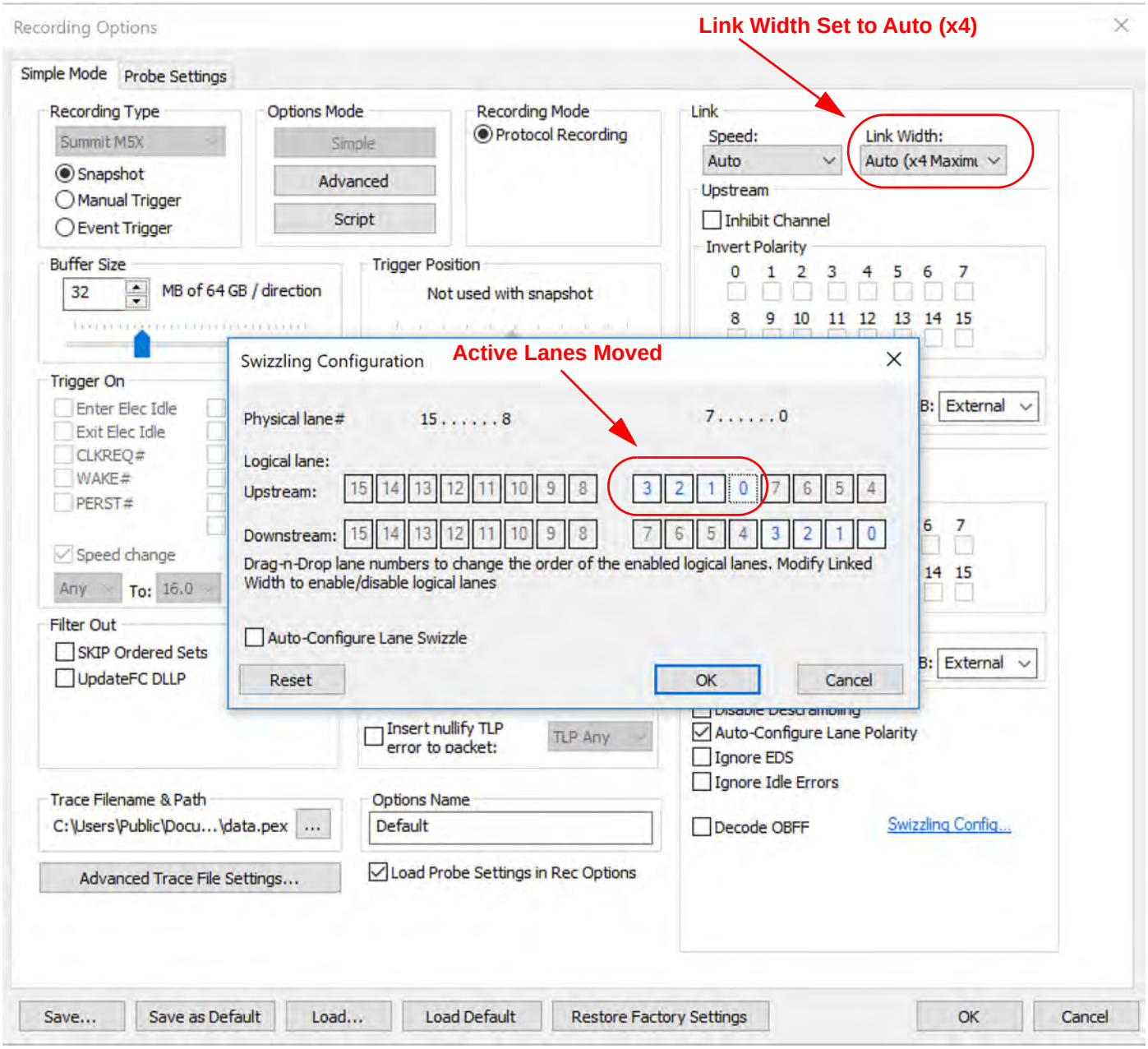


Figure 5.33: Manual Lane Swizzle Configuration: Moving Four Lanes

Note: In the example above Lane 0 through Lane 3 are the only active lanes. They can be moved to any lane that the analyzer supports. The analyzer in this case is the Summit M5x, which can support 16 lanes.

If you need the logical lane to be assigned to a position that has a number in gray color, you need to make sure the Link Width can support that lane by increasing the Link Width option. In the case shown below, we wanted to move Lane 7 to Lane 15. To make Lane 7 an active lane we had to increase the Link Width to x8. See Figure 5.34

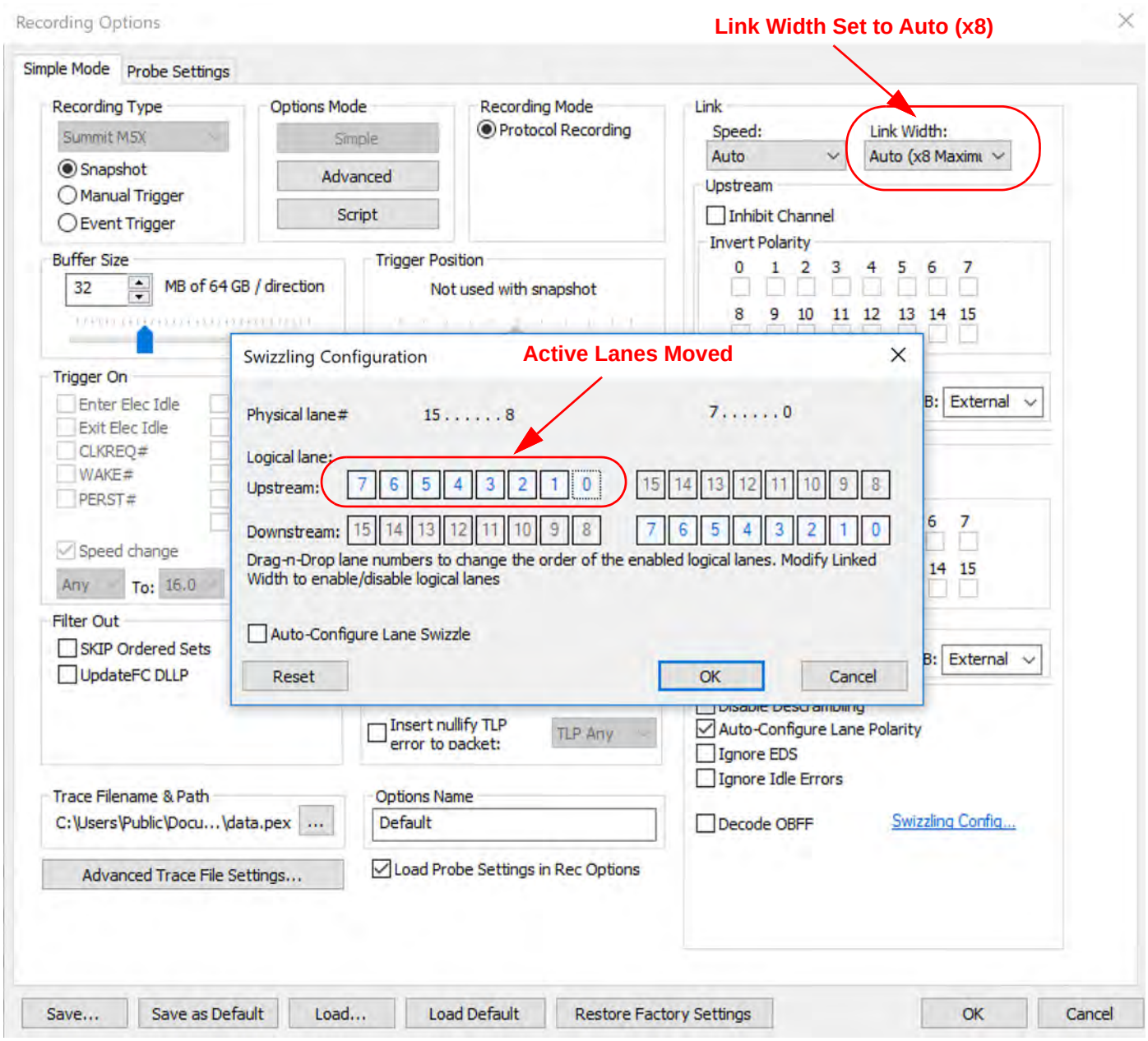


Figure 5.34: Manual Lane Swizzle Configuration: Moving Eight Lanes

Note: If the link you are trying to analyze is lower than x16 and the lane resides in a grayed position you need to select the Auto Link Width option that will include the physical lane to use.

5.17.9.5 Auto-Configure Lane Swizzle

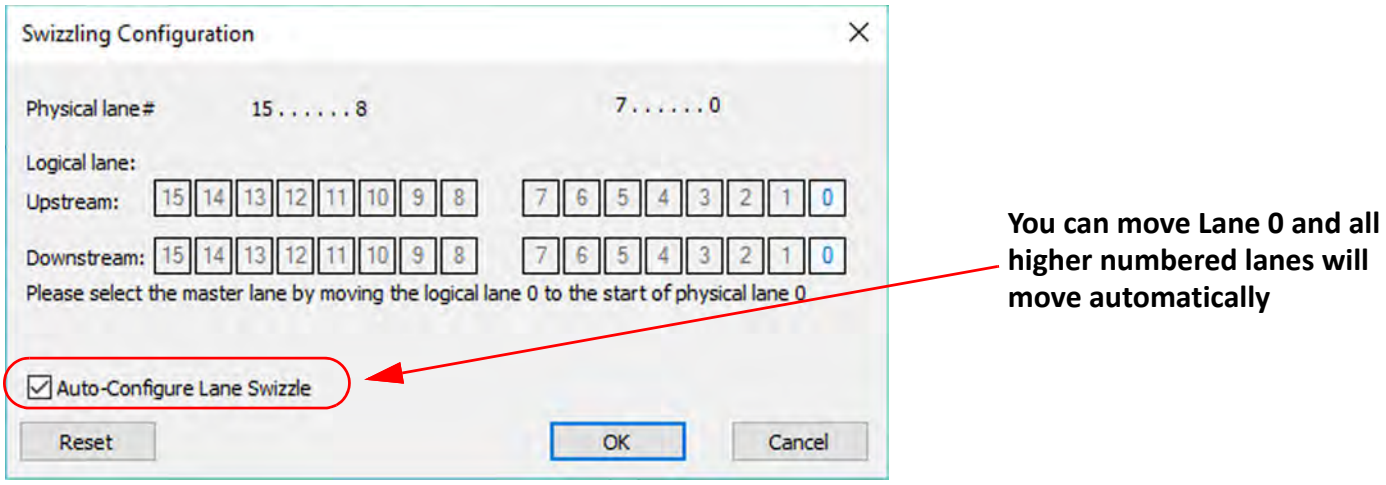


Figure 5.35: Swizzling Config Dialog

When the Auto-Configure Lane Swizzle option is checked the Summit Analyzer requires you to provide the physical location for at least one lane with active traffic. You can specify this by moving the enabled lane L0 to the physical location where either lane 0 is or any other active lane for the link. See Figure 5.36 on page 167.

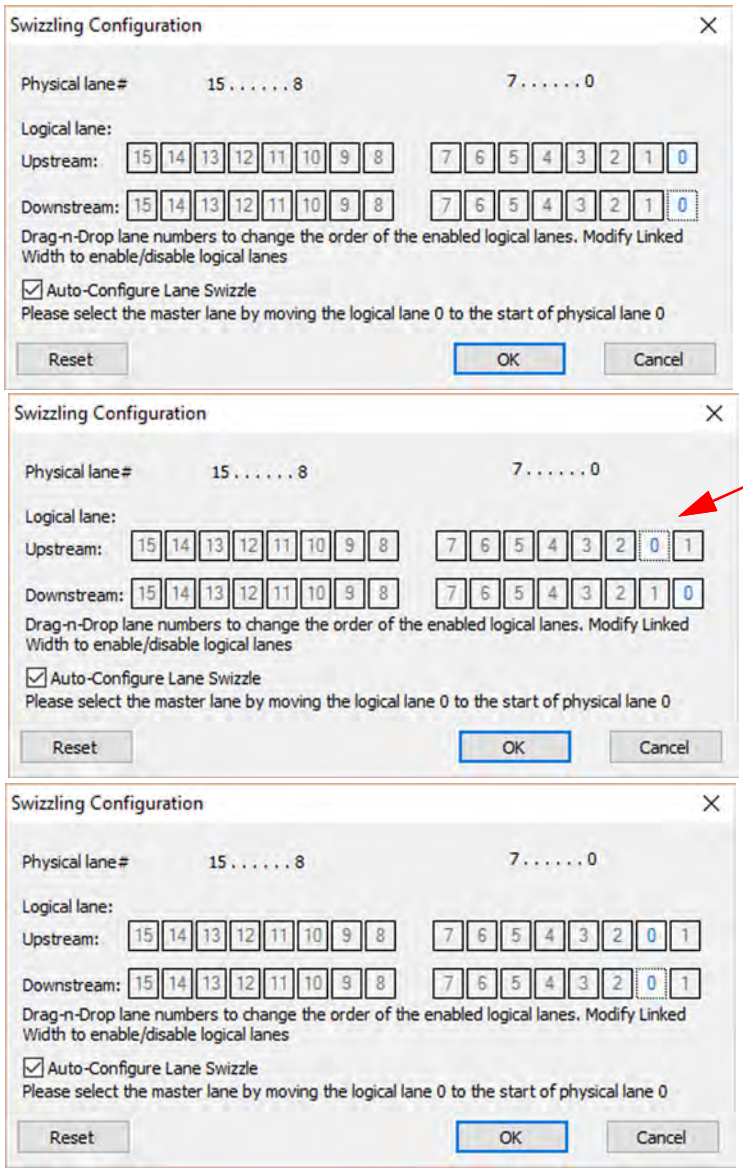


Figure 5.36: Manually Configuring Lane 0 when Auto-Configure Lane Swizzle is Checked

Note: Auto-Configure Lane Swizzle will not work properly if the link is bifurcating. Use manual swizzle instead.

5.17.10 Decode Optimized Buffer Flush/Fill (OBFF)

Select this checkbox to decode Optimized Buffer Flush/Fill (OBFF) events. See Figure 5.2 on page 134: 3K). As a system operates, each of its devices does not know the power state of each of the resources in the system. Without coordination, each of the devices will go in and out of their low-power states as necessary to execute the tasks they are assigned to do. This "asynchronous" behavior prevents the optimal power management of the CPU, host memory sub-system and other devices, because the intermittent traffic keeps the system permanently awake and unable to optimize power management across the system.

As part of an implementation of a system-level power strategy, the idle time and low-power states of the devices must be optimized to enable them to stay in their low-power states longer. Basically, a host can provide information to all devices by broadcasting a message about the system power state. The devices can utilize this information to group a load of requests, wait until the system wakes up, and burst out all of the requests at the same time. By doing this, the device does not wake up a sleeping CPU and/or the system memory sub-system. Waiting creates extended periods of system inactivity which saves overall system power. The host utilizes the OBFF to give devices a "hint" so they can optimize their behavior, which improves power management at the system level.

5.18 Triggering

Triggering Options can be set in both Simple and Advanced Modes. The options in both modes are the same, only the GUI is different where shortcuts for the events are displayed in the Simple Mode for easy access (see Figure 5.7 on page 139).

In the Advanced Mode triggering is set up via the Recording Rules (see “Triggering On (Advanced Mode)” on page 244. The Simple Mode allows you to simply define triggering by checking the boxes shown below (see Figure 5.8 on page 140).

Note: Ensure the correct analyzer is selected for the right options.

5.18.1 Triggering On (Advanced Mode)

The same triggering options are available in the Advanced Mode as in the Simple Mode. The Advanced Mode gives you additional flexibility to drill down and configure these options in greater detail via the Recording Rules dialog.

In the Advanced mode click on the Recording Rules tab to configure the settings. As shown in Figure 5.37 on page 169, the Recording Rules tab allows you to create New Events. For each event you can create Actions. A detailed explanation of the Recording Rules is given in the following sections.

Note:
- The External Input Trigger is combined with any other trigger defined in the sequencer.
- External Input Trigger is not configurable, it will always cause the analyzer to trigger on a toggle (change in level: Low to High or High to Low) when using “Manual Trigger” (see “Manual Trigger” on page 138) or triggering on any “Event Trigger” (see “Event Trigger” on page 138).

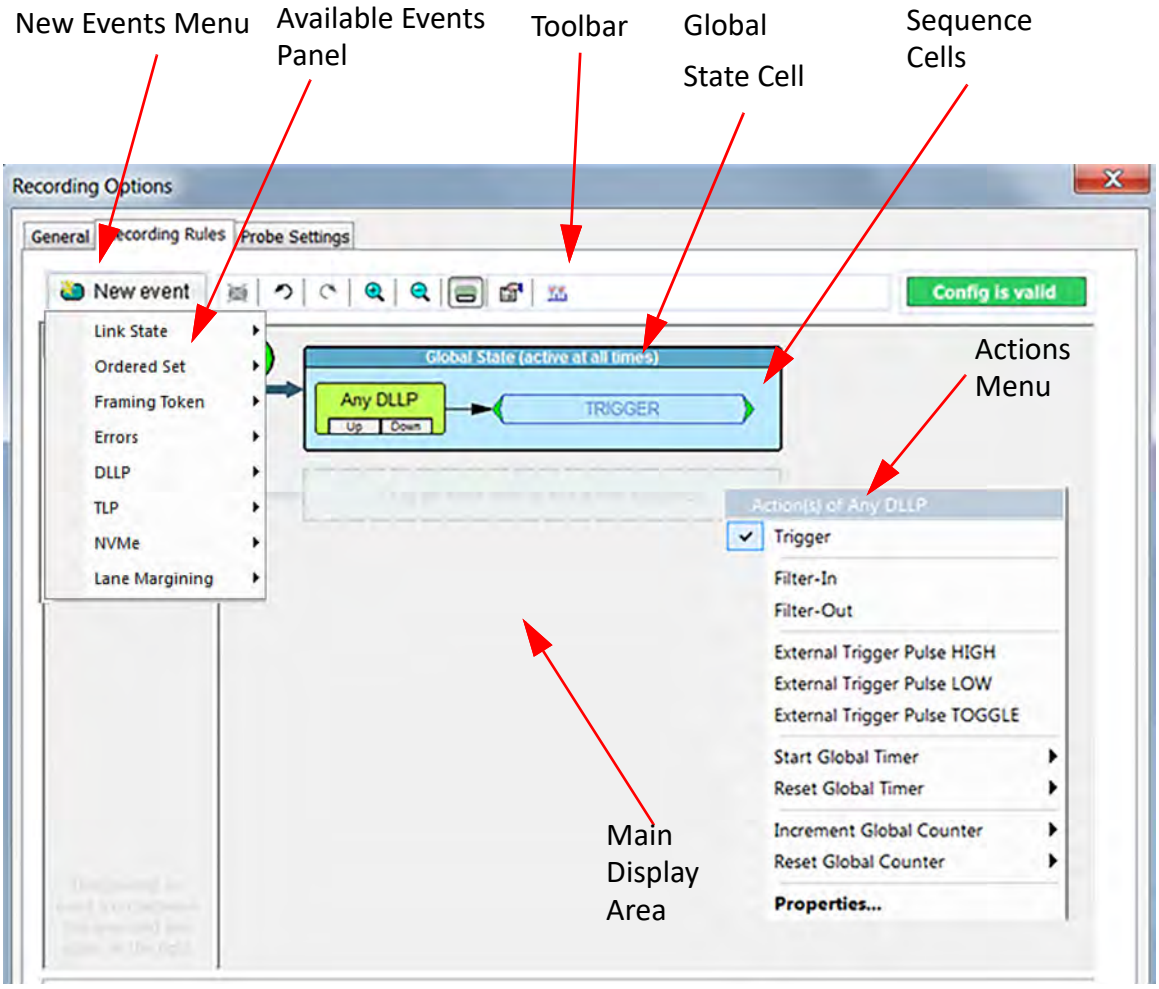


Figure 5.37: Recording Rules Tab

5.19 Navigating Recording Rules

The Recording Rules window has three main areas, the Toolbar, Available Events panel and the Main Display panel (see Figure 5.37 on page 169).

5.19.1 Toolbar

The toolbar contains buttons such as the New Events button for issuing commands, Delete Current Event, Undo, Redo, Zoom in and out, Show/Hide Channels, Properties, and Lane Trigger Configuration.

5.19.2 Available Events Area

The Available Events area is in the left repository panel where you can park buttons that you intend to use in the Main display area. The events in this panel do not affect the recording. You can drag and drop events in the Main Display panel.

5.19.3 Main Display Area

The Main Display area is the right panel where you create trigger and filter conditions. You create conditions by dragging buttons onto the Main display area from the Available Events area. You then create additional conditions by right-clicking a button and selecting options from a pop-up menu. See Creating Recording Rules.

5.19.4 Recording Rules Buttons

The Recording Rules toolbar allows you to create and edit recording rules:



TABLE 5.3: Recording Rules Toolbar Buttons

	New Event. Opens a drop-down menu with a list of events.		Zoom in
	Delete. Delete selected event.		Zoom out
	Undo. Undoes last action.		Show/Hide Channels. Shows/hides the channel buttons.
	Redo. Undoes last Undo command.		Show properties. Opens the Properties dialog for the selected item.
	Lane Trigger Configuration: Sets lane pre-conditions for event categories.		

5.20 Recording Rules Overview

The Recording Rules allows you to specify complex triggering and filtering options. The Summit M5x monitors incoming traffic and looks for specified events. It performs actions like triggering and filtering. Complex options can be created by putting Events in a sequence.

Events are based on Resources (see “Resources” on page 173).

5.20.1 Defining Recording Rules

The Recording Rules page is used to set triggers and filters. To access this page, select **Setup > Recording Options > Recording Rules**.

You can also access the New Event menu by right-clicking in the blue space in the Global State or in the Sequence State (see Figure 5.38).

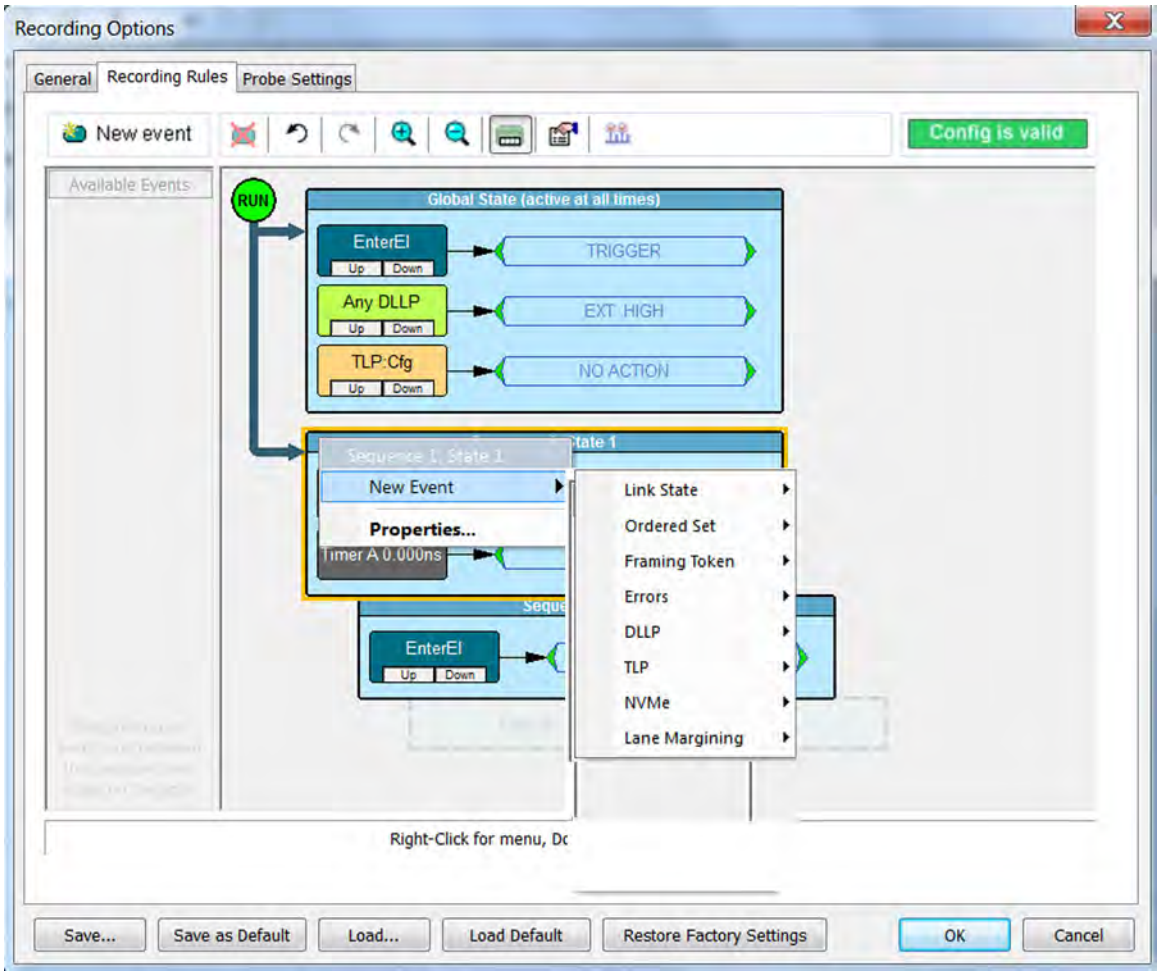


Figure 5.38: Defining New Events

5.20.1.1 Steps to Create a Recording Rule

There are three steps to creating a recording rule:

1. Select events.
2. Place the events in the Global State or Sequence cells.
3. Assign actions to the events.

Note: There are limits to the types of rules that can be created.

1. Click New event and select one or more events from the menu (see Figure 5.39). Selecting an event automatically places it in the Available Events area. This repository area serves as a parking lot where you can place event buttons without them having any effect on the Analyzer.

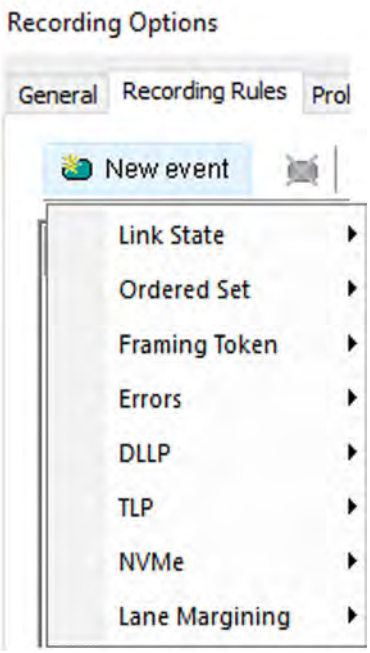
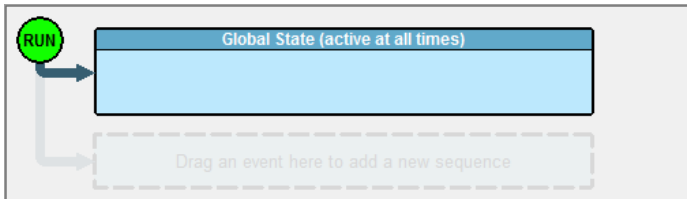


Figure 5.39: New Event Menu

2. Drag the selected events from the Available Events area into either the Global State Cell or the Sequence Cell (see “Recording Rules Overview” on page 170).



Global State Cell

If you want the Analyzer to always search for the event, place it in the cell marked **Global State**.

Sequence Cell

To create an event sequence, place two or more events in the faintly marked cell that reads **Drag an event here to add a new sequence**. At this point, the selected events have no effect because an action has not been assigned.

3. To select a sub-set of your selected event, right-click it and choose **Properties**. A Properties dialog opens that presents additional options. For example, if you open the Properties dialog for Errors, you can set the specific types of errors the Analyzer should look for.

4. Assign an action to the selected events by right-clicking each of the events, selecting **Specify Action** from the pop-up menu, and assigning an action such as **Trigger,**

Filter, or **Count**. Be sure to click the event itself and not the **State** cell that it is sitting in (which produces a different pop-up menu).

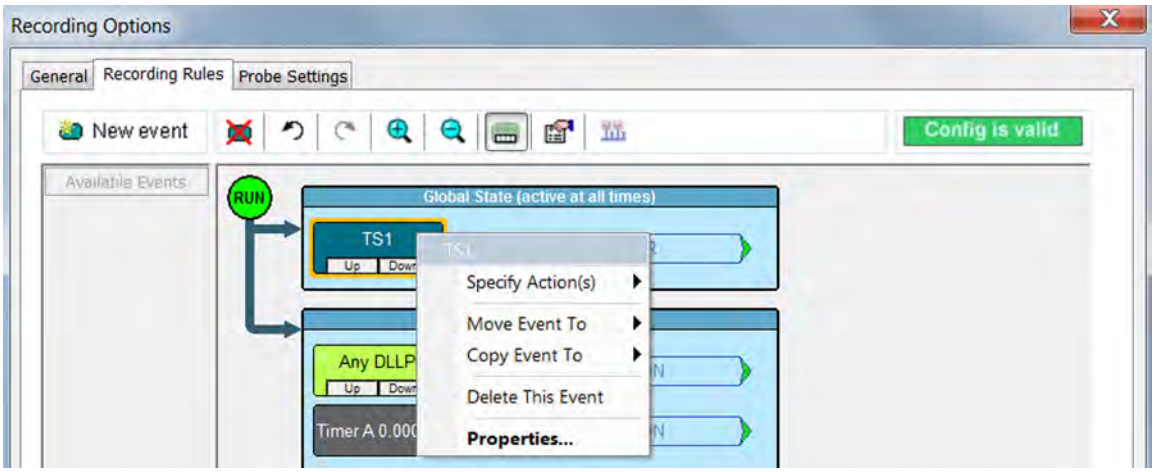


Figure 5.40: Assigning an Action

Note: You can also assign actions to events by double-clicking the event or action and selecting the Actions page when the Properties dialog opens (see "Event Properties Dialog Box Features" on page 186).

Click **OK** to close the dialog. At this point, assuming that the other options in the Recording Options dialog have been set (such as the General page), you can begin the recording by pressing the Start **Recording** button.

5.20.2 Resources

Events in Recording Rules are captured based on the Matching Resources available. There are four types of Matching Resources as follows:

- Basic Matchers (8 each)
- Ordered Set (OS) Matchers (8 each)
- Data Link Layer Packet (DLLP) Matchers (8 each)
- Transaction Layer Packet (TLP) Matchers (8 each)

These Matchers are hardware specific resources that are programmed internally to capture specified events and are not available to the user. Although they can be programmed to capture a wide variety of events you can define a very complex set of events which would need more resources than are available. It that case the Configuration button at the top right of the Recording Options dialog box will show Config is invalid .

If you click on the "Config is Invalid" box a detailed Warning message will pop up. See Figure 5.41 on page 174. In this case, too many basic resource events were defined in the Global State.

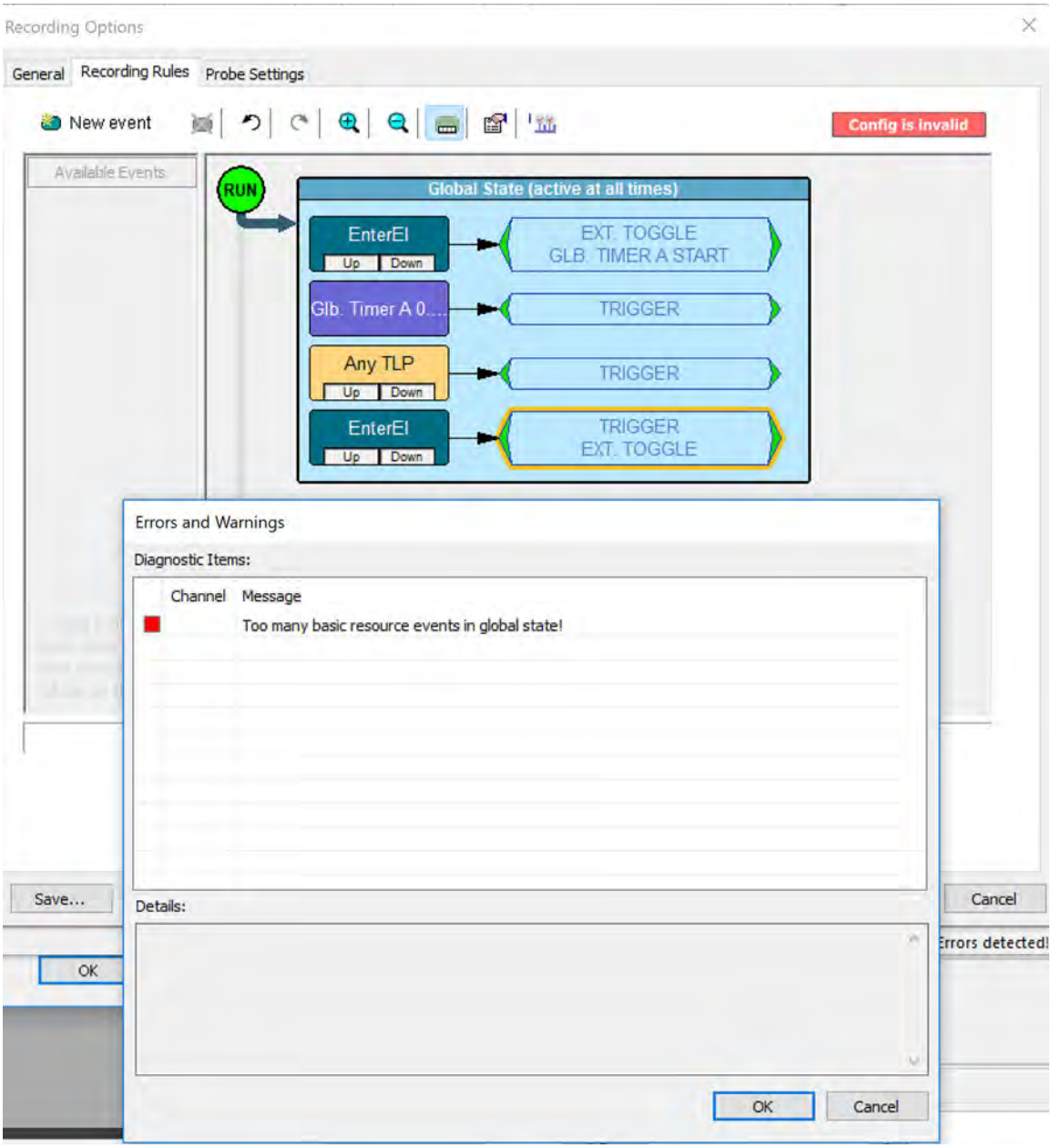


Figure 5.41: Config: Invalid -> Shows Warning Message

If you define a set of events that are missing actions or have inherent contradictions you'll see the Configuration button show Config warnings . If you click on the Configuration button it will produce a list of issues that will need to be corrected before you get the Config is valid .

5.20.2.1 Basic Matcher (x8)

The Basic Matcher generally are used internally to detect the Link State set of Events. See Figure 5.42.

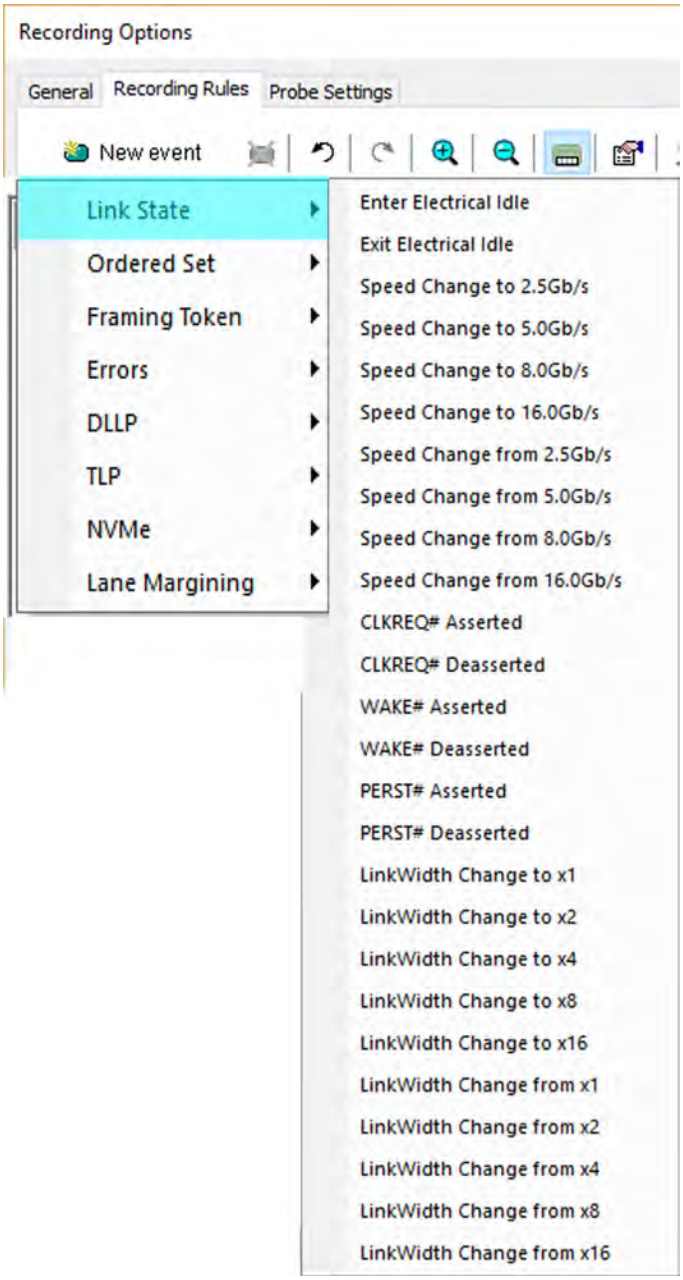


Figure 5.42: Setting Up a Packet Match Resource – Link State

5.20.3 Ordered Set (OS) Matcher (x8)

The Ordered Set Matcher is used internally to detect all of the Ordered Sets (OS). See Figure 5.43.

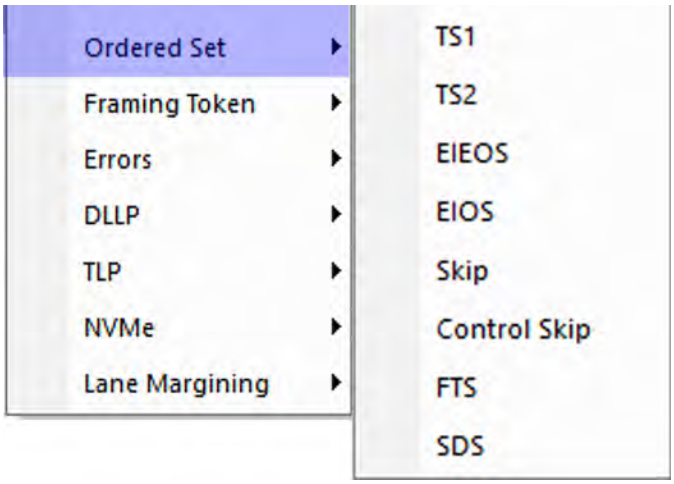


Figure 5.43: List of Ordered Sets (OS)

5.20.3.1 Trigger on Control Skip

You can trigger on Control Skips. See Figure 5.44 through Figure 5.48 on page 178.

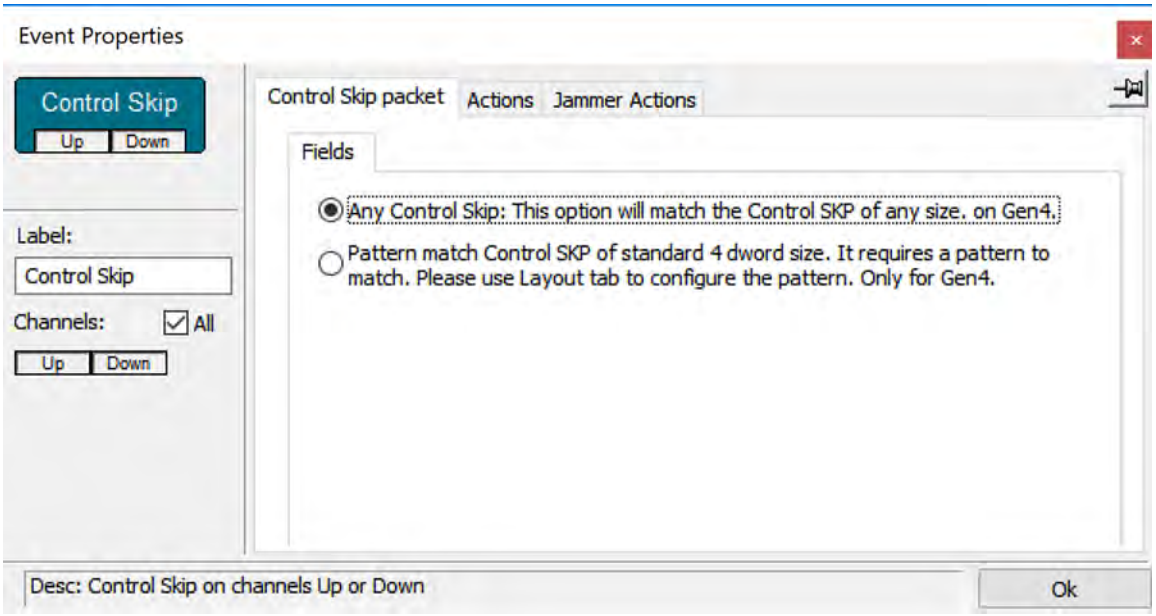


Figure 5.44: Trigger on Control Skips

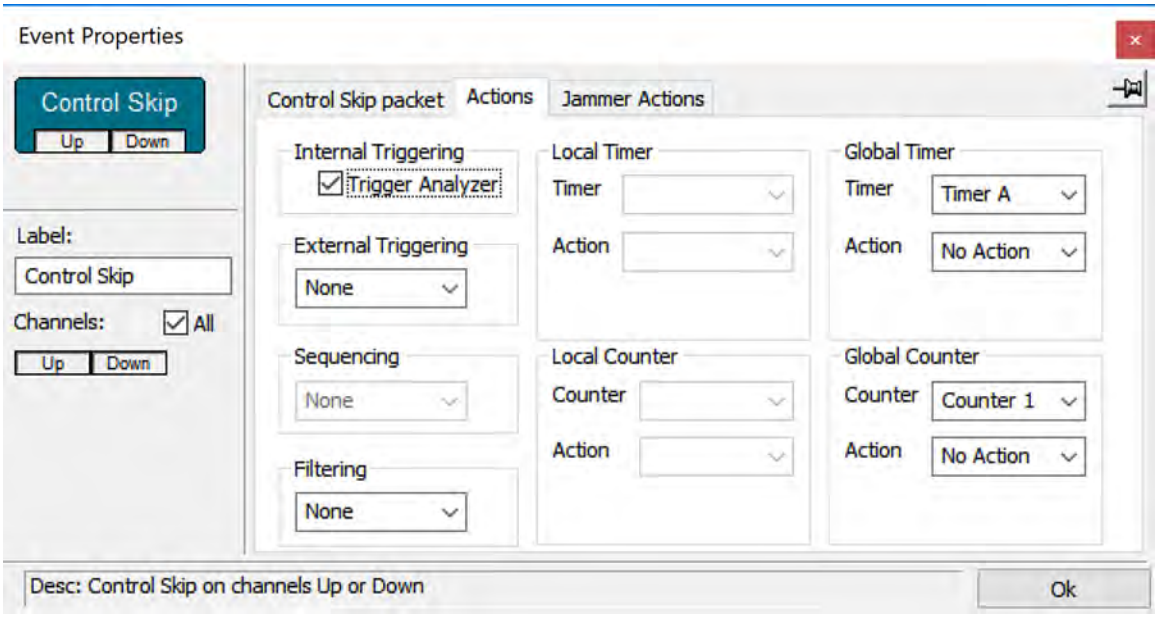


Figure 5.45: Trigger on Control Skip: Action → Trigger Analyzer

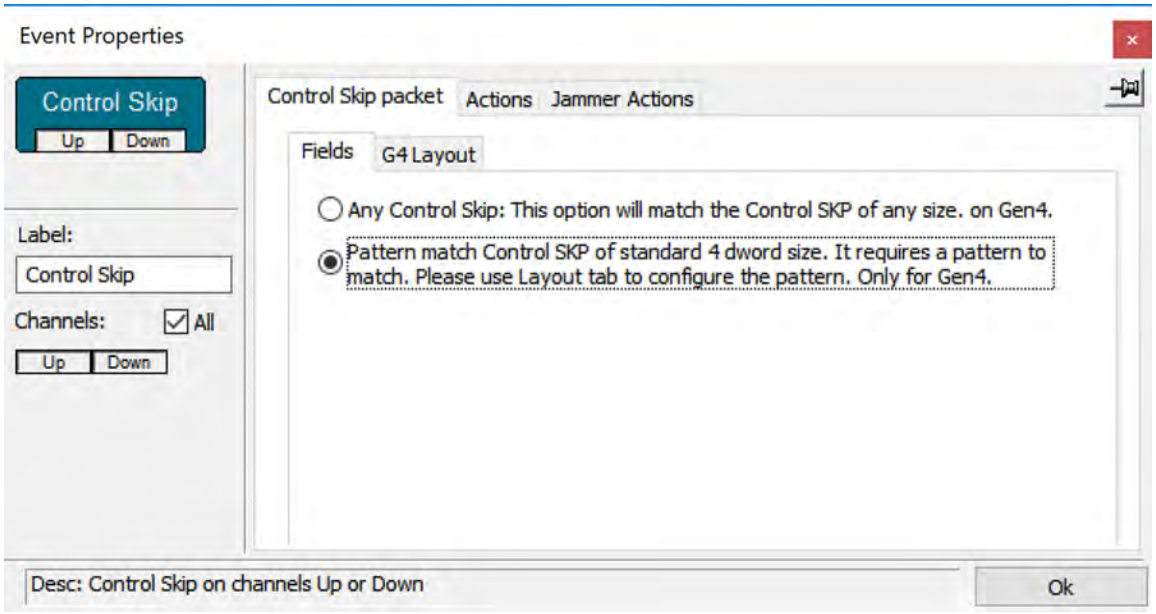


Figure 5.46: Trigger on Control Skip: Pattern Match

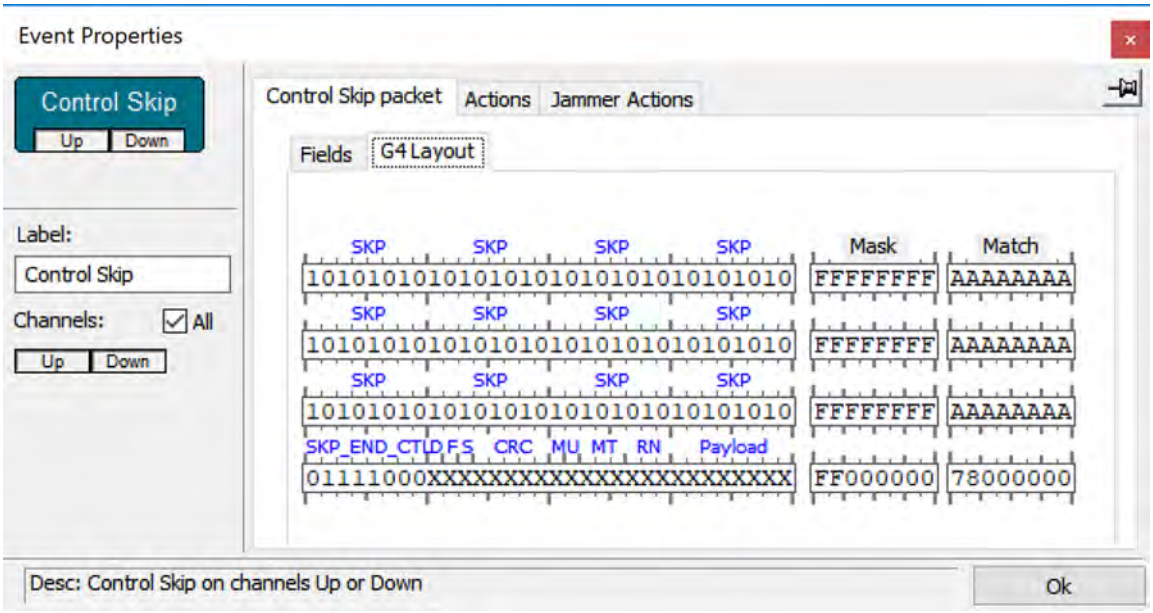


Figure 5.47: Trigger on Control Skip: Pattern Match -> G4 Layout

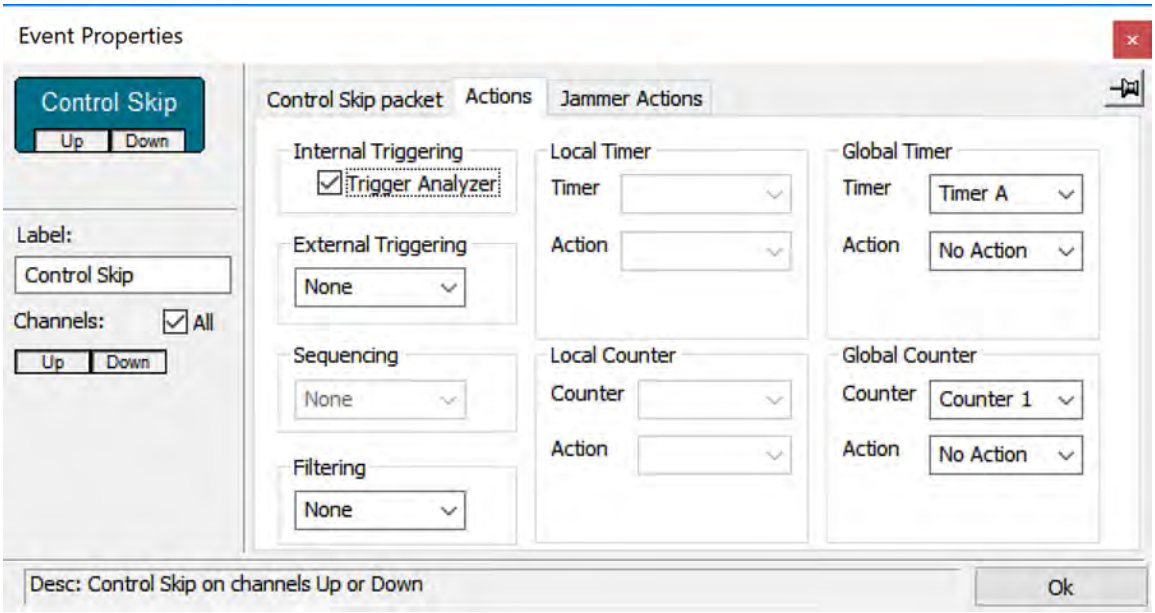


Figure 5.48: Trigger on Control Skip: Trigger Analyzer

5.20.4 Data Link Layer Packets (DLLPs) Matcher (x8)

The Data Link Layer Packets (DLLPs) Resource Matcher is used internally to detect DLLPs. See Figure 5.49.

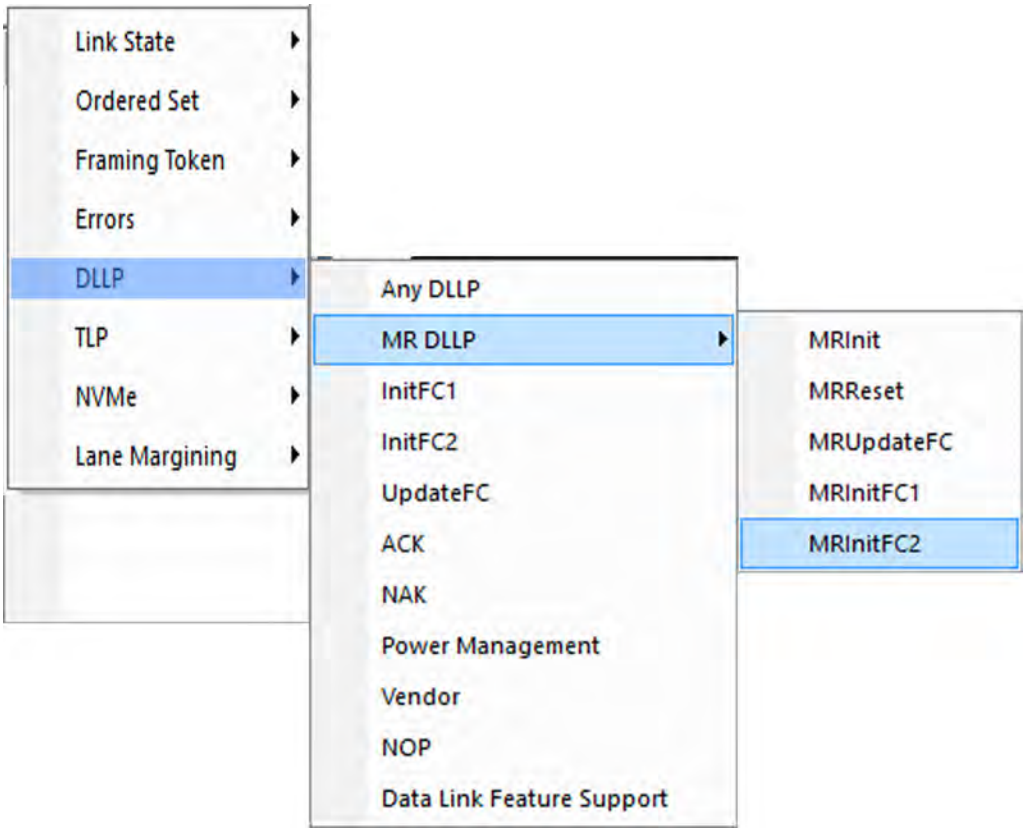


Figure 5.49: List of DLLPs

5.20.5 Transaction Layer Packets (TLPs) Matcher (x8)

The Transaction Layer Packets (TLPs) Resource Matchers are used internally to detect TLPs. See Figure 5.50.

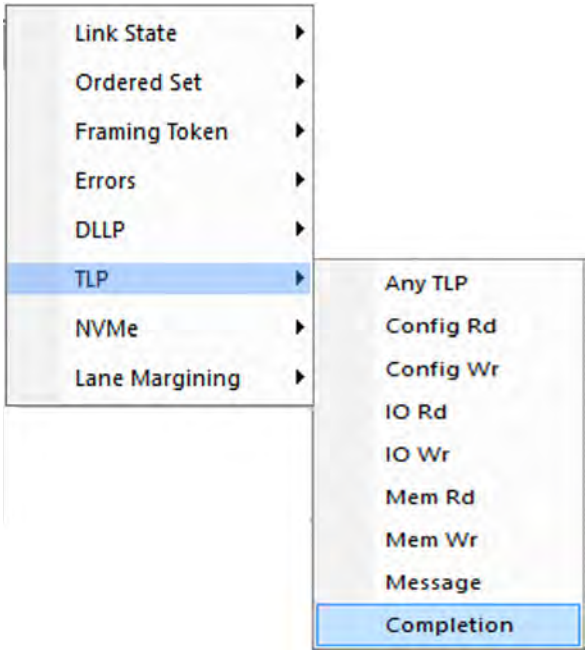


Figure 5.50: Transaction Layer Packets

5.20.6 Global State and Sequence States

The Main Display area in the center of the Recording Rules window has two cells that affect events differently, they are the Global State and Sequence State.



Figure 5.51: Global State Cell and Sequence State Cell

In the Global and Sequence State you can add events by clicking on the New Event button and after the event is in the State you can right-click to Specify Actions, Move, Copy or Delete the event. You can view the Properties dialog to make additional changes to the Property of the event (see Figure 5.51 on page 180). The description of these actions are given in Table 5.5 on page 207.

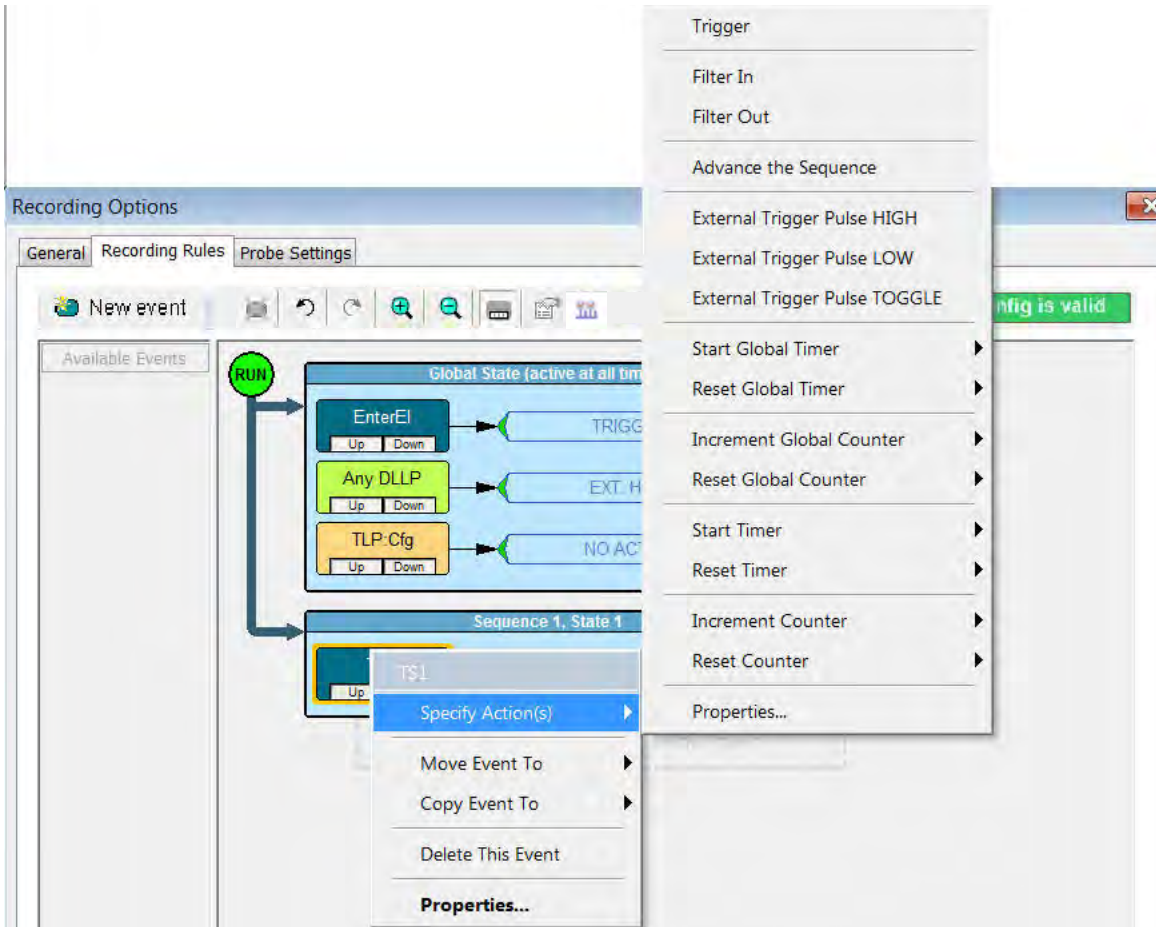


Figure 5.52: Global State Menu

5.20.6.1 Global State

The Global State is active all the time. The Summit T4 analyzers track all the Events and Actions defined in the Global State throughout the recording. In the Global State the Link

State, Ordered Set (except TS1 and TS2), Errors, Counter and the Timer use Basic Resources while TLP, DLLP, TS1 and TS2 use Packet Match Resources. The Global State has two Timers and two Counters.

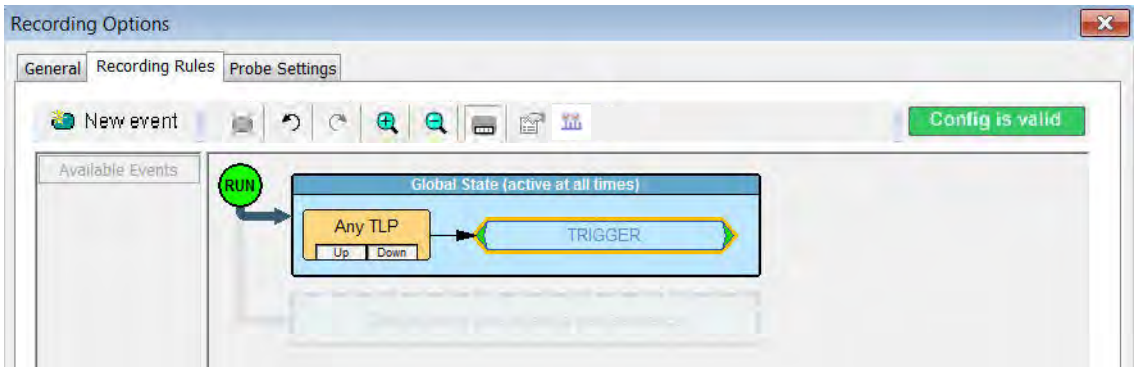


Figure 5.53: Global State

For the Global State there are only 2 Basic Resources for each Channel. Some optimization is done internally to accommodate additional resources. You can keep adding resources to the Global state so long as the **Config is valid** button stays green. If you add a new event which is not valid a window appears with a message prompting **Invalid Recording Rules Configuration** and the **Config is valid** button will turn red (see Figure 5.54 on page 182).

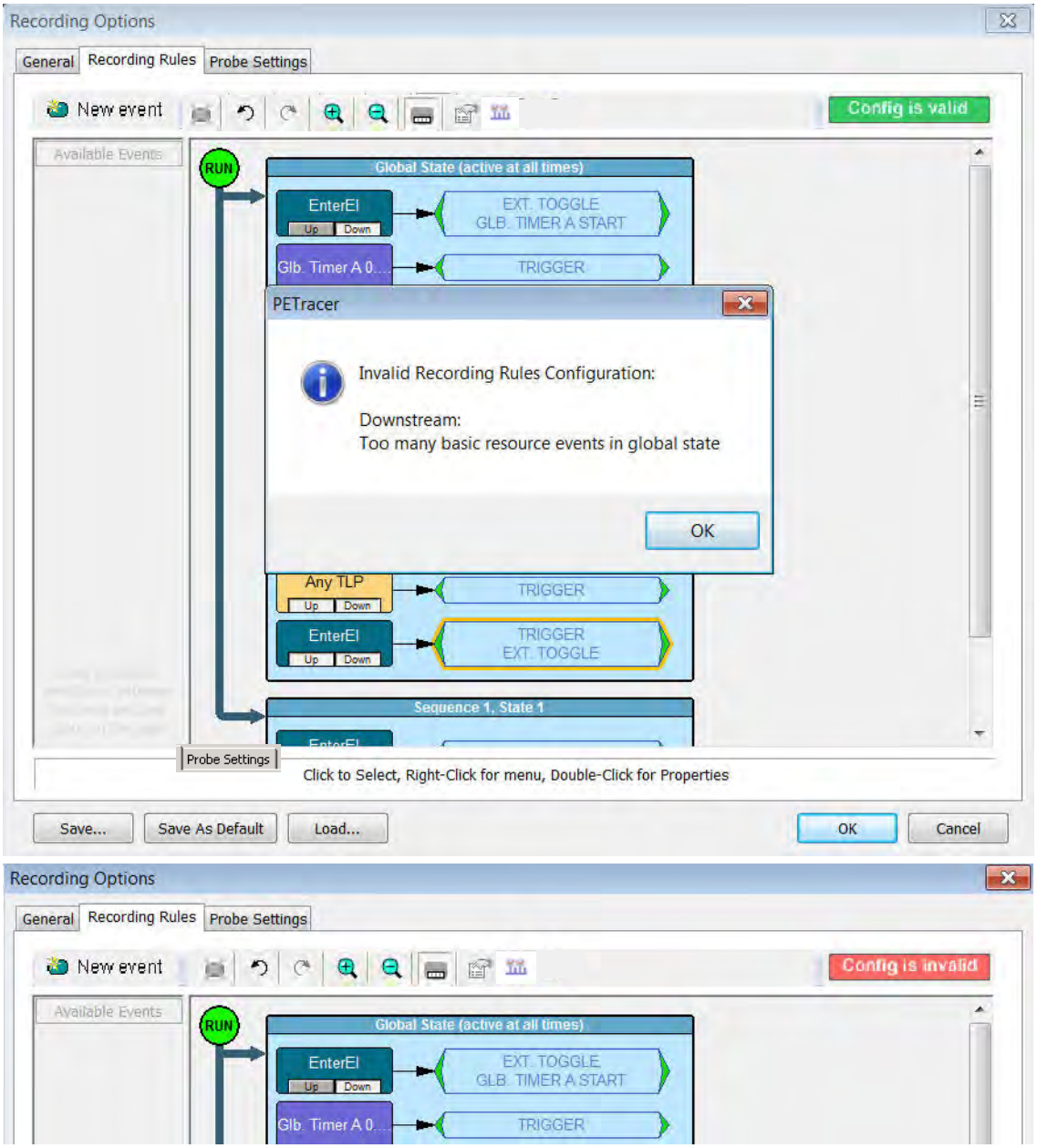


Figure 5.54: Valid and Invalid Recording Rules Configuration Dialogs

5.20.6.2 Sequence State

The cell marked **Drag an event here to add another sequence** is the Sequence State (see Figure 5.55). In the Sequence State you can define a sequence of Events and Actions which the Summit T3-16 Analyzer looks for at pre-determined times. Sequences are chains of events culminating in a trigger or any other action. A sequence which is a separate chain of events can be created with up to 16 states. A state is an event condition with an action within a sequence. Once a Sequence State is added the cell marked will read **Drag an event here to add another state.**

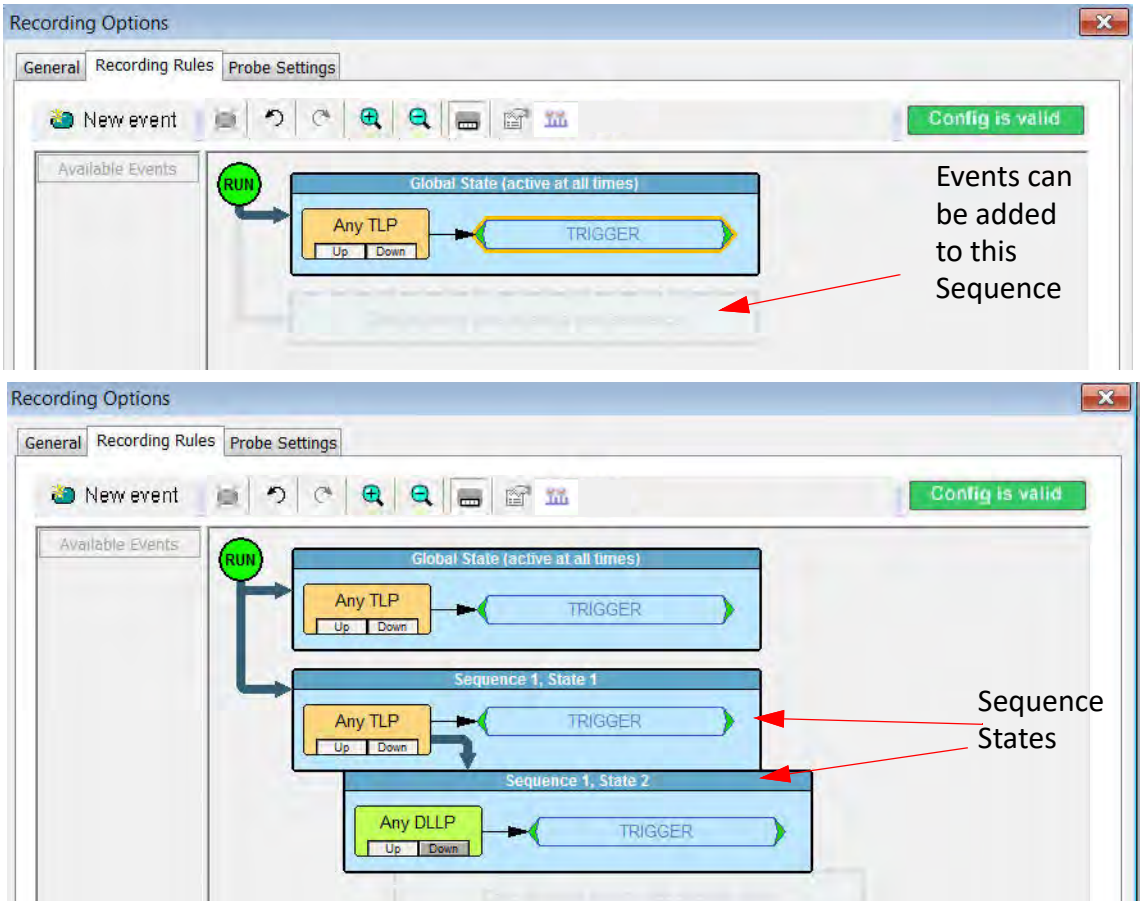


Figure 5.55: Sequence State Events

In the Sequence State the Link State, Ordered Set, Errors, Counter and the Timer use Basic Resources while DLLP and TLP use Packet Match Resources. There are four Timers and four Counters in the Sequence State.

Note: In each Sequence State up to eight Basic Resources and eight Packet Match Resources can be defined.

5.20.7 Recording Rules Events

There are eleven sets of Events that can configured and actions can be set for every Event.

TABLE 5.4: Events and Event Actions (Sheet 1 of 4)

Event	Pre-Defined Event Actions
Link State	
	Enter Electrical Idle
	Exit Electrical Idle
	Speed Change to 2.5Gb/s
	Speed Change to 5.0Gb/s
	Speed Change to 8.0Gb/s

TABLE 5.4: Events and Event Actions (Sheet 2 of 4)

Event	Pre-Defined Event Actions
	Speed Change to 16.0Gb/s
	Speed Change from 2.5Gb/s
	Speed Change from 5.0Gb/s
	Speed Change from 8.0Gb/s
	Speed Change from16.0Gb/s
	CLKREQ# Asserted
	CLKREQ# Deasserted
	WAKE# Asserted
	WAKE# Deasserted
	PERST# Asserted
	PERST# Deasserted
	LinkWidth Change to x1
	LinkWidth Change to x2
	LinkWidth Change to x4
	LinkWidth Change to x8
	LinkWidth Change to x16
	LinkWidth Change from x1
	LinkWidth Change from x2
	LinkWidth Change from x4
	LinkWidth Change from x8
	LinkWidth Change from x16
Ordered Set	
	TS1
	TS2
	EIEOS
	EIOS
	Skip
	Control Skip
	FTS
	SDS
Framing Token	
	EDS
	EDB
Errors	
	Disparity Error

TABLE 5.4: Events and Event Actions (Sheet 3 of 4)

Event	Pre-Defined Event Actions
	Symbol Error
	Block Align Error
DLLP	
	Any DLLP
	MR DLLP (MRInit, MRReset, MRUPdatFC, MRInitFC1, MRInitFC2
	InitFC1
	InitFC2
	UpdateFC
	ACK
	NAK
	Power Management
	Vendor
	NOP
	Data Link Feature Support
TLP	
	Any TLP
	Config Rd
	Config Wr
	IO Rd
	IO Wr
	Mem Rd
	Mem Wr
	Message
	Completion
NVME	
	NVME Register
	ACQ
	AQA
	ASQ
	CAP
	CC
	CQyHDBL
	CSTS

TABLE 5.4: Events and Event Actions (Sheet 4 of 4)

Event	Pre-Defined Event Actions
	INTMC
	INTMS
	NSSR
	Reserved (0x18...0x1B)
	Reserved (0x40...0xEFF)
	Reserved Command Set Specific
	SQyTDBL
	VS
	CMBLOC
	CMBSZ
Lane Margining	
	LM Packets

Note: NVME Command, PQI Command and SCSI command sets are available for selection when Link Width option is set to X4 or lower in the Recording Options.

5.20.8 Properties Dialog Boxes for Events

Properties dialog boxes provide additional settings for Events, States, and Actions in the Recording Rules page. You can access a Properties dialog by double-clicking an **Event, State, Action** or any other object. It allows you to set triggers and filters. For example, to set a trigger on a specific type of error, you open the Properties dialog.

5.20.8.1 Accessing the Properties Dialog

To see the Properties dialog, first create an event button by clicking the **New Event** button and choosing an event from the menu. Open the Event Properties dialog by doing one of the following:

- Double-click an event.
- Right-click an event and select Properties from the pop-up menu.
- Click the Properties button on the toolbar.

5.20.8.2 Event Properties Dialog Box Features

The following features are displayed in the any Event Properties dialog box (see Figure 5.56 on page 187).

Event Icon Preview

This icon shows you which event properties you are editing. The Icon Preview looks exactly like the icon in the Main Display area.

Icon Label

A text box for labeling the button. Whatever you type here appears on the button.

Channels

These controls allow you to select the channel(s) that the Analyzer should search when it is looking for the event.

Pin Button

The Pin Button on the top right corner of the dialog allows you to **pin** the Properties dialog to the application so that it does not go away when another object appears such as an event, state or action.

Description String

This area contains a textual description of the event.

Event-specific Settings

The largest part of the Event Properties dialog. The settings in this area vary for different events. Some events do not have any additional settings. After selecting the options you want click on the “OK” button.

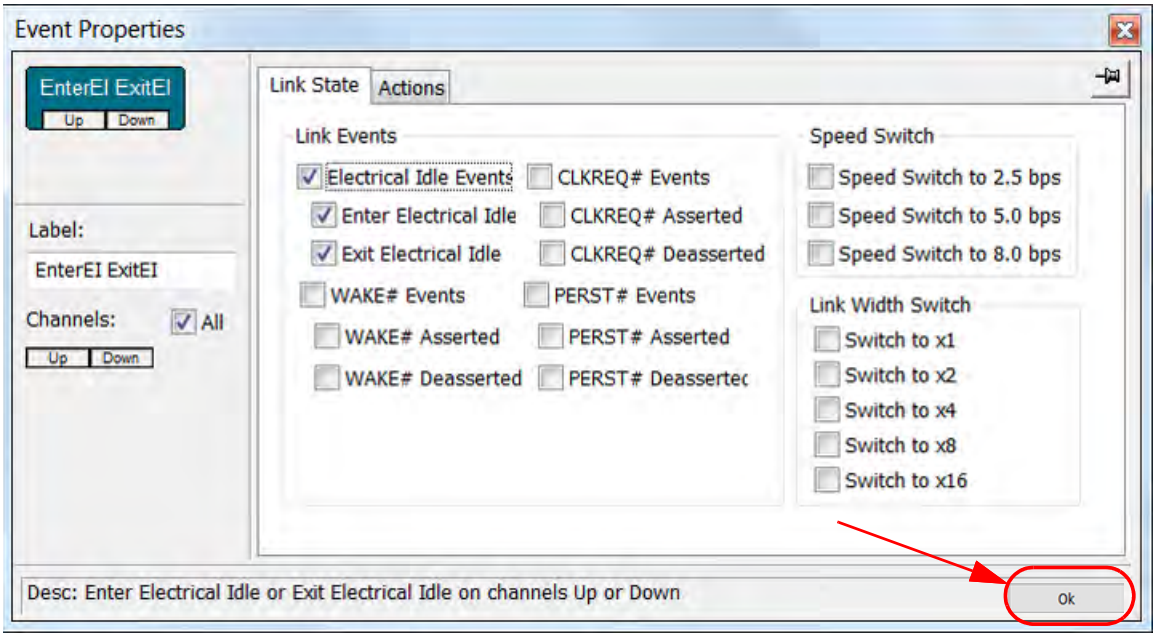


Figure 5.56: Properties Dialog Box

5.20.8.3 Link State Dialog

The Link Properties dialog lets you select the link state. In the case shown below, PERST# events are the Link States selected. See Figure 5.57. After selecting the options you want click on the “OK” button.

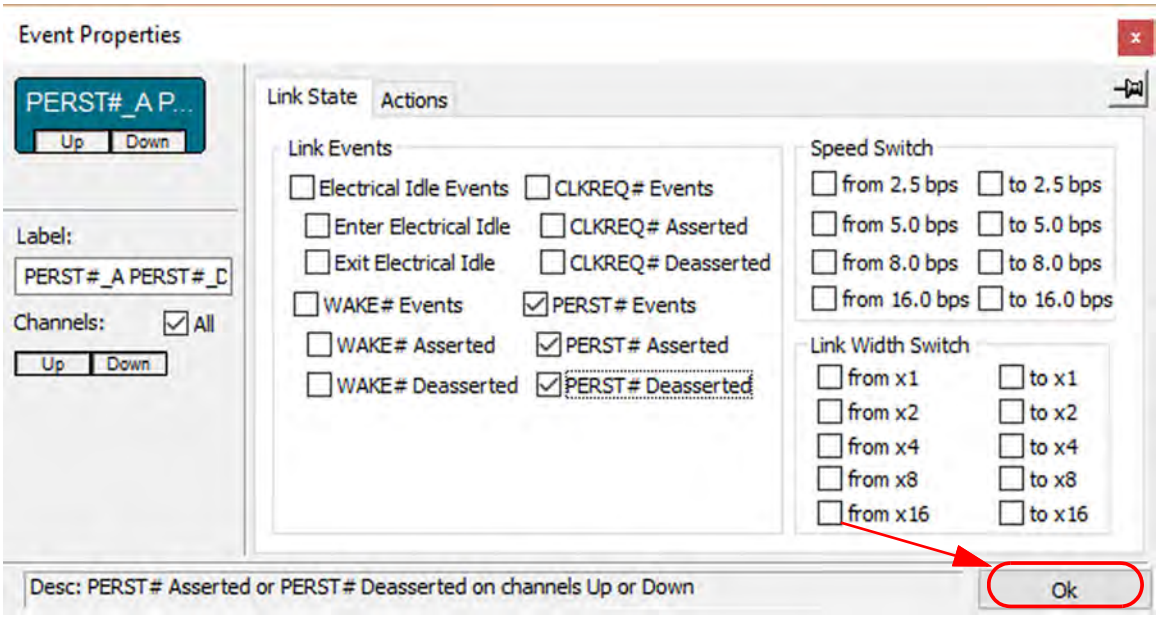


Figure 5.57: Link State Properties Dialog: PERST#

Link State Actions

In this case, the Link State Action to be taken would be to trigger the analyzer. See Figure 5.58. After selecting the options you want click on the “OK” button.

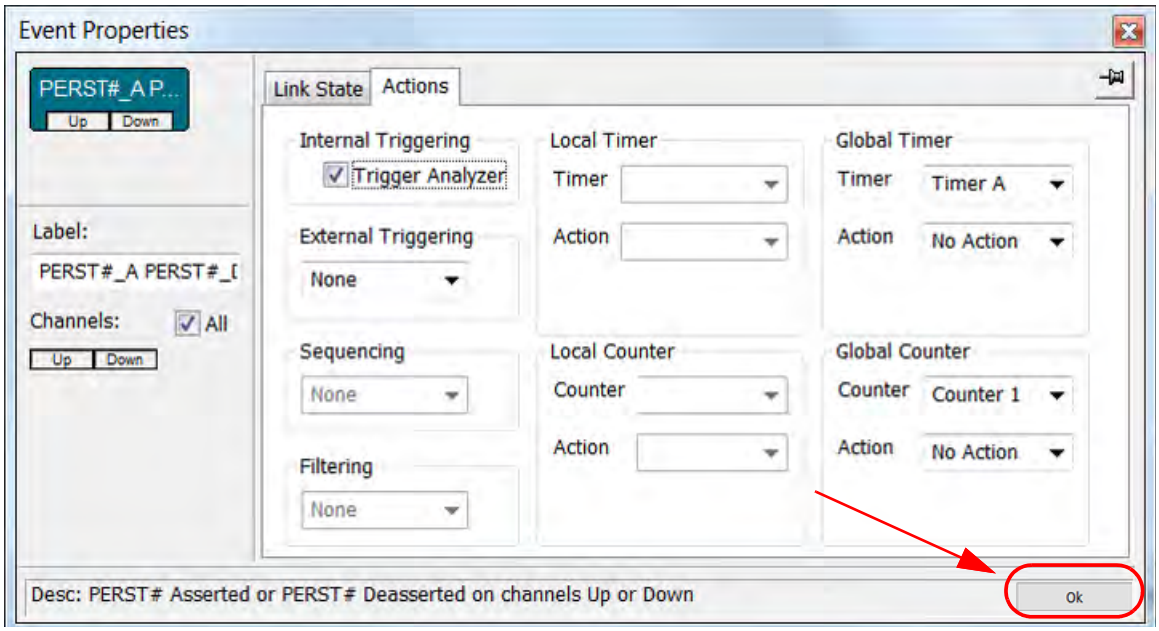


Figure 5.58: Event Properties: Link State Actions: Trigger Analyzer

Global State: CLKREQ# or PERST# Triggers

You could have either a PERST# or CLKREQ# event trigger the analyzer by applying those two conditions to the Global Settings. See Figure 5.59.

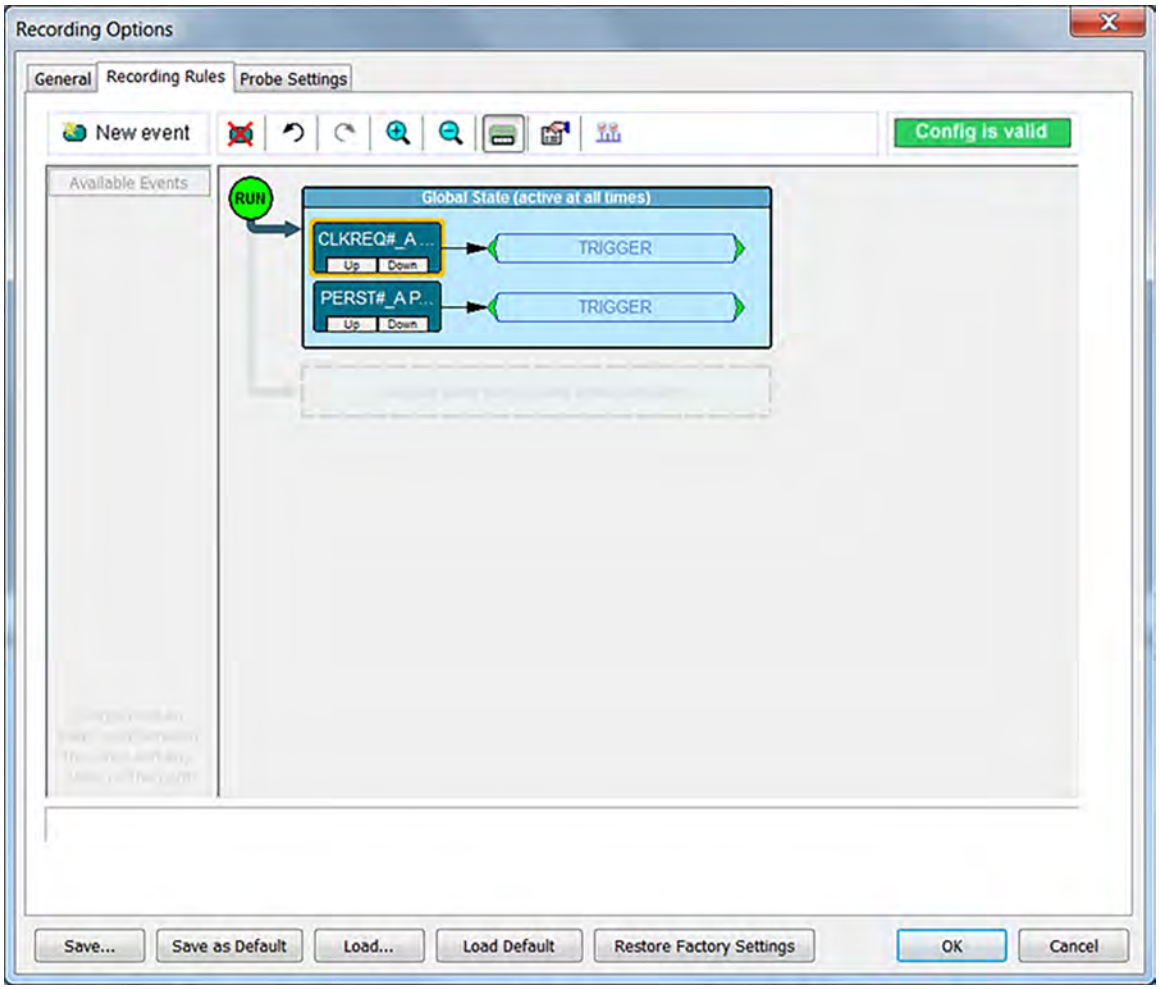


Figure 5.59: Global State: CLKREQ# or PERST# Triggers Analyzer

5.20.8.4 Ordered Sets

A typical Ordered Set Event would be a TS1 packet with the following fields:

- Link Number: Any or PAD
- Lane Number: Any, PAD or Use Lane Trigger
- N_FTS: Any
- Data Rate: Any, G1, G2, G3 or G4
- Atnms Change: Any, Set or Cleared
- Speed Change: Any, Set or Cleared
- Hot Reset: Any, Assert or De-Assert
- Disable Link: Any, Assert or De-Assert
- Loopback: Any, Assert or De-Assert
- Disable Scramble: Any, Assert or De-Assert
- Completion Received: Any, Assert or De-Assert
- Identifiers (6-15): Any, TS1(4Ah) or Custom

See Figure 5.60.

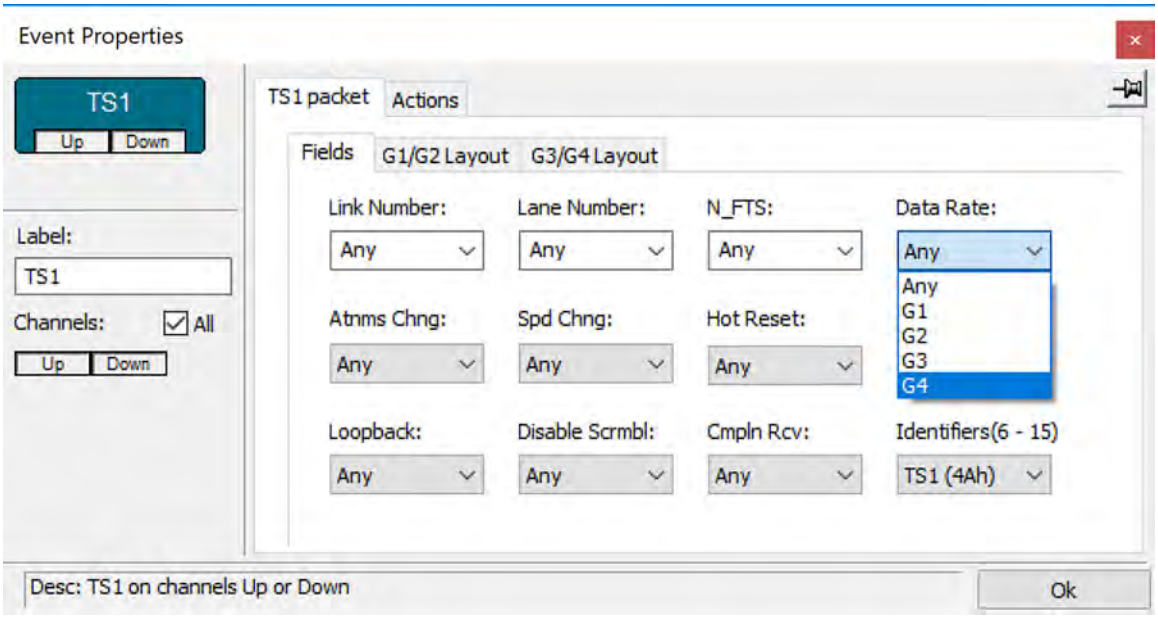


Figure 5.60: Typical Ordered Set: TS1 Event Fields

For G1/G2 Layout the options are shown in Figure 5.61 on page 191.

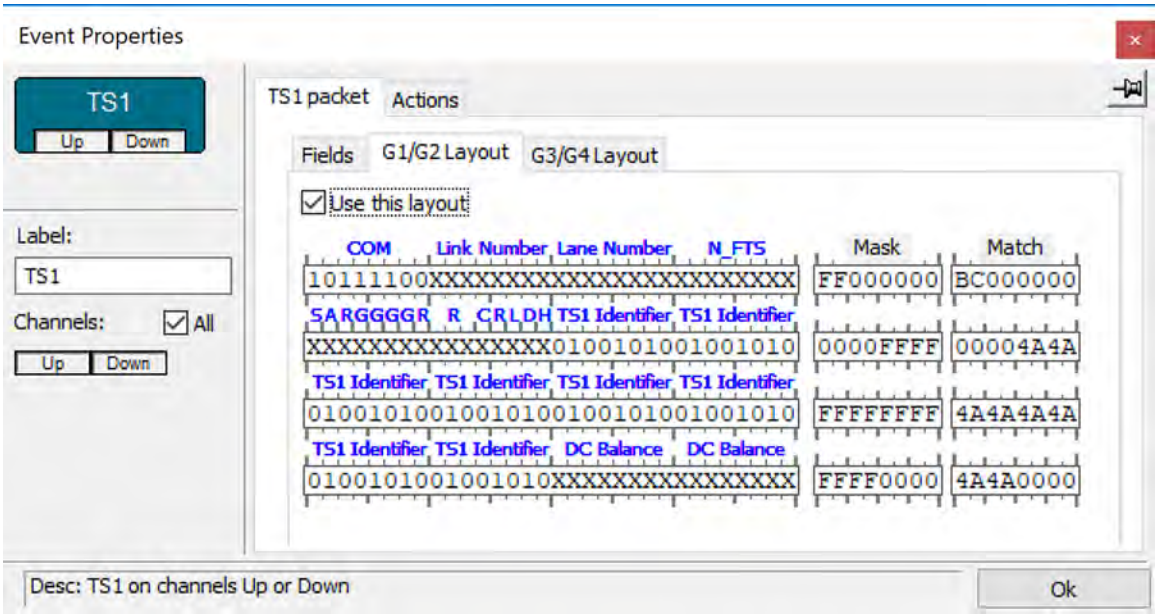


Figure 5.61: Ordered Set: TS1 -> G1/G2 Layout Options

For G3/G4 Layout the options are shown in Figure 5.62.

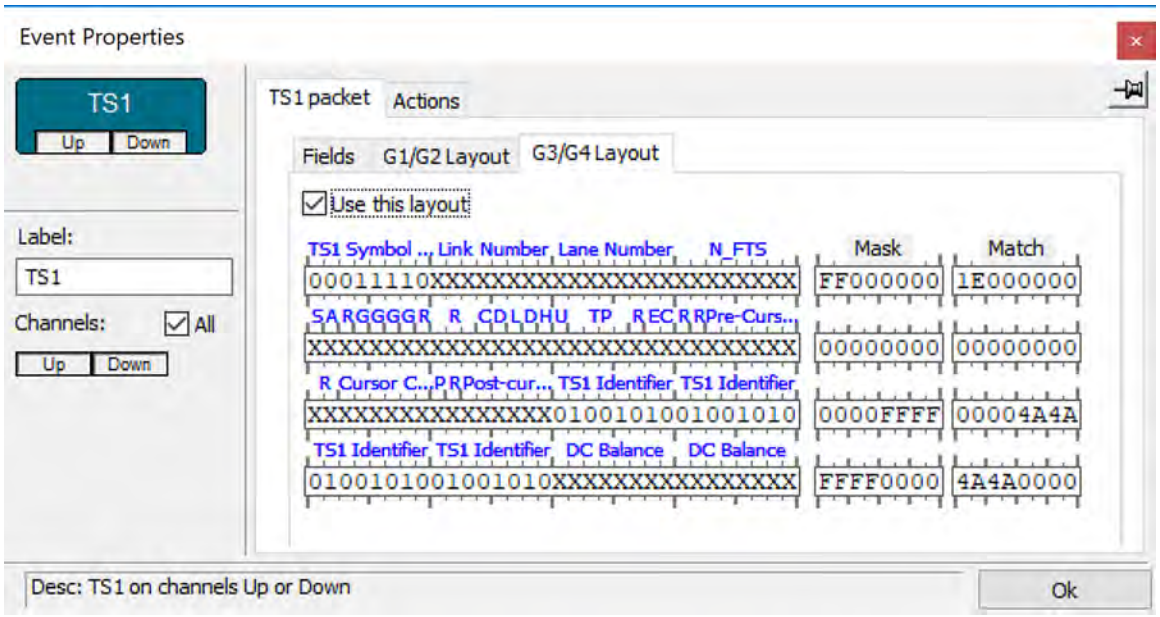


Figure 5.62: Ordered Set: TS1 -> G3/G4 Layout Options

TS1 Actions are shown in Figure 5.63 on page 192.

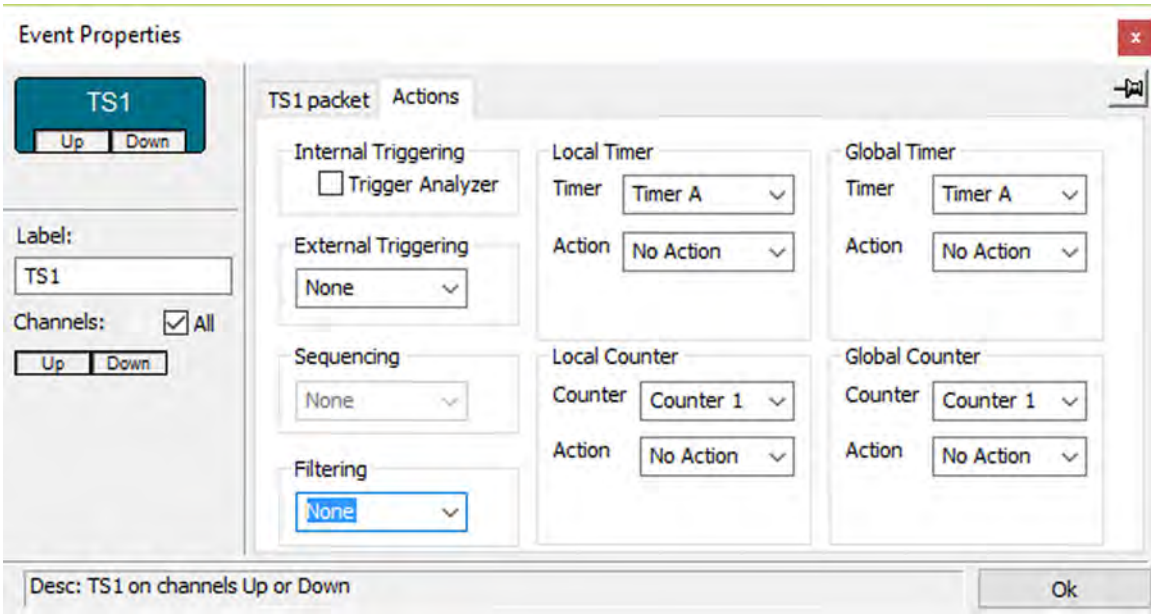


Figure 5.63: Ordered Sets: TS1 -> Actions

5.20.8.5 Framing Token

A Framing Token can be selected as shown in Figure 5.64.

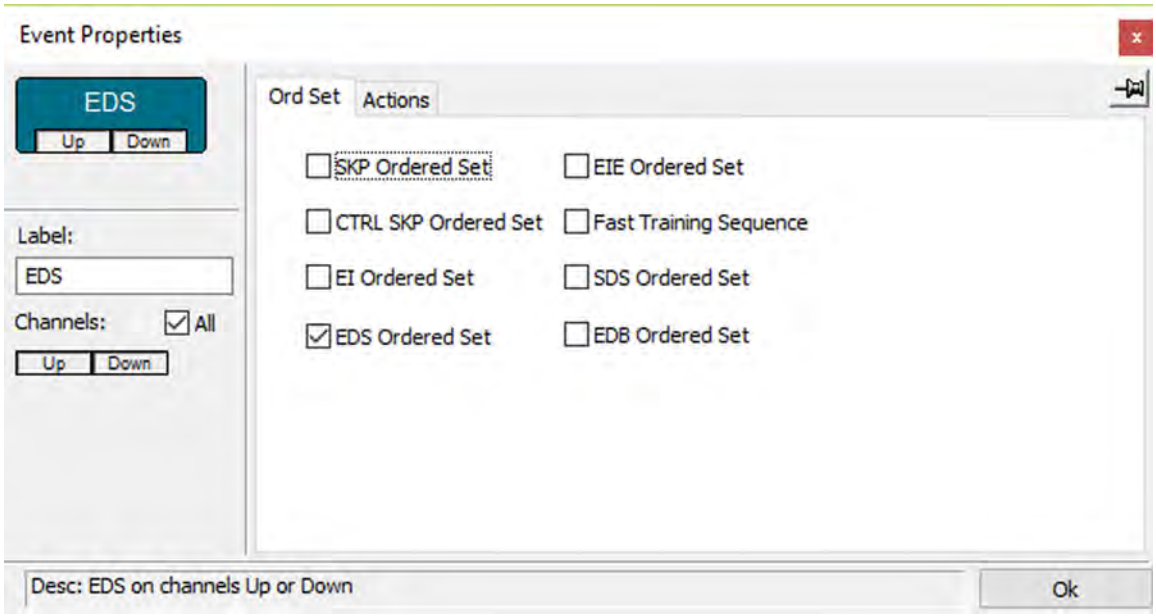


Figure 5.64: Framing Token: Event

The Framing Token Actions are shown below. See Figure 5.65 on page 194.

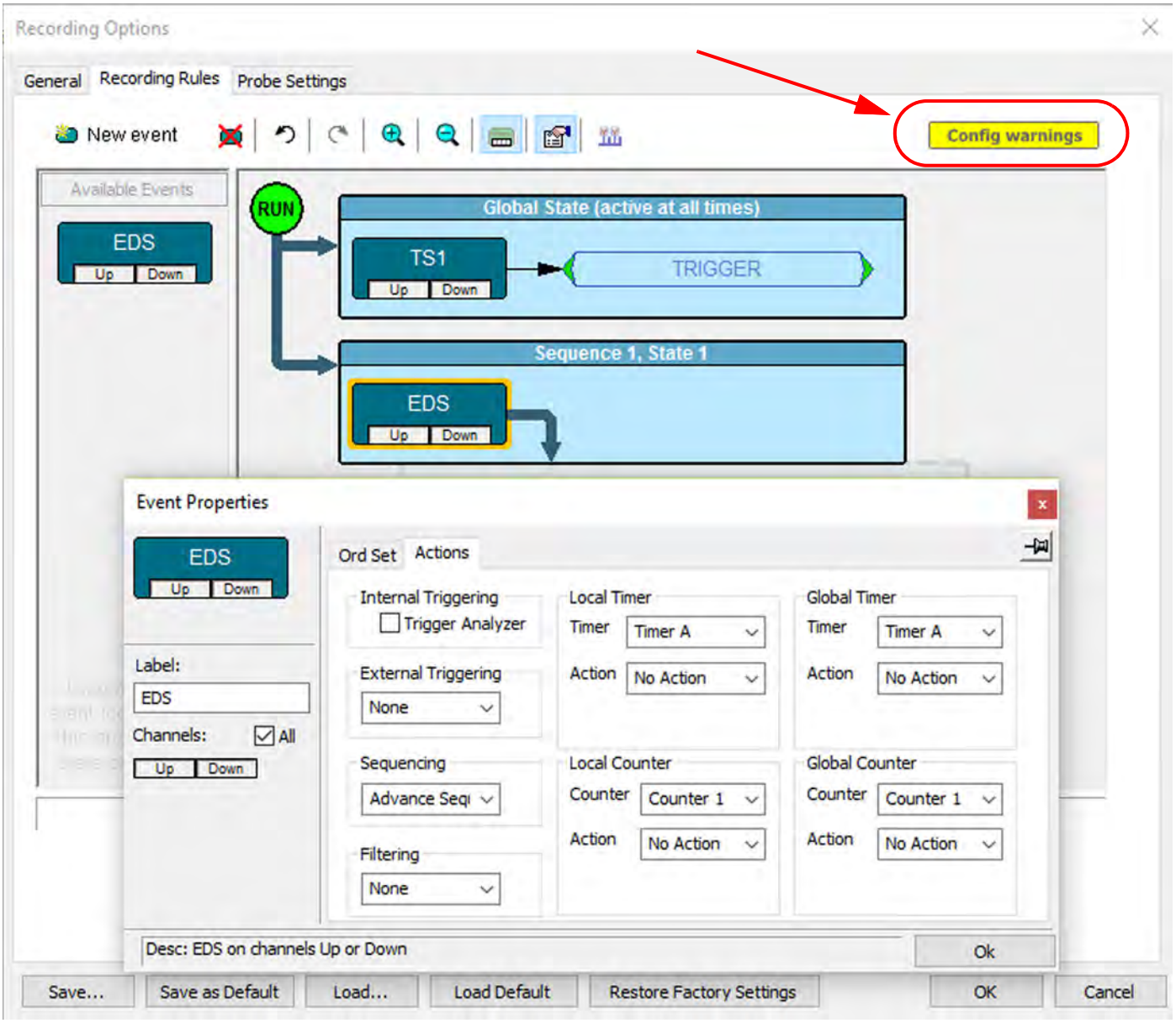


Figure 5.65: Framing Token: Actions

In this example the Advance Sequence was selected but no subsequent state was defined, so the Configuration button is showing: Config Warning. If you click on the Config Warning button a message dialog pops up, telling you what the problem is. See Figure 5.66 on page 195.

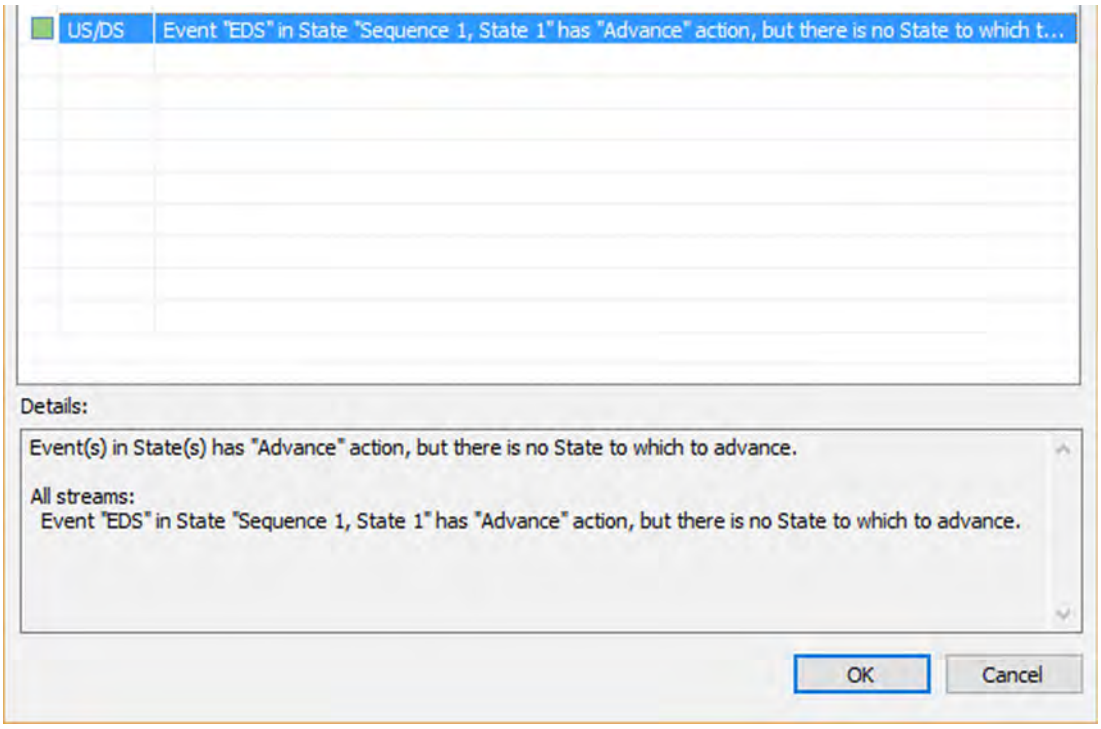


Figure 5.66: Configuration Warning Dialog

If you add another state, the Configuration will be valid. See Figure 5.67 on page 196.

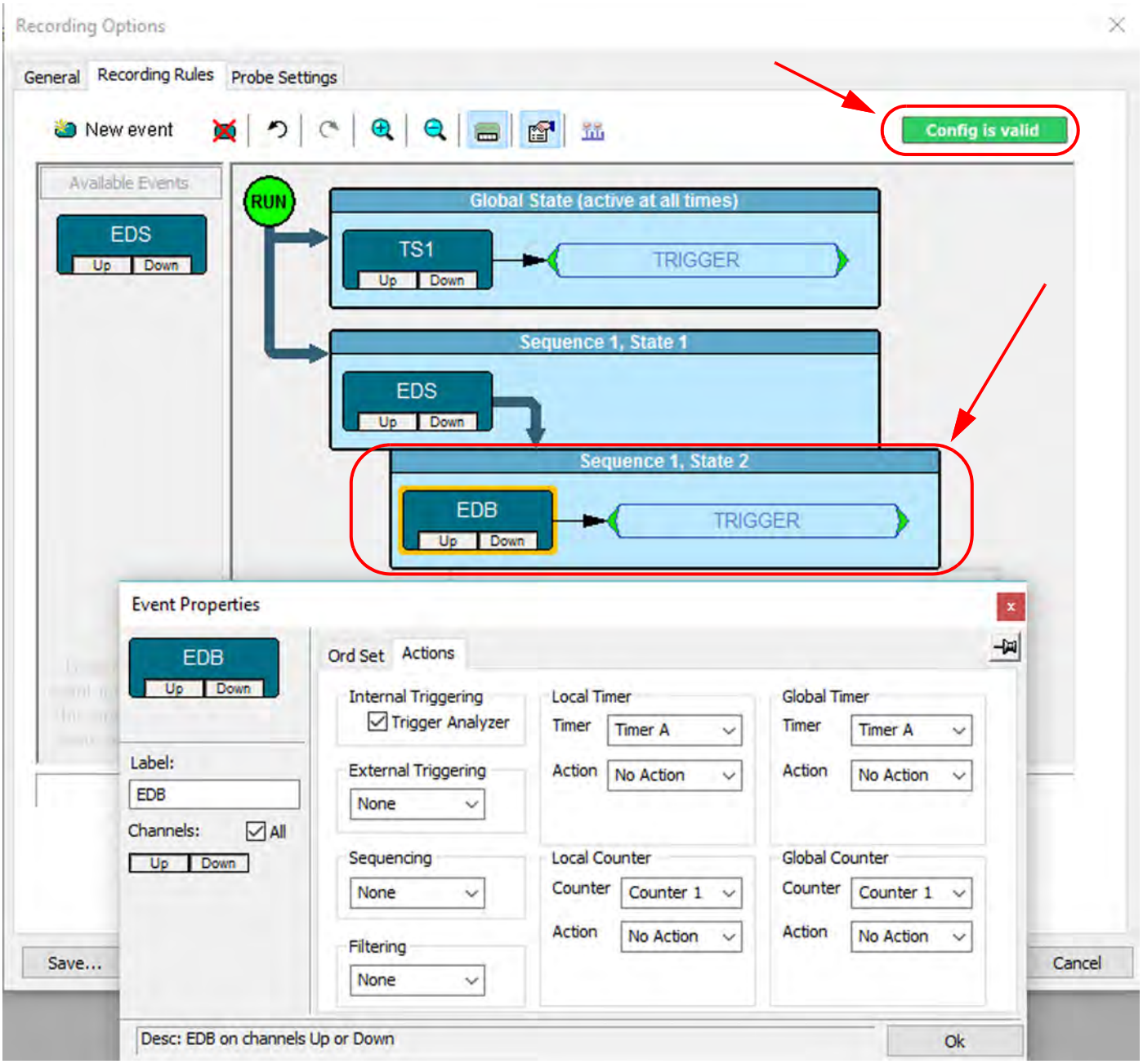


Figure 5.67: Add a State to get Valid Configuration

5.20.8.6 Error Properties Dialog

The Error Properties dialog lets you select specific error types for performing an action. There are three types of Errors:

- Disparity
- Symbol
- Block Align

Each Error type has it's own Event block and similar Actions that can be taken. See Figure 5.68.

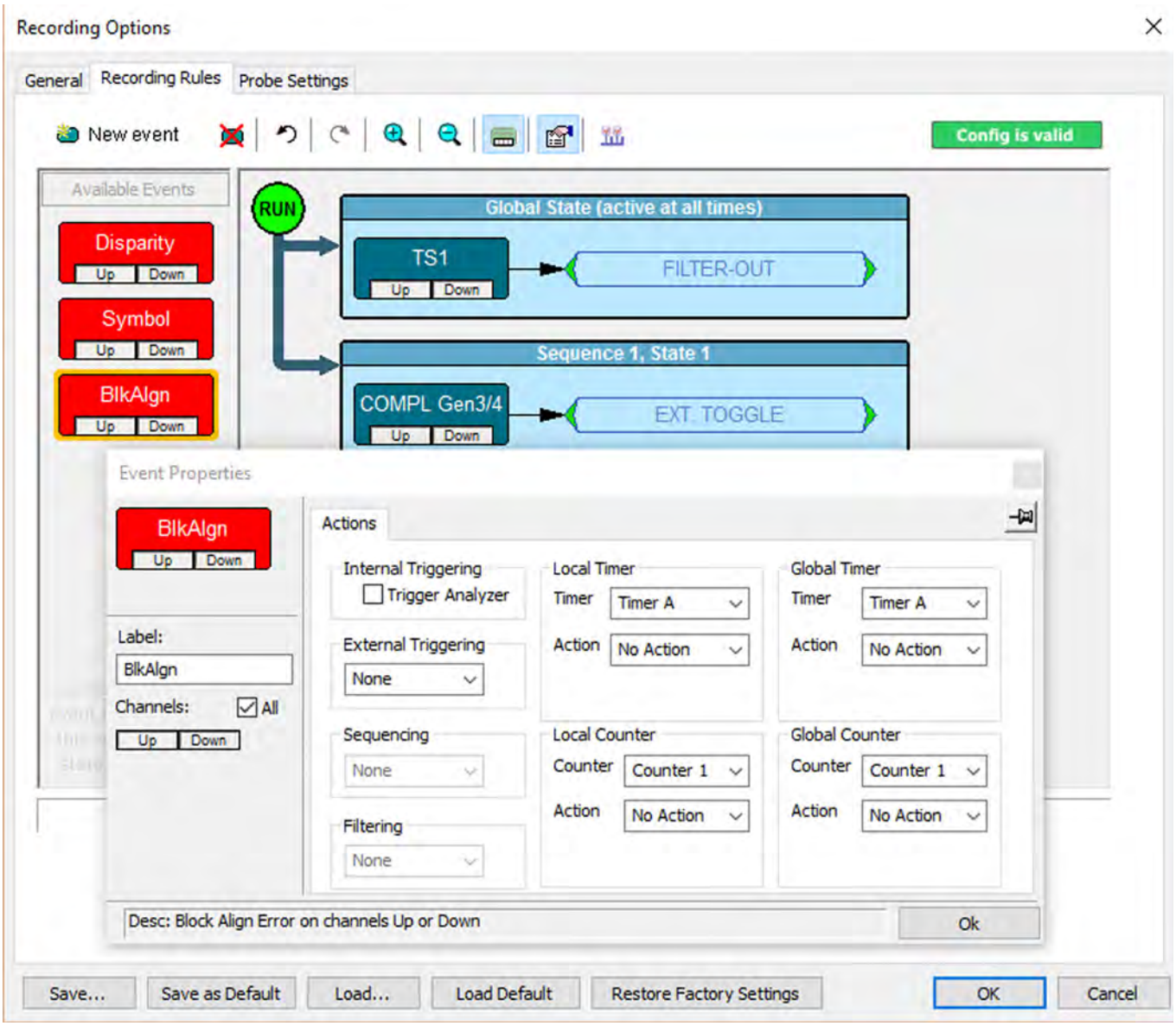


Figure 5.68: Error Events: Actions Dialog

5.20.8.7 DLLP Packet Properties Dialog

The DLLP Packet Properties dialog allows you to specify any DLLP field as shown below. After selecting the options you want click on the “OK” button. See Figure 5.69.

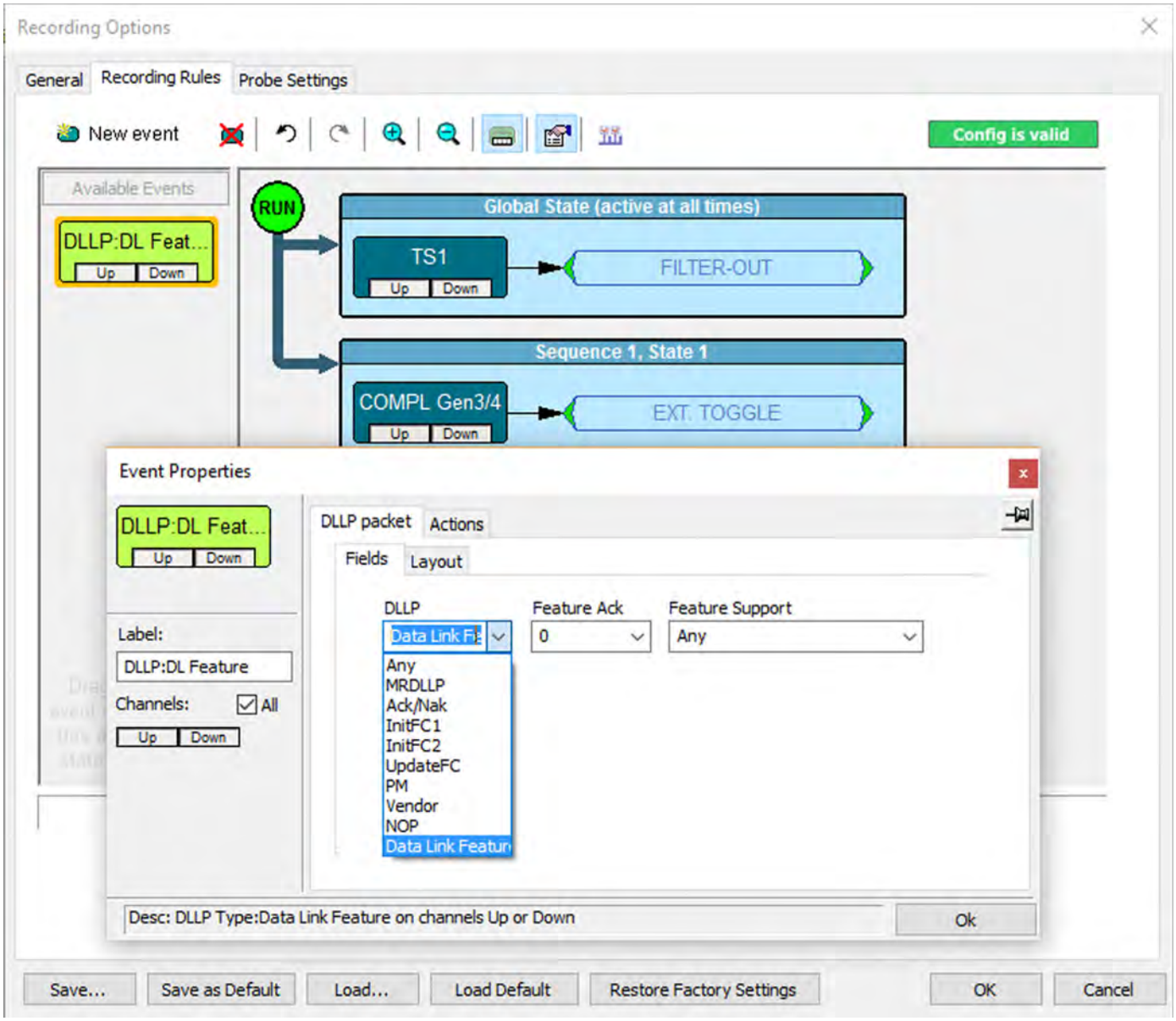


Figure 5.69: DLLP Packet Properties Dialog

The Layout tab of the DLLP Packet Properties dialog allows you to change the pattern and customize it by defining each specific bit as shown in the figure below. After selecting the options you want click on the “OK” button.

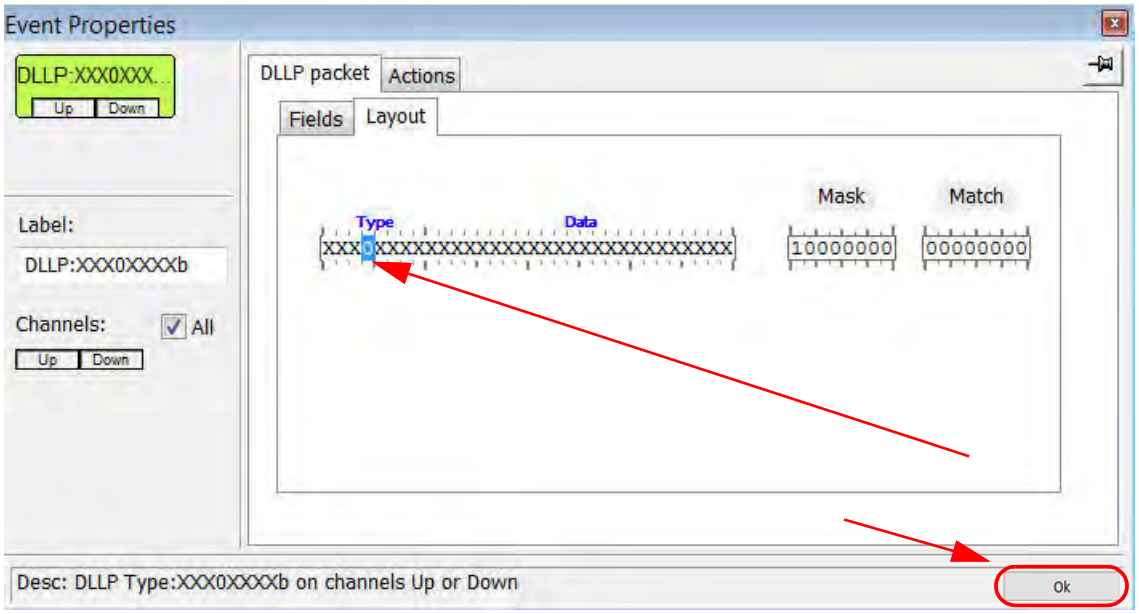


Figure 5.70: DLLP Packet Properties Dialog

Then you can choose the Action you want to occur after the Event is captured. See

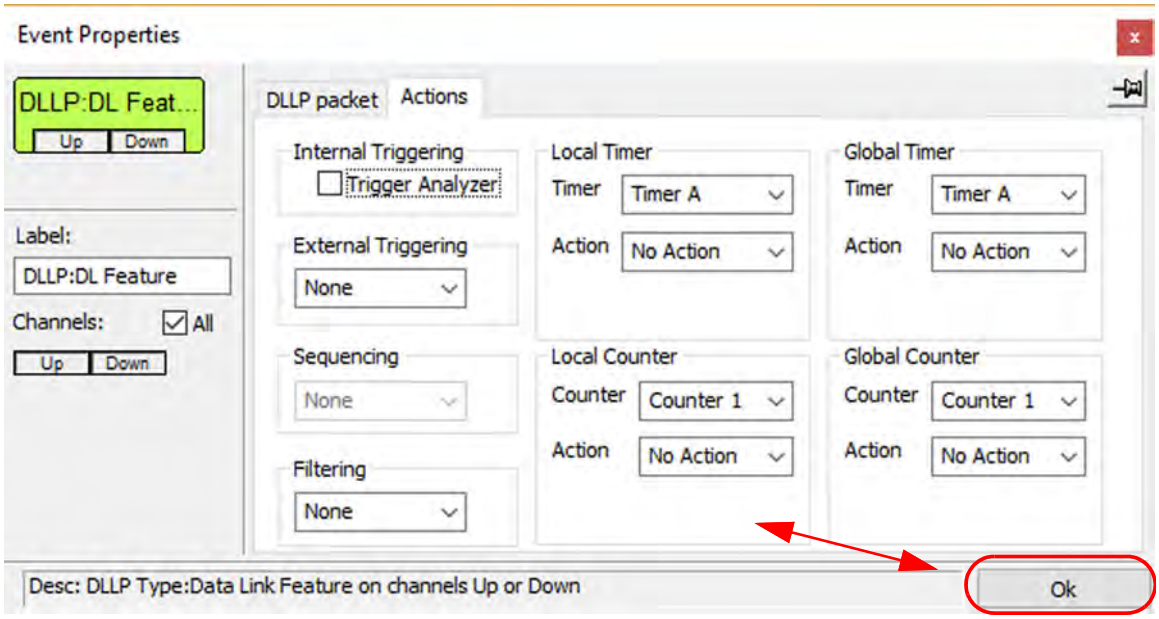


Figure 5.71: DLP Packet: Actions Available

5.20.8.8 TLP Header Properties Dialog

The TLP Header Properties dialog enables you to set the TLP Header Fields and Layout, TLP Prefixes and Actions. You can manually change the Requester/Completer ID. After selecting the options you want click on the “OK” button.

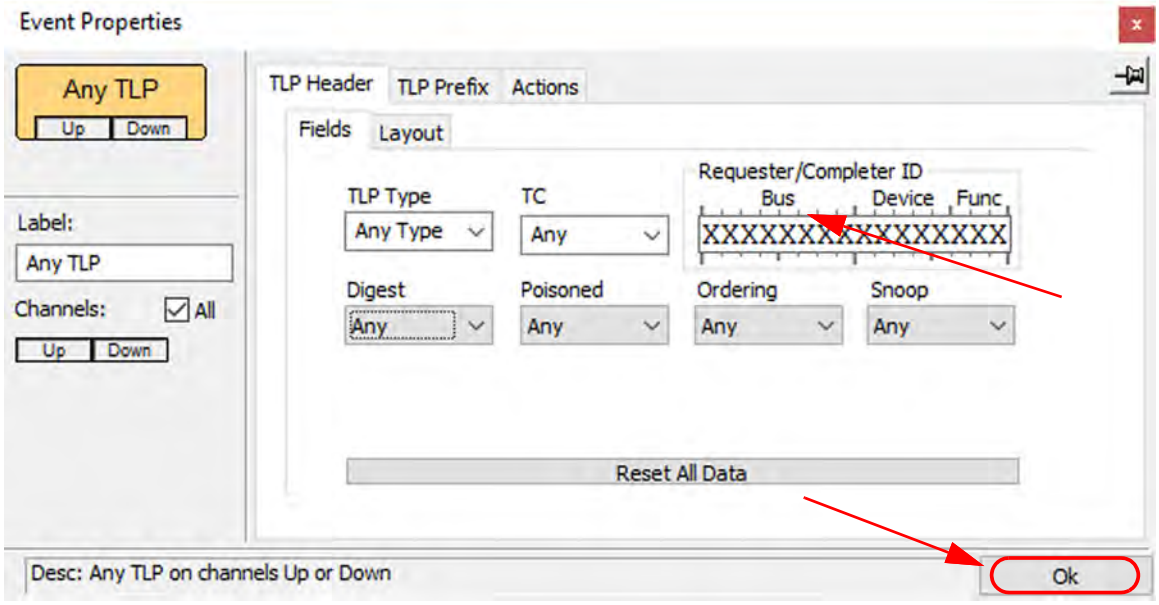


Figure 5.72: TLP Header Properties Dialog

5.20.8.9 TLP Prefix Properties Dialog

The Layout tab of the TLP Prefix Packet Properties dialog allows you to change the pattern and customize it by defining each specific bit as shown in the figure below. After selecting the options you want click on the “OK” button.

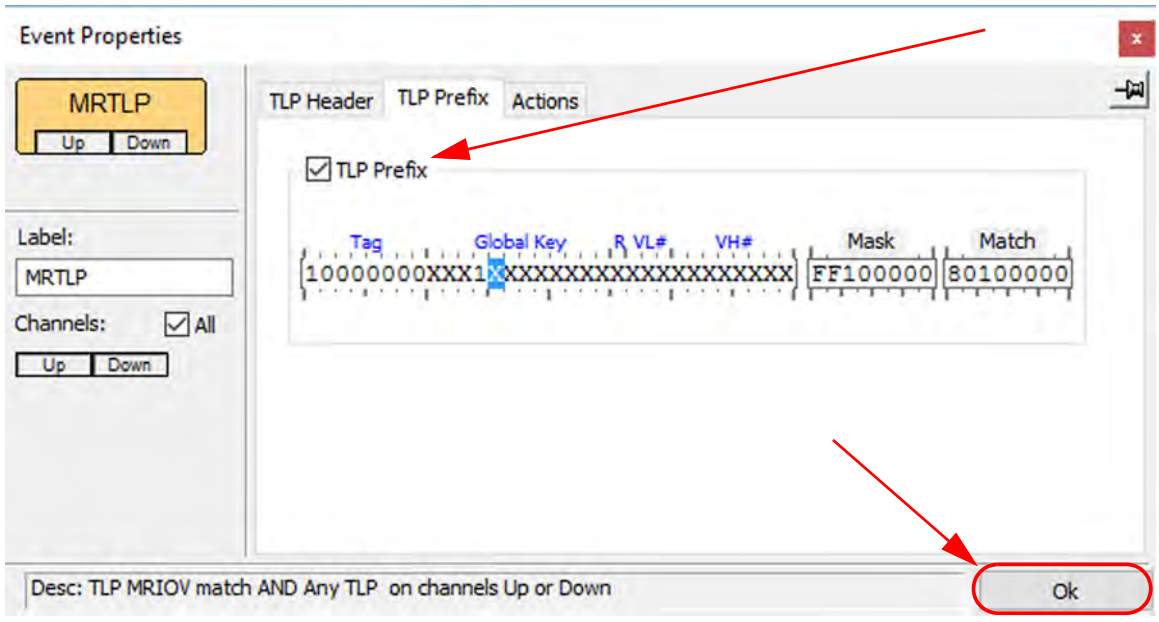


Figure 5.73: TLP Prefix Properties Dialog: (TLP MRIOV Match AND Any TLP)

TLP Actions are shown below in Figure 5.74.

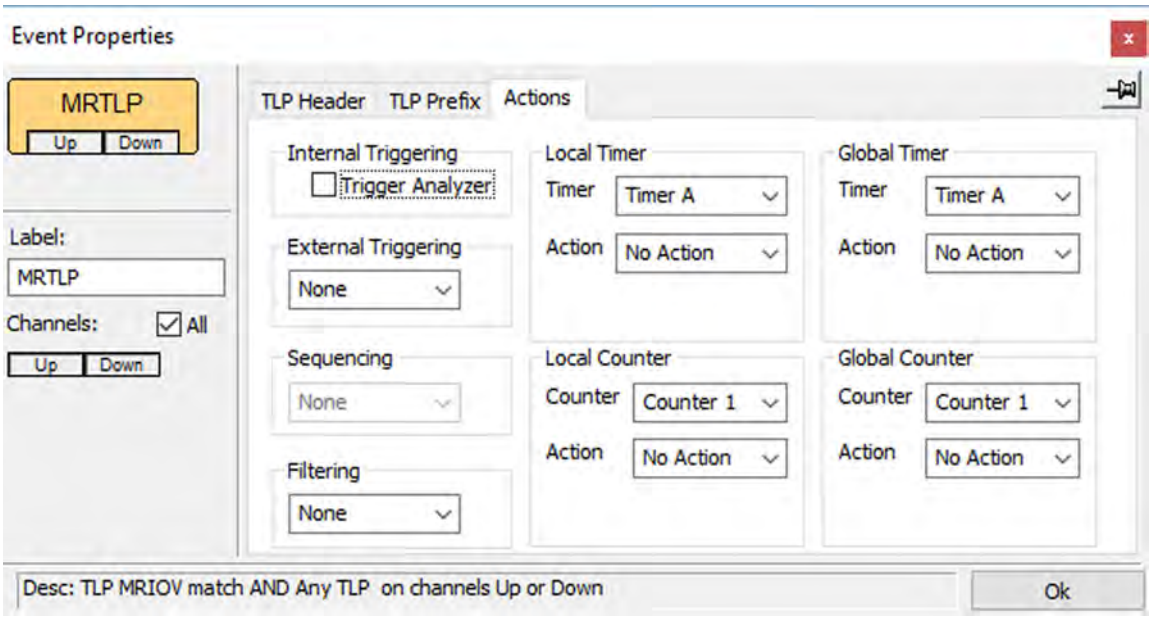


Figure 5.74: TLP MRIOV and Any TLP Event: Actions

TLP: Lightweight Notification → Message Properties Example

You can set the analyzer to trigger on a TLP Lightweight Notification Protocol Message by selecting TLP → Message and then setting the “L” bit to 1 in the TLP Header Layout field. See Figure 5.75.

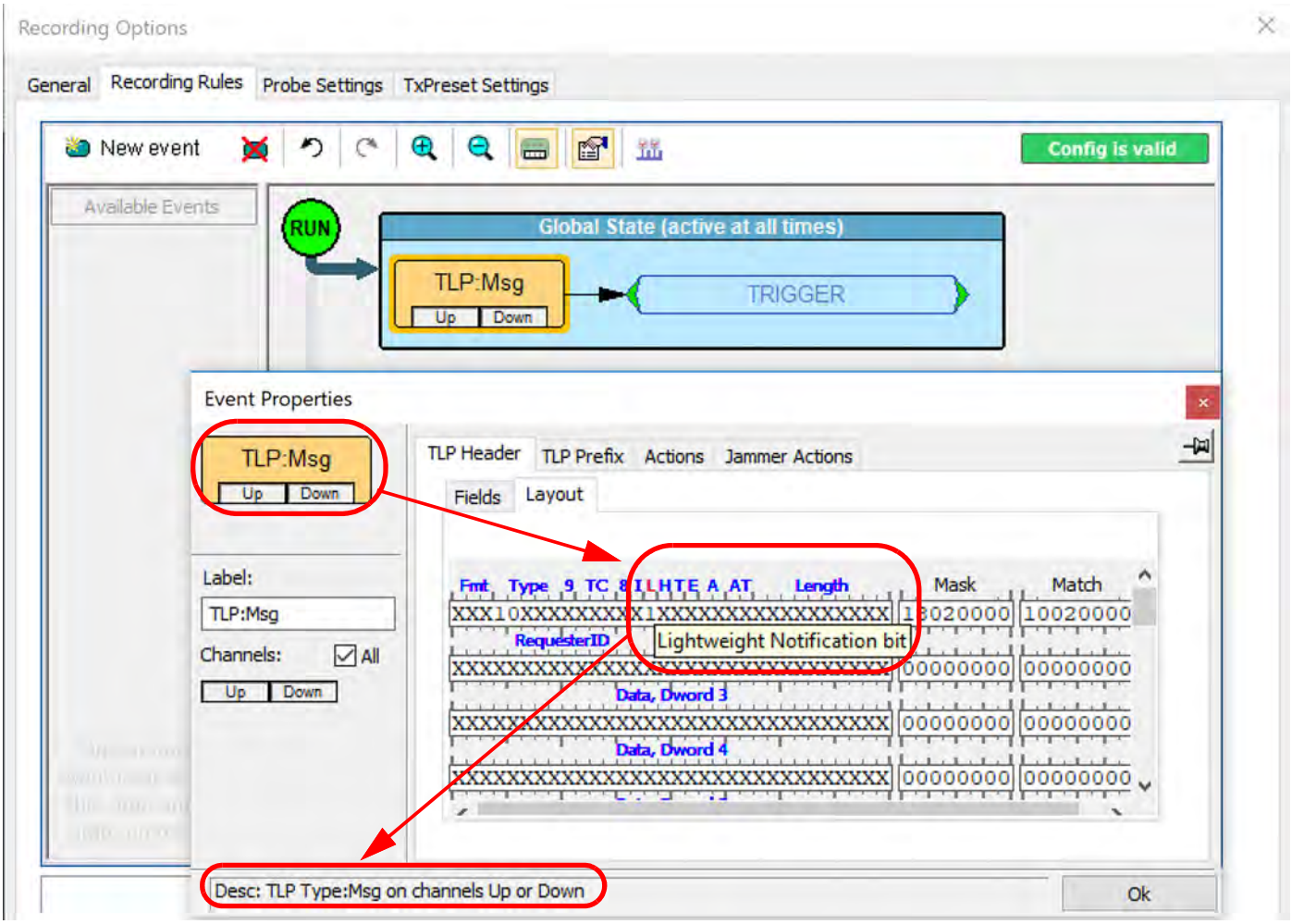


Figure 5.75: TLP: Lightweight Notification Protocol Message

TLP: Lightweight Notification -> Memory Read Example

You can set the analyzer to trigger on a TLP Lightweight Notification Protocol Memory Read by selecting TLP -> Memory Read and setting the “L” bit to 1 in the TLP Header Layout field. See Figure 5.76 on page 203.

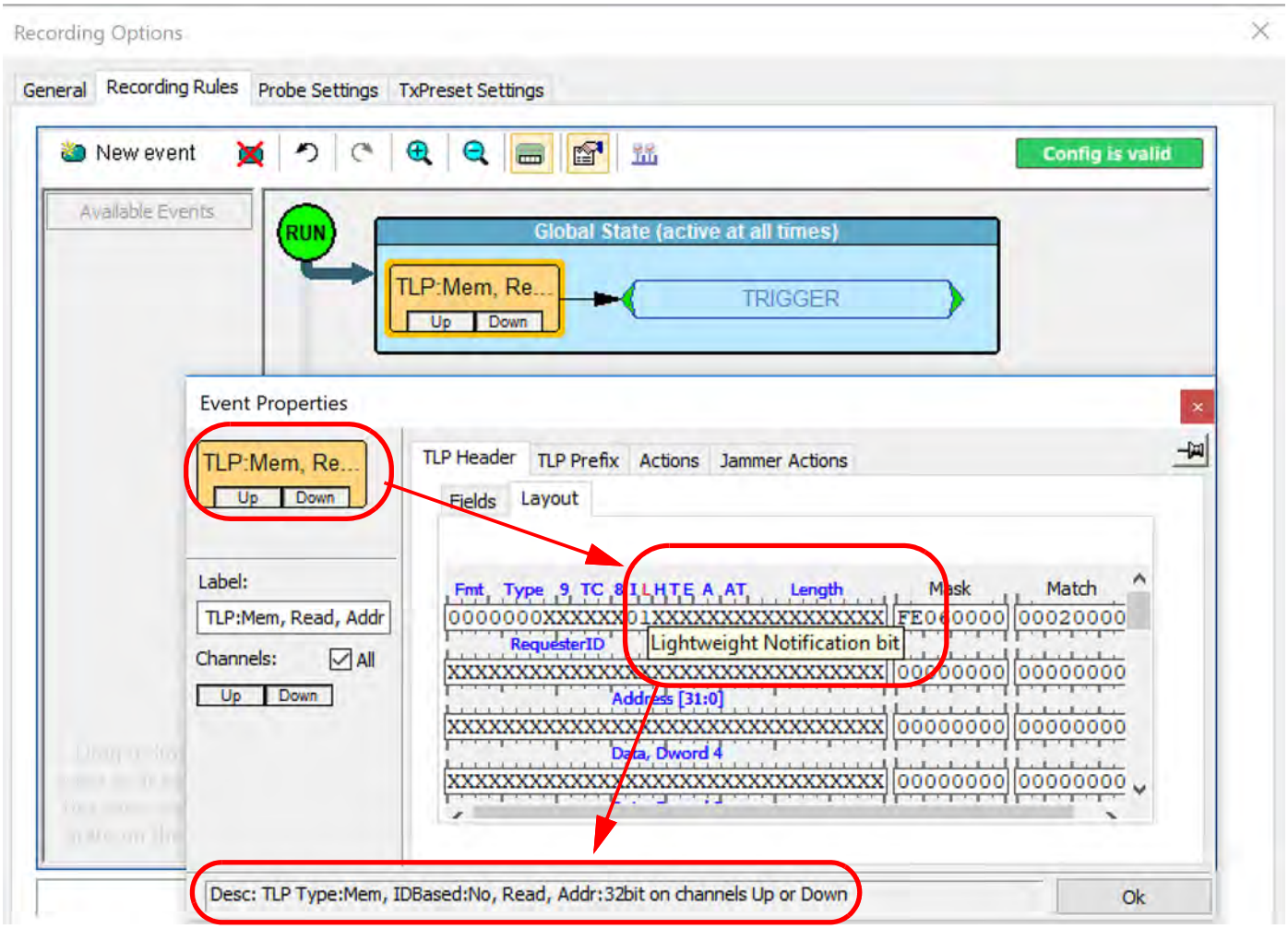


Figure 5.76: TLP: Lightweight Notification Protocol Memory Read

5.20.8.10 NVME Register Properties Dialog

Any of the NVMe Register options can be selected from the New Event list. The NVME Register options are shown in Figure 5.77 on page 204.

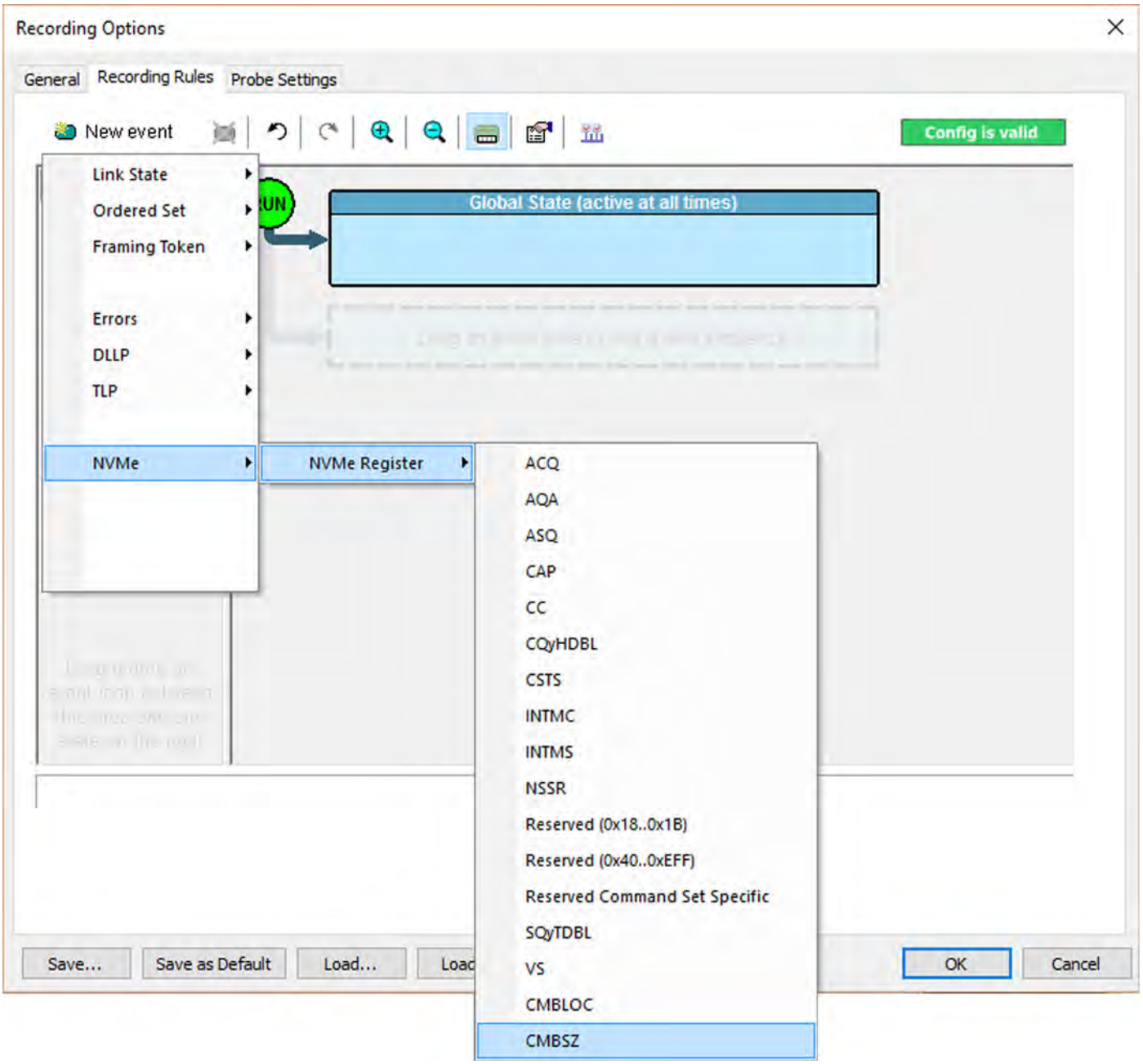


Figure 5.77: NVME Register Options Dialog

The NVME Register Properties dialog allows you to select the MBAR value, choose the Register and Address Type from the drop-down list and enter the offset. See Figure 5.78 on page 205.

The data pattern can be entered directly into the field, but some fields can be selected from the drop-down list. Click on the field name for a list of available registers as illustrated in and Figure 5.79 on page 205.

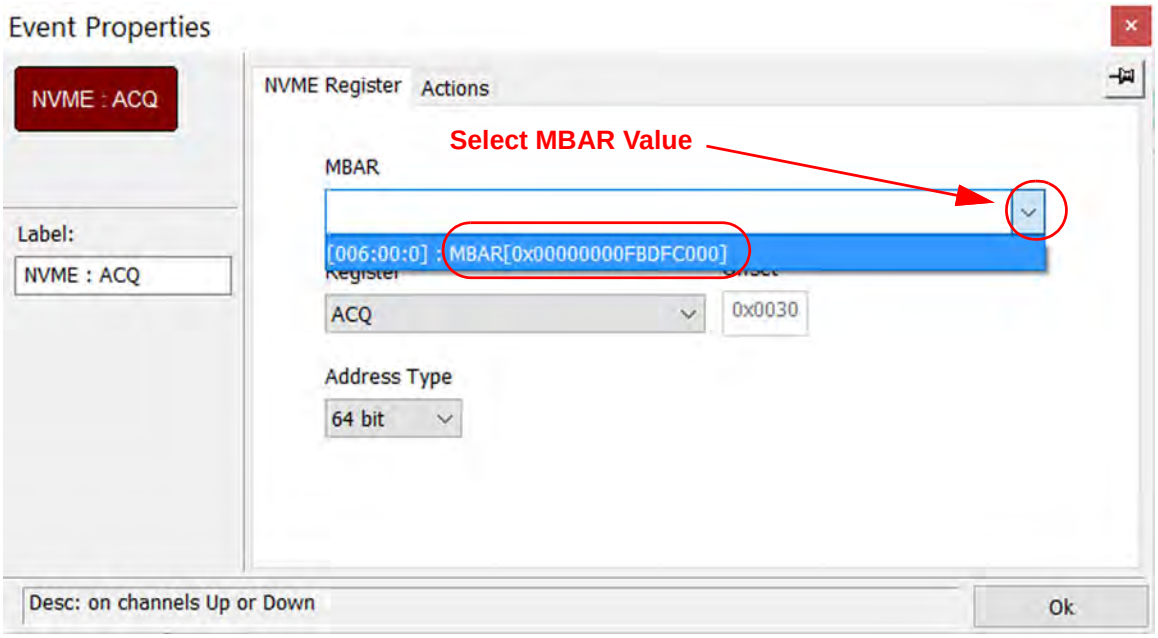


Figure 5.78: NVME Register Properties Dialog with MBAR Value Shown

Note: Triggering on register event with 32-bit address and payload defined is applicable to register write transactions only. After selecting the options you want click on the “OK” button.

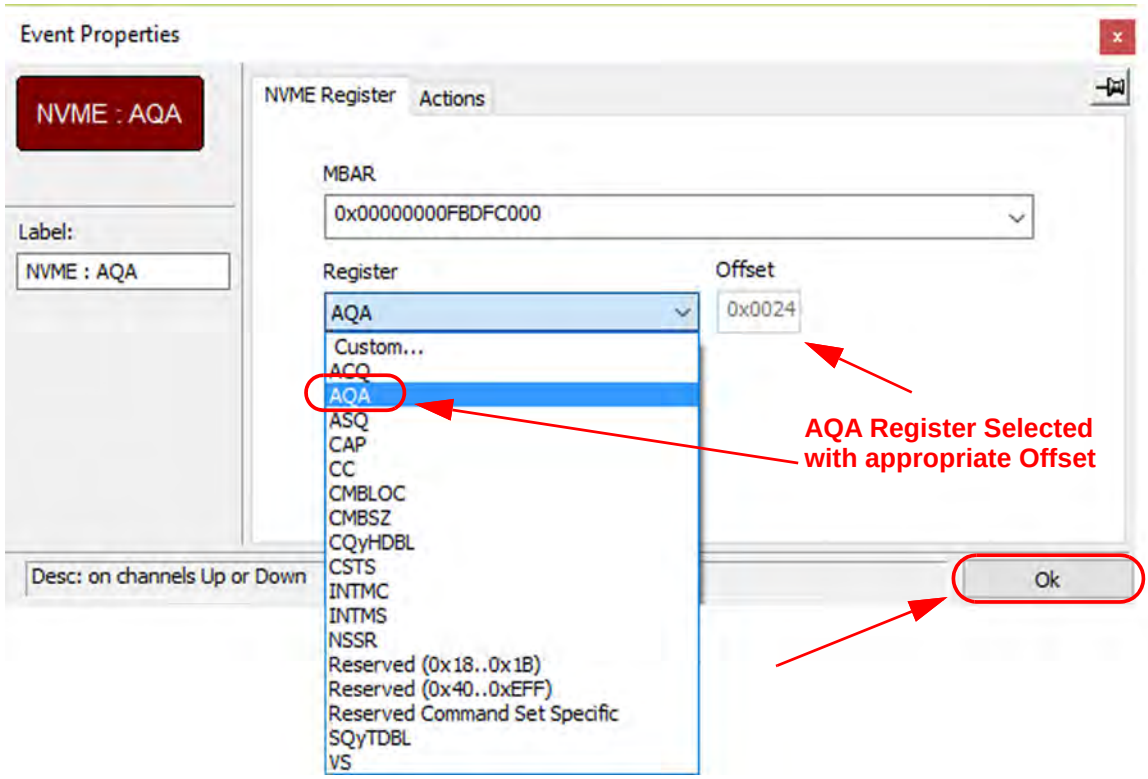


Figure 5.79: NVME Registers from Drop Down List

NVME Register Options: AQA Actions

Select an Action from the NVMe : AQA Actions dialog. See Figure 5.80 and click “OK”.

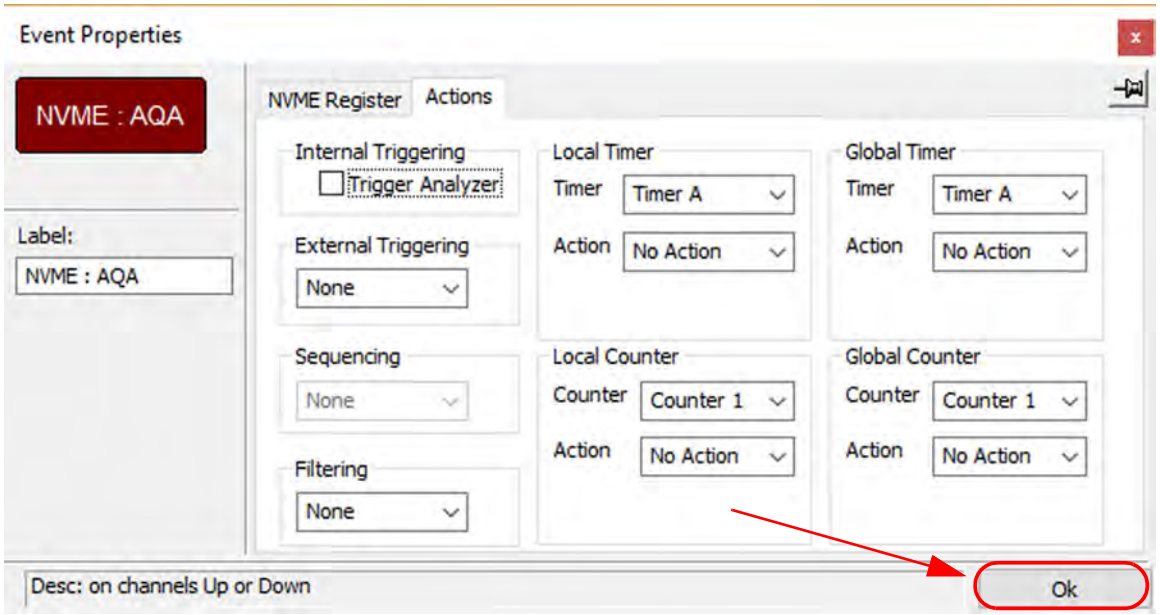


Figure 5.80: NVME Register Options: AQA Actions

5.20.8.11 PQI Register Properties Dialog

The PQI Register Properties dialog allows you to enter the MBAR value, choose the Register and Address Type from the drop-down list and enter the offset. After selecting the options you want click on the “OK” button.

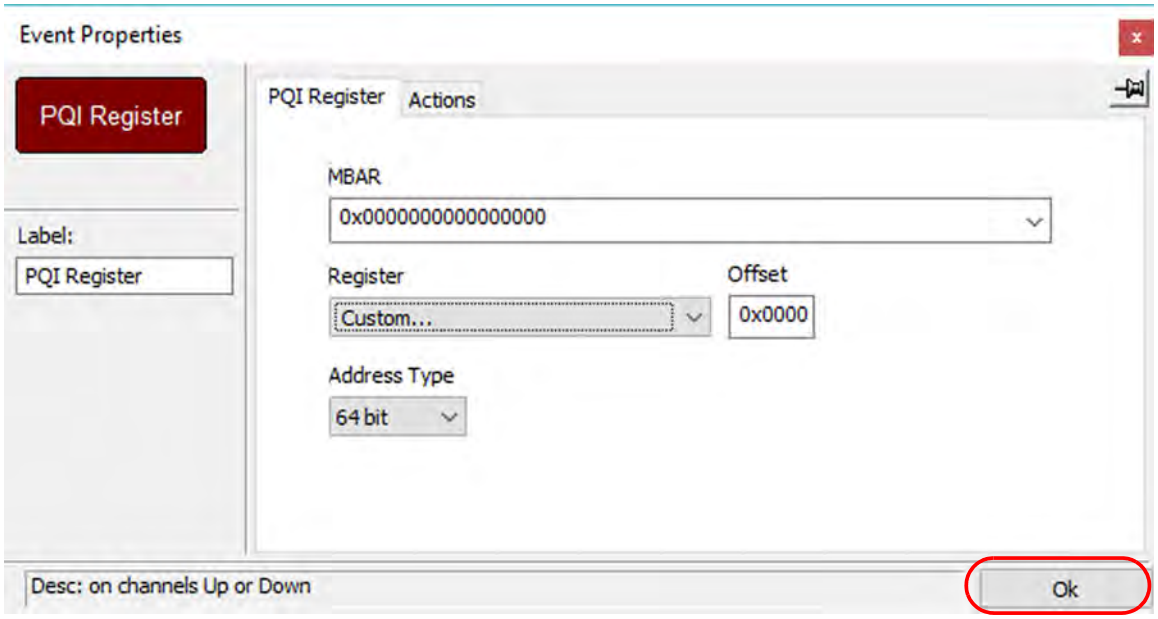


Figure 5.81: PQI Register Properties Dialog

Note: Triggering on register event with 32-bit address and payload defined is applicable to register write transactions only.

The select an Action from the PQI register Actions dialog. See Figure 5.82 and click “OK”.

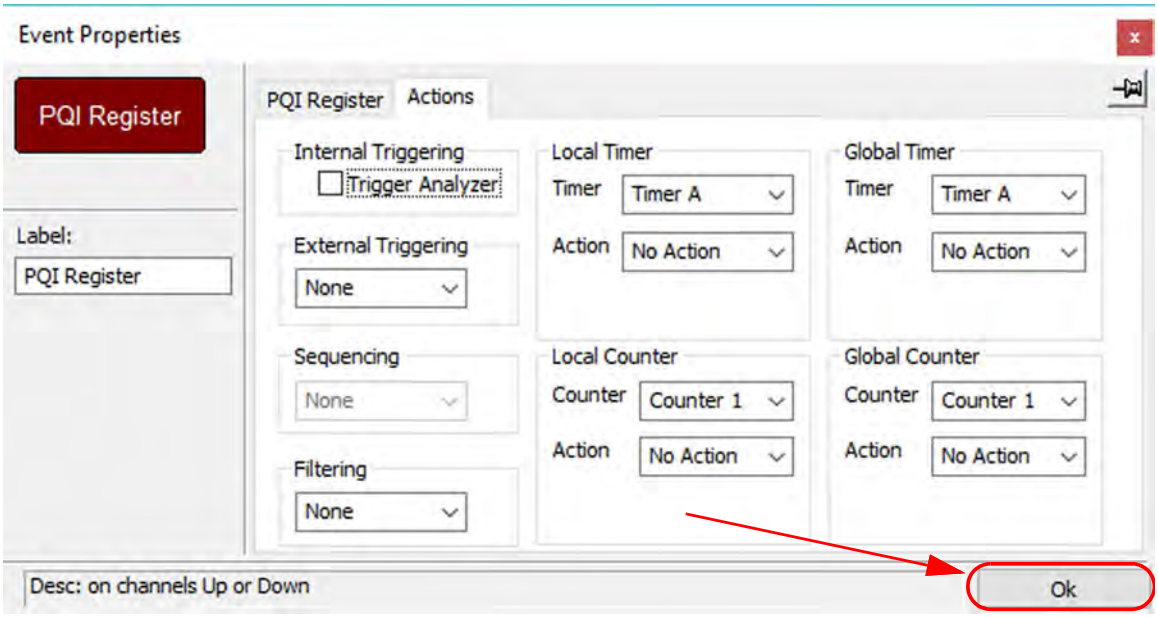


Figure 5.82: PQI Register: Actions Dialog

5.20.9 Actions Properties Dialog

Every Event has an Action tab as shown in Figure 5.83 on page 208.

The following tables describes the Actions for each Event.

TABLE 5.5: Event Actions

Action	Description
Label	Label the action.
Channels	Select Channels to go upstream or downstream.
Internal Triggering	Check the box to enable Internal Triggering from the Trigger In input. Any edge of the supplied signal will cause the analyzer to trigger.
External Triggering	Set the External Triggering to Low, High or Toggle. The default is None.
Sequencing	Set the Sequence to Advance. The default is None.
Filtering	Set the Filtering to Filter Out. You cannot Filter In in the Summit Z3-16. The default is None.
Local Timer	Set the Local Timer, there are four options available.

TABLE 5.5: Event Actions (Continued)

Action	Description
Action	You can set the Action of the timer to Start or Reset. When you reset the timer it resets to it's initial value. The default is No Action.
Local Counter	Set the Local Counter, there are four options available.
Local Counter Action	You can set the Action of the Counter to Increment or Reset. The Counter increments by one and resets to its initial value. The default is No Action.
Global Timer	Set the Global Timer, there are two options available.
Global Timer Action	You can set the Action of the timer to Start or Reset. When you reset the timer it resets to it's initial value. The default is No Action.
Global Counter	Set the Global Counter, there are two options available.
Global Counter Action	You can set the Action of the Counter to Increment or Reset. The Counter increments by one and resets to its initial value. The default is No Action.

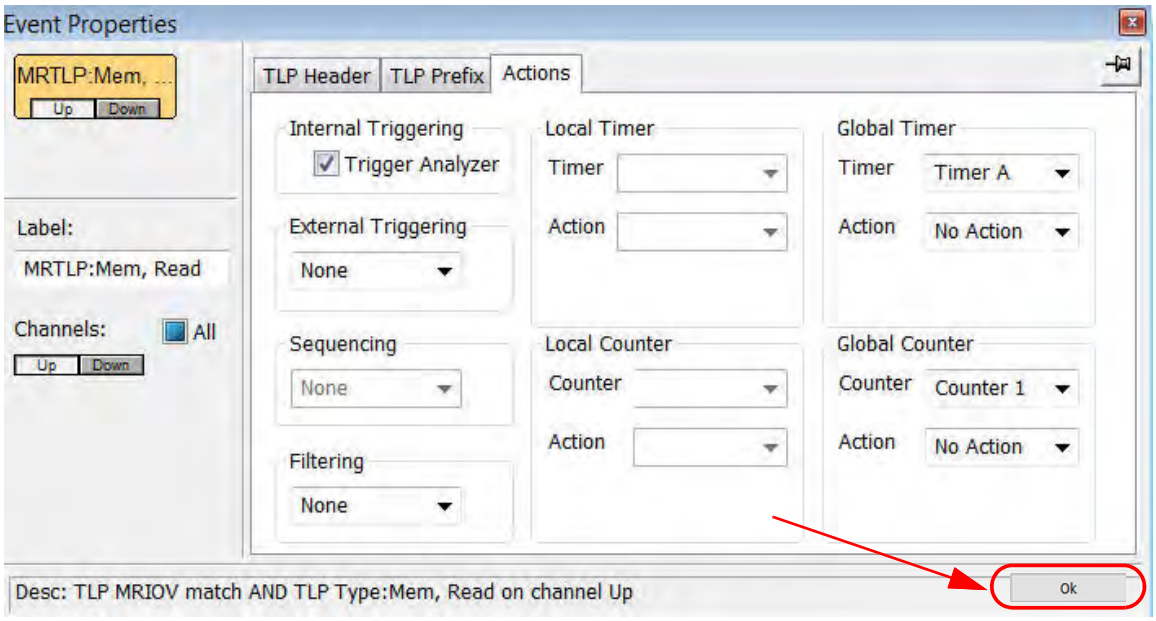


Figure 5.83: Actions Properties Dialog

5.20.9.1 Filter Out

A filter causes the Analyzer to filter out specified events from the recording. If events are filtered out of the recording, they are excluded from the Analyzer's buffer and not simply hidden from the CATC Trace. The purpose of "filtering out" is to preserve recording memory so you conduct longer recording sessions and exclude unnecessarybevents.

5.20.9.2 Filter-Out In Simple Mode

In Simple Mode you can filter out:

- SKIP Ordered Sets
- UpdateFC DLLP
- Compliance Pattern
- Modified Compliance Pattern
- End of Datastream (EDS)

See Figure 5.84.

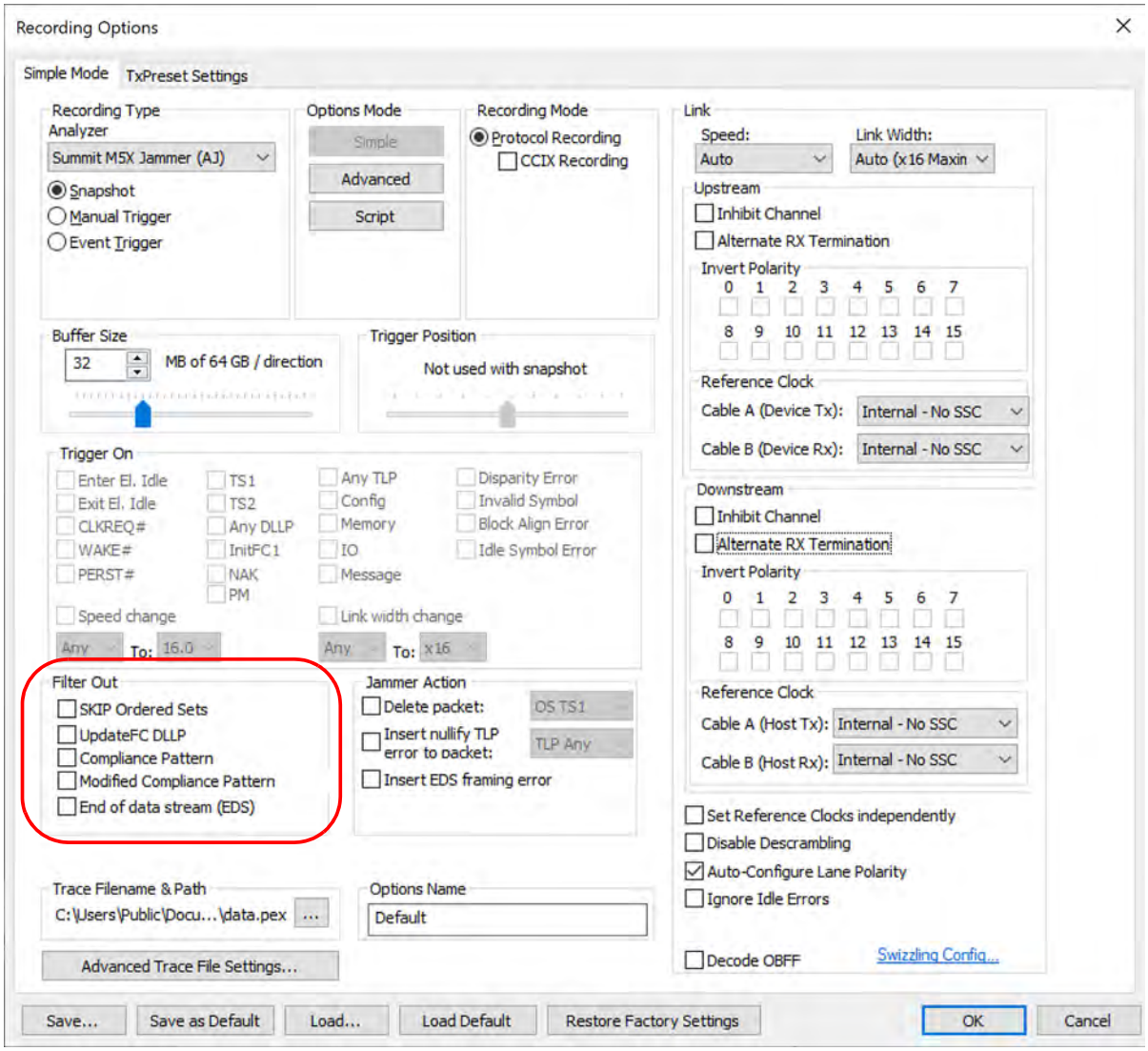


Figure 5.84: Simple Mode: Filter Out → Summit M5x

Note: If you Filter-Out all the events shown above, this creates an empty trace and displays a warning message.

5.20.9.3 Filter-Out in Advanced Mode

To enable “filter-out” in Advanced Mode, place an event button into either the **Global State** cell or the **Sequence** cell, then right-click the button and choose an **Action** (see previous topic).

From the sub-menu, select **Filter-Out.** See Figure 5.85.

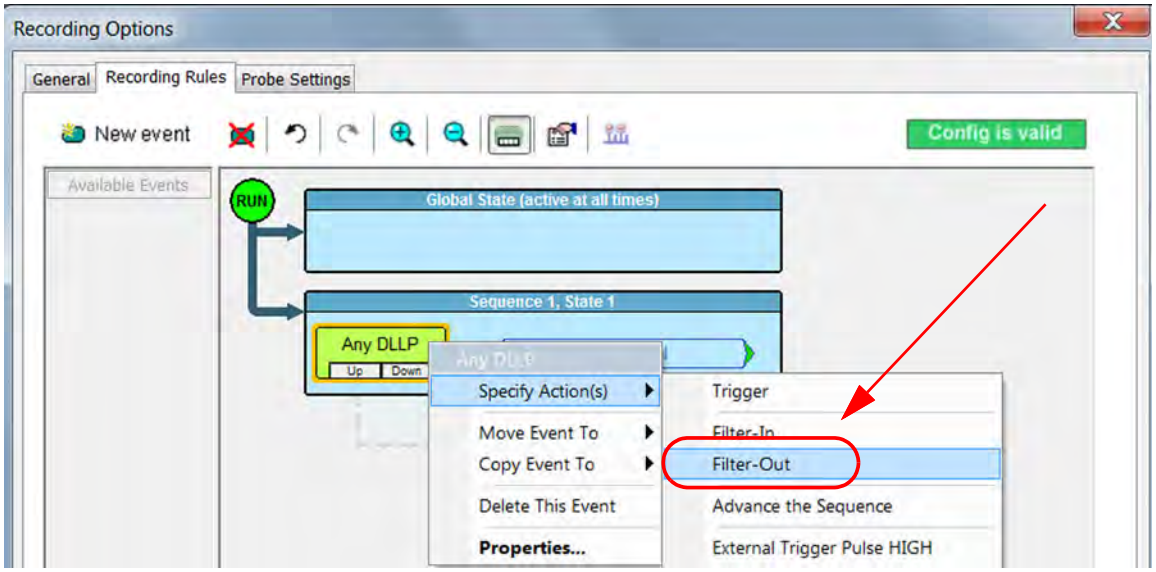


Figure 5.85: Filter Out Option

Note:
- The Filter-Out option is only available in the DLLP, TLP, TS1 and TS2 Ordered Sets, for Link Events Enter/Exit Electrical Idle, WAKE# Asserted/Deasserted, or CLKREQ# Asserted/Deasserted.
- If you Filter-Out all events (by mistake), this creates an empty trace and displays a warning message.

5.20.10 Filter In

“Filter in” is the logical opposite of “Filter Out”. In this case, you are specifically interested in capturing specific events or traffic and ignoring everything else. If events are filtered in to the recording, they are included in the Analyzer's buffer. The purpose of “filtering in” is to preserve recording memory so you conduct longer recording sessions and include only events that interest you. Filter -n is only available in Advanced Mode.

As an example, let’s say you want to capture **Any DLLP** and **Any NVMe:ACQ** Commands.

First switch to **Advanced Mode**.

To enable “Filter-In” place an event button (DLLP -> Any DLLP) into the **Global State** cell, then right-click the button and choose an **Action**. From the sub-menu select **Filter-In.**

Then select NVMe under New Event and NVMe Register:ACQ and place that event into the **Sequence 1, State 1** cell. Then right-click the button and choose an **Action**. From the sub-menu select **Filter-In.** See Figure 5.87 on page 212.

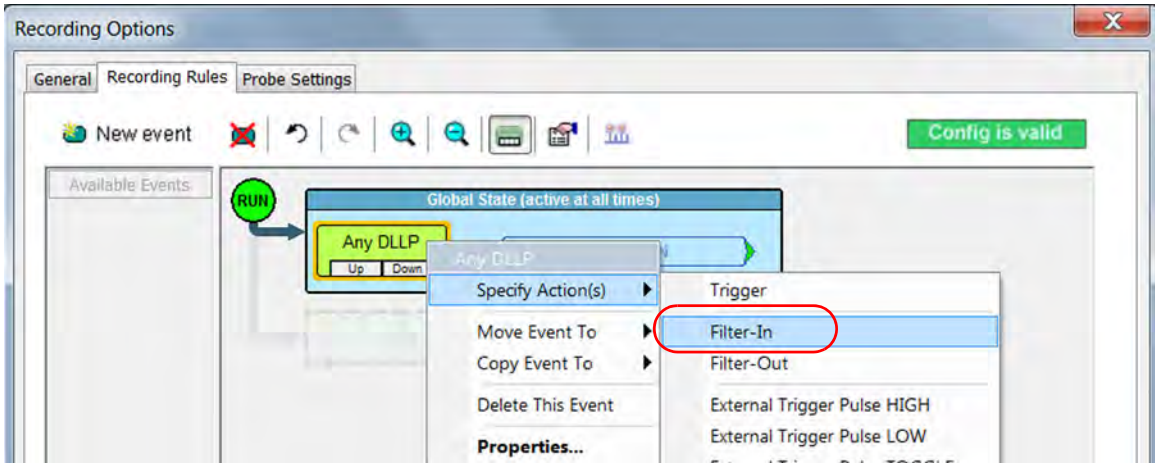


Figure 5.86: Filter In Option

Note: When a Filter-In is selected the analyzer filters out everything else by default

5.20.11 Valid Configuration

In this case, you have chosen a Global State Filter-In on any DLLP and Sequence 1, State 1 to have an NVMe Command:ACQ Filter-In. This is a valid configuration as shown in Figure 5.87.

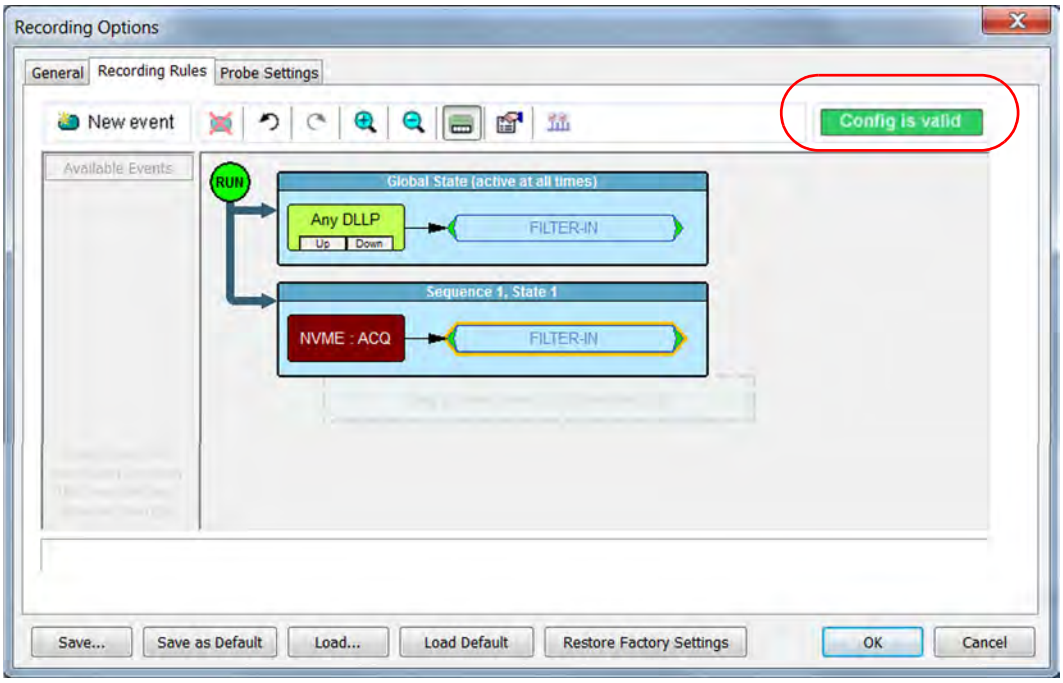


Figure 5.87: Filter In: Advanced Mode: Filter In Any DLLP and Any NVMe ACQ Command

Note: If you change the Global State to Any DLLP but switch to FILTER-OUT you will get the following warning message: See Figure 5.89 on page 218.

5.20.12 Invalid Configuration

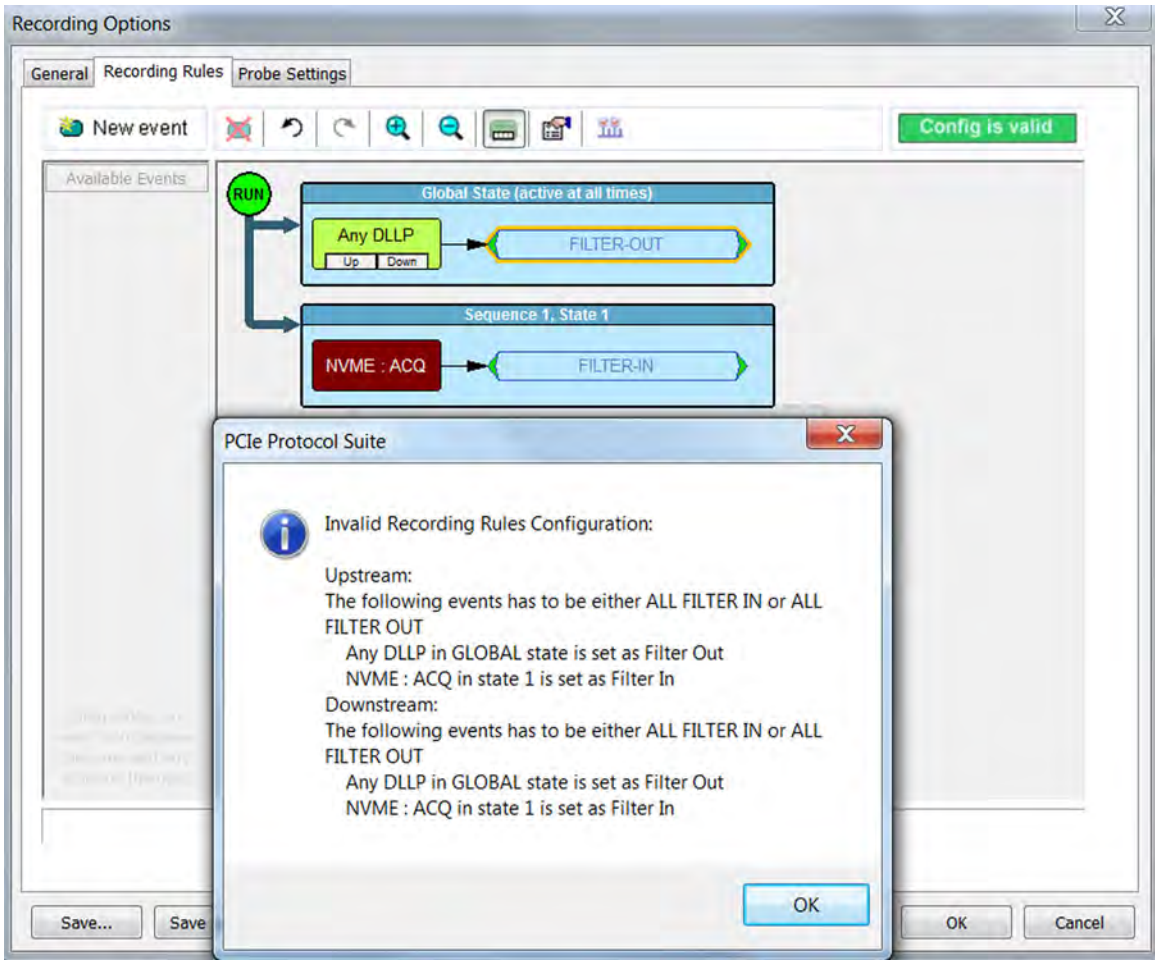


Figure 5.88: Warning Message for Invalid Configuration

The analyzer is warning you that you've set a Global Rule to Filter-Out Any DLLP and that condition will filter out the NVMe:ACQ Command you're looking for. So the recording rules have to be consistent. You'd get the same message if you set Any DLLP to Filter-In but set the NVMe:ACQ Command to Filter-Out. The warning message would pop up and if you hit OK, the **Config is Invalid** message will light up. See Figure 5.89 on page 214.

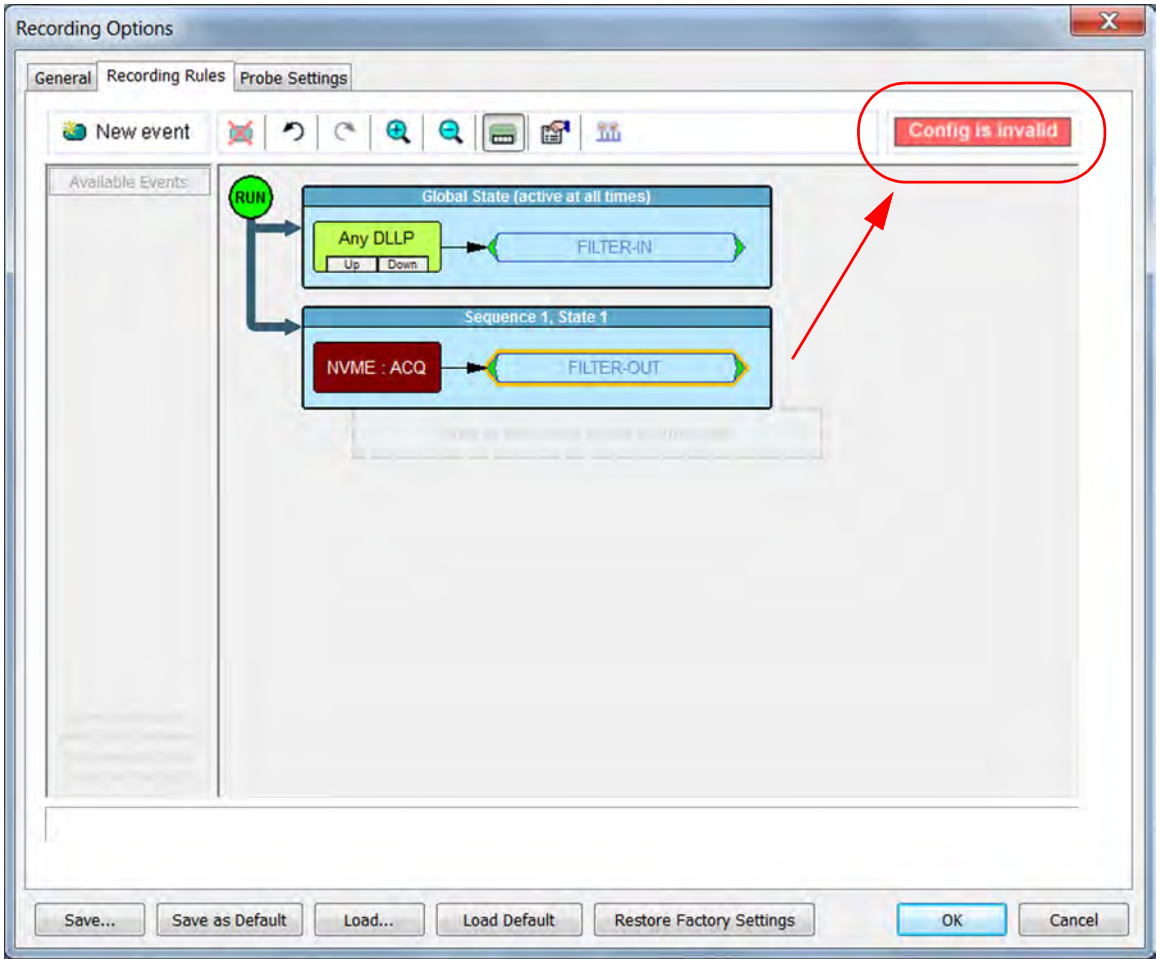


Figure 5.89: Filter In: Any DLLP, Filter Out Any NVMe:ACQ Command -> Invalid Config

So the tool won't let you try to set recording options that are logically inconsistent.

5.20.13 Filtering Events: (Electrical Idle, CLKREQ#, WAKE#)

To be able to Filter-In or Filter-out the following events (Electrical Idle, CLKREQ# and WAKE#), three conditions must be met:

- ❑ The event must be in a global state
- ❑ The event must be both asserted and de-asserted
- ❑ Triggering must be deselected

5.20.13.1 Example of CLKREQ# Filtering Enabled

See Figure 5.90 on page 215 and Figure 5.91 on page 215 for an example of CLKREQ# events in the global state, asserted and deasserted are both selected and triggering is deselected. Then you'll see that filtering of those events is enabled. After selecting the options you want click on the "OK" button.

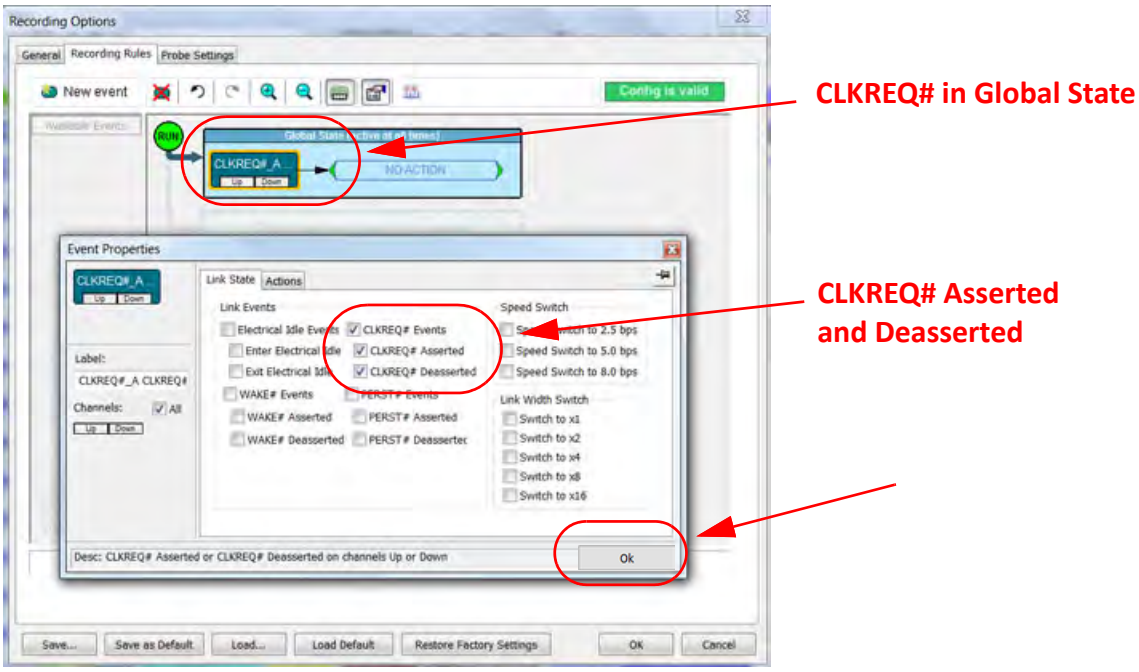


Figure 5.90: Link Event: CLKREQ# => Both Asserted and Deasserted Selected

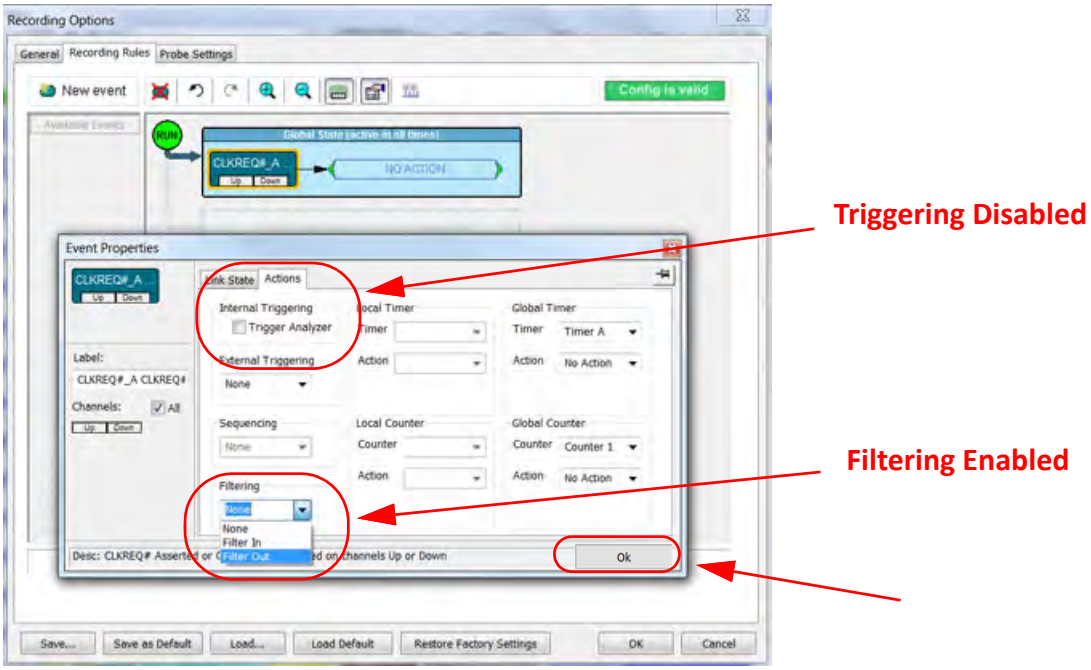


Figure 5.91: Link Event: CLKREQ# => Both Asserted and Deasserted => Filtering Enabled

5.20.13.2 Example of CLKREQ# Filtering Not Enabled

See Figure 5.92 for an example of CLKREQ# events in the global state, but only CLKREQ# has been asserted (deasserted is not selected) and triggering is deselected. So when one of the required conditions is not met (CLKREQ# being asserted and deasserted) Filtering is not enabled (see Figure 5.93 on page 216). After selecting the options you want click on the “OK” button.

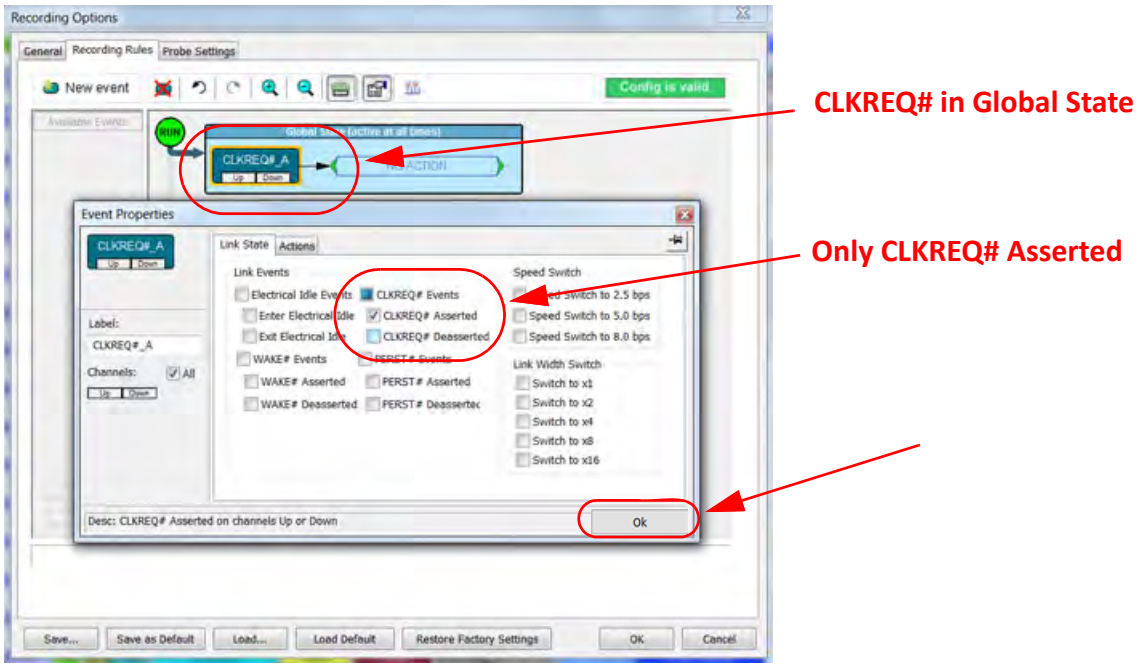


Figure 5.92: Link State: CLKREQ# => Asserted Only Selected

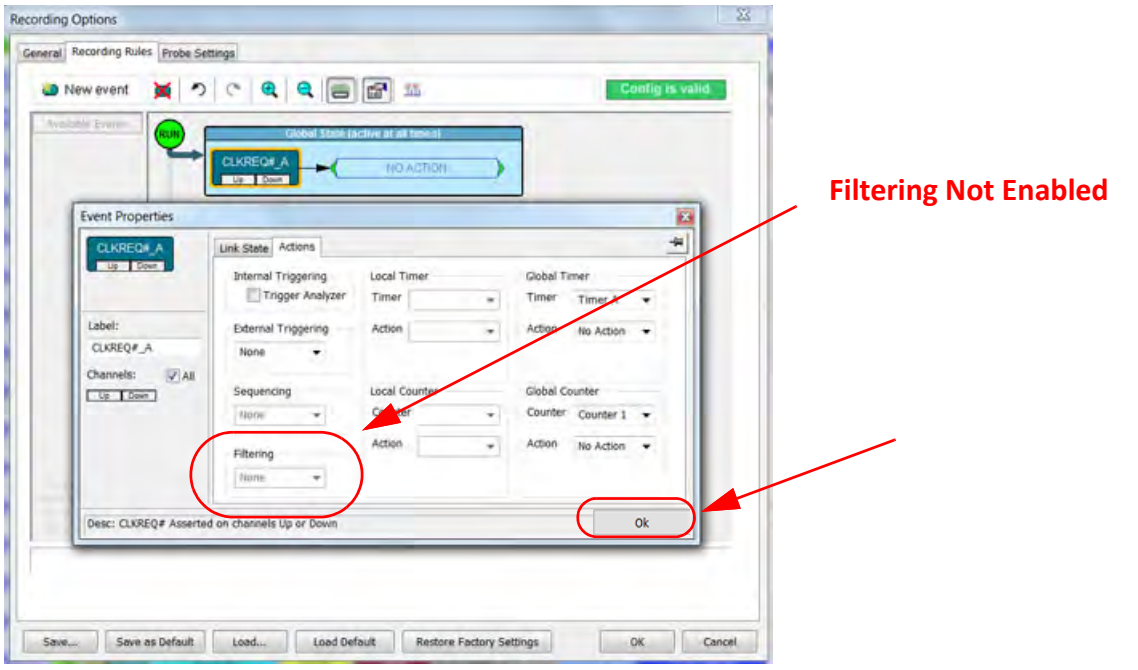


Figure 5.93: Link State: CLKREQ# => Asserted Only Selected => Filtering Disabled

5.20.14 Filtering Out NVMe CSTS, DLLP Ack and TLP Completions

To enable longer recordings, you can filter out NVMe CSTS, DLLP Acks and TLP Completions in Global Options by using the Advanced Recording Options. See Figure 5.94.

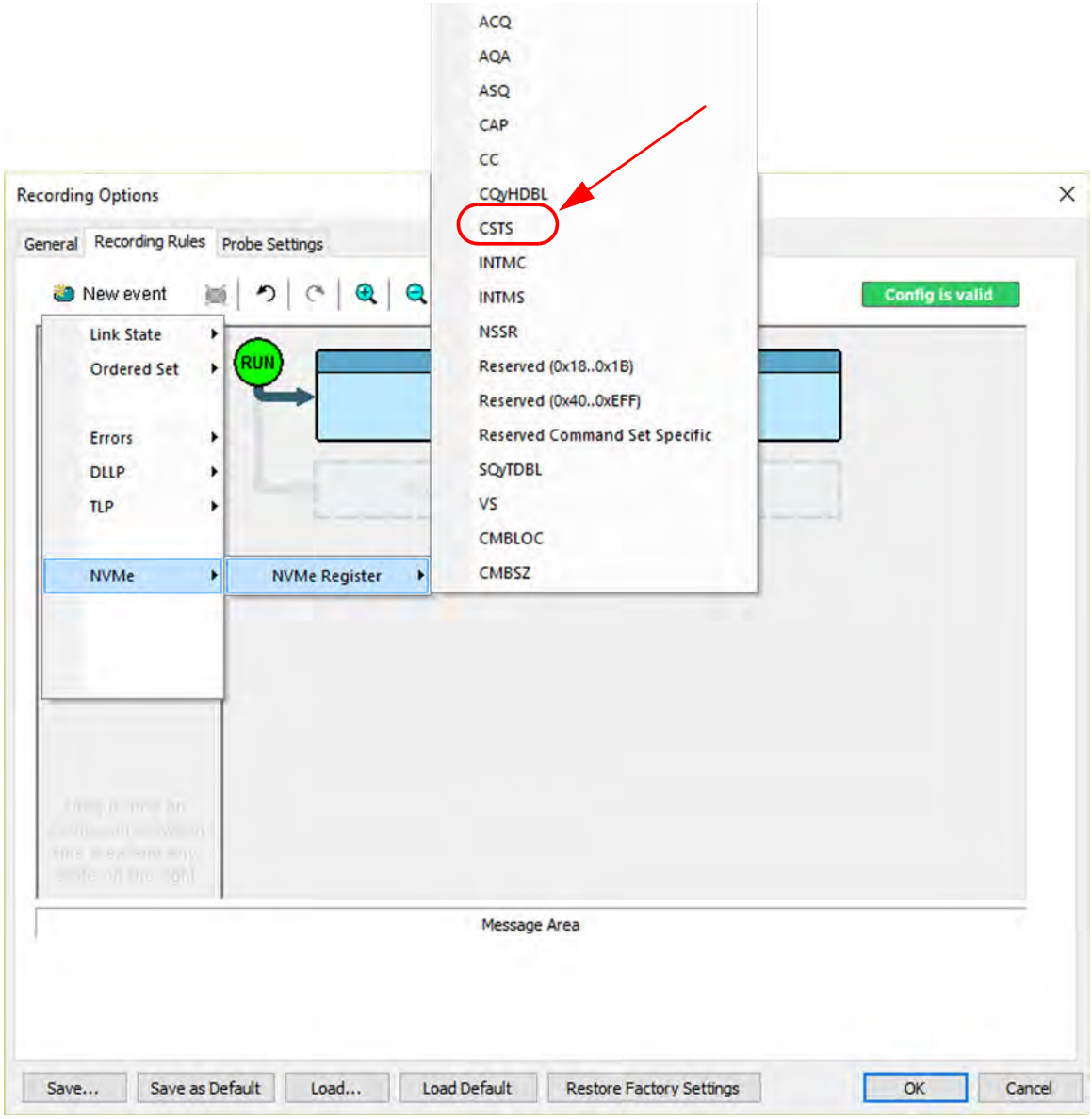


Figure 5.94: Filtering Out NVMe CSTS

If you select **New Event -> NVMe -> NVMe Register -> CSTS -> Actions** you'll have the option to filter out the CSTS events. See Figure 5.95 on page 218.

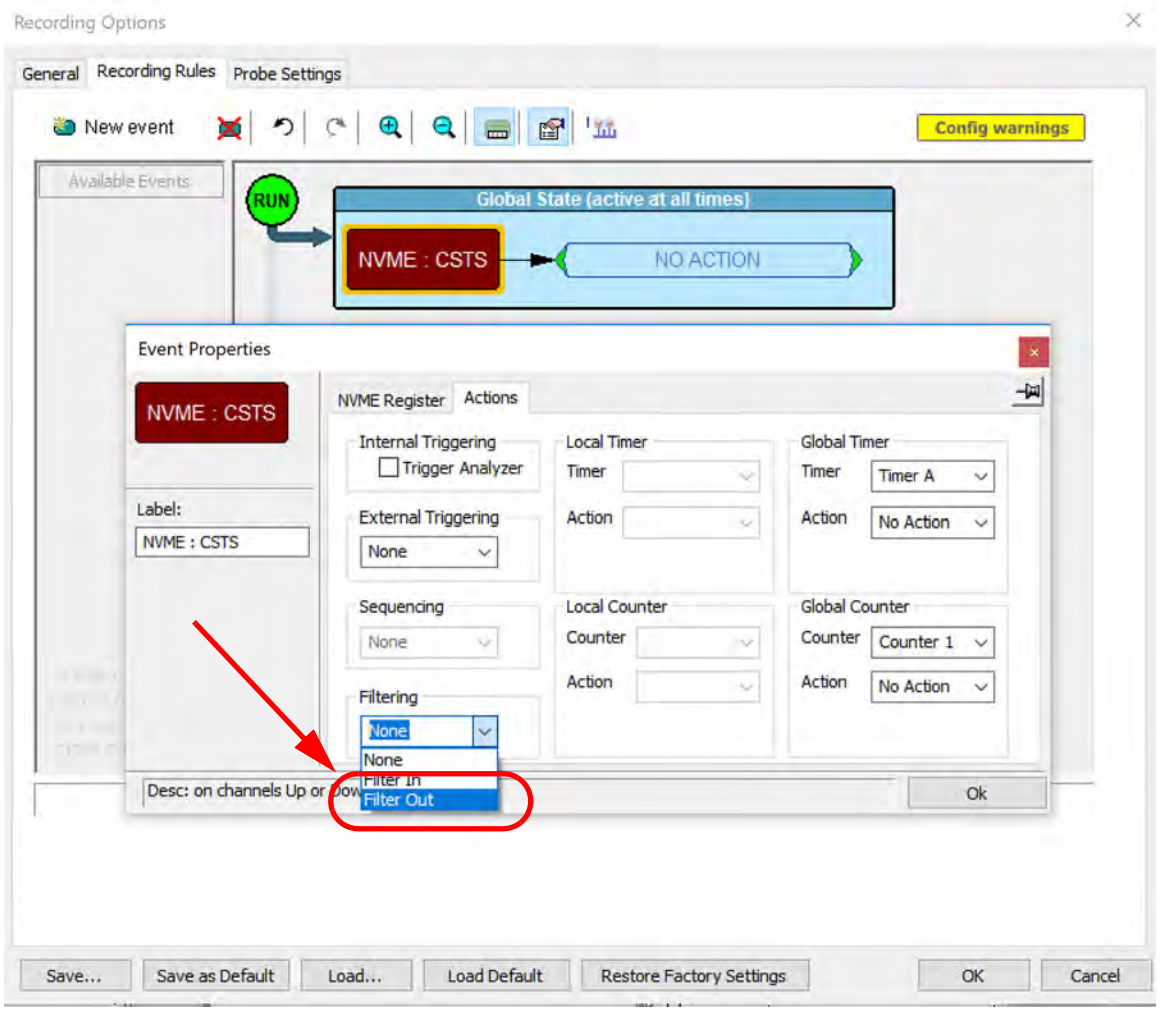


Figure 5.95: Selecting Recording Options: NVMe -> CSTS Event

Set the Action to Filter Out. Then click on “OK”. See Figure 5.96 on page 219.

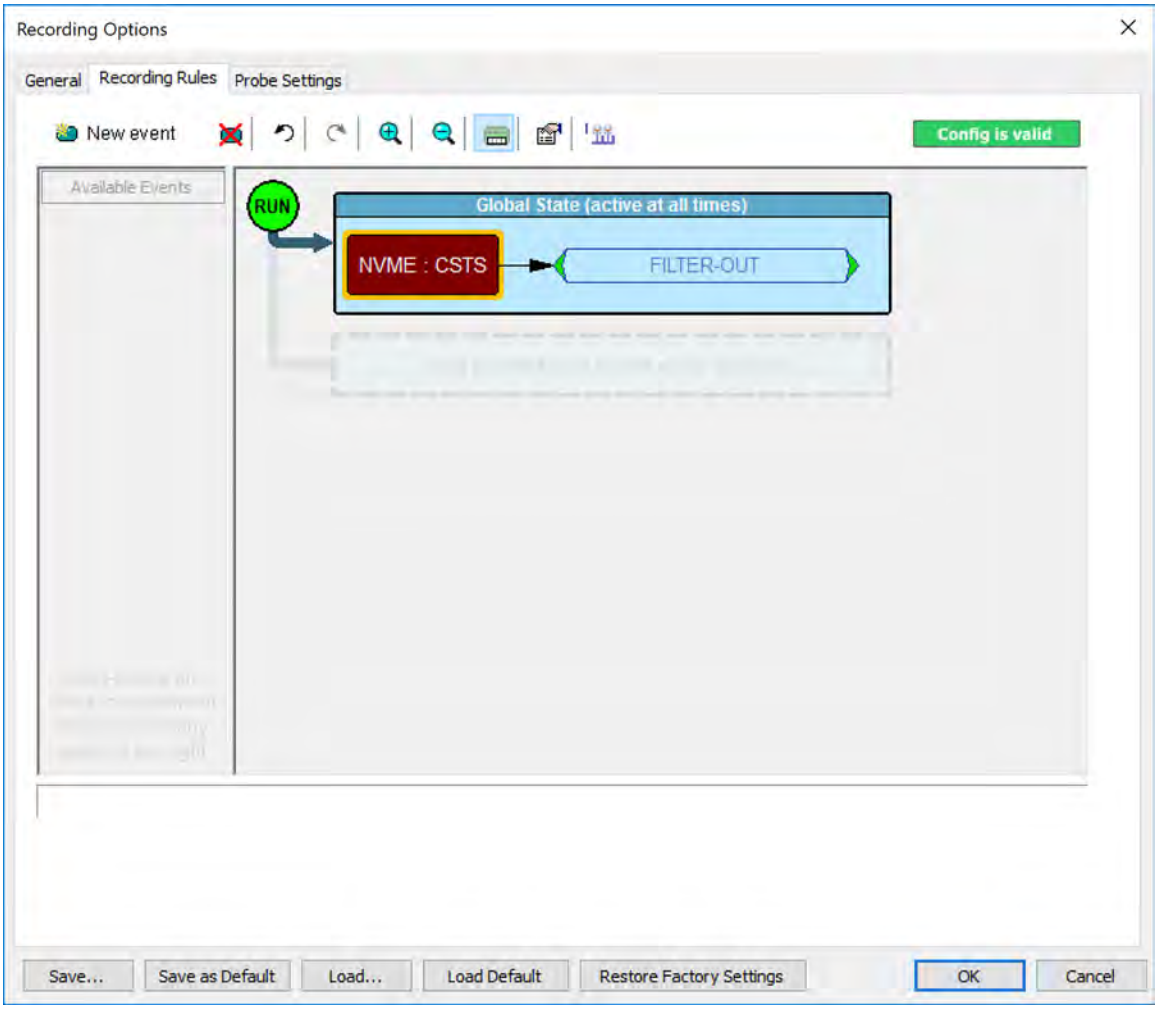


Figure 5.96: Recording Options: Filter Out NVME CSTS

Next add DLLP Acks to also be Filtered Out. See Figure 5.97 on page 220.

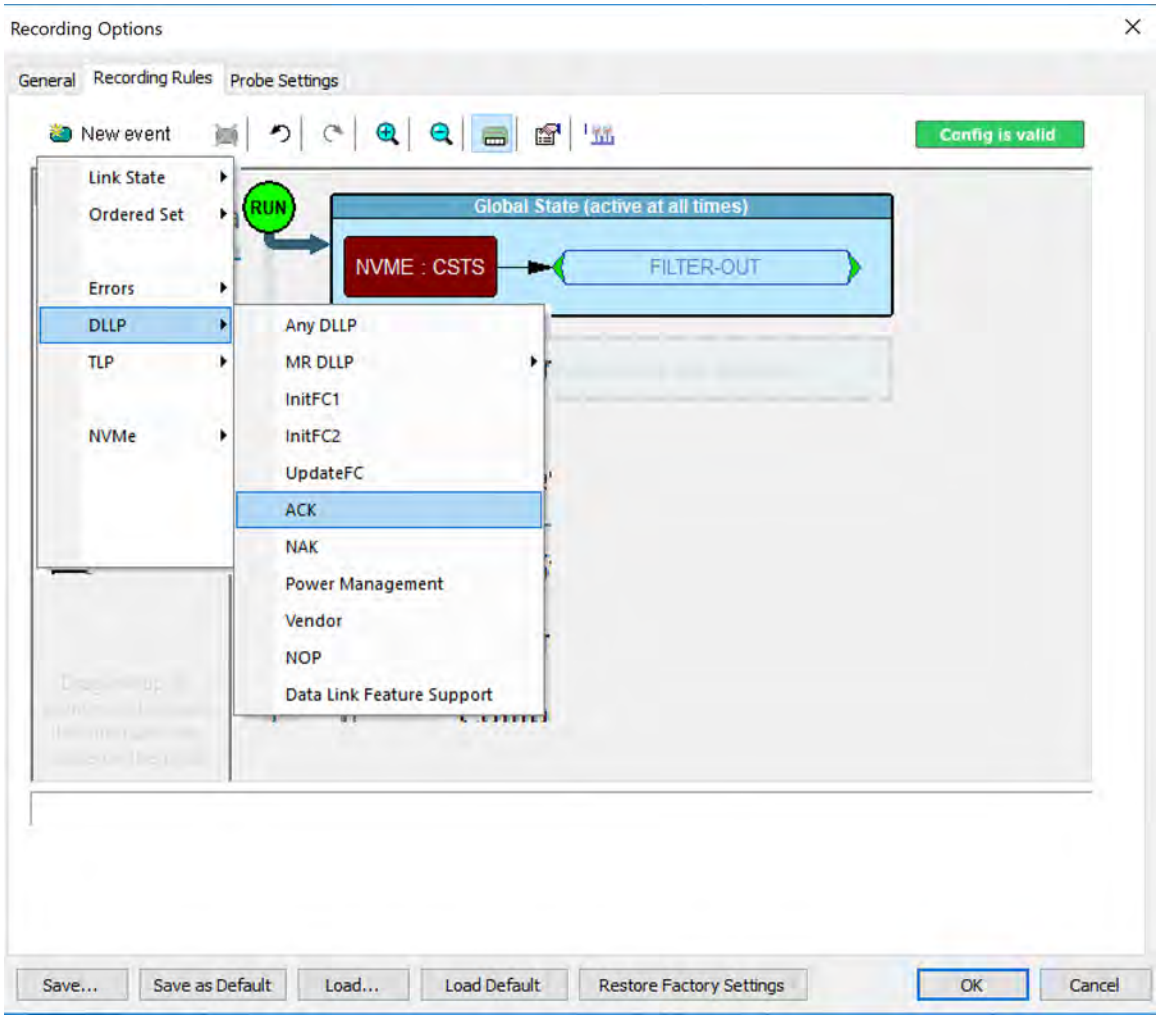


Figure 5.97: Recording Options: DLLP -> ACK

Click on “OK”, then add the Action -> Filter Out and place the DLLP in the Global State. See Figure 5.98 on page 221.

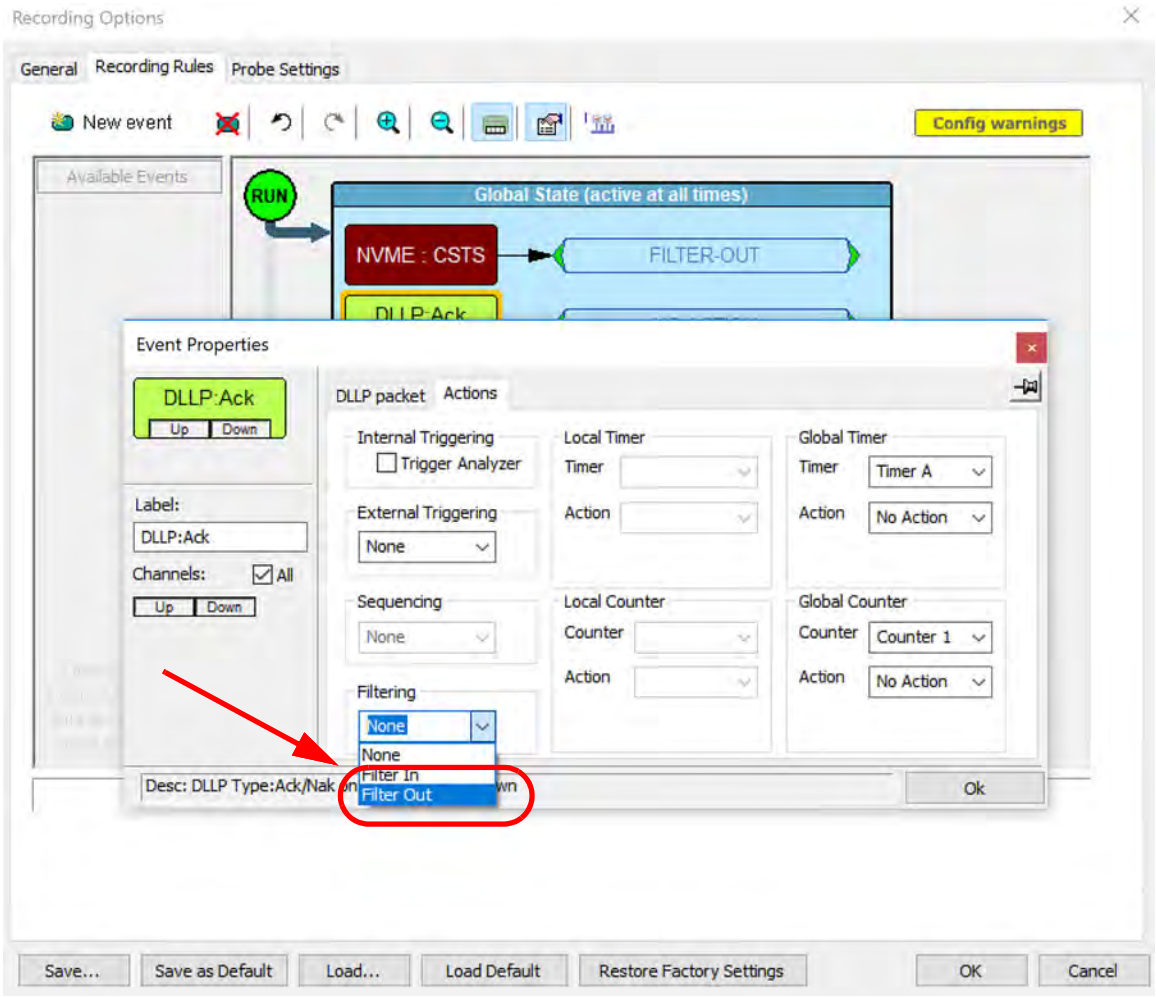


Figure 5.98: Select Action: Filter Out

Select Actions -> Filtered Out.

Click on “OK” and the DLLP:Ack with Action “Filter-Out” will be placed in the Global Options state. See Figure 5.99 on page 222.

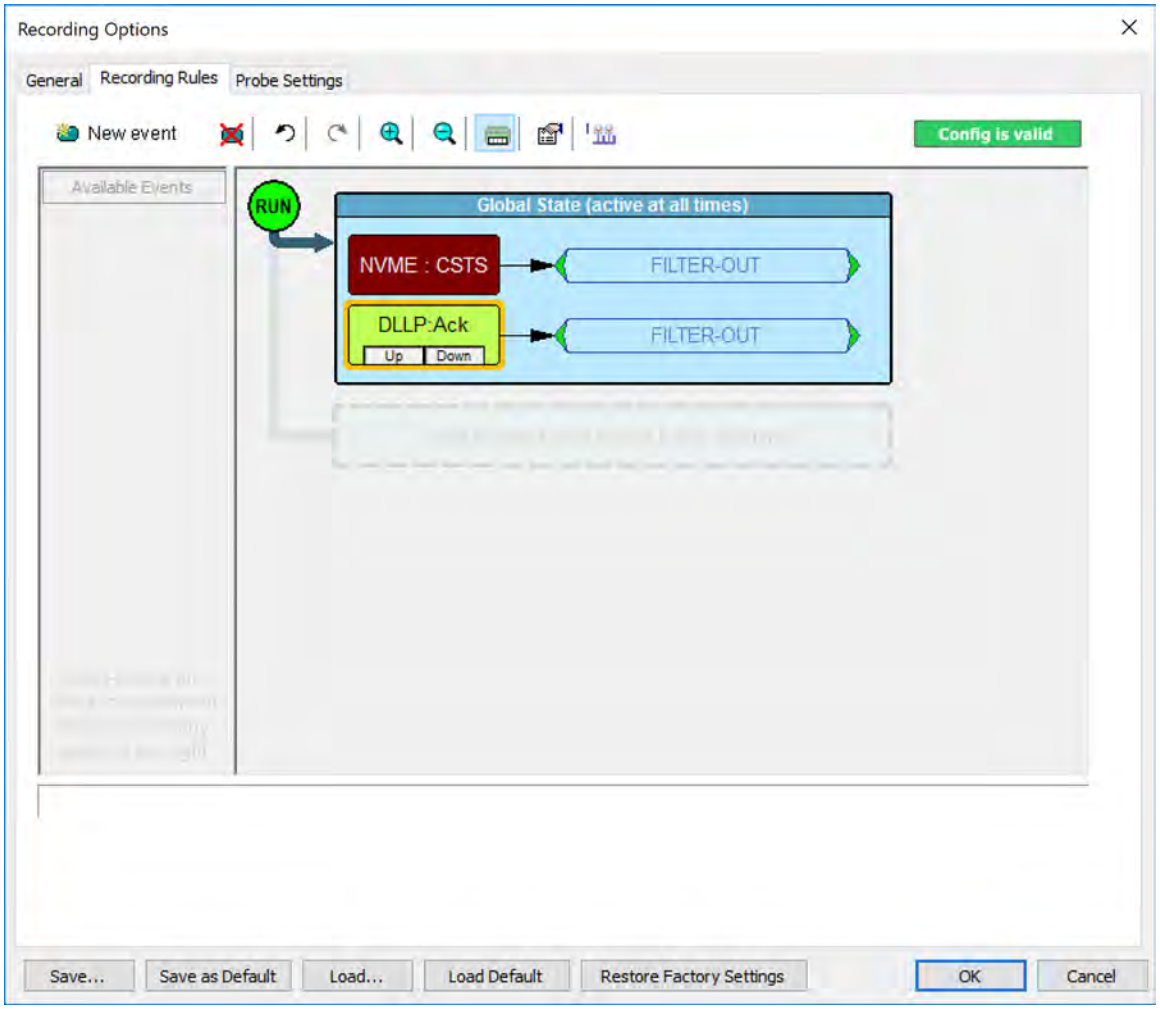


Figure 5.99: Place Recording Option: DLLP:Ack → Filter-Out in the Global State

To these Recording Options you can add TLP Completions. See Figure 5.100 on page 223.

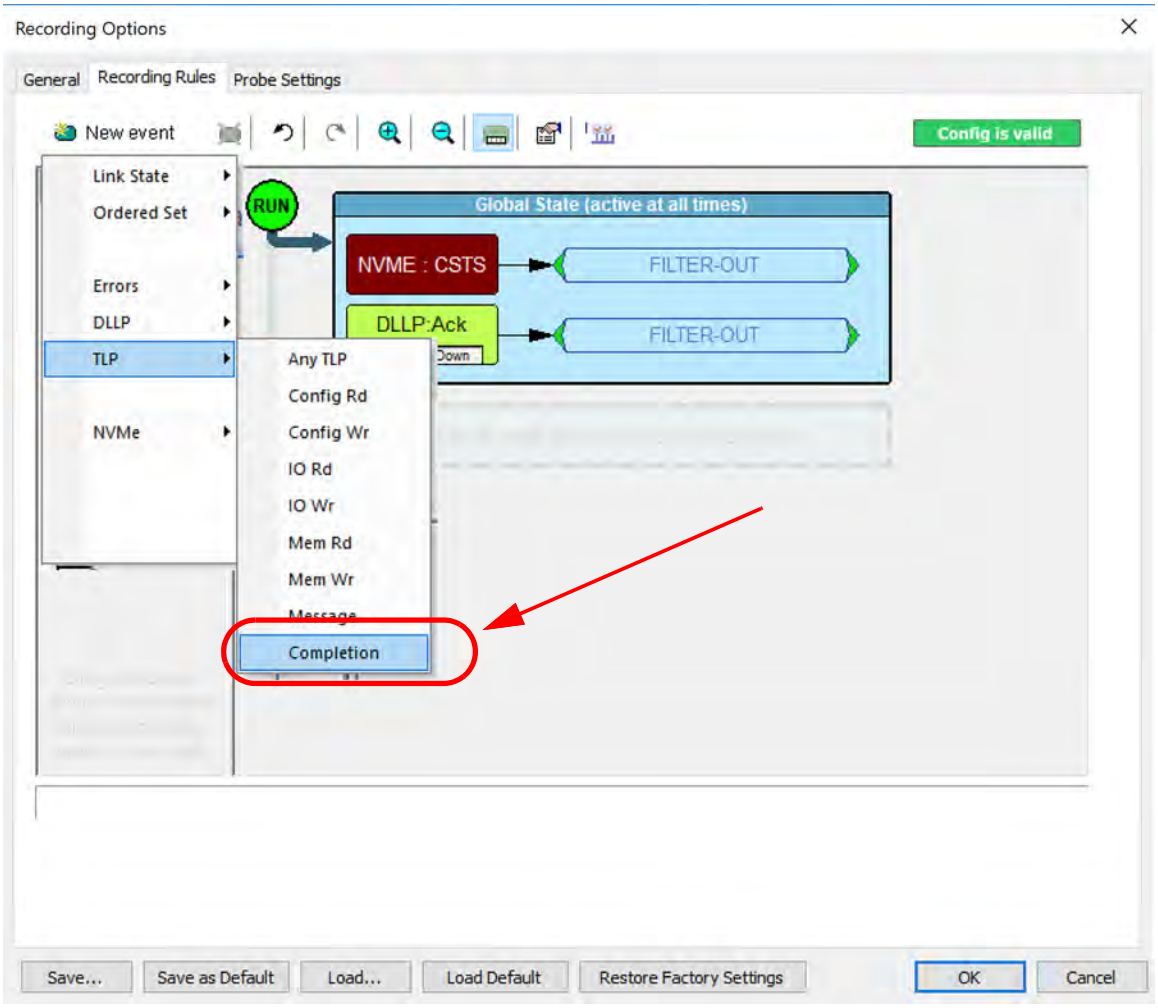


Figure 5.100: Recording Options: NVME, DLLP -> Filtered Out, Add TLP Completion

Then add the TLP Completion Layout Options. Set the Type to Cpl/CplD. See Figure 5.101 on page 224.

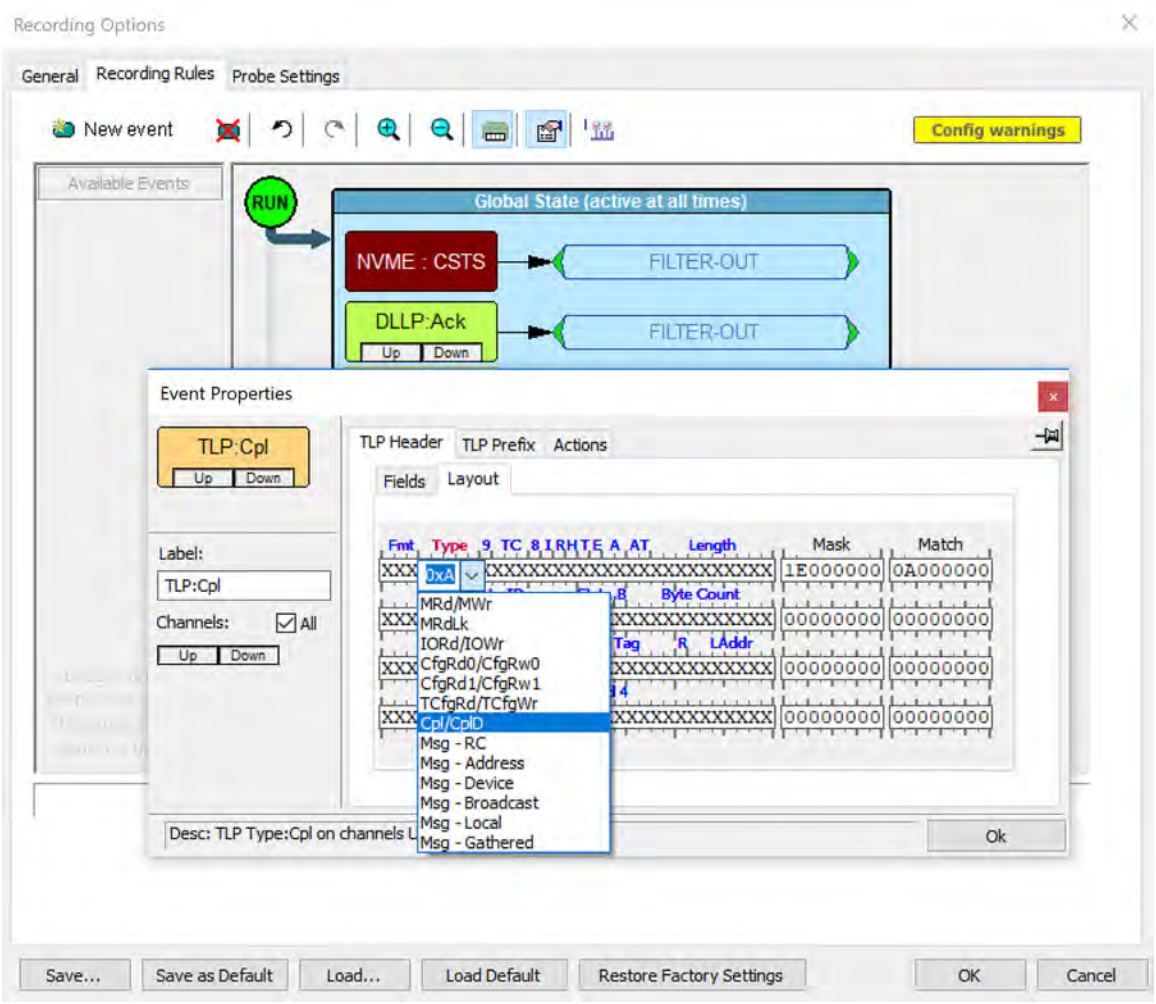


Figure 5.101: Recording Options: TLP:Cpl -> Select CPl/CplD

Next set the LAddr Layout Option to 0x1C. See Figure 5.102 on page 225

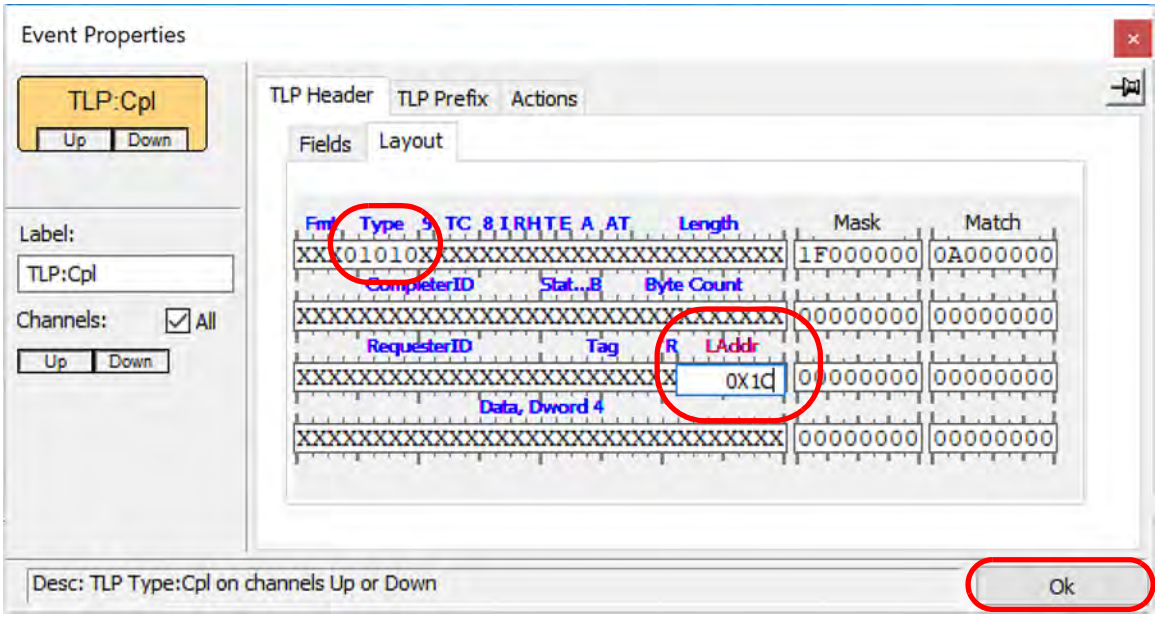


Figure 5.102: Recording Options: TLP:Cpl -> Layout Type: 01010, LAddr: 0x1C

This will set the Mask to 7F and the Match to 1C. See Figure 5.103.

Click on “OK” and then set the Action to Filter-Out.

See Figure 5.103 on page 226.

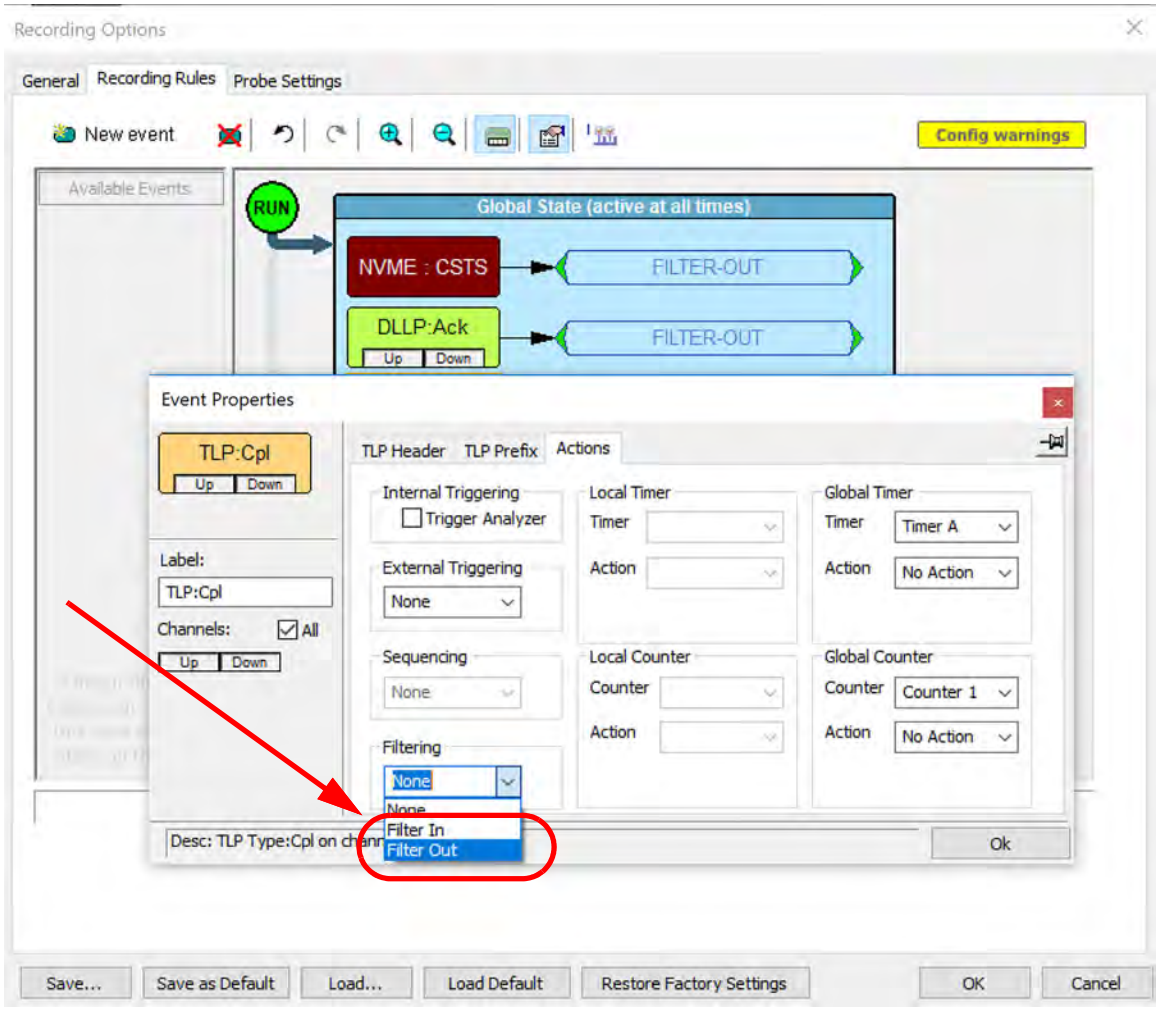


Figure 5.103: TLP:Cpl -> Actions: Filter-Out

Add this property to the Global State. See Figure 5.104 on page 227.

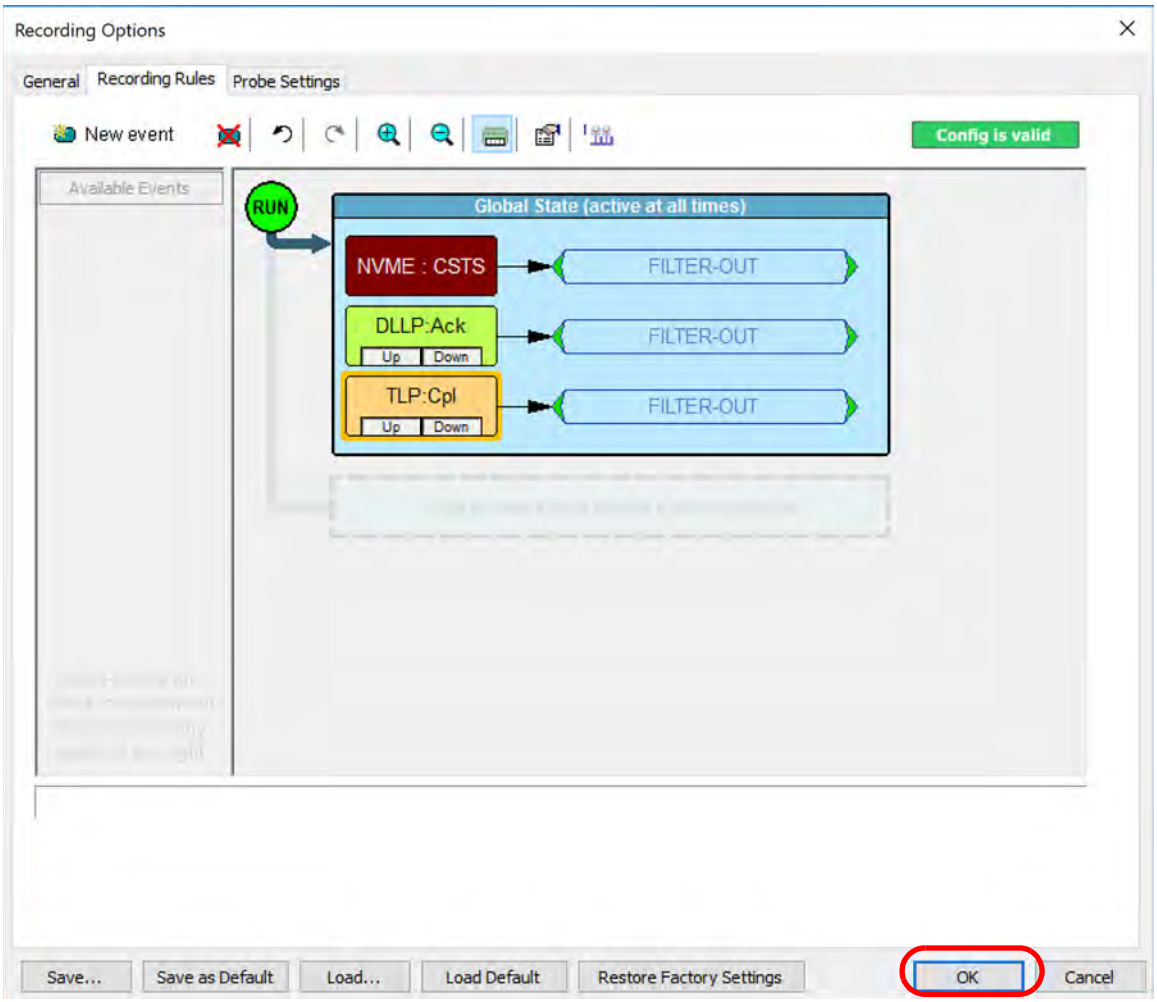


Figure 5.104: Recording Options: NVME, DLLP and TLP all Filtered-Out

Click on “OK” and these Properties will all be Filtered Out of the recording.

5.20.15 Triggering Configuration on a per Lane Basis

The Lane Trigger Configuration Icon (available on the Recording Options => Recording Rules toolbar see Figure 5.105) provides the user with the ability to add pre-conditions on specific lanes that the analyzer will use as an additional restriction on a defined triggering event.

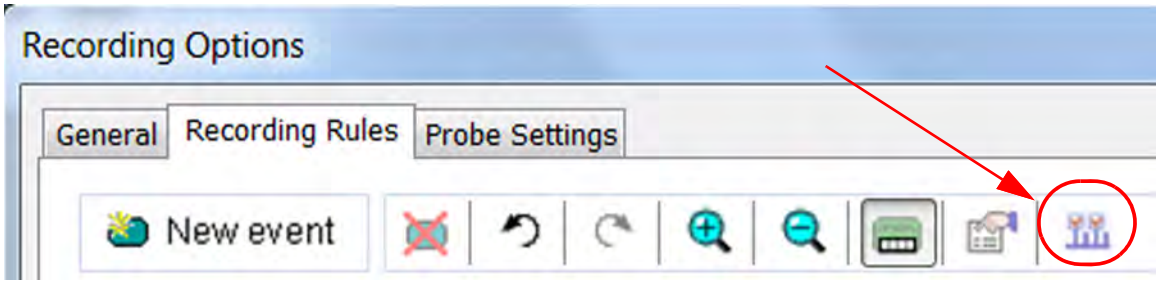


Figure 5.105: Lane Trigger Configuration

This option has three categories of events which can be made lane-based:

- DLLP/TLP Packets
- Errors
- Ordered Sets

Each of these events has restrictions on the lanes available, as spelled out in the GUI.

- These selections will be applied globally
- Lane selections will be applied to logical lane(s) and NOT physical lane(s)
- Default is “all Lanes”, but you can select one or more lanes as targets
- Filter-in/out will not function is you are using per lane triggering

5.20.15.1 DLLP/TLP Packets Category

For DLLP/TLP packets starting in selected lanes, the packet must start in lanes 0, 4, 8 or 12. One or more of these four lanes can be selected to look for the start of DLLP/TLP packets and the selection can be made for each direction by checking boxes.

See Figure 5.106.

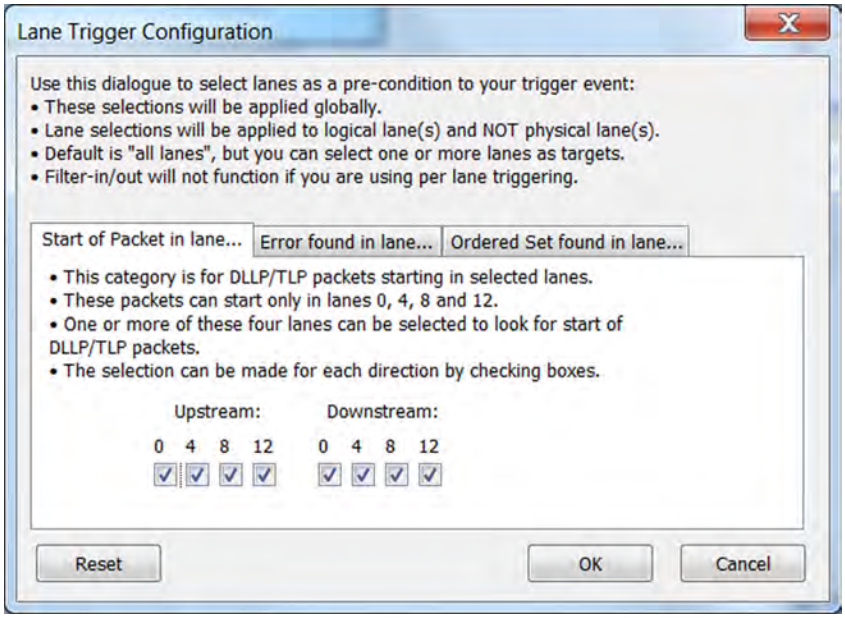


Figure 5.106: Start of Packet in lane GUI

5.20.15.2 Errors Category

Errors category can be used as a pre-condition to trigger on an event in selected Upstream or Downstream lanes. The types of errors that will be detected are limited to:

- Symbol errors
- Disparity errors
- Block errors

See Figure 5.107.

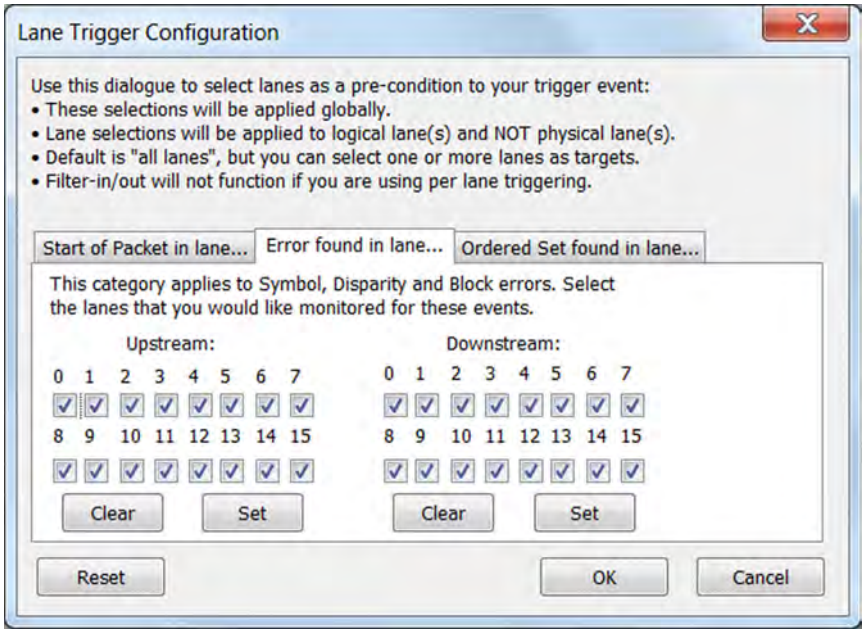


Figure 5.107: Error Found In Selected Lanes

5.20.15.3 Ordered Sets Category

This category includes all types of ordered sets (TS1, TS2, EIEOS, EIOS, Skip, FTS, and SDS).

If a specific lane is selected in the Event Properties dialog of a TS ordered set the same specific lane must be selected here or no triggering event will occur.

See Figure 5.108.

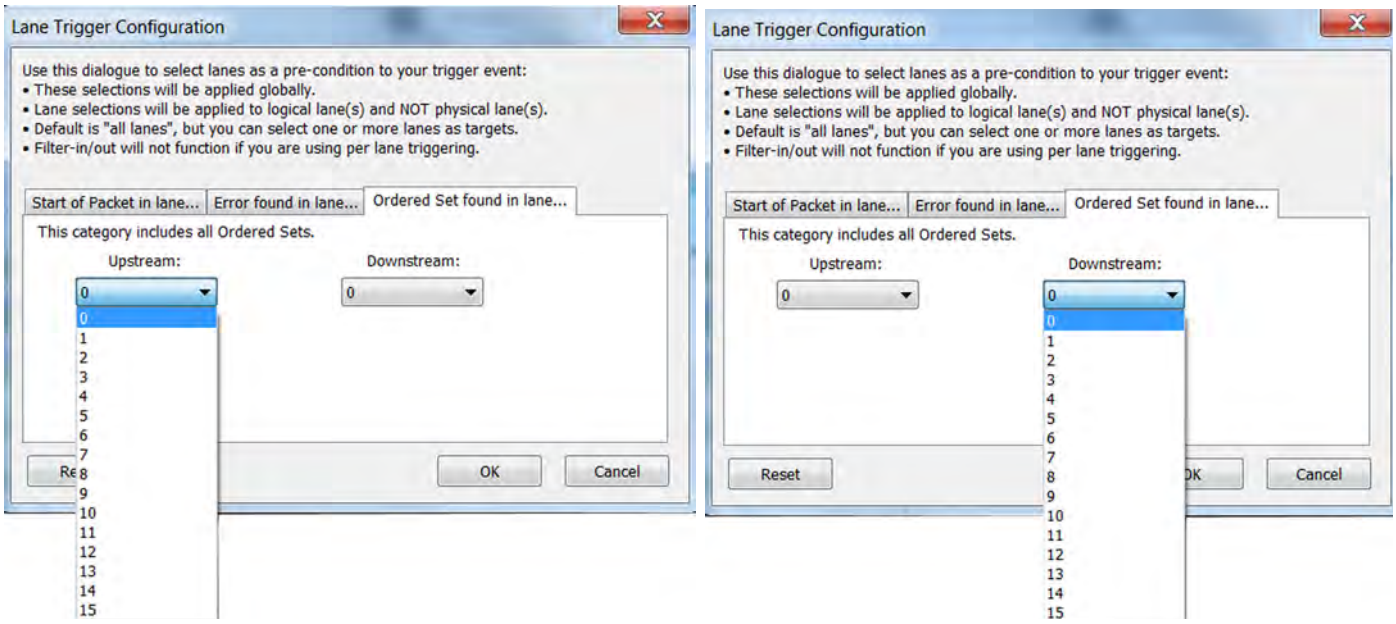


Figure 5.108: Ordered Sets Found in Upstream and Downstream Lanes

5.20.16 Lane Trigger Configuration

5.20.16.1 Example 1:

If you need to trigger on TLPs that start on lane 4 in the upstream direction perform the following selection (see Figure 5.109):

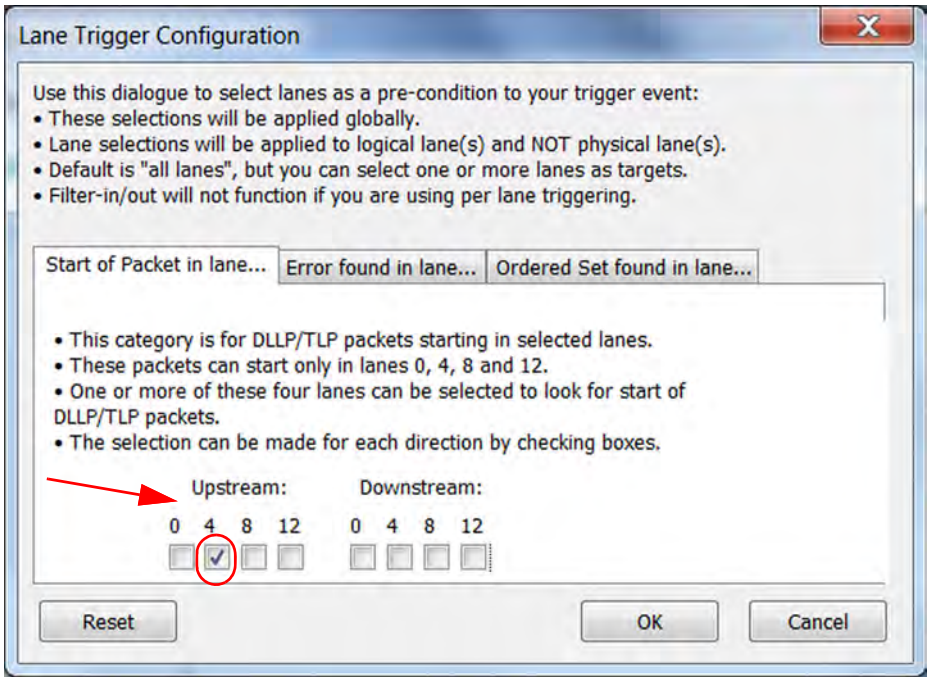


Figure 5.109: Lane Trigger Configuration: Example 1

Then select the appropriate event to trigger the analyzer.

5.20.16.2 Lane Trigger Configuration Example 2:

If you need to trigger the analyzer on errors happening on lanes 4 and 6 in the upstream direction, perform the following selections:

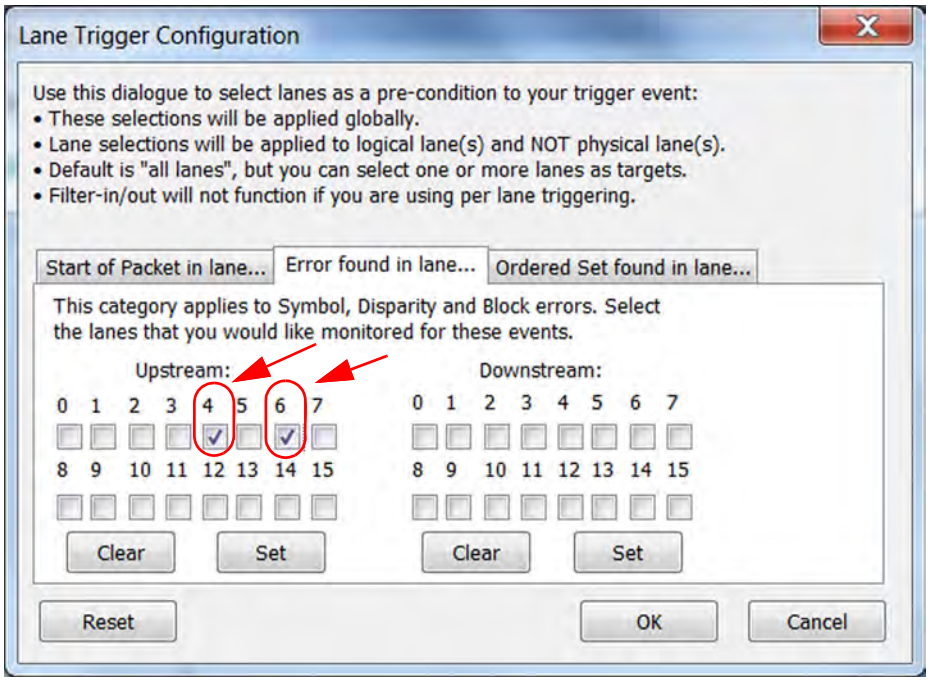


Figure 5.110: Lane Trigger Configuration: Upstream Errors on Lanes 4 and 6

Then select the appropriate event to trigger the analyzer.

5.20.16.3 Lane Trigger Configuration Example 3:

If you need to trigger on a TS1 Event with Link Number = 00 and Lane Number = PAD that happens on Lane 3 only in the Downstream direction, perform the following selections for Lane Triggering (see Figure 5.111):

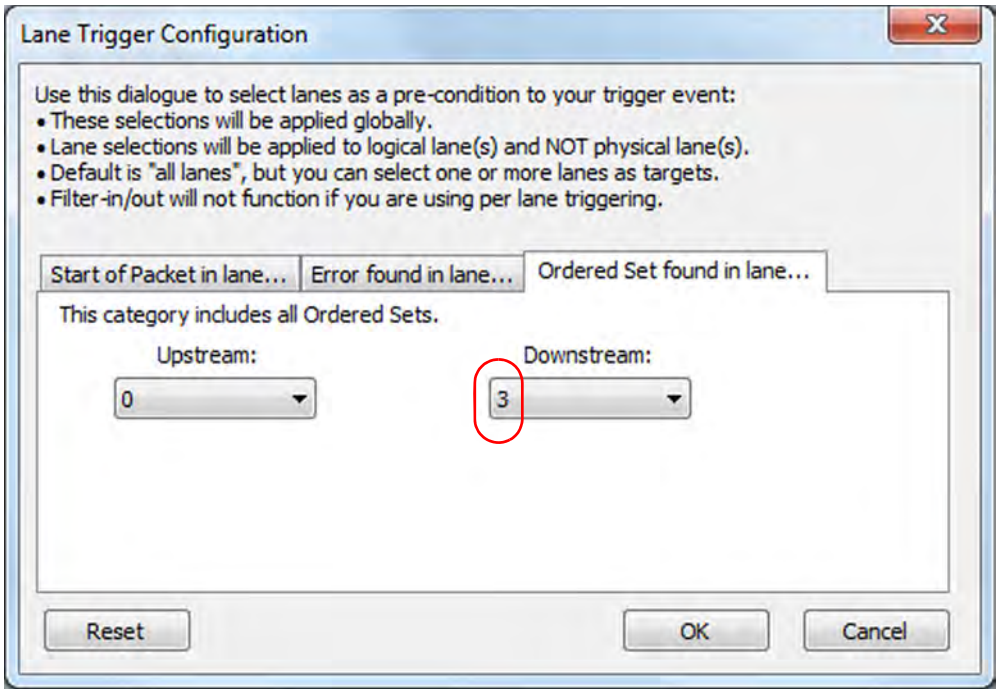


Figure 5.111: Lane Trigger Configuration: Downstream TS1, Downstream, Lane 3

Then select a TS1 Event and select only the Downstream direction, set Link Number = 00 and Lane number = PAD fields (see Figure 5.112). After selecting the options you want click on the “OK” button.

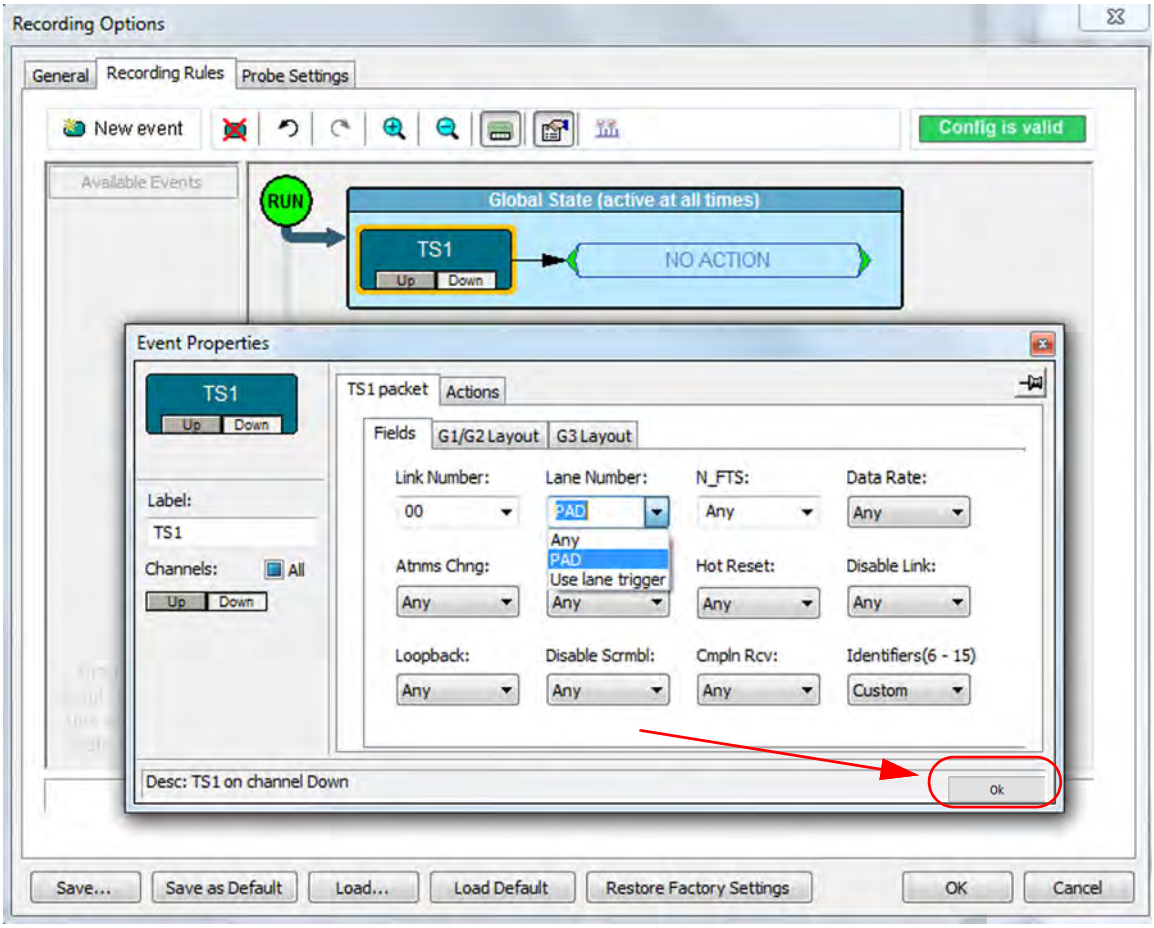


Figure 5.112: Setting the Event Properties for TS1 Downstream

Finally, set the Action Tab to trigger the analyzer (see Figure 5.113 on page 233). After selecting the options you want click on the “OK” button.

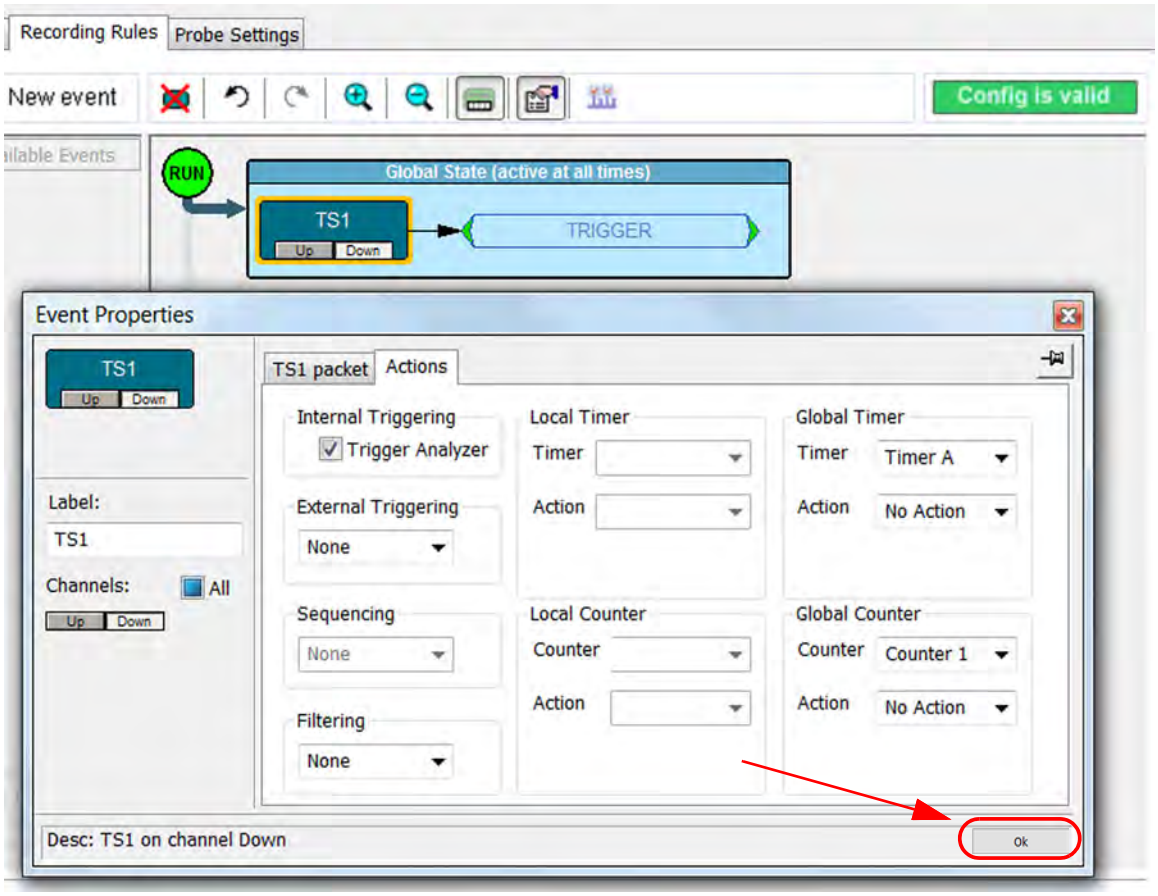


Figure 5.113: Event Properties: Actions = Trigger Analyzer

Now the analyzer will be triggered on a TS1 Event with Link Number = 00 and Lane Number = PAD that happens on Lane 3 only in the Downstream direction.

5.20.17 Counter

Counters can be created for any specific event or for multiple events (see Figure 5.114 on page 234). Counters function similar to an event and are independent of the event, thus allowing greater flexibility. You can select a counter for any event and if both channels are selected you can set the counter to count upstream and downstream. Counters can be reset providing further flexibility. The counter once set lives in the State. In an Advance to Sequence state once the action proceeds from one sequence state to the next, the counter in the preceding state will stop and the counter in the current state will start.

There are two Counters for the Global State and four Counters for the Sequence State.

The counters have different colors for the Global State and Sequence State. Each color signifies a different meaning in the Global and Sequence states.

Note: Counters can be controlled only from one direction not both, meaning starting, reset and incrementing must be done from events occurring in the same channel (upstream or downstream) of the selected counter.

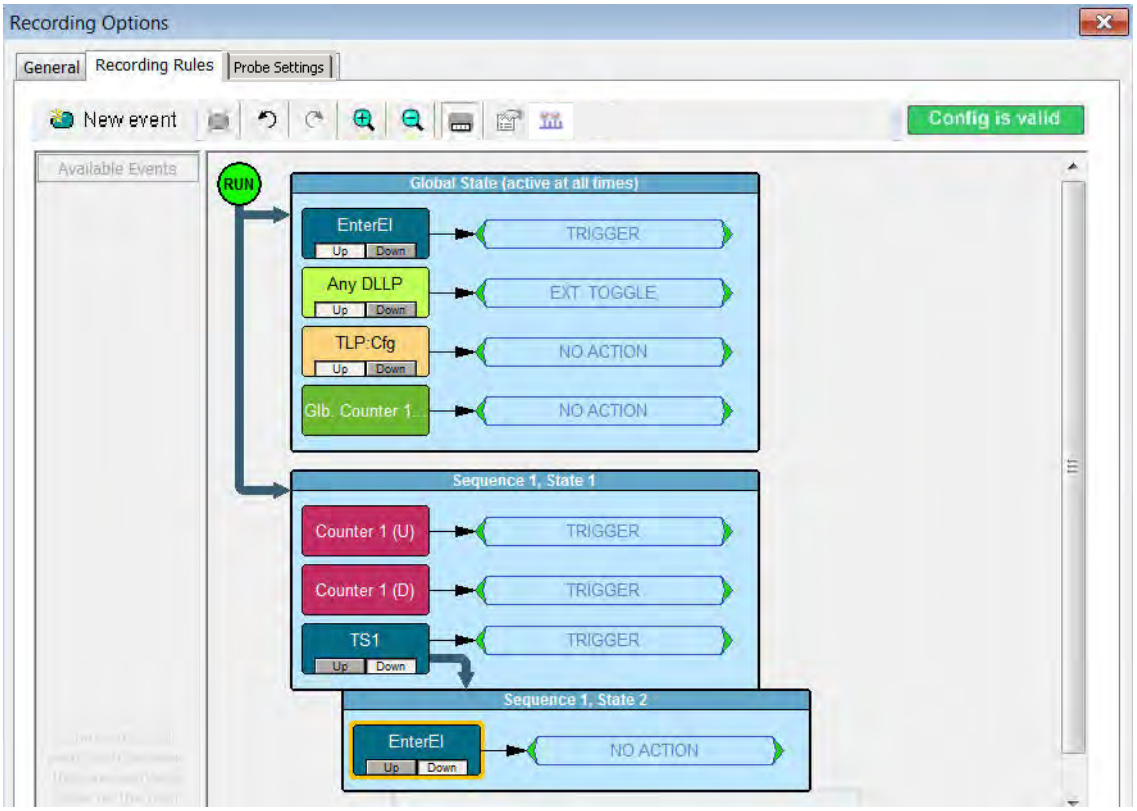


Figure 5.114: Global and Sequence State Counters

As shown in Figure 5.114 there is a Global Counter 1, set to the value of 2 on channel up displayed in green in the Global State and there are two counter 1s, set to the value of 2, one counting upstream and the other counting downstream displayed in pink in the Sequence State.

5.20.17.1 How to Set a Counter

Counters are events and you can add a counter to the Global State or the Sequence State as an event by doing the following:

Right-click in the blue space in the Global or Sequence State and **New Event > Counter > UpStream or DownStream**. See Figure 5.115 on page 235.

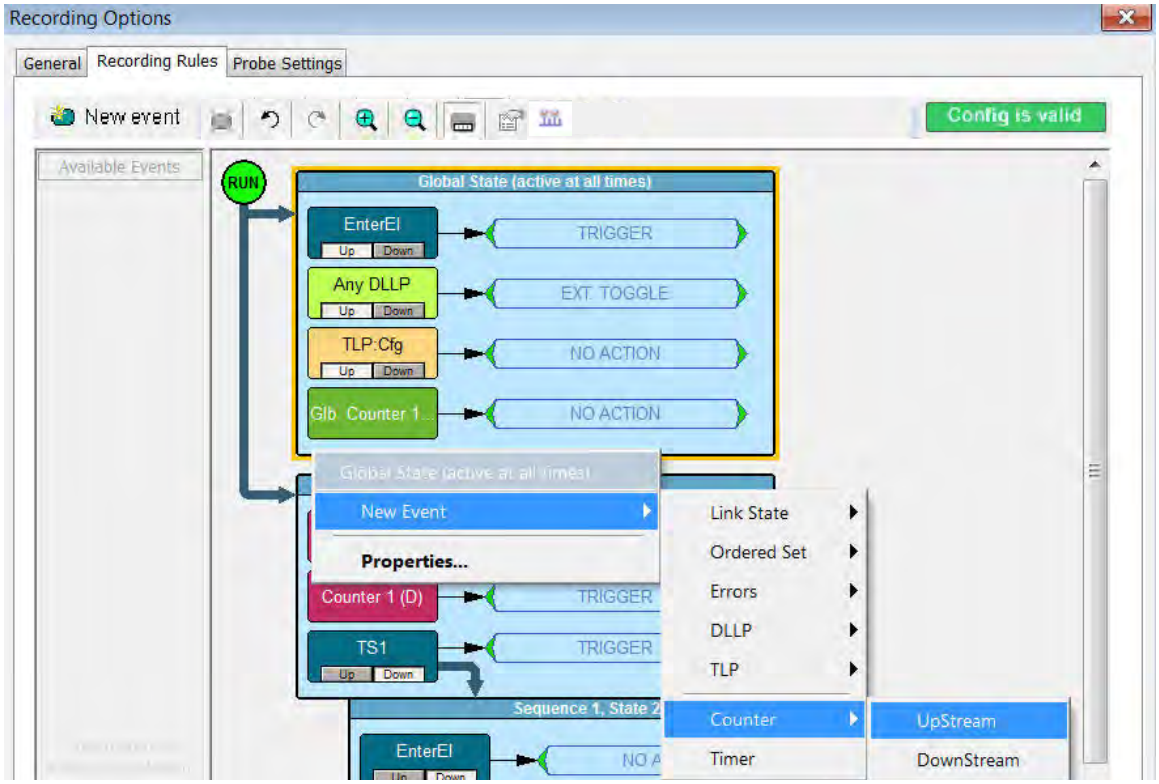


Figure 5.115: Setting Global and Sequence State Counter Events

5.20.17.2 How to Increment or Reset a Counter

You can Increment or Reset counters in the Global State and in the Sequence State by performing the following steps:

1. Open the Recording Rules page, select an event, and drag it to the **Global State** or **Sequence** cells. For details on these steps (see "Events with Channels" on page 242).
2. Right-click on an event and select **Specify Actions > Increment Global Counter > Global Counter 1** from the menu (see Figure 5.116 on page 236).

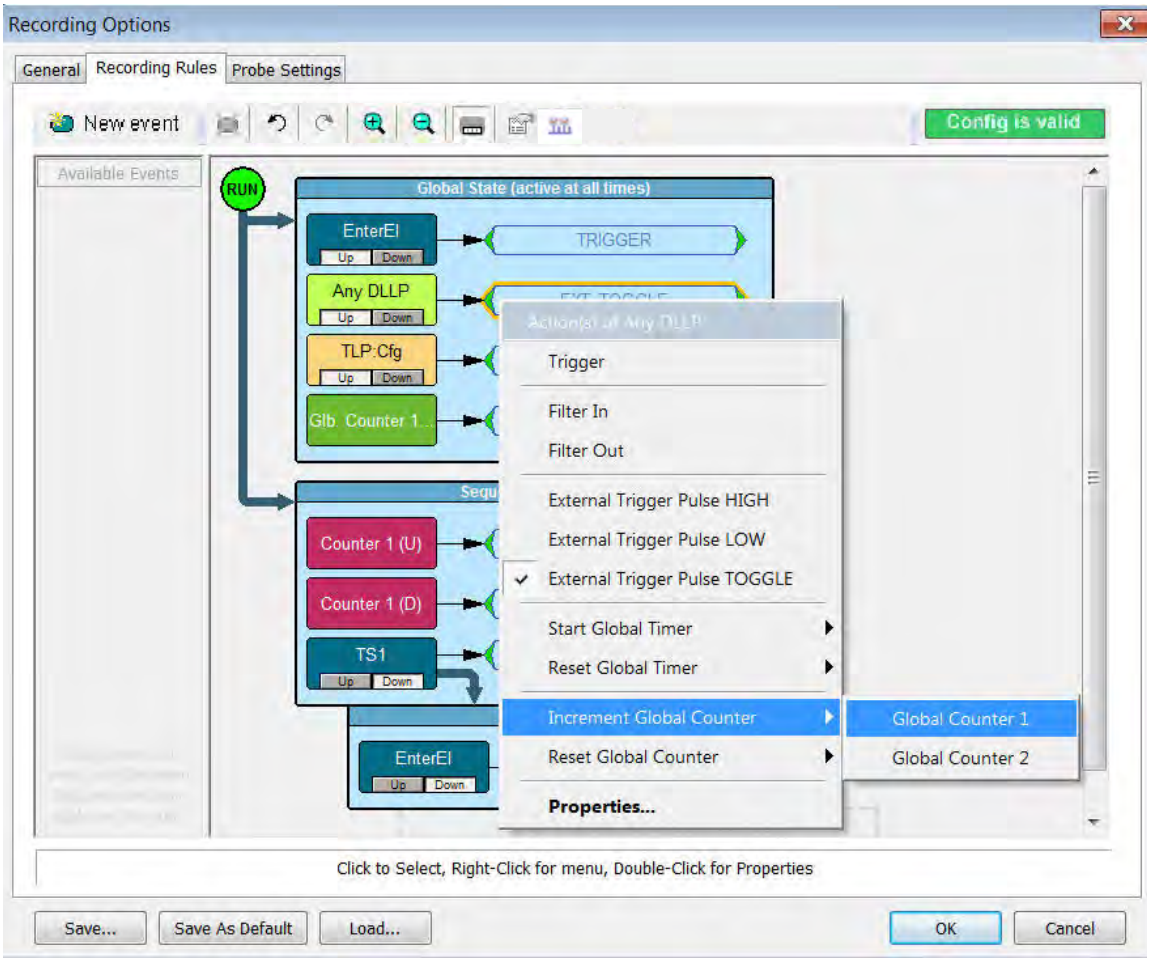


Figure 5.116: Incrementing and Resetting Global and Sequence State Counters

Note: Listed below are some of the considerations to note about the counter functionality.

1. If a counter is reset, it will restore to its original value, in this case the value defined by the user.
2. Resetting a counter will stop it and set it to its original value.
3. Local counters for a particular state will automatically reset if the sequencer advances to another state. Example: "Counter A" in State 1 and "Counter A" in State 2 are different timers not related to each other.
4. Local counters are controlled by events defined in the same state where the counters are defined.
5. In case of competing actions to control global counters using the same event from global and local states, the control from local states takes priority.

5.20.17.3 Changing the Value of the Counter

To change the value of the counter:

1. Double-click on the Counter.
2. Enter a new value in the pop-up dialog. This causes the new value to appear in the counter button.

5.20.17.4 Deleting a Counter

To delete a counter

1. Right-click on the Counter.
2. Select **Delete This Event.** The counter will disappear from the event.

5.20.18 Timer

The Timer has two options which are Start and Reset. When set to Start it starts the timer and when set to Reset it resets the timer to its initial value. When the timer count is down to 0 the action is triggered.

The Global State timer can trigger, start an action. It can also affect some other timers and counters.

The timers have different colors for the Global State and Sequence State. Each color signifies a different meaning in the Global and Sequence states.

There are two Timers for the Global State and four Timers for the Sequence State.

Note: Timers can be controlled (Start/Reset) deterministically from events happening in any channel (upstream or downstream direction) as long as these events are more than 380 ns apart. For timers controlled by events happening on a single direction the control happens at the line rate.

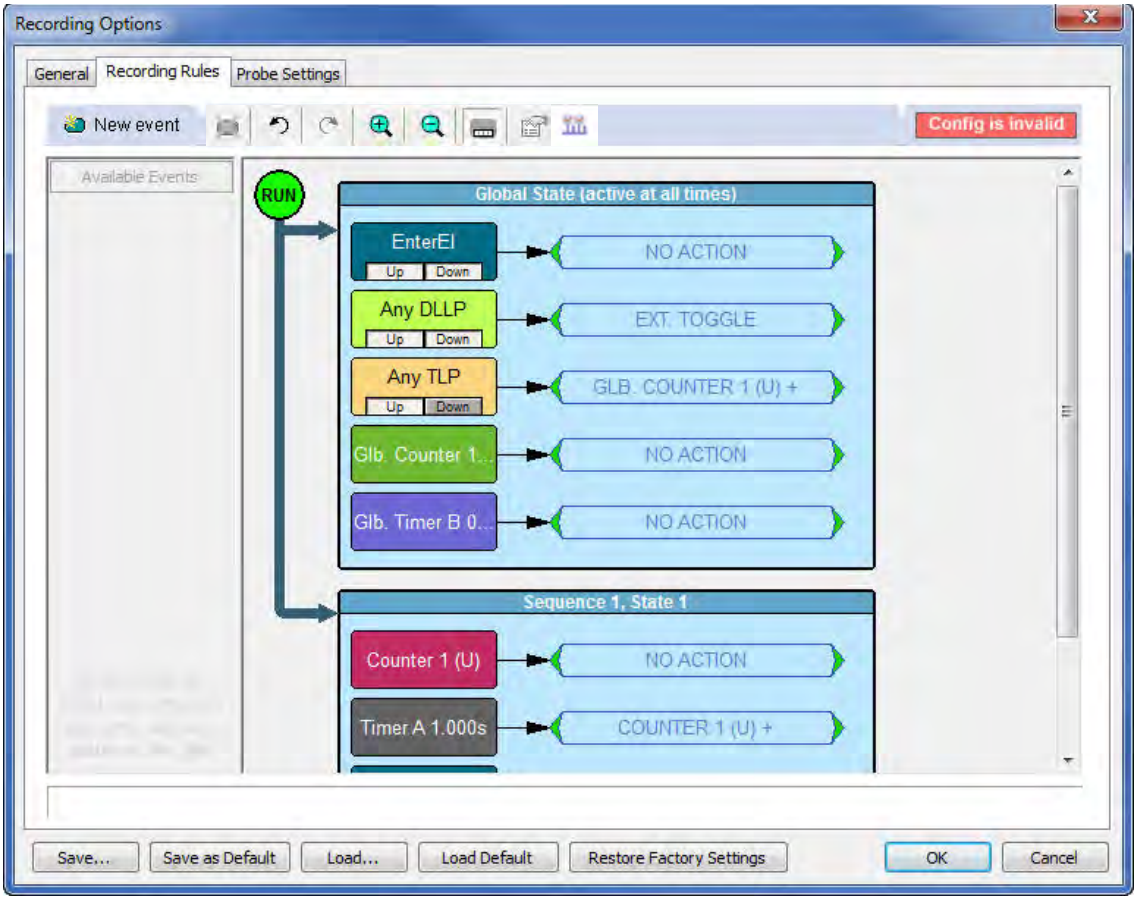


Figure 5.117: Global and Sequence State Timers

As shown in Figure 5.117 on page 238 there is a Global Timer A, set to the value of 1.000s on channel Up displayed in blue in the Global State and there is one timer A, set to the value of 1.000s on channel Down displayed in brown in the Sequence State.

5.20.18.1 How to Set a Timer

Timers are events and you can add a timer to the Global State or the Sequence State as an event by doing the following:

Right-click in the blue space in the Global or Sequence State and **New Event > Timer**.

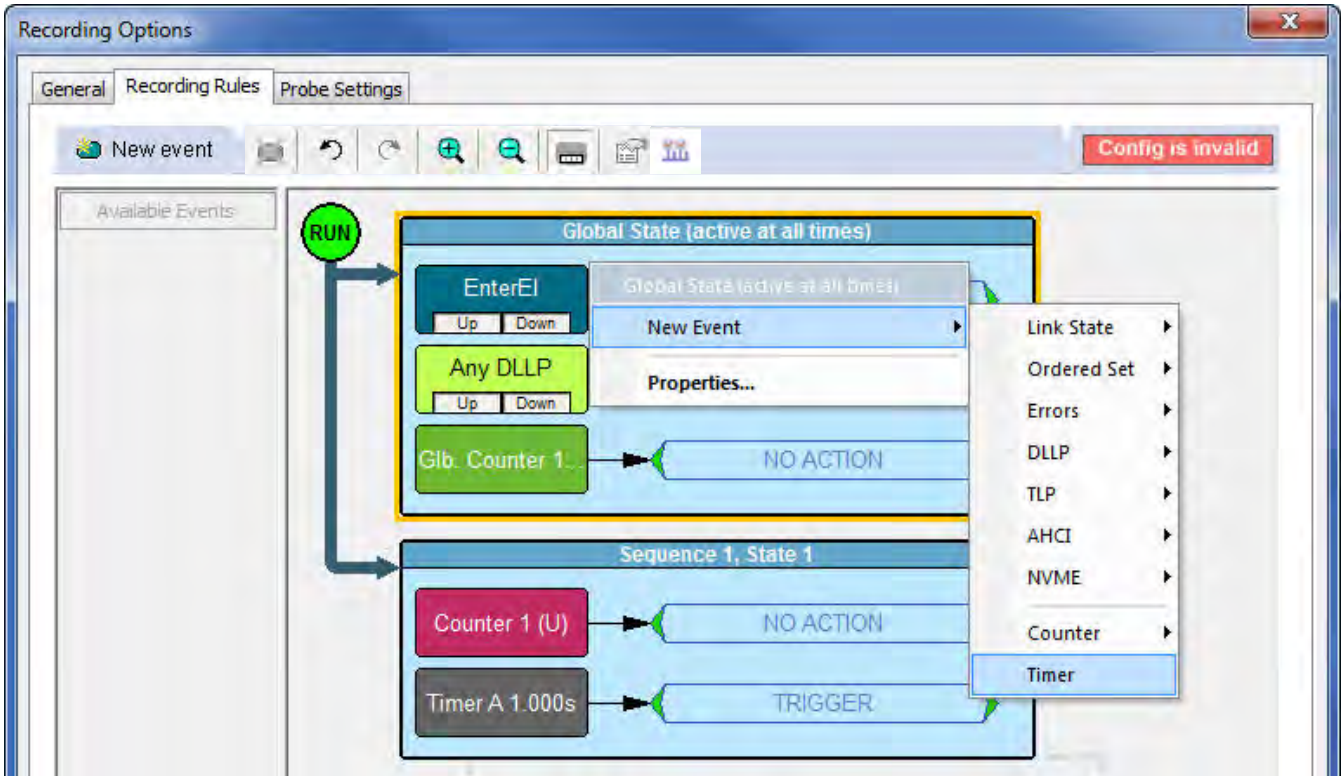


Figure 5.118: Setting Global and Sequence State Timer Events

5.20.18.2 How to Start or Reset a Timer

You can Start or Reset the Timer in the Global State and in the Sequence State by performing the following steps:

1. Open the Recording Rules page, select an event, and drag it to the **Global State** or **Sequence** cells. For details on these steps (see “Events with Channels” on page 242).
2. Right-click on an event and select **Specify Actions > Start Global Timer > Global Timer A** or **Timer B** from the menu (see Figure 5.119 on page 240).

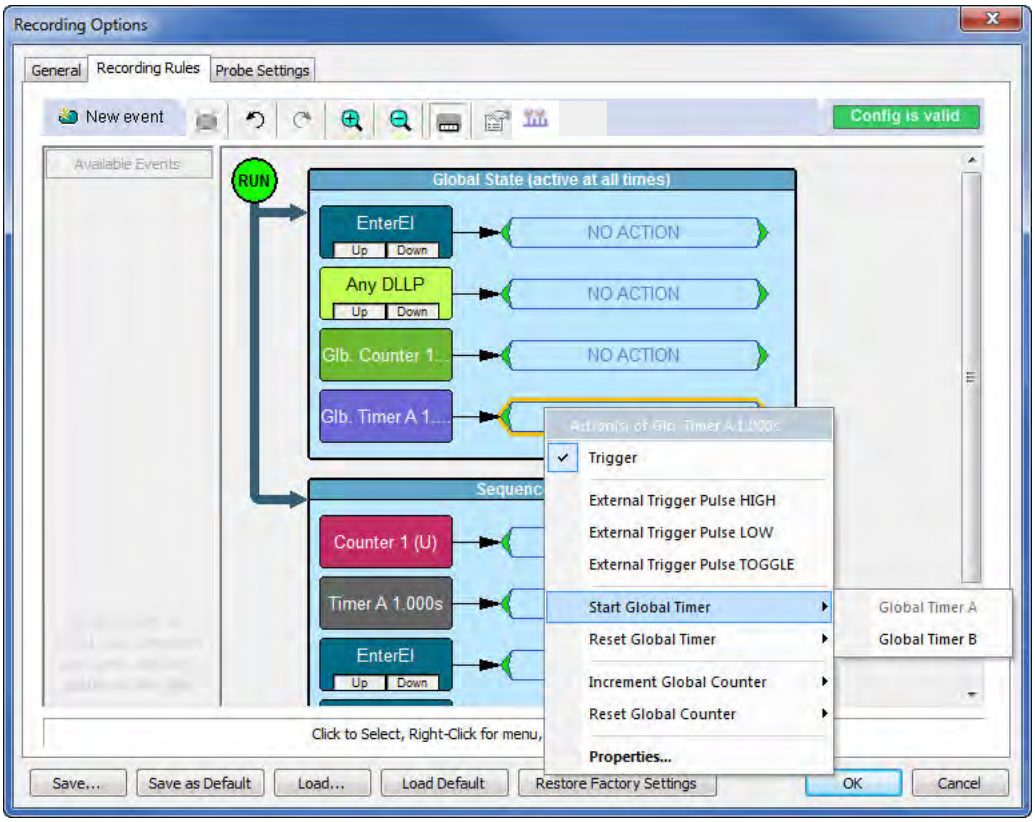


Figure 5.119: Starting and Resetting Global and Sequence State Timers

Note: Listed below are some of the considerations to note about timer functionality.

1. If a timer is reset, it will restore to it's original value, in this case the value defined by the user.
2. Resetting a timer will stop it and set it to it's original value.
3. Local timers for a particular state will automatically reset if the sequencer advances to another state. Example: "Timer A" in State 1 and "Timer A" in State 2 are different timers not related to each other.
4. Local timers are controlled by events defined in the same state where the timers are defined.
5. In case of competing actions to control global timers using the same event from global and local states, the control from local states takes priority.

5.20.18.3 Changing the Value of the Timer

To change the value of the timer (see Figure 5.120 on page 241):

1. Right-click on the Timer.
2. Select **Properties**

3. Enter in values for the Timer in the fields provides in Secs, Millisecs, Microsecs and Nanosecs on the Timer tab. After selecting the options you want click on the “OK” button.

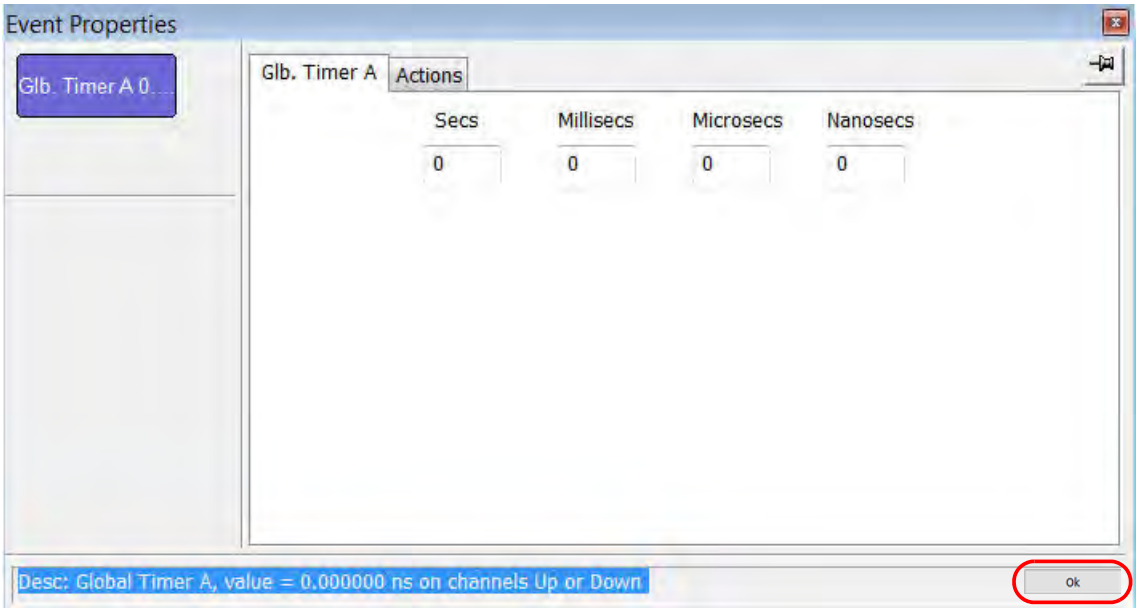


Figure 5.120: Setting the Timer Values

4. Click on the Actions tab and set the External and Internal Triggering, Sequencing and Filtering options. You can label the timer.

5.20.18.4 Deleting a Timer

To delete a Timer

1. Right-click on the Timer.
2. Select **Delete This Event.** The Timer will disappear from the event.

5.20.19 Channel

Every event has two channels, one upstream and the other downstream. You can use both channels with any event. The channels are independent of each other. If both channels are selected it is valid but no action occurs, and thus no timer and counter is created. Figure 5.121 shows three events in the Global State, the first event is on Channel Up and the 3rd event is on Channel Down.

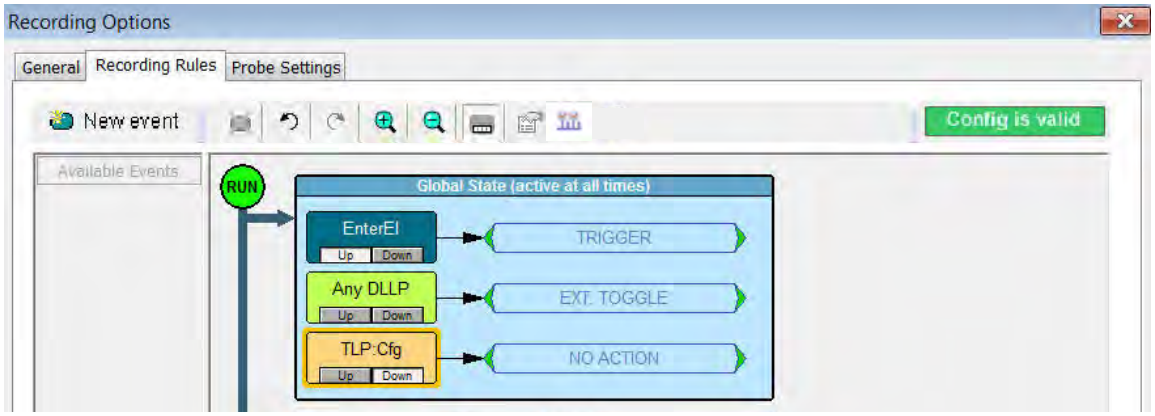


Figure 5.121: Events with Channels

5.20.20 Lane Margining

You can use Lane Margining as an Advanced Recording Rule. You need to define the following Fields:

- Margin Command
- Margin Type
- Receiver Name
- Margin Payload

See Figure 5.122 on page 243.

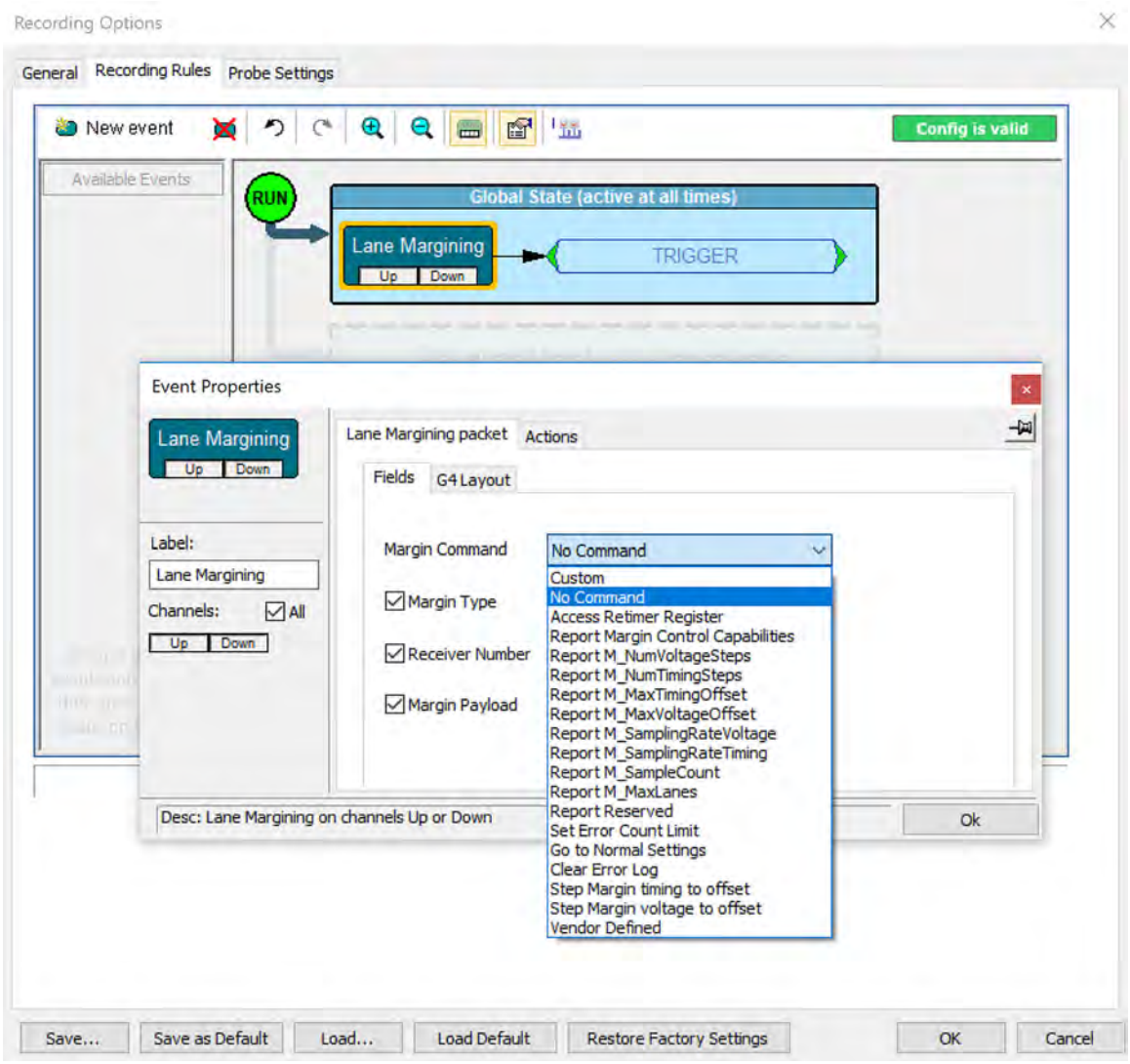


Figure 5.122: Lane Margining: Fields -> Margin Commands

You can also update the four DWORDS in the G4 Layout dialog box.See Figure 5.123 on page 244.

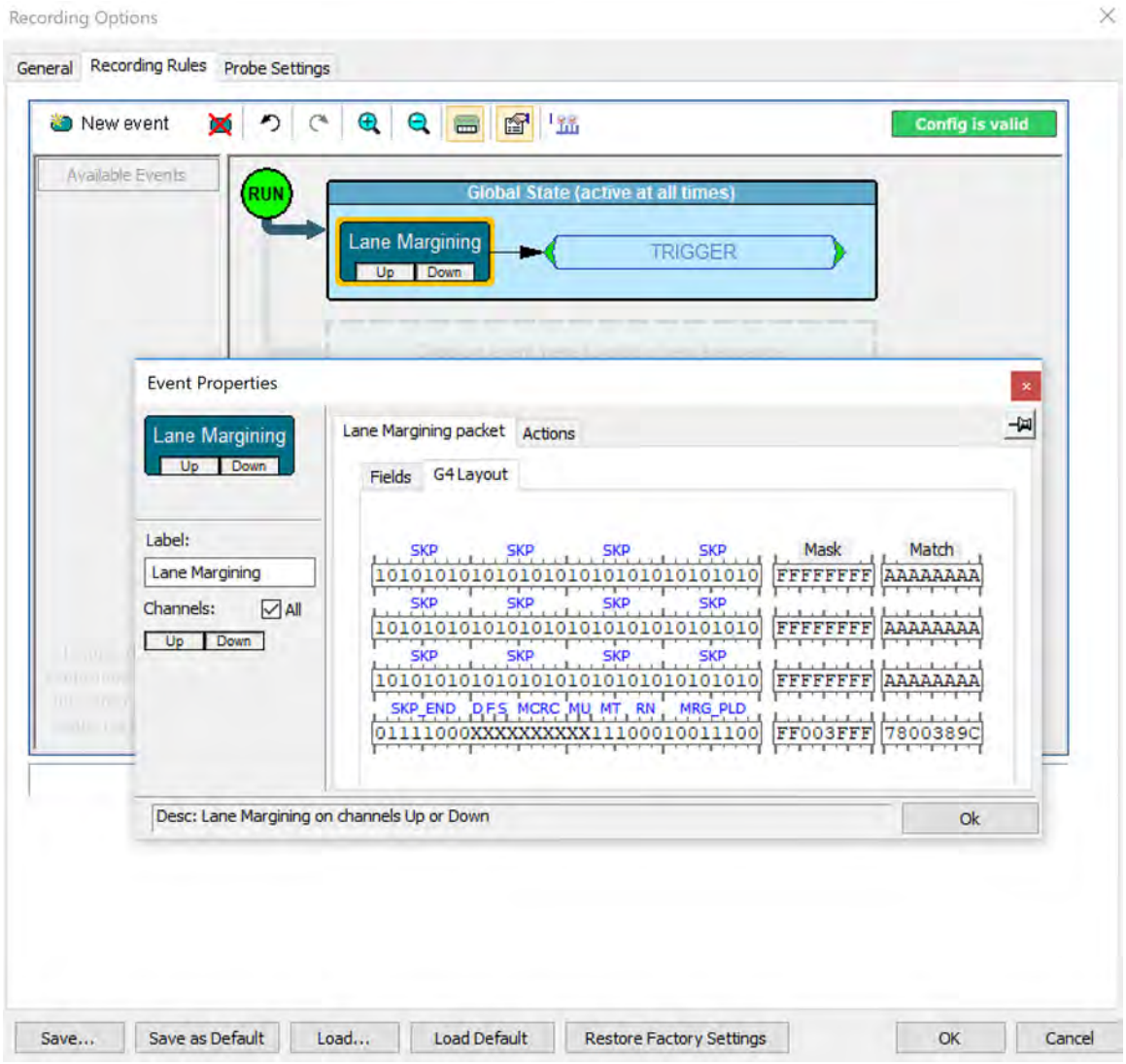


Figure 5.123: Four DWORDS Need to Define G4 Layout

5.21 Triggering On (Advanced Mode)

The General Settings for Advanced Mode Event Trigger are shown below (see Figure 5.124). The settings are the same for the Summit M5x.

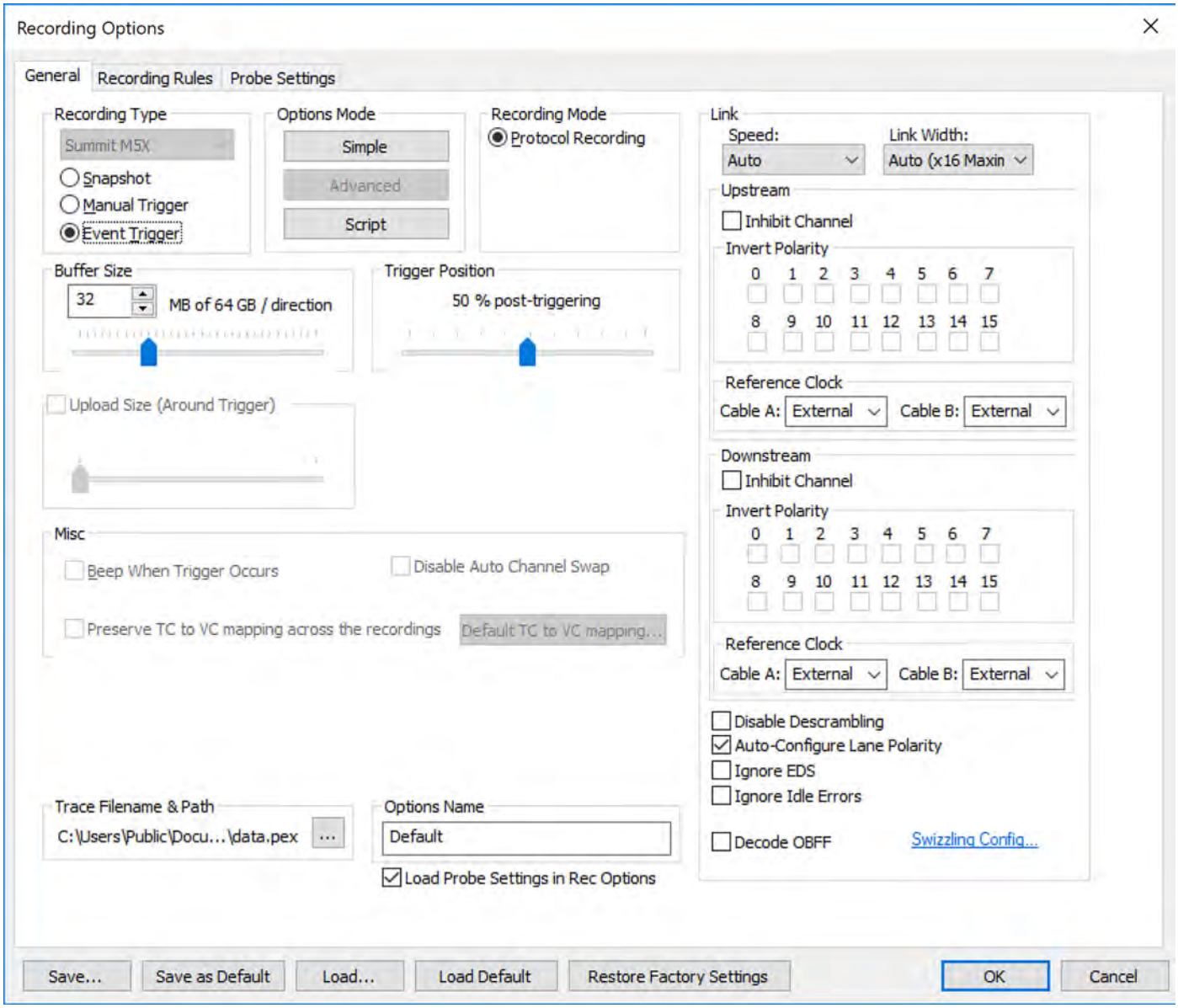


Figure 5.124: Advanced Mode Options: General

In Advanced Mode the General Recording Options are very similar to the Simple Mode General Recording options (see Figure 5.2 on page 134) except that the Triggers/Filters Options are part of the Recording Rules tab (see Figure 5.125 on page 246).

Note:
- The external trigger is ORed with any other trigger defined in the sequencer.
- External Input Trigger is not configurable, it will always cause the analyzer to trigger on a toggle when using manual trigger or triggering on any event.

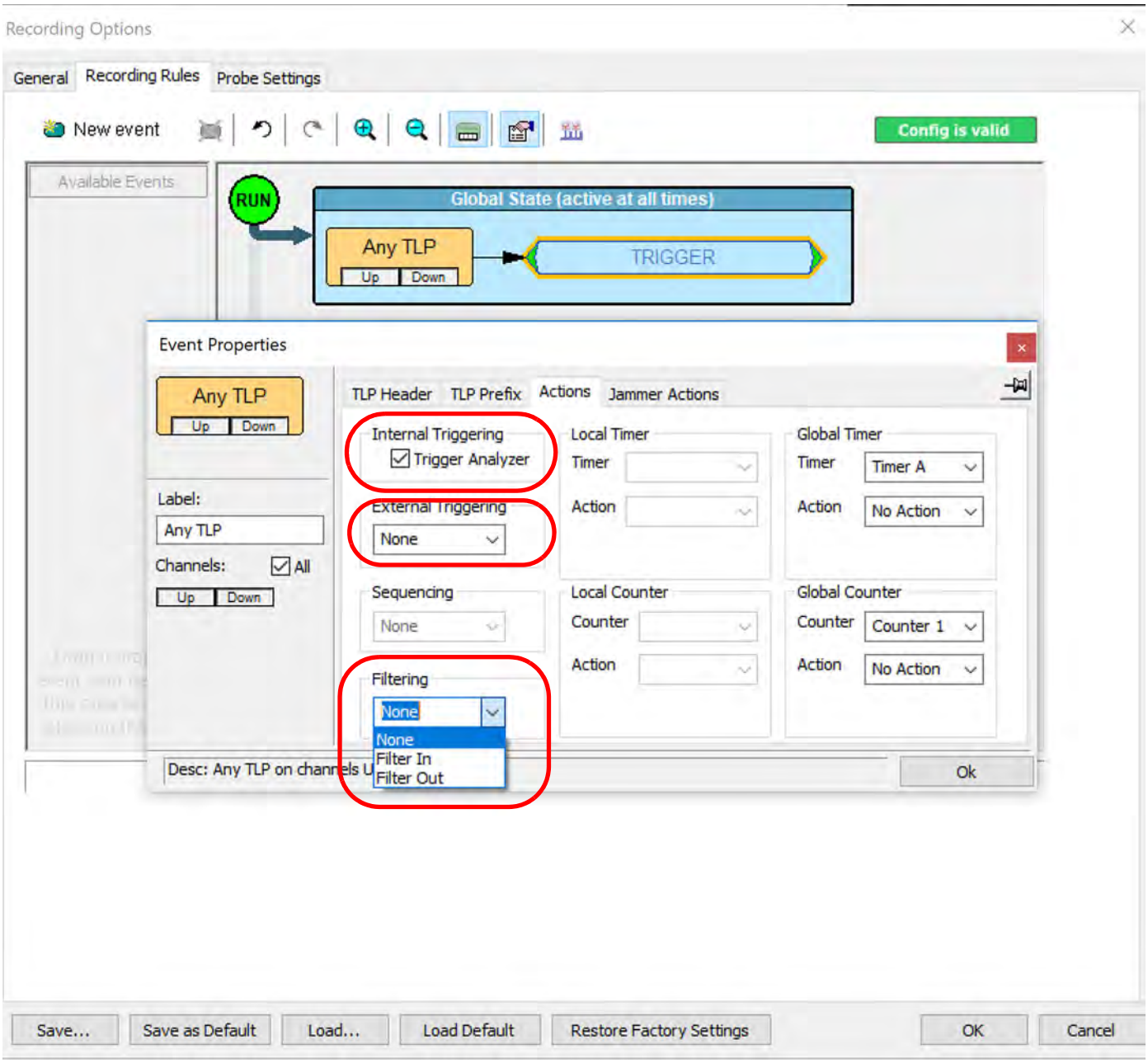


Figure 5.125: Advanced Mode: Recording Rules: Triggers/Filters

5.21.1 Triggering On (Advanced Mode)

5.21.1.1 Selecting Triggers/Filters to be Active

You can select any of the Triggers/Filteres shown in Figure 5.125 on page 246 and move then into the Selected (Active) Triggers/Filters window by clicking on the “>>” symbol. You remove them from the Selected (Active) Triggers/Filters window by selecting one and clicking on the “<<“ symbol:

- TLP
- DLLP

- Ordered Set
- Link State
- Errors

5.21.1.2 Selected Items Settings

You can choose from the following Selected Items Settings to be part of the Trigger/Filter:

- Channel
  - Up
  - Down
- Speed
  - Gen1
  - Gen2
  - Gen3
  - Gen4
- Action
  - Trigger
  - Filter Out
  - External Trigger

5.21.1.3 Direction

- Upstream or
- Downstream or
- Both

Speed Switch (GT/s):

Trigger Speed

- From:
  - Any
  - 2.5
  - 5.0
  - 8.0
  - 16.0
- To
  - 16.0
  - 8.0
  - 5.0
  - 2.5
  - Any

Linkwidth Change

Trigger Width

- From:
  - Any

- x1
- x2
- x4
- x8
- x16

❑ To

- x16
- x8
- x4
- x2
- x1
- Any

Note:
- Trigger Position slider becomes enabled only when Recording Type is set to Manual Trigger or Event Trigger.
- If you check 2 or more boxes the triggering will occur based on an OR condition, not AND condition.

External Input Trigger is not configurable, it will always cause the analyzer to trigger on a toggle when using manual trigger or triggering on any event.

5.22 Recording Options for Compute Express Link (CXL) Mode

Compute Express Link™ (CXL™) is a high-speed CPU-to-Device and CPU-to-Memory interconnect designed to accelerate next-generation data center performance. CXL technology maintains memory coherency between the CPU memory space and memory on attached devices, which allows resource sharing for higher performance, reduced software stack complexity, and lower overall system cost. This permits users to simply focus on target workloads as opposed to the redundant memory management hardware in their accelerators.

CXL is designed to be an industry open standard interface for high-speed communications, as accelerators are increasingly used to complement CPUs in support of emerging applications such as Artificial Intelligence and Machine Learning. The Summit M5x Analyzer is fully capable of recording and decoding CXL configurations.

To record in CXL mode you must first select the Summit M5x Analyzer (CXL) from the Recording Type option and Event Trigger. See Figure 5.126.

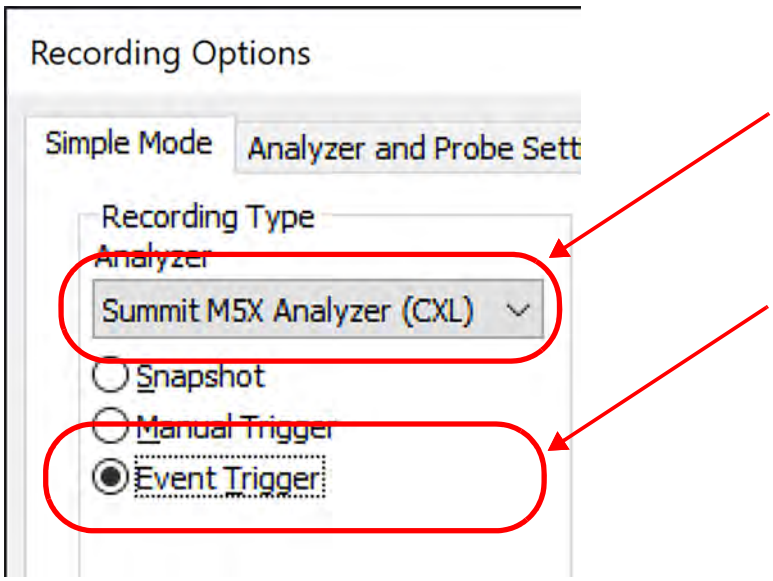


Figure 5.126: Recording Type: Summit M5x Analyzer (CXL) with Event Trigger selected

Selecting these options will bring up all the CXL options to select from. See Figure 5.127 on page 249.

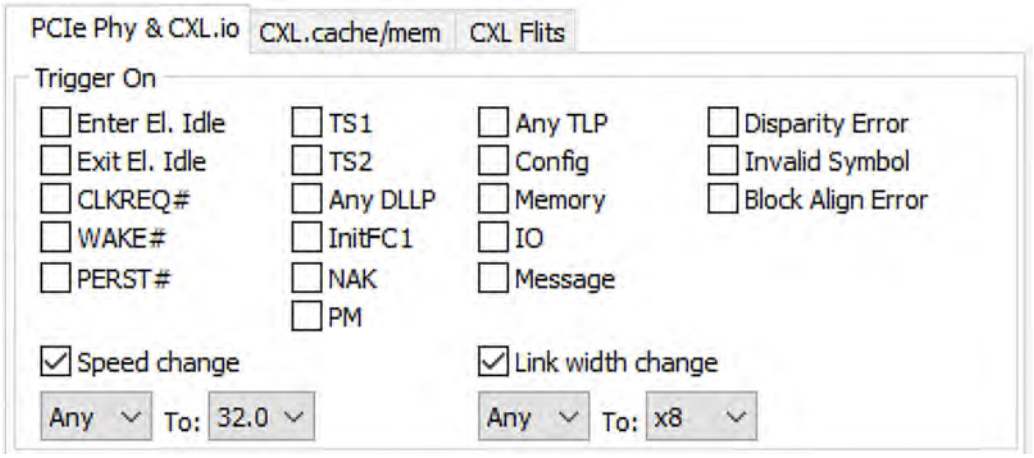


Figure 5.127: CXL Trigger Event Options

5.22.1 Triggering On (Simple Mode): PCIe Phy & CXL.io

You can check any of the boxes shown in Table 5.6 for Trigger On in Simple Mode (see Figure 5.127 on page 249).

TABLE 5.6: Simple Mode Trigger On Events (Upstream or Downstream)

Enter Elec Idle	Any TLP
Exit Idle	Config
CLKREQ#	Memory
WAKE#	IO
PERST#	Message

TABLE 5.6: Simple Mode Trigger On Events (Upstream or Downstream)

TS1	Disparity Error
TS2	Invalid Symbol
Any DLLP	Block Align Error
InitFC1	
NAK	
PM	
Speed Change: Any, 2.5, 5.0. 8.0, 16.0, 32.0 To: Any, 2.5, 5.0, 8.0, 16.0, 32.0	Link Width Change: Any, x1, x2, x4 or x8 To: Any, x1, x2, x4 or x8

Note:
- Trigger Position slider becomes enabled only when Recording Type is set to Manual Trigger or Event Trigger.
- If you check 2 or more boxes the triggering will occur based on an OR condition, not AND condition.
- External Input Trigger is not configurable, it will always cause the analyzer to trigger on a toggle when using manual trigger or triggering on any event.

5.22.2 Trigger On CXL.cache/mem

You can also trigger on CXL.cache/memory events as shown in Figure 5.128.

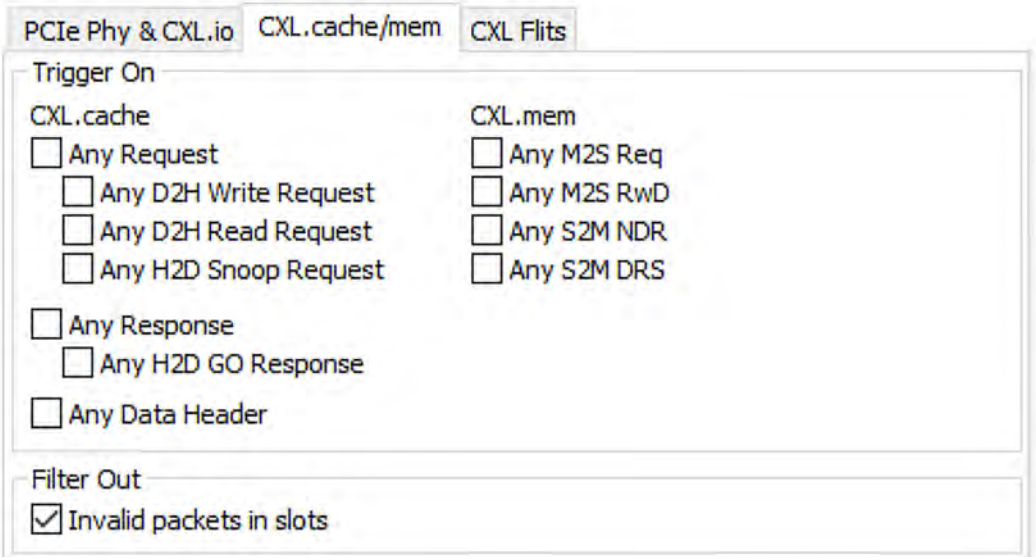


Figure 5.128: Trigger On CXL.cache/memory events

TABLE 5.7: Simple Mode Trigger On Events (CXL.cache/memory)

CXL.cache	CXL.memory
Any Request	Any M2S Req
Any D2H Write Request	Any M2S RwD
Any D2H read Request	Any S2M NDR
Any H2D Snoop Request	Any S2M DRS
Any Response	
Any H2D GO Response	
Any Data Header	

5.22.3 Trigger On CXL Flits

You can also trigger on CXL Flits. See Figure 5.129.

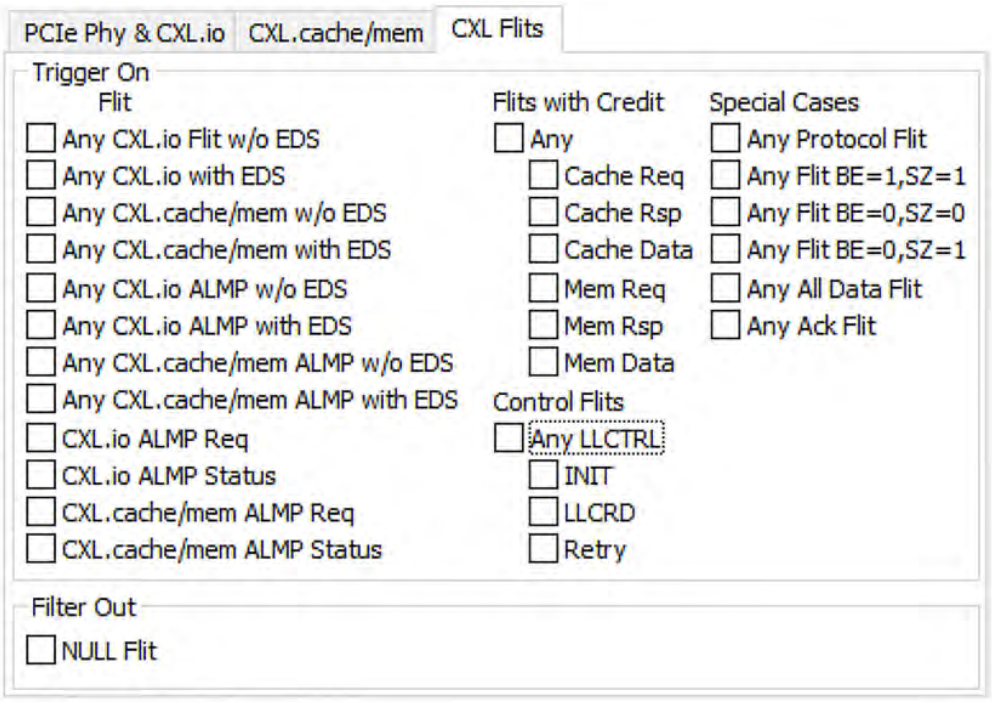


Figure 5.129: Trigger On CXL Flits

The options can also be seen in Table 5.8.

TABLE 5.8: Simple Mode Trigger On Events (CXL Flits)

Flits	Flits with credit	Special Cases
Any CXL.io Flit w/o EDS	Any	Any Protocol Flit
Any CXL.io with EDS	Cache Req	Any Flit BE = 1, SZ = 1
Any CXL.cache/mem w/o EDS	Cache Rsp	Any Flit BE = 0, SZ = 0
Any CXL.cache/mem with EDS	Cache Data	Any Flit BE = 0, SZ = 1

TABLE 5.8: Simple Mode Trigger On Events (CXL Flits)

Any CXL.io ALMP w/o EDS	Mem Req	Any All Data Flit
Any CXL.io ALMP with EDS	Mem Rsp	Any Ack Flit
Any CXL.cache/mem ALMP w/o EDS	Mem Data	
Any CXL.cache/mem ALMP with EDS	Control Flits	
Any CXL.io ALMP Req	Any LLCTRL	
Any CXL.io ALMP Status	INIT	
Any CXL.cache/mem ALMP Req	LLCRD	
Any CXL.cache/mem ALMP Status	Retry	

5.22.4 CXL: Filter Out for PCIe Phy and CXL.io

For PCIe Phy and CXL.io mode you can also Filter Out traffic you may not want to see in the trace. See Figure 5.130.

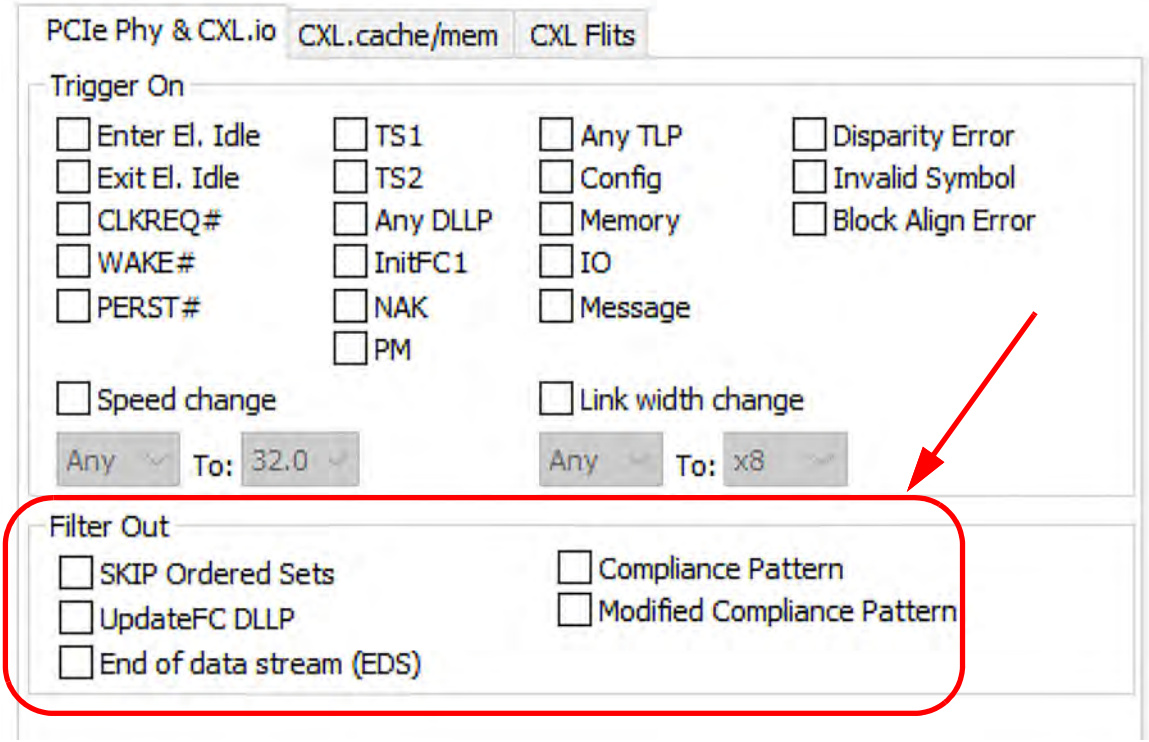


Figure 5.130: PCIe Phy and CXL.io Filter Out Options

These Filter Out options are also shown in Table 5.9.

TABLE 5.9: PCIe Phy and CXL.io Filter Out Options

SKIP Ordered Sets	Compliance Pattern
UpdateFC DLLP	Modified Compliance Pattern
End of data stream (EDS)	

5.22.5 CXL: Filter Out for CXL.cache/mem

For CXL.cache/mem mode you can also Filter Out traffic,
(Invalid packets in slots is selected by default). See Figure 5.131.

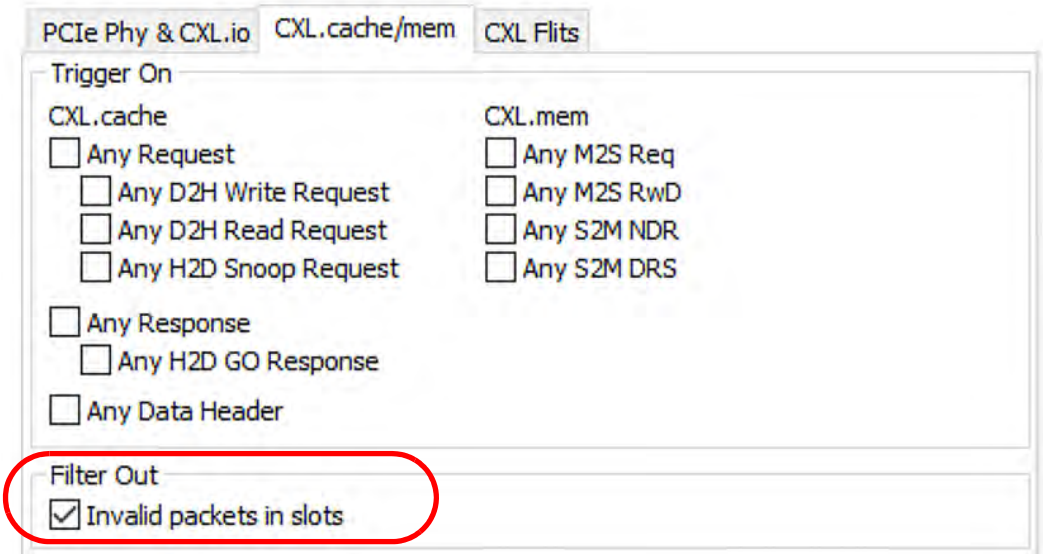


Figure 5.131: CXL.cache/mem Filter Out Options

5.22.6 CXL: Filter Out for CXL Flits

For CXL Flits mode you can also Filter Out NULL Flit traffic. See Figure 5.132.

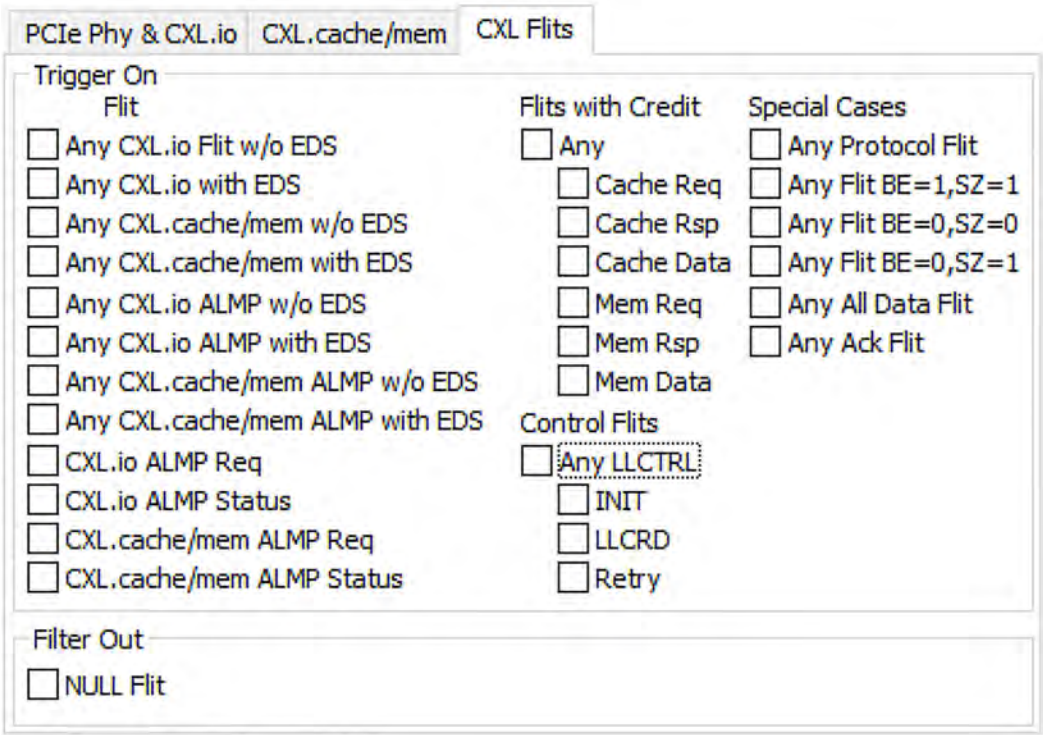


Figure 5.132: CXL Flits Filter Out Options

Chapter 6

Recording Options: AJA Mode

6.1 Jammer Mode Overview

6.1.1 Jammer Mode (AJ)

The Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior. The Summit M5x also introduces for the first time NVMe and NVMe-MI protocol jamming as well. The analyzer and jammer combination features on the Summit M5x make this a powerful testing tool for PCIe validation and development labs. This Jammer and Scripting capability is built into the PCIe Protocol Analysis software. After the software has been loaded (see “Installation and Setup” on page 45), you can access the Jammer functionality through the Recording Options of the PCIe Protocol Analysis software dialog (see Figure 6.1).

6.1.2 Jammer Mode (AJA)

In addition, the Summit M5x can also display the results of the Jamming operation. In the Summit M5x you can analyze a stream of traffic, modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint and then see the results of that jamming operation. See “Jammer Mode Overview (AJA)” on page 310 for more details.

6.1.3 PCIe Protocol Analysis Software

Selecting the **Setup** menu displays the following menu options shown in Figure 6.2 on page 248).

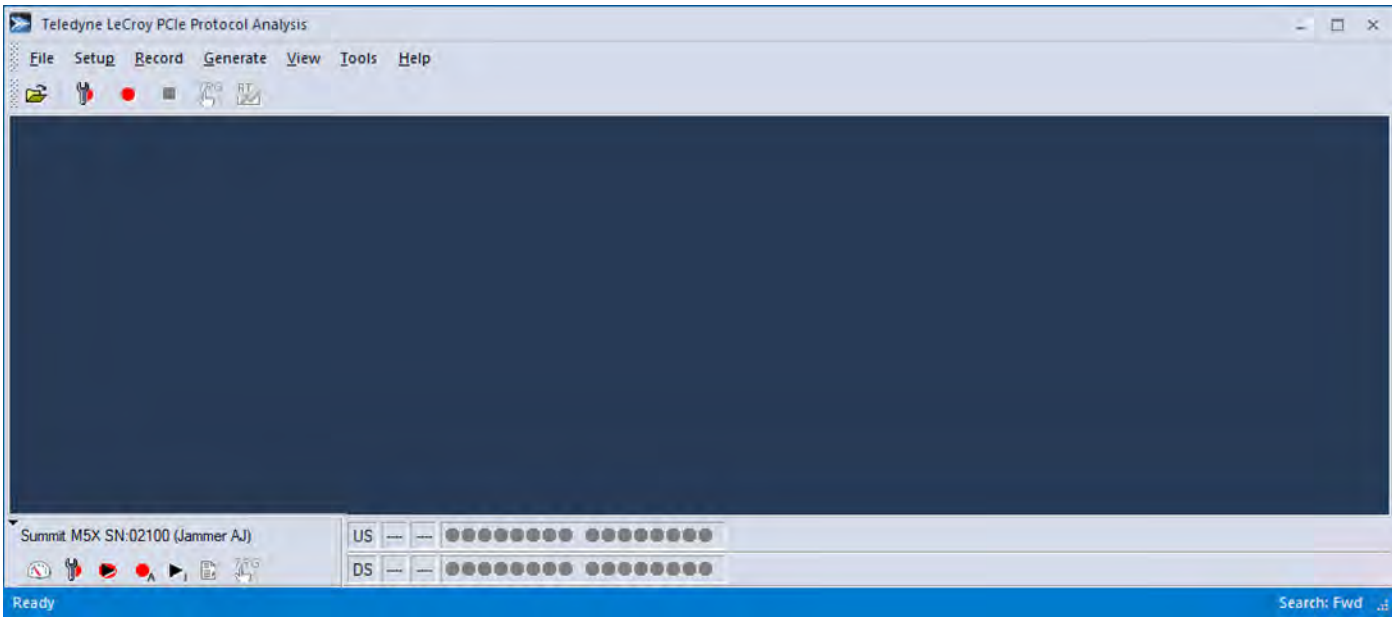


Figure 6.1: PCIe Protocol Analysis Software dialog

6.1.4 Recording Options

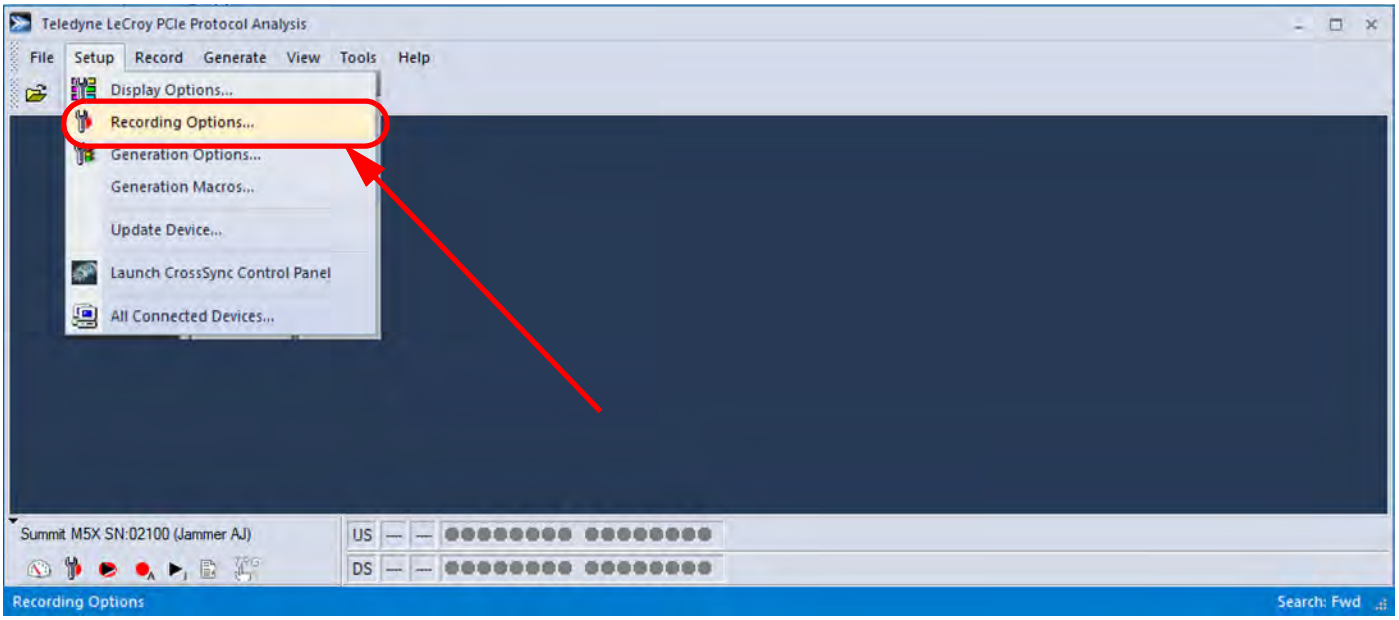


Figure 6.2: Recording Options

From the **Setup** menu, select **Recording Options...**. The Recording Options dialog displays (see Figure 6.3 on page 249).

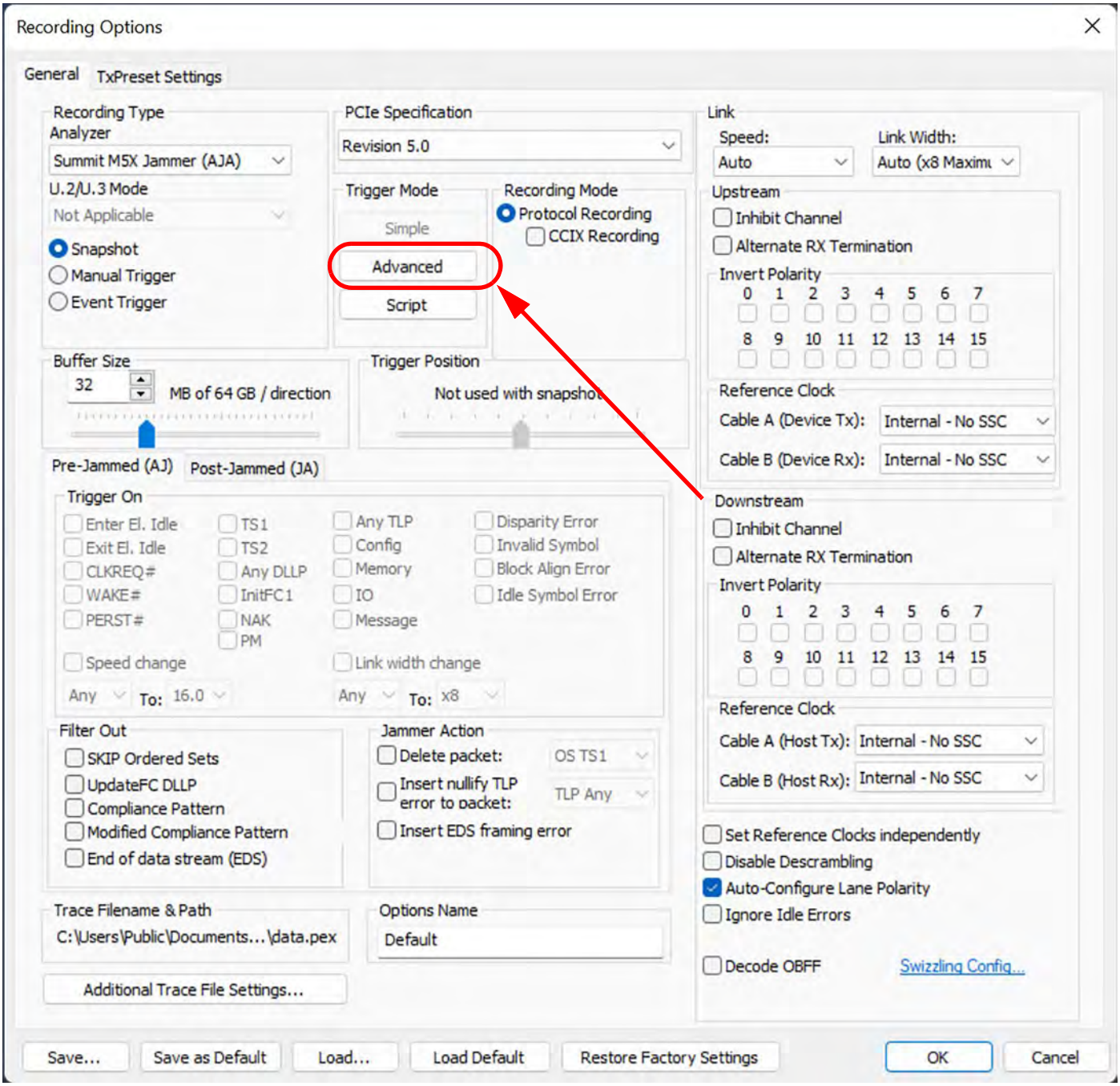


Figure 6.3: Summit M5x Recording Options Dialog

From the **Analyzer** drop down, select Summit M5x jammer (AJA). Click the **Advanced** button in the Trigger Mode zone. The Recording Rules tab will appear next to the General tab. See Figure 6.4 on page 250.

6.1.5 Recording Options: Recording Rules (AJ)

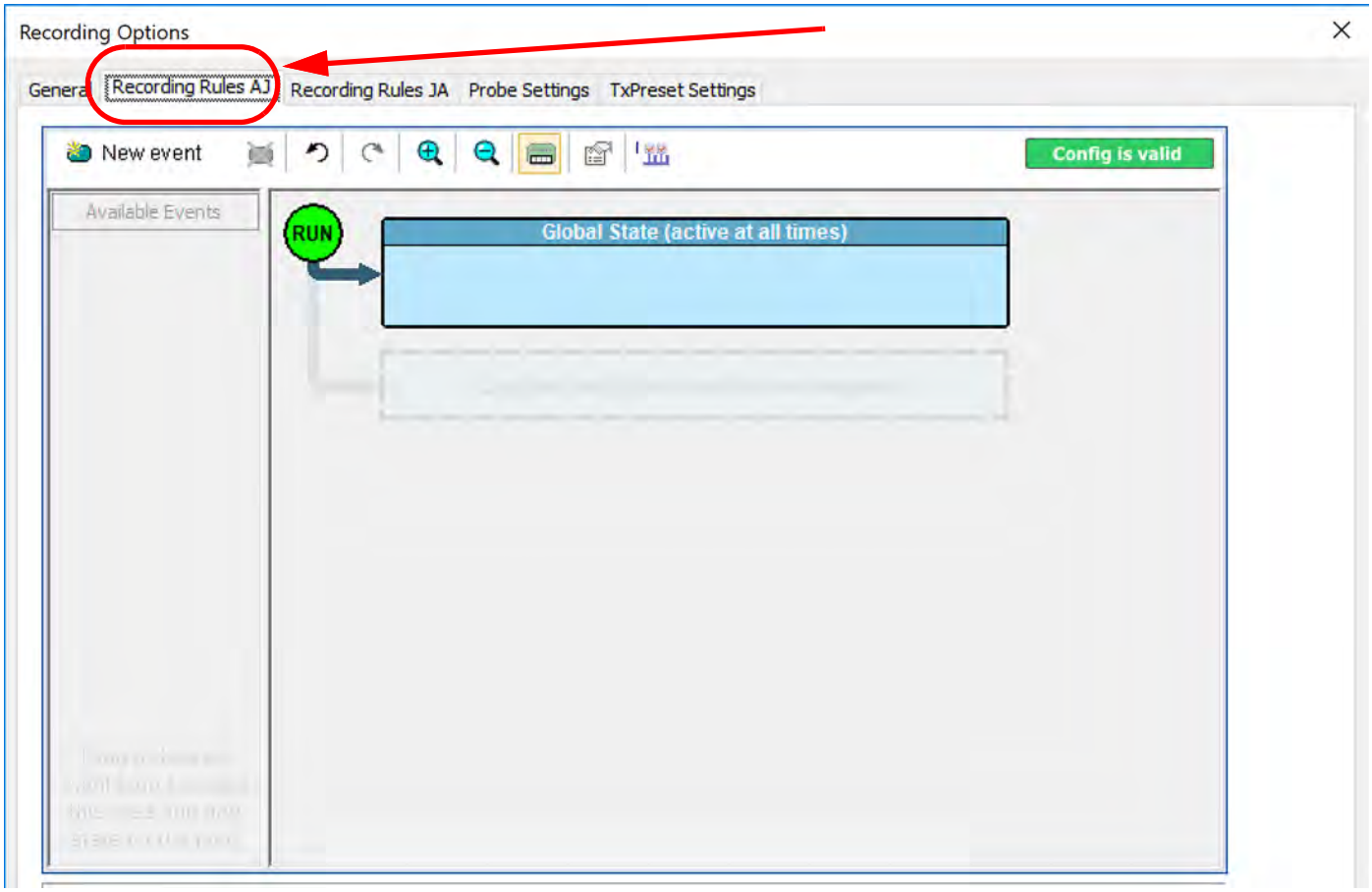


Figure 6.4: Recording Options: Recording Rules AJGUI

Select New Event. The available trigger options display below the button, as shown in Figure 6.5 on page 251.

6.1.6 Recording Rules AJ: New Events

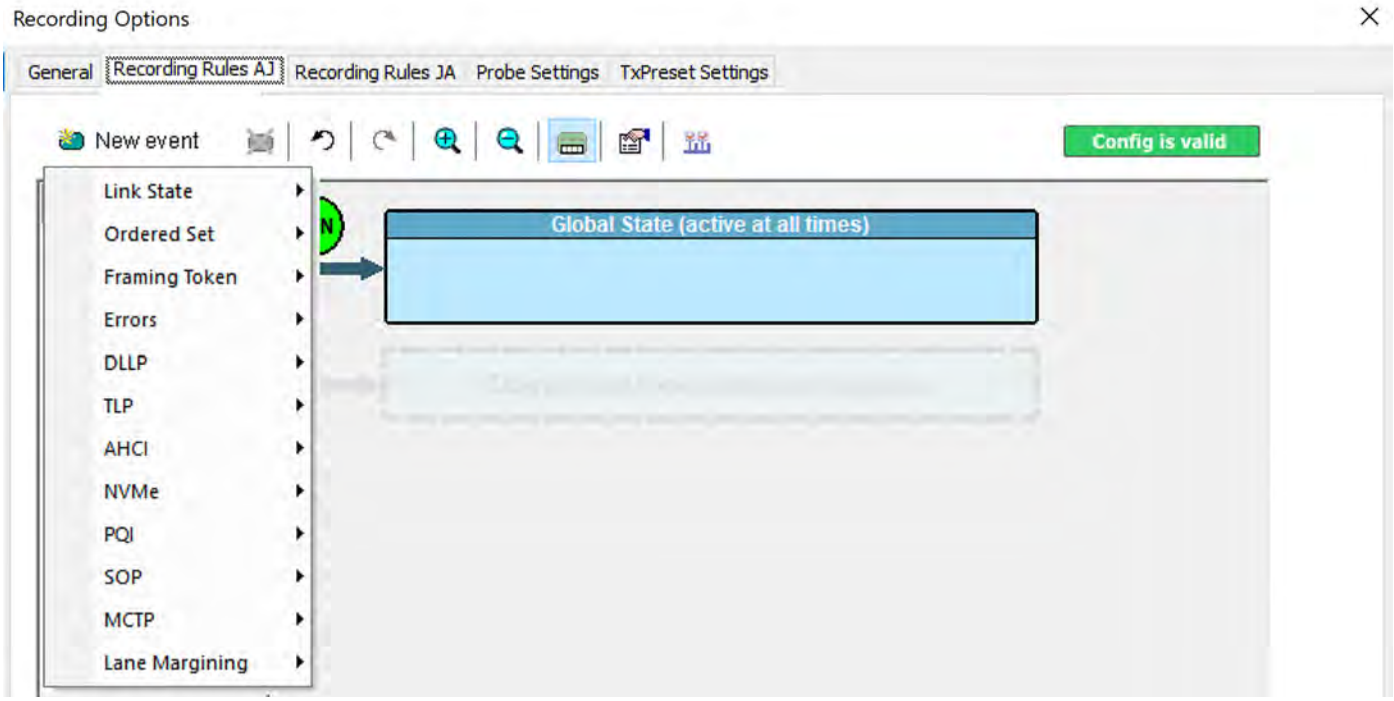


Figure 6.5: Recording Options: New Events List

The PCIe Protocol Analysis software enables you to configure a very complex set of Recording Rules or events and Jammer Actions from the GUI and then convert them into a script.

There are twelve (12) types of New events to choose from:

- Link State
- Ordered Set
- Framing Token
- Errors
- DLLP
- TLP
- AHCI
- NVMe
- PQI
- SOP
- MCTP
- Lane Margining

6.2 Converting Recording Rules and Jammer Actions from GUI to Script File (AJ)

6.2.1 Complex Recording Rules

We have defined a complex set of Recording Rules to which we can add Jammer Actions and then convert the GUI options into a script automatically. See Figure 6.6

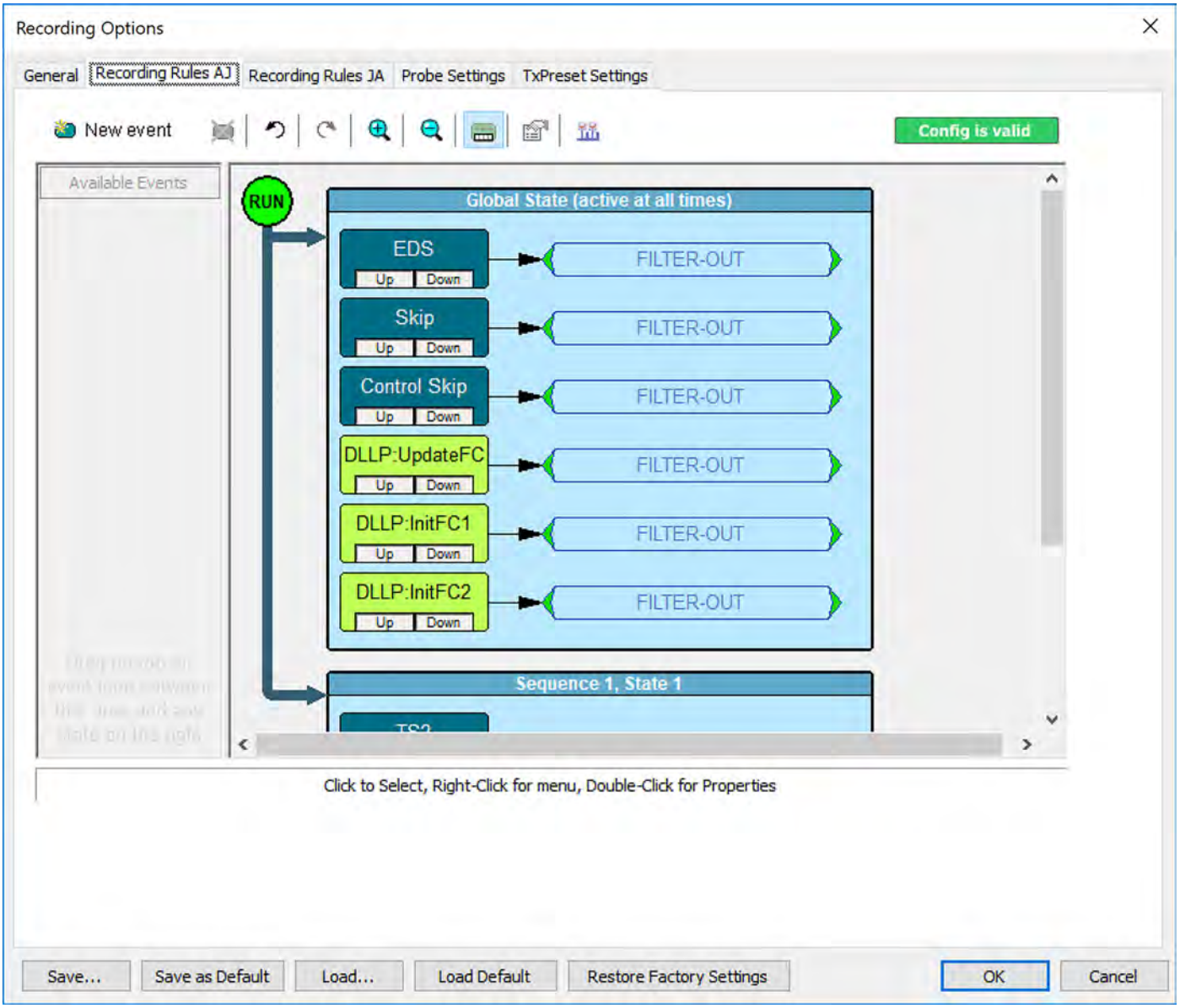


Figure 6.6: Complex Recording Rules: 1

If you use the scroll bar on the right you'll get to the final events. See Figure 6.7 on page 253.

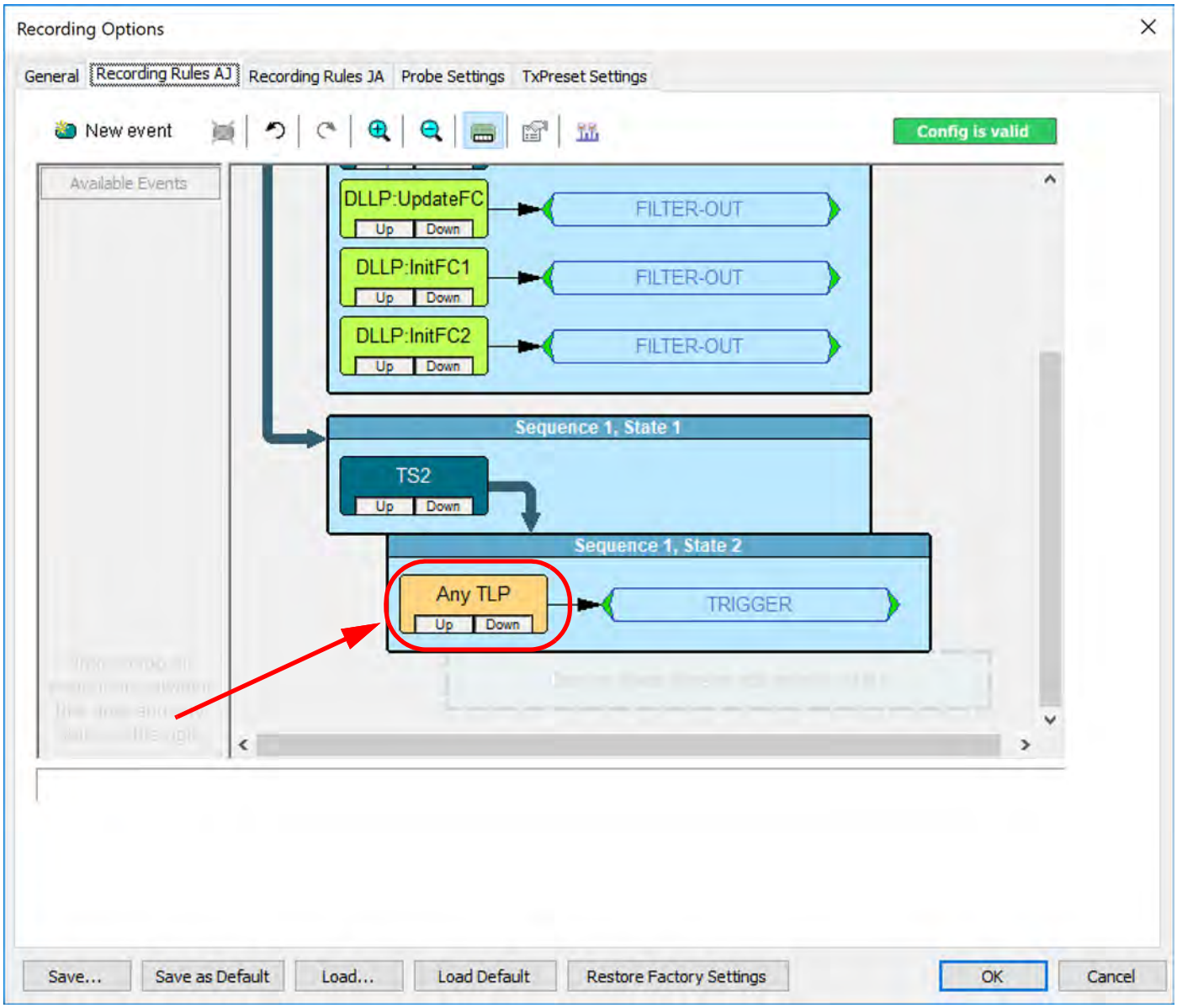


Figure 6.7: Complex Recording Rules: 2

If you right click on the Any TLP another dialog will pop up which allows you to choose a Jamming Action as well as triggering the analyzer. See Figure 6.8 on page 254.

6.2.2 Jammer Options

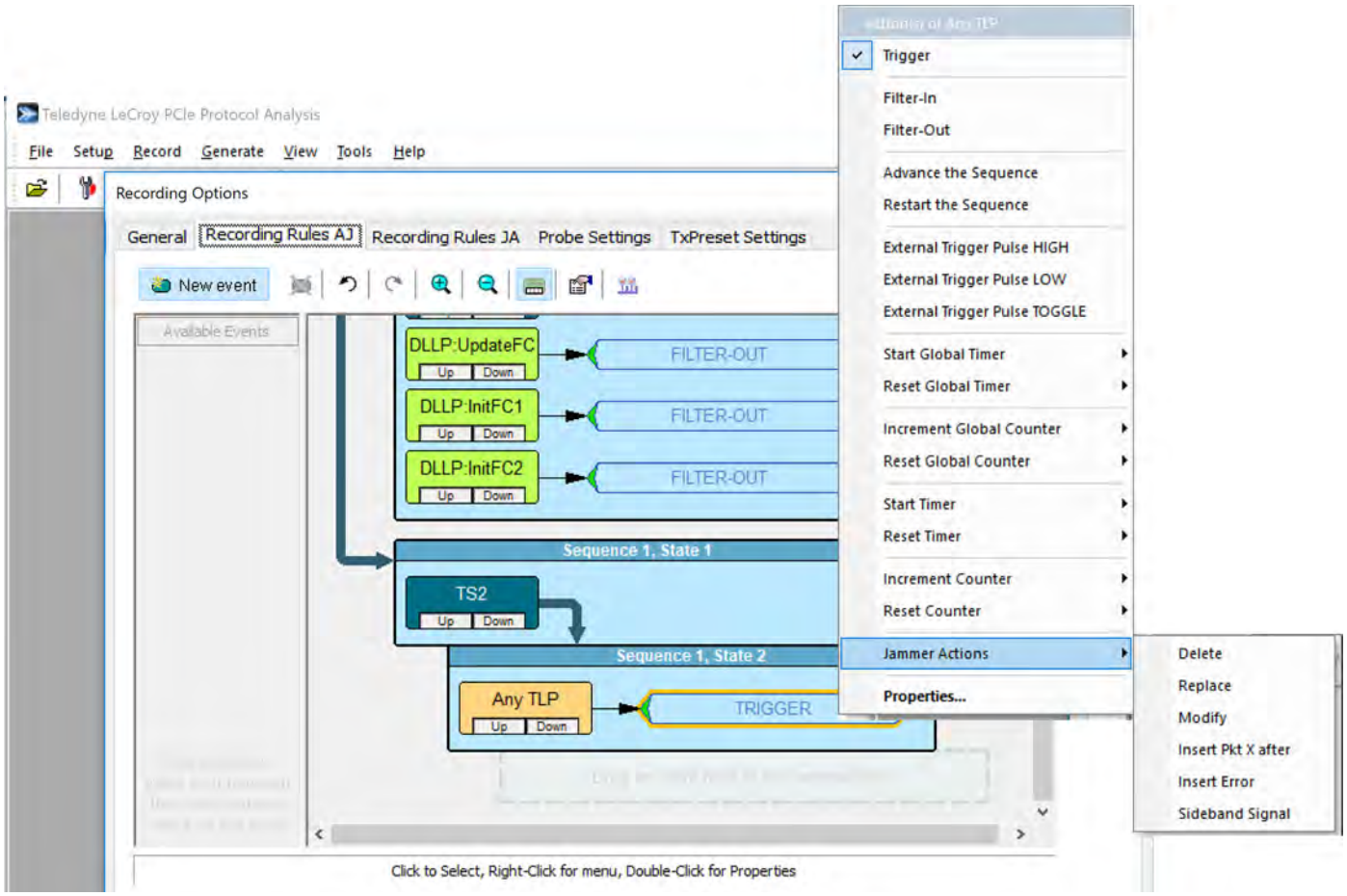


Figure 6.8: Jammer Actions

Now you can add the following Jammer Actions to the Trigger:

- Delete
- Replace
- Modify
- Insert Pkt X after
- Insert Error
- Sideband Signal

6.2.2.1 Example: Jammer Replace

You can set the Jammer Action: Replace options using the Raw Data button. See Figure 6.9.

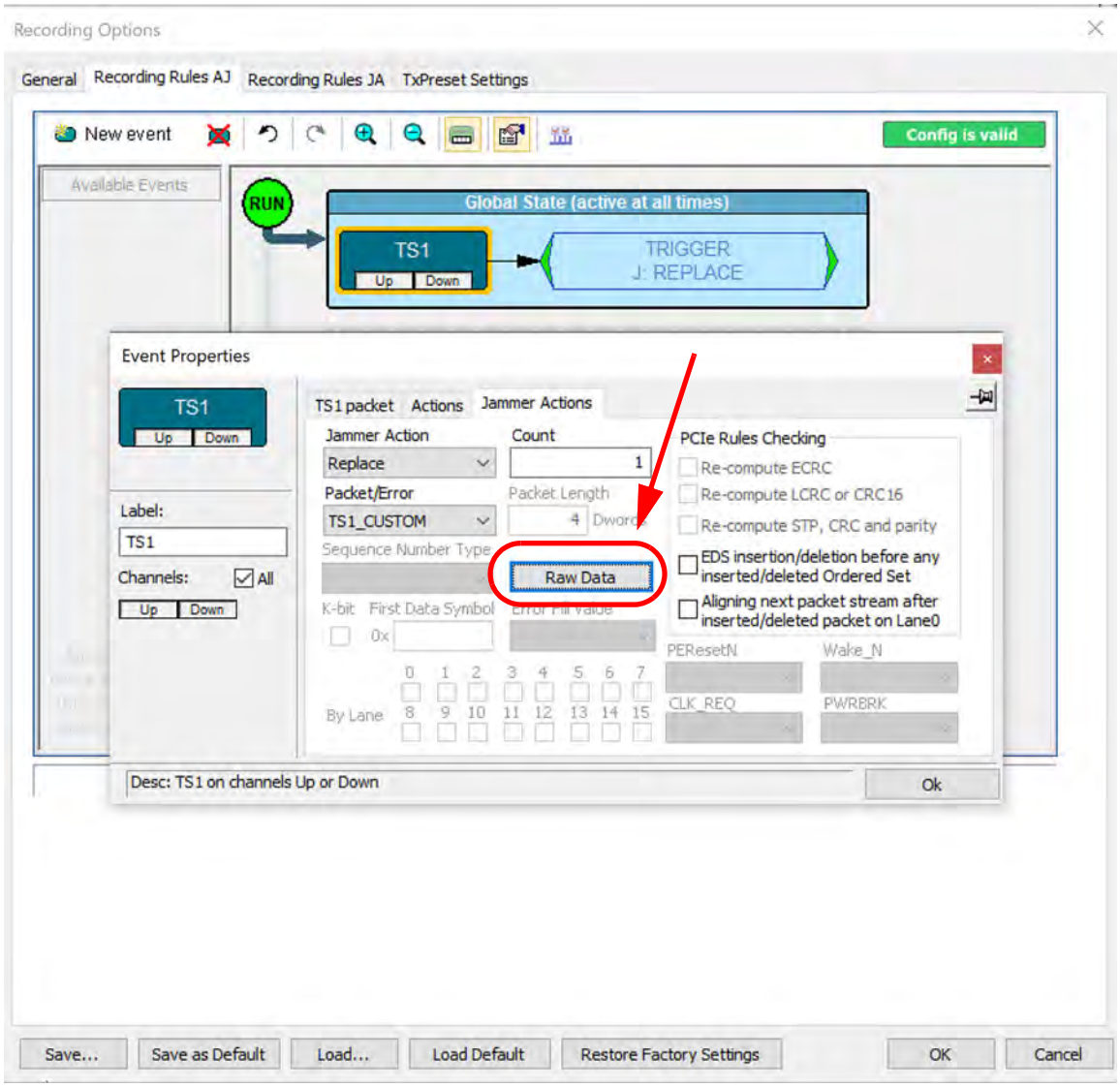


Figure 6.9: Recording Rules AJ: TS1Jammer Actions: Replace Packet, then Select Raw Data

In the Raw Data dialog you can set individual bits. See Figure 6.10 on page 256.

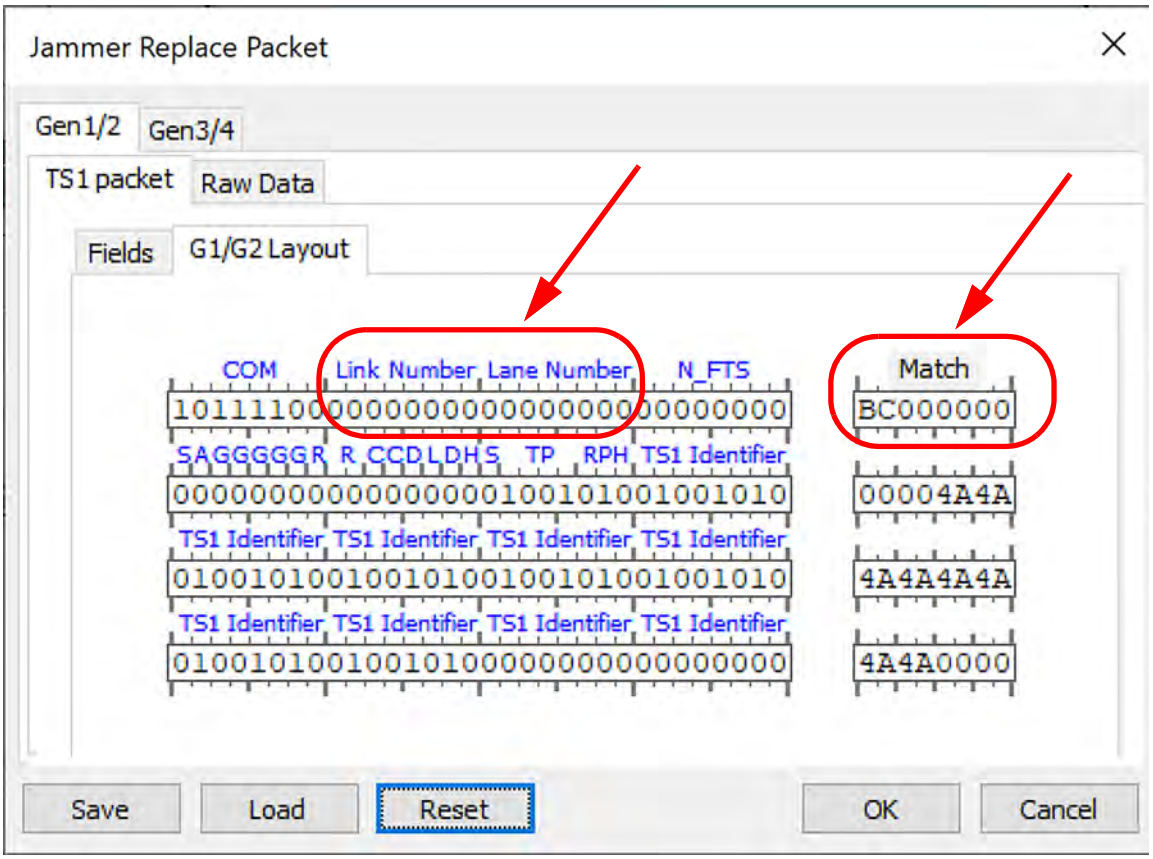


Figure 6.10: Jammer Replace Packet: Raw Data Default Values for Link and Lane Number

For example, you can enter values into the Link and Lane Numbers. See Figure 6.11 on page 257.

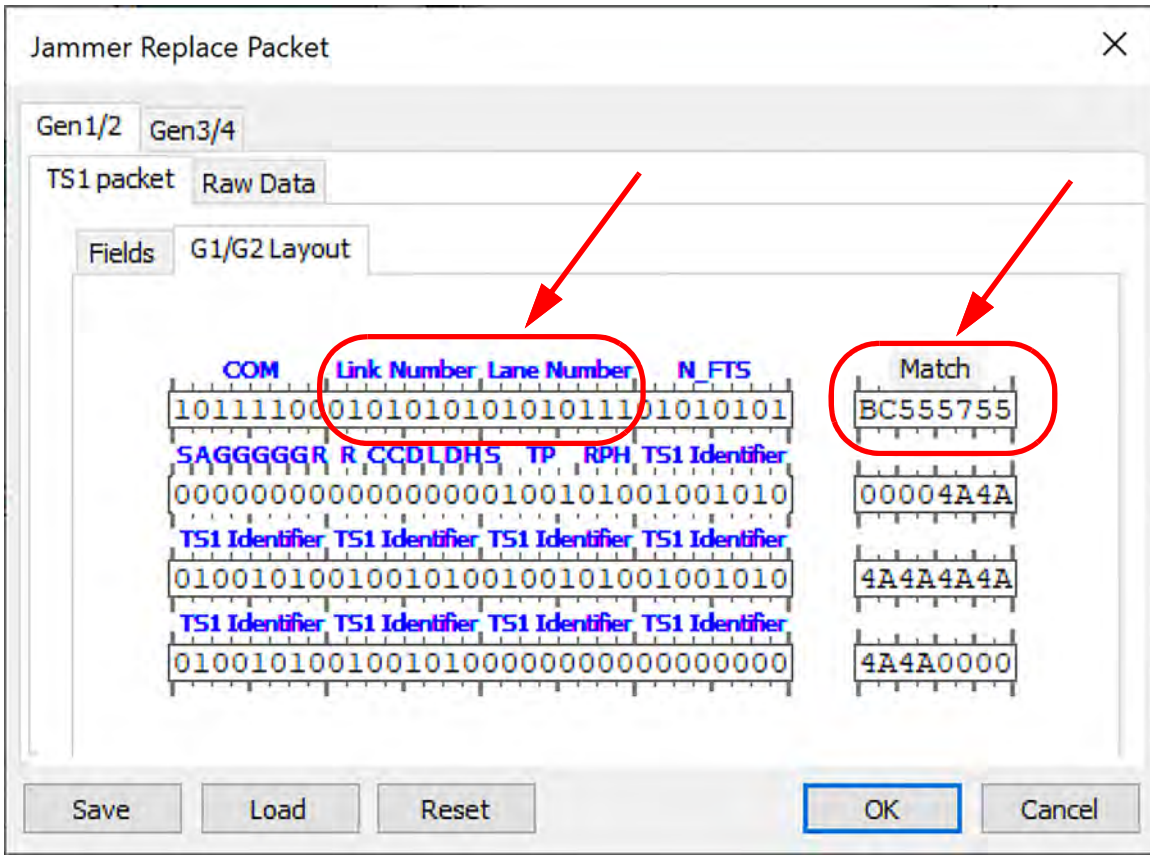


Figure 6.11: Jammer Replace: Raw Data Default Values for Link and Lane Number

At this point you can Click on “**OK**” to set the Link and Lanes values or you can Click on “**Save**”. If you select **Save** a window will pop up where you can Save the Raw Data values you have entered. See Figure 6.12 on page 258.

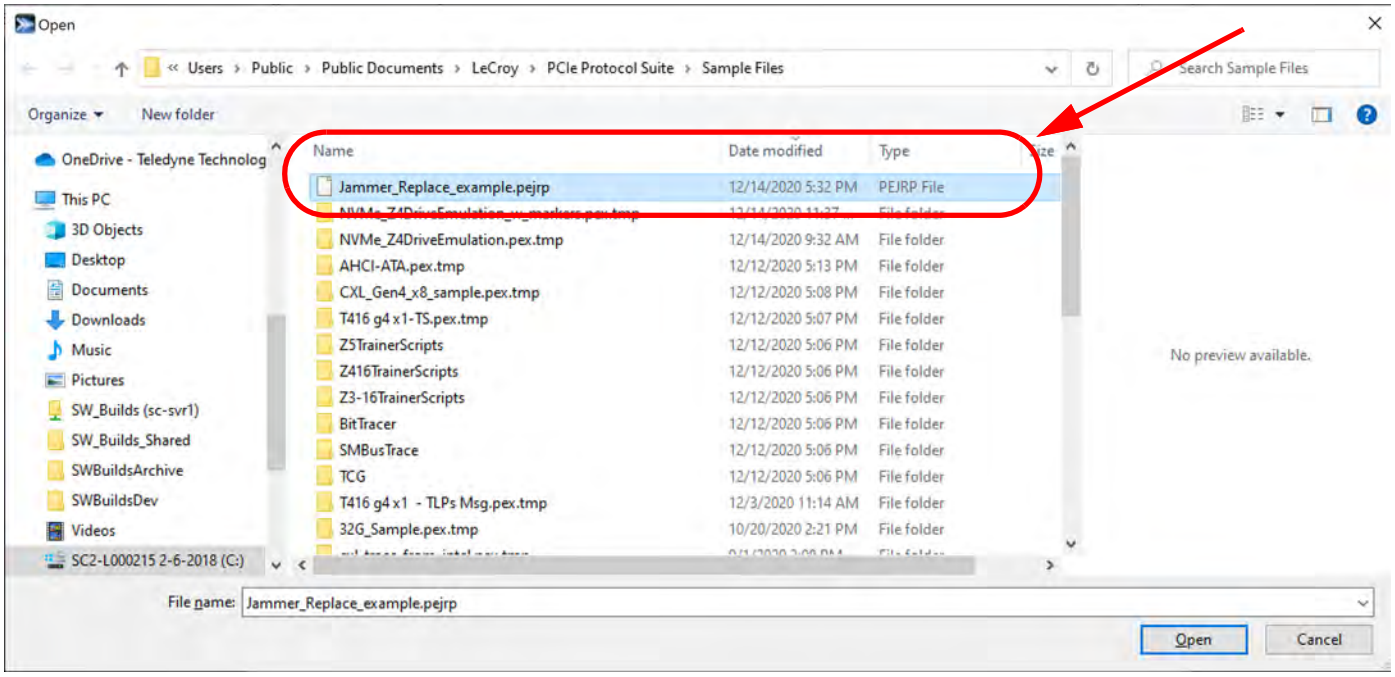


Figure 6.12: Jammer Replace Packet: Raw Data Default Values Saved for future use

The Raw Data values you entered will be Saved in the Sample Files folder.

If you want to use them in the future when defining Raw Data values in the **Jammer Replace Packet -> Raw Data** dialog, just Click on Load.

The Sample Files folder will pop up and you can select the file with the Raw Data values you entered before.

6.3 Script Mode

Script mode is currently available only for Summit M5x devices. If an Summit M5x device is not connected, then it is necessary to select a "Summit M5x" device to enable script mode selection. Script mode can be enabled on the "General" tab in Recording Options dialog using the "Script" button. After switching to script mode, the "Recording Script" tab with controls to modify a script will be added.

If Recording Rules in Advanced or in Simple mode contain some events, these events will be automatically converted to a script when switching to script mode.

If Script Mode UI contains script text, then it will be converted to Recording Rules when switching from script mode to GUI mode. See Figure 6.13 and Figure 6.14 on page 260.

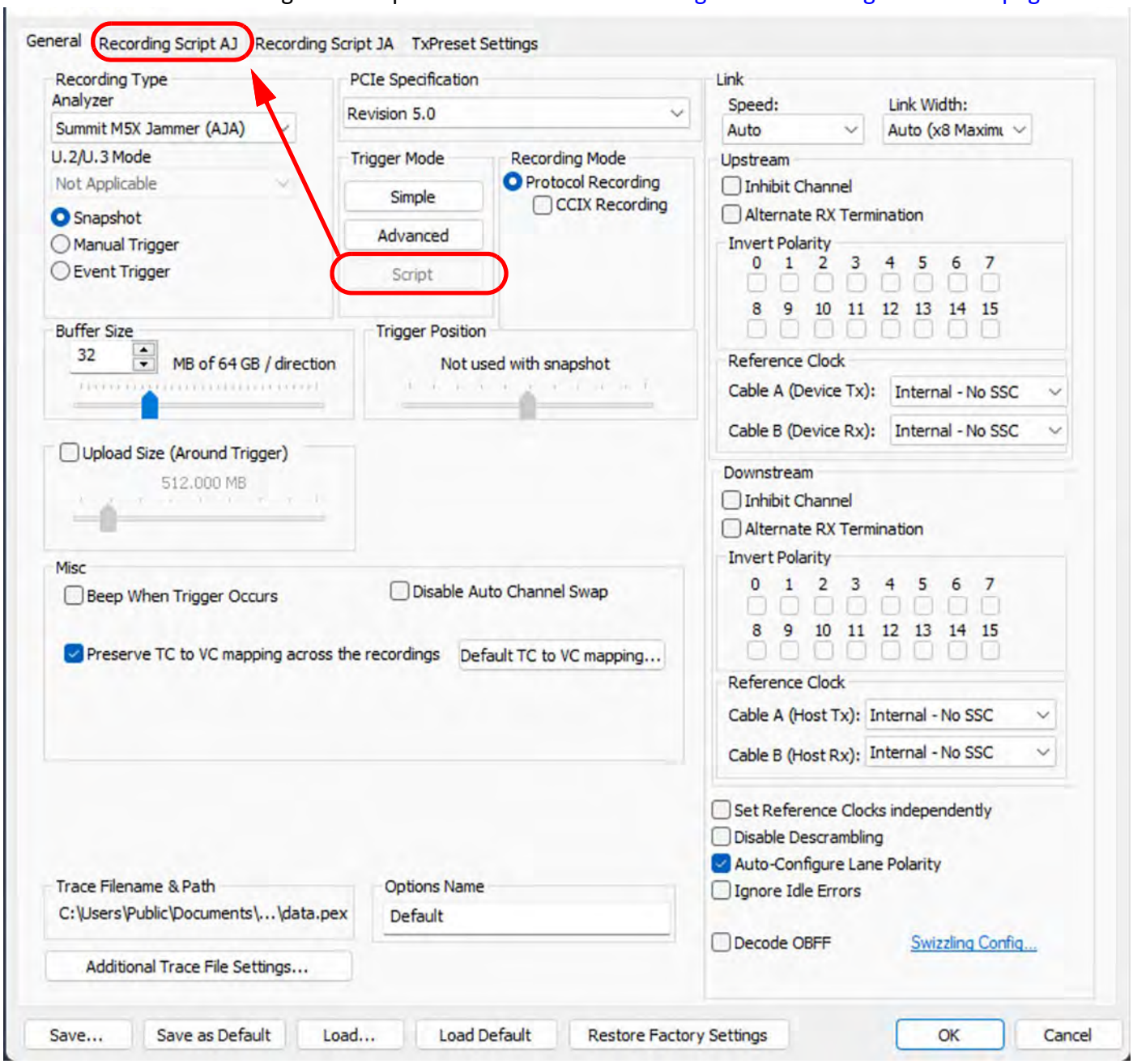


Figure 6.13: Recording Options: Advanced Mode -> Scripting

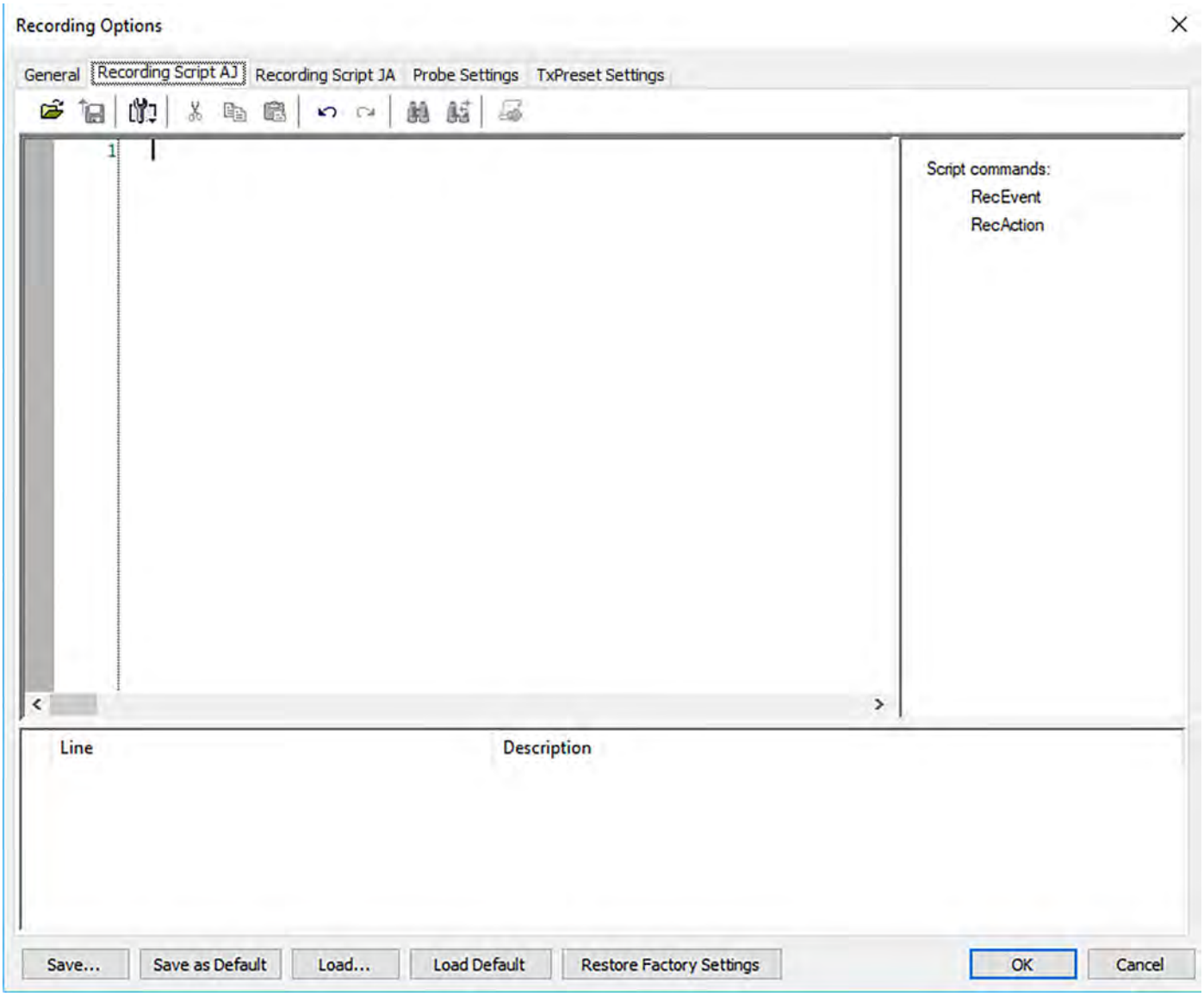


Figure 6.14: Scripting Dialog

The Recording Script mode dialog contains: text area, panel with hints, error list and toolbar.

Buttons in the toolbar include: Open/Save script, View Options of text area, Edit text (cut, copy, paste, undo, redo, find and replace) and Parse script.

Text for commands may be generated using menus "RecEvent" and "RecAction" on the right panel. They contain list of all supported events and actions. To generate text of commands it is necessary to click "RecEvent" or "RecAction" and select one of options from expanded context menu.

When the cursor (in the text area) is placed inside of braces of some command, then the hints panel will contain available properties for this command. See below in Figure 6.15 on page 261.

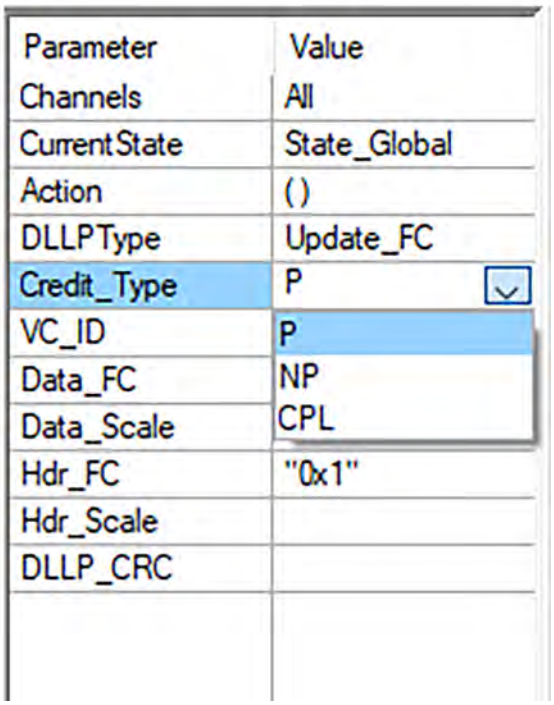


Figure 6.15: Scripting: Parameters and Values

The Errors list at the bottom will contain information (line number and description) about parse errors and warnings. It is possible to navigate to an error by double click on it. See Figure 6.16 on page 262.

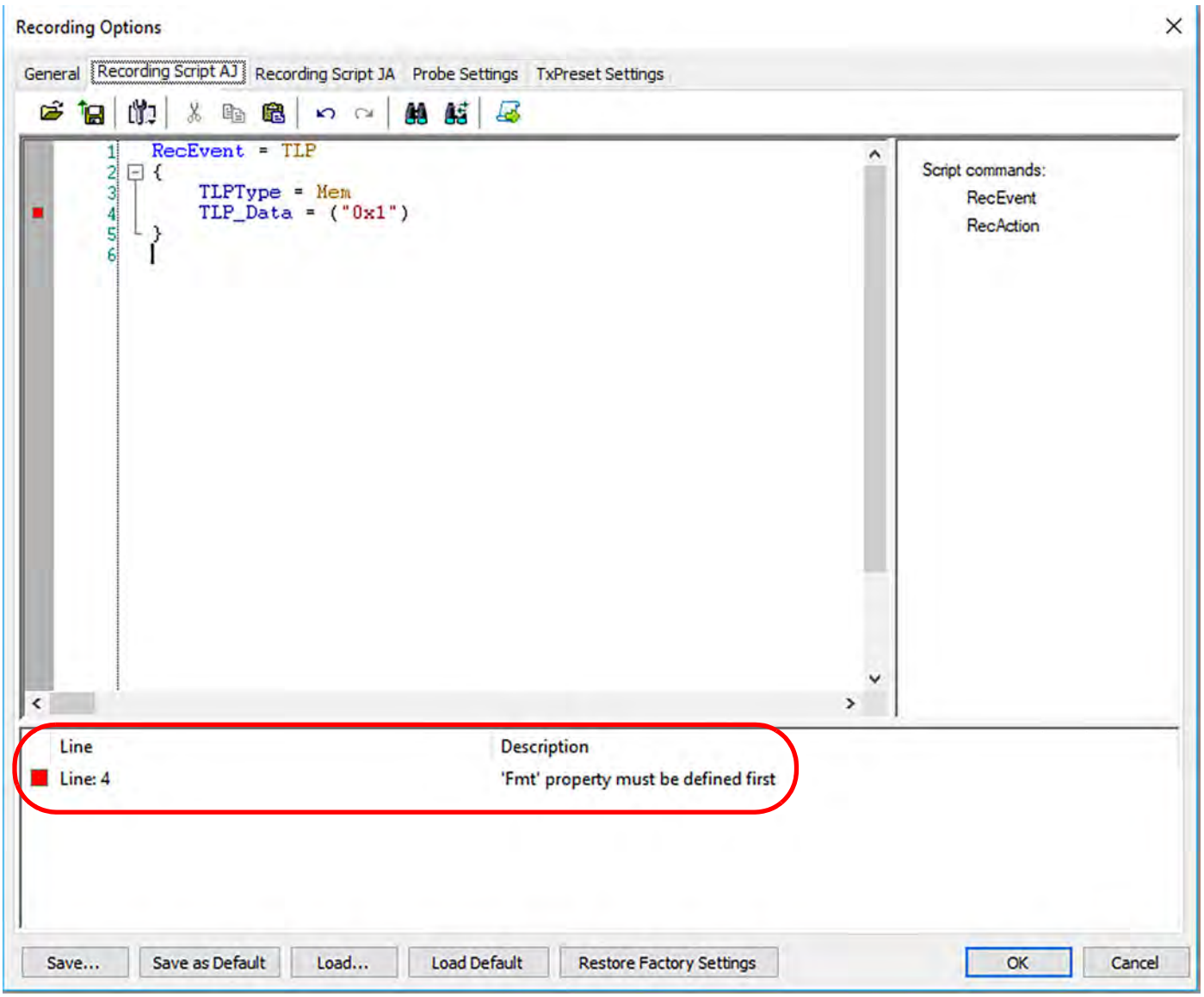


Figure 6.16: Script File with Error Shown

6.3.1 Script Parsing

Script parsing can be performed by clicking "Parse script" button at the toolbar or by pressing Ctrl + S combination. See Figure 6.17.

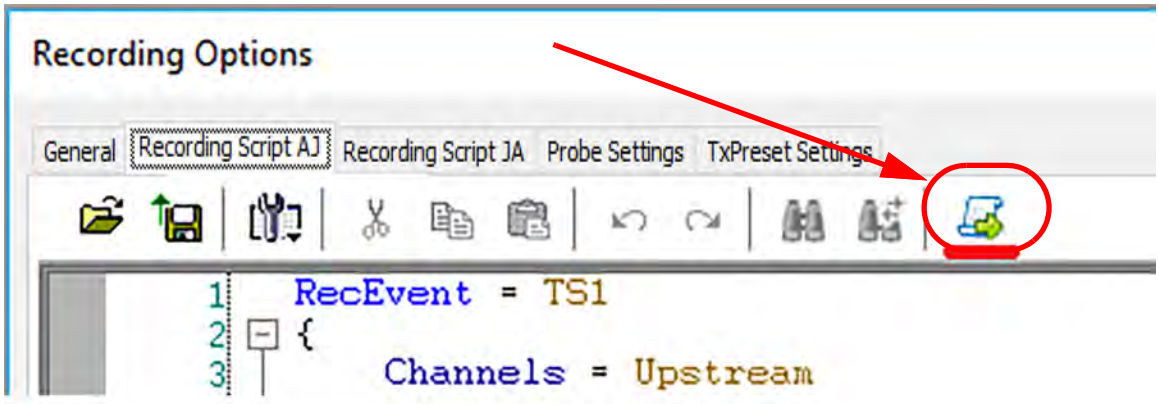


Figure 6.17: Script Parsing

The Script will be parsed when leaving the script page or by closing the Recording Options dialog. If the script contains parse errors, then a corresponding warning message will be shown. Leaving a script page which contains errors may not create recording rules correctly. See warning message in Figure 6.18.

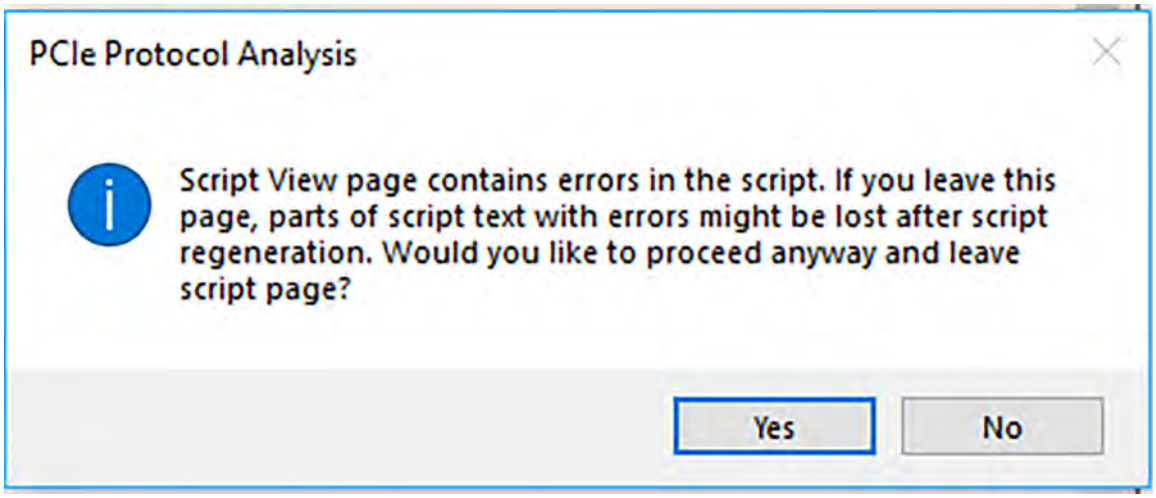


Figure 6.18: Script Warning Message

6.4 Commands

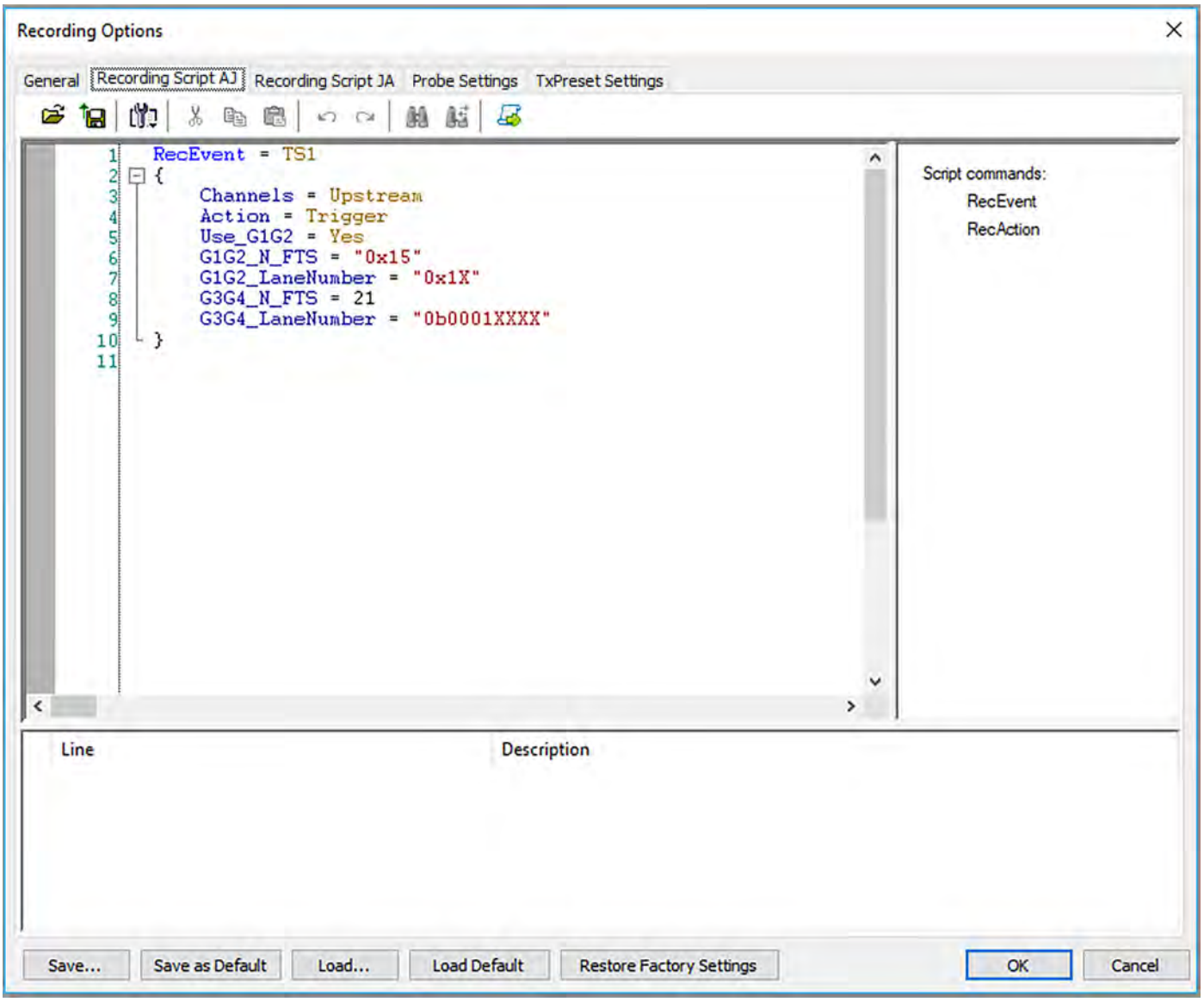


Figure 6.19: Typical Script Commands

Script commands have properties, which are placed inside braces. Each property should be defined as a key-value pair in form "Key = Value".

Each command has its own set of available keys.

There are different types of values: numeric, logical, mask/match and string.

Logical values are represented as "Yes" or "No" keywords.

Mask/match values can be specified as decimal numbers or as strings with hexadecimal ("0x1") or binary ("0b1001") numbers. A mask can be applied using the "X" symbol ("0x111X" or "0b1001X111"). In binary notation "X" corresponds to 1 bit, in hexadecimal notation to 4 bits. If the value is specified as a string with hexadecimal numbers without

mask, then the mask will not be applied to the whole field (for example, "0x1" equals "0x00000001" for 32 bit field).

Some properties have predefined constant values. Such values will be suggested when the "=" symbol is pressed. A list of such values can also be opened by pressing Ctrl + Alt + T or using context menu.

See example below in Figure 6.20.

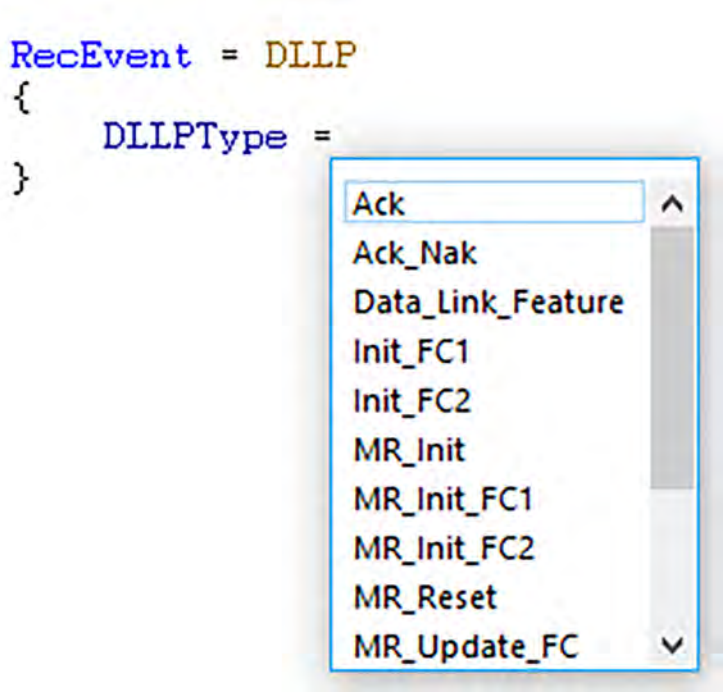


Figure 6.20: Example of Command with Context Menu

Some commands require certain properties to be defined. If such properties are not defined, then parse error will be added. If a command does not require a property and it is not defined, then a default value from UI will be set.

6.5 Events

RecEvent commands have several properties that are common almost for all events. Channels property defines event's channel(s): Upstream, Downstream, All or None. Current state property defines the state in which the event is located. It can be "State_Global" or one of 16 local states (for instance, "State_1"). Actions property defines the event's actions, which is used for triggering, sequencing, filtering etc. Action property is also used to connect events with jammer actions.

Timer and counter events have additional restrictions. Theyare divided into two groups: global and local. Global timers and counters can be created only in global state. Local timers and counters must be defined in the state property and cannot be created in global state.

A list of available properties may depend on the values of other properties. For example, TLP event's properties depend on TLP type.

6.6 Jammer Actions

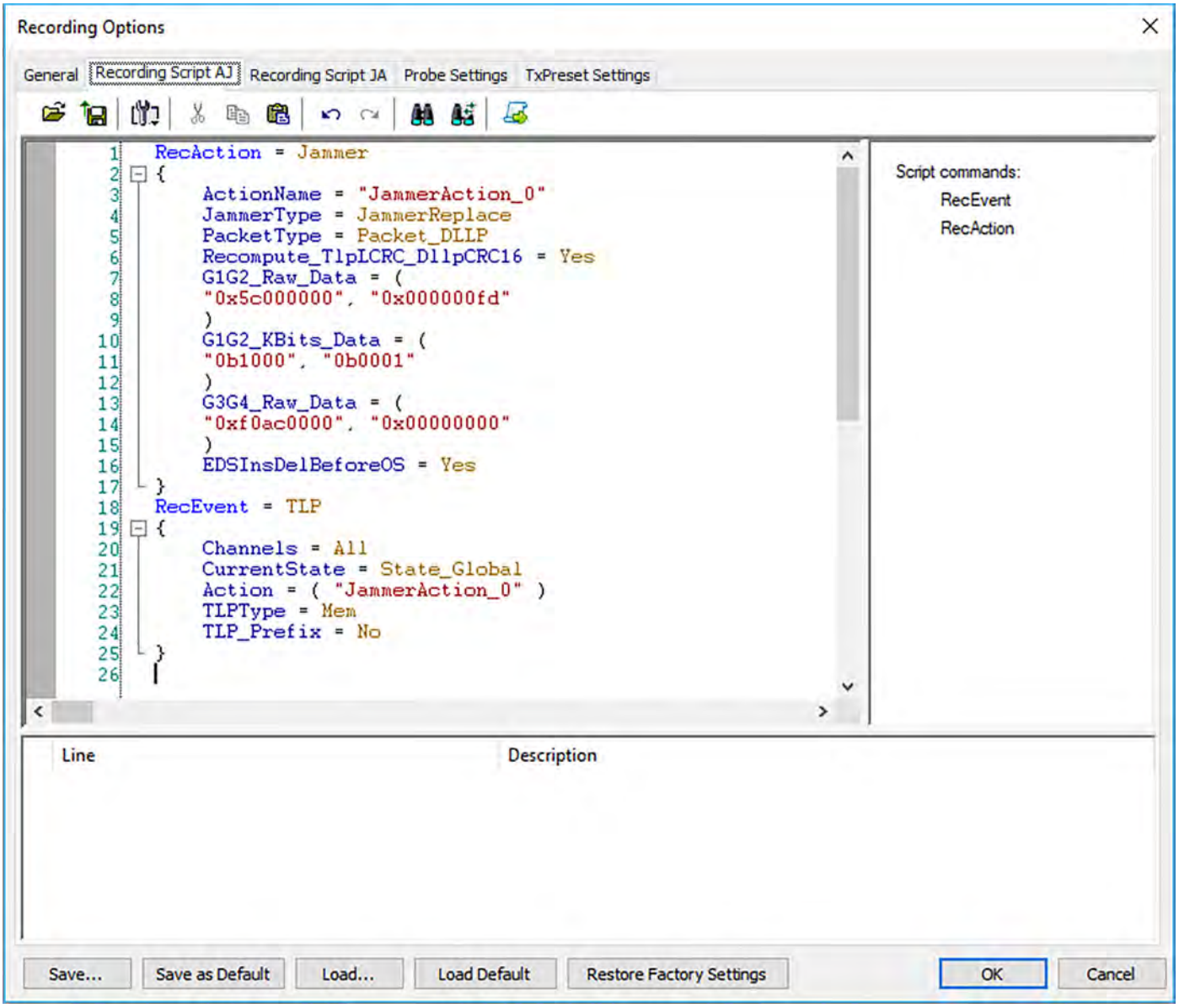


Figure 6.21: Jammer Actions

Jammer Action is a type of script RecAction command. The Jammer Action command must be connected with an event or it will not be created. Each jammer action must have a unique name and its type must be defined.

Jammer Action can be defined only before event in which it is used. To connect an event with a jammer action it is necessary to add a string with the jammer action name to the list of the event's actions.

If the Jammer Action modifies the raw data property and is not defined, then raw data will be the same as event's layout.

If raw data is not defined for Replace or Insert Pkt X After jammer actions, then raw data will be set to the default value for the Jammer Action's event type.

6.7 Scripting Jammer Functionality

There are seven (7) types of New events to choose from:

- Link State
- Ordered Set
- Framing Token
- Errors
- DLLP
- TLP
- NVMe

There are six types of Jammer Actions available which can be associated with any of the New event types list above:

- Delete
- Replace
- Modify
- Insert Pkt X after
- Insert Error
- Sideband Signal

6.7.1 Example: Select Jammer Action: Delete

If you select Delete as the Jammer Action the following dialog will pop up showing you the Jammer Action options. See Figure 6.22 on page 268.

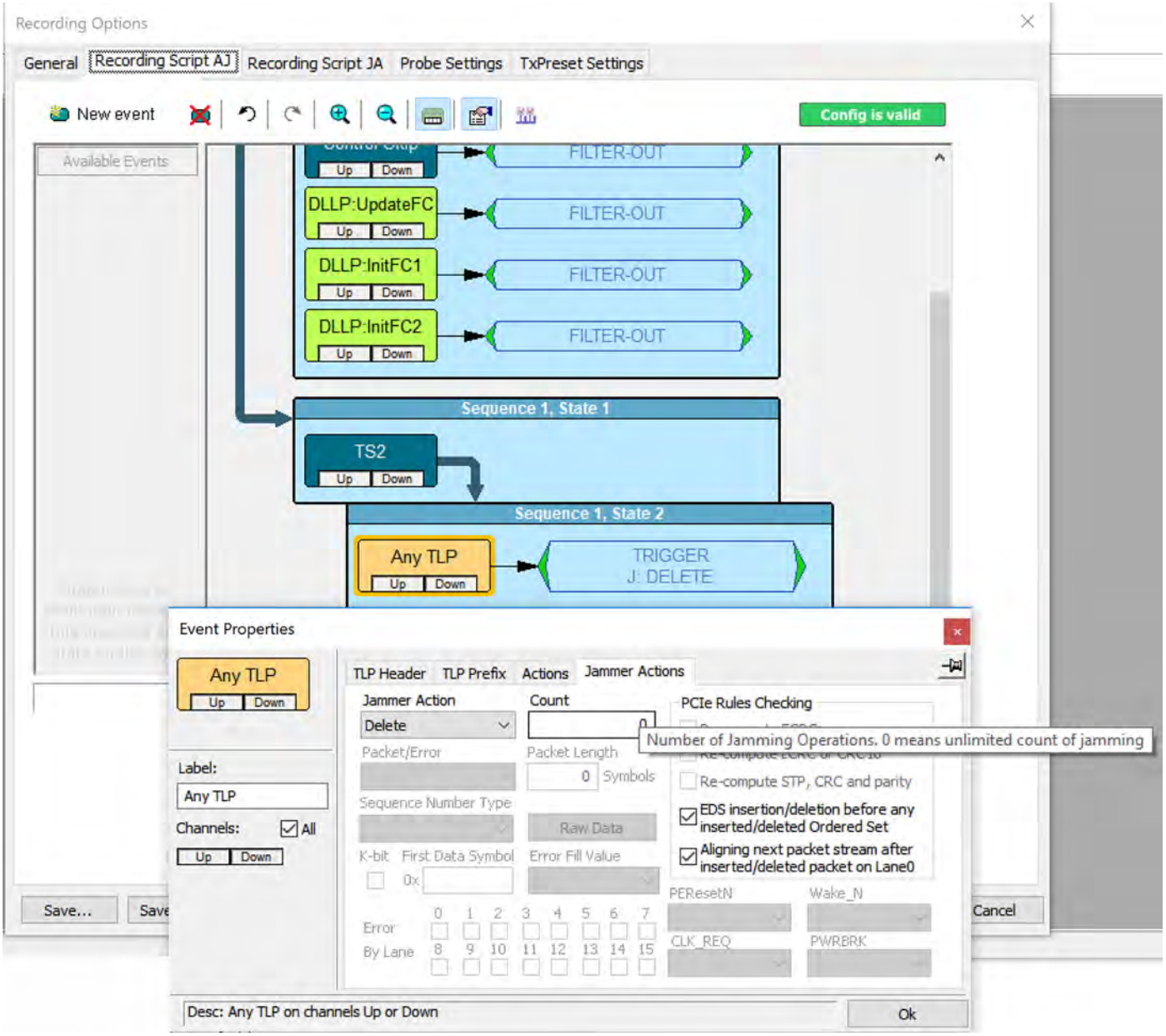
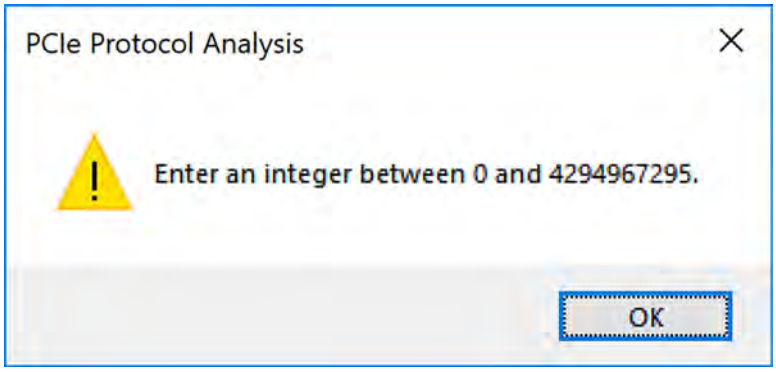


Figure 6.22: Jammer Action: Delete

For the Delete Action there are only three extra options:

- Count: Number of Jamming Operations -> **0 means unlimited**
  If you enter too large a number the following warning message will pop up. See Figure 6.23 on page 270.

WARNING: If you leave the Count Number at 0, an unlimited number of Jammer actions will take place, which means the script will not proceed beyond that point.



- For this example enter 10

- EDS insertion/deletion before any inserted/deleted Ordered Set
- Aligning next packet stream after inserted/deleted packet on Lane0

Click on OK to add the options to the Jammer Action.

If you select the General Tab (in Recording Options) the following dialog will appear. See Figure 6.23 on page 270.

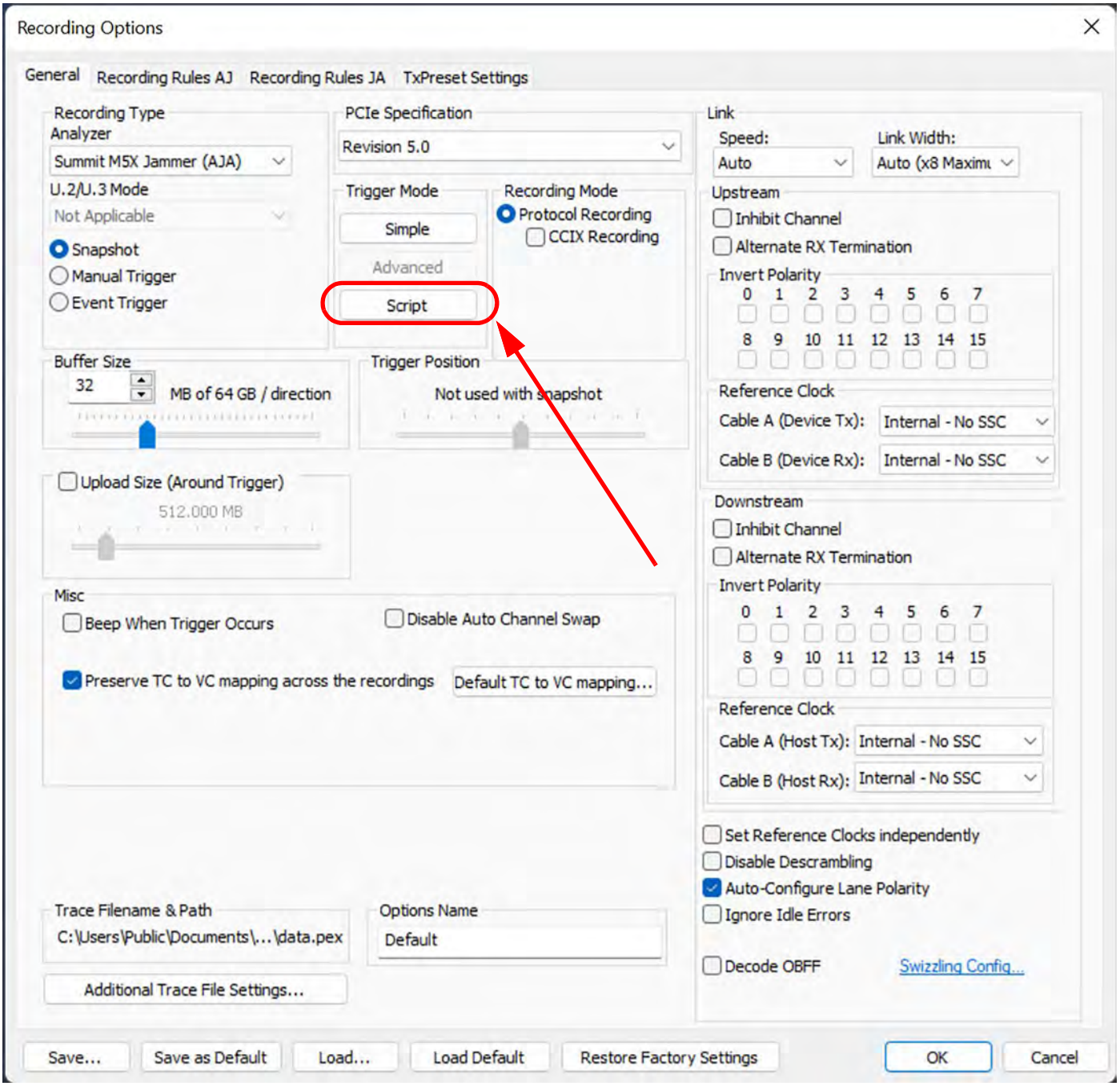


Figure 6.23: Recording Options: Script

If you select the Script Option under Options Mode the Recording Script Tab will appear in the Recording Options -> General dialog (see Figure 6.24 on page 271).

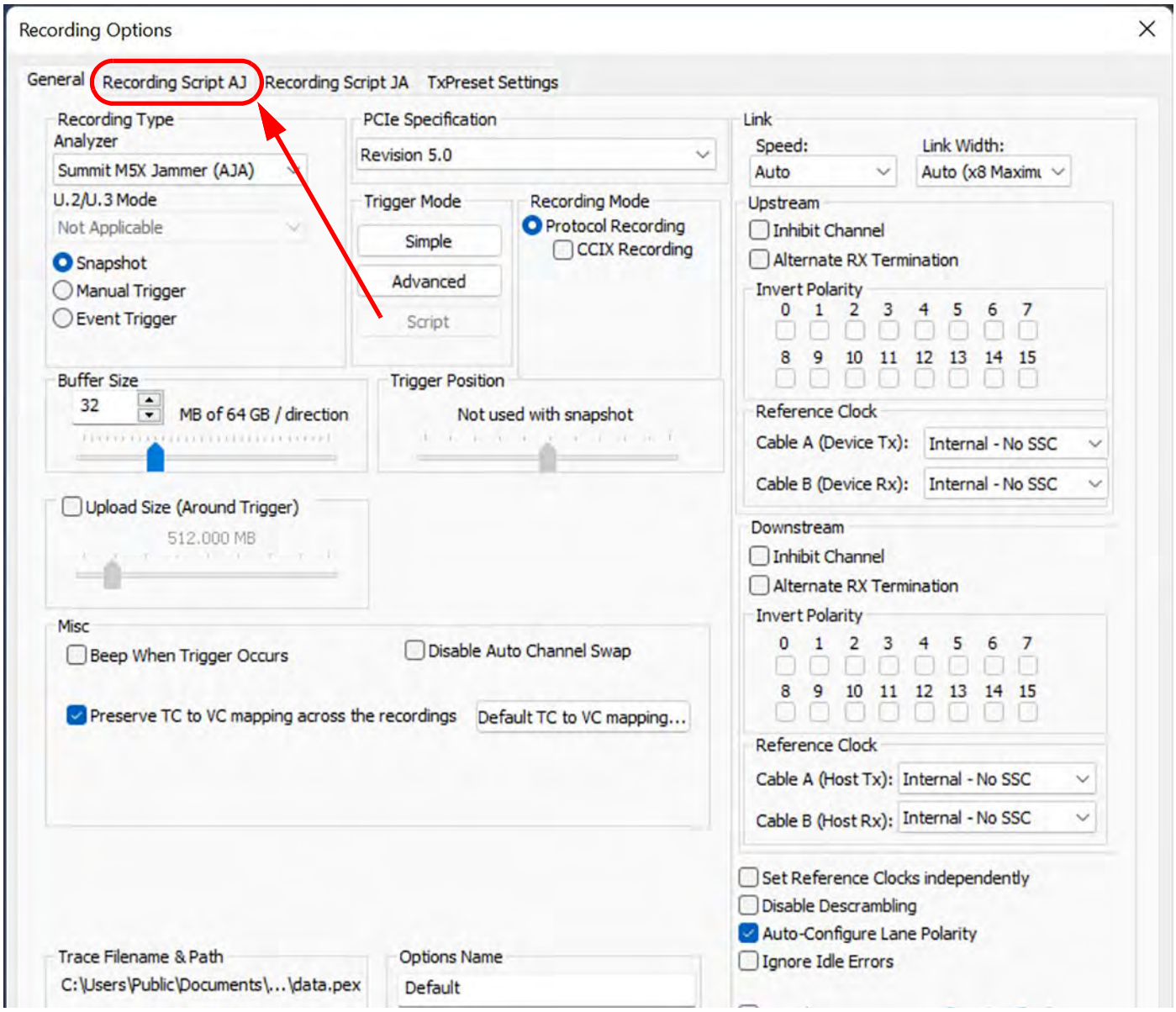


Figure 6.24: Recording Script Tab: Enabled

If you select the Recording Script tab the script to generate the complex Recording Options and Jammer Action will appear. See below in Figure 6.25 on page 272.

6.8 Recording Options and Jammer Action Script

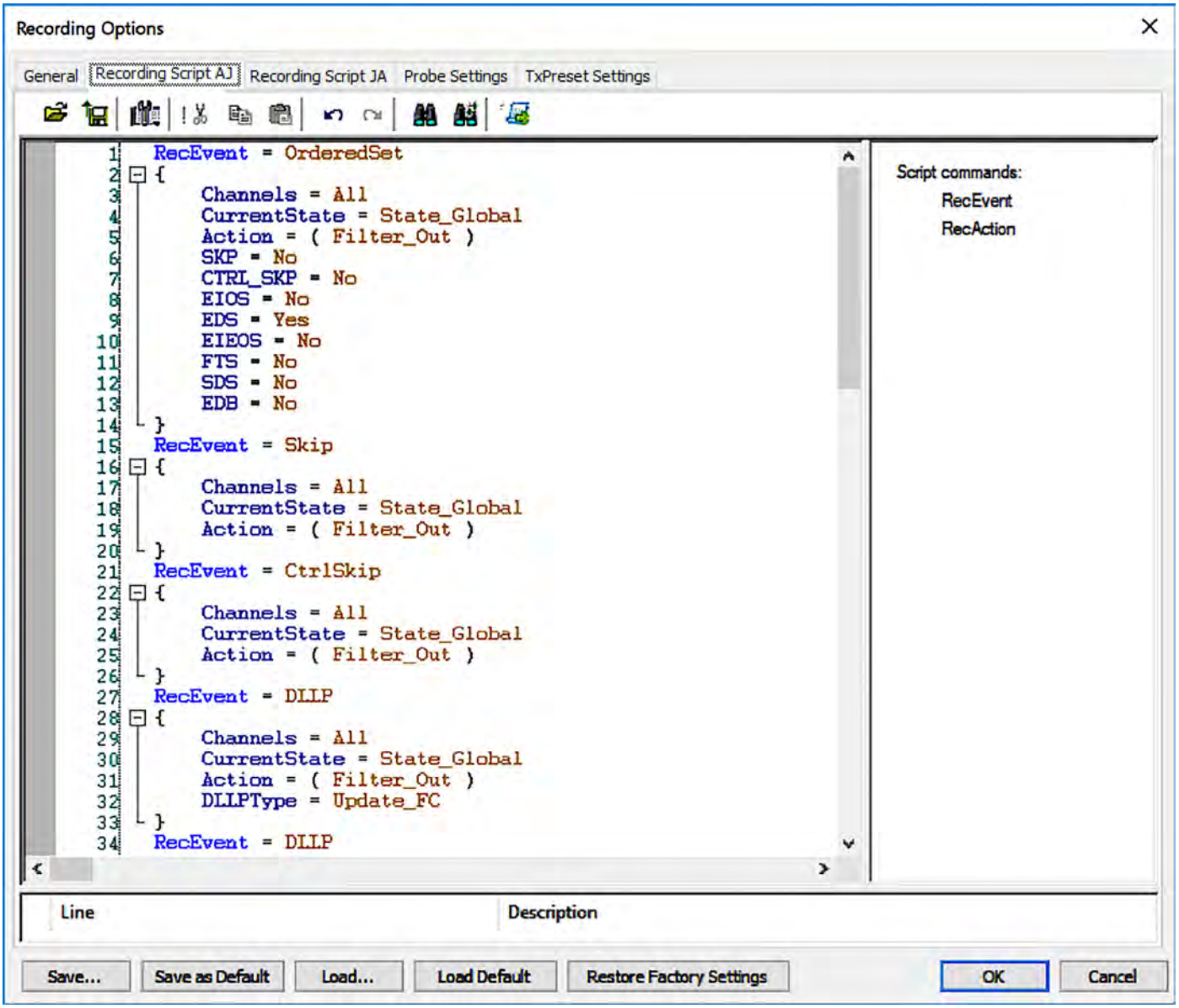


Figure 6.25: Recording Options and Jammer Action Script (1)

If you scroll down you'll see the rest of the script. See Figure 6.26 on page 273.

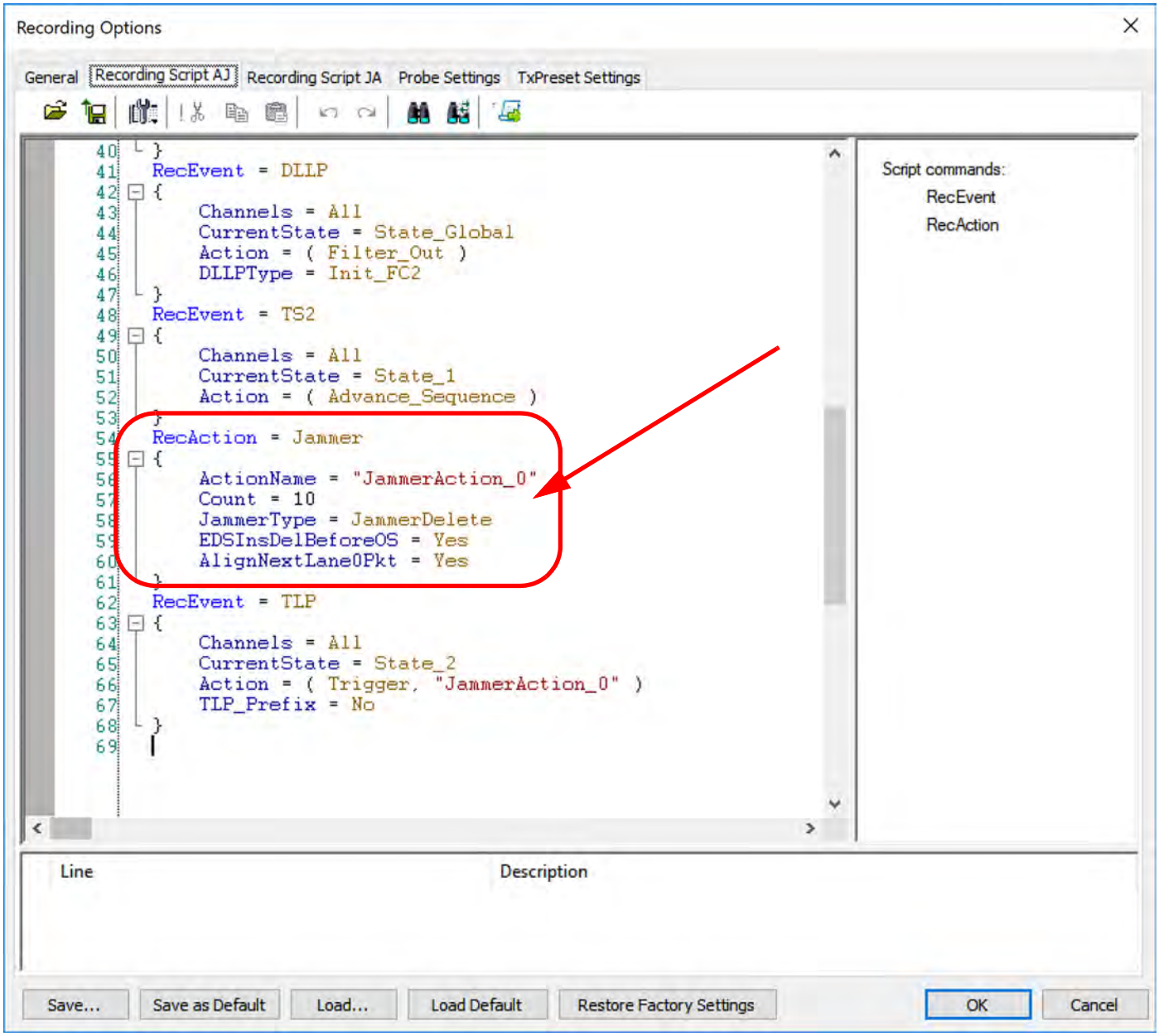


Figure 6.26: Recording Options and Jammer Action Script (2)

If you select the ActionName = "JammerAction_0" the details of the Jammer Action will appear on the right side of the dialog. See Figure 6.27 on page 274.

6.9 Updating Jammer Action Script

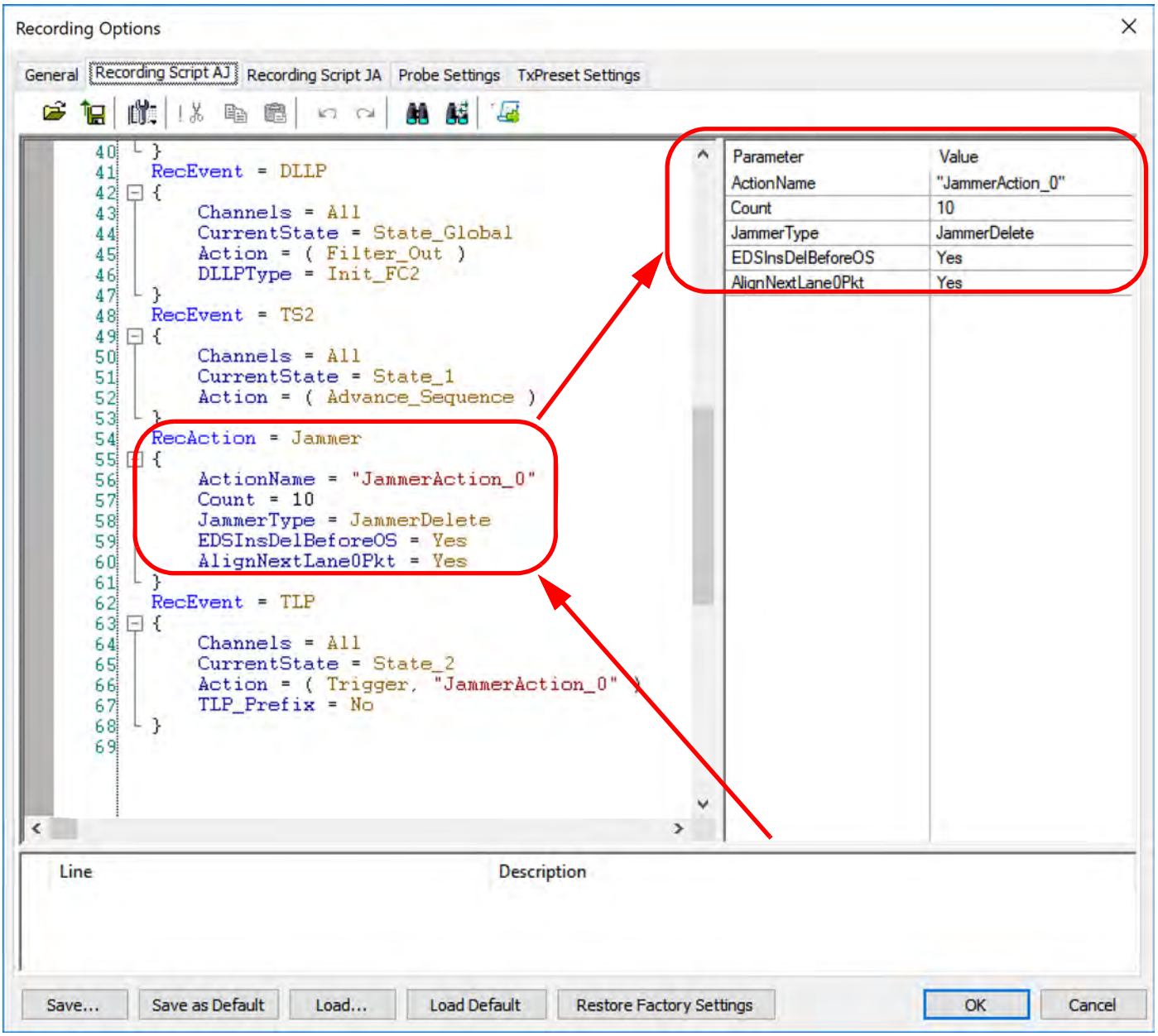


Figure 6.27: Updating Jammer Action Script

You can modify the script by selecting a Parameter Value as shown below in Figure 6.28 on page 275.

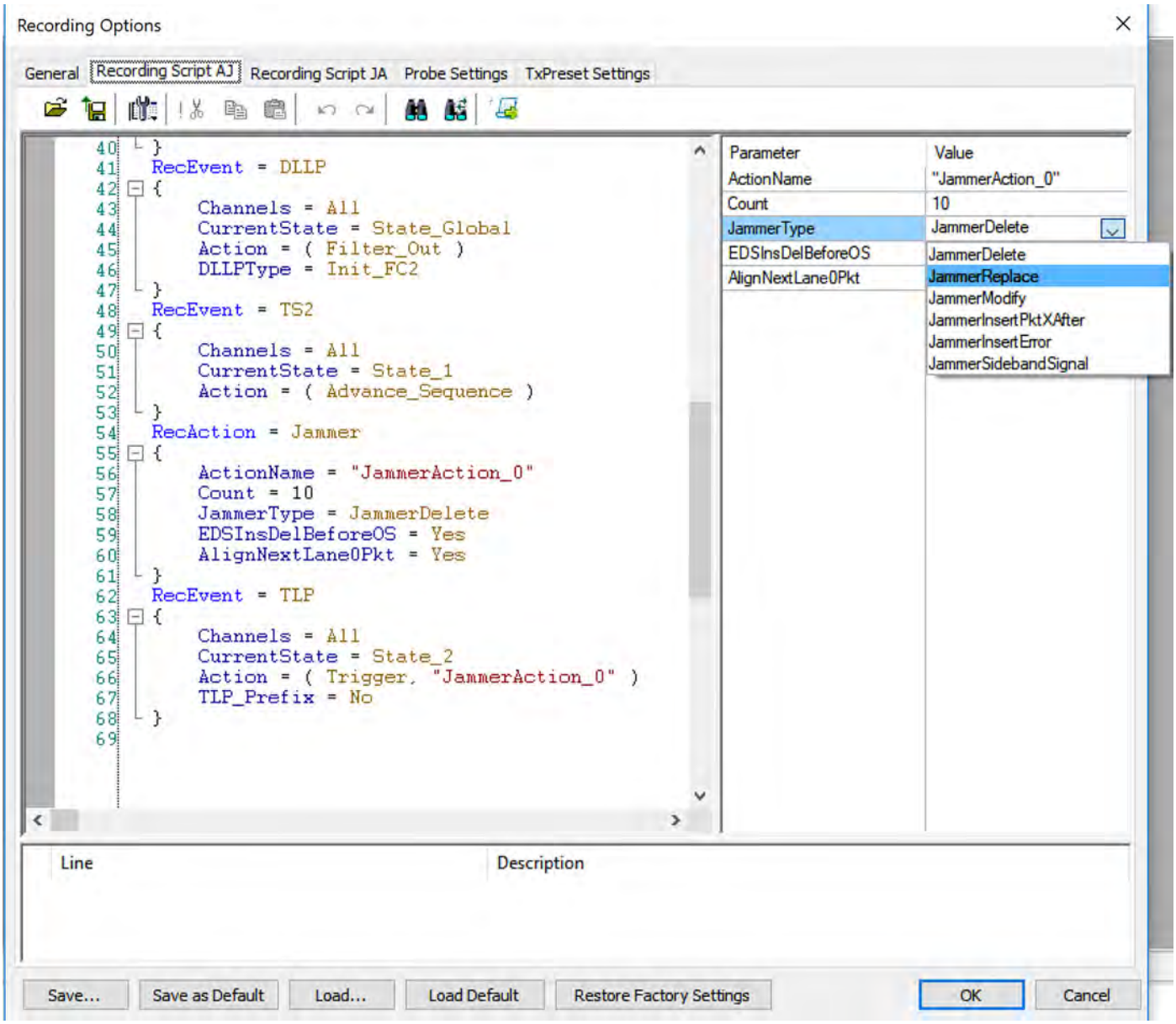


Figure 6.28: Updating Jammer Action from Delete to Replace

If you want to change the Jammer Action, just select the down arrow next to Jammer Delete and the other types of Jammer Actions will be available.

Select JammerReplace and the options for that Jammer Action will appear. See Figure 6.29 on page 276.

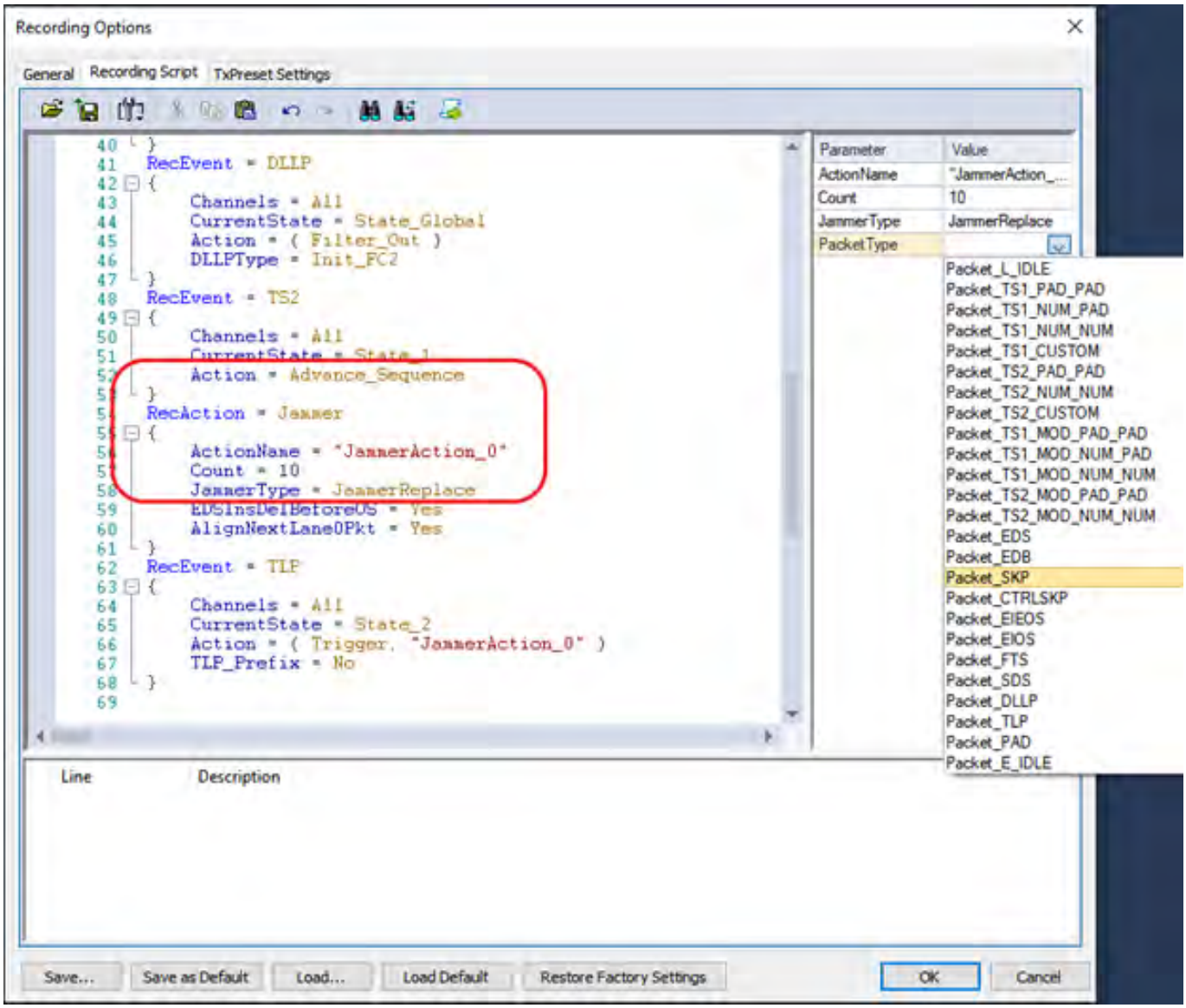


Figure 6.29: Packet Type: Packet_SKP Selected

After Packet_SKP has been selected the script will be updated. See Figure 6.30 on page 277.

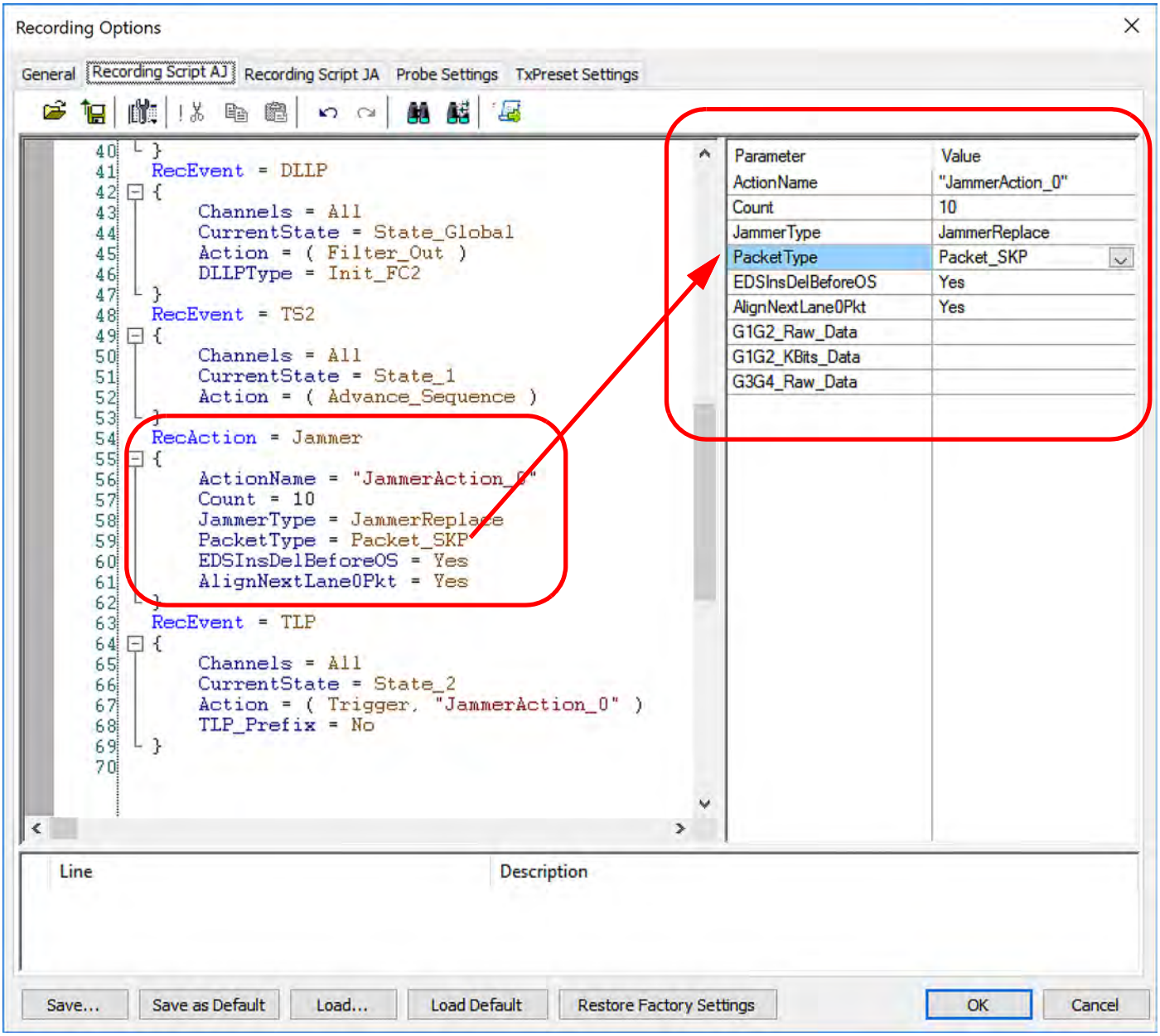


Figure 6.30: Packet_SKP Replaced Jammer Action

You can also modify the Count from 10 to 100.

Simply enter 100 into the Value block and move your cursor into the Count tab and click on the left mouse button. These actions will update the Count in the Script to 100. See Figure 6.31 on page 278.

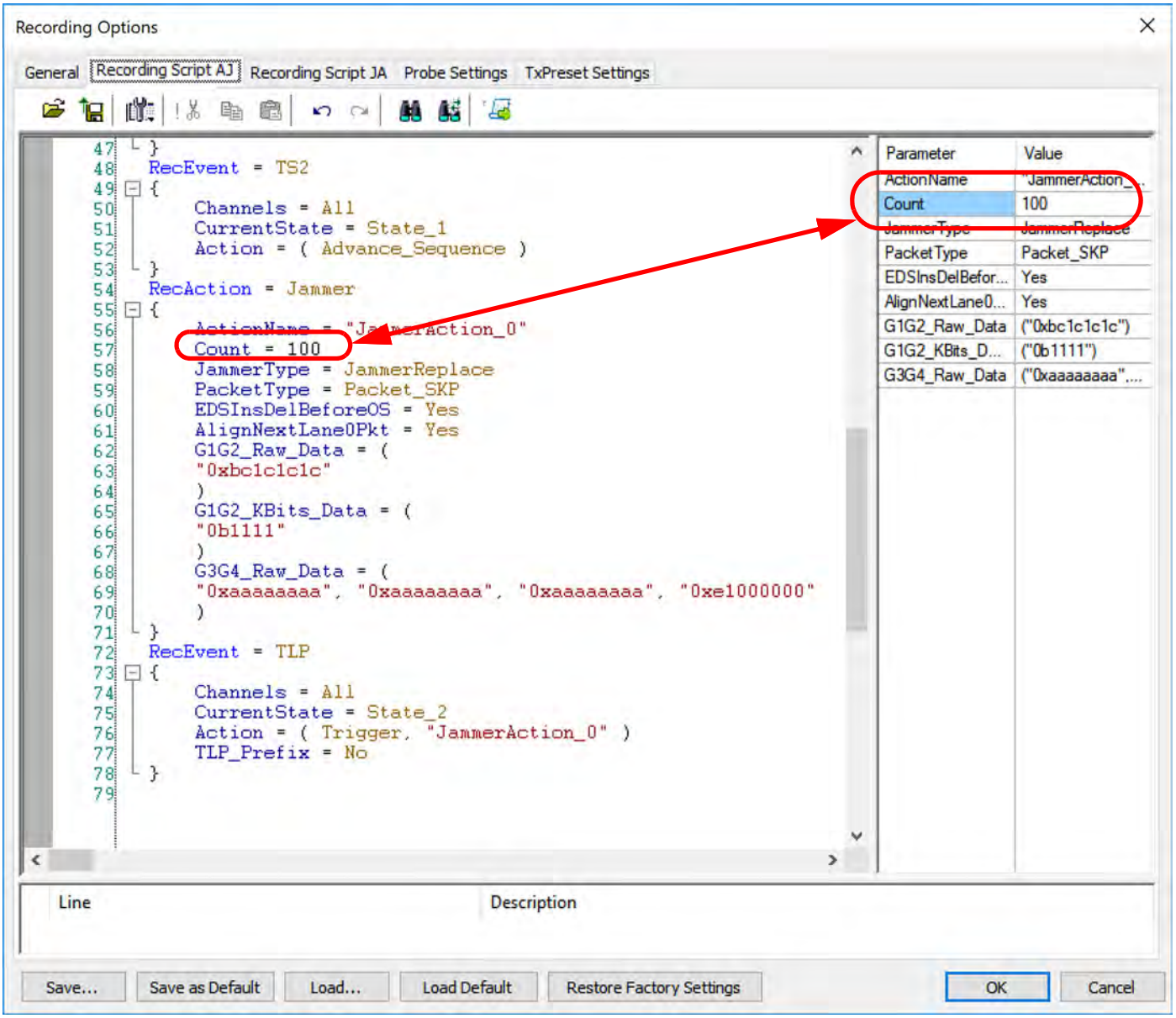


Figure 6.31: Change the Count from 10 to 100

Now that you've modified the script you can select the General tab and return to the GUI format.

6.10 Warning Message if Mistake in Jammer Script

If you make a mistake in the script, you'll see the following warning message and how to correct your mistake. See Figure 6.32.

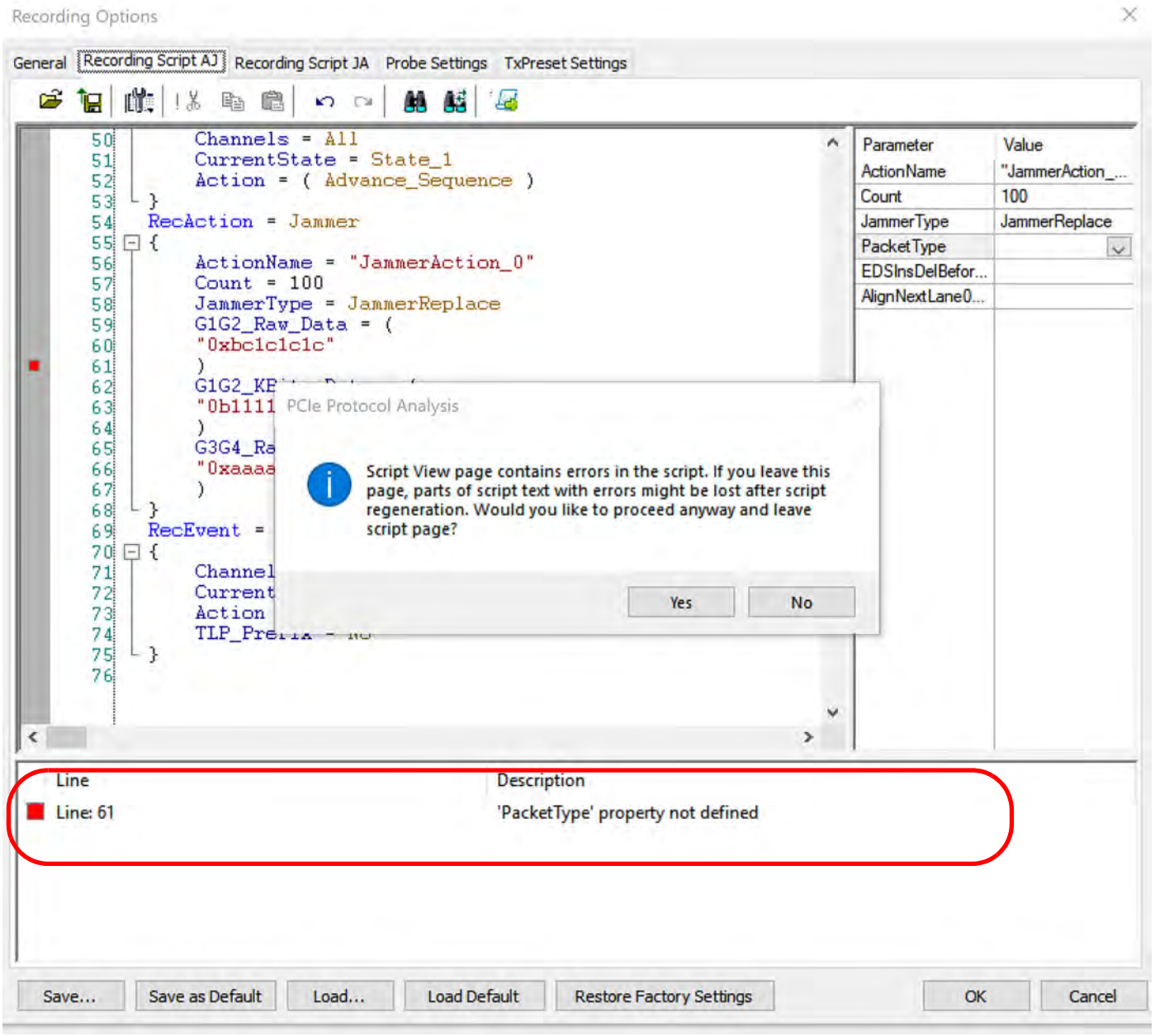


Figure 6.32: GUI Updated with Jammer Action

On Line 61 the Packet Type must be defined. Select No and correct the error. Once you do that and click “OK” you can return to the Recording Options -> Recording Script and see that your script has been modified and is correct. See below in Figure 6.33 on page 280.

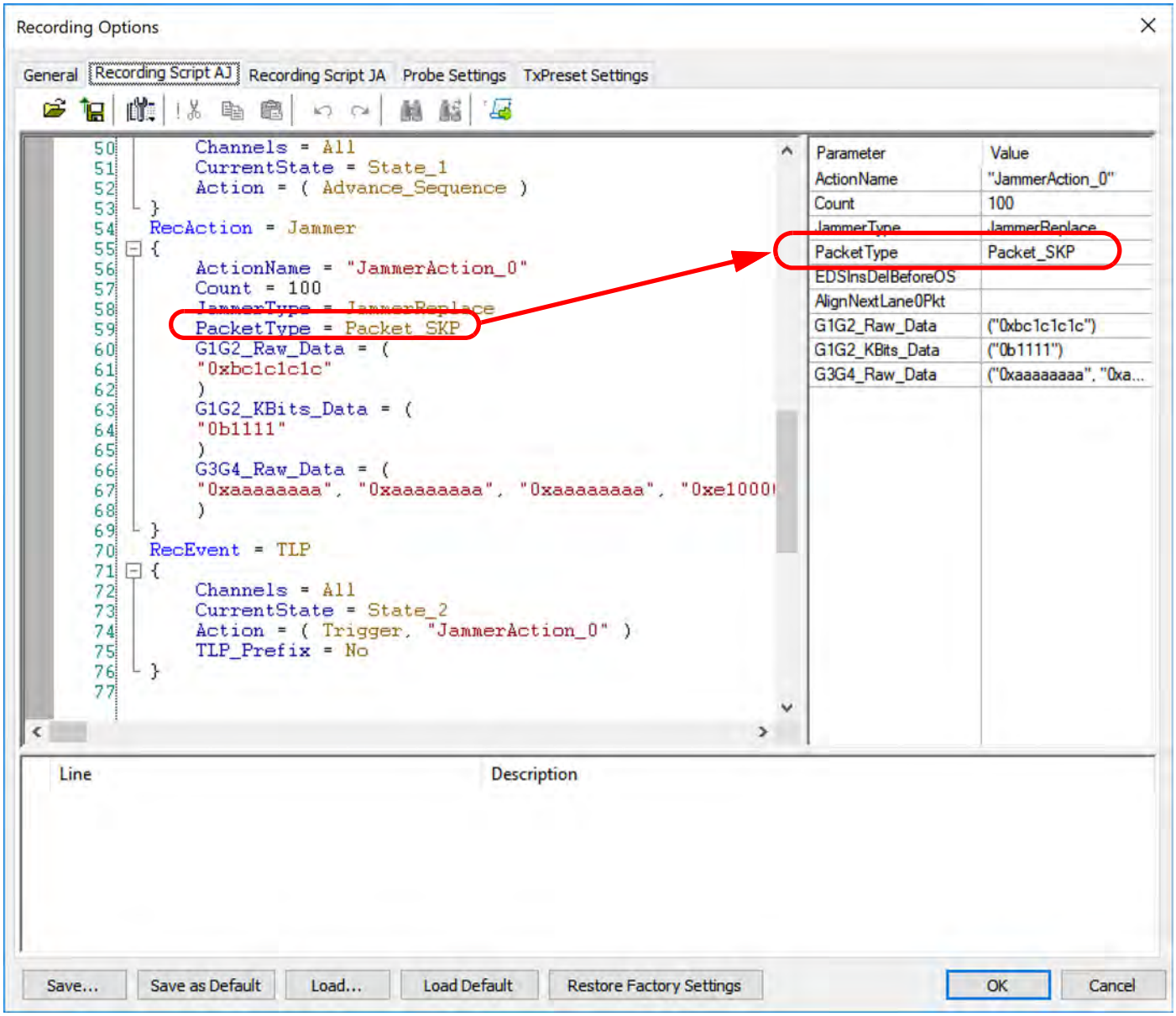


Figure 6.33: Corrected Script

Now you can select the General tab and go back to the GUI. You'll see the GUI has been updated to the changes you made in the script. See Figure 6.34 on page 281.

6.11 Updated GUI After Scripting Mistake Corrected

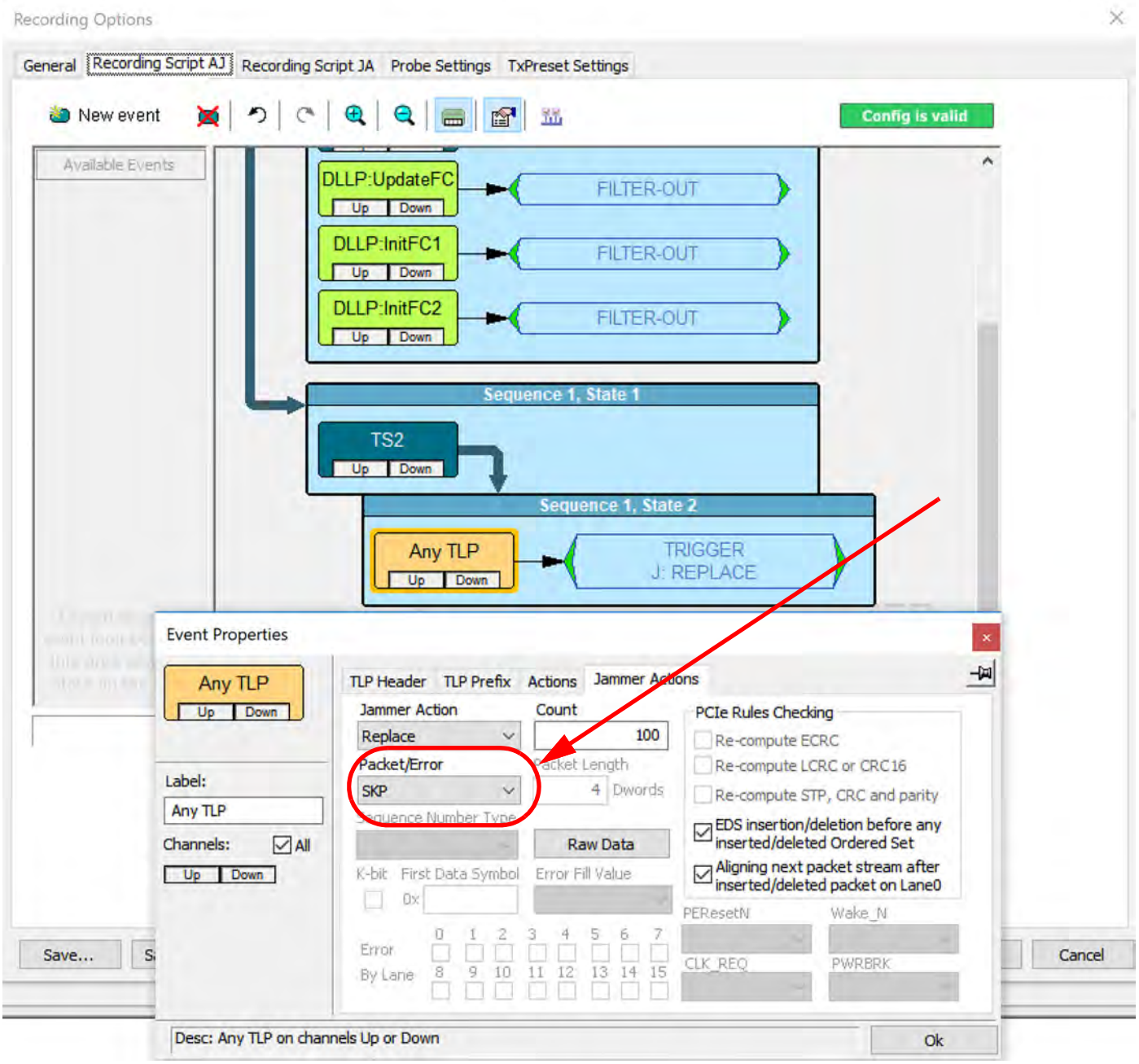


Figure 6.34: Corrected Script -> Corrected GUI

You can see that the Jammer Actions have been changed with a Packet of Type SKP.

6.12 Saving a Jammer Actions Script File

Another option you have is to Save the script file you've created with the Jammer Actions. See Figure 6.35.

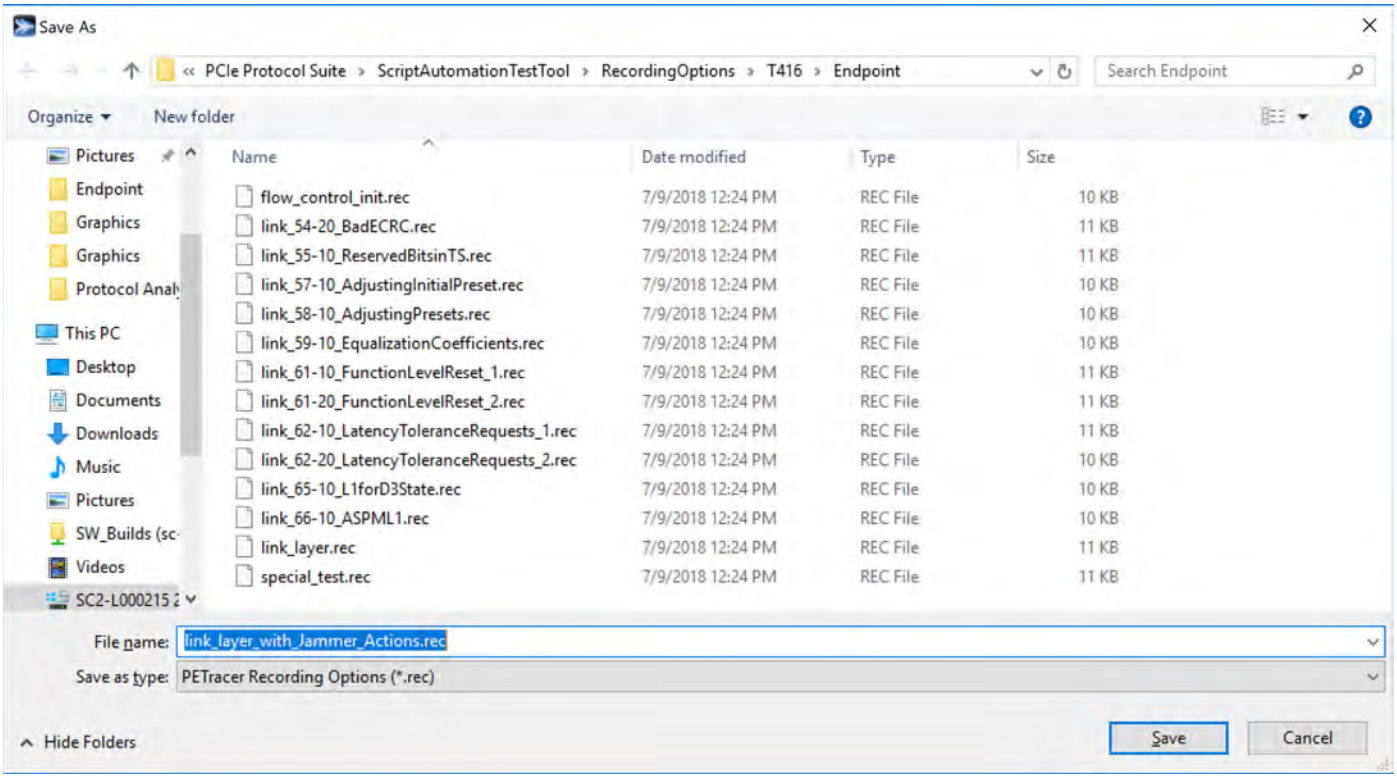


Figure 6.35: Save Jammer Script

Click on "Save" and the new Jammer Actions script will be saved, to be used in the future.

6.13 Loading a Jammer Script File

To load the Jammer Actions script file go to Setup -> Recording Options. Choose the Summit M5x and select Recording Rules.

Then select "Load" (see Figure 6.36).

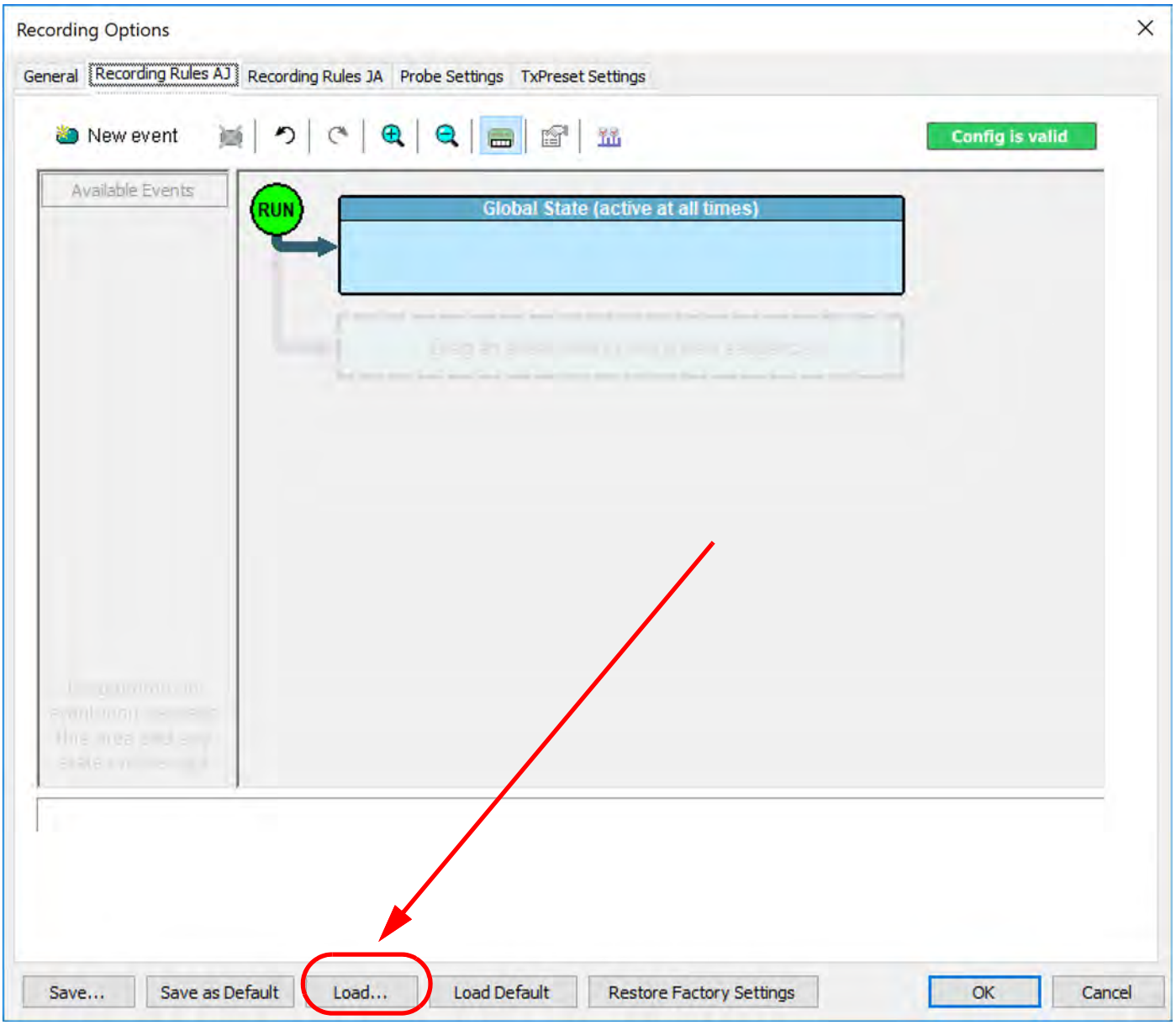


Figure 6.36: Loading a Jammer Action File

The Jammer Actions file will be available. See Figure 6.37 on page 284.

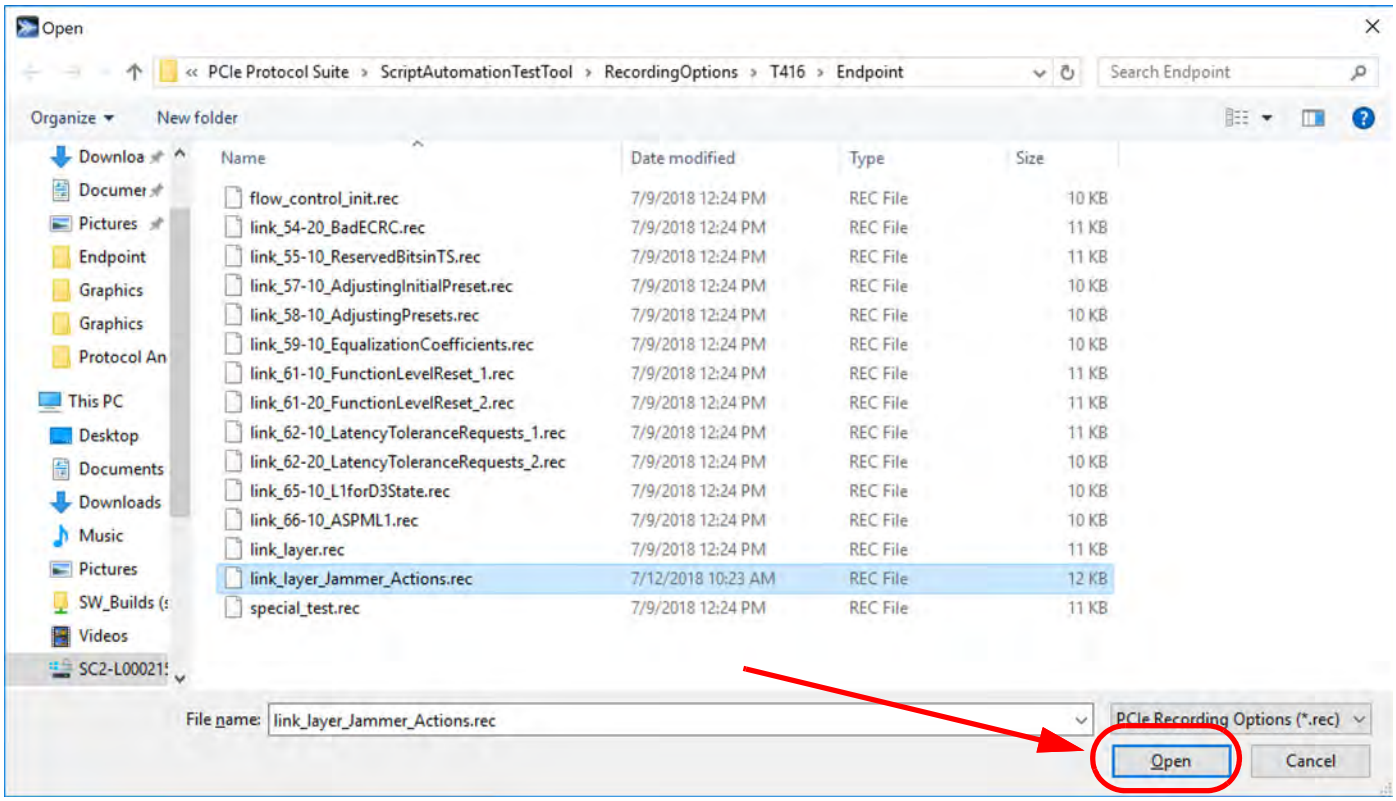


Figure 6.37: Jammer Actions File Loaded

Select the link_layer_Jammer_Actions.rec file and click on "Open". The file will be loaded as a script. See Figure 6.38 on page 285.

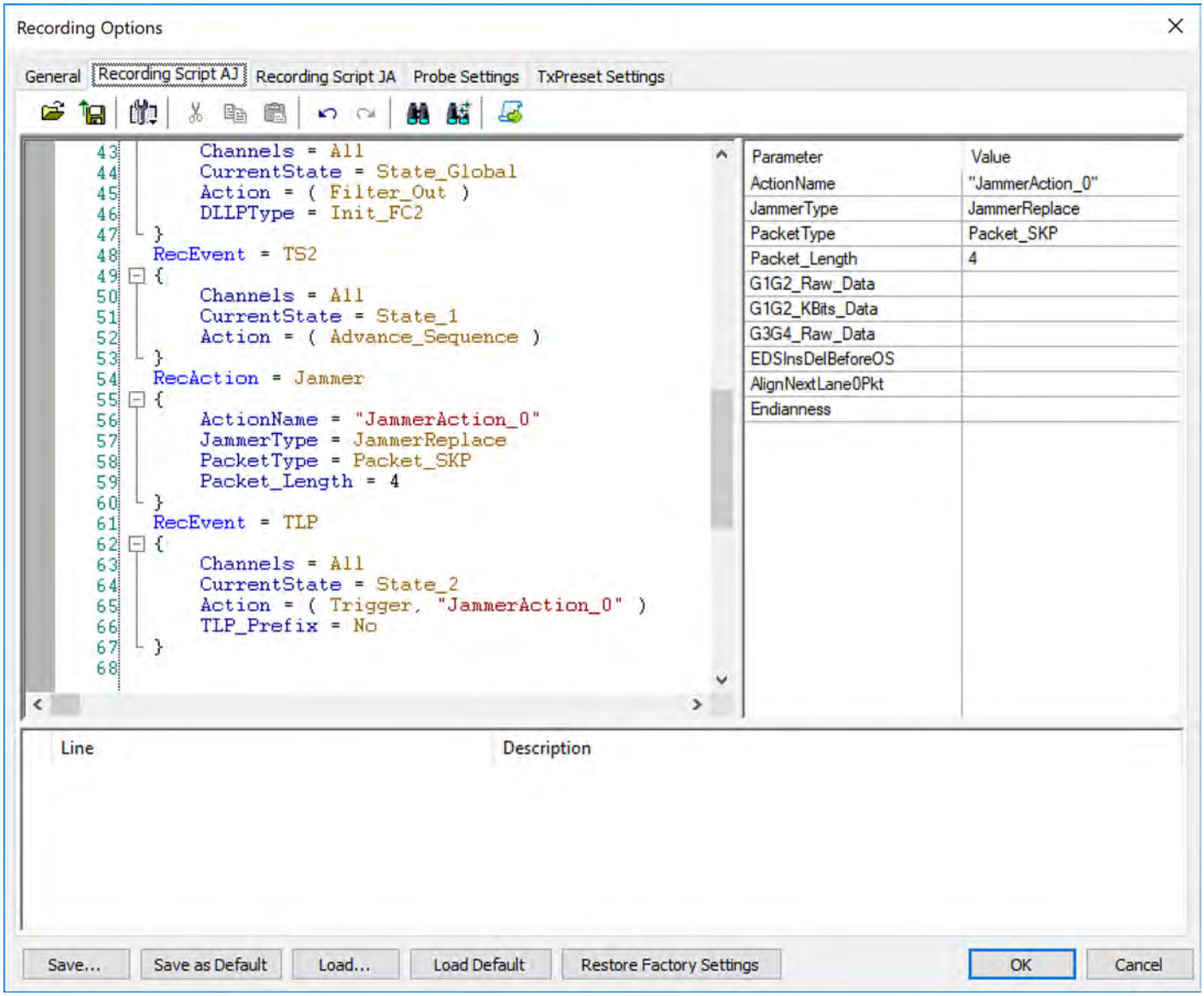


Figure 6.38: Jammer Action Script Loaded

If you want to see it in the GUI format, select General -> Advanced (see Figure 6.39 on page 286).

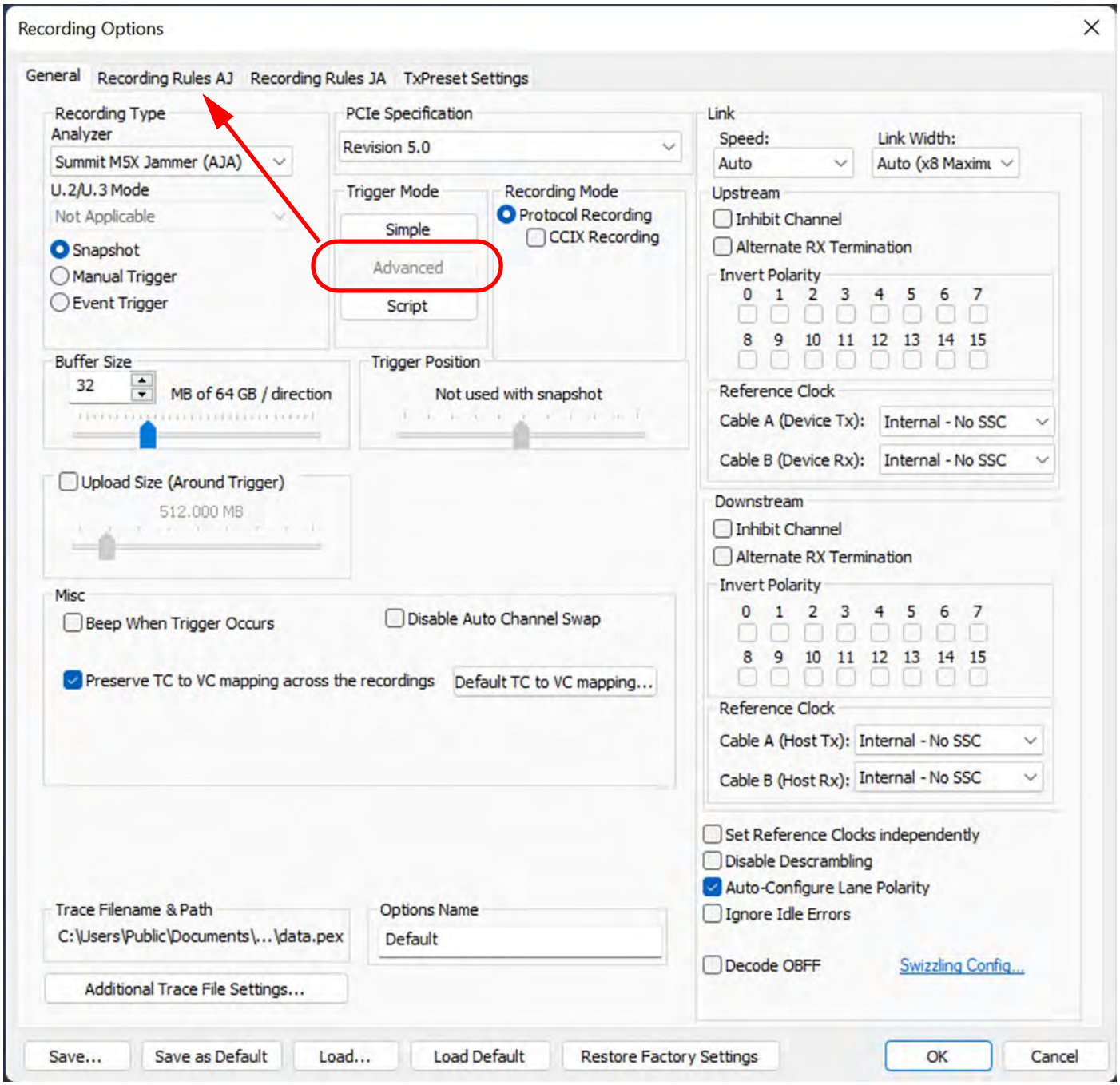


Figure 6.39: Recording Options: General -> Advanced

Select Advanced and the Recording Script tab will change to Recording Rules.

Select the Recording Rules tab and the GUI for the Jammer Actions file will pop up. See Figure 6.40 on page 287.

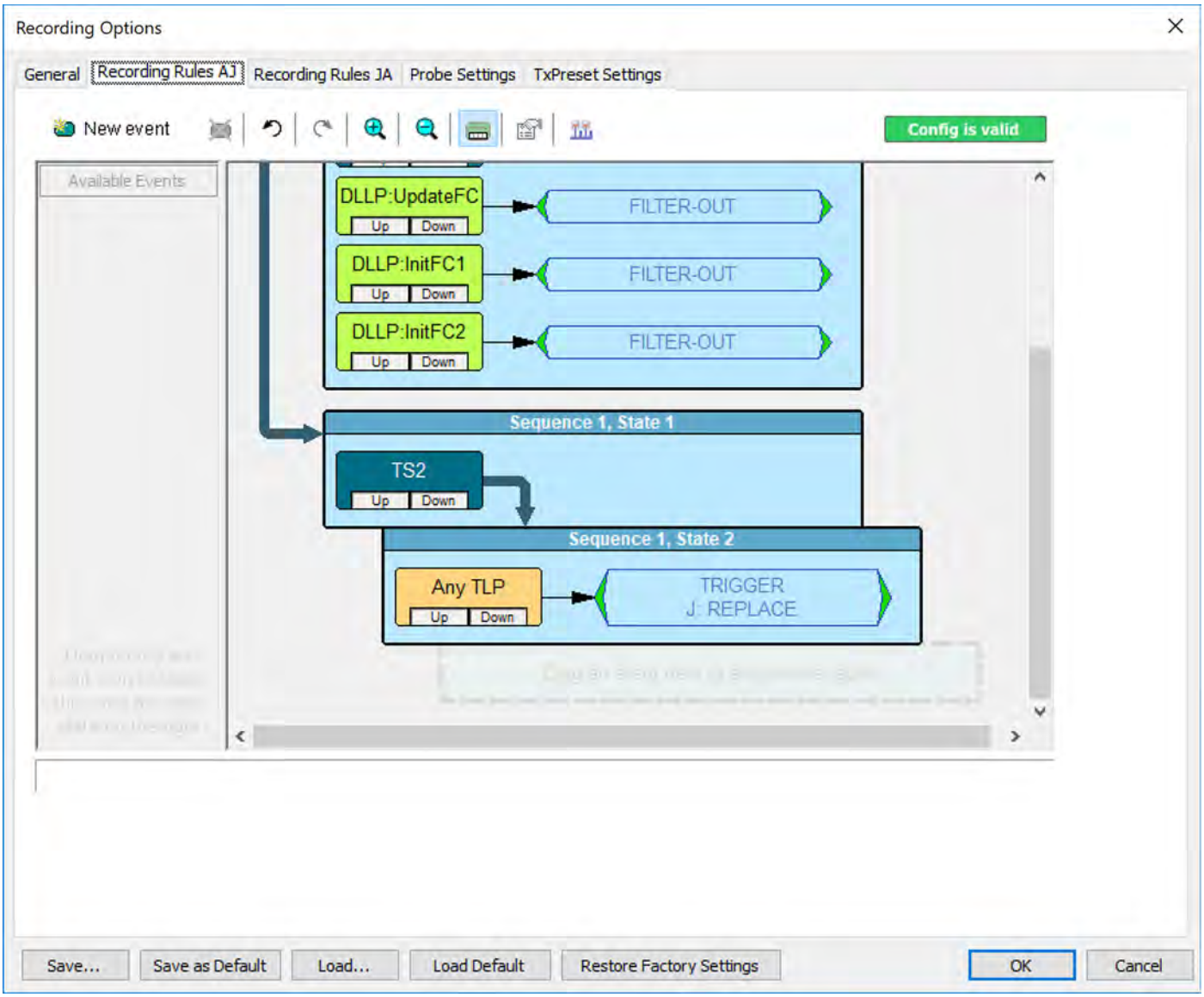


Figure 6.40: Jammer Action Script Loaded -> GUI

6.14 Examples of Scripting for Common Events with Jammer Actions

The following are examples common events and the script syntax for Jammer Actions:

TABLE 6.10: Jammer Actions

Event	Event Type
Link State	Speed Change
Ordered Set	TS2
Framing Token	EDS
Errors	Symbol Error

TABLE 6.10: Jammer Actions

Event	Event Type
DLLP	Any
TLP	Any
NVMe Register	
NVMe Command Submission	Any
NVMe Command Completion	Any

There are seven types of Jammer Actions which can be associated with any of the Events shown above:

- None
- Delete
- Replace
- Modify
- Insert Pkt X after
- Insert Error
- Sideband Signal

6.14.1 Link State: Speed Change

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

Then select New Event -> Link State -> Speed Change -> Insert Pkt X after

See GUI dialog below (see Figure 6.41 on page 289).

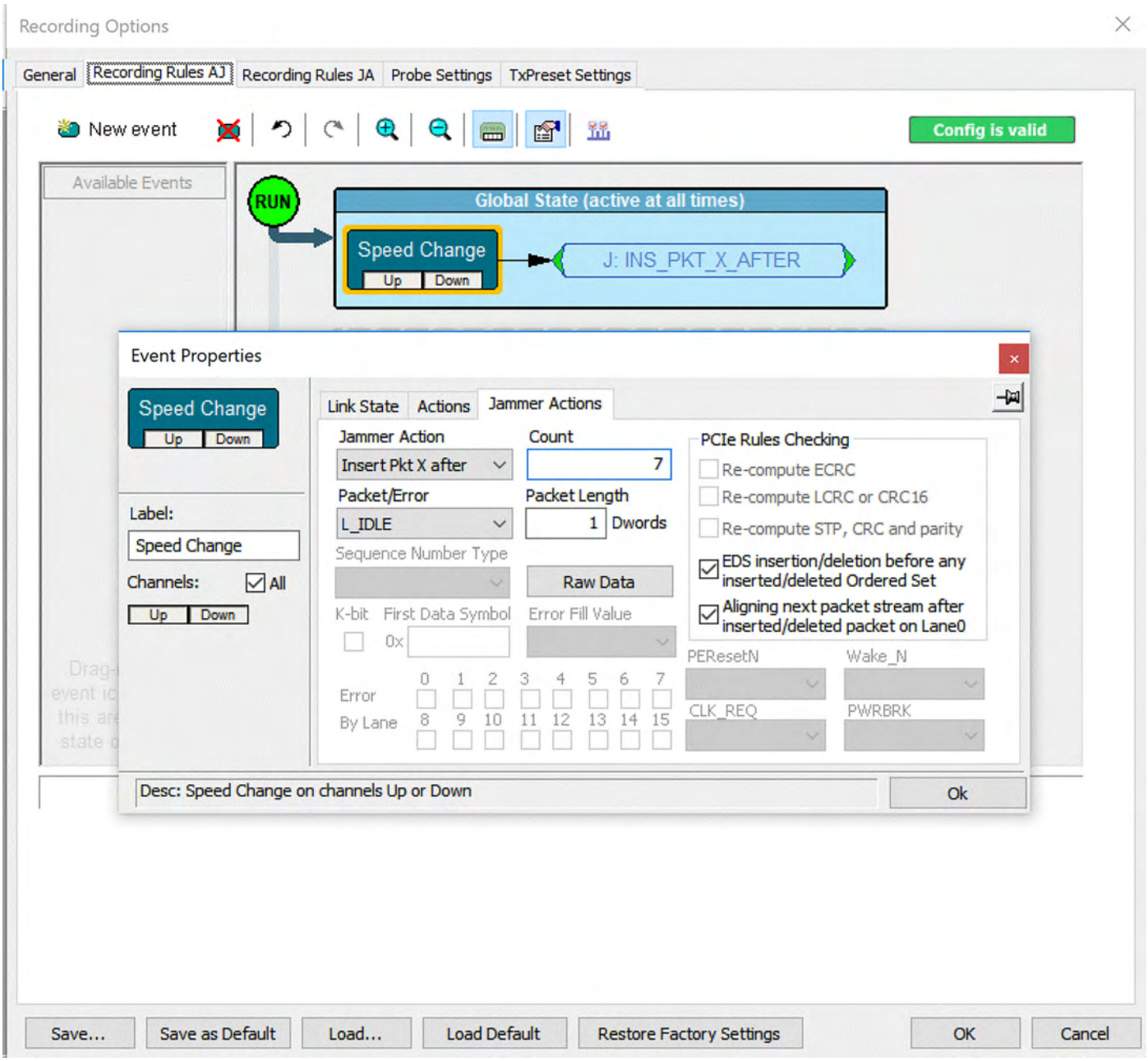


Figure 6.41: New Event: Link State -> Speed Change

Select the General tab then select the Script button under Trigger Mode. See Figure 6.42 on page 290.

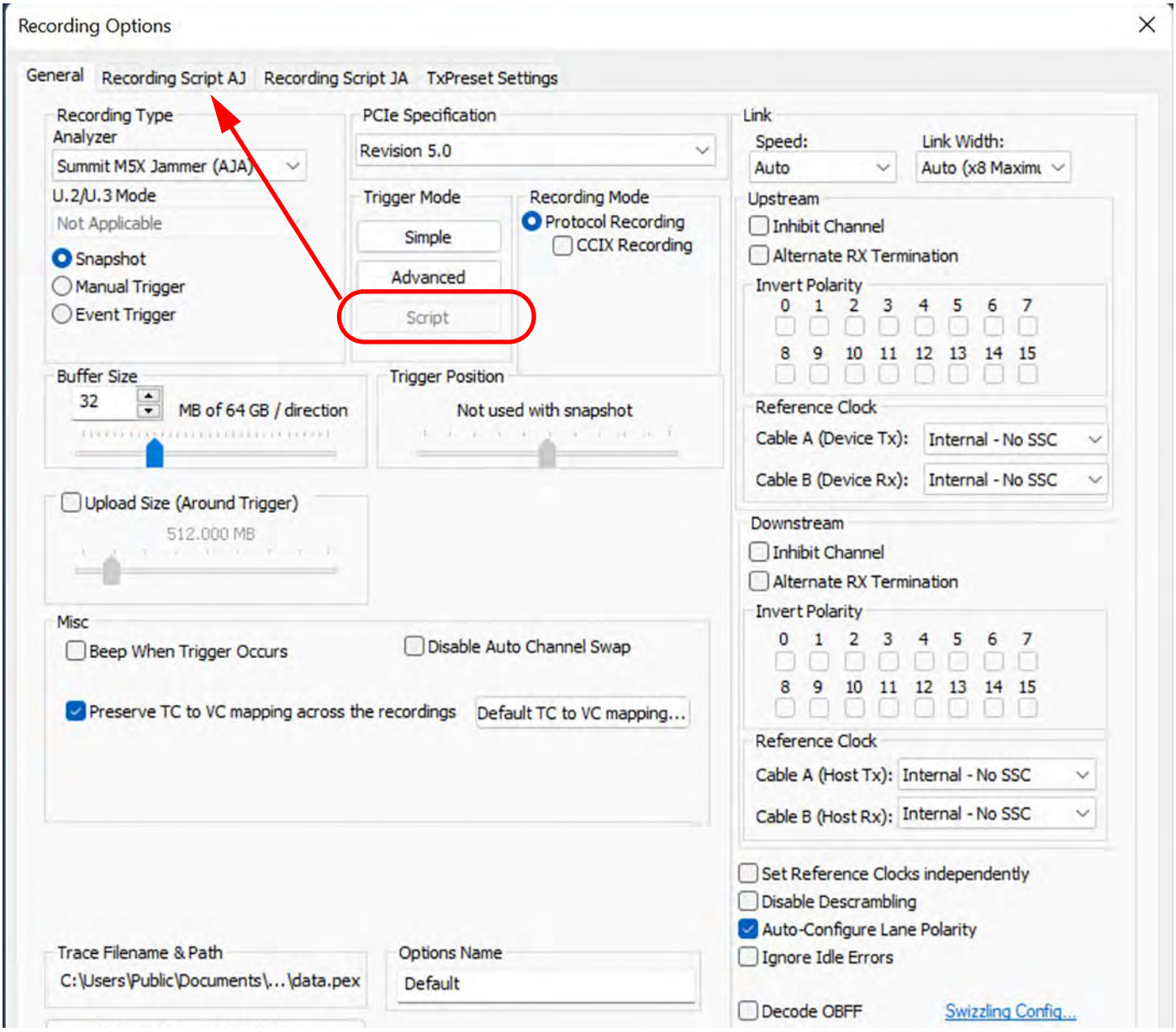


Figure 6.42: New Event: Link State -> Speed Change -> Insert Packet

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 6.43 on page 291.

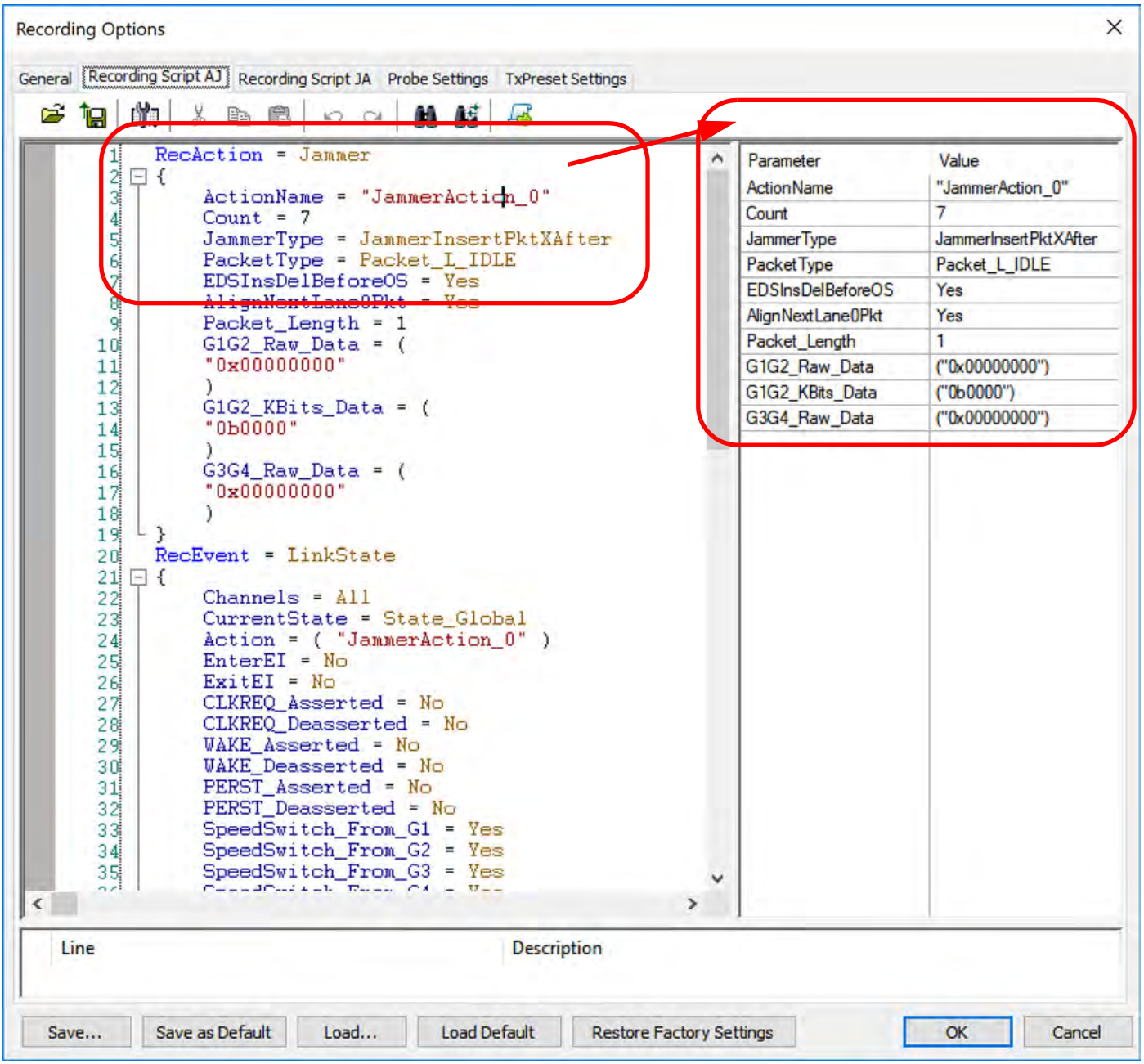


Figure 6.43: Jammer Action: Speed Change -> Insert Packet

6.14.2 Ordered Set: TS2

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Ordered Set -> TS2 -> Insert Error

See GUI dialog below in Figure 6.44.

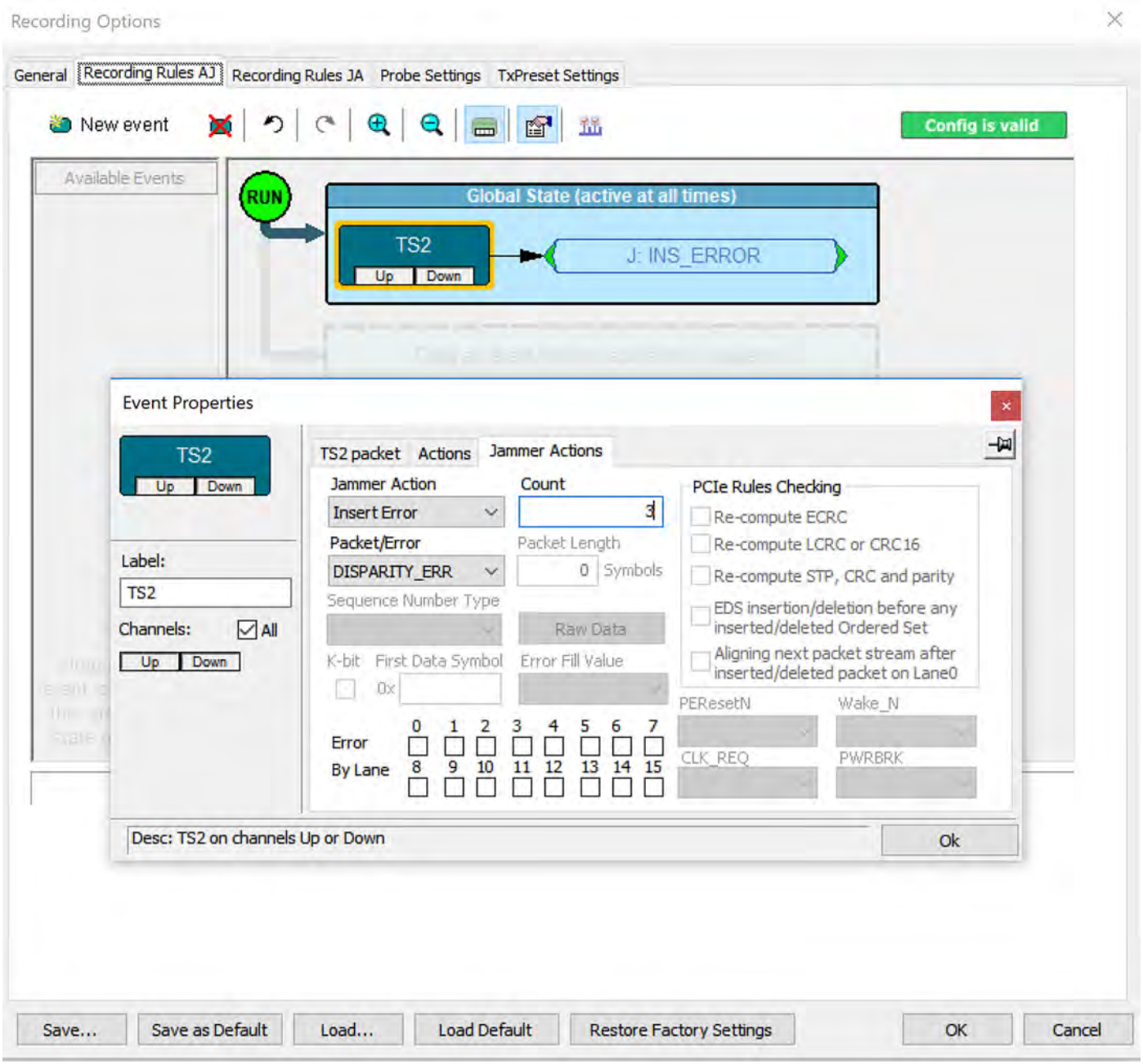


Figure 6.44: New Event: Ordered Set -> TS2 -> Insert Error

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 6.45 on page 293.

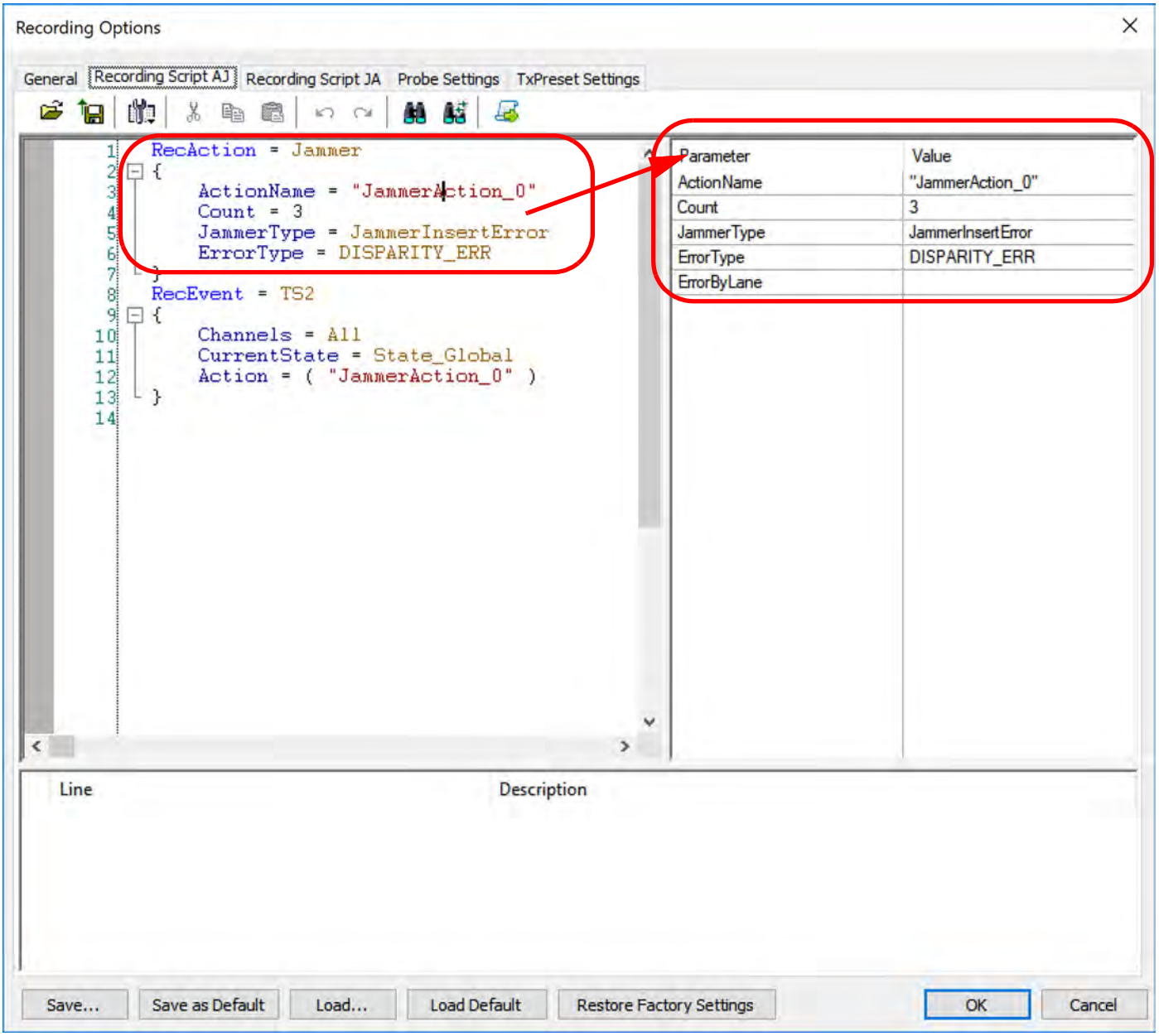


Figure 6.45: Jammer Action: Ordered Set -> TS2 -> Insert Error -> Diparity Error

6.14.2.1 Ordered Set: TS1

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Ordered Set -> TS1 -> Replace. See Figure 6.46 on page 294.

By default, jamming is enabled for all 16 lanes. It is possible to change jamming lanes by set checkboxes in the “Replace By Lane” section.

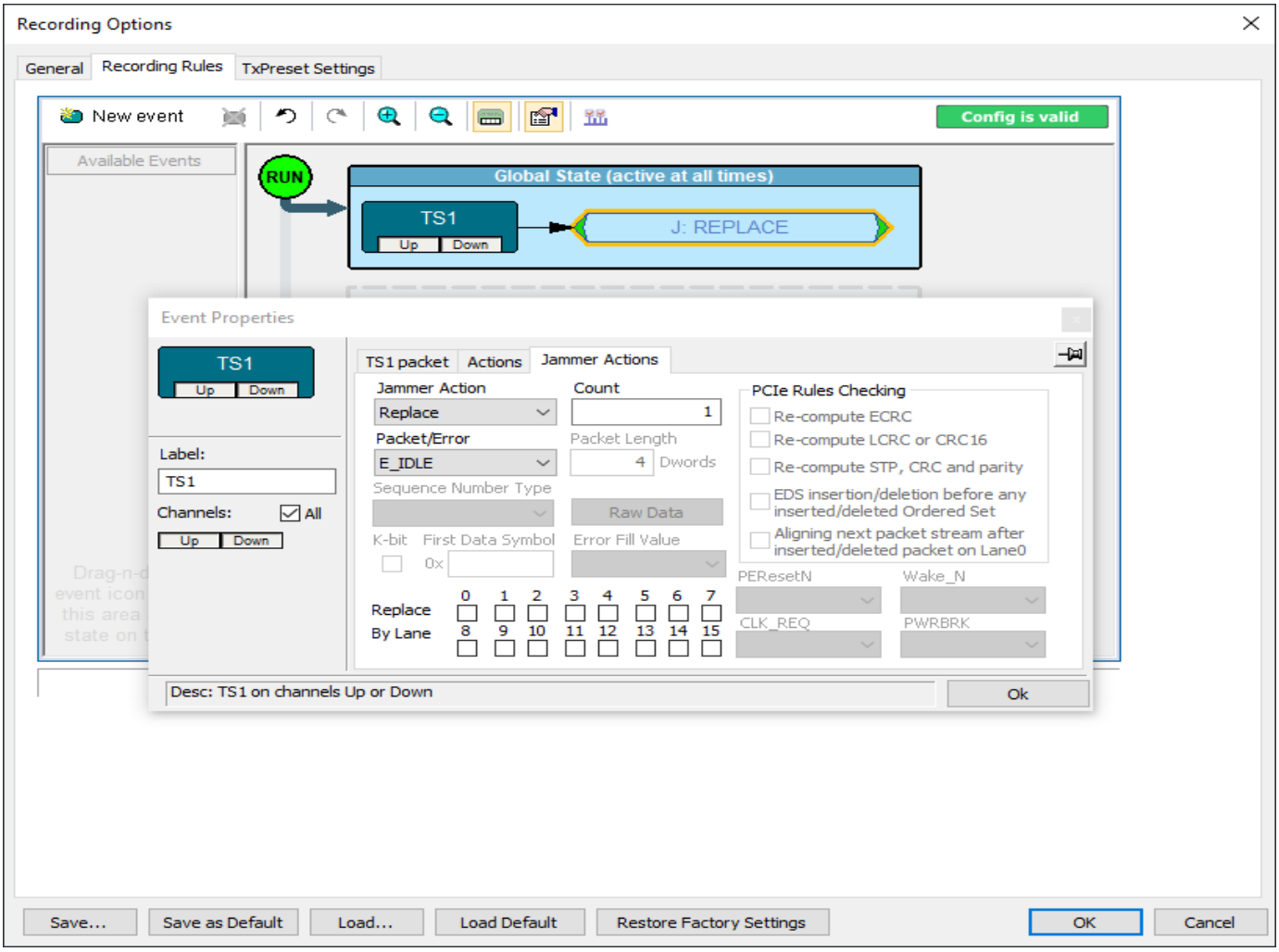


Figure 6.46: Jammer Action: Ordered Set -> TS1 -> Replace

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 6.47 on page 295.

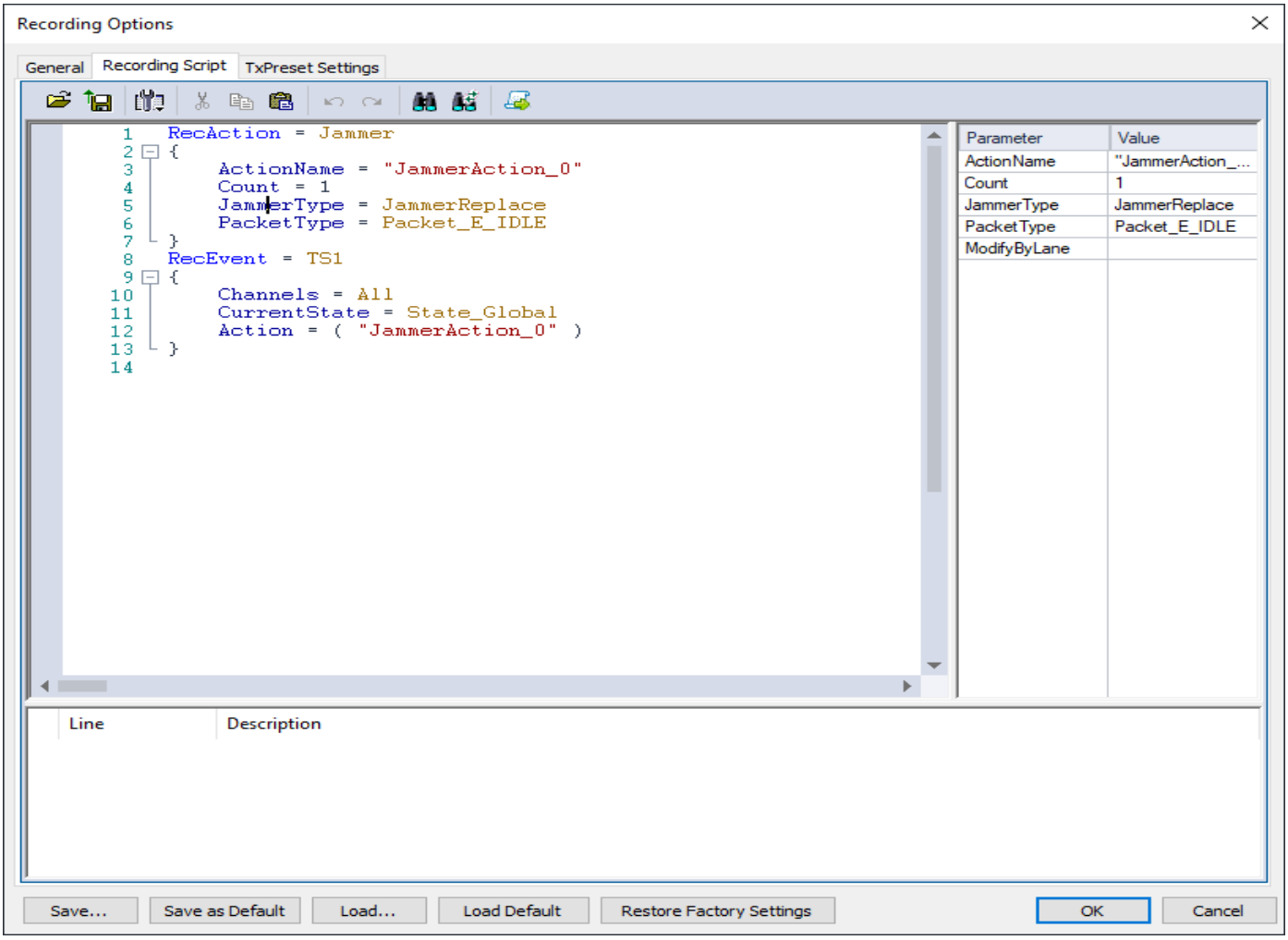


Figure 6.47: Jammer Action: Ordered Set -> TS1 -> Replace-> E_IDLE

6.14.3 Framing Token: EDS

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Framing Token -> EDS -> Delete

See GUI dialog below in Figure 6.48.

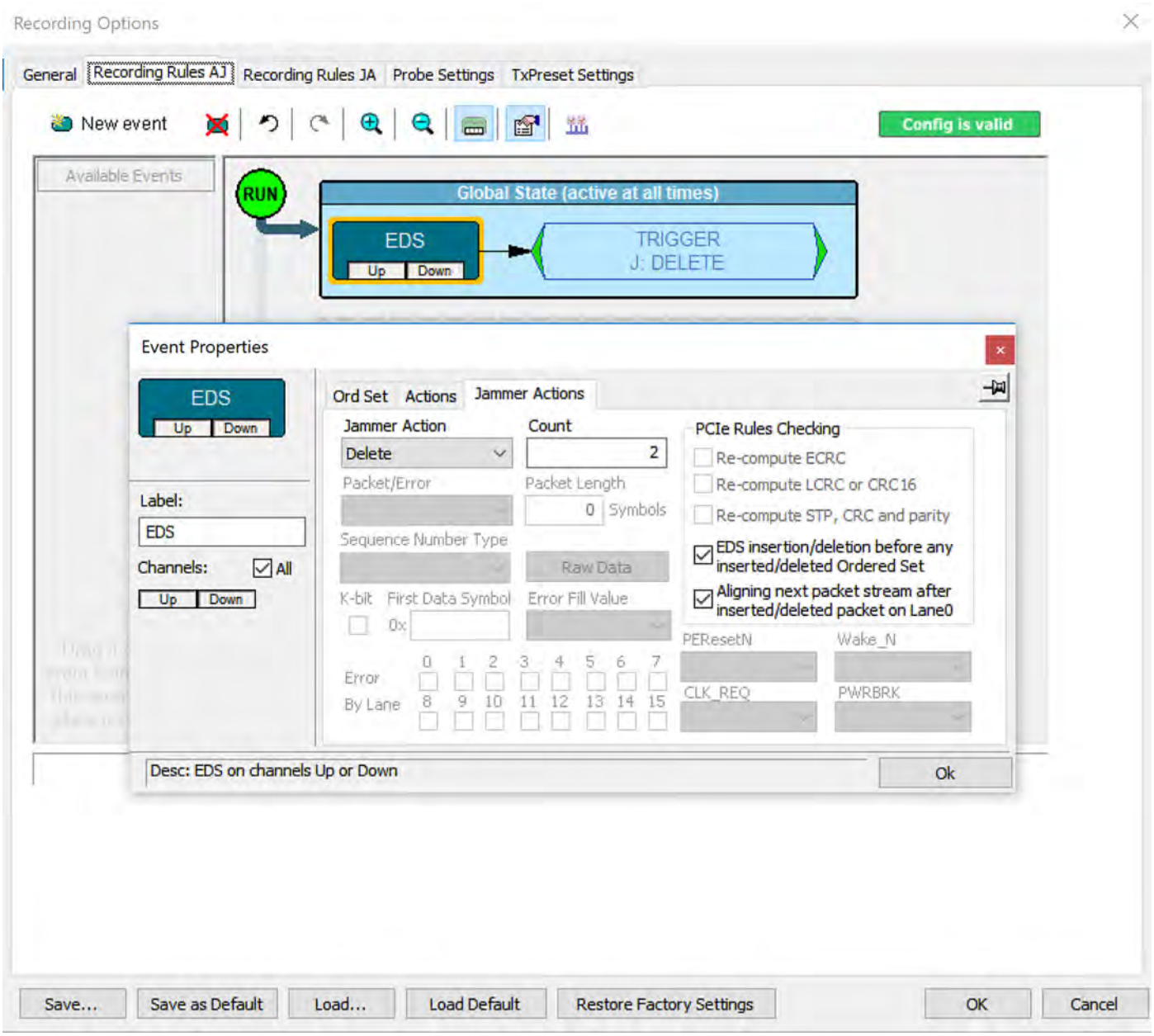


Figure 6.48: New Event: Framing Token -> EDS -> Delete

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 6.49 on page 297.

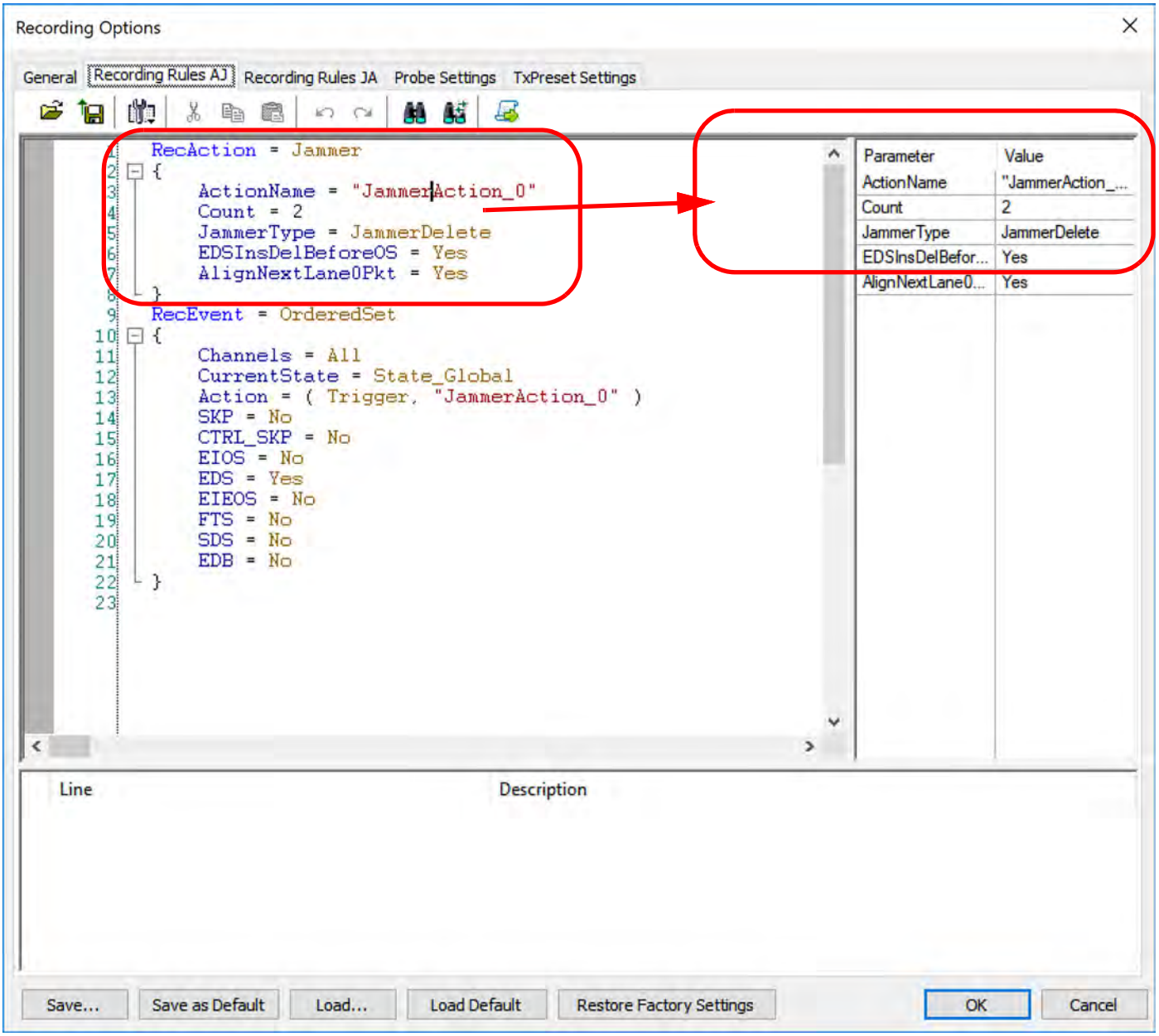


Figure 6.49: New Event: Framing Token -> EDS -> JammerDelete Script

6.14.4 Errors: Symbol Error

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Errors -> Symbol Error-> Insert Pkt X after

See GUI dialog below in Figure 6.50.

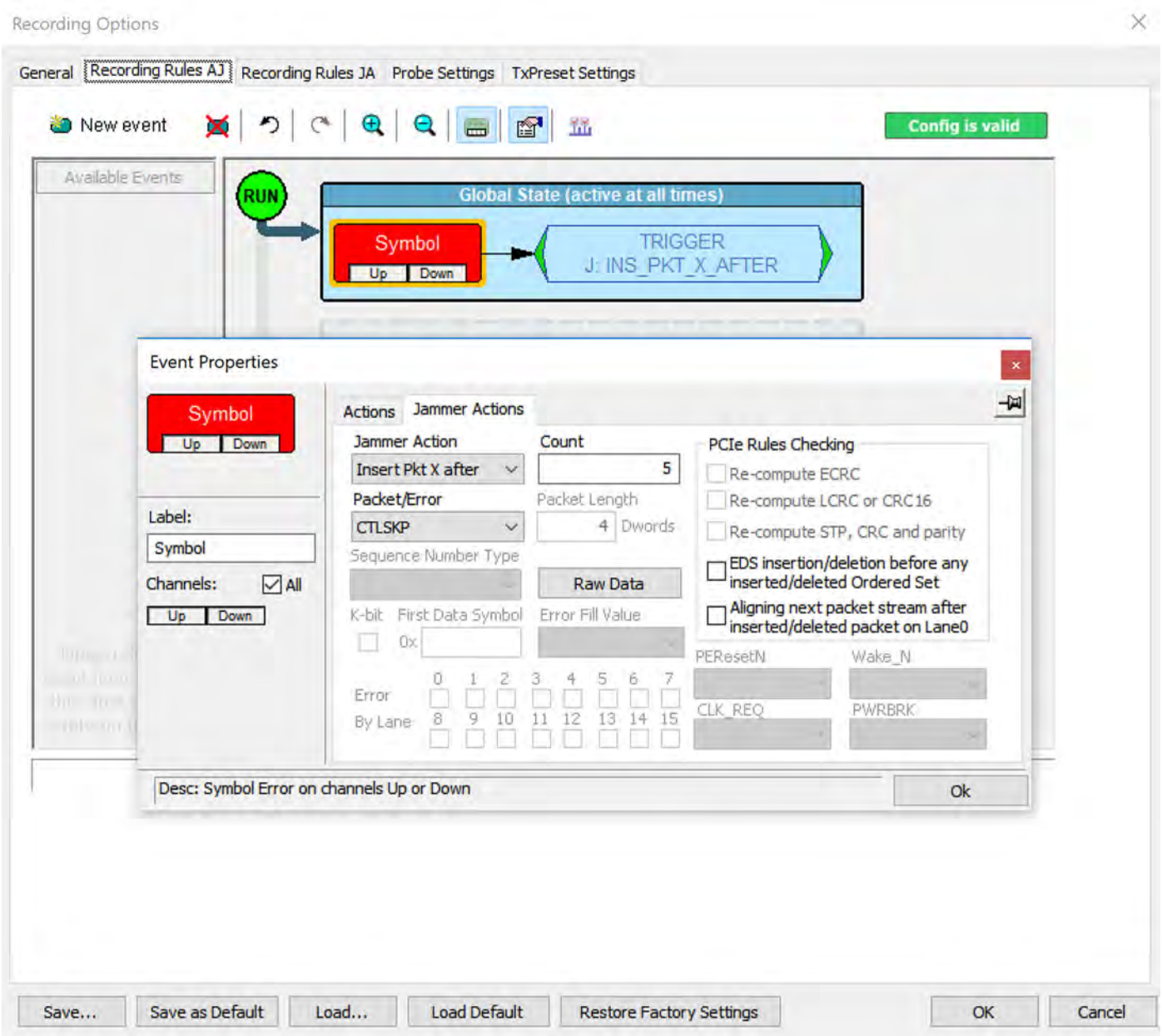


Figure 6.50: New Event: Errors -> Symbol Error-> Insert Pkt X after

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 6.51 on page 299.

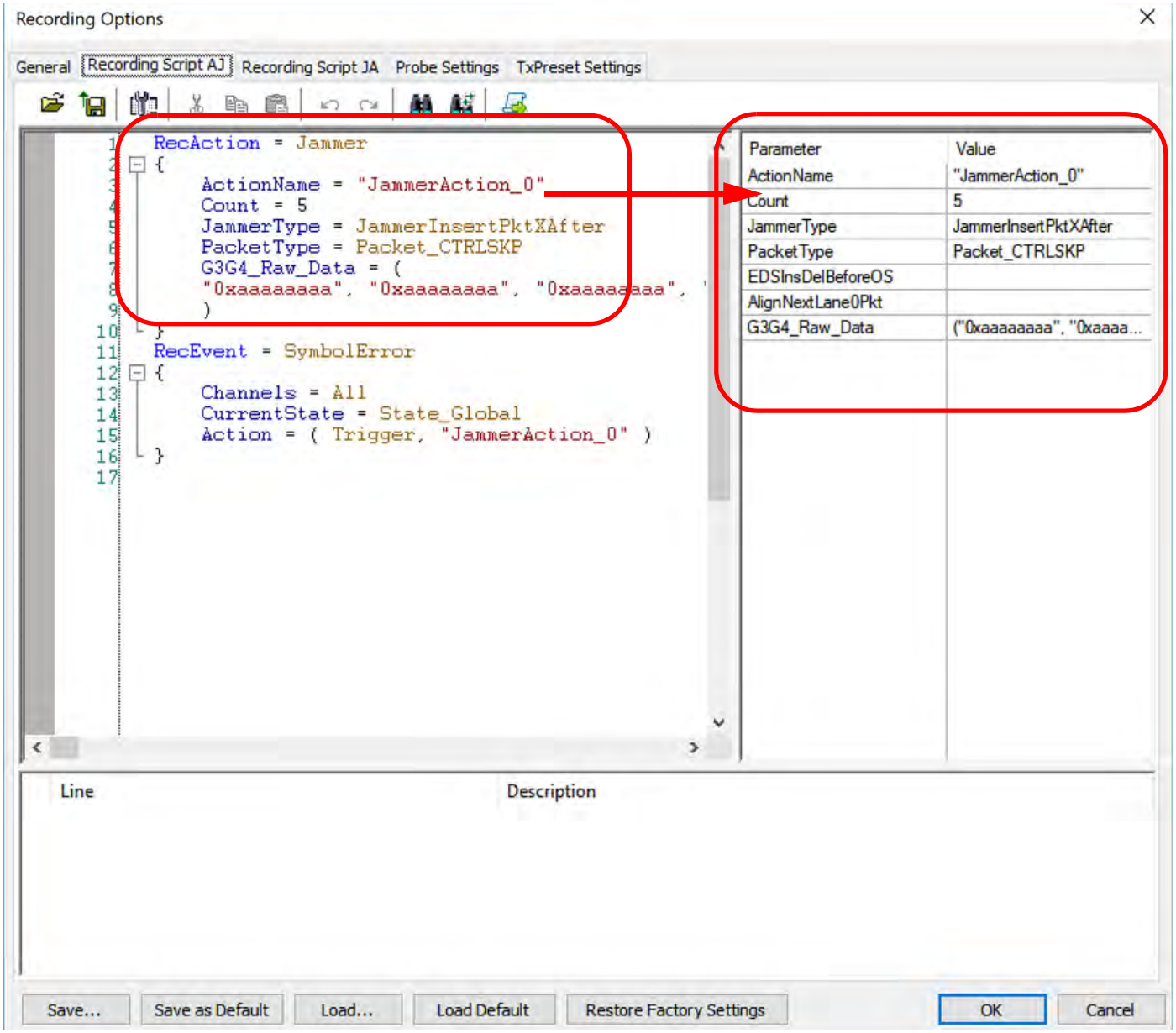


Figure 6.51: New Event: Errors -> Symbol Error-> Insert Script

6.14.5 DLLP: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> DLLP -> Any -> Replace (TS2_NUM_NUM)

See GUI dialog below in Figure 6.52.

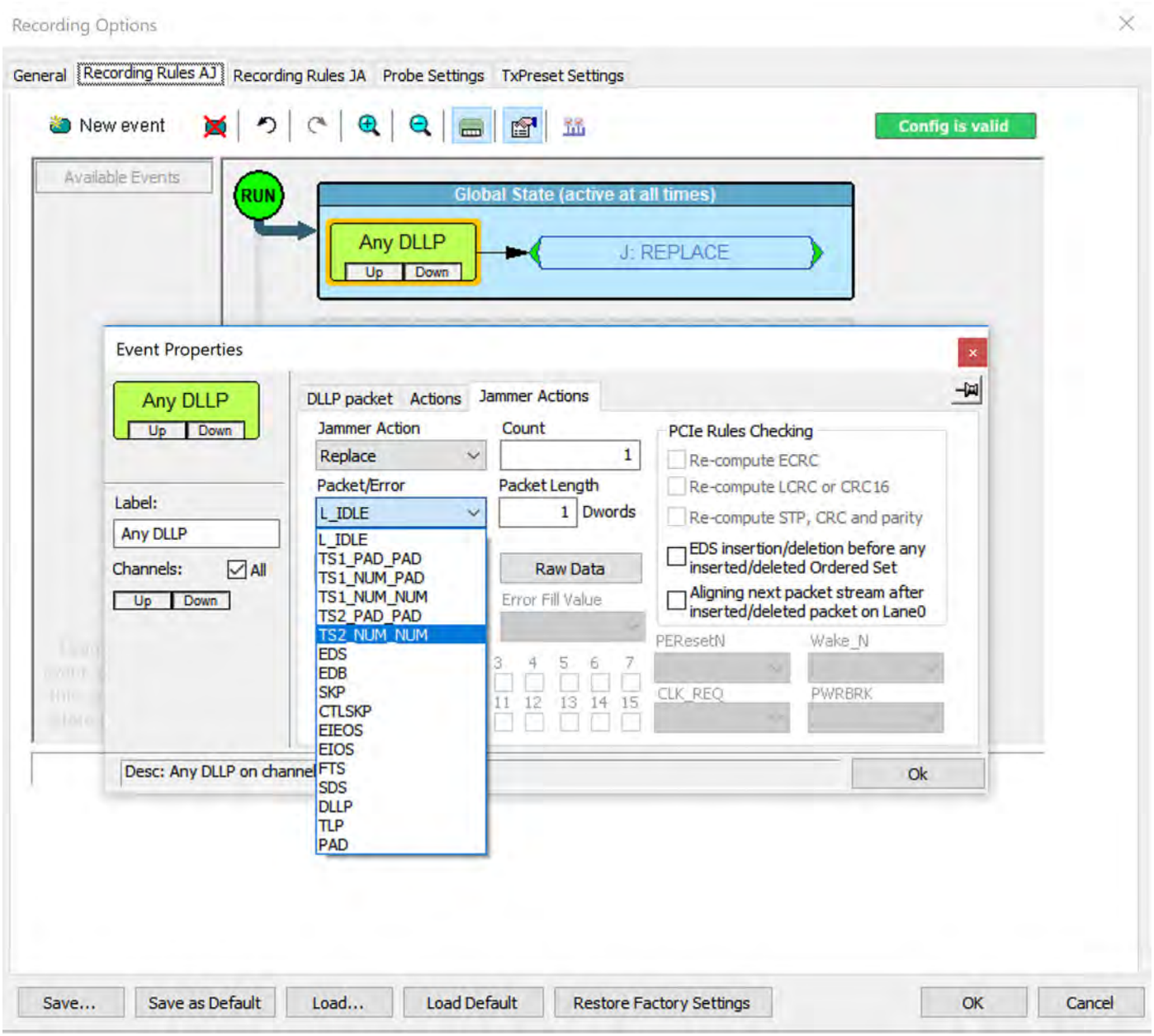


Figure 6.52: New Event: DLLP -> Any -> Replace (TS2_NUM_NUM)

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 6.53 on page 301.

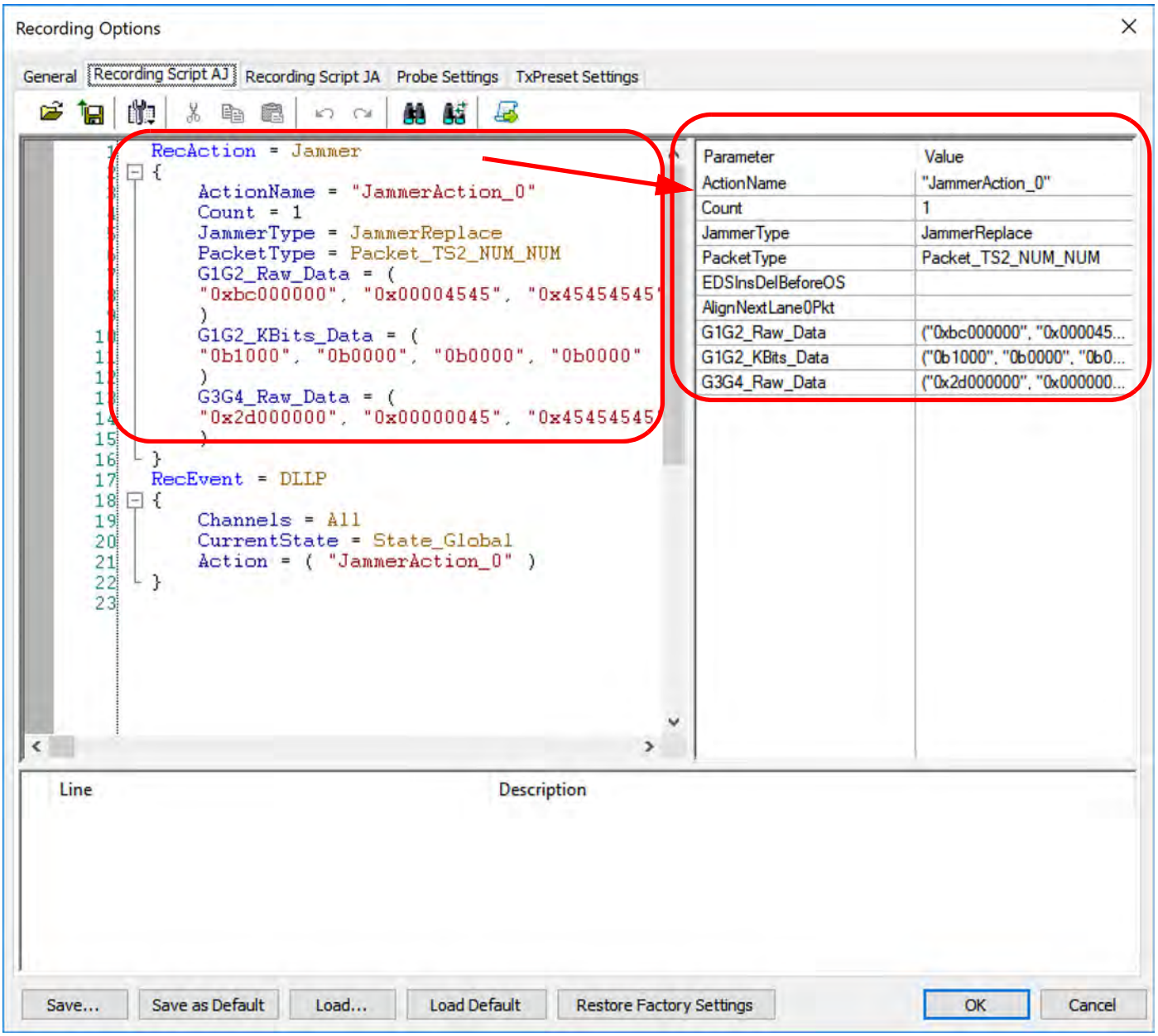


Figure 6.53: New Event: DLLP -> Any -> Replace (TS2_NUM_NUM) Script

6.14.6 TLP: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> TLP -> Any -> Modify

See GUI dialog below in Figure 6.54.

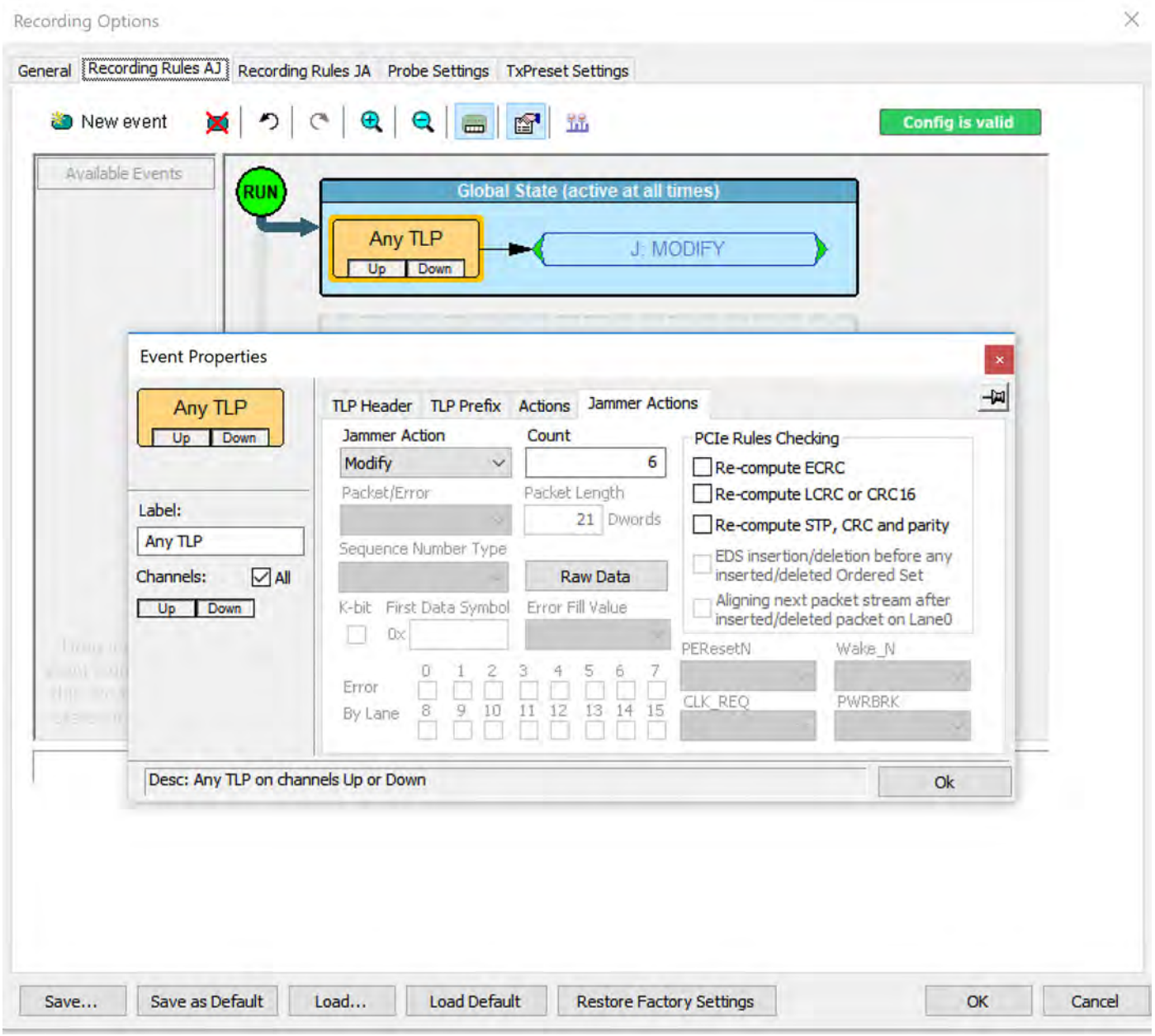


Figure 6.54: New Event: TLP -> Any -> Modify

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 6.55 on page 303.

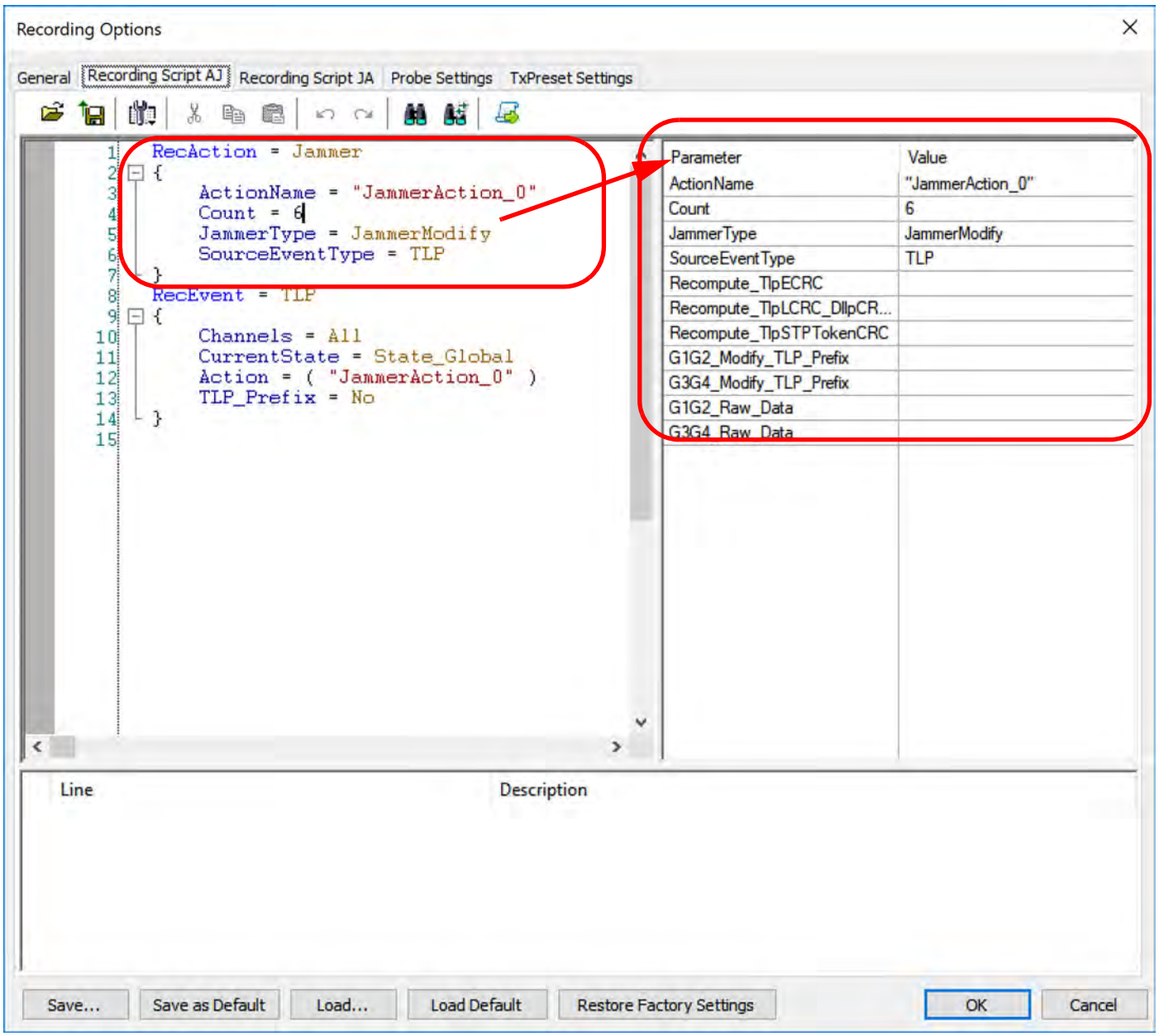


Figure 6.55: New Event: TLP -> Any -> Modify

6.14.7 NVMe

6.14.7.1 NVMe Register

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> NVMe Register -> ACQ -> Replace

See GUI dialog below in Figure 6.56.

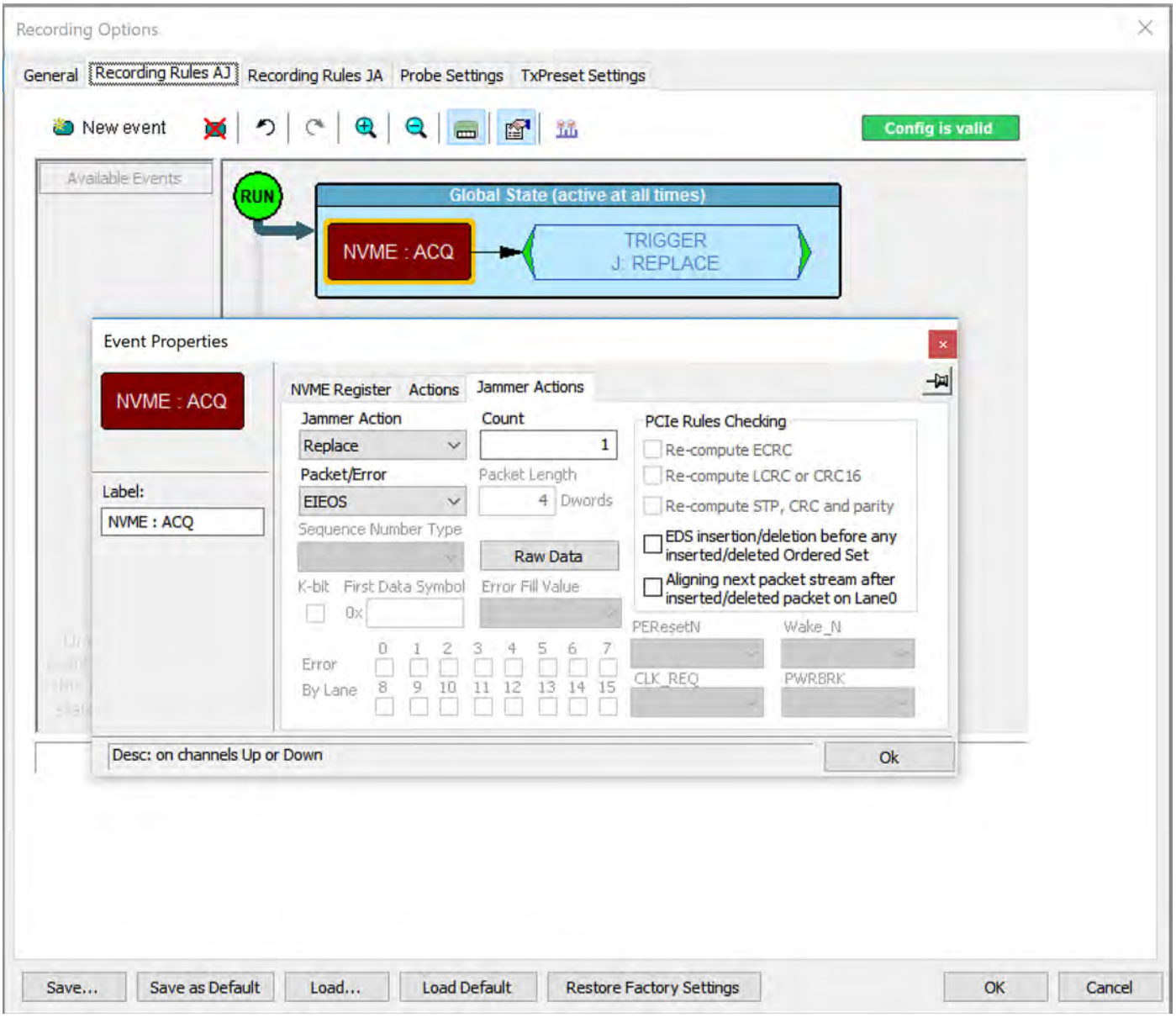


Figure 6.56: New Event: NVMe Register -> ACQ -> Replace

Select the General tab to see the generated script.

Now select Script under Trigger Mode, then click on the Recording Script tab.

See the resulting script below in Figure 6.57.

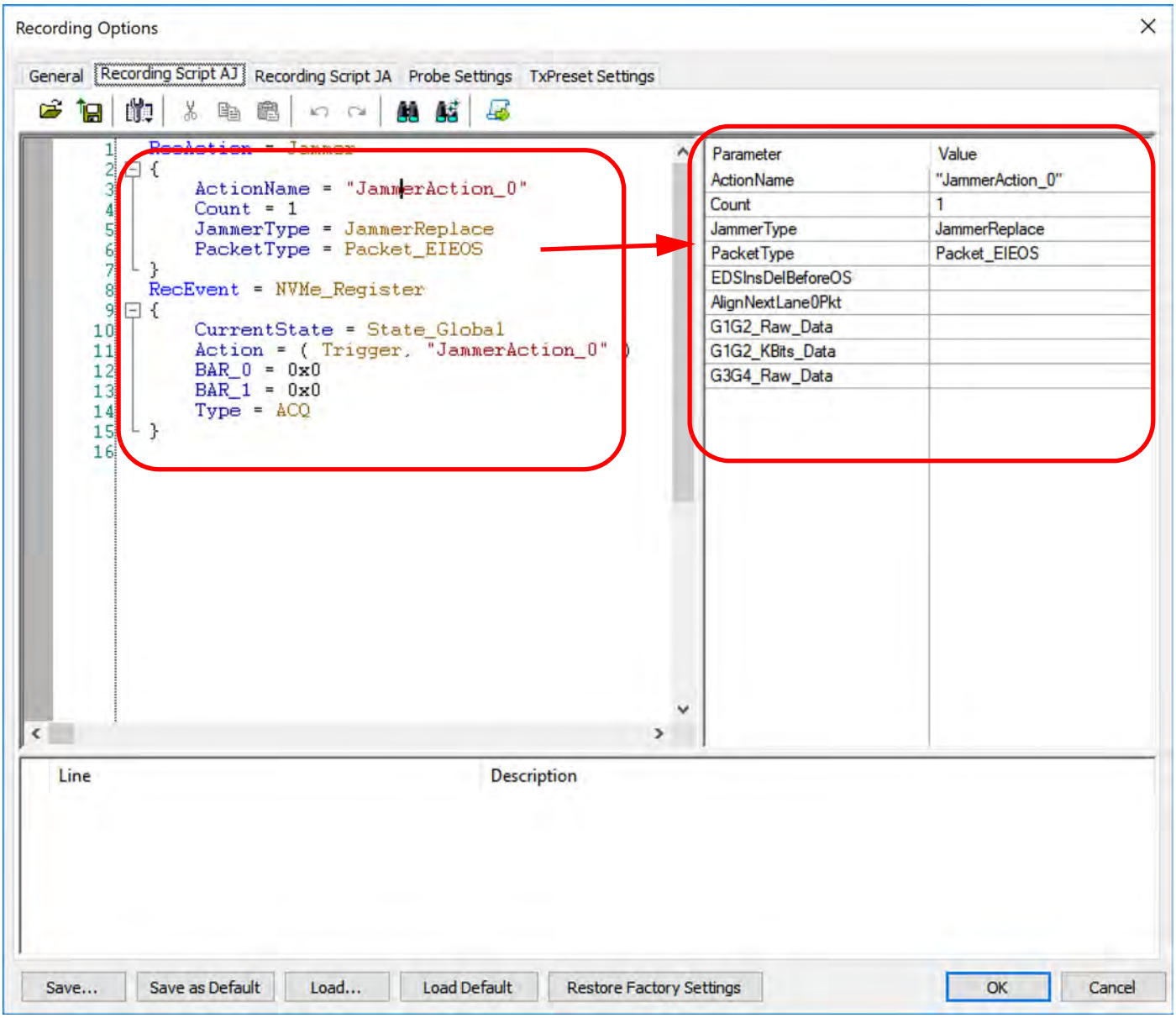


Figure 6.57: New Event: NVMe Register -> ACQ -> Replace Script

6.14.7.2 NVMe Command Submission: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> NVMe Command Submission -> Any -> Sideband

See GUI dialog below in Figure 6.58.

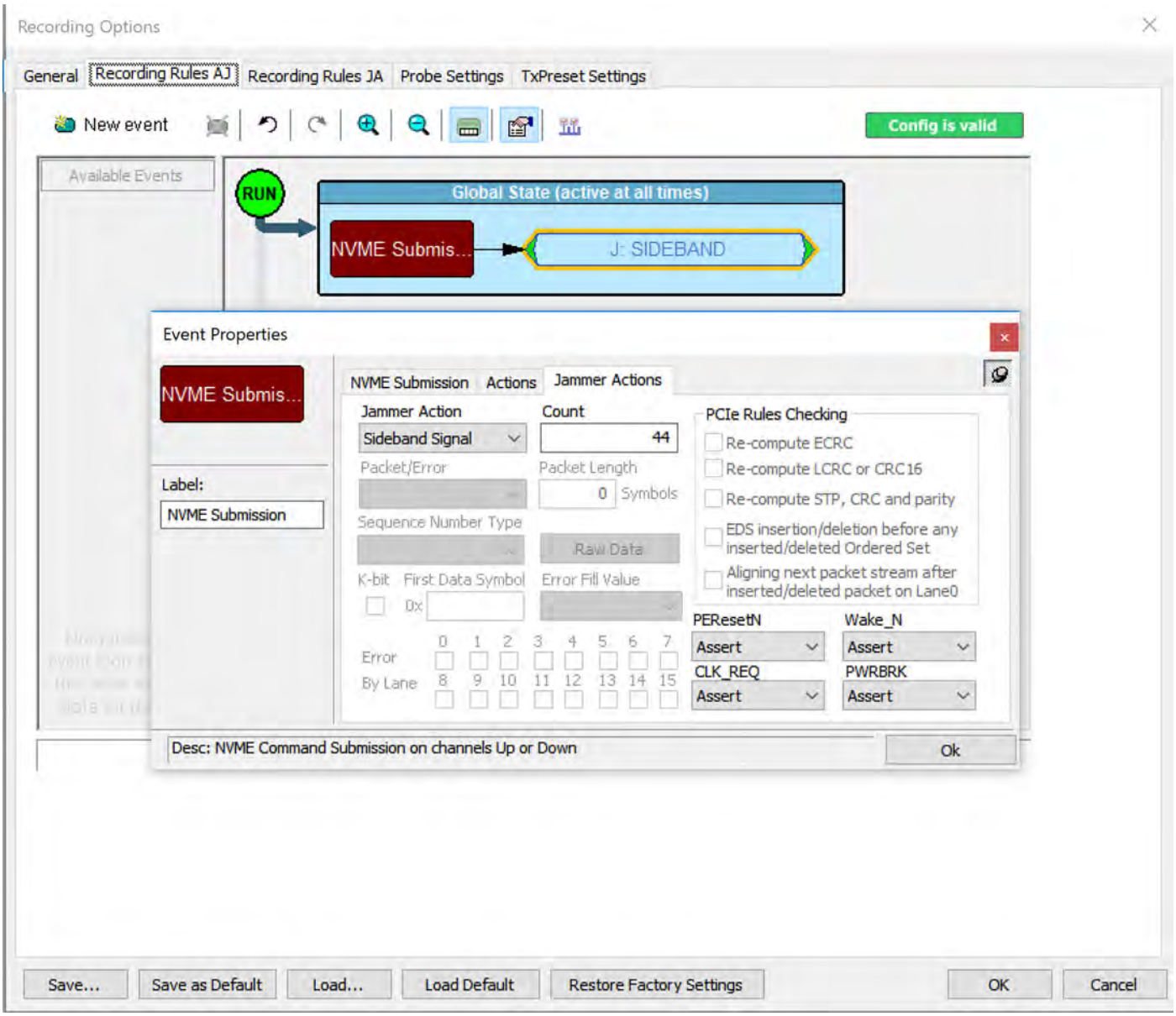


Figure 6.58: New Event: NVMe Command Submission -> Any -> Sideband

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 6.59 on page 307.

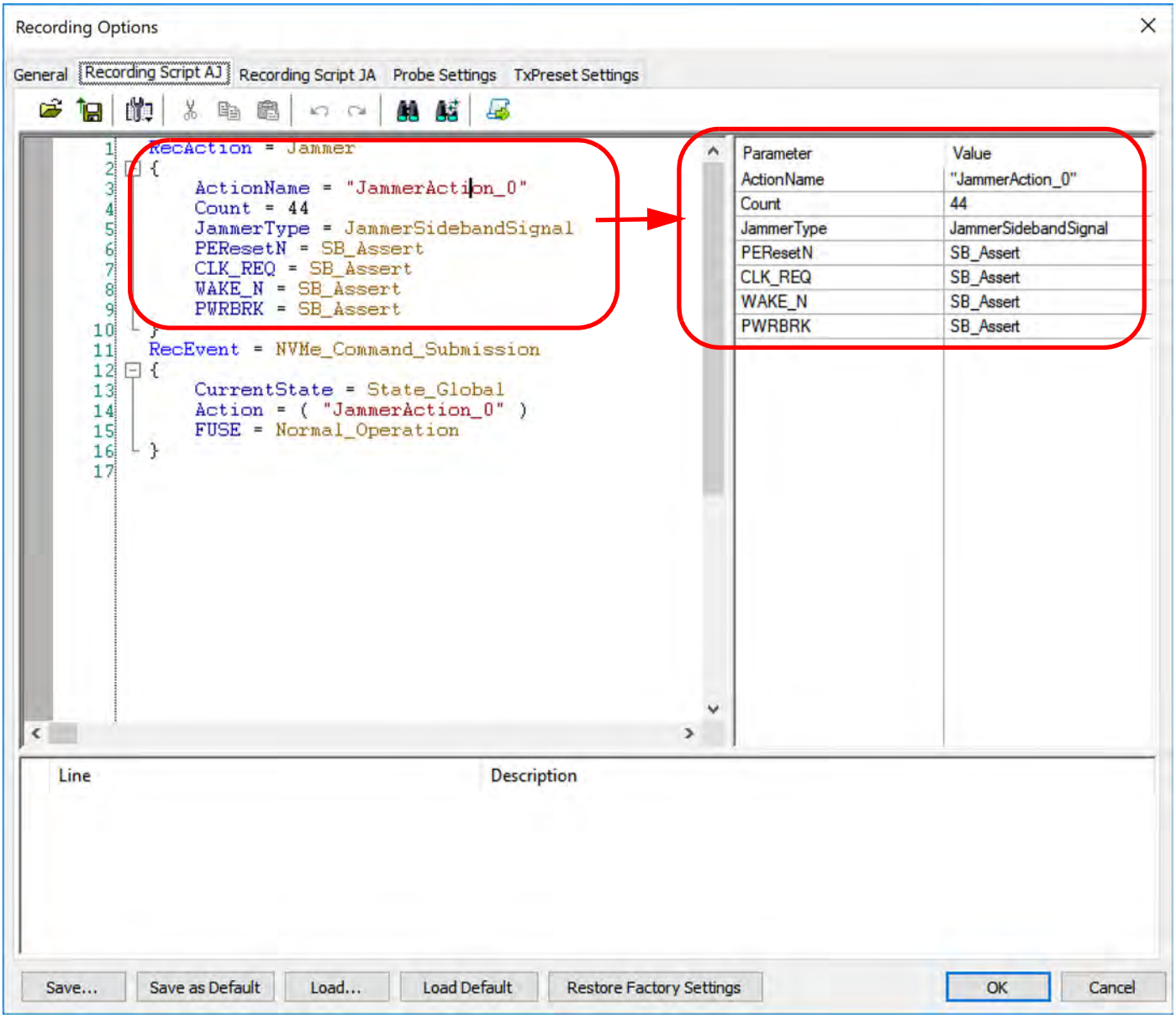


Figure 6.59: New Event: NVMe Command Submission -> Any -> Sideband Script

6.14.7.3 NVMe Command Completion: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> NVMe Command Completion -> Any -> Replace

See GUI dialog below in Figure 6.60.

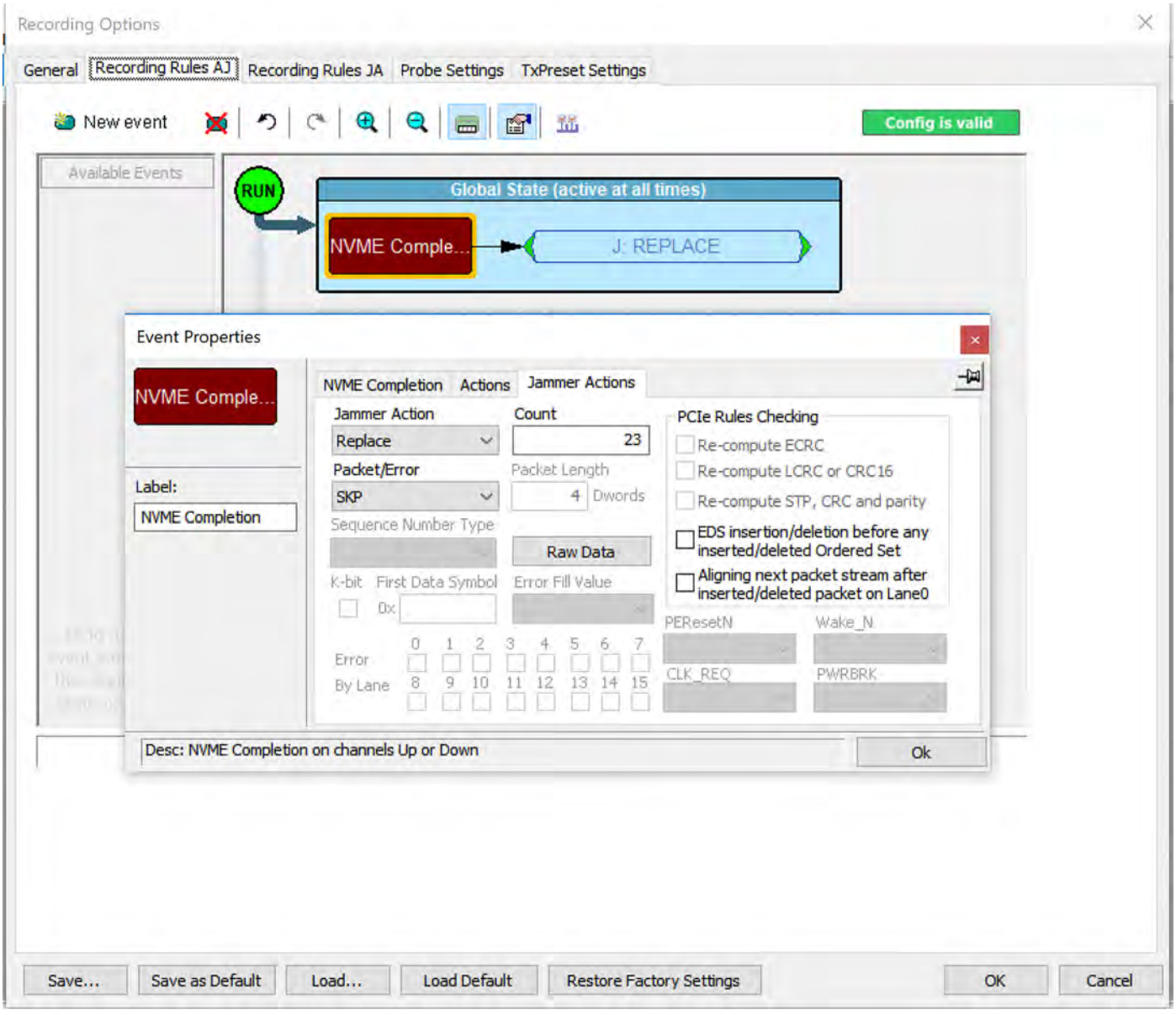


Figure 6.60: New Event: NVMe Command Completion -> Any -> Replace

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 6.61 on page 309.

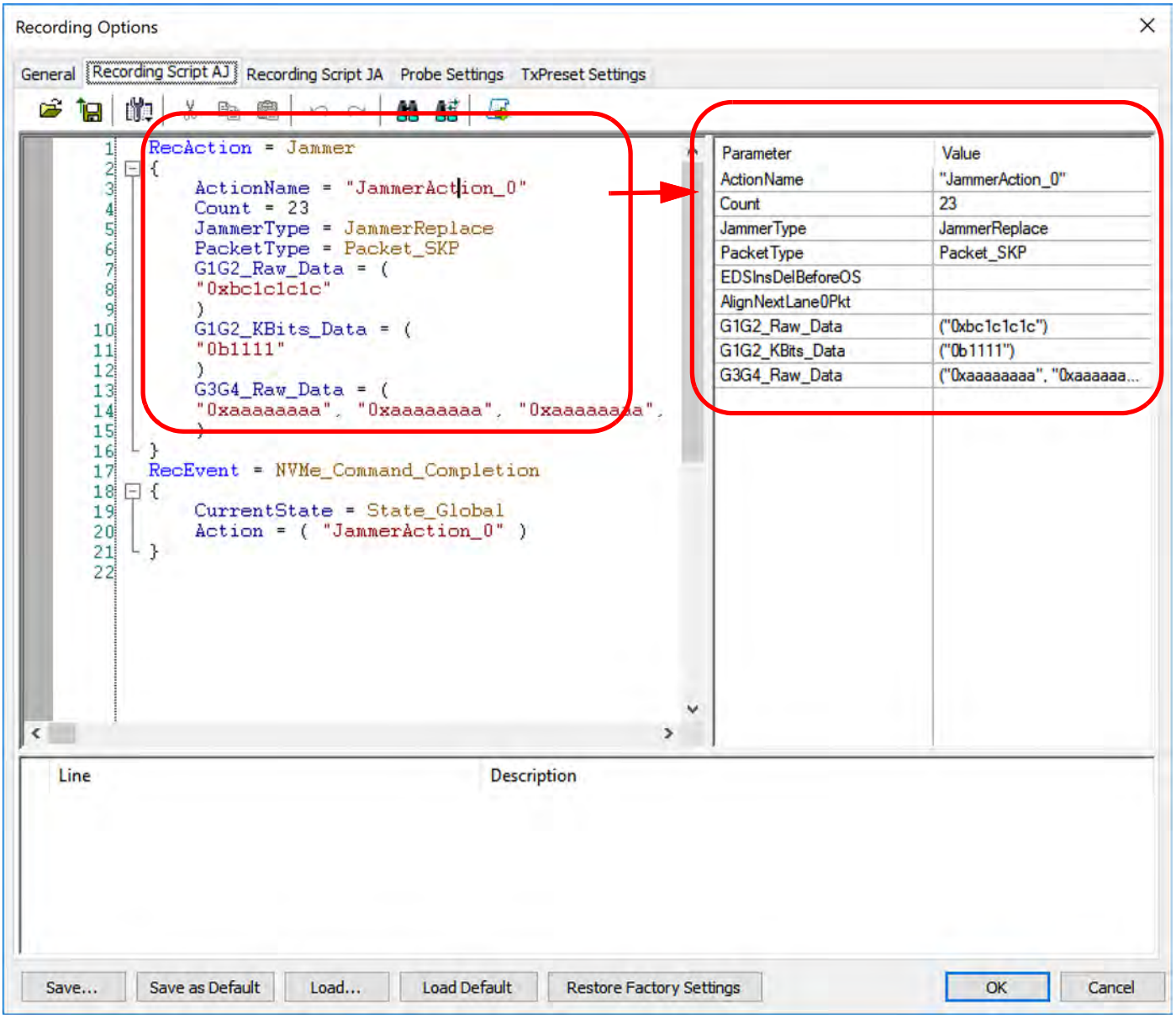


Figure 6.61: New Event: NVMe Command Completion -> Any -> Replace Script

6.15 Jammer Mode Overview (AJA)

The Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior. The Summit M5x also introduces for the first time NVMe and NVMe-MI protocol jamming as well. The analyzer and jammer combination features on the Summit M5x make this a powerful testing tool for PCIe validation and development labs. This Jammer and Scripting capability is built into the PCIe Protocol Analysis software.

In addition the Summit M5x can also display the results of the Jamming operation. In one product you can analyze a stream of traffic, modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint and then see the results of that jamming operation.

To select this mode of operaton in the Recording Options menu select Summit M5x Jammer AJA (Advanced). See Figure 6.62 on page 311.

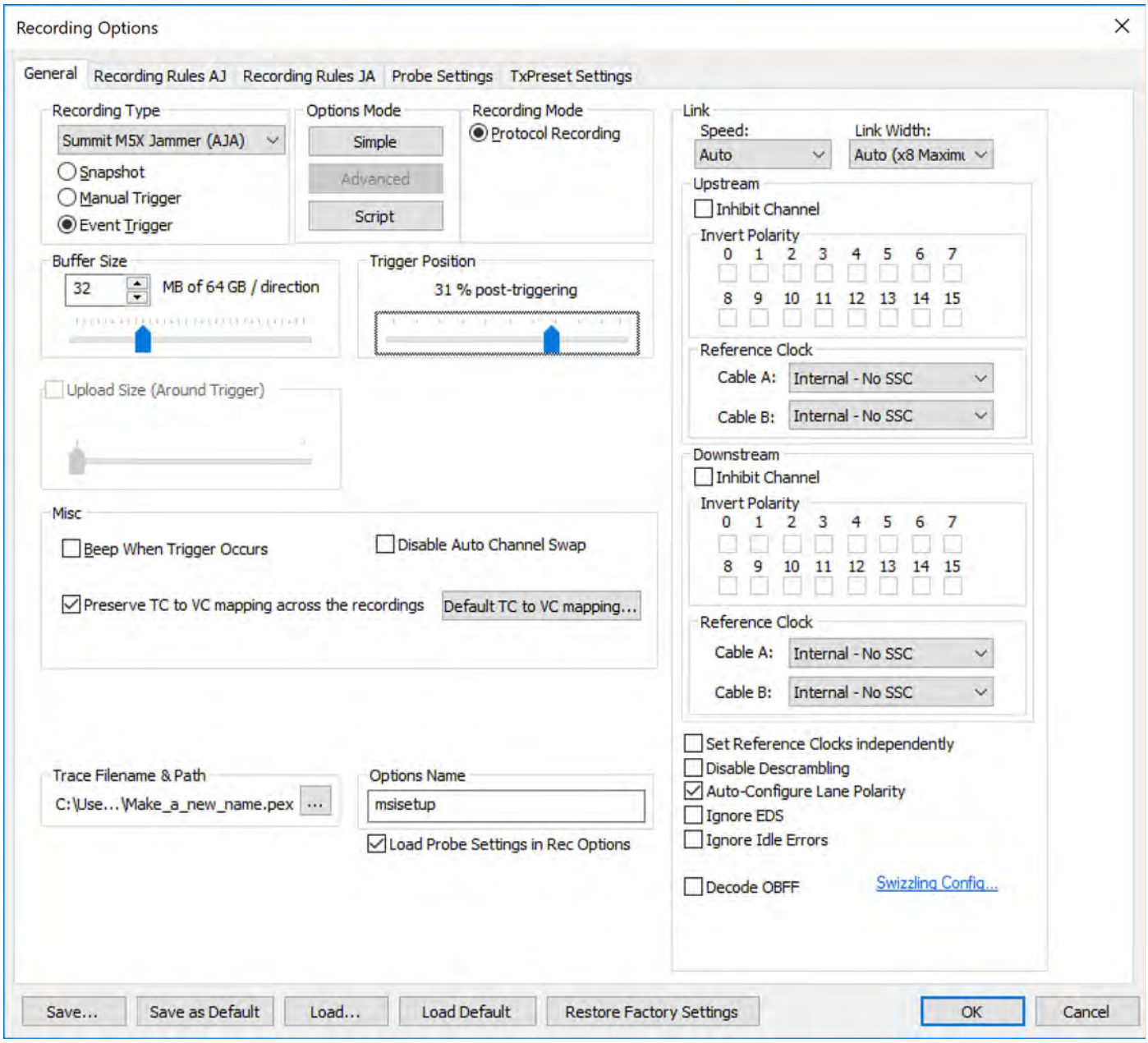


Figure 6.62: Selecting the Summit M5x AJA Mode for Recording

The Recording Rules JA tab is very similar to the Recording Rules AJ as explained in “Recording Options: Recording Rules (AJ)” on page 250 with the exception that there are no Jammer Rules options.

To generate a script you’d use the same methodolgy as shown in “Converting Recording Rules and Jammer Actions from GUI to Script File (AJ)” on page 252.

In the section below several examples of traces using the Analyzer/Jammer/Analyzer (AJA) are shown and described in detail.

6.15.1 Examples of AJA Traces (Jammer Actions and Results)

6.15.1.1 Delete: UpdateFC_P DLLP Packet

In the first example we **Delete an UpdateFC_P DLLP**. The loaded trace is shown in Figure 6.63. The tooltips associated with the Jammer function are also shown.

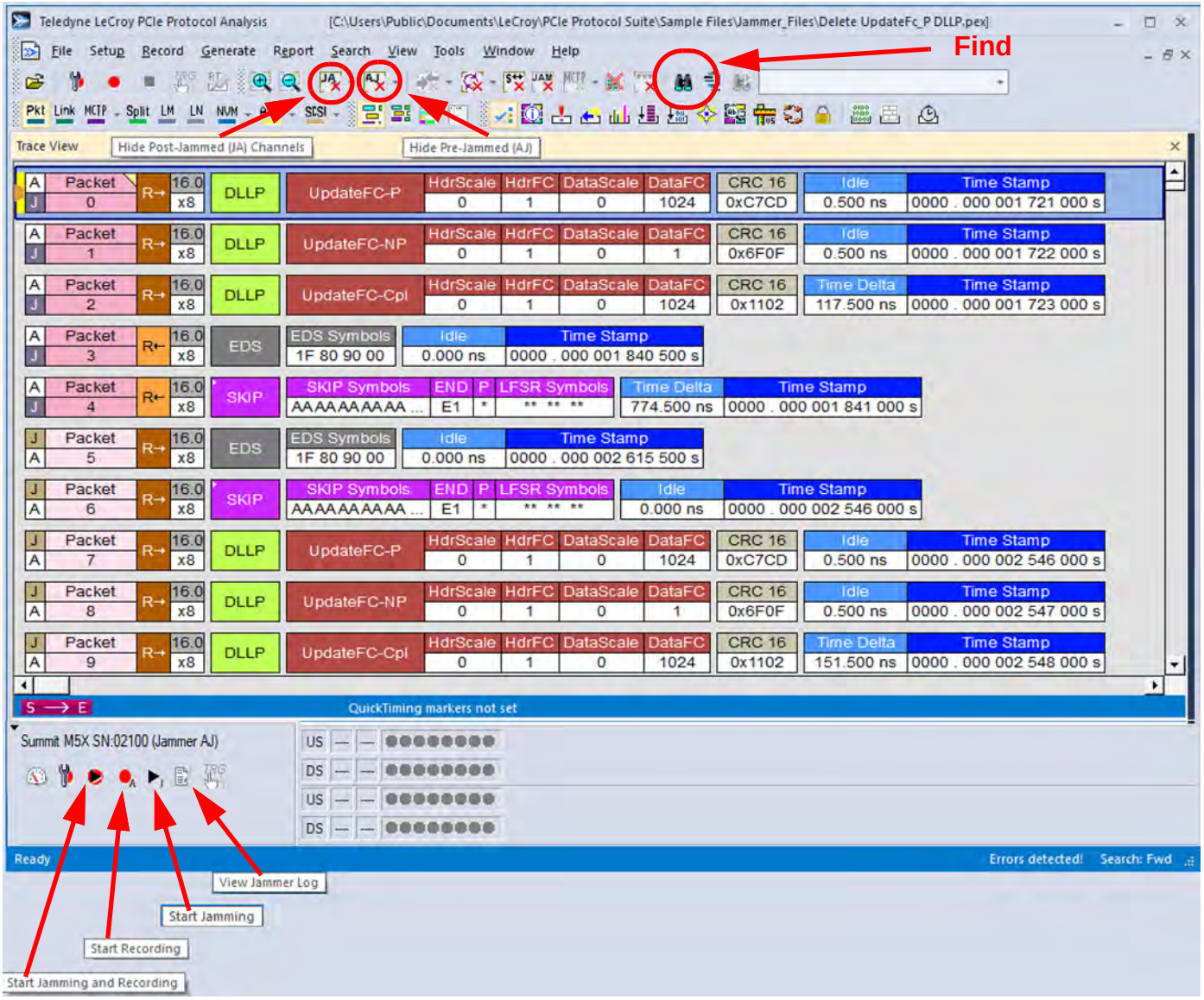


Figure 6.63: AJA Trace: Delete UpdateFc_P DLLP with tooltips

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 6.64 on page 313.

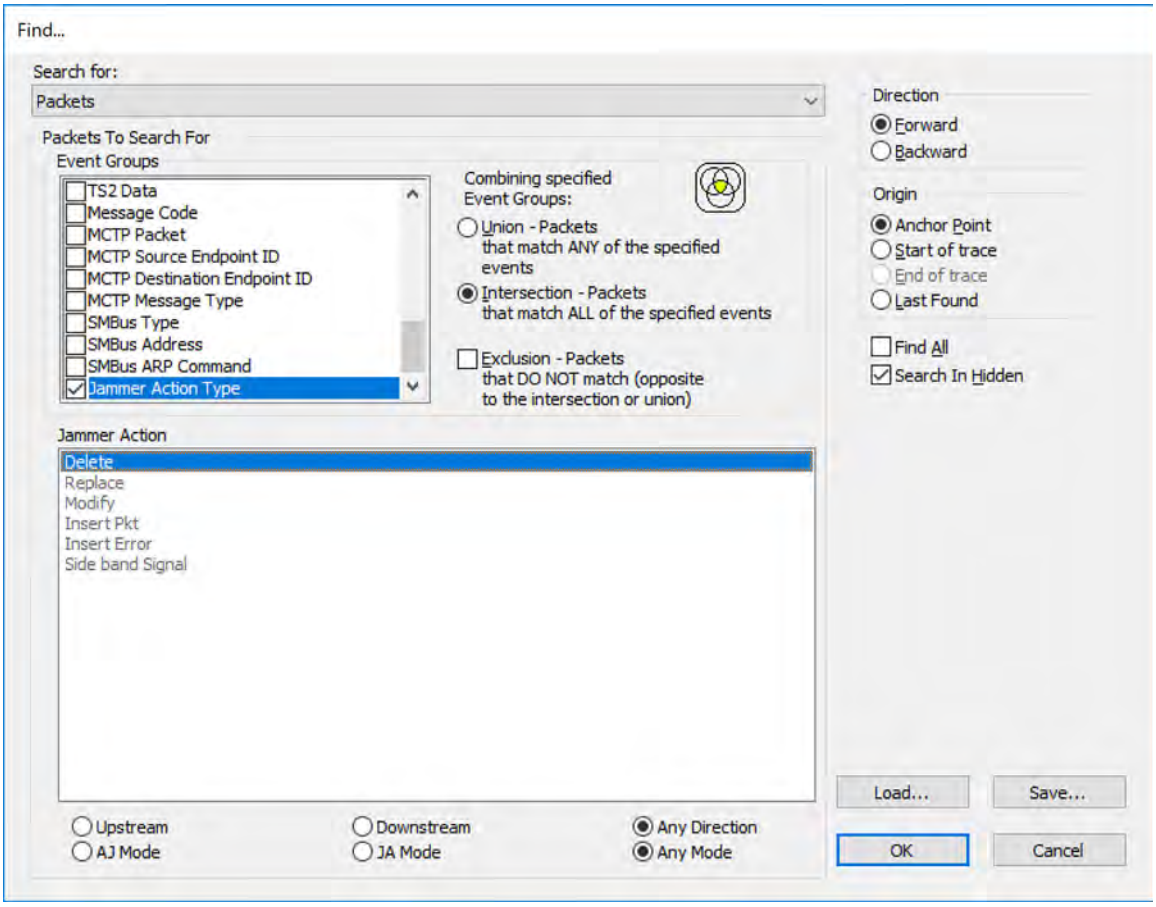


Figure 6.64: Find -> Search for: Packets -> Jammer Action Type: Delete

Click on OK and the Jammer Action and following it the results: A deleted UpdateFC_P packet. See Figure 6.65 on page 314.

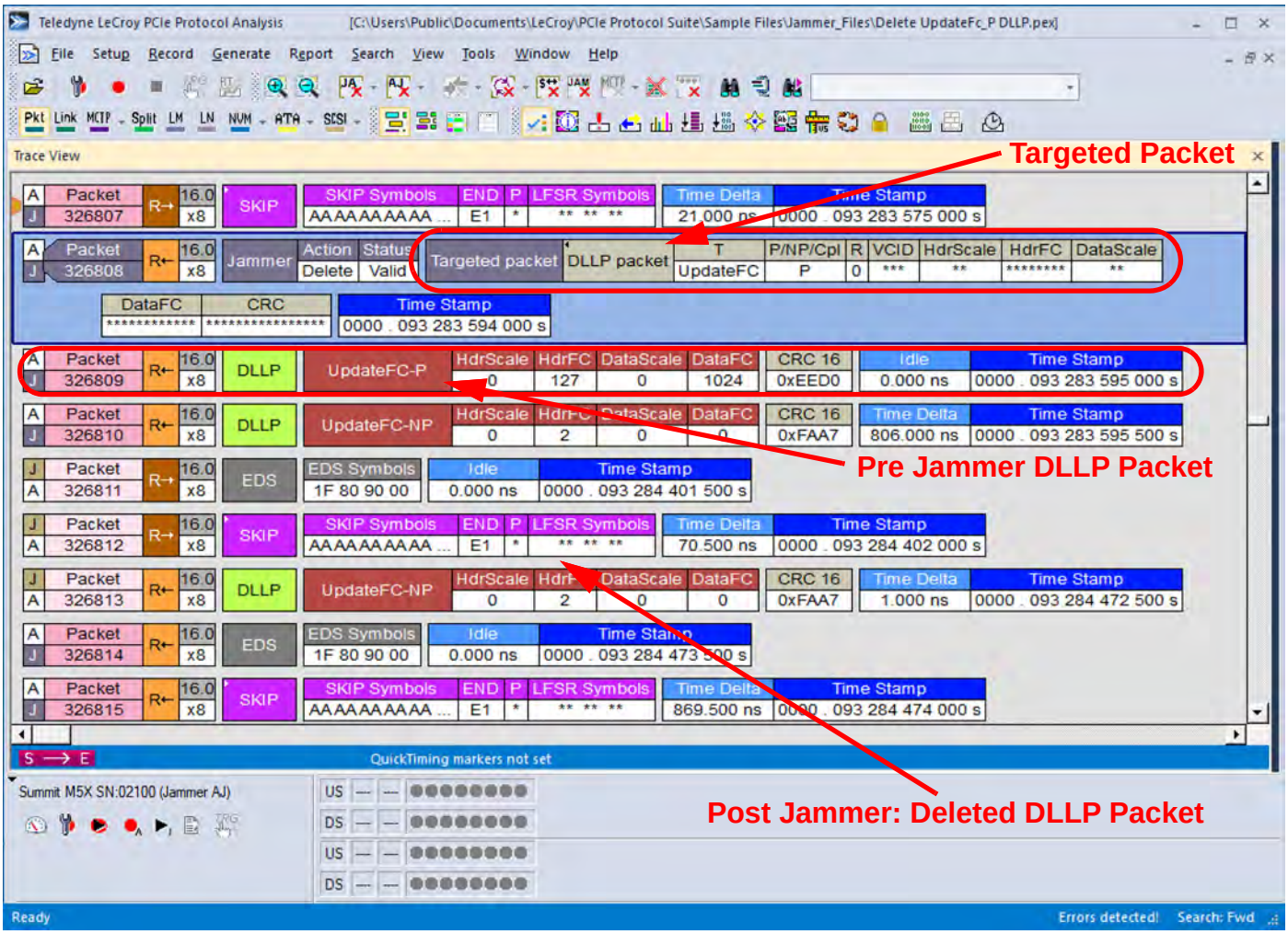


Figure 6.65: Trace with Jammer Function: Delete UpdateFC_P

6.15.1.2 Insert Error: DROP_STP_SDP for UpdateFC_P Packet

In he second example we drop an STP_SDP packet for an UpdateFC_P Packet. See Figure 6.66.

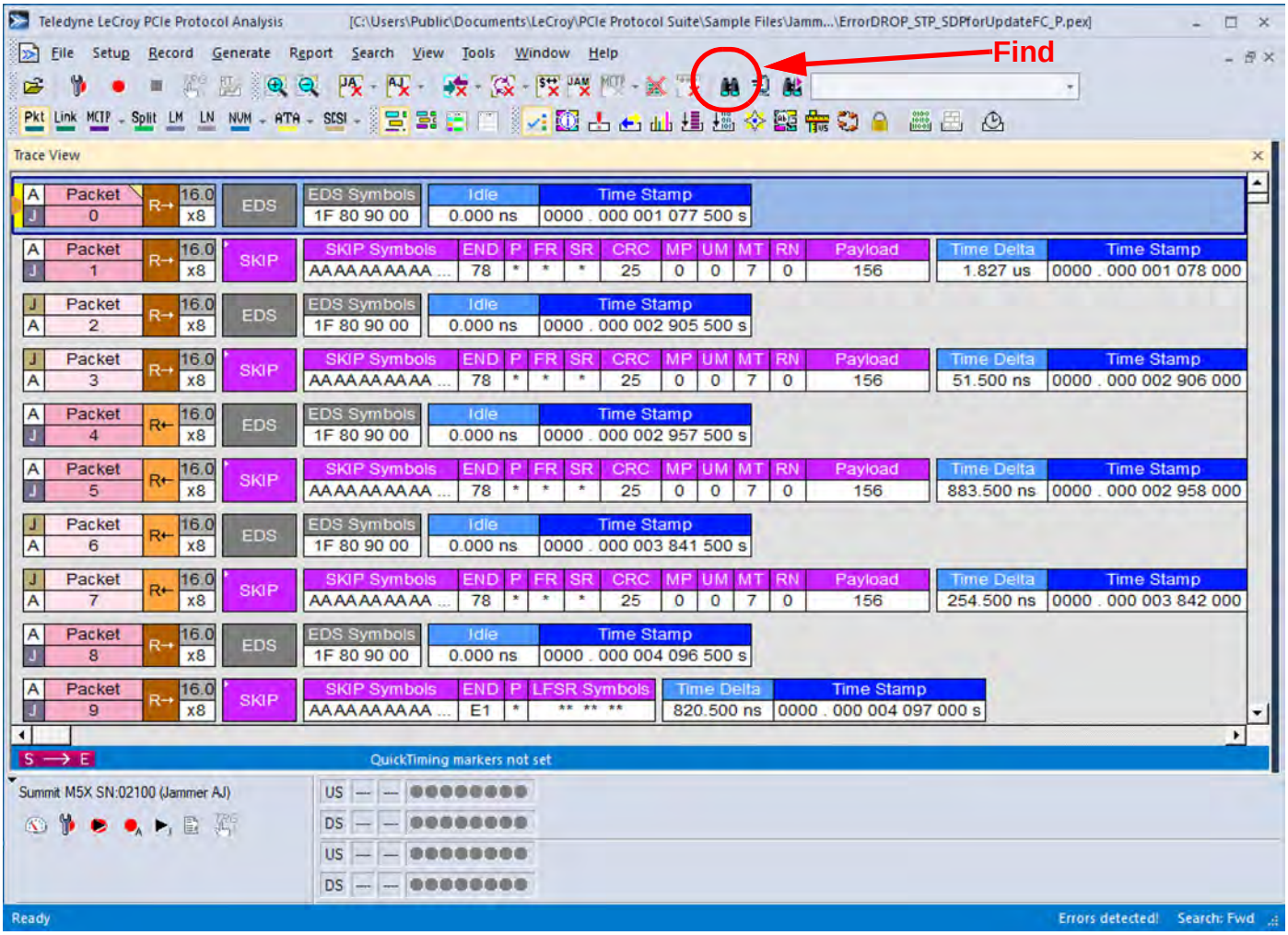


Figure 6.66: AJA Trace: Insert Error -> Drop STP_SDP for UpdateFC_P

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 6.67 on page 316.

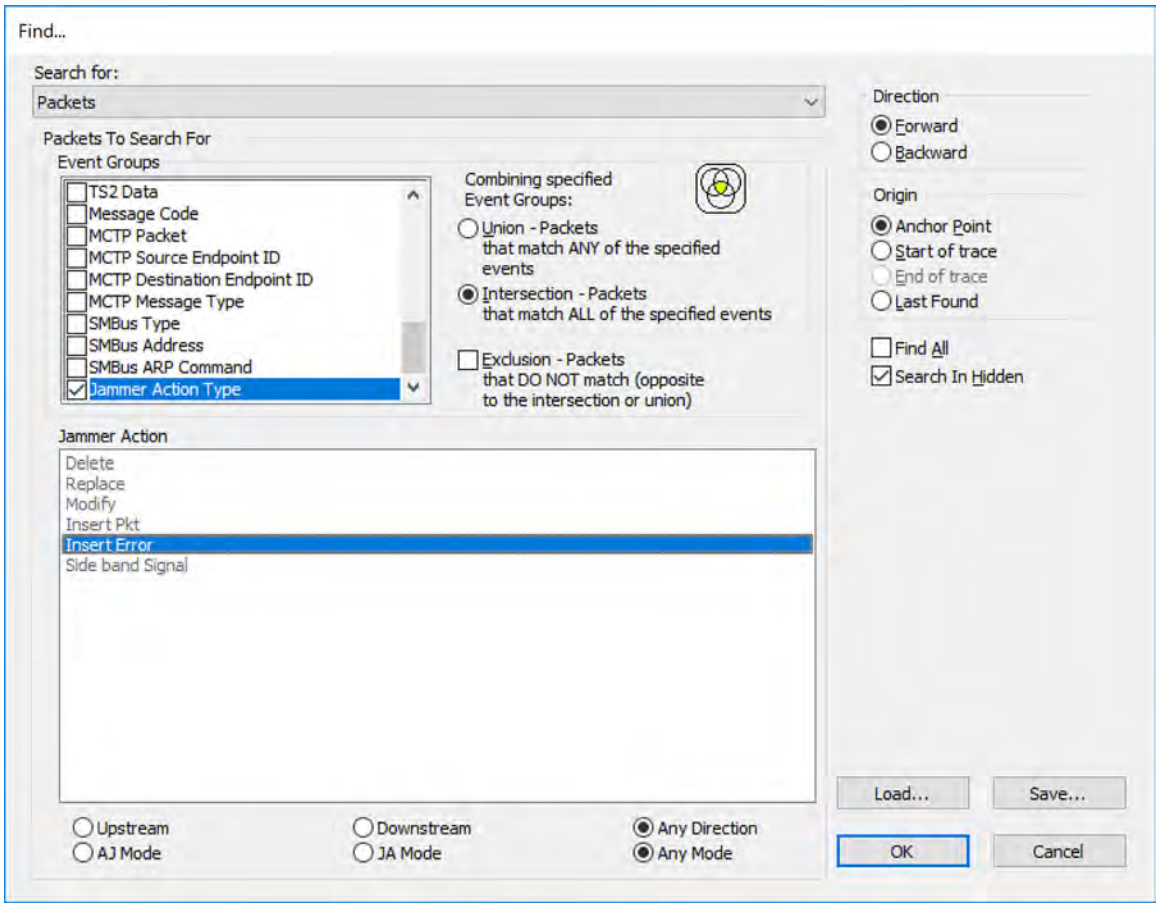


Figure 6.67: Find -> Search for: Packets -> Jammer Action Type: Insert Error

Click on OK and the Jammer Action and following it are the results:

Insert Error -> Drop STP_SDP for UpdateFC_P, which causes the UpdateFC_P packet to be missing. See Figure 6.68 on page 317.

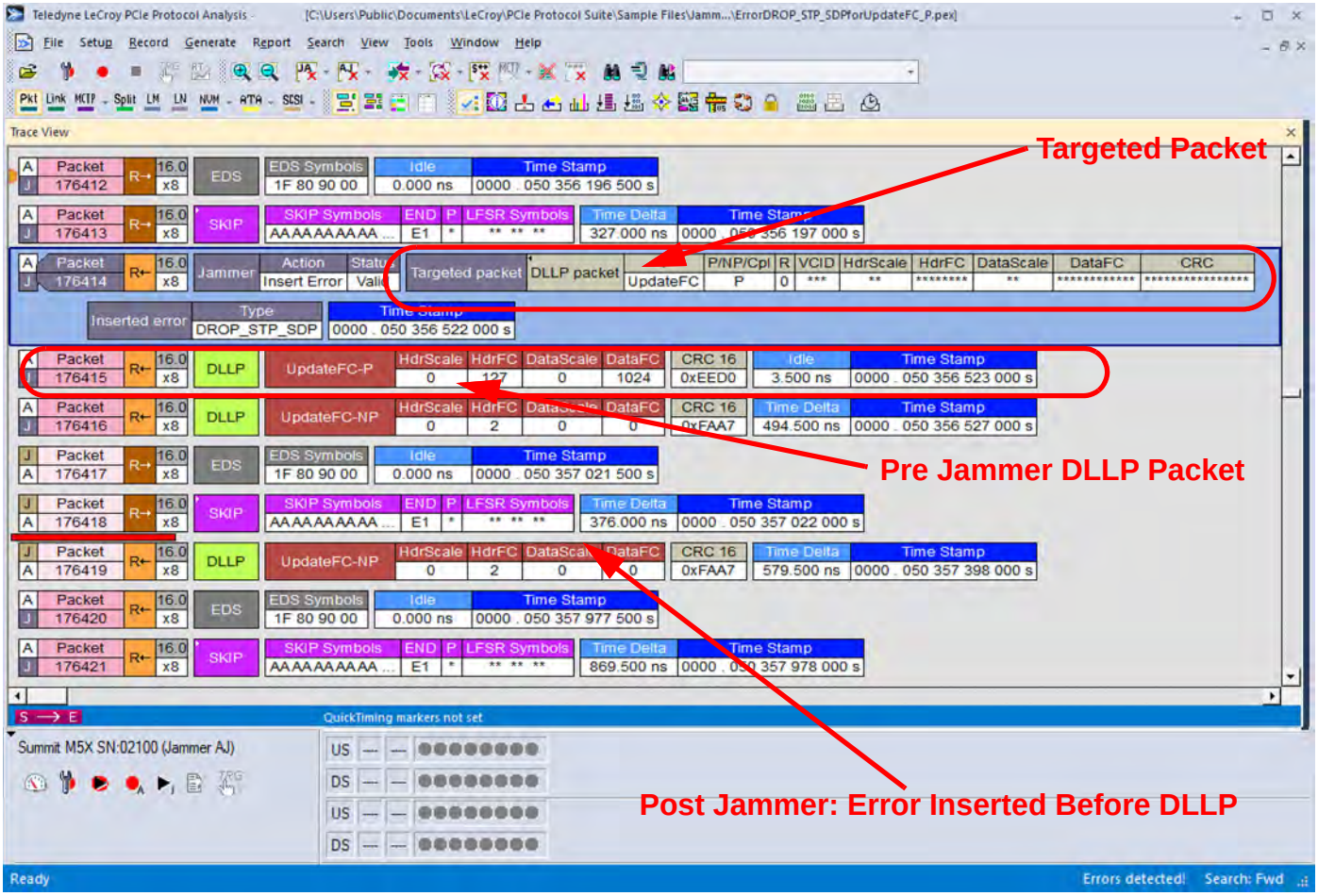


Figure 6.68: Trace with Jammer Function: Insert Error -> Drop STP/SDP for UpdateFC_P

6.15.1.3 Insert TLP After UpdateFC_NP Packet

In the third example we insert an TLP Packet after an UpdateFC_NP Packet. See Figure 6.69.

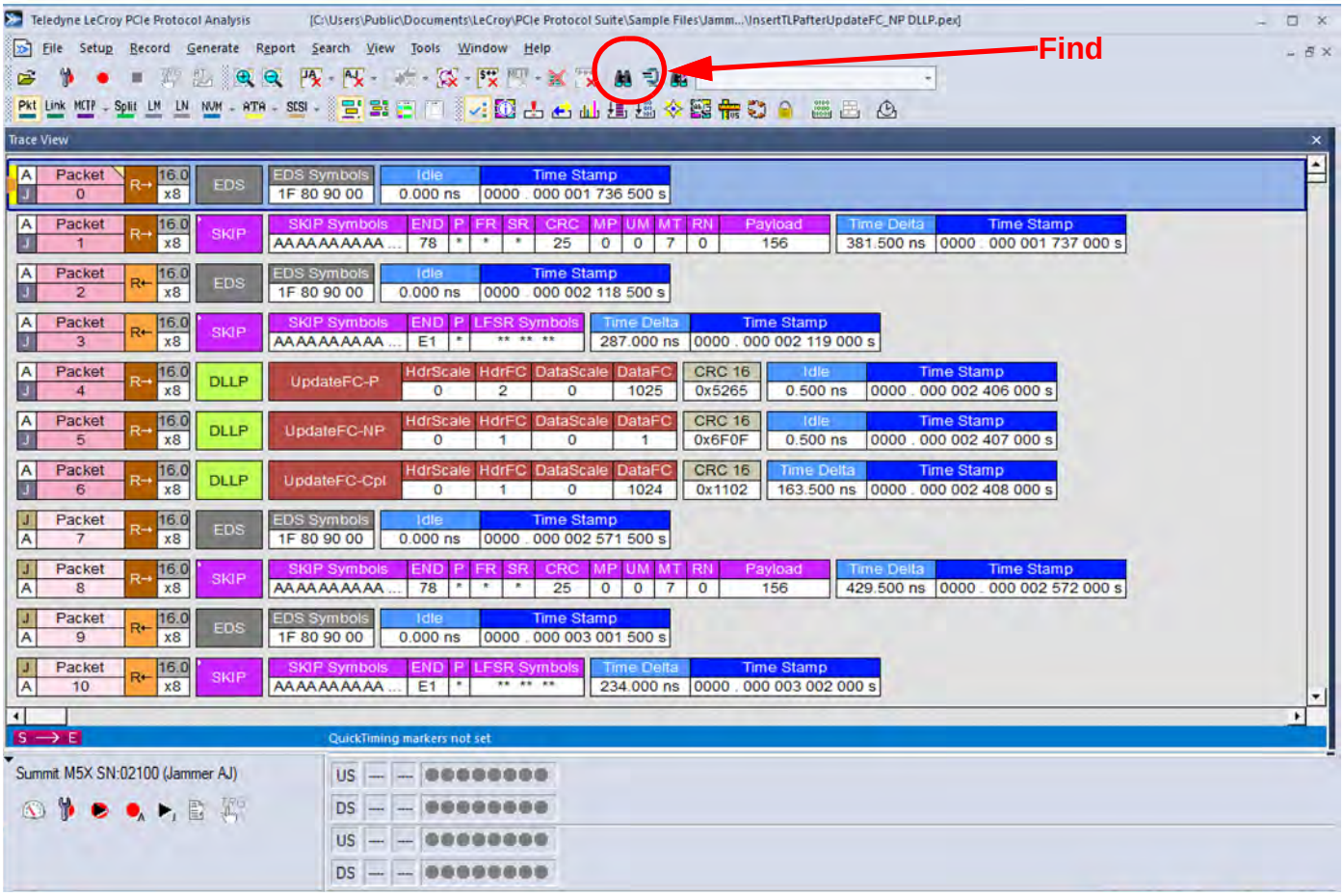


Figure 6.69: AJA Trace: Insert TLP After UpdateFC_NP Packet

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 6.70 on page 319.

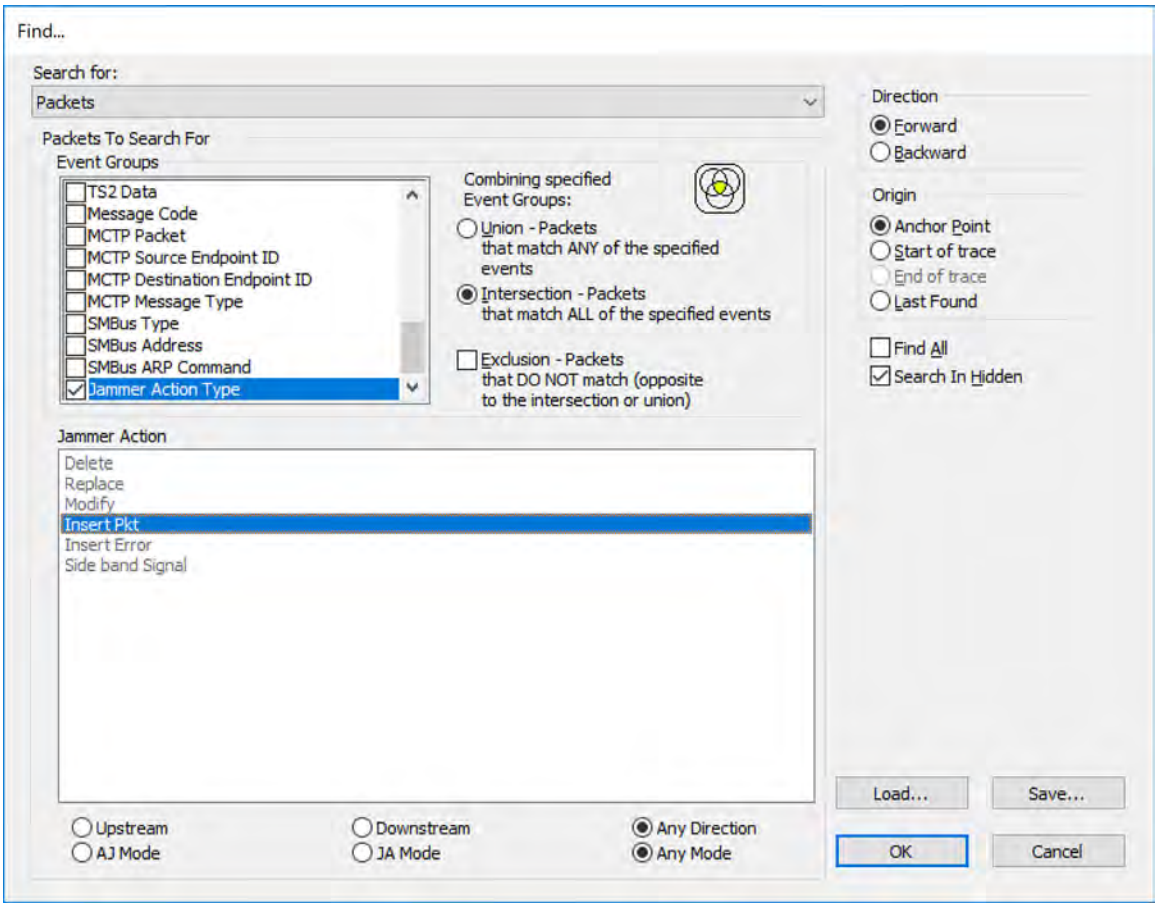


Figure 6.70: Find -> Search for: Packets -> Jammer Action Type: Insert packet

Click on OK and the Jammer Action and following it are the results:

Insert TLP After UpdateFC_NP Packet, which adds a TLP to the trace after the UpdateCF_NP packet. See Figure 6.71 on page 320.

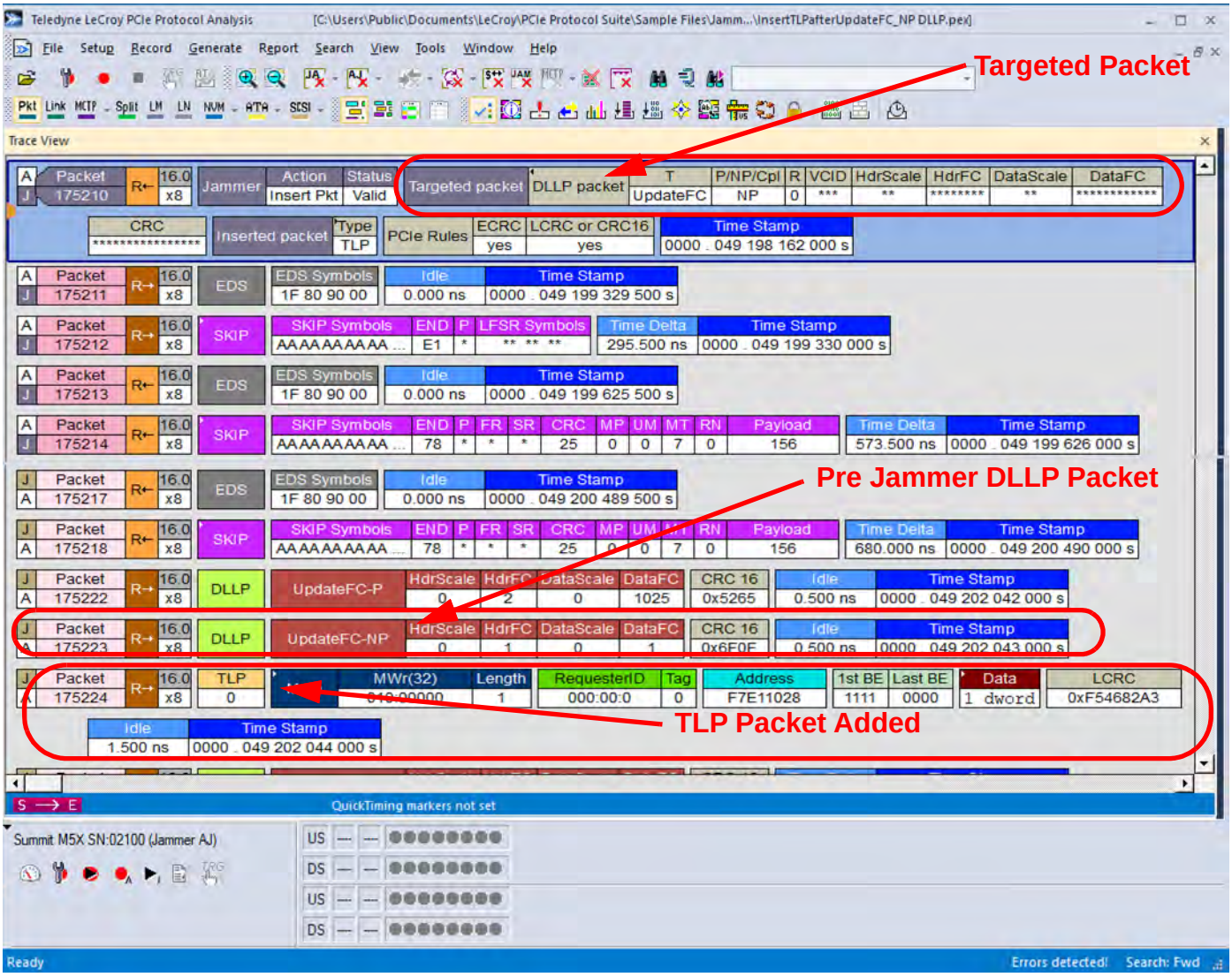


Figure 6.71: Trace with Jammer Function: Insert TLP Packet After UpdateFC_NP Packet

6.15.1.4 Modify: UpdateFC_P Packet to UpdateFC_NP Packet

In the fourth example we modify an UpdateFC_P Packet to an UpdateFC_NP Packet. See Figure 6.72.

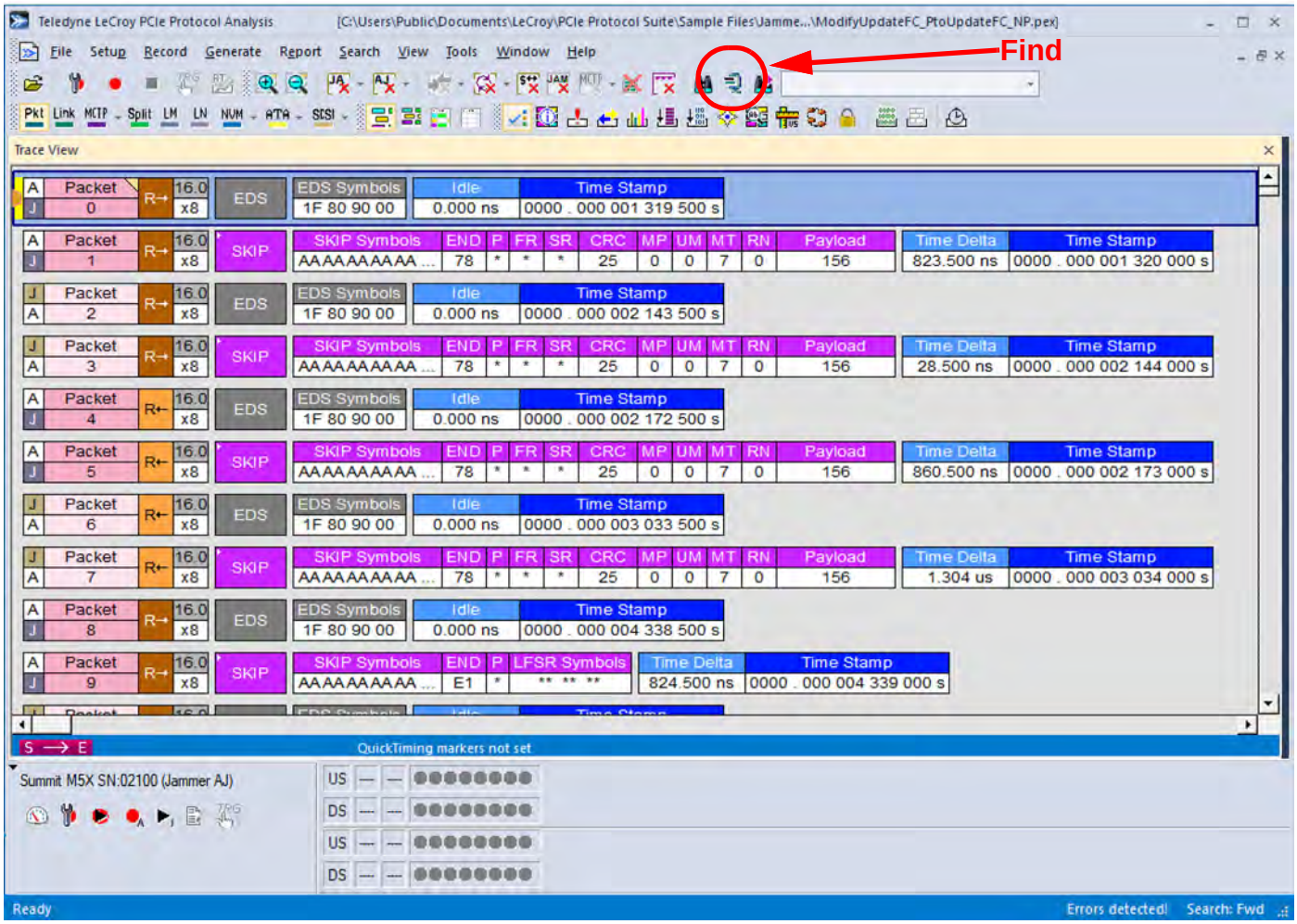


Figure 6.72: AJA Trace: Modify: UpdateFC_P Packet to UpdateFC_NP Packet

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 6.73 on page 322.

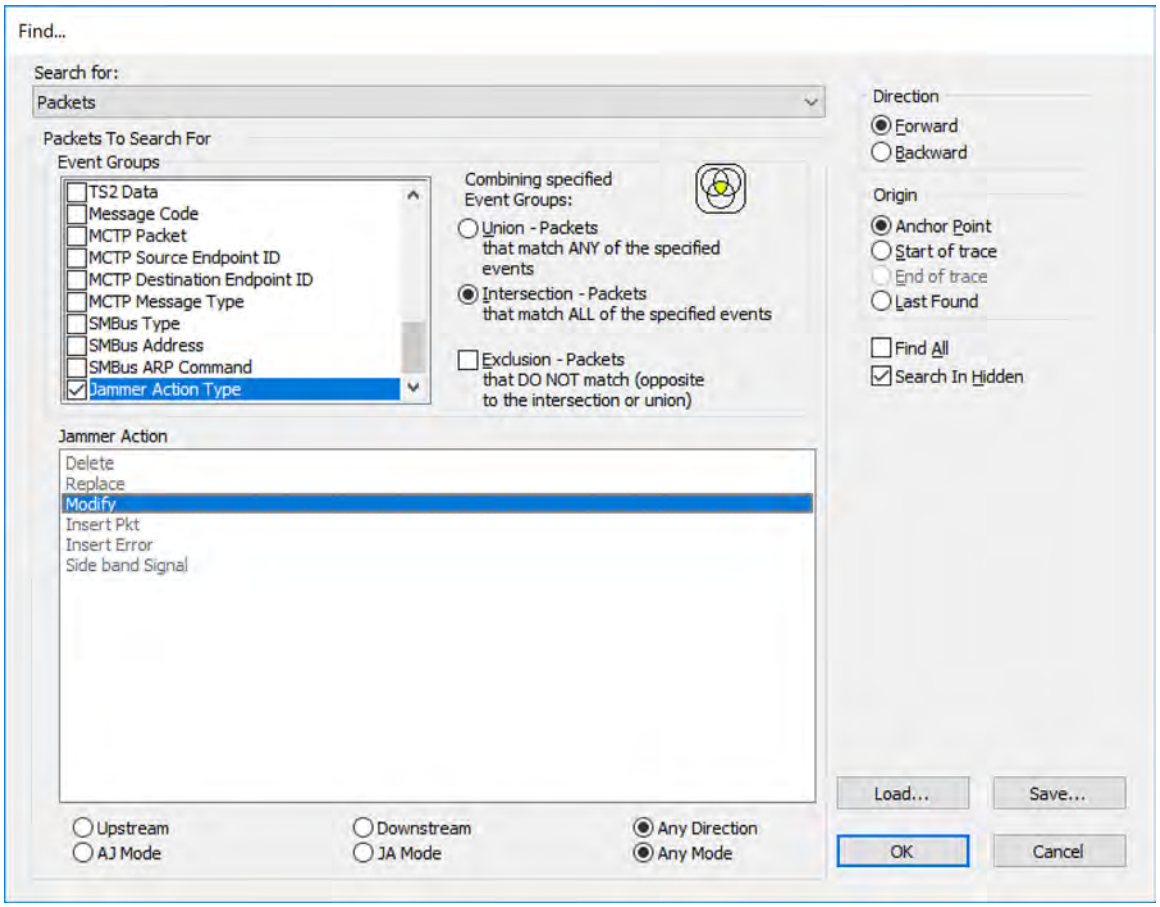


Figure 6.73: Find -> Search for: Packets -> Jammer Action: Modify Packet

Click on OK and the Jammer Action and following it are the results:

Insert Error -> Drop STP/SDP for UpdateFC_P, which causes the UpdateFC_P packet to be missing. See Figure 6.74 on page 323.

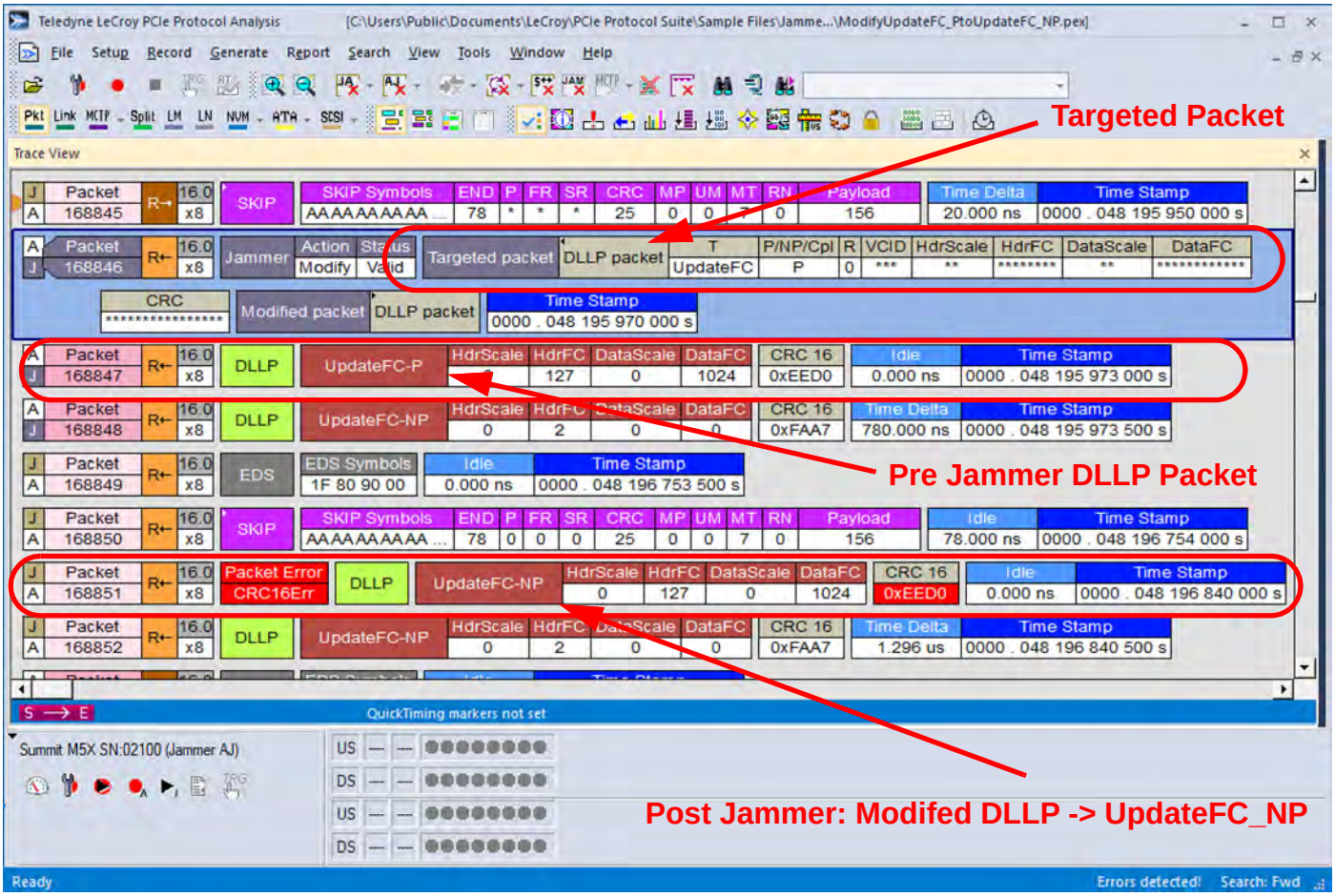


Figure 6.74: Trace with Jammer Function: Modify UpdateFC_N to UpdateFC_NP

6.15.1.5 Replace: UpdateFC_CP with TS1_PAD_PAD

In the fifth example we replace an UpdateFC_CP with a TS1_PAD_PAD packet. See Figure 6.75.

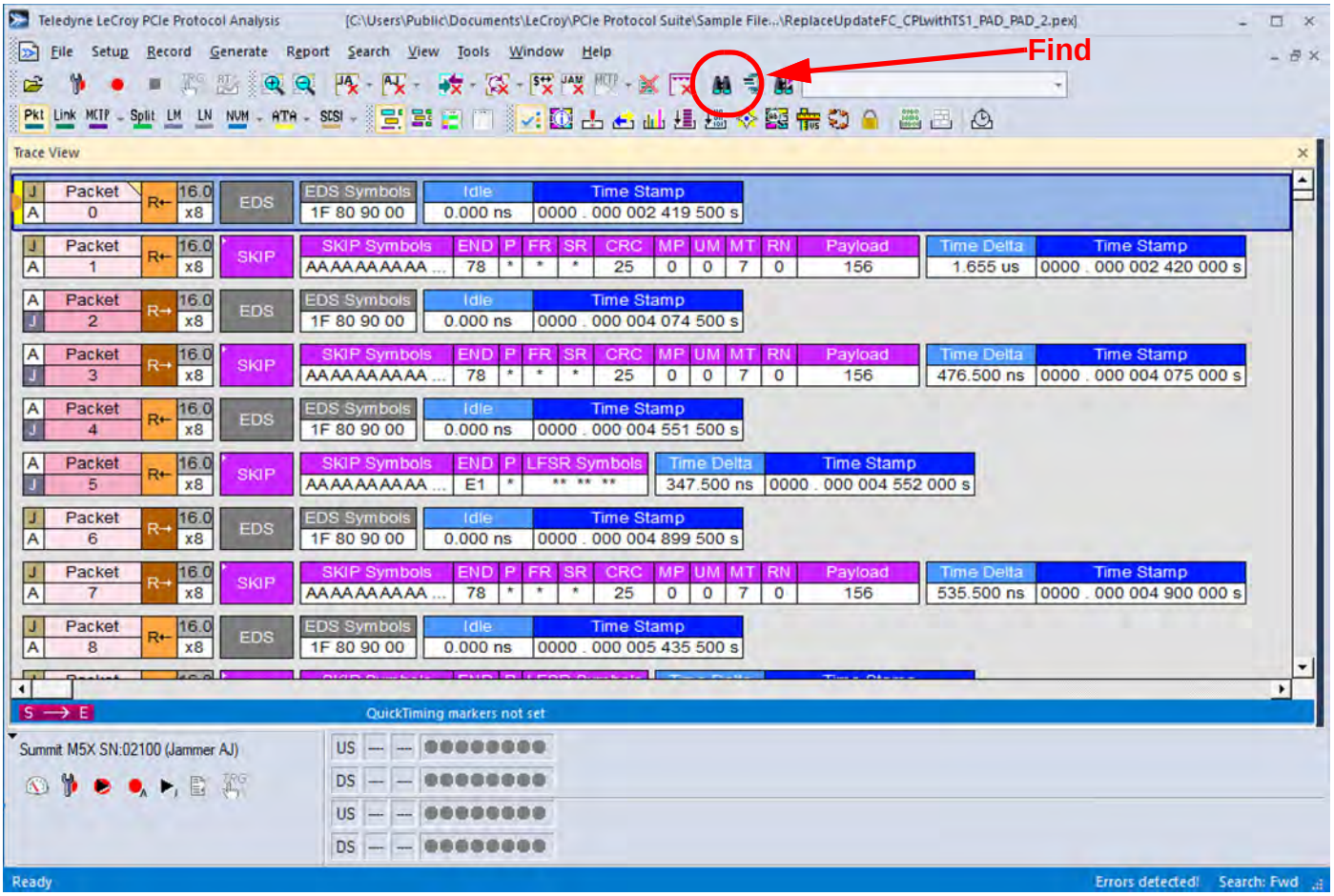


Figure 6.75: AJA Trace: Replace -> UpdateFC_CP with TS1_PAD_PAD

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 6.76 on page 325.

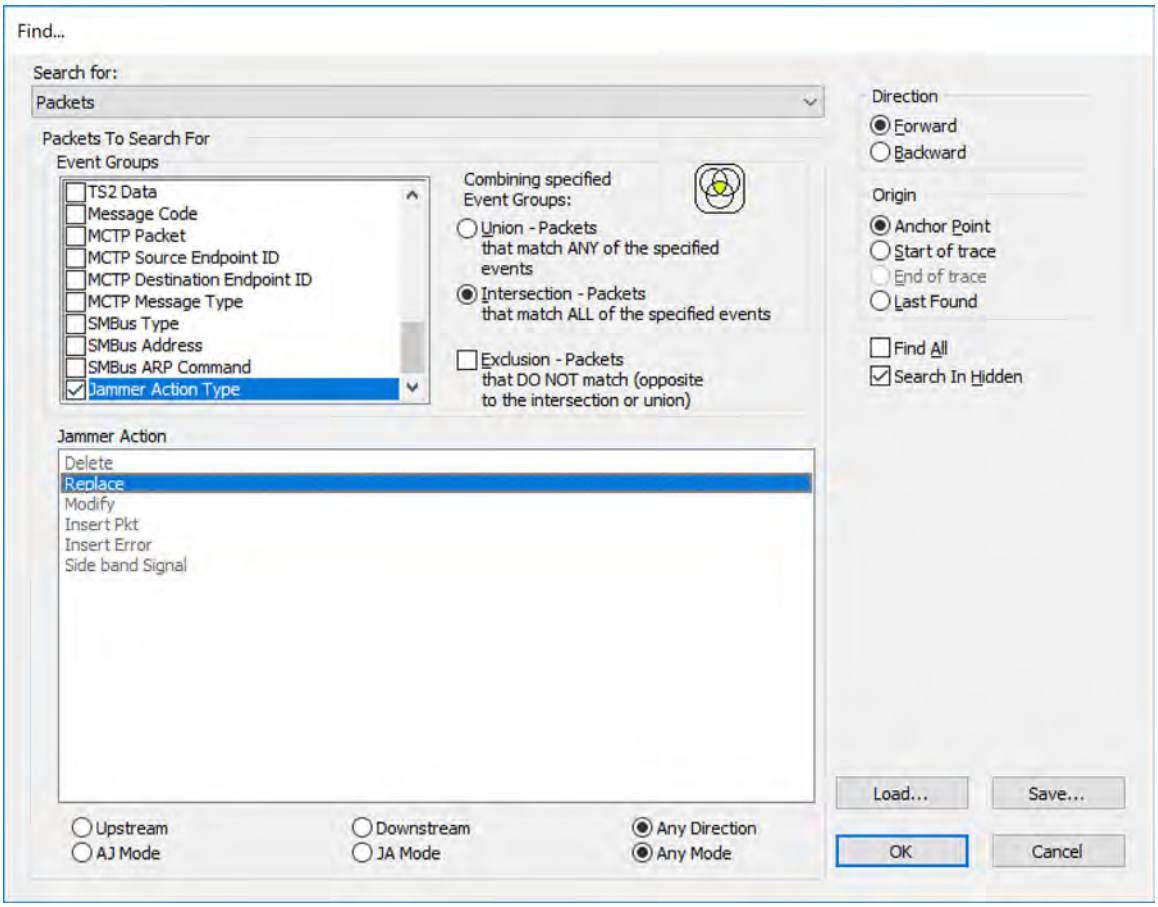


Figure 6.76: Find -> Search for: Packets -> Jammer Action: Replace

Click on OK and the Jammer Action and following it are the results:

Replace UpdateFC_CP with TS1_PAD_PAD. See Figure 6.77 on page 326.

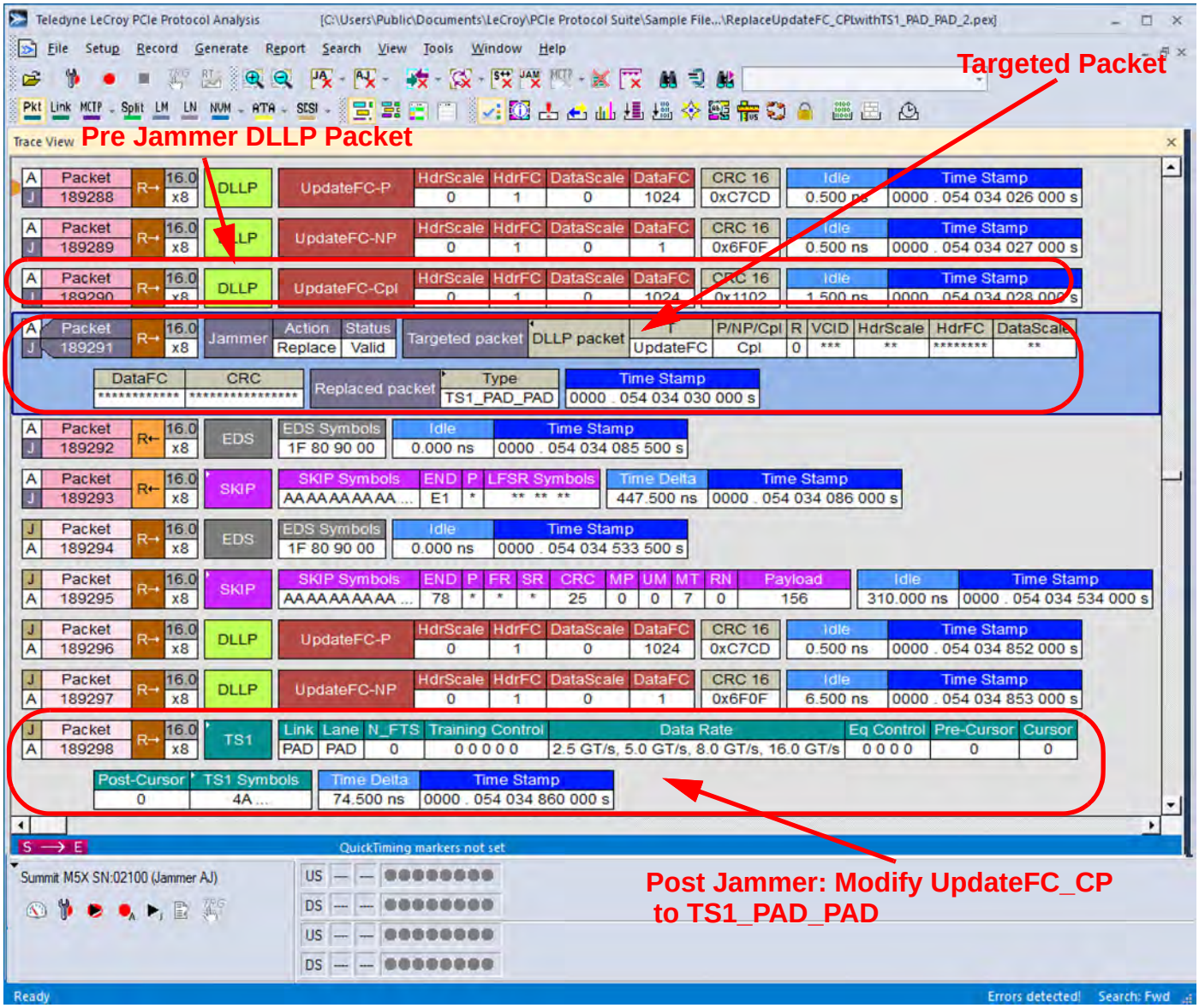


Figure 6.77: Trace with Jammer Function: Modify -> UpdateFC_CP with TS1_PAD_PAD

These examples give you an overview of the types of Jammer Actions that can be added to your traces.

All of the Jammer Actions are discussed in more detail in “Jammer Actions” on page 266.

All of the Jammer Actions can also be added to your script, as shown in “Script Mode” on page 259.

Chapter 7

Recording Options: Analyzer Only Mode

The Teledyne LeCroy Summit M5x™ is a PCI Express 5.0 compliant advanced recording and analysis system supporting 2.5/5.0/8.0/16.0/32.0 GT/s speeds at up to x8 link widths. For recording capabilities see Recording Overview below. For analysis capabilities see "Analysis Options" on page 427.

The recording for Gen5 bus is achieved by means of using a Teledyne LeCroy Gen5 x8 Interposer.

7.1 Recording Overview

After installing the software, recording options should be set prior to recording. The recording options define the behavior of the Summit M5x Gen5 Analyzer during recording. You can create, save and load previously saved recordings. This section explains how to define recording options on the Summit M5x Analyzer/Jammer when capturing Gen5 traffic.

Note: To Record and Analyze Gen5 traffic you need a separate license.

7.1 Recording Option Dialog

The Recording Options dialog is used to configure a recording.

To open the Recording Options window, click  or select the command **Setup > Recording Options**.

Note: There are separate sets of Recording Options for each Analyzer type. To set the Analyzer type, select the appropriate platform from the Target Analyzer menu in the General tab of the Recording Options.

The Recording Options dialog displays options that affect all recordings.

7.2 Select Summit M5x Analyzer for Recording

To record PCIe Express 5.0 traffic, you must select the Summit M5x Analyzer (Gen5) Recording Type Option. See Figure 7.1. The you will see the options available for Summit M5x recording (see Figure 7.1 on page 335).

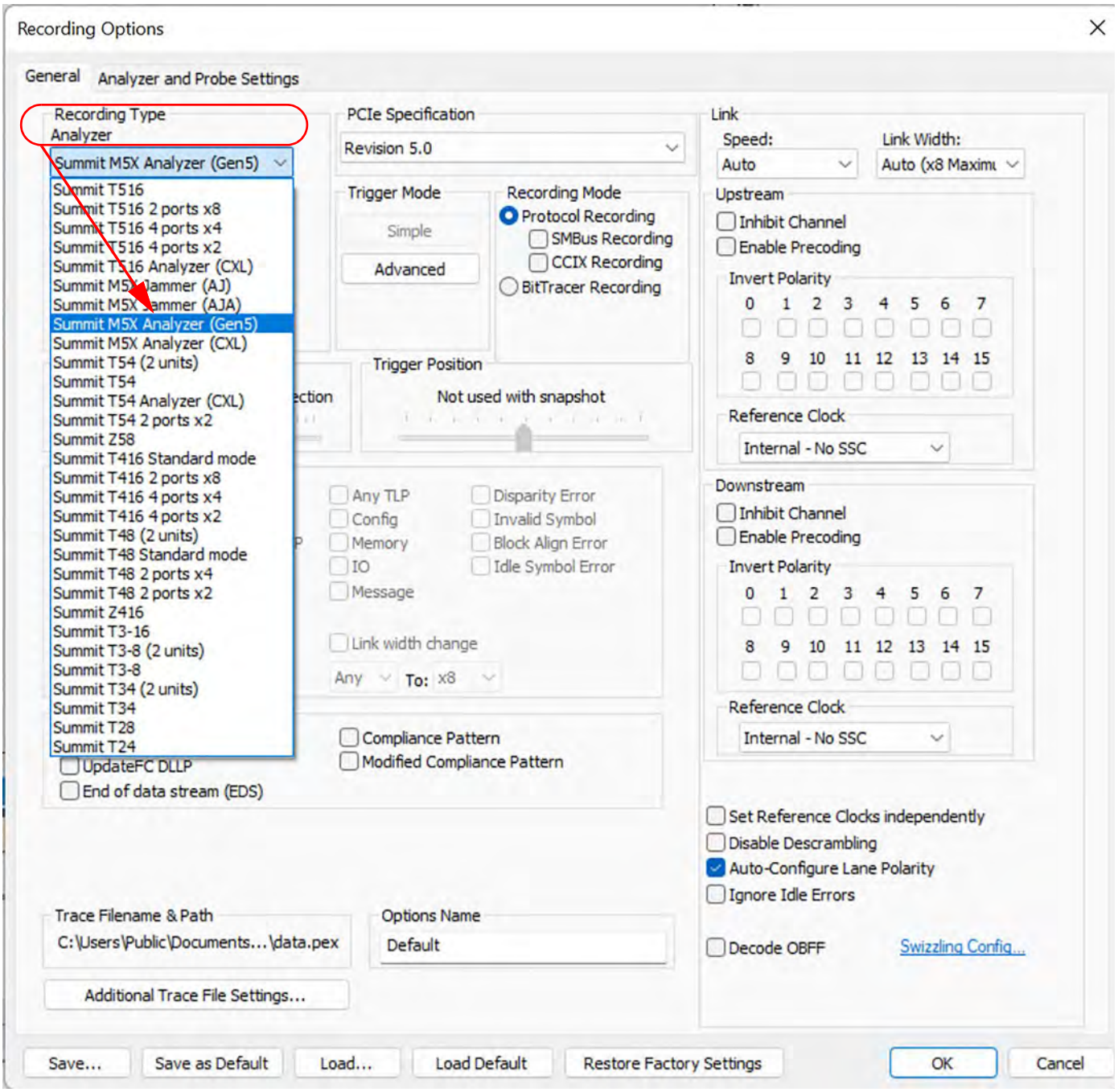


Figure 7.1: Select Summit M5x Anlayzer Only for Recording Options up to 32 GT/s

7.3 Recording Options M5x Analyzer: Simple Mode

This section describes the Simple Mode: Snapshot recording options. See Figure 7.1.

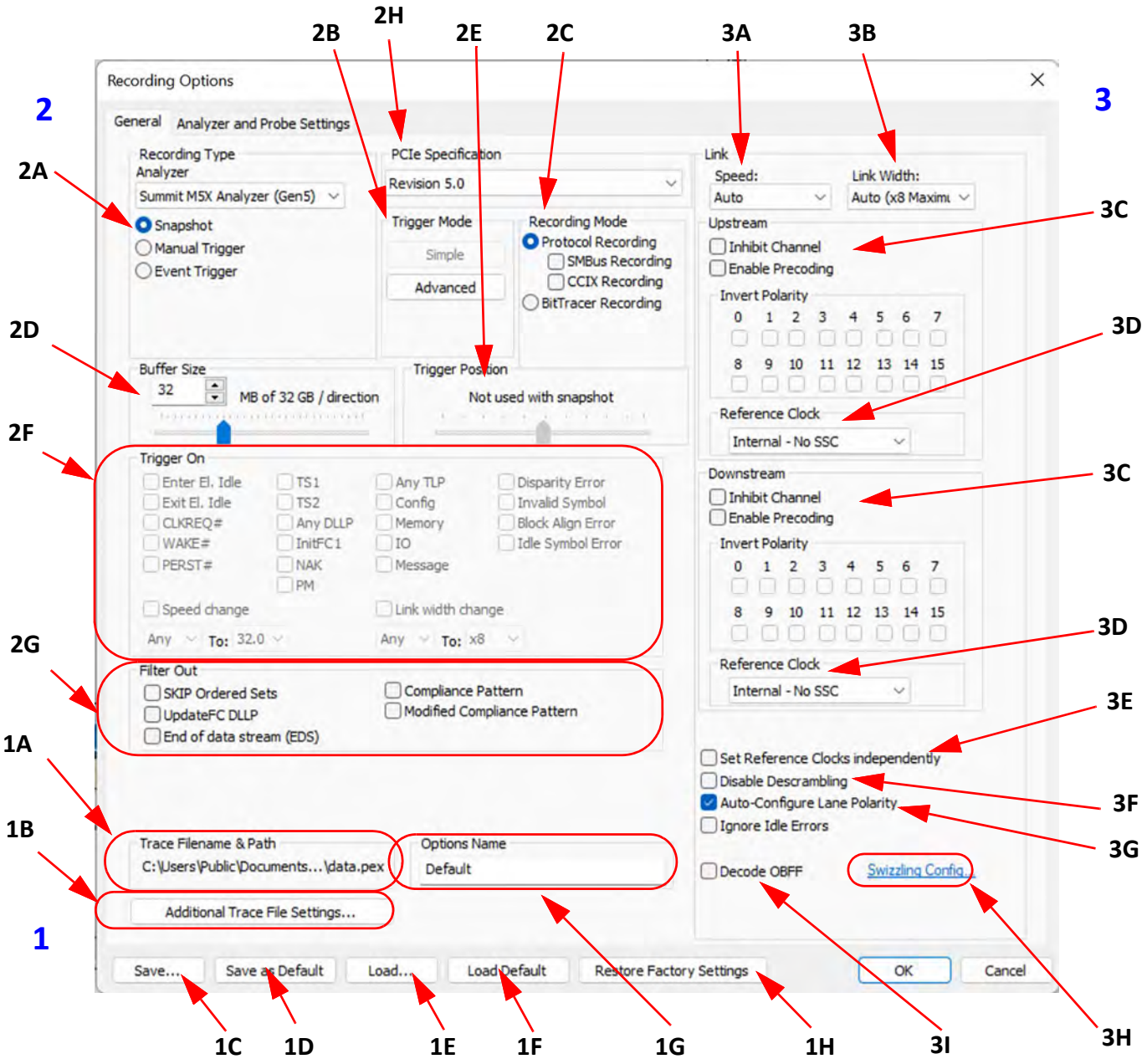


Figure 7.1: Summit M5x in Simple Recording Options

Note: Please refer to the figure callout numbers in each of the sections below to correlate to Figure 5.1 shown above. For instance, for Simple and Advanced Mode, see Figure 5.1: 1B.

For the Summit M5x Recording Options refer to Figure 7.1. In the following section with detailed explanations always refer to Figure 7.1 for the Summit M5x.

7.4 Recording Options M5x Analyzer: Event Trigger Mode

This section describes the Simple Mode: Event Trigger recording options. See Figure 7.2.

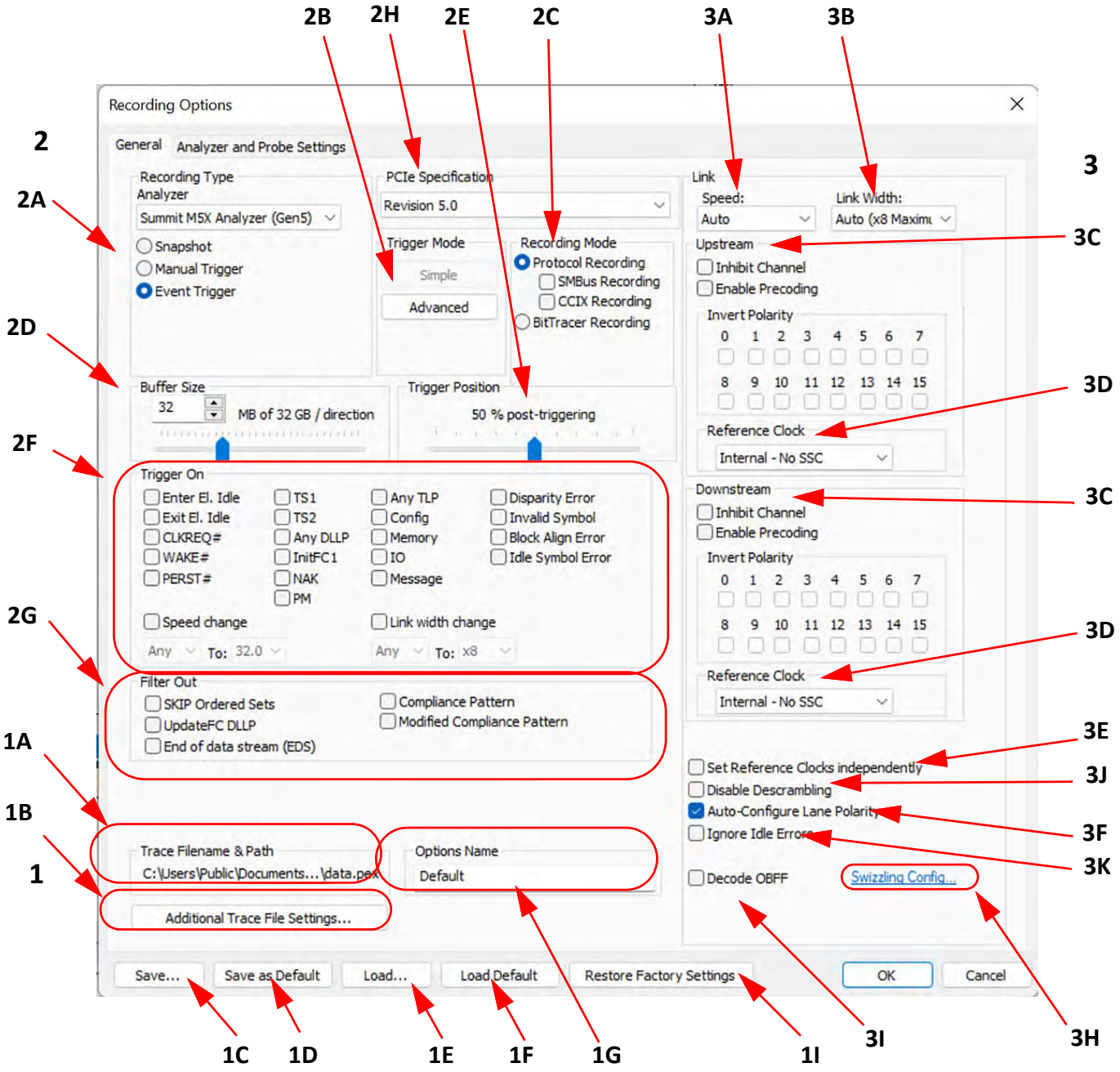


Figure 7.2: Summit M5x in Event Trigger Recording Options

7.5 Recording Options M5x Analyzer: Advanced Mode

If you select the Advanced Mode you'll see the Recording Rules tab at the top of the Recording Options menu. See Figure 7.3.

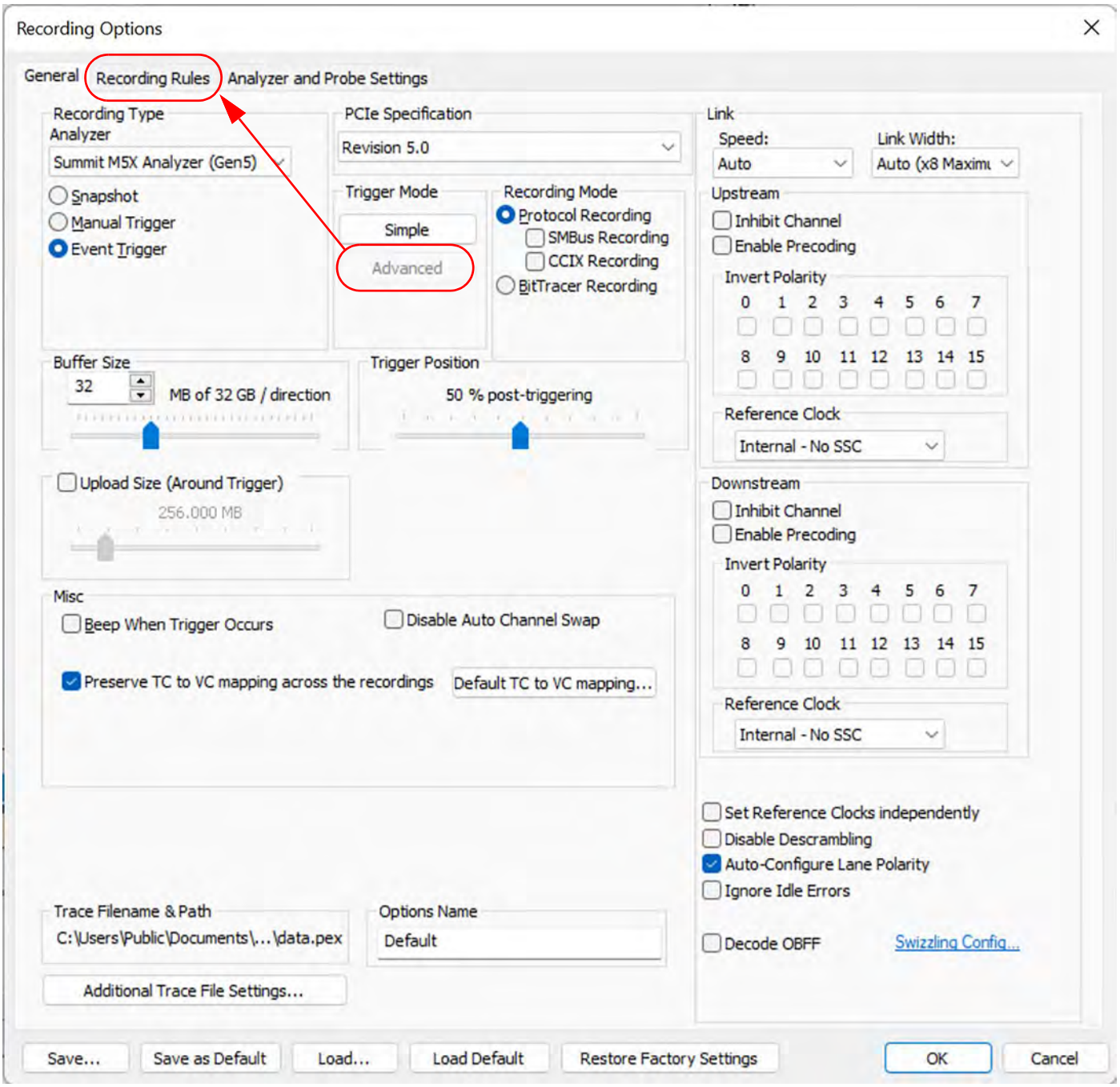


Figure 7.3: M5x Analyzer Only: Advanced Trigger Mode

If you select the Recording Rules tab the following options will become available. See Figure 7.4 on page 338.

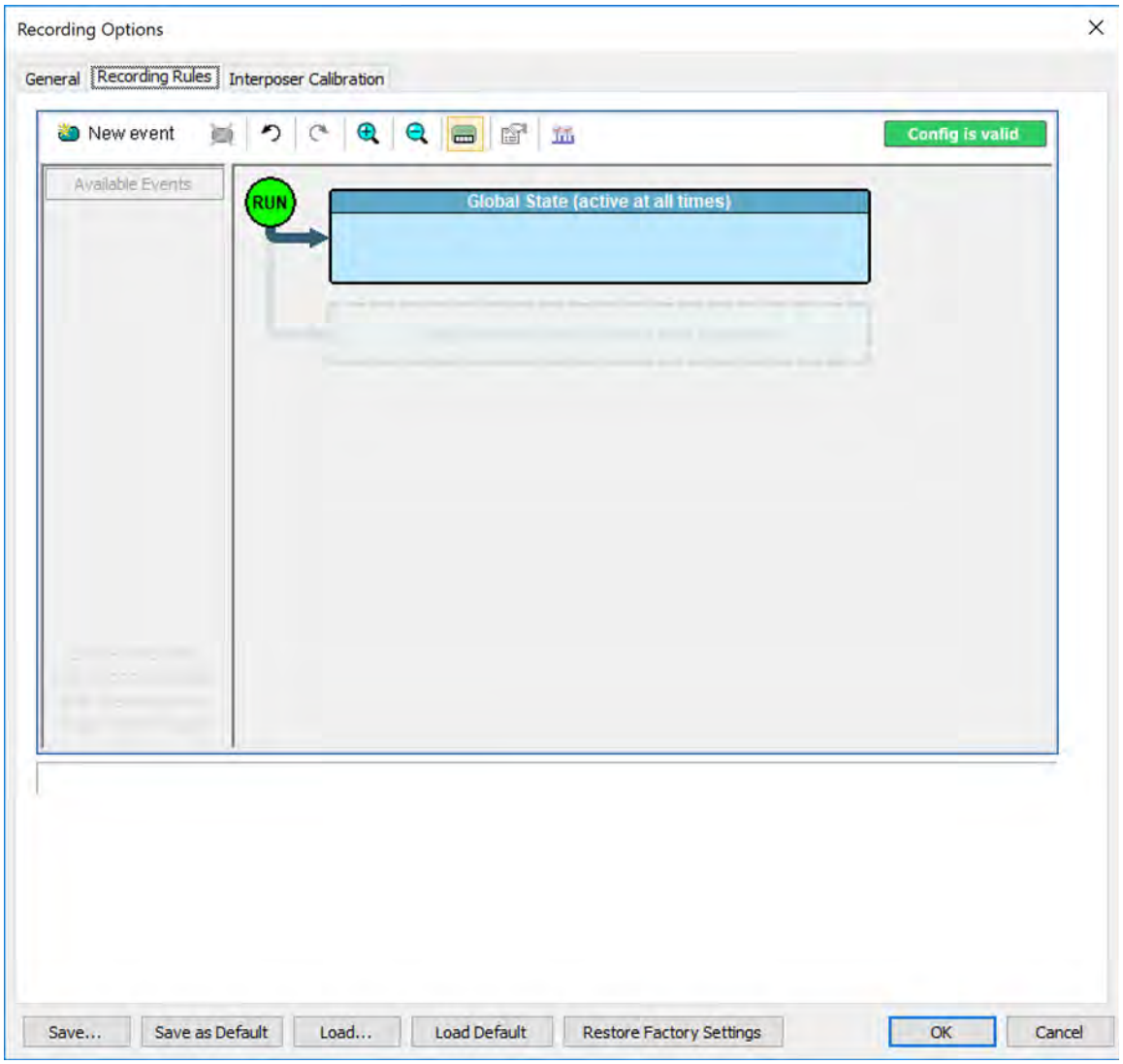


Figure 7.4: Advanced Mode Trigger Options

The Advanced Recording Rules are explained in detail in “Recording Options M5x Analyzer: Advanced Mode” on page 336.

7.6 Recording Type

You can find the Recording Types in Figure 7.1 on page 335: 2A.

7.6.1 Snapshot

A recording of a pre-determined length. You set the recording length in the Buffer Size box. Recording begins when you click the **Rec** button on the toolbar and ends when the selected buffer size is filled or when you press the **Stop** button.

7.6.2 Manual Trigger

Recording begins when you select **Start** in the application. Pressing the **Trigger** button allows the Analyzer to finish recording by switching between the pre-trigger buffer and

the post-trigger buffer. Recording continues until the post-trigger buffer has been filled. You can also end the recording immediately by pressing the **Stop** button in the application.

Note: Consider that when filtering is enabled, pressing the Trigger button will not necessarily cause the post-trigger buffer to fill automatically, due to packets being filtered and not stored. In this case you will have to use the Stop button to immediately end the recording.

7.6.3 Event Trigger

A recording that switches between the pre-trigger buffer and the post-trigger buffer when it is triggered by an event in the CATC Trace. An Event Trigger begins when you select **Start** in the application and ends when the specified triggering event occurs in the CATC Trace or you press **Stop**. If an event triggers the end of the recording, the Analyzer records a predefined amount of post-trigger data (specified by Trigger Position and Buffer Size.)

You can also terminate an Event Trigger recording by pressing the Manual Trigger button on the front of the Analyzer. When the Manual Trigger button is pressed, the Analyzer continues to record until the specified post-trigger buffer has been filled. See Figure 7.5 on page 340.

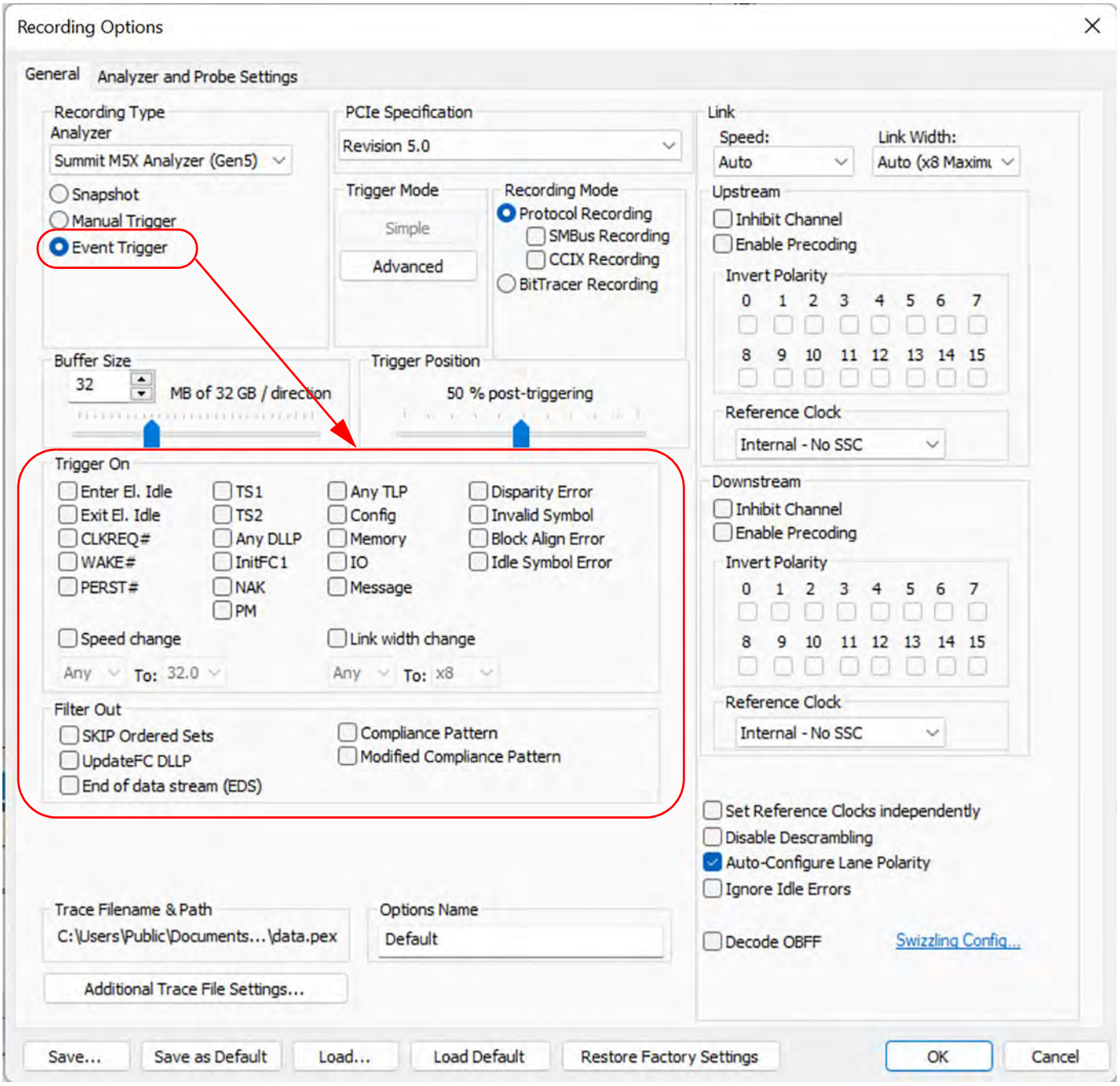


Figure 7.5: Simple Recording Options: Triggered Events -> Trigger On and Filter Out

7.6.3.1 Triggering On (Simple Mode)

You can check any of the boxes shown in Table 7.11 for Trigger On in Simple Mode (see Figure 7.6 on page 341 or Figure 7.1 on page 335: 2F).

TABLE 7.11: Simple Mode Trigger On Events (Upstream or Downstream)

Enter Elec Idle	TS1	Any TLP	RD Error
Exit Elec Idle	TS2	Config	Invalid Symbol

TABLE 7.11: Simple Mode Trigger On Events (Upstream or Downstream)

CLKREQ#	Any DLLP	Memory	Block Align Error
WAKE#	InitFC1	IO	Idle Symbol Error
PERST#	NAK	Message	
	PM		
	Link Speed Change: Any, 2.5, 5.0, 8.0 16.0, 32.0 To: Any, 2.5, 5.0, 8.0, 16.0, 32.0	Link Width Change: Any, x1, x2, x4 or x8 To: Any, x1, x2, x4 or x8	

Note: Trigger Position slider becomes enabled only when Recording Type is set to Manual Trigger or Event Trigger.

If you check 2 or more boxes the triggering will occur based on an OR condition, not AND condition.

External Input Trigger is not configurable, it will always cause the analyzer to trigger on a toggle when using manual trigger or triggering on any event.

Consider that when filtering is enabled, pressing the Trigger button will not necessarily cause the post-trigger buffer to fill automatically, due to packets being filtered and not stored. In this case you will have to use the Stop button to immediately end the recording.

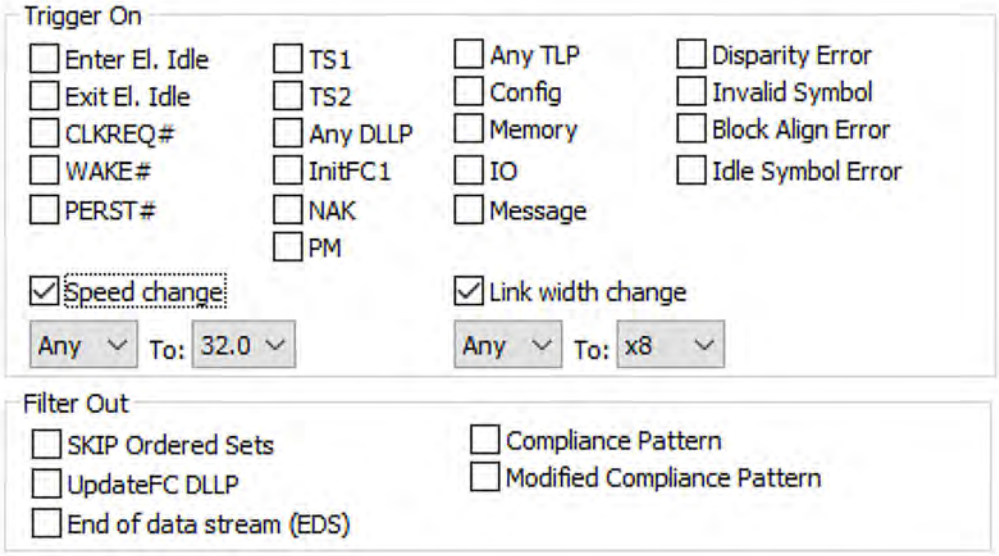


Figure 7.6: Simple Mode Triggering Options

7.6.3.2 Filter Out (Simple Mode)

You can check any of the boxes shown below for Filter Out in Simple Mode (see Figure 7.7 or Figure 7.5 on page 340: 2G).

- Skip Ordered Sets
- UpdateFC DLLP
- End of data stream (EDS)
- Compliance Pattern
- Modified Compliance Pattern



Figure 7.7: Event Trigger: Filter Out

7.7 Recording Mode

There is one recording mode option for Recording Mode with the Summit M5x (see Figure 7.1 on page 335: 2C):

- Protocol Recording
  - SMBus Recording
  - CCIX Recording
- BitTracer Recording

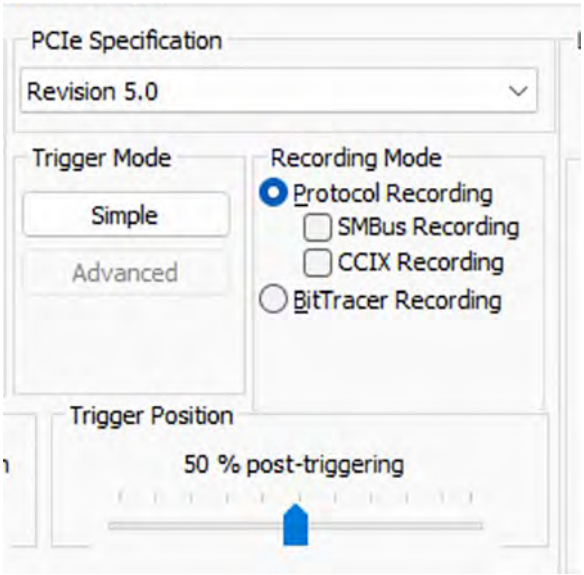


Figure 7.8: Recording Mode Options

Note: CCIX Recording not available with 11.38 version of PCIe Analysis Software

7.7.1 Protocol Recording

The Protocol Recording mode is an intelligent mode that understands the protocol and displays the recorded data according to the specification. By default it uses the CATC Trace View to show the traffic happening on the wire.

You can use most of the triggering, filtering and sequencing features.

7.7.2 Bit Tracer Recording

When the Bit Tracer Recording box is checked, the recording behaves as a regular serial logic analyzer. The data is displayed in Bit Tracer view which displays the symbols being transmitted on each PCI Express lane. In this mode, you can trigger on the same events and use the sequencer as with Protocol Recording Mode but filtering is not allowed. The Bit Tracer mode will record all the traffic.

Note: Leaving all the boxes unchecked results in no trigger in that direction. For more information, see "BitTracer Recording" on page 429.

7.8 Buffer Size

The Buffer Size allows the Analyzer to record traffic to its buffer and then upload the CATC Trace to the host machine. Recordings are limited in size to the size of the Analyzer's buffer, see Figure 7.1 on page 335: 2D (64 GB per direction for the Summit M5x). The Buffer Size slide-bar allows you to set the size of the recording buffer (see Figure 7.9).

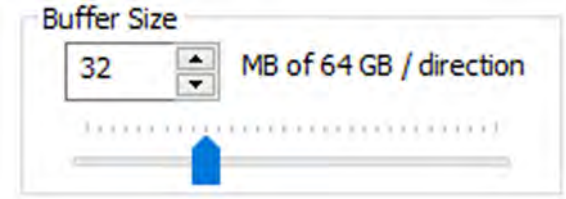


Figure 7.9: Buffer Size Slide Bar (Summit M5x)

The size selection is per direction. For example, selecting 32 MB creates two memory areas of that size.

After you have set the Buffer Size, you must set the Recording type and Trigger position options. These options determine how the buffer is used.

Note: The Buffer Size slide-bar does not precisely portray the buffer size because of the way the packets are stored in the Analyzer's memory.

7.9 Trigger Position

This Trigger Position slide-bar lets you adjust the amount of recording buffer allocated to recording pre-trigger and post-trigger traffic (See Figure 7.1 on page 335: 2E).

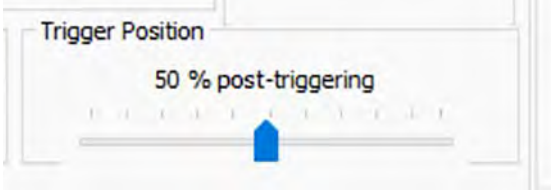


Figure 7.10: Trigger Position Slide Bar

For example, if you set the Trigger Position to 90% Post-Triggering Traffic, the Analyzer records 10% pre-trigger traffic and 90% post-trigger traffic.

Trigger Position is only available when Manual Trigger or Event Trigger is selected.

7.10 Advanced Trace File Settings

You can set the maximum number of traces that can be opened at one time when recording (from 1 to 10). You can also auto-delete traces if your recording session goes beyond the limit set (from 1 to 10). See Figure 7.1 on page 335: 1B or Figure 7.11 and Figure 7.12.

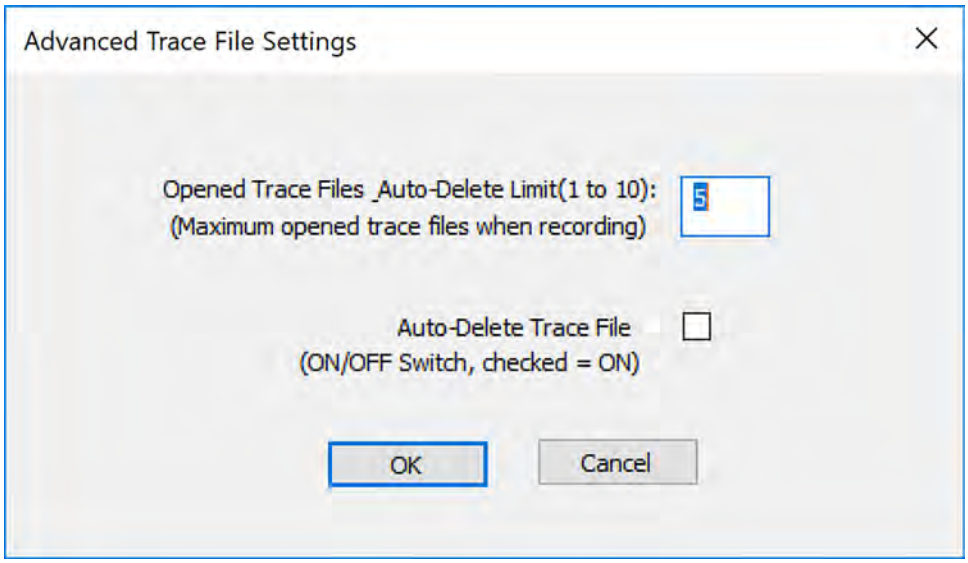


Figure 7.11: Advanced Trace File Settings: 5 Open Traces at a time

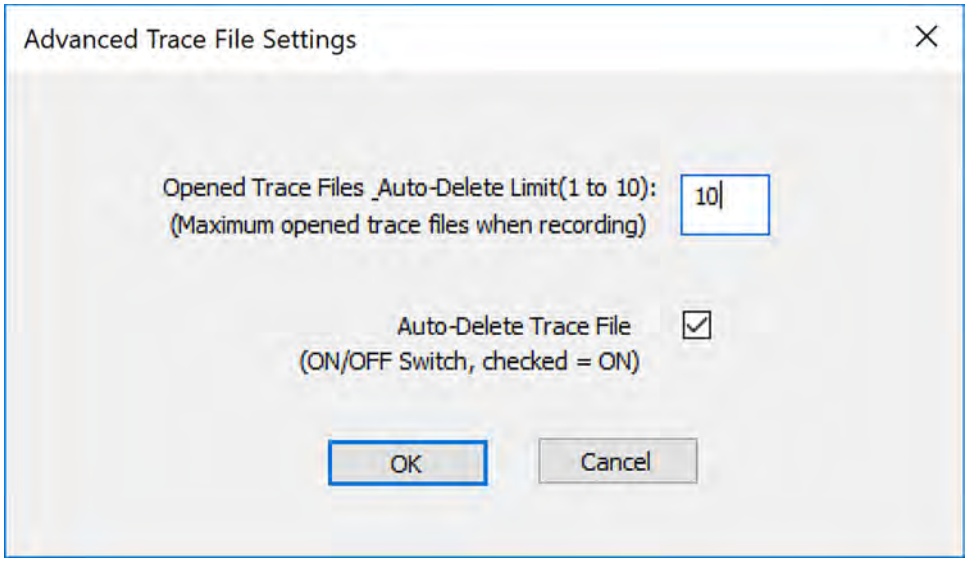


Figure 7.12: Advanced Trace File Settings: 10 Open Traces at a time, Auto-Delete when maximum number reached (10)

7.11 Analyzer & Probe Settings

This tab allows you to access a list of presets, which can be selected from the library and immediately applied, and to view your connected Analyzer (Figure 7.13).

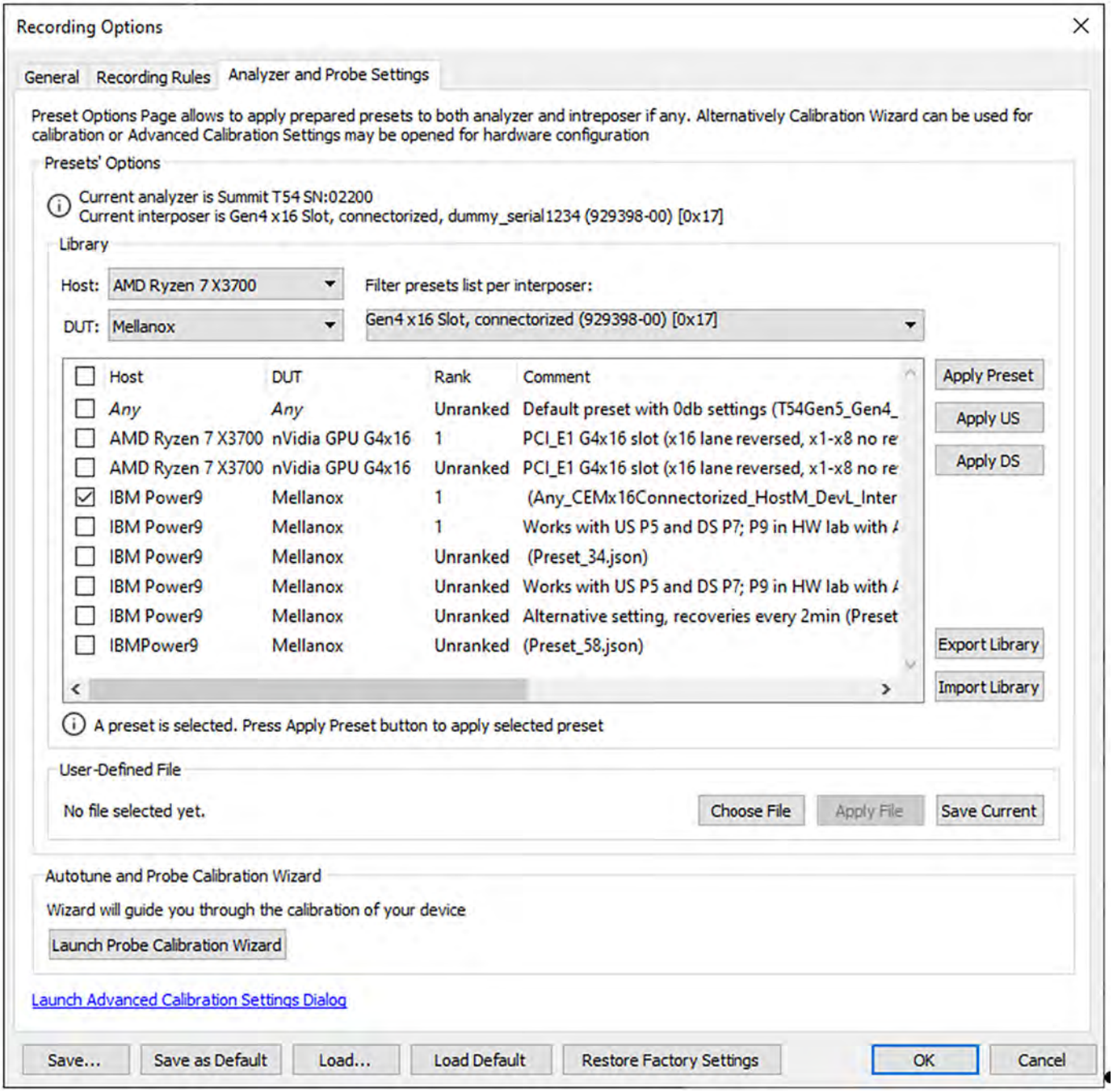


Figure 7.13: Recording Options Presets' Options

7.11.1 Library

The Library contains the presets you can apply and includes the following combo-boxes (Figure 7.14):

- Host – Lists all available Hosts

- DUT – Lists all available DUTs
- Interposer – Lists all available Interposers

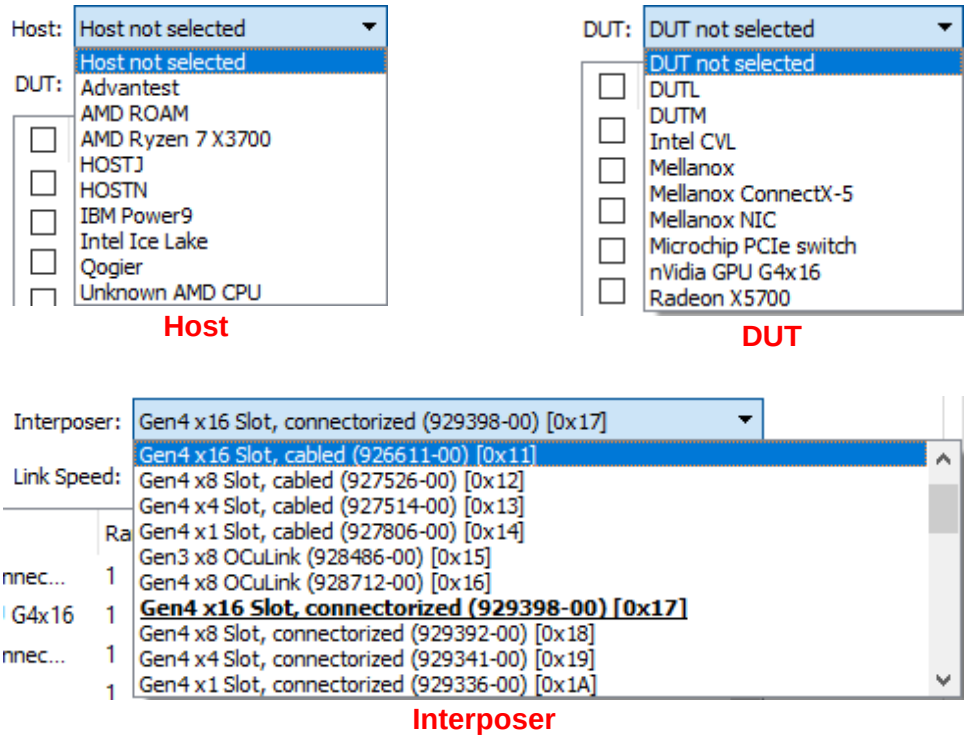


Figure 7.14: Combo-Boxes of Presets' Options

The Interposer connected to the setup is shown in bold and underlined.

When the Analyzer and Probe Settings tab is opened, the connected interposer is automatically displayed in Interposer combo-box. In this example, the list of available Hosts and DUTs is limited to those presets that support current Interposer.

7.11.2 Search Filter

When you select a Host and DUT for the connected Interposer, the presets are shown in the following order:

1. Presets with full match of Host and DUT (displayed in bold)
2. Presets with match in Host
3. Presets with Match in DUT

Note: Currently, only one preset can be selected.

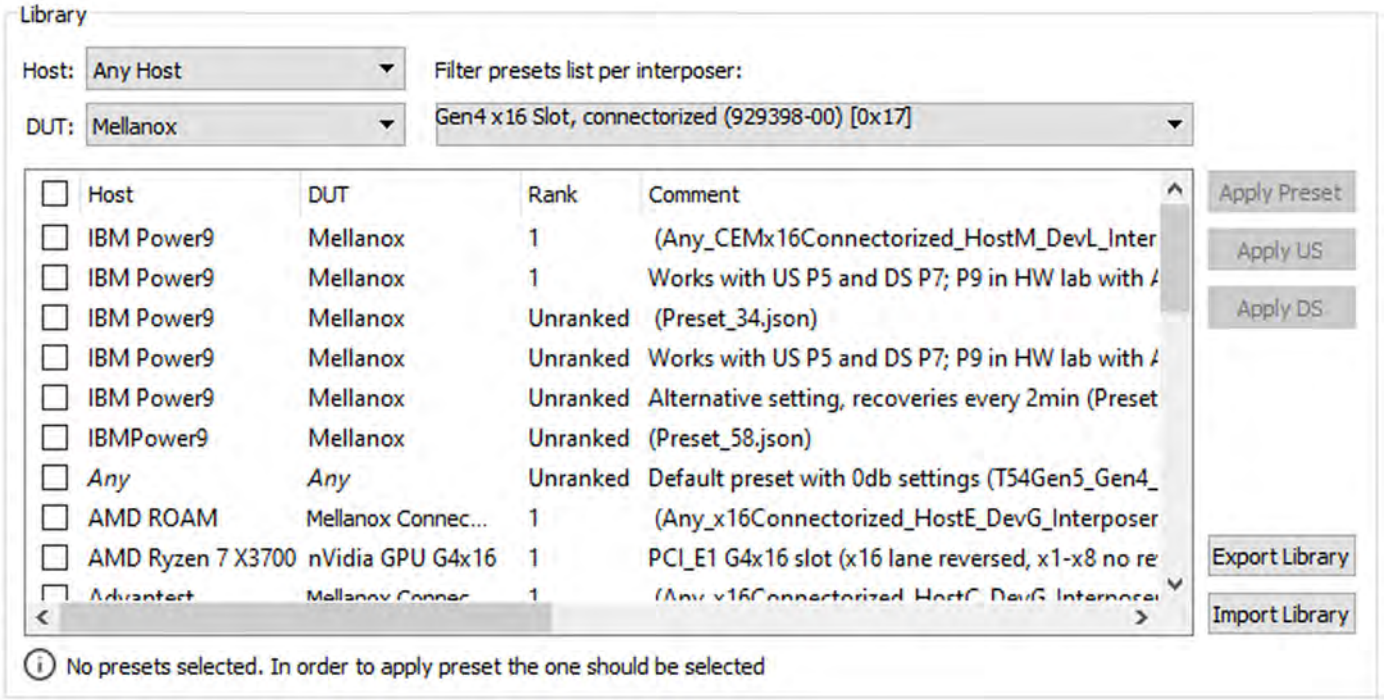


Figure 7.15: Presets' Match in DUT

Selected preset can be applied either on both channels using **Apply Preset** or separately, using **Apply US** or **Apply DS**. Applied presets are applied in Rec Options and written to the Interposer to all Calibration tables.

Note: The Host may need to be rebooted to ensure the DUT is able to reach the necessary speed.

Note: **Column Rank** shows the rate of errors on the link on the scale from 1 to 10, where 1 indicates that there are few or zero errors (Figure 5.137). The larger Rank number indicates that the Preset will contain more errors. It is not recommended to use a Preset with rank higher than 6, because the number of errors on the link will be high.

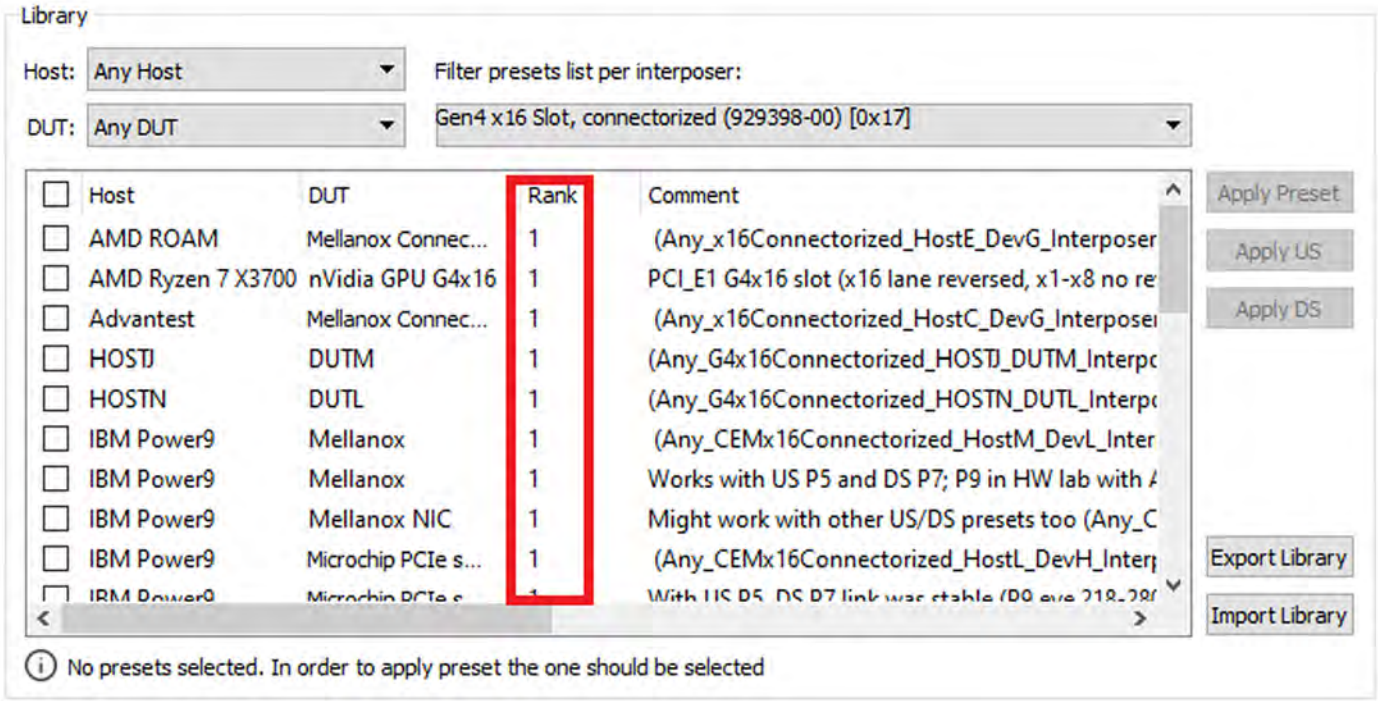


Figure 7.16: Preset with Low Rank Number

Note: It is not recommended that you apply a Preset with a different board ID as it will not be accurate.

7.11.3 Saving a Selected Preset

To save the selected Preset file:

1. Click the **Save Current** button (Figure 7.17) to save the selected Preset file. The Add Configuration File Info dialog box opens, where you can add more configuration details (Figure 7.18).

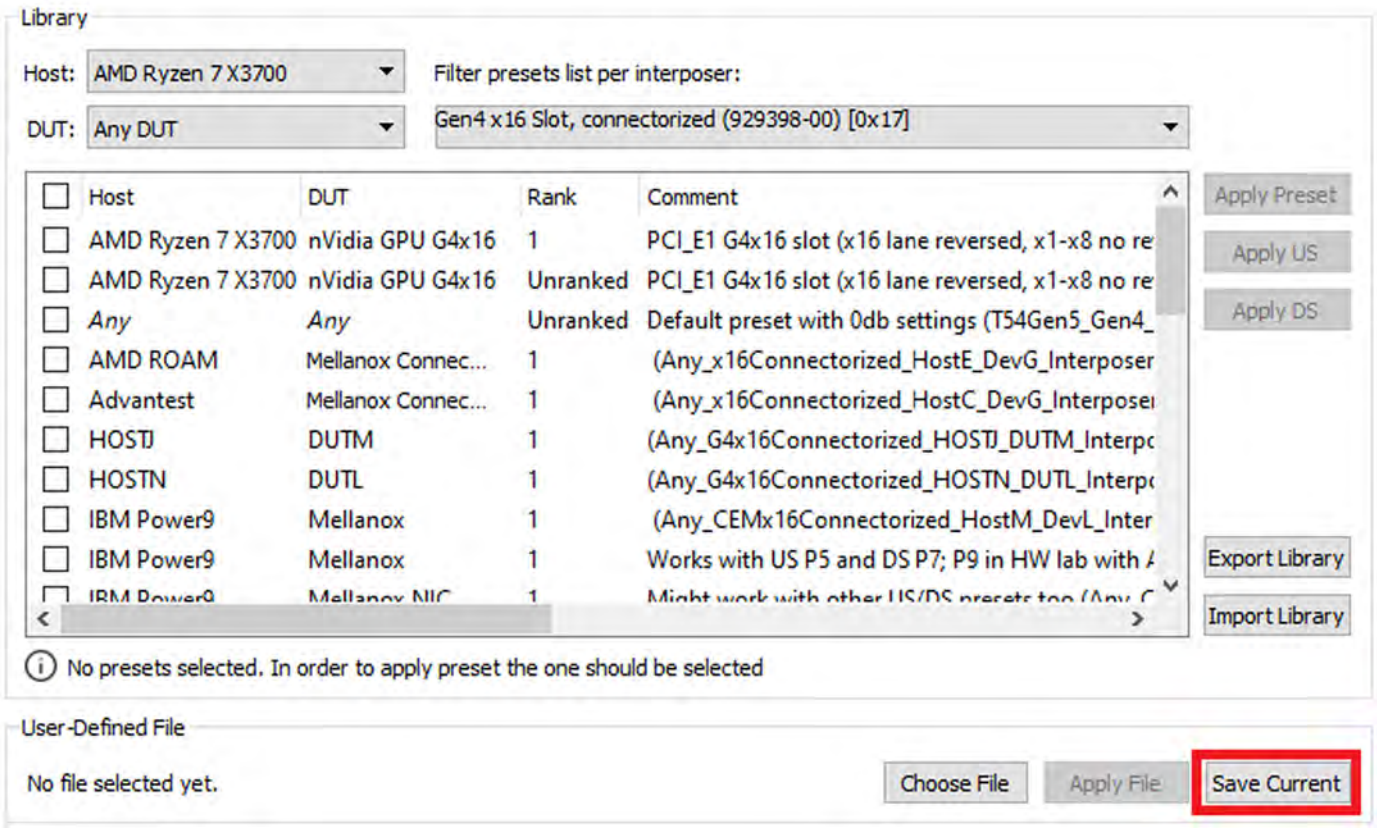


Figure 7.17: Save the Currently Selected Preset

2. Provide a Platform Name and all other details to ensure future searches find the saved values (Figure 7.18).

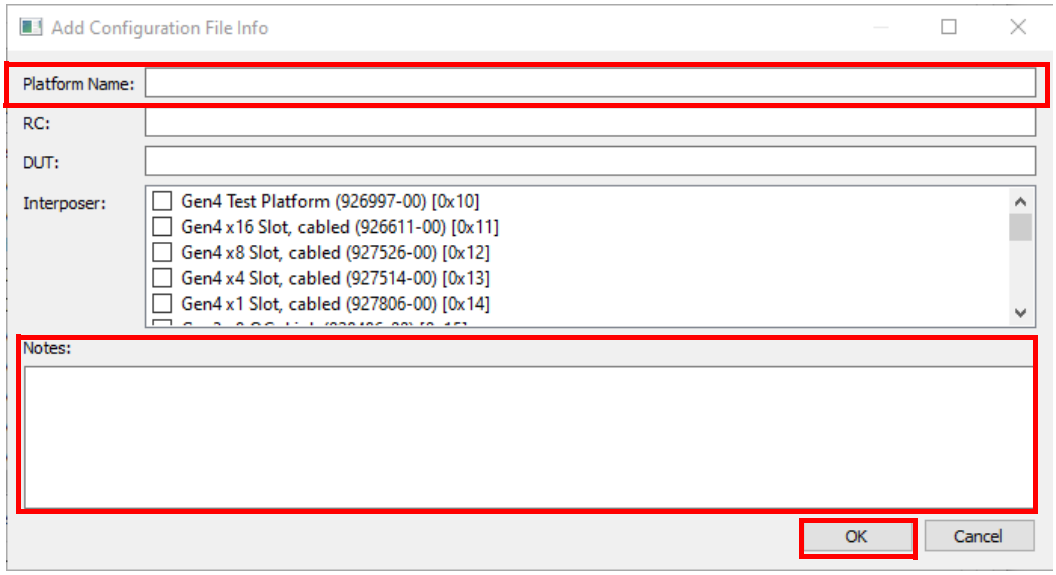


Figure 7.18: Add Configuration File Info Dialog Box

3. If desired, enter additional comments and information into the **Notes** field.
4. Click **OK**. The *Save settings file* window opens (Figure 7.19).

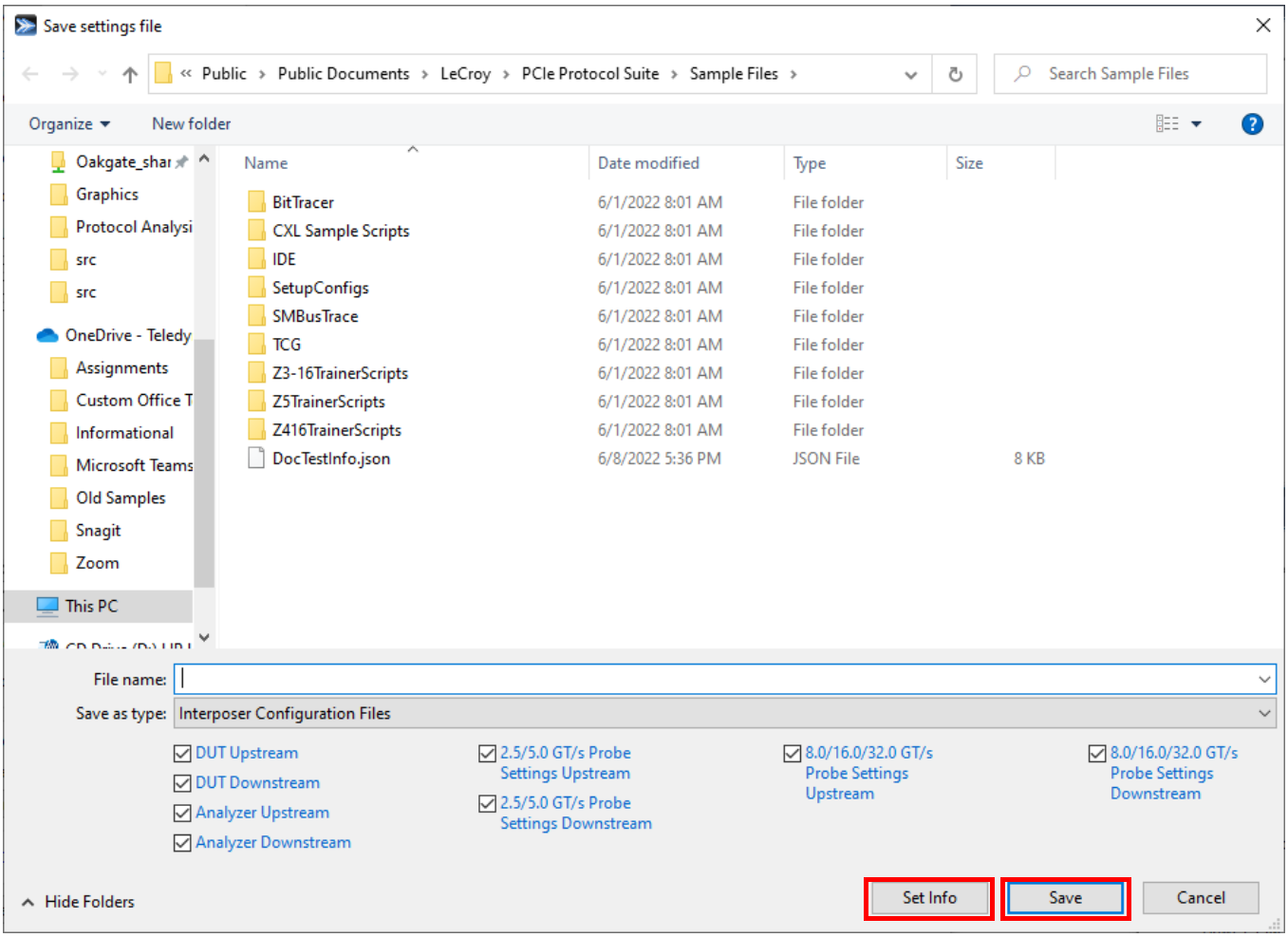


Figure 7.19: Save Settings File Window

5. Enter a file name and click **Save**.

Note: You can skip Step 5 to allow the software to automatically define the interposer.

6. If you wish to specify additional details to the Configuration File, click **Set Info** and follow the prompts.

Note: If you are saving the preset to C:\Users\Public\Documents\LeCroy\PCIe Protocol Suite\InterposerCfgPresets, it will appear in the library and will be exported along with other presets in the folder.

7.11.4 Library Operations

Teledyne LeCroy maintains an online database of presets.

If you are connected to the Internet when you launch the PCIe Protocol Analysis software, your local presets will be automatically updated with the latest information from the online database. If you have no Internet connection, you can easily import the exported library file into the application.

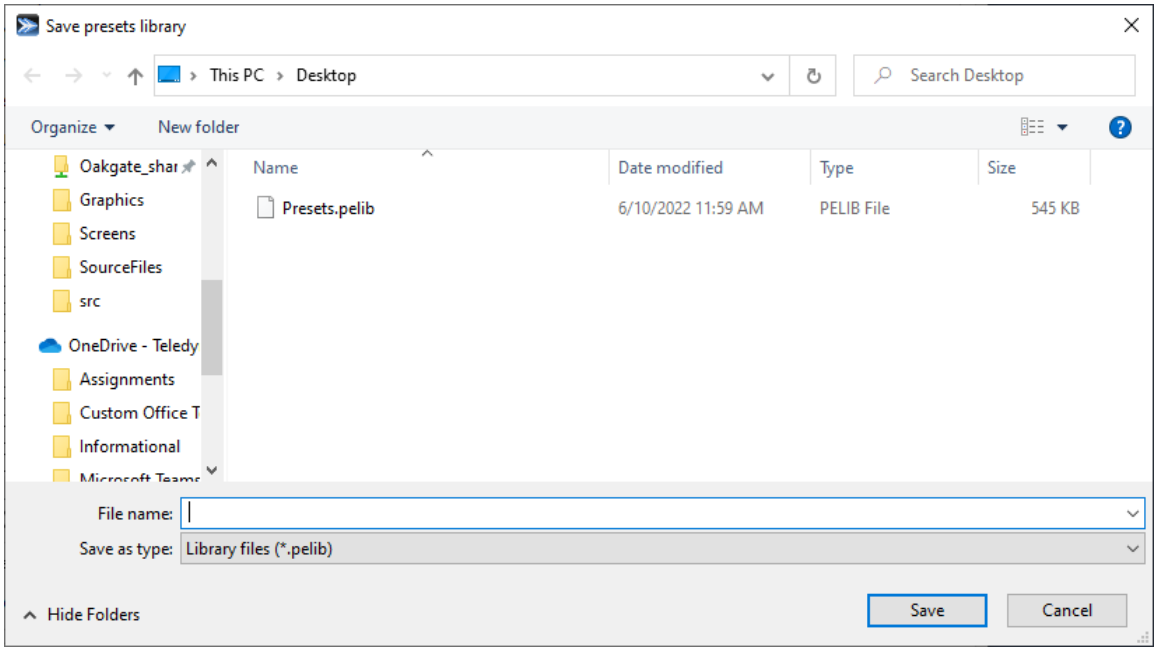


Figure 7.20: Export Library to Computer – User Defined File

7.11.4.1 Buttons & Functions

TABLE 7.1: Buttons – Analyzer & Probe Settings (Sheet 1 of 2)

Button	Function/Description
Apply Preset	Applies settings to both upstream and downstream channels for the selected Preset.
Apply US	Applies settings to upstream channels only for the selected Preset.
Apply DS	Applies settings to downstream channels only for the selected Preset[1].
Export Library	Creates a file in which all of the presets in the Library can be exported into one file in *.pelib format.
Import Library	Opens the Library with all of the presets without an Internet connection. It automatically rewrites the folder C:\Users\Public\Documents\LeCroy\PCIe Protocol Suite\InterposerCfgPresets
Choose File	Loads the preset. You can choose to load presets with all of the tables or only your selected presets.
Apply File	Saves Rec Options and writes the values to the Interposer from Presets on the selected tables. **Note:** If the Preset was created for a different Interposer board ID, the warning prompt shown in Figure 7.21 appears.
Save Current	Saves the manually selected values and writes to the interposer in all three tabs: • Interposer Host to DUT Path • Interposer to Analyzer Path • Analyzer Calibration both 2.5/5.0 GT/s and 8.0/16.0/32.0 GT/s
Launch Probe Calibration Wizard	Opens the Autotune and Calibration Wizard. This will lead you through the steps for both Autotuning the Analyzer and Calibrating the Probe. 7.16.4, *Using the Autotune and Probe Calibration Wizard*.
Launch Advanced Calibration Settings Dialog — Link that opens the Advanced Calibration Setting dialog window. Use this option to manually adjust the probes. See 7.16.3, *Analyzer Calibration*.	
Save...	Saves the Rec Options.
Save as Default	Saves the current Recording Options as default 1.
Load...	Opens File Explorer with a path to the PCIe Protocol Suite. Select a folder and click **Open** to apply the Rec Options.
Load Default	Loads the default Recording Options
Restore Factory Settings	Restores all Recording Options (including defaults) back to the original factory settings

TABLE 7.1: Buttons – Analyzer & Probe Settings (Sheet 2 of 2)

Button	Function/Description
OK	Applies the settings.
Cancel	Discards any changes that were made in Rec Options and closes Rec Options window

1. Once you click **Apply**, you will be prompted to reboot the Host to correctly apply the selected Preset.

Note: If you select a Preset, which was not developed for the current interposer, the interposer will try to map the values.

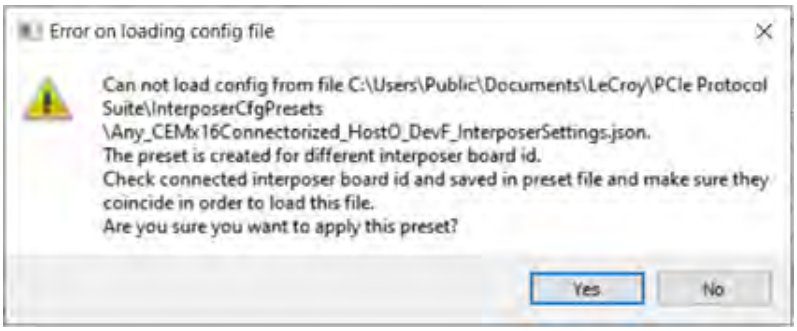


Figure 7.21: Warning Prompt – Error Loading Config File

7.12 Trace Filename and Path

The Trace Filename and Path button sets the path and CATC Trace name for the recording. It allows you to change the default file name and path for the recorded CATC Trace file. The pre-defined name is **data.pex**. See Figure 7.1 on page 335: 1A.

1. Select the **Recording File Name** button.
2. The Specify Trace File Name dialog opens to navigate to the directory you want.
3. Enter the new file name in the File name field.
4. Click the **Save** button.

   This action does not do any immediate save operation. It just changes the default name and uses it in subsequent recordings.

7.13 Saving and Loading Previously Saved Recording Options

You can save a recording or load previously saved recordings. In the Recording Options dialog the following Save options are available (see Figure 7.1 on page 335: 1C and 1E).

7.13.1 Saving Recording Options

To save the current recording options into the default Recording Options file:

For example, if your Recording Options file were named **StandardSettings.rec**, your Options Name could be a long descriptive label such as **Standard Record Options used for all normal Recordings**.

Save: See Figure 7.1 on page 335: 1C

Saves the current options to whatever file name you provide in the Options name box (Figure 7.1 on page 335 1G).

Save As Default: See Figure 7.1 on page 335: 1D

Saves the current options into the default options file. This file is called **default.rec** or any other name you have assigned to the default options file. Whenever the Teledyne LeCroy PCIe Protocol Analysis begins execution, it automatically loads the default file, if one exists.

You can Save your recording options by entering a name into the Options Name box. See Figure 7.1 on page 335: 1G.

7.13.2 Loading Recording Options

Load: See Figure 7.1 on page 335: 1E

Loads a previously saved set of recording options.

Load Default: See Figure 7.1 on page 335: 1F

Loads the default set of recording options.

Restore Factory Settings: Figure 7.1 on page 335: 1H

This will restore the Factory Settings for Recording options.

OK

Applies changes and closes the Recording Options dialog.

Cancel

Cancels changes and closes the Recording Options dialog.

7.13.3 Loading Recording Options

In the Recording Options menu, you can load a previously saved recording options file.

To load Recording Options:

1. Select **Setup > Recording Options** from the menu.
2. Click the **Load** button from the Recording Options dialog (see Figure 7.1 on page 335 1E). The Load dialog opens and lists previously saved options files (***.rec**).
3. Select a file and click **OK**. The options file loads.

7.13.4 Saving Recording Options

Recording Options settings can be saved and later reused. Recording options settings are stored in ***.rec** files.

1. Open the Recording Options dialog by selecting **Setup > Recording Options.**
2. Set your options, then click **Save** (see Figure 7.1 on page 335 1C).
3. Enter a unique file name. The **.rec** extension is added by default.(optional) To add a descriptive label to this file to help you remember what options were set, use the **Options Name** box. See Figure 7.1 on page 335: 1G.

7.14 Viewing Legacy Multi-Segmented CATC Traces

Current PCIe Protocol Analysis handles traces as large as the maximum buffer size selected. It does not need to generate segmented traces, but is able to open segmented traces generated with older software versions. Simply open the *.pem extension file and the trace will be converted to a new format single trace. If opening a *.pex file part of a segmented trace make sure not to update the file in order for the original segmented index to work properly.

7.15 Link Settings

The Link options panel allows you to manage links (see Figure 7.22 for the Summit M5x Analyzer). You can define the basic link parameters or leave it on Auto detect. The various link settings are described in this section (See Figure 7.1 on page 335: 3A and 3B).

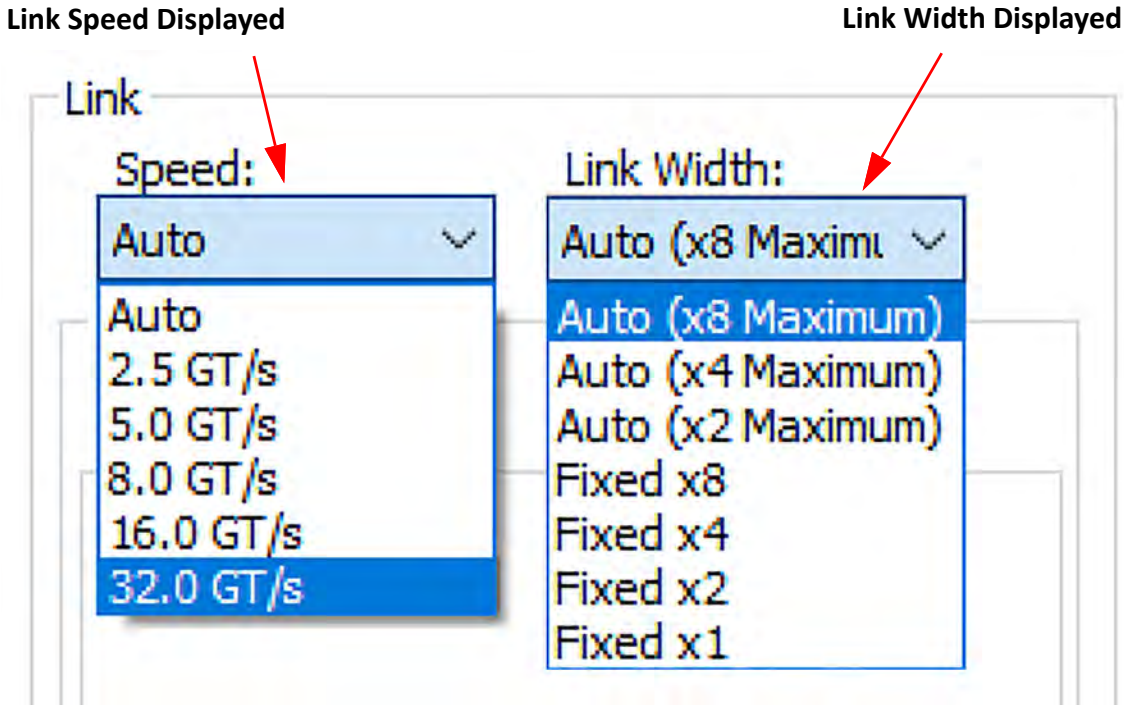


Figure 7.22: Link Options for Summit M5x Analyzer: Speeds up to 32.0 GT/s

7.15.1 Speed

The Speed can be set at Auto, 32.0 GT/s, 16.0 GT/s, 8.0 GT/s, 5.0 GT/s, or 2.5 GT/s for the Summit M5x from the drop-down menu. The default is Auto (see Figure 7.1 on page 335: 3A or Figure 7.22 on page 355 above left side).

Note: When set to Auto, Teledyne LeCroy's embedded software automatically determines the speed. **Disable Descrambling** is also enabled. See Figure 7.23 on page 358.

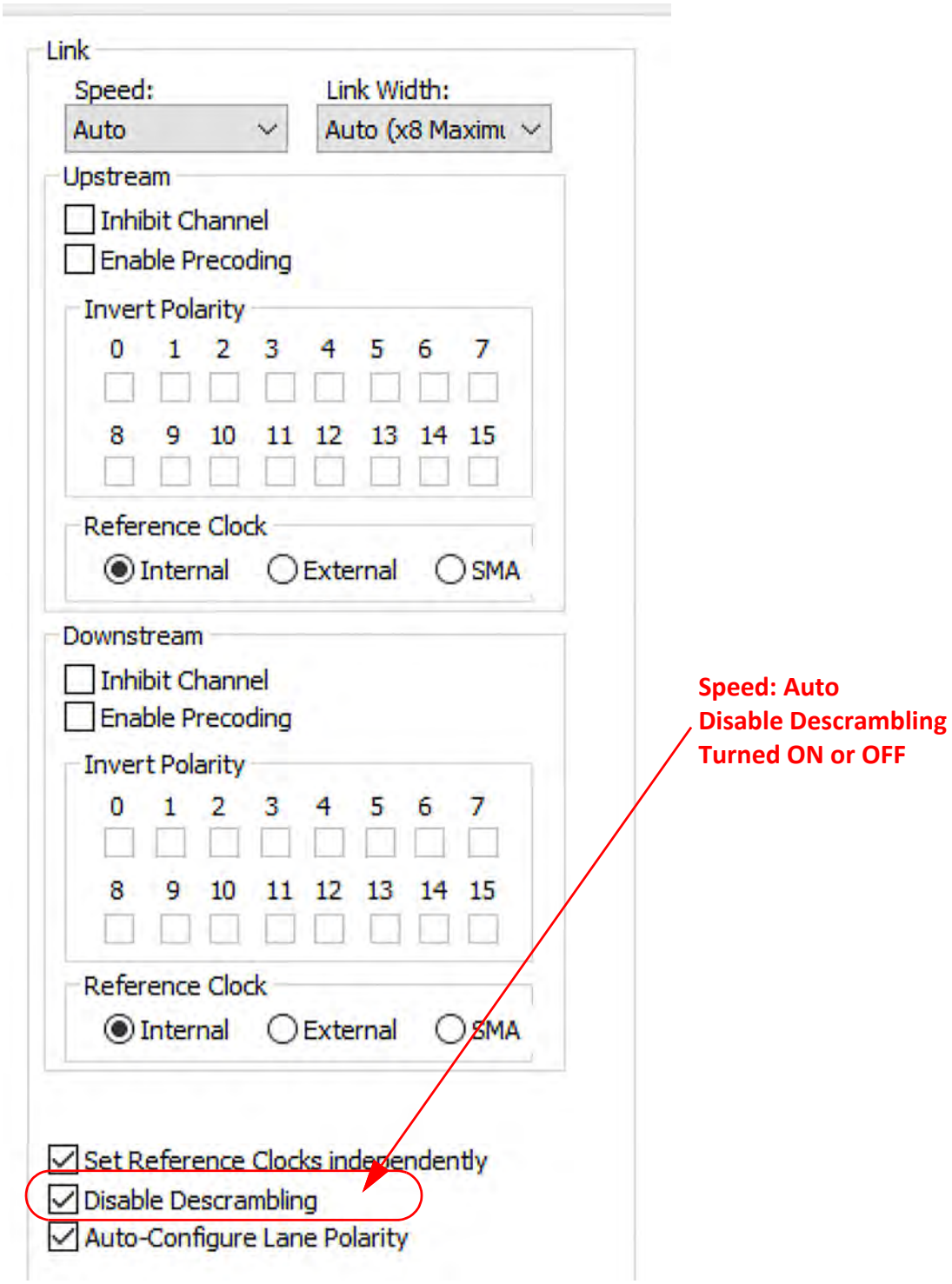

Link
Speed:
Auto
Link Width:
Auto (x8 Maximu
Upstream
Inhibit Channel
Enable Precoding
Invert Polarity
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
Reference Clock
Internal External SMA
Downstream
Inhibit Channel
Enable Precoding
Invert Polarity
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
Reference Clock
Internal External SMA
Set Reference Clocks independently
Disable Descrambling
Auto-Configure Lane Polarity
Speed: Auto
Disable Descrambling
Turned ON or OFF

Figure 7.23: Speed set to Auto: Descrambling Enabled or Disabled

Note: When set to a specific speed (32.0 GT/s, 16.0 GT/s, 8.0 GT/s, 5.0 GT/s, or 2.5 GT/s) Teledyne LeCroy's software forces the hardware to record at that speed.

When set to a specific speed, (End of Data Stream) EDS detection is disabled.

For Auto speed setting to work the polarity setting of lane 0 has to be correct. The polarity can be set manually if the link is already in L0 state, or, for automatic polarity detection, the bus has to go through a training sequence so the analyzer can track the polarity.

Note: When selecting Auto in the Speed drop-down list the embedded software is able to find the correct speed even if the link does not go through a training sequence.

7.15.2 Link Width

The Link Width sets the physical width of the link. Select the Link Width from the drop-down menu (see Figure 7.1 on page 335: 3B or Figure 7.22 on page 355 right side for the Summit M5x). The available options (and the default) will be shown according to the detected product.

Auto Max X8: Calculates link width automatically up X8

Auto Max X4: Calculates link width automatically up X4

Auto Max X2: Calculates link width automatically up X2

Fixed X1 Link is assumed to be always X1

Fixed X2 Link is assumed to be always X2

Fixed X4 Link is assumed to be always X4

Fixed X8 Link is assumed to be always X8

Note: If the bus goes to a link width different from the one selected as fixed option, the trace will be full of errors. The appropriate Auto option needs to be selected in this case.

When selecting Auto in the Link Width drop-down list the embedded software is able to find the correct link width even if the link does not go through a training sequence.

If an Auto Link Width is selected, there is no Lane Reversal. If a Fixed Link Width is selected, the Reverse Lanes checkbox is enabled. See Figure 7.24 on page 359 for the Summit M5x.

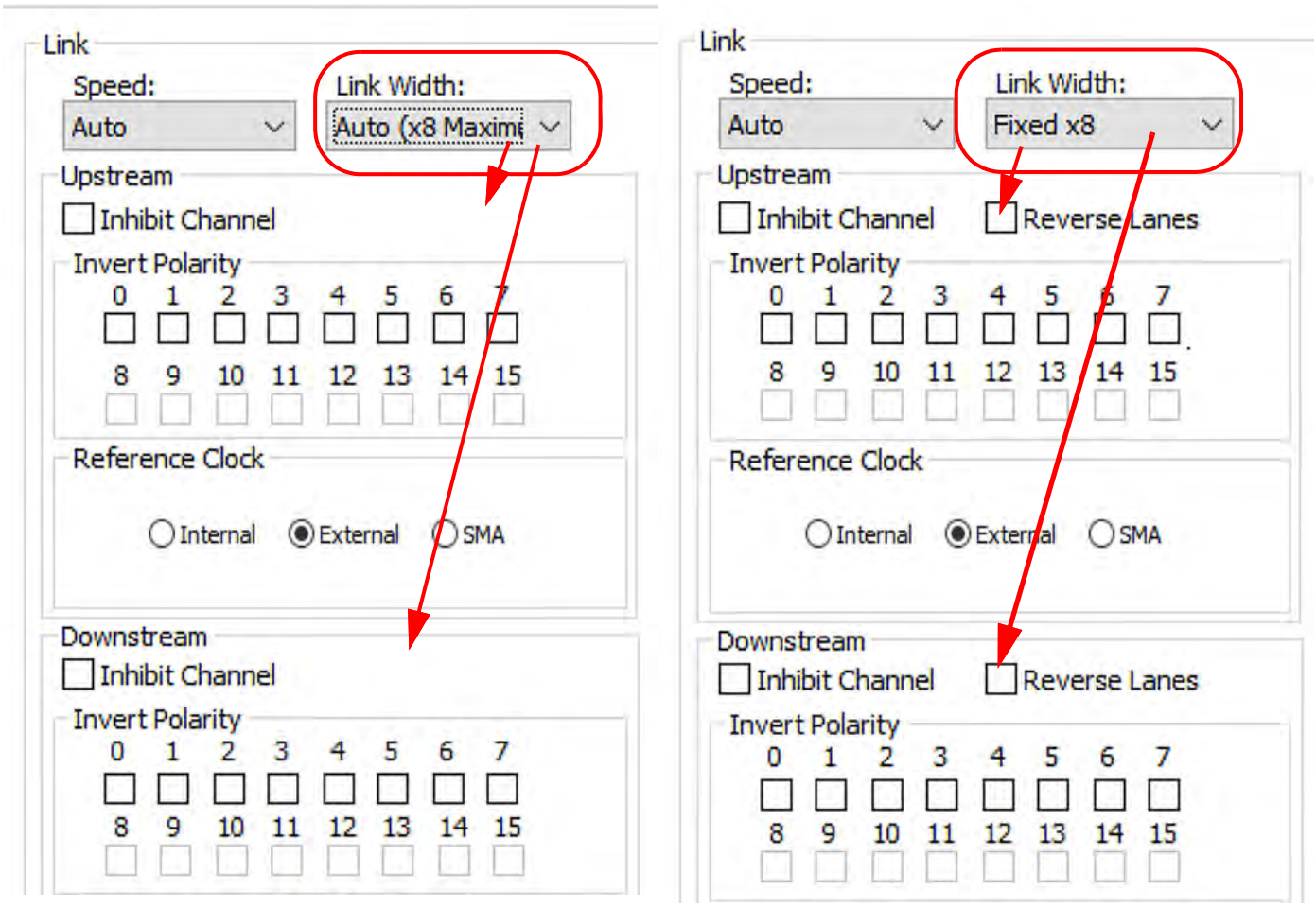


Figure 7.24: Summit M5x Gen 5 Link Width: Auto -> No Lane Reversal,
Fixed Lane Width -> Lane Reversal Check Box is Enabled

7.15.3 Upstream and Downstream

Gives you low-level control over each link direction. The heading for these boxes indicates the port and/or unit to which the following options are applied based on the current Analyzer configuration (see Figure 7.1 on page 335: 3C for the Summit M5x).

- Inhibit Channel: Do not record/upload this channel
- Precoding: This is a feature that is being introduced for 32GT/s, which reduces the chance of a big string of 0s that will break the CRC mechanism. When precoding is enabled at the transmitter, it only acts upon scrambled bits.

7.15.4 Reference Clock

See Figure 7.1 on page 335: 3D for the Summit M5x Analyzer Only.

Usually, both Upstream and Downstream directions use the same clock option, this is why the recording option Reference Clock Independently is set by default.

In cases when you have to use different clocks for the different traffic directions you must select the “Set Reference Clock Independently” option (see Figure 7.1 on page 335: 3F) and set the upstream and downstream clock to come from different sources. See “Set Reference Clock Independently” on page 363.

You can chose the Reference Clock to be one of three sources: the Internal Clock (100MHz +/-300ppm No SSC clock generated in the analyzer), an External Source (Reference clock from the PCIe bus routed through the interposer cable) or SMA connector on the front panel.

In both the Upstream and Downstream directions, you have the following sources for the Reference Clock (see Figure 7.25 on page 361):

- Internal
- External
- SMA

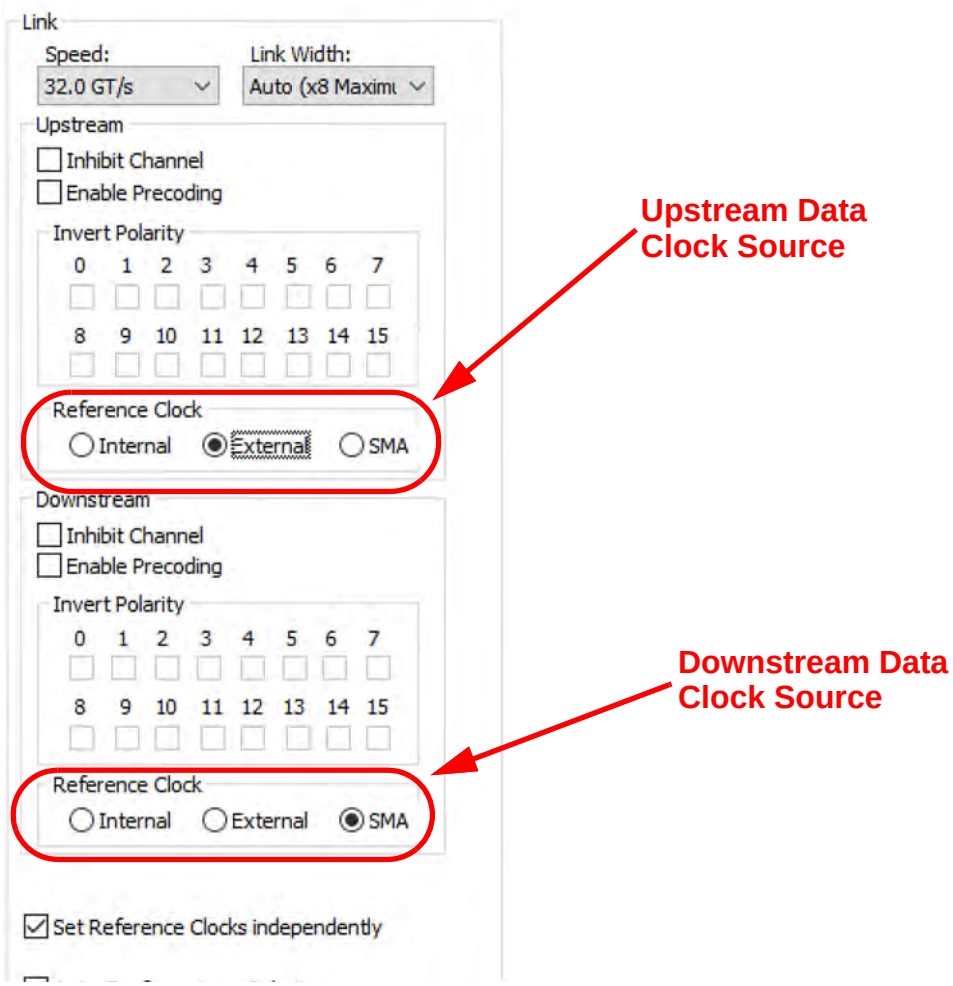


Figure 7.25: Reference Clock: Upstream and Downstream

7.15.4.1 Internal

The analyzer has an internal clock generator that can be used for recording when the Device Under Test does not supply a reference clock. In this case, you select the Internal option.

Note: Due to long exit latency from low power sub states, some loss of traffic has been observed when analyzer latency exceeds DUT latency using the common reference clock. Teledyne recommends the use of the internal reference clock setting for low power sub-states testing.

7.15.4.2 External

For the Summit M5x , External Clock means to use the clock that is supplied through the cable from the Probe card. The Probe card cable gets its clock from the specific Host of Device being used with the analyzer/jammer. You need to select the External Reference Clock option.

Teledyne LeCroy's Summit M5x Probe cards support separate clocks for SRIS applications.

Note: If the PCI Express link under analysis uses spread-spectrum clocking, then the Analyzer must use an external reference clock from the system. Select the External Reference Clock option.

7.15.4.3 SMA

The SMA clock recording option refers to the **Ref Clk In** SMA input connectors on the front panel of the analyzer/jammer. Both the Upstream data and the Downstream data support using a clock from the SMA input connectors. When using the SMA option both clock cables must be connected and the clock must be supplied by the system in order for the recording to happen correctly. The standard PCI Express compliant reference clock is supported. You also need to select the SMA Reference Clock option.

7.15.5 Set Reference Clock Independently

This option allows you to set the options for the Upstream clock and the Downstream clock independently. See Figure 7.1 on page 335: 3E for the Summit M5x). An example of independent Reference Clocks is shown in Figure 7.26.

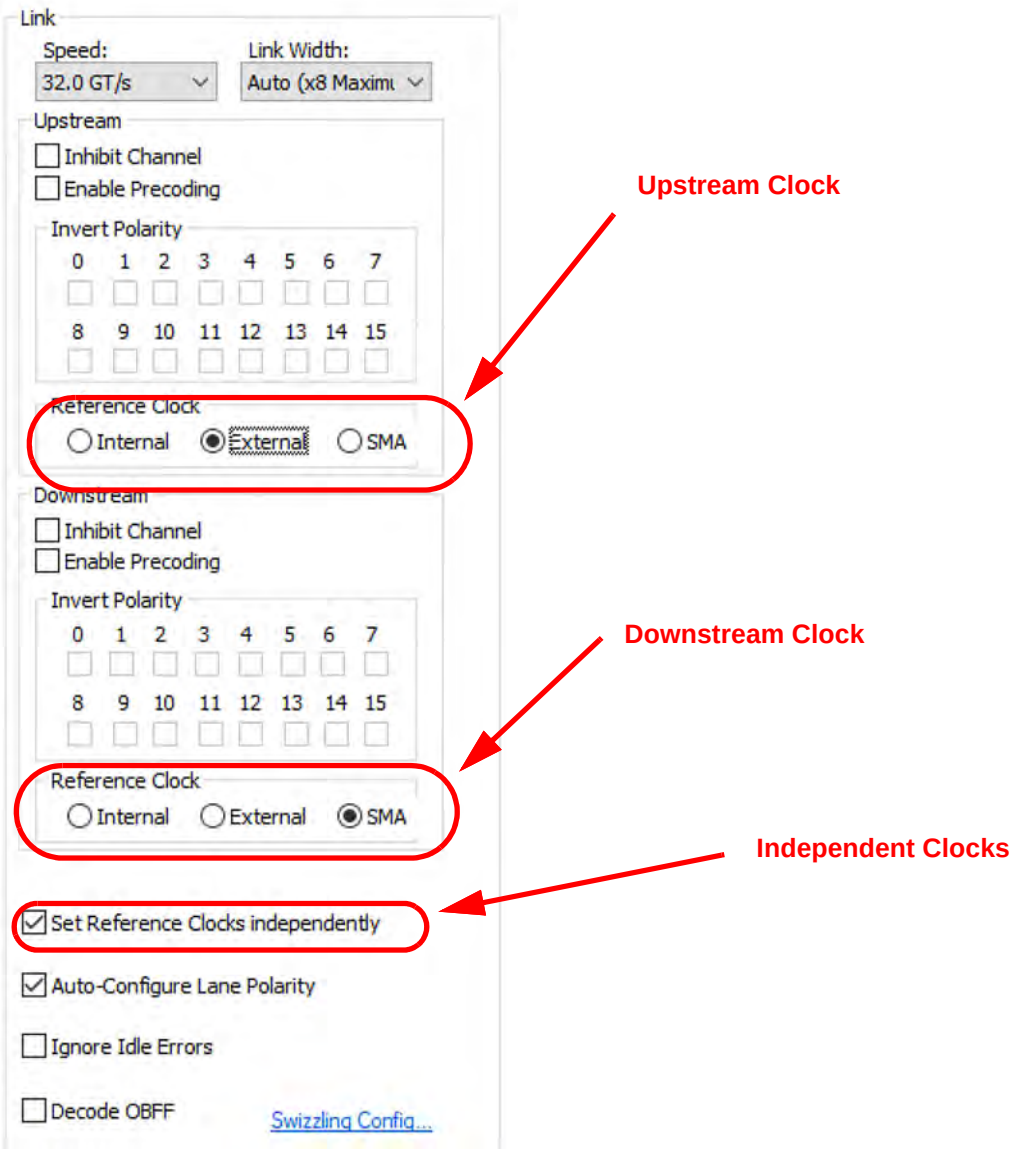


Figure 7.26: Independent Reference Clocks: Upstream vs. Downstream

7.15.6 Auto-Configure Lane Polarity

Lets the Analyzer determine lane polarity (see Figure 7.1 on page 335: 3F) for the Summit M5x). Auto functions such as Auto Configure polarity rely on Gen1 or Gen2 training sequences to properly discover their values. If the speed option is set to fixed Gen3, the analyzer will never see these sequences and the polarity discovery will not be reported properly in the dashboard dialog.

7.15.7 Ignore Idle Errors

When set, the analyzer will not store errors in between packets into memory. This option helps to preserve analyzer memory to store more packets in cases where memory efficiency is critical. This option filters out Compliance Pattern as well. See Figure 7.1 on page 335: 3G for the Summit M5x.

7.15.8 Swizzling Config...

The Swizzling Config dialog allows you to reconfigure the logical order of the lanes in a link separately for Upstream and Downstream PCIe directions. You can perform the logical to physical assignment manually or let the analyzer detect this on its own (Auto-Configure Lane Swizzle option checked). See Figure 7.1 on page 335: 3H for the Summit M5x.

Note: Autoswizzle works only when the analyzer sees the LTSSM Configuration state link training sequence.

7.15.8.1 Manual Configure Lane Swizzle

If you know how your physical link is connected and the lane numbers advertised for each lane, then you can use the manual swizzle option (Auto-Configure Lane Swizzle option unchecked). On the Swizzling Configuration dialog, drag the number of the logical lane (in blue) to the desired lane physical position.

In the case shown below the Link Width is set to Auto (x8 Maximum) for the Summit M5x Gen5, so all 8 lanes are available to be manually configured. See Figure 7.27 on page 365 for the Summit M5x.

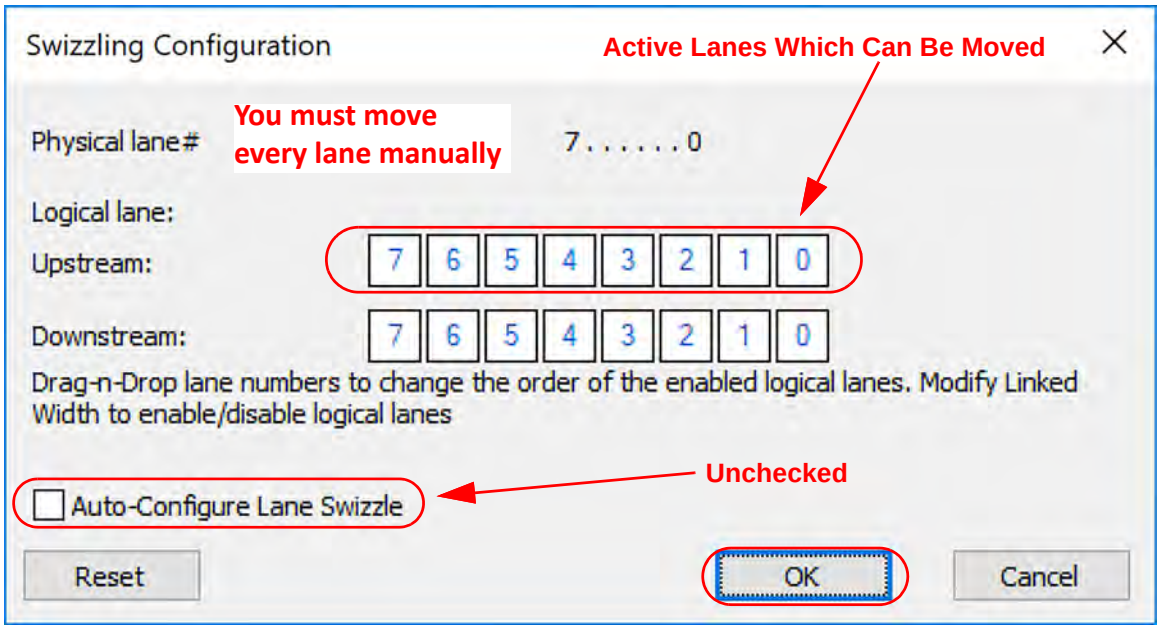


Figure 7.27: Manual Swizzle: Link Width Set to Auto (x8)

In the example shown below, we re-assigned the Upstream Physical lanes as follows:

- Lane 7 to Lane 0
- Lane 6 to Lane 1
- Lane 5 to Lane 2
- Lane 4 to Lane 3
- Lane 3 to Lane 4
- Lane 2 to Lane 5
- Lane 1 to Lane 6
- Lane 0 to Lane 7

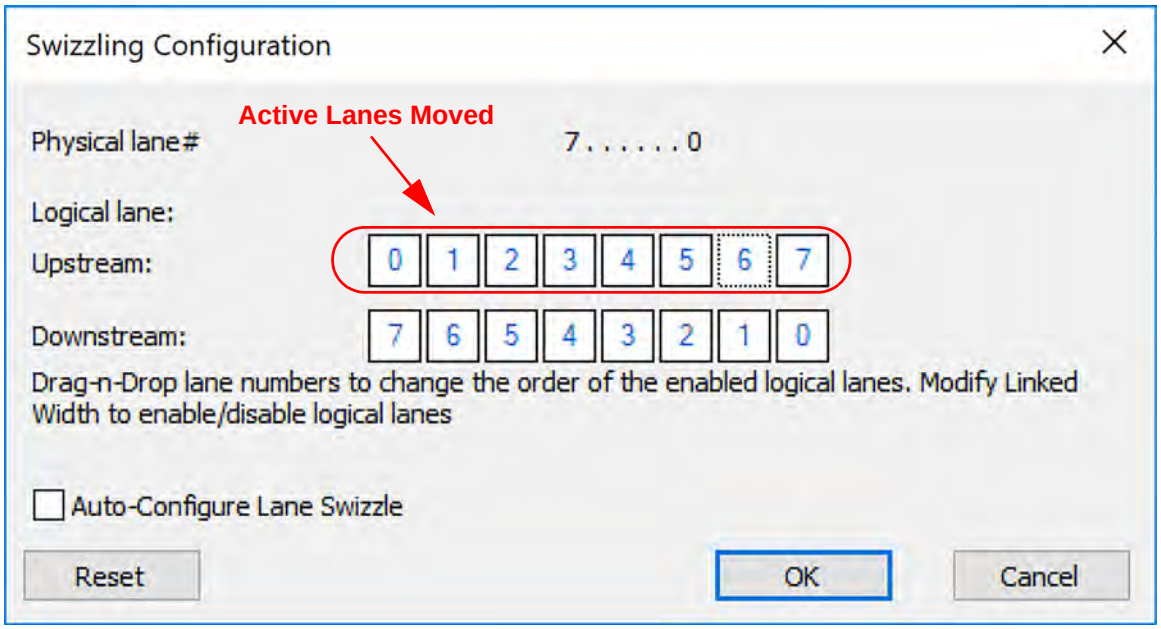


Figure 7.28: Manual Swizzle Configuration

Note: The simplest way to make new lane assignments is to always move the highest source lane number to the highest destination lane number.

If the source lane has a lower number than the lane it is replacing, then the software performs a right shift to the higher numbered replaced lane. If the source lane has a higher number than the lane it is replacing the software performs a left shift to the lower numbered replaced lane.

7.15.8.2 Example: Move Highest Source Lane First

In the example below we replaced Lane 7 with Lane 3 and Lanes 7 through 4 were shifted to the right. Then Lane 7 was replaced with Lane 2 and Lanes 7 through 4 were shifted to the right. Then Lane 7 was replaced with Lane 1 and Lanes 7 through 4 were shifted to the right. Finally Lane 7 was replaced with Lane 0 and Lanes 7 through 4 were shifted to the right.

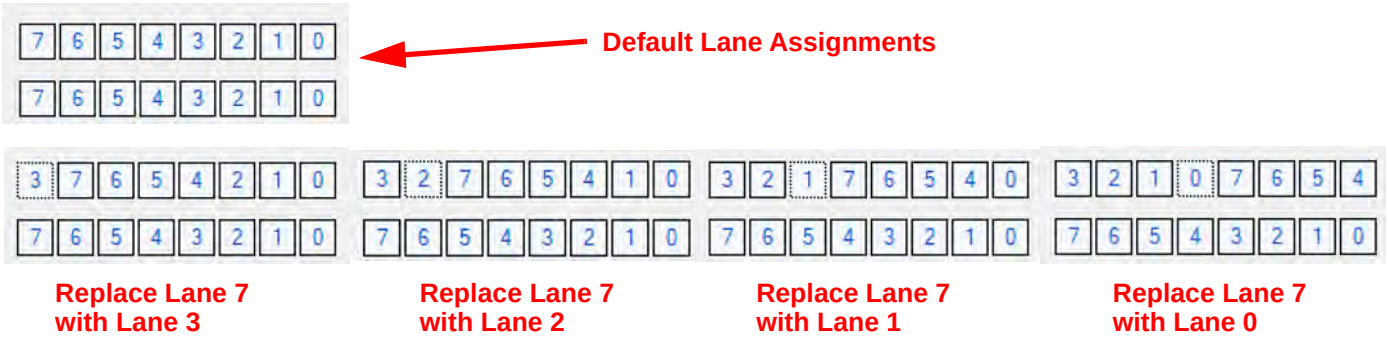


Figure 7.29: Manually Moving Lane Assignments: Highest Numbered Lane First

7.15.8.3 Example: Move Lowest Source Lane First

If you start with the lowest numbered lane you will get completely different results.

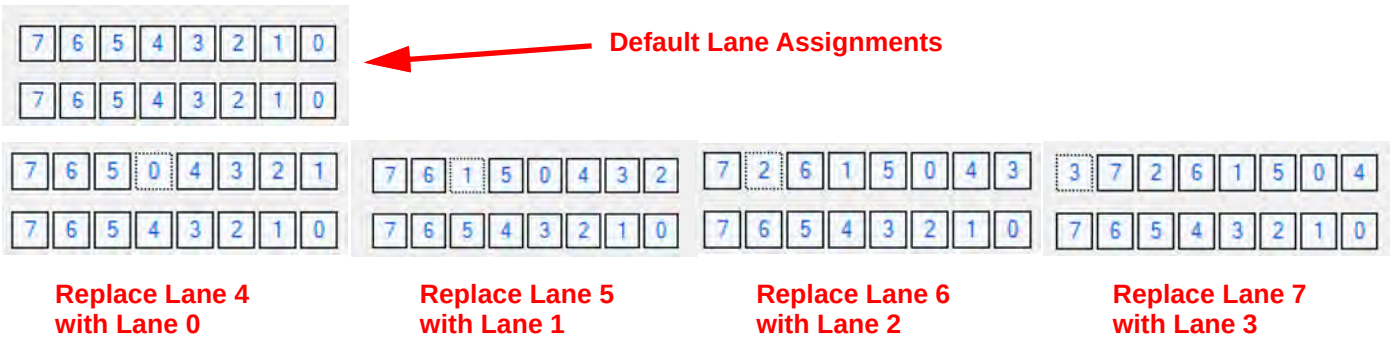


Figure 7.30: Manually Moving Lane Assignments: Lowest Numbered Lane First

7.15.8.4 Working with Less Than Eight Lanes

If the lane number in the box is not in blue this means that the lane is not participating in the link from the Summit analyzer's point of view. This may happen because the Link Width selected is less than x8. See Figure 7.31.

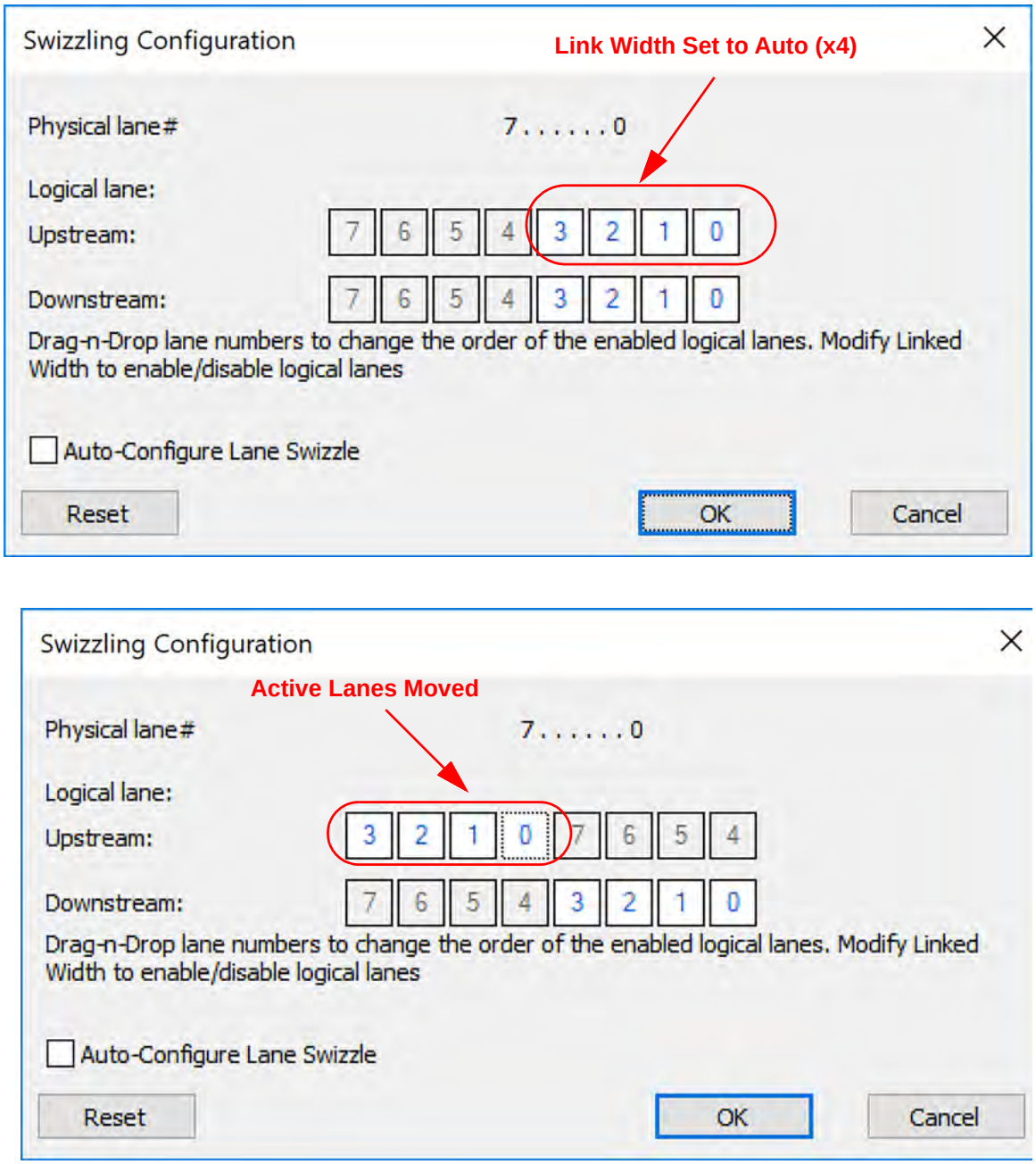


Figure 7.31: Manual Lane Swizzle Configuration: Moving Four Lanes

Note: In the example above Lane 0 through Lane 3 are the only active lanes. They can be moved to any lane that the analyzer supports. The analyzer in this case is the Summit M5x, which can support 8 lanes.

7.15.8.5 Auto-Configure Lane Swizzle

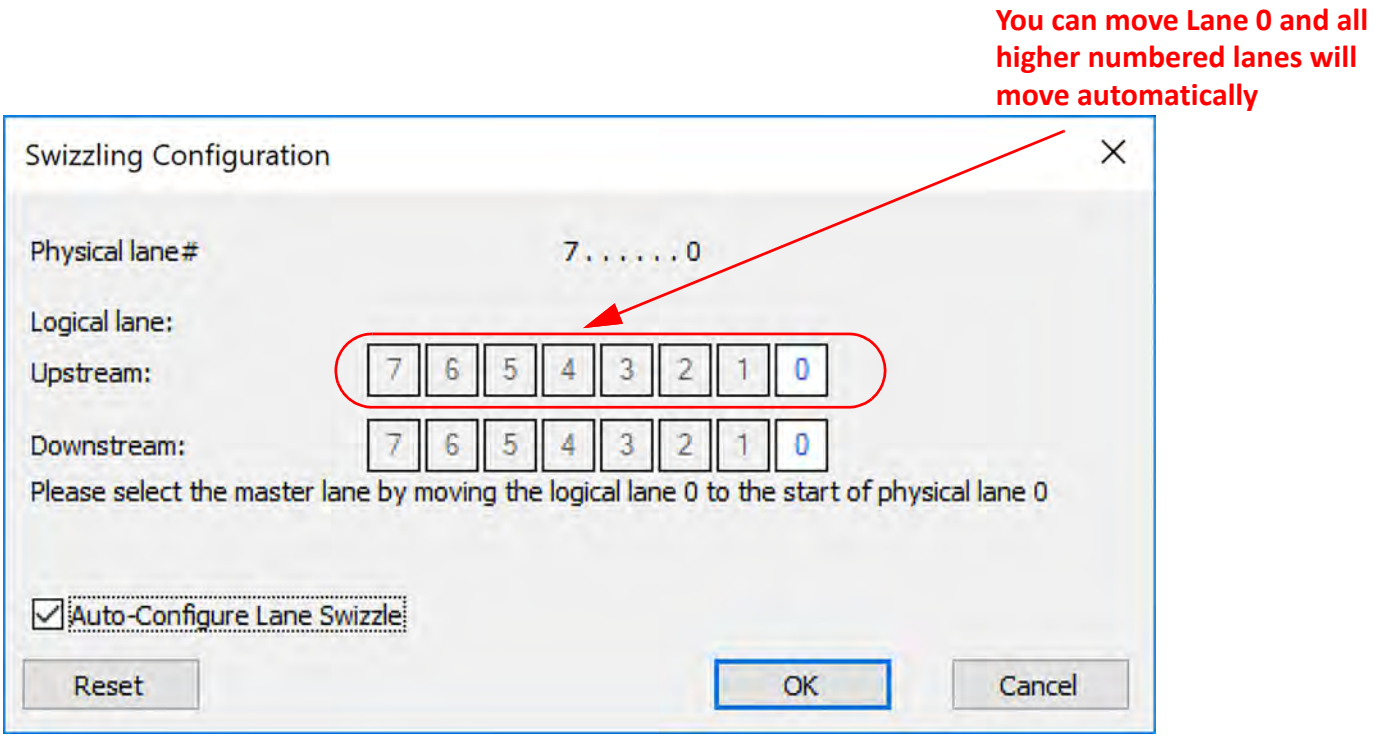


Figure 7.32: Swizzling Config Dialog

When the Auto-Configure Lane Swizzle option is checked the Summit Analyzer requires you to provide the physical location for at least one lane with active traffic. You can specify this by moving the enabled lane L0 to the physical location where either lane 0 is or any other active lane for the link. See Figure 7.33 on page 370.

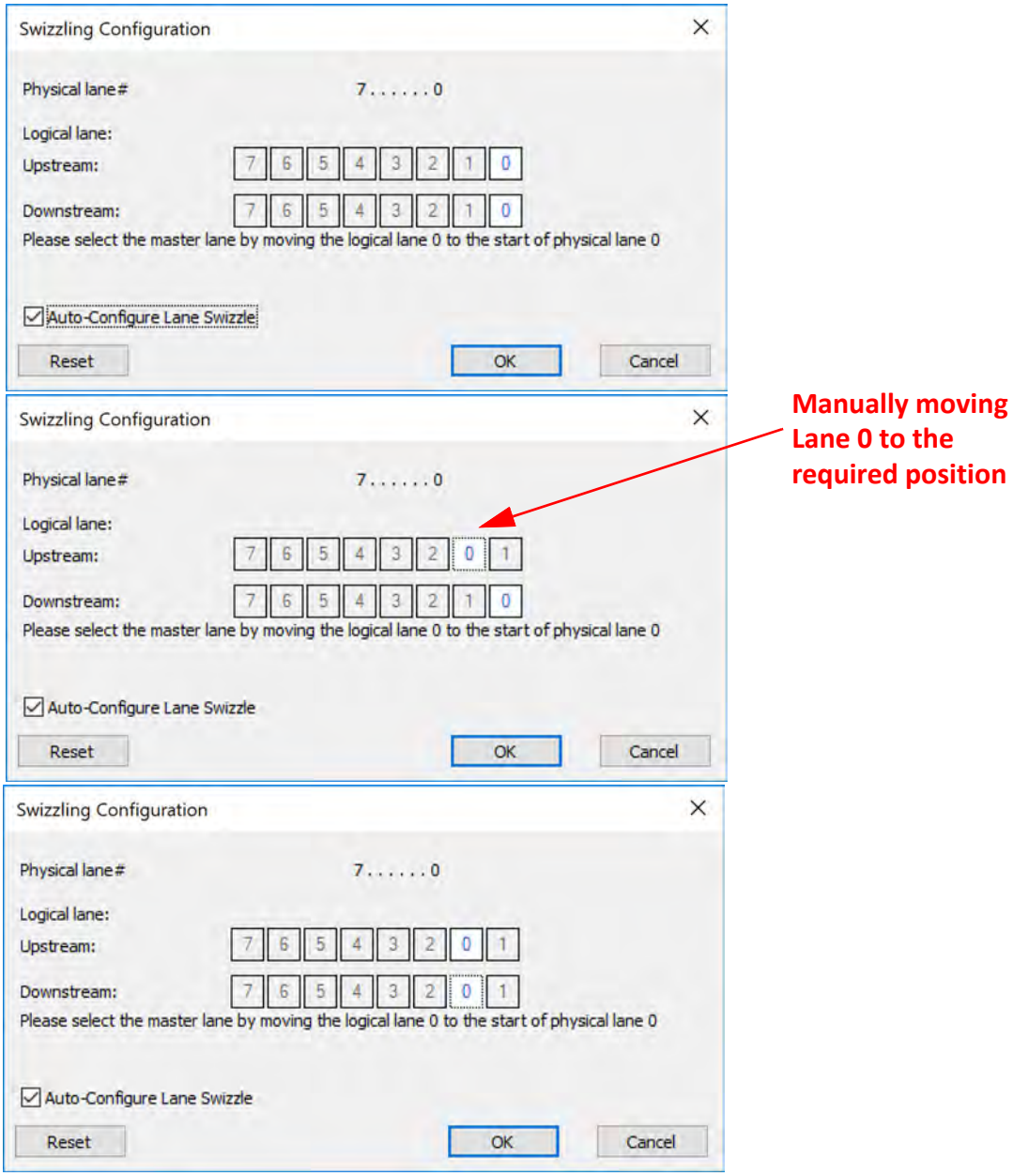


Figure 7.33: Manually Configuring Lane 0 when Auto-Configure Lane Swizzle is Checked

Note: Auto-Configure Lane Swizzle will not work properly if the link is bifurcating. Use manual swizzle instead.

7.15.9 Decode Optimized Buffer Flush/Fill (OBFF)

Select this checkbox to decode Optimized Buffer Flush/Fill (OBFF) events. See Figure 7.1 on page 335: 3I). As a system operates, each of its devices does not know the power state of each of the resources in the system. Without coordination, each of the devices will go in and out of their low-power states as necessary to execute the tasks they are assigned to do. This "asynchronous" behavior prevents the optimal power management of the CPU, host memory sub-system and other devices, because the intermittent traffic keeps the system permanently awake and unable to optimize power management across the system.

As part of an implementation of a system-level power strategy, the idle time and low-power states of the devices must be optimized to enable them to stay in their low-power states longer. Basically, a host can provide information to all devices by broadcasting a message about the system power state. The devices can utilize this information to group a load of requests, wait until the system wakes up, and burst out all of the requests at the same time. By doing this, the device does not wake up a sleeping CPU and/or the system memory sub-system. Waiting creates extended periods of system inactivity which saves overall system power. The host utilizes the OBFF to give devices a "hint" so they can optimize their behavior, which improves power management at the system level.

7.15.10 Disable Descrambling

If checked, causes the Analyzer to assume that none of the PCI Express traffic is scrambled. By default, the Analyzer determines the scrambling state of the devices under test (see Figure 7.2 on page 336: 3J).

Note: When selecting Gen3 speed the disable scrambling option is not available. This option can be used only for Gen1 or Gen2 speeds. It will show as well for Auto speed but it affects only Gen1 or Gen2 traffic.

7.15.11 Ignore EDS

Lets the Analyzer ignore End of Stream (EDS) token. See Figure 7.2 on page 336: (3K).

7.16 General guidelines to do the Calibration and AutoTuning

Following are some general guide lines to help stream line this process.

1. First make sure that the device is getting link up with underlying host, if needed set the BIOS parameters.
2. The device should be visible to the host OS, in order to do the auto-tuning and calibration, if it is not present, please try the presets manually and reboot the Host OS, check again, if device is getting detected then the auto-tuning / calibration routine can work on it. Note: it is not necessary to have the stable or clean link, just a link, may be a Gen1 x1 is good enough to start the calibration / tuning process. The process will bring the device to the max level possible in terms of Speed and Linkwidth.

3. Once the device is detected by Host OS, first start the Host to DUT path auto-tuning. (“Interposer Host to DUT Path” on page 373).
4. Once that is done, then start the Interposer to Analyzer Path autotuning (“Interposer to Analyzer Path” on page 407).
5. In the end if there are still errors, then try to do Analyzer Calibration (“Analyzer Calibration” on page 410).
6. Another approach to Auto Tuning and Probe Calibration is to use the Auto Tune and Probe Calibration wizard, which automates the process for you (“Using the Autotune and Probe Calibration Wizard” on page 414).

7.16.1 Interposer Host to DUT Path

This dialog box allows you to Autotune the Interposer Host to DUT path settings.

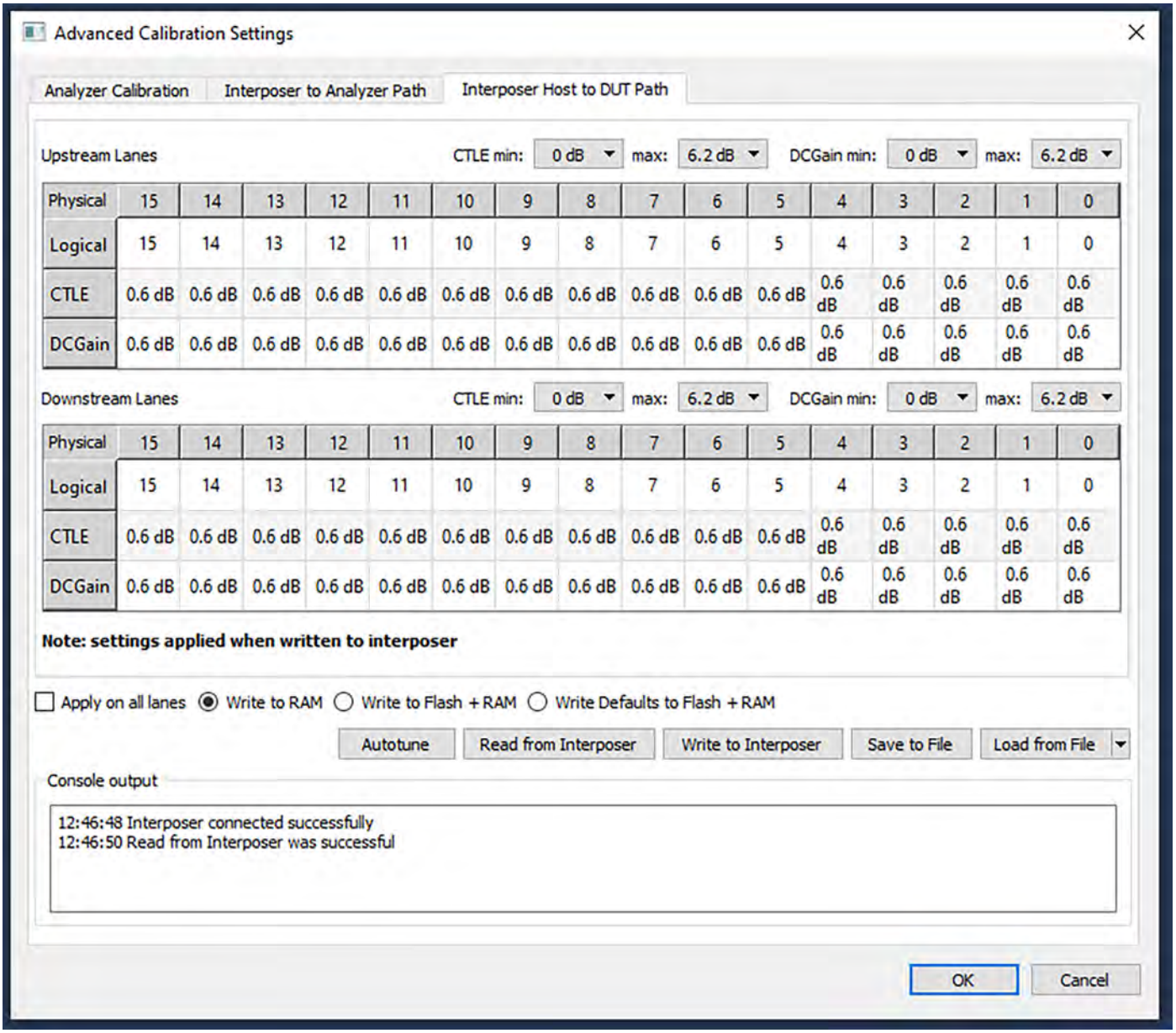


Figure 7.34: Interposer Host to DUT Path

7.16.1.1 Interposer Host to DUT CTLE and DCGain Settings

Combo-boxes are provided above the Upstream and Downstream lanes allowing you to specify CTLE and DCGain minimum and maximum value ranges.

If no custom ranges were saved in the RAM of the interposer, the system displays the full range that the current model supports.

To set a custom range, select the values from the CTLE and DCGain drop down menus, as shown in Figure 7.35.

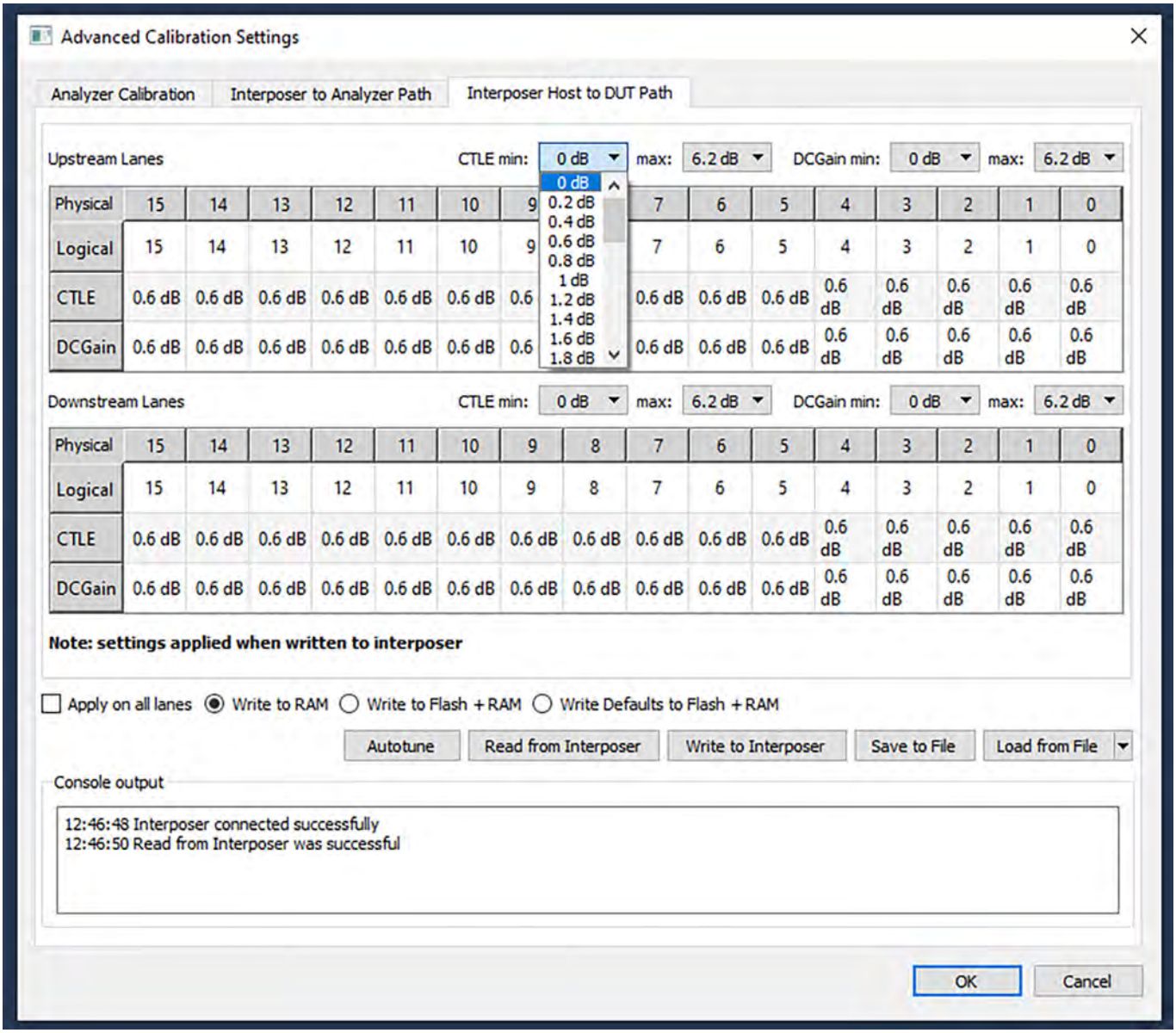


Figure 7.35: Advanced Calibration Settings: Selecting CTLE Range

You can only select numbers within the range available in the lane table. Selecting a the minimum or maximum range outside of the specified ranges causes the lanes to turn red (Figure 7.36).

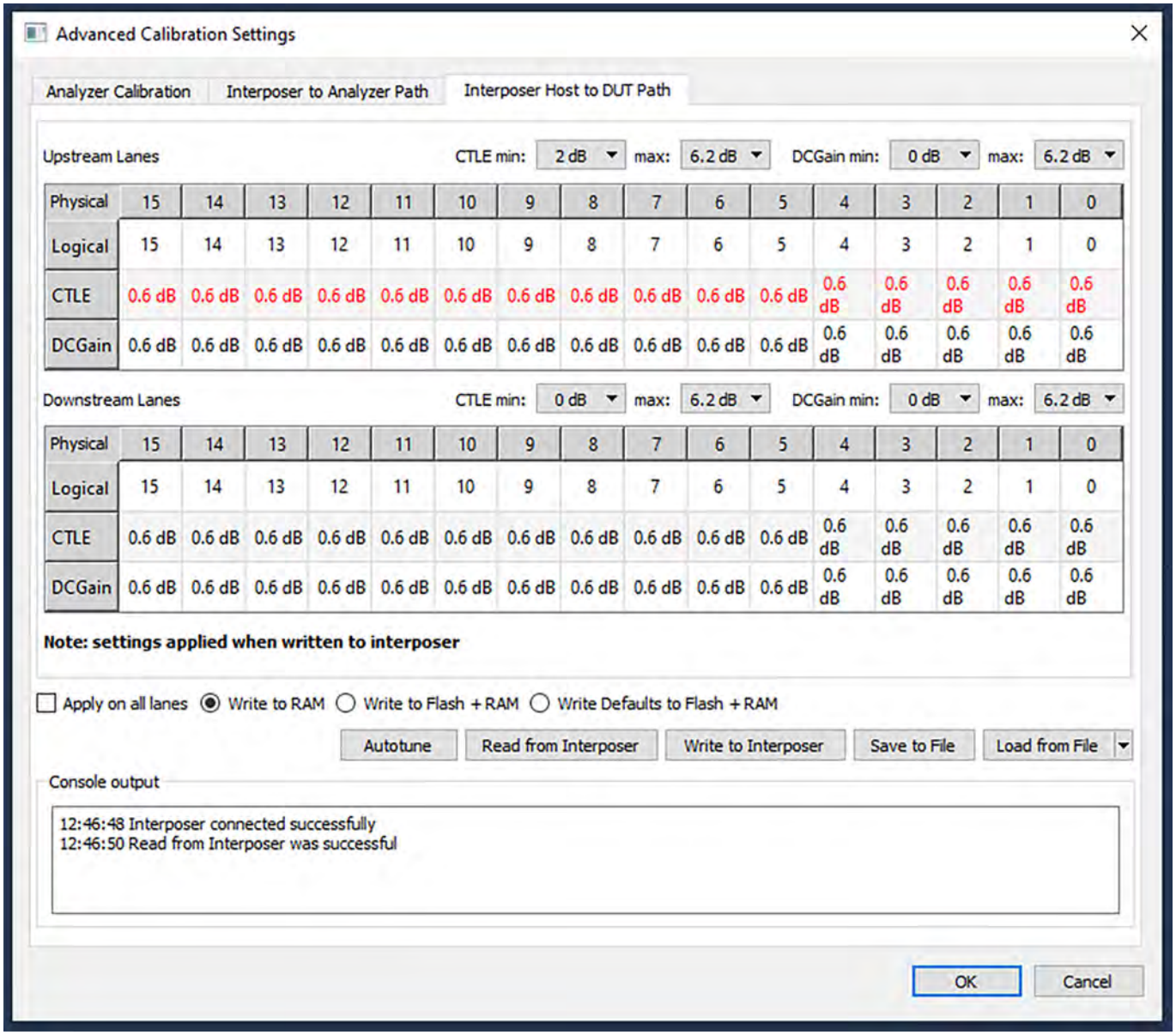


Figure 7.36: Advanced Calibration Settings: CTLE Outside of Range

A warning also displays, as shown in Figure 7.37.

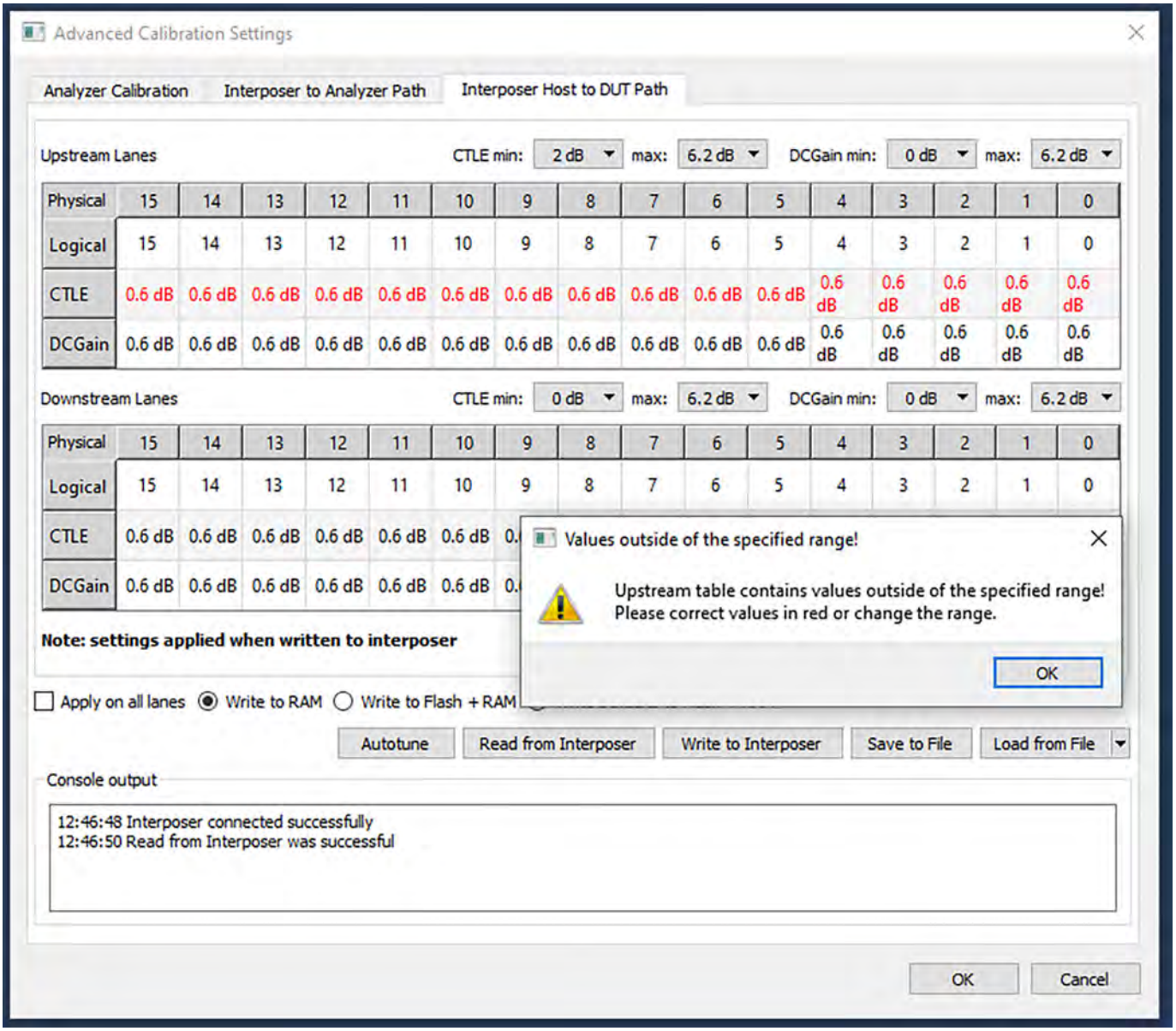


Figure 7.37: Advanced Calibration Settings: Values Outside Specified Range

You must fix the values before you can **Save to File**, **Write to Interposer**, **Read from Interposer**, or start the **Autotune** process.

To fix all the red values in the row to the minimum specified value within the range:

1. First, click the column of the values that need to change.
2. Change the values. Use the <tab> button to navigate between values.

Once the values are in range, you can select **Write to Interposer** or **Read from Interposer**. Clicking **Write to interposer** or **Read from Interposer** also writes /reads the

selected ranges to the RAM / Flash.

Note: When selecting **Write to Interposer**, the selected Ranges will be reset to those supported by the current interposer.

7.16.1.2 Interposer Host to DUT Autotune

The goal of DUT auto-tuning is to get the device to the target link speed and width with minimal error rate, by adjusting CTLE and DCGain values. Target link speed and width can be selected in the dialog before starting the auto-tuning.

The auto-tuning routine automatically sets and writes to the interposer CTLE and DCGain values, measures error rate and if necessary resets the DUT or reboots the host.

Typical Setup

Typical setup for this feature consists of two PCs as described below:

- Target Host PC where the interposer is connected
- Client PC running the PCIe Protocol Analysis software application which can perform the following tasks:
  - adjust analyzer settings
  - adjust interposer settings
  - perform recording/analysis of a captured trace
  - manage the Target Host PC via client software:
    - queries list of installed hardware
    - queries of the DUT/Root complex settings
    - OS reboot

The Target Host PC may be managed either through Windows or Linux OS (Operating System). Depending on the host OS there are two possible solutions.

- SSH (Secure Shell -> Linux OS)
- SSL (Secure Sockets Layer -> Windows OS)
- SSH (TDY Provided -> Linux OS)

The choice of SSH vs. SSL depends on which method is easier for setting up the Target Host PC.

Notes on SSH and SSL

SSH (Secure Shell) uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary. There are several ways to use SSH; one is to use automatically generated public-private key pairs to simply encrypt a network connection, and then use password authentication to log on. Another is to use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password. In this scenario, anyone can produce a matching pair of different keys (public and private). The public key is placed on all computers that must allow access to the owner of the matching private key (the owner keeps the private key secret). While authentication is based on the private key, the key itself is never transferred through the network during authentication. SSH only verifies whether the same person offering the public key also owns the matching private key. In all versions of SSH it is important to verify unknown public keys, i.e. associate the public keys with identities, before accepting them as valid. Accepting an attacker's public key without validation will authorize an unauthorized attacker as a valid user.

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data

passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.
The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) - a data file also containing your details. You should then submit the CSR. During the SSL Certificate application process, the Certification Authority will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL. Your web server will match your issued SSL Certificate to your Private Key. Your web server will then be able to establish an encrypted link between the website and your customer's web browser.

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals.
Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

Access to Configuration Space

The Target Host PC with installed Interposer, the DUT and the client software (Auto-tuning process) **REQUIRES** access to device configuration space, which is achieved by using a software program that runs on the Target Host PC:

- InterposerAutotuningAgent.exe if the Target Host PC OS is Windows.
- Bash scripts, if the Target Host PC OS is Linux.

7.16.1.3 Using Z516 or Z58 as a DUT

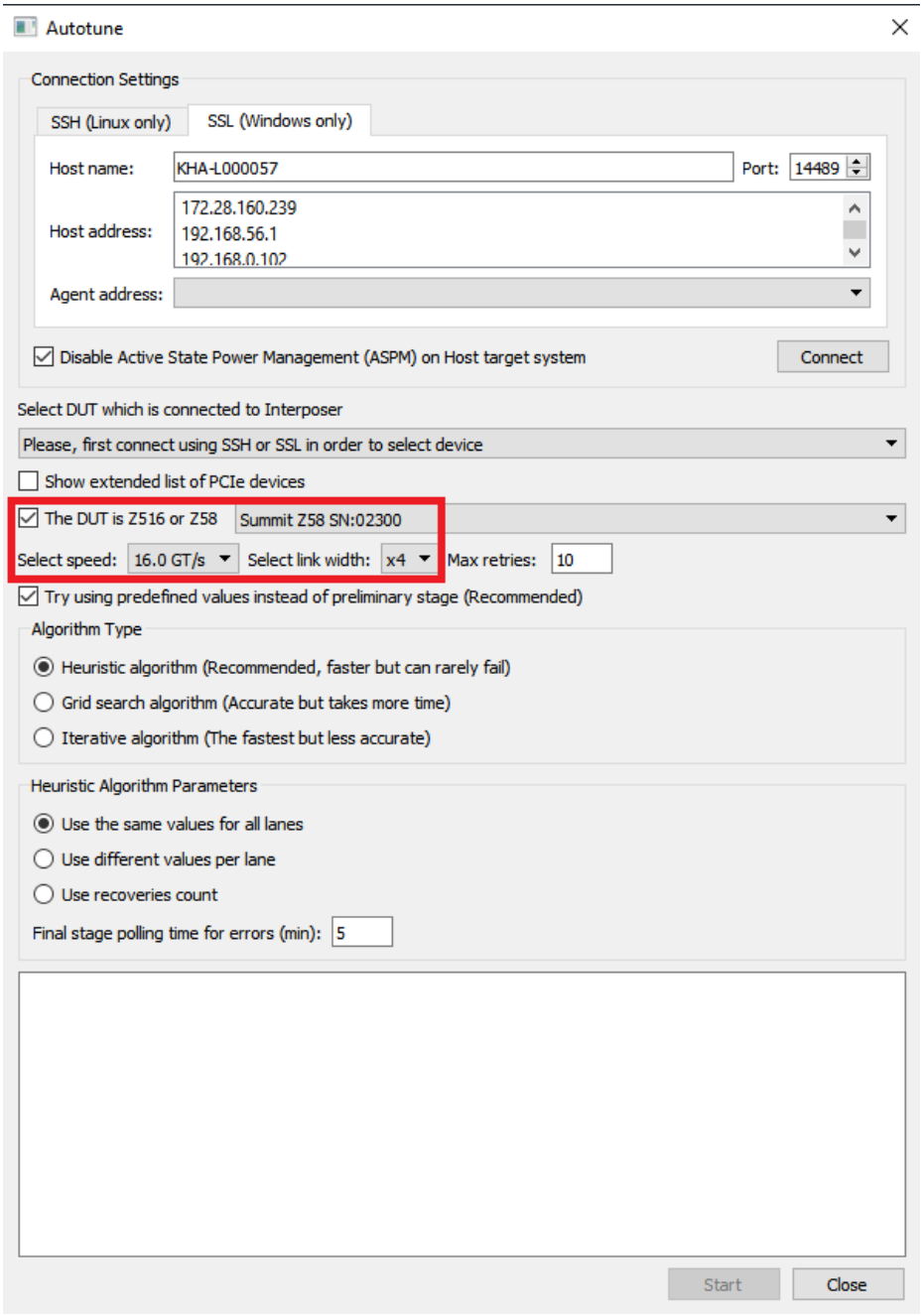


Figure 7.38: The DUT is Z516 or Z58 option

If the DUT is Z516 or Z58 exerciser, then **The DUT is Z516 or Z58** must be selected and the connected host device must be chosen from the list. See Figure 7.38.

If this option is enabled, then during the auto-tuning:

- Link state (current link width and link speed) is read from the register in the configuration space of the port of the selected DUT instead of the configuration space of the DUT.

- Connect macros is executed for the chosen Exerciser instead of performing software link reset.

7.16.1.4 Auto-tuning Algorithms

The Autotune dialog allows selecting one of several algorithms. The selected algorithm determines the steps that are performed during the process to find optimal CTLE and DCGain settings.

For most algorithms the auto-tuning routine uses the number of correctable and non-fatal errors read from the device and port as a link quality metric (the read values are reported in the log after each measurement). Consult the PCI Express® Base Specification for the definition of correctable and non-fatal errors. Since this error number is a link-

wide metric, all algorithms except Predictive with enabled **Use different values per lane** option use equal values of CTLE and DCGain for all lanes.

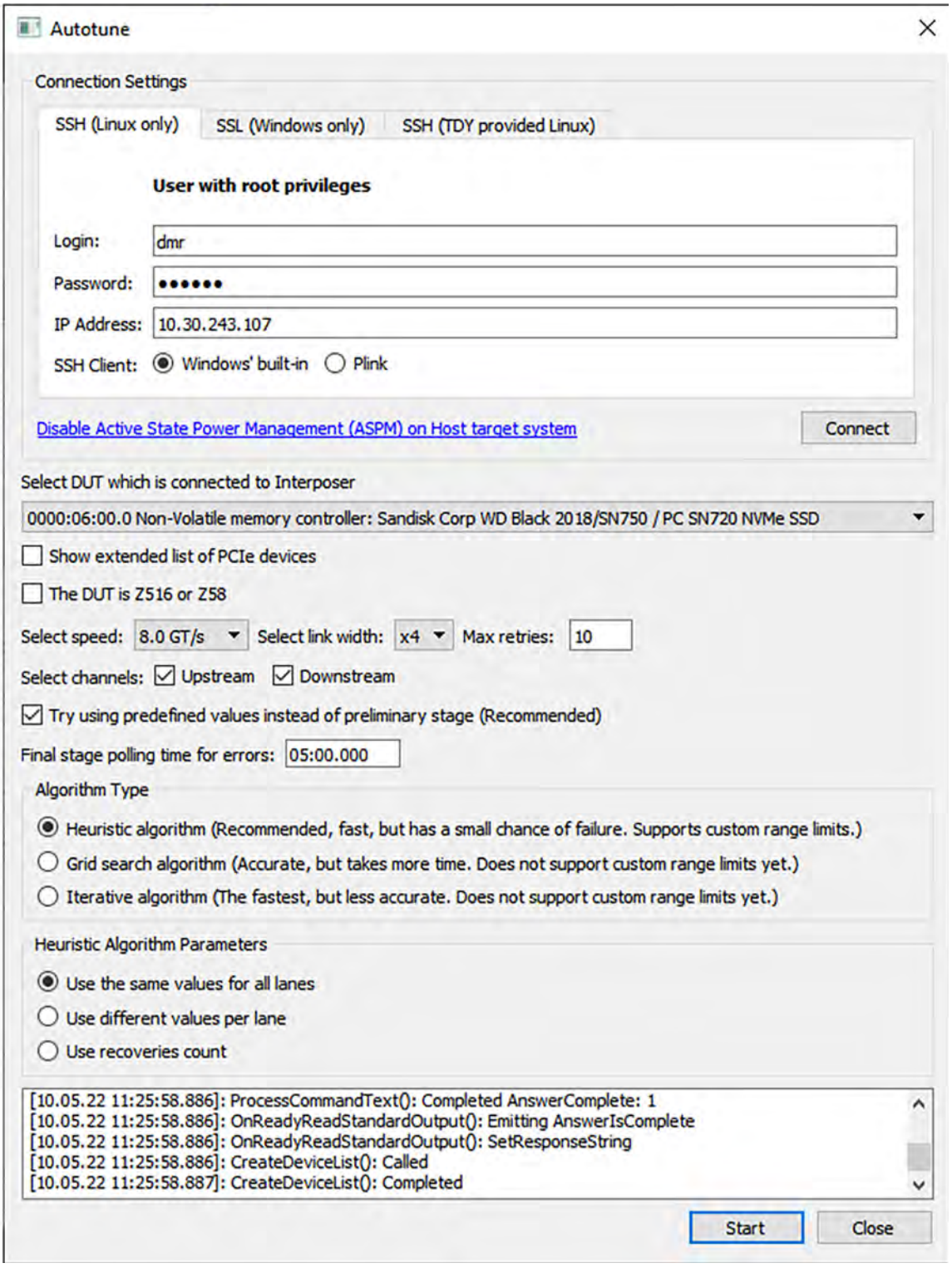


Figure 7.39: Auto-Tune: Algorithm Selection Options

Below is the list of the available algorithms with their descriptions:

Hueristic algorithm

If this option is selected, then a heuristic search method is used. It utilizes information from the previous measurements to determine the direction in which settings with lower number of errors may be.

Auto-tuning is performed separately for upstream and downstream. For each direction there are several stages. Each subsequent stage has a larger error polling interval. The advance to the next stage occurs when zero error rate is archived on the current stage. The found settings are used as the starting point for the algorithm in the next stage. If the routine cannot find settings with a zero error rate, then the auto-tuning stops.

First the routine performs an exhaustive search with large steps (which is described below) with duration stage time 500 millisecond. As a result, it saves some best points (by error rates) to start next algorithm from them.

The durations of all stages but the last are predefined. The first stage is 500 milliseconds. Then error polling time gradually increases: 2, 5, 10, 20, 40 seconds and 1, 2, 5, 10, 20, 30 minutes. For the final stage the errors polling time may be configured using **Final stage polling time for errors (min)** option in the Autotune dialog. It may be from 1 to 60 minutes. Note that if, for example, 5 minutes is specified, then the stages with longer error polling time (10, 20 and 30 minutes stages) are not performed.

Note that this algorithm starts from the CTLE and DCGain produced by first Grid search run. In case algorithm fails to find good values from first point then procedure starts again (without additional Grid search run) selecting next point until good values are found or all saved points are tested.

This algorithm also supports custom range limits. The only values within the appropriate range will be tested by the algorithm and during the checking for presets.

Note: For custom ranges to apply, the "Try using predefined Values …" option must be selected. Otherwise, the algorithm ignores the custom range.

In addition, after any write to interposer in scope of this algorithm DUT is reset to adopt to new line characteristics

Also for this algorithm it is possible to configure how errors are measured. The following options are available in **Predictive Algorithm Parameters** in the Autotune dialog:

- **Use the same values for all lanes**
  The same values for parameters (CTLE and DCGain) are set for all lanes on one channel. The number of correctable and non-fatal errors read from the device and port will be used to determine the link quality.
- **Use different values per lane**
  Parameters for each lane are tuned separately. In this case to determine number of errors on each lane an analyzer is used.
- **Use recoveries count**
  The same values for parameters are set for all lanes on one channel. The number of recoveries counted on the analyzer are used to determine the link quality. This number is applied for entire link so the same values should be used for each lane.

This is the main algorithm which often produces accurate results and does not take as much time as Grid search.

Grid search algorithm

If this option is selected, then the auto-tuning routine performs an exhaustive search through the predefined subset of settings for both channels at the same time.

There are three stages. During the first stage the routine uses large steps to find spots with settings, with which the device is able to work at the target link width and speed (as specified in the Autotune dialog). Then the same process but with smaller steps is repeated in the found spots. Then on the final stage each value inside the found on the second stage good spots is checked to find zero error rate.

Note that since a lot of different combinations of CTLE and DCGain values are checked, this algorithm may take more time to complete than other algorithms but is more accurate because more values are tested.

Iterative Algorithm

In this algorithm, there are several calibration stages where the auto-tuning routine tries adjacent value combinations to minimize error rate. It is done separately for upstream and downstream.

For the first stage the step is 0.6 dB, and for all subsequent stages the step is 0.2 dB. Each stage beginning from the second stage uses a larger error-collection interval, which allows the algorithm to detect less frequent errors but also slows the tuning process. If at any stage except the first stage (that is, every stage with minimal steps) the algorithm cannot achieve zero error rates for its interval, tuning stops.

During this process DUT reset is done (without rebooting host), after that, error rate is re-checked, and the tuning stage is repeated if needed. This algorithm is the fastest of all but may not produce accurate results.

Note: The Autotune dialog allows selecting the target speed and width of the link. If the current speed or link width reported by the DUT does not match the target values and the selected Algorithm Type is Predictive algorithm or Coordinate descent, then an additional step is performed before starting the selected algorithm. On this step the software routine is trying to walk with large steps through the CTLE/DCGain space to find spots where the link is good enough for the device to switch to the target speed and link width. If the link width is less than required, then the host is rebooted. If the speed is less than required, then the DUT reset is performed without reboot. The software routine is careful not to disrupt the link so much that the device becomes unavailable, making a host reboot needed, but it can happen sometimes. At this stage, the software routine is checking very few CTLE/DCGain combinations in predefined patterns. The error rate is not checked on this stage.

Host PC is running Window OS

Prerequisites

1. On the client PC (where PCIe Software Suite is installed) go to the folder "C:\Program Files\LeCroy\PCIe Protocol Suite\" and copy InterposerAutotuningAgentLauncher.exe to the removable media.
2. Run PCIe Protocol Analysis software. Go to 'Recording Options' -> Interposer 'Auto-Tuning' tab. Push 'Auto-Tune button'. Open 'SSL (Windows only)' tab. Write down the values of 'Host address'/'Port' fields (see Figure 7.40 on page 385).

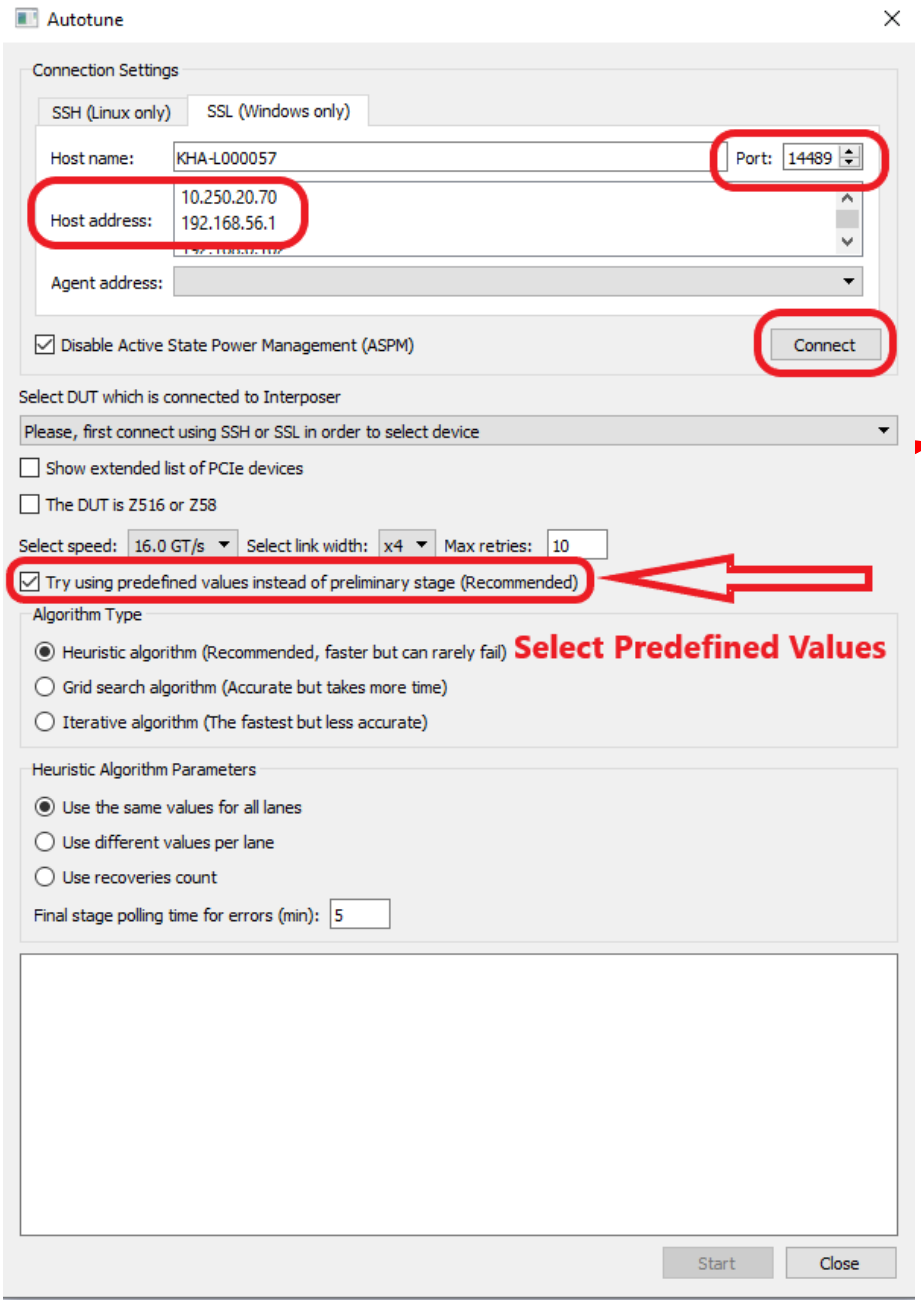


Figure 7.40: Auto-Tune: Select Predefined Values

If you select the Predefined Values for Auto-Tune and return to the Host to DUT Settings dialog box, click on the Load from File tab (see Figure 7.41 on page 386) and you'll see a list of devices (see Figure 7.42 on page 387).

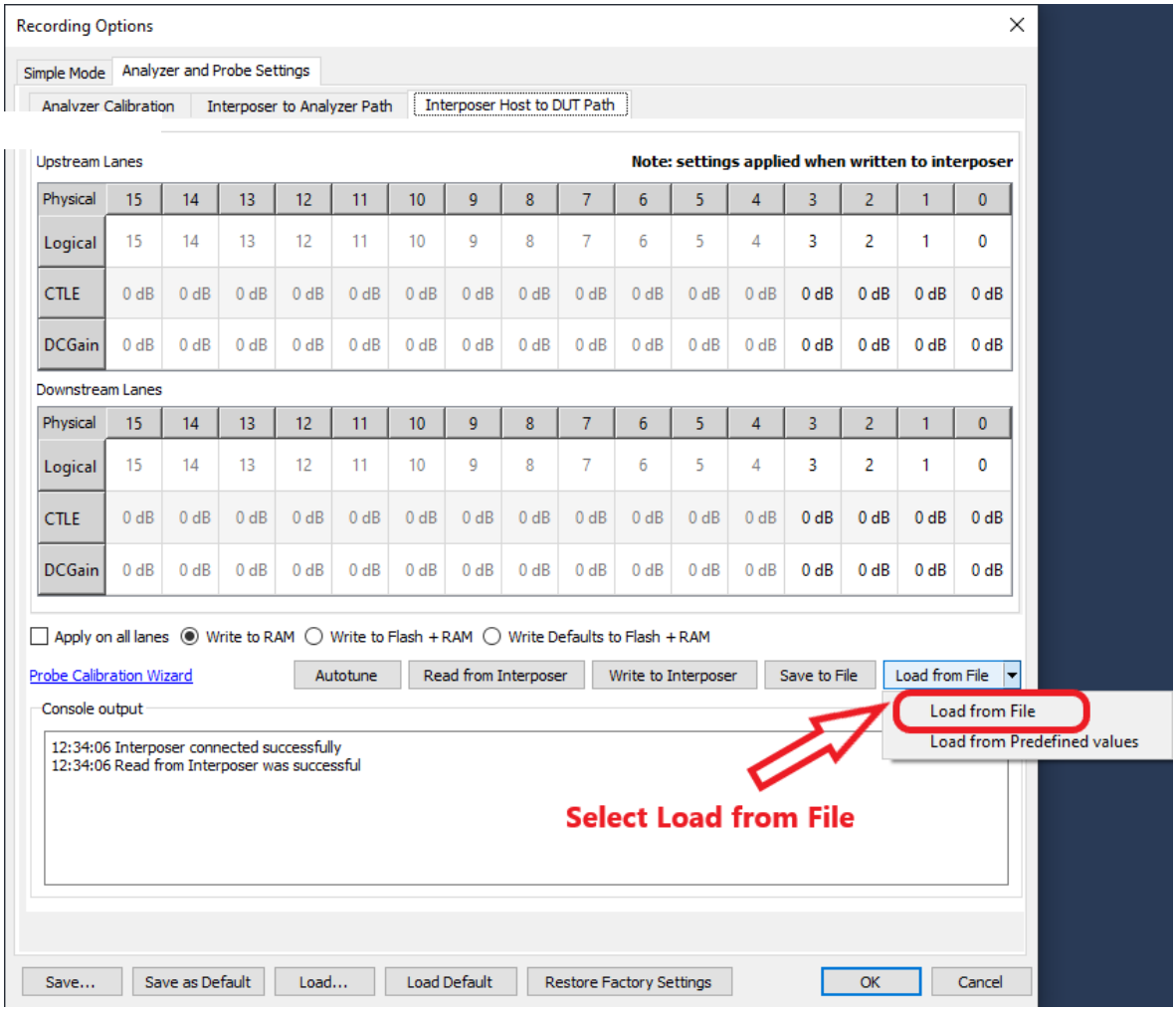


Figure 7.41: Host To DUT Settings: Load From File

If you select Load from File a List of DUT Settings will pop up. See Figure 7.42 on page 387.

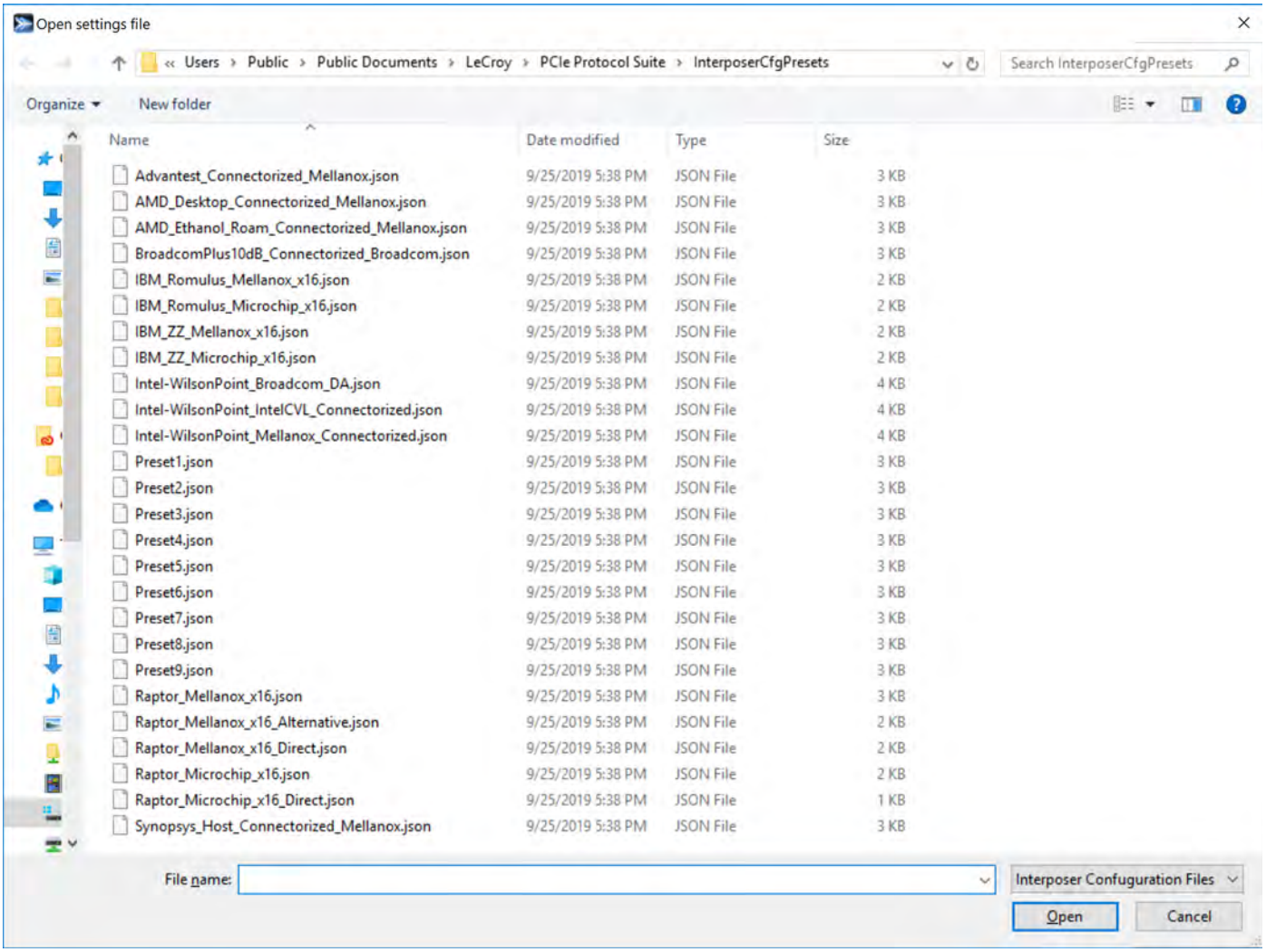


Figure 7.42: Load from File: List of Files to choose from

Another way to view the Predefined Values is to select Load from Predefined Values tab and the Choose Predefined values dialog box will pop up. See Figure 7.43 on page 388.

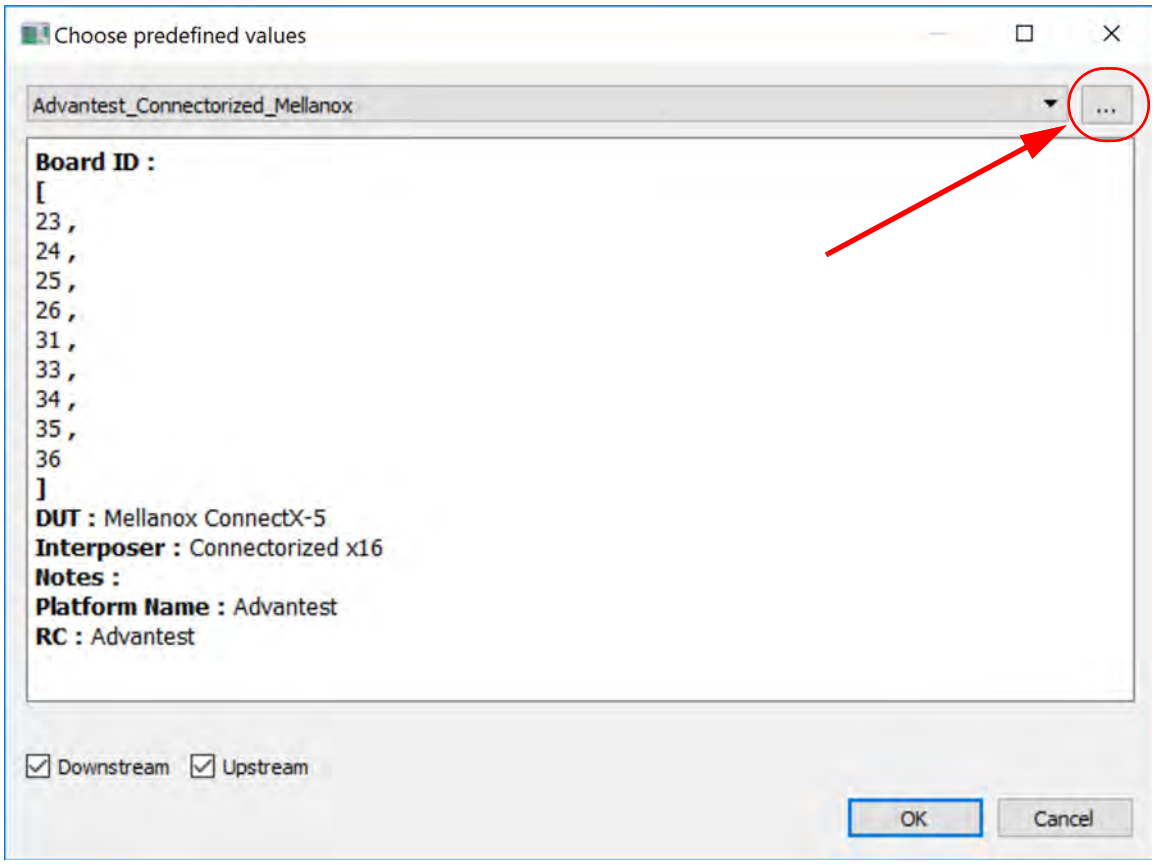


Figure 7.43: Chose predefined values

If you select the ... tab you'll see a list of all the predefined DUT Settings. See Figure 7.44 on page 389.

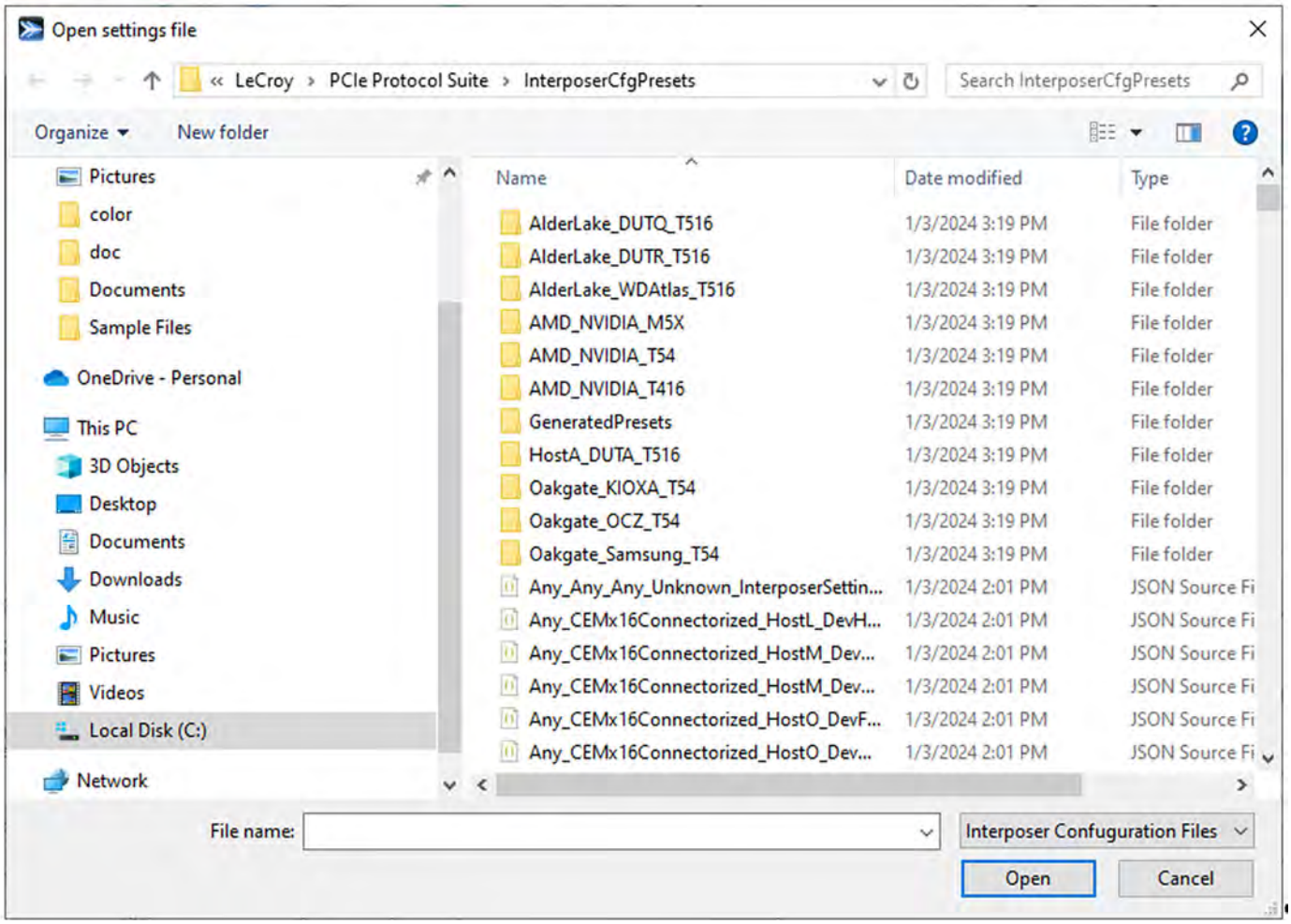


Figure 7.44: Set of Predefined DUT Settings

Another way to select a set of Predefined Values is to select the small black down pointing arrow and the list of predefined DUTs will appear. See Figure 7.45.

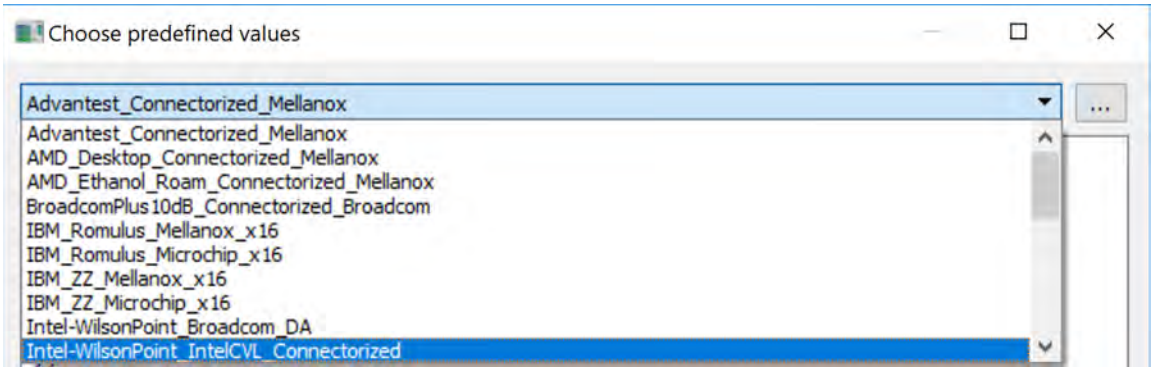


Figure 7.45: Choose predefined Values: Arrow

After you select a device (in this case the Intel-WilsonPoint_IntelCVL_Connectorized) the data for that device will pop up in the Choose predefined values dialog box. See Figure 7.46.

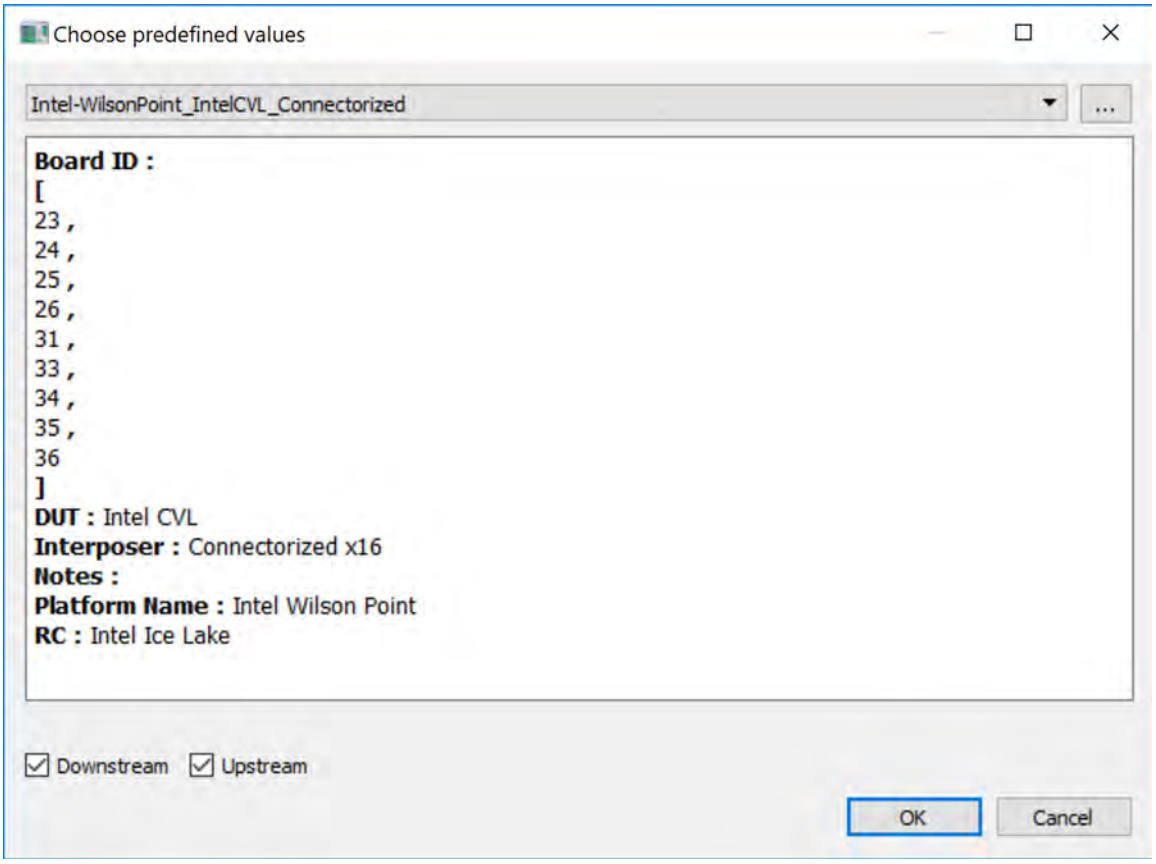


Figure 7.46: Choose predefined values: Intel-WilsonPoint...

InterposerAutotuningAgent installation on target host

1. Copy **InterposerAutotuningAgentLauncher.exe** to the target host PC.
2. Run **cmd.exe** with administrative credentials.
3. Run **InterposerAutotuningAgentLauncher.exe**.
4. Make sure that PMA driver installed successfully.
5. Enter IP Main host and port address (see step 2 from prerequisites).
6. Press **Enter**. Make sure there are no warning and error messages. See Figure 7.47.
7. Close command prompt.

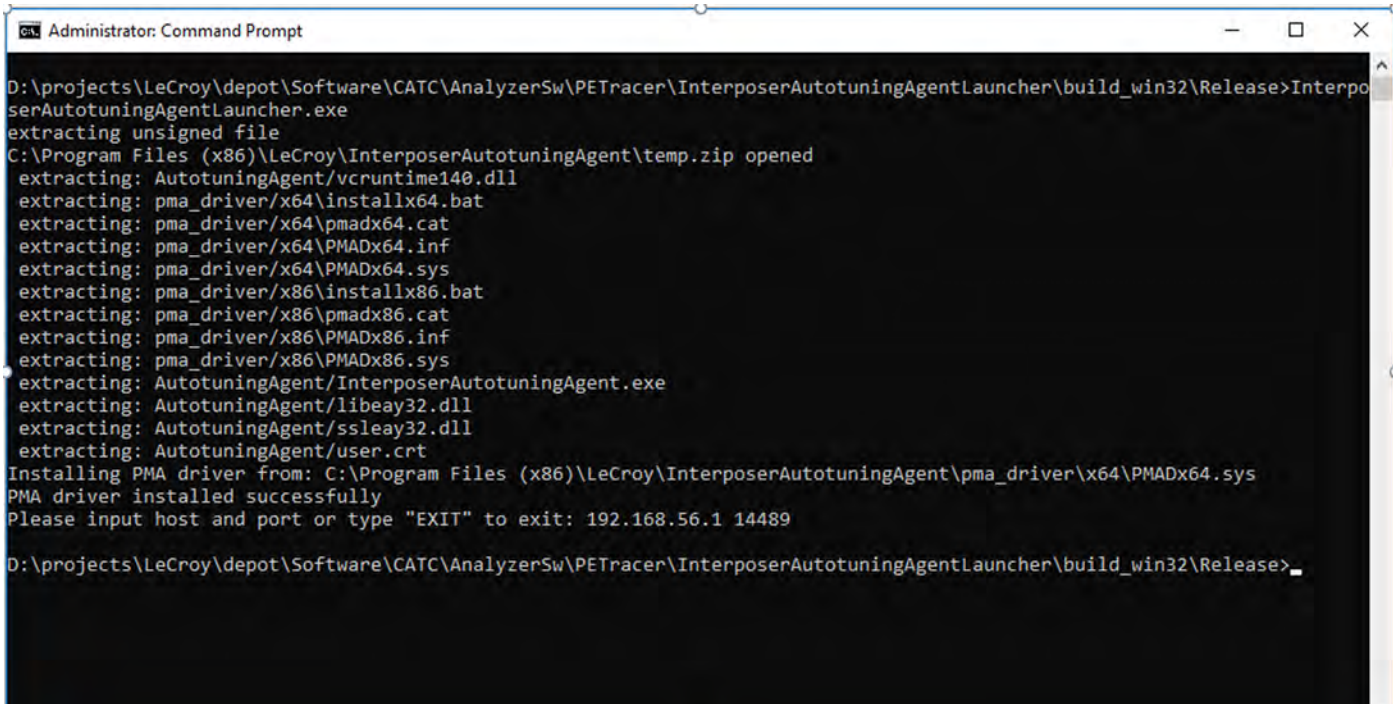


Figure 7.47: Administrator: Command Prompt

If unsuccessful, uninstall launcher using "Add/Remove Programs" and repeat “InterposerAutotuningAgent installation on target host”.

Uninstalling InterposerAutotuningAgent

1. Go to Windows settings -> 'Add or remove programs'
2. Remove 'Interposer Autotuning Agent'

Verify the service is correctly installed and running on target Host PC.

After successful InterposeAutotuningAgent installation new windows service must appear and be “Running”. See Figure 7.48.

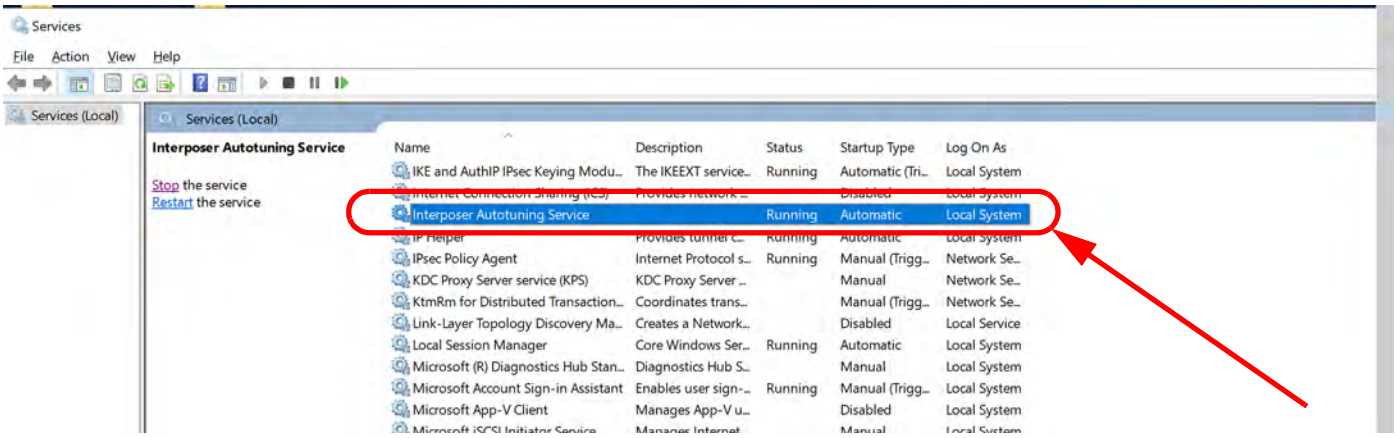


Figure 7.48: Services: Interposer Autotuning Service

After Agent startup, it immediately attempts to connect the client PC for every 5s. Such behavior may cause false positive warning of antivirus software or IDS (intrusion detection systems). It is recommended to uninstall/disable agent as soon as it is no longer needed.

User has option to stop Agent remotely from Auto-tuning dialogue. In such cases Agent stops service and tries to uninstall itself.

Start auto-tuning process:

1. From the PC where analyzer is connected.
2. Open PCIe Protocol Analysis software.
3. Connect to Analyzer.
4. Open "Recording Options" dialog.
5. Switch to "Host-to-DUT settings" tab.

See Figure 7.49 on page 393.

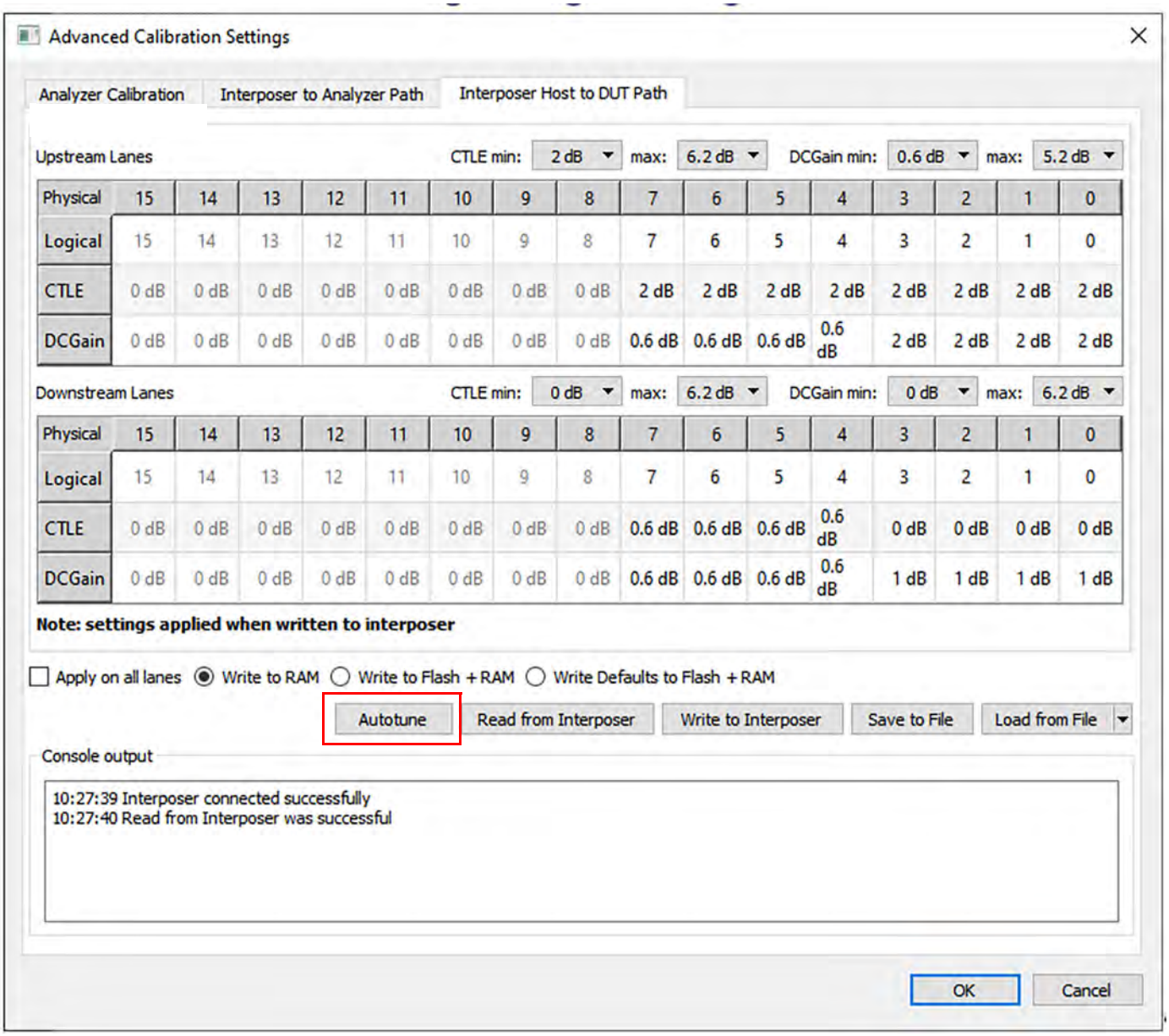


Figure 7.49: Recording Options: Interposer Host to DUT Path -> Autotune

6. Click on "Autotune" button (see Figure 7.49), this will bring up the Autotune dialog. See Figure 7.50 on page 394.

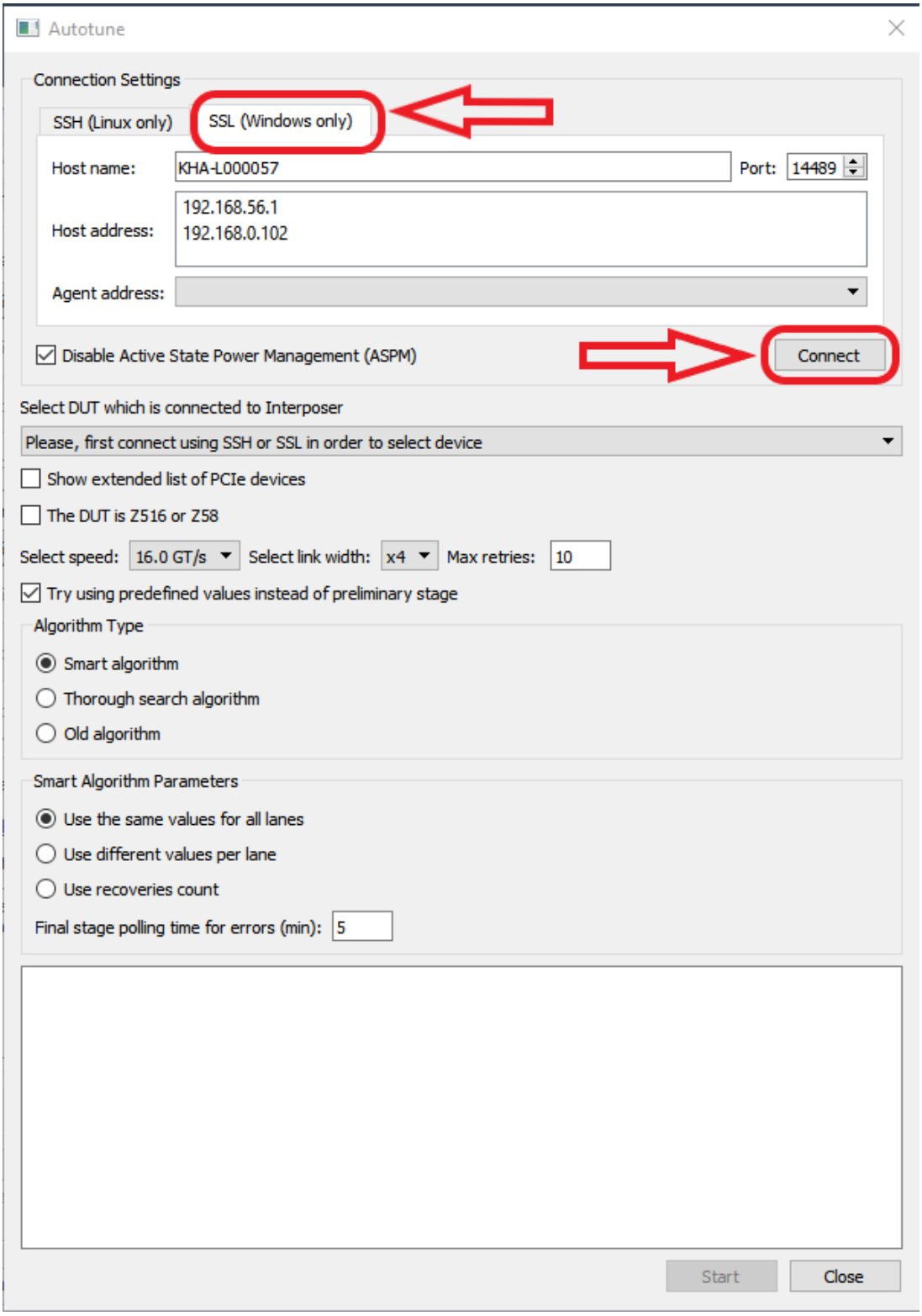


Figure 7.50: Auto-Tune Dialog

7. Select SSL (Windows only), complete the agent install process as describe above (put ref. mark here), before the next step.

8. Dialog window will open, with options to do DUT path.
9. Click "Connect" button. Connection to target host will be established (it may take several seconds) and then list of devices on host will appear. See Figure 7.51.

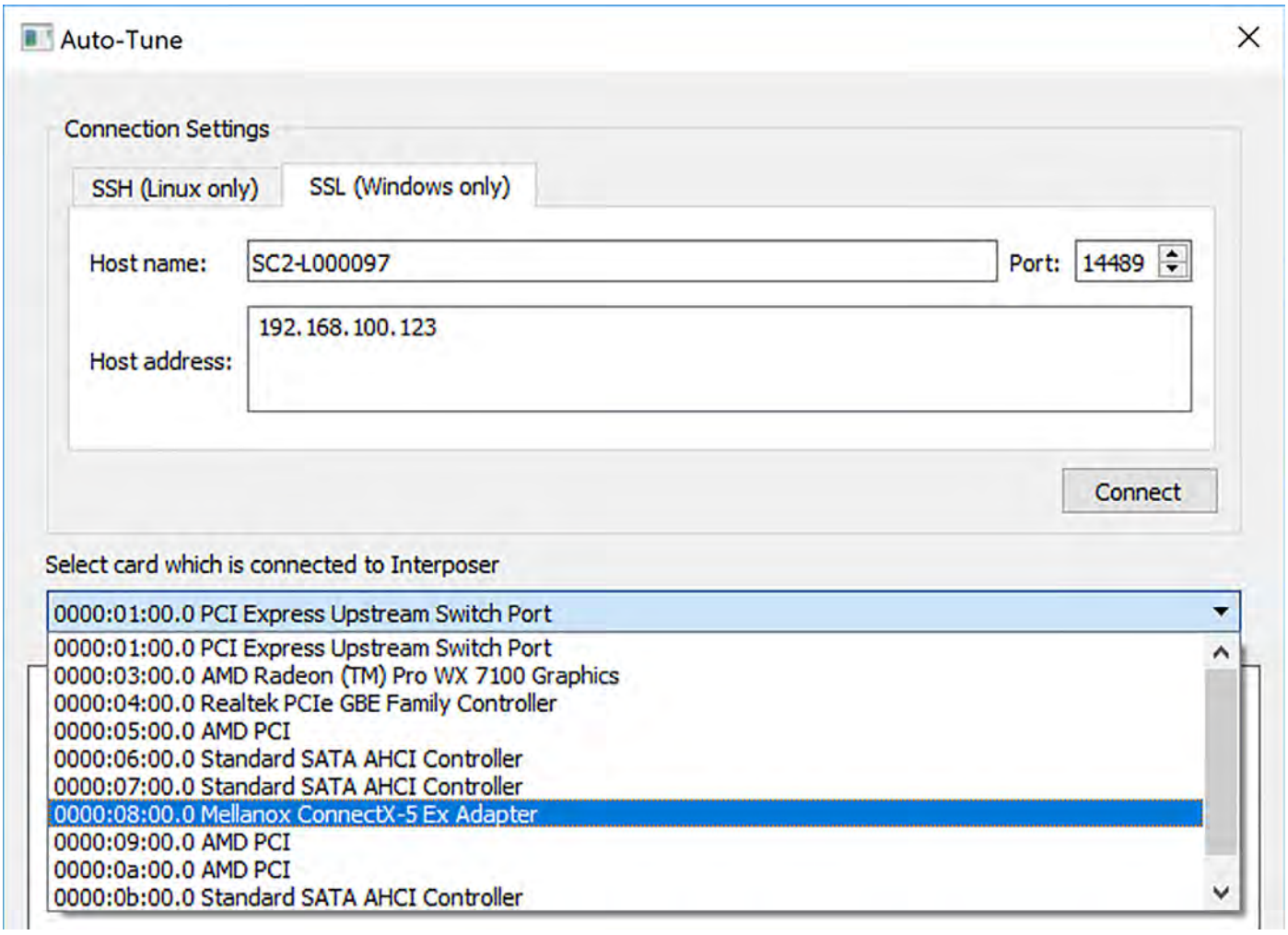


Figure 7.51: List of PCIe Devices

If the list of devices on the host does not appear and the error as shown on Figure 7.38 is reported in the log, then the InterposerAutotuningAgent should be reinstalled on the target host using the steps described in “Uninstalling InterposerAutotuningAgent” and “InterposerAutotuningAgent installation on target host” sections above.

This error may occur if the InterposerAutotuningAgent from one of the previous PCIe Protocol Analysis versions is installed on the target host.

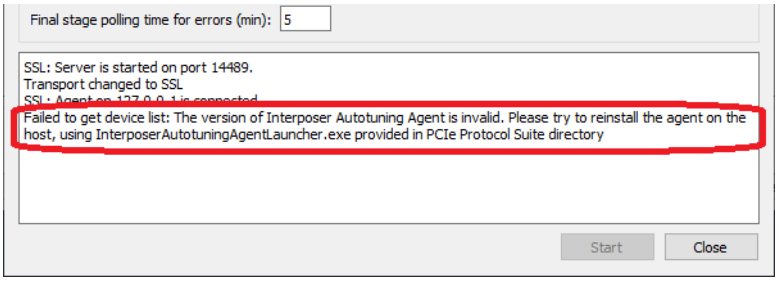


Figure 7.52: Incorrect Agent Version Error

10. Select desired link width, speed and algorithm parameters.
11. Select DUT in this list. There is no way for software to detect if selected device is a correct one or not. If wrong device was selected calibration will still start but of course will not do anything useful. In most cases it will stop after about two minutes and then user can re-run it selecting correct device this time. In this case we chose the Mellanox PCIe card to Auto-Tune.

Note: This is a critical step, please select the correct device, not the bridge, otherwise the tuning will not work.

12. After clicking "OK" tuning will begin, detailed progress report will be shown in the log area. User can press the "Stop" button which will abort tuning process, but this may leave link unstable or absent in which case setting some reasonable interposer parameters and rebooting of target host may be needed.

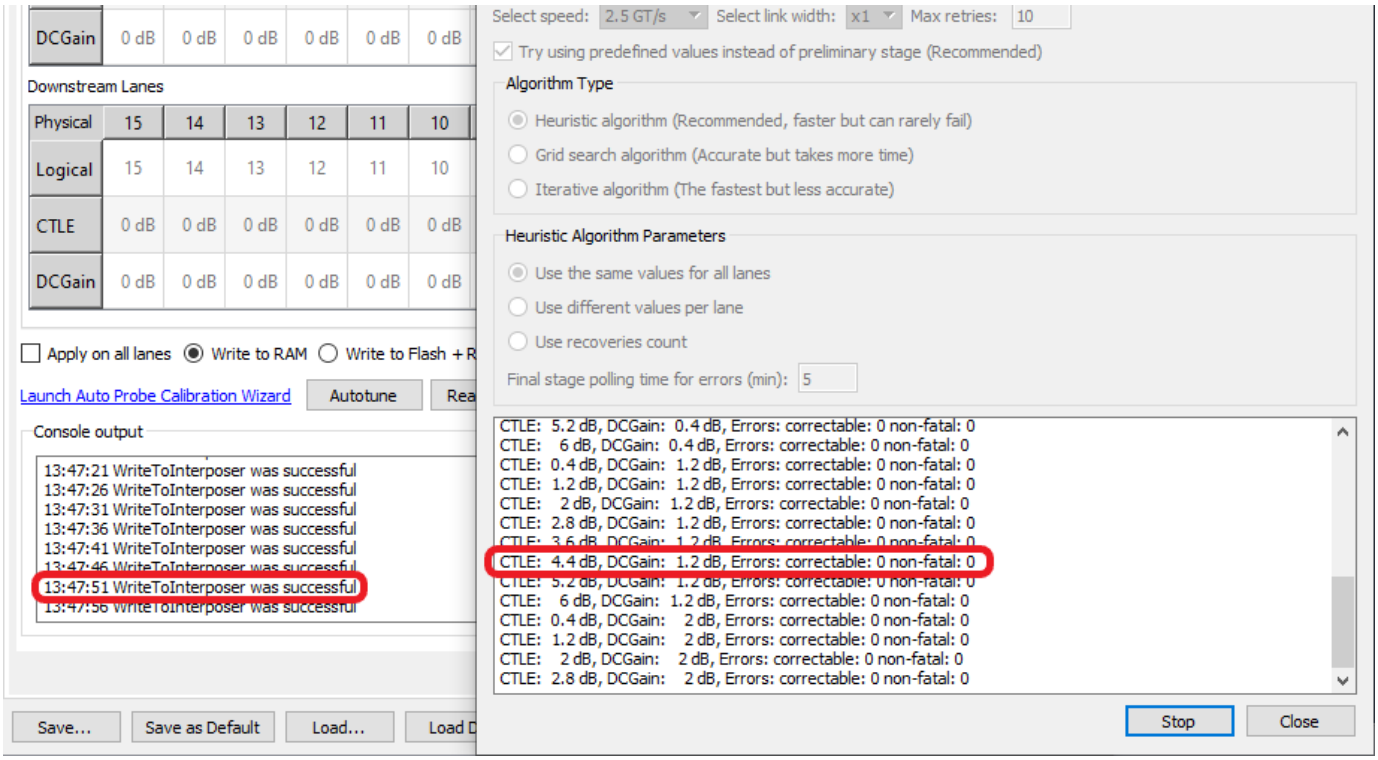


Figure 7.53: PCIe Card Selected: Auto-Tune Started

As you can see from Figure 7.53 as Auto-Tuning proceeds new CTLE and DC Gain values are written to the Interposer.

13. If any error occurs, it will be reported in dialog window as well as in the log area. It is meant as unattended process. There is no specific estimate of time it will take, but on most setups, it will be in the range from 3 to 30 minutes. On some setups it may take a lot longer (as long as several hours)
14. Depending upon the host, it is possible that the host reboot process hangs, in this case, if it cannot come back up even after 10 minutes, timeout popup will be shown with request to reboot host manually, but overall process is automatic.
15. When tuning is finished, a dialog is shown which allows users to keep newly-found settings or return to previous settings.
16. If SSL agent is used user will be prompted to stop auto-tuning agent on closing auto-tuning dialog. If agent is stopped user will need to reinstall it to do DUT path tuning again.

7.16.1.5 Host is on Linux OS:

For Linux hosts SSH connection is used, meaning network connectivity to target host and SSH credentials are required. These credentials should either directly give root privileges on host or be enough to get root access using 'sudo' command. Required tools will be transferred to target host automatically. The target host PC may be rebooted several times during calibration it should be

connectable by SSH after reboots without manual intervention (i.e. SSH server should be started on boot, port should be opened in firewall and so on).

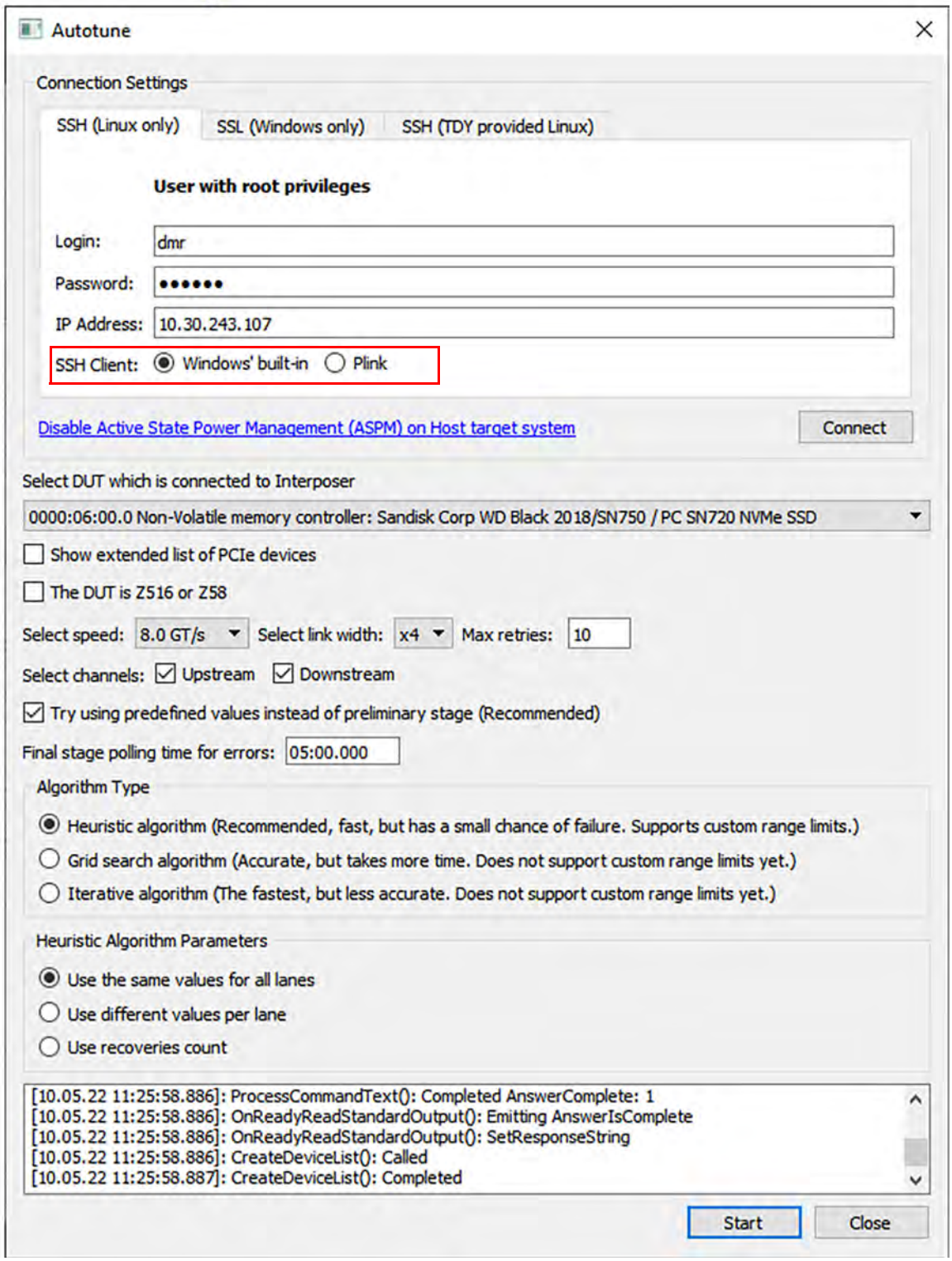


Figure 7.54: Autotuning Options

Autotuning uses one of two methods for communication with the Host with SSH Client:

- "Windows' built-in" - Autotuning uses an ssh.exe and scp.exe which are provided as part of the Windows installation.
- "Plink" - Autotuning uses a separate Plink utility. It is installed automatically together with PCIe Protocol Analysis software. This option may cause issues with connection to the Host if it uses ANSI escape sequences during SSH communication.

Commands to Validate the Setup:

Connecting to Linux host from Windows cmd.exe: (see Figure 7.55)

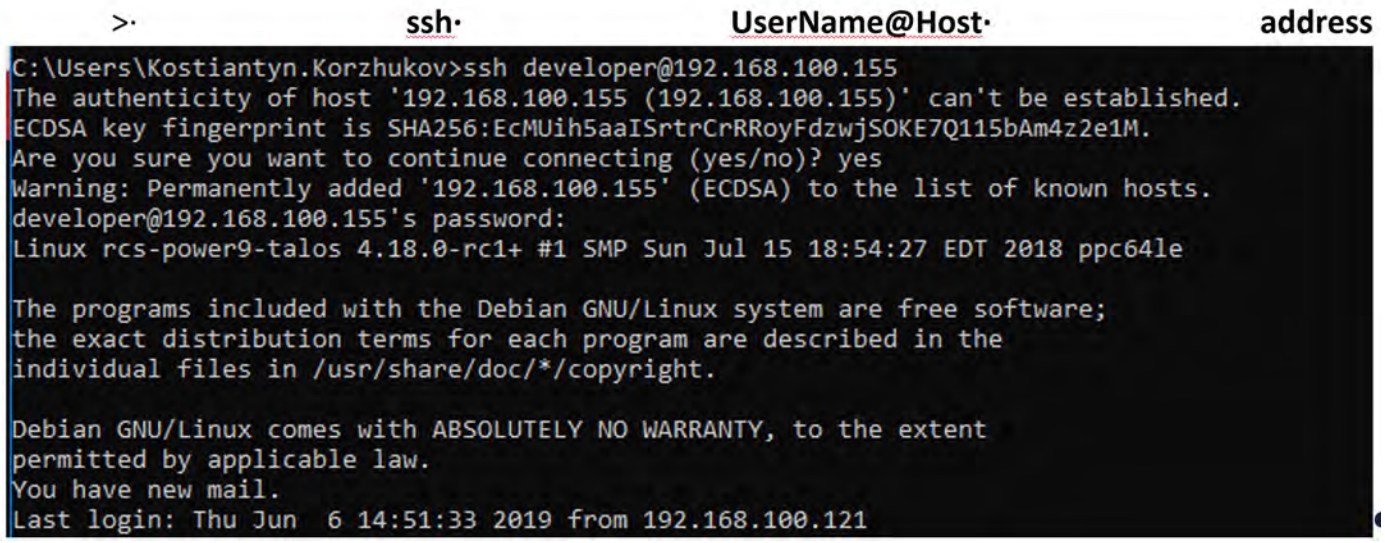


Figure 7.55: Connecting to Linux host from Windows cmd.exe

Get list all installed PCIe devices: # lspci (see Figure 7.56).

```
developer@rcs-power9-talos:~$ lspci
0000:00:00.0 PCI bridge: IBM Device 04c1
0001:00:00.0 PCI bridge: IBM Device 04c1
0001:01:00.0 SATA controller: Marvell Technology Group Ltd. 88SE9235 PCIe 2.0 x2 4-port SATA 6 Gb/s Controller (rev 11)
0002:00:00.0 PCI bridge: IBM Device 04c1
0003:00:00.0 PCI bridge: IBM Device 04c1
0003:01:00.0 USB controller: Texas Instruments TUSB73x0 SuperSpeed USB 3.0 xHCI Host Controller (rev 02)
0004:00:00.0 PCI bridge: IBM Device 04c1
0004:01:00.0 Ethernet controller: Broadcom Limited NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
0004:01:00.1 Ethernet controller: Broadcom Limited NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
0005:00:00.0 PCI bridge: IBM Device 04c1
0005:01:00.0 PCI bridge: ASPEED Technology, Inc. AST1150 PCI-to-PCI Bridge (rev 04)
0005:02:00.0 Multimedia video controller: ASPEED Technology, Inc. ASPEED Graphics Family (rev 41)
0030:00:00.0 PCI bridge: IBM Device 04c1
0030:01:00.0 VGA compatible controller: Advanced Micro Devices, Inc. [AMD/ATI] Ellesmere [Radeon Pro WX 7100]
0030:01:00.1 Audio device: Advanced Micro Devices, Inc. [AMD/ATI] Ellesmere [Radeon RX 580]
0031:00:00.0 PCI bridge: IBM Device 04c1
0031:01:00.0 Non-Volatile memory controller: Samsung Electronics Co Ltd NVMe SSD Controller SM961/PM961
0032:00:00.0 PCI bridge: IBM Device 04c1
0033:00:00.0 PCI bridge: IBM Device 04c1
```

Figure 7.56: Get List of all Installed PCIe Devices

Note: The device under test (DUT) should be present in this list, otherwise the auto-tuning will not work.

Reboot target host from command line

In some cases installed PCI hardware doesn't detect correctly, usually reboot attempts will help.

sudo reboot (see Figure 7.57).

```
developer@rcs-power9-talos:~$ sudo reboot
[sudo] password for developer:
Connection to 192.168.100.155 closed by remote host.
Connection to 192.168.100.155 closed.
```

Figure 7.57: Reboot Command

Start auto-tuning process

1. From the PC where analyzer is connected.
2. Open Petracer.
3. Connect to Analyzer.
4. Open "Recording Options" dialog.
5. Switch to "Host-to-DUT settings" tab (see Figure 7.58 on page 401).

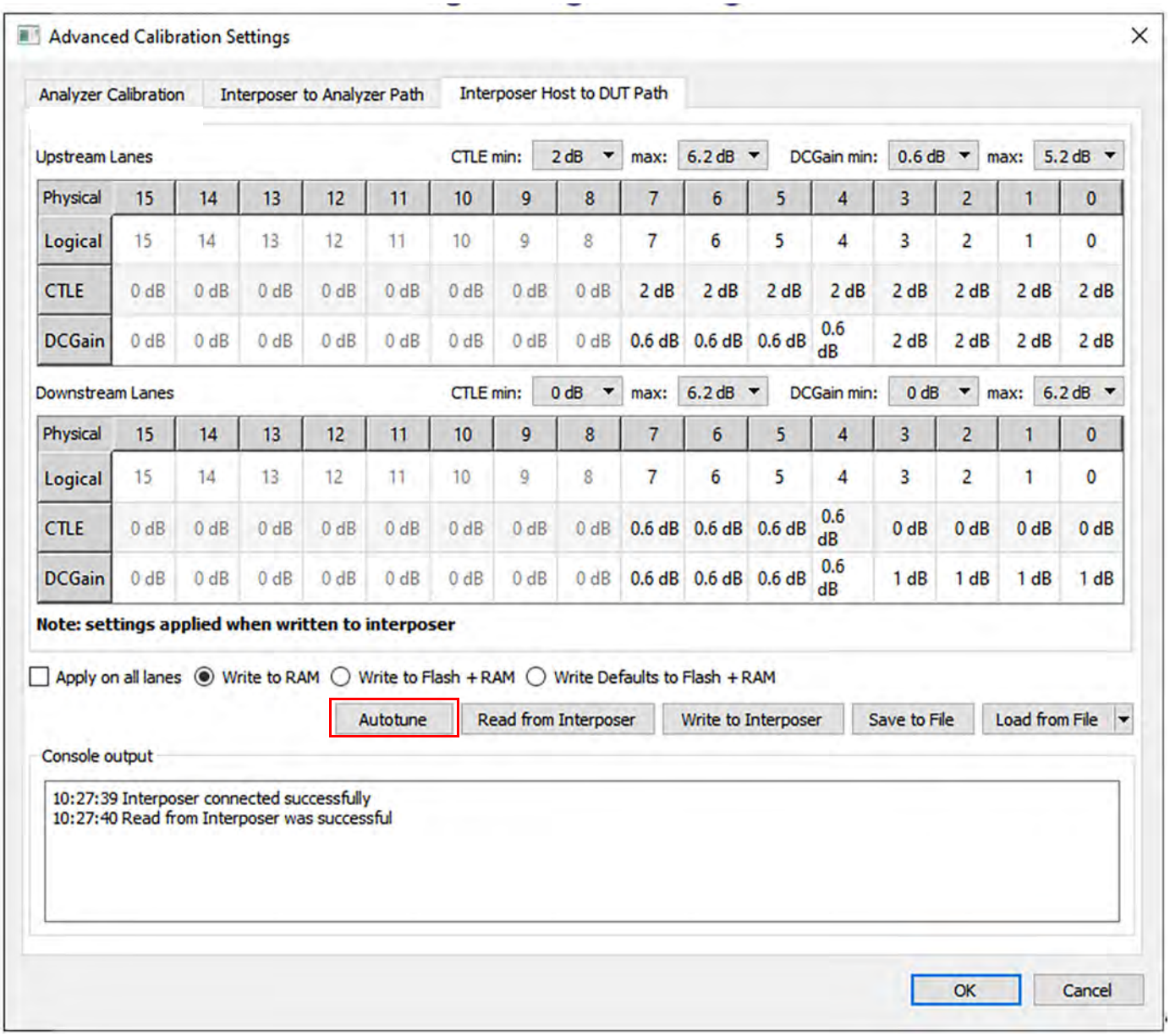


Figure 7.58: Host to DUT Settings

6. Click the **Autotune** button. The Autotune dialog box for the Host to DUT Settings appears, with options to do the DUT path (see Figure 7.59 on page 402).

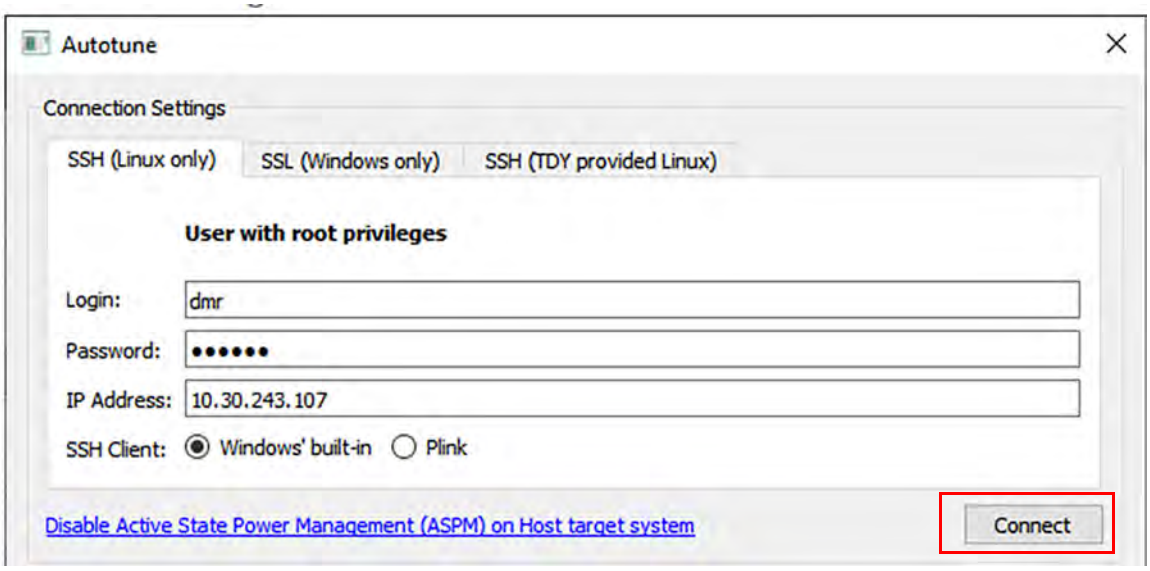


Figure 7.59: Options for Tuning the DUT Path

7. Enter target host settings:
   a. Select what kind of connection to remote host should be used from settings configured in the upper section:
   b. To auto-tune device connected to Linux host: Enter user, password and IP address of the target host and click **Connect**. (see Figure 7.59).
8. The connection to target host will be established (it may take several seconds), then list of devices on host will appear. Select the DUT from this list. There is no way for the software to detect if the selected device is the correct one. If the wrong device was selected, calibration will still start but will not do anything useful. In most cases, it will stop after about two minutes. Then, re-run it selecting the correct device.
9. Select desired link width, speed and algorithm parameters.
10. Click OK to begin the calibration.
    - A detailed progress report will be shown in the log area.
    - You can press the **Stop** button to abort the tuning, but this may leave the link unstable or absent. In this case, setting some reasonable interposer parameters and rebooting of target host may be needed.
11. If any error occurs, it will be reported in dialog window and duplicated in log area. It is meant as unattended process. There are no specific estimates time it takes to complete, but on most setups, it will be in the range from 3 to 30 minutes. On some setups it may take a lot longer (as long as several hours)
12. Under some conditions target host may reboot one or several times. As a last-resort option if it cannot come back up after 10 minutes timeout popup will be shown with request to reboot host manually, but overall process is automatic.
13. When calibration is finished dialog window will be shown which allows users to keep newly-found settings or return to previous settings.

14. If SSL agent is used user will be prompted to stop auto-tuning agent on closing auto-tuning dialog. IF agent is stopped user will need to reinstall it to do DUT path calibration again.
15. Perform Analyzer path calibration:
    a. Go to **TAP4Settings → Interposer Analyzer Path**.
    b. Press **Calibrate → OK**. The calibration begins and a detailed progress report will be shown in the log area.
    c. You can press **Stop** to abort tuning, but this may leave the link unstable or absent.

Auto-tuning cannot break host/DUT link. If error rate is high enough, small estimate is used which goes in 1dB intervals through CTLE/DC Gain, and search for a point with minimal error rate. This is done independently for upstream and downstream. Then final stage walks around this point finding per-lane error-free combination of CTLE/DC Gain. If zero error rate was achieved this stage will be repeated with increased error measurement interval, up to 60 seconds.

7.16.1.6 Write to Interposer

Press this button to write equalization settings to the interposer.

The result of this operation depends on selected radio button above

Note: While writing is in progress, the Application title bar may show “Not Responding”. This is normal and will go away after writing is complete.

7.16.1.7 Write to RAM

If “Write to RAM” radio button is selected then equalization settings will be written to interposer but would not remain on the interposer after power-cycling it.

7.16.1.8 Write to Flash + RAM

If “Write to Flash + RAM” radio button is selected then settings will be written and saved into Flash Memory on the interposer. These setting would remain on the interposer even after power-cycling it.

7.16.1.9 Write Default to Flash + RAM

If “Write Default to Flash + RAM” radio button is selected then write will restore the interposer to its default settings.

Note: Writing to Flash takes several minutes to complete. While writing is in progress, the Application title bar may show “Not Responding”. This is normal and will go away after writing is complete.

7.16.1.10 Configurations: U2 x2, U2 x4

When the analyzer is connected to U.2 Interposer, a drop down list becomes available and presents the supported configurations:

- U.2 x2 (Port A and Port B): Can record up to 2 x2 Links, Port A being on Lanes 0, 1 and Port B being on Lanes 2,3 

- U.2 x4: Can record up to x4 Link 

Once a user attaches the Interposer to the respective host system, the configuration is automatically detected and set. To manually change the U.2 configuration, check " Write to Flash ", change the U.2 Configuration, write to the interposer, and then power cycle the interposer.

7.16.1.11 Read from Interposer

Press this button to read the equalization settings from the interposer.

Note: While reading is in progress, the Application title bar may show "Not Responding". This is normal and will go away after reading is complete.

7.16.1.12 Set All Lanes

Check this box and change the values in Lane 0 to change all the values in the corresponding column.

7.16.1.13 Log

This log would also be saved in the same location as the ".exe" file. The log should provide some preliminary information about connection and display values read / written.

7.16.1.14 Save to File

You can save your settings to a file.

7.16.1.15 Load from File or Predefined Values

You can load predefined CTLE and DC Gain values from a file or load CTLE and DC Gain values from a set of Predefined values for a specific configuration of hardware. See Figure 7.60

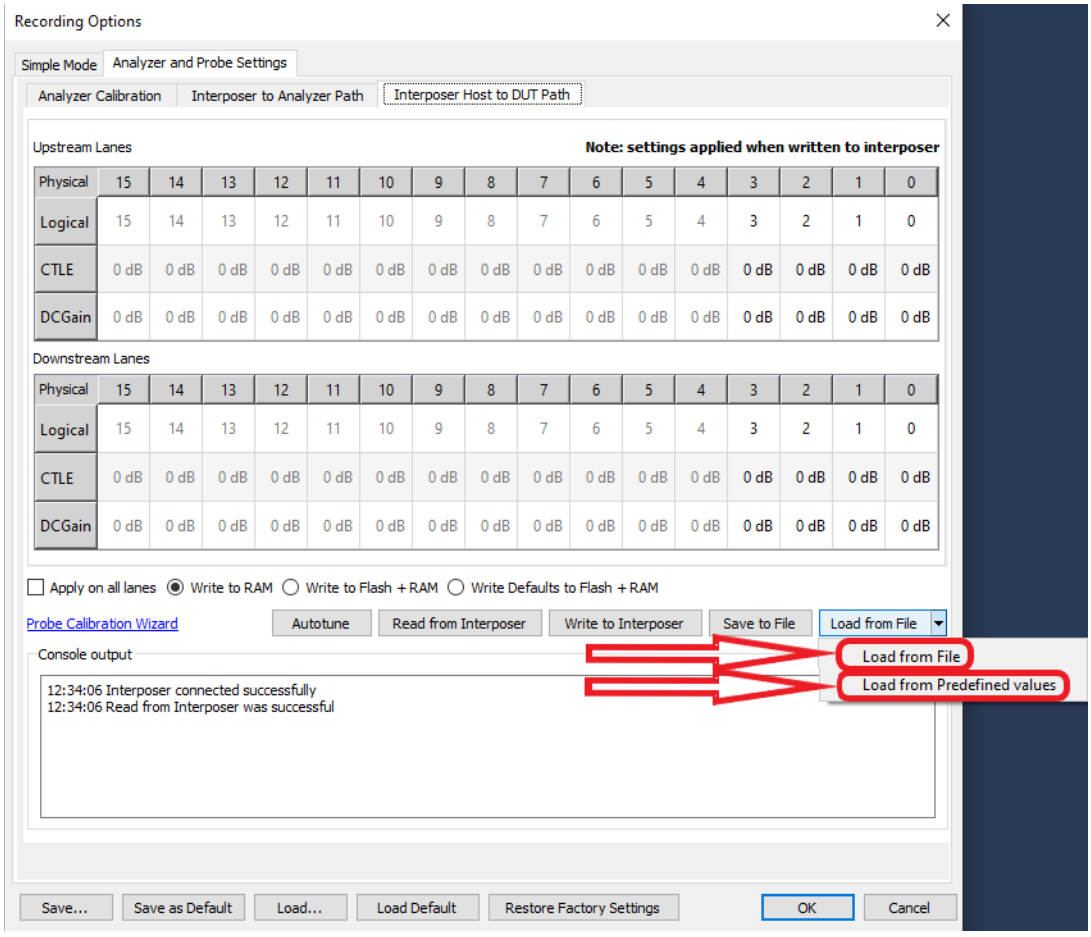


Figure 7.60: Load from File

You can chose from either:

- Load from File: Opens a dialog box to choose a file from where the application was loaded (see Figure 7.61 on page 406)
- Load from Predefined values: Opens a dialog box with a specific configuration of hardware (see Figure 7.62 on page 407)

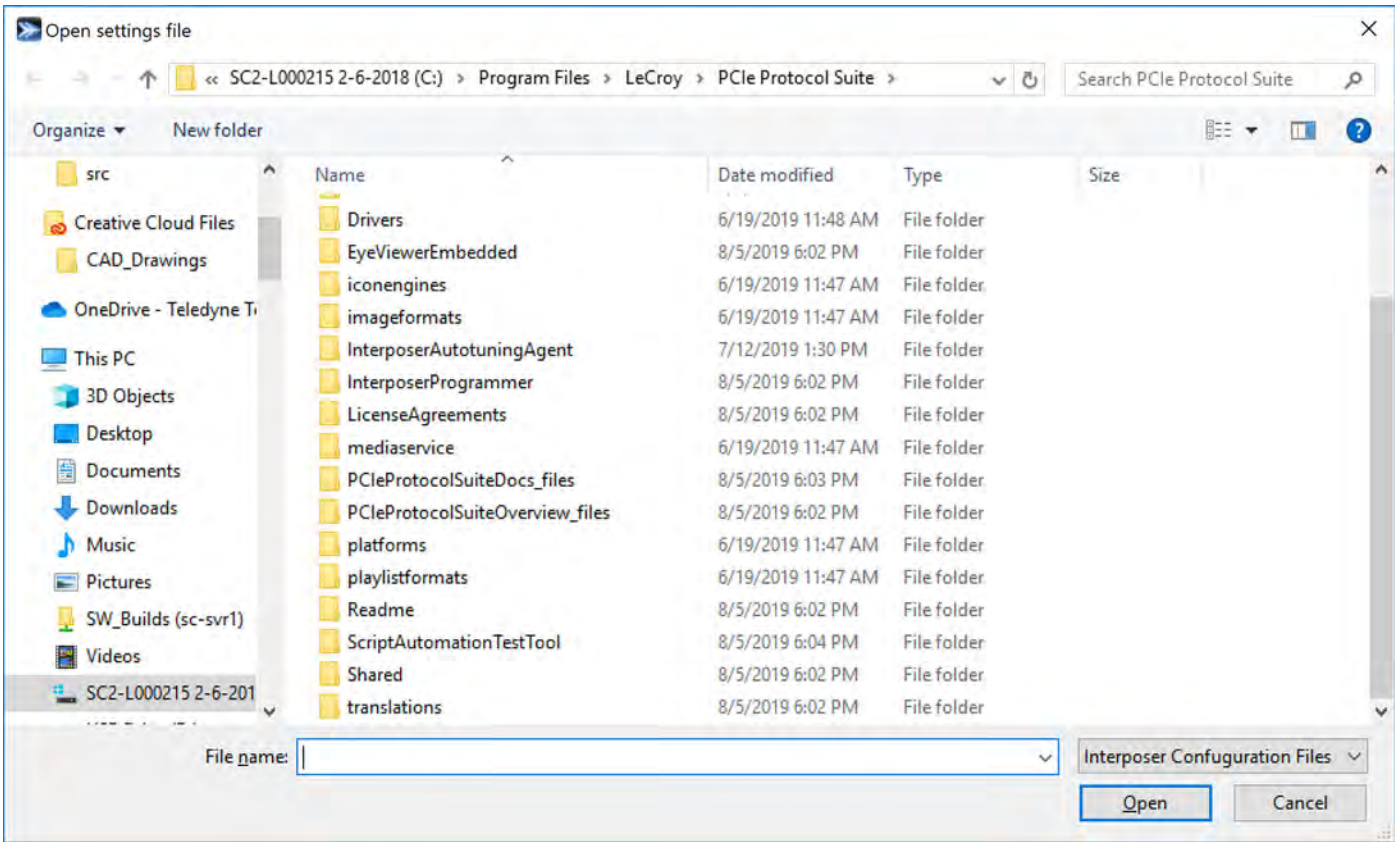


Figure 7.61: Load from File

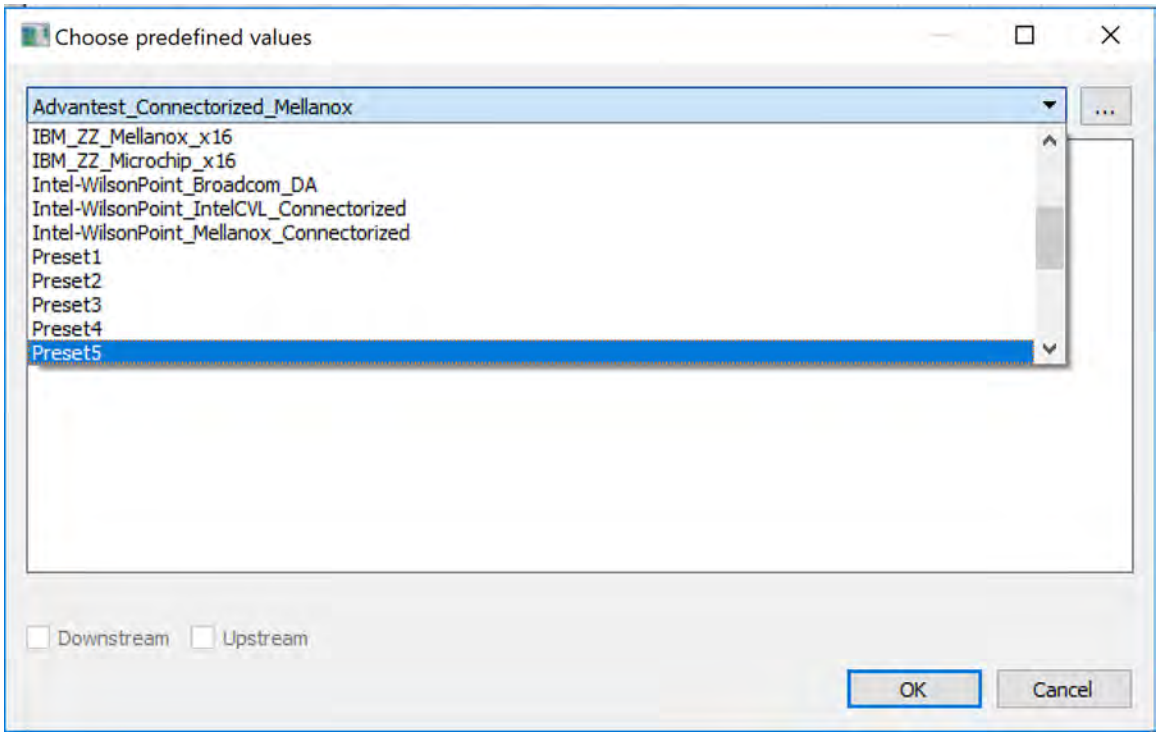


Figure 7.62: Load from Predefined values: Specific configurations or 1 of 9 Presets

7.16.2 Interposer to Analyzer Path

At this stage all the interposer related tuning is complete, now user can calibrate the “Front-End” of the analyzer by automatically finding the best presets for “Equalizer Settings” (see Figure 7.63).

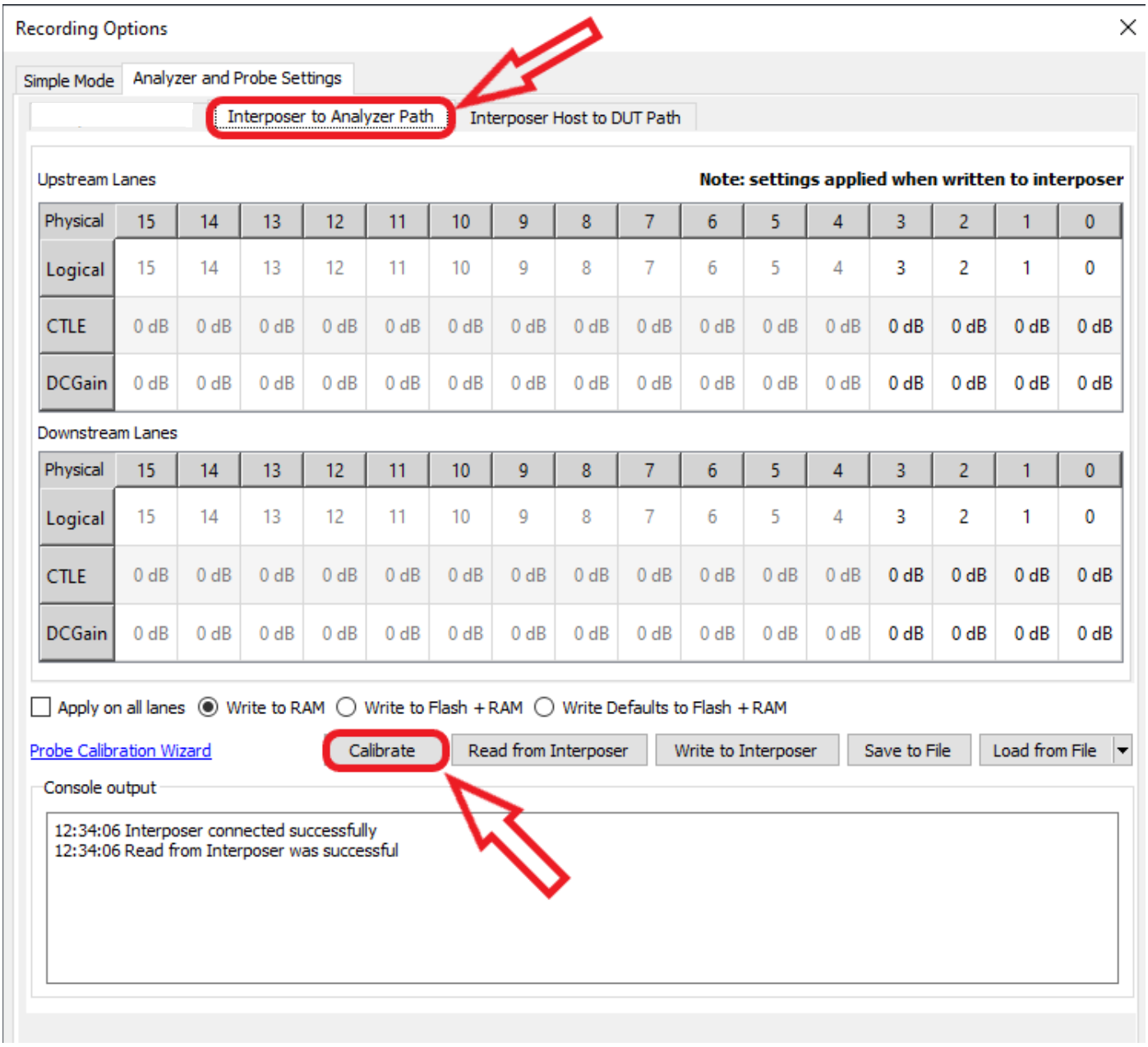


Figure 7.63: Interposer to Analyzer Path

7.16.2.1 Calibration Sequence

The dialog for calibration of Interposer to Analyzer Path allows selecting one of several algorithms. The selected algorithm determines the steps that will be performed during the process to find optimal CTLE and DCGain settings.

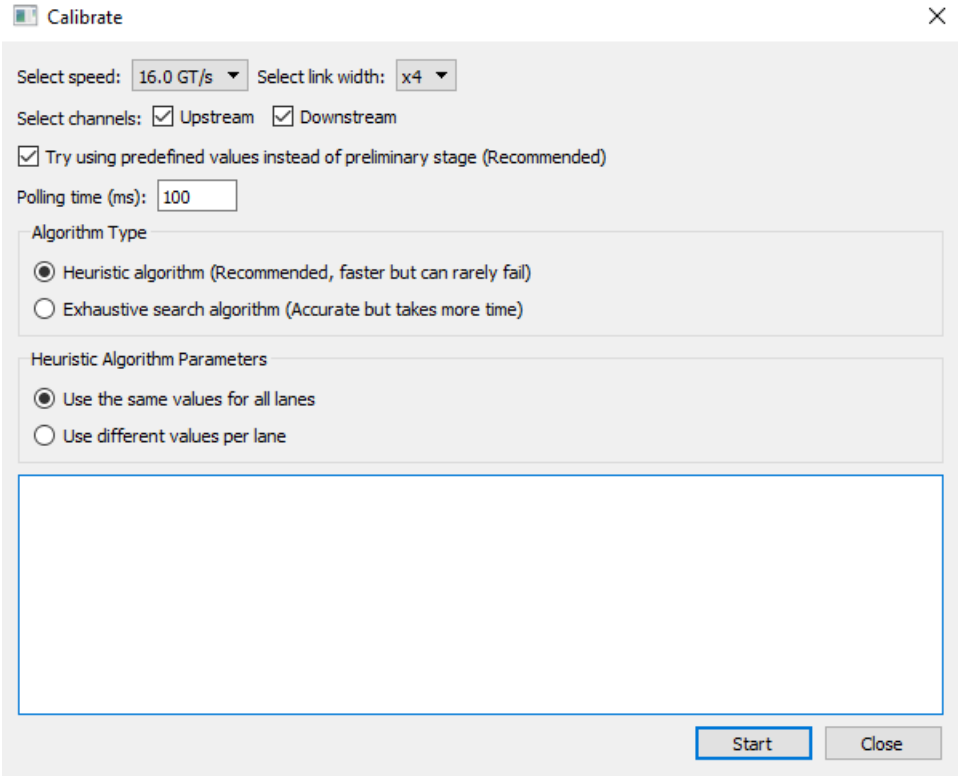


Figure 7.64: Interposer to Analyzer Path Calibration dialog

Below is a list of the available algorithms for calibration with descriptions:

Heuristic algorithm

This option is similar to Heuristic algorithm for auto-tuning. It also uses the same heuristic search method and performs the calibration in several stages. Please see the algorithm details in the “Auto-tuning Algorithms” on page 381 section.

The maximal error polling time is shorter for calibration and only four stages are performed: first 500 milliseconds and then 2, 5, 10 seconds stages. Final stage polling time can be configured in milliseconds in appropriate option.

Exhaustive search algorithm

The calibration routine checks all possible combinations of CTLE and DCGain settings (the same value is used for all lanes).

There are two stages:

1. On the first stage errors are measured for combinations of each CTLE value and DCGain values with step 1dB.

2. On the second stage errors are measured for combinations of each CTLE value and each DCGain value.

Firstly, all values are checked with polling time 1 ms and then some best values are retested with selected polling time.

If the settings are found with which error rate is zero for each lane on both channels, then the calibration finishes without checking all combinations.

7.16.3 Analyzer Calibration

The Summit M5x can be calibrated to work with specific links. The T.A.P.5 is a proprietary Teledyne LeCroy technology that allows DUT signaling to be optimized for the purposes of recording a clean trace. The Analyzer and Probe Settings tab allows for this optimization to be performed on each lane of the link by modifying different settings such as CTLE, DC Gain and Signal Detection threshold.

Select **Recording Options > Analyzer and Probe Settings -> Analyzer Calibration** from the **Setup** menu to display the available modes that can be used for Analyzer Calibration:

- Auto (See Figure 7.65 on page 411): Calibrating at 16.0 GT/s
  - CTLE and DC Gain are selected
- Manual

7.16.3.1 Analyzer Calibration: Auto Option

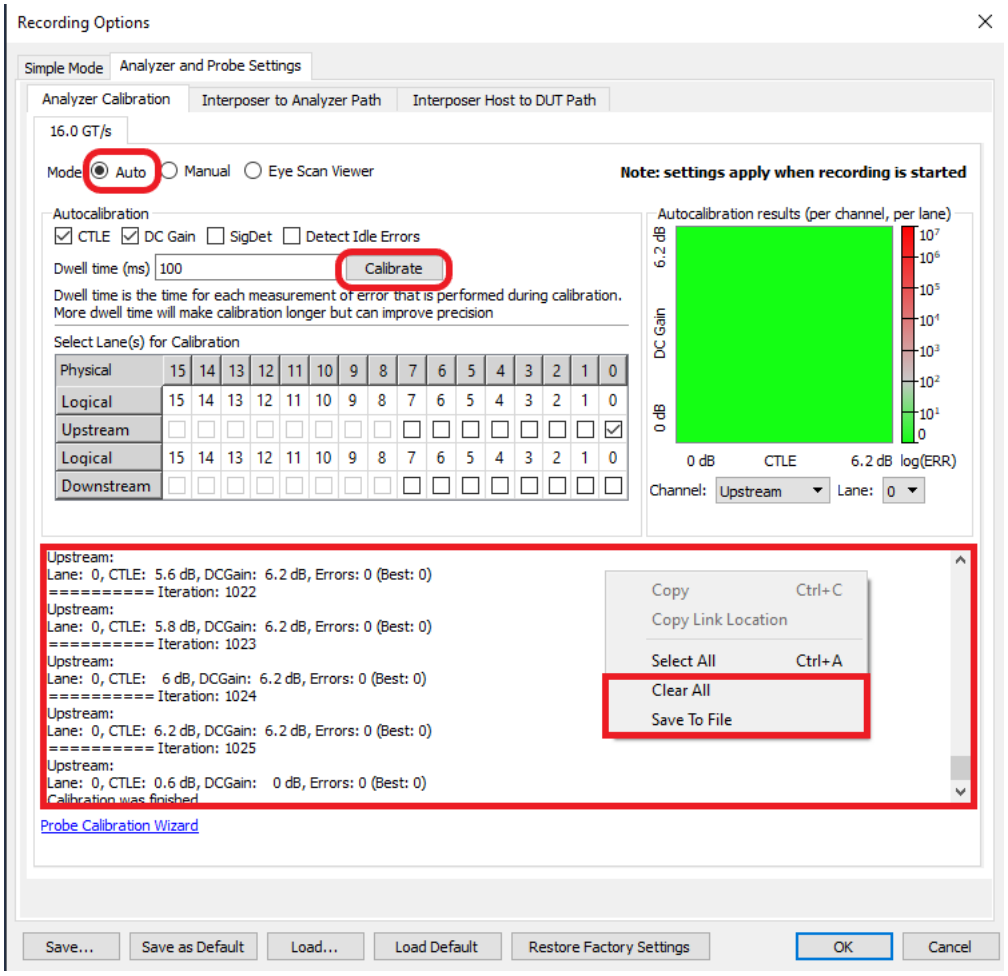


Figure 7.65: M5x: Analyzer Calibration Auto Mode

There is a log area where all checked values with current and best number of errors are listed during calibration process. On right mouse button click context menu is opened where log can be cleared or saved to .txt file.

The Calibration is done in this sequence:

1. Correctly set the lane polarity manually, auto lane polarity is not supported.
2. Calibration requires a fixed speed, so, if the speed selection is “Auto”, then user is required to select the speed at the time of starting the calibration.
3. In “Auto-calibration” area check lanes that need calibration. Usually all lanes will need calibration. All lanes in some direction (upstream or downstream) can be checked by clicking on accordingly named button in front of row of lane checkboxes.

4. Select some of checkboxes for CTLE, DC Gain and SigDet. It is recommended to check both CTLE and DC Gain to produce better results, but it will increase time needed for calibration because more values will be checked.

Note: SigDet option is not available for all devices and this option may be absent.

5. Decide if analysis of packets should be used to check their correctness instead of simpler checks. If so check “Detect Idle errors” checkbox. Usually is recommended to check it.
6. Select interval during which errors will be counted on each calibration step. Longer interval will give more precise results, but calibration time will be increased linearly. Usually default value (100 ms) is good enough for quick check and to estimate how long calibration will take, but longer intervals would be preferable.

Note: All values will be tested with an interval equal to 1 ms and then best found values will be re-checked with the selected time.

7. Press “Calibrate” button. Calibration process will start with progress bar shown.
8. After calibration finish per-lane error data are presented, separately for upstream and downstream.
9. Calibration results can be saved by clicking "OK".

7.16.3.2 Analyzer Calibration: Manual Option

In **Recording Options > Analyzer and Probe Settings -> Analyzer Calibration -> Manual Mode** each lane selected has the following options to achieve the best signal for detection and recording:

- CTLE (Continuous Time Linear Equalization): 0 to 6.2 dB in 0.2 dB steps
- DC Gain: 0 to 6.2 dB in 0.2 dB steps
- SigDetect (Signal detection threshold): 30 mV to 410 mV in 7 steps

The default is for SigDet 60 mV but you can vary the threshold from 30 mV to 410 mV depending on the amplitude of the signals being generated and correctly detected in your system. You can also set the CTLE value and the DC Gain in conjunction with the threshold SigDet level to get a high quality signal for recording and analysis. See Figure 7.66 on page 413.

- Measure: You can also set the Measure value to be 16.0 GT/s or 8.0 GT/s.

Note: When using the MidBus Probe, SigDet is recommended to be set at 40 mV for each lane.

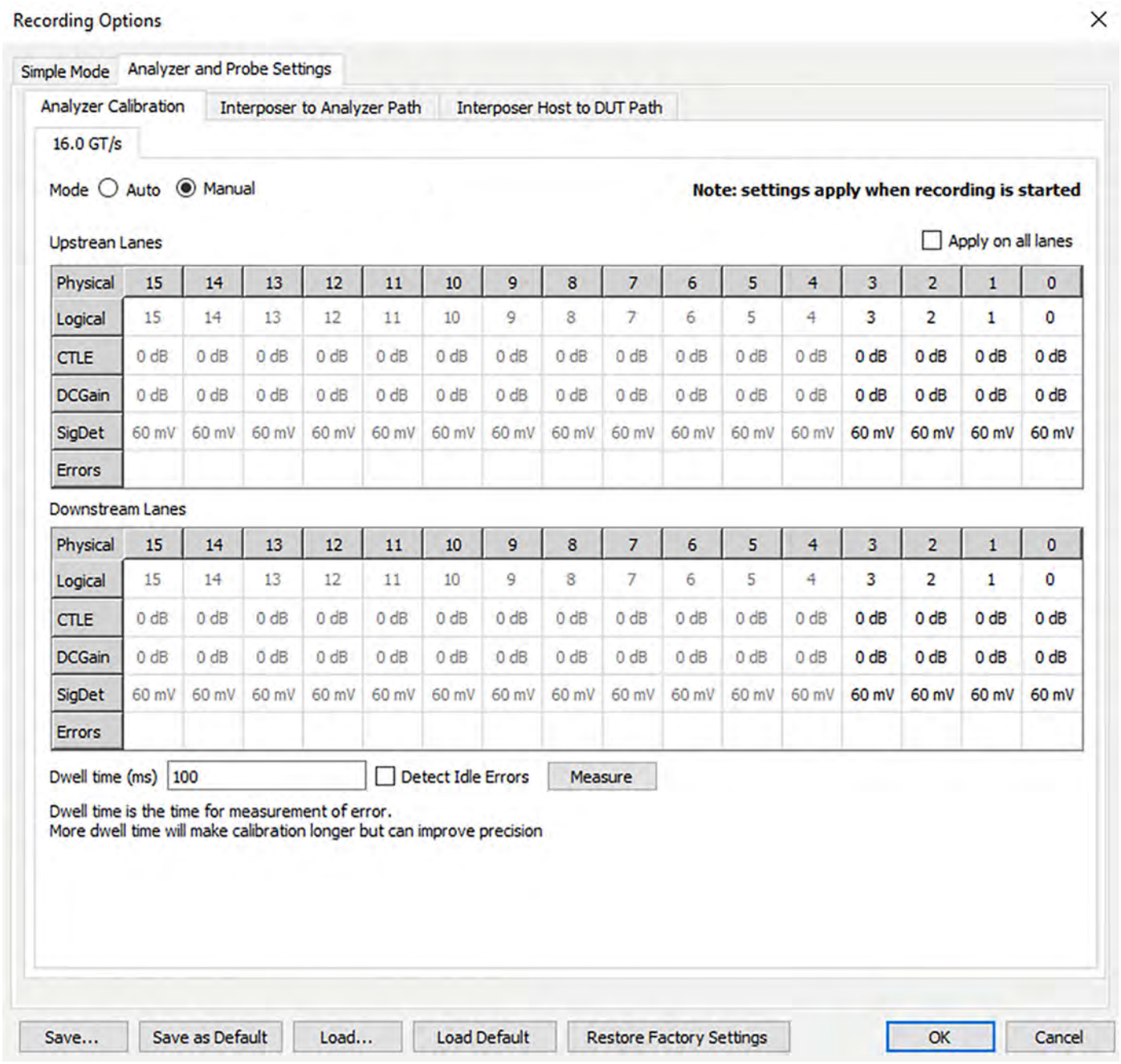


Figure 7.66: M5x: Analyzer Calibration Manual Mode

7.16.4 Using the Autotune and Probe Calibration Wizard

The Autotune and Probe Calibration wizard guides you through both the Autotune and Probe Calibration process steps as outlined below:

- ❑ Analyzer Verification
- ❑ Interposer Verification
- ❑ Setting Parameters
- ❑ Setting Polarity
- ❑ Precalibration
- ❑ Calibration Finished

To start the Autotune and Calibration Wizard select **Recording Options -> Analyzer and Probe Settings** (see Figure 7.67)

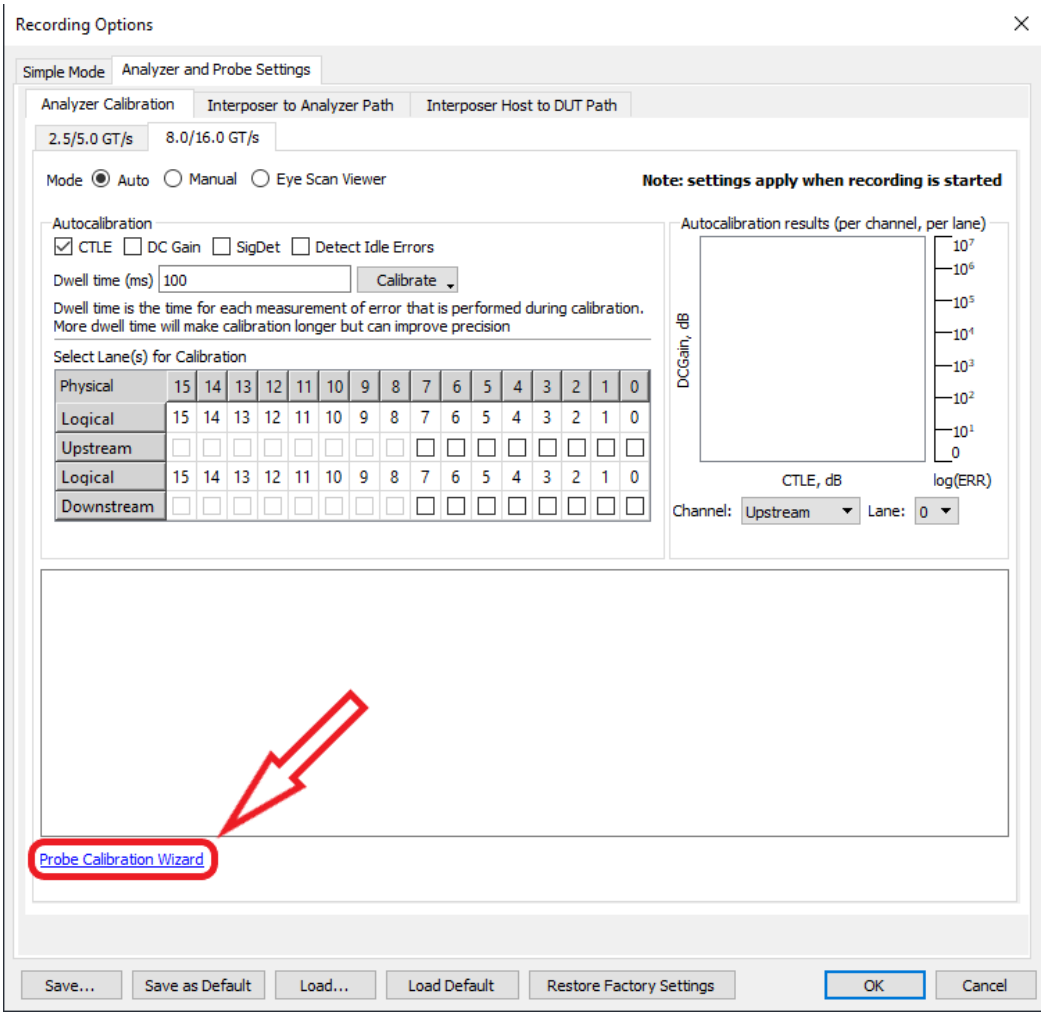


Figure 7.67: Select Recording Options -> Analyzer and Probe Settings

Select the Probe Calibration Wizard link. The following dialog box will pop up and lead you through the steps for both Autotuning the analyzer and Calibrating the Probe. See Figure 7.68 on page 415.

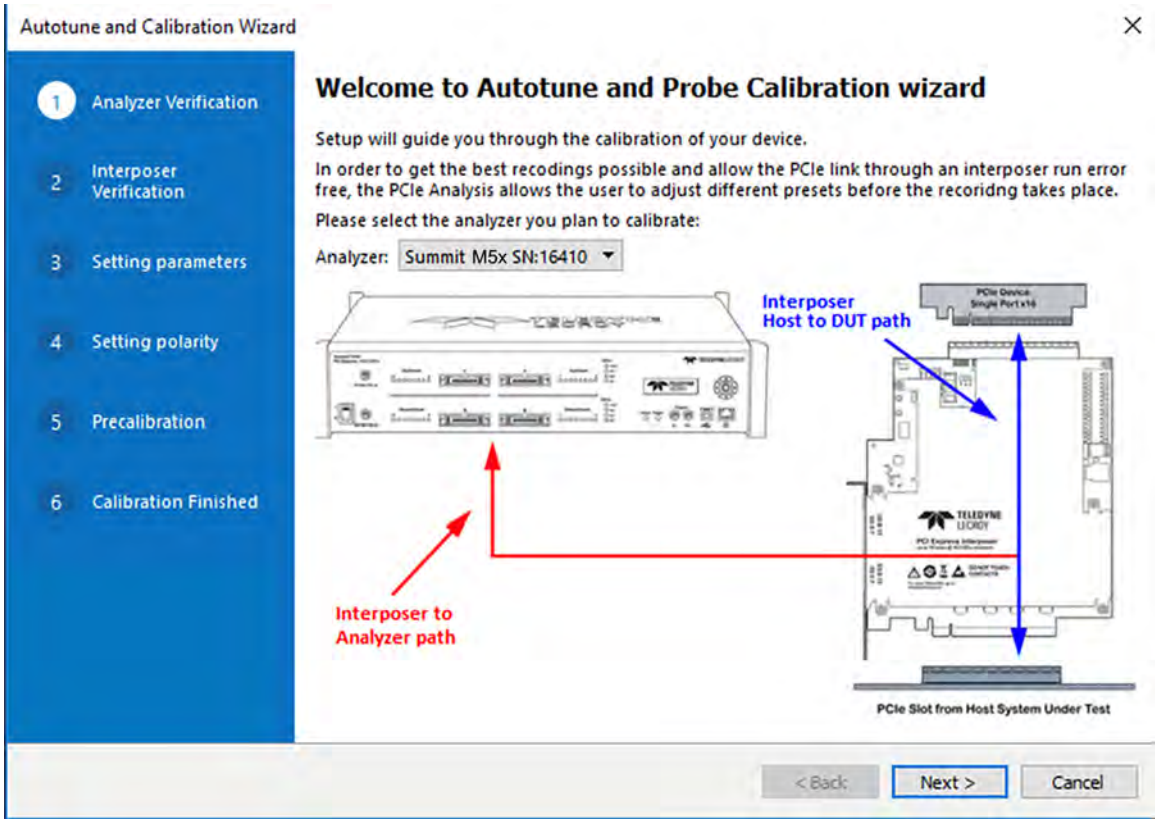


Figure 7.68: Autotune and Probe Calibration Wizard: Step 1 -> Analyzer Verification

First you choose the Analyzer you plan to calibrate.

Then click on next to go to Step 2: Interposer Verification (see Figure 7.69 on page 416).

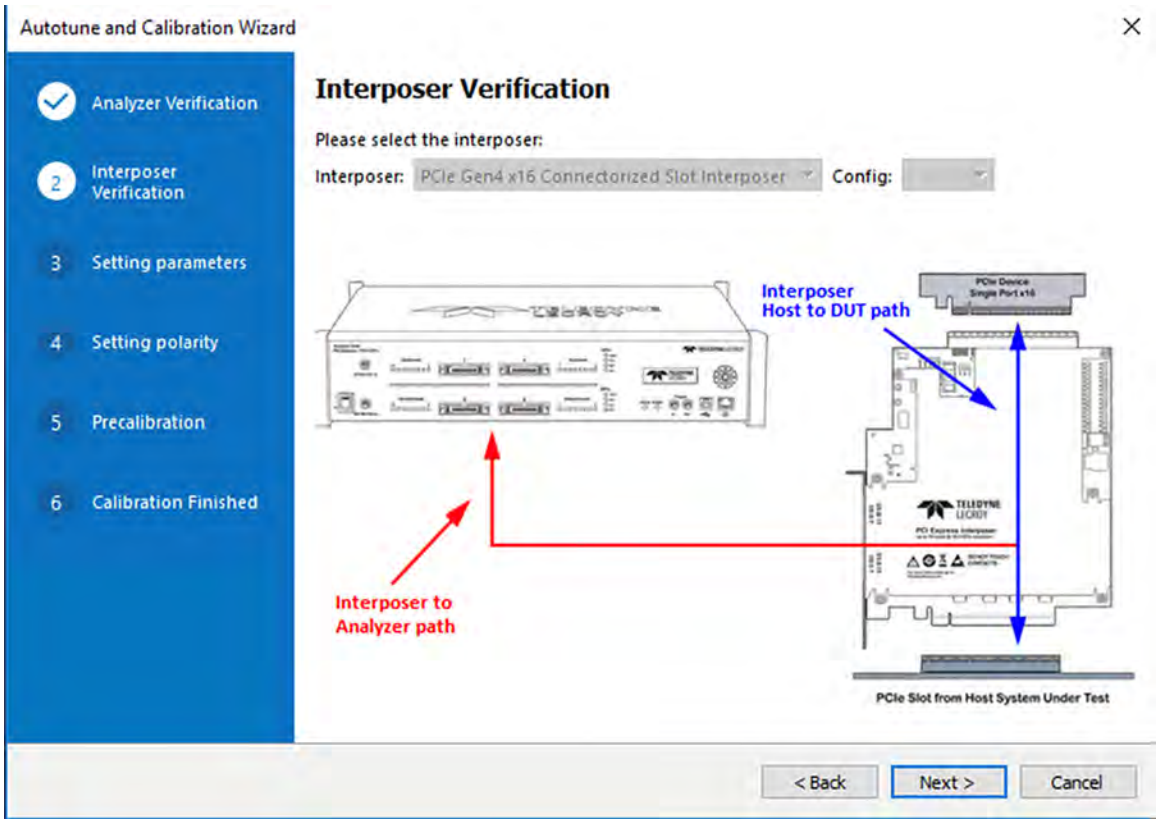


Figure 7.69: Autotune and Probe Calibration Wizard: Step 2 -> Interposer Verification

Note: We are working with the Gen4 x16 Slot Interposer but the steps for working with a Gen5 x8 Slot Interposer are similar.

Click on Next to go to Step 3: Setting parameters (see Figure 7.70 on page 417).

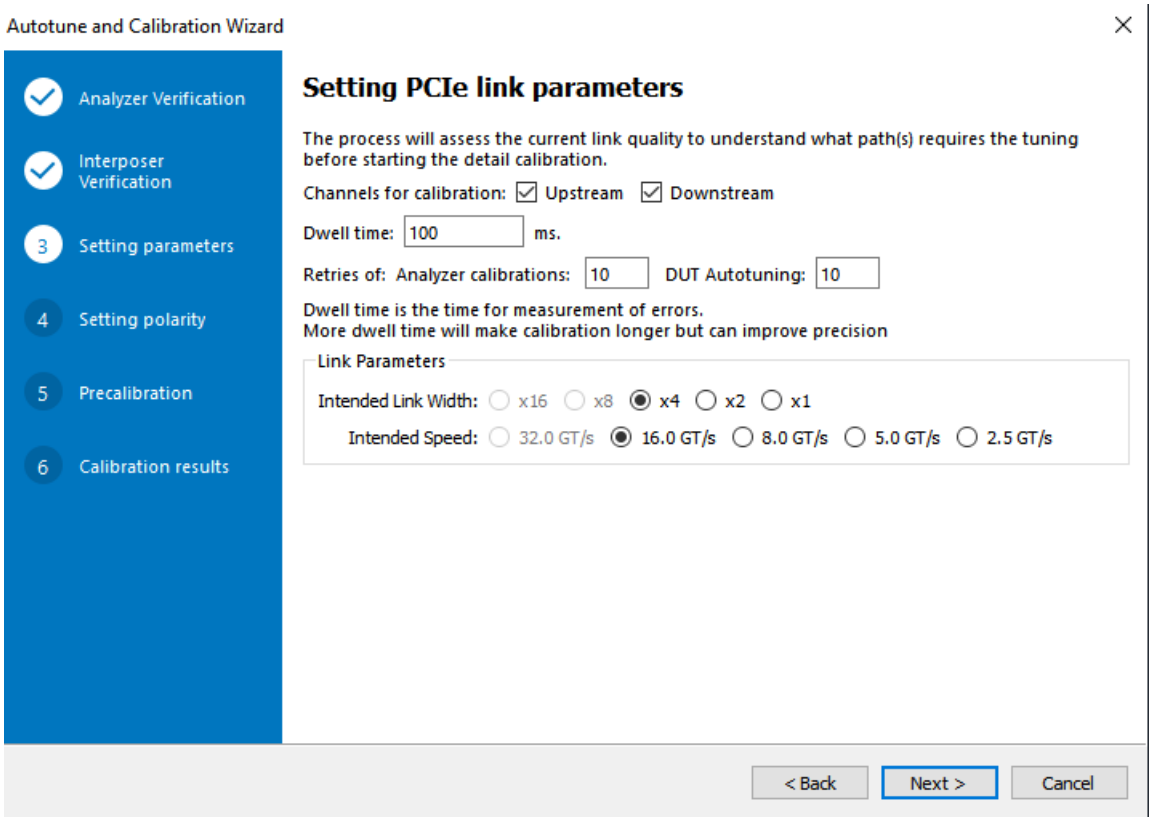


Figure 7.70: Autotune and Probe Calibration Wizard: Step 3 -> Setting Parameters

In this step you can set Channels for calibration, the Dwell time for measurement errors, select maximum number of retries of Analyzer calibration and DUT Autotuning and set up the link parameters.

Then click on Next to Set polarity (see Figure 7.71 on page 418).

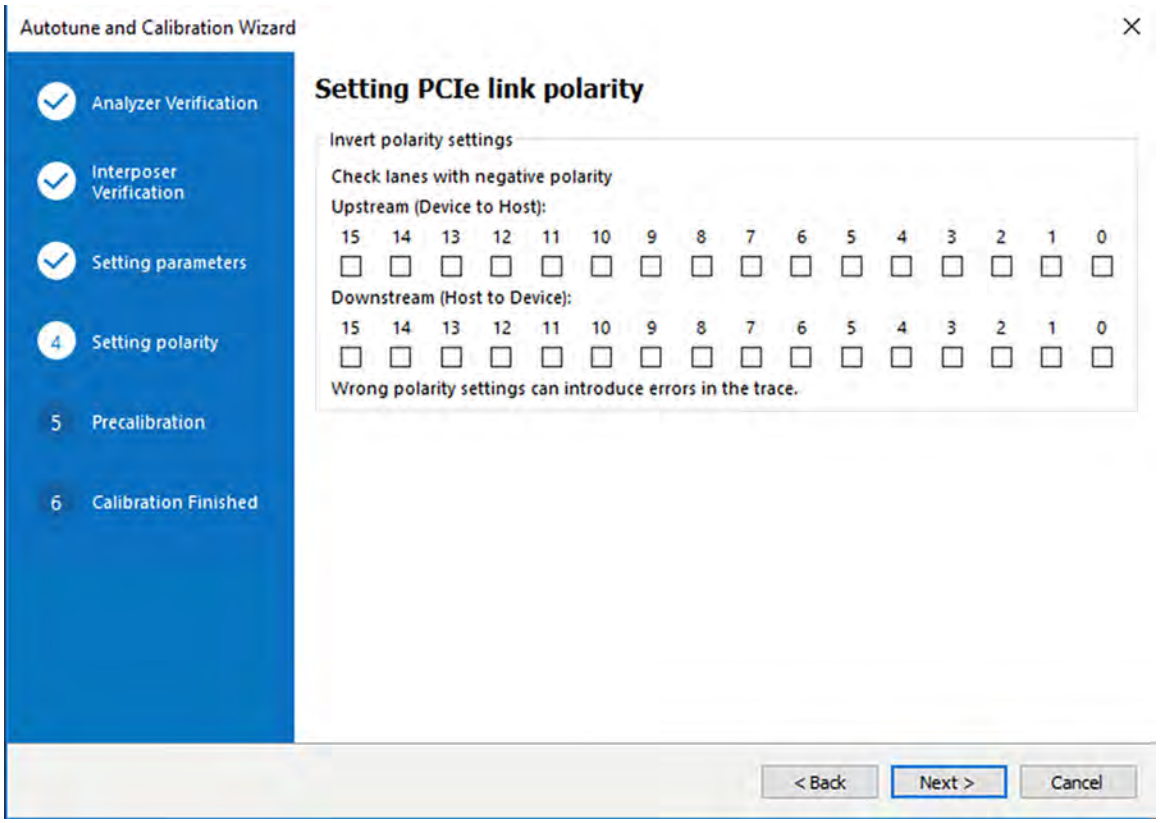


Figure 7.71: Autotune and Probe Calibration Wizard: Step 4 -> Setting Link Polarity

Here you can invert the polarity of Upstream or Downstream lanes.

Then click on Next to go to the Precalibration step (see Figure 7.72 on page 419).

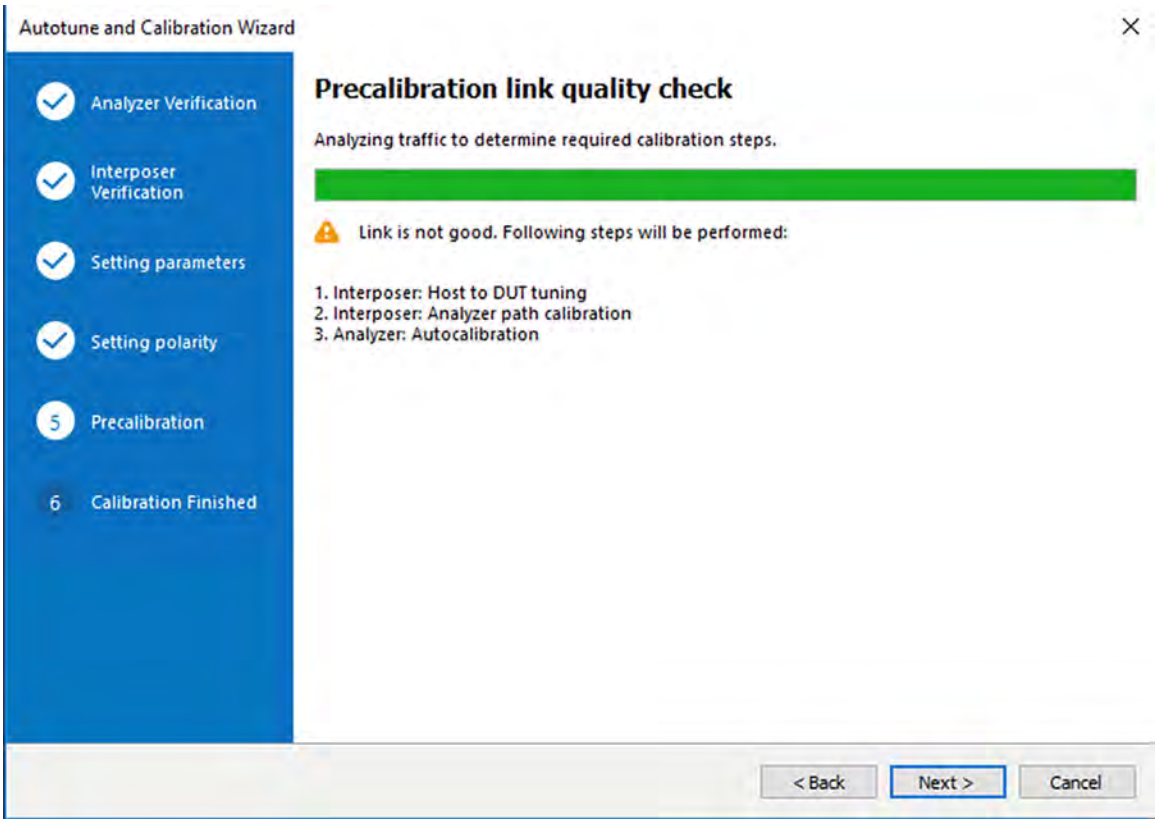


Figure 7.72: Autotune and Probe Calibration Wizard: Step 5 -> Precalibration Link Quality Check

This step check the quality of the link before calibration.

In this case the Link Quality was not good, so the following steps were taken:

- ❑ Interposer: Host to DUT Tuning
- ❑ Interposer: Analyzer path calibration
- ❑ Analyzer: AutoCalibration

To perform the steps outlined above the DUT, Host and operating system must be selected (see Figure 7.73 on page 420).

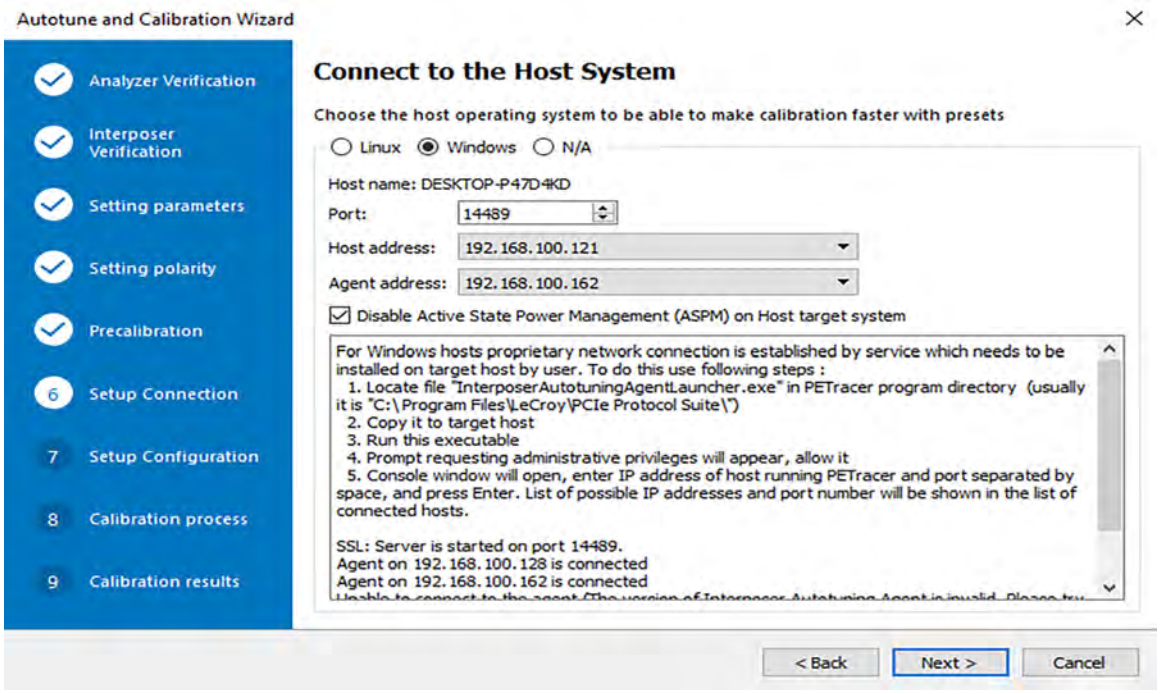


Figure 7.73: Autotune and Probe Calibration Wizard: Step 6 -> Host and DUT Configuration

Once you have selected the DUT, the Host and the Host operating system, click on Next and proceed to the step, which involved connecting to the Host system. See Figure 7.74 on page 421).

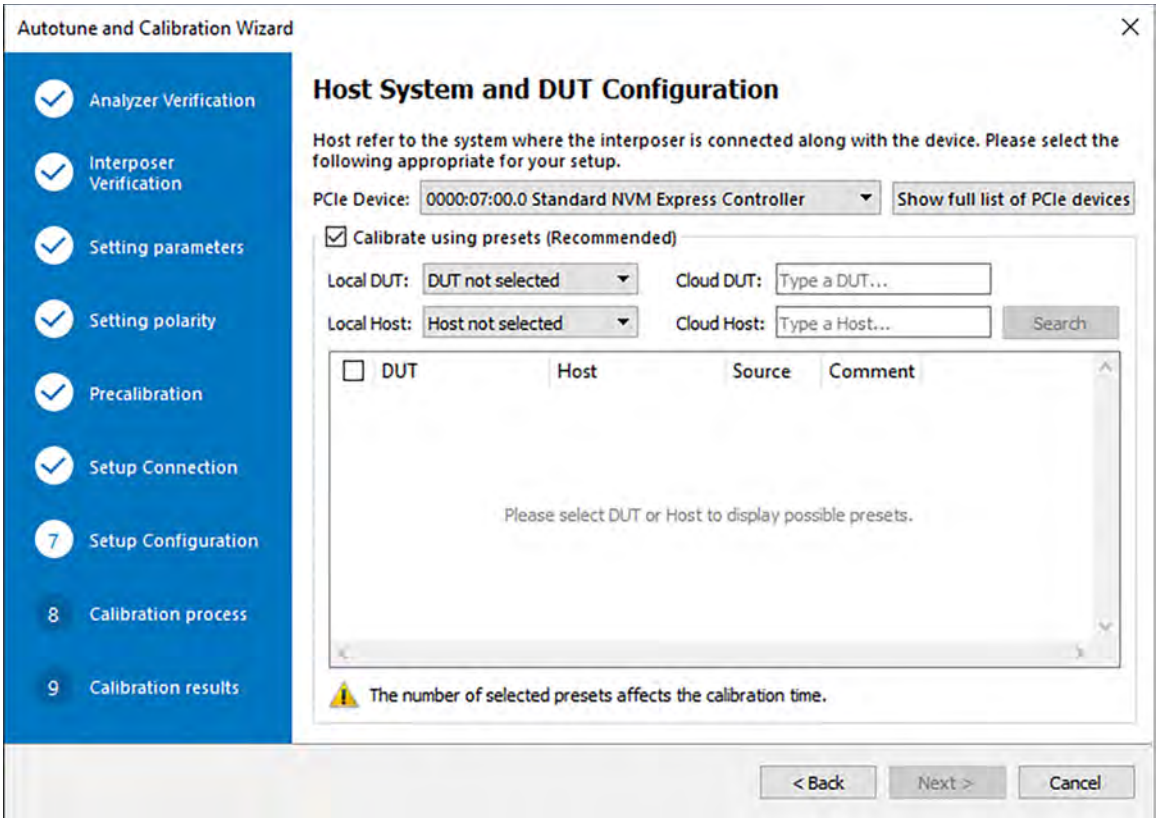


Figure 7.74: Autotune and Probe Calibration Wizard: Step 7 -> Setup Connection

In this step you must enter the Host Name, Port Number and Host IP Address then selct Connect. You must also select the DUT you are using. In this case it is a Standard NVM Express Controller.

Once you have setup the Host and DUT, select Next and the Calibration and Autotuing process will begin. See Figure 7.75 on page 422.

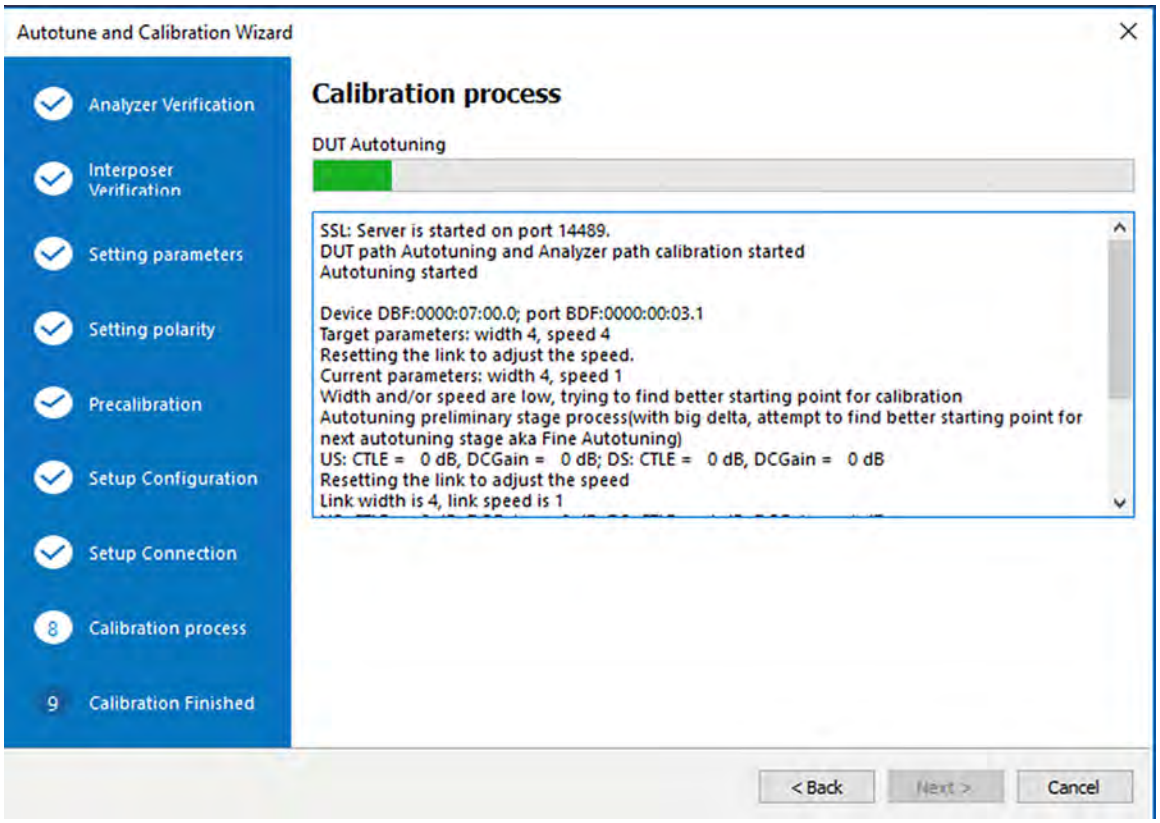


Figure 7.75: Autotune and Probe Calibration Wizard: Step 8 -> Calibration Process

In this step you can see from the log window the Autotuning and Calibration steps being taken by the PCIe Analysis software. After the Calibration process has completed (and this make take awhile), select Next and a dialog box will pop up that shows a link to the Calibration results. See Figure 7.76 on page 423.

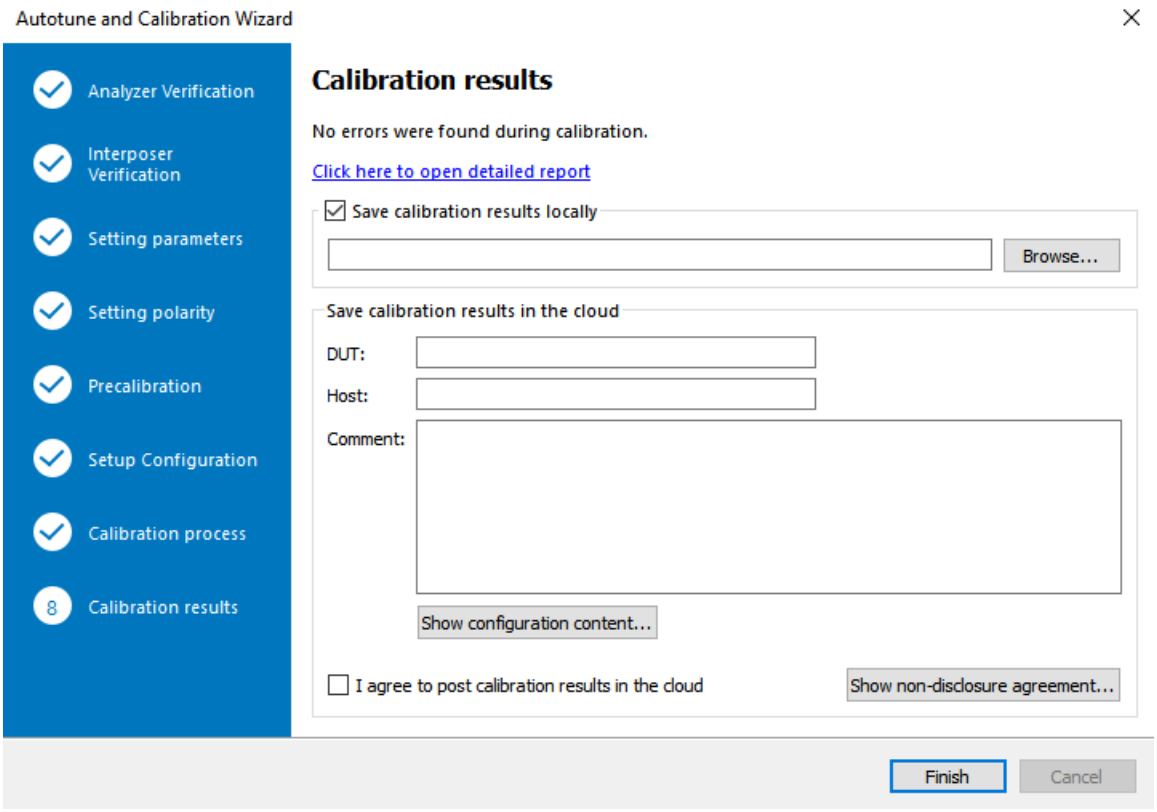
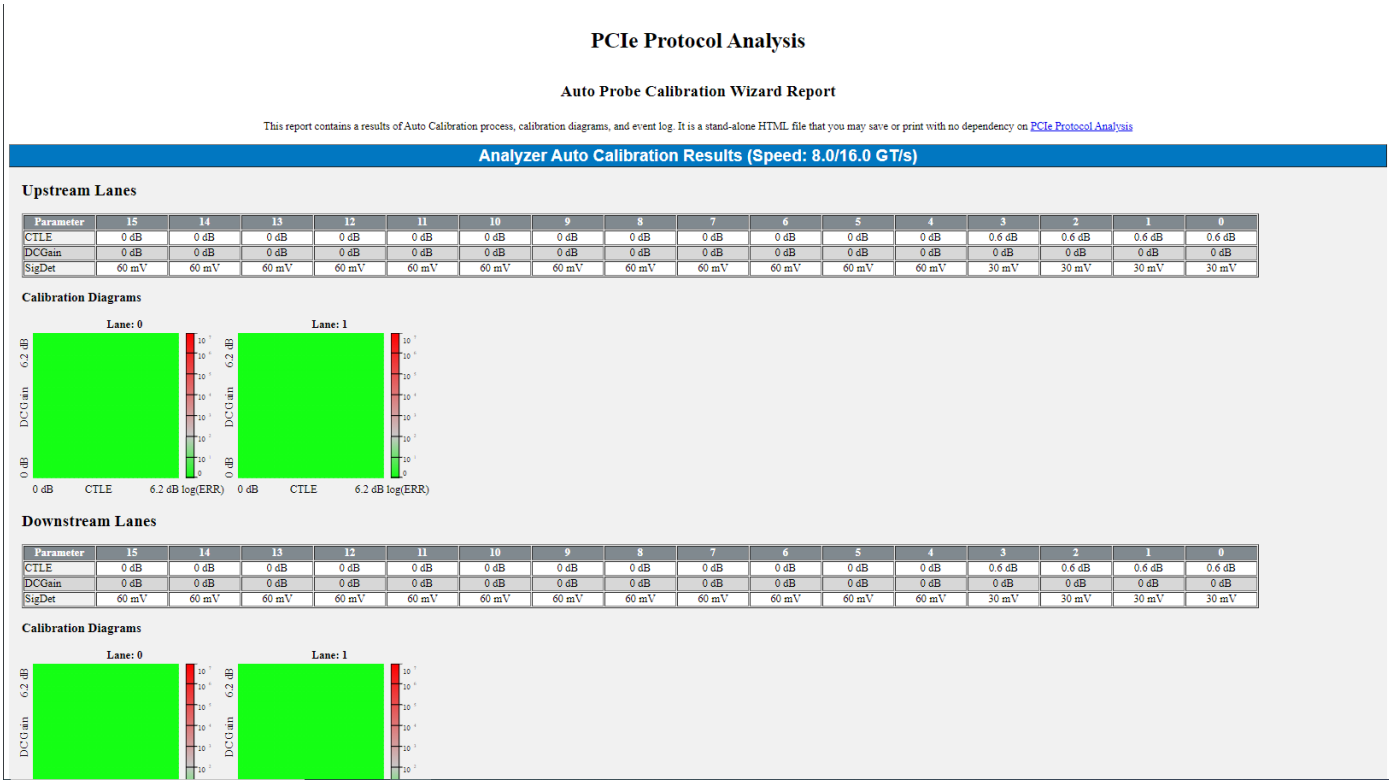


Figure 7.76: Autotune and Probe Calibration Wizard: Step 9 -> Calibration Results

Click on the link to view the Calibration results. See Figure 7.77 on page 424.



PCIe Protocol Analysis

Auto Probe Calibration Wizard Report

This report contains a results of Auto Calibration process, calibration diagrams, and event log. It is a stand-alone HTML file that you may save or print with no dependency on PCIe Protocol Analysis

Analyzer Auto Calibration Results (Speed: 8.0/16.0 GT/s)

Upstream Lanes

Parameter	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
CTLE	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0.6 dB	0.6 dB	0.6 dB	0.6 dB
DCGain	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB
SigDet	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	30 mV	30 mV	30 mV	30 mV

Calibration Diagrams

Lane: 0 Lane: 1

6.2 dB DCGain 0 dB 0 dB CTLE 6.2 dB log(ERR) 6.2 dB DCGain 0 dB 0 dB CTLE 6.2 dB log(ERR)

Downstream Lanes

Parameter	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
CTLE	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0.6 dB	0.6 dB	0.6 dB	0.6 dB
DCGain	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB	0 dB
SigDet	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	60 mV	30 mV	30 mV	30 mV	30 mV

Calibration Diagrams

Lane: 0 Lane: 1

6.2 dB DCGain 6.2 dB DCGain

Figure 7.77: Autotune and Probe Calibration Wizard: Step 10 -> Calibration Results

From the Calibration Report you can see the values used for each lane (Upstream and Downstream):

- CTLE
- DCGain
- SigDet

7.16.5 Interposer Settings for Bifurcated Multiport Link

Currently the only possible option to change the presets of a Bifurcated multiport link is to use the USB connection, to do this the user can bring the dialog by selecting "**Tools -> Interposer Programmer**" (see Figure 7.78).

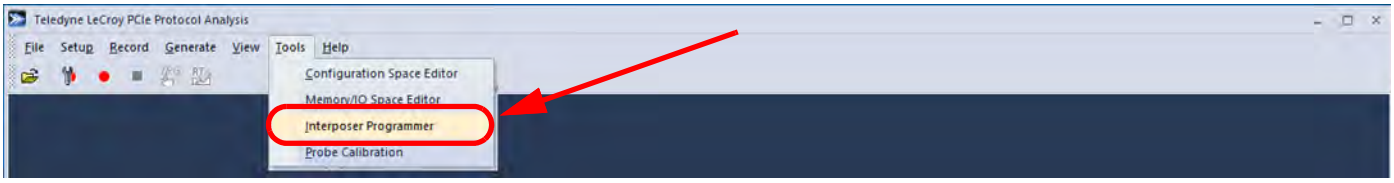


Figure 7.78: Tools: Interposer Programmer

This will bring the dialog with an option to connect the interposer via USB. See Figure 7.79 on page 426.

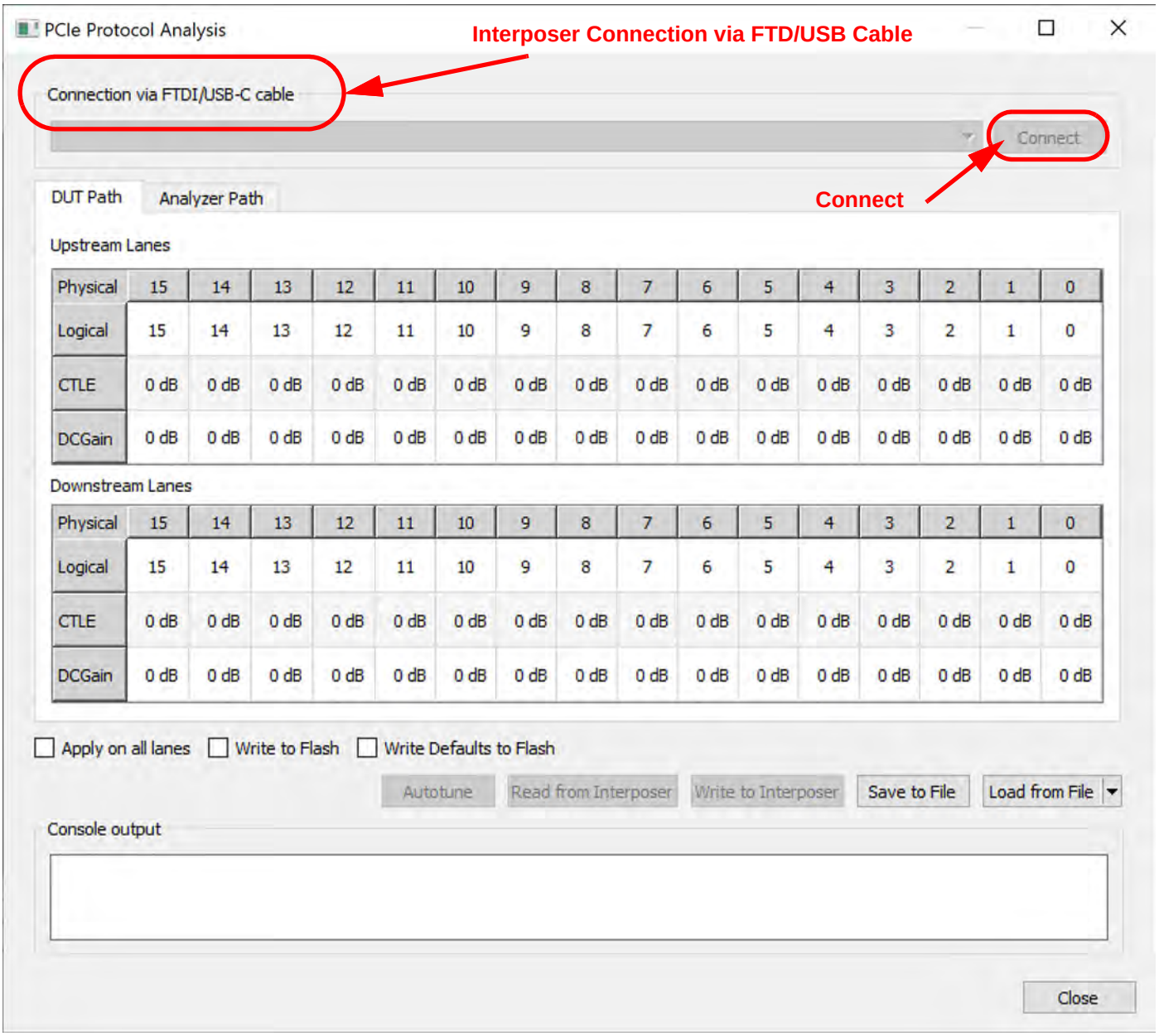


Figure 7.79: PCIe Interposer Programmer Utility

1. Power on the Interposer (if not already powered up).
2. Select the Connect button on the right side of the dialog box. See Figure 7.79 on page 426.

Again, this is only needed for bifurcated link setups and if there is an error on the recoding option dialog i.e. on "Host-To-DUT" tab. The dialog control will work the same as described earlier in the section (“Start auto-tuning process:” on page 392).

7.16.6 Saving Auto-Tune and Calibration Results

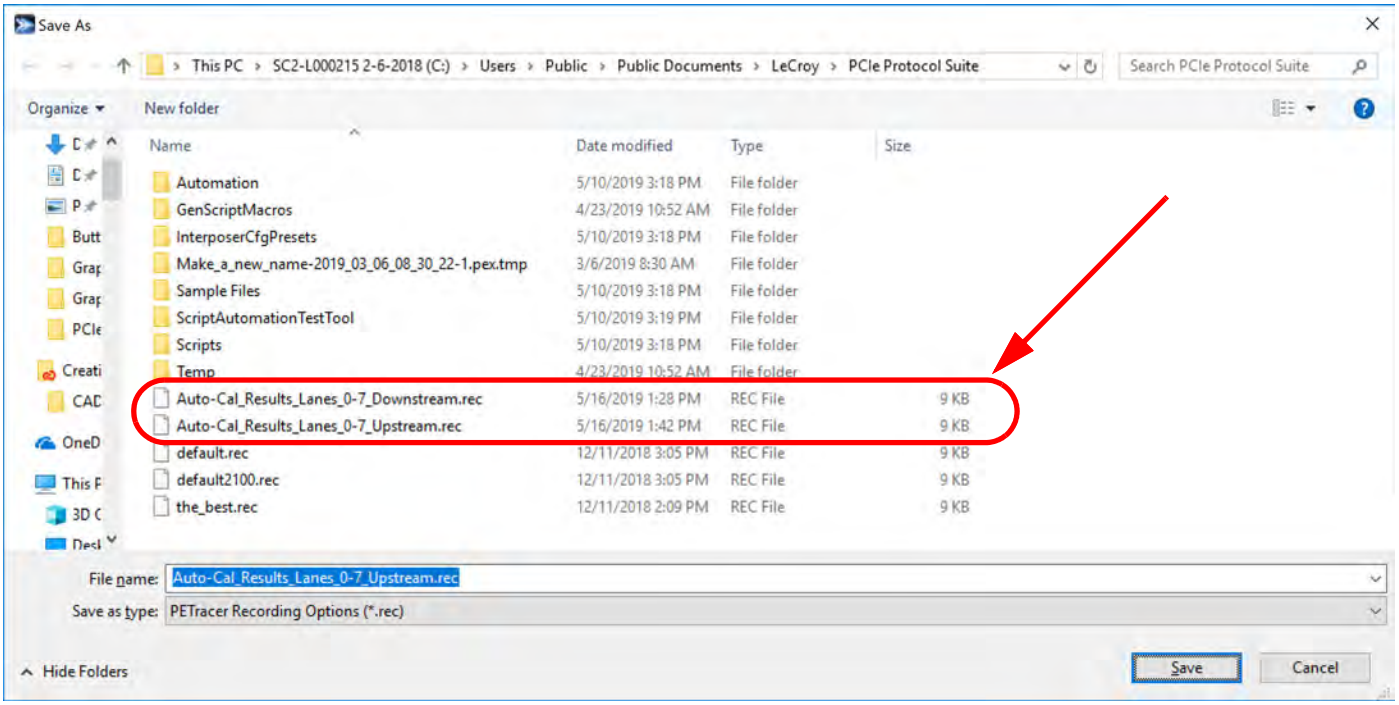
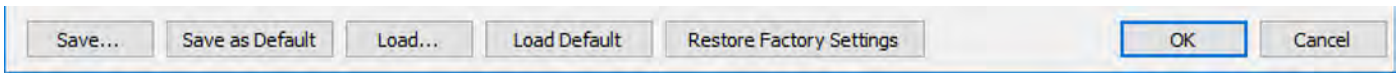


Figure 7.80: Directory ot Saved Auto-calibration Results

You can also Save, Save as Default, Load, Load Default or Restore Factory Settings. See Figure .



Save, Save as Default, Load, Load Default or Restore Factory Settings

7.17 Analysis Options

The Summit M5x Analyzer has the analyzer capabilities described in detailed in Chapter 9, “Reading CATC Traces,” on page 529, Chapter 10, “Searching CATC Traces,” on page 659, Chapter 9, “Display Options,” on page 391 and Chapter 12, “Reports and Tools,” on page 733 except that it’s Link Width is restricted to x8.

7.17.1 Example: Gen5 Trace

The trace below shows Gen5 traffic being recorded. See Figure 7.81.

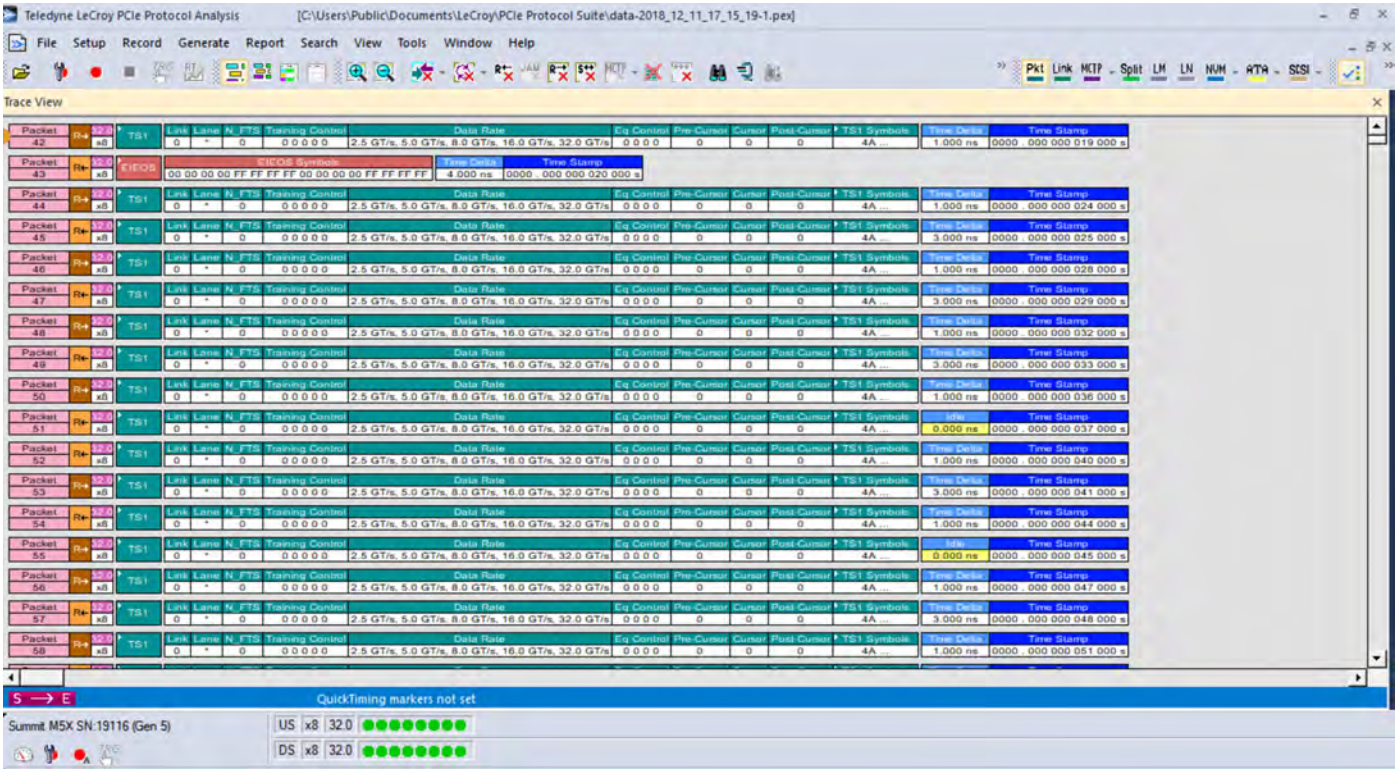


Figure 7.81: Gen5 32.0 GT/s x8 Traffic Being Recorded

A more detailed view of the start of the first few packets is shown in Figure 7.82.

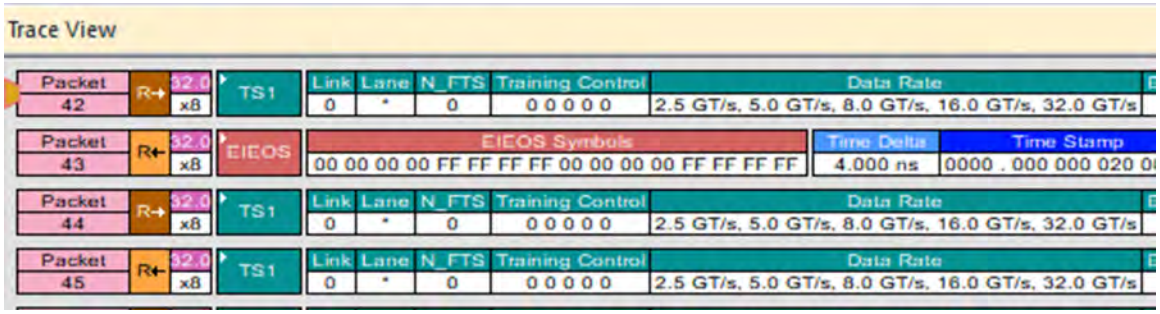


Figure 7.82: Detailed View of First Packets in Trace

The dashboard of the Summit M5x is shown below. See Figure 7.83 on page 428.

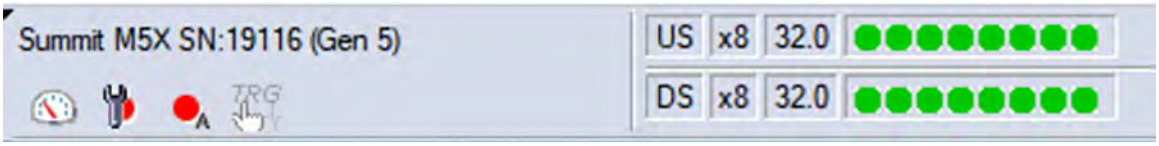


Figure 7.83: Details of Dashboard

7.18 BitTracer Recording

Note: BitTracer Recording is an optional feature.

The Summit M5x analyzer has an optional **BitTracer** data capture mode, which captures bi-directional link traffic in raw format. The BitTracer recording mode captures and displays traffic before lane-to-lane de-skew operations and before descrambling of 10b bytes. The BitTracer mode includes support for multiple logical links (bifurcations) on a single physical link.

The BitTracer recording mode has its own user interface, which provides characterizations of link traffic that are not available in the standard protocol analyzer mode. You can export BitTracer recordings for viewing in CATC Trace format.

Note: This feature can be included at initial purchase or added in the field with a software upgrade license. To obtain a software license key to add this feature, contact Teledyne LeCroy.

7.18.1 Enabling BitTracer Recording

To enable the BitTracer recording mode, open the **Recording Options**.

Select **Summit M5x Analyzer Only** and **BitTracer Recording.**

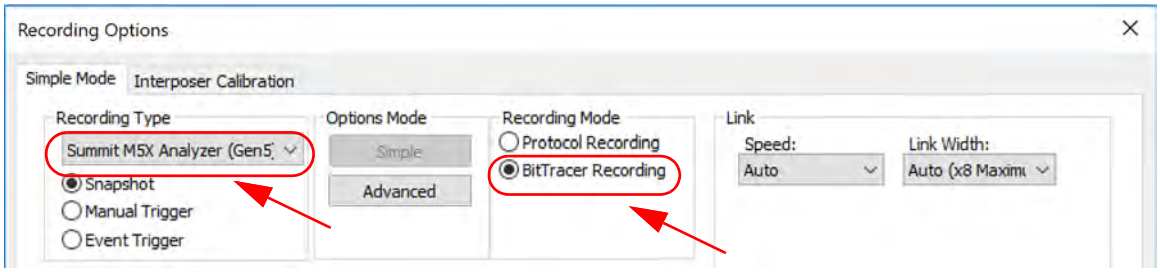


Figure 7.84: Recording Mode: Summit M5x and BitTracer Mode

In Bit Tracer Recording, you can use the Snapshot, Manual Trigger, and Event Trigger recording types.

Note: You can also use other standard Recording Options, such as Link Width, Buffer Size, and Lane Polarity Settings, to characterize the link.

7.18.2 Triggering in Simple Mode

If you select Event Trigger, you may select basic trigger settings in the Trigger On dialog.

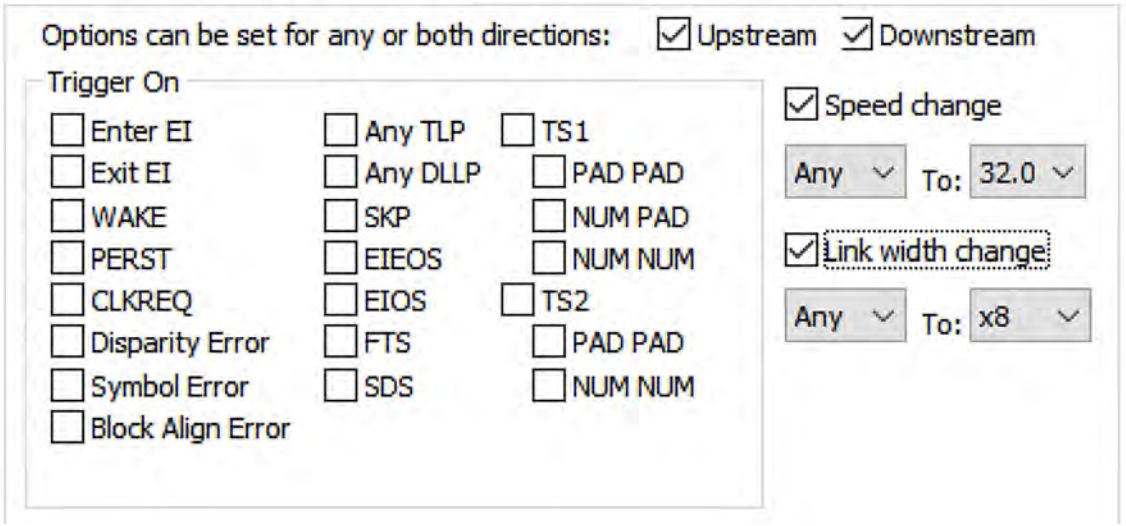


Figure 7.85: Trigger On Dialog

7.18.3 Views Available for Captured Data

BitTracer mode displays captured data lane-by-lane and byte-by-byte in each direction (upstream and downstream), with the time scale progressing left to right.

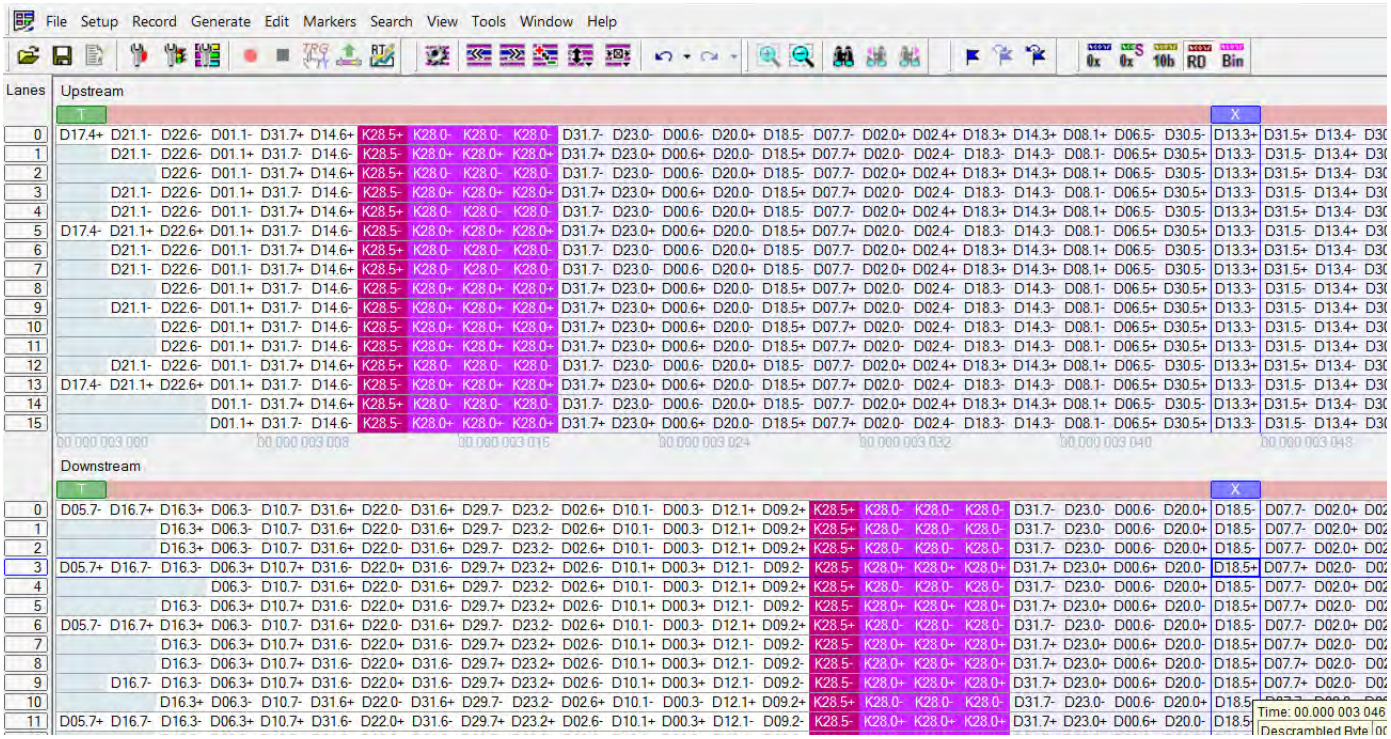


Figure 7.86: Captured Data

Other views are provided for timing measurements, marker placement, physical layer errors, captured symbol types, packets, events, and decoding of ordered sets and packets. You can view any or all displays simultaneously, using the **Windows** selection in the View menu.

7.18.4 De-skewing Data

By default, BitTracer recordings display captured data in time de-skewed format, across all lanes for both directions. When lanes are not de-skewed, individual bytes are as they were captured on the recorded link, before the receiver device on the link (or the receiver logic on the PCIe Protocol Analysis analyzer) has performed lane-to-lane de-skew operations. You can manually skew the captured data, left or right, in increments of one symbol time using the associated toolbar buttons. See Figure 7.87 on page 431.

Note: For Gen3, you can manually skew the captured data by: left or right, in increments of 1 bit using the associated toolbar buttons.

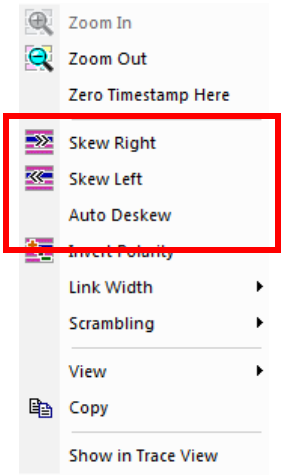


Figure 7.87: Skewing Data

You can automatically de-skew an entire lane direction. First, left-click on the direction in the data window. Then right-click to display a popup menu. Then select **Auto De-Skew.**

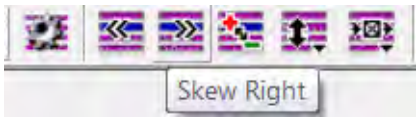


Figure 7.88: De-Skew Data

You can de-skew only one direction for each right-click operation. To automatically de-skew the opposite direction, first left-click on that direction in the data window.

Note: The skew observed in the bit tracer is the actual skew of the lanes in the link plus the skew introduced by the analyzer interface. The De-skew Bypass option is not intended for skew measurements or estimations.

7.18.5 Data Display Formats

To display traffic in K/D symbol (with Running Disparity indicated), scrambled, descrambled, 10-bit, and Binary code formats:

- Use the toolbar.

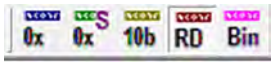


Figure 7.89: Data Formats

- Right-click to display a menu.
- Place the cursor over any given byte to display all byte formats (including an LFSR value) in pop-up list.

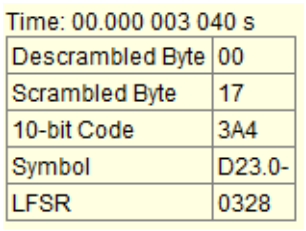


Figure 7.90: Pop-up List

Note: Descrambled values can only be displayed after the first recorded skip ordered set. Data prior to the skip is displayed in scrambled values, due to the unknown LFSR.

For Binary Data Display Format, bits are shown in order of transmission on the bus.

7.18.6 Color-Coding of BitTracer Contents

To increase visual understanding of BitTracer displays, different symbol types have color-coding:

- Presence or non-presence of a lane's byte-lock
- Idle data characters (D0.0)
- K codes
- Invalid 10b symbols
- Signal presence
- Background of the Markers Bar (see "Markers/Speed Bar" on page 433). (color coded according to traffic speed).
- All symbols of a TS1/TS2 ordered set

By default, these color selections match the standard color selections used in the CATC Trace format. You can modify them in the Display Options menu, accessible from the Main toolbar or the Setup menu.

7.18.7 Report and Analysis Windows

In the report windows, BitTracer mode provides several functions to analyze traffic:

- Statistical information
- Timing measurements
- Packet decoding

To activate/deactivate a report window, use **Views > Windows,** see Figure 7.91 on page 433.

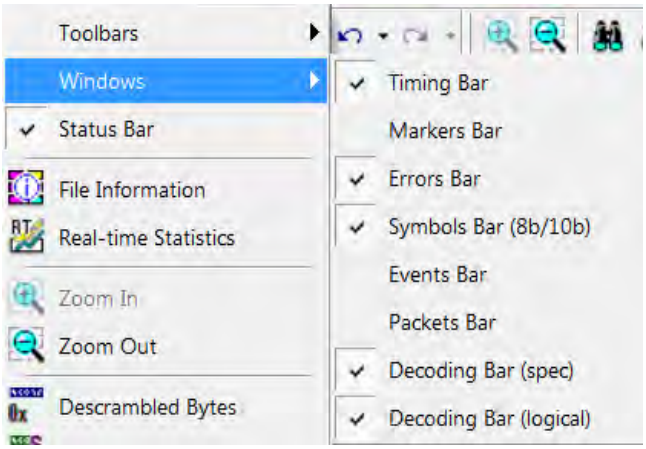


Figure 7.91: Activate/Deactivate Reports

You can rearrange the report windows.

All report windows are dockable.

7.18.8 Timing Measurements Bar

BitTracer mode provides timing measurements on captured data:

- Measurements from the Trigger position relative to user-selected X and Y markers
- X-Y measurements
- Measurements between user-defined markers

7.18.8.1 Markers/Speed Bar

Markers are displayed in the speed bar above the data. Place your cursor in the speed bar and the Current speed will be displayed. In this case, the traffic was running at 5.0 GT/s when the trace was taken. See Figure 7.92.

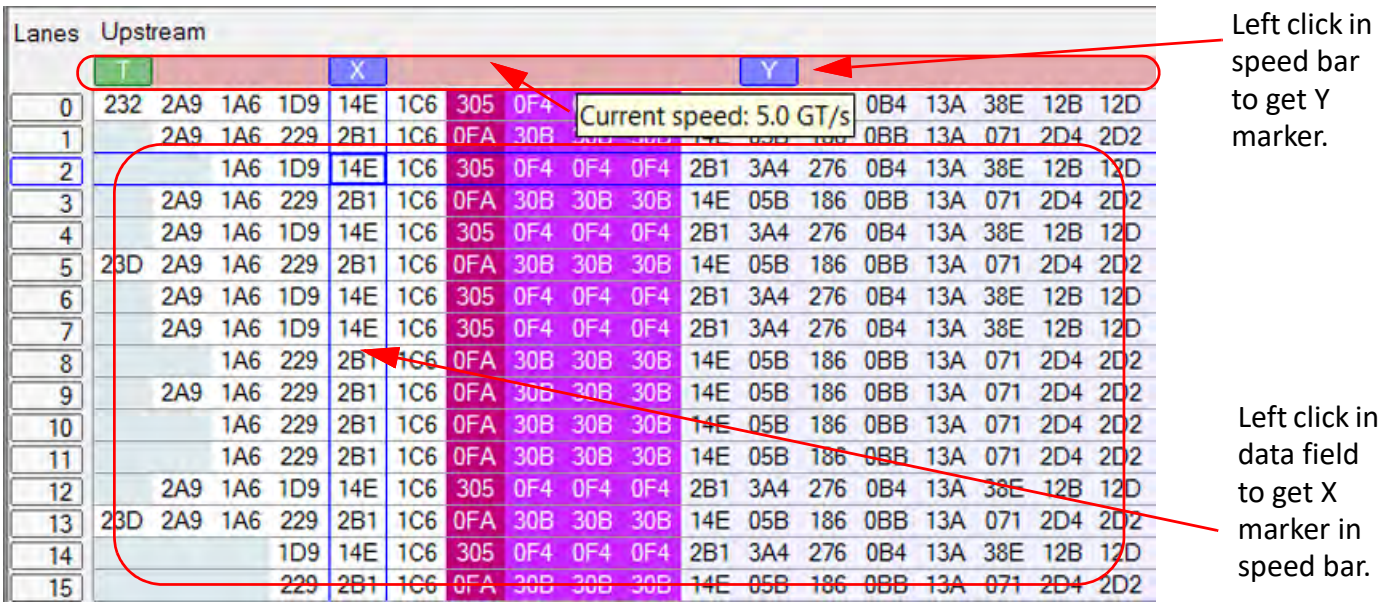


Figure 7.92: Marker/Speed Bar Example

The Trigger marker T is at the point where BitTracer recognized the user-defined trigger condition.

To set an X marker X, left-click anywhere in the data display, see Figure 7.92.

To set a Y marker Y, left-click in the narrow speed bar where the T and X markers are displayed. See Figure 7.92.

7.18.8.2 Defining a Marker

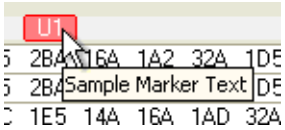
To define a marker, select the **Set Marker** command in the Markers menu or use the **Toggle Marker** icons in the toolbar. You can also use the Jump to Next or Previous marker icons in the toolbar.



User-defined markers are numbered in the order they were placed:

- U1 U1, U2, and so on in the upstream direction
- D1, D2 D2, and so on in downstream direction.

You can set a marker with text using the **Set Marker with Text...** command in the Markers menu. After setting the marker, when the mouse pointer is on the marker symbol, the marker text displays as a tooltip.



You can also display the Markers window, which lists all markers and their locations, including a hyperlink for each.

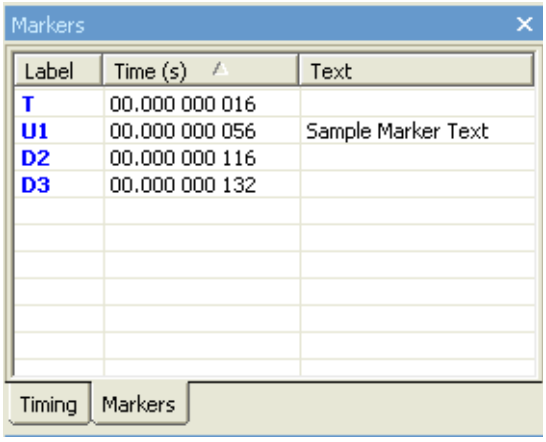


Figure 7.93: Markers Window

Timing measurements between all combinations of X, Y, U, and Trigger cursors are in the Timing window. See Figure 7.11 on page 344.

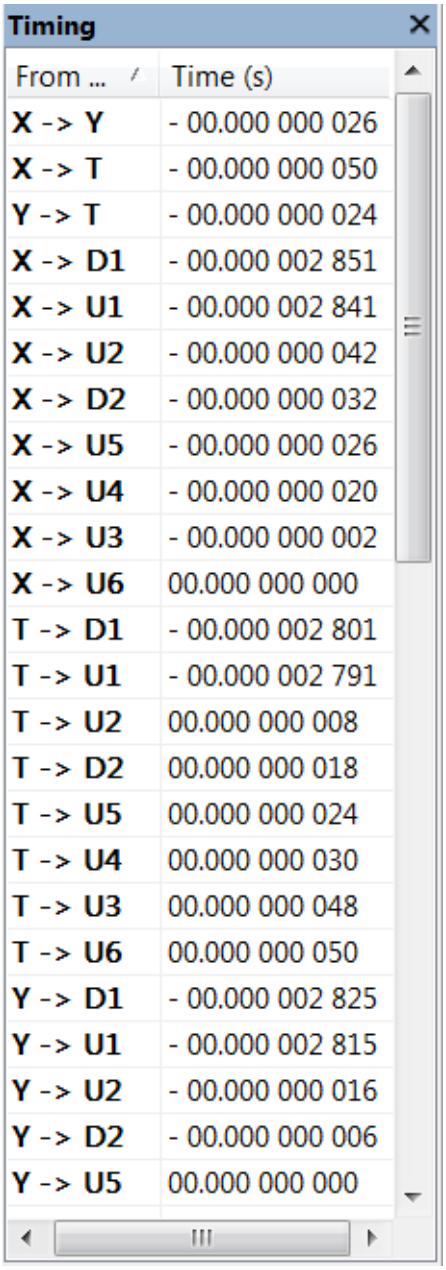


Figure 7.94: Timing Window

7.18.9 Errors Bar

BitTracer mode provides a summary of 10b errors (invalid symbols) and disparity errors in the Errors window. The window shows the total error count and errors per-lane for each error type. Hyperlinks allow jumps to selected errors. See Figure 7.12 on page 344.

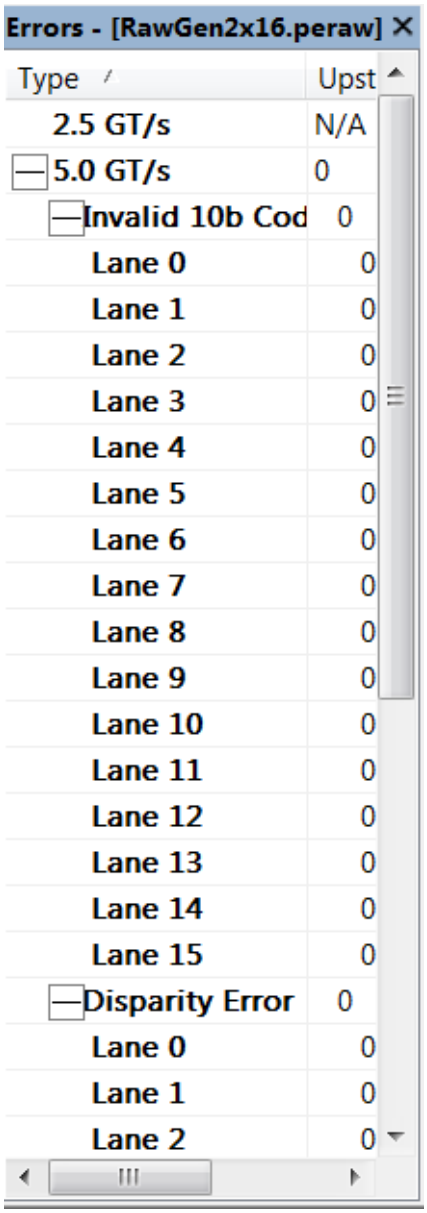


Figure 7.95: Errors Window

BitTracer mode also highlights errors:

- Invalid symbols have a black background.
- Bytes with incorrect running disparity have red borders.

7.18.10 Symbols Bar

The Symbols window provides a summary of the different symbol types captured, by quantity and direction, and includes hyperlinks for jumps to selected symbols.
Expanding the + sign at the left of each symbol provides a summary of symbols by lane.

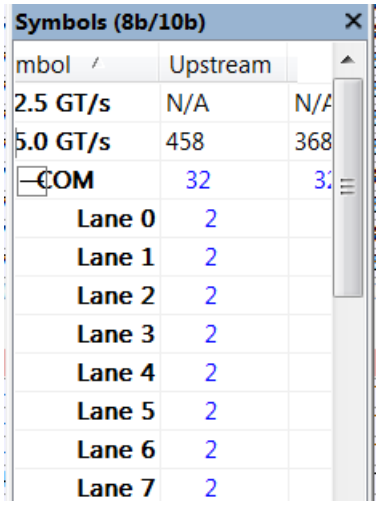


Figure 7.96: Symbols Window

7.18.11 Events Bar

The Events report window summarizes Link Up, Link Down, and Speed Switch events for Upstream and Downstream.

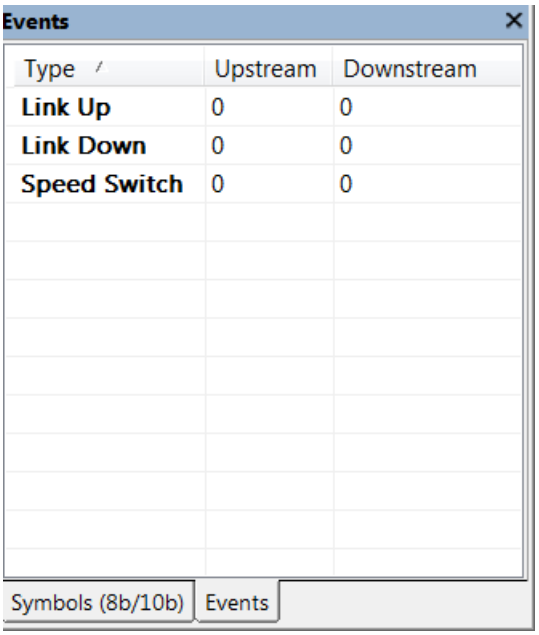


Figure 7.97: Events Window

Note: The table entries are hyperlinks.

7.18.12 Packets Bar

The Packets report window summarizes packet types detected in the file.

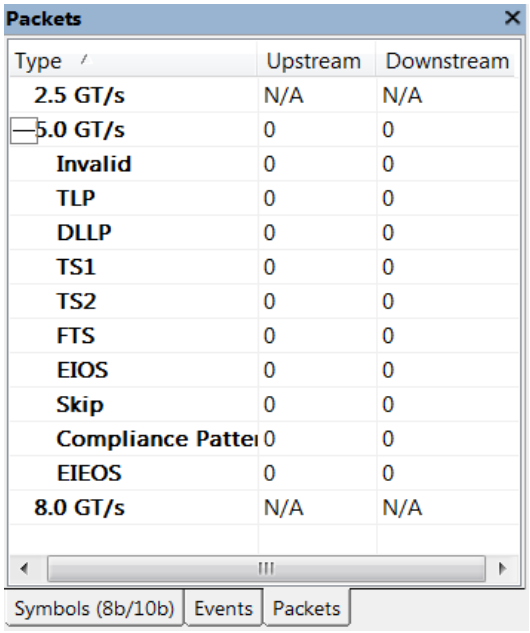


Figure 7.98: Packets Window

Note: To obtain packet types, you must perform a post-capture "Analyze" step. After capture, when you open the Packets Bar for the first time, items can display the command "Analyze". To start the analysis, click the word Analyze. After analysis finishes, the results are saved with the file. Therefore, you do not need to click Analyze the next time.
The table entries are hyperlinks.

If you edit anything, the results are no longer valid, and the system requires you to click Analyze again.

After analysis, the Packets Bar looks like the following (see the following figure):

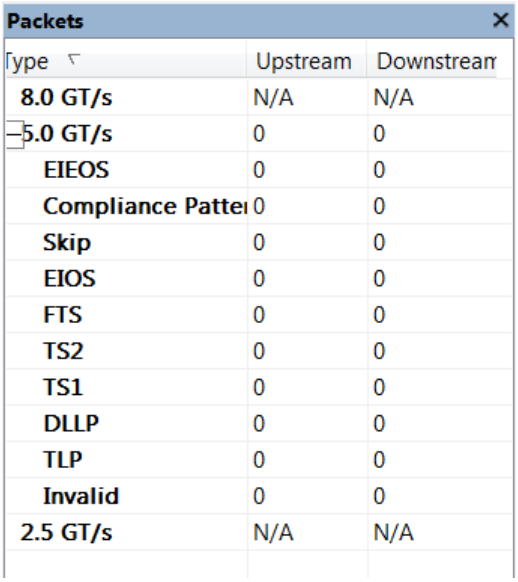


Figure 7.99: Packets after Analyzing

7.18.13 Decoding Bar

If you select them in the data view, or search or jump locates a feature, BitTracer mode displays ordered sets and packets in the Decoding dialog (see Figure 7.100 on page 441).

- **Logical view** is identical to CATC Trace format.
- **Specification view** provides a more elementary display. The Specification view includes an option to display data in hex or binary format.

Note: Packets and ordered sets translate directly to this view from data capture and use any post-capture skew manipulations you add, or use natural lane-to-lane skew present on the link if you have not added post-capture skew manipulations. Typically, you would perform an Auto De-Skew before viewing ordered sets and packets in this view.

Use the left and right arrows to search for the next or previous symbol type.

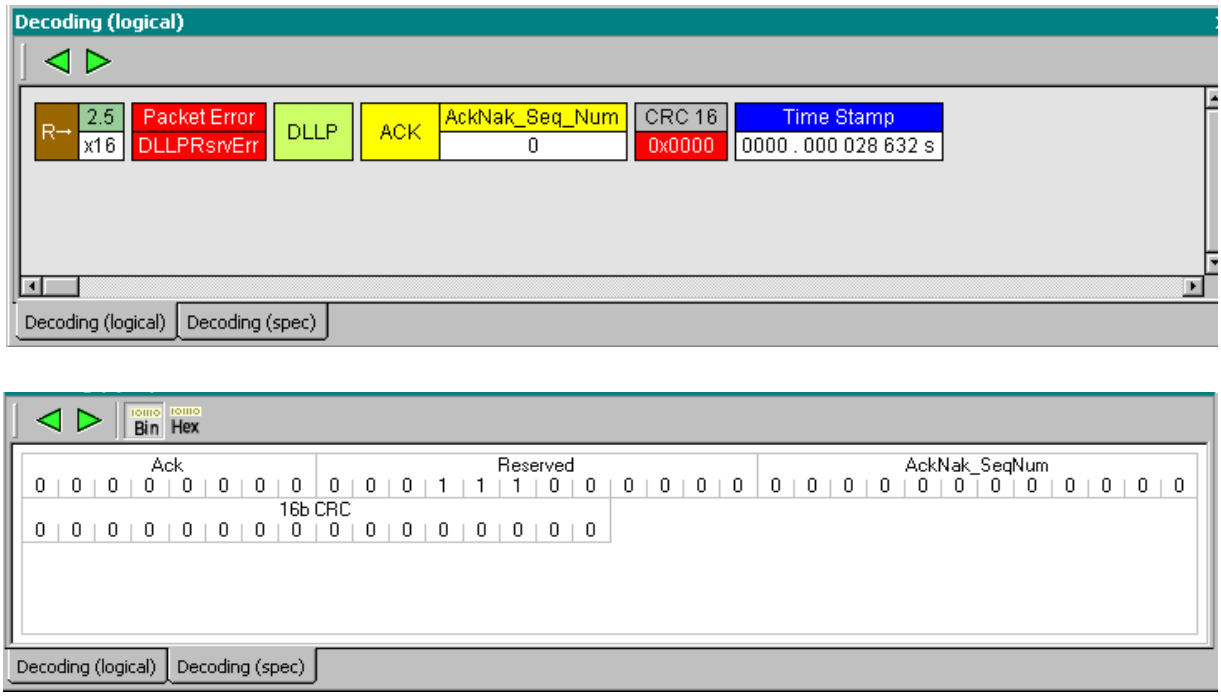


Figure 7.100: Decoding Dialog

7.18.14 Search

To search, use the Search toolbar.



Clicking the **Search** icon displays the Search dialog (see Figure 7.101 on page 442).

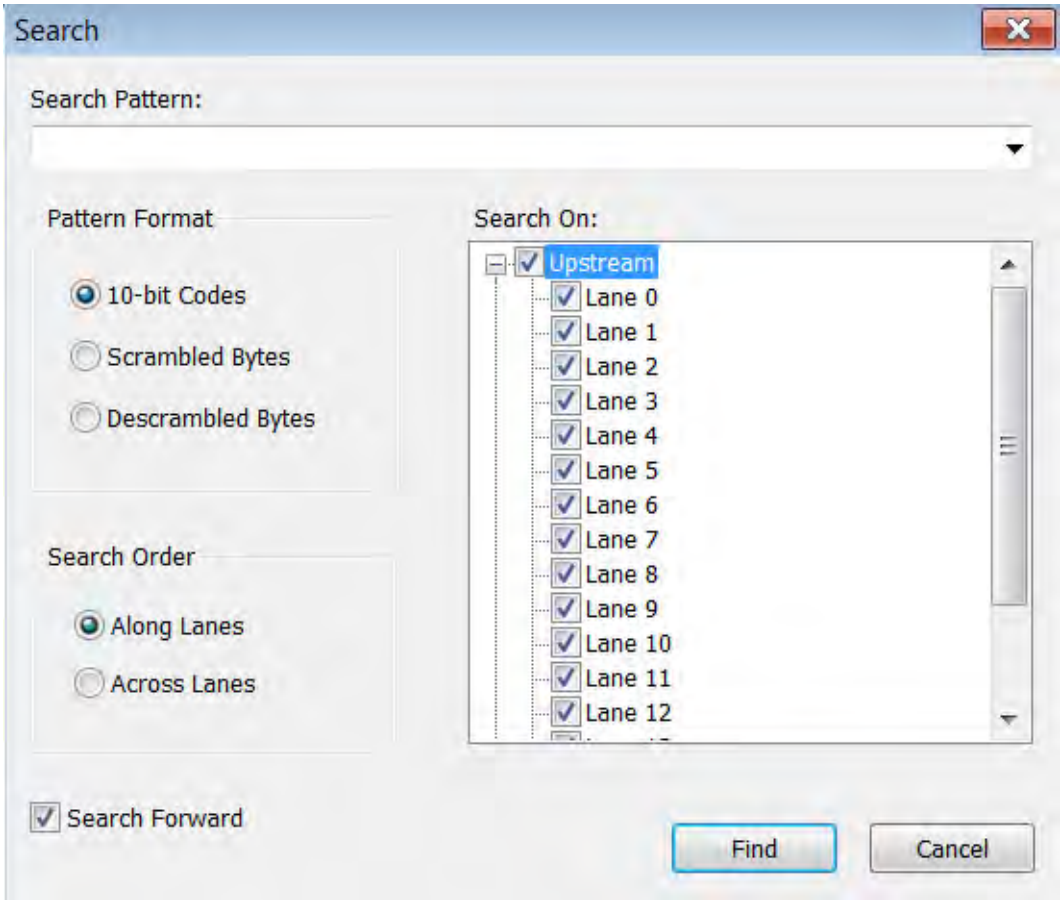


Figure 7.101: Search Dialog

You can copy data shown in the BitTracer display across a lane (horizontally) or across multiple lanes (vertically), and then paste it into the Search Pattern window.

The Search Pattern window stores previous search values, which you can recall by selecting the Search Pattern drop-down button.

In the Pattern Format section, select to search in 10-bit Codes, Scrambled Bytes, or Descrambled Bytes format.

In the Search Order section, select to search Across Lanes (multiple lanes, vertically) or Along Lanes (individual lanes, horizontally).

To define the direction (upstream or downstream) and the lanes on which to search, use the Search On section.

7.18.15 Link Configuration

Use the toolbar icon or right-click in the data views to display the Link Configuration dialog (see the following figure). This dialog allows you to associate logical lanes with physical lanes, thereby providing support for lane bifurcation (multiple logical links on the same physical link).

After logical lanes map to physical lanes, BitTracer mode reconfigures the display to show the selected logical link (and the logical link width, as the link width selected in the dialog).

Use the arrows to force symbol time skew on any lane.

Use the polarity checkbox to invert lane polarity on the selected lane or use the **+/-** toolbar icon.



Use the scrambling option to select a scrambling algorithm, as per specification 1.0a or legacy specification 1.0.

Select **Edit > Edit Link** or click the  icon to display the Link Configuration for Upstream dialog (see Figure 7.102).

Note: This dialog applies to one direction at a time (upstream or downstream). Left-click in the direction in the data display to edit the configuration for that direction.

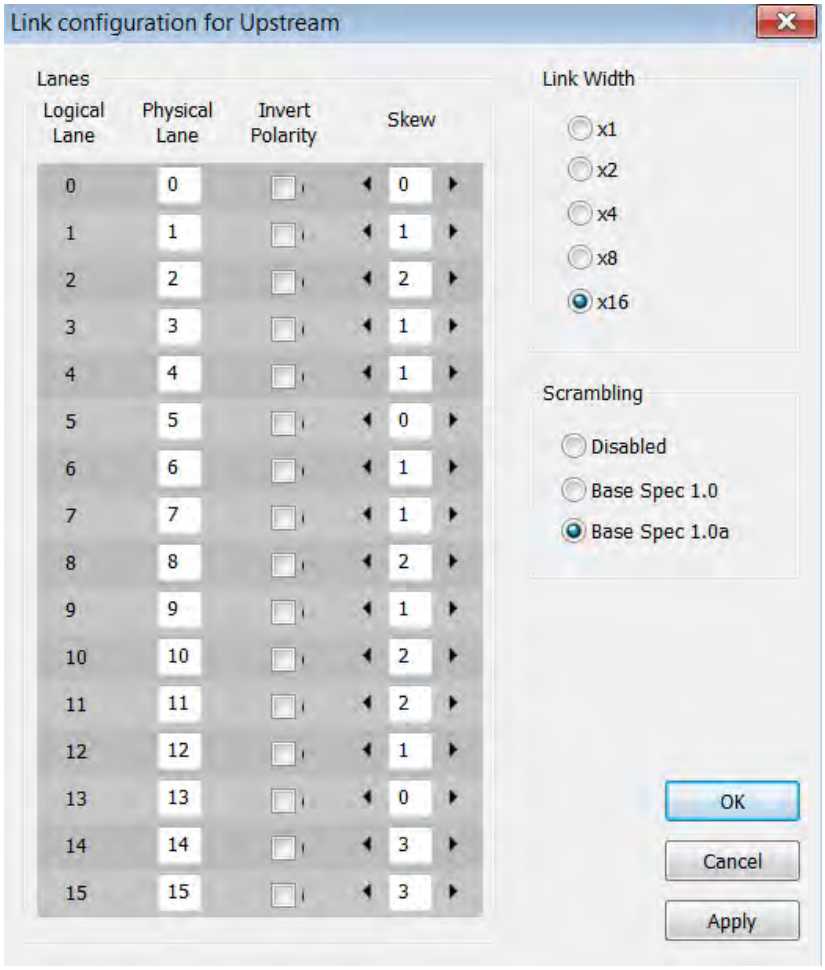


Figure 7.102: Link Configuration for Upstream Dialog

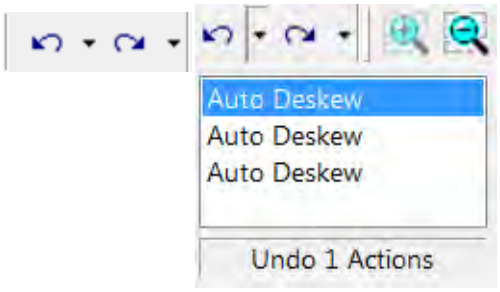
As you perform operations that affect display configurations, the application records them. To undo or redo operations, use the Undo and Re-do icons on the toolbar.

7.18.16 Export of BitTracer Capture to CATC Trace Format

You can export BitTracer captures to standard CATC Trace file formats, selecting the **Export** option from the File menu.

Note: If the bit trace is not deskewed, you should use the Auto De-skew feature before using the export feature.

.



The exported CATC Trace keeps association information with the original BitTracer file. Such traces scroll synchronously when you select the **Synchronize Traces** option in the Windows menu.

You can navigate between BitTrace and CATC Trace using the **Show in Trace View/ Show Packet in Raw Trace** context menu.

7.18.16.1 Exports Involving Multiple Logical Links on One Physical Link

If a single BitTrace capture contains more than one logical link, you can export each logical link to CATC Trace format. You may then cascade or tile the various BitTracer exports, which then scroll together in linked fashion, along with the original BitTracer file. The Export dialog provides options to export a limited range within the BitTrace capture and to automatically open the exported capture in CATC Trace format.

7.18.16.2 Export To CSV Text

Select **File > Export > Packets to CSV Text** to display the Export Packets to comma delimited text dialog. Select desired options from the From and To Segment, Marker and Time drop-down lists (see Figure 7.103 on page 445).

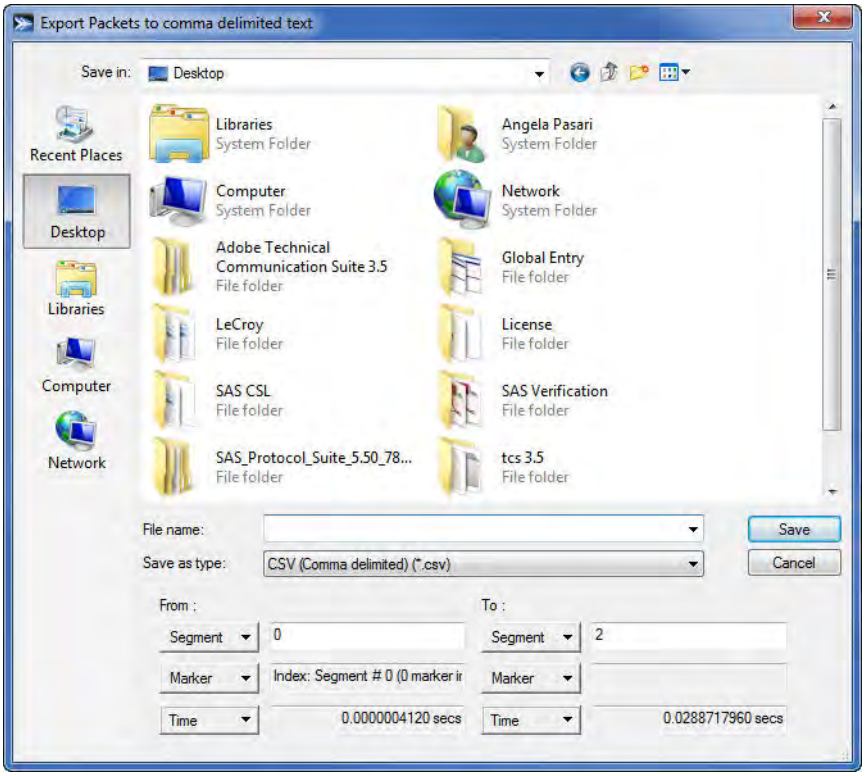


Figure 7.103: Export Packets to Comma Delimited Text Dialog

7.18.16.3 Exporting Data from Bit Tracer to a Trace File

Matching Link Width

Note: To export data correctly from Bit Tracer to a Trace file the Link Width of the recorded data traffic must match the Link Width of the Trace. If the Link Width is altered the result will be a Trace with errors in it.

In the example below, a raw data file is loaded with a recorded Link Width of x8 (see Figure 7.104).

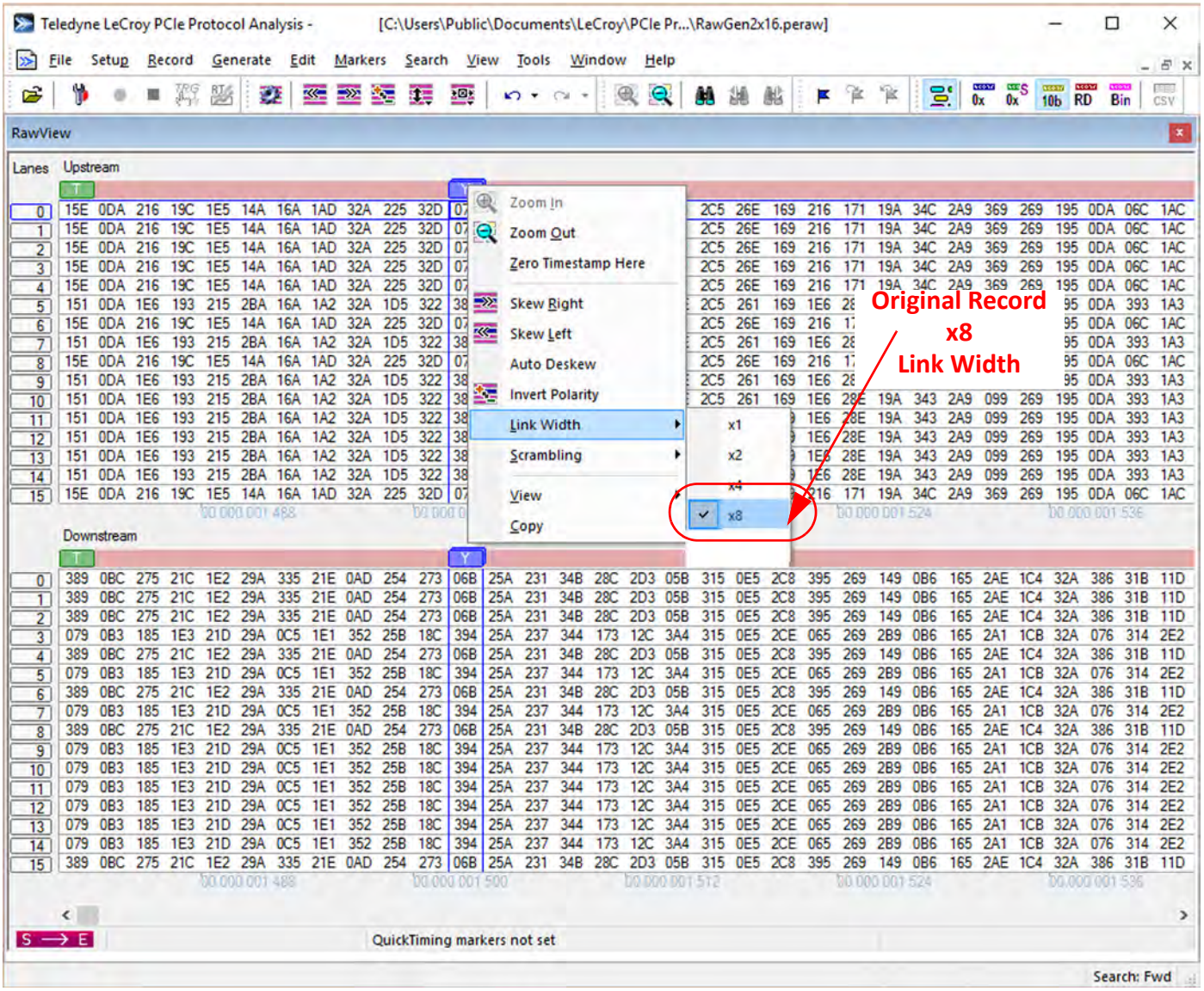


Figure 7.104: Raw Data File Loaded with x16 Link Width

Then the Raw Data File is Exported to Trace (see Figure 7.105 on page 447).

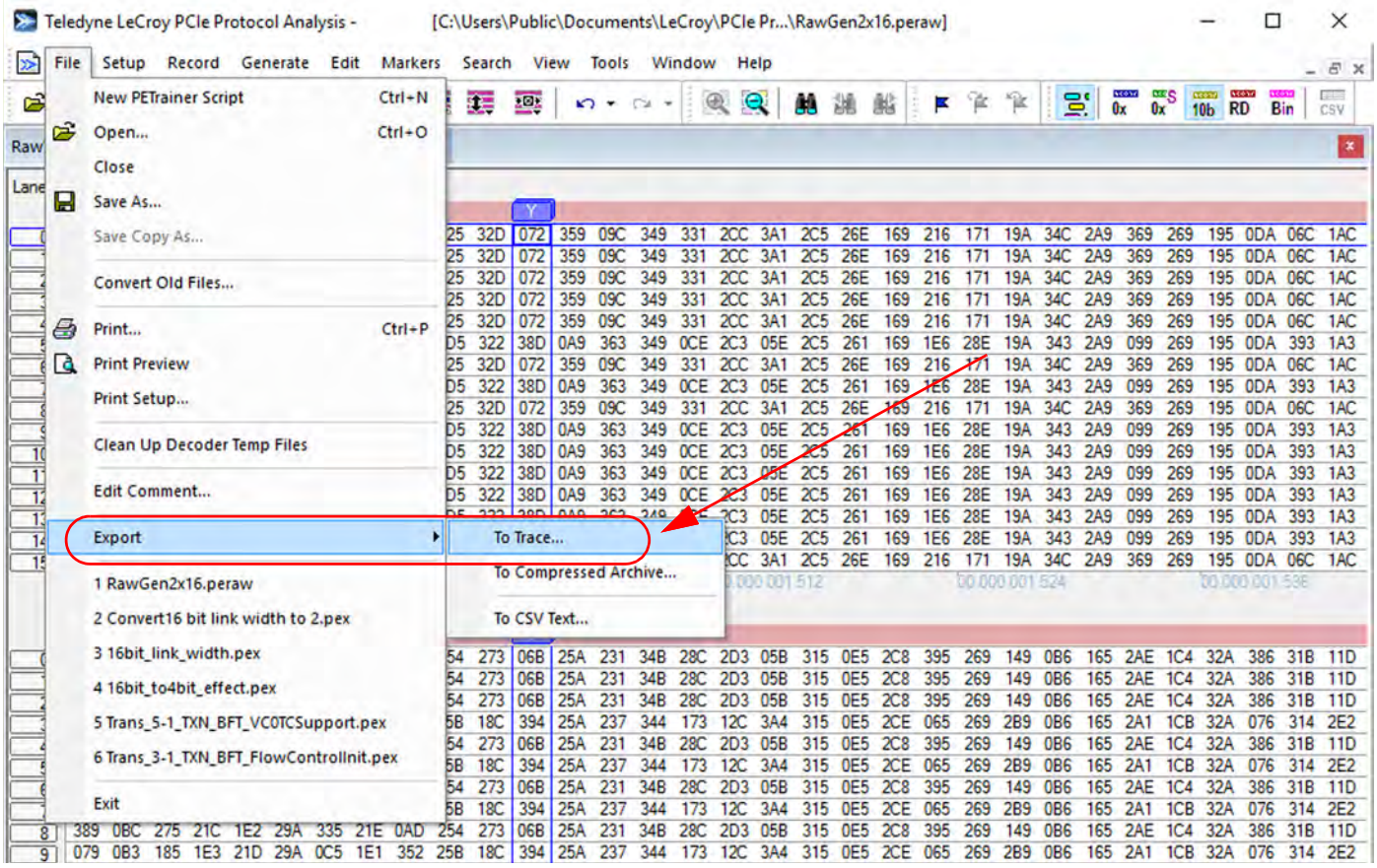


Figure 7.105: Raw Data File Exported from Bit Tracer to Trace File

The resulting trace file shown in CATC View (see Figure 7.106 on page 448).

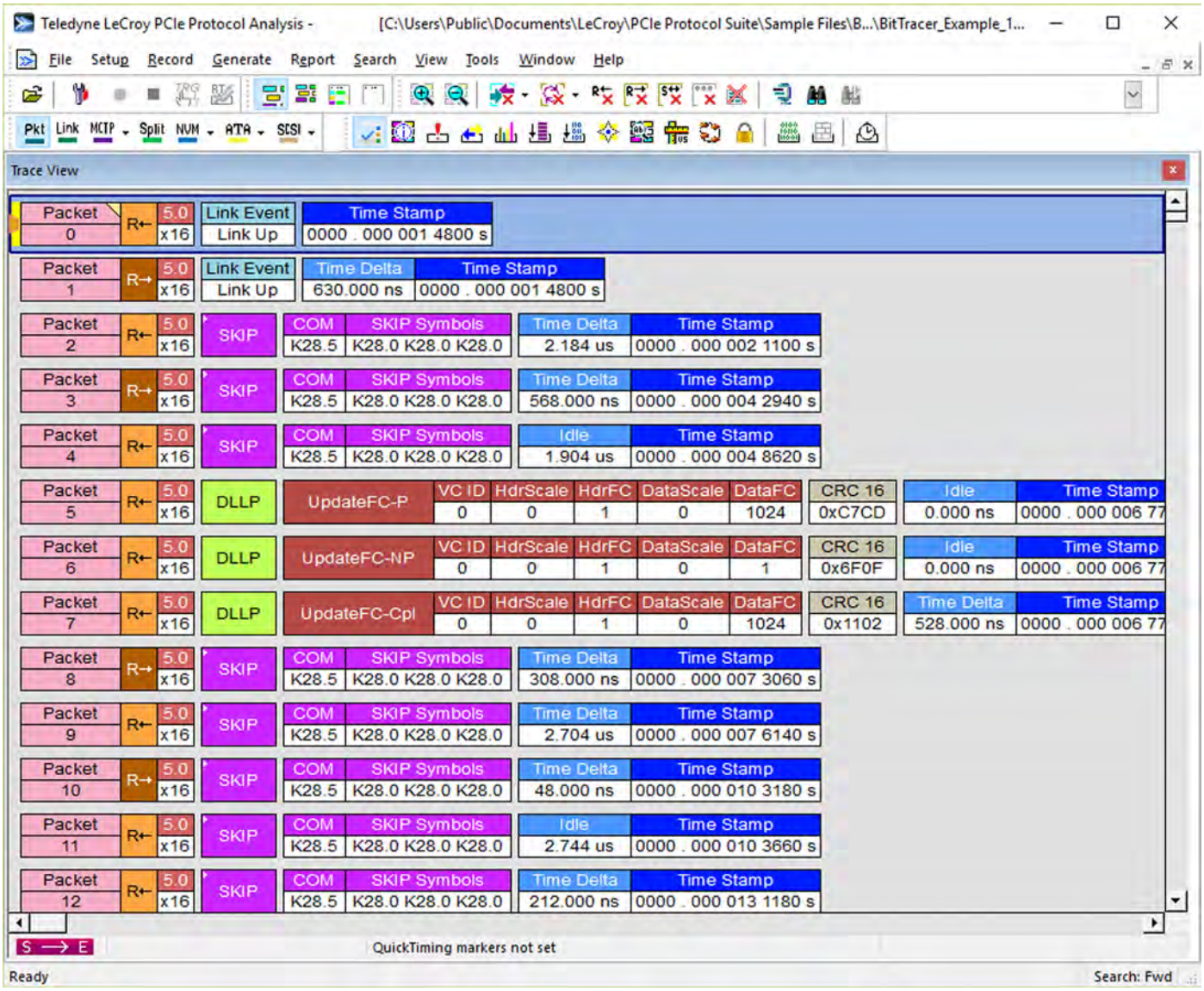


Figure 7.106: Exported Trace File from Bit Tracer

Changing Link Width from Original Recording

If you change the Link Width of the data traffic from the original recording and Export that data traffic to a Trace, the Trace will be decoded with errors. See Figure 7.107 and Figure 7.108 on page 450.

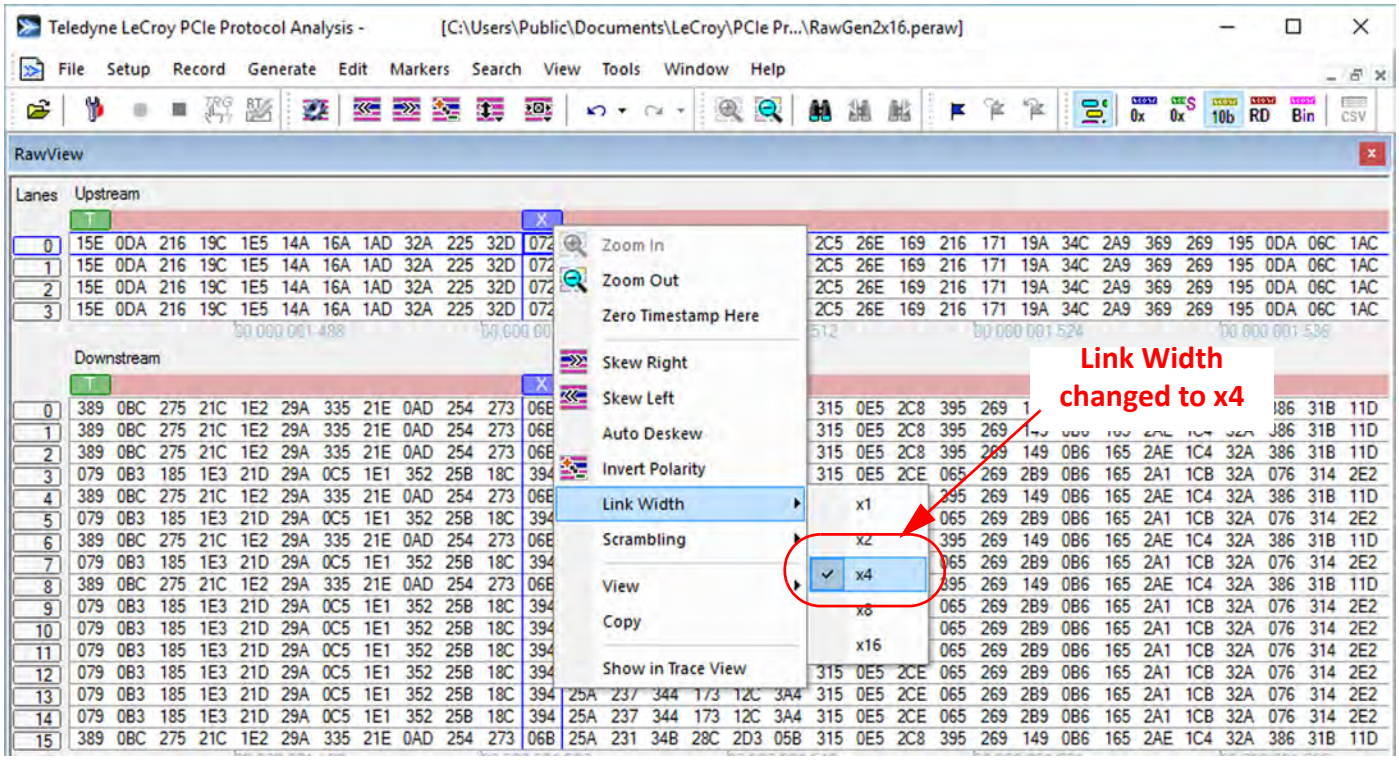


Figure 7.107: Link Width Changed From x16 to x4

Exporting the Data Traffic to a Trace will result in decoding errors (see Figure 7.108 on page 450.

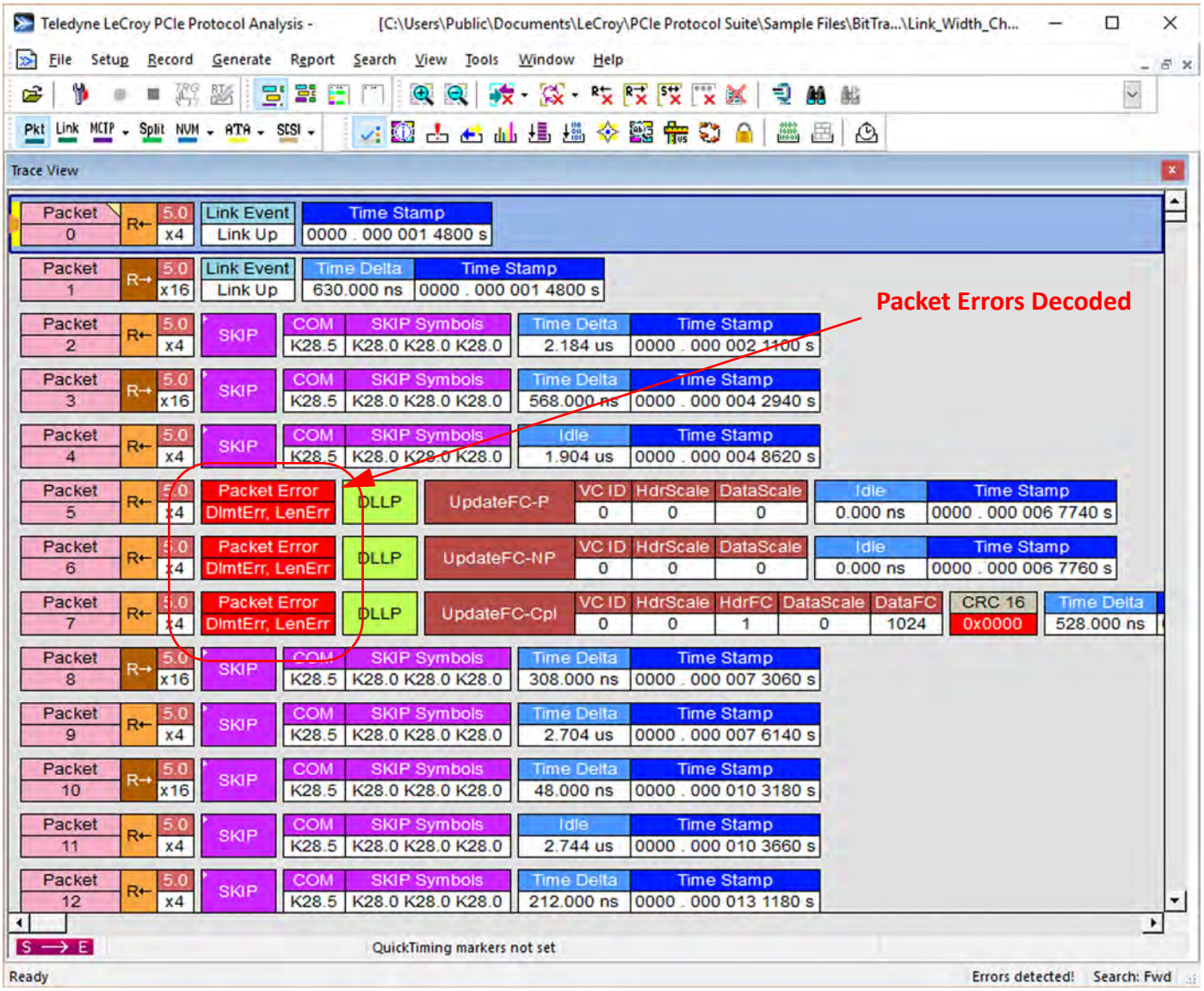


Figure 7.108: Export Data File with Changed Link Width (from x16 to x4)

7.18.17 Compressing and Expanding the Data View

You can compress (zoom out) the horizontal timing of the displayed data to view higher-order link behaviors. You can expand (zoom in) to examine higher-resolution views.

To zoom in or zoom out, right-click the data view, then select a command or select a zoom icon on the toolbar.



Alternatively, to zoom in, left-click and drag across a desired range of data.

7.18.18 Opening and Saving BitTracer Captures

You can save BitTracer captures in various file types.

You can collate and archive these files for transport, using the **Export to Compressed Archive** feature in the File menu.

The main BitTracer files have a ***.peraw** extension.

You can open these files in the PCIe Protocol Analysis application using the **File > Open** command.

Chapter 8

Jammer Options

8.1 Jammer Mode Overview

8.1.1 Jammer Mode (AJ)

The Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior. The Summit M5x also introduces for the first time NVMe and NVMe-MI protocol jamming as well. The analyzer and jammer combination features on the Summit M5x make this a powerful testing tool for PCIe validation and development labs. This Jammer and Scripting capability is built into the PCIe Protocol Analysis software. After the software has been loaded (see “Installation and Setup” on page 45), you can access the Jammer functionality through the Recording Options of the PCIe Protocol Analysis software dialog (see Figure 8.1).

8.1.2 Jammer Mode (AJA)

In addition, the Summit M5x can also display the results of the Jamming operation. In the Summit M5x you can analyze a stream of traffic, modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint and then see the results of that jamming operation. See “Jammer Mode Overview (AJA)” on page 497 for more details.

8.1.3 PCIe Protocol Analysis Software

Selecting the "Setup" tab will pop up the following options dialog box (see Figure 8.2 on page 440).

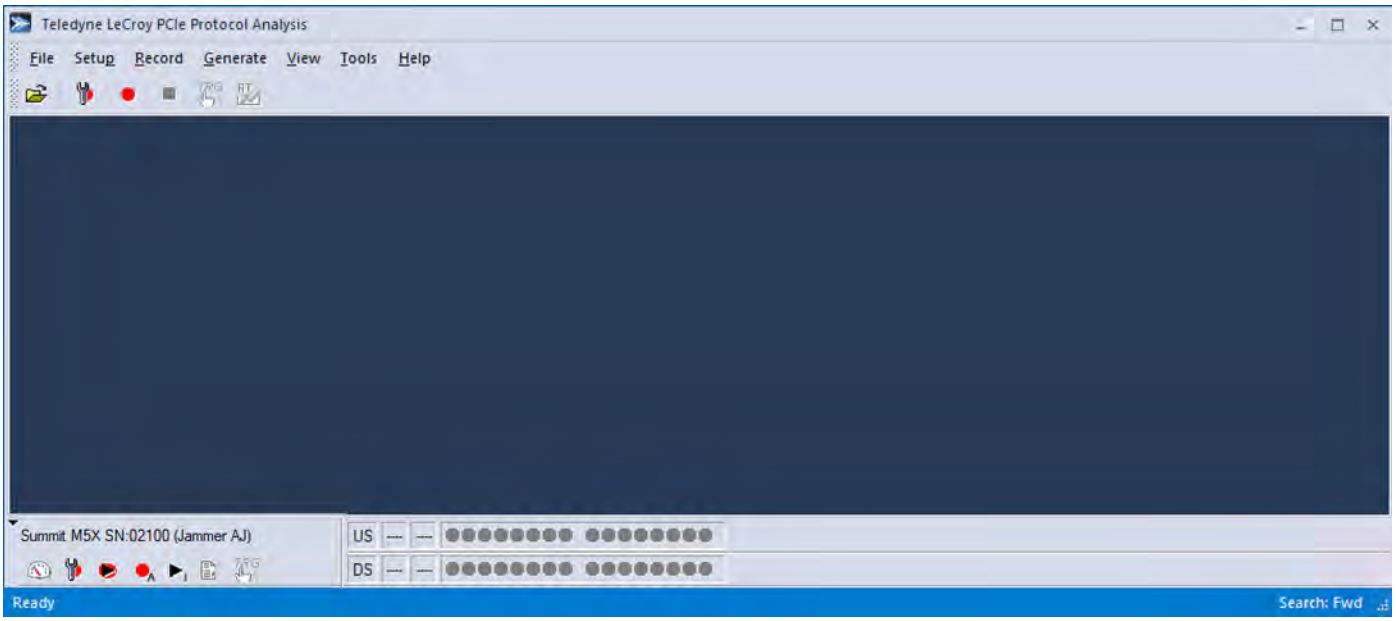


Figure 8.1: PCIe Protocol Analysis Software dialog

8.1.4 Recording Options

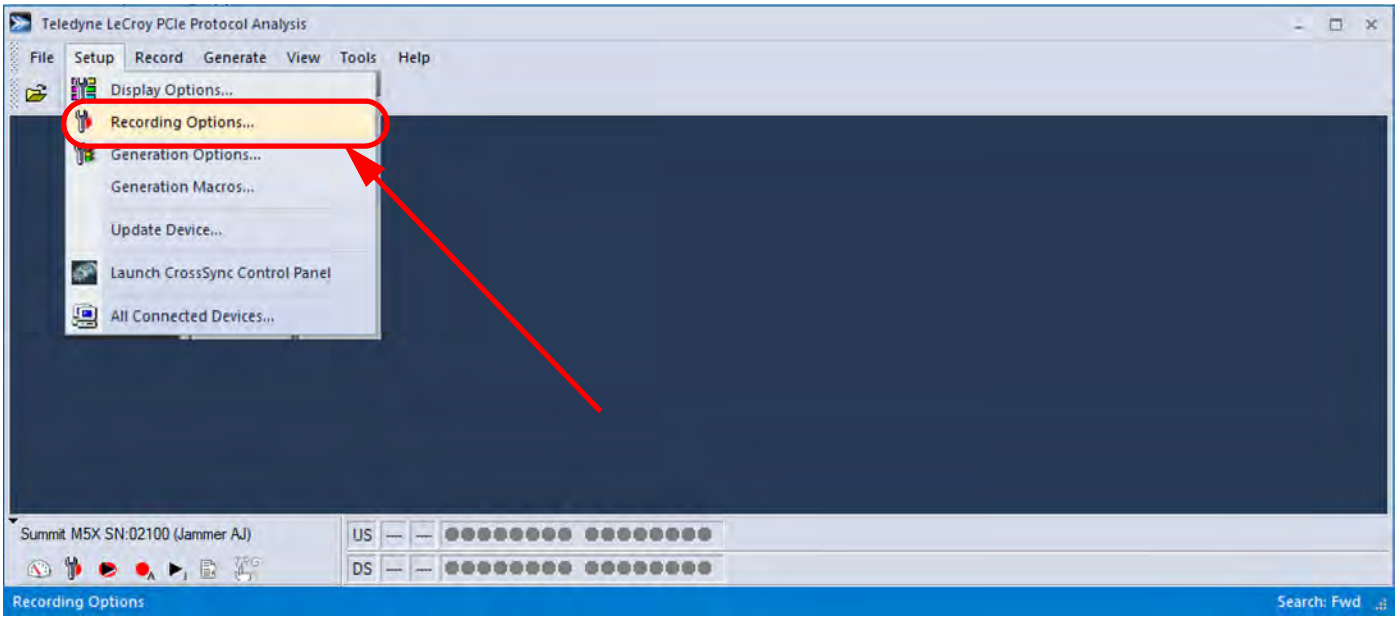


Figure 8.2: Recording Options

Select the Recording Options and a new dialog box will pop up (see Figure 8.3 on page 441).

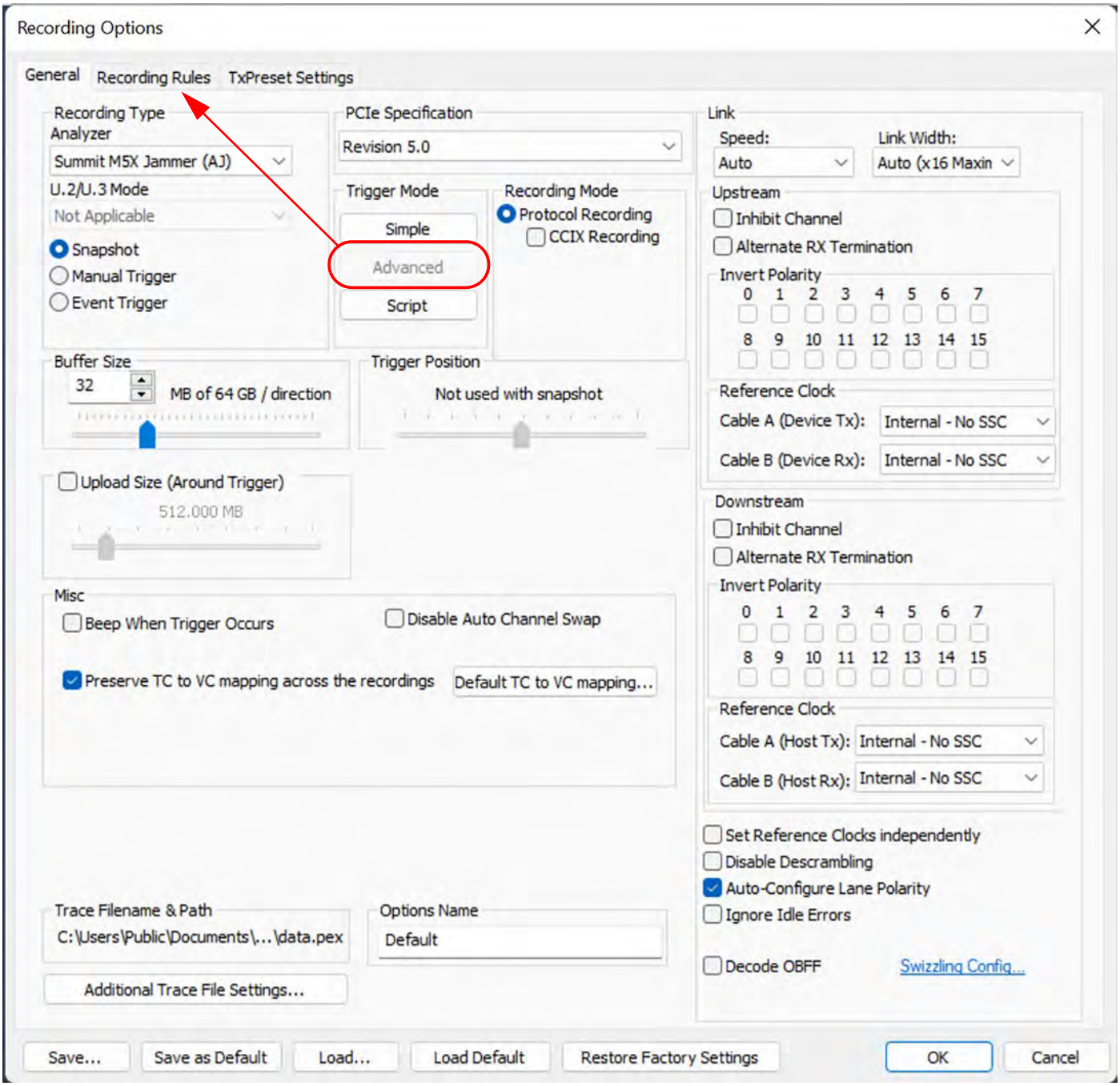


Figure 8.3: Summit M5x Recording Options Dialog

Select the Advanced Recording options and the Recording Rules tab displays. Click ther Recording Rules tab. See Figure 8.4 on page 442.

8.1.5 Recording Options: Recording Rules (AJ)

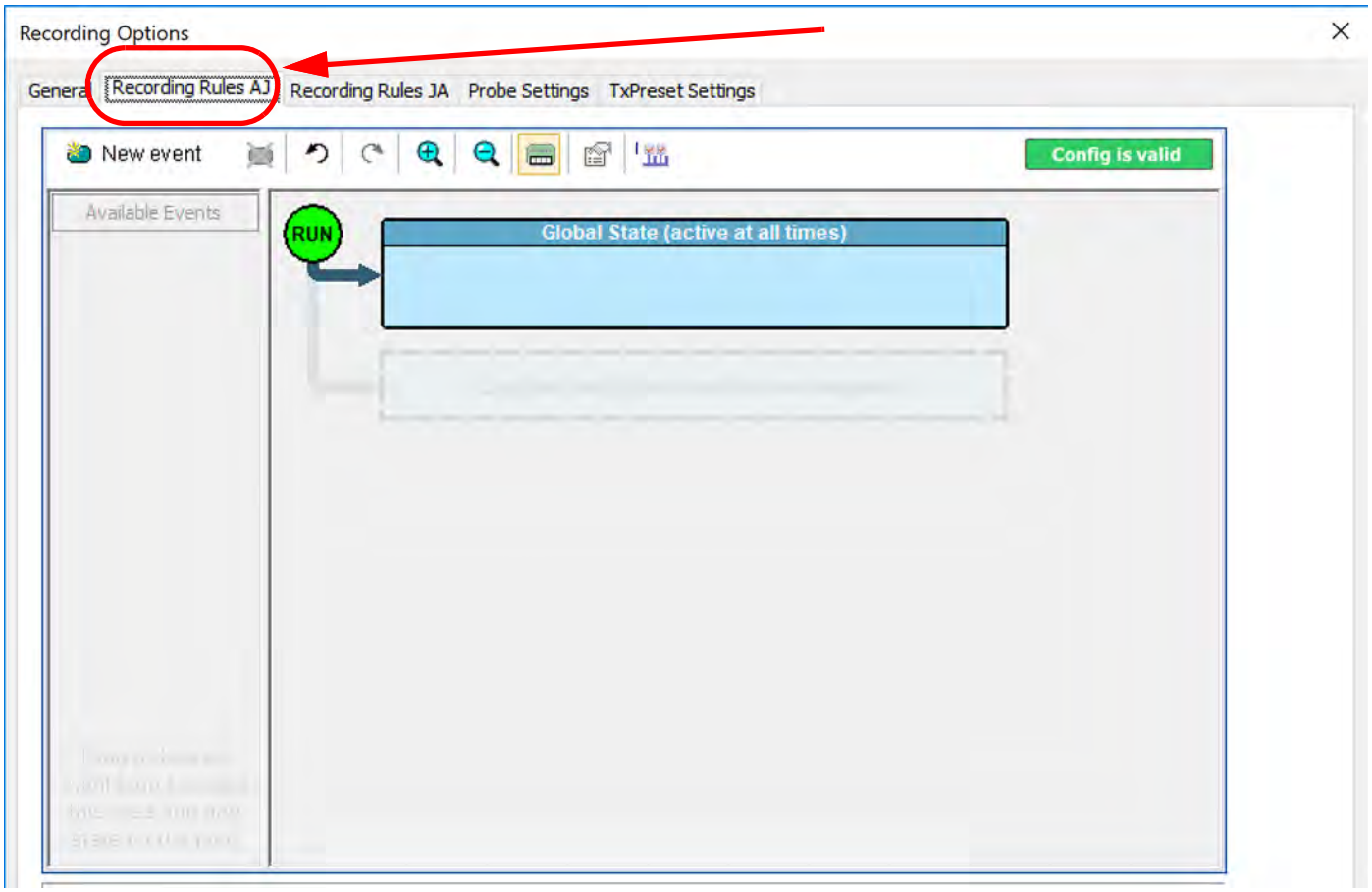


Figure 8.4: Recording Options: Recording Rules AJGUI

If you select the New Event tab, you'll see all the New Event options available to Trigger on. See Figure 8.5 on page 443.

8.1.6 Recording Rules AJ: New Events

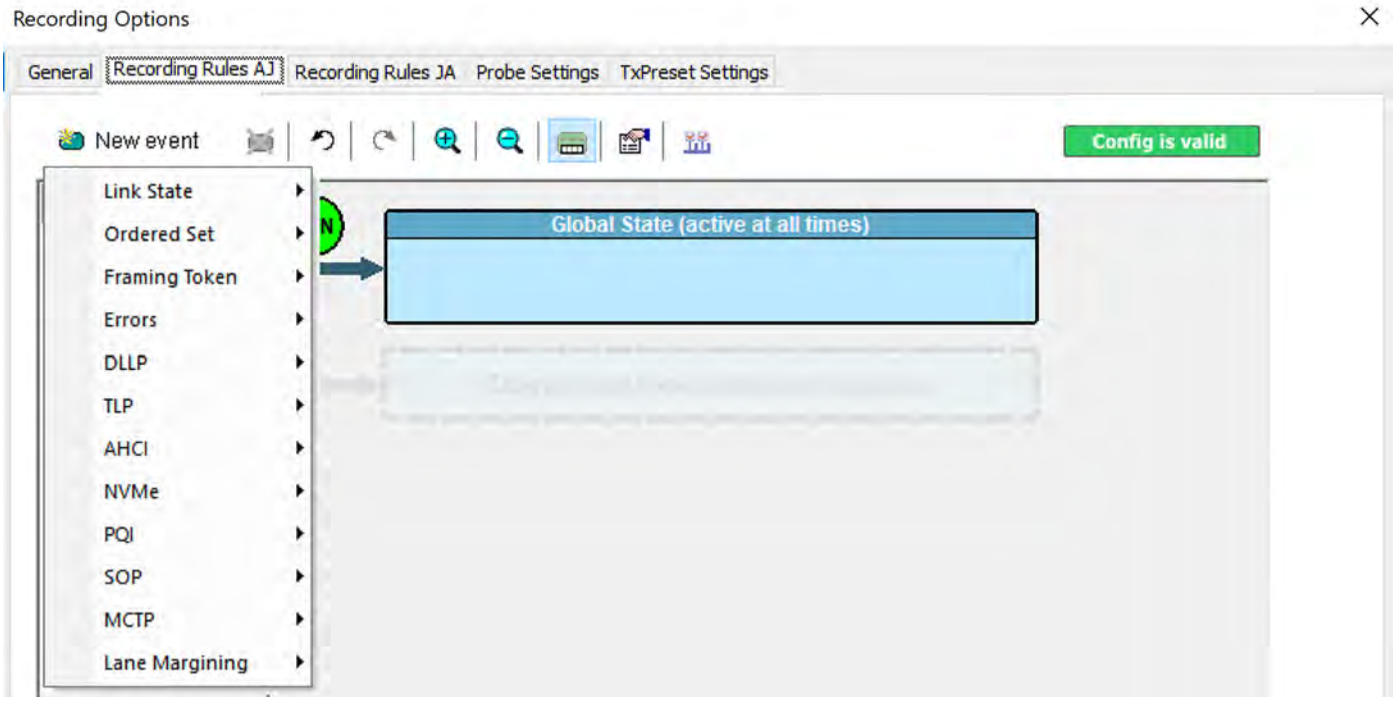


Figure 8.5: Recording Options: New Events List

The PCIe Protocol Analysis software enables you to configure a very complex set of Recording Rules or events and Jammer Actions from the GUI and then convert them into a script.

There are twelve (12) types of New events to choose from:

- Link State
- Ordered Set
- Framing Token
- Errors
- DLLP
- TLP
- AHCI
- NVMe
- PQI
- SOP
- MCTP
- Lane Margining

8.2 Converting Recording Rules and Jammer Actions from GUI to Script File (AJ)

8.2.1 Complex Recording Rules

We have defined a complex set of Recording Rules to which we can add Jammer Actions and then convert the GUI options into a script automatically. See Figure 8.6

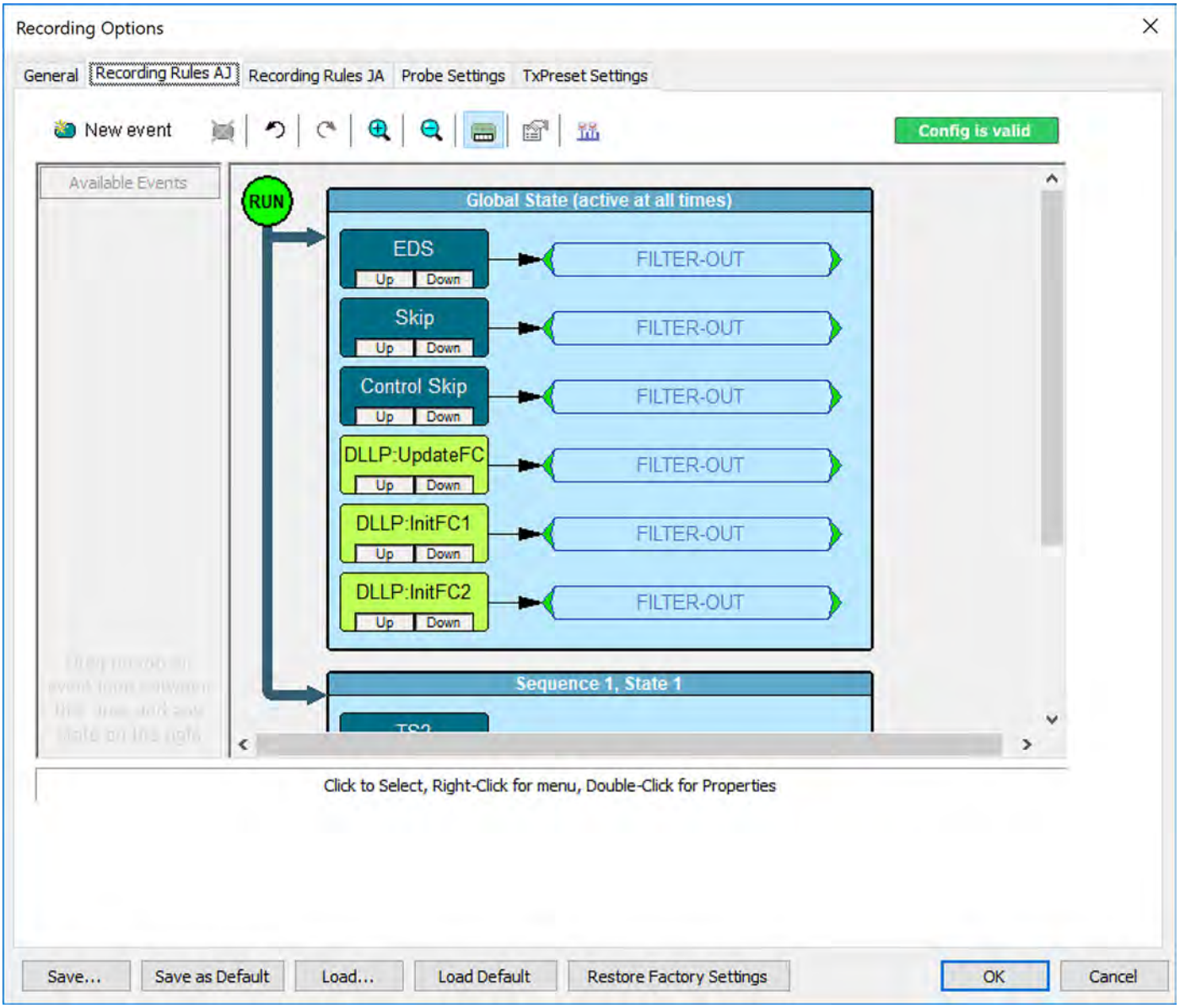


Figure 8.6: Complex Recording Rules: 1

If you use the scroll bar on the right you'll get to the final events. See Figure 8.7 on page 445.

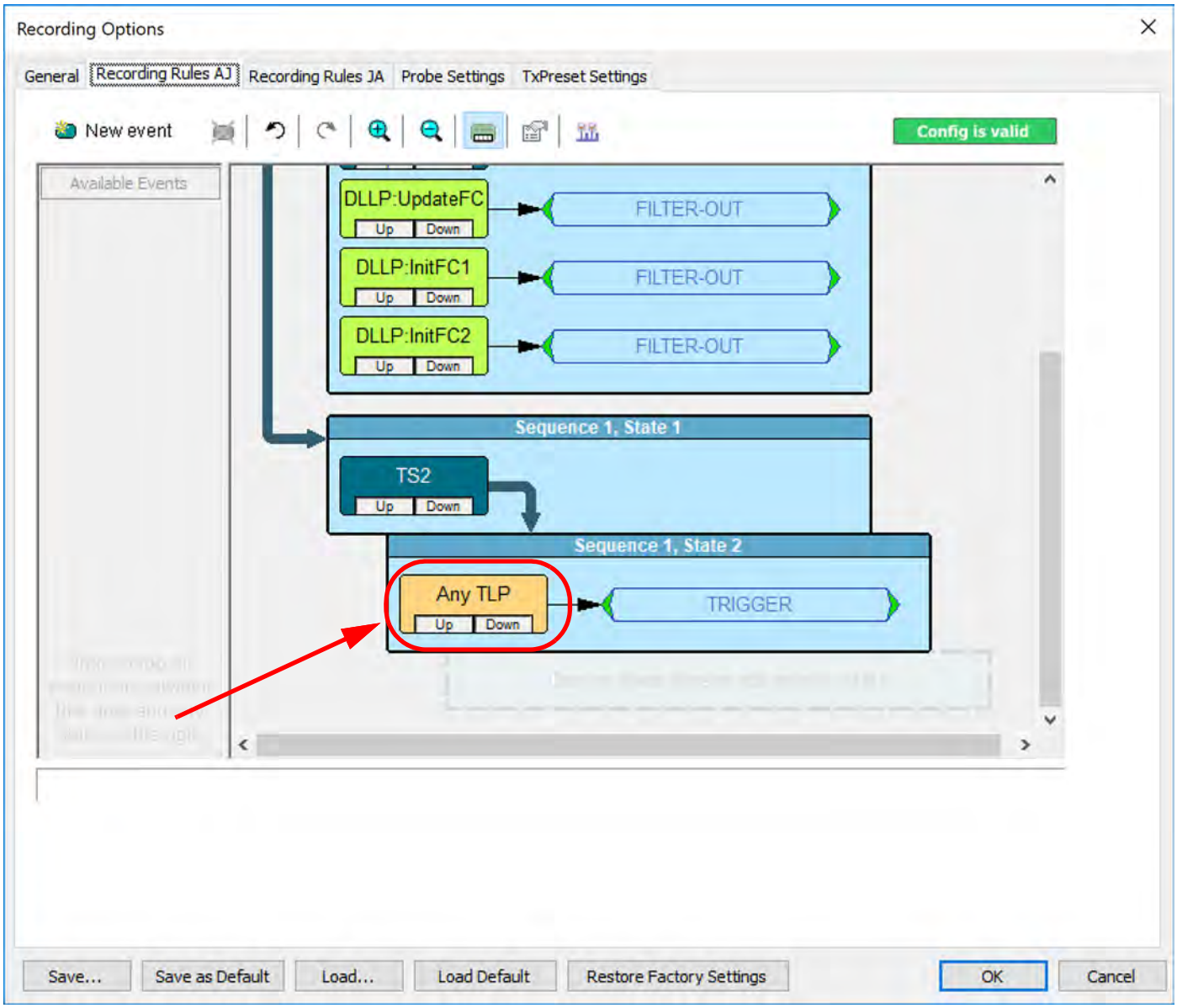


Figure 8.7: Complex Recording Rules: 2

If you right click on the Any TLP another dialog will pop up which allows you to choose a Jamming Action as well as triggering the analyzer. See Figure 8.8 on page 446.

8.2.2 Jammer Options

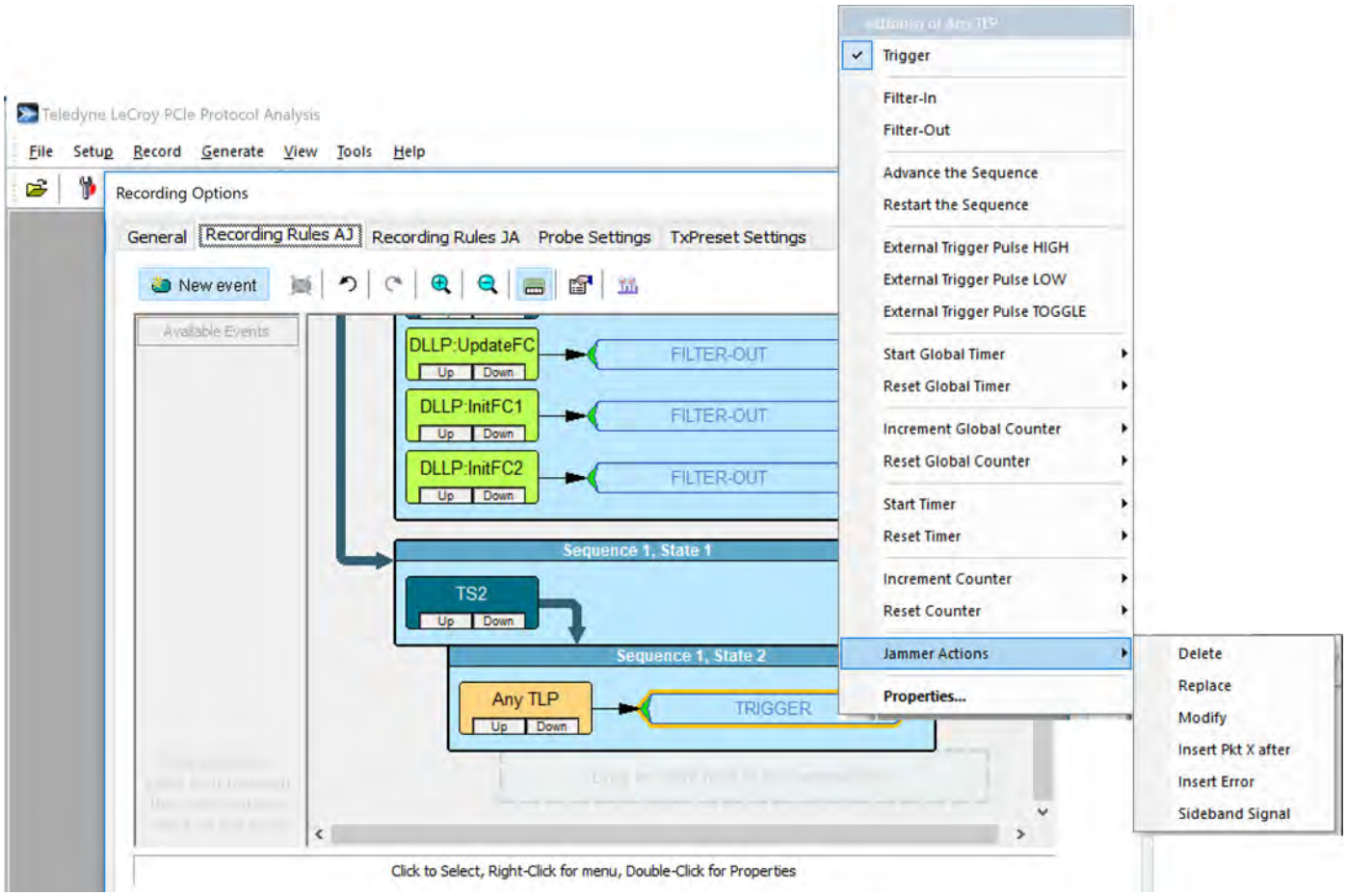


Figure 8.8: Jammer Actions

Now you can add the following Jammer Actions to the Trigger:

- Delete
- Replace
- Modify
- Insert Pkt X after
- Insert Error
- Sideband Signal

8.3 Script Mode

Script mode is currently available only for Summit M5x devices. If an Summit M5x device is not connected, then it is necessary to select "Summit M5x" device to enable script mode selection. Script mode can be enabled on the "General" tab in Recording Options dialog using the "Script" button. After switching to script mode, the "Recording Script" tab with controls to modify a script will be added.

If Recording Rules in Advanced or in Simple mode contain some events, these events will be automatically converted to a script when switching to script mode.

If Script Mode UI contains script text, then it will be converted to Recording Rules when switching from script mode to GUI mode. See Figure 8.9 and Figure 8.10 on page 448.

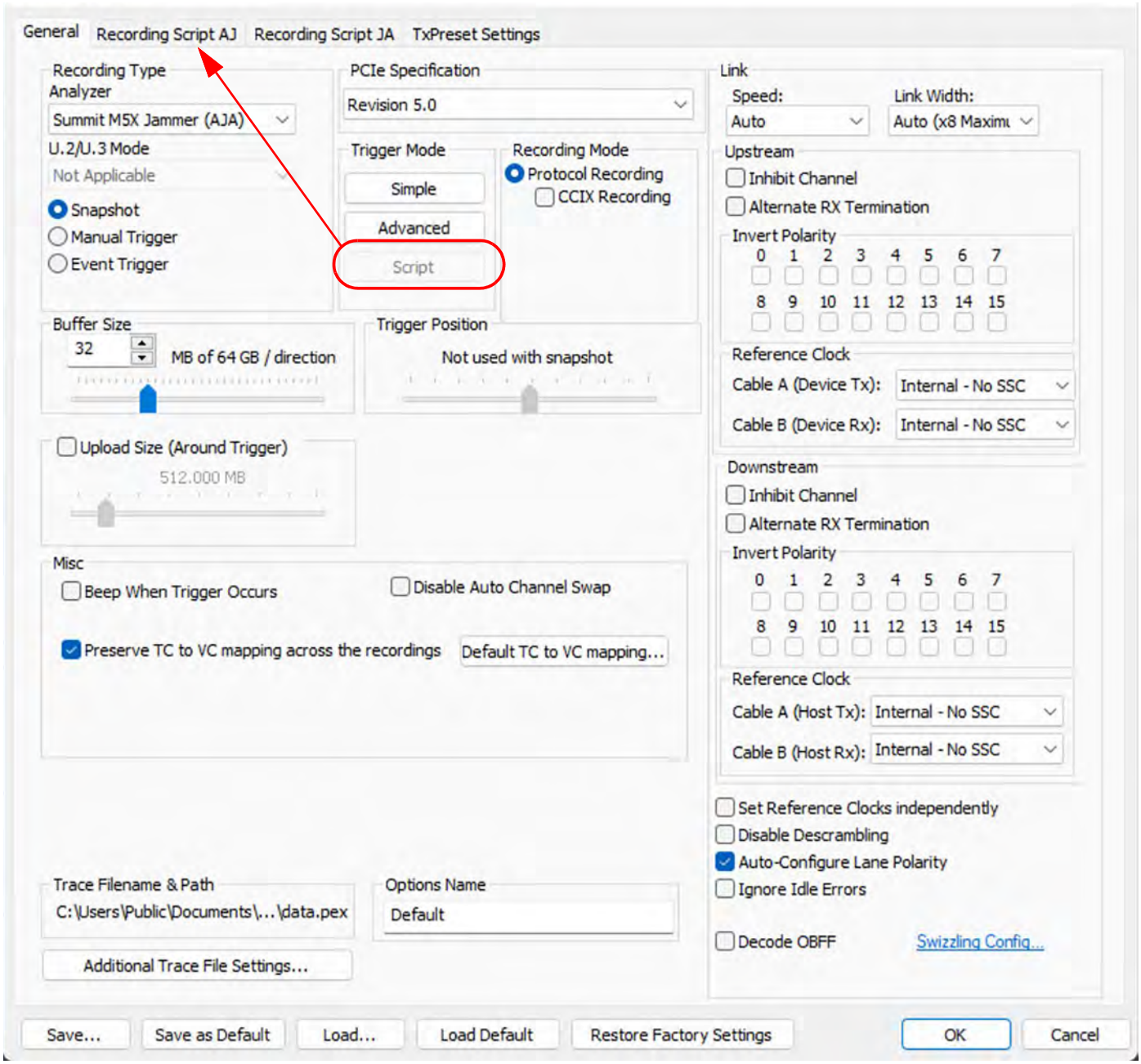


Figure 8.9: Recording Options: Advanced Mode -> Scripting

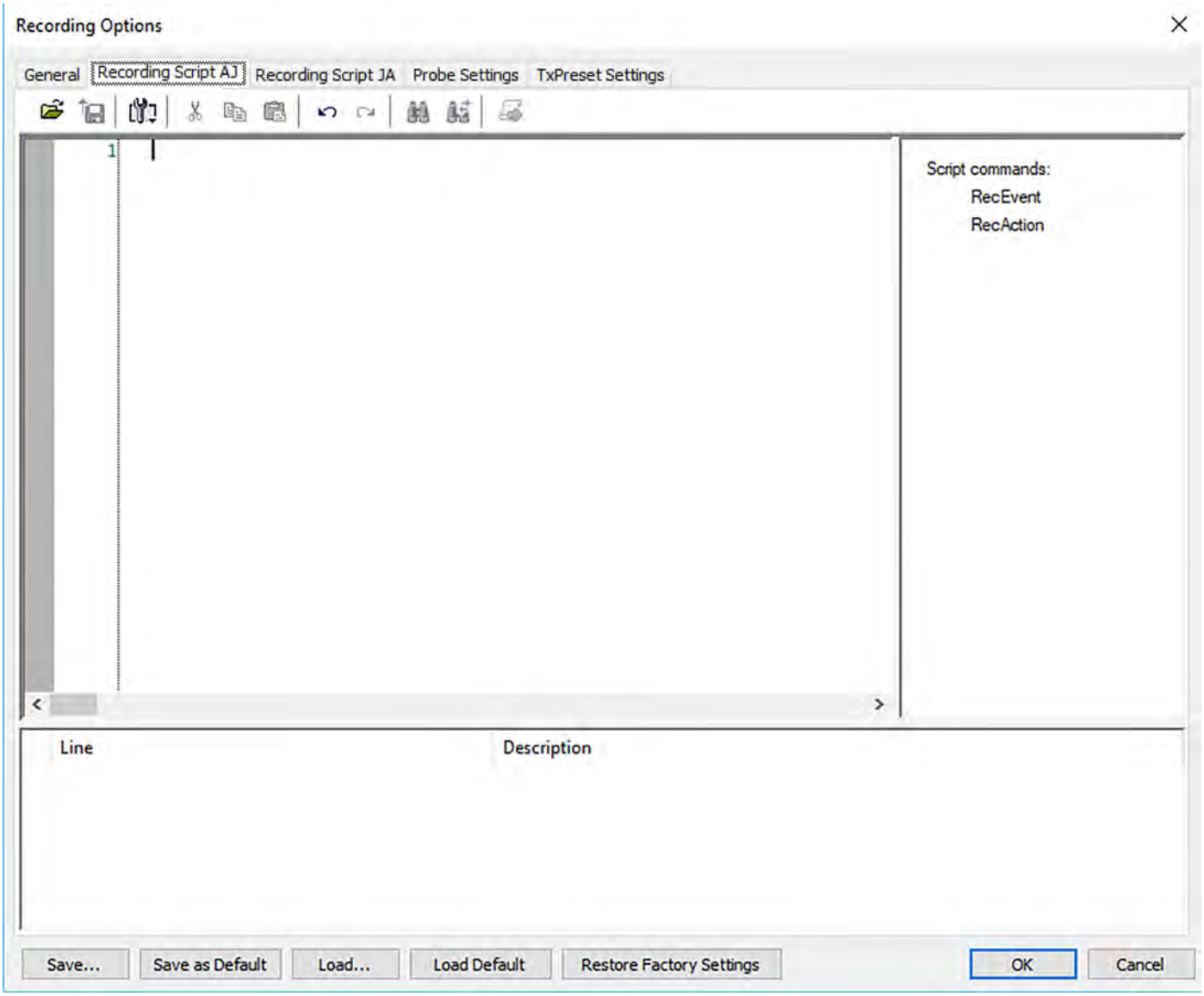


Figure 8.10: Scripting Dialog

The Recording Script mode dialog contains: text area, panel with hints, error list and toolbar.

Buttons in the toolbar include: Open/Save script, View Options of text area, Edit text (cut, copy, paste, undo, redo, find and replace) and Parse script.

Text for commands may be generated using menus "RecEvent" and "RecAction" on the right panel. They contain list of all supported events and actions. To generate text of commands it is necessary to click "RecEvent" or "RecAction" and select one of options from expanded context menu.

When the cursor (in the text area) is placed inside of braces of some command, then the hints panel will contain available properties for this command. See below in Figure 8.11 on page 449.

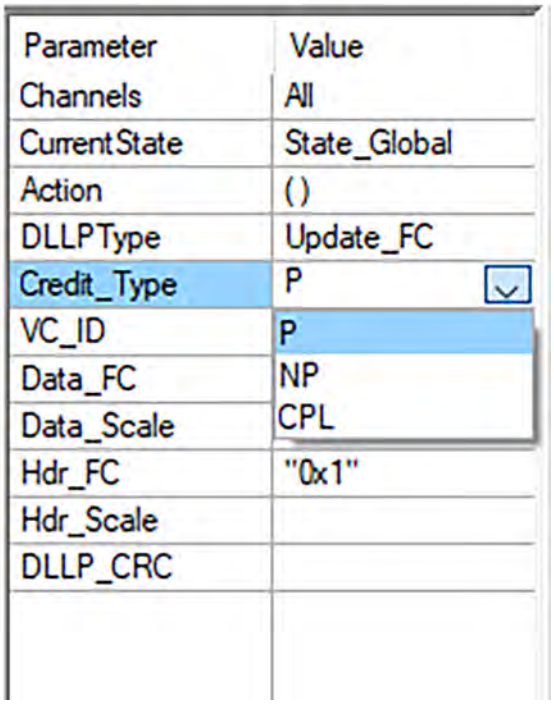


Figure 8.11: Scripting: Parameters and Values

The Errors list at the bottom will contain information (line number and description) about parse errors and warnings. It is possible to navigate to an error by double click on it. See Figure 8.12 on page 450.

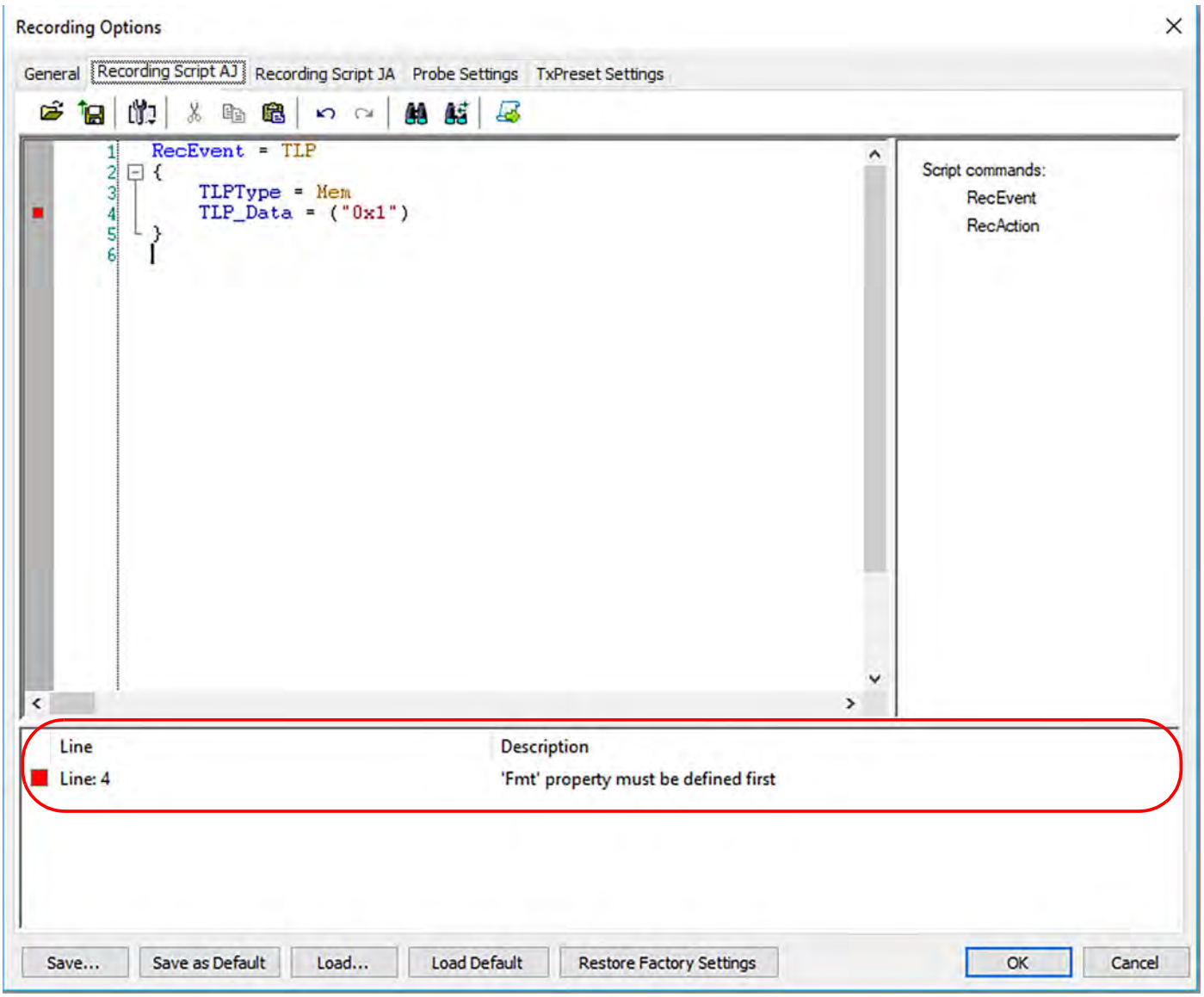


Figure 8.12: Script File with Error Shown

8.3.1 Script Parsing

Script parsing can be performed by clicking "Parse script" button at the toolbar or by pressing Ctrl + S combination. See Figure 8.13.

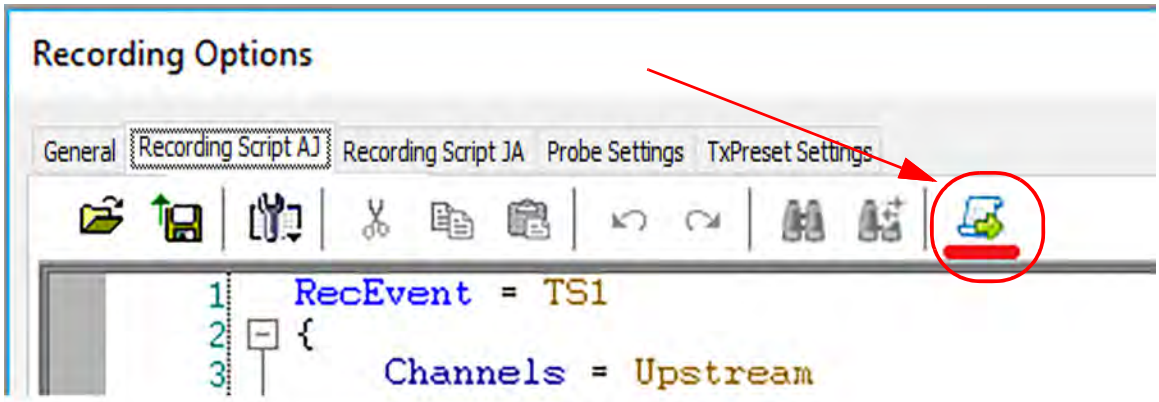


Figure 8.13: Script Parsing

The Script will be parsed when leaving the script page or by closing the Recording Options dialog. If the script contains parse errors, then a corresponding warning message will be shown. Leaving a script page which contains errors may not create recording rules correctly. See warning message in Figure 8.14.

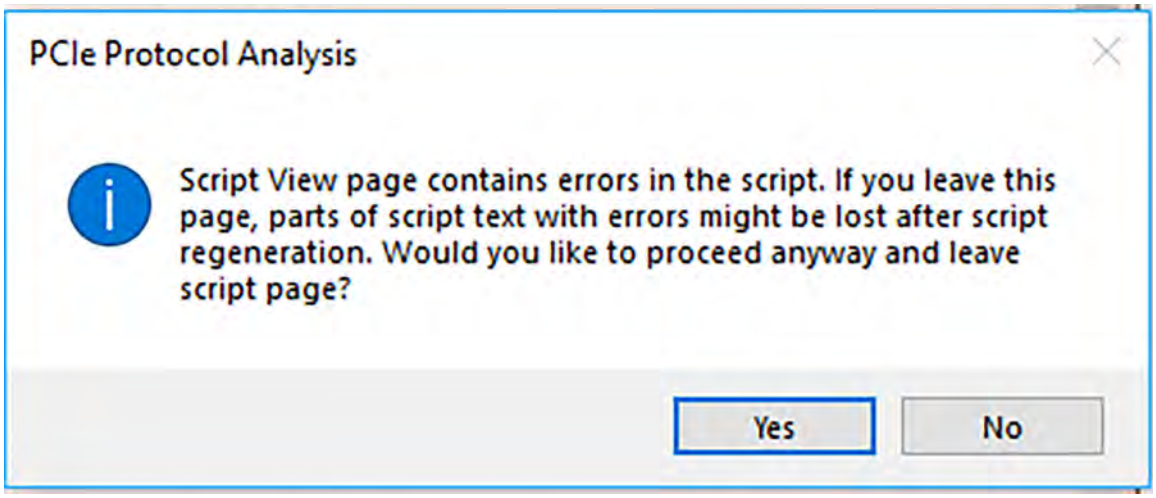


Figure 8.14: Script Warning Message

8.4 Commands

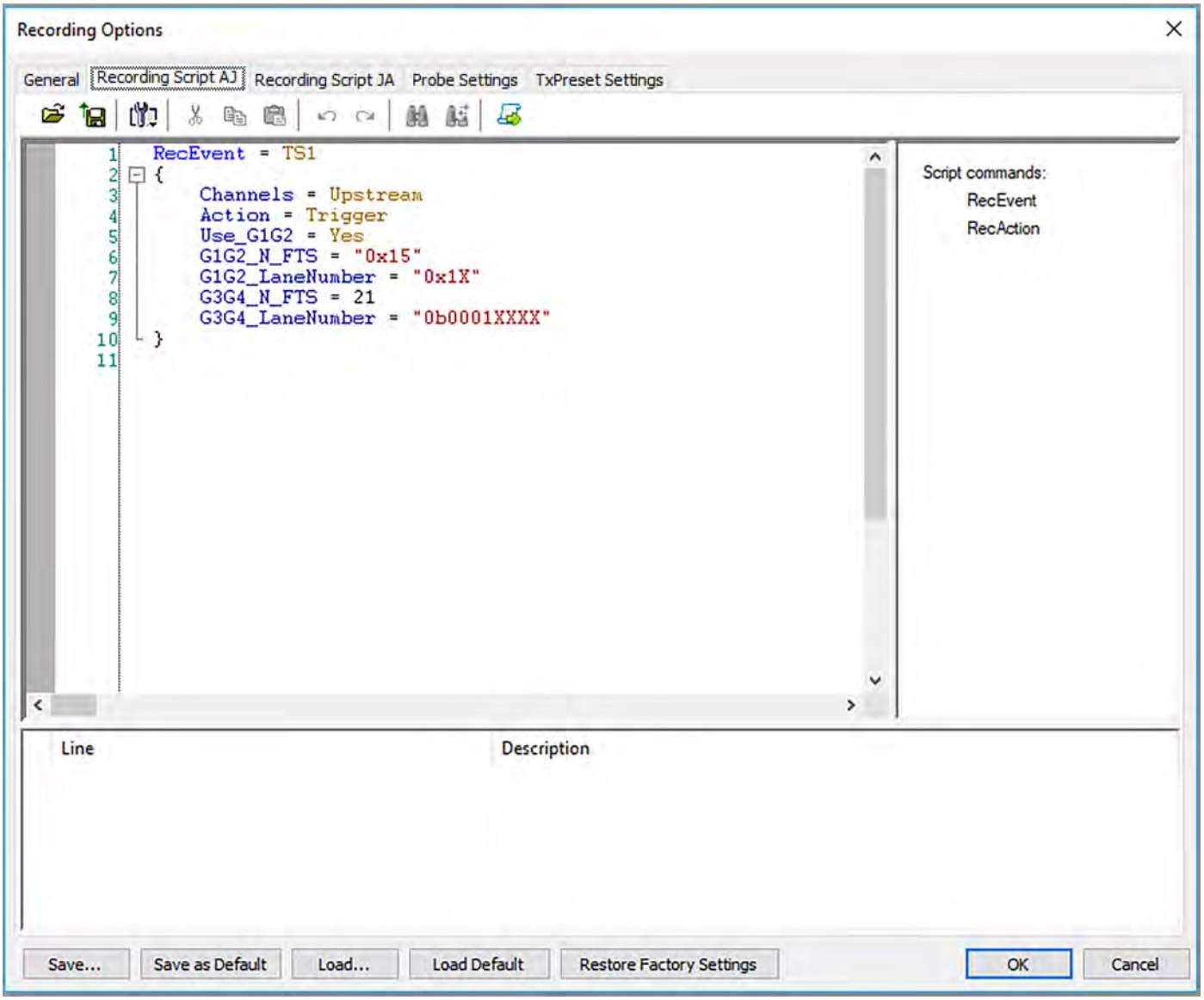


Figure 8.15: Typical Script Commands

Script commands have properties, which are placed inside braces. Each property should be defined as a key-value pair in form "Key = Value".

- Each command has its own set of available keys.
- There are different types of values: numeric, logical, mask/match and string.
- Logical values are represented as "Yes" or "No" keywords.

Mask/match values can be specified as decimal numbers or as strings with hexadecimal ("0x1") or binary ("0b1001") numbers. A mask can be applied using the "X" symbol ("0x111X" or "0b1001X111"). In binary notation "X" corresponds to 1 bit, in hexadecimal notation to 4 bits. If the value is specified as a string with hexadecimal numbers without mask, then the mask will not be applied to the whole field (for example, "0x1" equals "0x00000001" for 32 bit field).

Some properties have predefined constant values. Such values will be suggested when the "=" symbol is pressed. A list of such values can also be opened by pressing Ctrl + Alt + T or using context menu.

See example below in Figure 8.16.

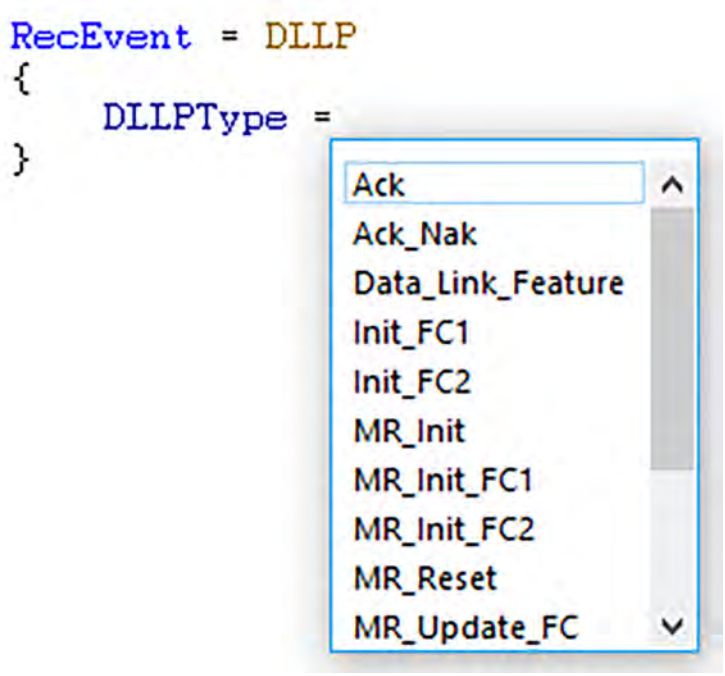


Figure 8.16: Example of Command with Context Menu

Some commands require certain properties to be defined. If such properties are not defined, then parse error will be added. If a command does not require a property and it is not defined, then a default value from UI will be set.

8.5 Events

RecEvent commands have several properties that are common almost for all events. Channels property defines event's channel(s): Upstream, Downstream, All or None. Current state property defines the state in which the event is located. It can be "State_Global" or one of 16 local states (for instance, "State_1"). Actions property defines the event's actions, which is used for triggering, sequencing, filtering etc. Action property is also used to connect events with jammer actions.

Timer and counter events have additional restrictions. Theyare divided into two groups: global and local. Global timers and counters can be created only in global state. Local timers and counters must be defined in the state property and cannot be created in global state.

A list of available properties may depend on the values of other properties. For example, TLP event's properties depend on TLP type.

8.6 Jammer Actions

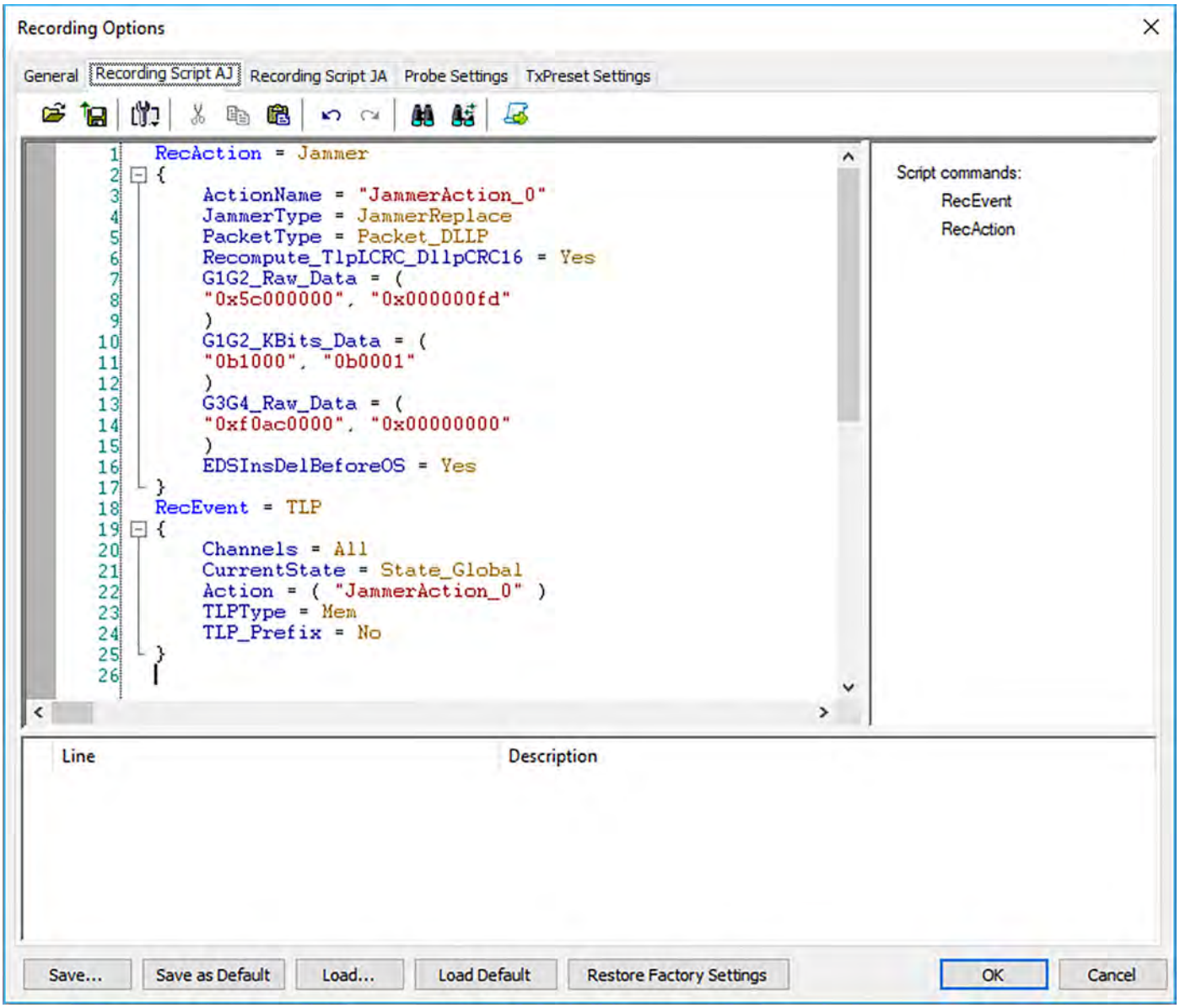


Figure 8.17: Jammer Actions

Jammer Action is a type of script RecAction command. The Jammer Action command must be connected with an event or it will not be created. Each jammer action must have a unique name and its type must be defined.

Jammer Action can be defined only before event in which it is used. To connect an event with a jammer action it is necessary to add a string with the jammer action name to the list of the event's actions.

If the Jammer Action modifies the raw data property and is not defined, then raw data will be the same as event's layout.

If raw data is not defined for Replace or Insert Pkt X After jammer actions, then raw data will be set to the default value for the Jammer Action's event type.

8.7 Scripting Jammer Functionality

There are seven (7) types of New events to choose from:

- Link State
- Ordered Set
- Framing Token
- Errors
- DLLP
- TLP
- NVMe

There are six types of Jammer Actions available which can be associated with any of the New event types list above:

- Delete
- Replace
- Modify
- Insert Pkt X after
- Insert Error
- Sideband Signal

8.7.1 Example: Select Jammer Action: Delete

If you select Delete as the Jammer Action the following dialog will pop up showing you the Jammer Action options. See Figure 8.18 on page 456.

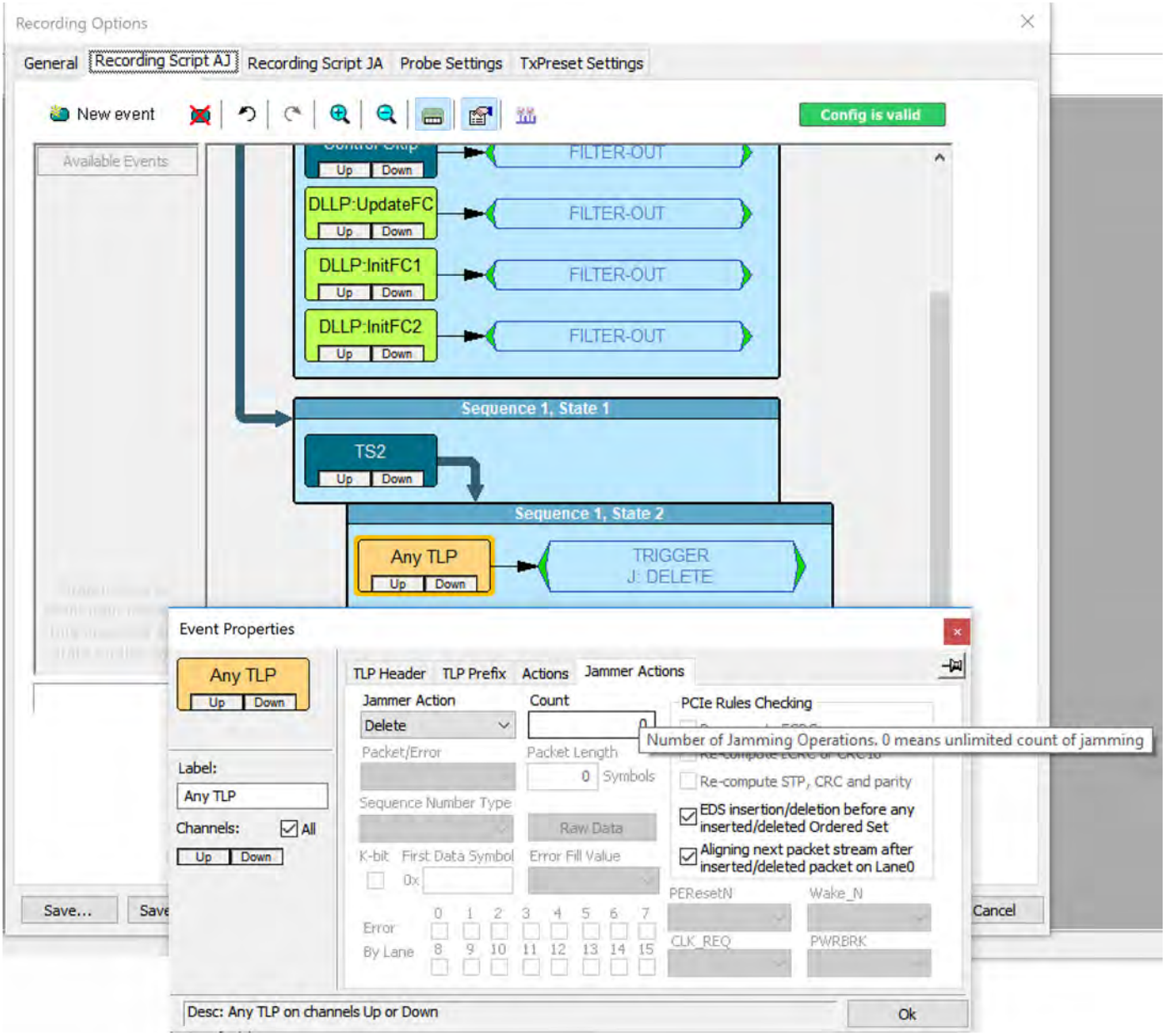
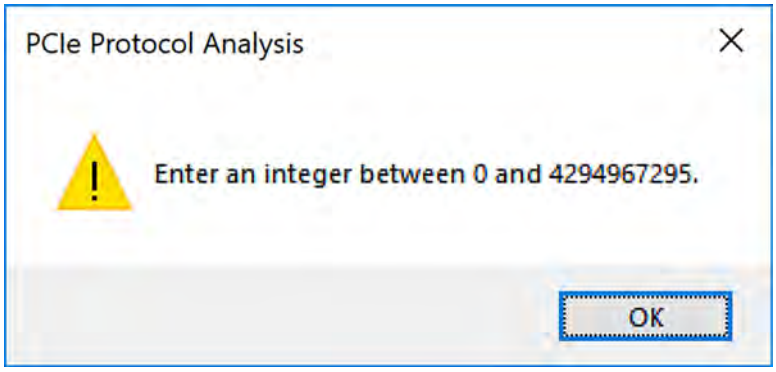


Figure 8.18: Jammer Action: Delete

For the Delete Action there are only three extra options:

- Count: Number of Jamming Operations -> **0 means unlimited**
  If you enter too large a number the following warning message will pop up. See Figure 8.19 on page 458.

WARNING: If you leave the Count Number at 0, an unlimited number of Jammer actions will take place, which means the script will not proceed beyond that point.



- For this example enter 10

- EDS insertion/deletion before any inserted/deleted Ordered Set
- Aligning next packet stream after inserted/deleted packet on Lane0

Click on **OK** to add the options to the Jammer Action.

If you select the General Tab (in Recording Options) the following dialog will appear. See Figure 8.19 on page 458.

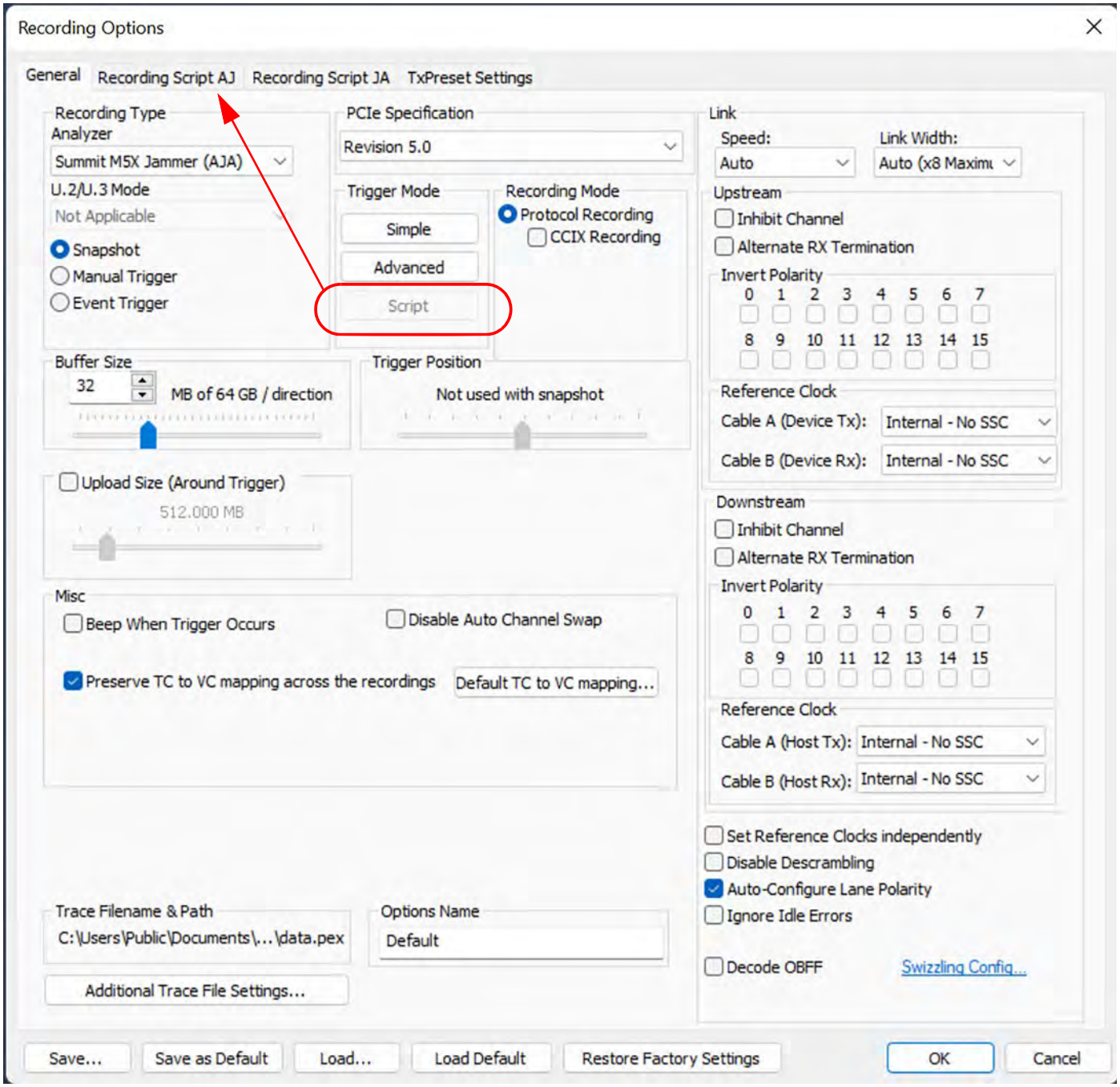


Figure 8.19: Recording Options: Script

Select the Script Option under Trigger Mode.The Recording Script Tab will appear in the Recording Options -> General dialog.

Select the Recording Script tab. The script to generate the complex Recording Options and Jammer Action displays. See Figure 8.20 on page 459.

8.8 Recording Options and Jammer Action Script

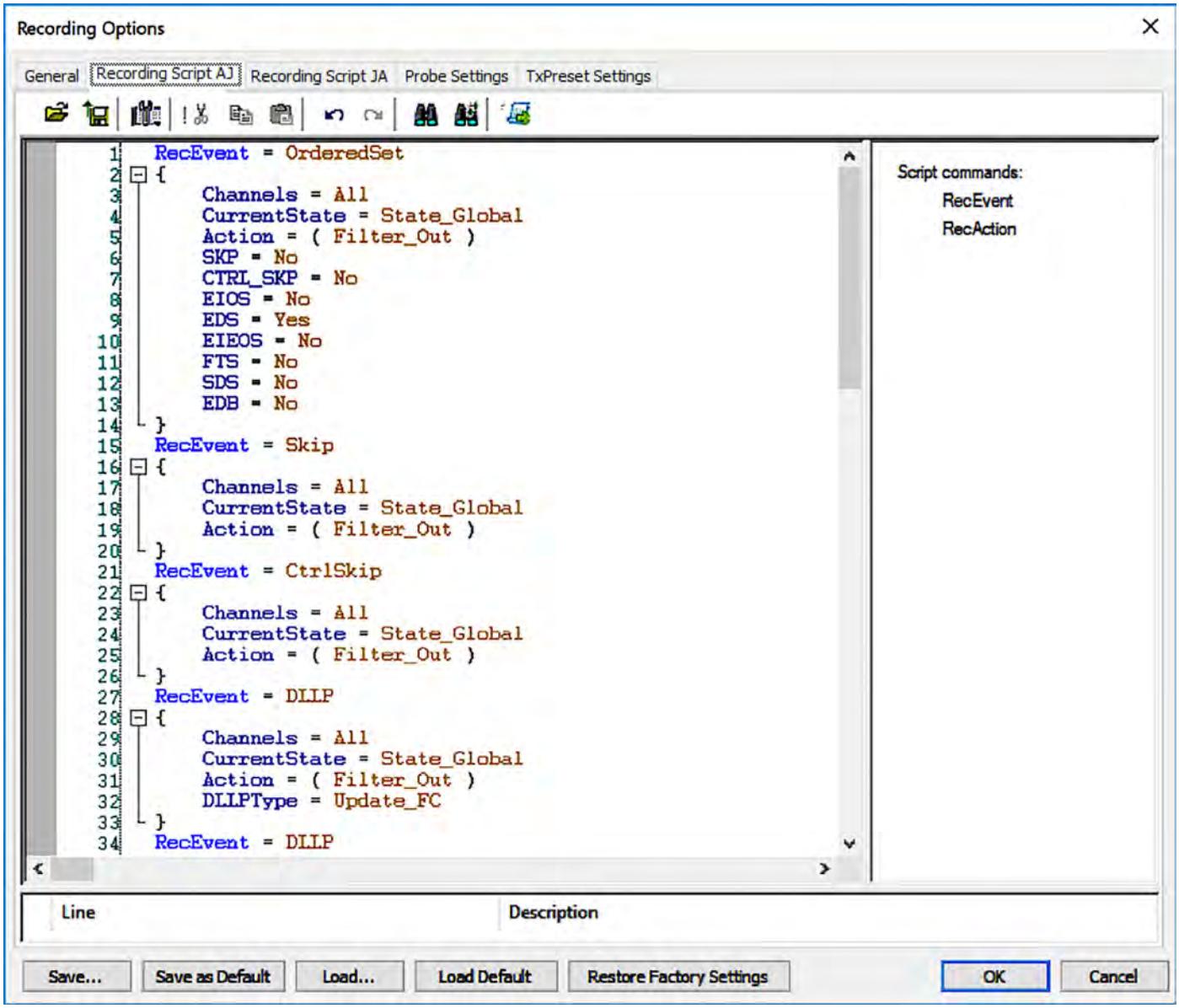


Figure 8.20: Recording Options and Jammer Action Script (1)

If you scroll down you'll see the rest of the script. See Figure 8.21 on page 460.

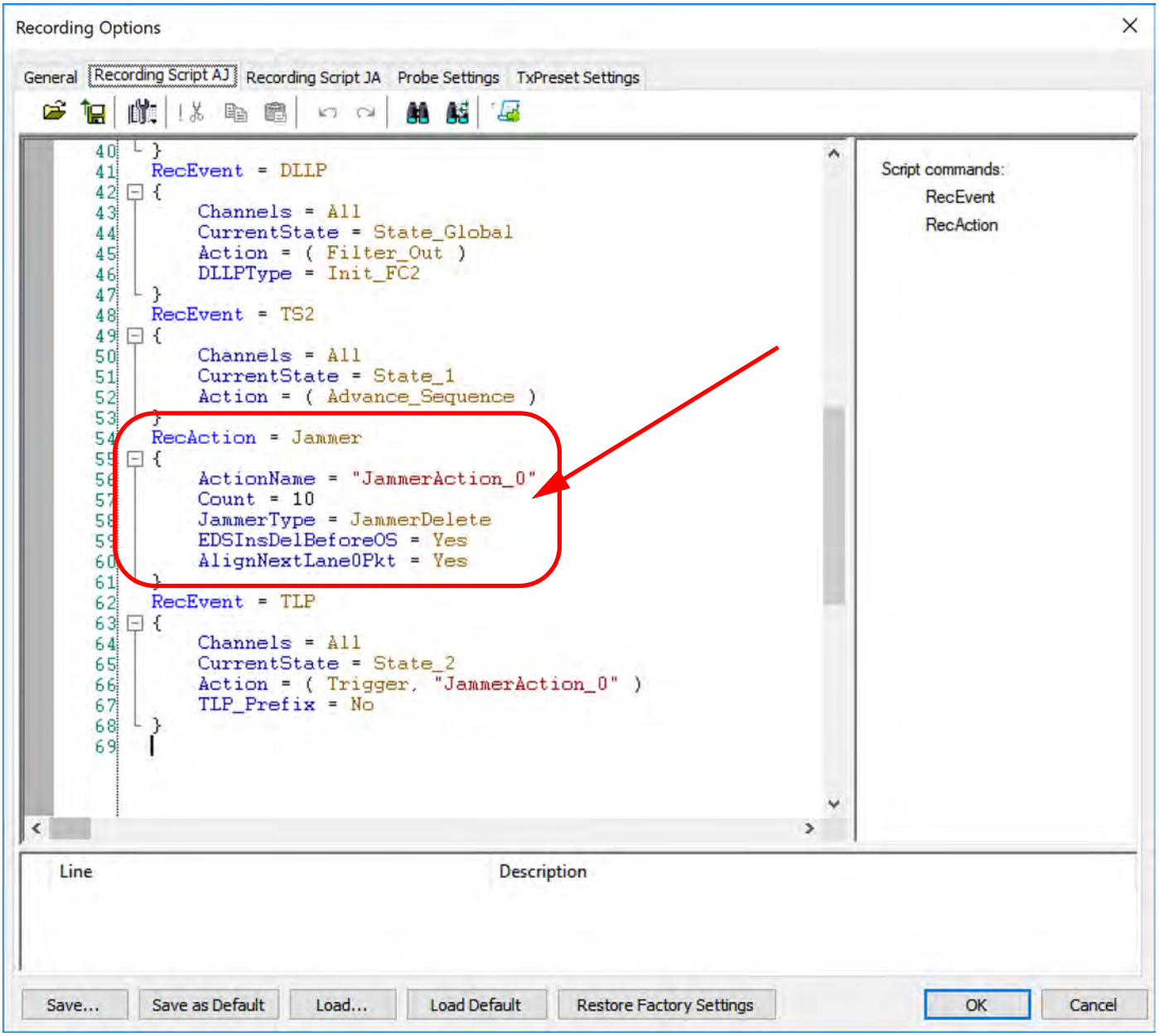


Figure 8.21: Recording Options and Jammer Action Script (2)

If you select the ActionName = "JammerAction_0" the details of the Jammer Action will appear on the right side of the dialog. See Figure 8.22 on page 461.

8.9 Updating Jammer Action Script

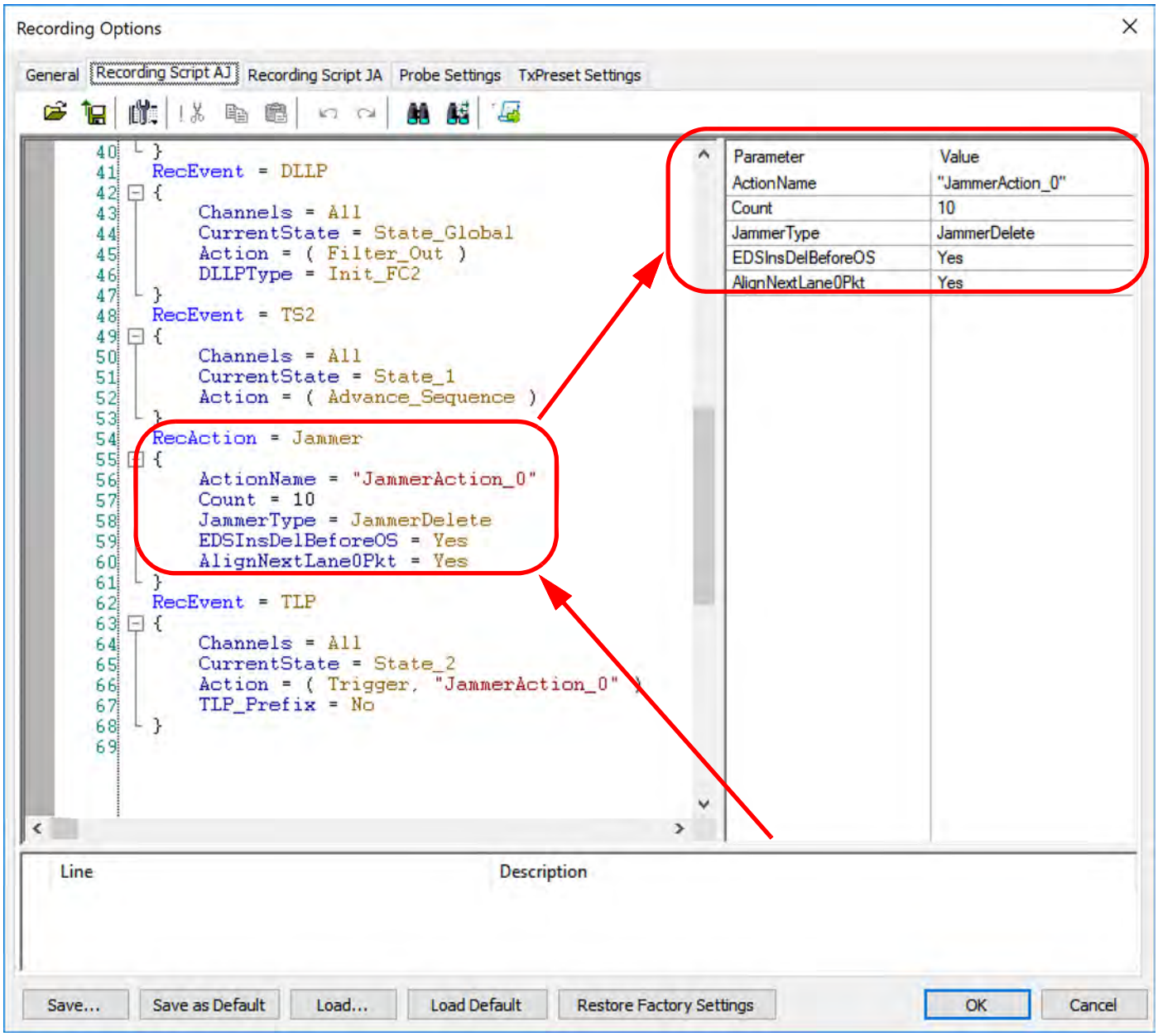


Figure 8.22: Updating Jammer Action Script

You can modify the script by selecting a Parameter Value as shown below in Figure 8.23 on page 462.

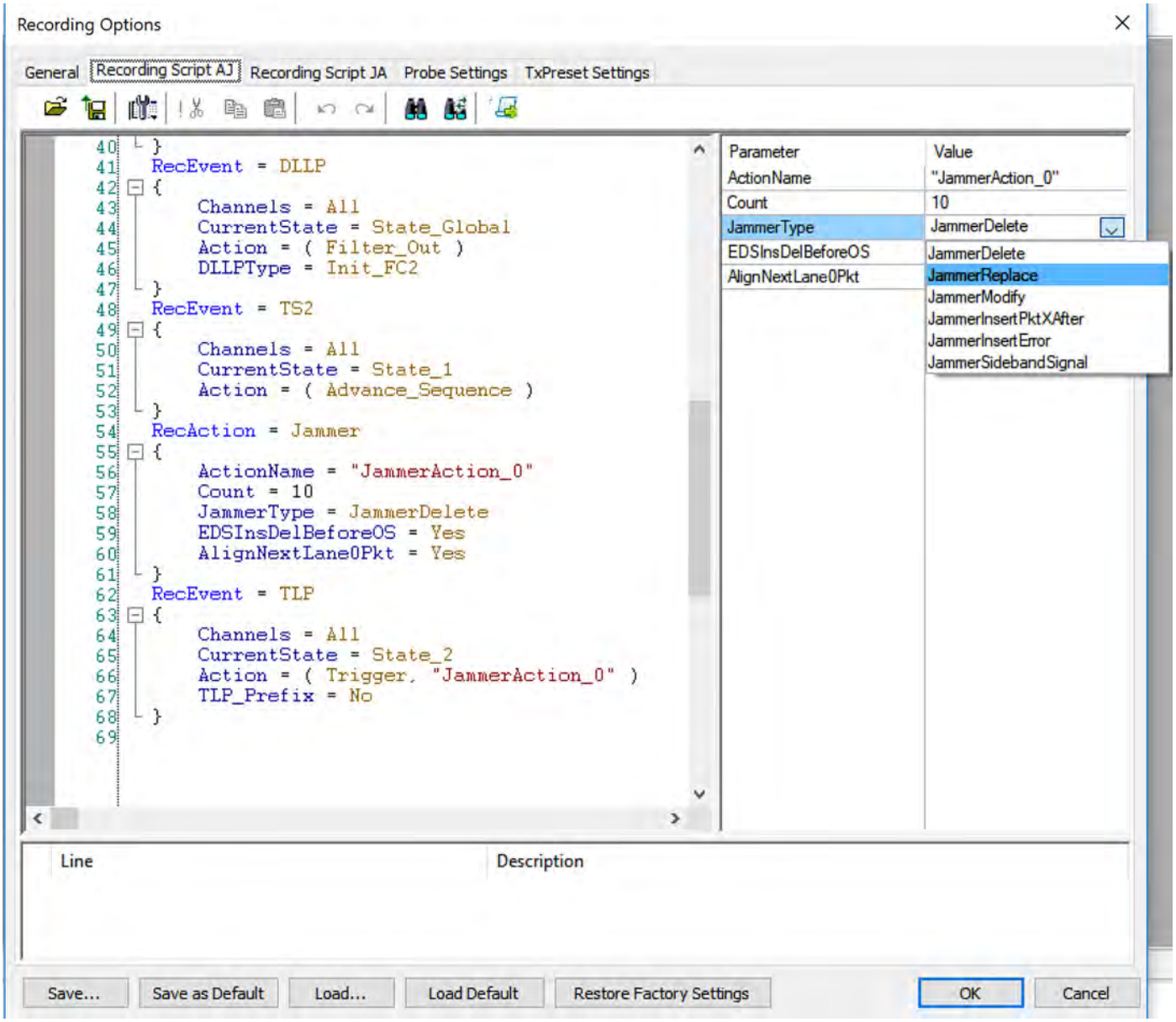


Figure 8.23: Updating Jammer Action from Delete to Replace

If you want to change the Jammer Action, just select the down arrow next to Jammer Delete and the other types of Jammer Actions will be available.

Select JammerReplace and the options for that Jammer Action will appear. See Figure 8.24 on page 463.

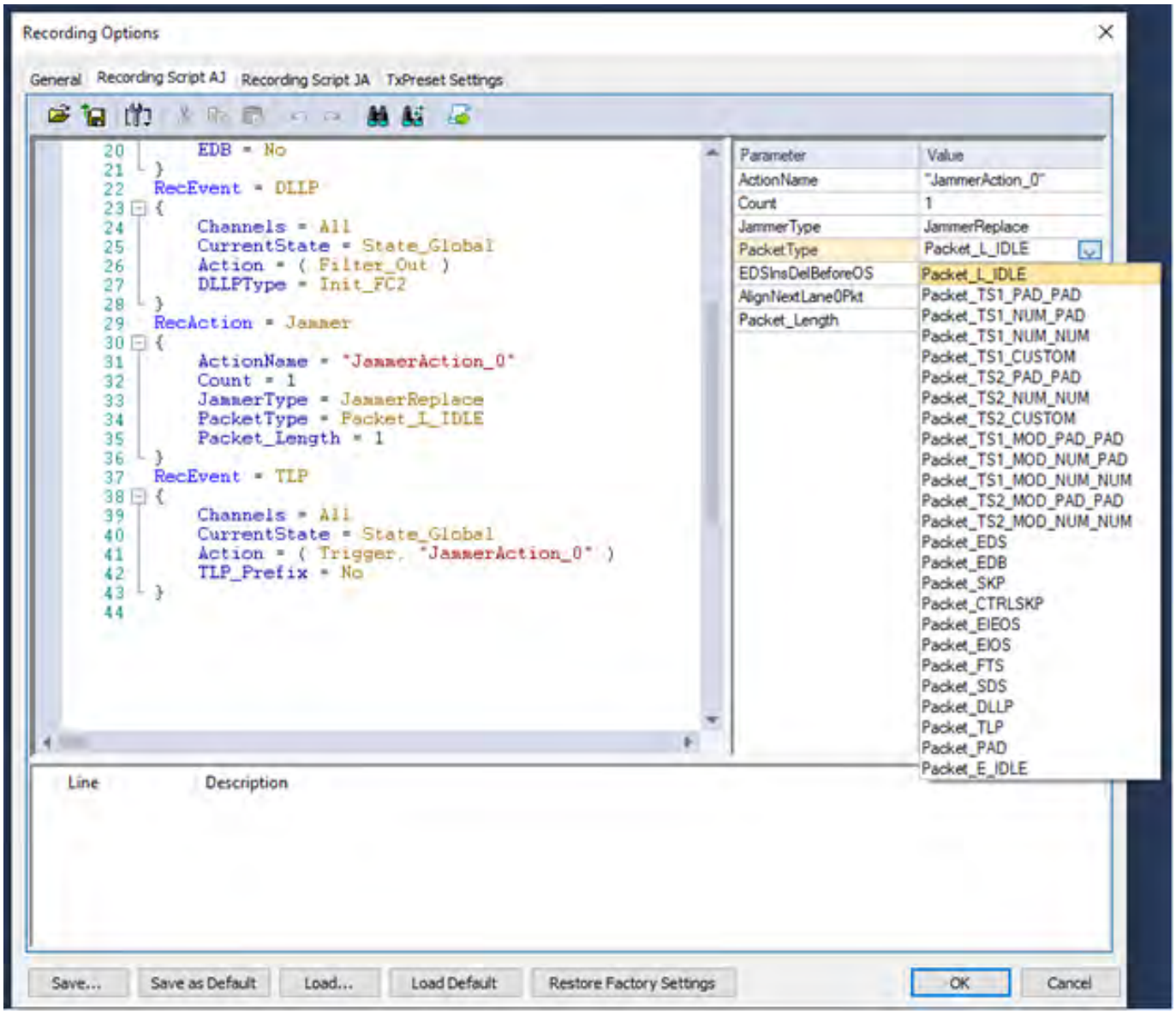


Figure 8.24: Packet Type: Packet_SKP Selected

After Packet_SKP has been selected the script will be updated. See Figure 8.25 on page 464.

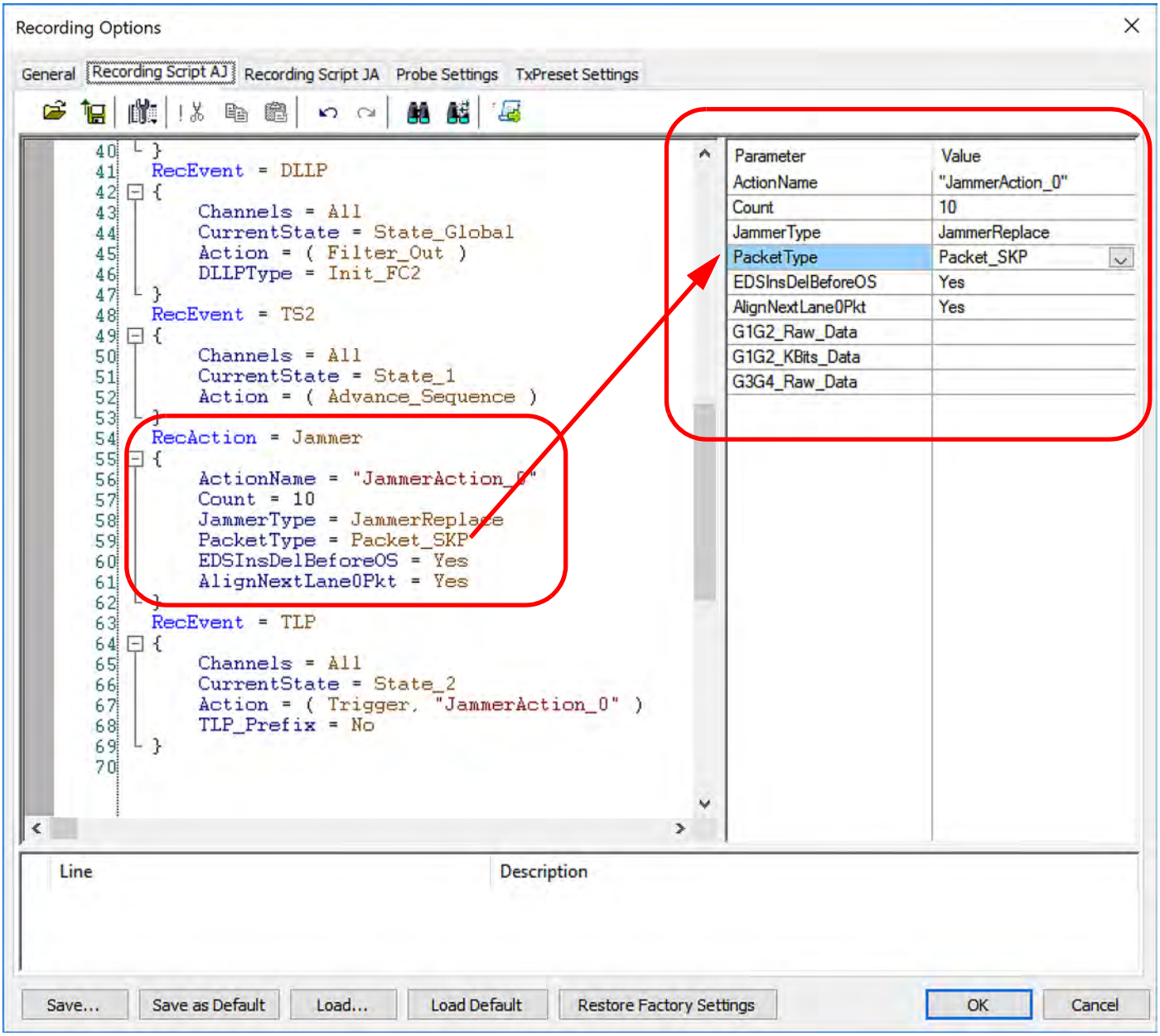


Figure 8.25: Packet_SKP Replaced Jammer Action

You can also modify the Count from 10 to 100.

Simply enter 100 into the Value block and move your cursor into the Count tab and click on the left mouse button. These actions will update the Count in the Script to 100. See Figure 8.26 on page 465.

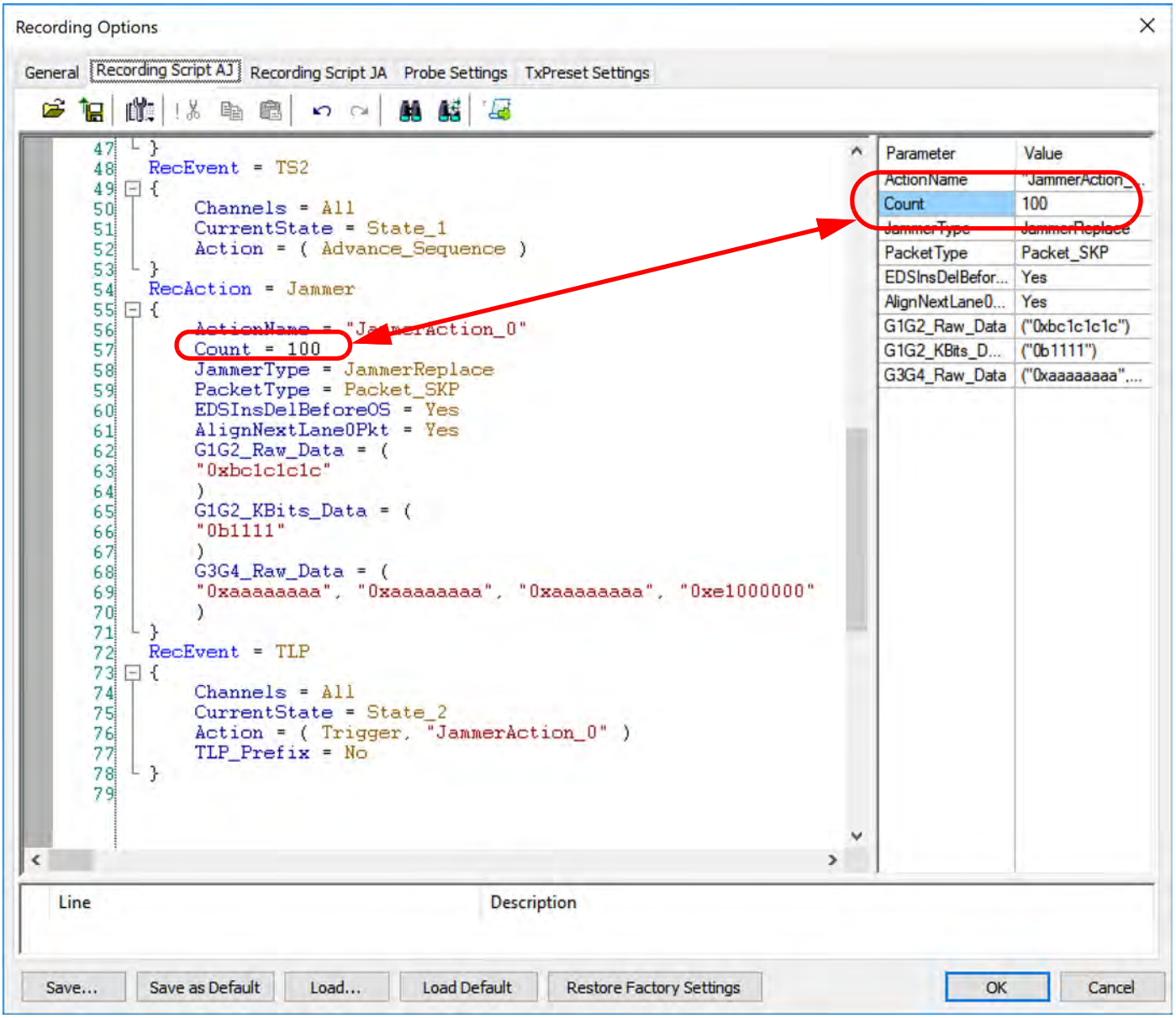


Figure 8.26: Change the Count from 10 to 100

Now that you've modified the script you can select the General tab and return to the GUI format.

8.10 Warning Message if Mistake in Jammer Script

If you make a mistake in the script, you'll see the following warning message and how to correct your mistake. See Figure 8.27.

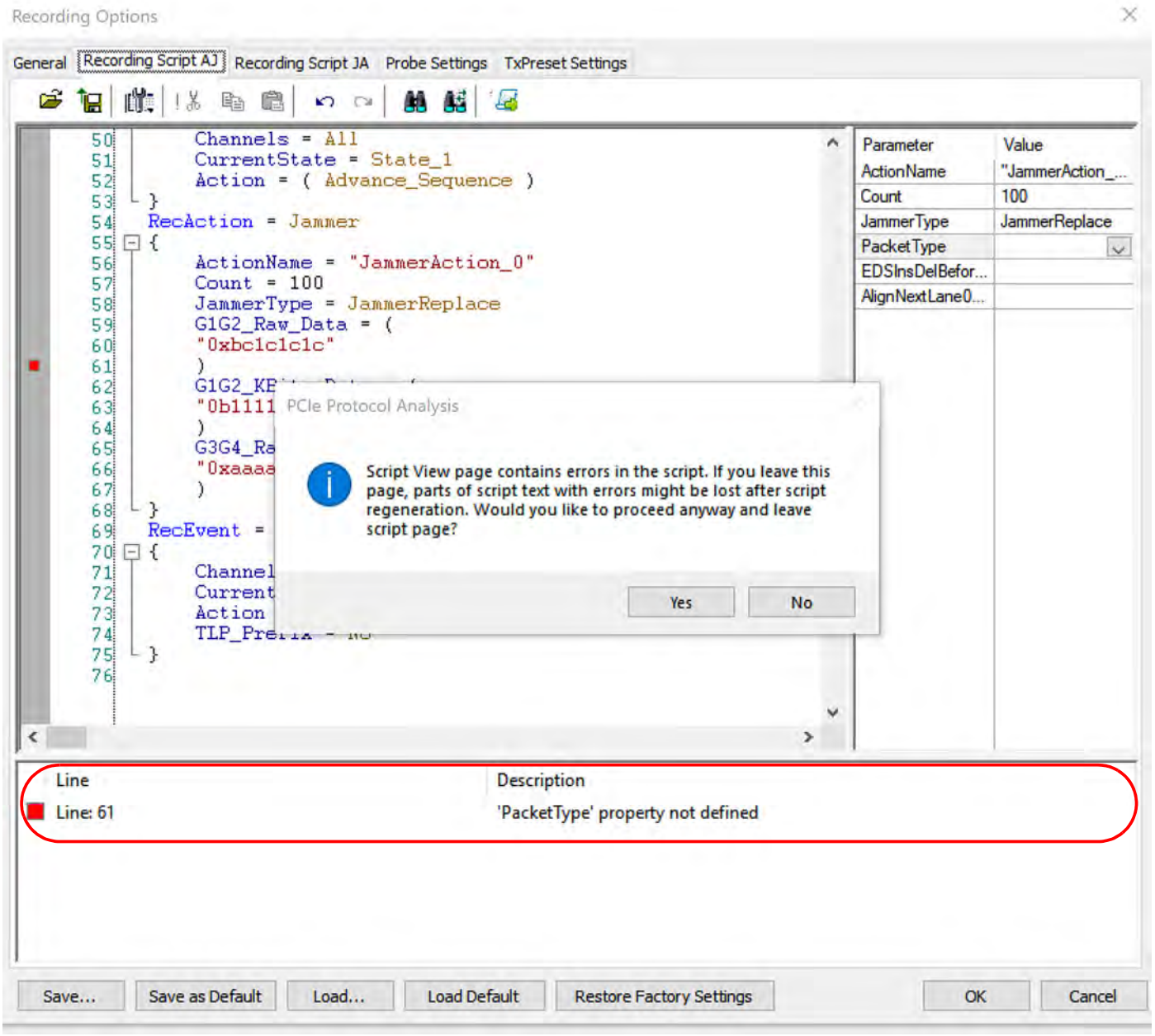


Figure 8.27: GUI Updated with Jammer Action

On Line 61 the Packet Type must be defined. Select No and correct the error. Once you do that and click “OK” you can return to the Recording Options -> Recording Script and see that your script has been modified and is correct. See below in Figure 8.28 on page 467.

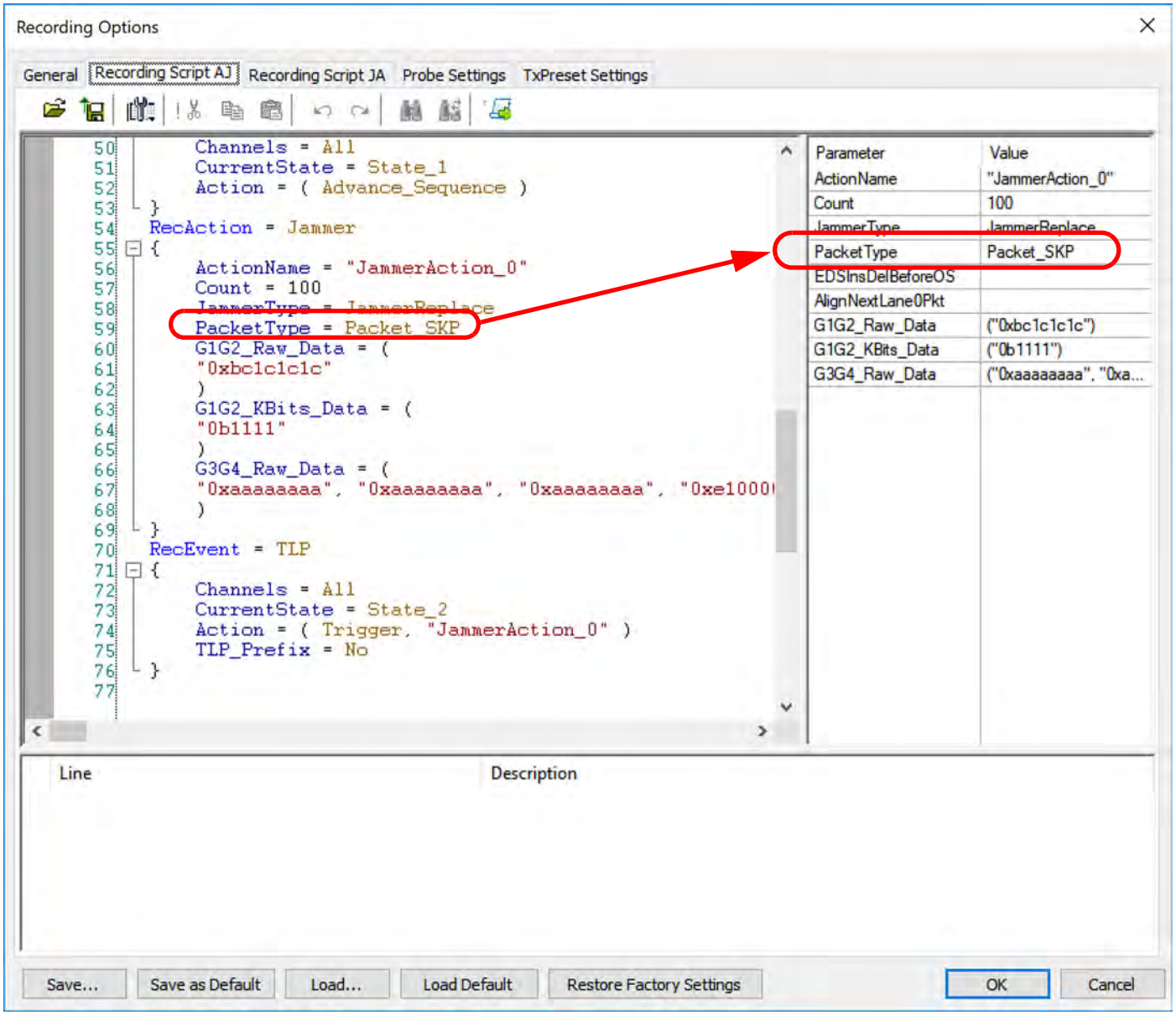


Figure 8.28: Corrected Script

Now you can select the General tab and go back to the GUI. You'll see the GUI has been updated to the changes you made in the script. See Figure 8.29 on page 468.

8.11 Updated GUI After Scripting Mistake Corrected

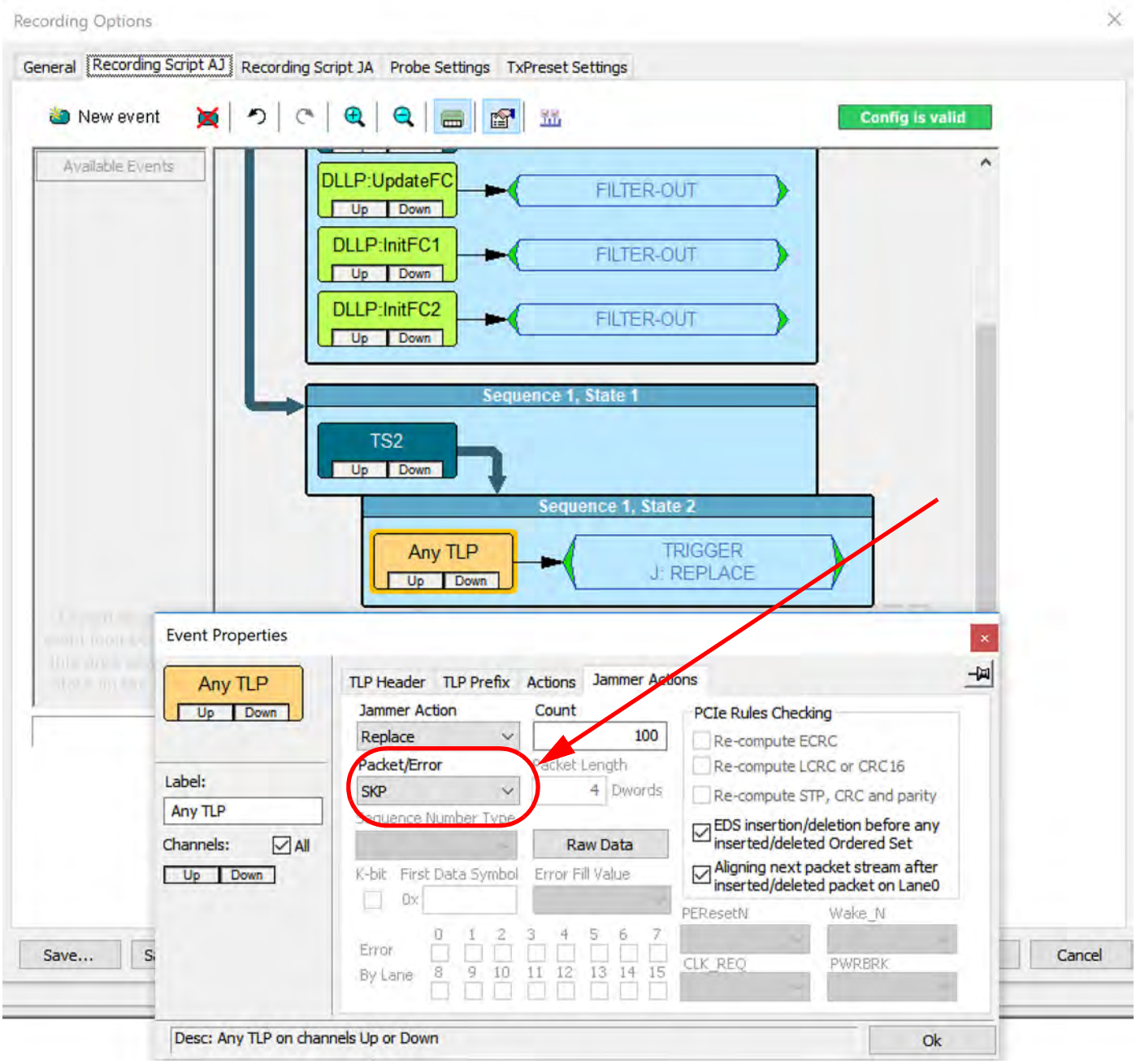


Figure 8.29: Corrected Script -> Corrected GUI

You can see that the Jammer Actions have been changed with a Packet of Type SKP.

8.12 Saving a Jammer Actions Script File

Another option you have is to Save the script file you've created with the Jammer Actions. See Figure 8.30.

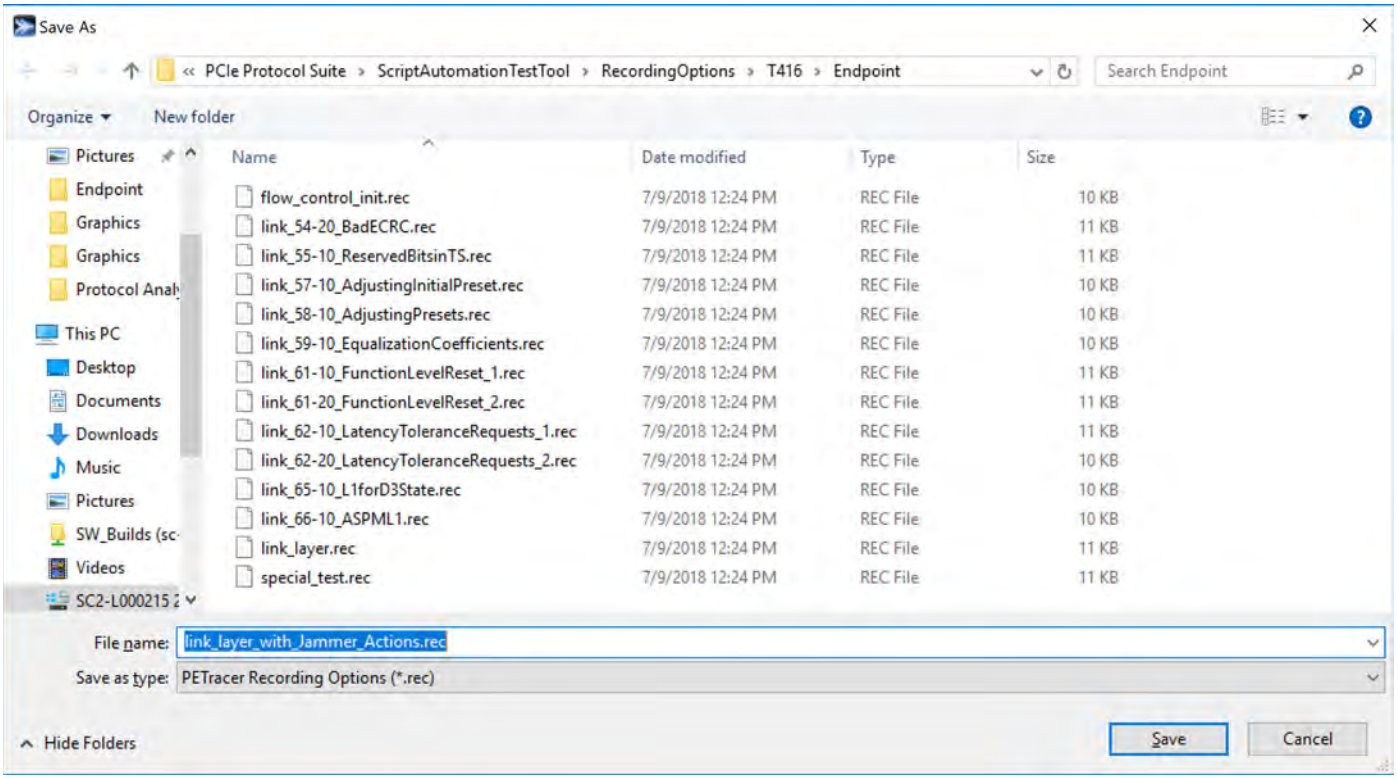


Figure 8.30: Save Jammer Script

Click on "Save" and the new Jammer Actions script will be saved, to be used in the future.

8.13 Loading a Jammer Script File

To load the Jammer Actions script file go to Setup -> Recording Options. Choose the Summit M5x and select Recording Rules.

Then select "Load" (see Figure 8.31).

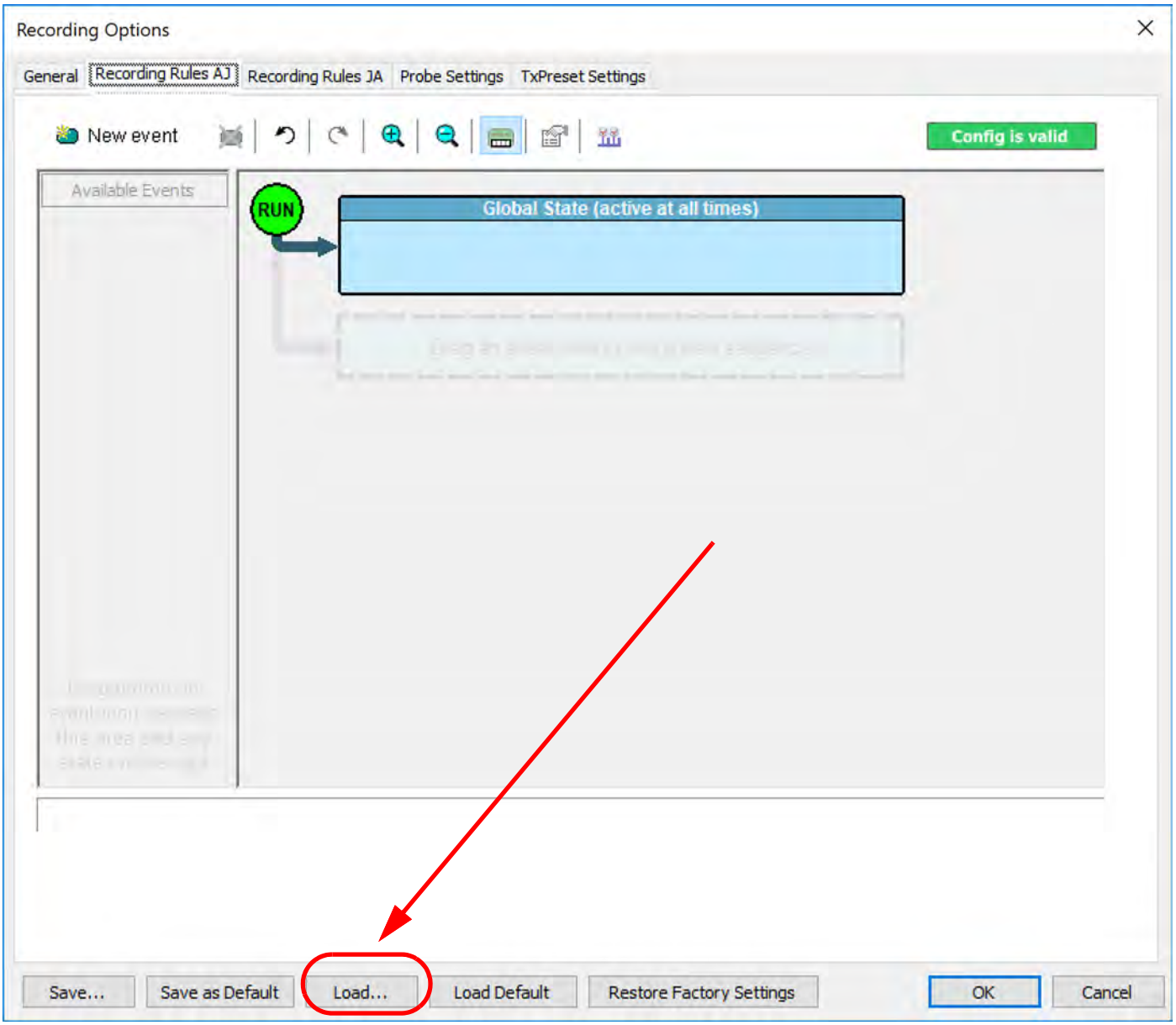


Figure 8.31: Loading a Jammer Action File

The Jammer Actions file will be available. See Figure 8.32 on page 471.

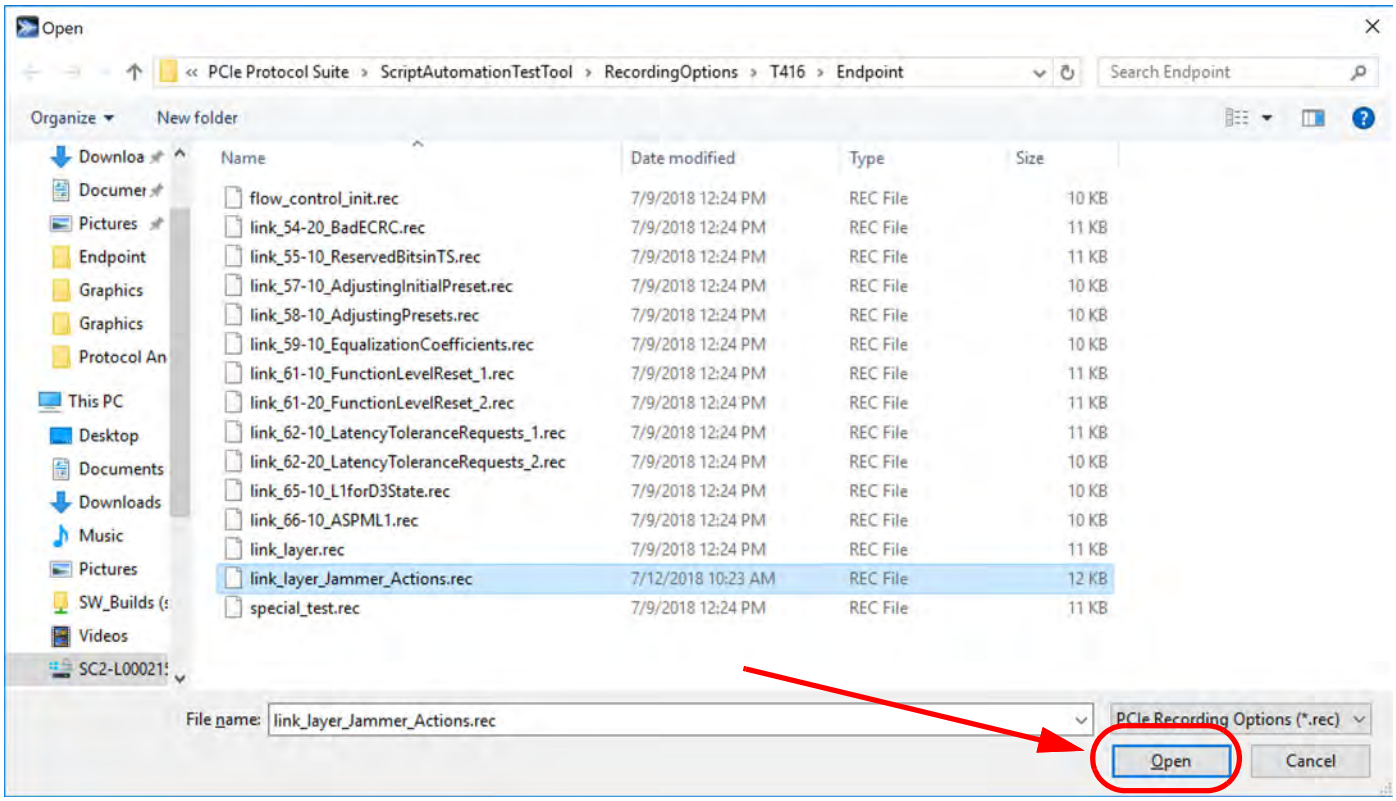


Figure 8.32: Jammer Actions File Loaded

Select the link_layer_Jammer_Actions.rec file and click on "Open". The file will be loaded as a script. See Figure 8.33 on page 472.

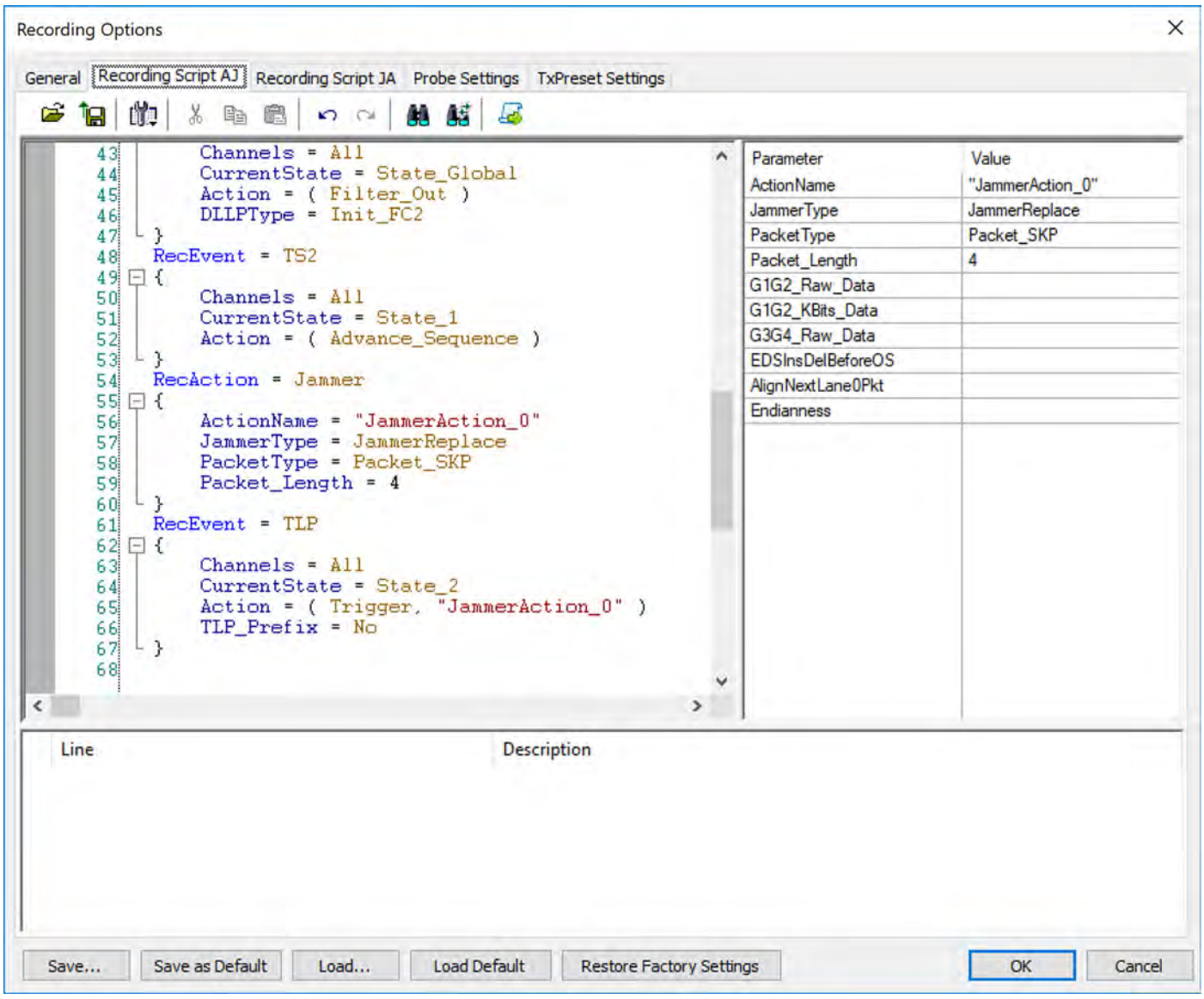


Figure 8.33: Jammer Action Script Loaded

If you want to see it in the GUI format, select General -> Advanced (see Figure 8.34 on page 473).

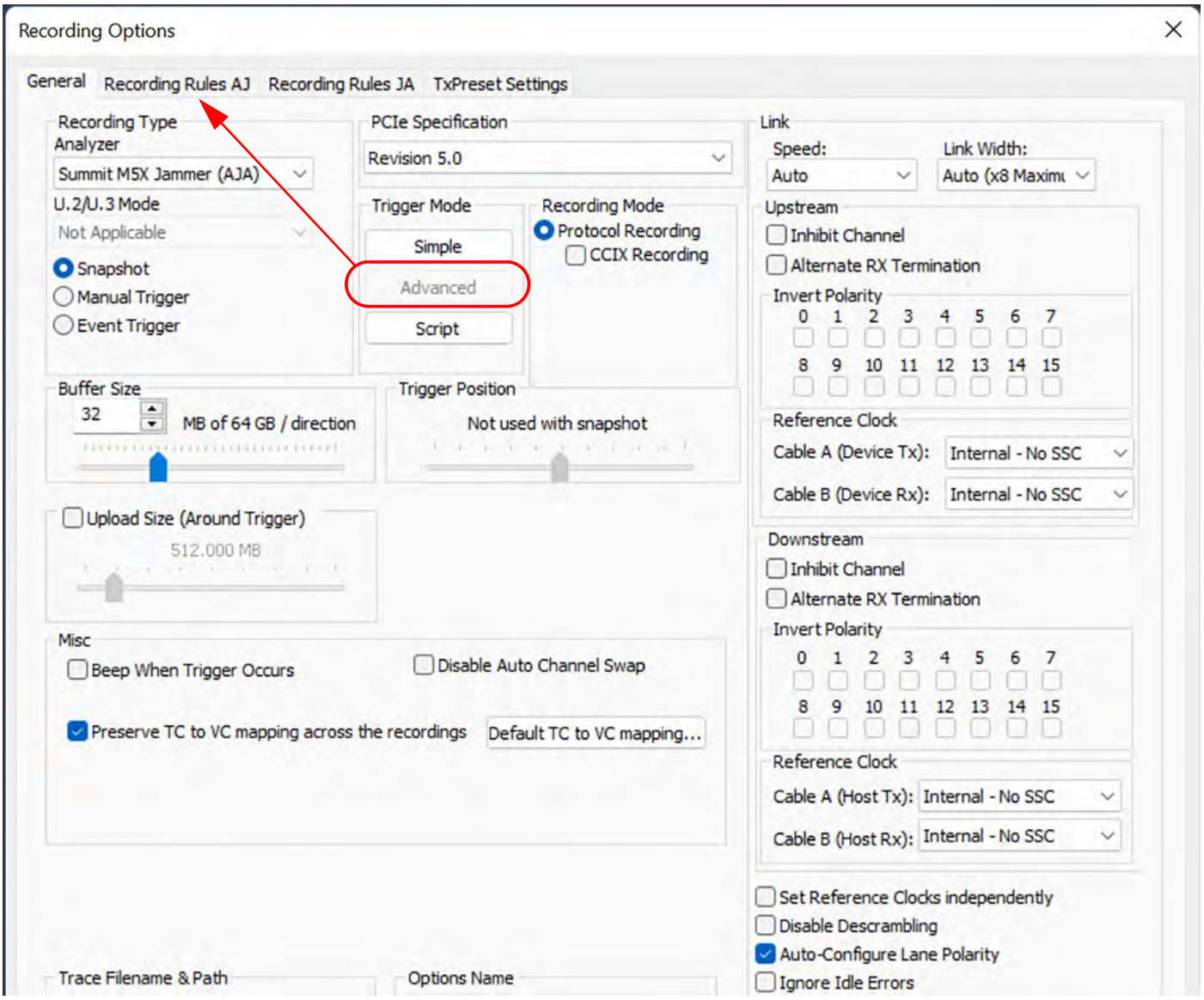


Figure 8.34: Recording Options: General -> Advanced

Select Advanced and the Recording Script tab will change to Recording Rules.

Select the Recording Rules tab and the GUI for the Jammer Actions file will pop up. See Figure 8.35 on page 474.

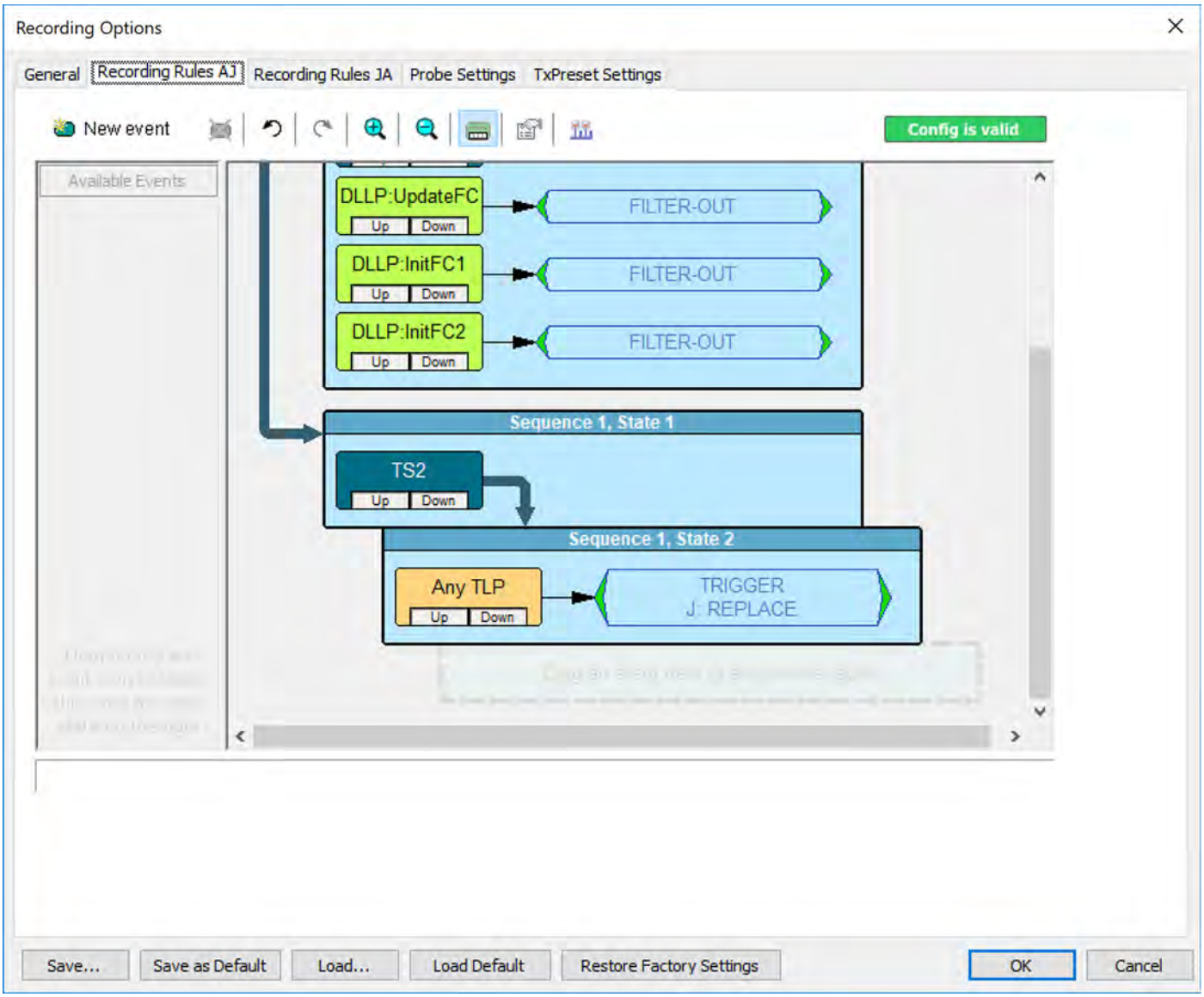


Figure 8.35: Jammer Action Script Loaded -> GUI

8.14 Examples of Scripting for Common Events with Jammer Actions

The following are examples common events and the script syntax for Jammer Actions:

TABLE 8.12: Jammer Actions

Event	Event Type
Link State	Speed Change
Ordered Set	TS2
Framing Token	EDS
Errors	Symbol Error
DLLP	Any

TABLE 8.12: Jammer Actions

Event	Event Type
TLP	Any
NVMe Register	
NVMe Command Submission	Any
NVMe Command Completion	Any

There are seven types of Jammer Actions which can be associated with any of the Events shown above:

- None
- Delete
- Replace
- Modify
- Insert Pkt X after
- Insert Error
- Sideband Signal

8.14.1 Link State: Speed Change

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

Then select New Event -> Link State -> Speed Change -> Insert Pkt X after

See GUI dialog below (see Figure 8.36 on page 476).

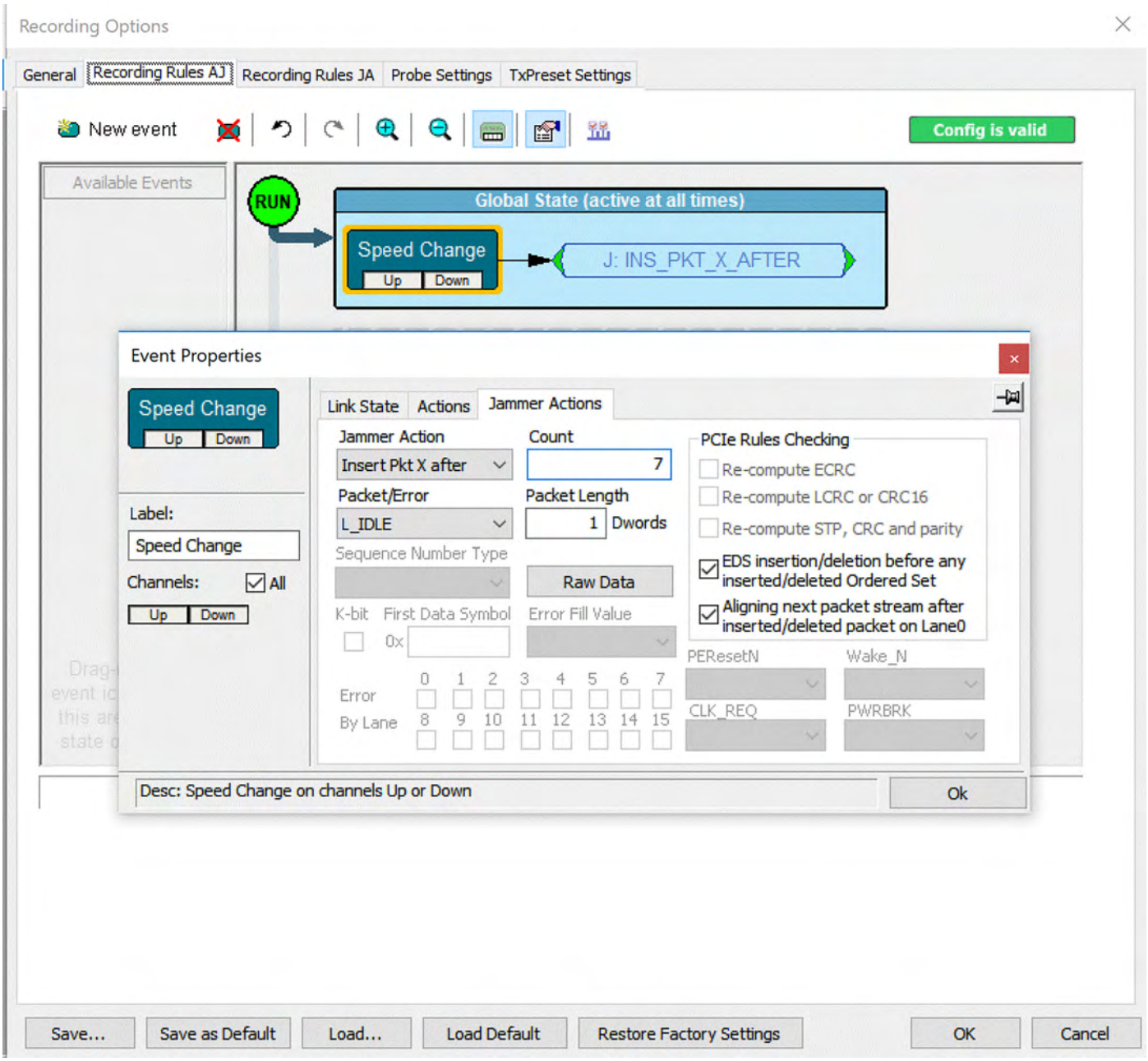


Figure 8.36: New Event: Link State -> Speed Change

Select the General tab to see the Script tab. See Figure 8.37 on page 477.

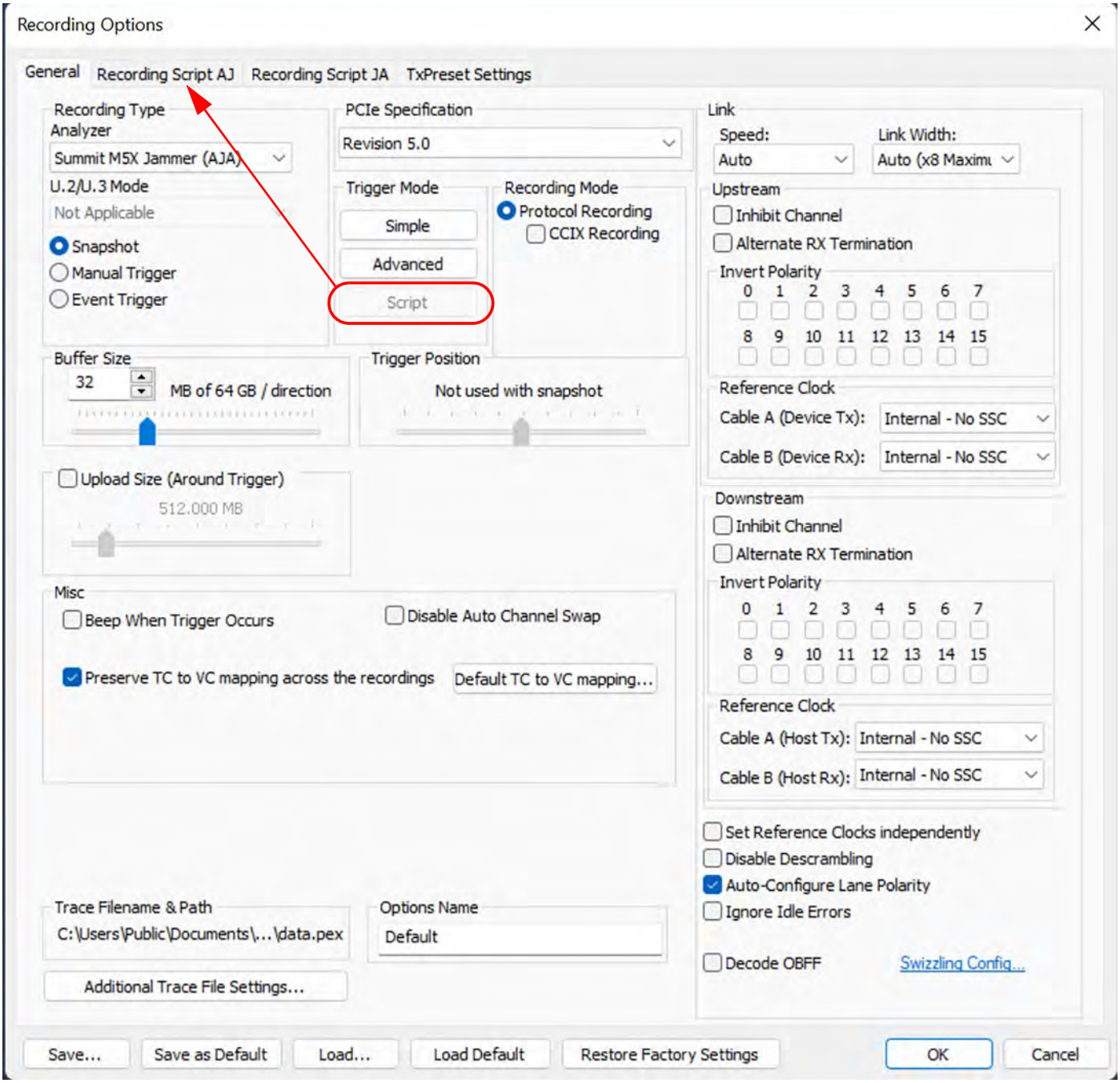


Figure 8.37: New Event: Link State -> Speed Change -> Insert Packet

Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 8.38 on page 478.

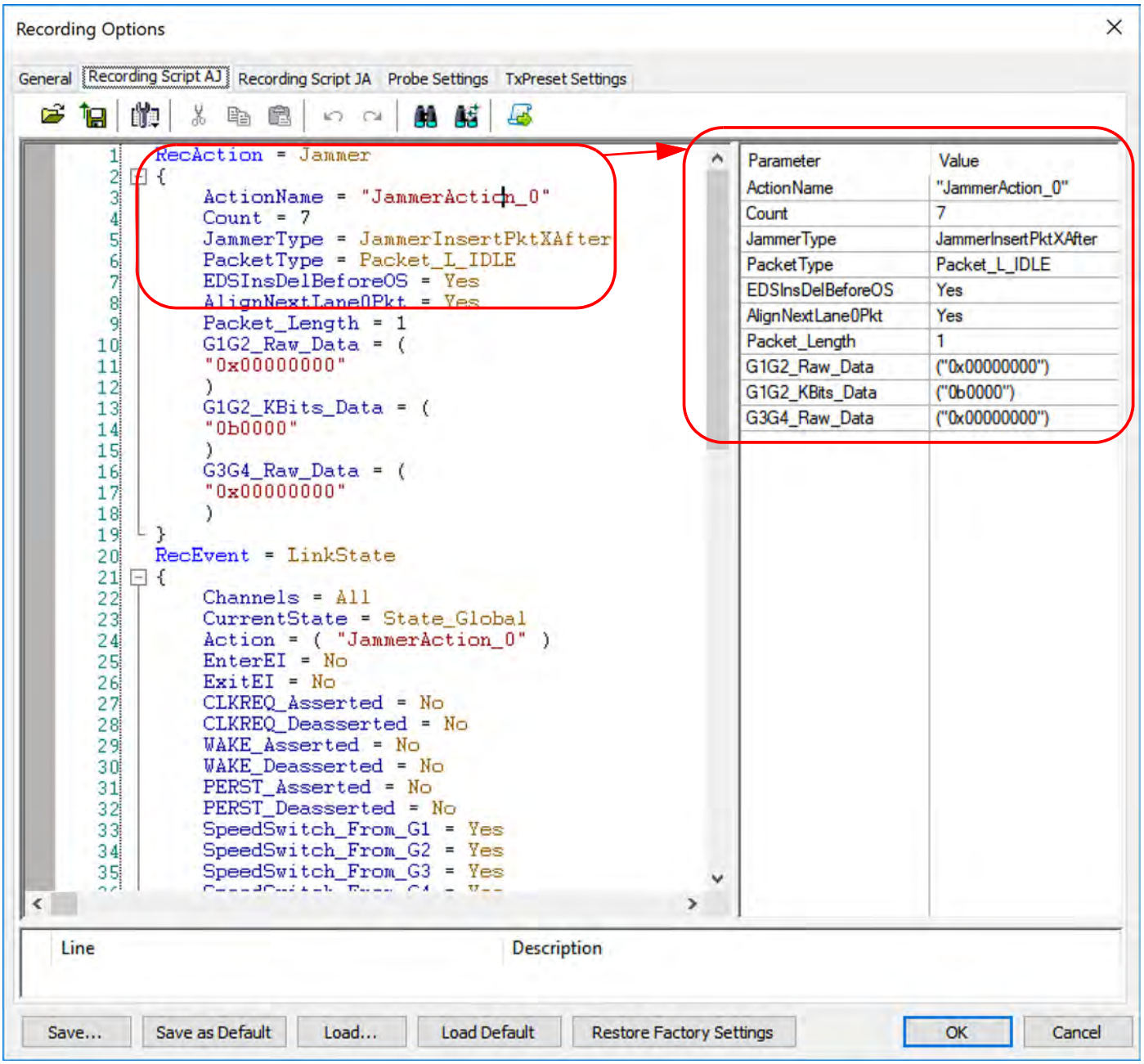


Figure 8.38: Jammer Action: Speed Change -> Insert Packet

8.14.2 Ordered Set: TS2

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Ordered Set -> TS2 -> Insert Error

See GUI dialog below in Figure 8.39.

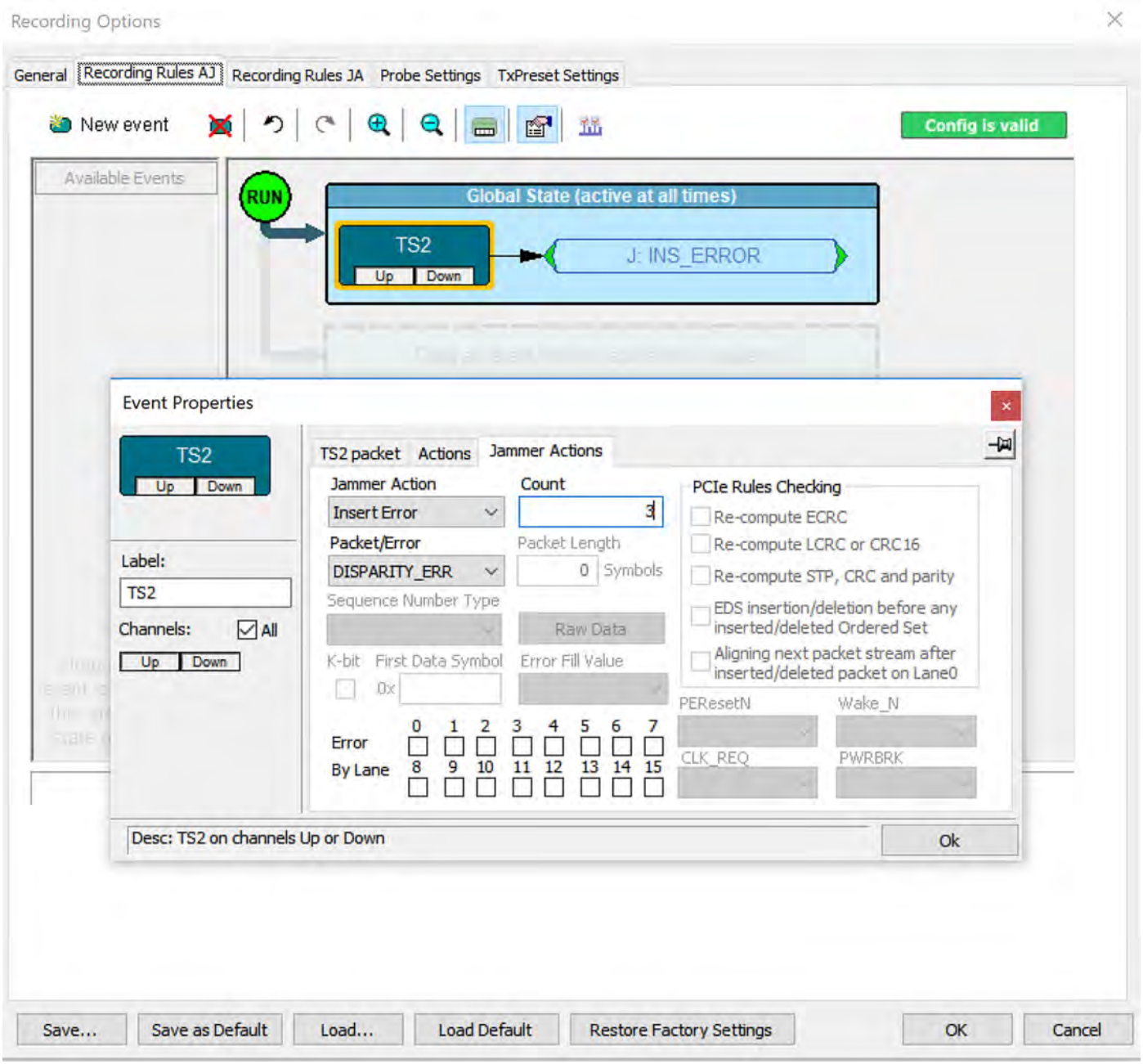


Figure 8.39: New Event: Ordered Set -> TS2 -> Insert Error

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 8.40 on page 480.

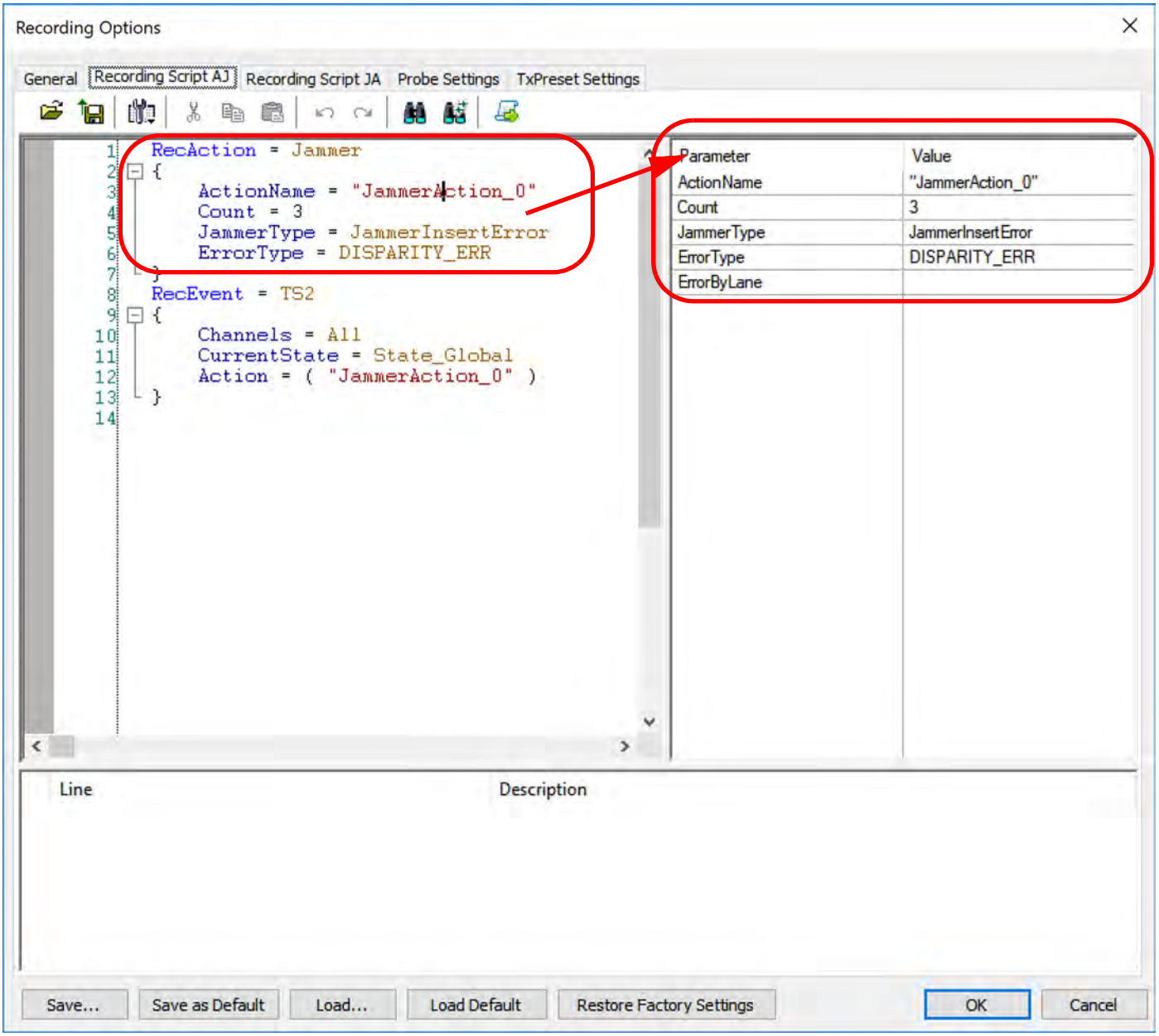


Figure 8.40: Jammer Action: Ordered Set -> TS2 -> Insert Error -> Disparity Error

8.14.2.1 Ordered Set: TS1

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Ordered Set -> TS1 -> Replace. See Figure 8.41 on page 481.

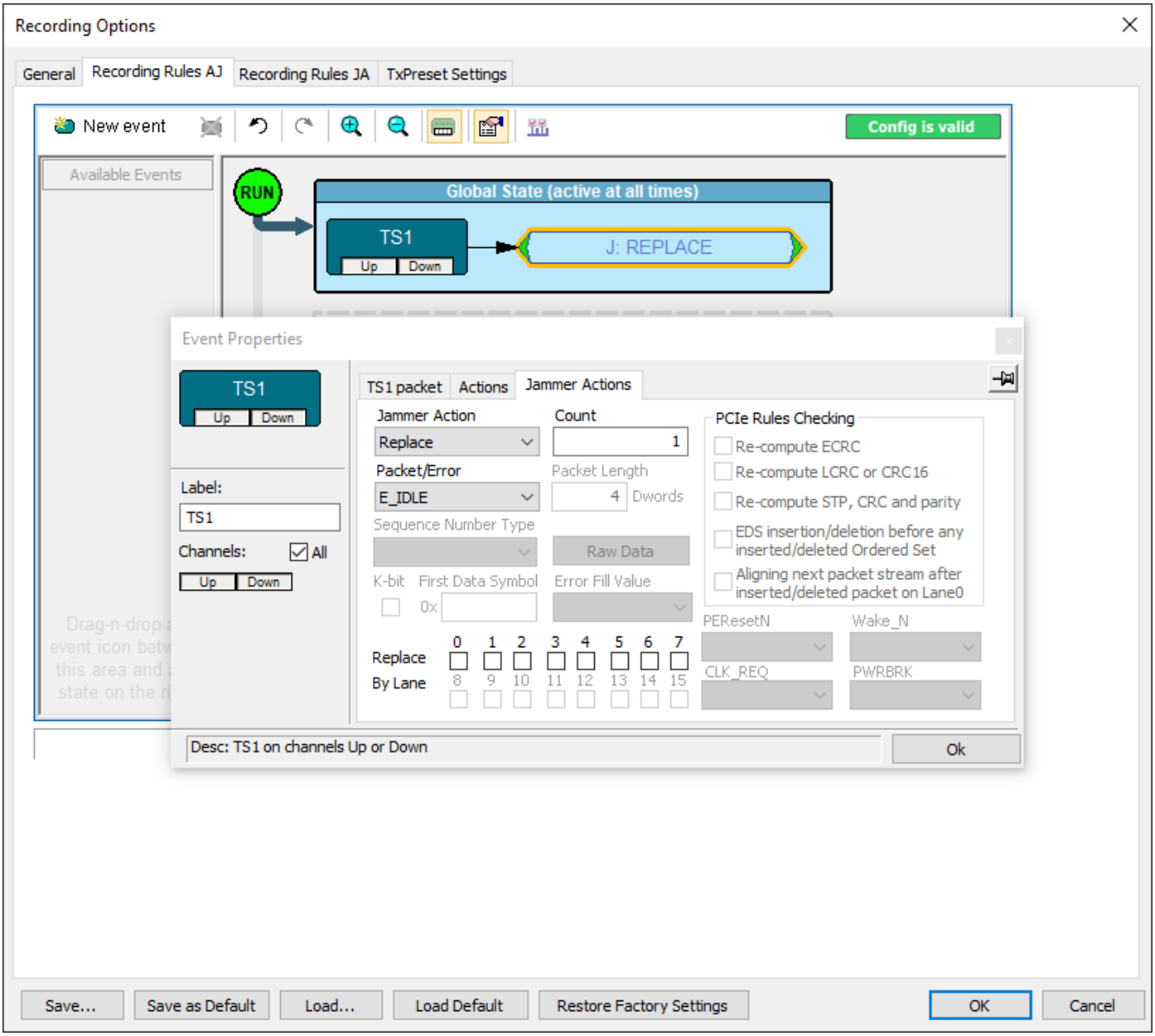


Figure 8.41: New Event: Ordered Set -> TS1 -> Replace

By default, jamming is enabled for all 8 lanes. It is possible to change jamming lanes by set checkboxes in the “Replace By Lane” section.

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 8.42 on page 482.

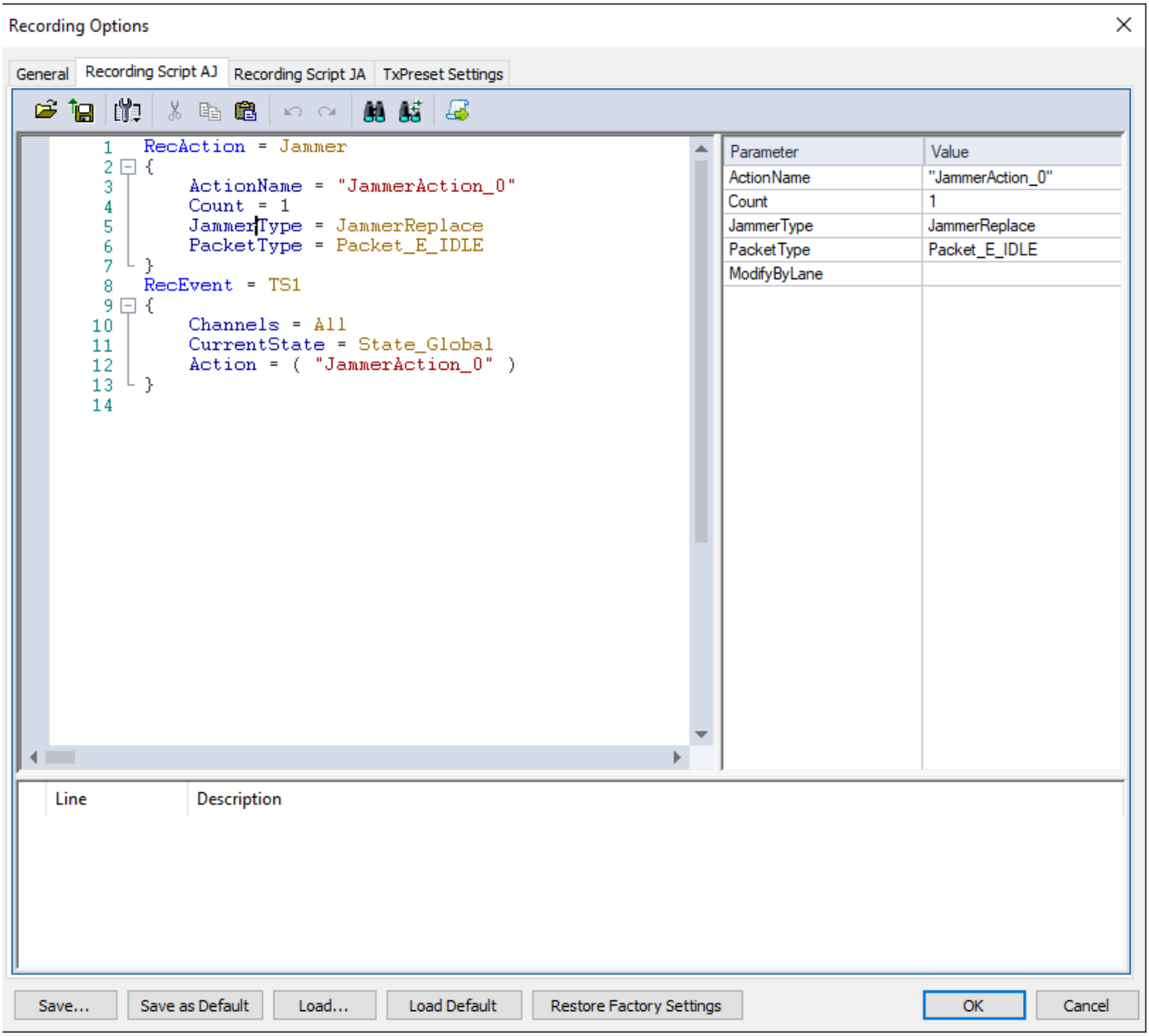


Figure 8.42: Jammer Action: Ordered Set -> TS1 -> Replace-> E_IDLE

8.14.3 Framing Token: EDS

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Framing Token -> EDS -> Delete

See GUI dialog below in Figure 8.43.

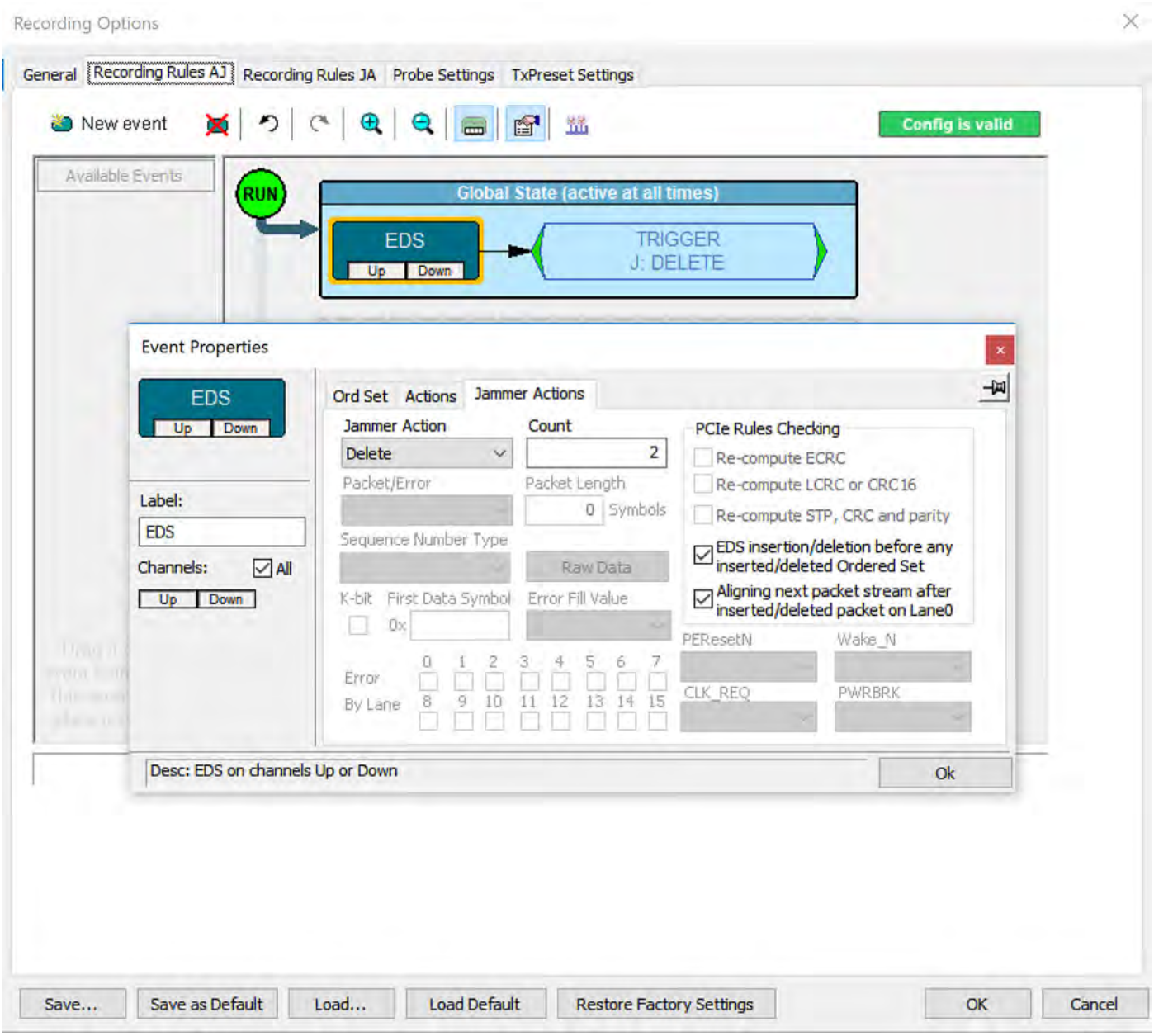


Figure 8.43: New Event: Framing Token -> EDS -> Delete

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 8.44 on page 484.

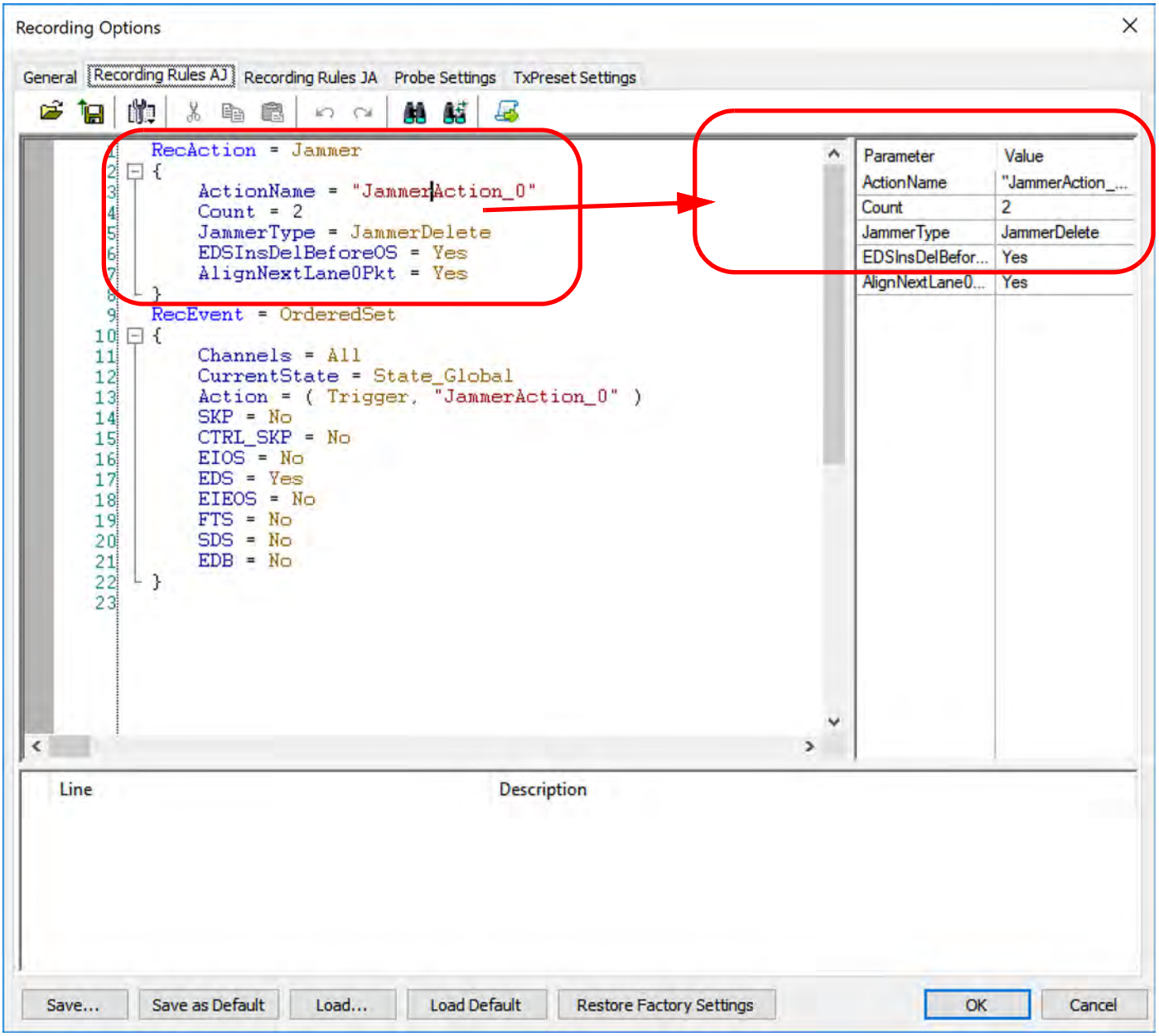


Figure 8.44: New Event: Framing Token -> EDS -> JammerDelete Script

8.14.4 Errors: Symbol Error

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> Errors -> Symbol Error-> Insert Pkt X after

See GUI dialog below in Figure 8.45.

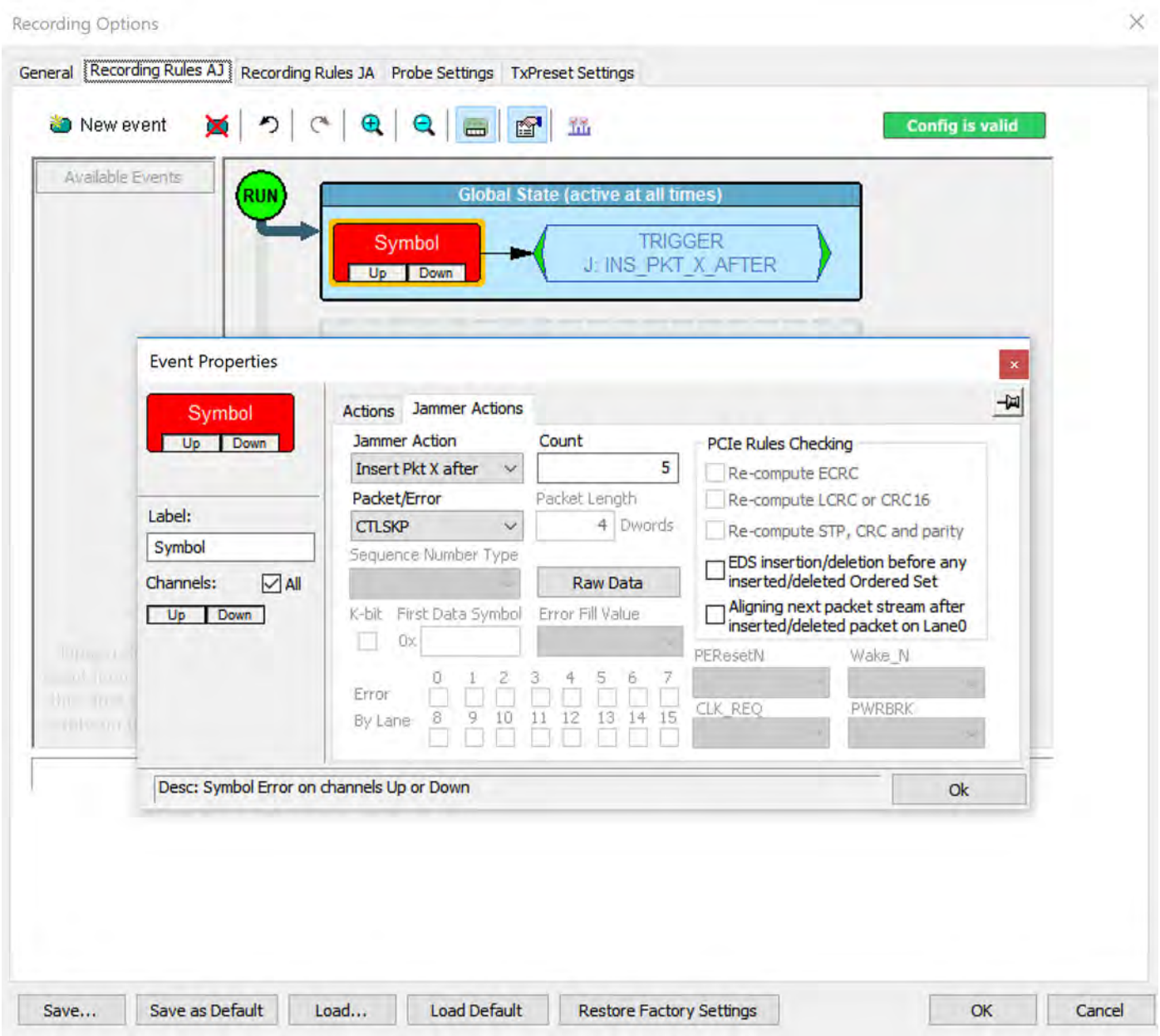


Figure 8.45: New Event: Errors -> Symbol Error-> Insert Pkt X after

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 8.46 on page 486.

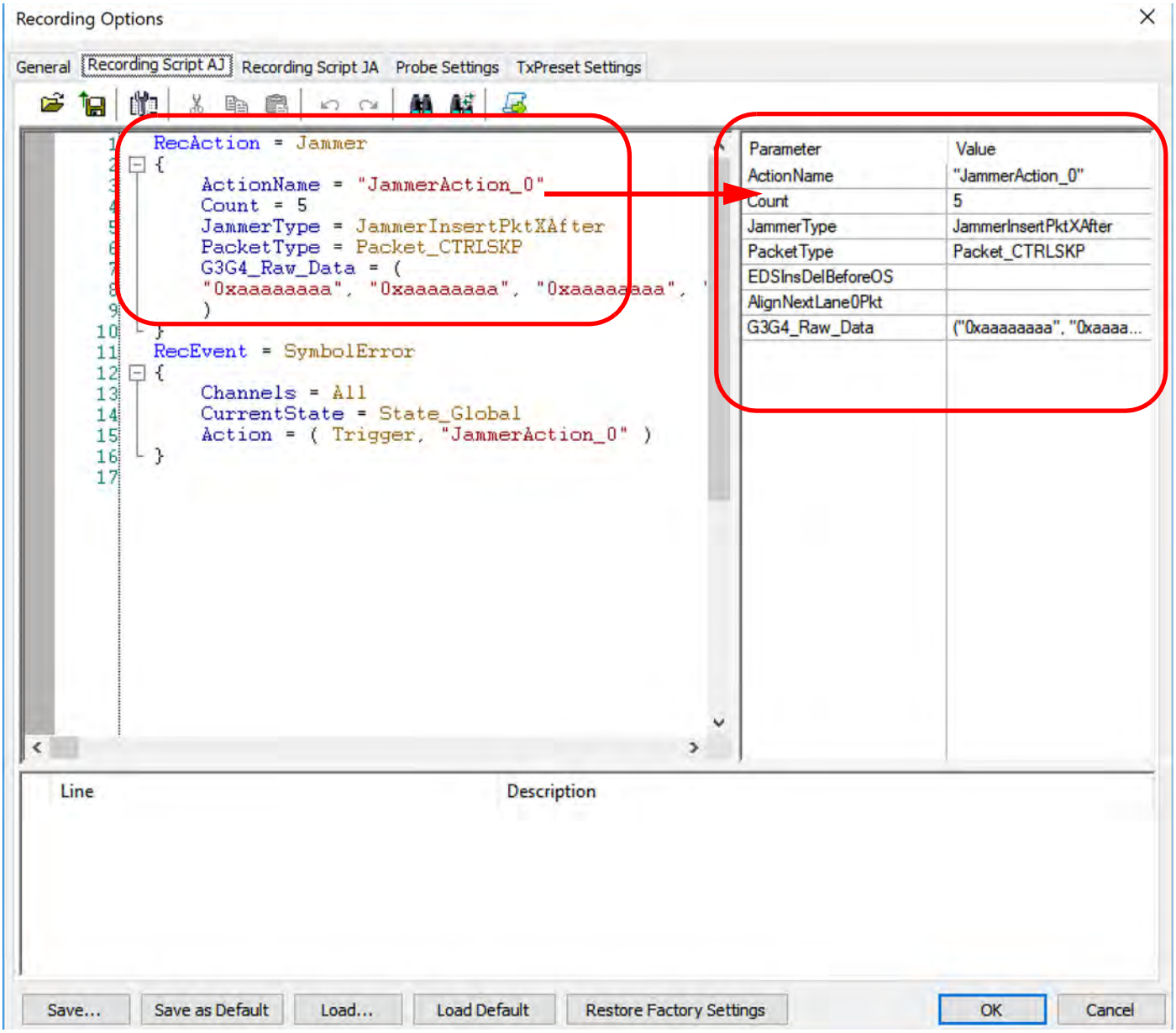


Figure 8.46: New Event: Errors -> Symbol Error-> Insert Script

8.14.5 DLLP: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> DLLP -> Any -> Replace (TS2_NUM_NUM)

See GUI dialog below in Figure 8.47.

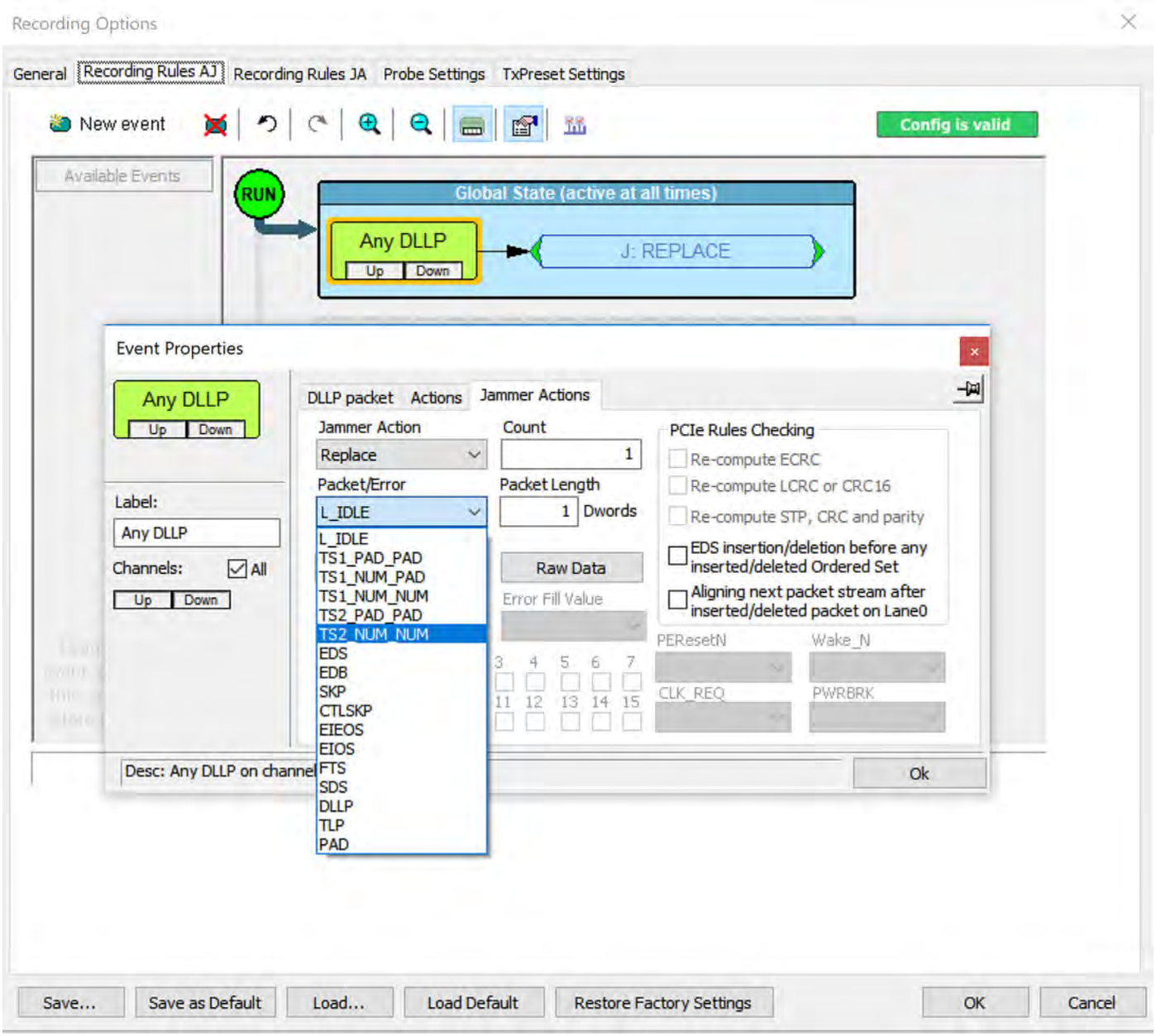


Figure 8.47: New Event: DLLP -> Any -> Replace (TS2_NUM_NUM)

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 8.48 on page 488.

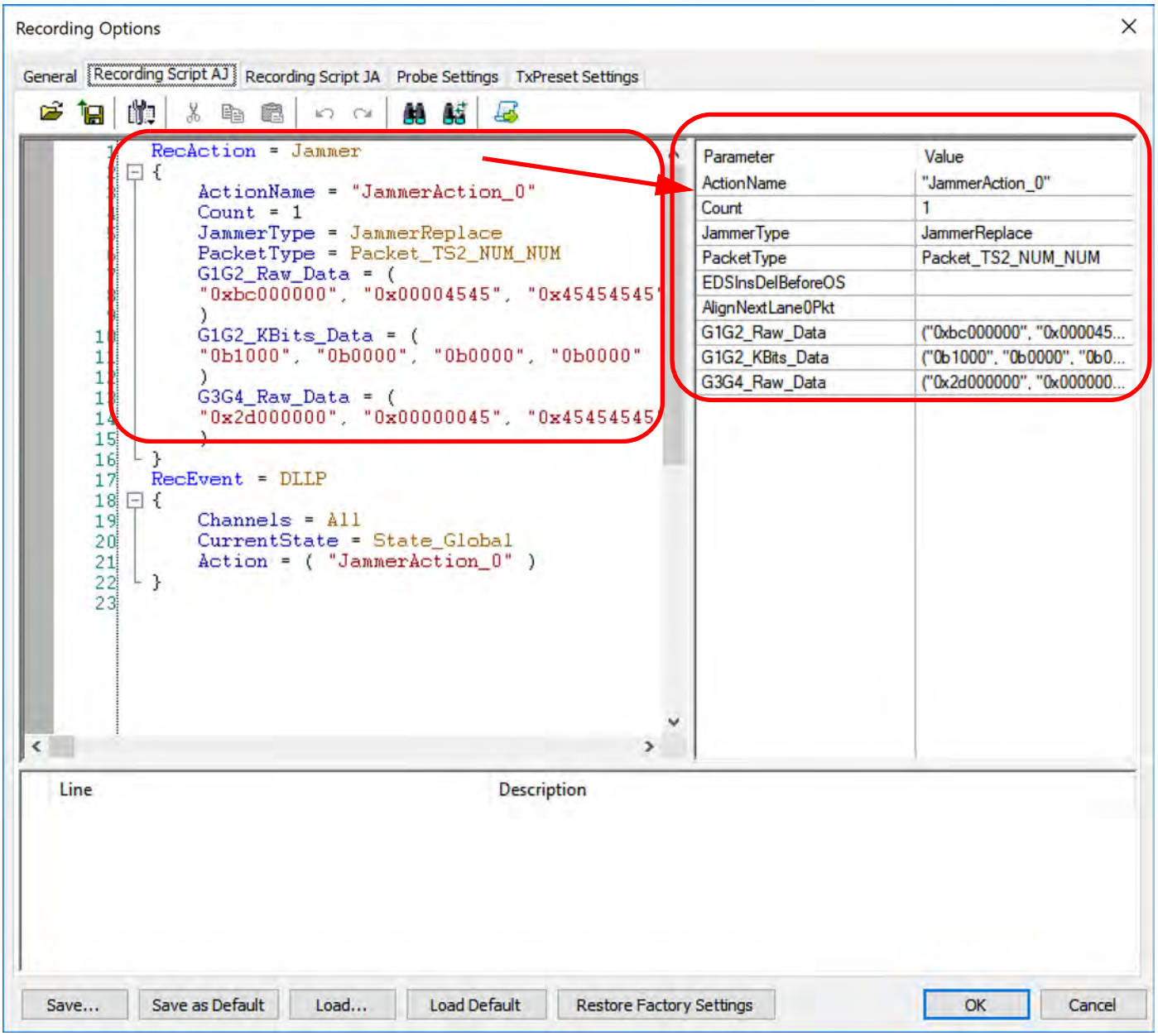


Figure 8.48: New Event: DLLP -> Any -> Replace (TS2_NUM_NUM) Script

8.14.6 TLP: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> TLP -> Any -> Modify

See GUI dialog below in Figure 8.49.

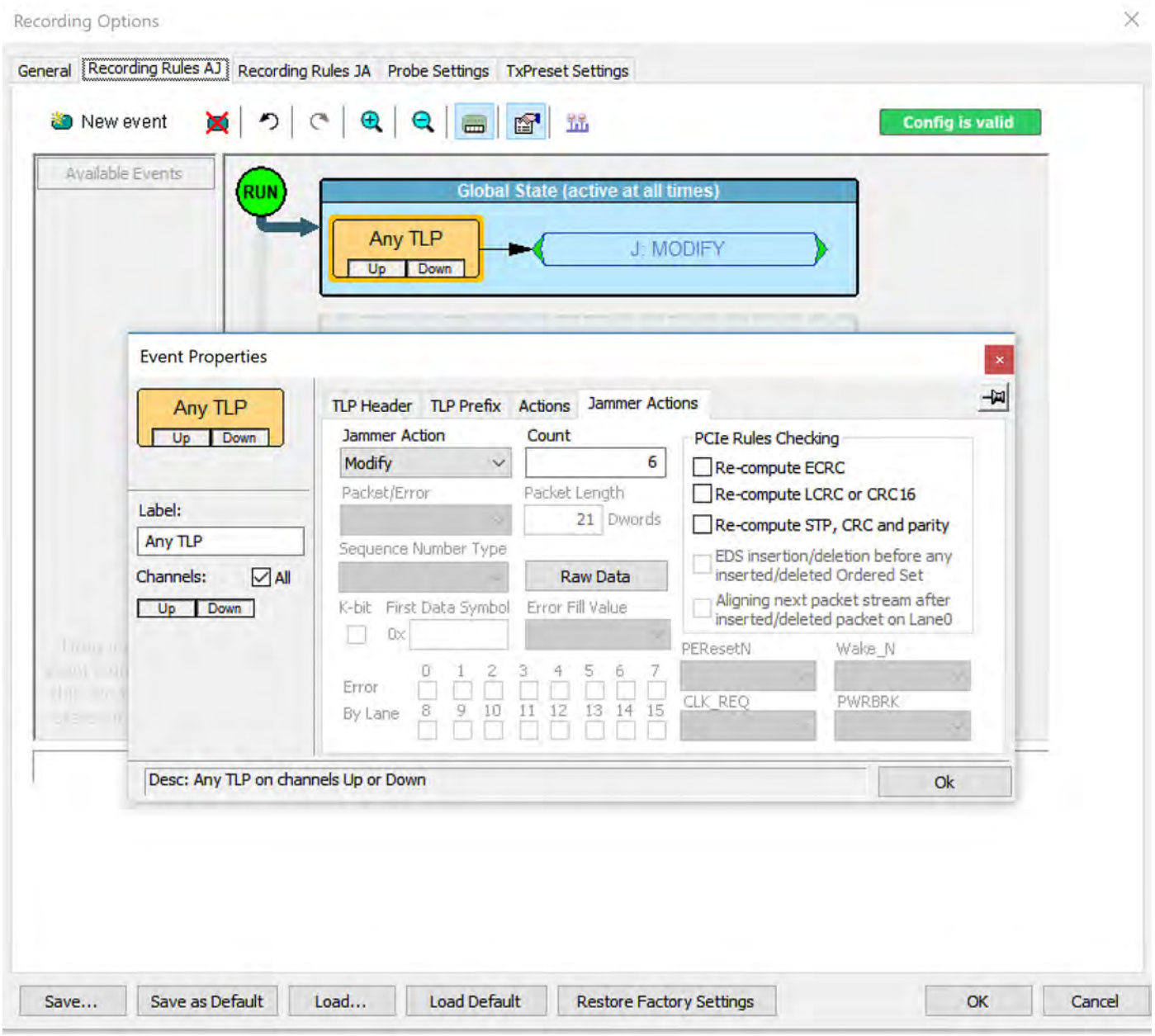


Figure 8.49: New Event: TLP -> Any -> Modify

Select the General tab to see the generated script. Now select Script, then click on the Recording Script tab. See the resulting script below in Figure 8.50 on page 490.

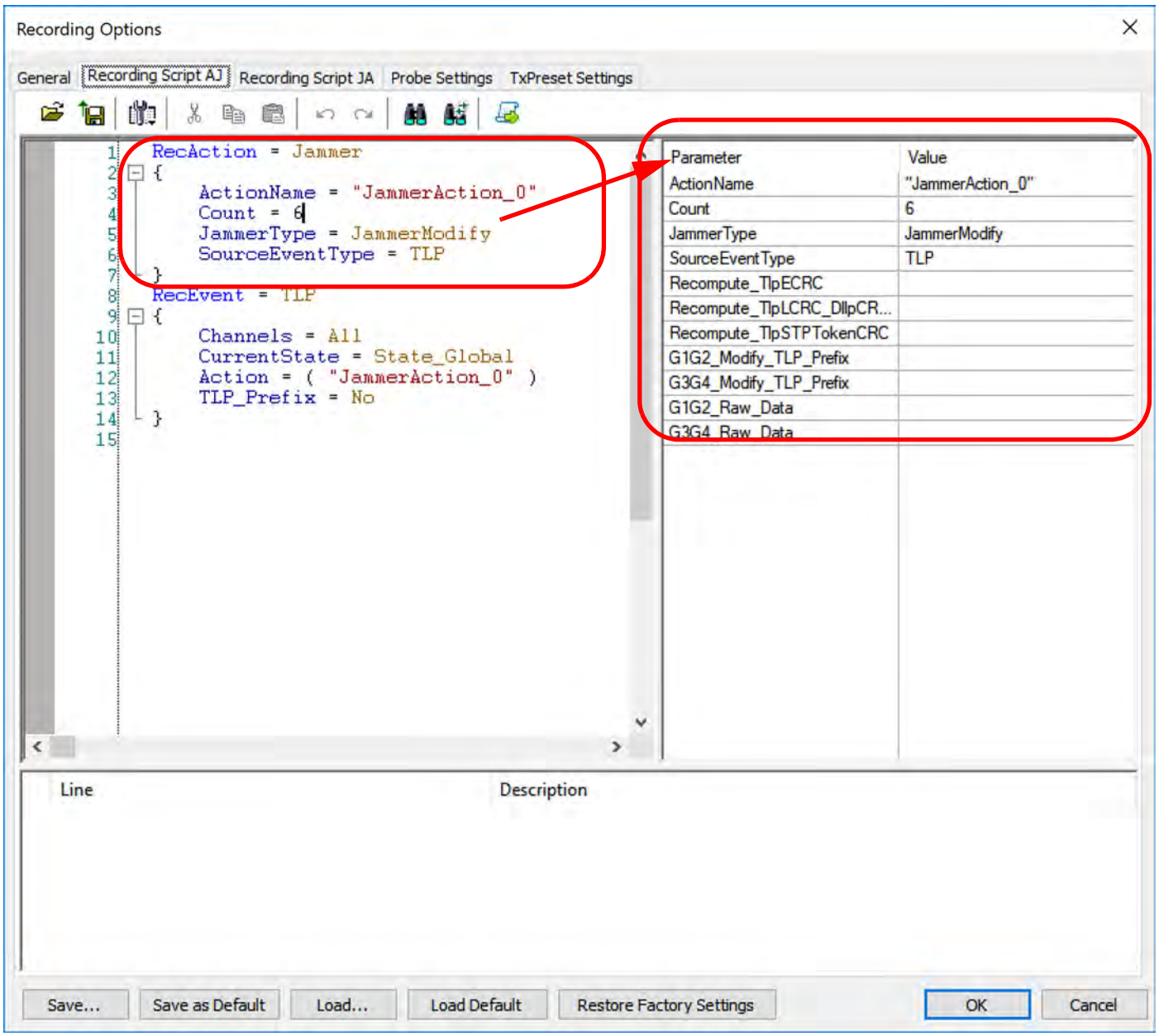


Figure 8.50: New Event: TLP -> Any -> Modify

8.14.7 NVMe

8.14.7.1 NVMe Register

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> NVMe Register -> ACQ -> Replace

See GUI dialog below in Figure 8.51.

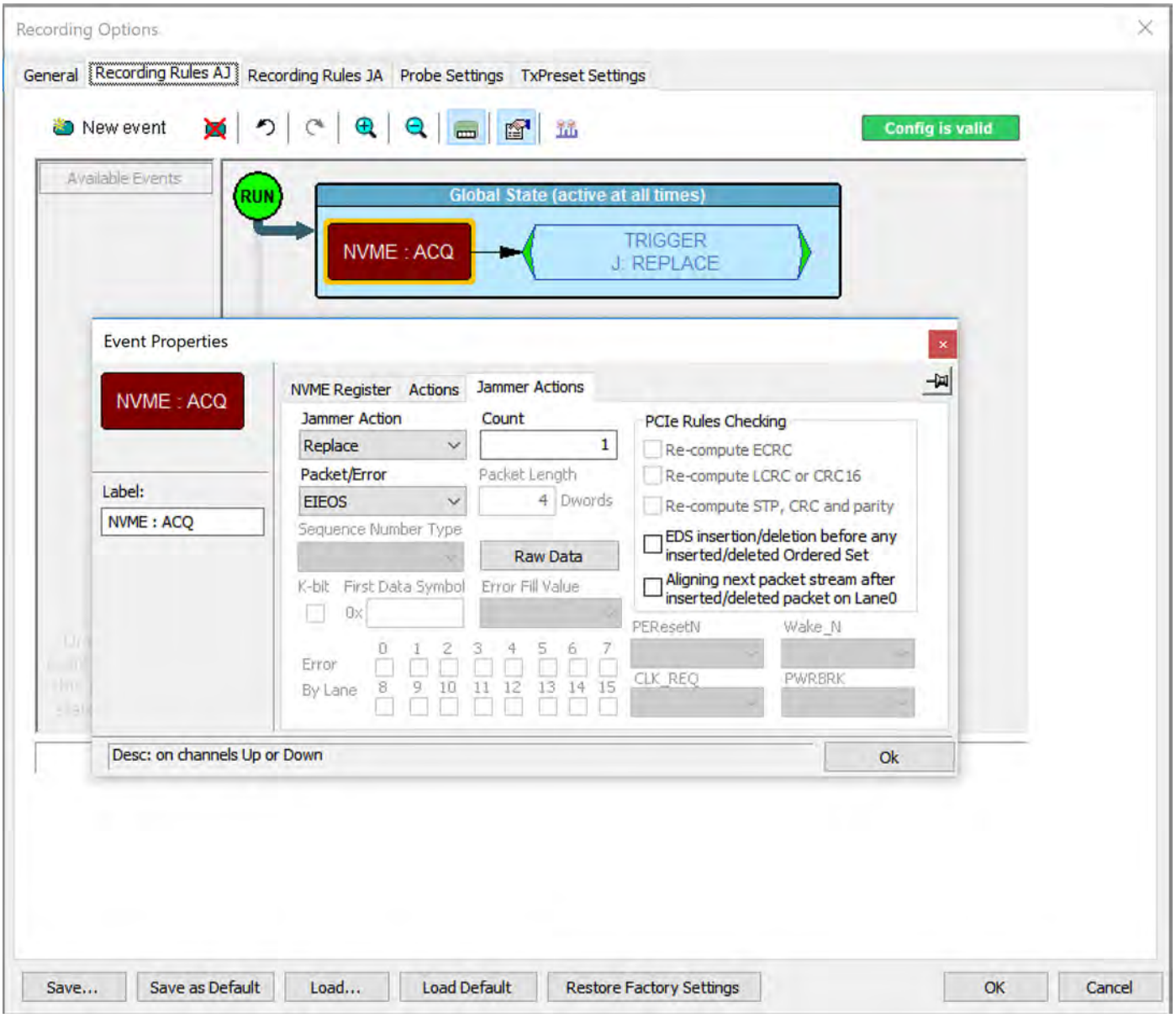


Figure 8.51: New Event: NVMe Register -> ACQ -> Replace

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 8.52.

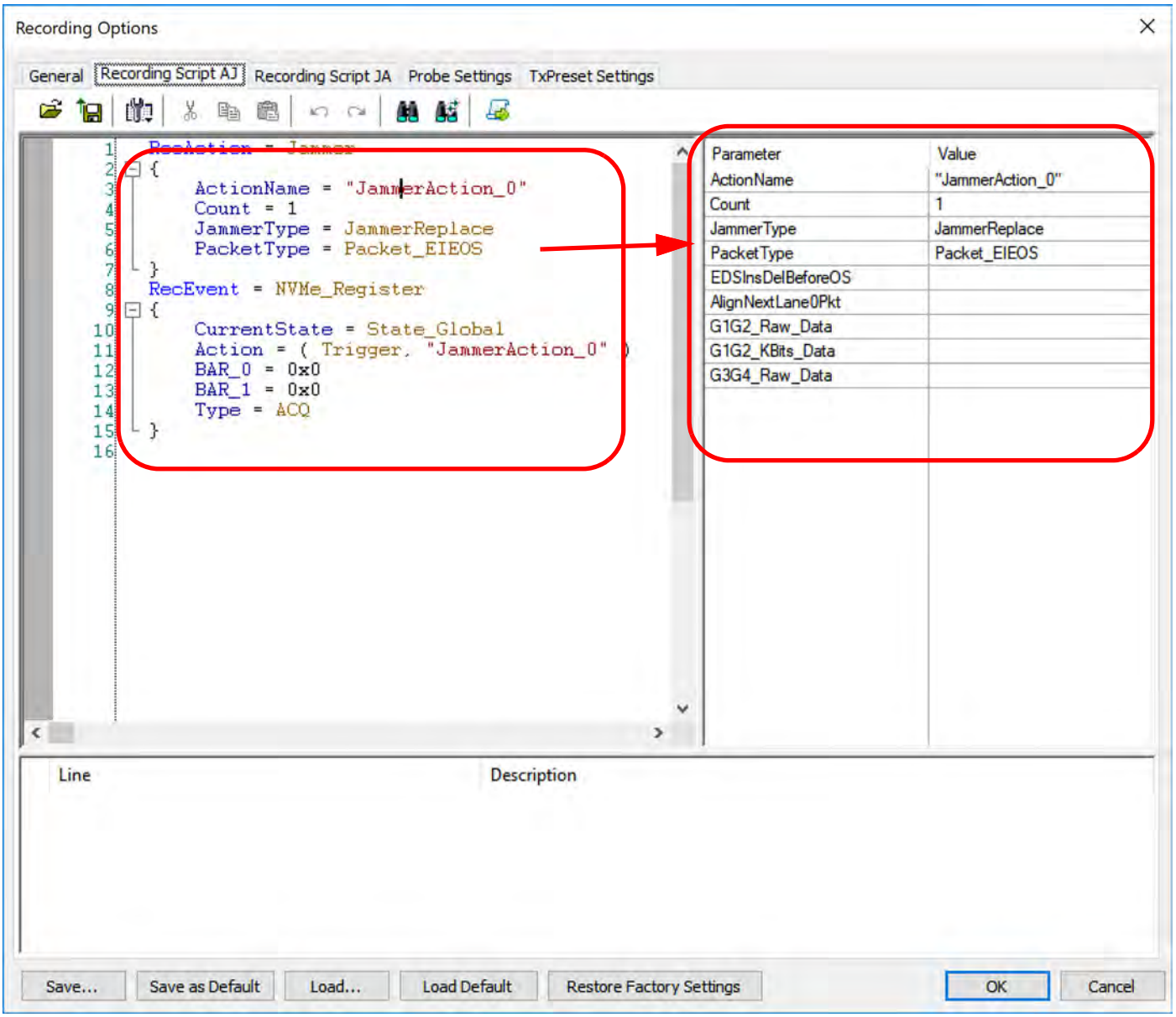


Figure 8.52: New Event: NVMe Register -> ACQ -> Replace Script

8.14.7.2 NVMe Command Submission: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> NVMe Command Submission -> Any -> Sideband

See GUI dialog below in Figure 8.53.

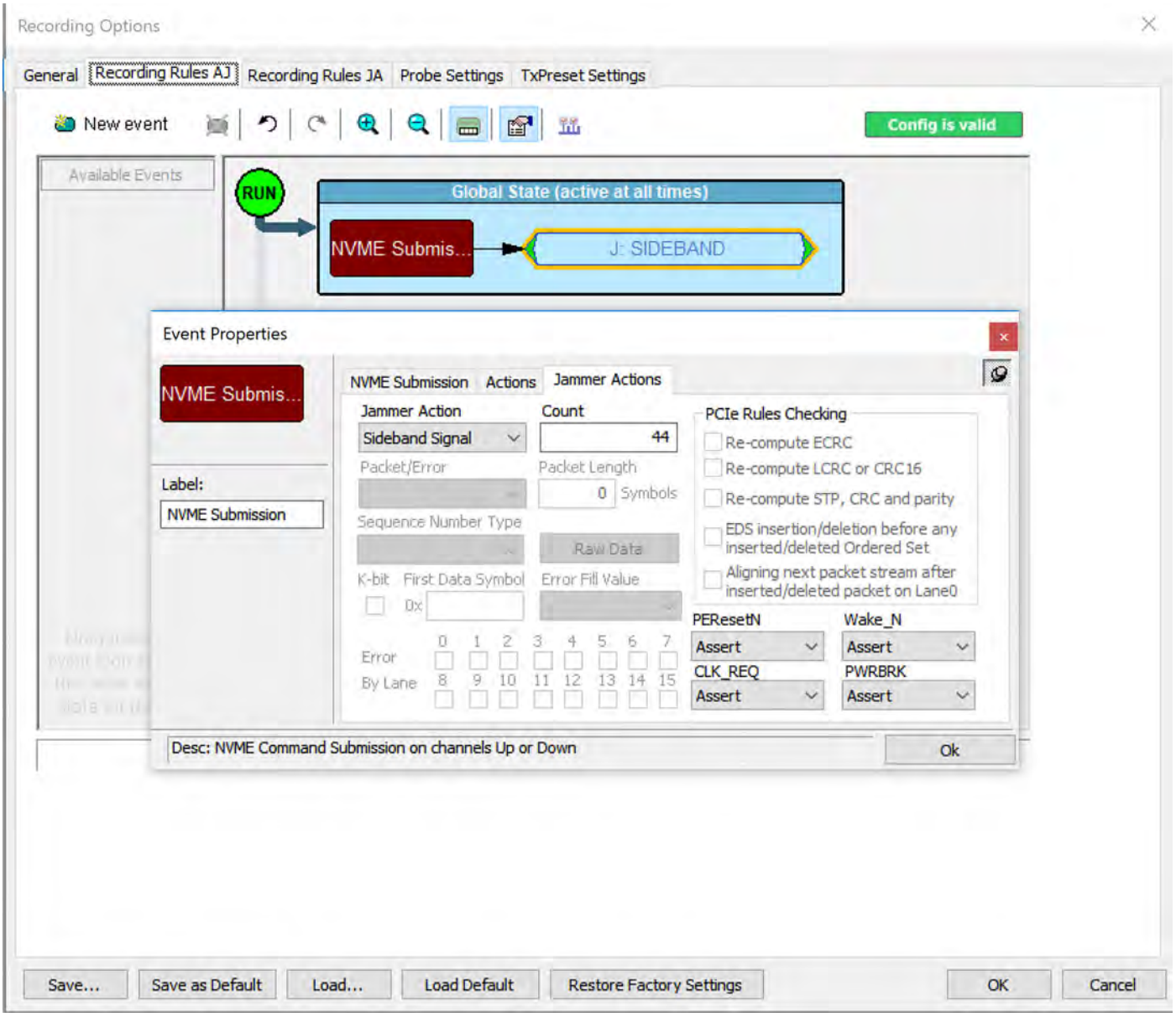


Figure 8.53: New Event: NVMe Command Submission -> Any -> Sideband

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 8.54 on page 494.

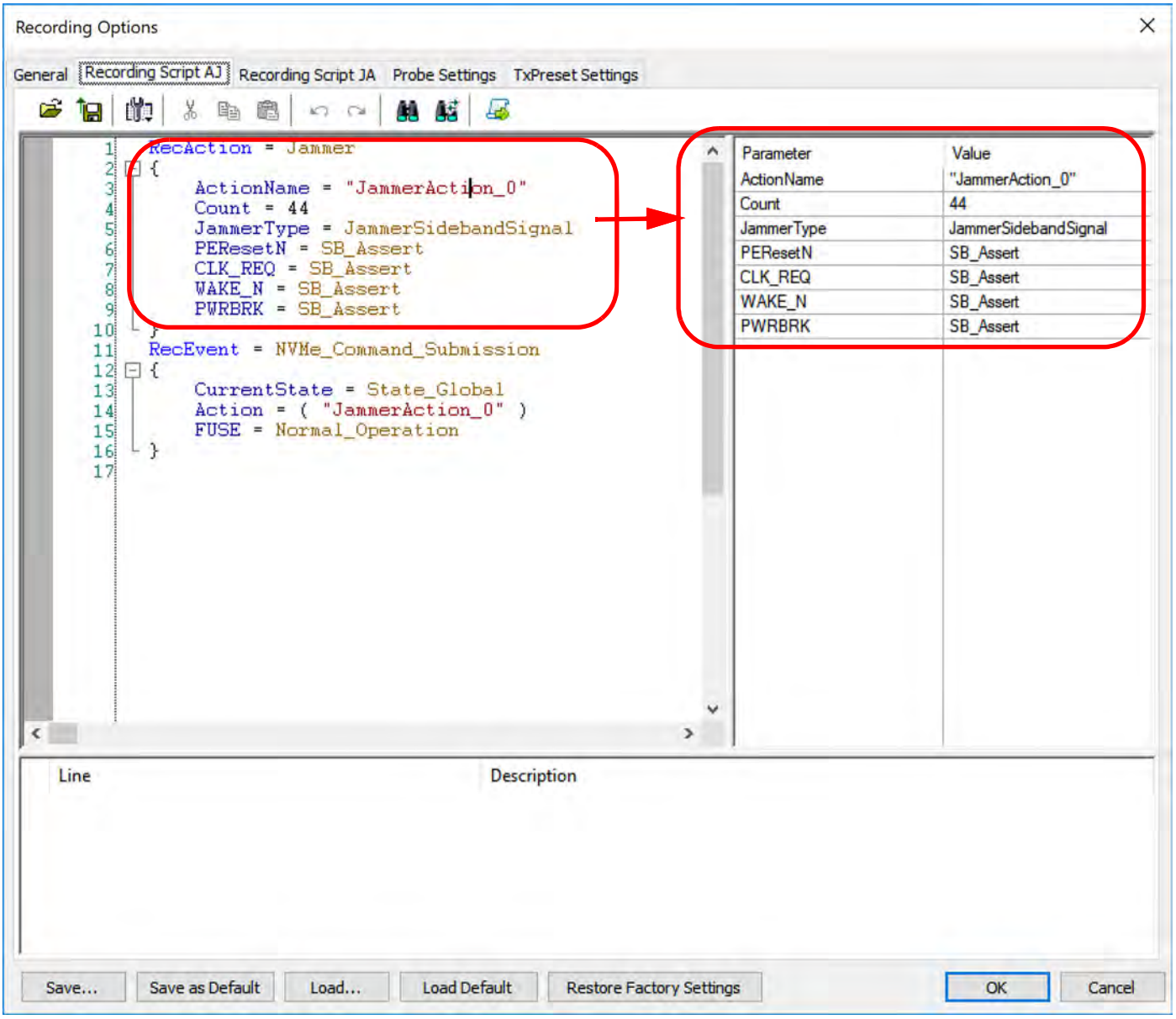


Figure 8.54: New Event: NVMe Command Submission -> Any -> Sideband Script

8.14.7.3 NVMe Command Completion: Any

Set up the PCIe Protocol Analysis software for the Summit M5x -> Set -> Recording Options -> Recording Rules.

The select New Event -> NVMe Command Completion -> Any -> Replace

See GUI dialog below in Figure 8.55.

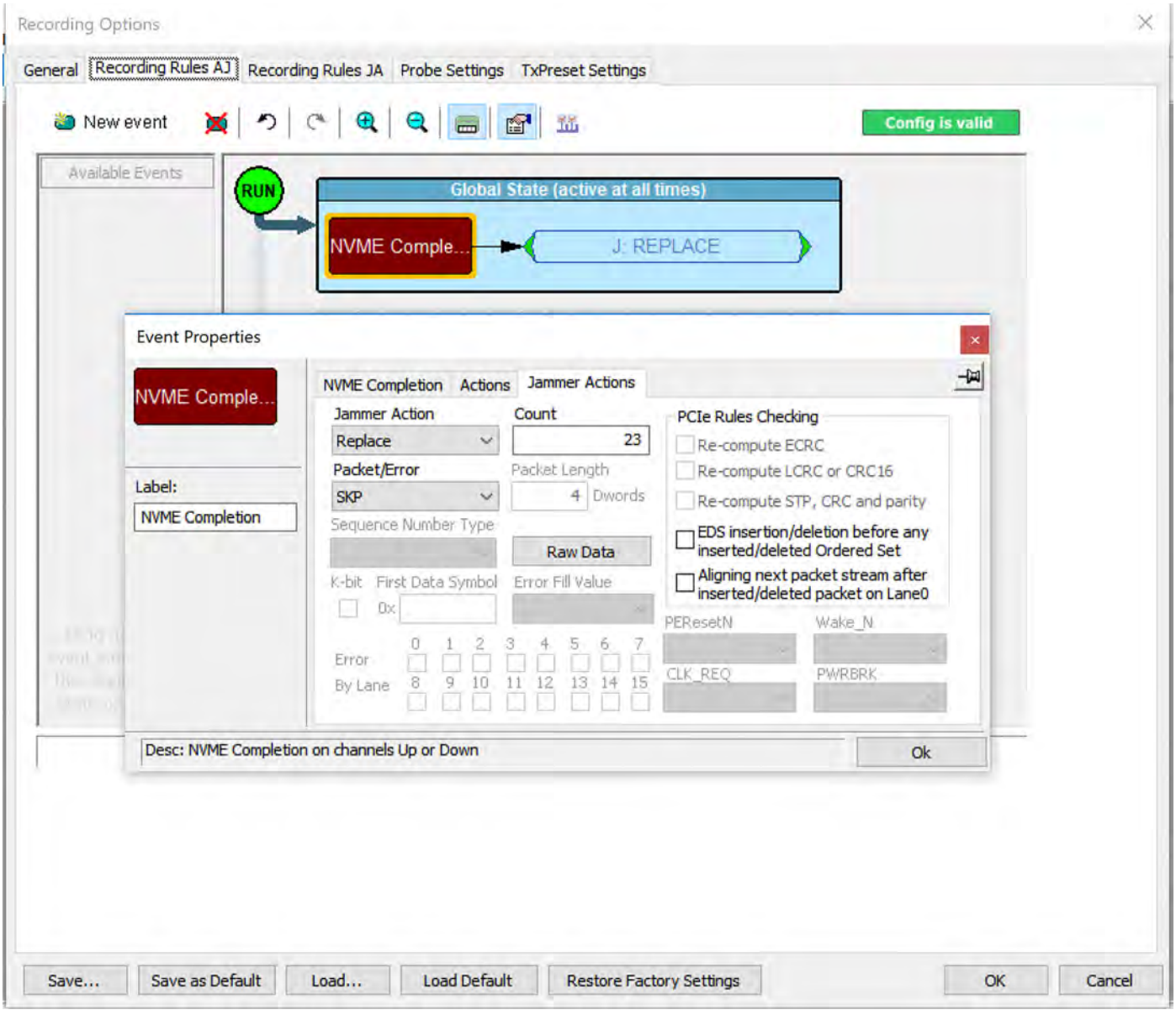


Figure 8.55: New Event: NVMe Command Completion -> Any -> Replace

Select the General tab to see the generated script.

Now select Script, then click on the Recording Script tab.

See the resulting script below in Figure 8.56 on page 496.

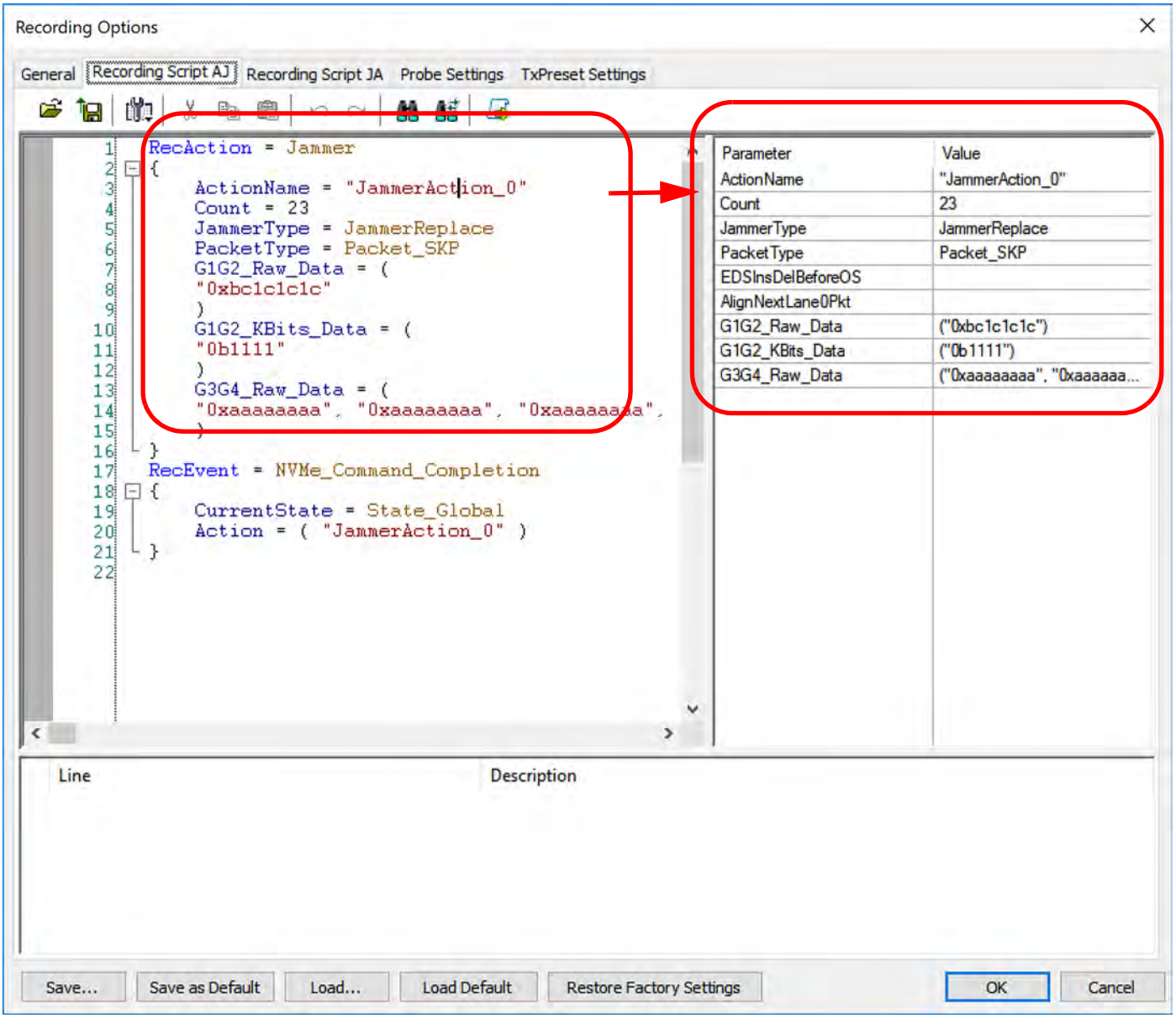


Figure 8.56: New Event: NVMe Command Completion -> Any -> Replace Script

8.15 Jammer Mode Overview (AJA)

The Summit M5x can modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint to verify adherence to design specifications and identify potential errors in protocol behavior. The Summit M5x also introduces for the first time NVMe and NVMe-MI protocol jamming as well. The analyzer and jammer combination features on the Summit M5x make this a powerful testing tool for PCIe validation and development labs. This Jammer and Scripting capability is built into the PCIe Protocol Analysis software.

In addition the Summit M5x can also display the results of the Jamming operation. In one product you can analyze a stream of traffic, modify, replace, insert or delete real-time traffic between a PCIe root complex and endpoint and then see the results of that jamming operation.

To select this mode of operaton in the Recording Options menu select Summit M5x Jammer AJA (Advanced). See Figure 8.57 on page 498.

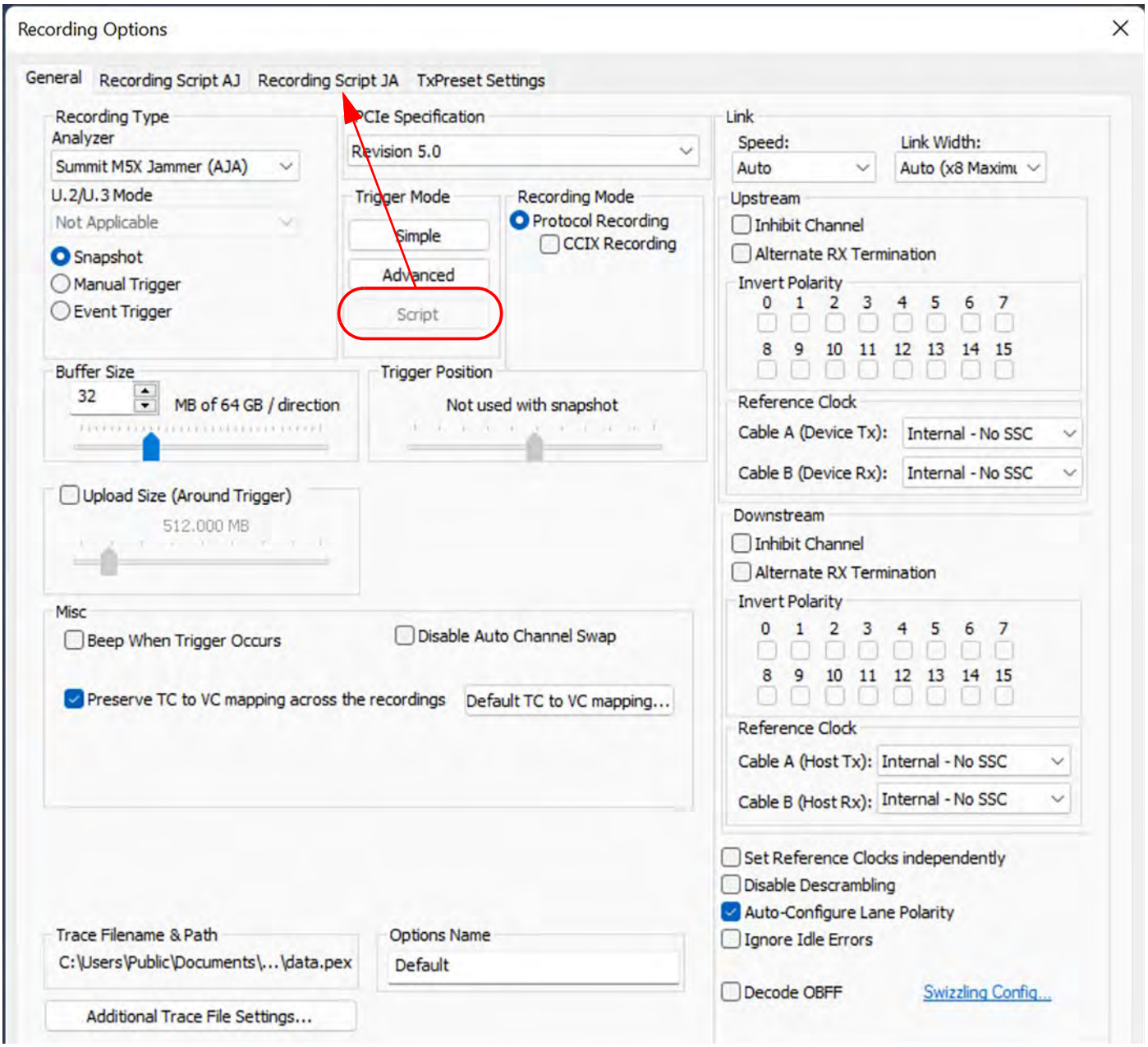


Figure 8.57: Selecting the Summit M5x AJA Mode for Recording

The Recording Rules JA tab is very similar to the Recording Rules AJ as explained in “Recording Options: Recording Rules (AJ)” on page 442 with the exception that there are no Jammer Rules options.

To generate a script you’d use the same methodolgy as shown in “Converting Recording Rules and Jammer Actions from GUI to Script File (AJ)” on page 444.

In the section below several examples of traces using the Analyzer/Jammer/Analyzer (AJA) are shown and described in detail.

8.15.1 Examples of AJA Traces (Jammer Actions and Results)

8.15.1.1 Delete: UpdateFC_P DLLP Packet

In the first example we **Delete an UpdateFC_P DLLP**. The loaded trace is shown in Figure 8.58. The tooltips associated with the Jammer function are also shown.

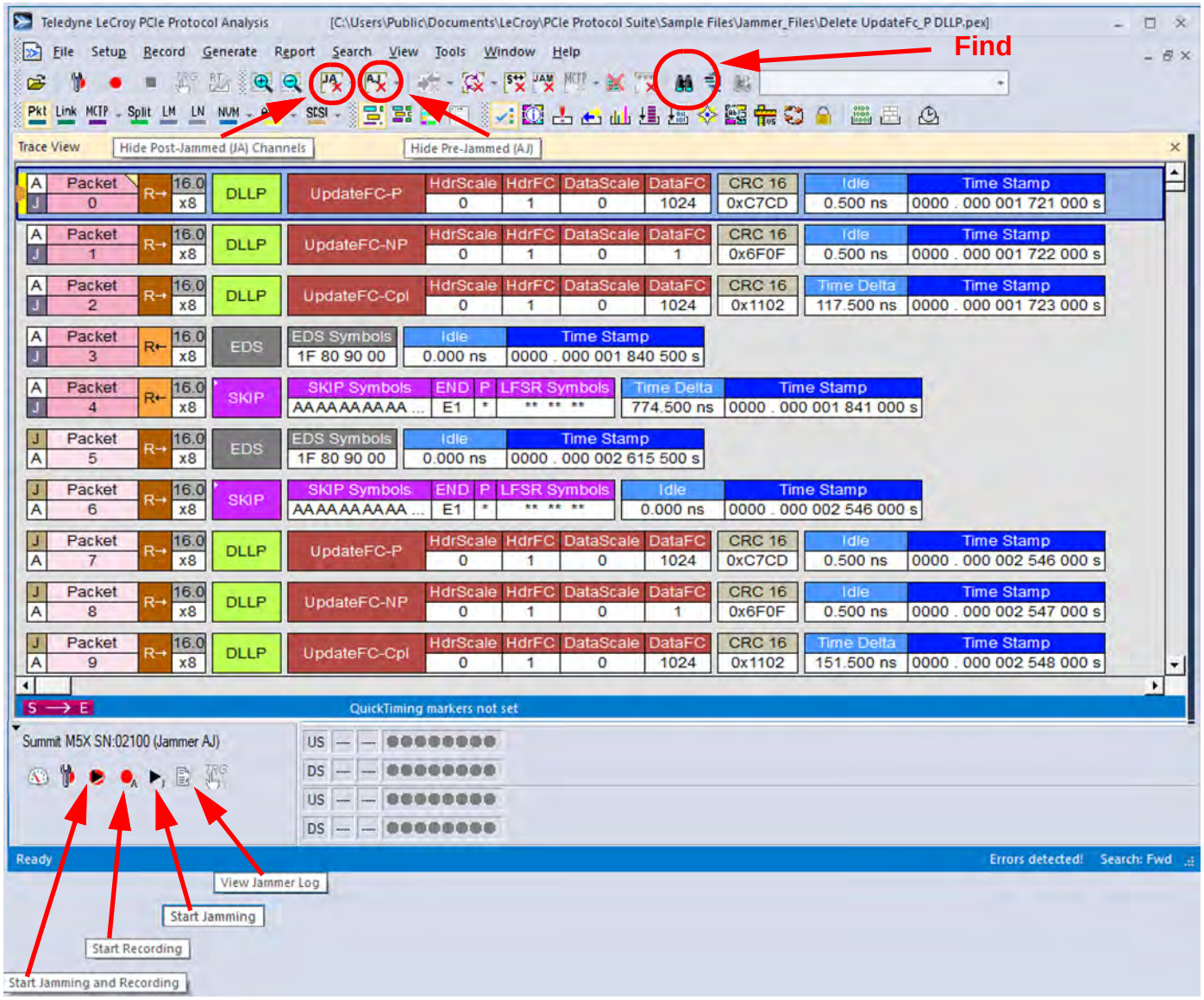


Figure 8.58: AJA Trace: Delete UpdateFc_P DLLP with tooltips

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 8.59 on page 500.

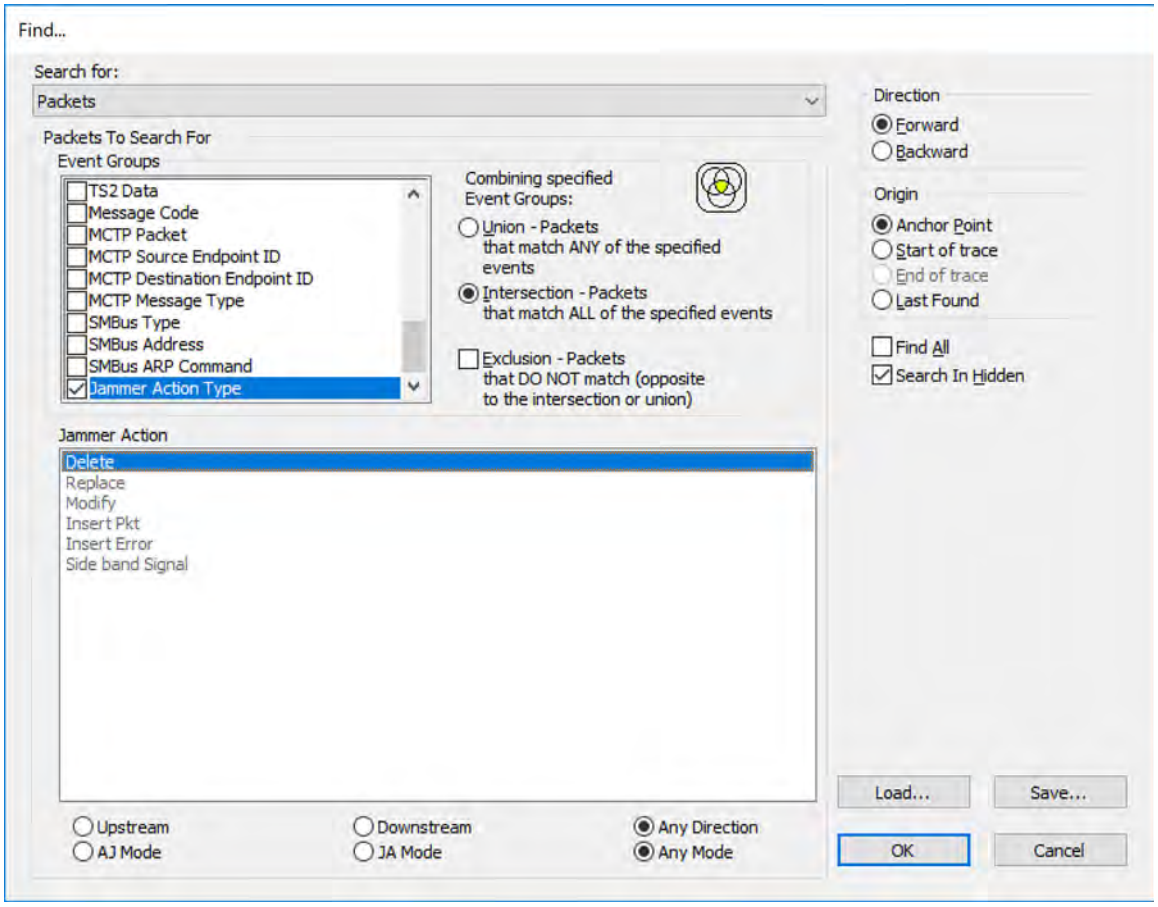


Figure 8.59: Find -> Search for: Packets -> Jammer Action Type: Delete

Click on OK and the Jammer Action and following it the results: A deleted UpdateFC_P packet. See Figure 8.60 on page 501.

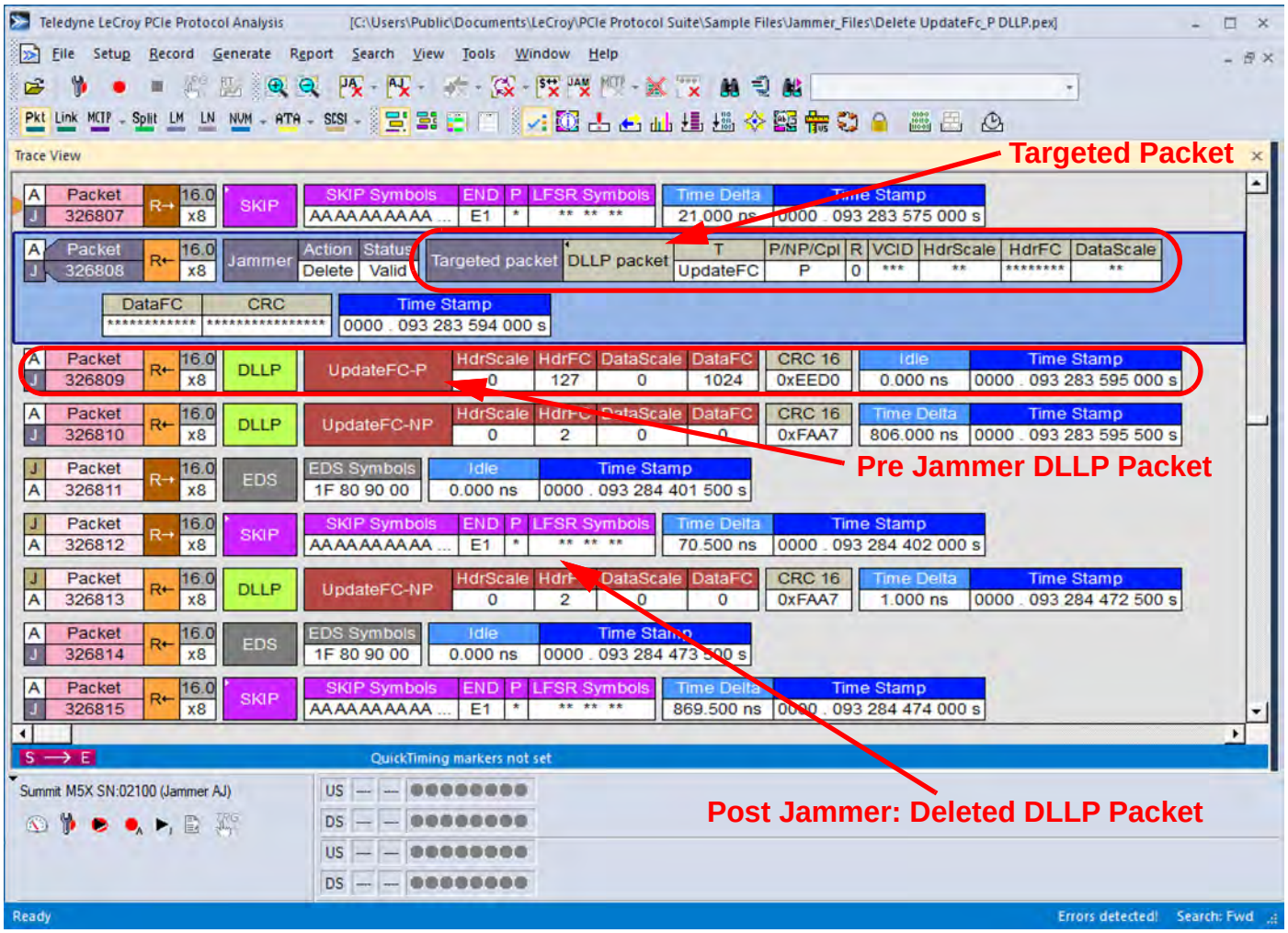


Figure 8.60: Trace with Jammer Function: Delete UpdateFC_P

8.15.1.2 Insert Error: DROP_STP_SDP for UpdateFC_P Packet

In he second example we drop an STP_SDP packet for an UpdateFC_P Packet. See Figure 8.61.

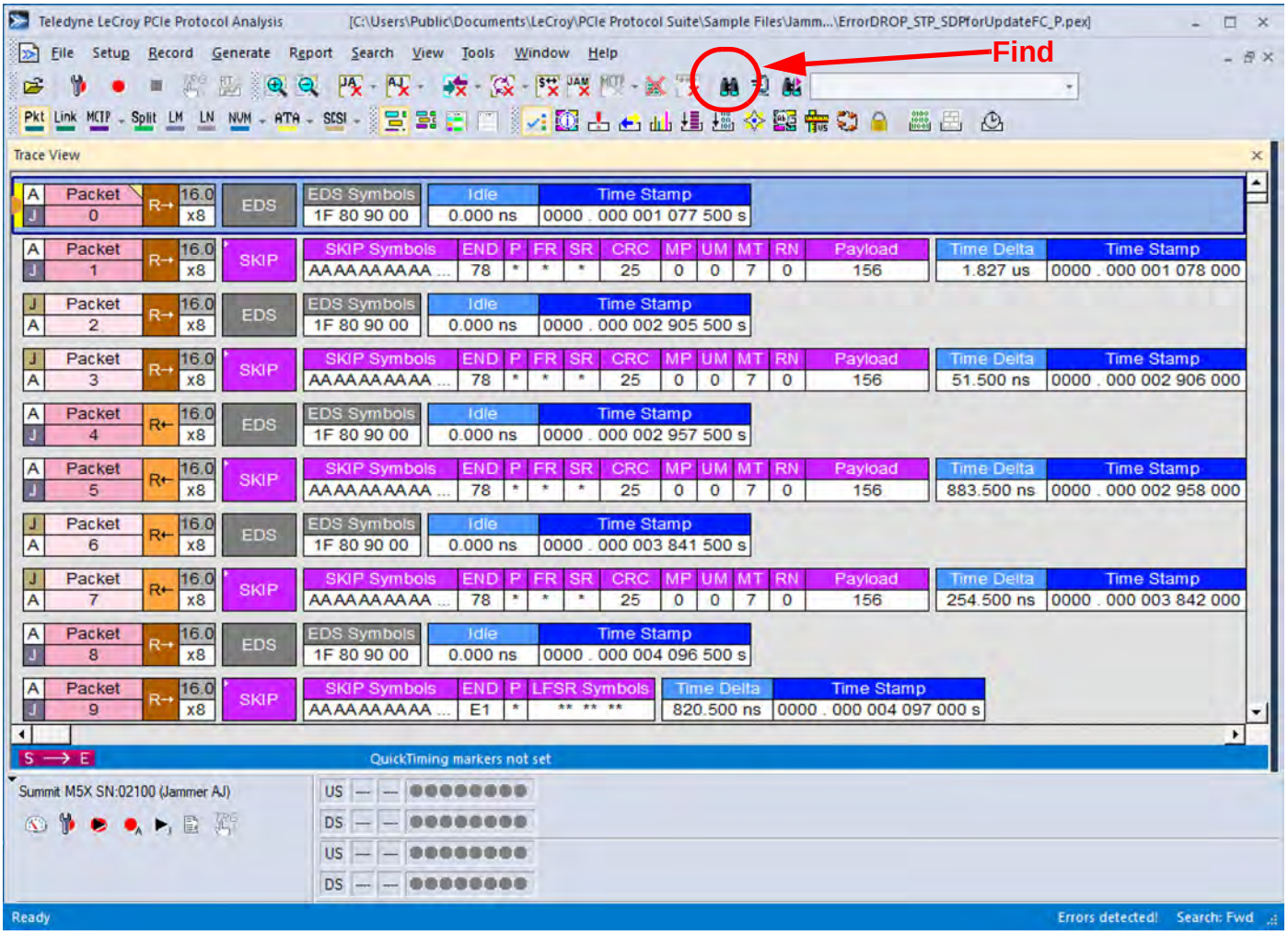


Figure 8.61: AJA Trace: Insert Error -> Drop STP_SDP for UpdateFC_P

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 8.62 on page 503.

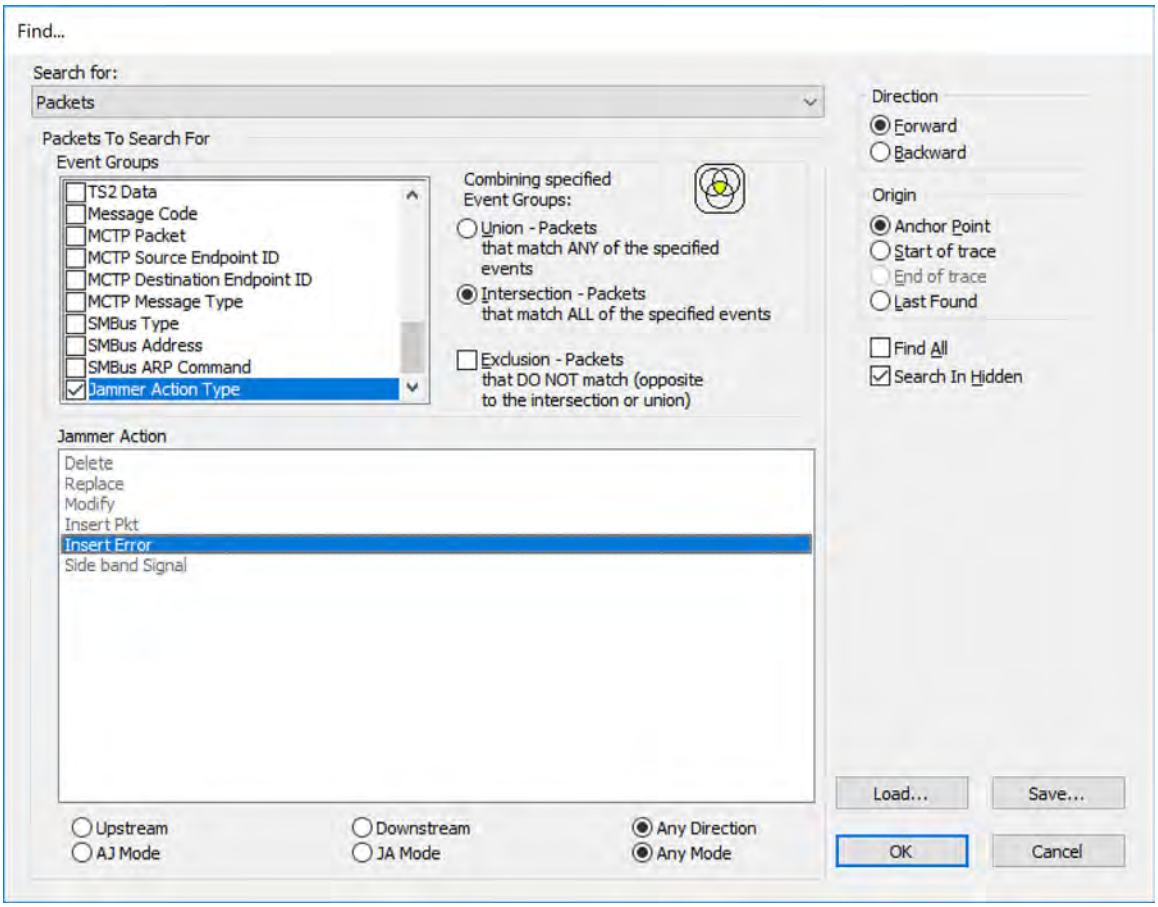


Figure 8.62: Find -> Search for: Packets -> Jammer Action Type: Insert Error

Click on OK and the Jammer Action and following it are the results:

Insert Error -> Drop STP_SDP for UpdateFC_P, which causes the UpdateFC_P packet to be missing. See Figure 8.63 on page 504.

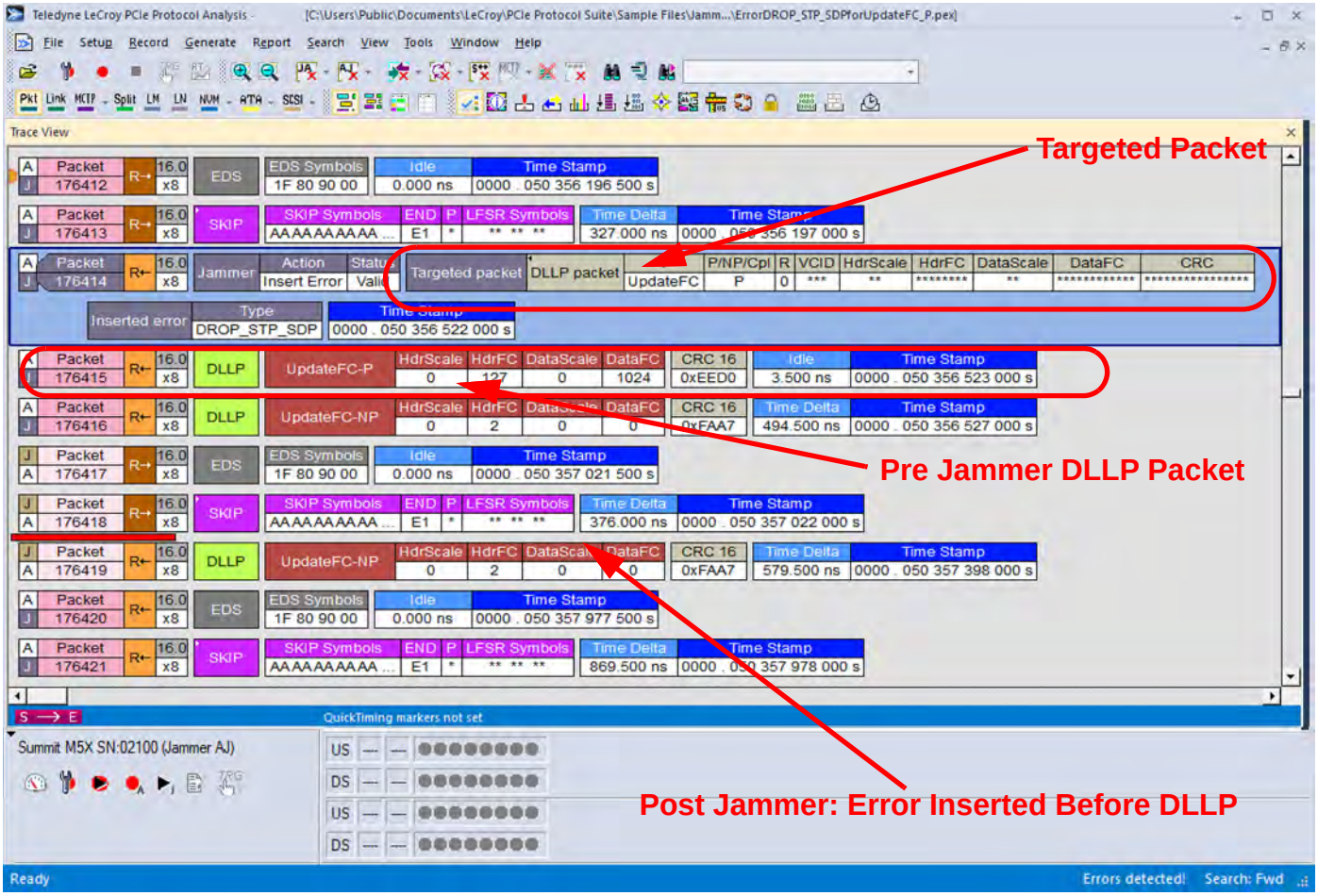


Figure 8.63: Trace with Jammer Function: Insert Error -> Drop STP/SDP for UpdateFC_P

8.15.1.3 Insert TLP After UpdateFC_NP Packet

In the third example we insert an TLP Packet after an UpdateFC_NP Packet. See Figure 8.64.

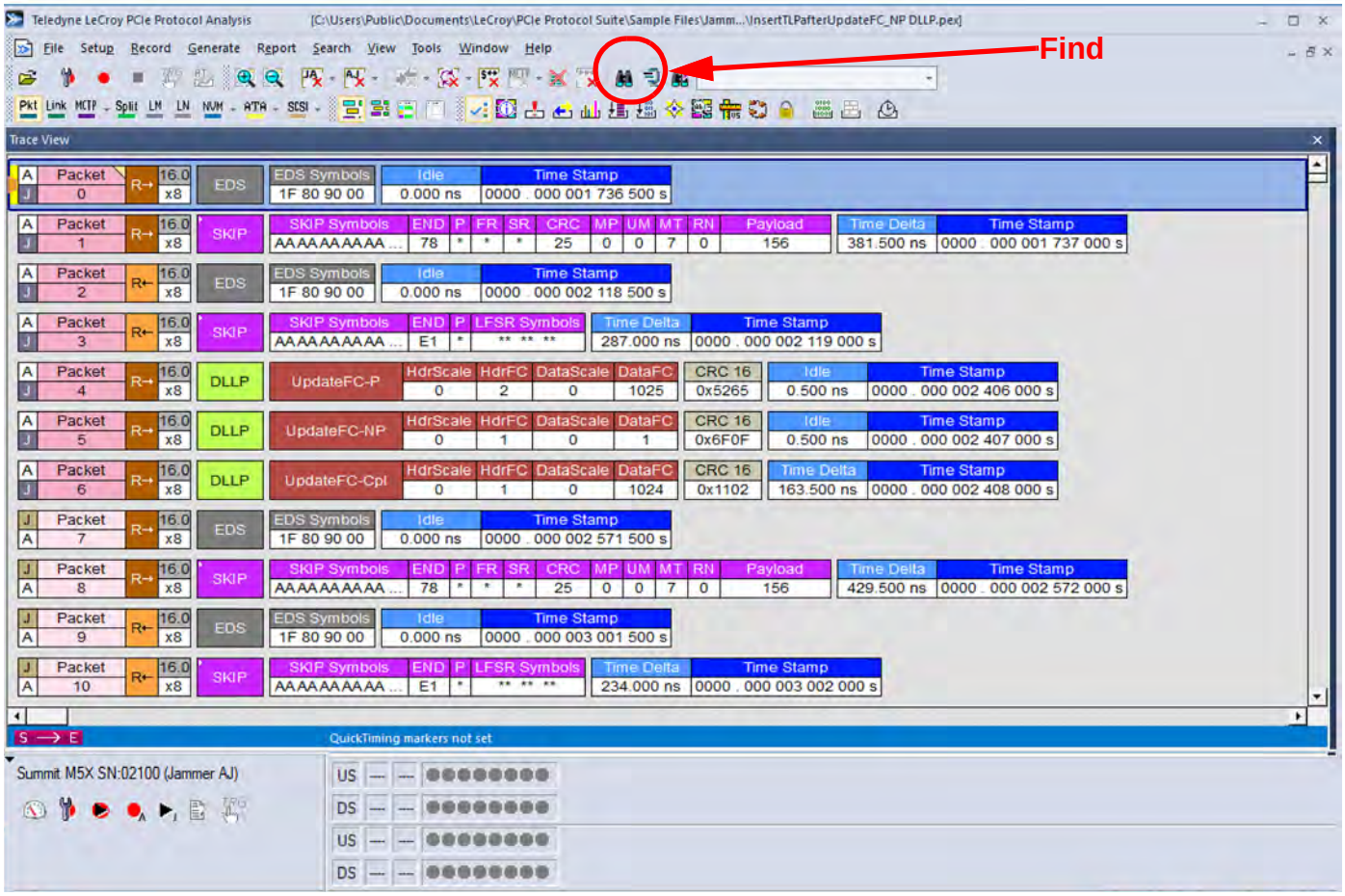


Figure 8.64: AJA Trace: Insert TLP After UpdateFC_NP Packet

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 8.65 on page 506.

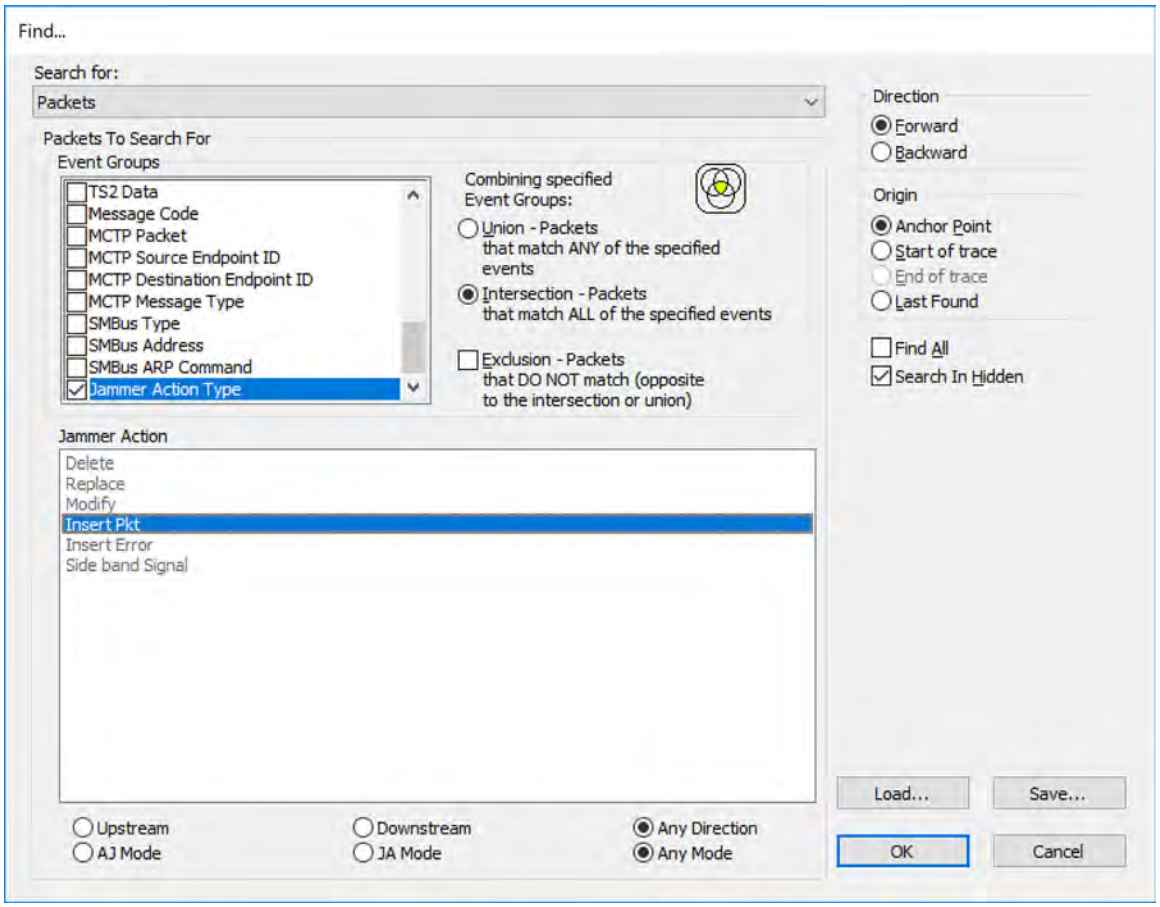


Figure 8.65: Find -> Search for: Packets -> Jammer Action Type: Insert packet

Click on OK and the Jammer Action and following it are the results:

Insert TLP After UpdateFC_NP Packet, which adds a TLP to the trace after the UpdateCF_NP packet. See Figure 8.66 on page 507.

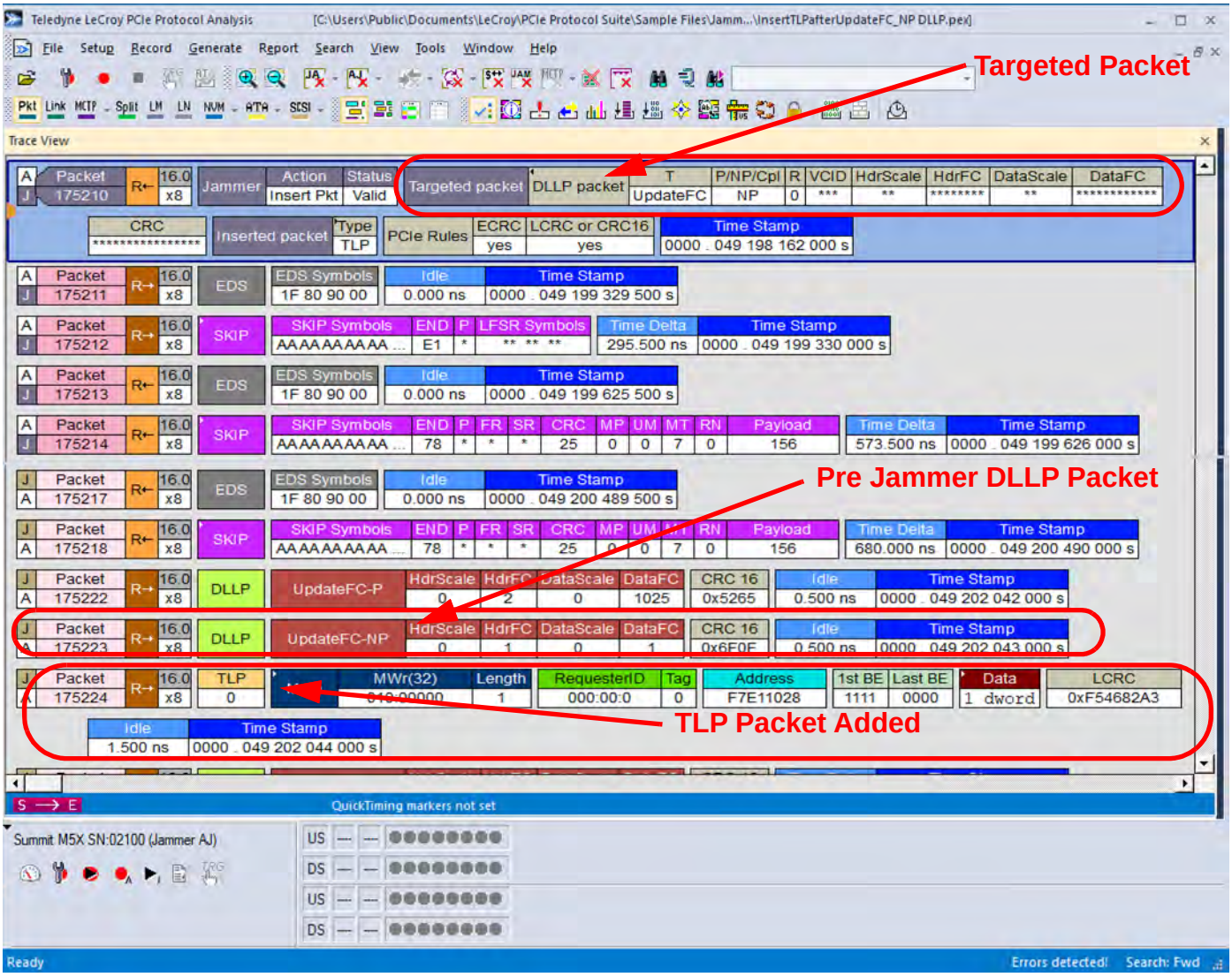


Figure 8.66: Trace with Jammer Function: Insert TLP Packet After UpdateFC_NP Packet

8.15.1.4 Modify: UpdateFC_P Packet to UpdateFC_NP Packet

In the fourth example we modify an UpdateFC_P Packet to an UpdateFC_NP Packet. See Figure 8.67.

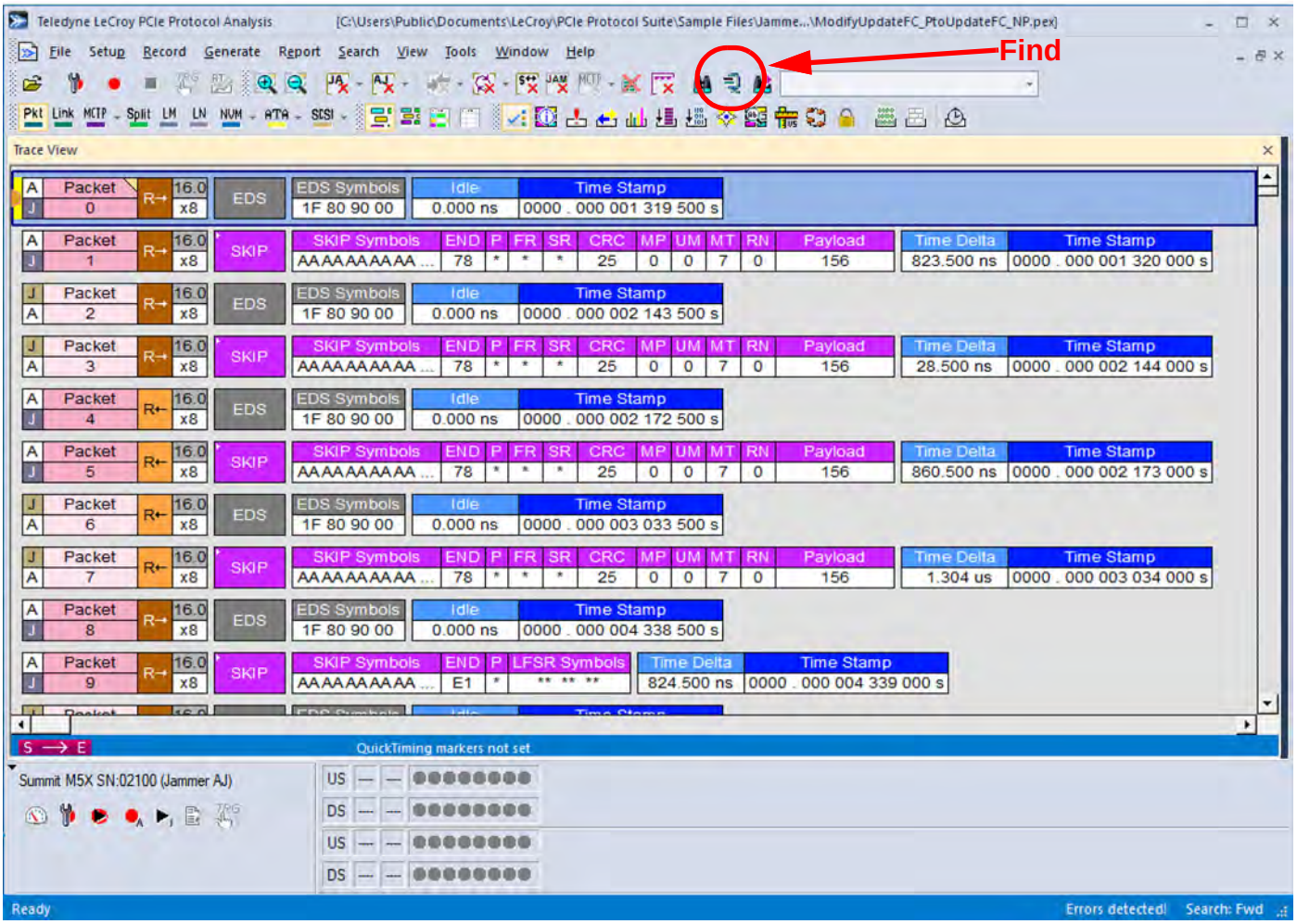


Figure 8.67: AJA Trace: Modify: UpdateFC_P Packet to UpdateFC_NP Packet

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 8.68 on page 509.

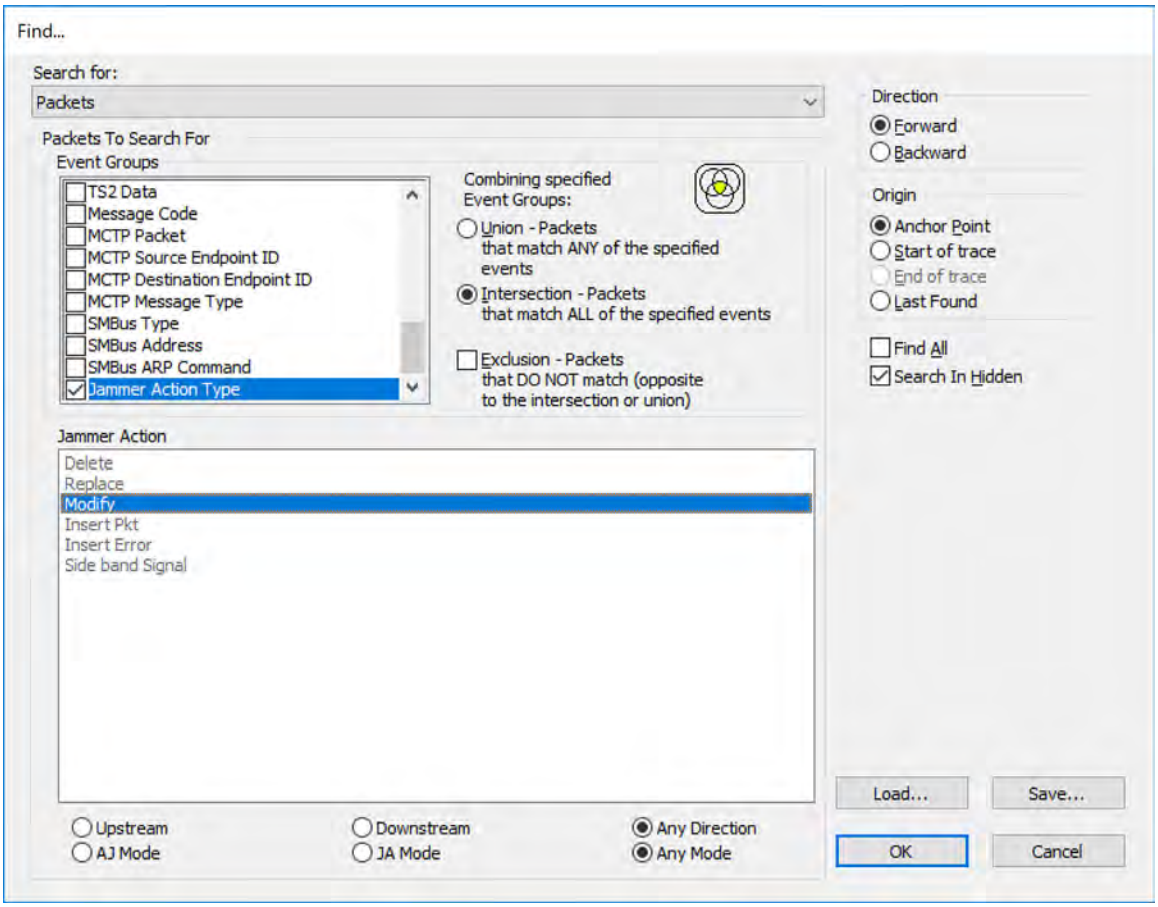


Figure 8.68: Find -> Search for: Packets -> Jammer Action: Modify Packet

Click on OK and the Jammer Action and following it are the results:

Insert Error -> Drop STP/SDP for UpdateFC_P, which causes the UpdateFC_P packet to be missing. See Figure 8.69 on page 510.

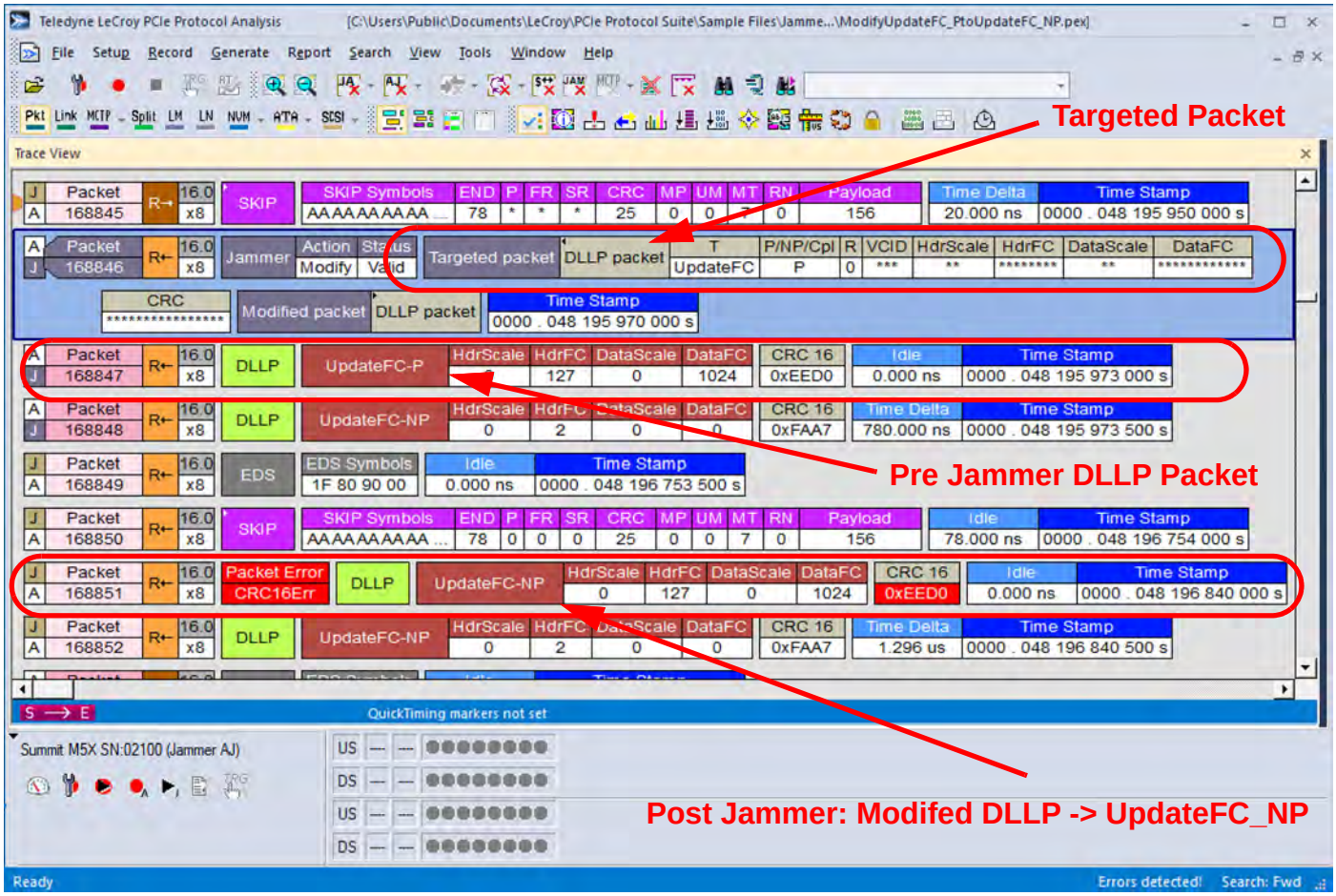


Figure 8.69: Trace with Jammer Function: Modify UpdateFC_N to UpdateFC_NP

8.15.1.5 Replace: UpdateFC_CP with TS1_PAD_PAD

In the fifth example we replace an UpdateFC_CP with a TS1_PAD_PAD packet. See Figure 8.70.

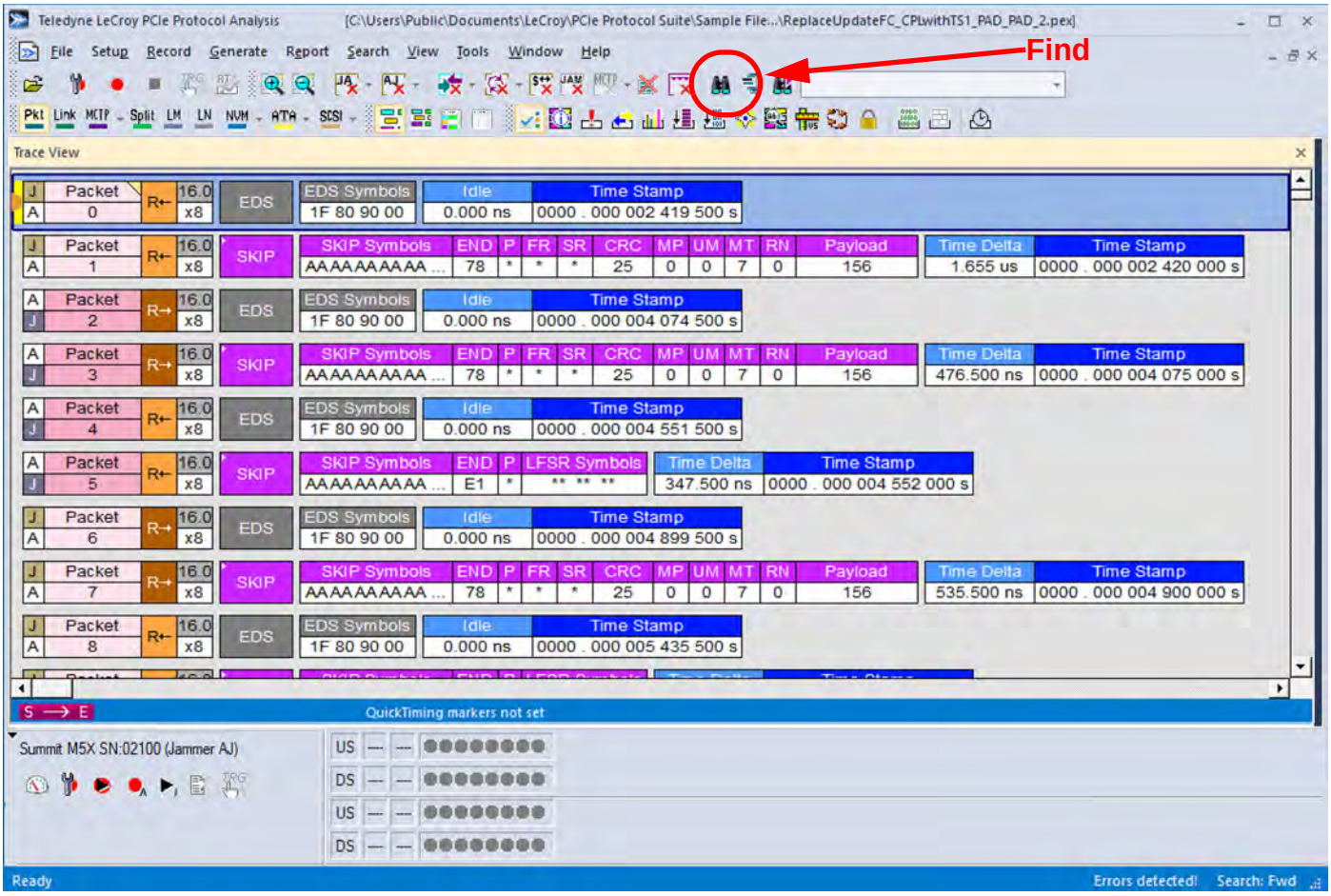


Figure 8.70: AJA Trace: Replace -> UpdateFC_CP with TS1_PAD_PAD

To find the Jamming event click on the binoculars to search for a Packet: Jammer Action Type. See Figure 8.71 on page 512.

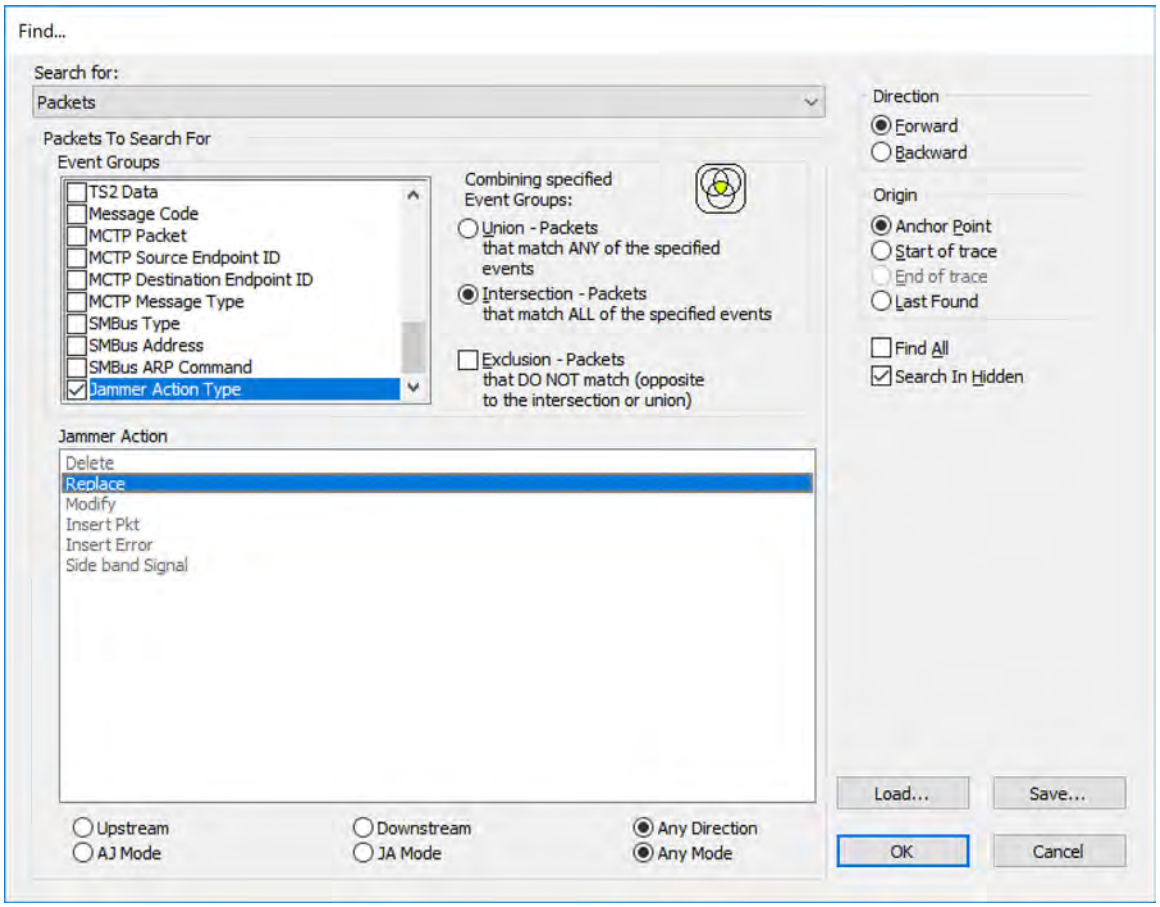


Figure 8.71: Find -> Search for: Packets -> Jammer Action: Replace

Click on OK and the Jammer Action and following it are the results:

Replace UpdateFC_CP with TS1_PAD_PAD. See Figure 8.72 on page 513.

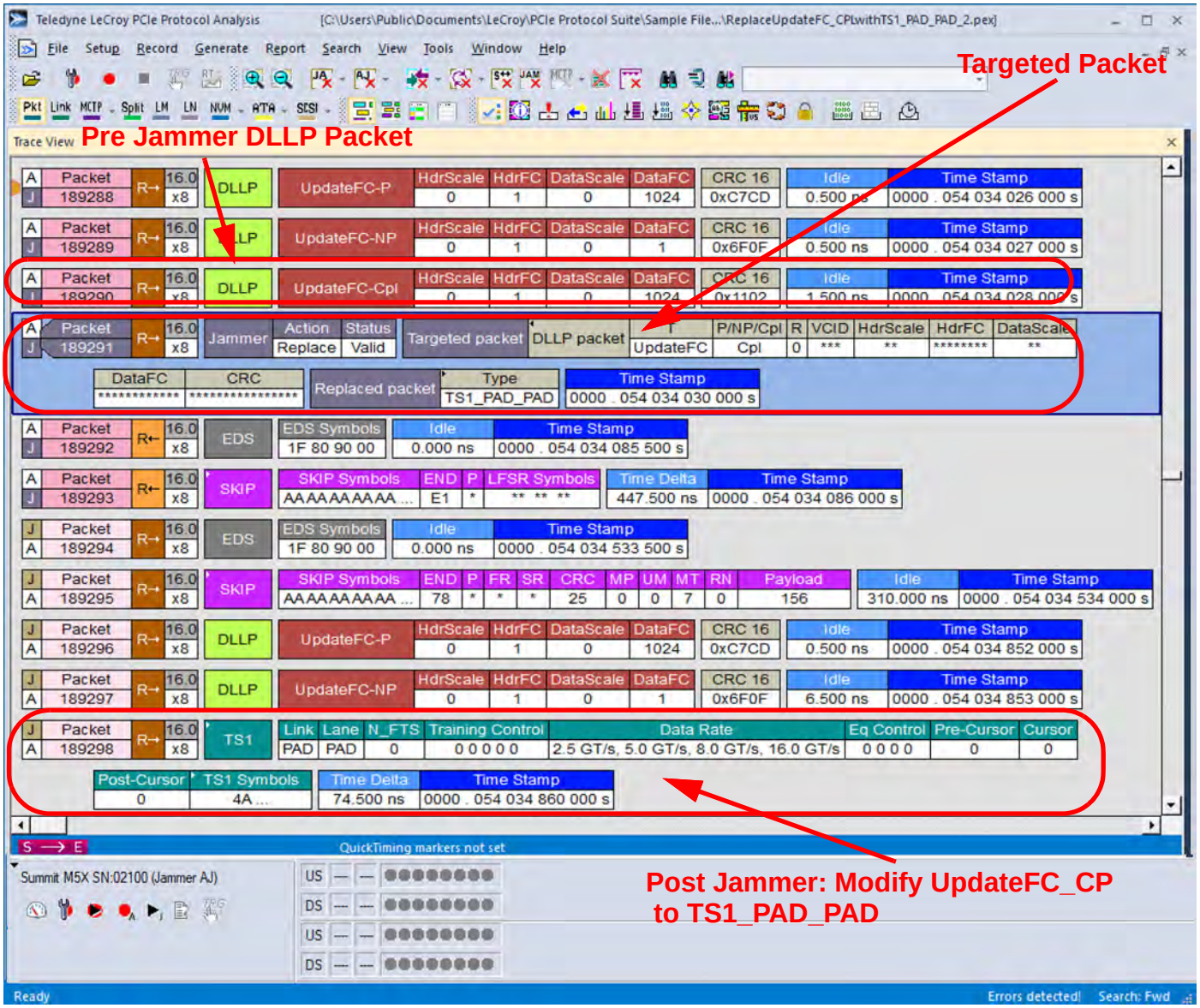


Figure 8.72: Trace with Jammer Function: Modify -> UpdateFC_CP with TS1_PAD_PAD

These examples give you an overview of the types of Jammer Actions that can be added to your traces.

All of the Jammer Actions are discussed in more detail in “Jammer Actions” on page 453.

All of the Jammer Actions can also be added to your script, as shown in “Script Mode” on page 447.

Chapter 9

Reading CATC Traces

9.1 Viewing PCI Express CATC Traces

PCIe Protocol Analysis™ displays traffic as labeled, color-coded, and time-stamped rows.

Note: The time stamp resolution is 1 nano second and the accuracy is 16 nano seconds.

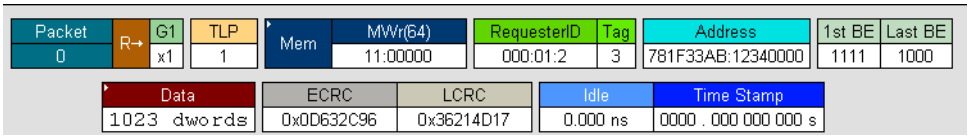


Figure 9.1: Typical CATC Trace

Tool tips provide details about fields within the CATC Trace. Hold the mouse cursor over a field to see a tool tip.

Additional information is available from pop-up menus. For example, if you click the left mouse button on the first cell in a packet a menu appears with an option to view Raw 10b Codes.

9.2 Expand and Collapse Data Fields

Packet data fields are displayed in a short format by default.

You can view a data field's long format by performing one of the following three actions:

- Click the **small triangle** in the left corner.
- Double-click anywhere in the data field.
- Click once in the Data Field with the left mouse button, then choose **Expand Data** from the context menu.

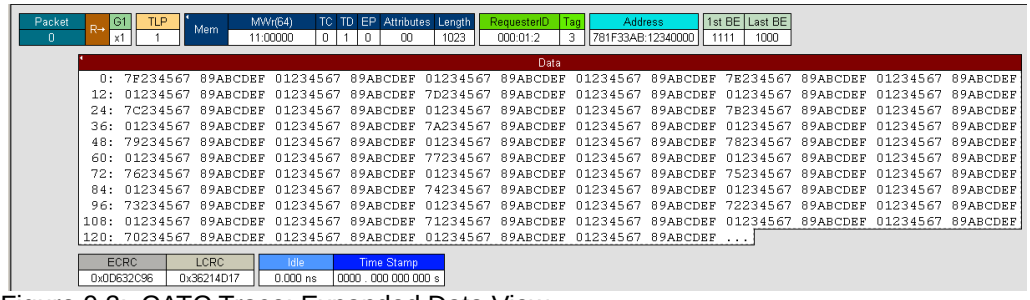


Figure 9.2: CATC Trace: Expanded Data View

A repeat of any above methods causes the display to return to a Short Data format.

9.3 Resizing Cells

Data cells can be resized by pointing the mouse pointer on the edge of a data cell, depressing and holding the left mouse button, and then repositioning the mouse pointer while keeping the mouse button depressed.

9.4 Context Menus

The Analyzer software makes extensive use of pop-up context menus. In some instances, context menus provide the only means of accessing dialogs that contain detailed information about cells within the CATC Trace, for example, the Show Configuration Space dialog.

To see the context menus, left-click or right-click a **cell** within the CATC Trace. Right-click or left-click behavior depends on the Display Options setting. For default left-click, the right-click menu is not cell-dependent. For other left-click behavior, the type of menu that opens varies depending on the selected cell. Take some time to explore CATC Traces and the various context menus available.

9.4.1Address Context Menu

The Address context menu allows you to search for a specific address from the trace. Select Addresses from the Trace View or from the Data View. Right click on the address cell (of the packet, link, or split transaction). This opens the context menu with the options, below:

Show Header Fields	Displays the Header Fields for the packet.
Find next packet with address …	Finds the next packet with the same address in the trace.
Find all packets with address …	Finds all packets with the same address in the trace.
Add address … to search	Adds the address to the **Search by address** search category in the Find dialog. See the “Find Feature” on page 88 for more information on the Find dialog.
Set Marker	Adds a marker to the address.

See Figure 9.3 and Figure 9.4 for examples of the Address context menu.

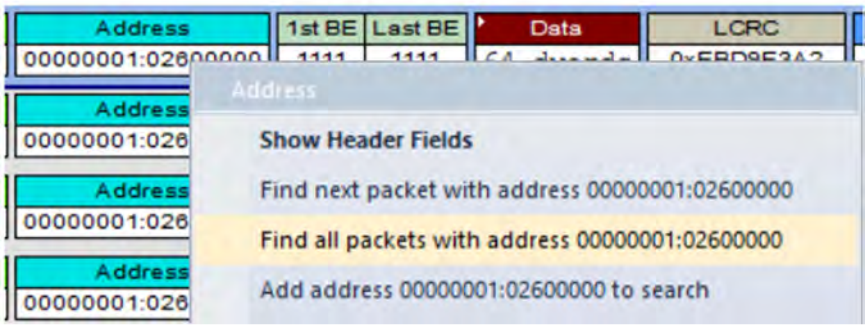


Figure 9.3: Address Context Menu with Find all packets highlighted

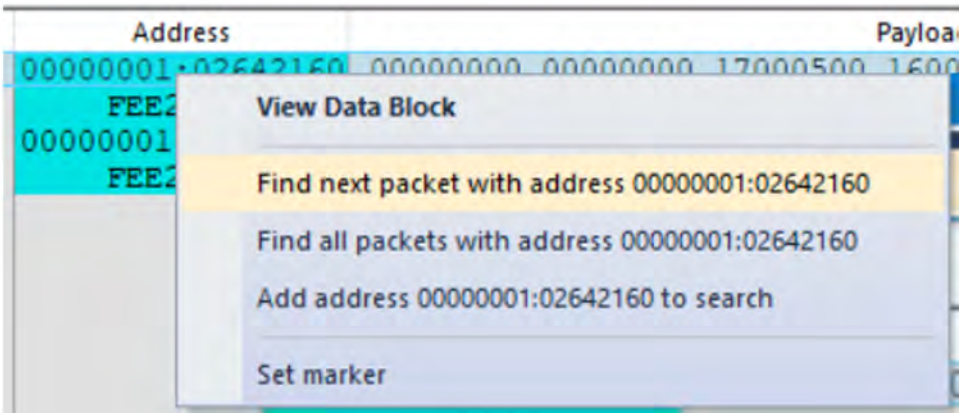


Figure 9.4: Address Context Menu with Find next packet highlighted

Selecting **Find next packet with address** or **Find all packet with address** clears all other entered addresses values from the **Search by address** search option in the **Find** Dialog. Selecting **Add address** adds an address to the already entered values and does not clear them. See Figure 9.5.

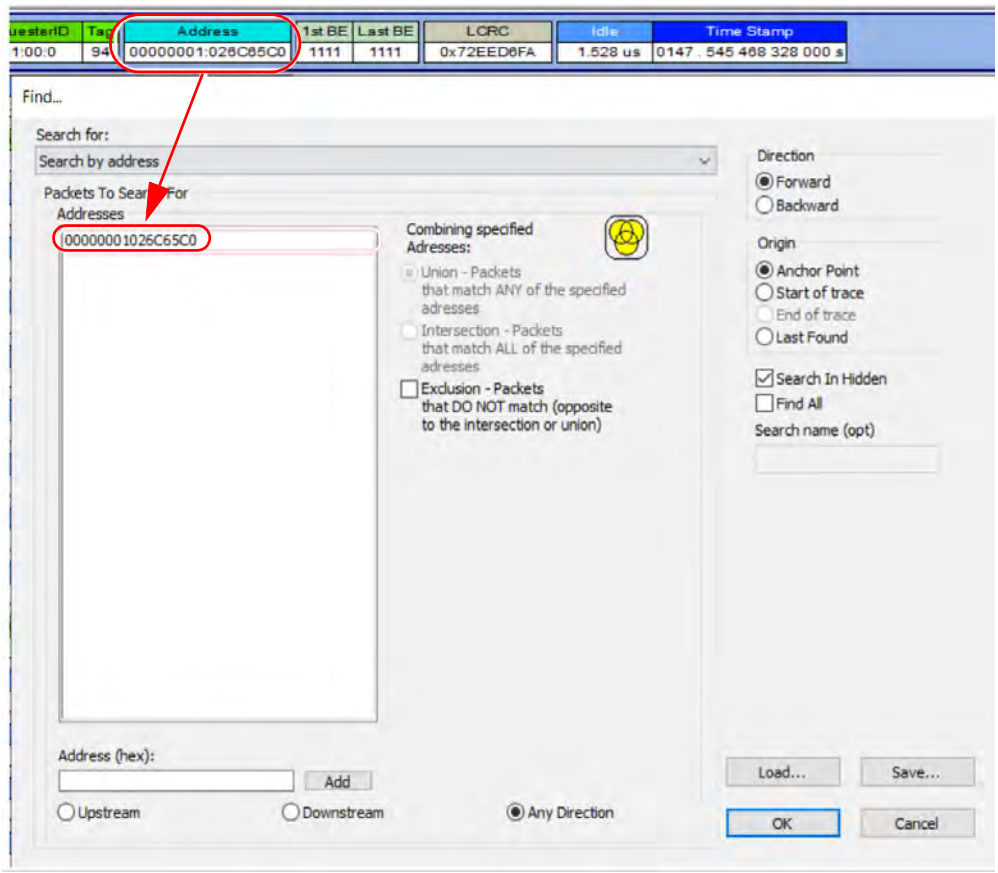


Figure 9.5: Address from Trace appears in the Find Dialog

9.5 View Data Block

To view the raw bits that make up the data in a data field, left-click a data field, then click  from the select **View Data Block** from the context menu to display the Data Block window

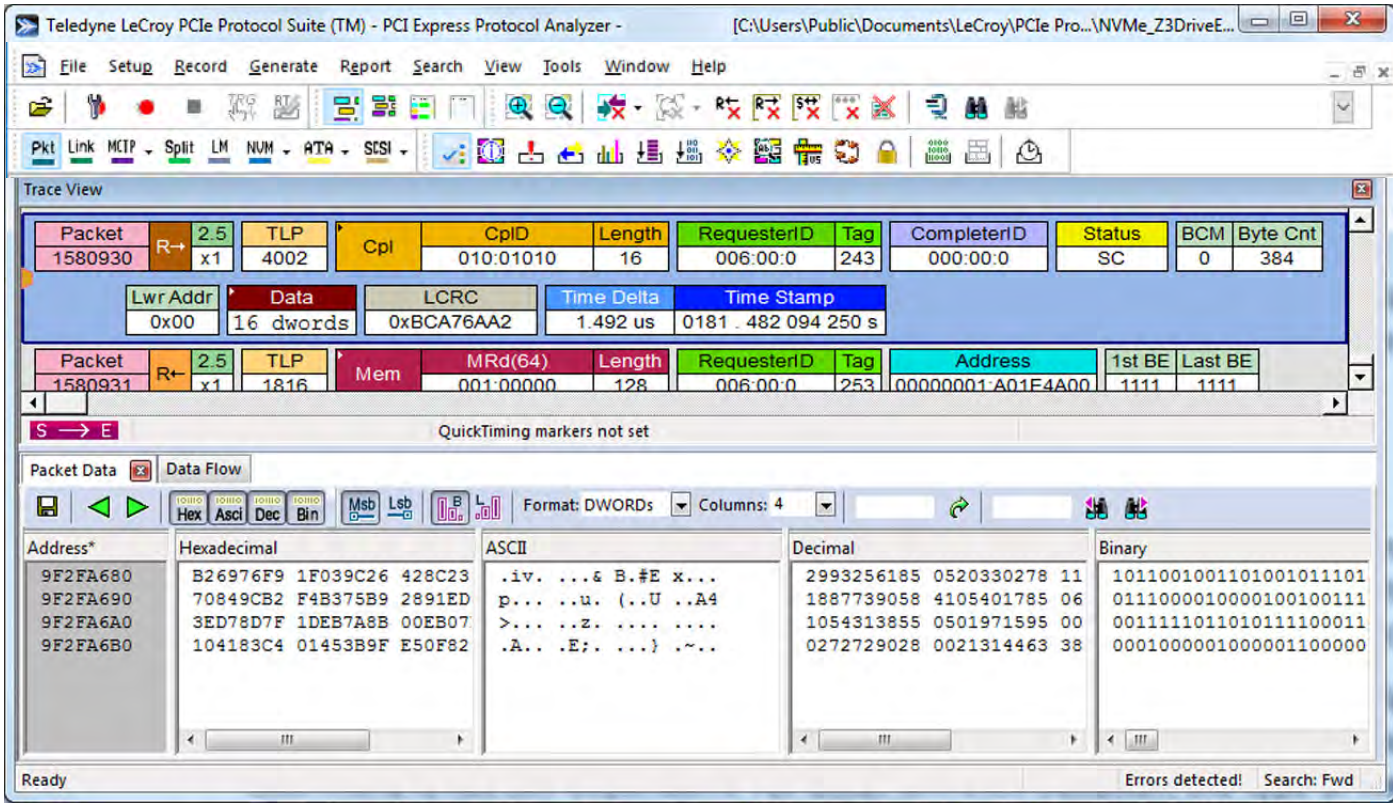


Figure 9.6: Viewing a Data Block

There are several ways to display data:

- You can display data in Hexadecimal, ASCII, Decimal, or Binary formats.
- Bit Order is Most Significant Bit or Least Significant Bit.
- You can display data in Big Endian or Little Endian.
- **Format** lets you display data as BYTEs, WORDs, or DWORDs.
- **Columns** lets you select the number of columns.
- You can enter hexadecimal offset values.
- You can go to or search Previous or Next.

9.5.1 Save Data Block

You can also **Save** the data in Hexadecimal, ASCII, Decimal, or Binary formats. See Figure 9.7.

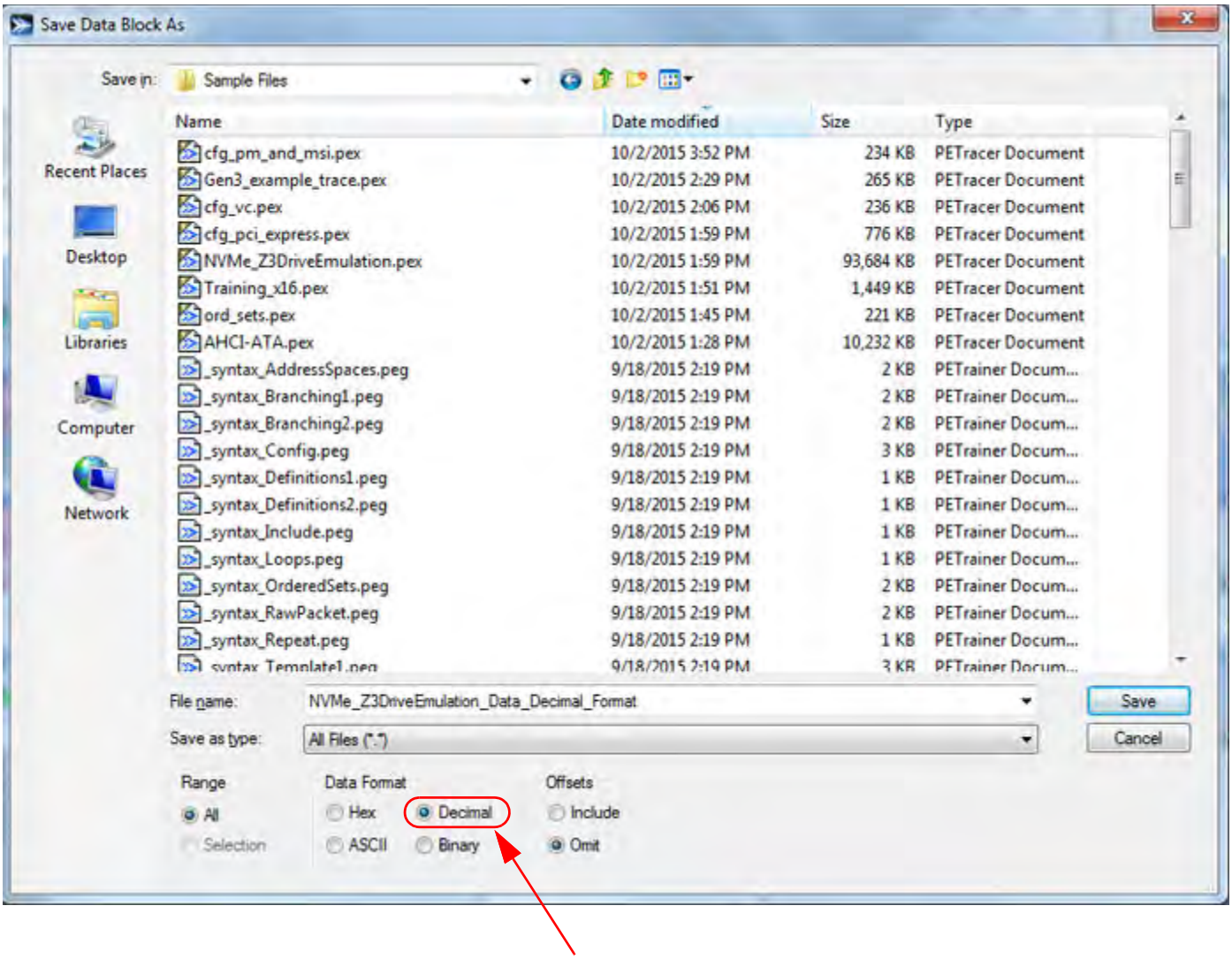


Figure 9.7: Save Data Block In Hex, Decimal, ASCII or Binary

The Saved file is shown in Figure 9.8 on page 524.

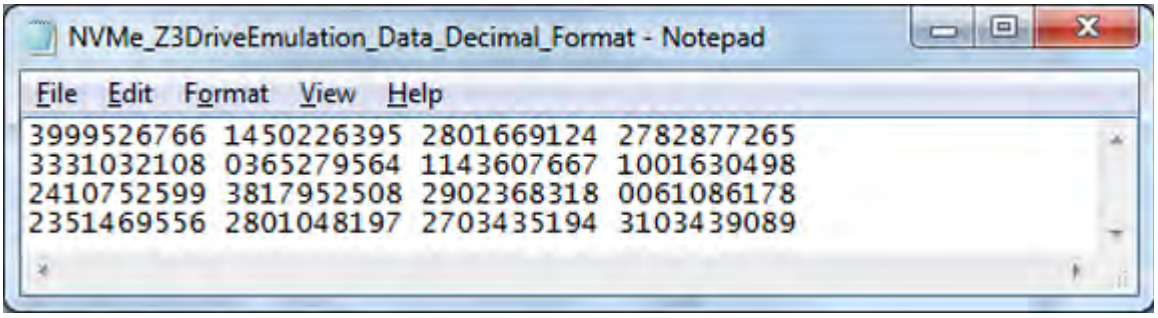


Figure 9.8: Saved Data File in Decimal Format

9.6 Show Raw 10b Codes

You can view the raw bits that make up the data field by right-clicking the field and selecting **View Data Block** from the pop-up menu.

To view Raw 10b Codes:

1. Right-click the **first cell** in a packet.
2. Select **Show Raw 10b Codes** from the pop-up menu to display the Raw 10b Codes window.

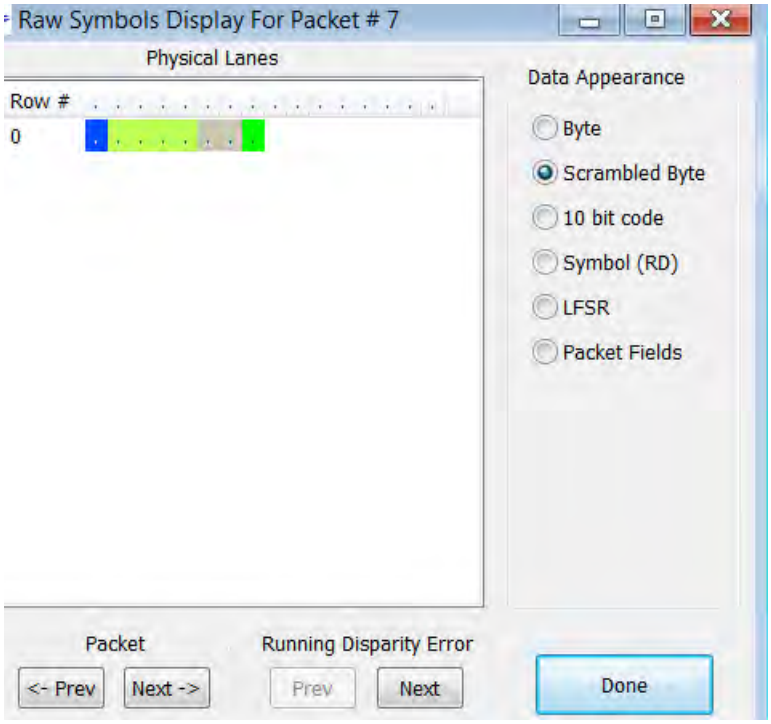


Figure 9.9: Show Raw 10b Codes Dialog

3. To change the format of the data, use the options along the right side of the dialog.
4. To navigate the CATC Trace, use the **Prev** and **Next** buttons.

9.7 Show Header Fields

You can view details about header fields by opening the Show Header Fields dialog.

1. Right-click a **header.** A context menu displays, as shown in Figure 9.10.

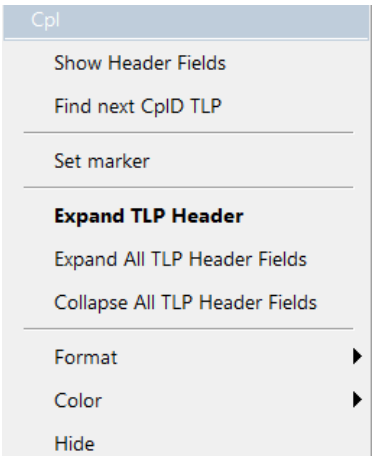


Figure 9.10: CATC Trace View: Header Context Menu

2. Select **Show Header Fields**. The Header Fields dialog opens, as shown in Figure 9.11.

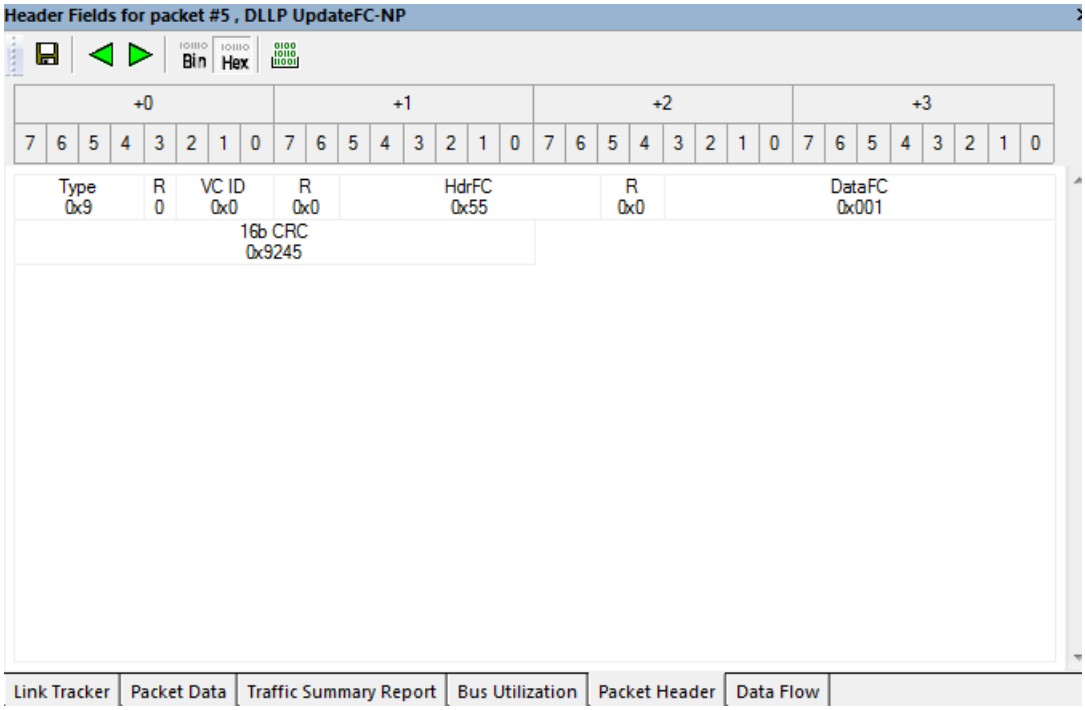


Figure 9.11: Viewing Packet Fields

3. Use the **Prev** and **Next** buttons to navigate to other headers.

9.8 Packet Cell Context Menus

The Packet cell has a right-click context menu that includes the topics shown in Figure 9.12.

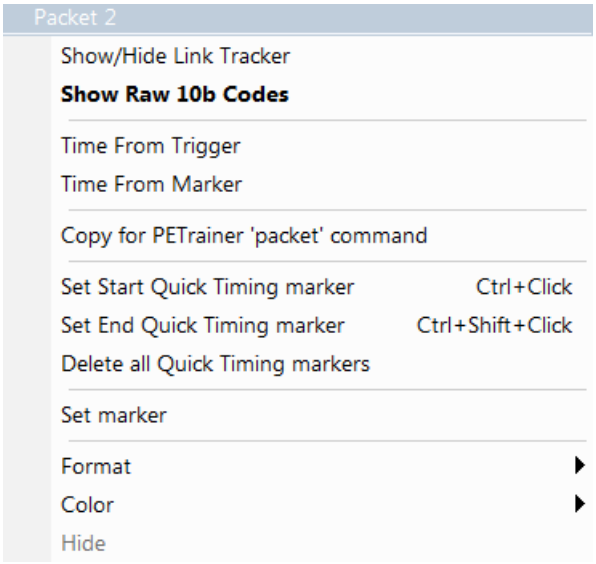


Figure 9.12: Packet Cell Popup Menu

Each topic can be selected to show more information about the topic. The following sections describe each of the topics in the menu.

9.8.1 Show/Hide Link Tracker

Click on the “Show/Hide Link Tracker” and the Link Tracker View will show in the Main Display window. See Figure 9.13.

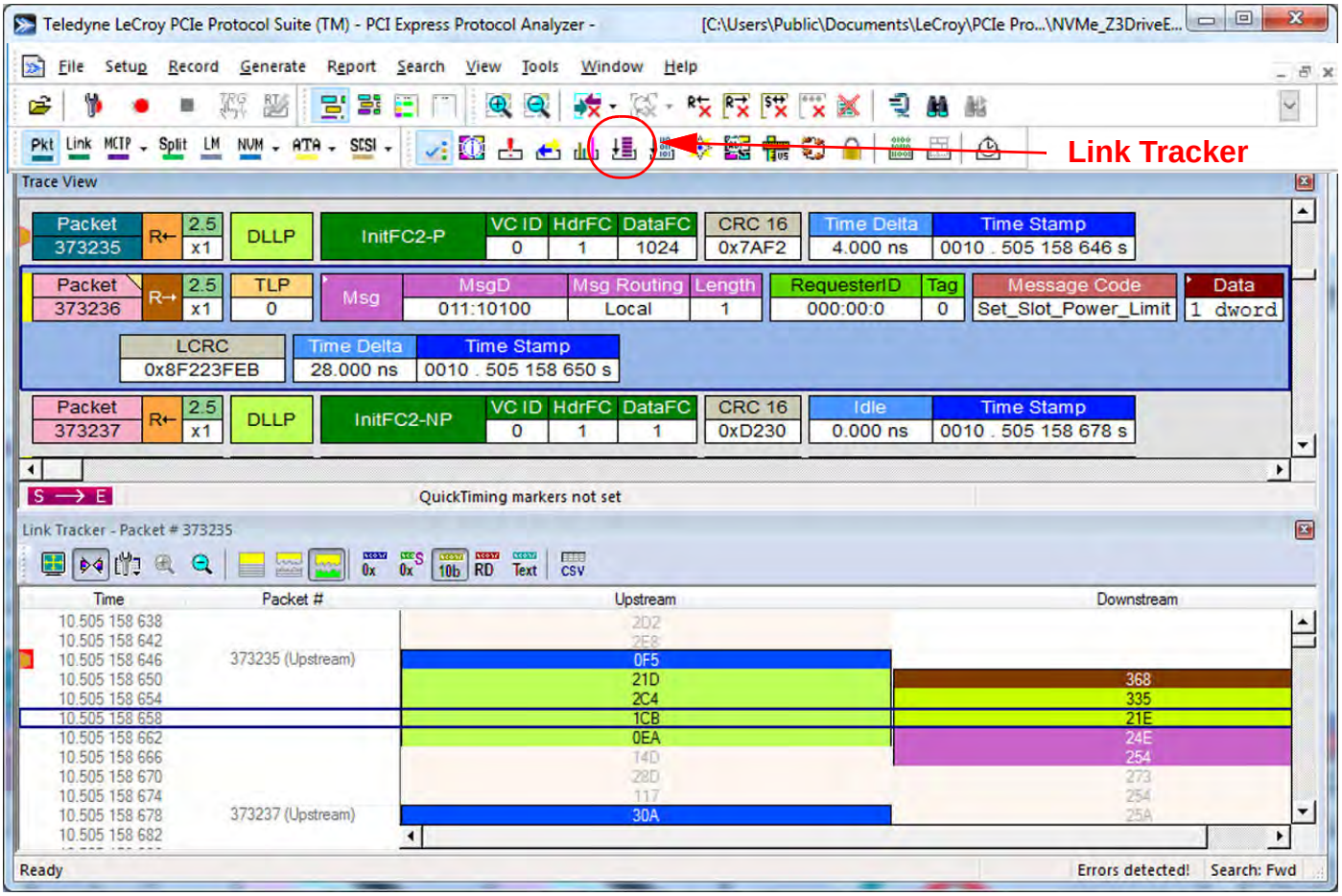


Figure 9.13: Packet Cell Popup Menus: Trace View and Link Tracker View

Link Tracker is discussed in more detail in “Link Tracker” on page 775.

9.8.2 Show Raw 10b Codes

Click on Show Raw 10b Codes and the Raw Symbols Display for the selected Packet pops up. See Figure 9.14.

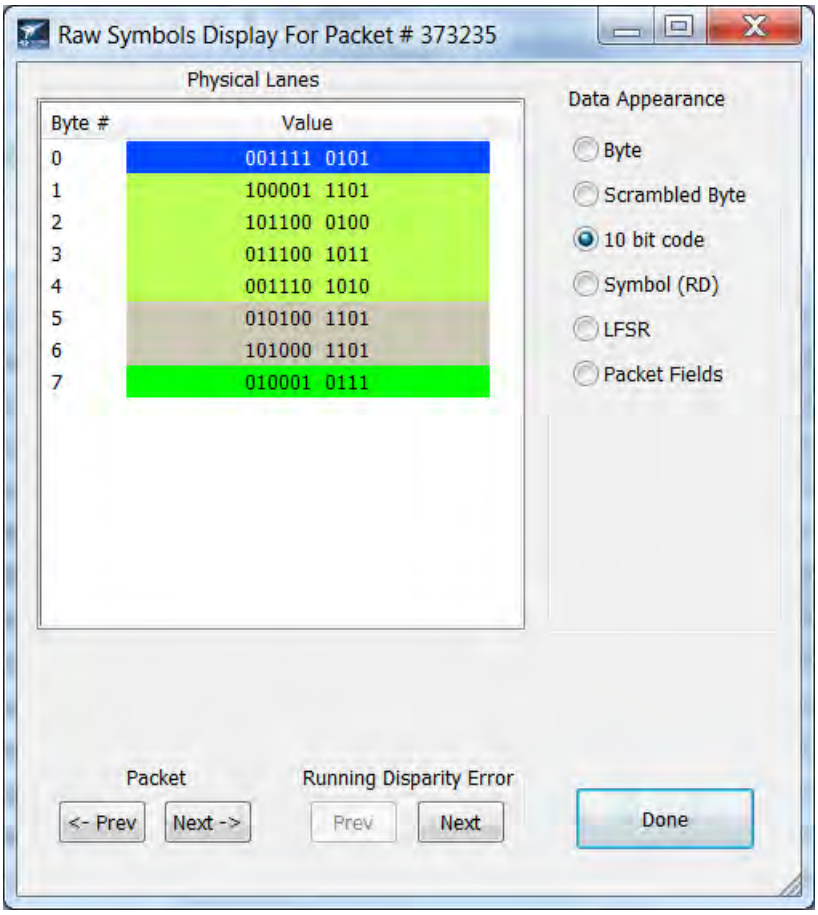


Figure 9.14: Packet Cell Popup Menus: Show Raw 10b Codes

Raw 10b Codes is discussed in more detail in “Show Raw 10b Codes” on page 525.

9.8.3 Time From Trigger

Select Time From Trigger and the Timing Calculator pops up. See Figure 9.15.

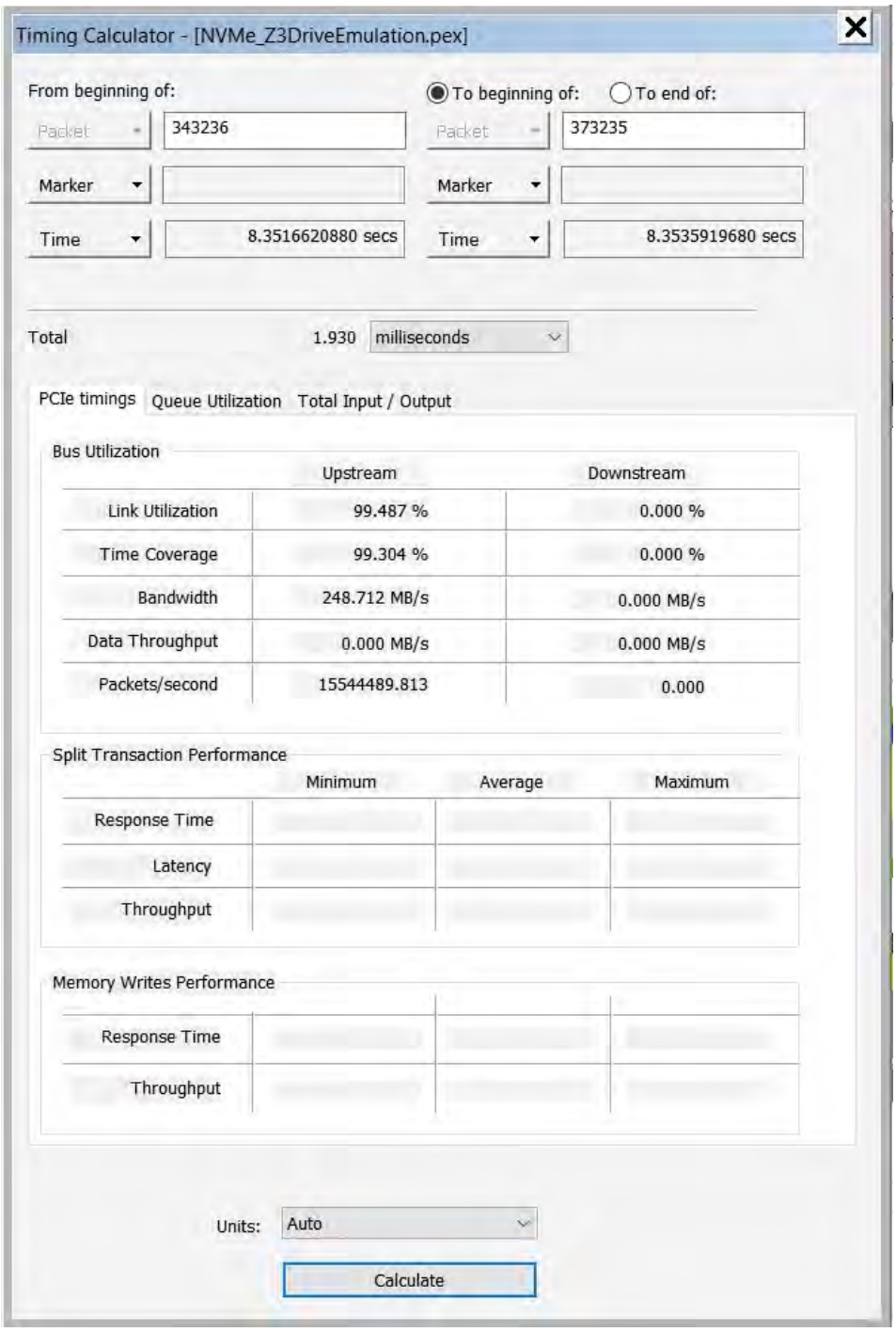


Figure 9.15: Packet Cell Popup Menus: Timing Calculator

The Timing Calculator is discussed in more detail in "Timing Calculator" on page 839.

9.8.4 Time From Marker

Click on Time From Marker and the following menu pops up along with the Timing Calculator. See Figure 9.16.

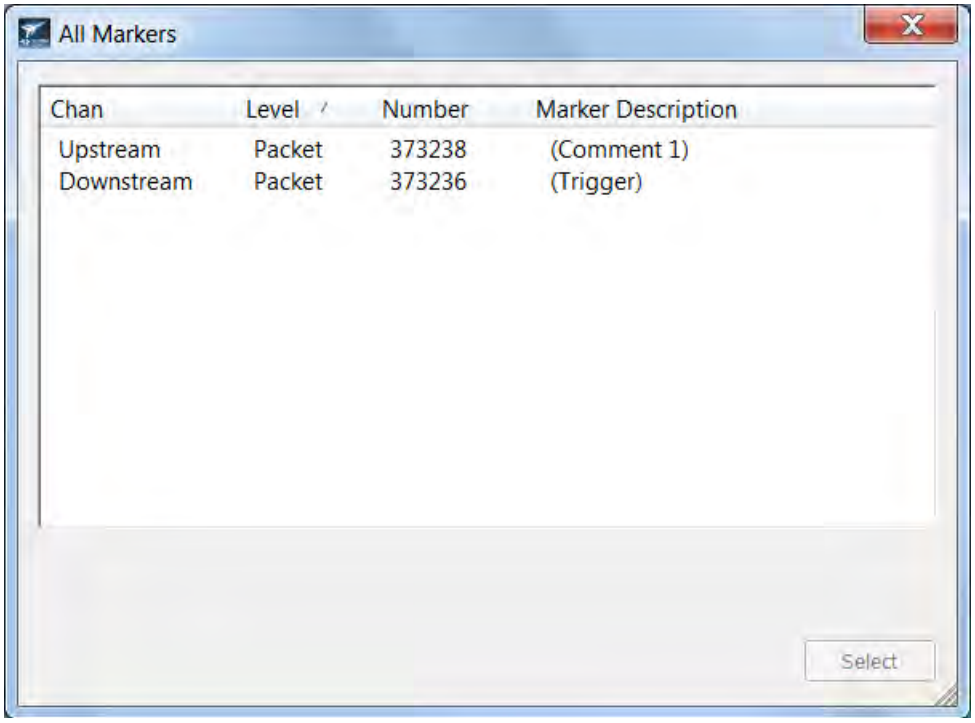


Figure 9.16: Packet Cell Popup Menus

Markers are discussed in more detail in “Set Marker” on page 536 and the Timing Calculator is discussed in more detail in “Timing Calculator” on page 839.

9.8.5 Copy for PETrainer ‘packet’ command

Select a packet, right click to bring up the Packet Cell Popup Menu, select the Copy for PETrainer ‘packet’ command and the tool will copy the Packet information which can then be copied into a PETrainer script for use with Teledyne LeCroy exercisers (Z3-16 etc.).

An example is shown below of a typical Packet and the PETrainer commands generated:

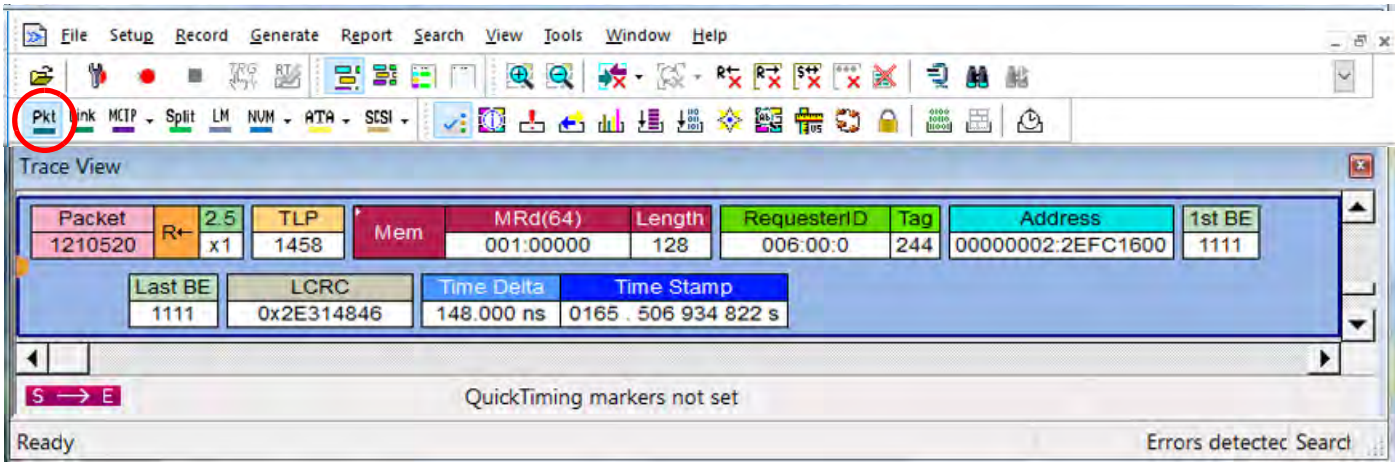


Figure 9.17: Packet Cell Popup Menus: Copy for PETrainer ‘packet’ Command

The script produced looks like this and can be copied into an existing trainer script:

```
packet = TLP {
    PSN = 0x5B2
    TLPType = MRd64
    TC = 0x0
    TD = 0x0
    TH = 0x0
    EP = 0x0
    IDBasedOrdering = 0x0
    Ordering = 0x0
    Snoop = 0x0
    AT = 0x0
    Length = 0x80
    RequesterId = (6:0:0)
    Tag = 0xF4
    LastDwBe = 0xF
    FirstDwBe = 0xF
    AddressHi = 0x2
    AddressLo = 0x2EFC1600
}
```

9.8.6 Set Start Quick Timing Marker

Sets the start packet for the Quick Timing marker. An S symbol is displayed at the packet.

Quick Timing provides immediate time deltas and bandwidth calculations. If the Start is placed on a packet that contains an Address and Endpoint, the bandwidth for that combination is displayed in the Status Bar below the trace data.

Quick Timing Markers are special ""Start"" and ""End"" markers used to mark the boundaries of the calculations. The results are shown in a special Quick Timing Bar at the bottom of the TraceView. The markers are set from a context sensitive menu.



Figure 9.18: Packet Cell Popup Menus: Set Start Quick Timer Marker

9.8.7 Set End Quick Timing Marker

Sets the end packet for the Quick Timing marker. An E symbol is displayed at the packet.

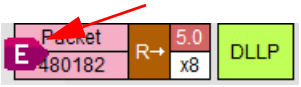


Figure 9.19: Packet Cell Popup Menus: Set End Quick Timer Marker

9.8.8 Tag Context Menu

You can get a "Tag" context menu if you right-click a RequesterID's associated Tag block as shown below (see Figure 9.20). The Summit M5x can decode the following tags:

- Use 5/8/10 bit tag (no phantom functions)
- Use 9 bit phantom function tag
- Use 10 bit phantom function tag
- Use 11 bit phantom function tag

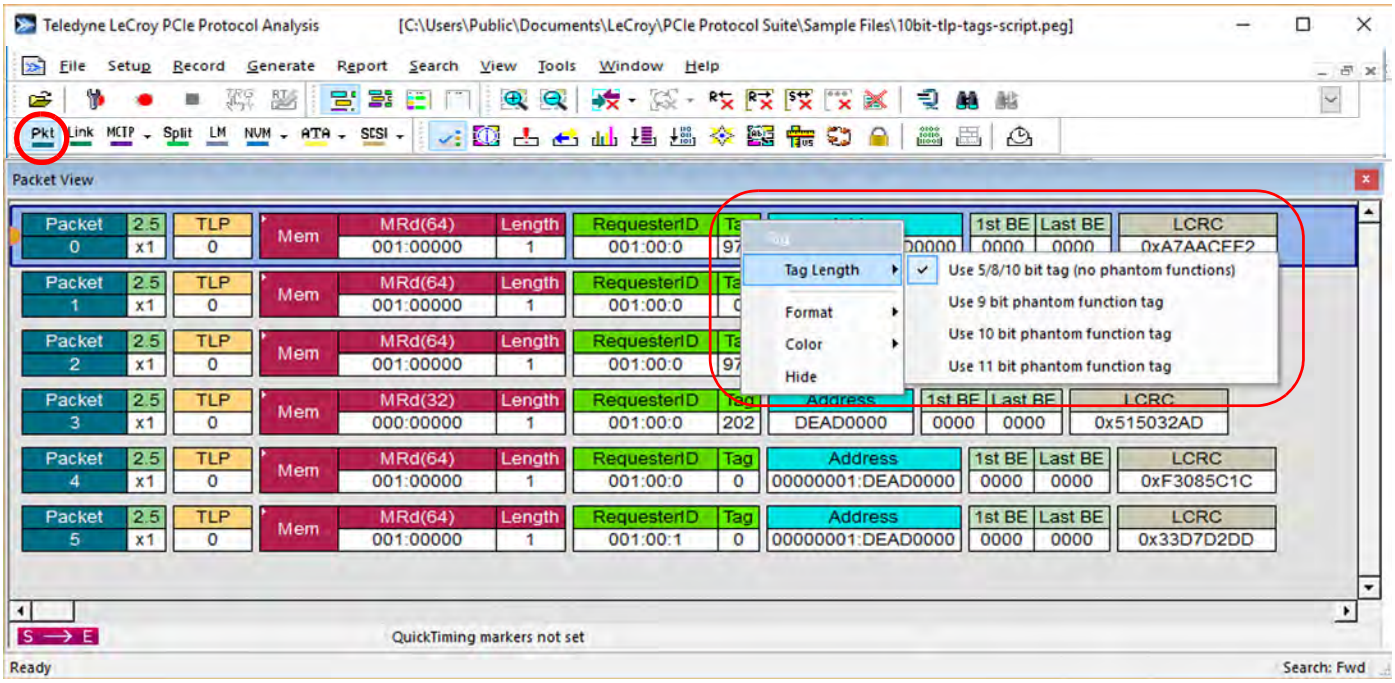


Figure 9.20: Packet Cell Popup Menus: Tag Length Pop Up Menu selections

The tag also has a tooltip associated with it to give you more information about the Packet's RequesterID Tag. See Figure 9.21 on page 535 and Figure 9.22 on page 535.

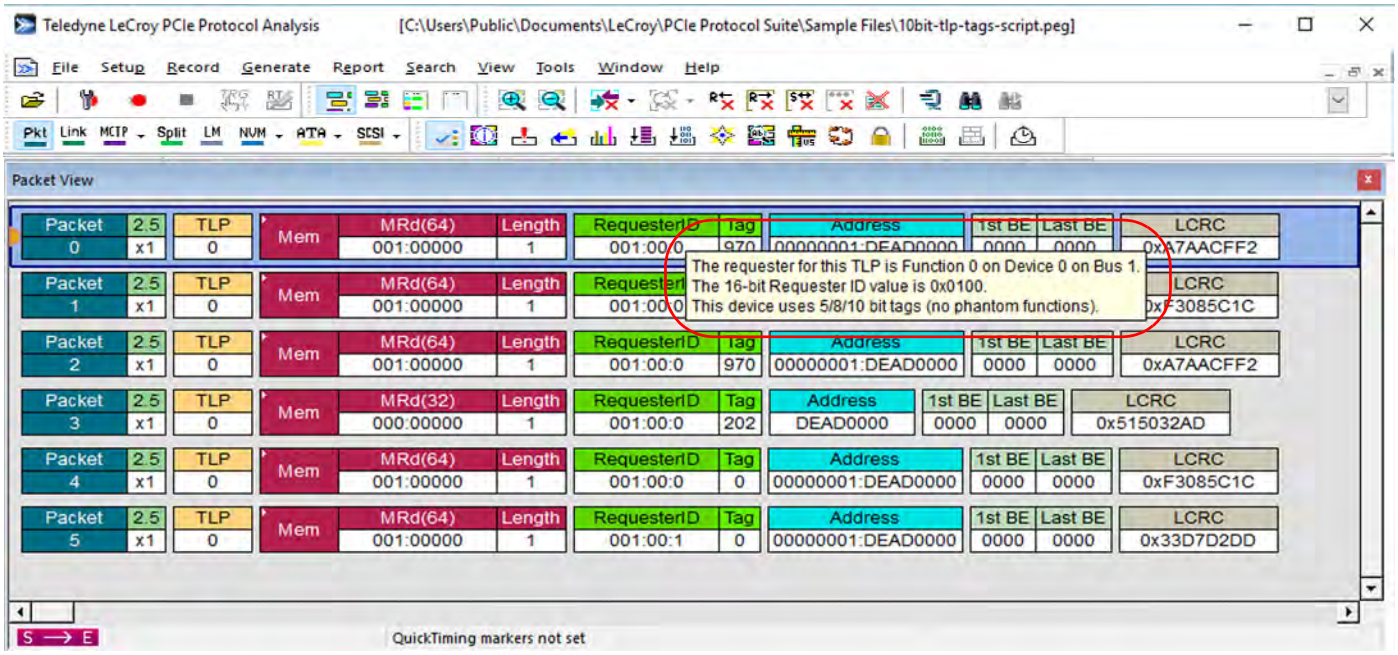


Figure 9.21: Packet Cell: Tag Tooltip

The Summit M5x can also decode RegisterID blocks that use phantom function tags. As shown in the figure below. See Figure 9.22.

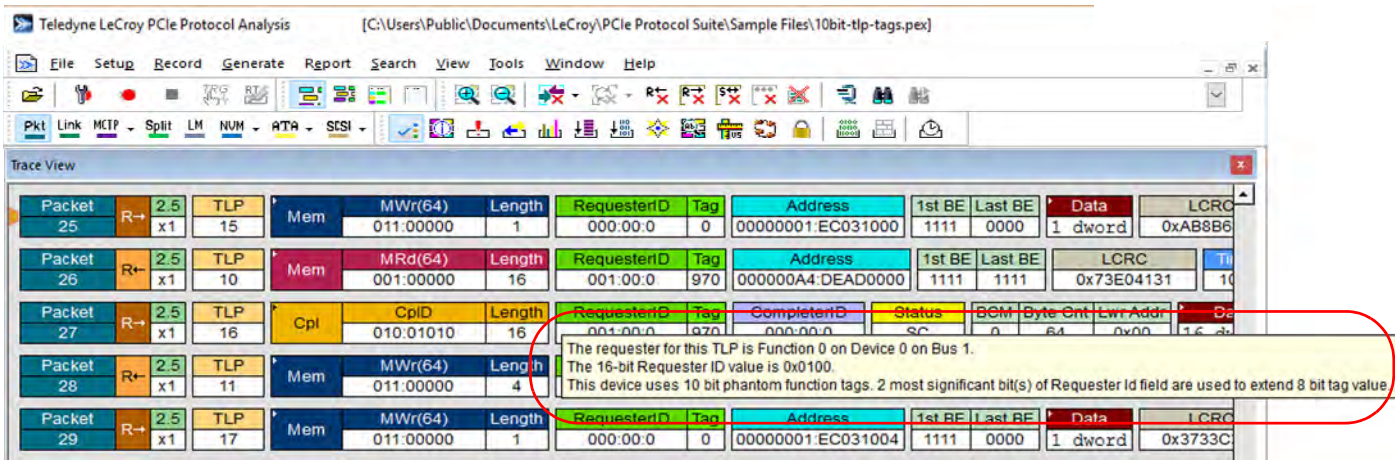


Figure 9.22: Packet Cell: Phantom Function Tag Tooltip

9.8.8.1 Quick Timing Bar

The Quick Timing Bar (see Figure 9.23 on page 536) at the bottom of the Trace View display window shows the following data between Markers:

- Delta Time
- Bus Utilization (both from Device to Host and from Host to Device)
- Data Throughput (both from Device to Host and from Host to Device)

Right click in the Quick Timing Bar to pop-up the menu to include or exclude the last selected packet/transaction from the timing, bus utilization and throughput calculations.

The data can be displayed in any available from selection units. Each value is described in bytes or bits value, to be comparable. Auto mode will select MB or GB automatically depending on result value so that values are more readable. The same units can be selected in theTiming Calculator dialog.

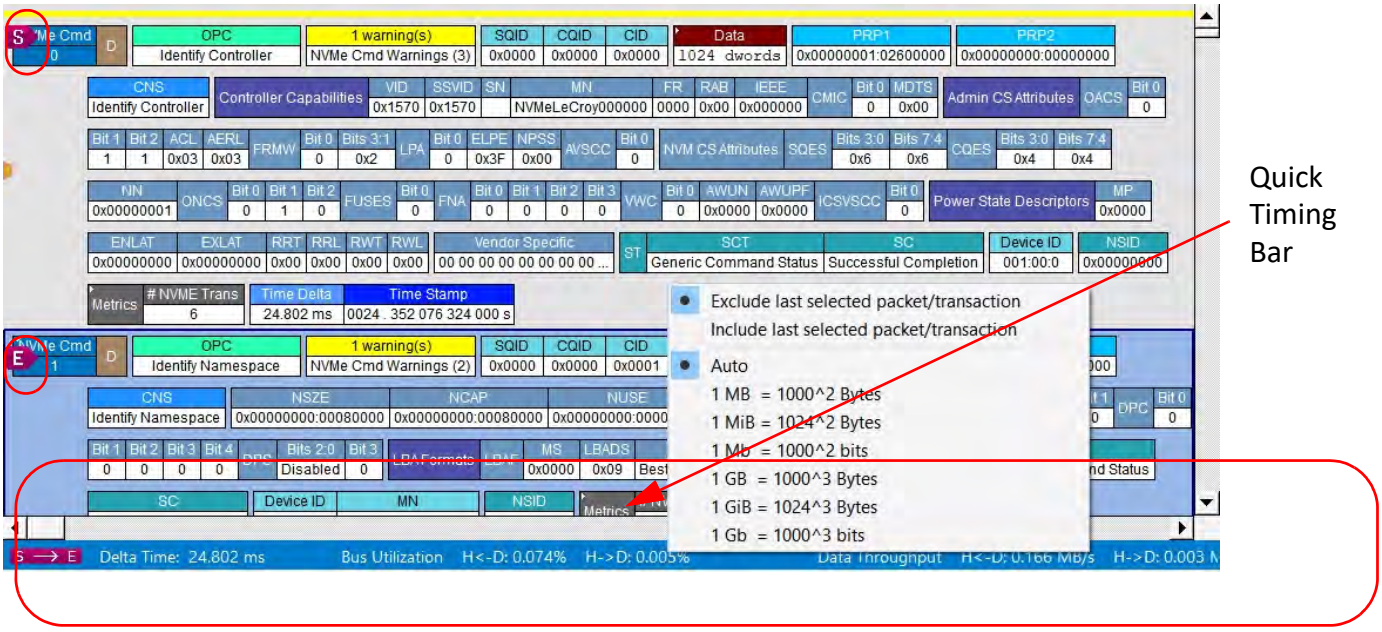


Figure 9.23: Quick Time Bar

9.8.9 Delete All Quick Timing Markers

Deletes all Quick Timing markers.

9.8.10 Set Marker

A marker is a unique label for a packet that allows you to go to that packet and also serves as a **comment string** for a specific packet. When you select a marker, the identified packet appears at the top of the screen. Packets that have been **marked** have a red bar on the left edge.

To set a marker, perform the following steps:

1. Right-click the **Packet** field of the packet you want to mark (see Figure 9.24 on page 537) or hover over the packet and click **Ctrl+K,** or select the packet and click **Ctrl+L**.

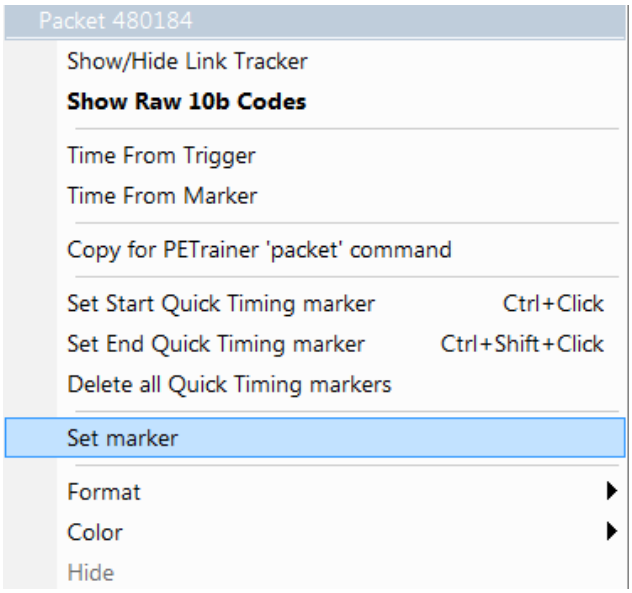


Figure 9.24: CATC Trace: Set Marker

2. Click **Set Marker**.
3. When the Create Marker for Packet # pop-up displays (see Figure 9.25), enter a unique identifier for the packet in the Comment field.

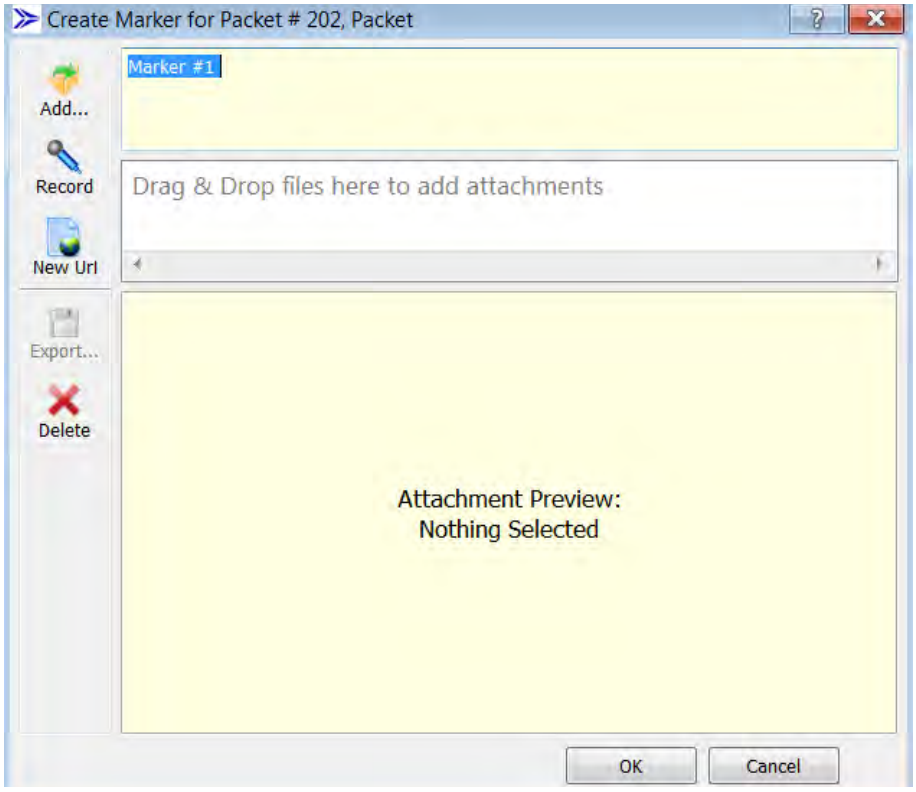


Figure 9.25: Create Marker for Packet Dialog

Later, you can go directly to this packet using the Go To Marker operation in the Search Menu.

9.8.11 Edit or Clear Marker

To change a markers identifier, or clear (delete) the marker:

1. Right-click the **Packet** field of the desired packet to display a pop-up menu (see Figure 9.26).

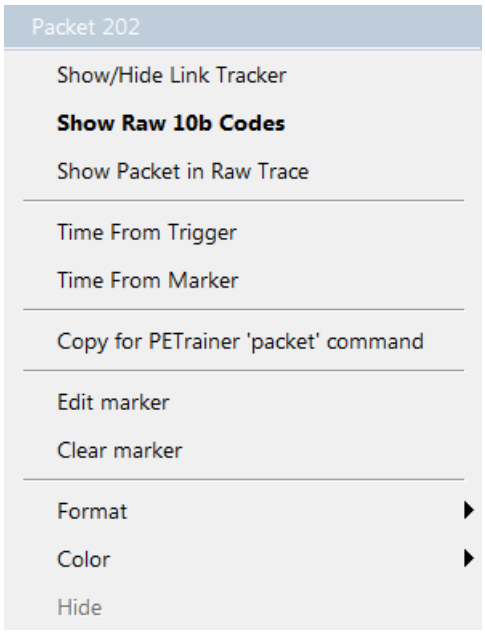


Figure 9.26: Edit Marker Pop-up Menu

2. Choose **Edit Marker** and enter a new identifier into the Edit Marker for Packer # pop-up, or
choose **Clear Marker**. When you choose Clear Marker, the marker is removed and the red line disappears.

9.8.12 Format

Selecting Format from the Packet Cell Popup Menus will allow you to change the format of the data from Hex, Decimal, Binary or ASCII. See Figure 9.27.

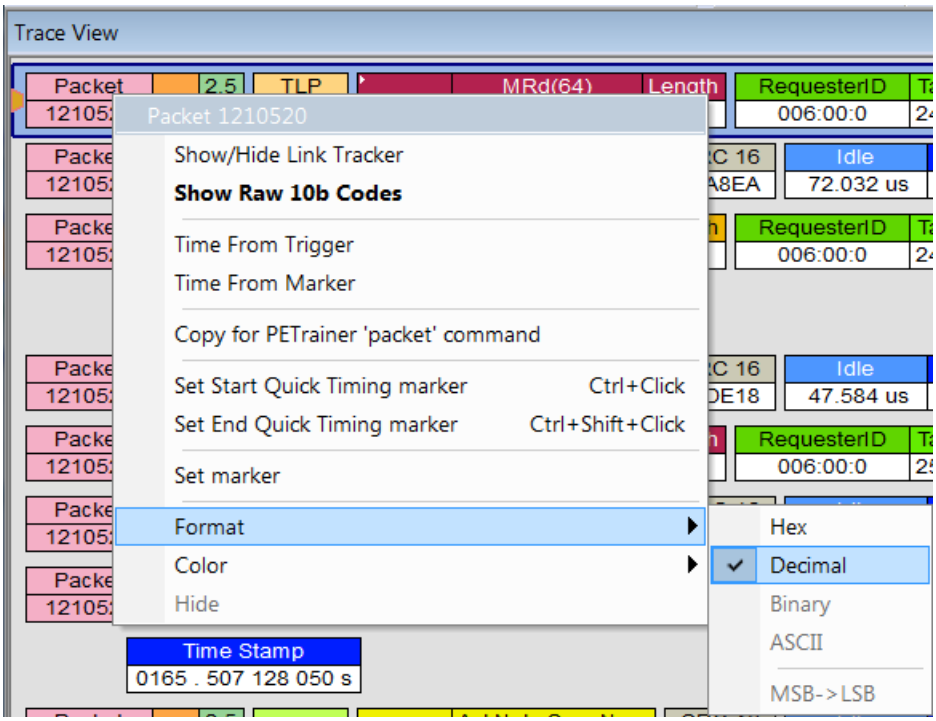


Figure 9.27: Packet Cell Popup Menus: Format

9.8.13 Color

Selecting the Packet Cell Popup Menu Color allows you to change the color of the Packet Cell. See Figure 9.28. Choose one of the twenty standard colors or pick Other for more choices.

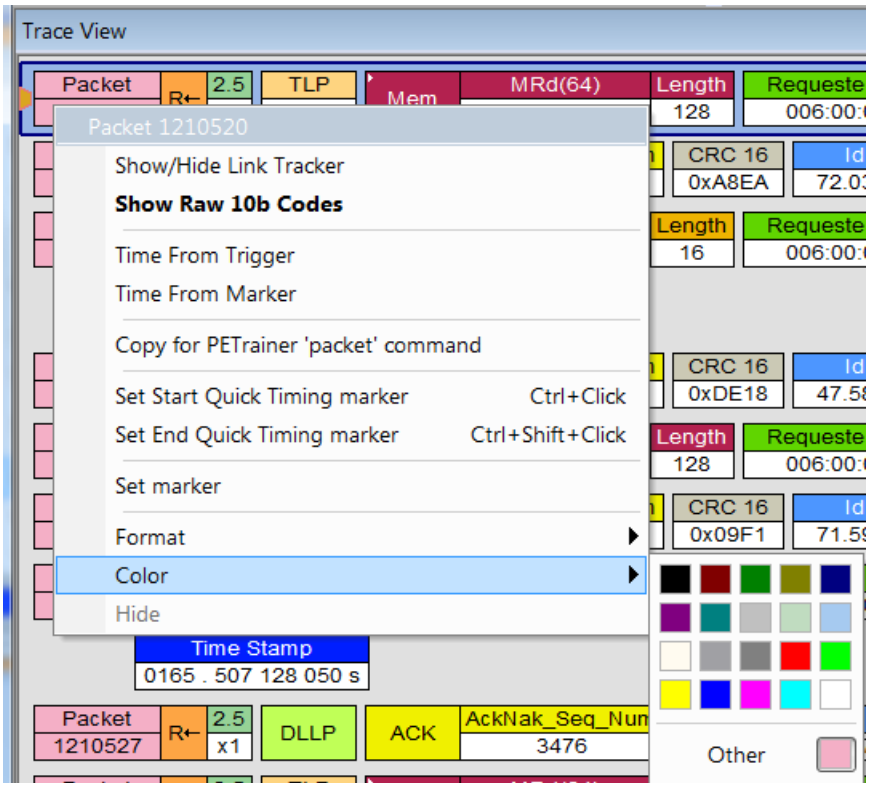


Figure 9.28: Packet Cell Popup Menus: Color

9.8.14 Other Packet Cell Context Menus

9.8.14.1 Packet Header R-> Cell Popup Menu

The Packet Header R-> cell context menu (see Figure 9.29) with the Swap Upstream/Downstream command, which changes the directionality of the packets in the CATC Trace.

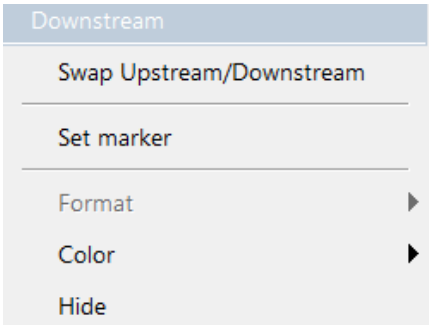


Figure 9.29: CATC Trace View: Packet Header Direction Popup Menu

9.8.14.2 Packet Header Speed Cell Popup Menu

The Packet Header Speed cell has a pop-up menu with the Show Header Fields command (see "Show Header Fields" on page 525), which exposes a detailed view of the selected Header field (see the following figure).

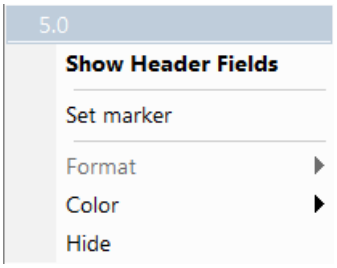


Figure 9.30: CATC Trace View: Packet Header Speed Popup Menu

9.9 Compressed CATC Trace View

The Compressed CATC Trace view shows fields in the format “Attribute: Value”, whereas the normal CATC View shows the attribute name on top and the value below.

The Compressed CATC Trace view has almost all the information of the normal CATC View and behaves mostly the same way, while displaying more information on each window (see Figure 9.31 on page 542).

To compress the CATC Trace:

- Click  on the toolbar.

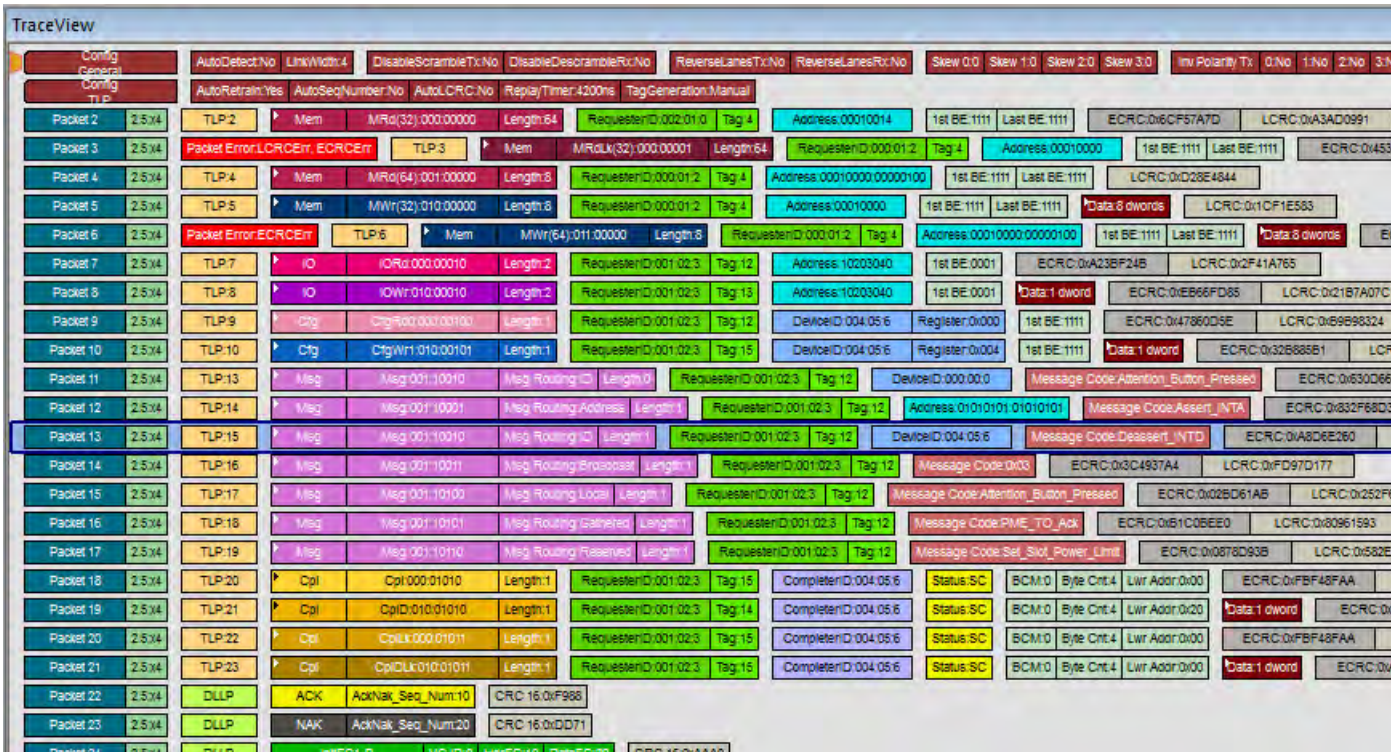


Figure 9.31: Compressed CATC Trace

- Click  on the toolbar to return to the normal CATC Trace View, or Select **View > Trace Views > CATC Trace.**

9.10 Spreadsheet View

You can view the CATC Trace as a spreadsheet in color or black and white.

Click  on the toolbar to display the Spreadsheet View (see Figure 9.32 and Figure 9.33).

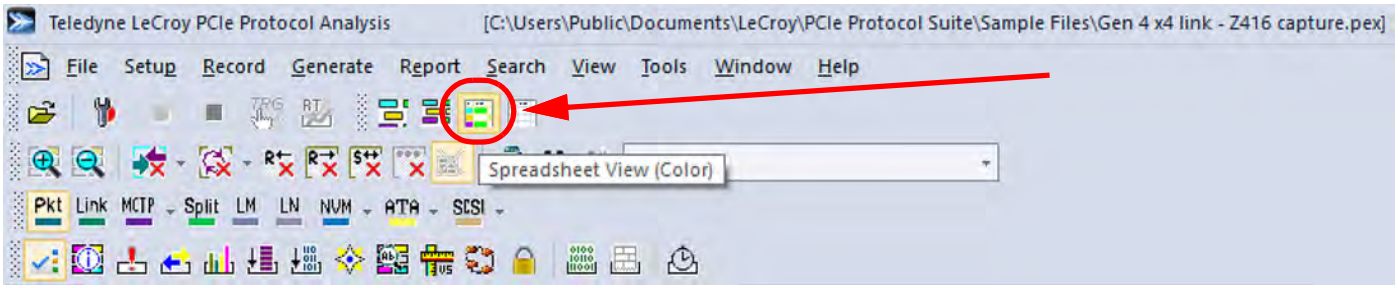


Figure 9.32: Spreadsheet View Icon in Toolbar

You can see the resulting Spreadsheet View of the trace below.

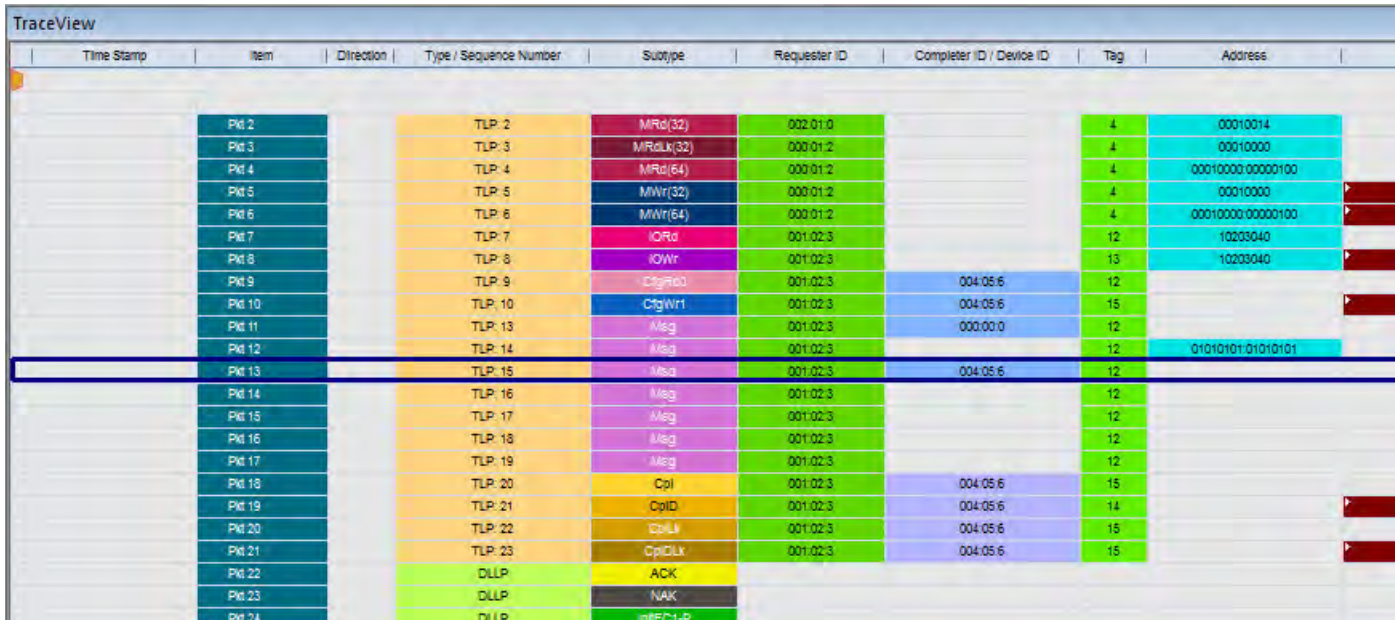
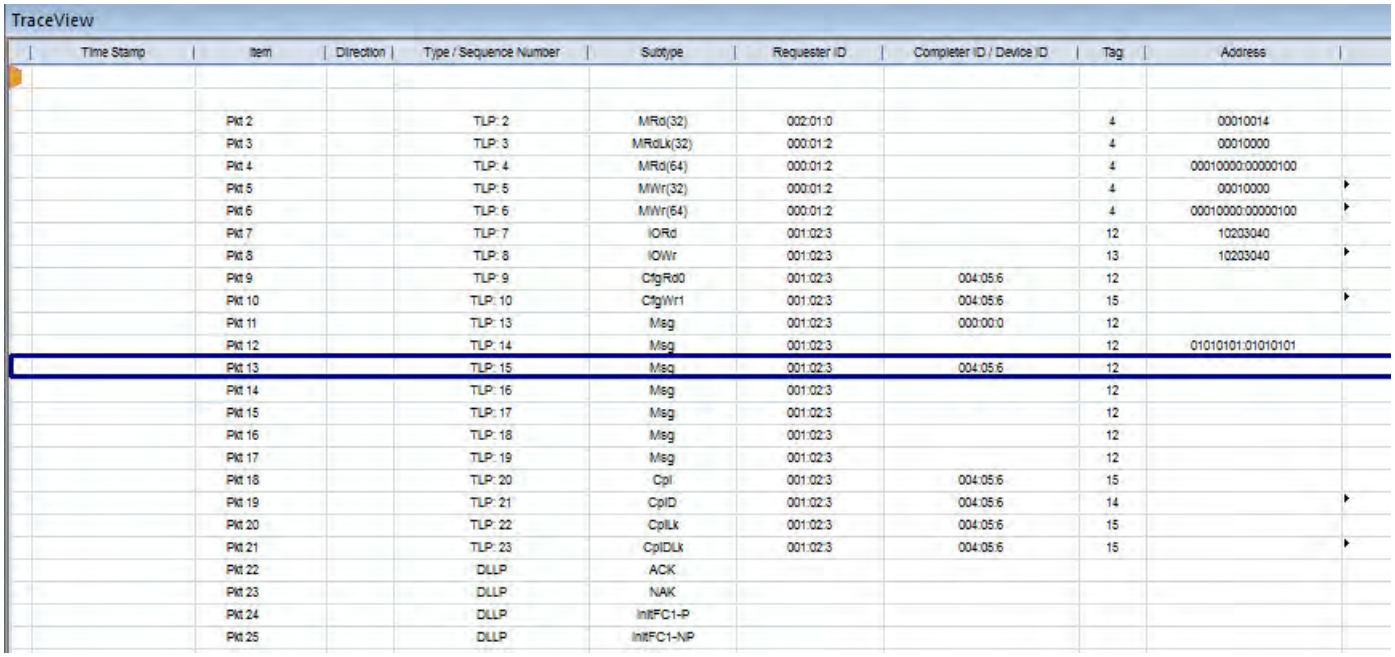


Figure 9.33: Spreadsheet View (Color)

- Click  on the toolbar to display the Spreadsheet View B/W.



TraceView

Time Stamp	Item	Direction	Type / Sequence Number	Subtype	Requester ID	Completer ID / Device ID	Tag	Address
	Pkt 2		TLP: 2	MRd(32)	002:01:0		4	00010014
	Pkt 3		TLP: 3	MRdLk(32)	000:01:2		4	00010000
	Pkt 4		TLP: 4	MRd(64)	000:01:2		4	00010000:00000100
	Pkt 5		TLP: 5	MWr(32)	000:01:2		4	00010000
	Pkt 6		TLP: 6	MWr(64)	000:01:2		4	00010000:00000100
	Pkt 7		TLP: 7	IORd	001:02:3		12	10203040
	Pkt 8		TLP: 8	IOWr	001:02:3		13	10203040
	Pkt 9		TLP: 9	CfgRd0	001:02:3	004:05:6	12	
	Pkt 10		TLP: 10	CfgWr1	001:02:3	004:05:6	15	
	Pkt 11		TLP: 13	Msg	001:02:3	000:00:0	12	
	Pkt 12		TLP: 14	Msg	001:02:3		12	01010101:01010101
	Pkt 13		TLP: 15	Msg	001:02:3	004:05:6	12	
	Pkt 14		TLP: 16	Msg	001:02:3		12	
	Pkt 15		TLP: 17	Msg	001:02:3		12	
	Pkt 16		TLP: 18	Msg	001:02:3		12	
	Pkt 17		TLP: 19	Msg	001:02:3		12	
	Pkt 18		TLP: 20	Cpl	001:02:3	004:05:6	15	
	Pkt 19		TLP: 21	CplD	001:02:3	004:05:6	14	
	Pkt 20		TLP: 22	CplLk	001:02:3	004:05:6	15	
	Pkt 21		TLP: 23	CplDLk	001:02:3	004:05:6	15	
	Pkt 22		DLLP	ACK				
	Pkt 23		DLLP	NAK				
	Pkt 24		DLLP	InitFC1-P				
	Pkt 25		DLLP	InitFC1-NP				

Figure 9.34: Spreadsheet View (Black And White)

9.10.1 Columns

Right click on any column and the following options pop up. See Figure 9.35.

You can perform the following options:

- Add a Standard Column if one has been deleted
- Add a column with specific types of information for the current row selected
- Remove a column
- Restore the default columns

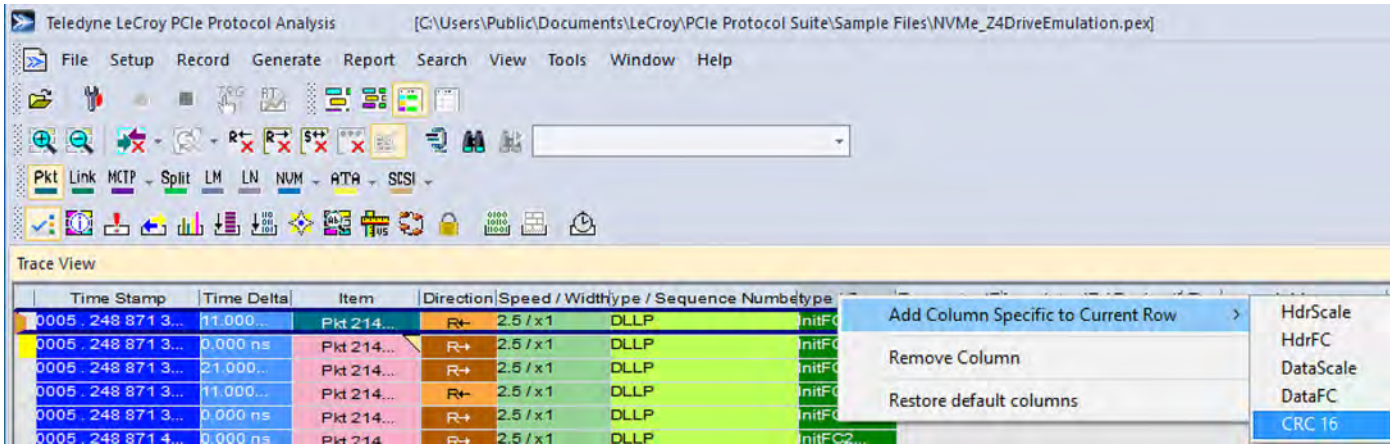


Figure 9.35: Add Columns Specific to Current Row

You can add a column with the CRC 16 values. See Figure 9.36

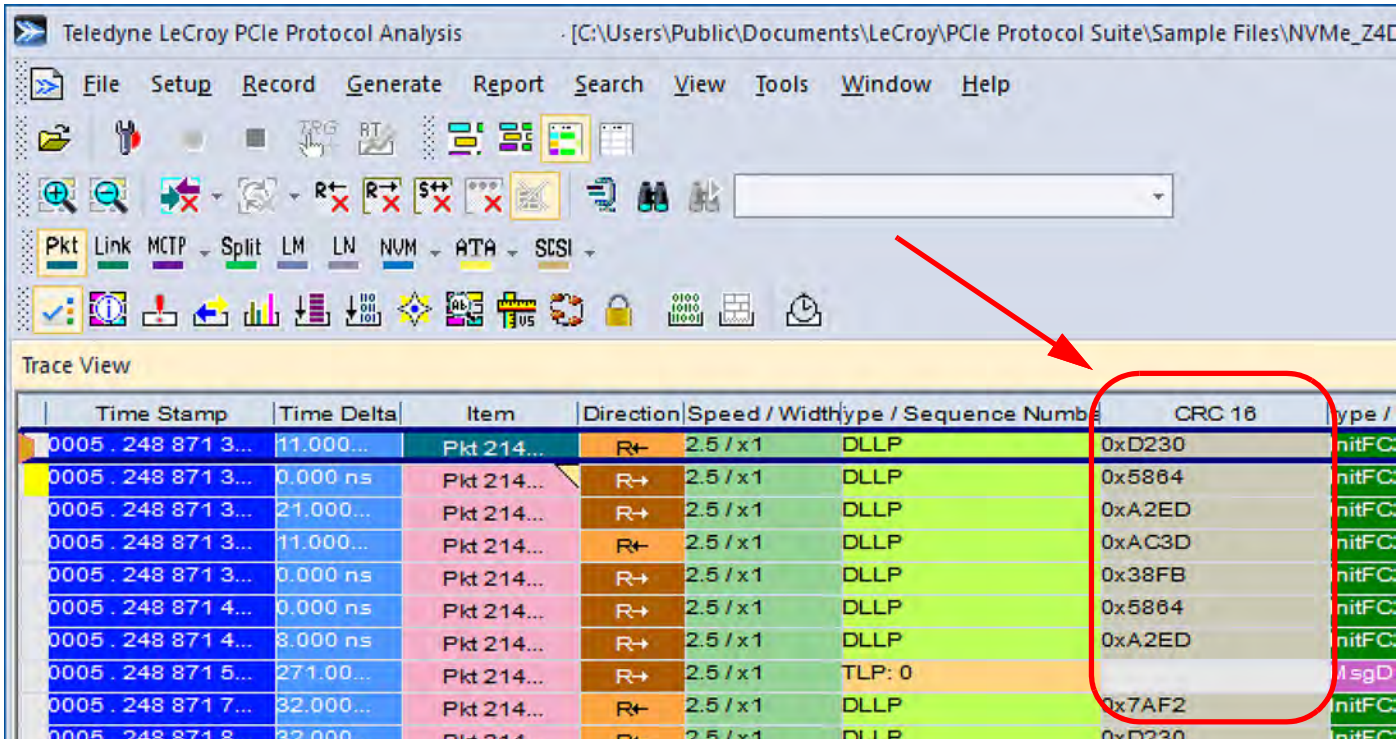


Figure 9.36: Added Column with CRC 16

You can delete the column that you right clicked on. See Figure 9.37.

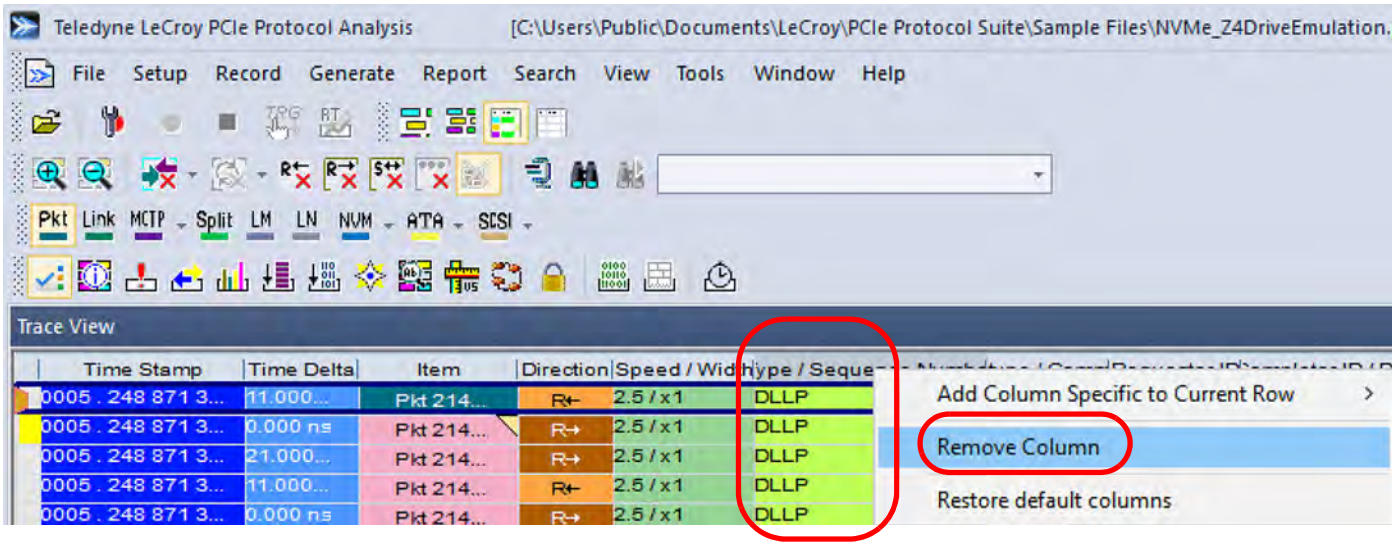


Figure 9.37: Right Click on Type/Sequence Number Column

Click on Remove Column and it's deleted from Spreadsheet View. See Figure 9.38.

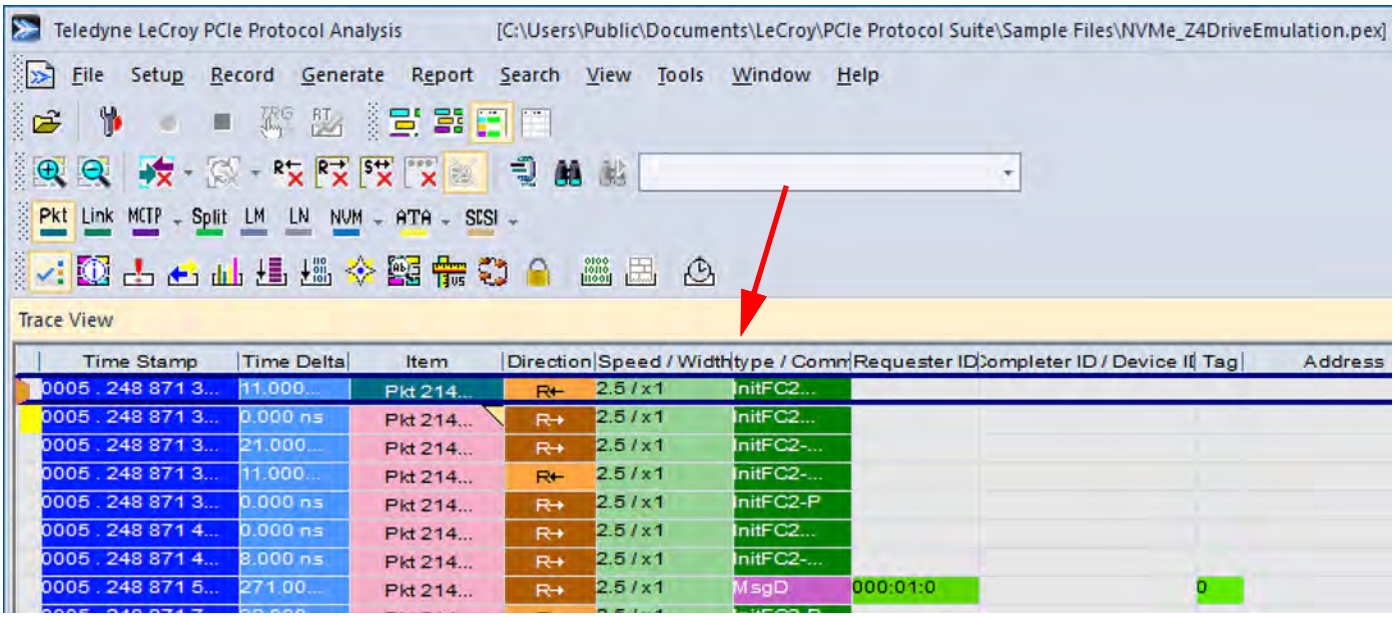


Figure 9.38: Selected Column Removed

You can also Restore the set of system Default columns. See Figure 9.39 on page 547.

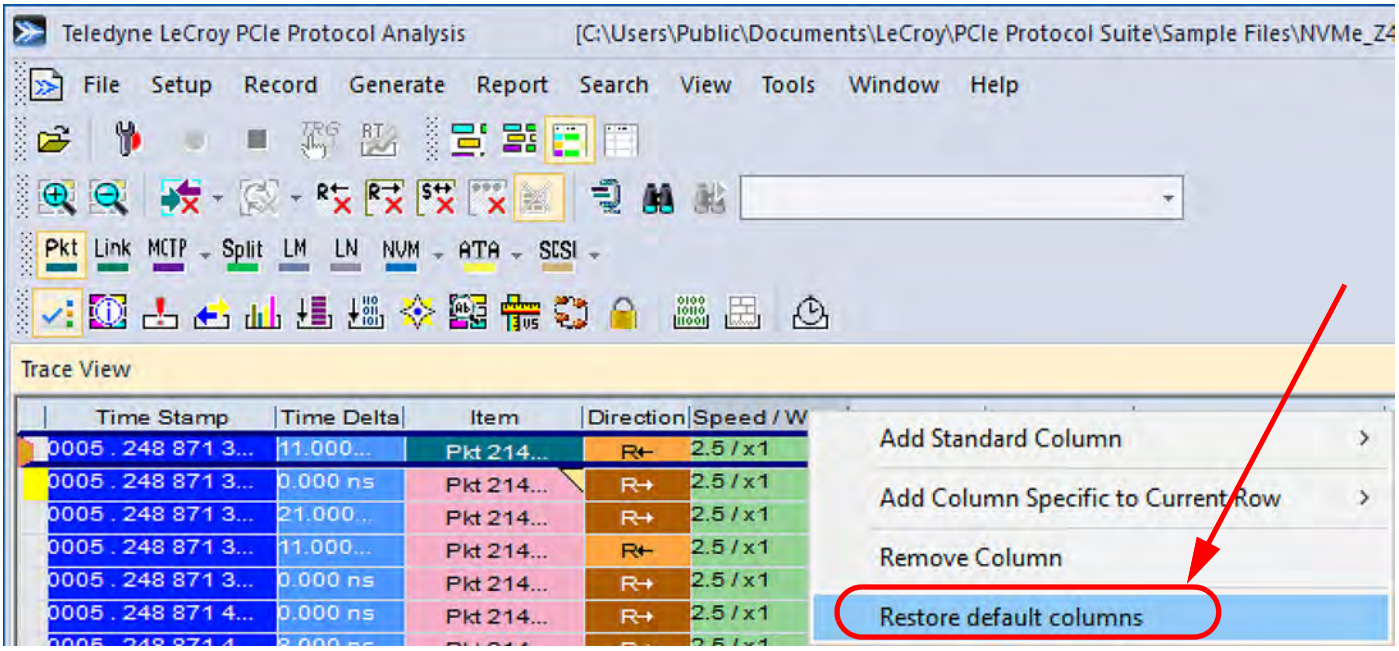


Figure 9.39: Restore Default Columns

If you select Restore default columns you'll get a Warning message. See Figure 9.40.

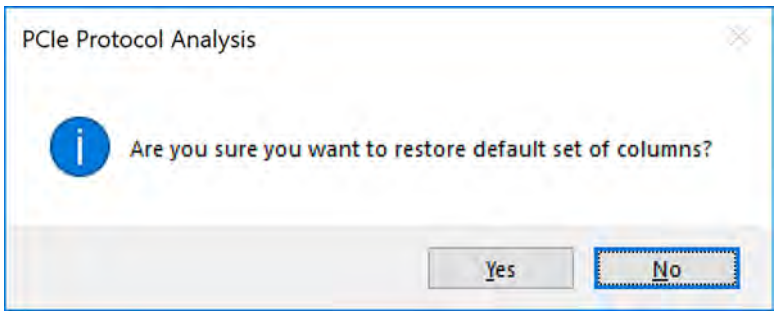


Figure 9.40: Warning Message about Restoring Default Set of Columns

Click on Yes and you'll get the default set of columns. See Figure 9.41 on page 548.

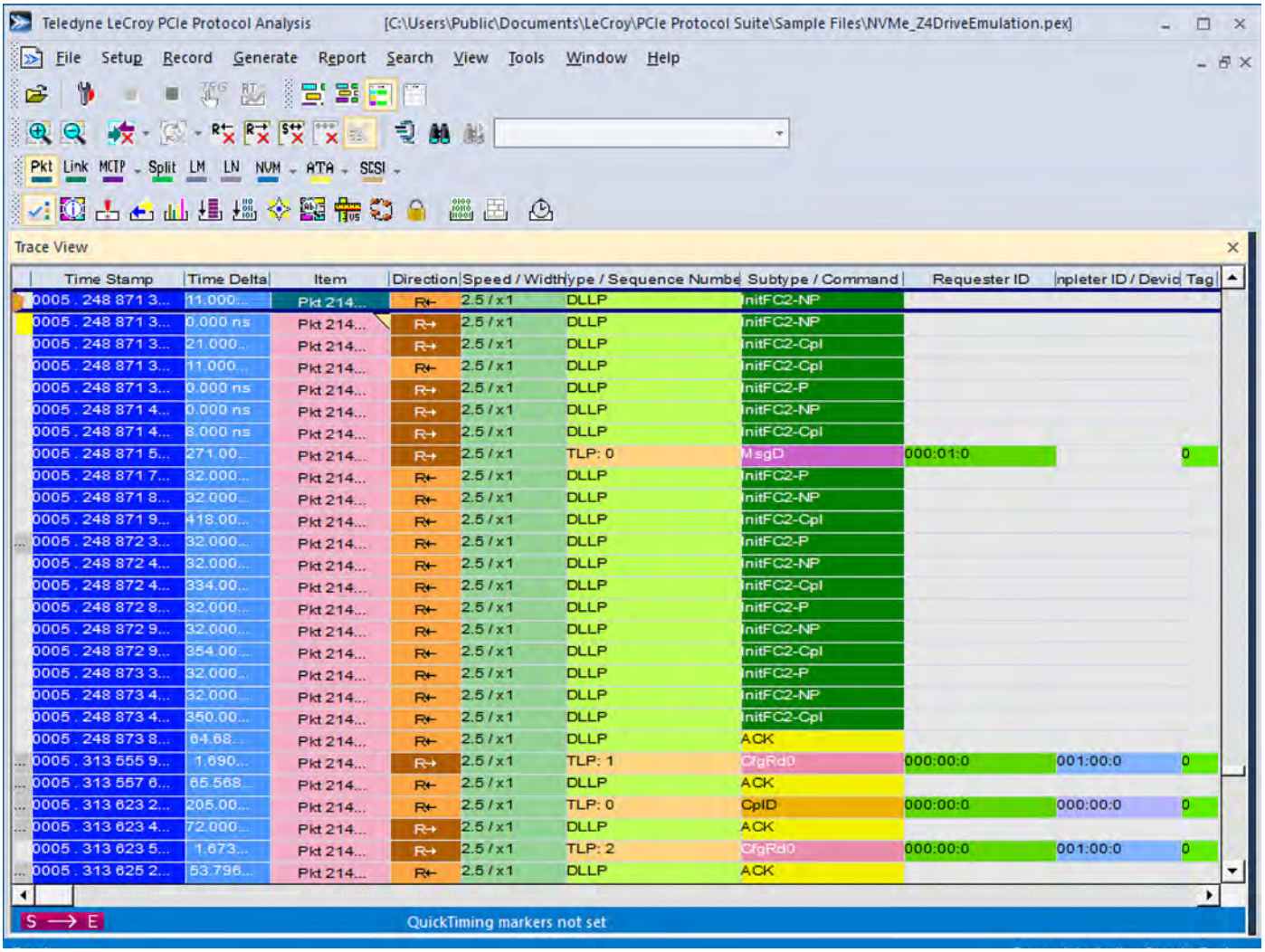


Figure 9.41: Default Set of Columns

9.10.2 Detail View and Spreadsheet View

In the Spreadsheet View, double-click a packet, transaction, or transfer, or select a field and then click on the toolbar, to display the Detail View (see Figure 9.42 on page 549).

To put a Detail View header as a column in the Spreadsheet View, drag the header to a column divider in the Spreadsheet View.

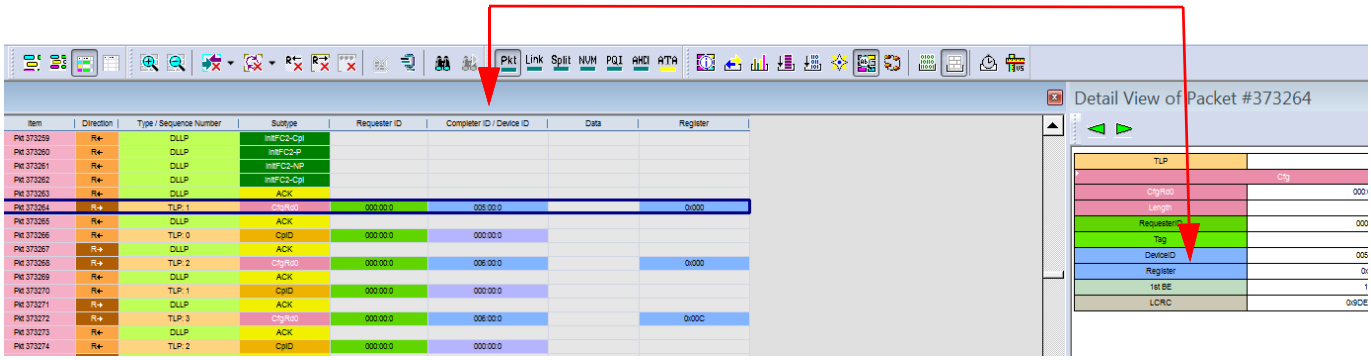


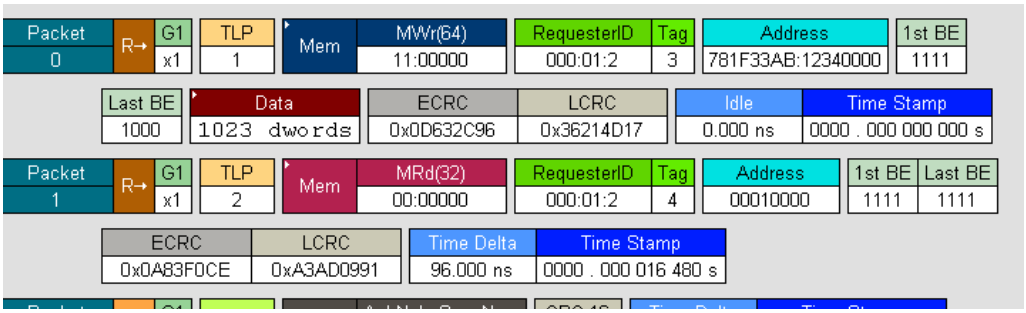
Figure 9.42: Detail View in Spreadsheet View

9.11 Decoding Traffic

The PCIe Protocol Analysis has several decode levels:

9.11.1 Packet

Packet level decode Pkt includes all TLP packets, DLLP packets, and all ordered sets.



Note: The PCI-E 3.0 (and 2.1 with Errata) specifications state that there are two formats of the AER capability structure, and the AER_CAP_VER field indicates if format 1 or format 2 is used.

The difference between format 1 and format 2 is whether or not the TLP Prefix Header section is present in the AER capability, even if it is not actually implemented.

This means that:

- If AER_CAP_VER = 1 and it is not a Root Port or RC Event Collector, there are 11

DWs (00h to 24h)in the total AER Capability structure.

- If AER_CAP_VER = 1 and it is a Root Port or RC Event Collector, there are 14 DWs (00h to 34h)in the total AER Capability structure.
- If AER_CAP_VER = 2 then, there are 18 DWs (00h to 44h) in the total AER Capability structure.

There are PCI-E 3.0 compliant devices that have AER_CAP_VER=1.

Example H/W:

A PCI-E 3.0 device that supports Multiple Header Recording, but does NOT support TLP Prefixes. This device is allowed to have AER_CAP_VER=1, and Multiple_Header_Recording_Capable=1

Therefore, the Teledyne LeCroy software decodes the Multiple_Header_Recording_Capable field regardless of the value of AER_CAP_VER.

Note: The Protocol Mode of the CATC View may show individual symbols grouped as a "packet" such as in the case where electrical symbols arrive before fast training sequences. Such group of symbols will also be reported in the summary. See Figure 9.43 on page 551.

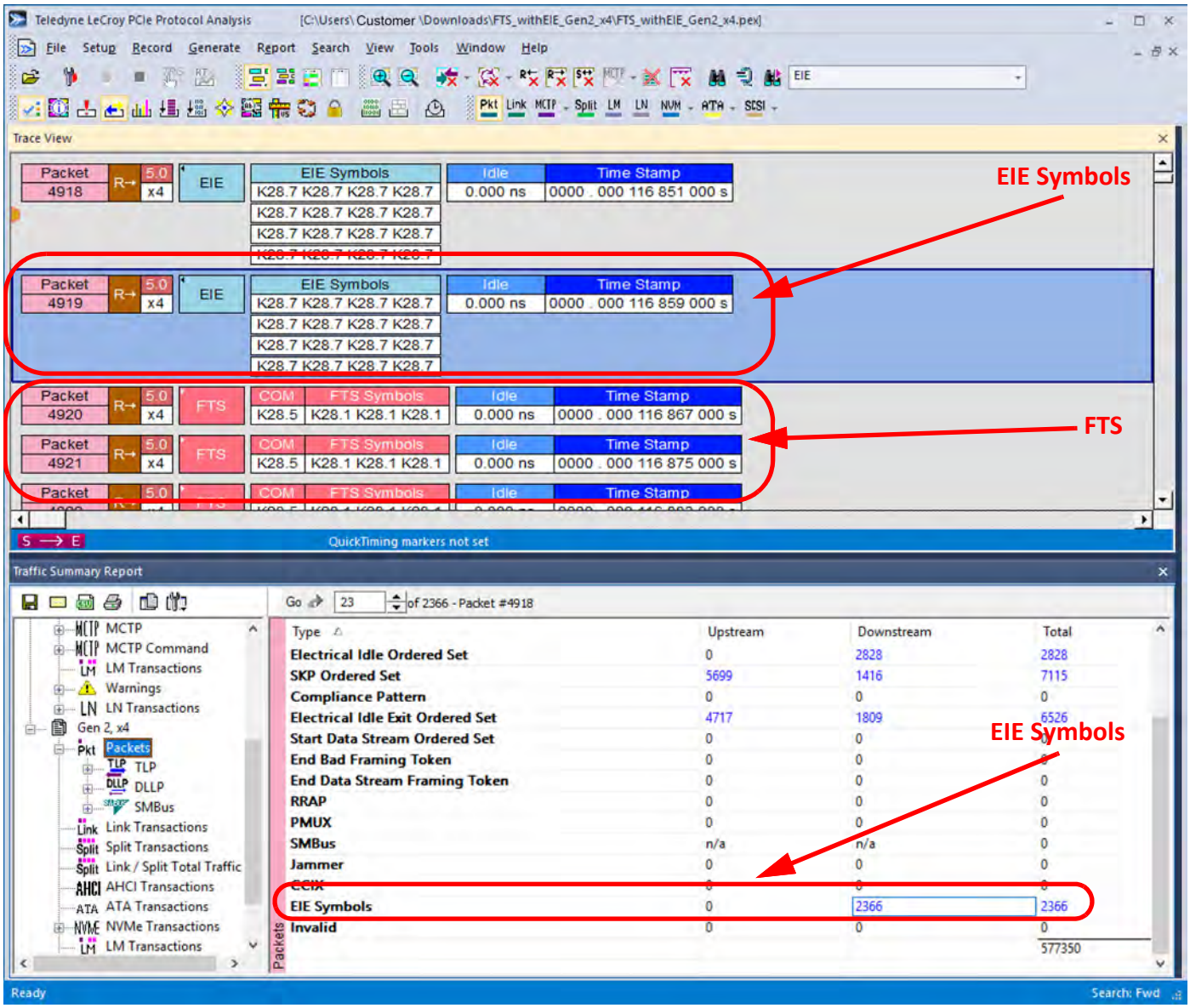
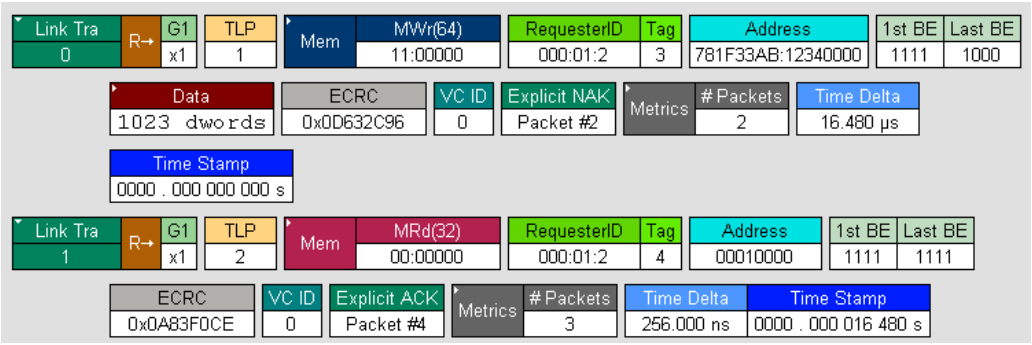


Figure 9.43: EIE Symbols Decoded before FTS

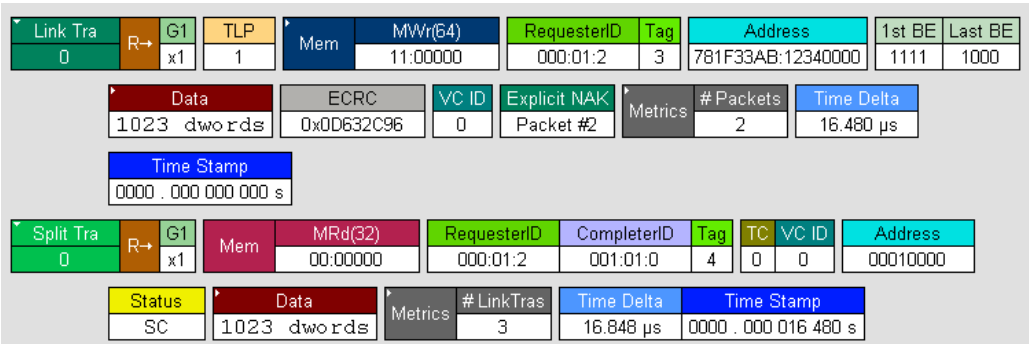
9.11.2 Link

Link level decode  is composed of TLP packets matched with a corresponding ACK or NAK coming from the opposite direction.



9.11.3 Split

Split level decode  is composed of two Link transactions, the Request TLP and the Completion TLP from the other direction.



9.11.4 Lane Margining Decoding

The purpose Lane Margining LM is to determine if the PCIe Protocol Analysis software can run a series of commands to do the equivalent of moving the sampling point of the transceiver backwards or forwards in time (time margining) or at a higher or lower voltage (voltage margining). If there is enough margin to still reliably capture data without errors at that new sampling point then the system software can determine how much margin exists within the system. An example trace that shows some of the commands and response is shown below. See Figure 9.44.

9.11.4.1 Typical Lane Margining Commands and Responses

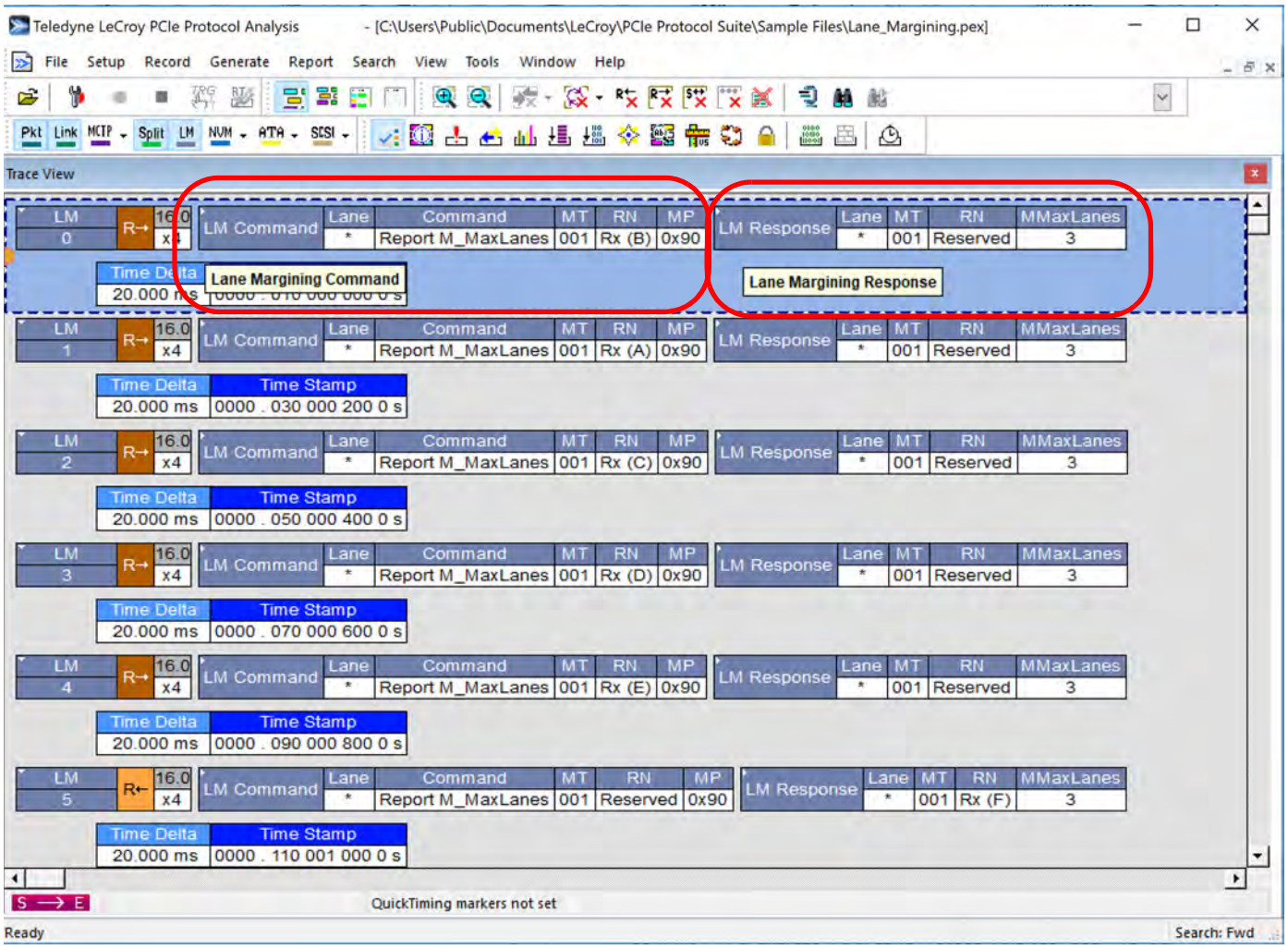


Figure 9.44: Lane Margining Decoding: Command and Response

More Lane Margining Commands and Responses are shown in Figure 9.45 on page 554.

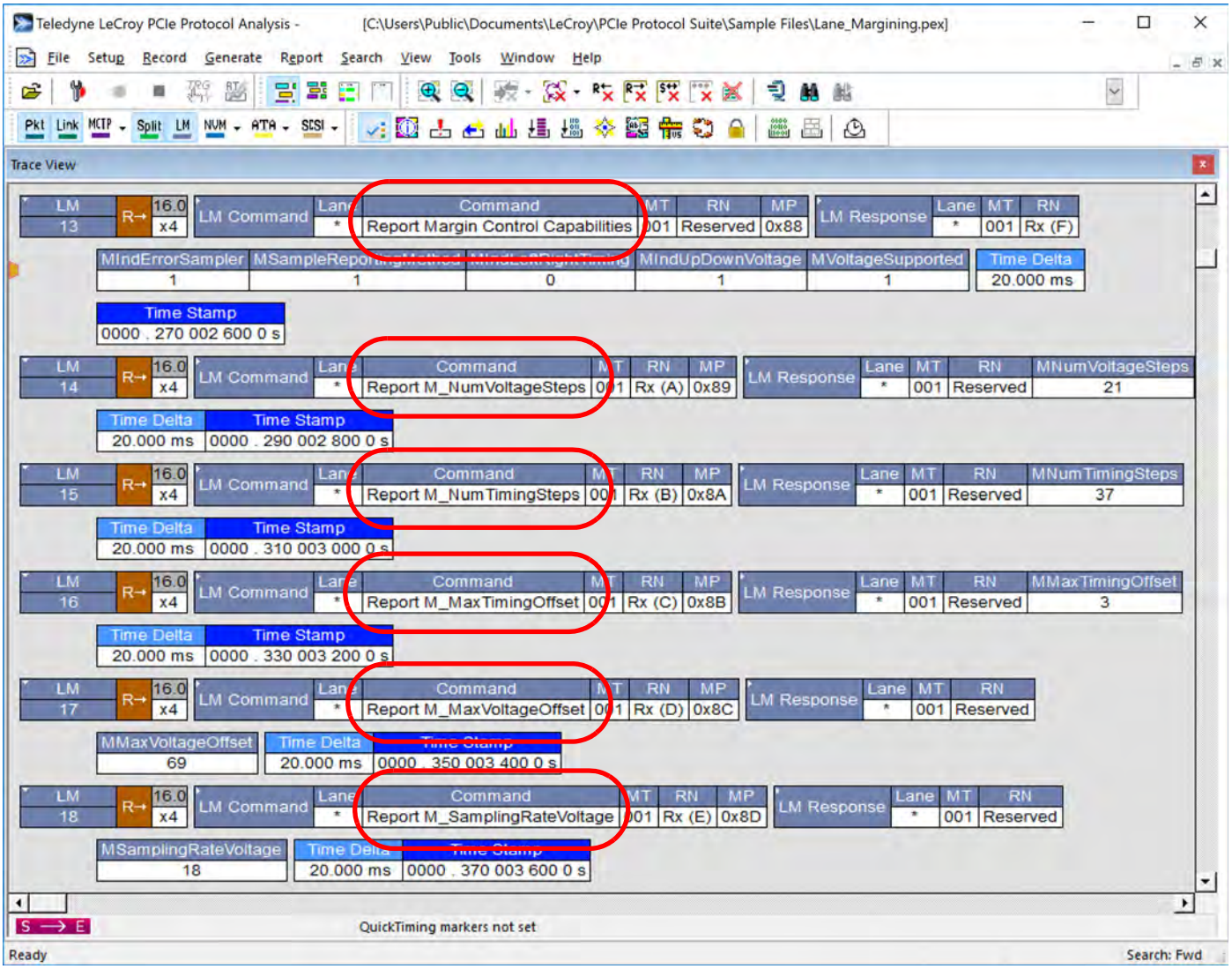


Figure 9.45: More Lane Margining Commands and Responses

9.11.4.2 Lane Margining Command: Step Margin to Timing Offset

The Lane Margining Command: Step Margin to Timing Offset in shown in Figure 9.46.

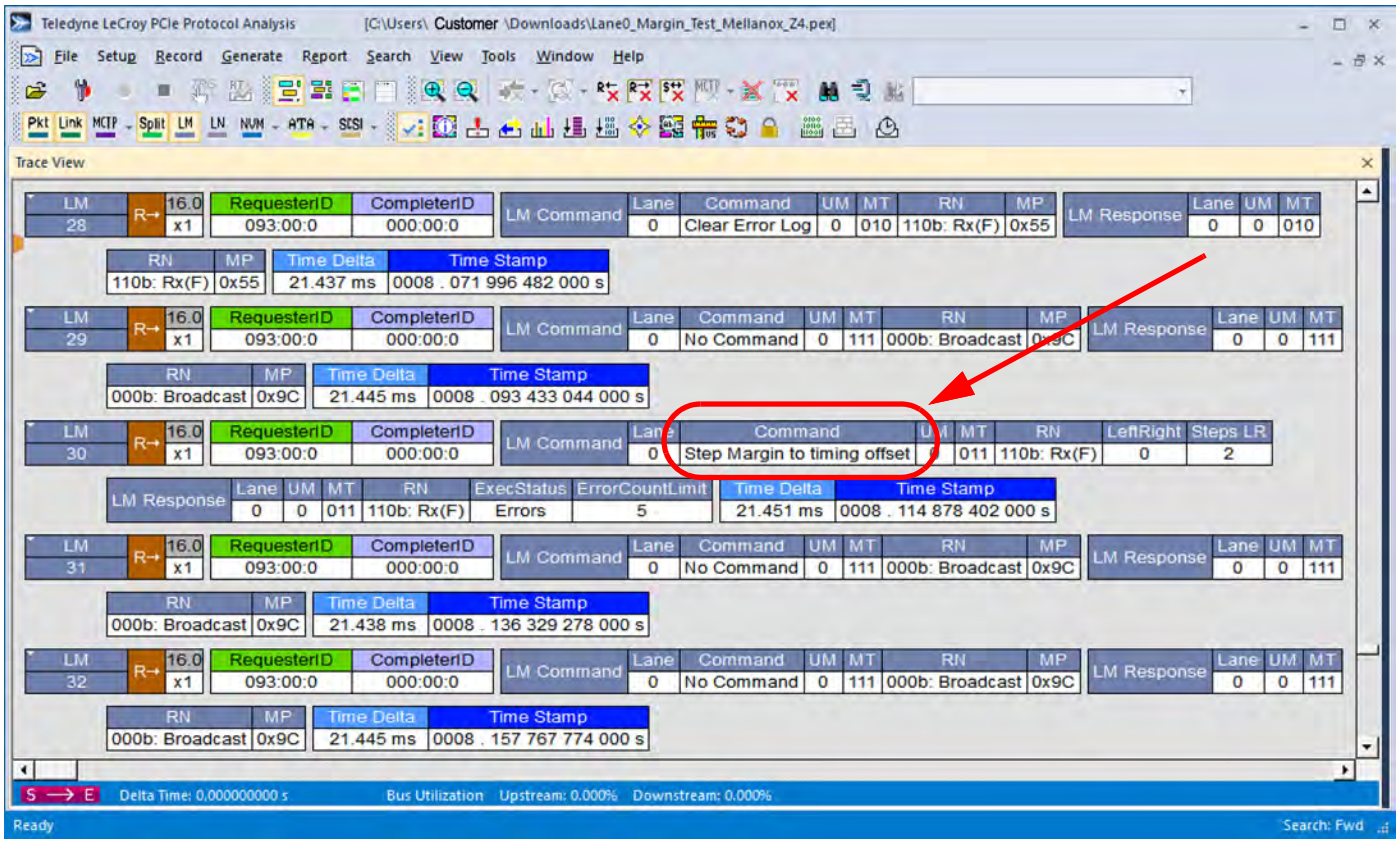


Figure 9.46: Lane Margining Command: Step Margin to Timing Offset

9.11.4.3 Lane Margining Errors

Lane Margining errors can also be decoded. As shown in the sample below (see Figure 9.47).

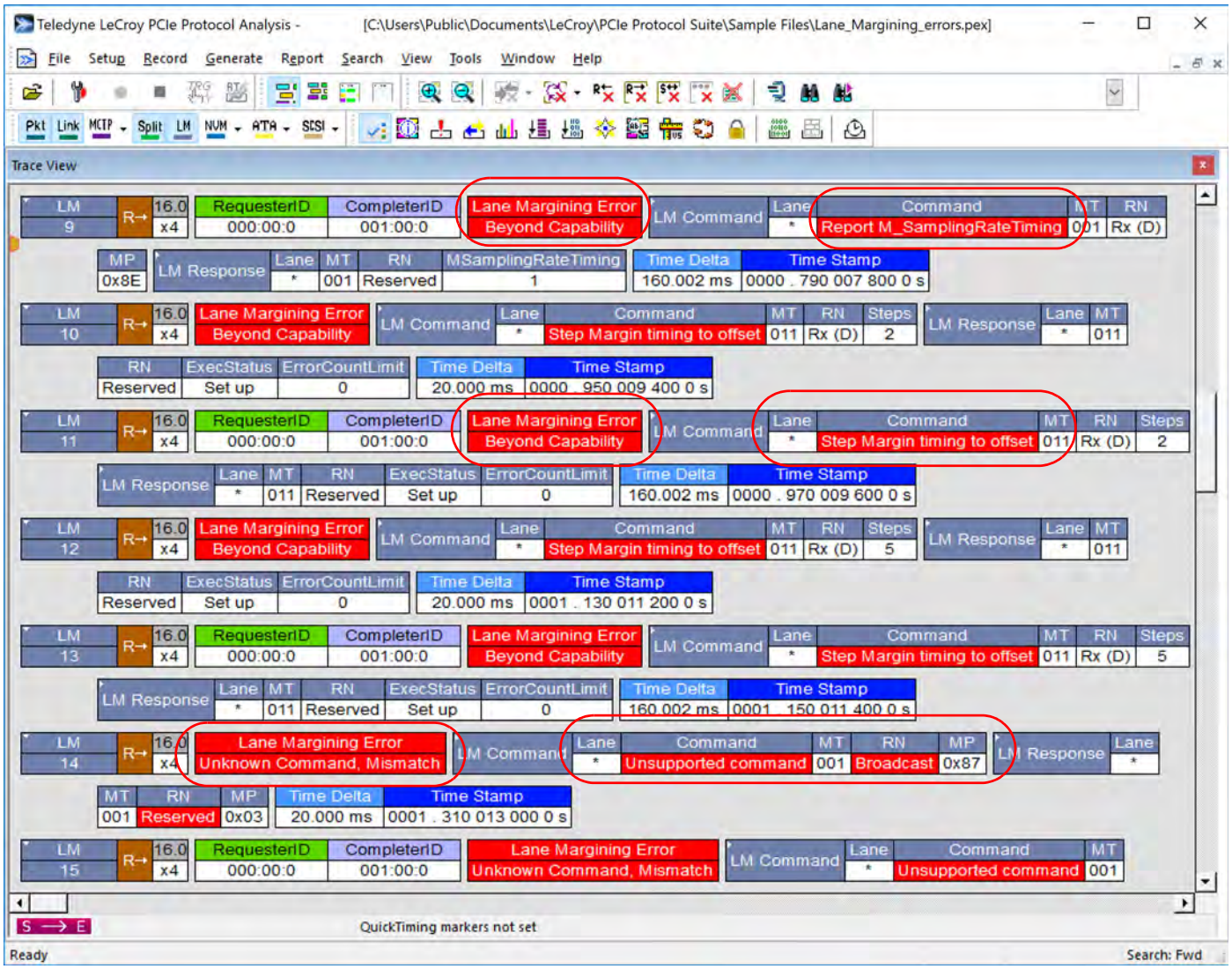


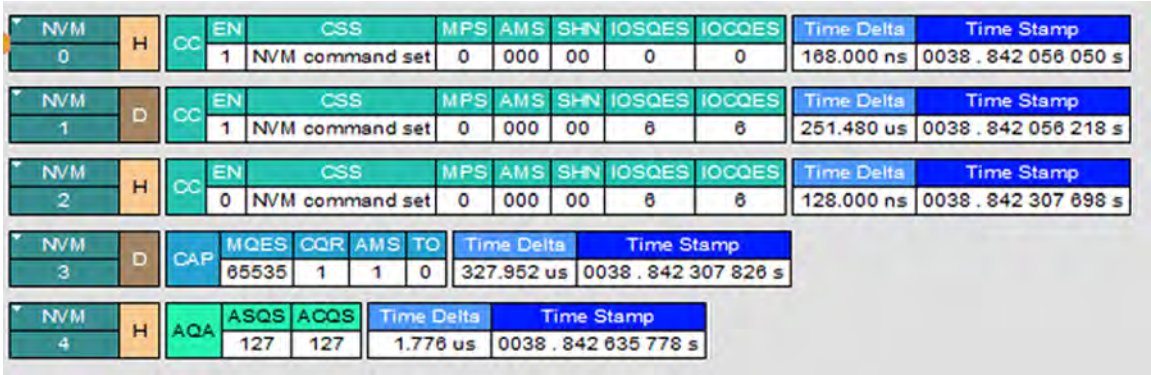
Figure 9.47: Lane Margining Errors: Decoded

9.11.5 NVMe Decoding

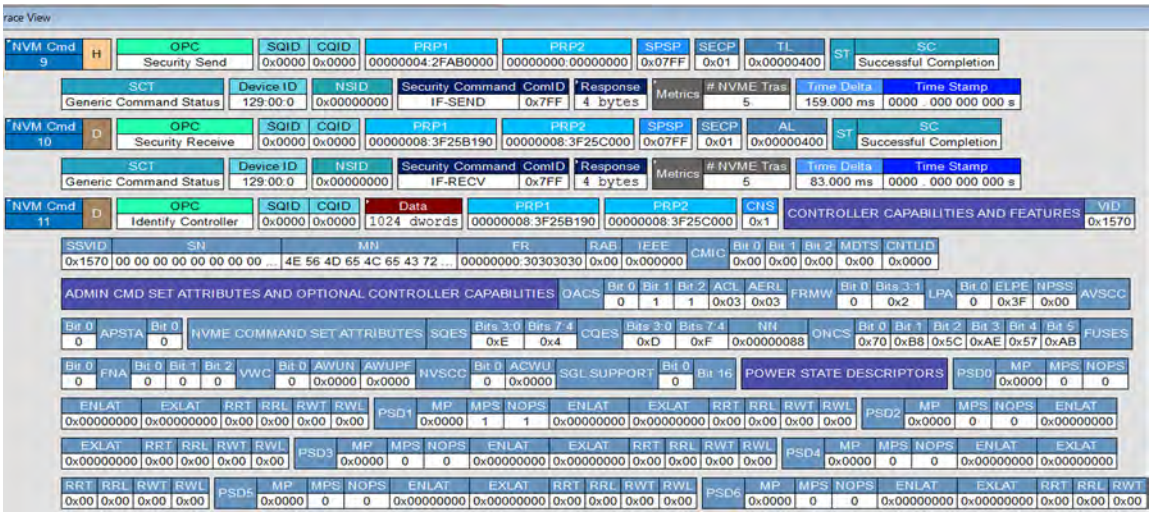
To decode the NVMe protocol there are two levels available: NVMe Transaction level, which decodes the individual NVMe transactions from the PCI Express protocol and NVMe Command level, which gathers NVMe transactions into a single command. If the top level button 

is selected, it will decode the NVMe Command level directly.

The NVMe Transaction level option displays NVMe transactions. PCIe Protocol Analysis decodes the storage commands starting from lower PCI Express Transaction Layer decodes. In the case of NVMe, it will decode first the Packet Level, then the Link Transaction level, then the Split Transaction Level and finally the NVMe Transaction decode level.



The NVMe Command level option displays NVMe Commands. The NVME commands decode all the lower level decodes first.



Note: As of software version 7.34, the NVMe decoding will be performed properly even if the ACK DLLPs have been filtered.

Note: As of software version 7.34, once the NVMe decoding has been applied, it will be kept in a separate temporary file not the Trace file (see "Trace File Structure" on page 113). The next time the trace is opened for review there will be no need to re-decode, making opening of the file in NVMe mode faster.

Note: As of software version 7.36 Beta, the NVMe decoding can handle multiple controller resets within the same recording.

9.11.5.1 NVMe: Device ID and Model Name Decoded

As of software version 7.34, the Device ID and Device Model Name field is displayed in the decoded command (see Figure 9.48 and Figure 9.49 on page 559).

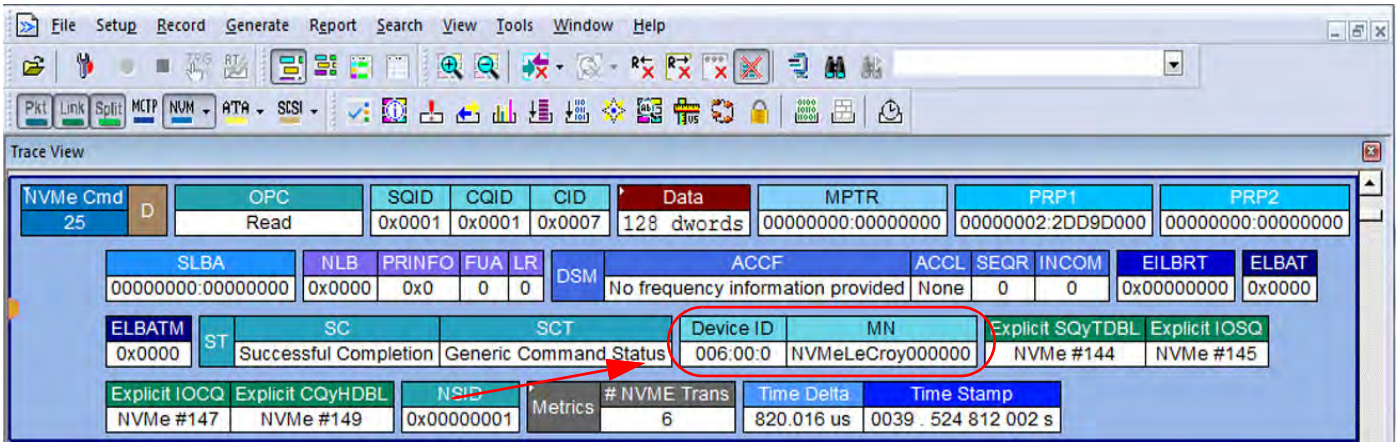


Figure 9.48: Device ID and Model Number Decoded from NVMe Trace

The trace must contain the device enumeration sequence so the decoding picks up the associated base addresses and NVMe transactions can be properly decoded. If the enumeration sequence is not available the base addresses must be manually entered in the PCIe SSD Configuration dialog from the Tools menu. See Figure 9.49 on page 559.

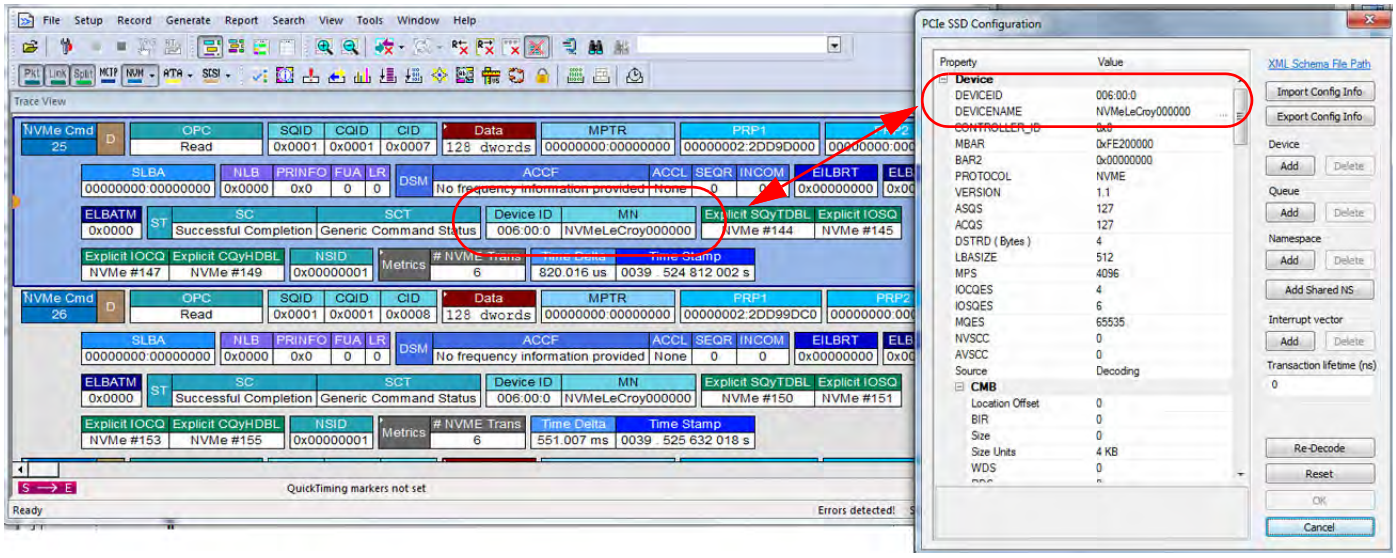
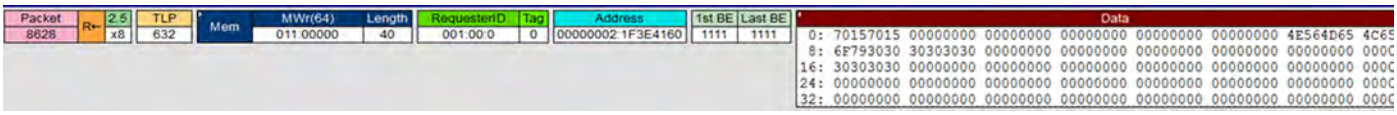


Figure 9.49: Device ID and Device Model Name Shown in SSD Configuration Dialog

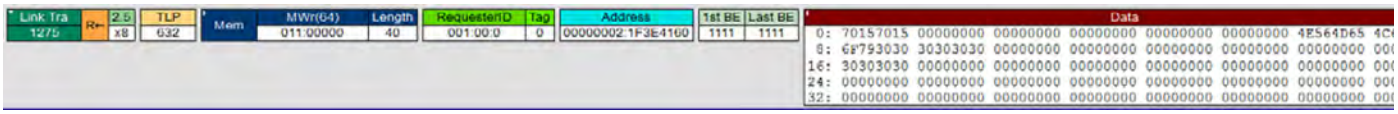
9.11.5.2 NVMe: Data Field on Packets

While the data field section displayed for a PCIe packet shows the actual payload for that PCIe packet (as shown below):

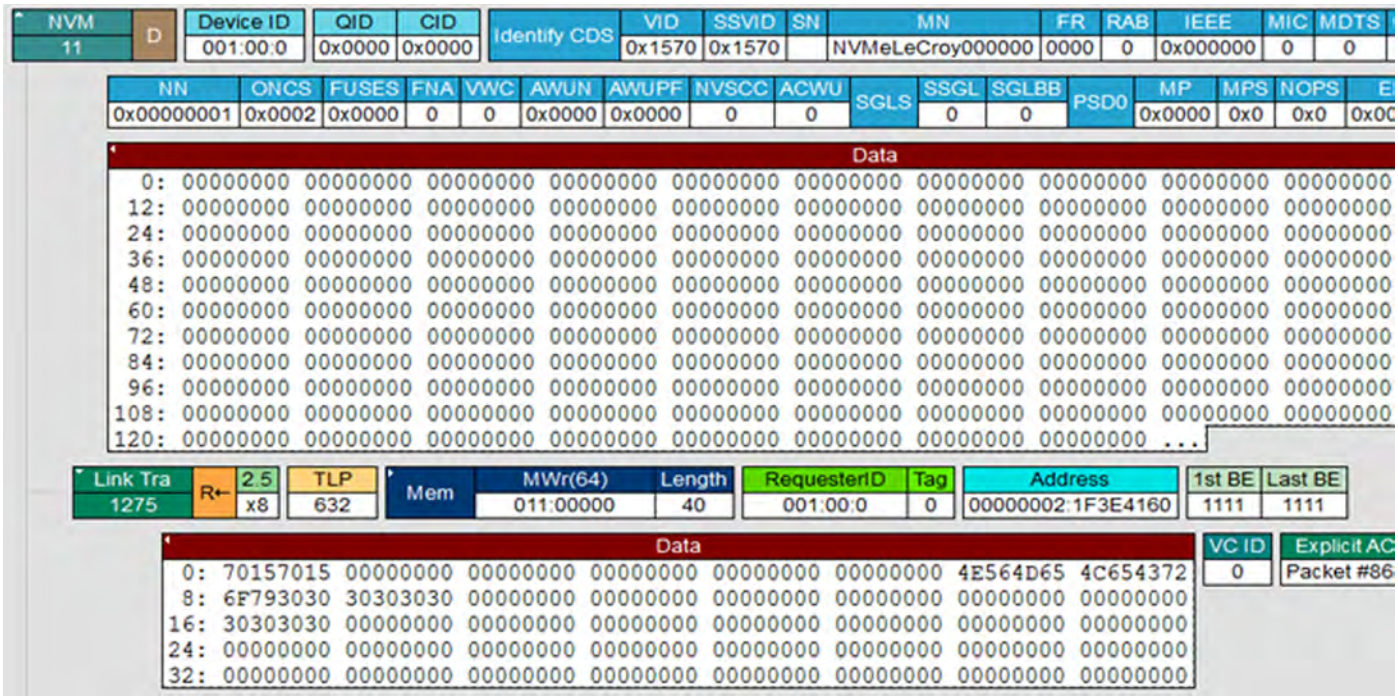


The content for this field changes depending on the decode level selected and the particular command decoded.

For example, at the PCIe transaction level, this field still reflects the PCIe payload field involved in the PCIe transaction (as shown below):

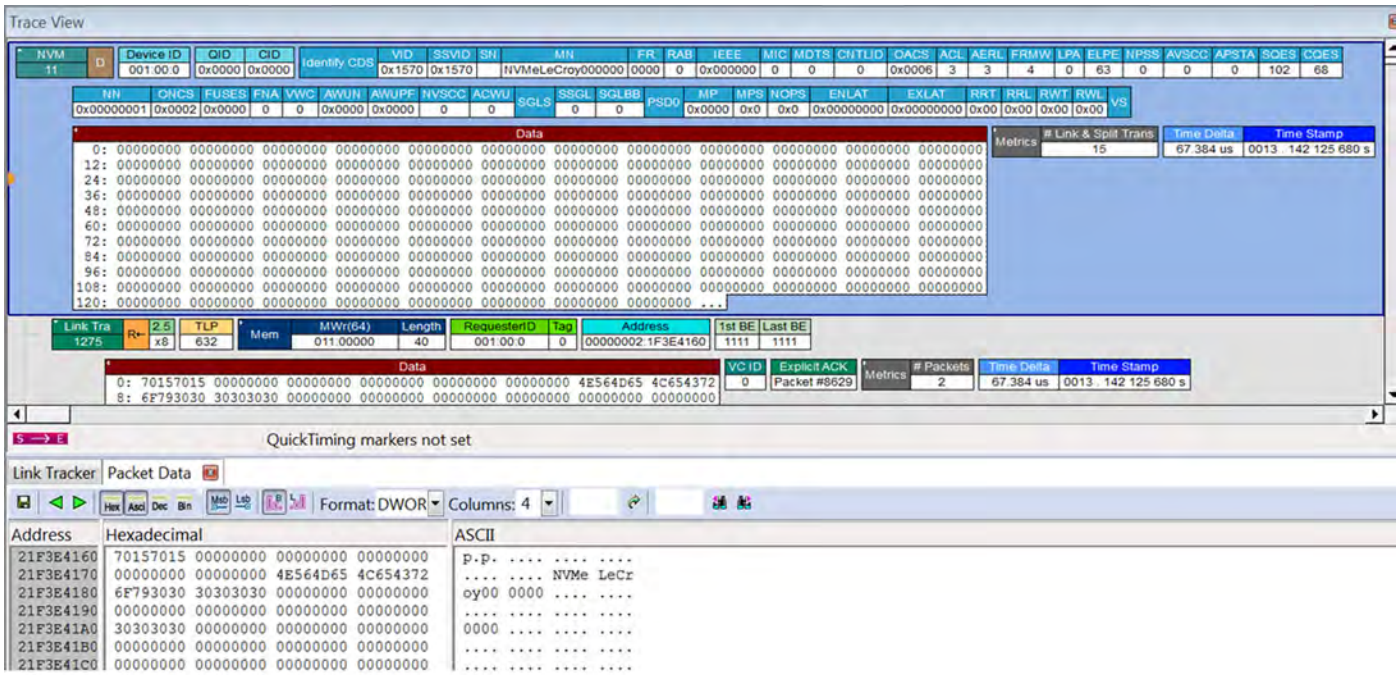


At the NVMe transaction level for identify command is shown below:



The data is shown according to NVMe specification. The portion of data that can be parsed into fields is parsed and drawn in named cells. The portion of data that cannot be parsed (i.e. 'vendor specific' portion is not parsed and is shown as a plain data).

In case you need to see this plain data (not parsed by named fields) the packet data view can be used. (as shown below):


Trace View
NVM
11
D
Device ID
001:00:0
QID
CID
0x0000
0x0000
Identify CDS
VID
SSVID
SN
MN
FR
RAB
IEEE
MIC
MDTS
CNTLID
OACS
ACL
AERL
FRMW
LPA
ELPE
NPSS
AVSCC
APSTA
SQES
CQES
0x1570
0x1570
NVMeLeCroy000000
0000
0
0x000000
0
0
0
0x0006
3
3
4
0
63
0
0
0
102
66
NN
ONCS
FUSES
FNA
VWC
AWUN
AWUPF
NVSCC
ACWU
SGLS
SSGL
SGLBB
PSDO
MP
MPS
NOPS
ENLAT
EXLAT
RRT
RRL
RWT
RWL
VS
0x00000001
0x0002
0x0000
0
0
0x0000
0x0000
0
0
0
0
0x0000
0x0
0x0
0x00000000
0x00000000
0x00
0x00
0x00
0x00
Data
0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
12: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
24: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
36: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
48: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
60: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
72: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
84: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
96: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
108: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
120: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ...
Metrics
Link & Split Trans
15
Time Delta
67.384 us
Time Stamp
0013 . 142 125 680 s
Link Tra
1275
R+
2.5
x8
TLP
632
Mem
MWr(64)
011.00000
Length
40
RequesterID
001:00:0
Tag
0
Address
00000002:1F3E4160
1st BE
1111
Last BE
1111
Data
0: 70157015 00000000 00000000 00000000 00000000 00000000 4E564D65 4C654372
8: 6F793030 30303030 00000000 00000000 00000000 00000000 00000000 00000000
VC ID
0
Explicit ACK
Packet #8629
Metrics
Packets
2
Time Delta
67.384 us
Time Stamp
0013 . 142 125 680 s
QuickTiming markers not set
Link Tracker
Packet Data
Hex
Asci
Dec
Bin
Msb
Lsb
Format: DWOR
Columns: 4
Address
Hexadecimal
ASCII
21F3E4160 70157015 00000000 00000000 00000000 p.p. ....
21F3E4170 00000000 00000000 4E564D65 4C654372 .... NVMe LeCr
21F3E4180 6F793030 30303030 00000000 00000000 oy00 0000 ....
21F3E4190 00000000 00000000 00000000 00000000 ....
21F3E41A0 30303030 00000000 00000000 00000000 0000 ....
21F3E41B0 00000000 00000000 00000000 00000000 ....
21F3E41C0 00000000 00000000 00000000 00000000 ....

9.11.5.3 NVMe: Trusted Computing Group Decode

Trusted Computing Group decodes are shown using the NVMe Command Level if they are present in the trace, as shown in Figure 9.50.

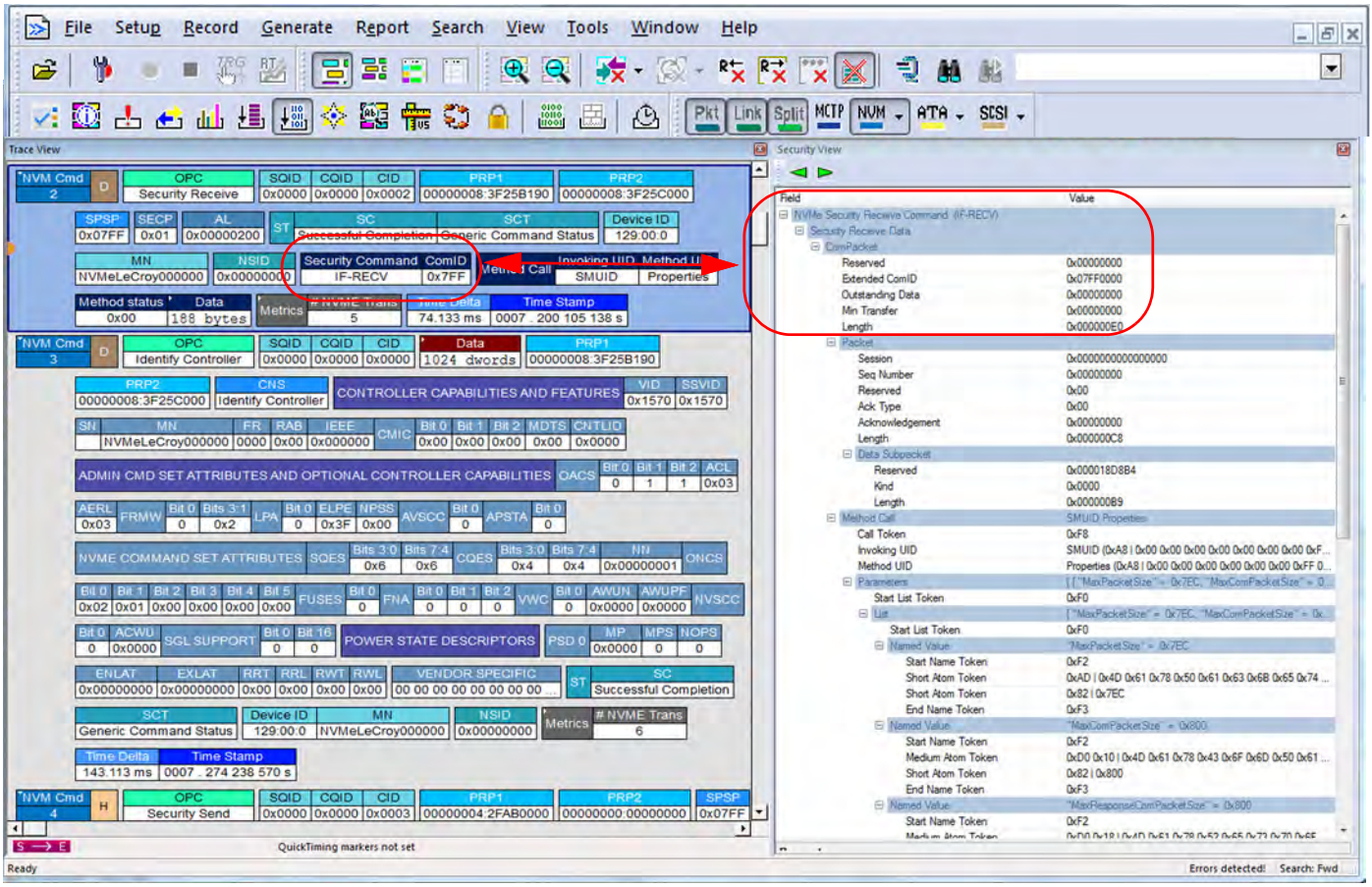


Figure 9.50: NVMe Command with TCG Details

9.11.5.4 The Opal Storage Specification

The Opal Storage Specification is a set of specifications for features of data storage devices (such as disk drives) that enhance their security. For example, it defines a way of encrypting the stored data so that an unauthorized person who gains possession of the device cannot see the data. That is, it is a specification for self-encrypting drives (SED).

The specification is published by the Trusted Computing Group Storage Workgroup.

The Opal SSC (Security Subsystem Class) is an implementation profile for Storage Devices built to:

- Protect the confidentiality of stored user data against unauthorized access once it leaves the owner's control (involving a power cycle and subsequent deauthentication).
- Enable interoperability between multiple SD vendors.

NVMe: TCG Opal Decoded

The PCIe Protocol Software can decode and display Opal TCG fields. See Figure 9.51.

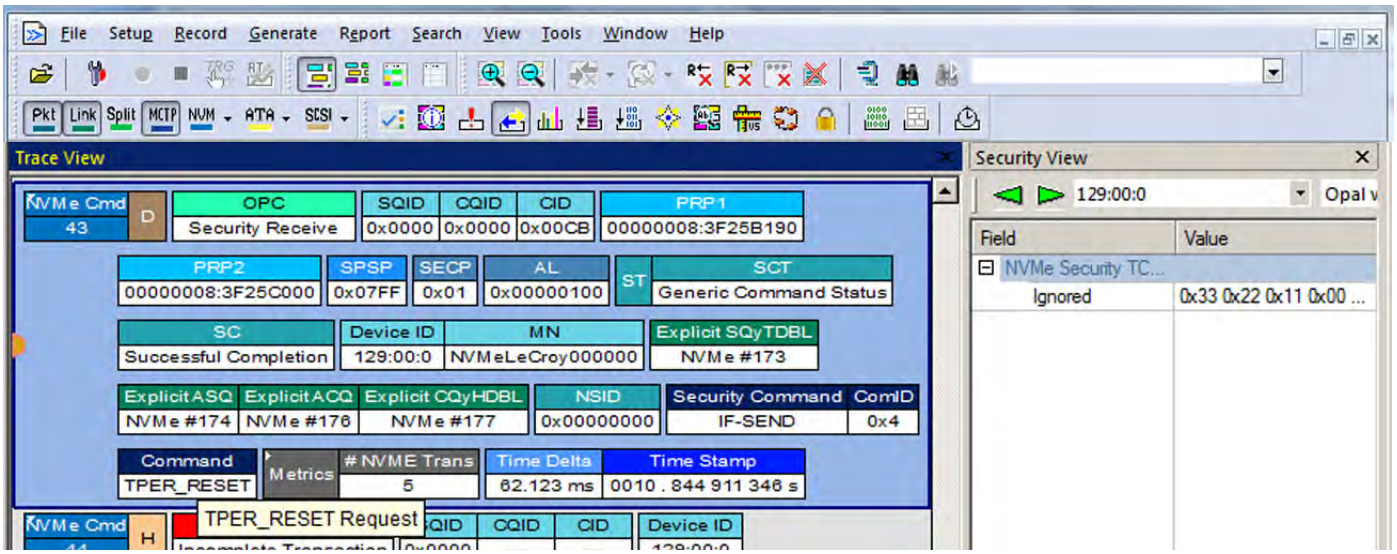


Figure 9.51: NVMe Trace: Opal TCG Security Fields Decoded

A more detailed view of the security field is shown in Figure 9.52 on page 564.

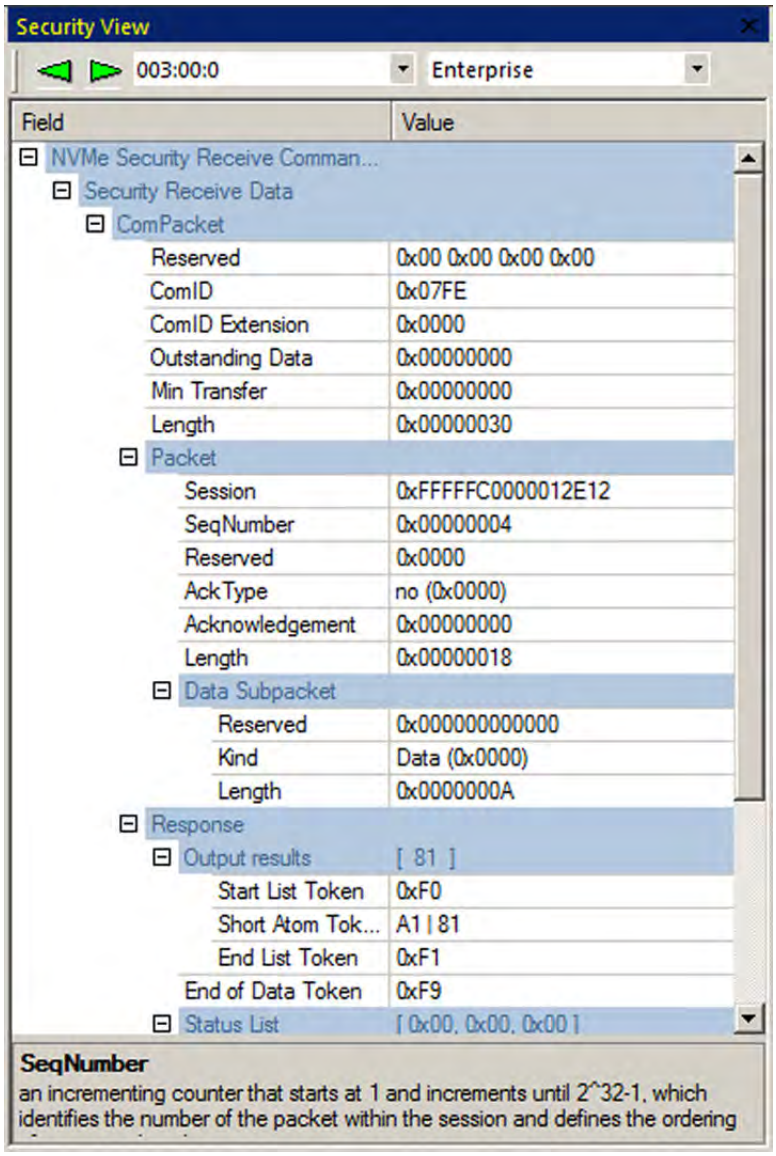


Figure 9.52: NVMe Trace: Opal TCG Security Fields Decoded in Detail

9.11.5.5 Opalite Version 0.1: Decoded

The PCIe Protocol Analysis software can decode the TCG transaction: Opalite Security Version 0.1 (as shown in Figure 9.53 and Figure 9.54 on page 566 below):

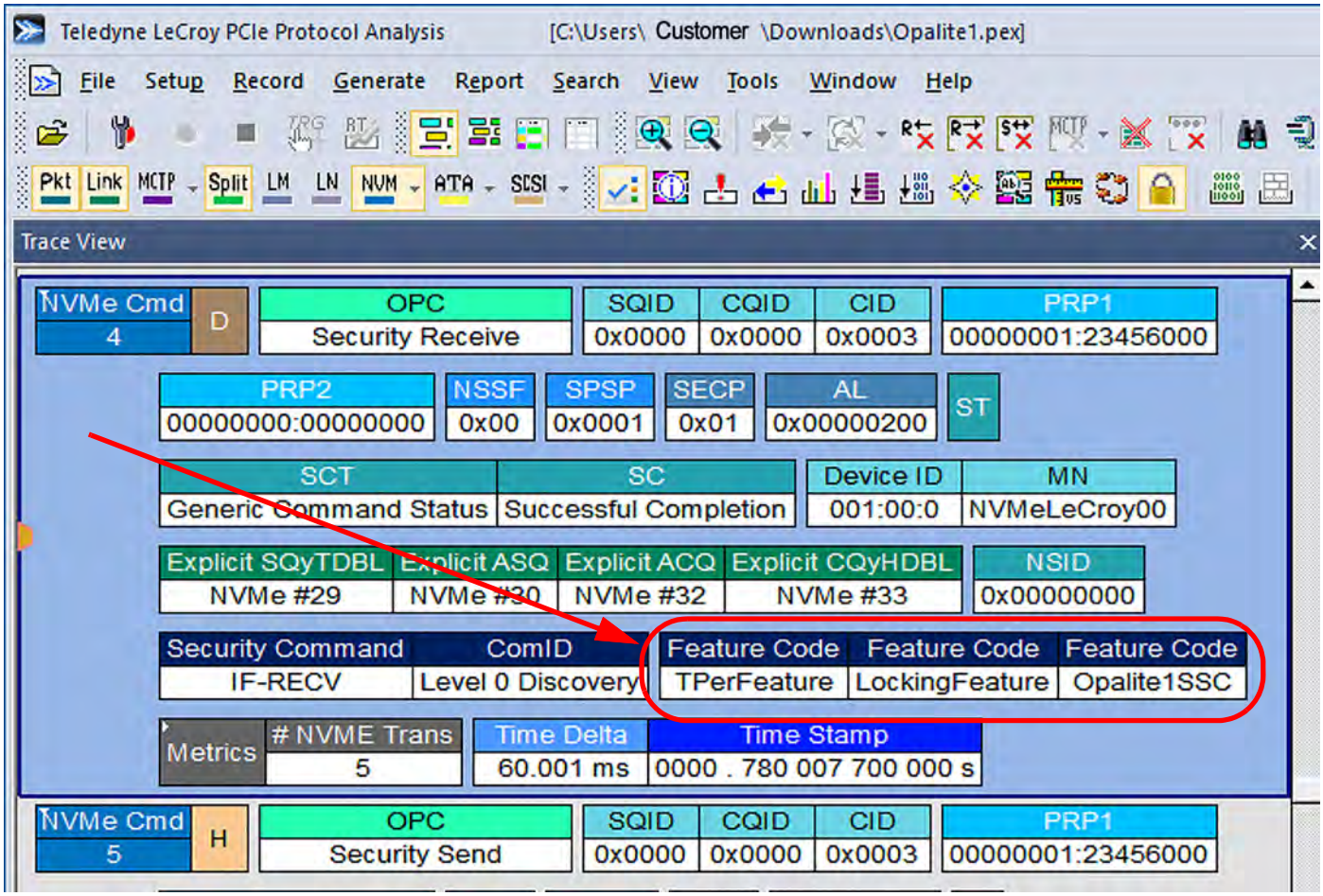


Figure 9.53: NVMe Trace: Opalite v0.1 TCG Security Fields Decoded

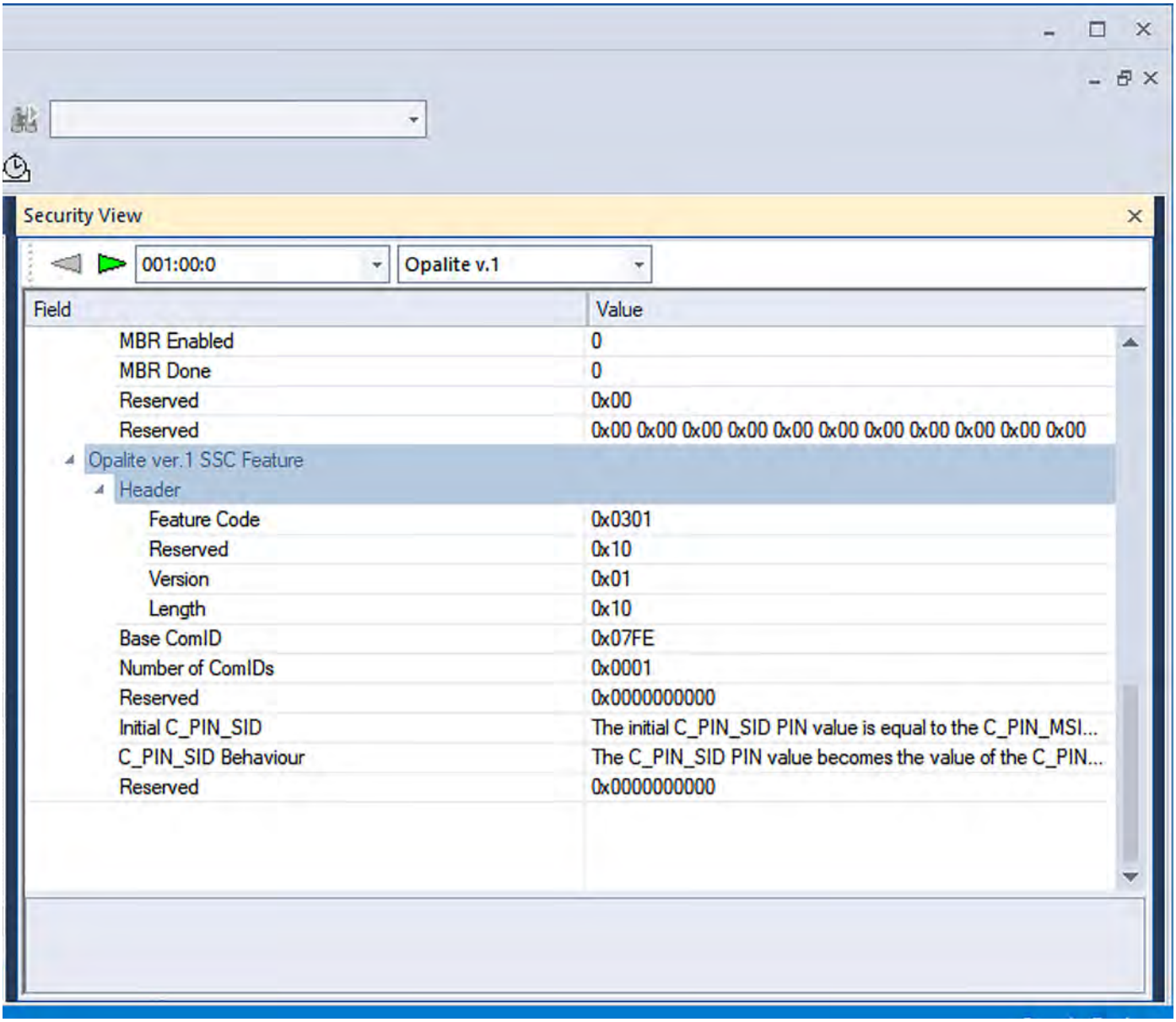


Figure 9.54: NVMe Trace: Opalite v0.1 TCG Security Fields Decoded -> Details

9.11.5.6 NVMe: Command IOPS and Doorbell Statistical Information

IOPS and Doorbell statistical information can be displayed from an NVMe Trace by selecting an NVMe Packet with a Read or Write Command and viewing the Metrics box. See Figure 9.55 and Figure 9.56 on page 567.

The Doorbell statistics include:

- SQdoorbell to CQdoorbell,
  (time from Submission Doorbell to Completion Doorbell)
- SQDoorbell to CQentry,
  (time from SQ doorbell to command completion)
- SQentry to CQentry,
  (time from submission command to command completion

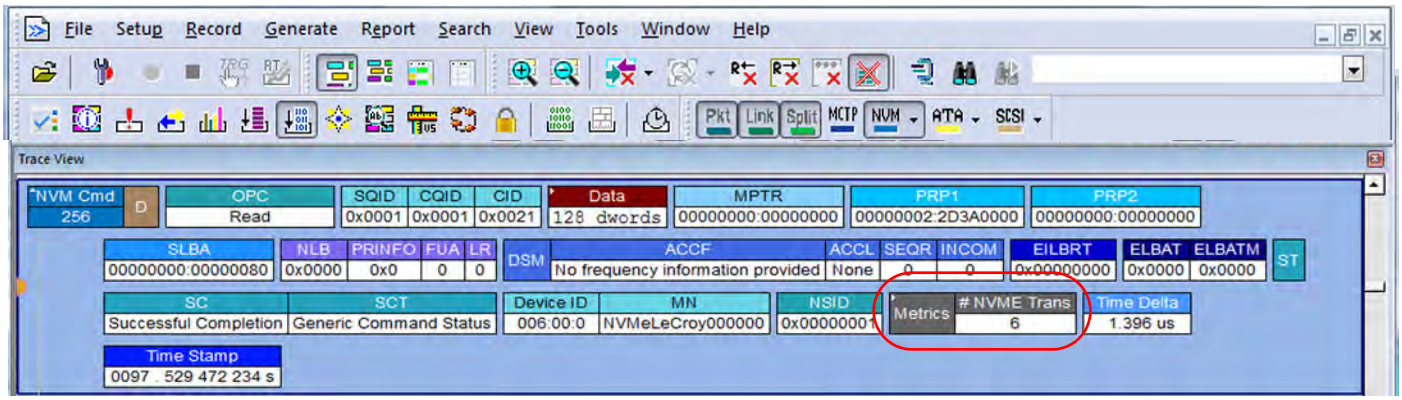


Figure 9.55: NVMe Read Command Packet with Metrics Box

Move the cursor over the Metrics box to display the information about the NVMe Command. See Figure 9.56.

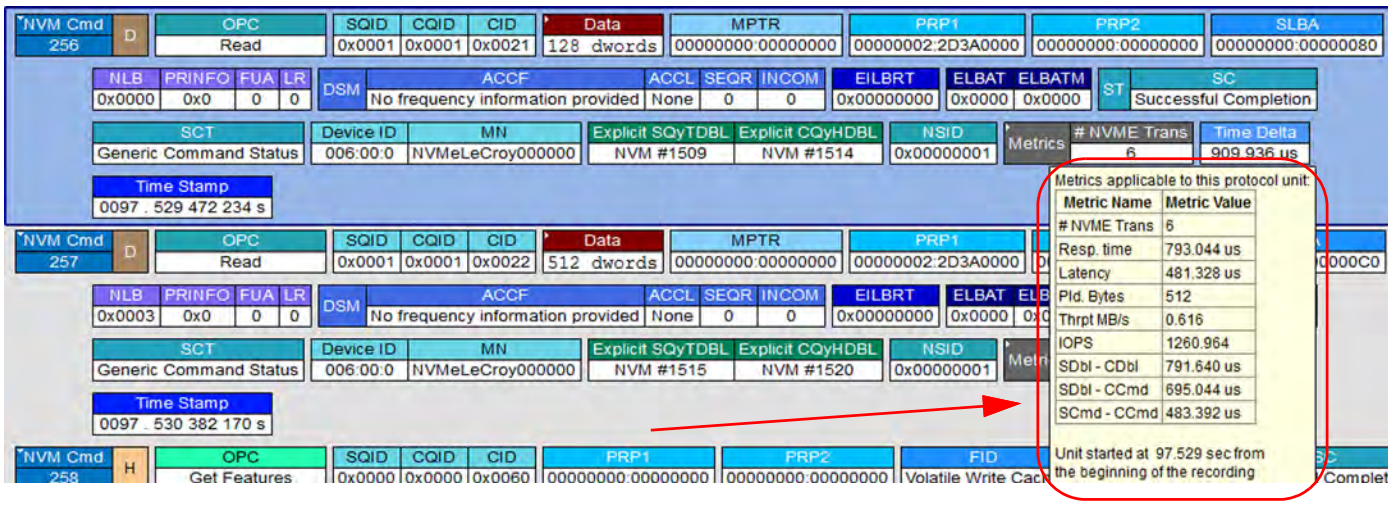


Figure 9.56: NVMe Read Command Packet with Metrics Displayed

If you click on the white arrow in the Metrics box, the information about the packet will be displayed in the Trace. See Figure 9.57.

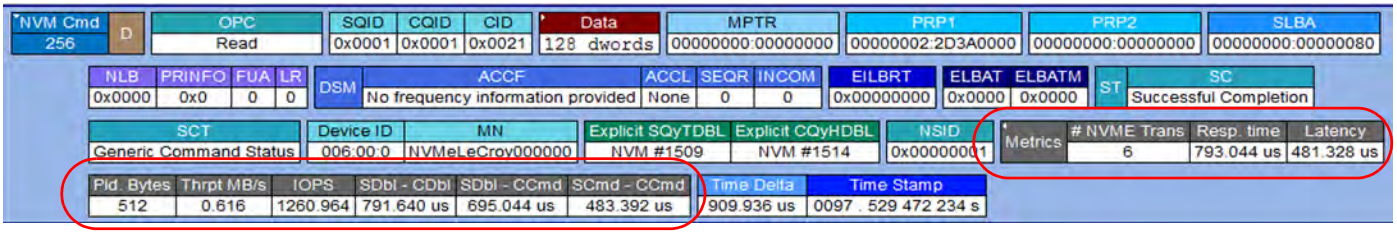


Figure 9.57: NVMe Read Command Packet with Metrics Displayed in Trace

The IOPS value is defined when you move the cursor over the IOPS box. See Figure 9.58.

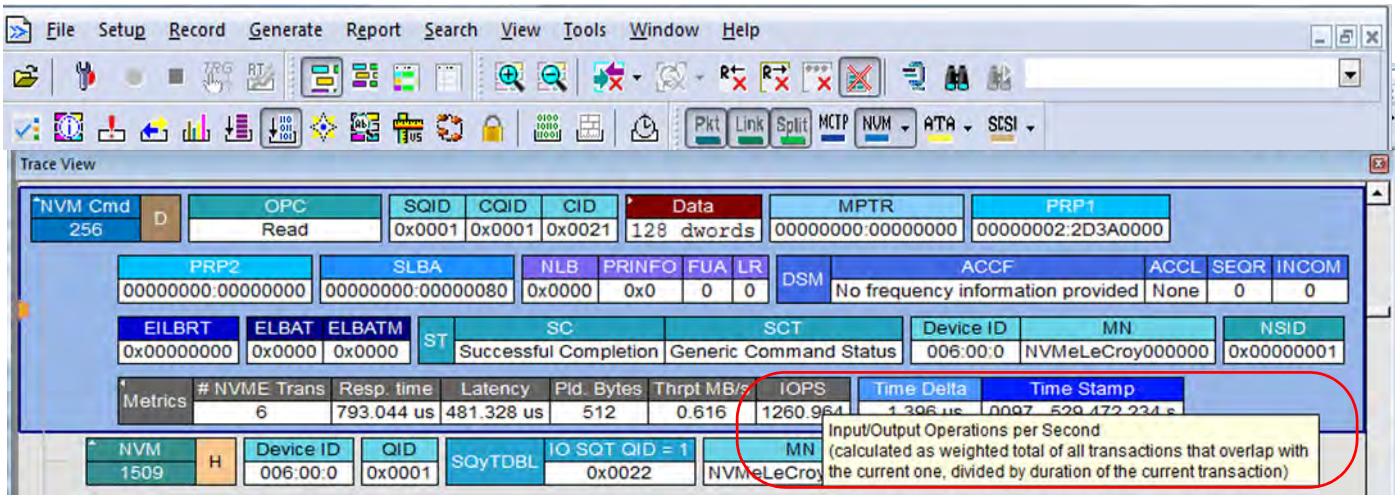


Figure 9.58: NVMe READ Command: IOPS Defined

The NMV Command IOPS can be viewed in Bus Utilization mode by selecting the Bus Utilization icon in the toolbar and selecting the Graph areas icon. See Figure 9.59.

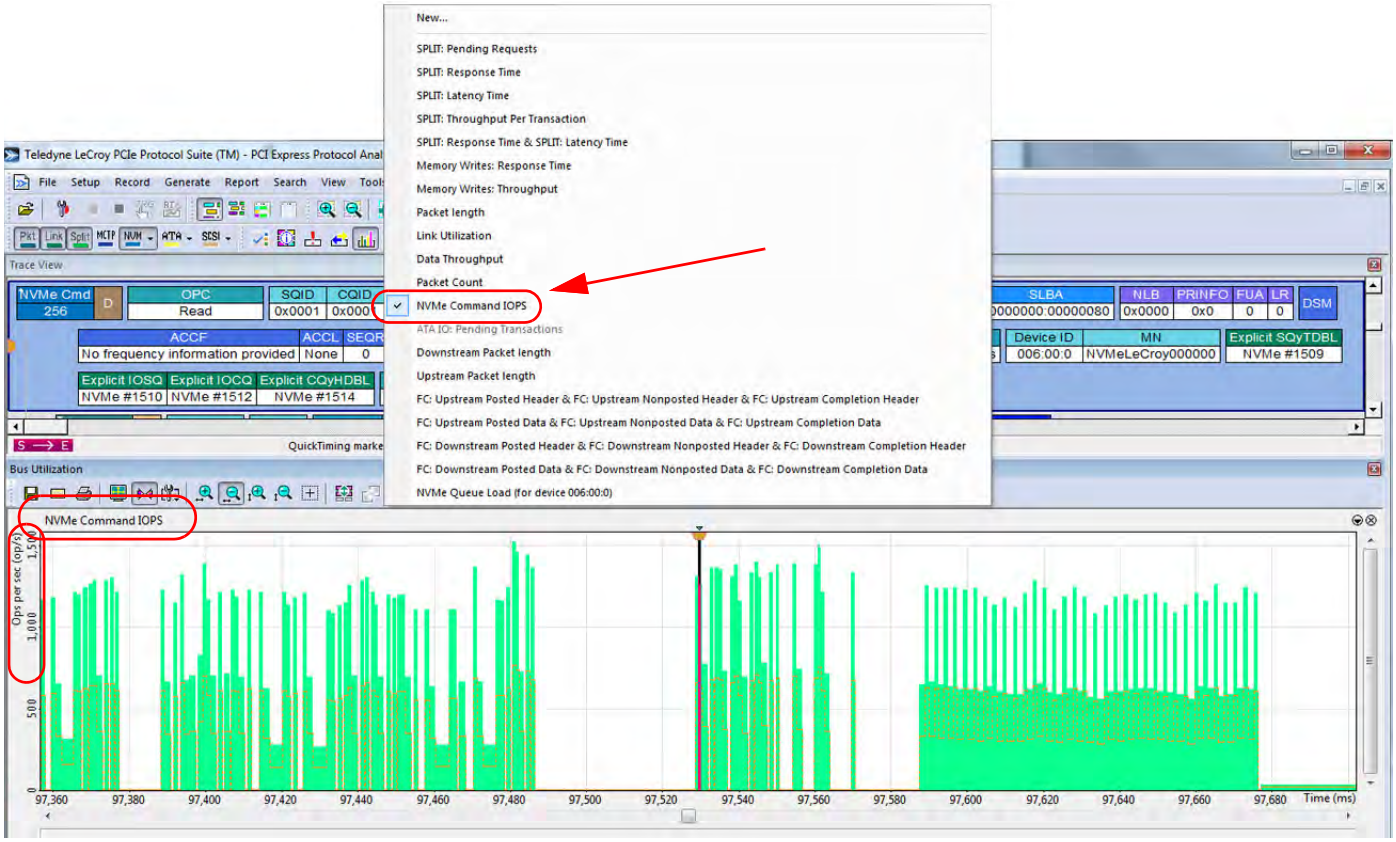


Figure 9.59: NVMe READ Command: Bus Utilization -- IOPS

NVMe Command IOPS is also displayed in the Spreadsheet and Detailed Views. See Figure 9.60.

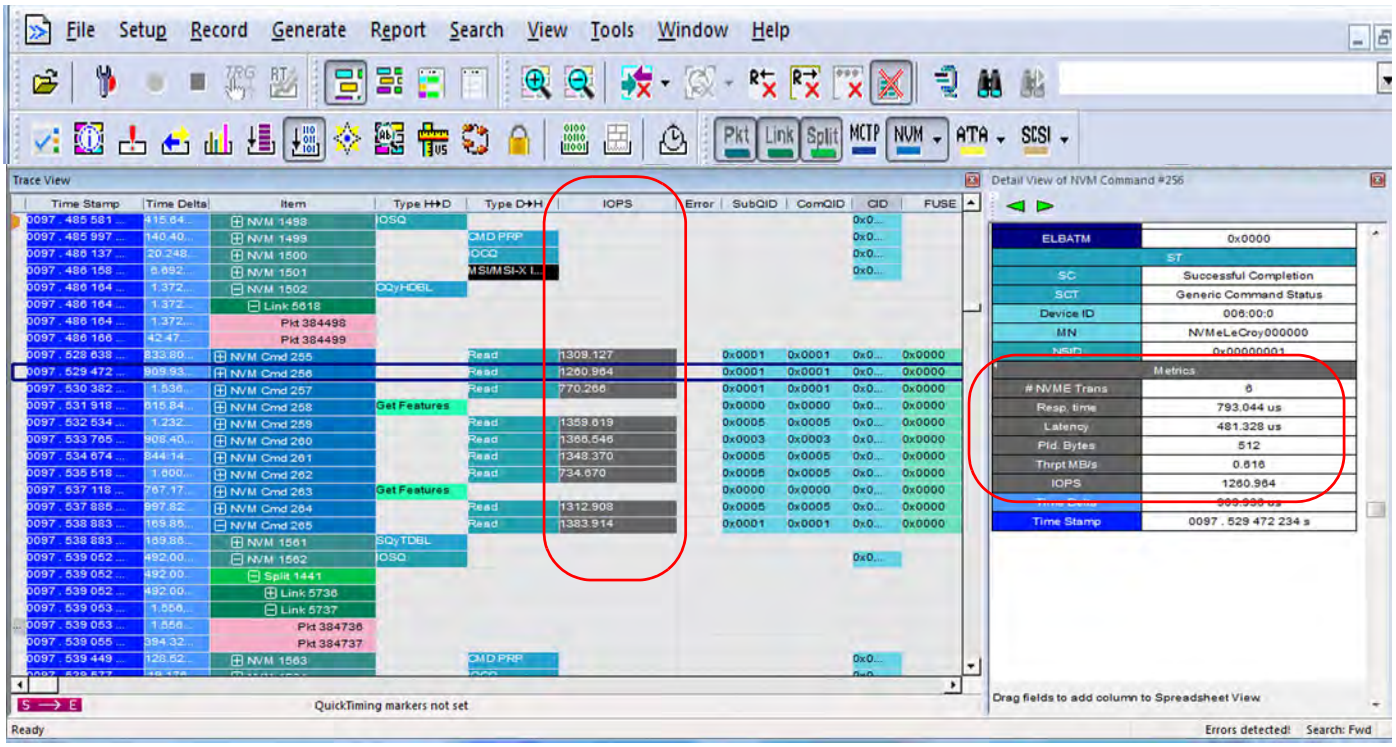


Figure 9.60: NVMe READ Command: IOPS Statistics

9.11.5.7 NVMe: Decode for Doorbells

Each type of doorbell's cell of an NVMe command is able to represent 1 of 4 states:

- Explicit (NVMe command contain concrete DBL). See Figure 9.61 on page 572.
- Implicit (Some doorbells implicitly complete previous commands. Such commands do not have a doorbell that can be associated one to one. This will be indicated in the trace.)
- Missing (NVMe cmd Is Incomplete, and DBL missing)
- Filtered (DBL is filtered out in Recording rules)

Tooltips:

- For SQyTDBL: Command was explicitly/implicitly initiated by SQyTDBL in NVMe #number (See Figure 9.61 on page 572)
- For CQyHDBL: Command was explicitly/implicitly finished by CQyHDBL in NVMe #number
- For Missing Doorbells: Doorbell is missing
- For Filtered: Doorbells are filtered out

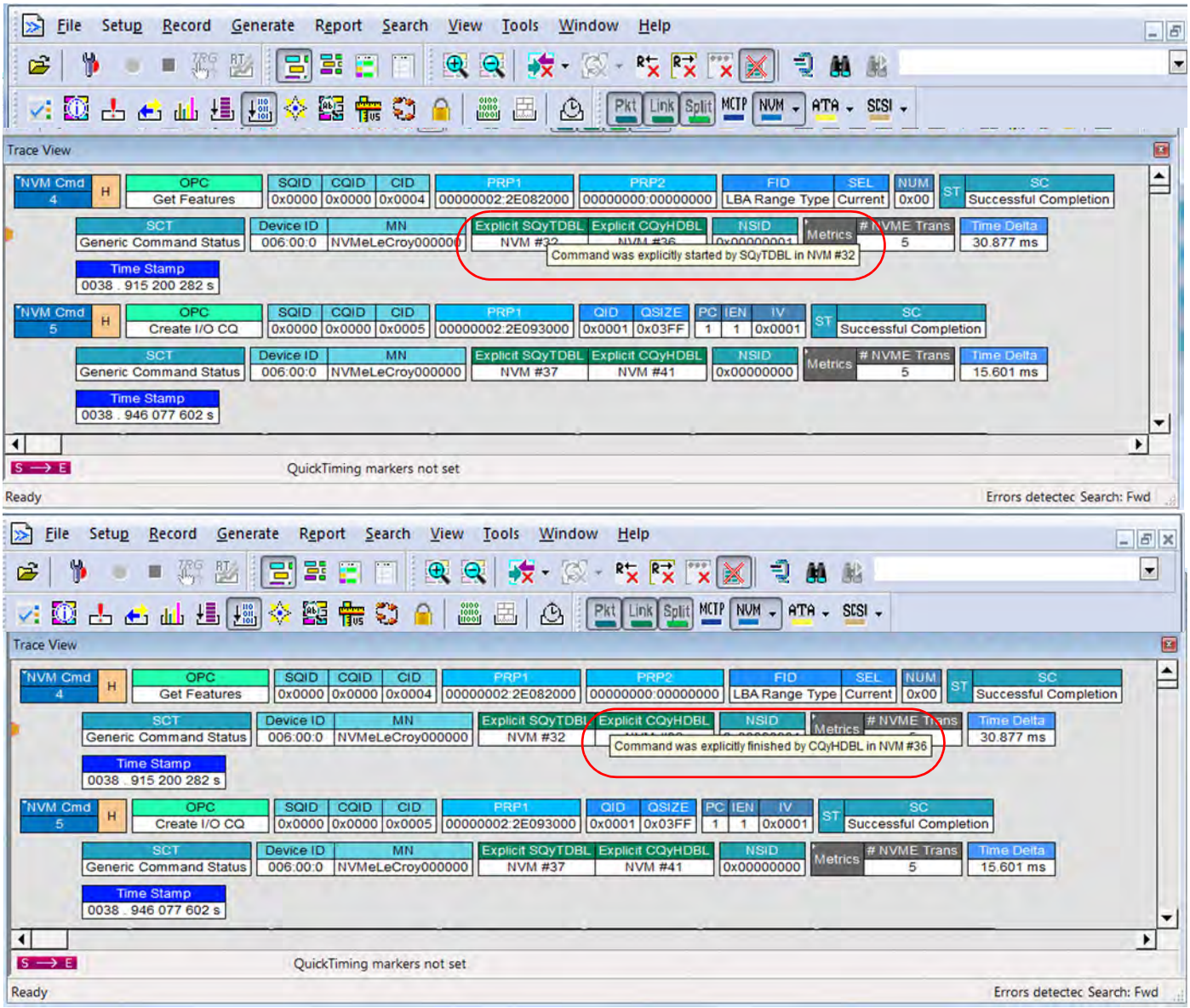


Figure 9.61: NVMe Decoding: Example of Explicit Doorbell in Trace with Tool Tips

9.11.5.8 Time Stamp from Implicit Start

The time stamp for an NVMe command can either be referenced from the recorded trace start time (see Figure 9.62) or from the implicit start of the command (see Figure 9.63). If you right click on the Time Stamp, the Time Stamp Context Menu will pop up. This allows you to Check or Uncheck the "Calculate Timestamp from implicit start if present" box.

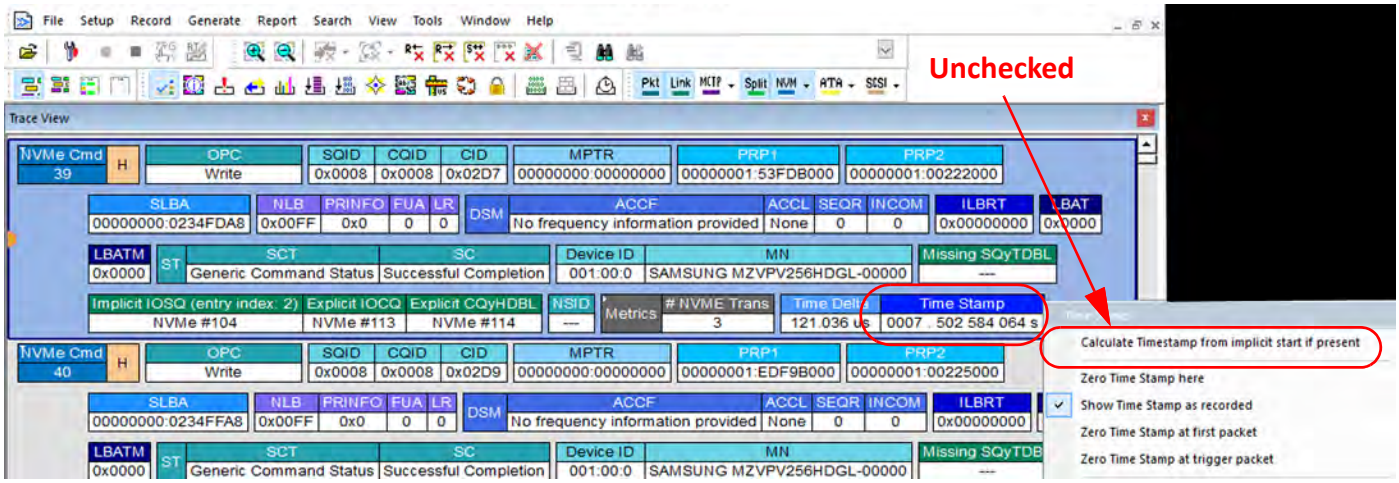


Figure 9.62: Timestamp Referenced from Start of Trace = 7.502584064 seconds

If you select "Calculate Timestamp from implicit start if present" you'll get the following results. In this case, the Implicit Start was earlier in the trace than the NVMe command so the timestamp for the NVMe command is earlier (see Figure 9.63).

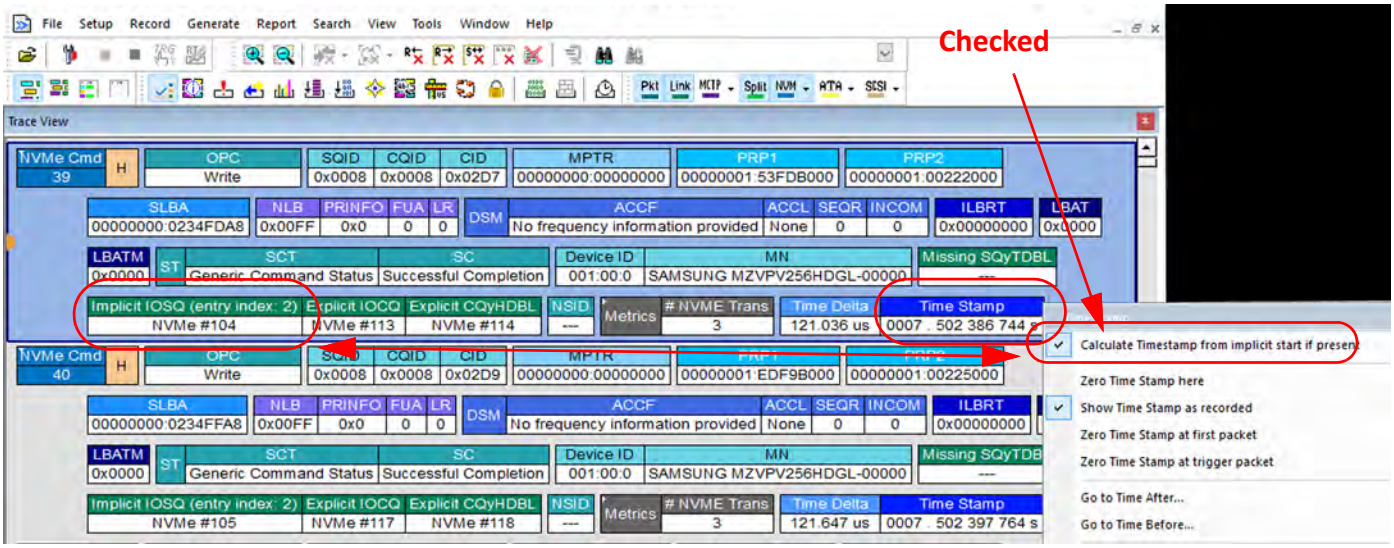


Figure 9.63: Timestamp Referenced from the Implicit Start = 7.502386744 seconds

9.11.5.9 NVMe Commands and Transactions: Data Throughput

Data Throughput is defined as the Payload divided by response time, expressed in MB per second (MB = 1024*1024 bytes) for both Commands and Transactions. See Figure 9.64 and Figure 9.65.

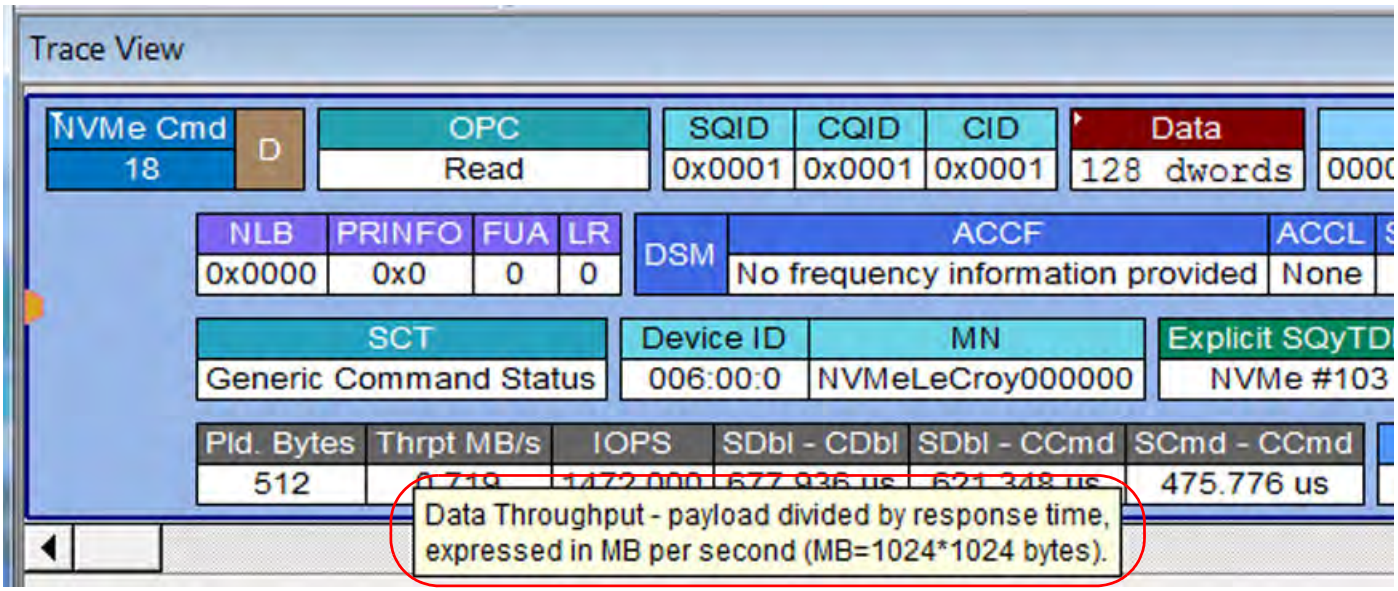


Figure 9.64: NVMe Command: Data Throughput

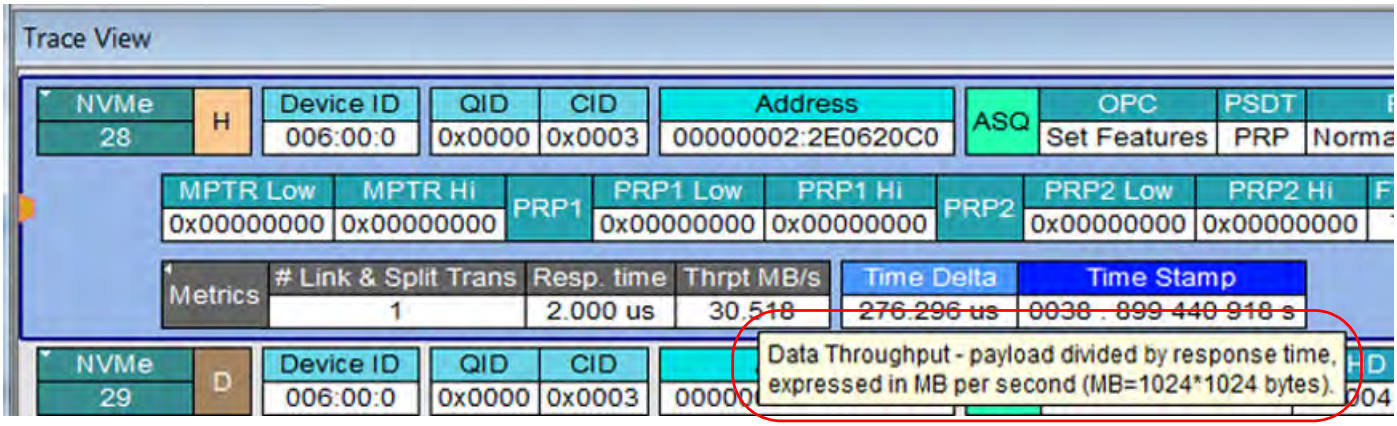


Figure 9.65: NVMe Transaction: Data Throughput

9.11.5.10 NVMe Decoding vs. NVMe Specification

After decoding an NVMe Trace you can view both the NVME data traffic in the Trace View as well as formatted per the NVMe Specification. The NVMe Specification View is brought up by selecting the NVMe Specification icon  in the tool bar (see Figure 9.66).

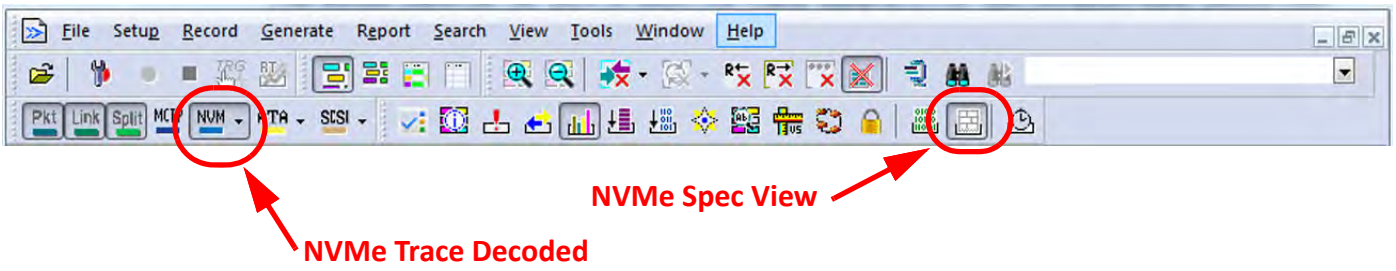


Figure 9.66: PCIe Protocol Analysis Toolbar -> NVMe Specification View

The NVMe data can be seen in both the Trace View and the Specification view below (see Figure 9.67 and Figure 9.68 on page 576).

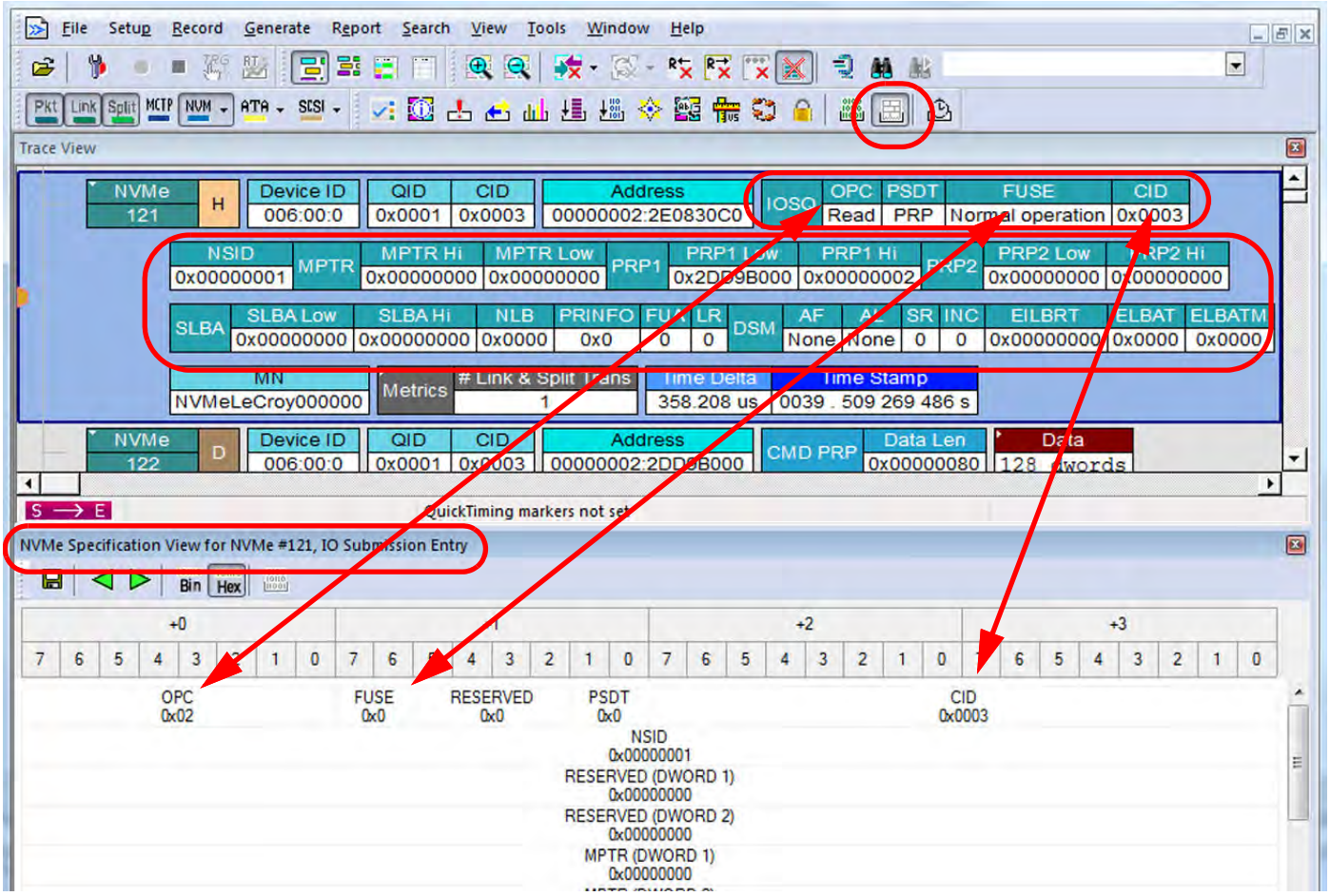


Figure 9.67: Decoding NVMe Trace -> Trace View vs. Spec View (Part 1)

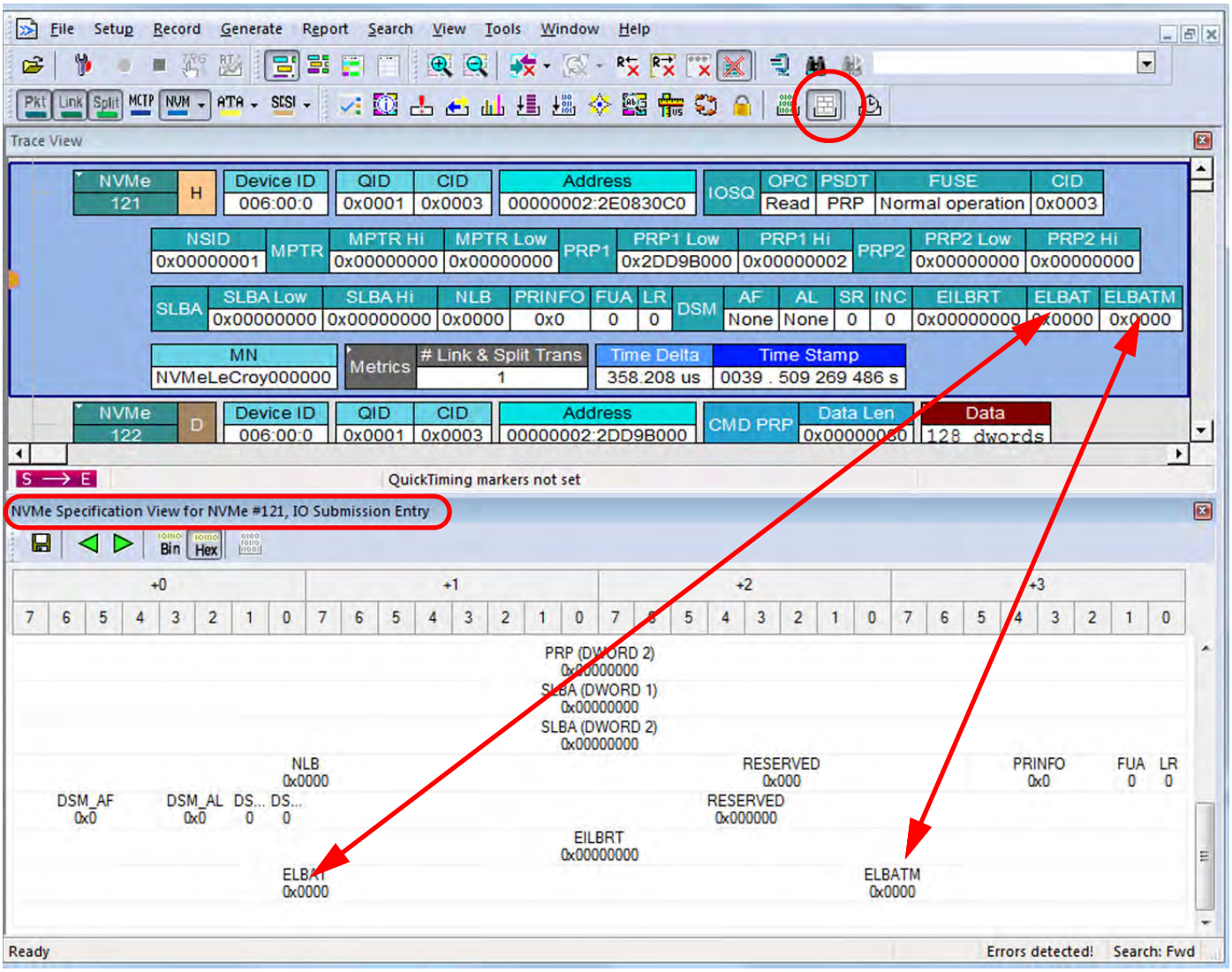


Figure 9.68: Decoding NVMe Trace -> Trace View vs. Spec View (Part 2)

If you move the cursor over a specific data block a Tool Tip will pop up with more information about the data block. See Figure 9.69

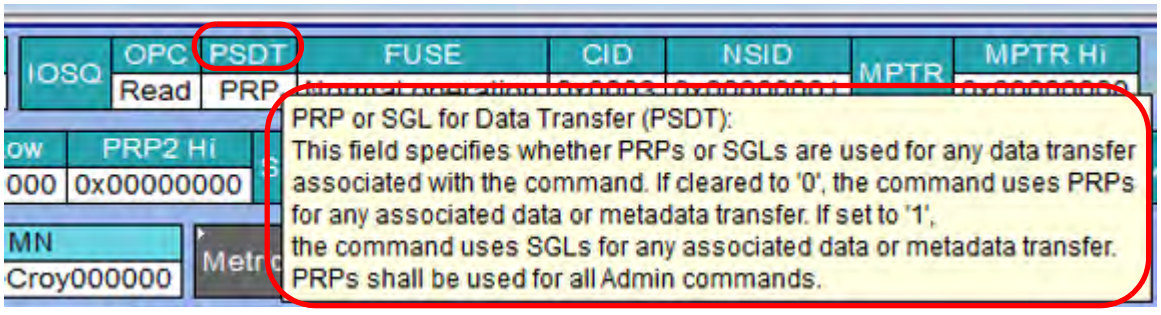


Figure 9.69: NVMe Specification: Trace View Tool Tip

Similar Tool Tips are available in the NVMe Specification View. See Figure 9.70 on page 577.

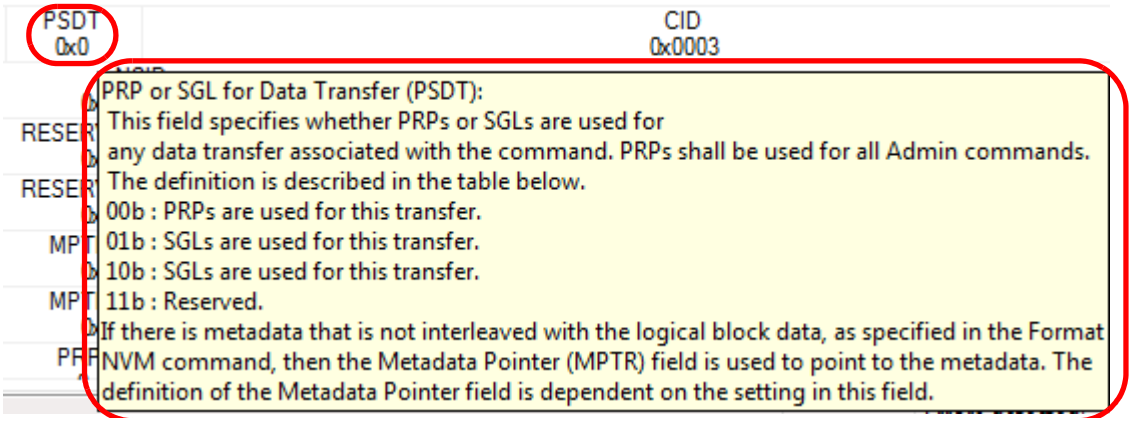


Figure 9.70: NVMe Specification View: Tool Tip

The NVMe Specification View is also available from the Main Toolbar under Report -> NVMe Specification. See Figure 9.71.

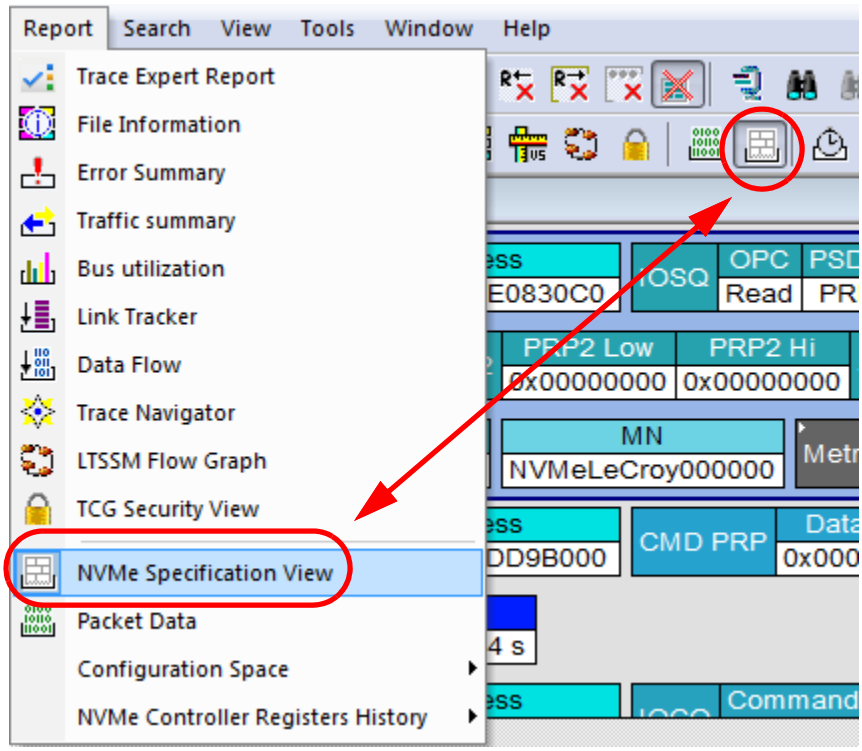


Figure 9.71: Report: NVMe Specification

9.11.5.11 NVMe Controller Register

To view the NVMe Controller Registers perform the following steps:

1. Load a trace with NVMe data traffic.
2. Select Packet, Link, Split, NVMe, Hide Unrelated Traffic and View -> Wrap to produce the following display (see Figure 9.72).

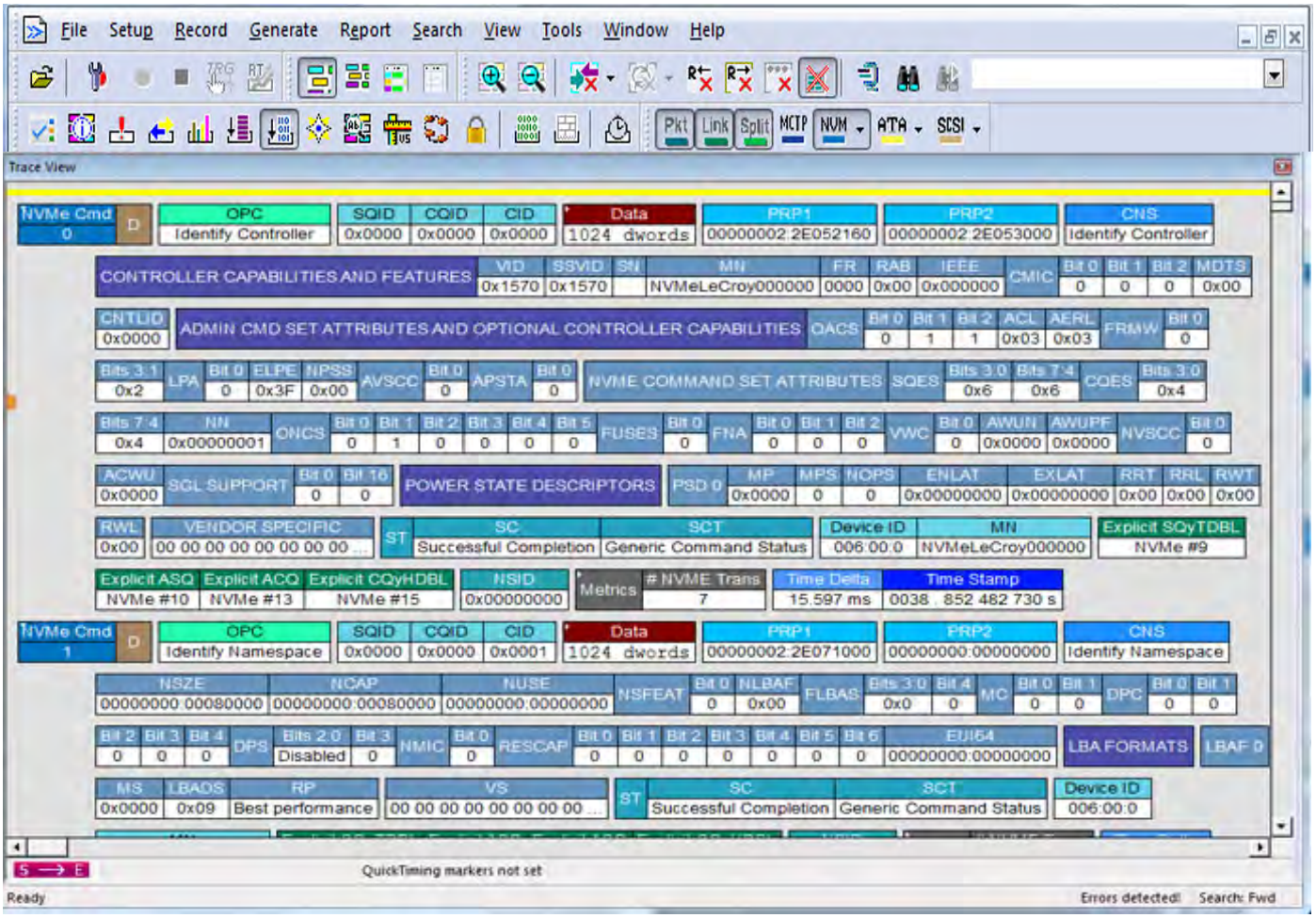


Figure 9.72: NVMe Trace Loaded

3. Select Reports -> NVMe Controller Registers History (see Figure 9.73 on page 579).

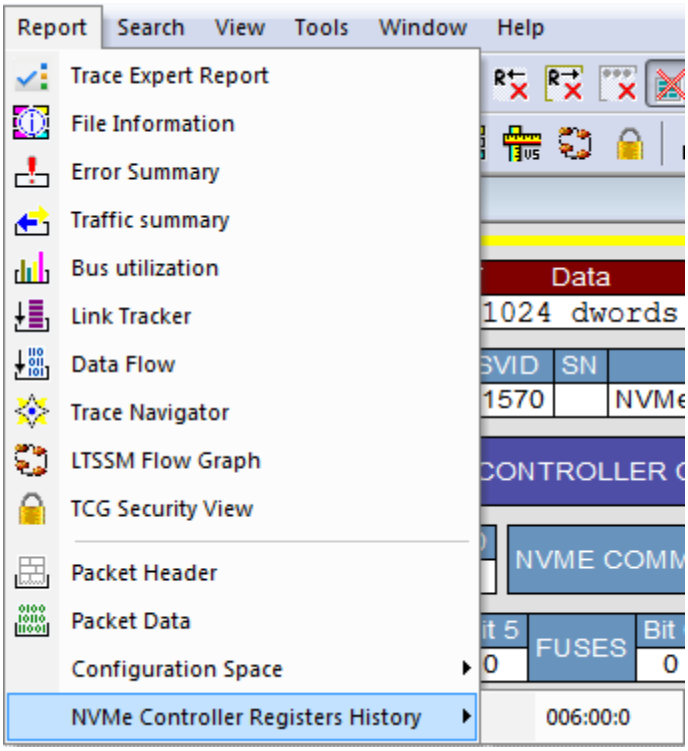


Figure 9.73: Reports -> NVMe Controller Registers History

4. Select the time shown (006:00:0) and the following display will pop up. See Figure 9.74 on page 580.

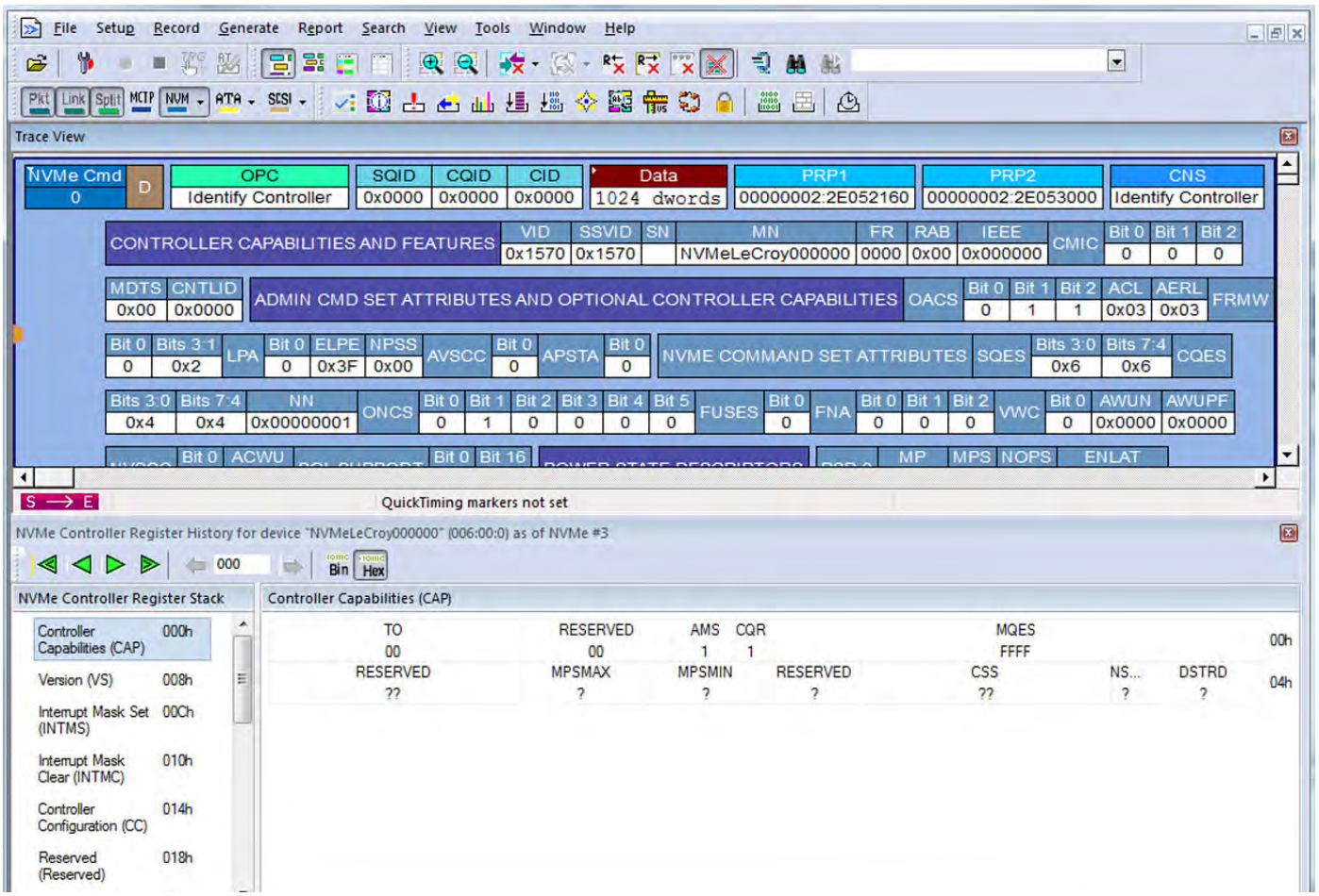


Figure 9.74: Reports -> NVMe Controller Registers History Displayed

5. If you zoom in on the green arrows, you can:
   a. Go to the First NVMe Controller Register
   b. Go to the Previous NVMe Controller Register
   c. Go to the Next NVMe Controller Register
   d. Go to the Last NVMe Controller Register

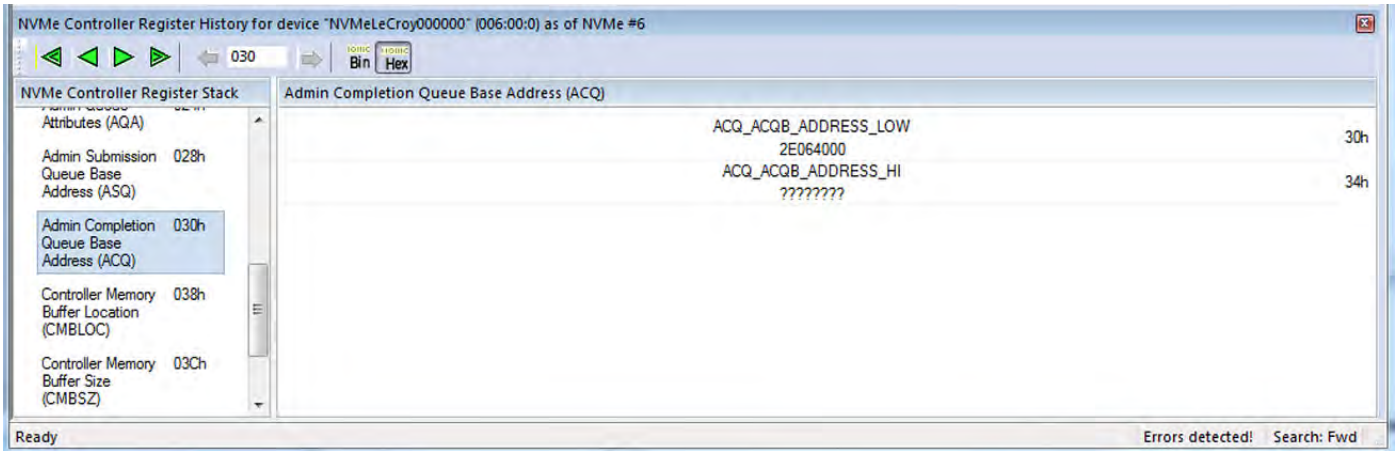


Figure 9.75: NVMe Controller Registers: Admin Completion (ACQ) 30h Displayed

6. As an example you could click on the Next NVMe arrow and the Admin Queue Attributes would be displayed (see Figure 9.76).

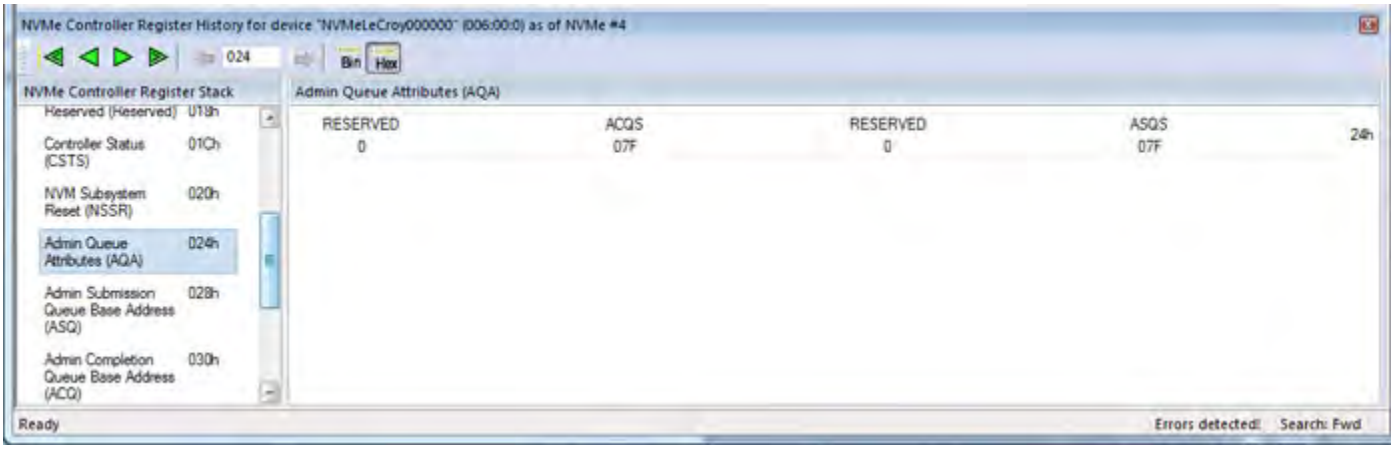


Figure 9.76: NVMe Controller Registers: Admin Queue Attributes (AQA) 024h Displayed

7. You can continue clicking the Green arrow to see more of the NVMe Controller Register Stack. See Figure 9.77 on page 581.

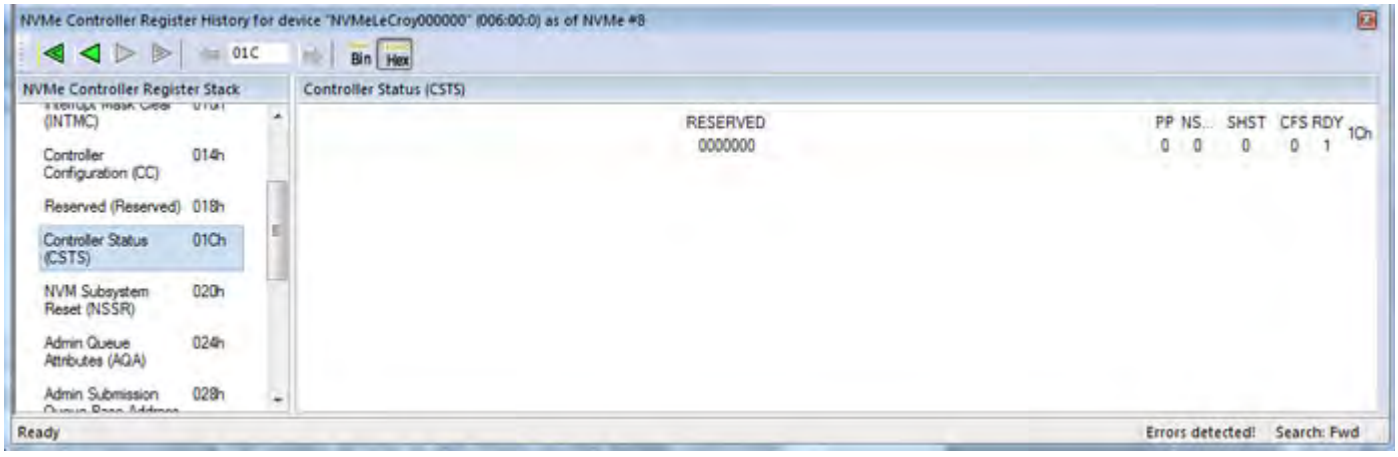


Figure 9.77: NVMe Controller Registers: Controller Status (CSTS) 01Ch

9.11.5.12 Decoding Multiple NVMe Commands for a Single MemRead or MemWrite

In some cases, a controller may fetch multiple NVMe commands in a single Memory Read or Write. At the NVMe Command level, the Analyzer software will decode this and show that there is an Implicit I/O Submission Queue Entry for that command and refer to the NVMe Transaction where the command was fetched from the Submission Queue. See Figure 9.78. NVMe transactions that are part of the current NVMe command are labeled as Explicit. In this case, the I/O Completion Queue contains NVMe transaction 311924 and it's labeled as an Explicit entry (also shown in Figure 9.78).

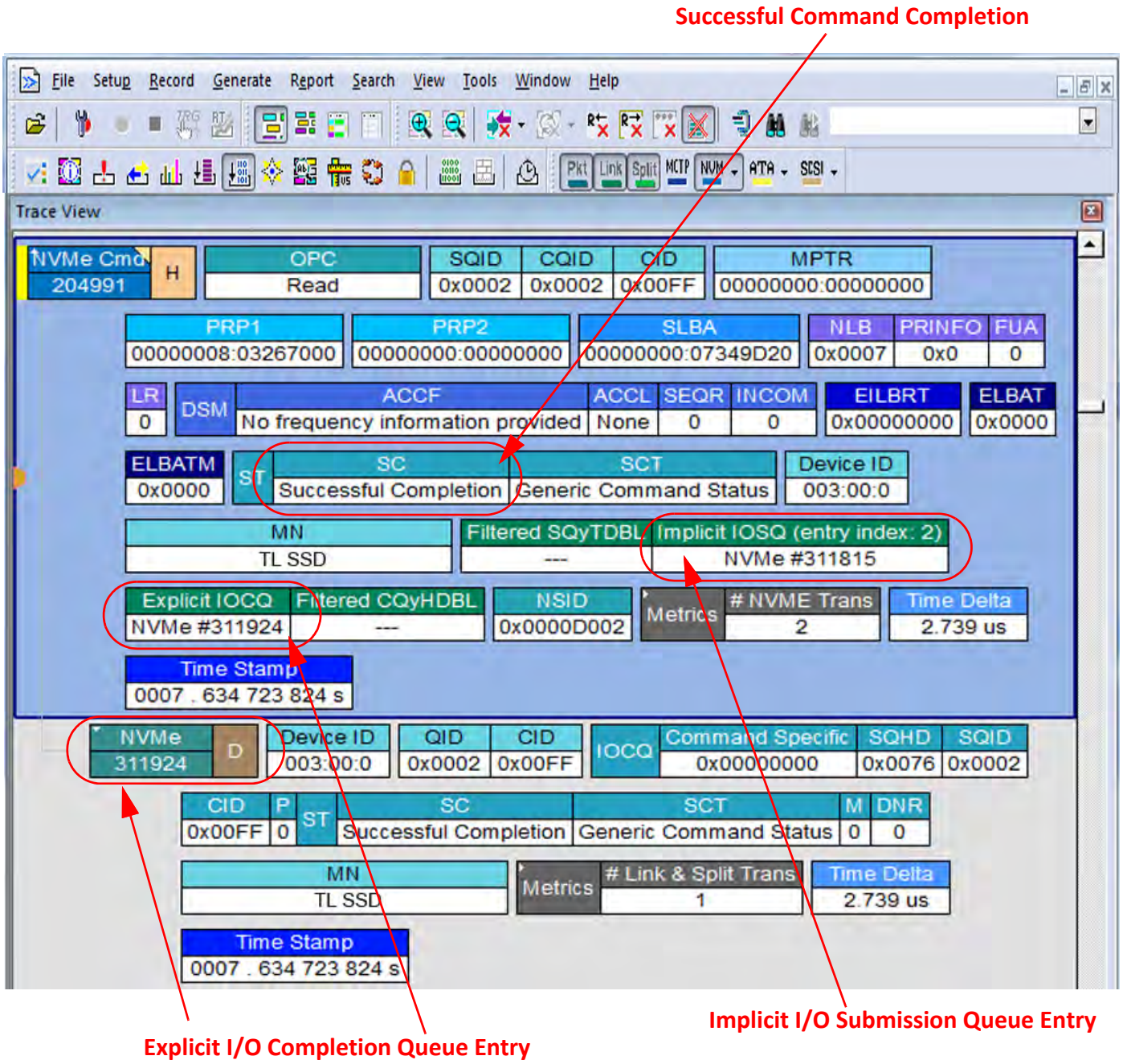


Figure 9.78: Implicit I/O Submission Queue Entry (IOSQ) and Explicit I/O Completion Queue Entry (IOCQ)

NVMe Transactions Decoded for NVMe Read Command:

- Implicit IOSQ: NVMe Transaction #311815 (entry index: 2)
- Explicit IOCQ: NVMe Transaction #311924 (part of this NVMe command: 204991)

The Implicit NVMe transaction (referenced by the Implicit label vs. Explicit label) can be found by right clicking on the NVMe transaction number in the trace display (see Figure 9.79).

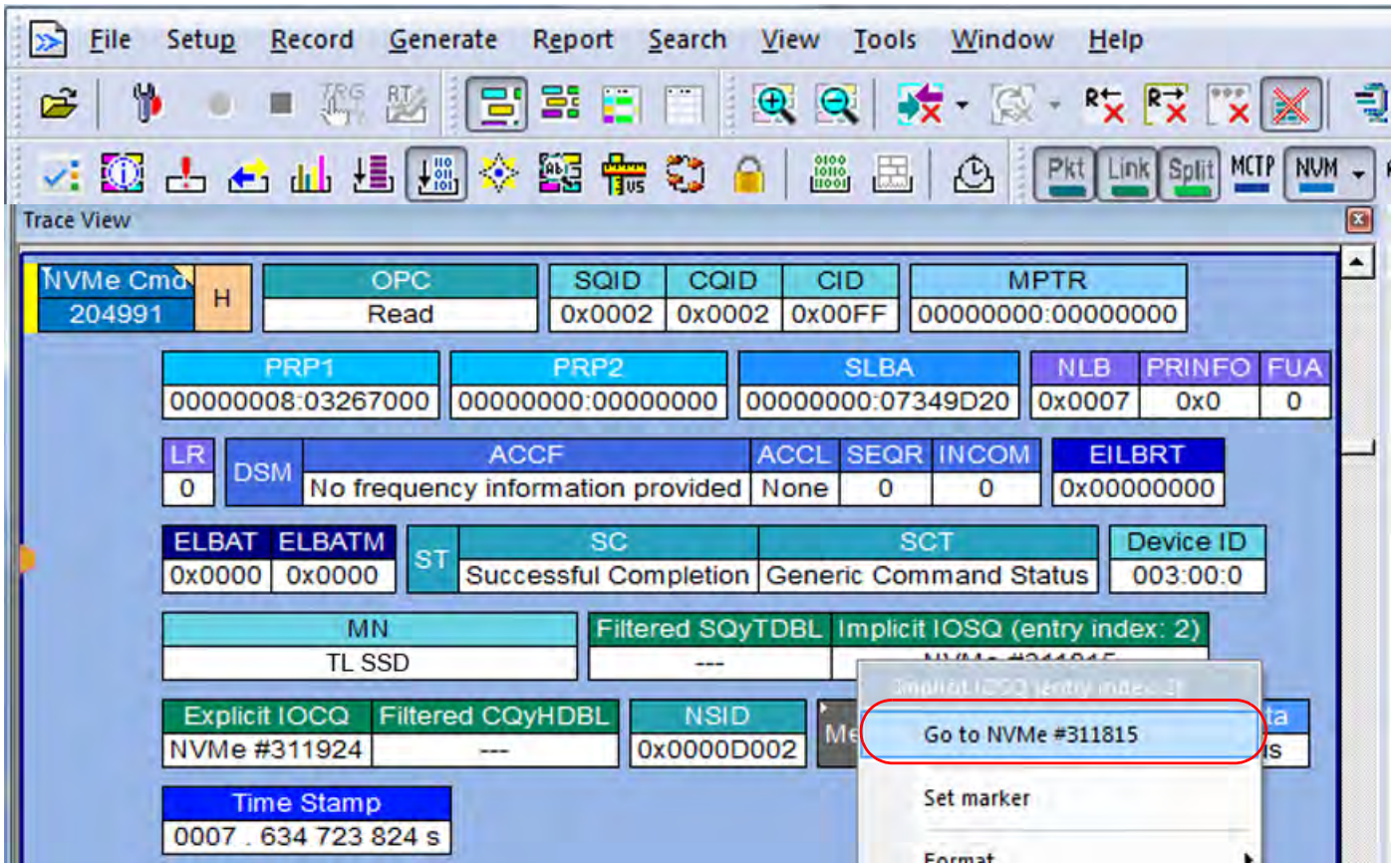


Figure 9.79: Implicit IOSQ Command

The display will be updated to that NVMe Transaction Number (and show the NVMe Command that it's a part of. In this case the Implicit NVMe Transaction (311815) is part of NVMe Command Number 204918. See Figure 9.80 on page 584)

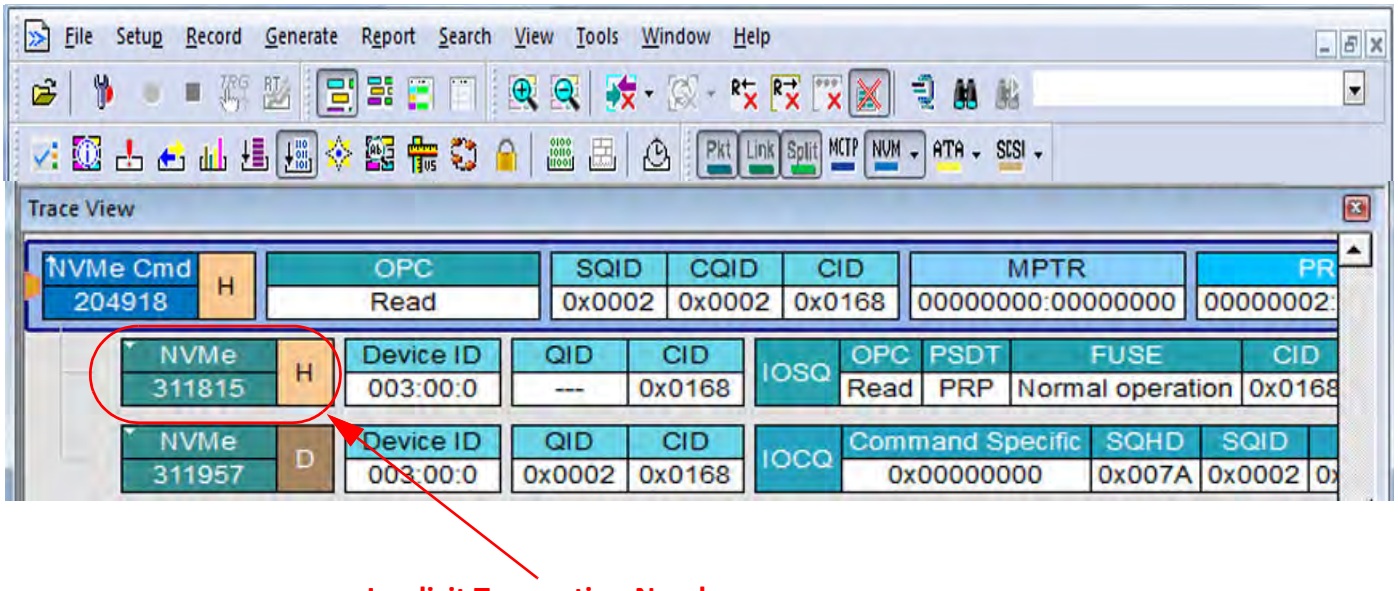


Figure 9.80: NVMe Transaction #318815: Part of NVMe Command 204918

If you expand the NVMe Transaction 311815 down to the Packet level (312224), you'll see two commands (32 DWORDS). See Figure 9.81.

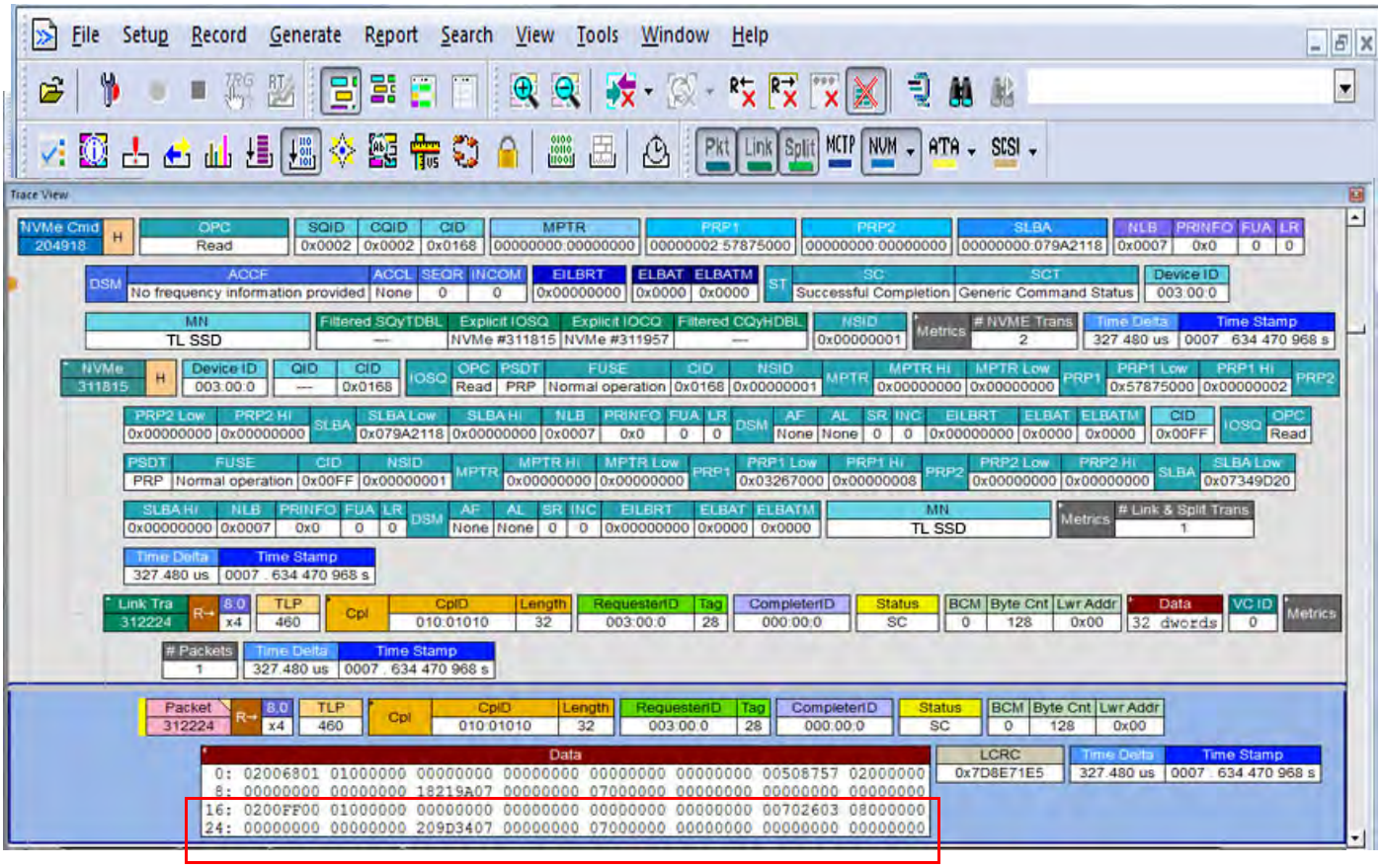


Figure 9.81: Implicit NVMe Transaction Decoded to Packet Level with Two Commands

9.11.6 NVMe 1.2 Specification Decoding

The PCIe Protocol Analysis has several enhancements to decode the NVMe 1.2 Specification (as seen in the following figures: Figure 9.82, Figure 9.83, Figure 9.84 on page 587 and Figure 9.85 on page 588).

- Name Space Management
- Replay Protected Memory Blocks
- SSD Dialog Shared NameSpace
- SSD Dialog Version and CMB Configurations

The figure below (Figure 9.82) shows the support added for decoding of the namespace management commands in NVMe data traffic.

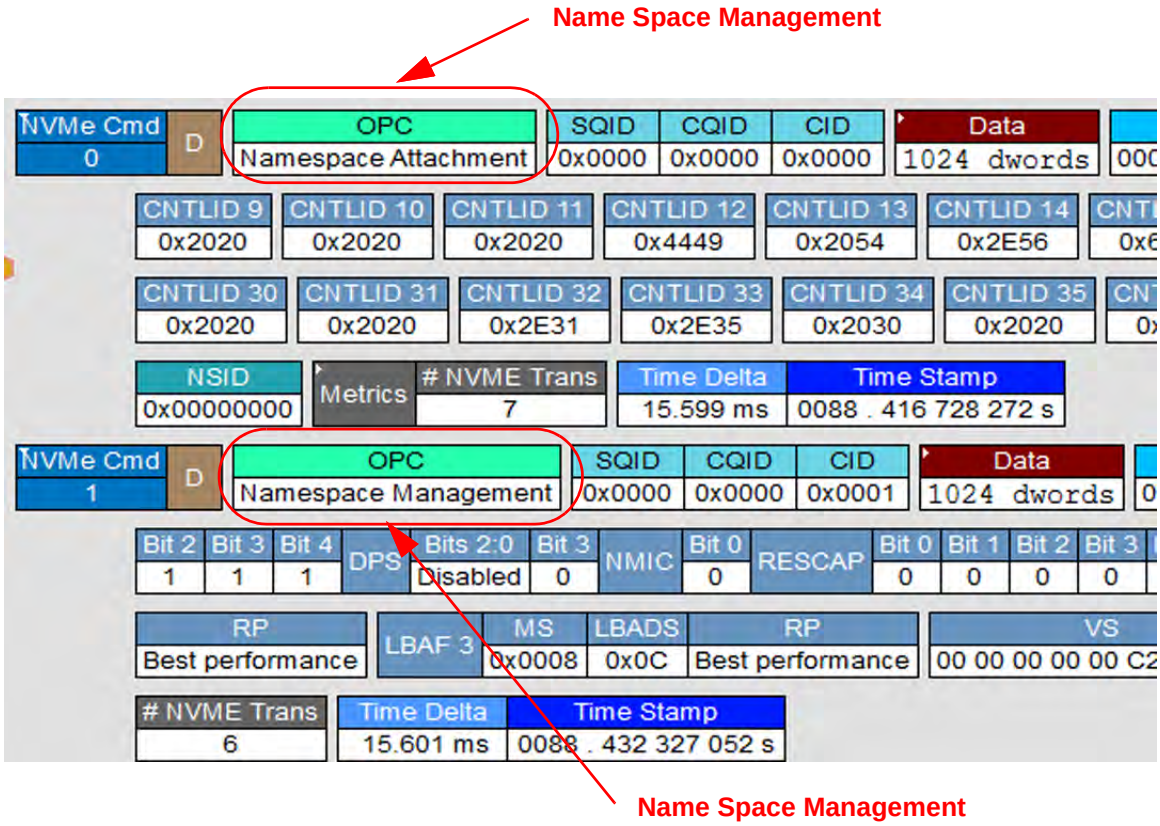


Figure 9.82: NVMe 1.2 Specification: Name Space Management

The Namespace Management command is used to create a namespace or delete a namespace. The Namespace Attachment command is used to attach and detach controllers from a namespace. Namespace management is intended for use during manufacturing or by a system administrator.

When a namespace is detached from a controller or deleted it becomes an inactive namespace on that controller. Previously submitted but uncompleted or subsequently submitted commands to the affected namespace are handled by the controller as if they were issued to an inactive namespace.

The figure below (Figure 9.83) shows the support added for the Replay Protected Memory Block (RPMB) command in NVMe data traffic.

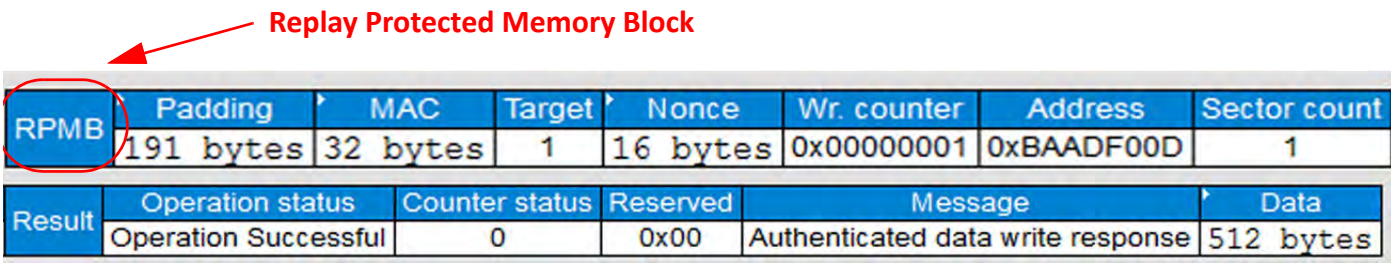


Figure 9.83: NVMe 1.2 Specification: Replay Protected Memory Block

The Replay Protected Memory Block (RPMB) provides a means for the system to store data to a specific memory area in an authenticated and replay protected manner. This is provided by first programming authentication key information to the controller that is used as a shared secret. The system is not authenticated in this phase, therefore the authentication key programming should be done in a secure environment (e.g., as part of the manufacturing process). The authentication key is utilized to sign the read and write accesses made to the replay protected memory area with a Message Authentication Code (MAC). Use of random number (nonce) generation and a write count register provide additional protection against replay of messages where messages could be recorded and played back later by an attacker.

The figure below (Figure 9.84) shows the support added for the Shared Namespace command in NVMe data traffic.

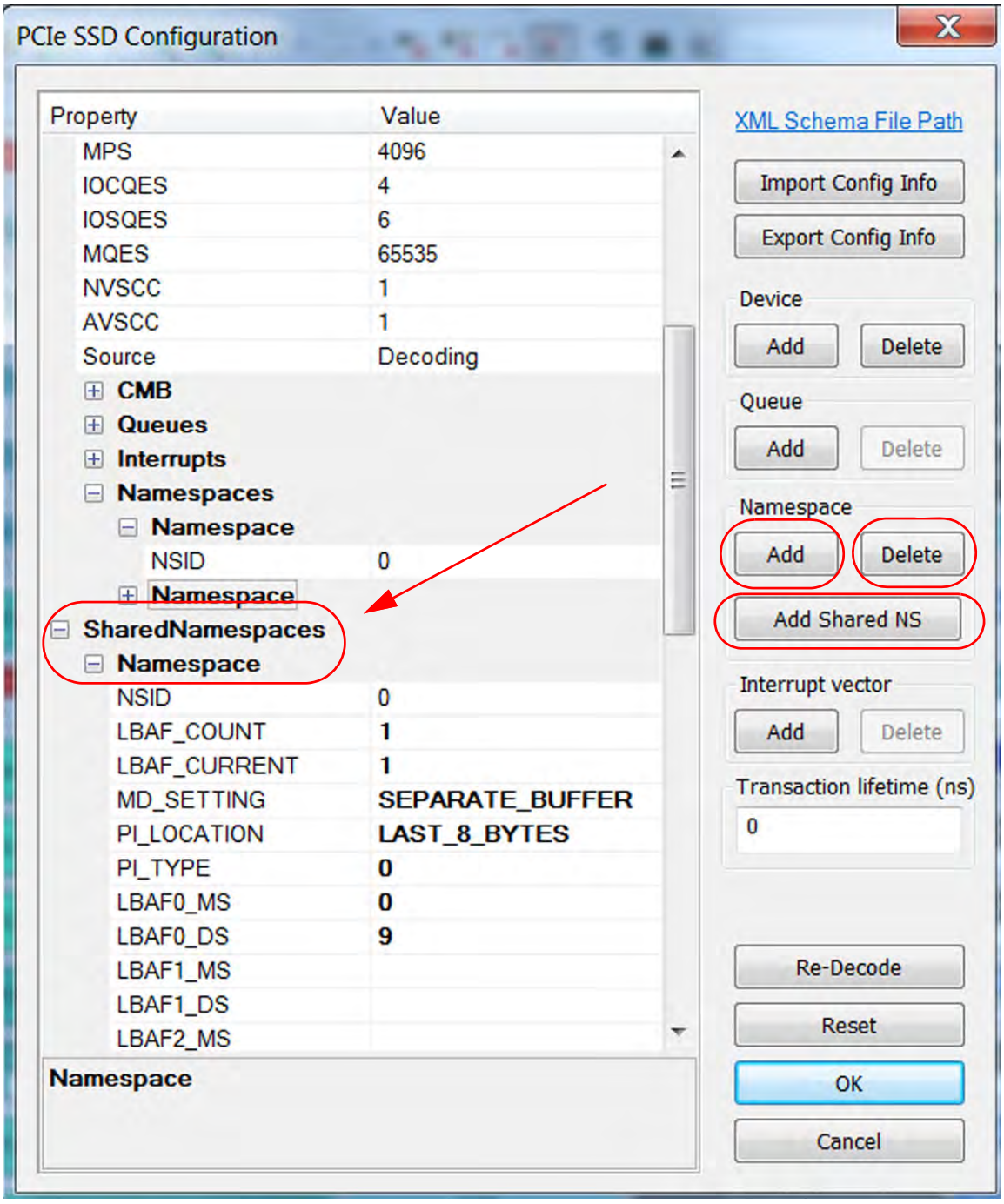


Figure 9.84: NVMe 1.2 Specification: Shared Namespaces

You can “Add” or “Delete” a namespace or Add a Shared namespace. A shared namespace is defined as a namespace that is accessible by two or more controllers in an NVM subsystem. A host may determine whether a namespace is a private namespace or may be a shared namespace by the value of the Namespace Multi-path I/O and Namespace Sharing Capabilities (NMIC) field in the Identify Namespace data structure.

The figure below (Figure 9.85) shows the added support for the Controller Memory Buffer (CMB) as defined in the NVMe 1.2 Spec.

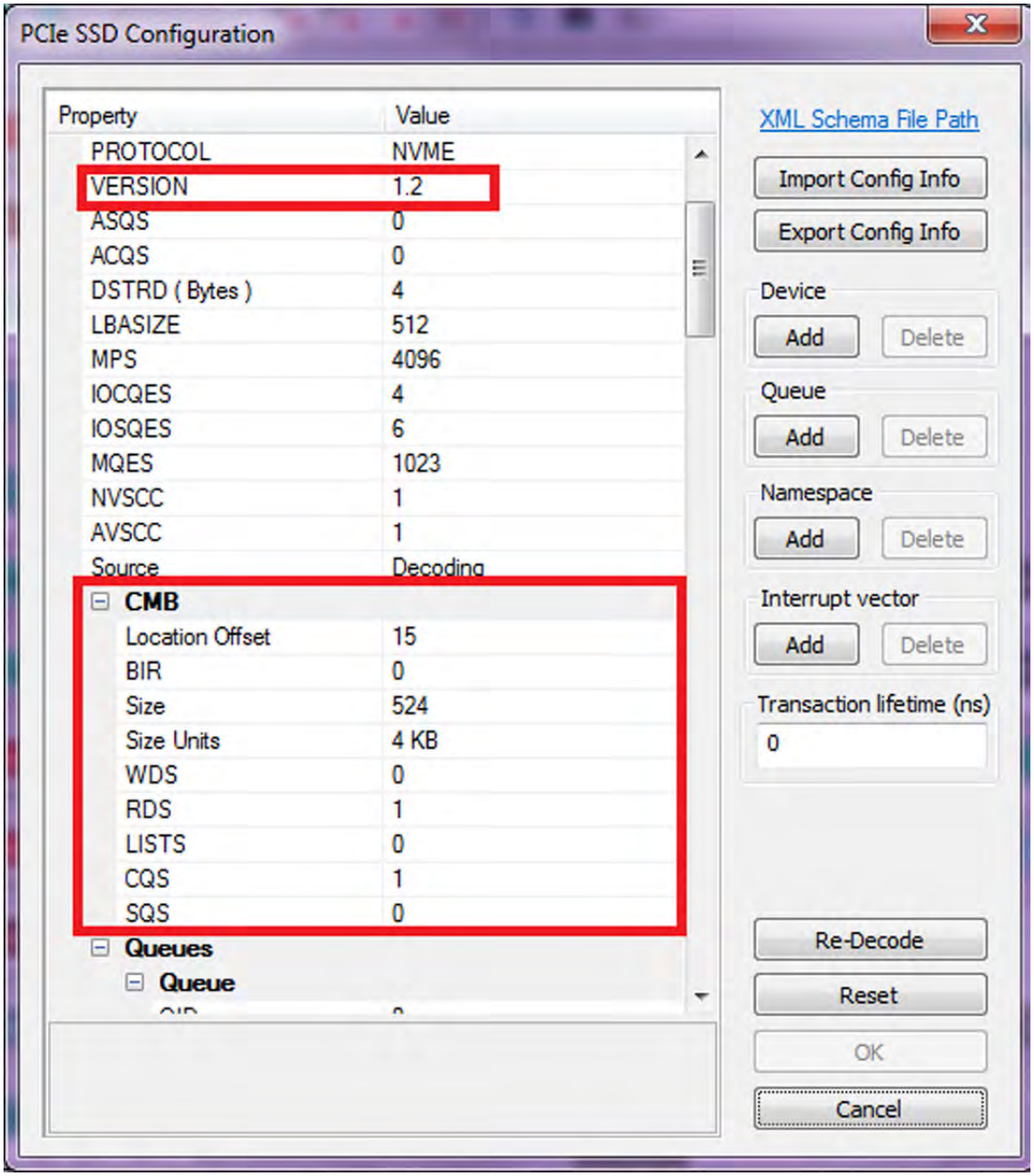


Figure 9.85: NVMe 1.2 Specification: SSD Dialog Version and CMB Configuration

The Controller Memory Buffer (CMB) is a region of general purpose read/write memory on the controller that may be used for a variety of purposes. The controller indicates which purposes the memory may be used for by setting support flags in the CMBSZ register.

9.11.7 Support for Physical Region Page (PRP) and Scatter Gather List (SGL) in Controller Memory Buffer (CMB)

The PCIe Protocol Analysis software supports PRP and SGL in CMB. See Figure 9.86 through Figure 9.88 on page 591.

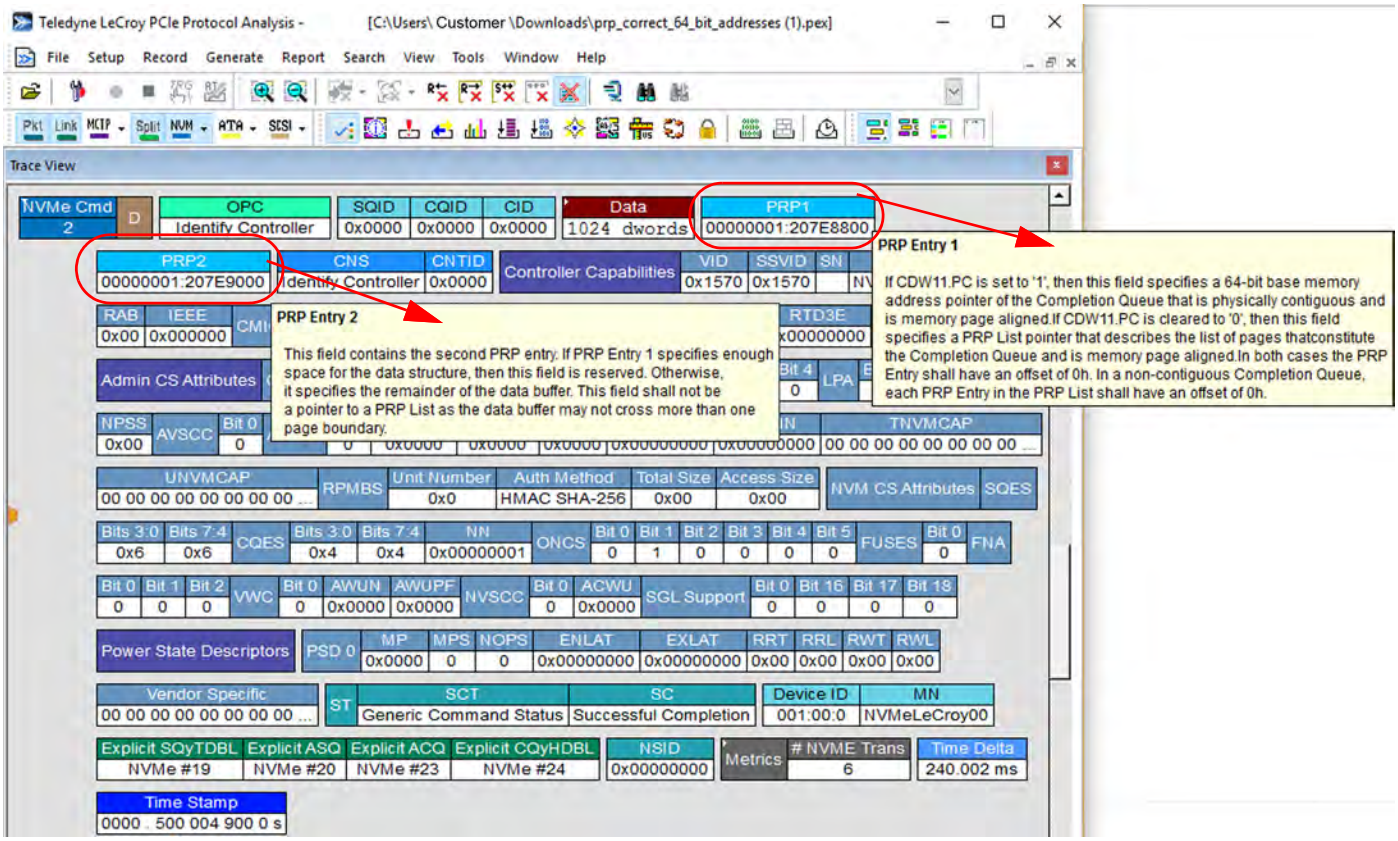


Figure 9.86: PRP1 and PRP2 in CMB Supported in PCIe Protocol Analysis Software

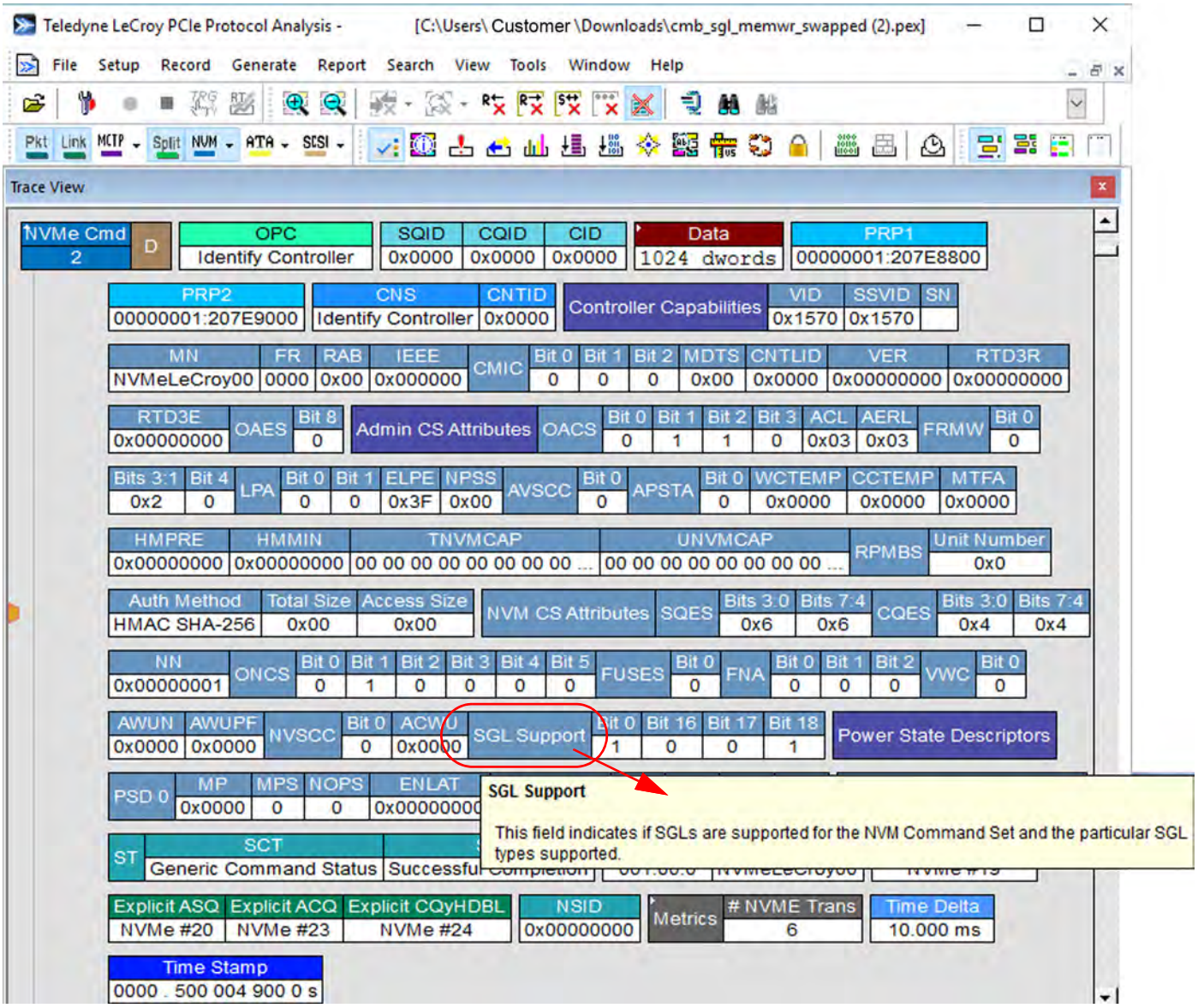


Figure 9.87: SGL Descriptor Supported in PCIe Protocol Analysis Software

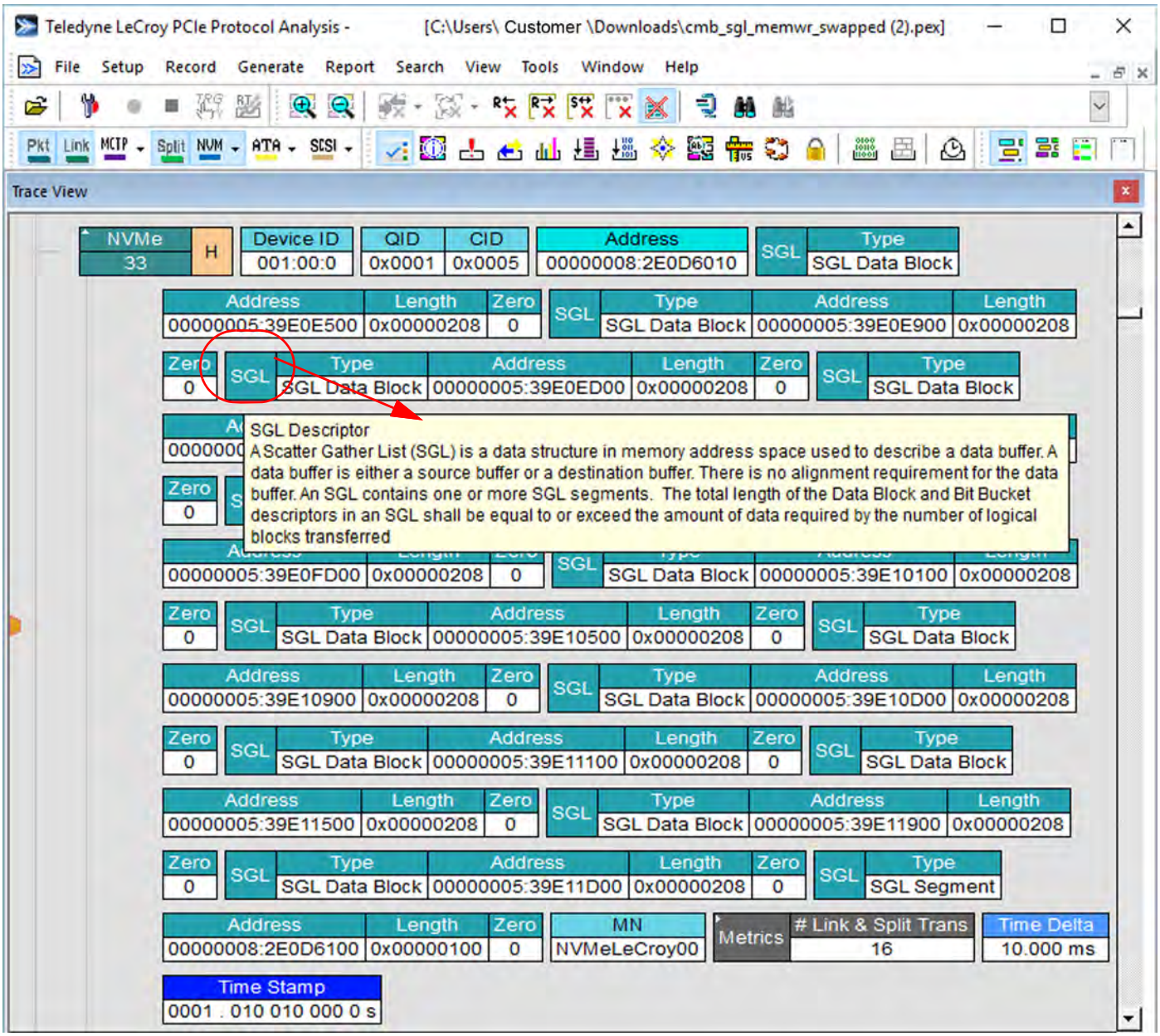


Figure 9.88: SGL Descriptor Tooltip

9.11.8 NVMe Decoding for Host Memory Buffer FID

The PCIe Protocol Analysis software can decode NVMe Host Memory Buffer FID as shown in Figure 9.89.

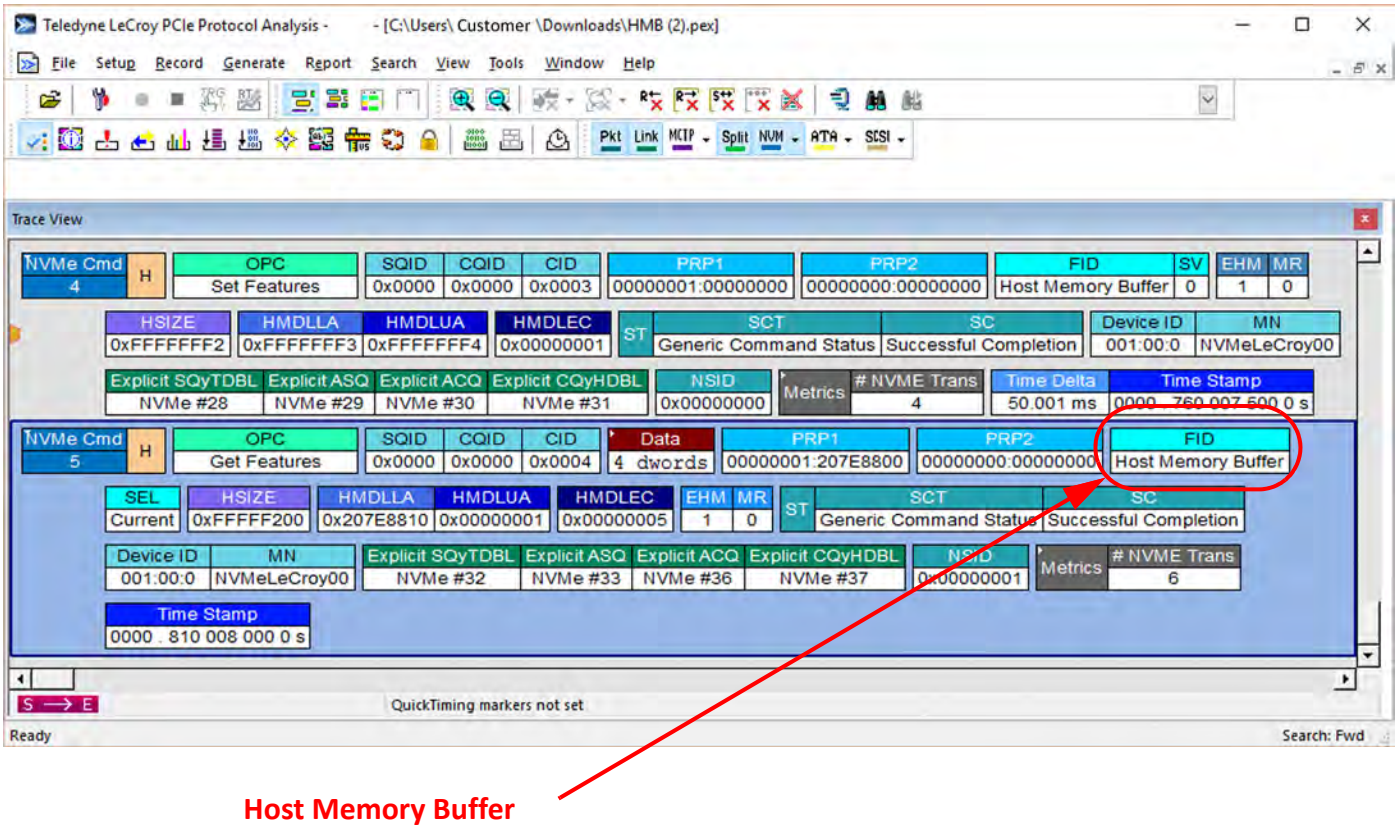
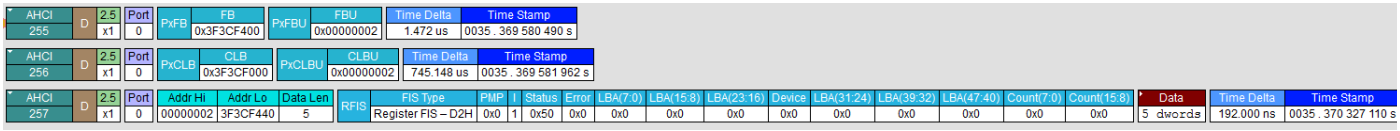


Figure 9.89: NVMe Trace with Host Memory Buffer FID Properly Decoded

9.11.9 AHCI

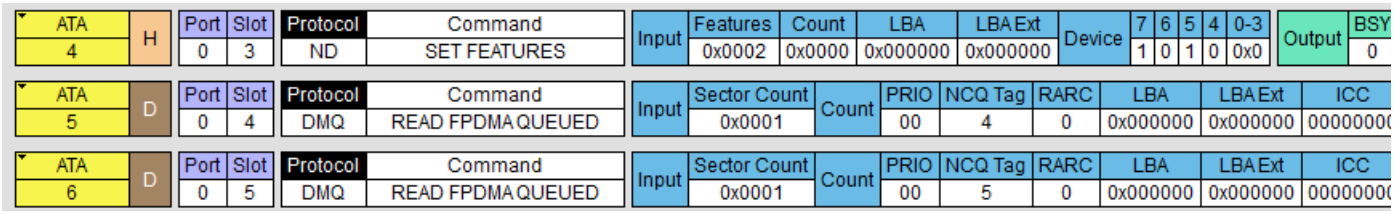
AHCI level decode displays AHCI transactions. PCIe Protocol Analysis decodes the storage commands starting from lower Transaction Layer decodes. In the case of AHCI, it will decode first the Packet Level, then the Link Transaction level, then the Split Transaction Level and finally the AHCI decode level.



Note: The trace must contain the device enumeration sequence so the decoding picks up the associated base addresses and AHCI transactions can be properly decoded. If the enumeration sequence is not available the base addresses must be manually entered in the PCIe SSD Configuration dialog from the Tools menu.

9.11.10 ATA

ATA level decode displays ATA transactions. PCIe Protocol Analysis decodes the storage commands starting from lower Transaction Layer decodes. In the case of ATA, it will decode first the Packet Level, then the Link Transaction level, then the Split Transaction Level, then AHCI level and finally the ATA decode level.



Note: The trace must contain the device enumeration sequence so the decoding picks up the associated base addresses and ATA transactions can be properly decoded. If the enumeration sequence is not available the base addresses must be manually entered in the PCIe SSD Configuration dialog from the Tools menu.

9.11.10.1 ATA IO: Pending Transactions Statistical Report

ATA IO Pending Transactions statistical information can be displayed from an ATA Trace by selecting an ATA Packet and viewing the Metrics box. See Figure 9.90.

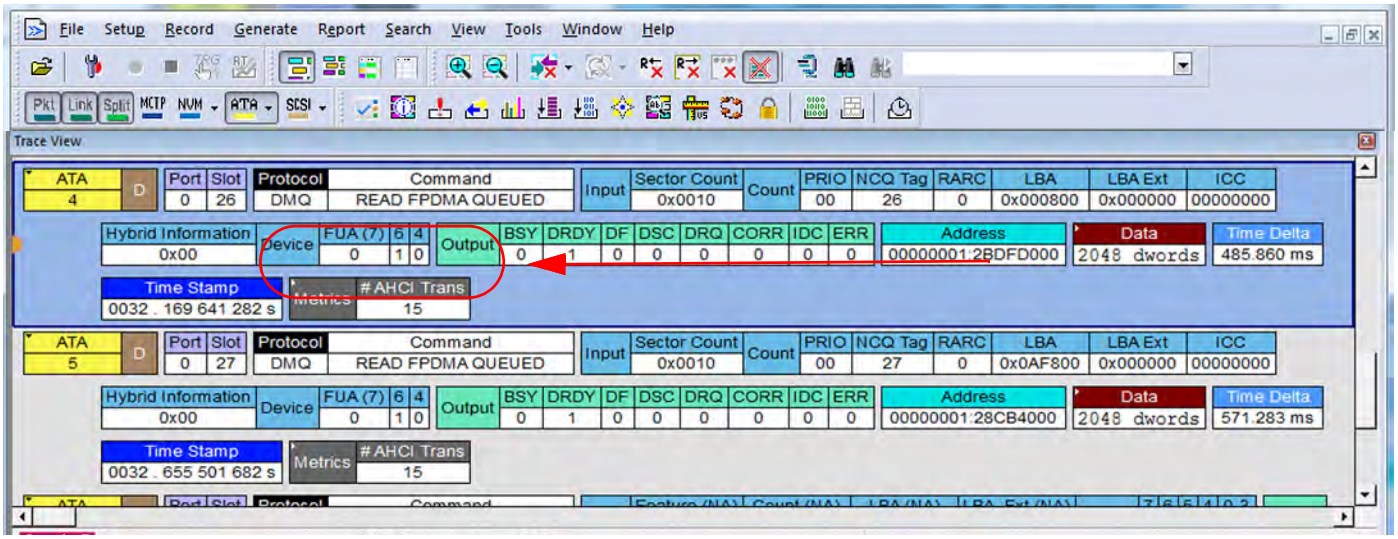


Figure 9.90: ATA IO Pending Transactions: Metrics Box

Move the cursor over the Metrics box to display the information about the ATA Packet. See Figure 9.91 on page 594.

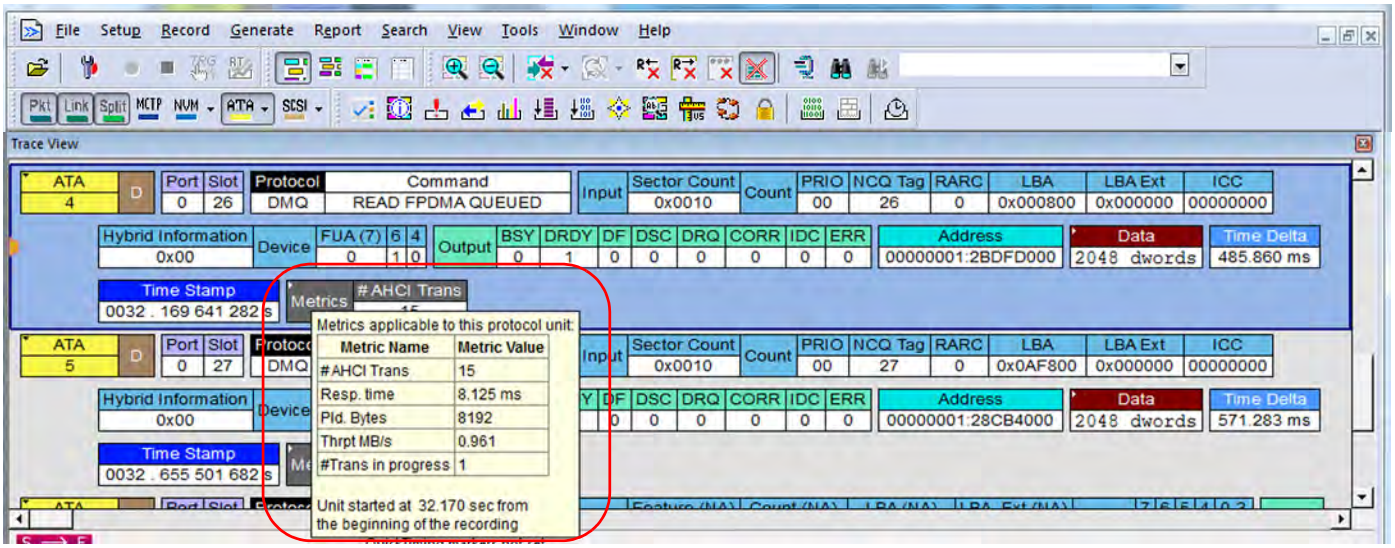


Figure 9.91: ATA IO Pending Transactions: Metrics Box -- Information Displayed

You can click on the small white arrow in the Metrics box to display the information in the Trace. See Figure 9.92 on page 595.

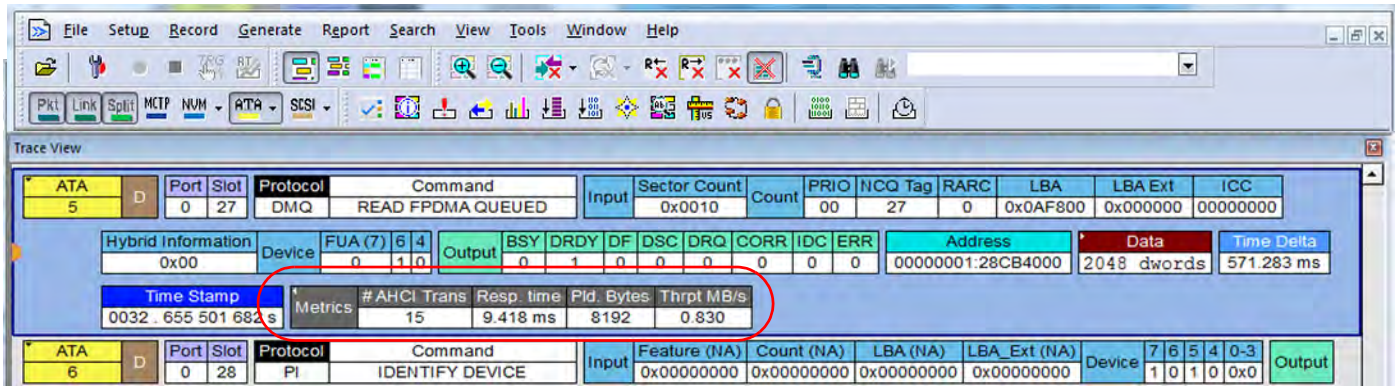


Figure 9.92: ATA IO Pending Transactions: Metrics Displayed in Trace

You can also view the ATA IO Pending Transactions by selecting the Bus Utilization icon in the toolbar and selecting the Graph Areas icon. See Figure 9.93 on page 596.

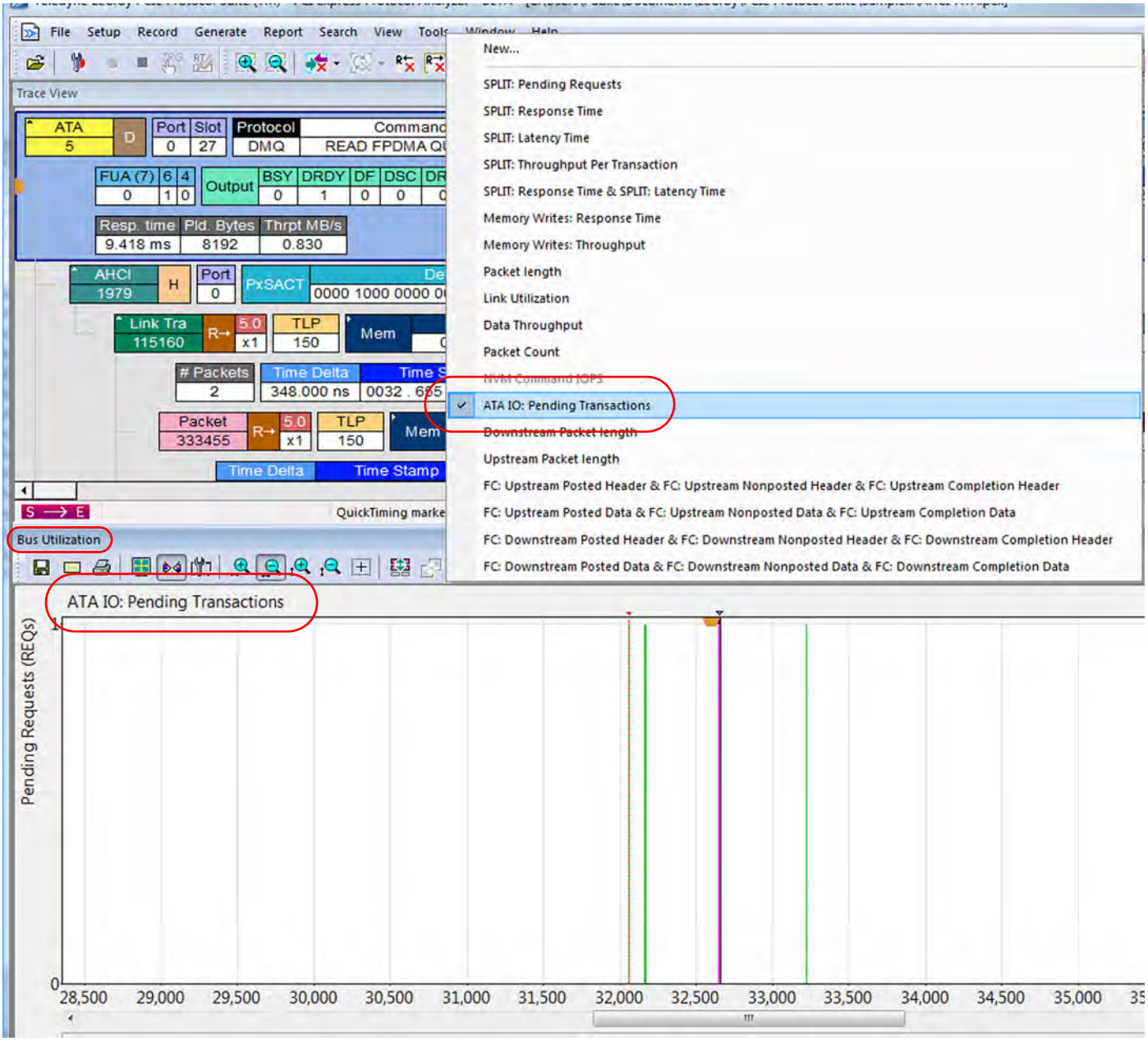
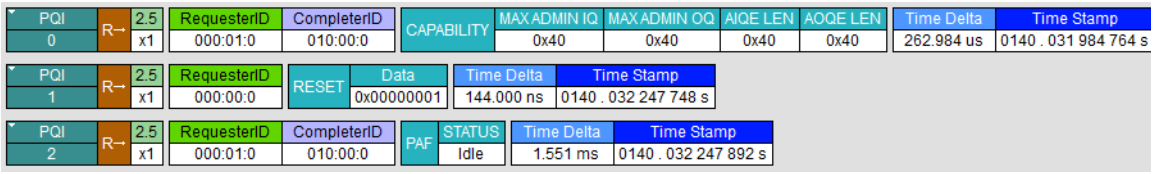


Figure 9.93: ATA IO Pending Transactions: Bus Utilization View

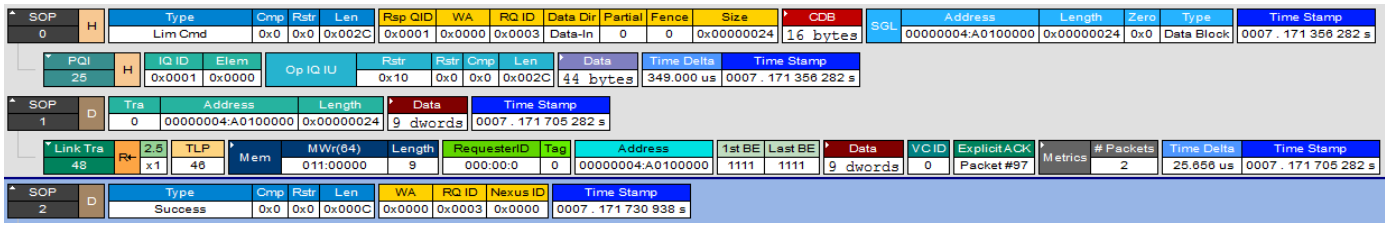
9.11.11 PQI

PQI level decode PQI displays PQI transactions. PCIe Protocol Analysis decodes the storage commands starting from lower Transaction Layer decodes. In the case of PQI, it will decode first the Packet Level, then the Link Transaction level, then the Split Transaction Level and finally the PQI decode level.



9.11.12 SOP

SOP level decode SOP displays SOP transactions. PCIe Protocol Analysis decodes the storage commands starting from lower Transaction Layer decodes. In the case of SOP, it will decode first the Packet Level, then the Link Transaction level, then the Split Transaction Level, then PQI level and finally the SOP decode level.



Note: The trace must contain the device enumeration sequence so the decoding picks up the associated base addresses and SOP transactions can be properly decoded. If the enumeration sequence is not available the base addresses must be manually entered in the PCIe SSD Configuration dialog from the Tools menu.

9.11.13 SCSI

SCSI level decode SCSI displays SCSI transactions. PCIe Protocol Analysis decodes the storage commands starting from lower Transaction Layer decodes. In the case of SCSI, it will decode first the Packet Level, then the Link Transaction level, then the Split Transaction Level, then PQI level and finally the SCSI decode level.



SCSI	SCSI CDB	OpCode	Obsolete	EVPD	Page Code	AllocLen	CONTROL	INQUIRY	LUN	Metrics	# SOP IUs	Time Stamp
0	INQUIRY	0x12	Not set	Not set	0x0	36	0x00	Response	0		3	0007 . 171 356 282 s

Note: The trace must contain the device enumeration sequence so the decoding picks up the associated base addresses and SCSI transactions can be properly decoded. If the enumeration sequence is not available, the base addresses must be manually entered in the PCIe SSD Configuration dialog from the Tools menu.

9.11.14 Decoding MCTP (Management Component Transport Protocol)

Note: The Summit M5x can decode MCTP traffic per specifications outlined in the *Readme* file.

9.11.14.1 MCTP Levels in Floating Transactions Bar Window

To decode MCTP traffic you must first load a trace containing MCTP traffic. You can get a visual representation of the MCTP Command structure by pulling the Transaction Level Toolbar (see Figure 9.94) down into the trace and the Floating Transaction Level Bar Window will be shown (see Figure 9.95). The Transaction Level Window shows that the MCTP Command is made up of Links and Packets. You can also see that NVMe, ATA and SCSI traffic consists of Link and Split transactions.



Figure 9.94: Transaction Level Toolbar

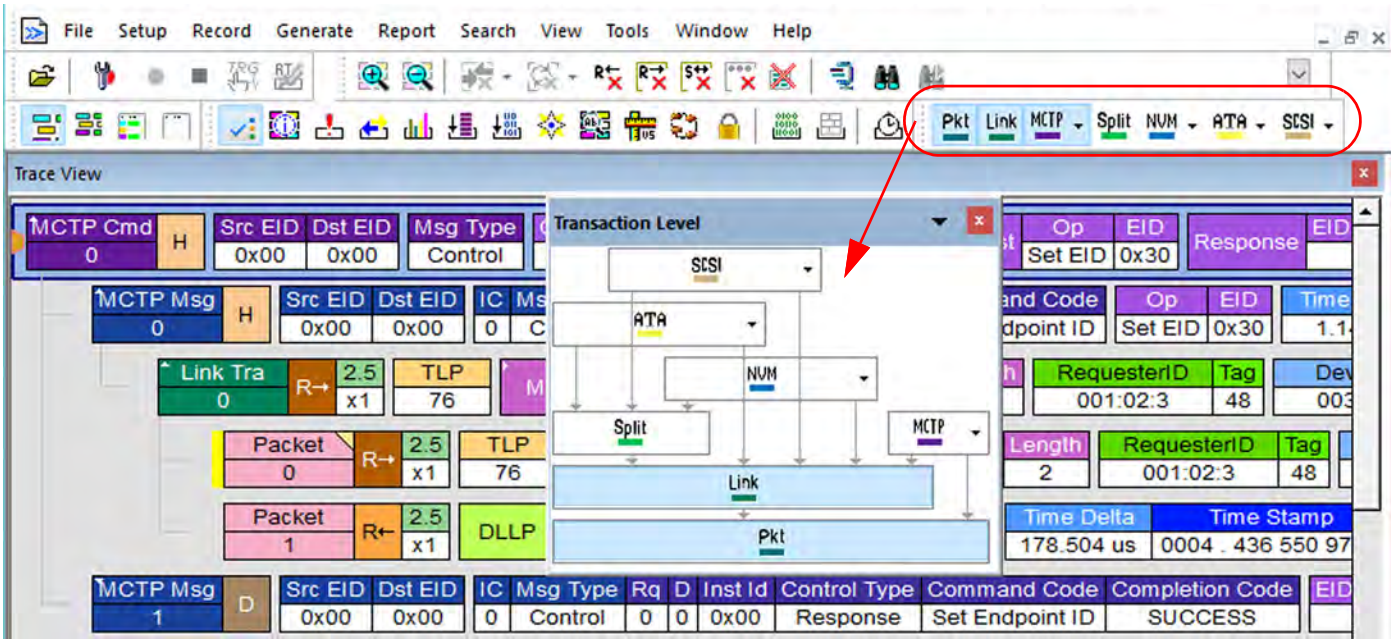


Figure 9.95: MCTP Levels in Floating Transaction Bar Window

9.11.14.2 Decoding MCTP Commands

MCTP traffic can be decoded and displayed as either MCTP Commands or MCTP Messages.

To decode MCTP traffic you must first load a trace containing MCTP traffic. Then click the MCTP icon on the toolbar and select MCTP Commands. See Figure 9.96.

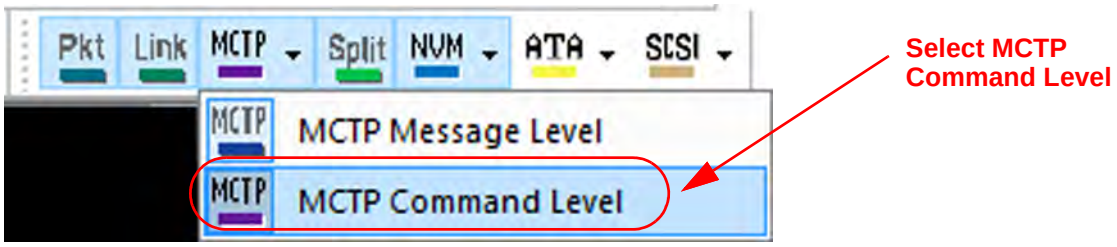


Figure 9.96: MCTP Decoding Icon on Toolbar

This will decode MCTP Commands in the trace. The following types of MCTP Message Types can be decoded:

- MCTP Control: See Figure 9.97 on page 601
- NC-SI: See Figure 9.97 on page 601
- PLDM: See Figure 9.98 on page 602
- PLDM: Firmware Commands Decoded -> See Figure 9.99 on page 602 and Figure 9.100 on page 603.

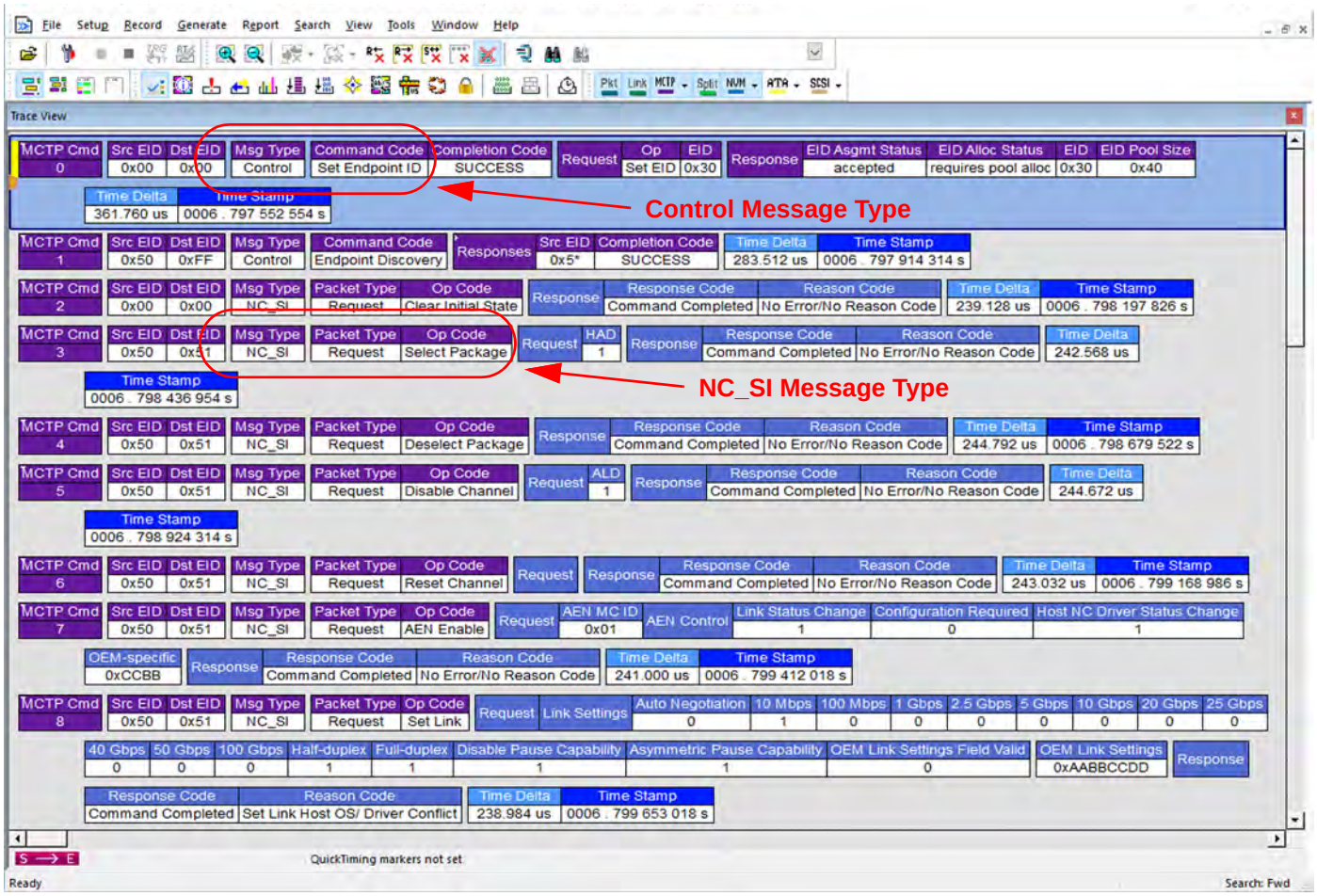


Figure 9.97: MCTP Commands Decoded: Control and NC_SI Types

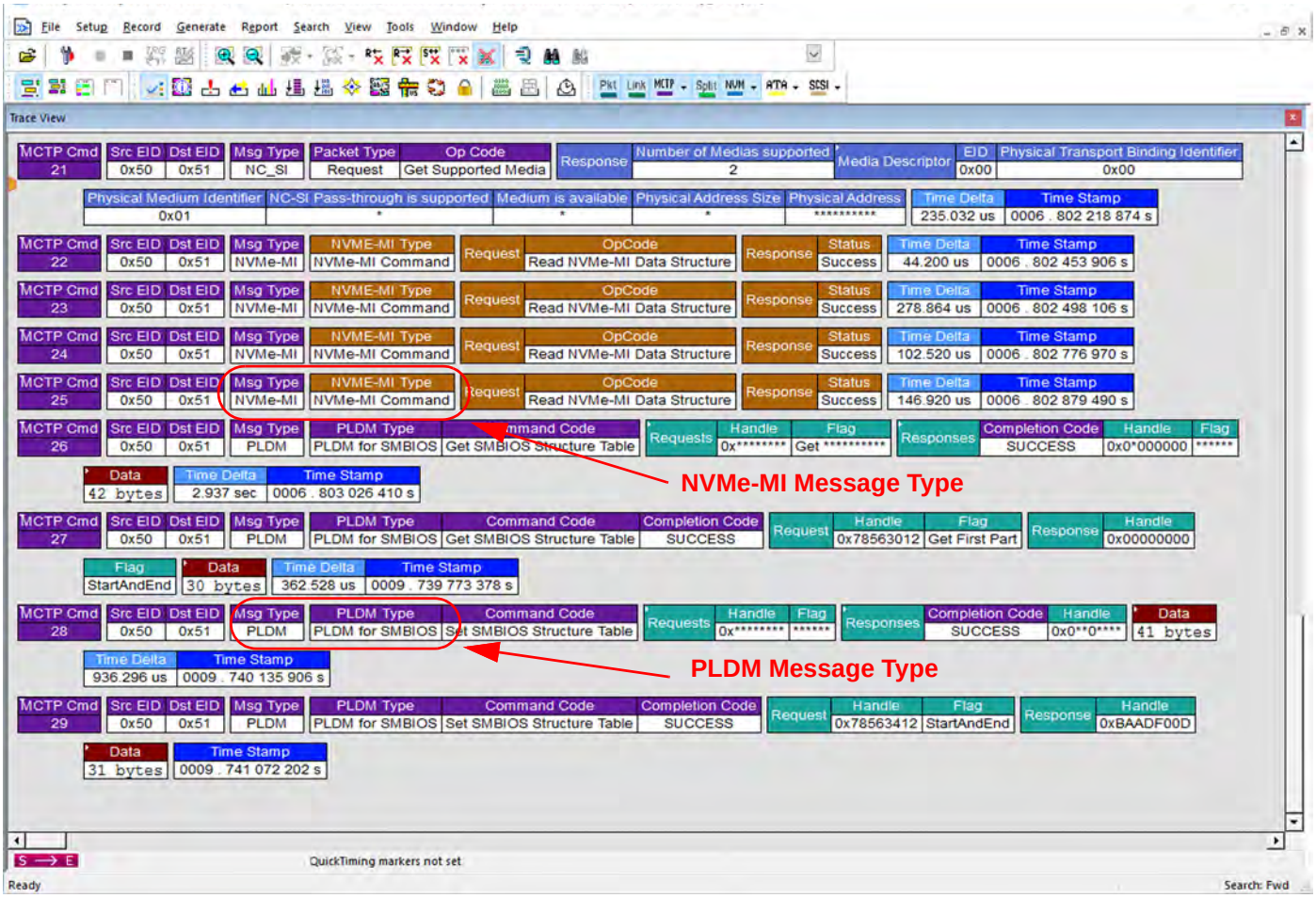


Figure 9.98: MCTP Commands Decoded: NVMe-MI and PLDM Types

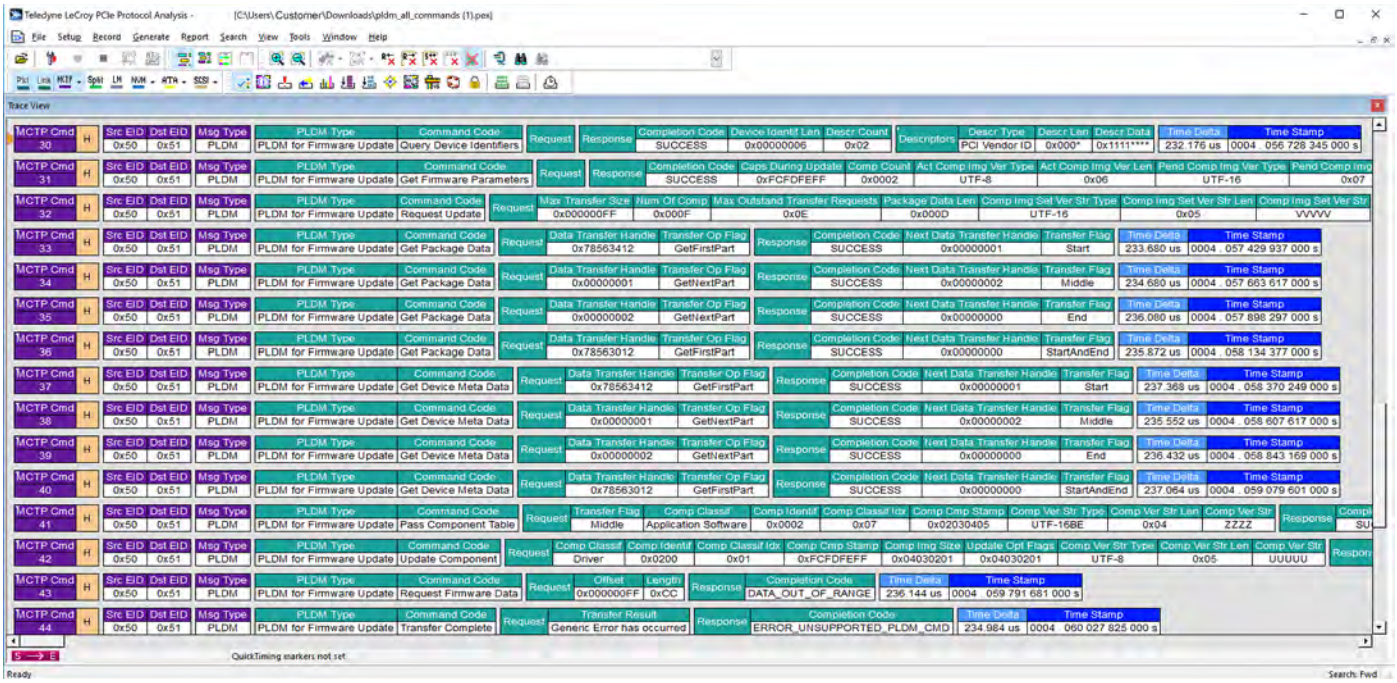


Figure 9.99: PLDM Firmware Update Commands Decoded

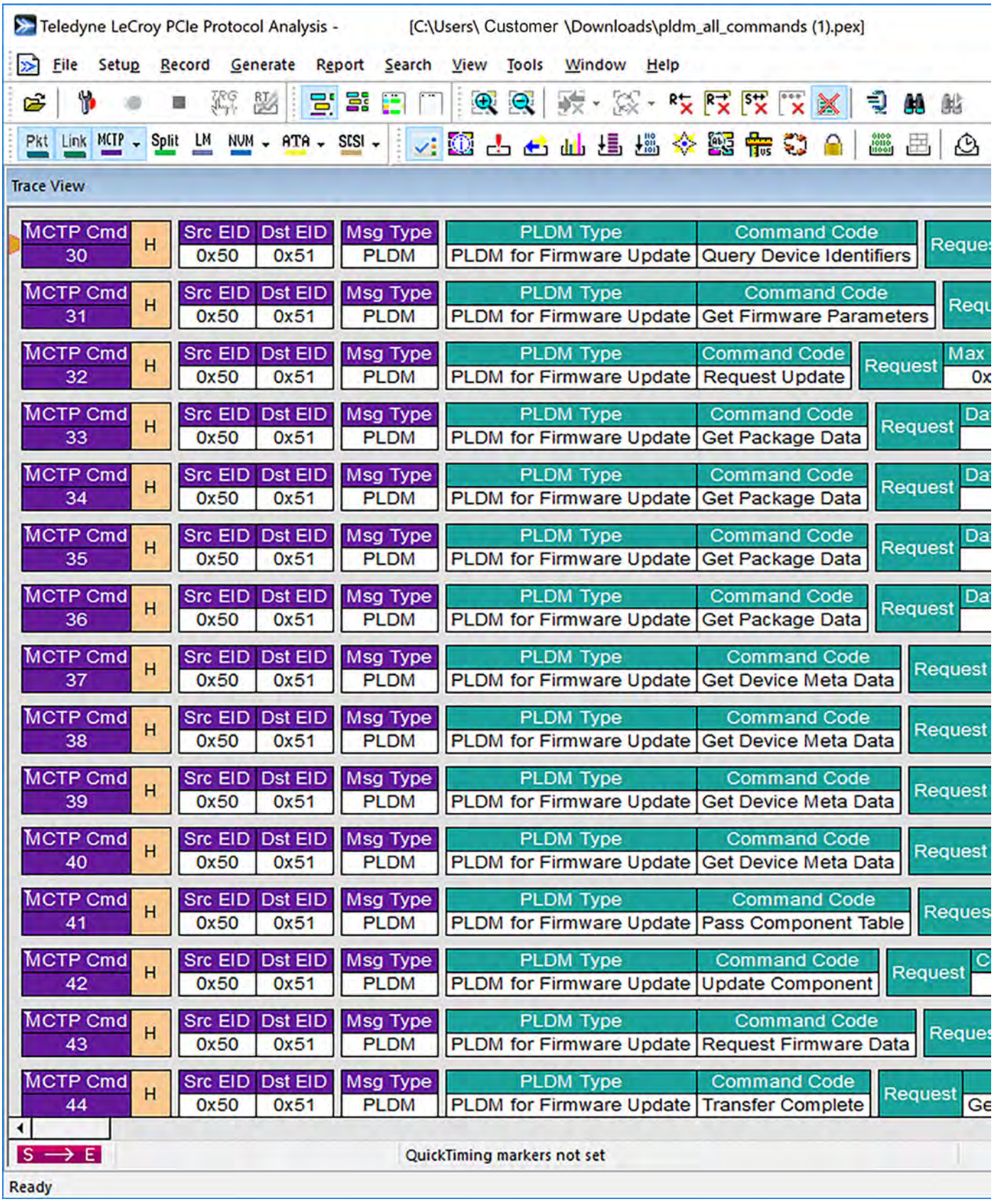


Figure 9.100: PLDM Firmware Update Commands Decoded (Details shown)

9.11.14.3 Expanding MCTP Commands

If you expand any MCTP command, you'll see all of the MCTP messages and lower level packets that make up the command. In this case we expanded MCTP Command 0. It consists of MCTP Message 0 from the Host and MCTP Message 1 from the Device. If you expand MCTP Message 0, you'll see that it consists of Link Transaction 0, which can be expanded down to Packet 0 and Packet 1. Notice that MCTP Command 0, MCTP Message 0, Link Transaction 0 and Packet 0 all have the same Timestamp: 0006.797.552.554 seconds. The response from the Device occurs as 0006.797.553.698 seconds. See Figure 9.101 on page 604.

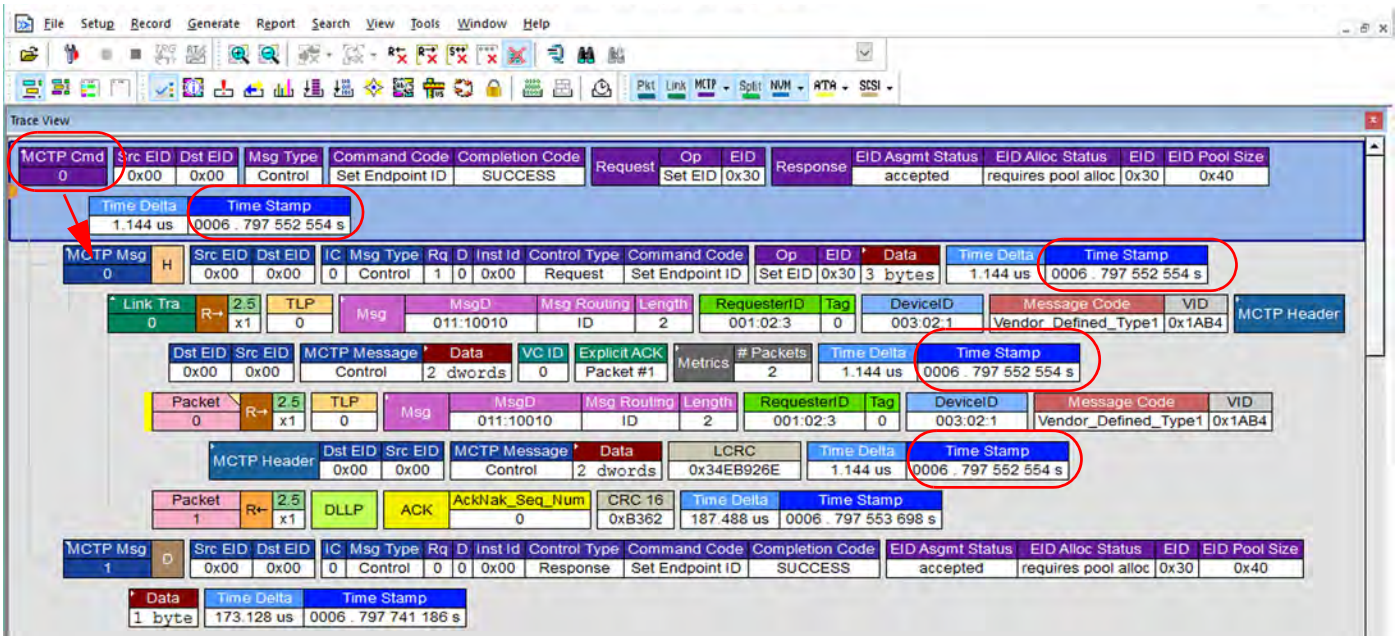


Figure 9.101: MCTP Command 0 Expanded

9.11.14.4 Decoding MCTP Messages

If you had selected MCTP Messages to be decoded instead of Commands, only the MCTP Messages would be displayed. See Figure 9.102.

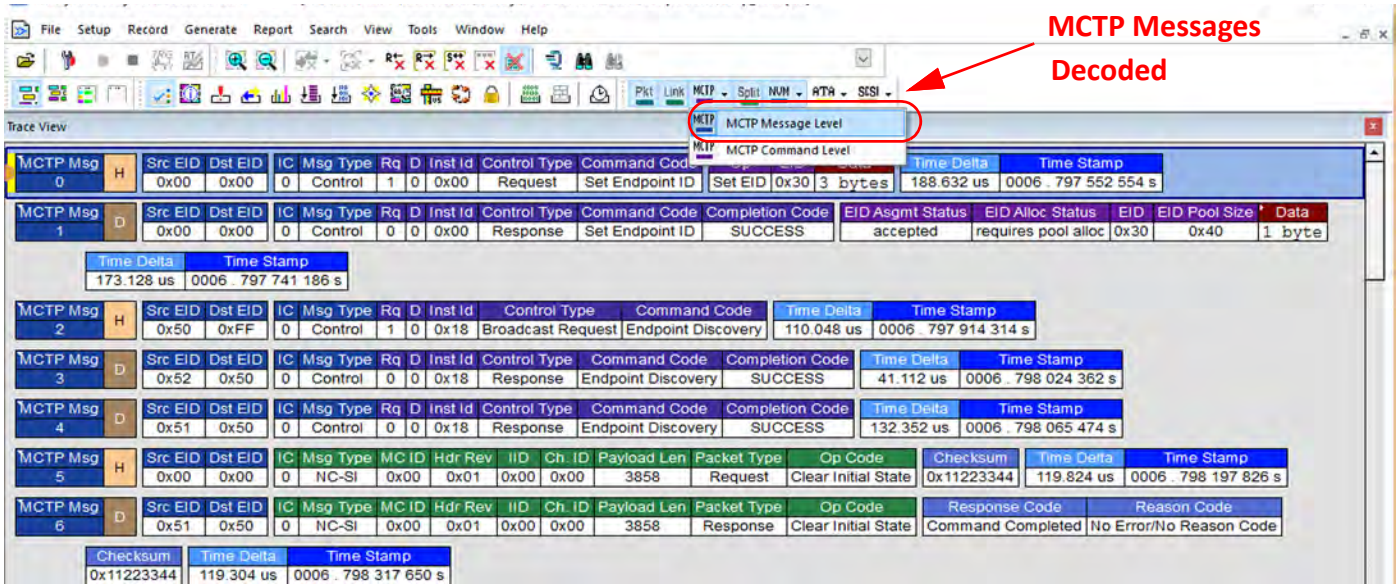


Figure 9.102: MCTP Messages Decoded

If you expand the MCTP Message you'll see the same information you saw by expanding the MCTP Command. See Figure 9.103 on page 605.

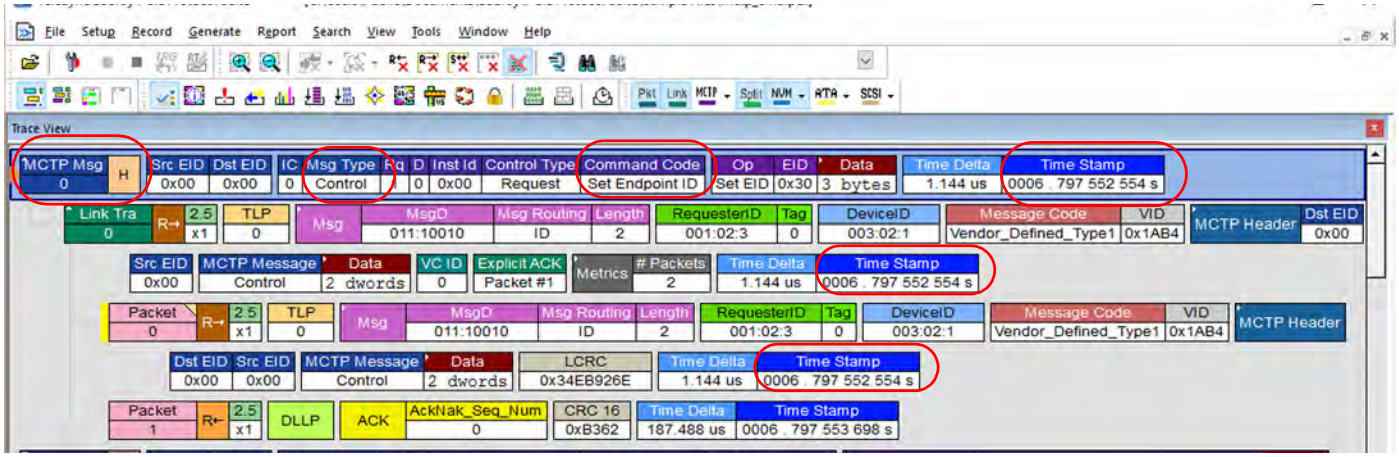


Figure 9.103: Expanding MCTP Message

9.11.14.5 MCTP Commands with SMBus Traffic

To decode an MCTP command with SMBus traffic you must first load a trace with the appropriate traffic. Then decode MCTP traffic by clicking on the MCTP icon in the toolbar. In the example shown below we've loaded a trace that has SMBus traffic within an MCTP message that is part of an MCTP command. See Figure 9.104.

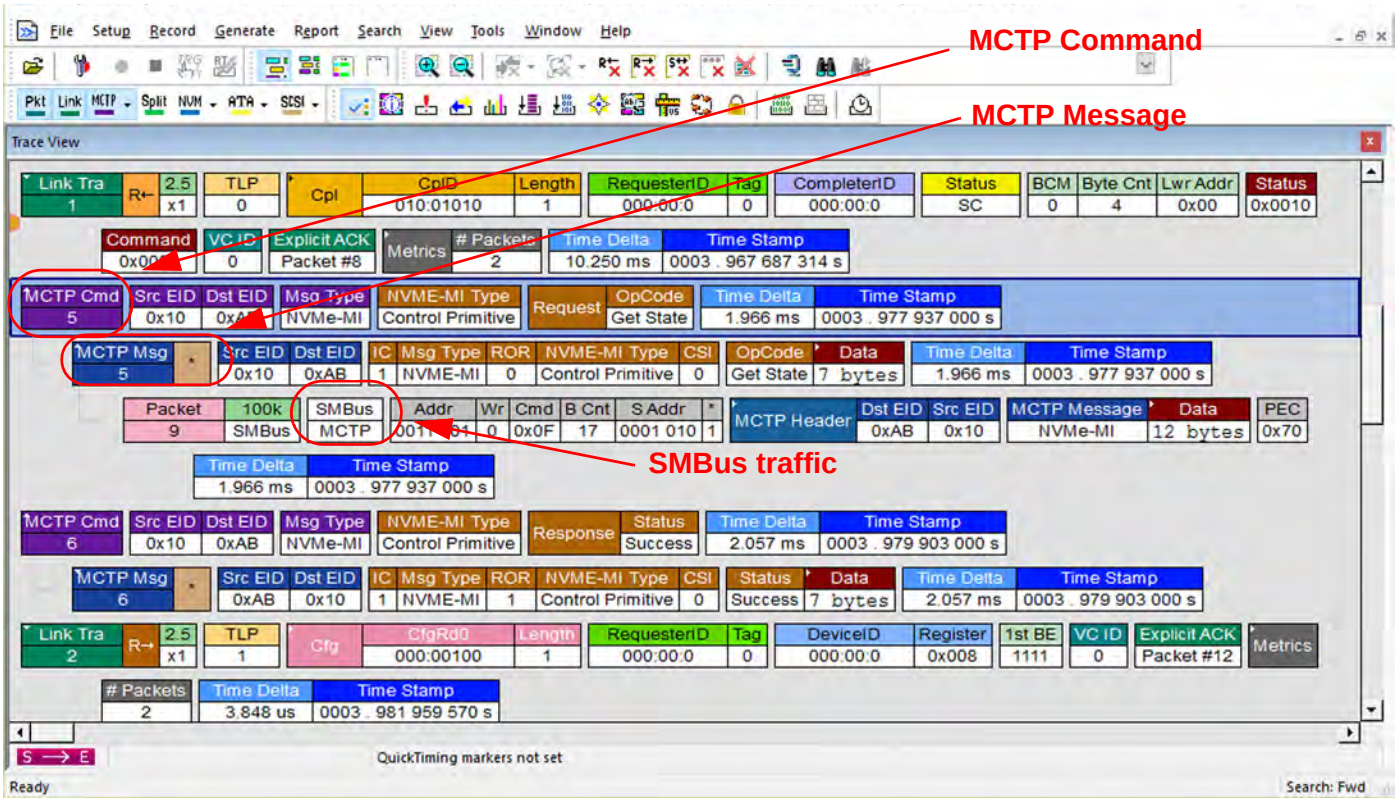


Figure 9.104: MCTP Command with SMBus Traffic

9.11.14.6 MCTP Commands: Request from Host, Response from Device

MCTP commands can be decoded as shown below (see Figure 9.105). As you can see the MCTP Command is made up of MCTP messages. One is from the Host the response is from the Device.

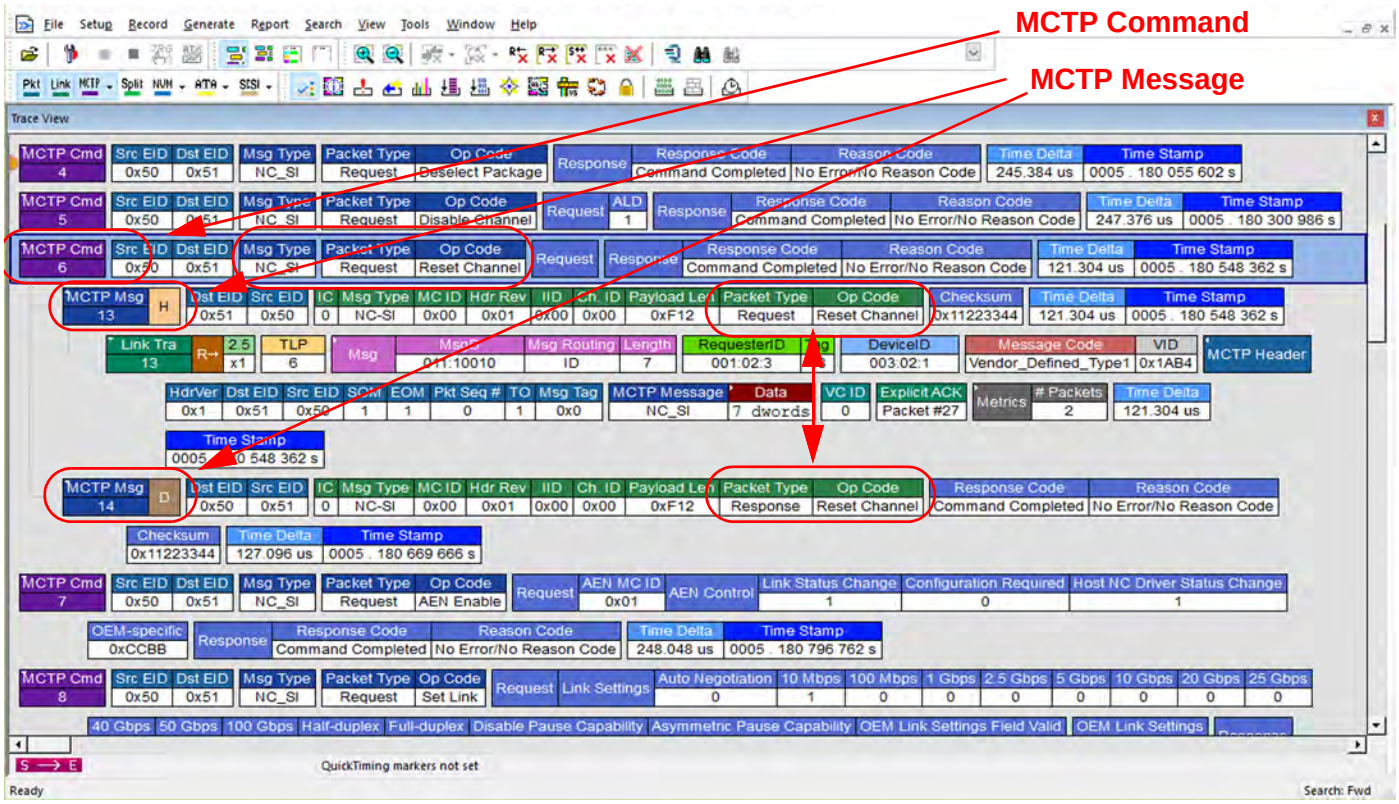


Figure 9.105: Decoding MCTP Commands

9.11.14.7 Decoding MCTP Messages and Transactions

Note: To decode MCTP messages and transactions you'll need a license for your analyzer. If you don't have a MCTP license a warning message will pop up. See Figure 9.106.

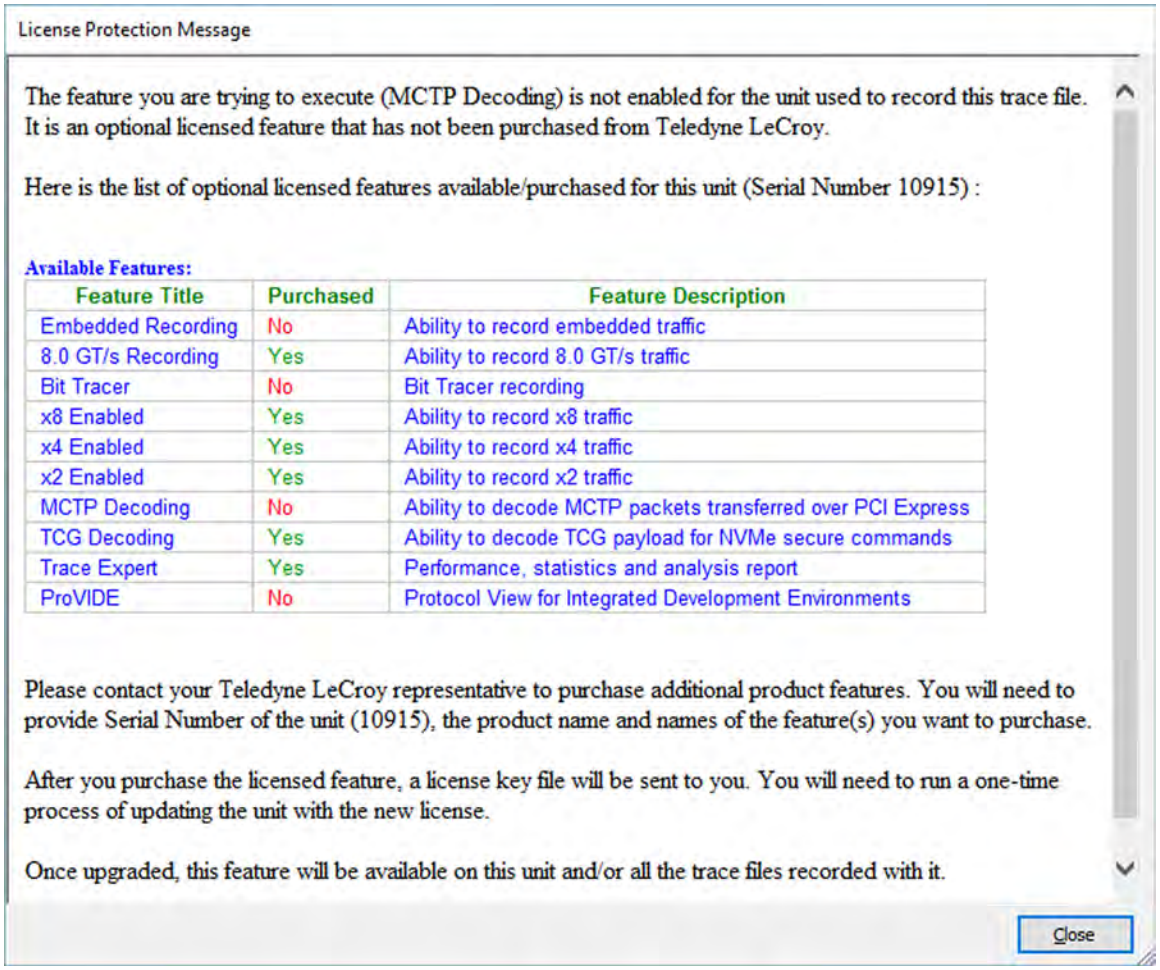


Figure 9.106: Warning Message: No MCTP License

You can decode both MCTP messages and transactions within traces by selecting CATC Trace View, Decoding Packets, Links and MCTP 

. You'll see that the transaction contains an MCTP Header and an MCTP Message. See Figure 9.107 on page 609.

9.11.14.8 MCTP Messages

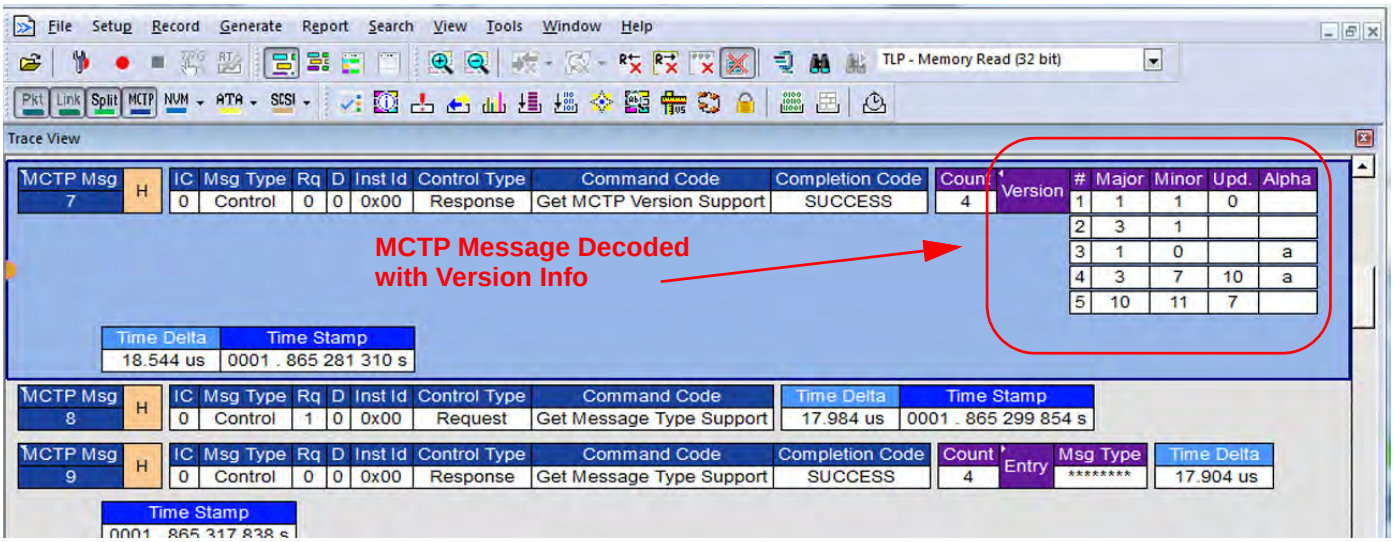


Figure 9.107: MCTP Message Decoded

9.11.14.9 MCTP Transactions

The Link Transaction will decode an MCTP Header and an MCTP Message containing a Msg Type, a Control Type and a Command Code. See Figure 9.108.

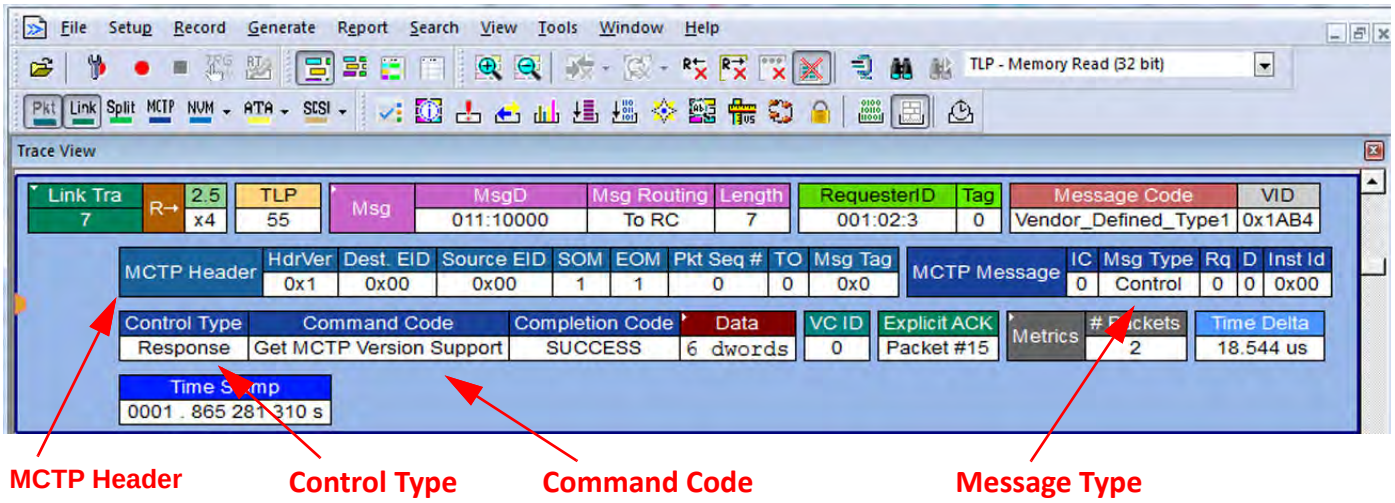


Figure 9.108: Decoding MCTP Transactions

9.11.14.10 MCTP Errors Reported

You can also display the following types of Errors from the Detailed View of the Trace:

- RsvdNotNull: RSVD field shall be 0
- InvalidHdrVer: Header version field should be set to 1
- InvalidDstEId: Destination Endpoint IDs 1 through 7 are reserved for future definition
- InvalidSrcEId: Source Endpoint IDs 1 through 7 are reserved for future definition
- ICNotNull: IC bit shall always be 0 for MCTP control messages

See Figure 9.109 on page 610.

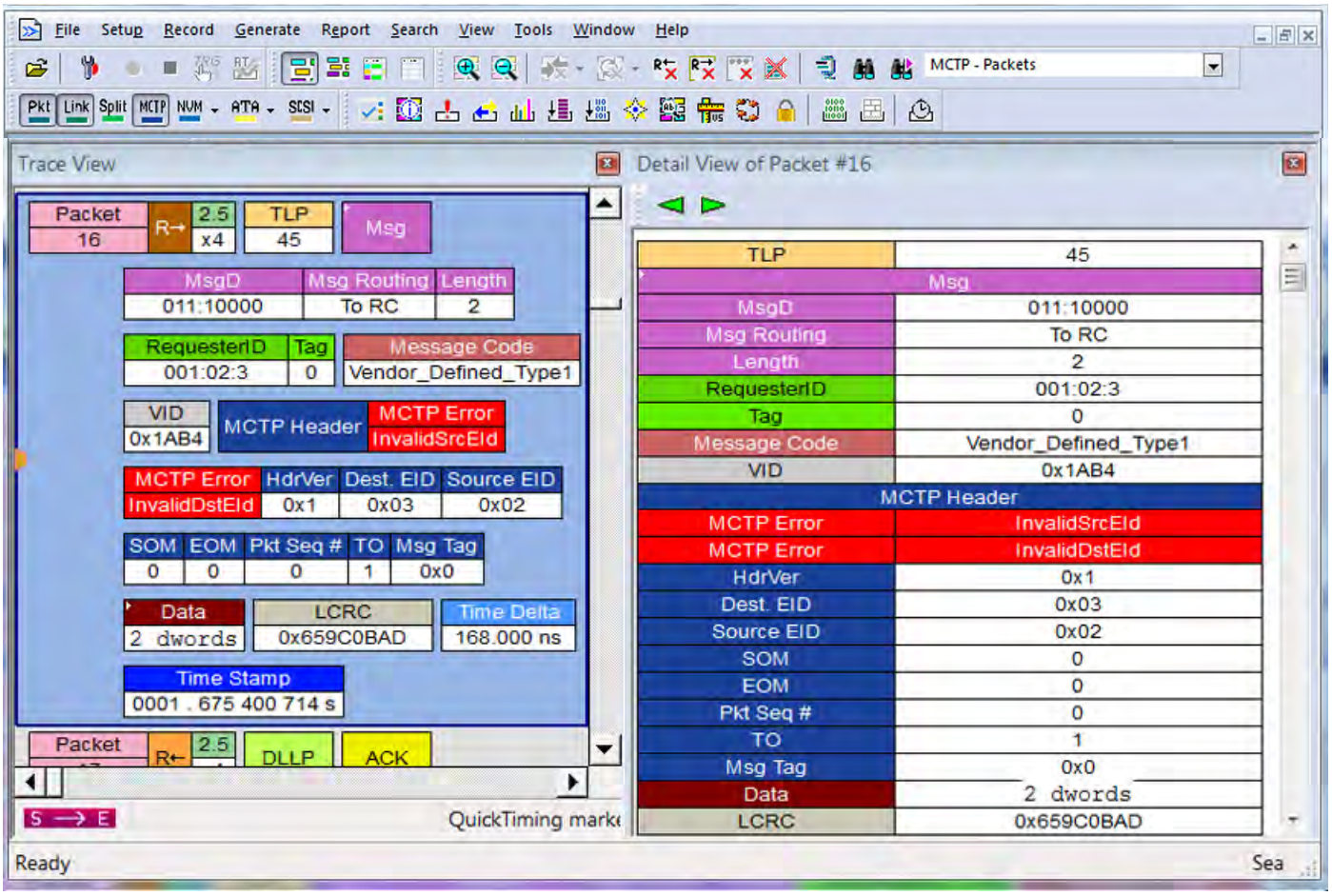


Figure 9.109: MCTP Transaction Errors Reported

9.11.14.11 MCTP Trace In Spreadsheet View

MCTP Traces can be displayed in Spreadsheet View. See Figure 9.110.

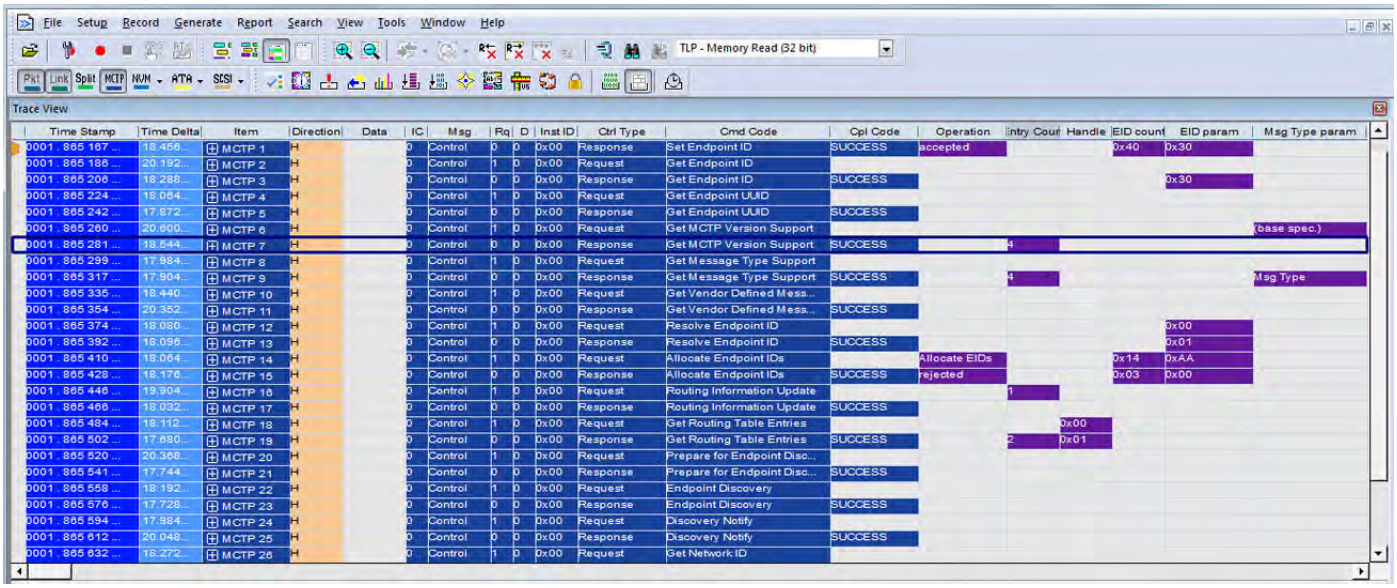


Figure 9.110: MCTP Trace in Spreadsheet View

9.11.14.12 Decoding MCTP Messages with PLDM Message Types

You can decode MCTP Messages with Platform Level Data Model (PLDM) Message types within traces by selecting CATC Trace View, Decoding Packets, Links and MCTP  . You'll see that the message contains an MCTP Header and an PLDM Message. See Figure 9.111. In the example shown below there are both PLDM Requests and PLDM Responses.

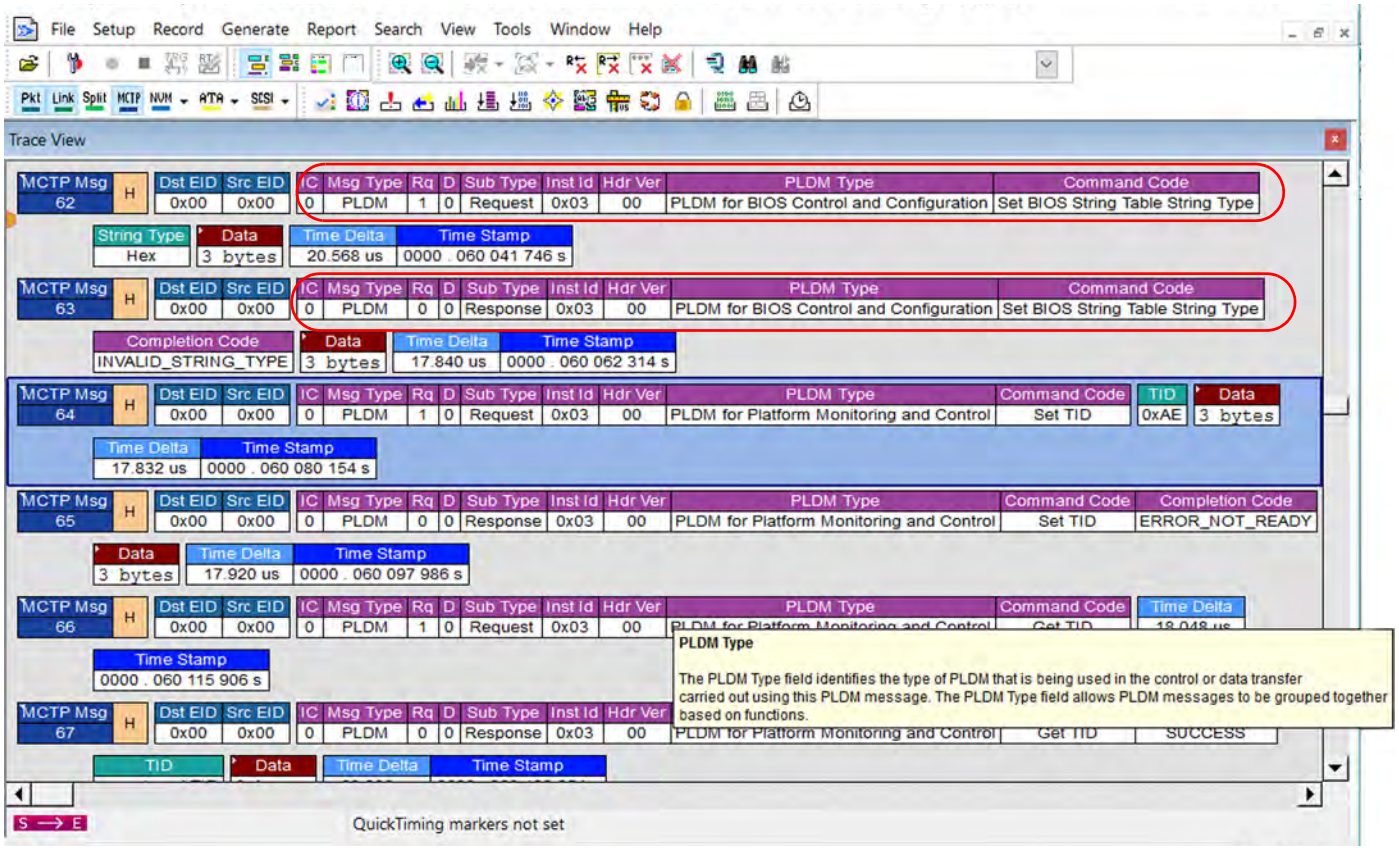


Figure 9.111: MCTP Message with PLDM Message Type

9.11.14.13 Decoding MCTP Messages with NC-SI Message Types

You can decode MCTP Messages with Network Controller Side Band Interface (NC-SI) Message types within traces by selecting CATC Trace View, Decoding Packets, Links and MCTP 

. You'll see that the message contains an MCTP Header and an NC-SI Message. See Figure 9.112. In the example shown below, there is an NC-SI Request packet type followed by the NC-SI packet Response.

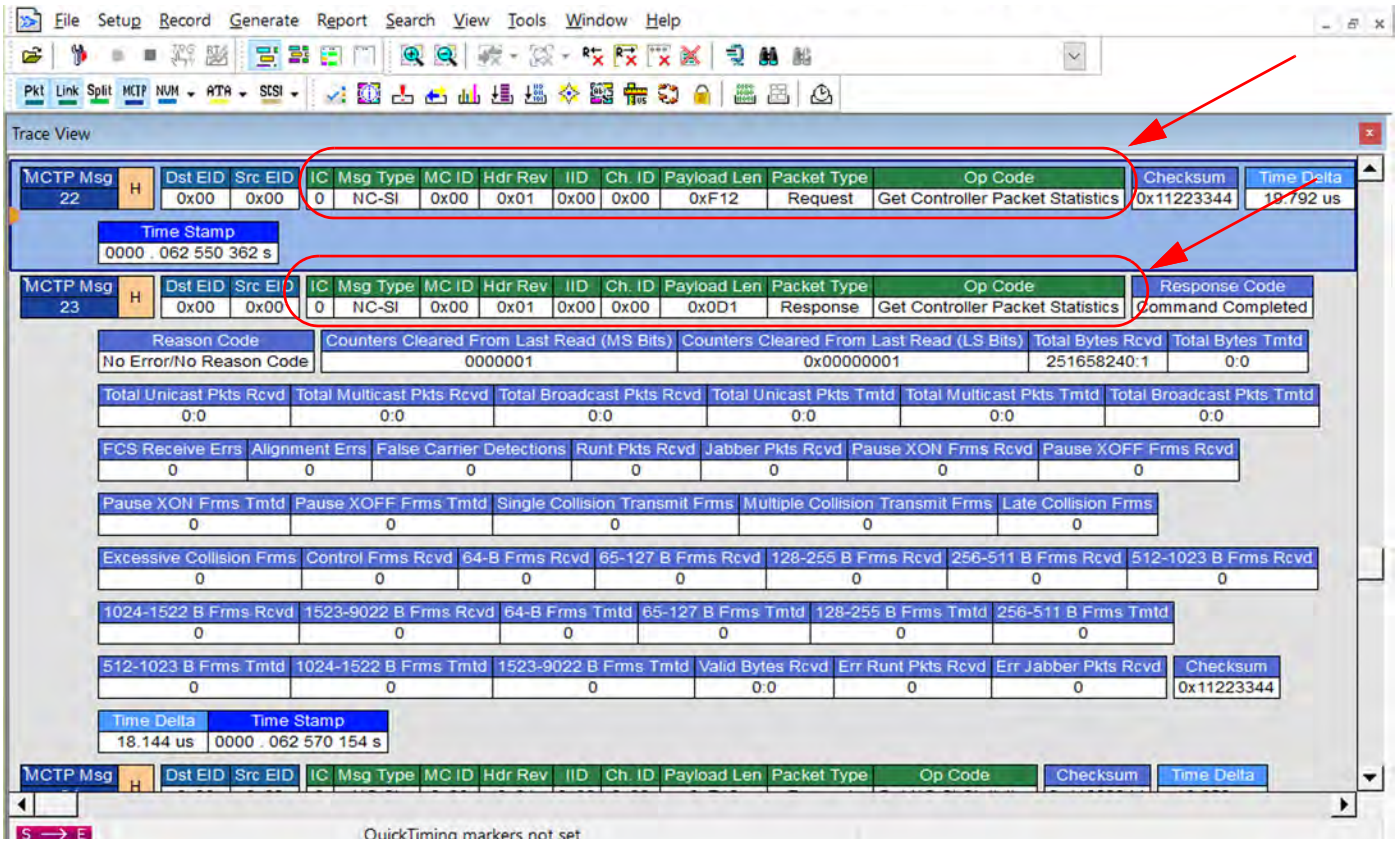


Figure 9.112: MCTP Message with NC-SI Message Type

9.11.14.14 MCTP Command with NVMe-MI Errors Decoded

The PCIe Protocol Analysis can detect, decode and display NVMe-MI errors in MCTP traffic, as shown below in Figure 9.113.

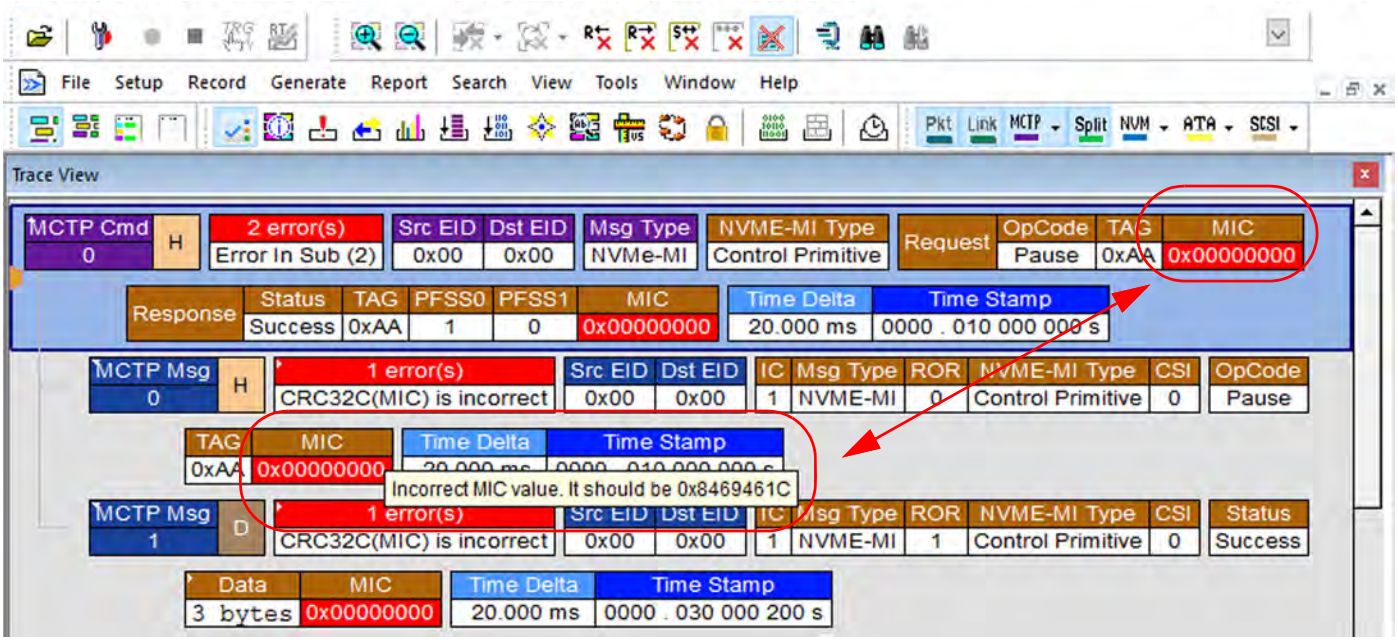


Figure 9.113: Errors Decoded In MCTP/NVMe-MI Traffic

9.11.14.15 MCTP Message Type and IC Cells

You can decode MCTP Messages and IC cells. See Figure 9.155.

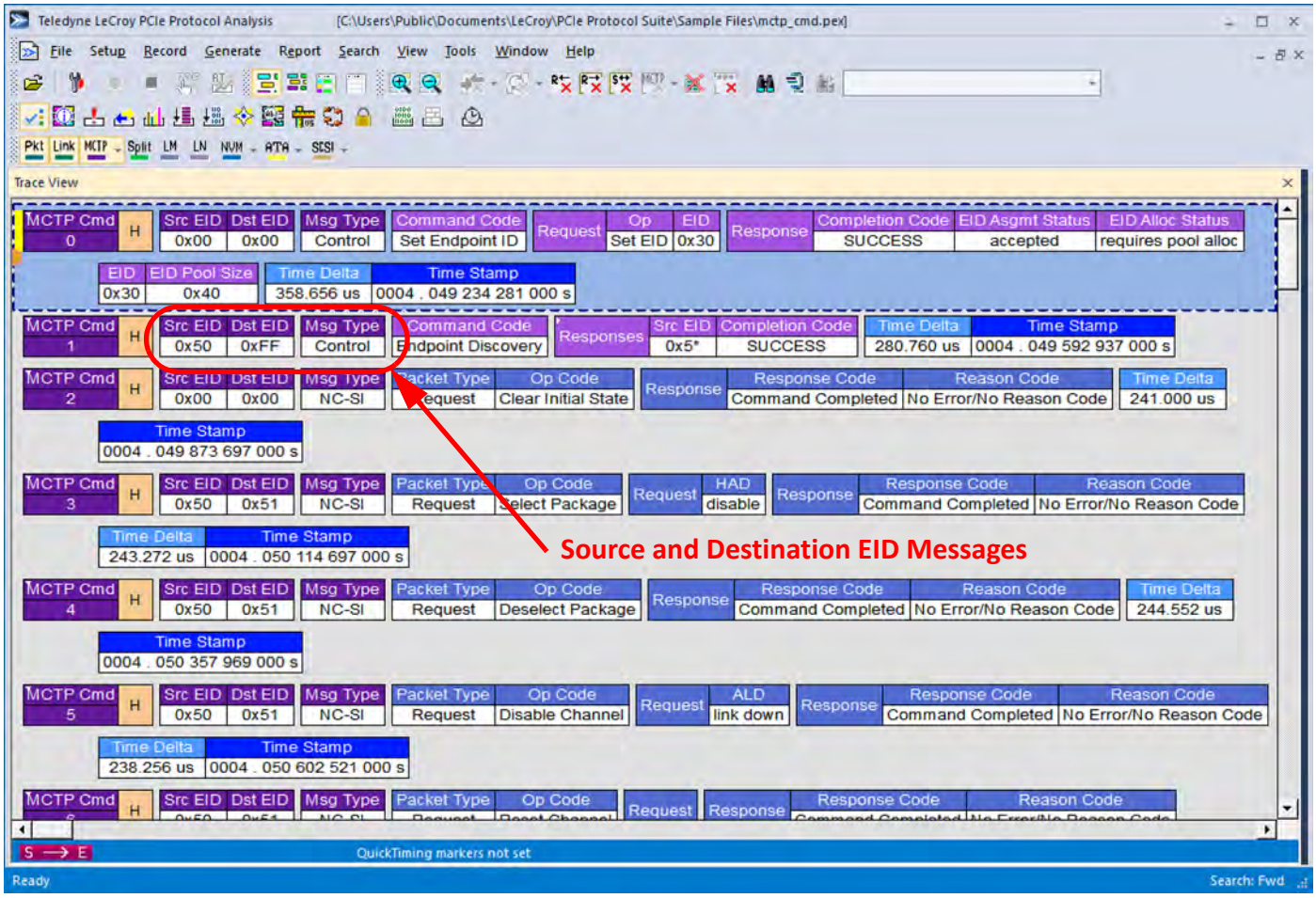


Figure 9.114: MCTP Messages Types and IC Cells Decoded

The colors of the MCTP Messages can be seen in the Display Options. See Figure 9.156 on page 657

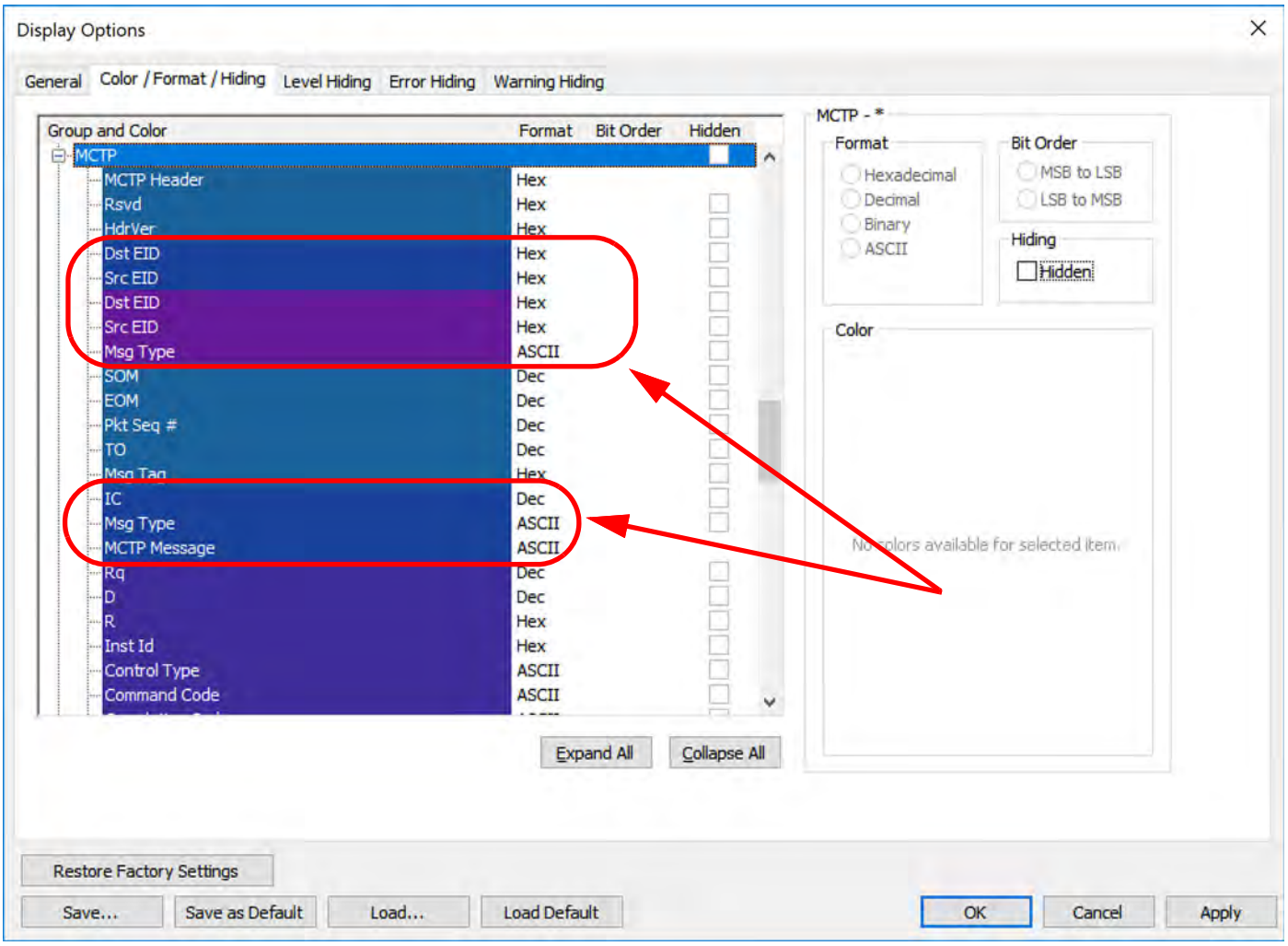


Figure 9.115: MCTP Commands and Transaction Colors from Display Options

9.11.15 Decoding MCTP Messages with SMBus Traffic

The System Management Bus (abbreviated to SMBus or SMB) is a single-ended simple two-wire bus for the purpose of lightweight communication. Most commonly it is found in computer motherboards for communication with the power source for ON/OFF instructions.

It is derived from I²C for communication with low-bandwidth devices on a motherboard, especially power related chips such as a laptop's rechargeable battery subsystem (see Smart Battery System). Other devices might include temperature, fan or voltage sensors, lid switches and clock chips. PCI add-in cards may connect to an SMBus segment.

A device can provide manufacturer information, indicate its model/part number, save its state for a suspend event, report different types of errors, accept control parameters and return status. The SMBus is generally not user configurable or accessible. Although SMBus devices usually can't identify their functionality, a new PMBus coalition has extended SMBus to include conventions allowing that.

The Summit T416 or Summit T48 can capture SMBus traffic and display it as part of an MCTP message along with normal PCIe Data traffic, as shown in Figure 9.116 and Figure 9.117 on page 618.

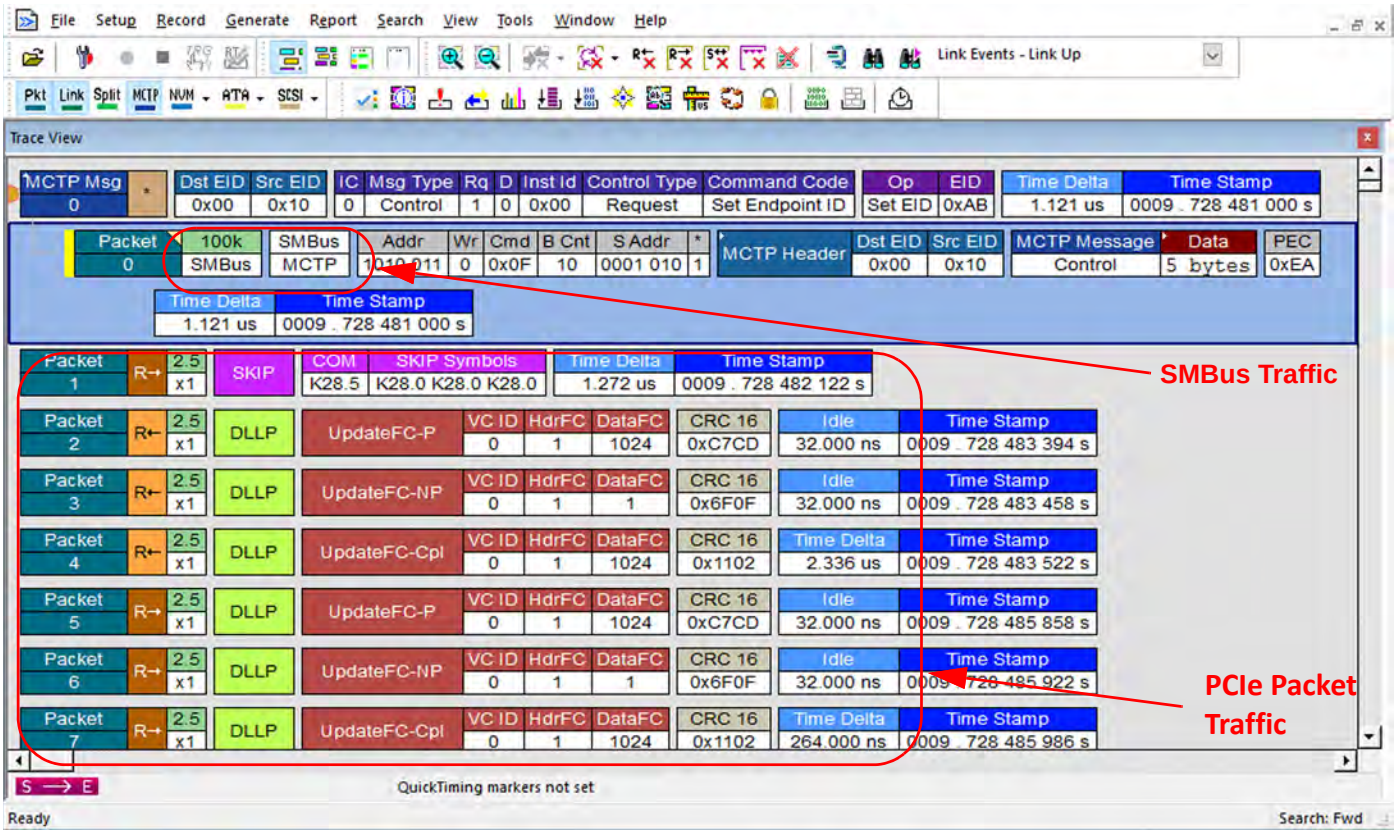


Figure 9.116: MCTP Message with SMBus Sideband Traffic and PCIe Packet Traffic

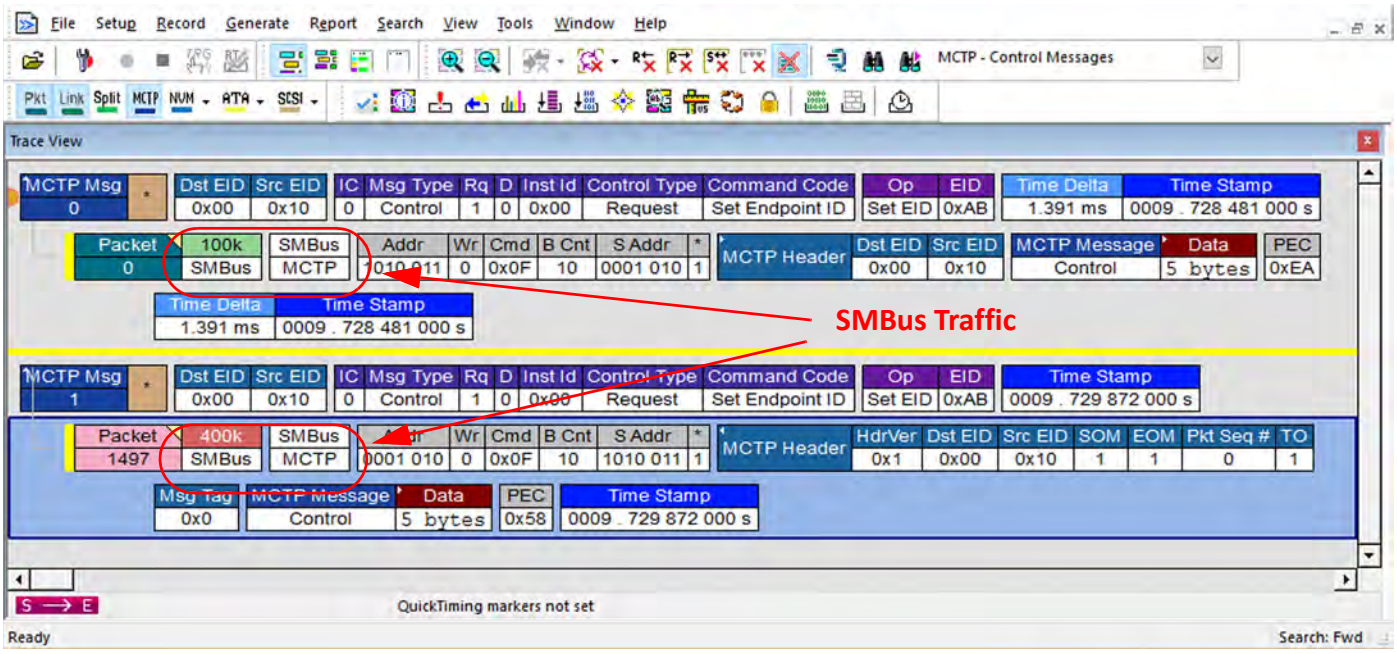


Figure 9.117: SMBus Traffic within two MCTP Messages

Sideband Traffic: Displayed or Hidden

You can decide to Display or Hide Sideband traffic (this includes SMBus traffic) by selecting the Hide Sideband icon in the toolbar. This will Hide the SMBus Traffic. Figure 9.118 shows Sideband traffic displayed. Figure 9.119 on page 620 shows the SMBus traffic Hidden.

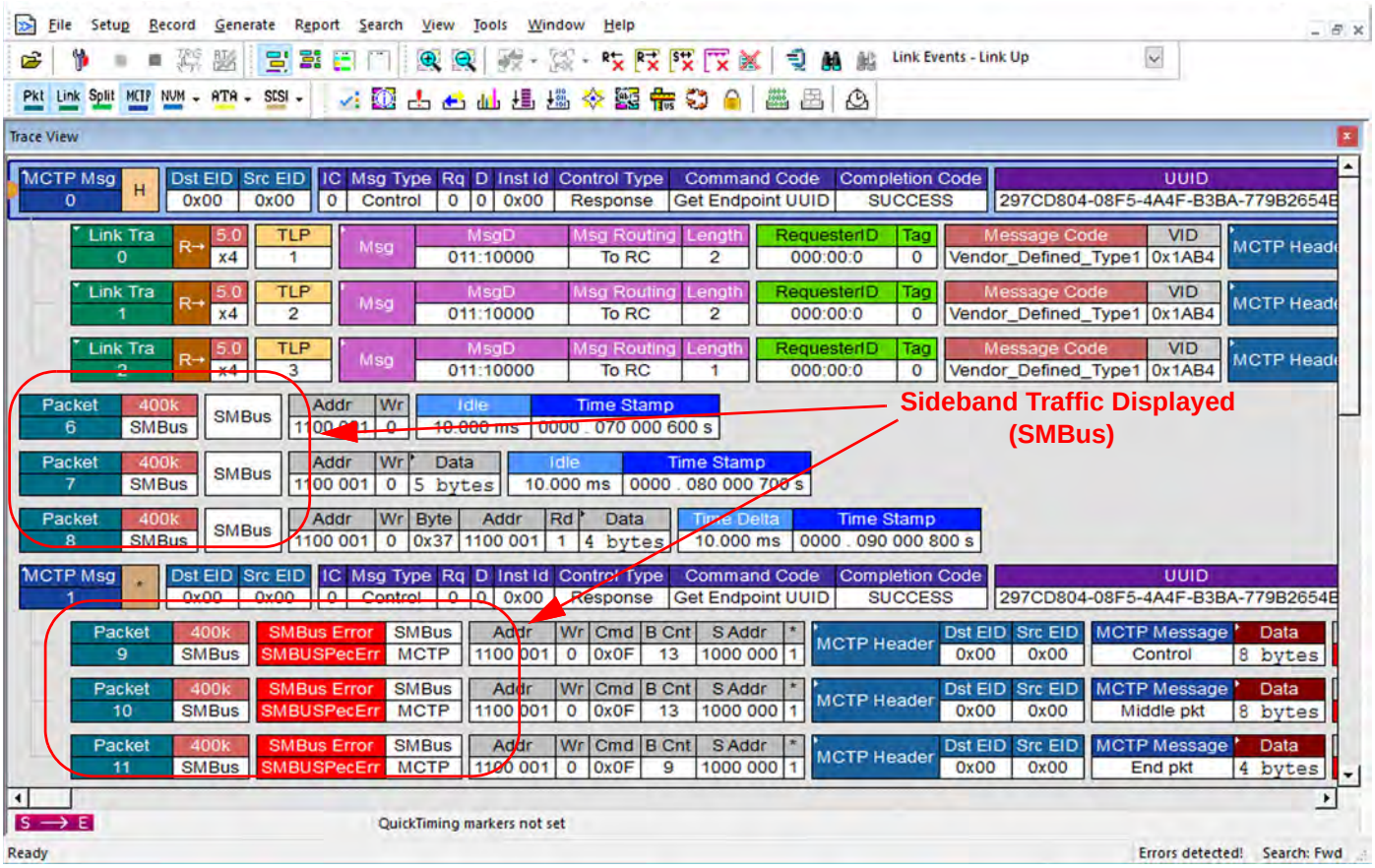


Figure 9.118: Displaying Sideband Traffic (SMBus)

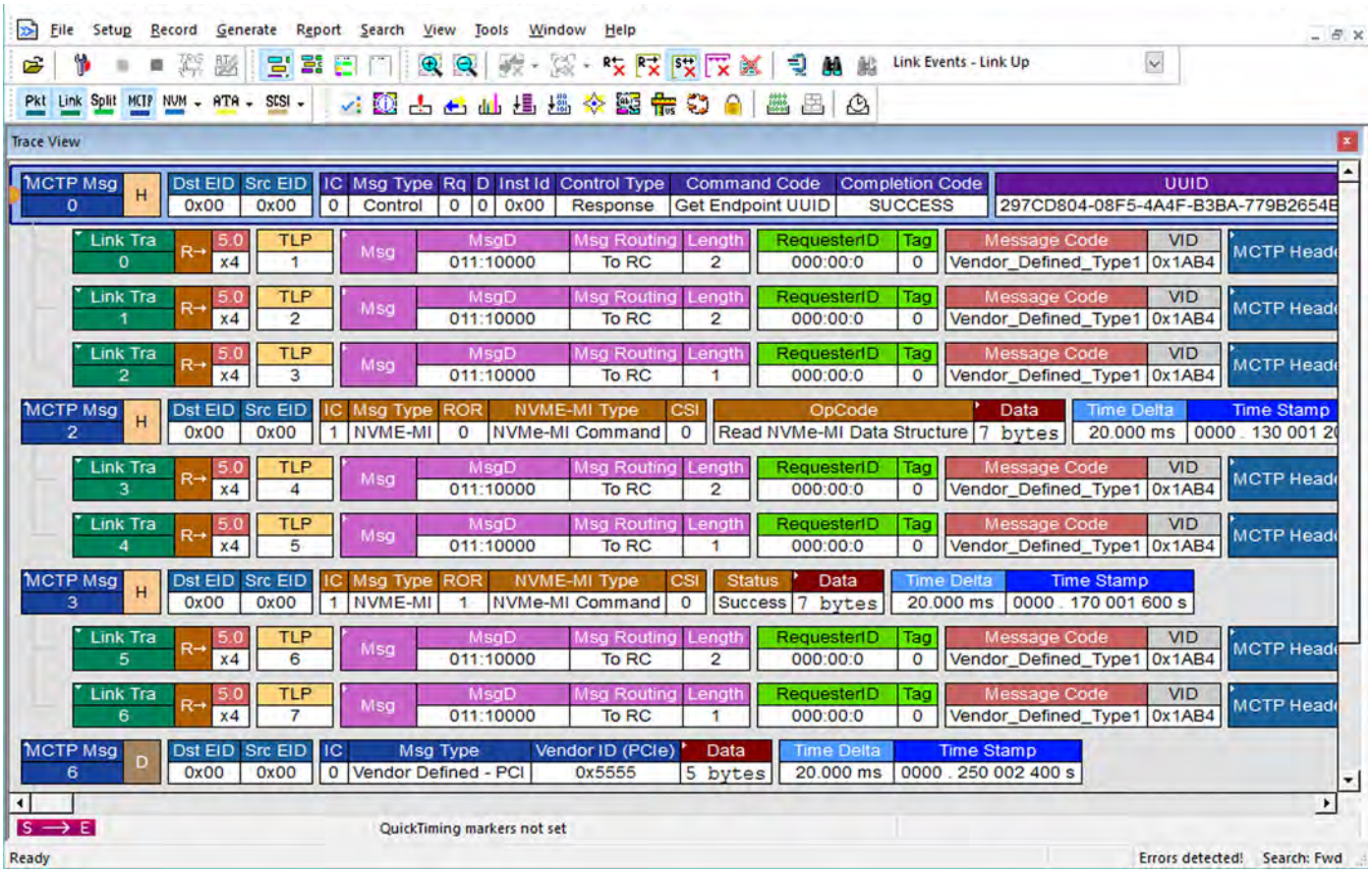


Figure 9.119: Hiding Sideband Traffic (SMBus)

If you compare Figure 9.118 on page 619 and Figure 9.119 you'll see that all the SMBus traffic has been hidden in Figure 9.119. Specifically, Packets 6 - Packet 8 are hidden, which had SMBus traffic and the SMBus traffic in Packets 9 and 10, which were part of MCTP Message 1 are also hidden.

SMBus Errors

The Summit T416 or Summit T48 analyzer can detect a wide variety of SMBus errors (as shown in Figure 9.120 and Figure 9.121 on page 622).

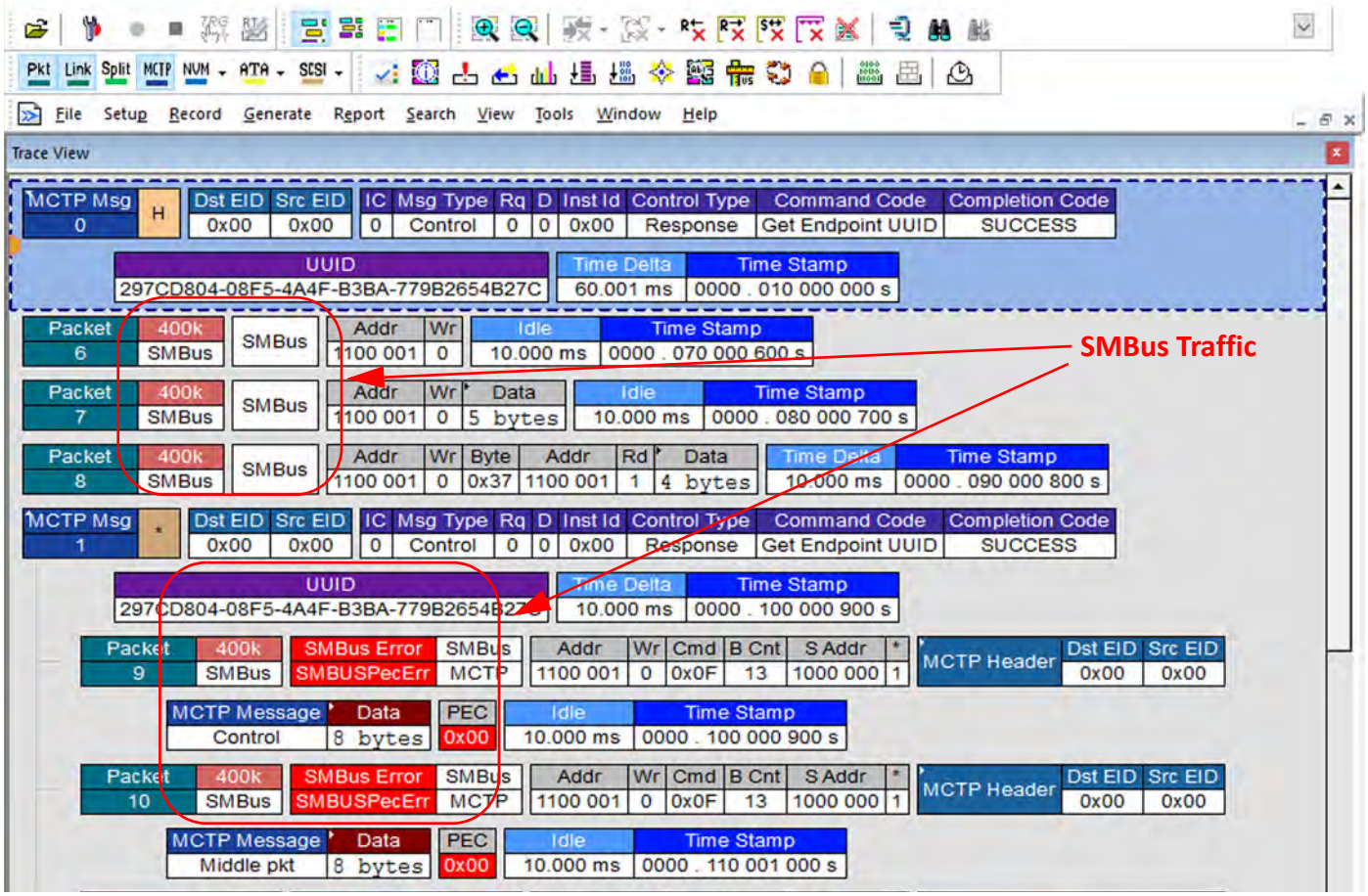


Figure 9.120: SMBus Traffic within two MCTP Messages with Errors

SMBus Error Tooltip

If you scroll over each SMBus Error a tooltip with a detailed explanation of the error will popup. See Figure 9.121.

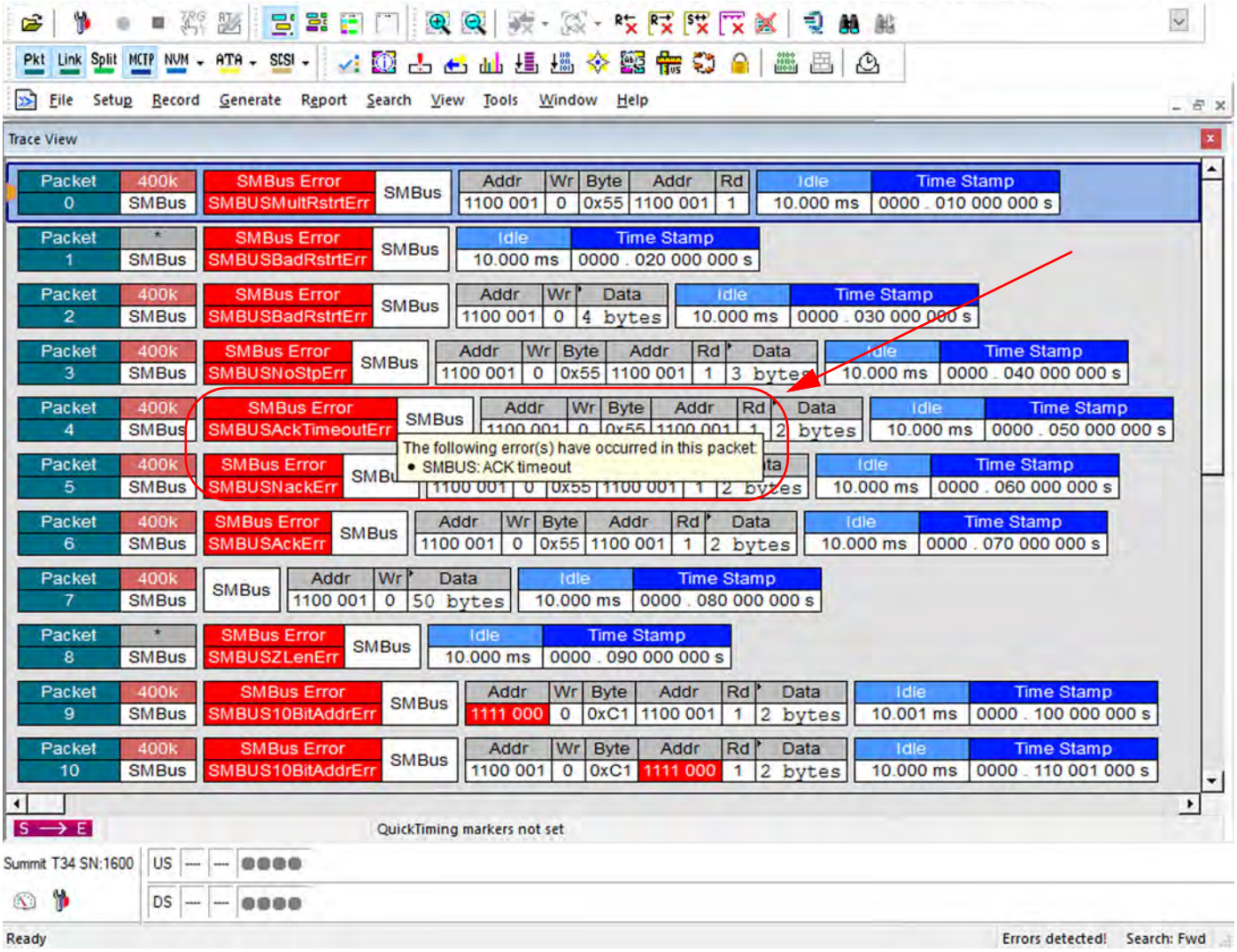


Figure 9.121: Decoding SMBus with Errors

Traffic Summary Report: SMBus Errors

Another way of displaying the SMBus errors is to select the Traffic Summary Report (as shown in Figure 9.122).

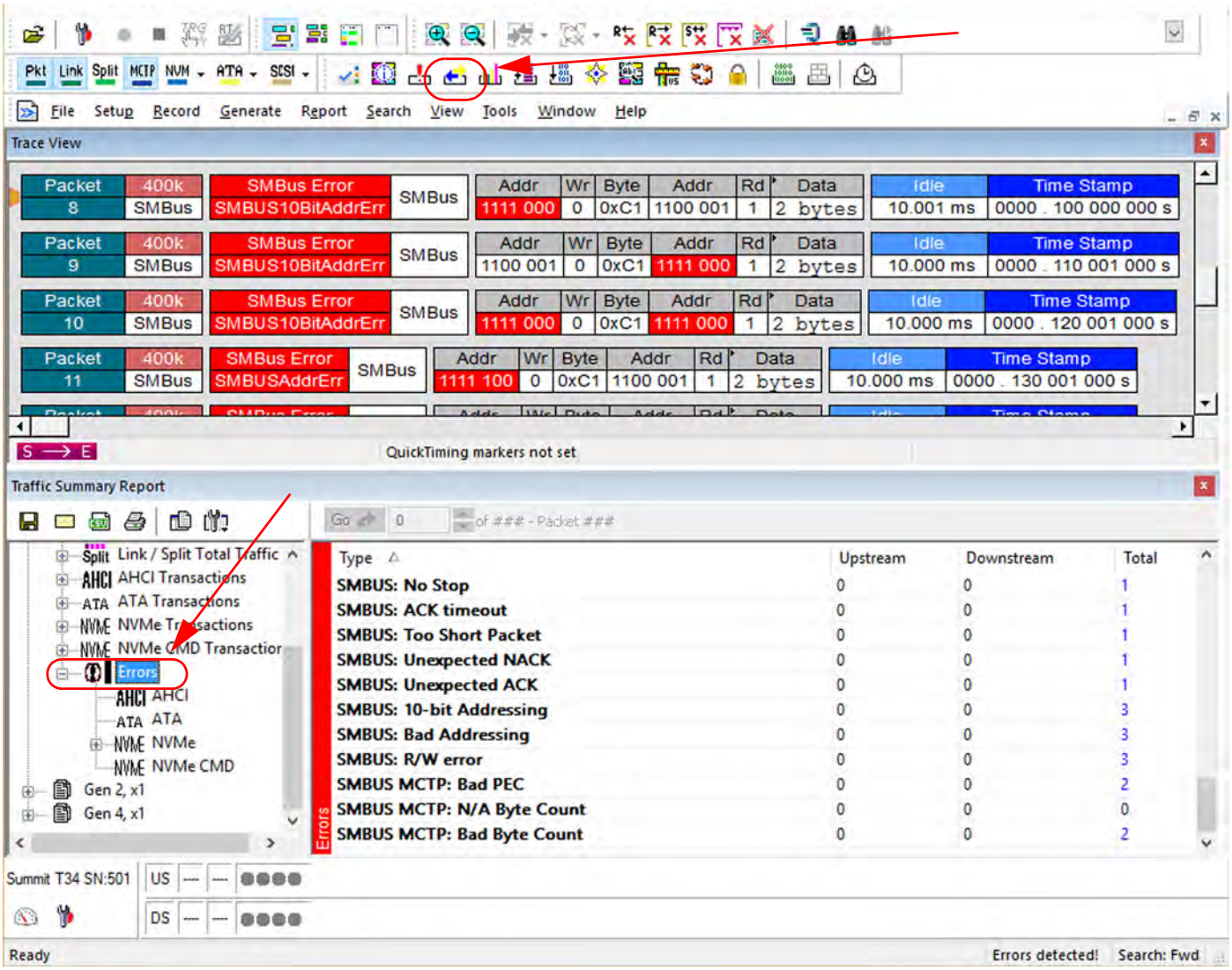


Figure 9.122: Traffic Summary Report: SMBus Errors

The complete set of SMBus errors that the Summit T416 or Summit T48 can detect is contained in the table below: Table 9.13.

TABLE 9.13: SMBus Errors

Bus Error	Description
SMBUSLongPktErr	SMBUS: Too Long Packet
SMBUSMultRstrtErr	SMBUS: More Than One Restart
SMBUSBadRstrtErr	SMBUS: Bad Restart
SMBUSNoStpErr	SMBUS: No Stop
SMBUSAckTimeoutErr	SMBUS: ACK Timeout
SMBUSZLenErr	SMBUS: Too Short Packet
SMBUSNackErr	SMBUS: Unexpected NACK
SMBUSAckErr	SMBUS: Unexpected ACK
SMBUS10BitAddrErr	SMBUS: 10-bit Addressing
SMBUSAddrErr	SMBUS: Bad Addressing
SMBUSRwErr	SMBUS: R/W error
SMBUSPecErr	SMBUS MCTP: Bad PEC
SMBUSNaByteCntErr	SMBUS MCTP: N/A Byte Count
SMBUSByteCntErr	SMBUS MCTP: Bad Byte Count

9.11.16 Decoding SMBus with Address Resolution Protocol (ARP)

The PCIe Protocol Analysis can decode SMBus traffic with Address Resolution Protocol as shown below in Figure 9.123.

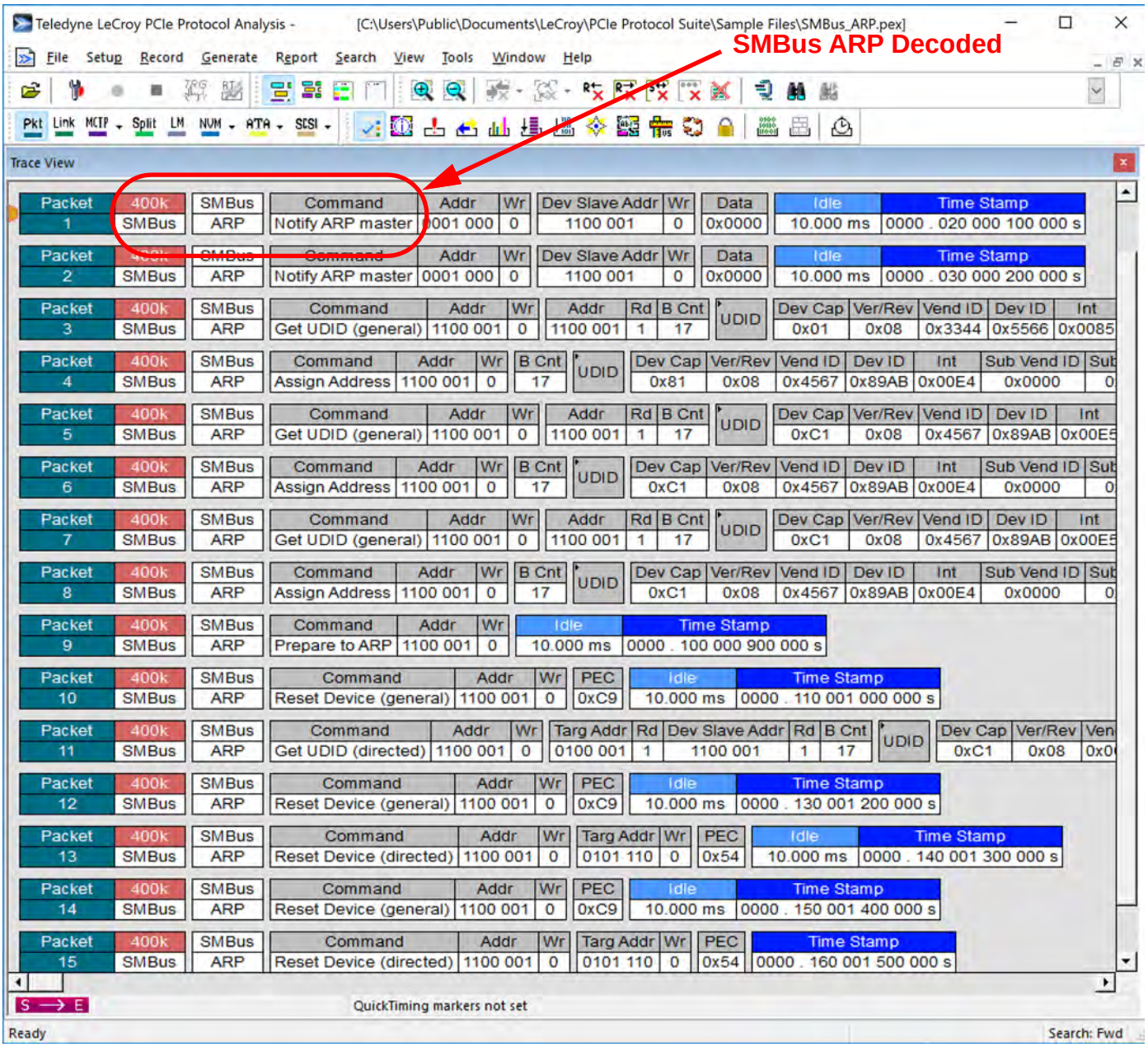


Figure 9.123: SMBus Address Resolution Protocol Decoded

9.11.17 Decoding MCTP Traffic with Vendor Defined Messages (VDM)

The PCIe Protocol Analysis can decode MCTP traffic with Vendor Defined Messages (VDM) as shown below in Figure 9.124.

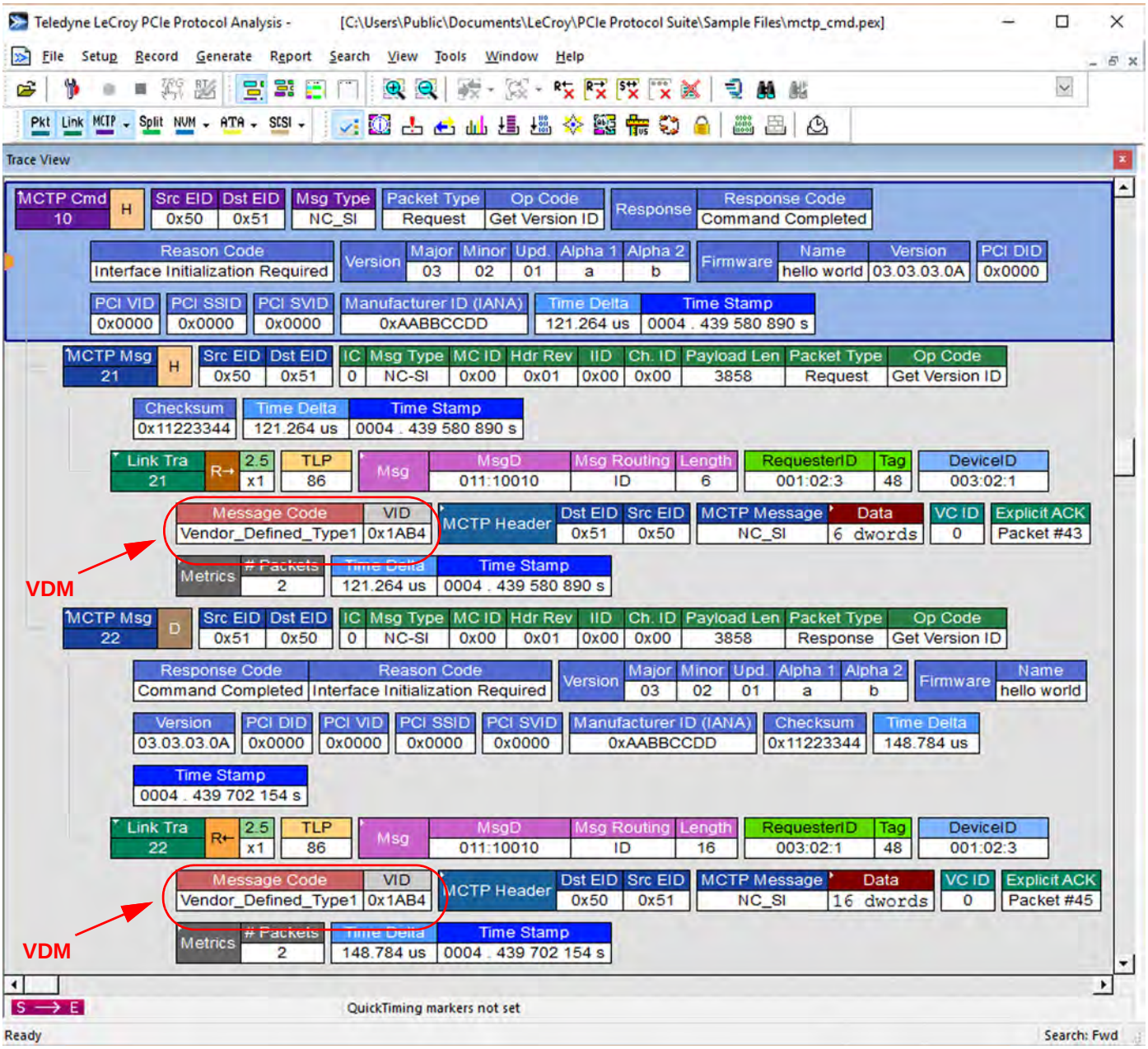


Figure 9.124: MCTP Traffic: Decoding Vendor Defined Messages (VDM)

9.11.18 Decoding Side Band Signals

There are a number of side band signals which are decoded by the PCIe Protocol Analysis and will be displayed in the Trace View:

- PERST# (Asserted and Deasserted)
- WAKE# (Asserted and Deasserted)
- CLKREQ# (Asserted and Deasserted)

These signals are displayed as Link Events. They can be found in the trace by using the **Search -> Go to -> Link Event** function from the Main Toolbar.

Since these signals have no direction they will be displayed once in the upstream direction and once in the downstream direction.

Note: If left floating in the bus, PERST#, WAKE# and CLKREQ# may show up in the trace as events. Make sure these signals are pulled up according to the specification. During beacon phase there might be transitions of WAKE# that will show up in the trace.

9.11.19 PMUX Channel ID Found and PMUX Packet Error Decoded in Trace

In the trace both the PMUX Channel ID was found and a Packet PMUX Error was decoded. See Figure 9.125.

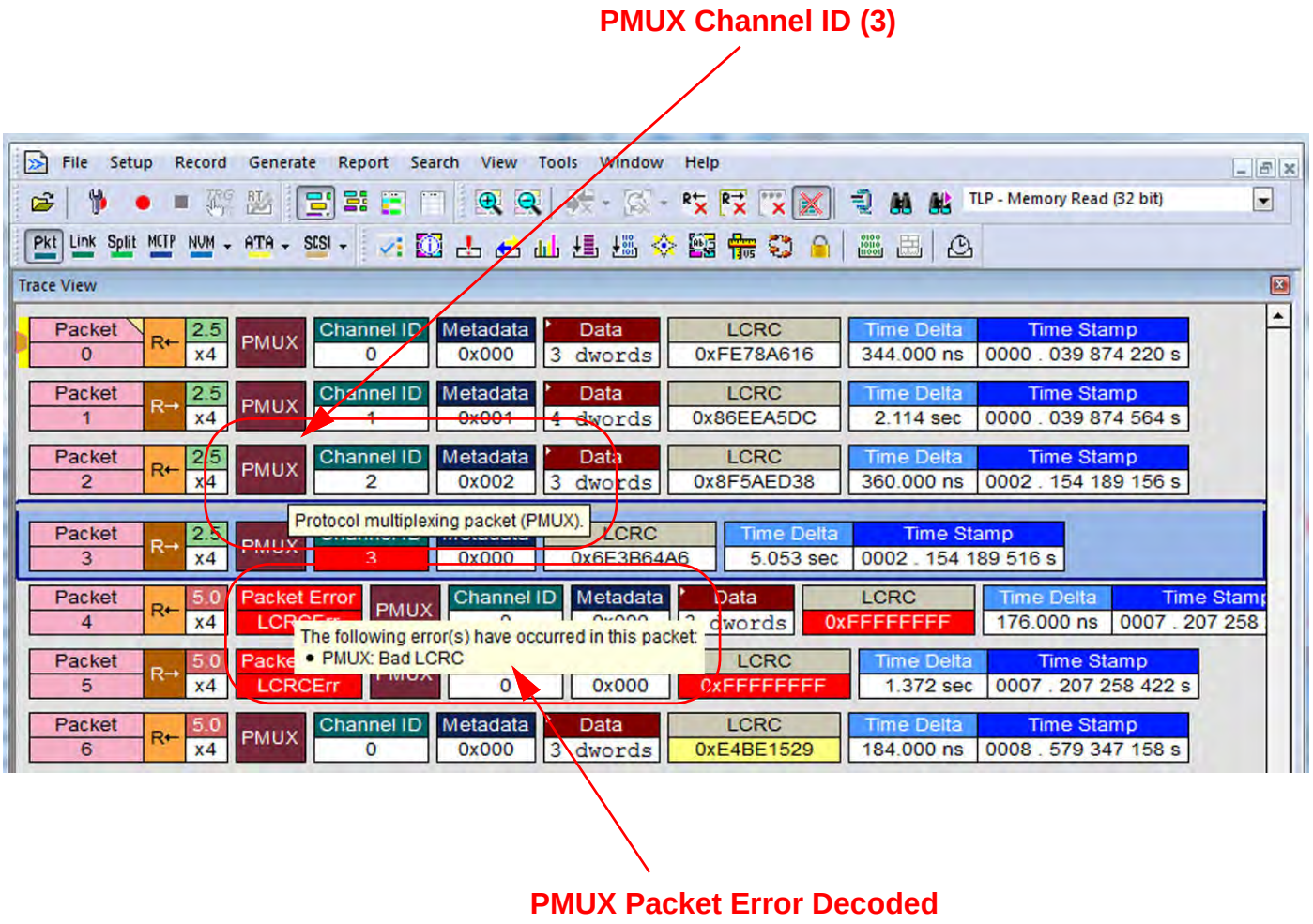


Figure 9.125: PMUX Channel ID (3) Found in Trace and Packet Error Decoded

9.11.20 Decoding Traces with Different Class Codes

PCIe Protocol Analysis initially assumes all traces have unknown class codes and that the decoder selected and trace class codes are the same. If after decoding the trace, the class codes of the trace and the decoder selected are different, a warning message pops up showing the correct class code of the trace.

9.11.20.1 Example: Loading an NVMe Trace and Decoding for ATA

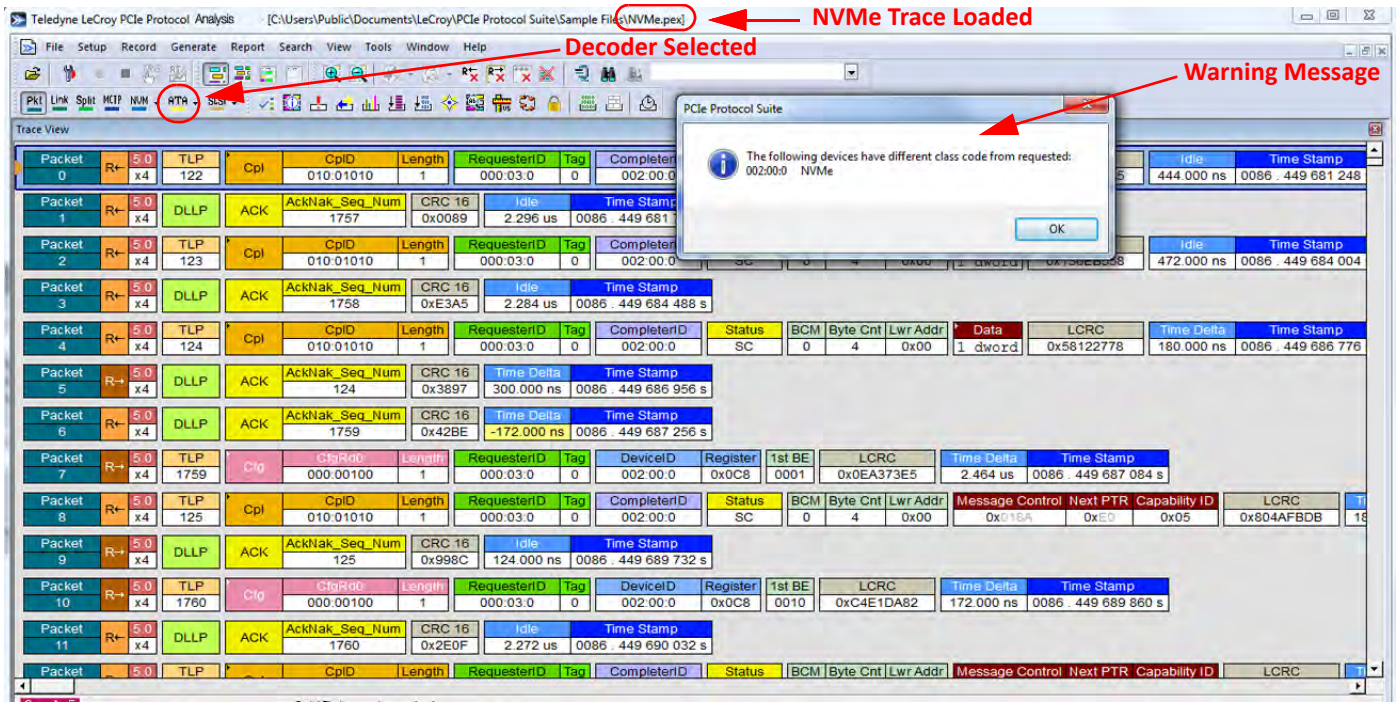


Figure 9.126: NVMe Trace Loaded Different Than ATA Decoder Selected

9.11.20.2 Example: Loading a PQI Trace and Decoding for NVMe

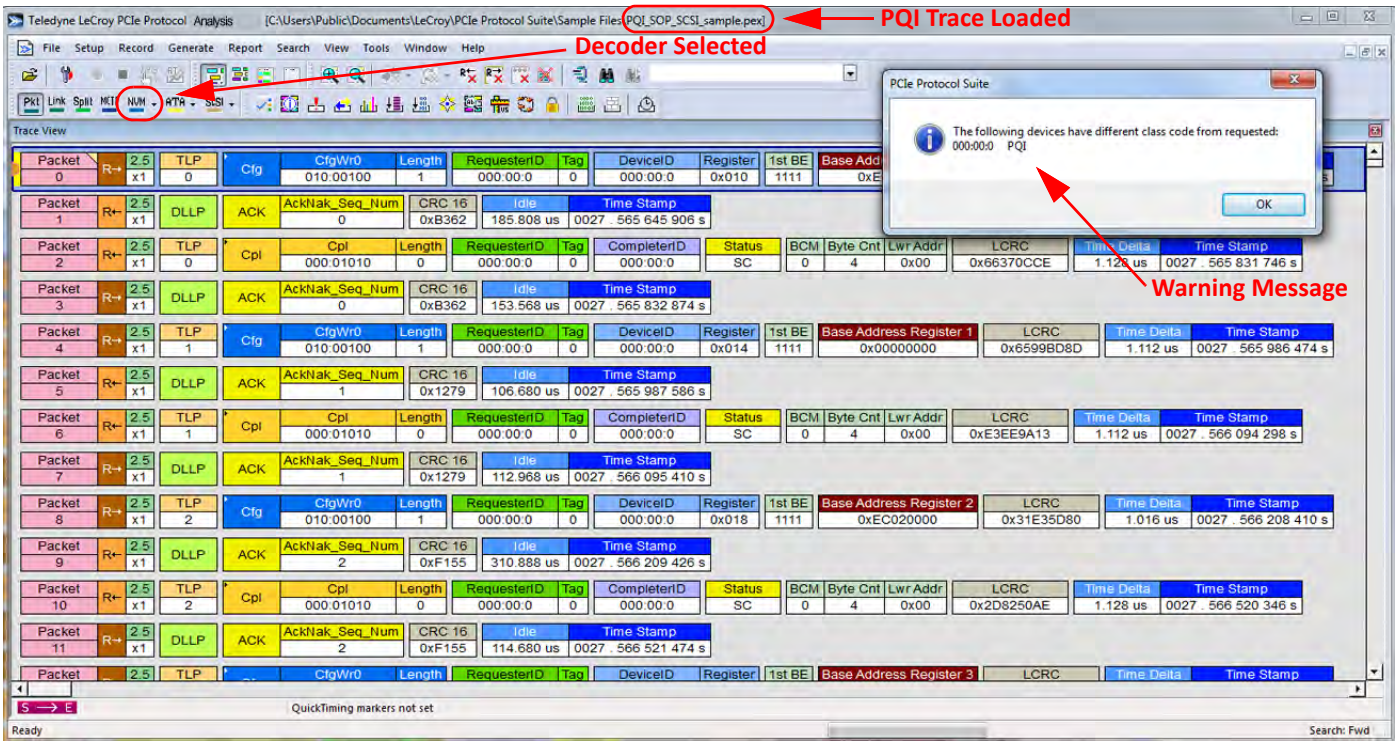


Figure 9.127: PQI Trace Loaded Different Than NVMe Decoder Selected

9.11.21 Data Link Features

The Summit M5x can decode Data Link Features as shown in Figure 9.128.

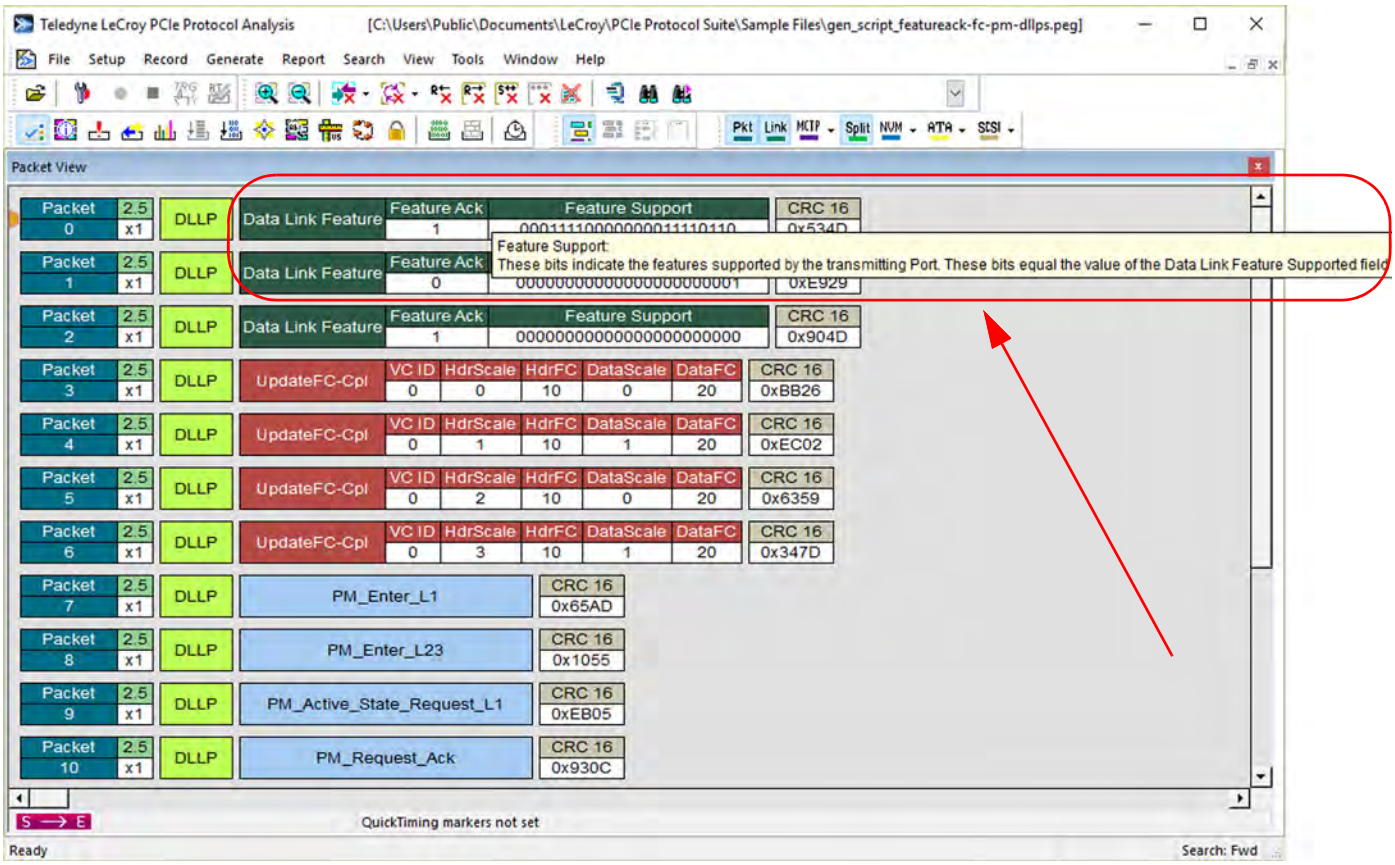


Figure 9.128: Decoding Data Link Features

The supported Data Link Features are defined in the PCIe Specification:

PCI Express® Base Specification Revision 4.0 Version 0.7 dated 11 November 2016.

They are outlined in Table 3.1 on page 202 and are shown below:

TABLE 9.14: Data Link Feature Supported Bit Definition

Bit Location	Description
0	**Scaled Flow Control** – indicates support for Scaled Flow Control. Scaled Flow Control must be supported in Ports that support 16.0 GT/s or higher operation.
Others	Reserved

9.11.22 Decode for NVMe 1.3c Specification

The PCI Express Analysis includes decoding for the following NVMe 1.3c Specification:

- Command Specific Status Code
- Opcodes for Admin commands
- Doorbell Buffer Config commands
- Device Self-Test command
- Directive Receive command
- Directive Send command
- Firmware Commit
- Features
- Get Log Page
- Identify command
- NVMe-Mi Receive command
- NVMe-MI Send command
- Format NVM
- Sanitize command
- Write
- Write Zeros
- Identifier Format 7.10

Some examples are shown below (see Figure 9.129 through Figure 9.132 on page 635).

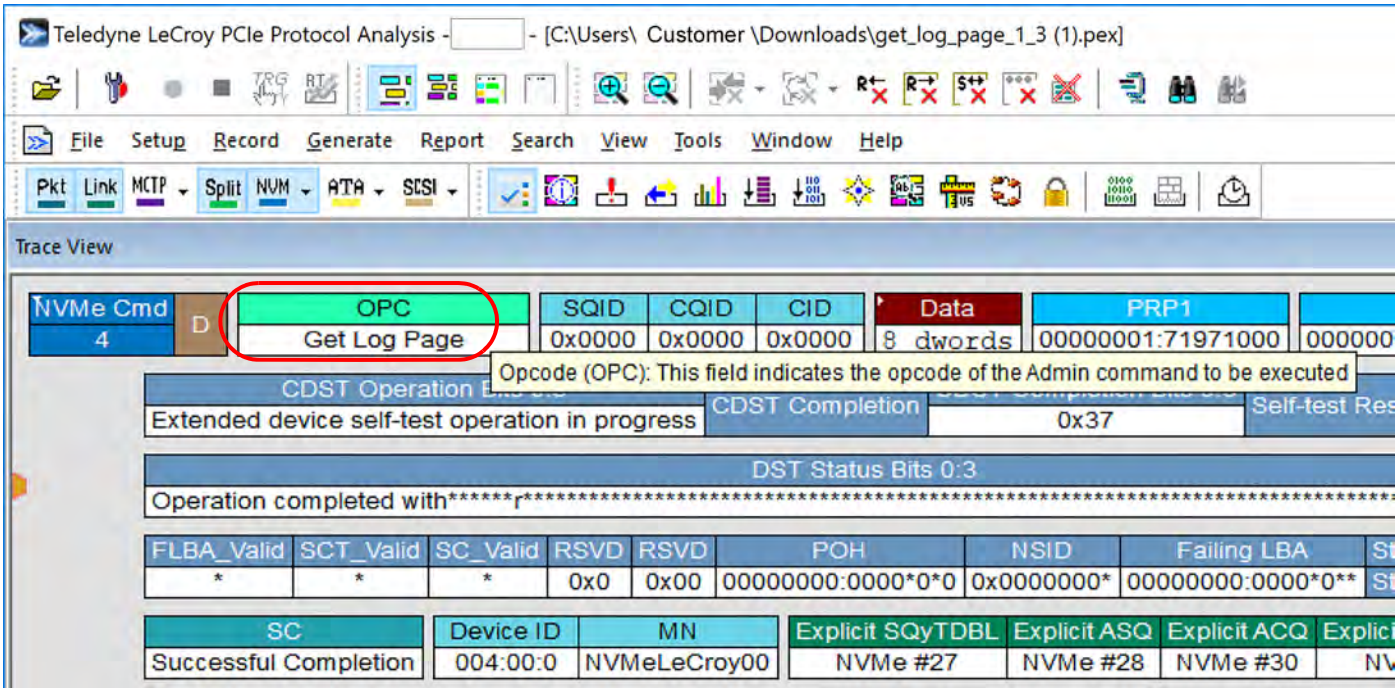


Figure 9.129: NVMe 1.3c Spec: Decodes --> Get Log Page

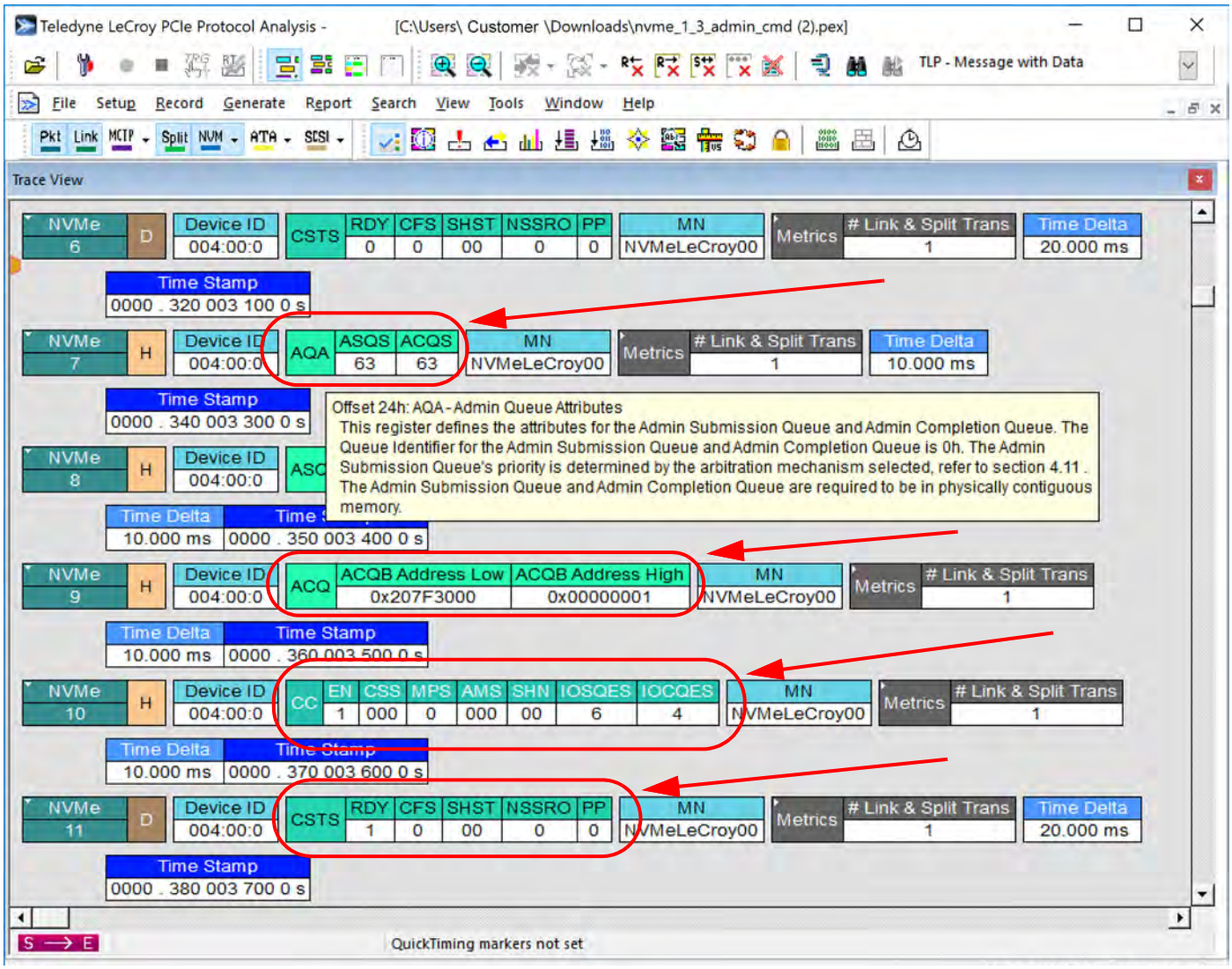


Figure 9.130: NVMe 1.3c Spec: Decodes --> Admin Commands

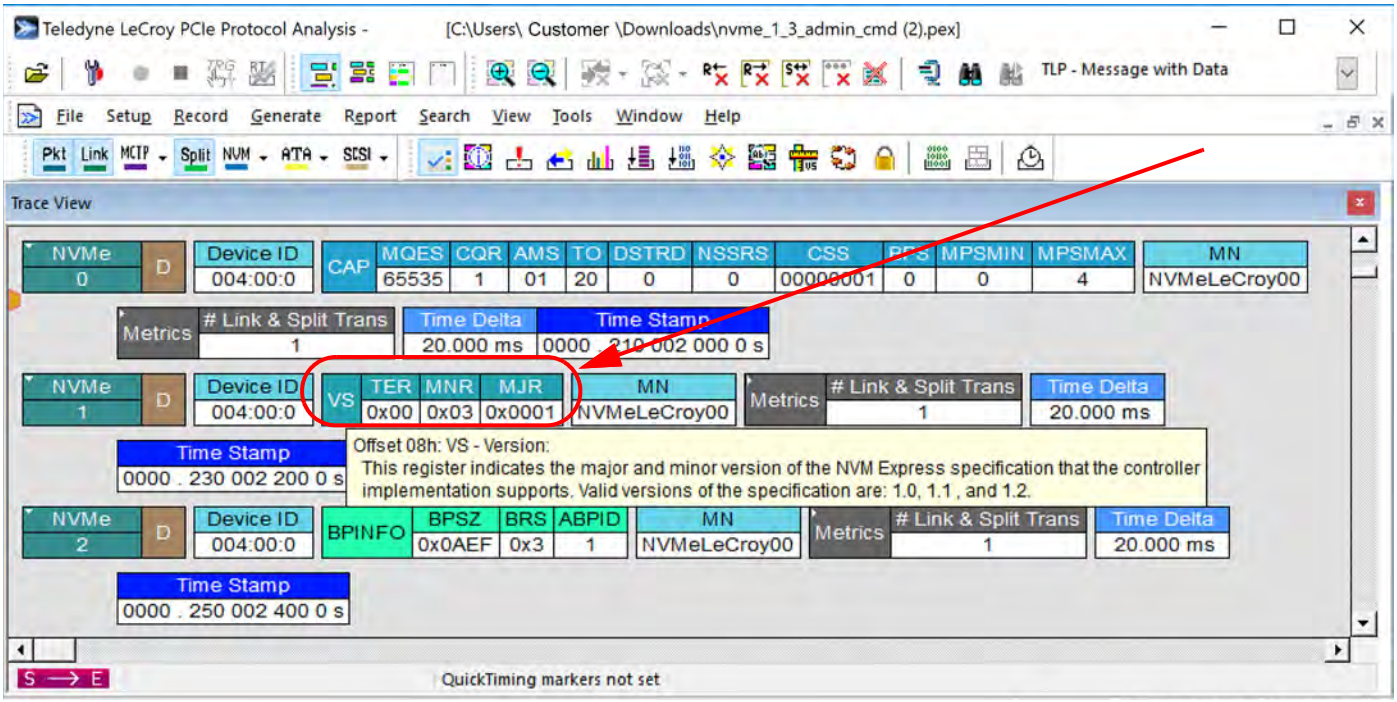


Figure 9.131: NVMe 1.3c Spec: Decodes --> Spec Version 1.3c

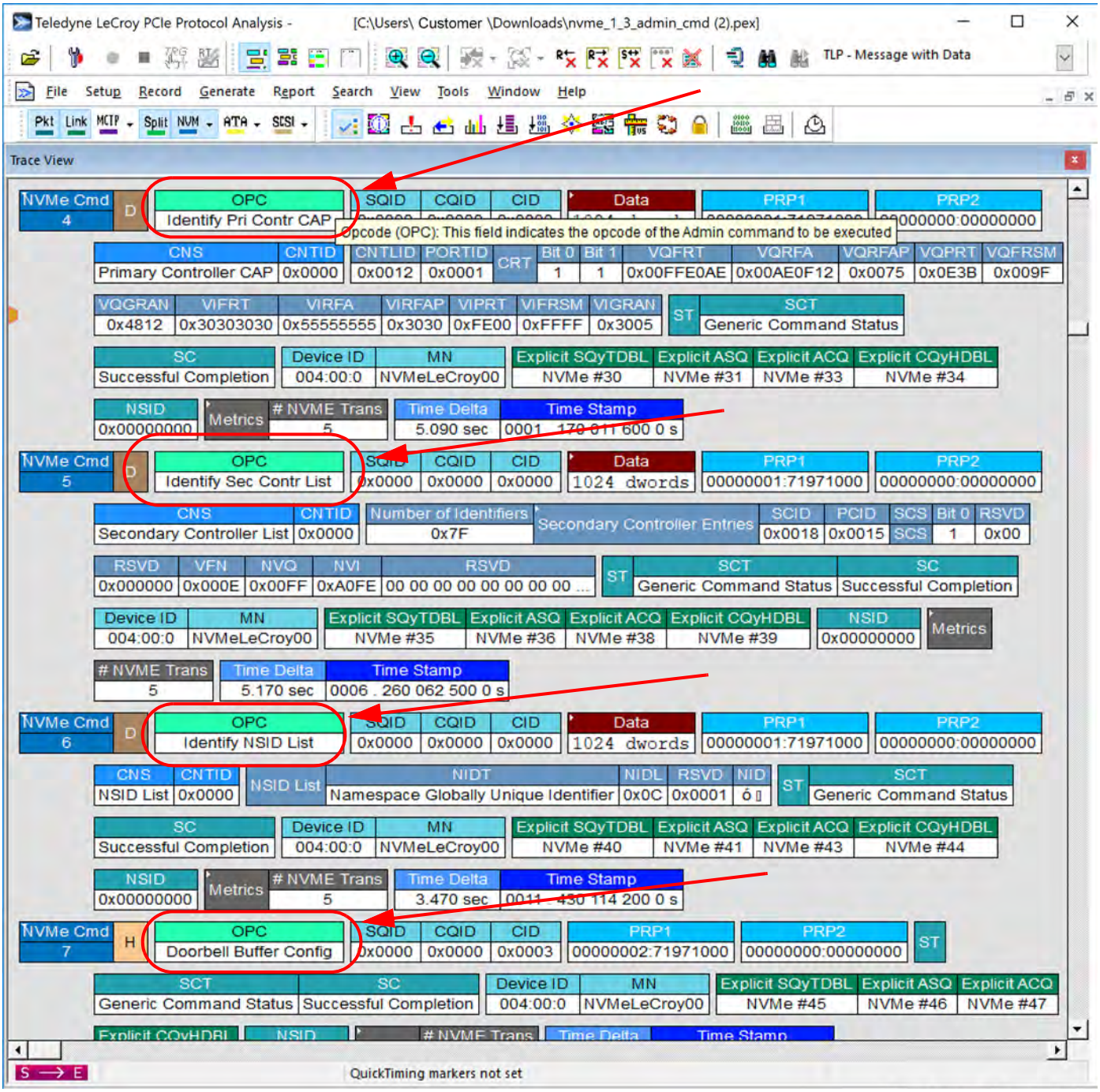


Figure 9.132: NVMe 1.3c Spec: Decodes --> Opcodes

9.11.23 NVMe Warning Messages

The PCIe Protocol Analysis software is capable of decoding the following NVMe Warning messages:

- Trace View
- Traffic Summary
- Search for NVMe Commands
- Search for NVMe Transactions
- Hiding Options

9.11.23.1 Trace View

If you decode for NVMe Commands and Transactions you'll see the following types of warning messages: See Figure 9.133, Figure 9.134 on page 637, Figure 9.135 on page 637.

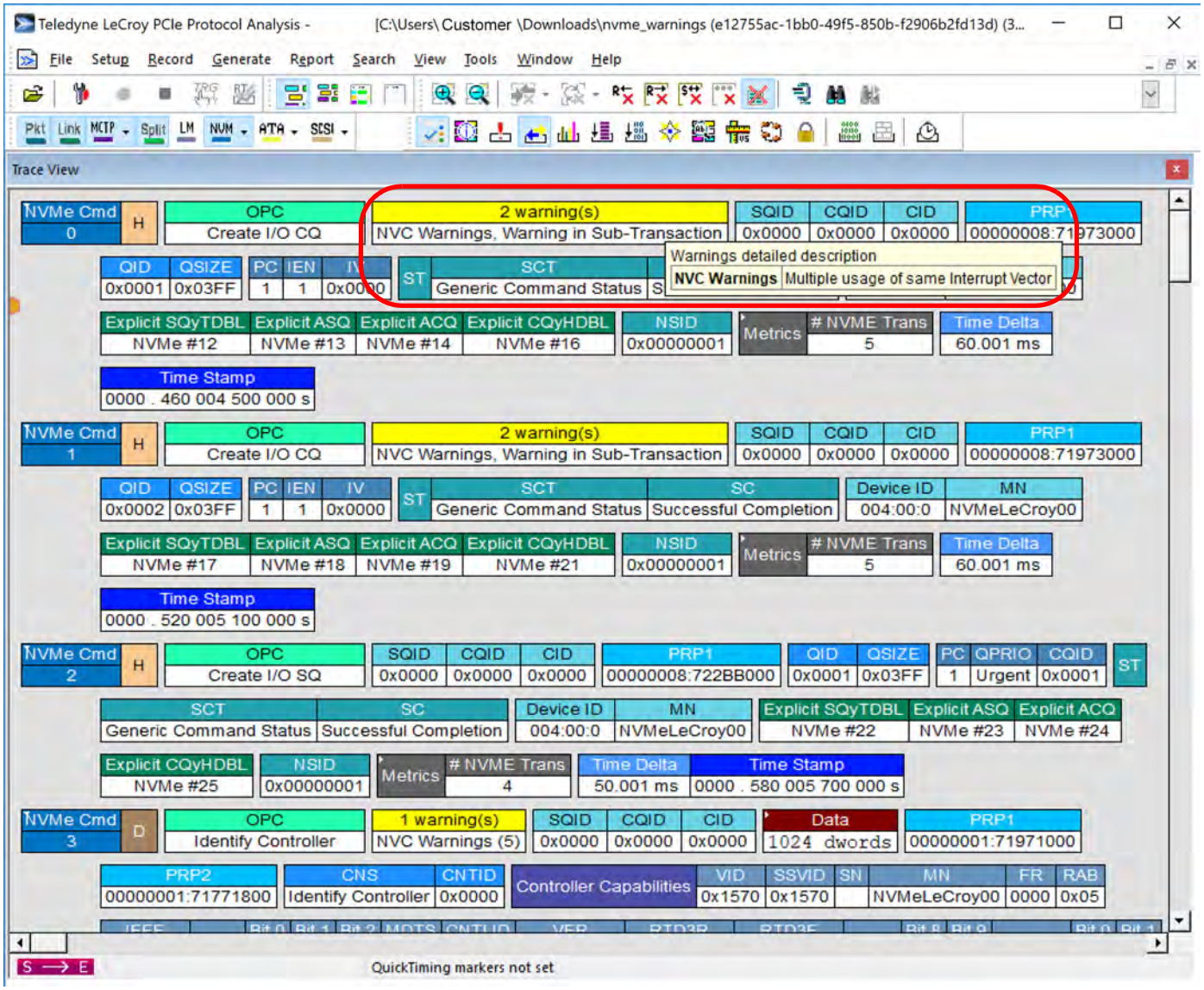


Figure 9.133: NVMe Command: Warning Message 1

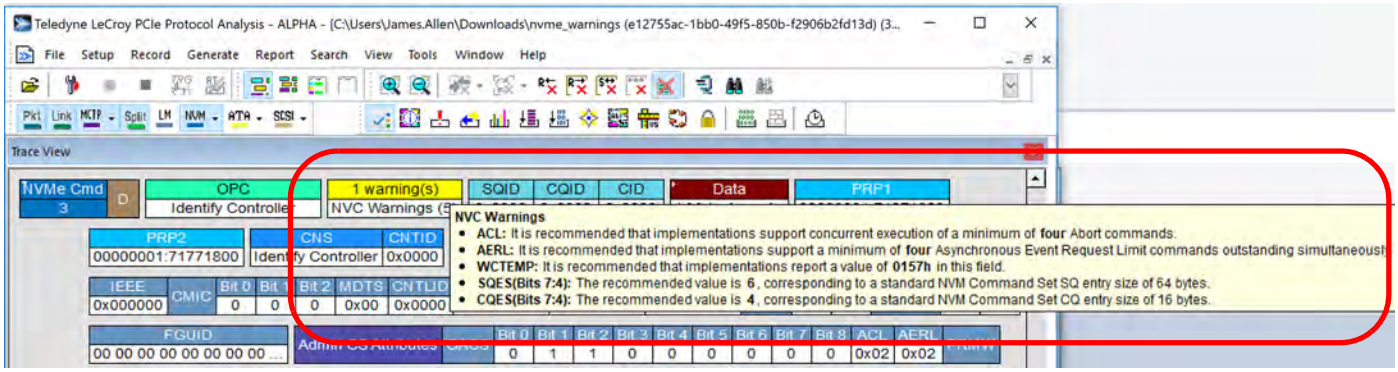


Figure 9.134: NVMe Command: Warning Message 2

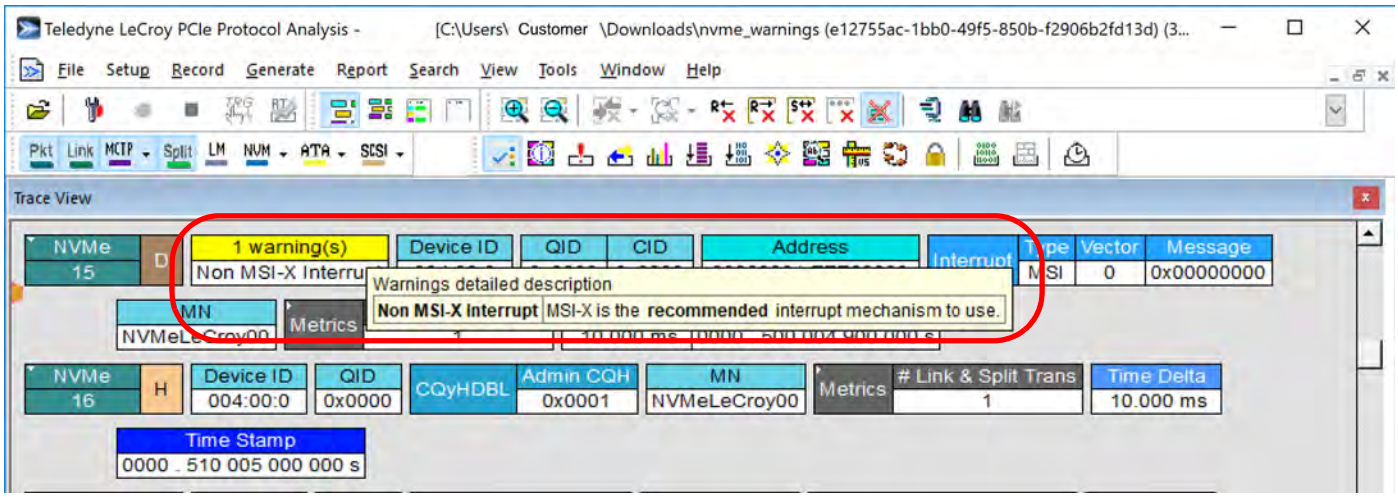


Figure 9.135: NVMe Transaction: Warning Message

9.11.23.2 Traffic Summary View

The NVMe Warning Messages can be seen in the Traffic Summary Reports (see Figure 9.136, Figure 9.137 on page 639 and Figure 9.138 on page 640) below:

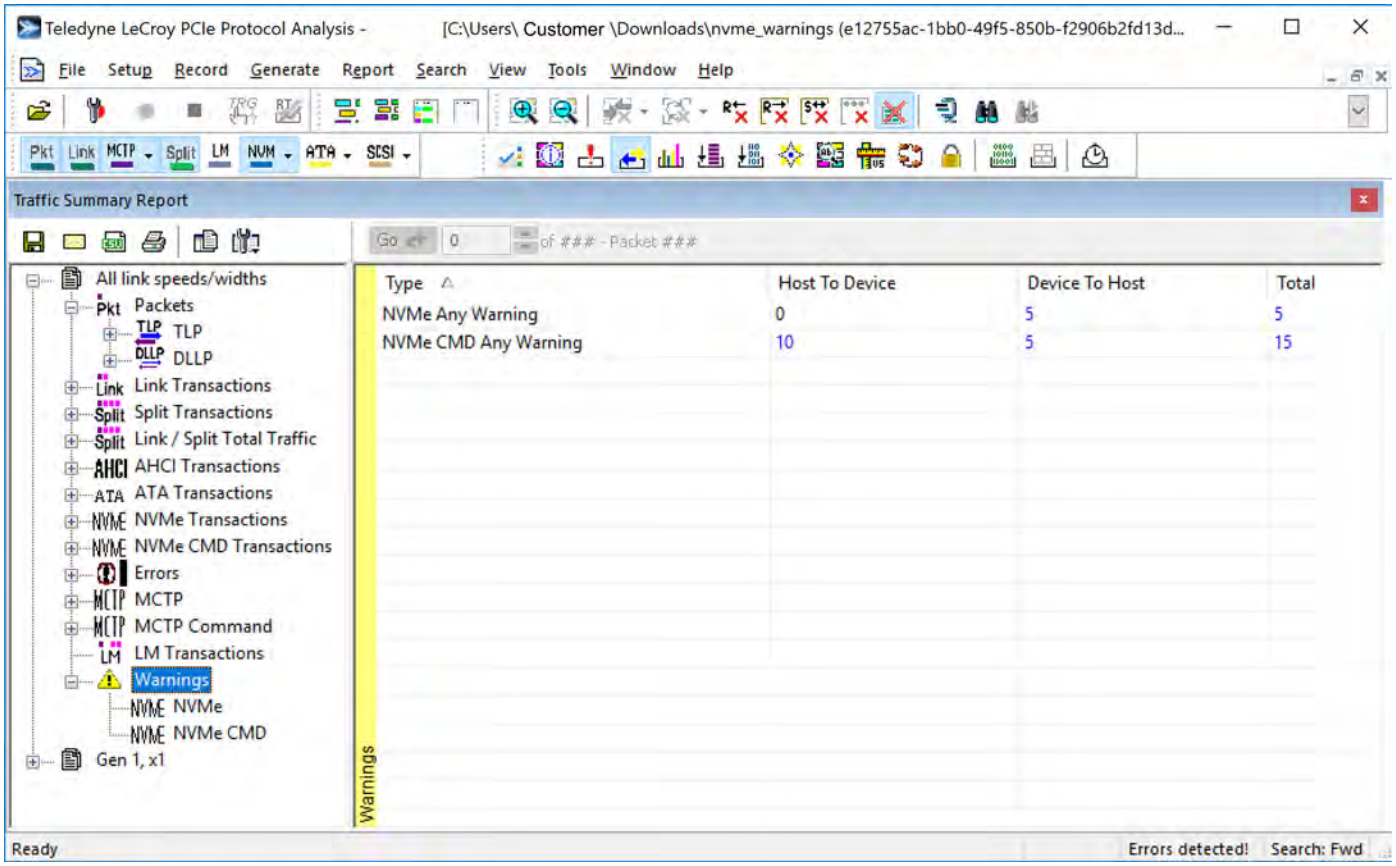


Figure 9.136: NVMe Warning Messages: Traffic Summary

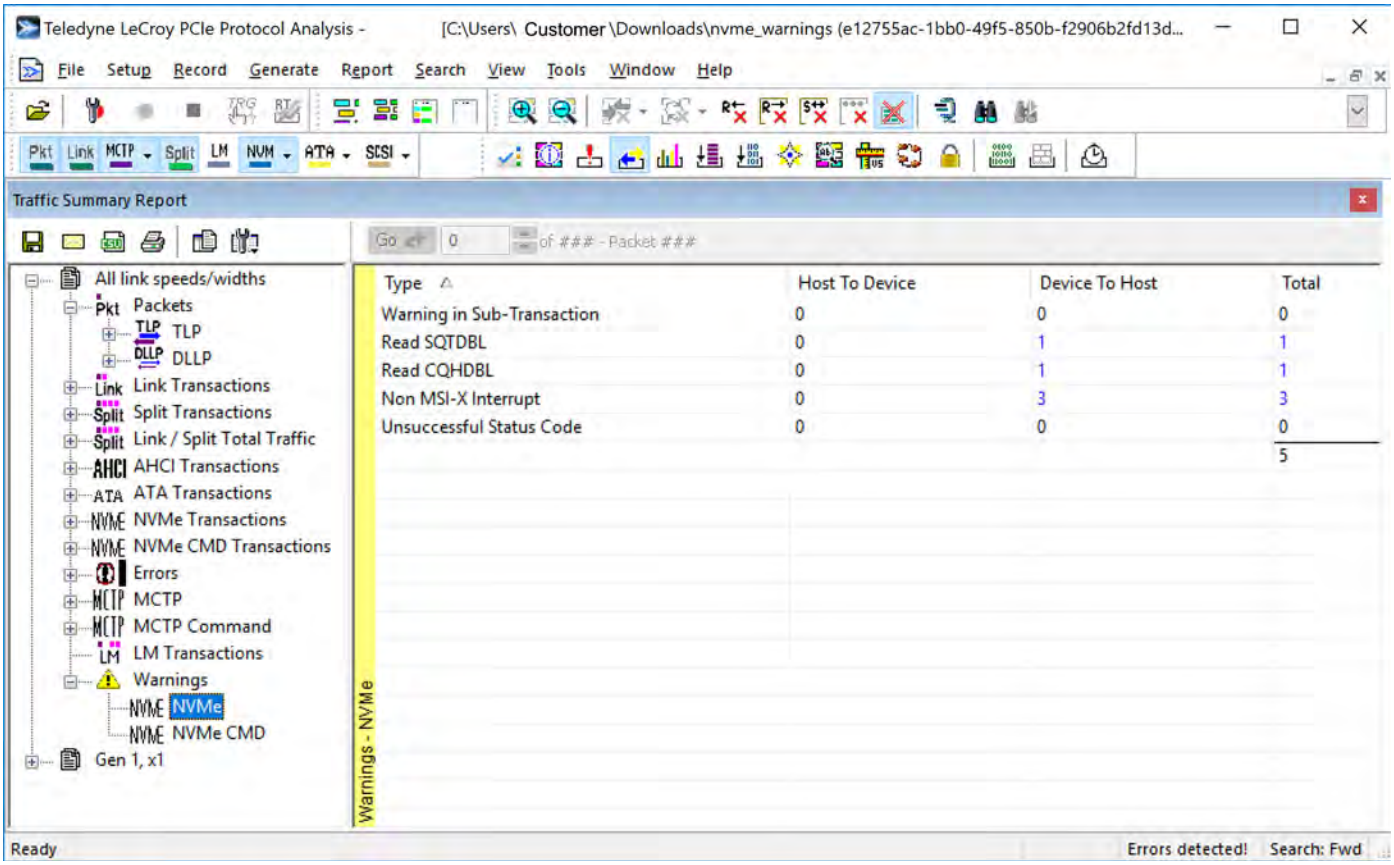


Figure 9.137: NVMe Warning Messages: Traffic Summary NVMe

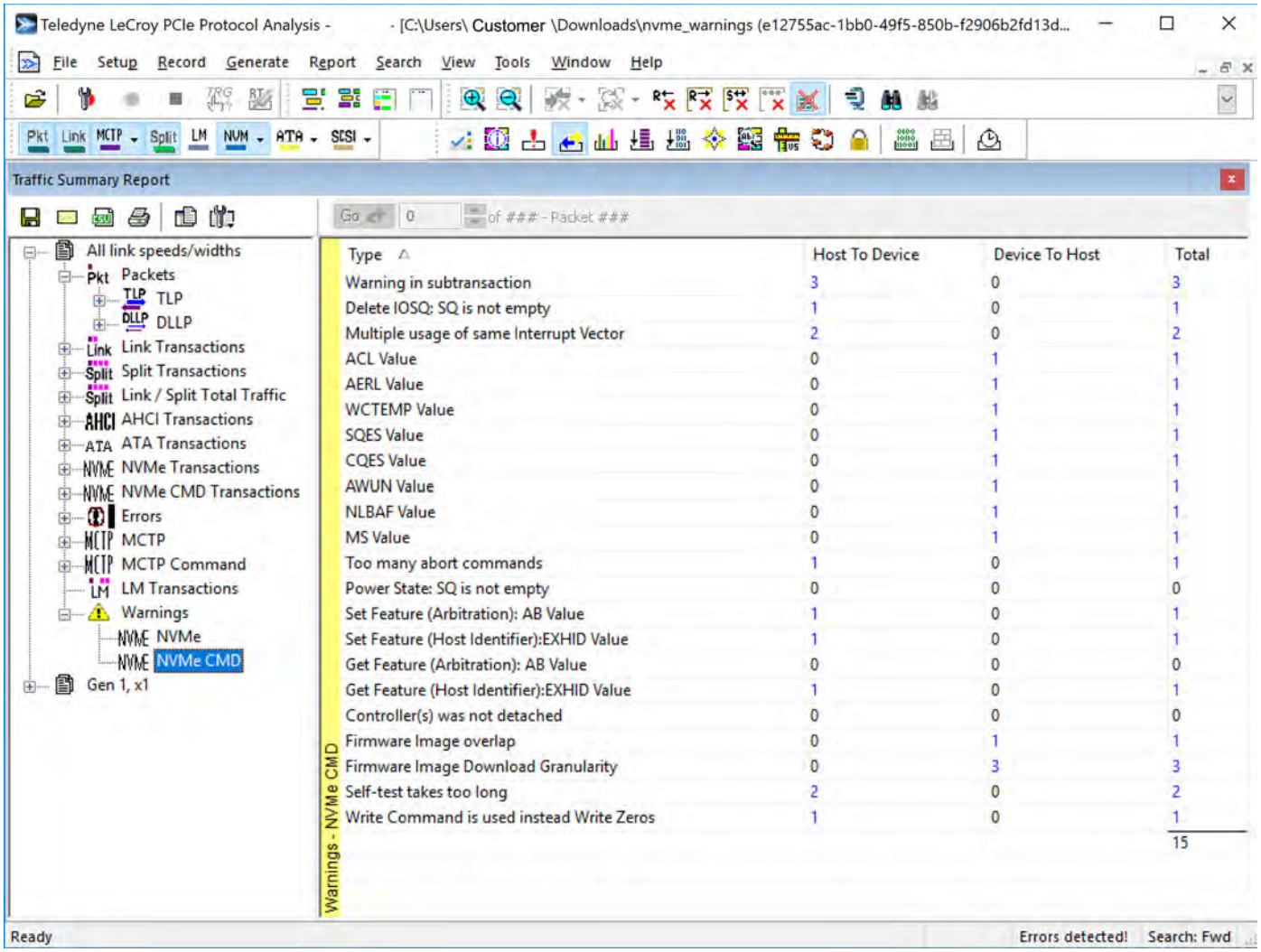


Figure 9.138: NVMe Warning Messages: Traffic Summary NVMe CMD

9.11.23.3 Find NVMe Commands and Transactions

You can use the "Find" function  to display the NVMe Commands and Transactions Warning Messages. See Figure 9.139 on page 641 and Figure 9.140 on page 642.

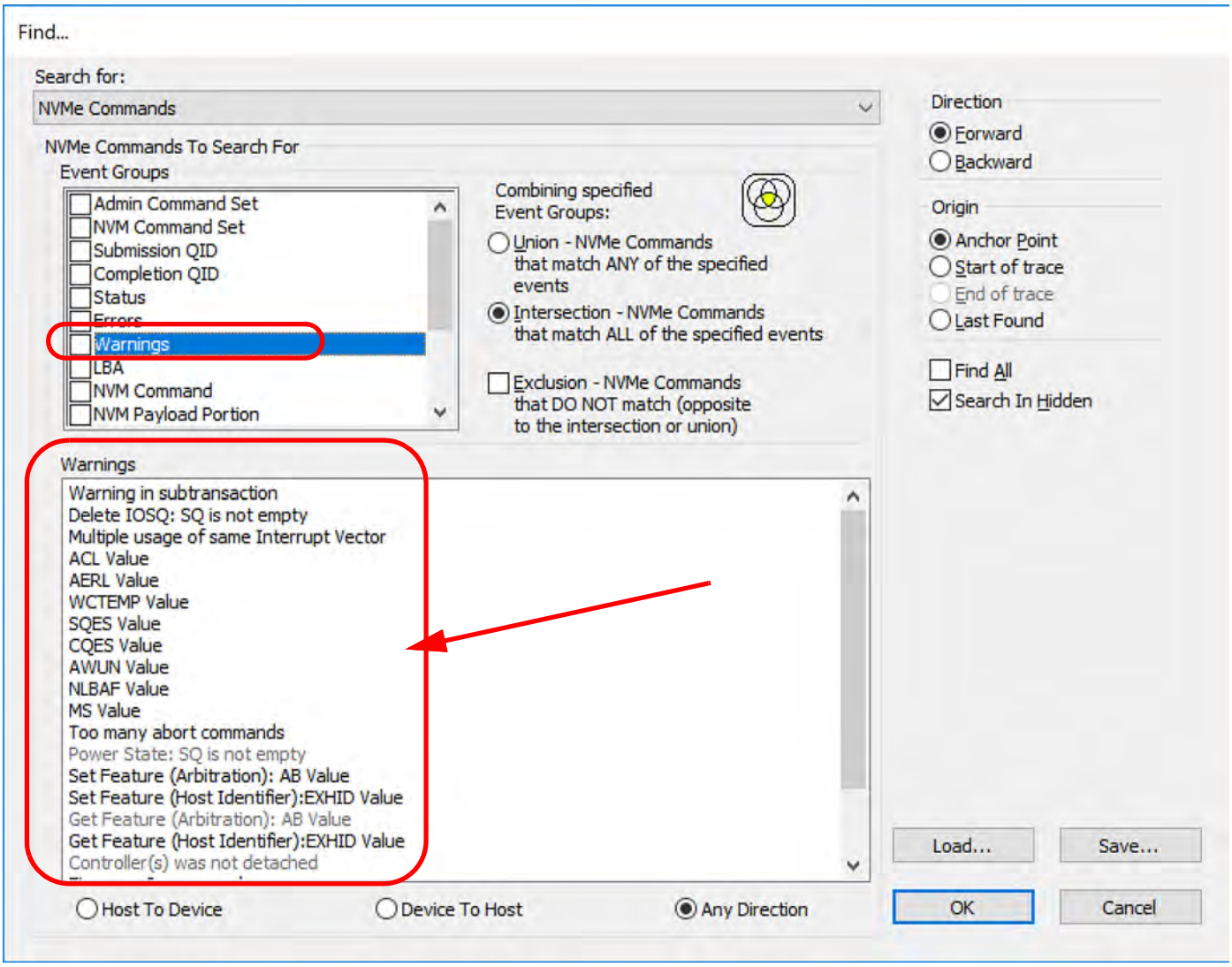


Figure 9.139: Find: NVMe Commands -> Warning Messages

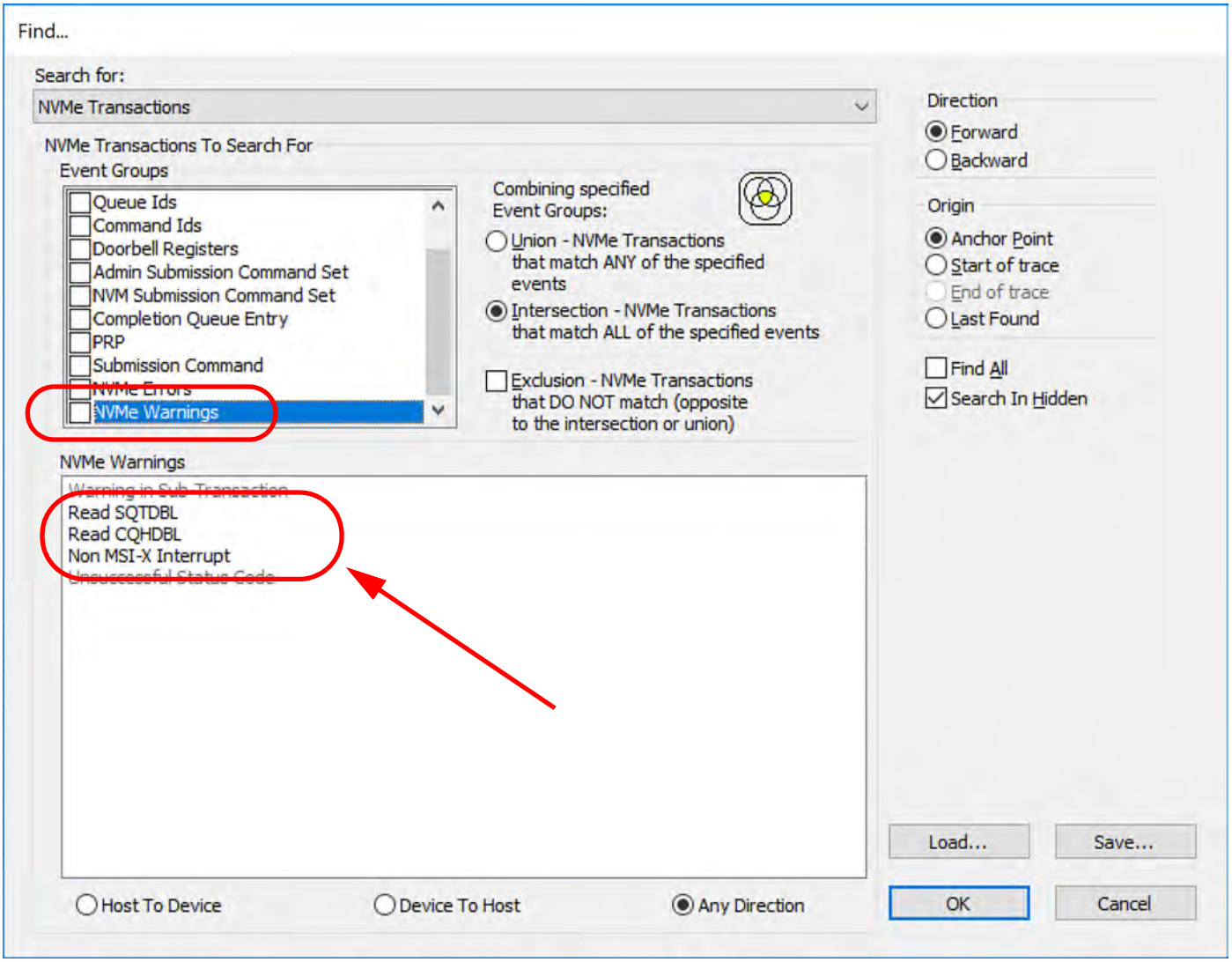


Figure 9.140: Find: NVMe Transactions -> Warning Messages

9.11.23.4 Hiding NVMe Warning Messages

You can also Hide  NVMe Warning Messages to remove them from the traffic. See Figure 9.141 on page 643.

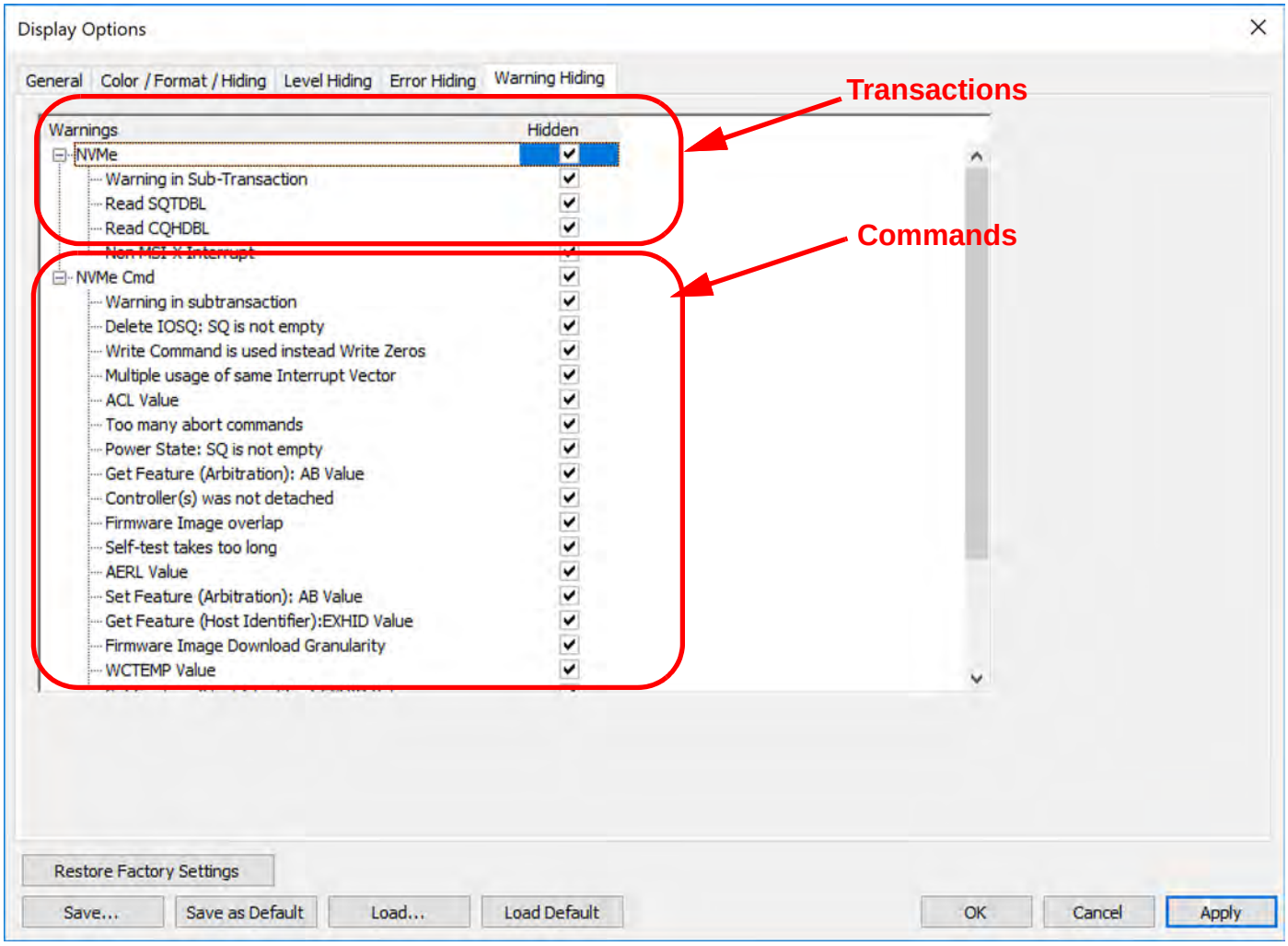


Figure 9.141: Hide -> NVMe Warning Messages

9.11.24 Decoding Lightweight Notification (LN) Protocol

The Lightweight Notification Protocol extension would allow co-processors or peripheral chips to talk to each other through system memory using a PCIe transaction without interrupting a host processor. For example, an Ethernet switch could respond to commands to encrypt and decrypt specific data packets while a host processor is inactive.

The PCIe Protocol Analysis software supports the decoding of Gen4 1.0 Lightweight Notification (LN) Protocol as shown in Figure 9.142 as well as the Traffic Summary Report.

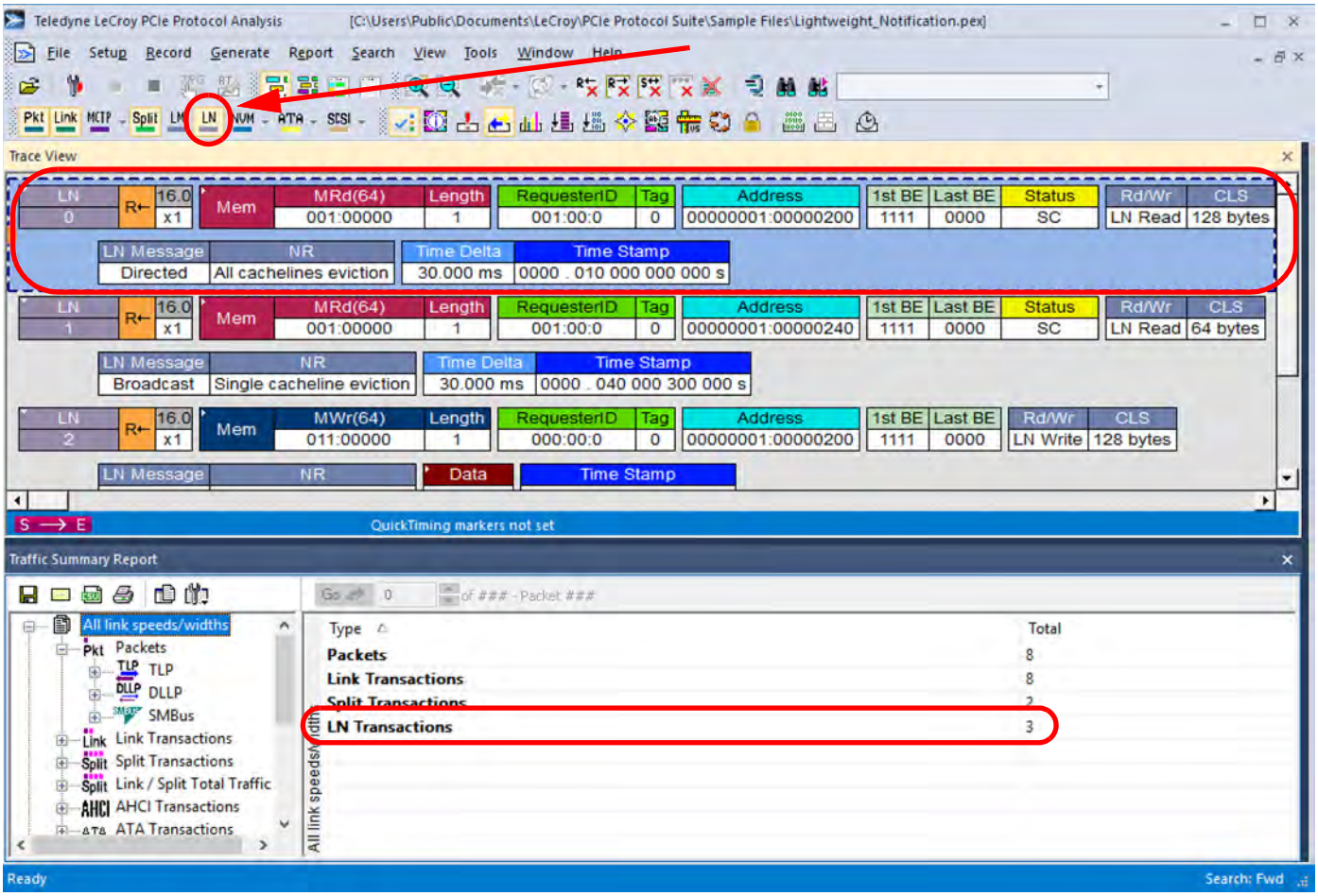


Figure 9.142: Decoding Lightweight Notification (LN) Protocol

9.11.24.1 Lightweight Notification Protocol Errors

The PCIe Protocol Analysis software also decodes any errors in the LN protocol. See Figure 9.143

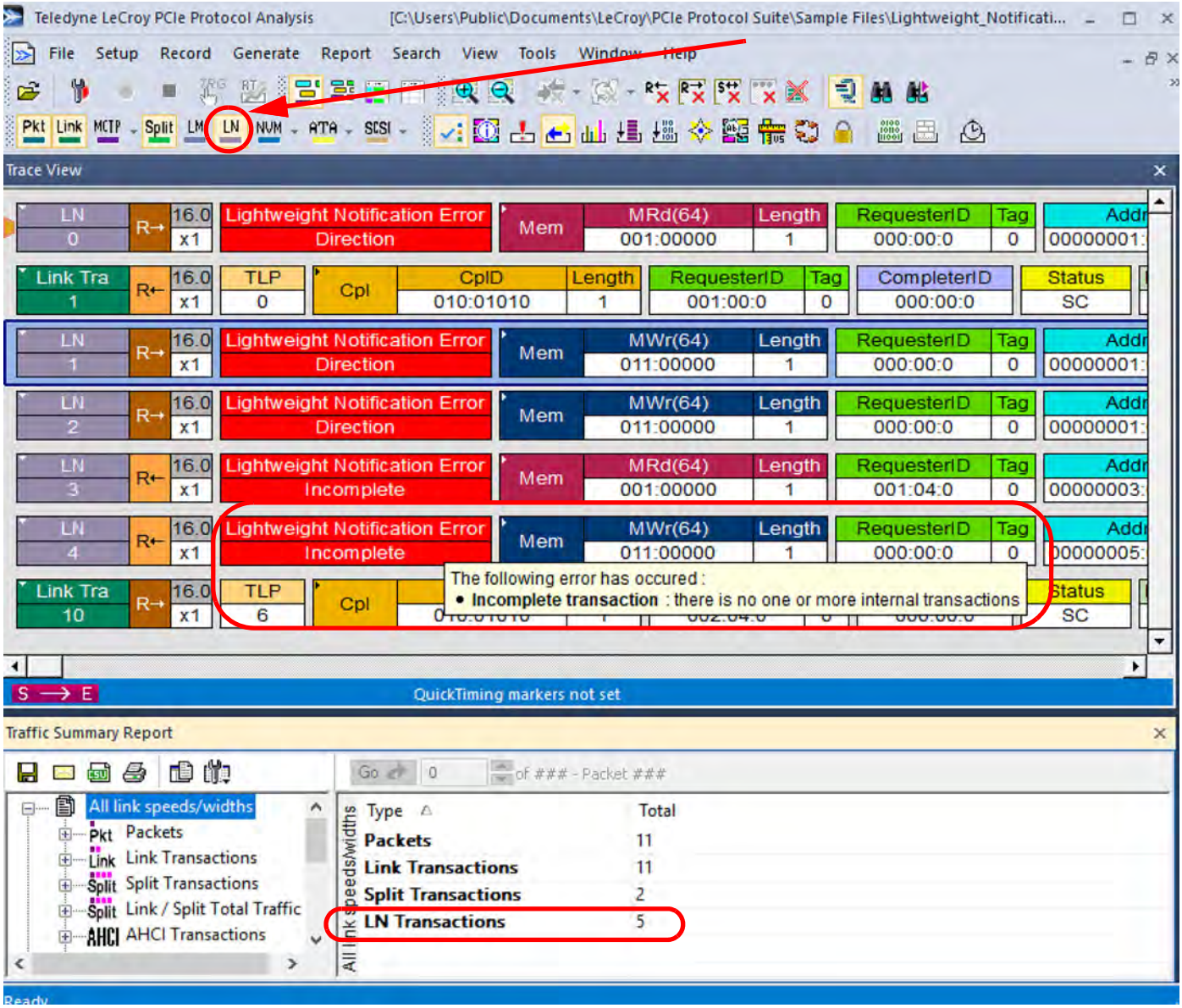


Figure 9.143: Decoding Errors in Lightweight Notification Protocol

9.11.24.2 Lightweight Notification Protocol in Trace Expert

The LN Protocol is also shown in the Trace Expert View (see Figure 9.144).

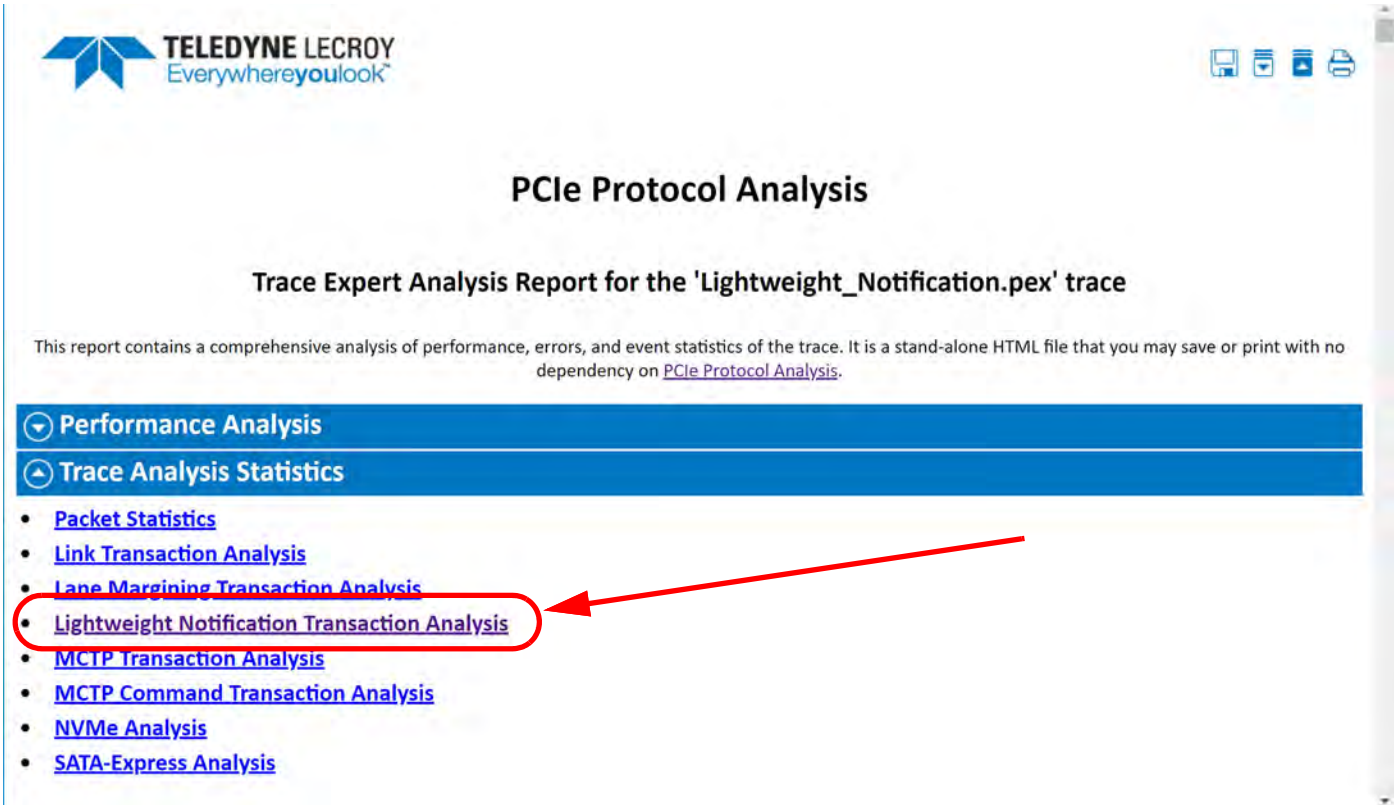
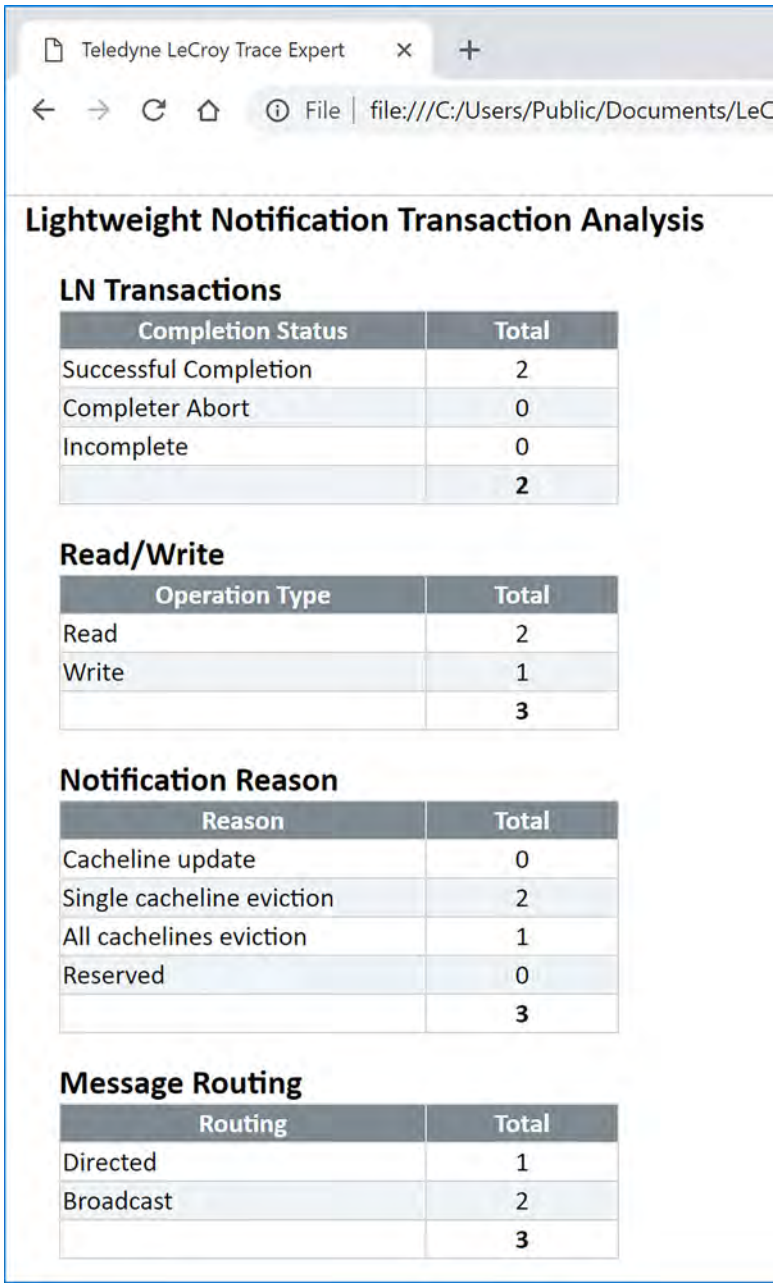


Figure 9.144: Lightweight Notification Transaction Analysis

The details of that LN Transaction Analysis can be seen in Figure 9.145 on page 647.



Lightweight Notification Transaction Analysis

LN Transactions

Completion Status	Total
Successful Completion	2
Completer Abort	0
Incomplete	0
	2

Read/Write

Operation Type	Total
Read	2
Write	1
	3

Notification Reason

Reason	Total
Cacheline update	0
Single cacheline eviction	2
All cachelines eviction	1
Reserved	0
	3

Message Routing

Routing	Total
Directed	1
Broadcast	2
	3

Figure 9.145: LN Transaction Analysis

9.11.24.3 Lightweight Notification Transaction Analysis Errors: Trace Expert

Lightweight Notification Transaction Analysis Errors can also be seen in Trace Expert. See Figure 9.146.

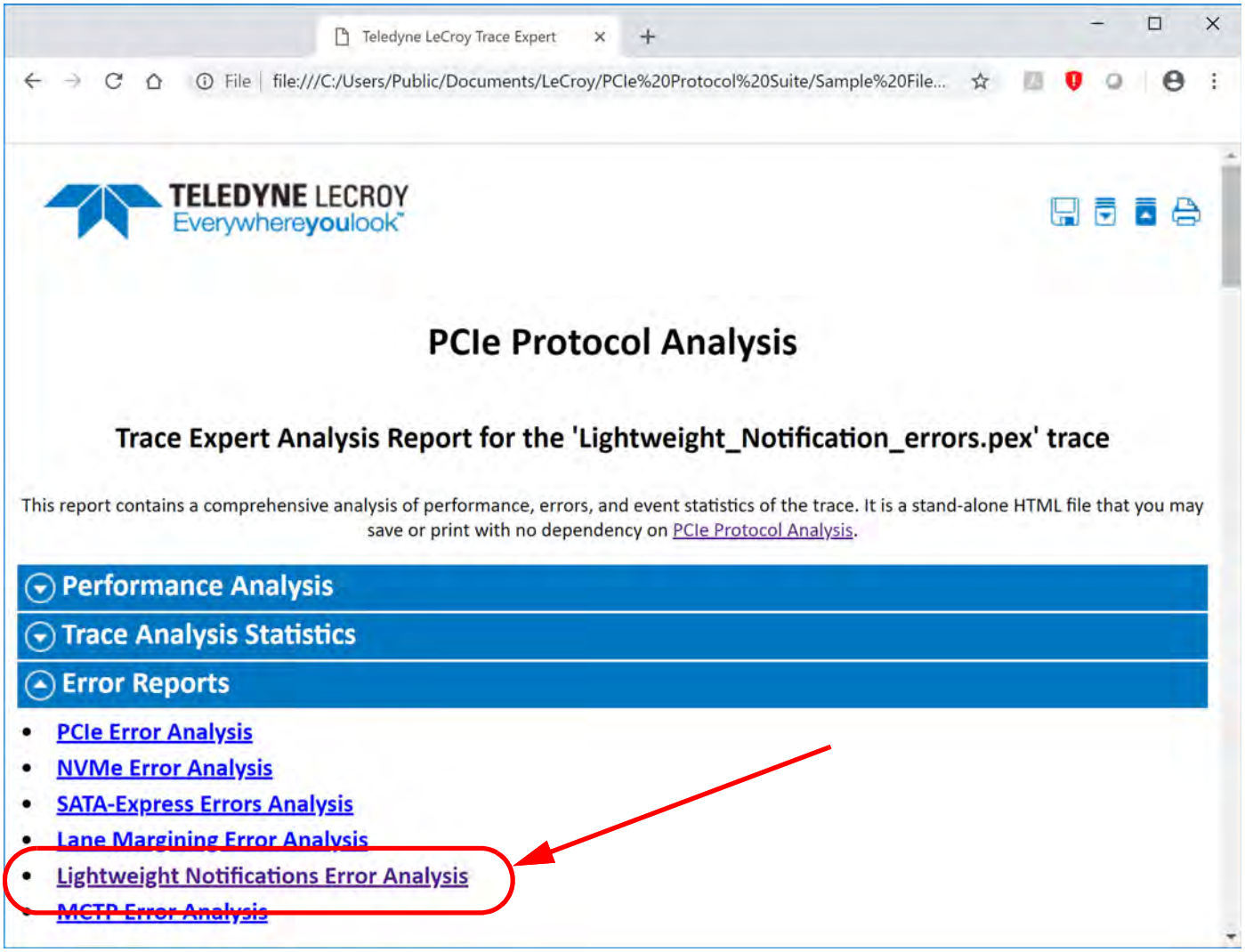


Figure 9.146: Trace Expert: Lightweight Notification Transaction Analysis Errors

Those errors can be seen in detail in Trace Expert (see Figure 9.147 on page 649).

Lightweight Notifications Error Analysis

Lightweight Notifications Errors

Error	Total
Incomplete Transaction	2
Wrong Read/Write Direction	3
Wrong Message Direction	1
Any Error	5

Figure 9.147: Lightweight Notification Errors from Trace Expert

9.11.24.4 Find: Lightweight Notification Transactions

You can use the Find tool to locate Lightweight Notification transactions. See Figure 9.148.

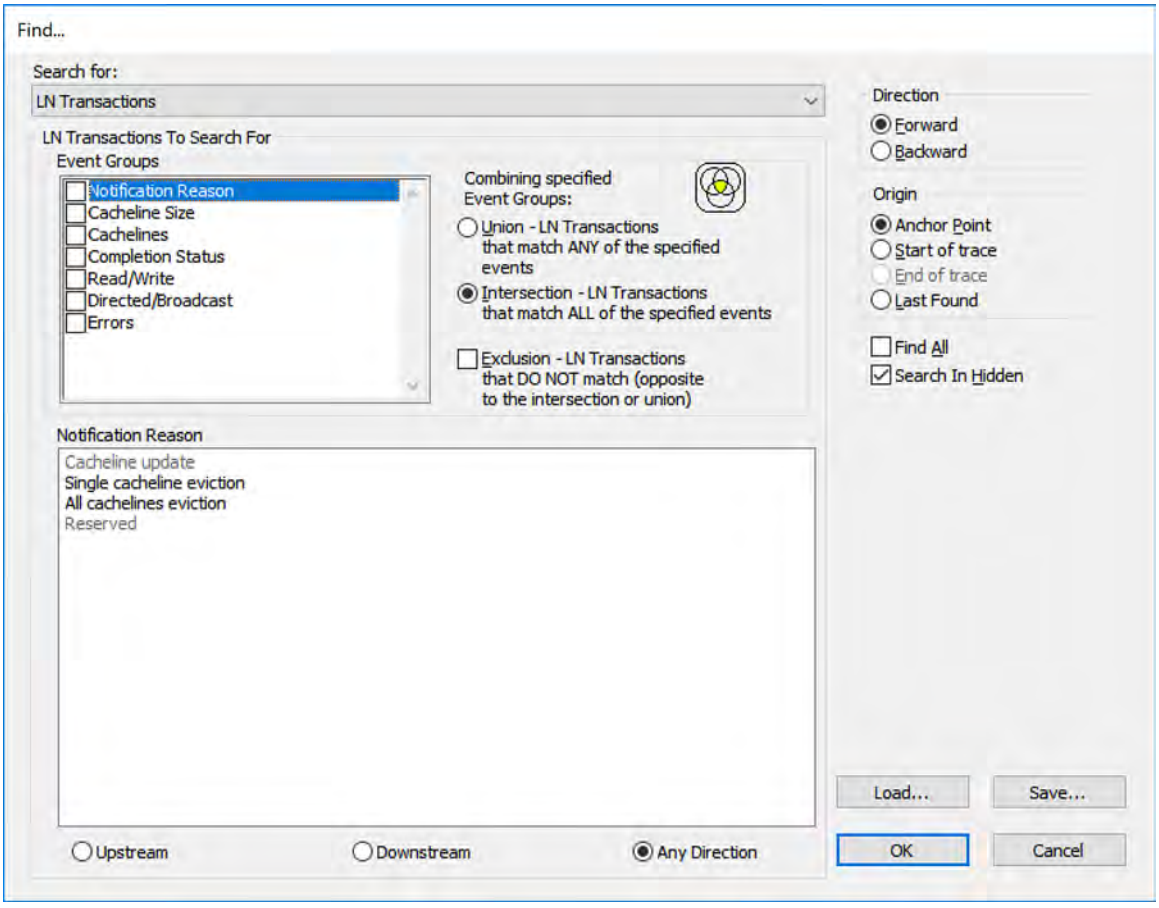


Figure 9.148: Lightweight Notification transactions

9.11.25 Decoding CCIX Protocol

PCIe Protocol Analysis software can decode the Cache Coherent Interconnect for Accelerators (CCIX) transaction protocol.

CCIX is a high-performance, low latency, chip-to-chip interconnect architecture that provides a cache coherent framework for heterogeneous system architectures. Cache coherency is automatically maintained at all time between the central processing unit and the various other accelerators in the system. Operating over standard PCIe, CCIX supports signaling rates between 16 GT/s and 25 GT/s per link with support for port aggregation for higher performance.

CCIX is largely an extension of the PCI Express architecture, consists of a number of stacked protocol layers.

- CCIX Protocol Layer - coherency protocol that manages memory reads and writes, provides a mapping for the on-chip architecture-dependent coherency protocols (e.g., AMBA CHI/ACE). This layer also defines the cache state (e.g. shared/unique, clean/dirty).
- CCIX Link Layer - formatting protocol for transport (e.g., PCIe). This layer also manages link aggregation.
- CCIX Transport Specification
- PCIe Transaction Layer - Handles PCIe transactions. The layer also supports virtual channels, permitting transmission for different data streams across a single shared link.
- CCIX Transaction Layer - Handles CCIX transactions. This layer optimizes out superfluous PCIe packet fields, reducing overhead.
- PCIe Data Link Layer - Handles standard data link layer (e.g., CRC, ACK).
- CCIX/PCIe Physical Layer - Handles standard PCIe physical layer. This layer also supports 25 GT/s ESM mode.

9.11.26 Decoding TCG Support of Pyrite

The PCIe Protocol Analysis software is capable of decoding Trusted Computing Group (TCG) Pyrite transactions. See Figure 9.149.

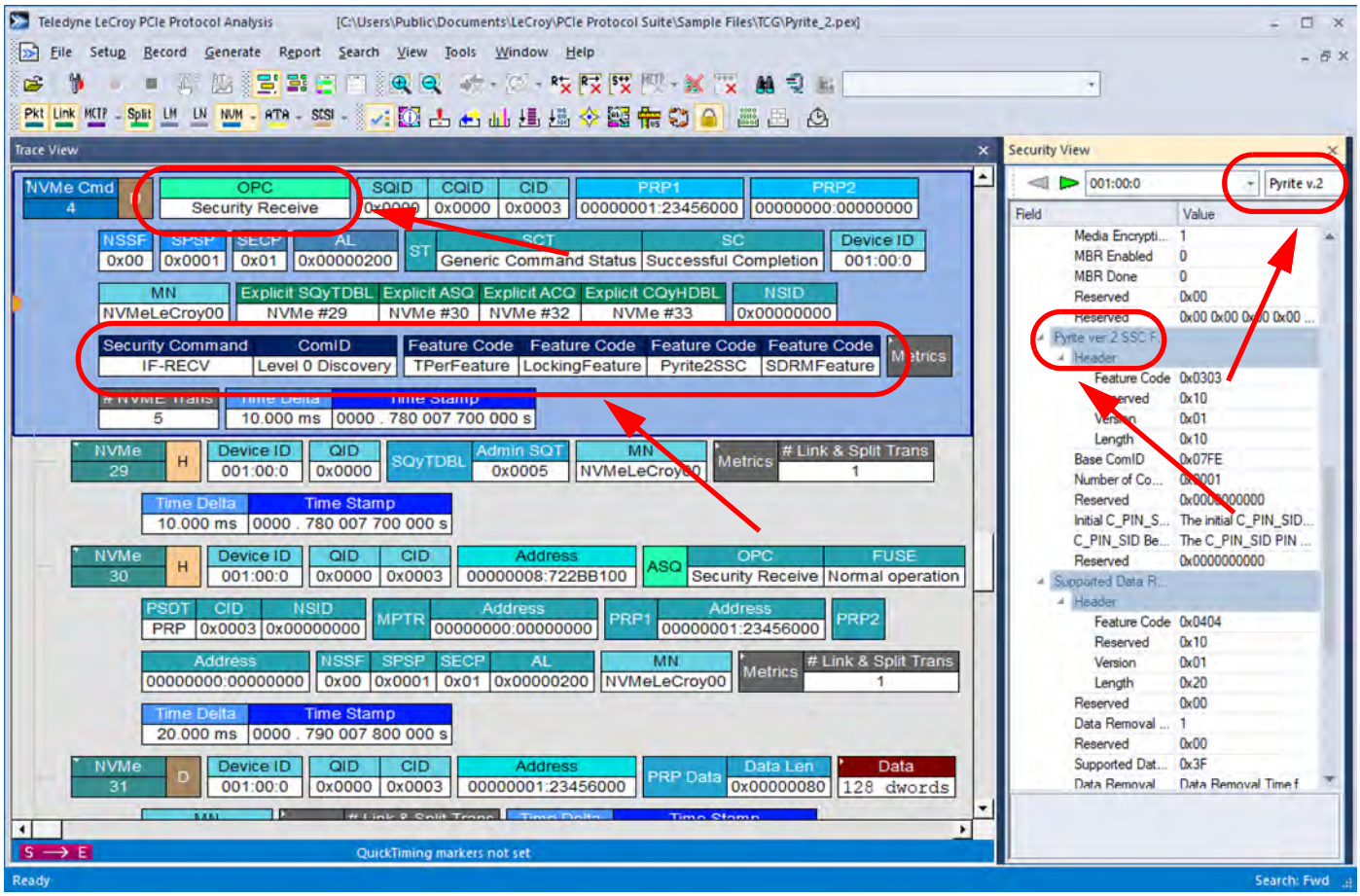


Figure 9.149: TCG Transactions: Decoded -> Pyrite

9.11.27 MCTP: Simple Hiding

You can hide (or filter out) either MCTP VDM traffic or SMBus MCTP traffic or both by using the MCTP Hide button on the toolbar. See Figure 9.150.

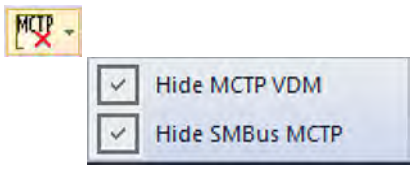


Figure 9.150: MCTP: Simple Hiding Icon

9.11.27.1 MCTP: Hide VDM Traffic

If you chose to hide only the MCTP VDM traffic a sample trace is shown below without the VDM traffic hidden (see Figure 9.151) and with VDM traffic hidden (see Figure 9.152 on page 653).

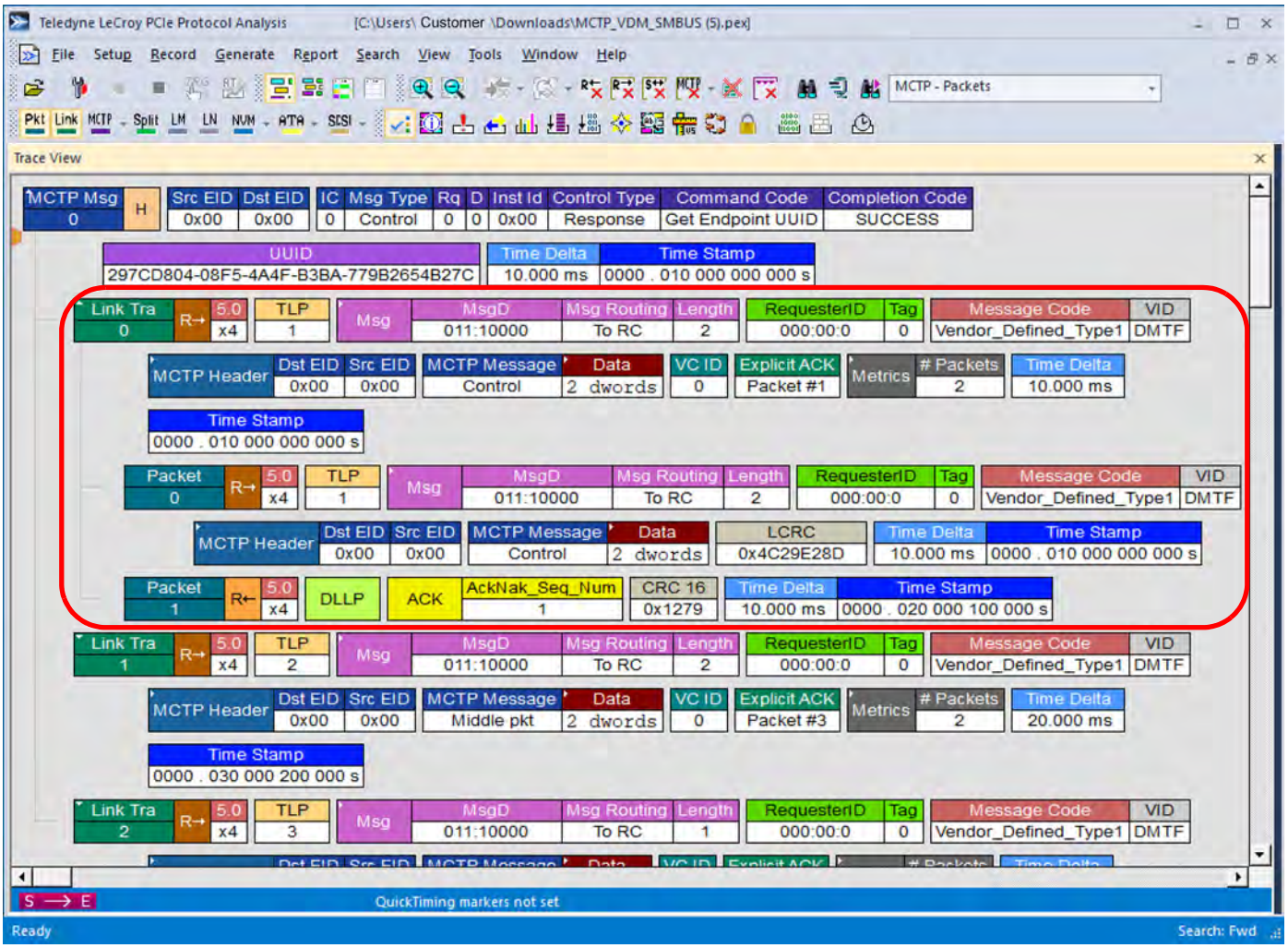


Figure 9.151: MCTP VDN Traffic: Link 0, Packet 0 -> Shown

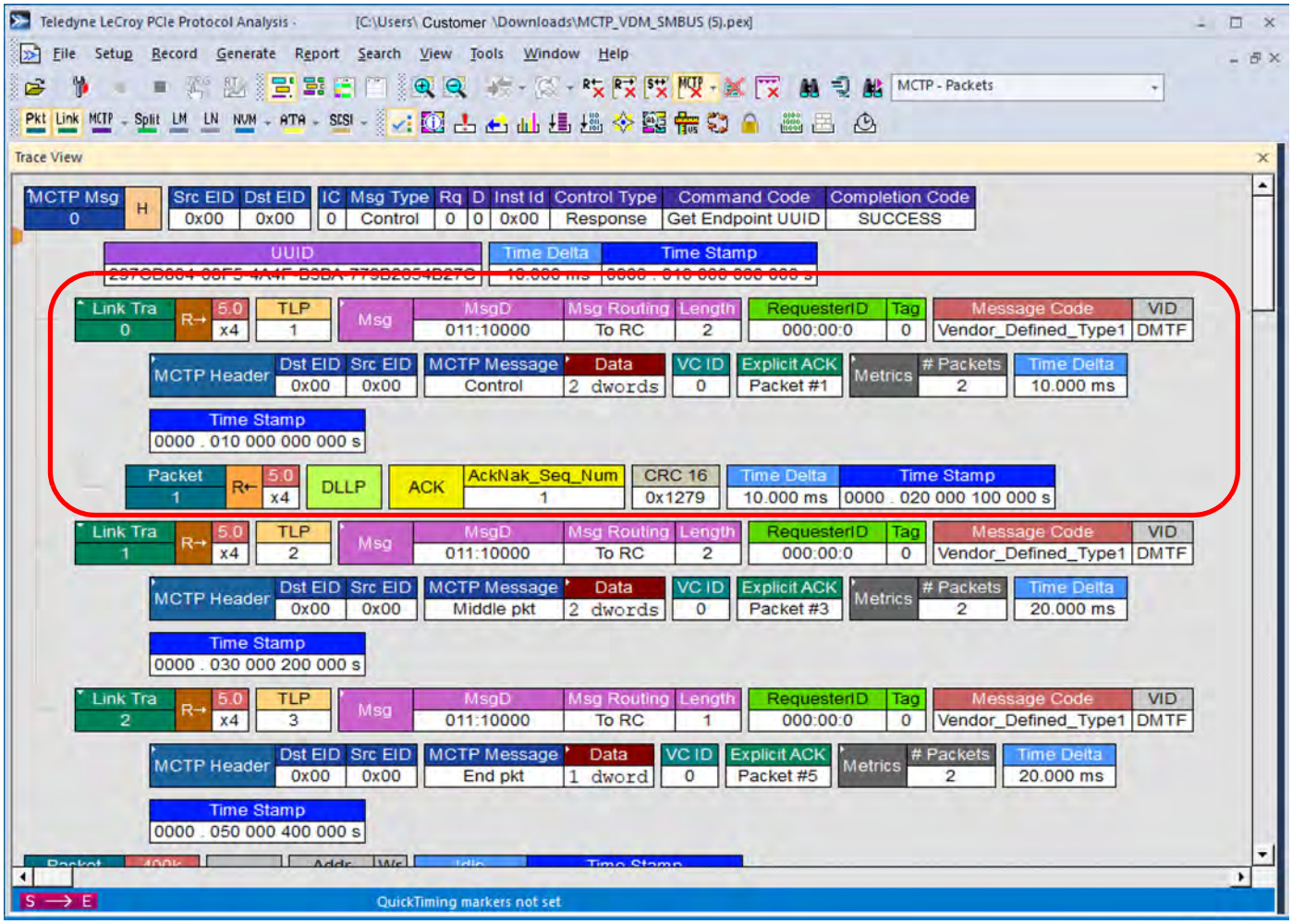


Figure 9.152: MCTP VDN Traffic: Link 0, Packet 0 -> Hidden

9.11.27.2 MCTP: Hide SMBus Traffic

If you chose to hide only the SMBus MCTP traffic a sample trace is shown below without the SMBus traffic hidden (see Figure 9.153) and with SMBus MCTP traffic hidden (see Figure 9.154 on page 655).

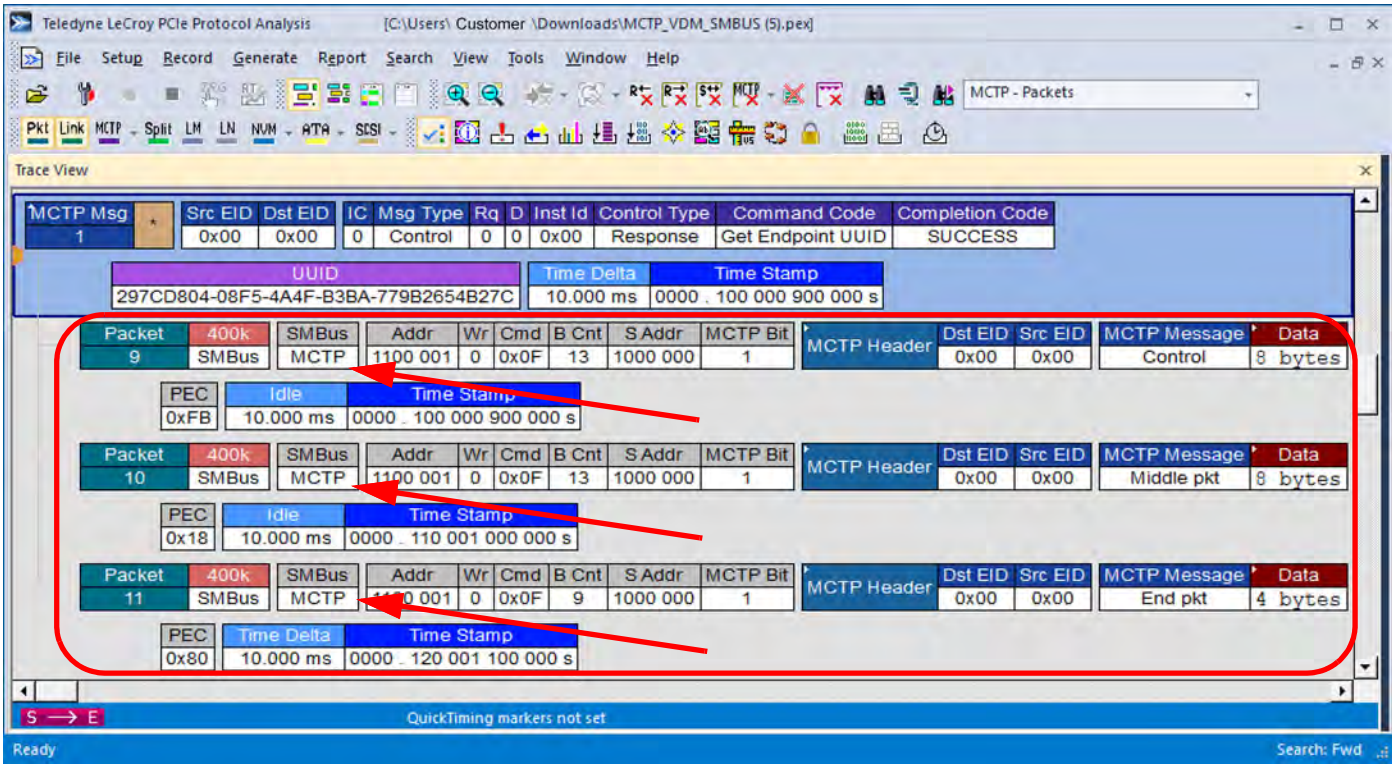


Figure 9.153: MCTP SMBus Traffic: Shown

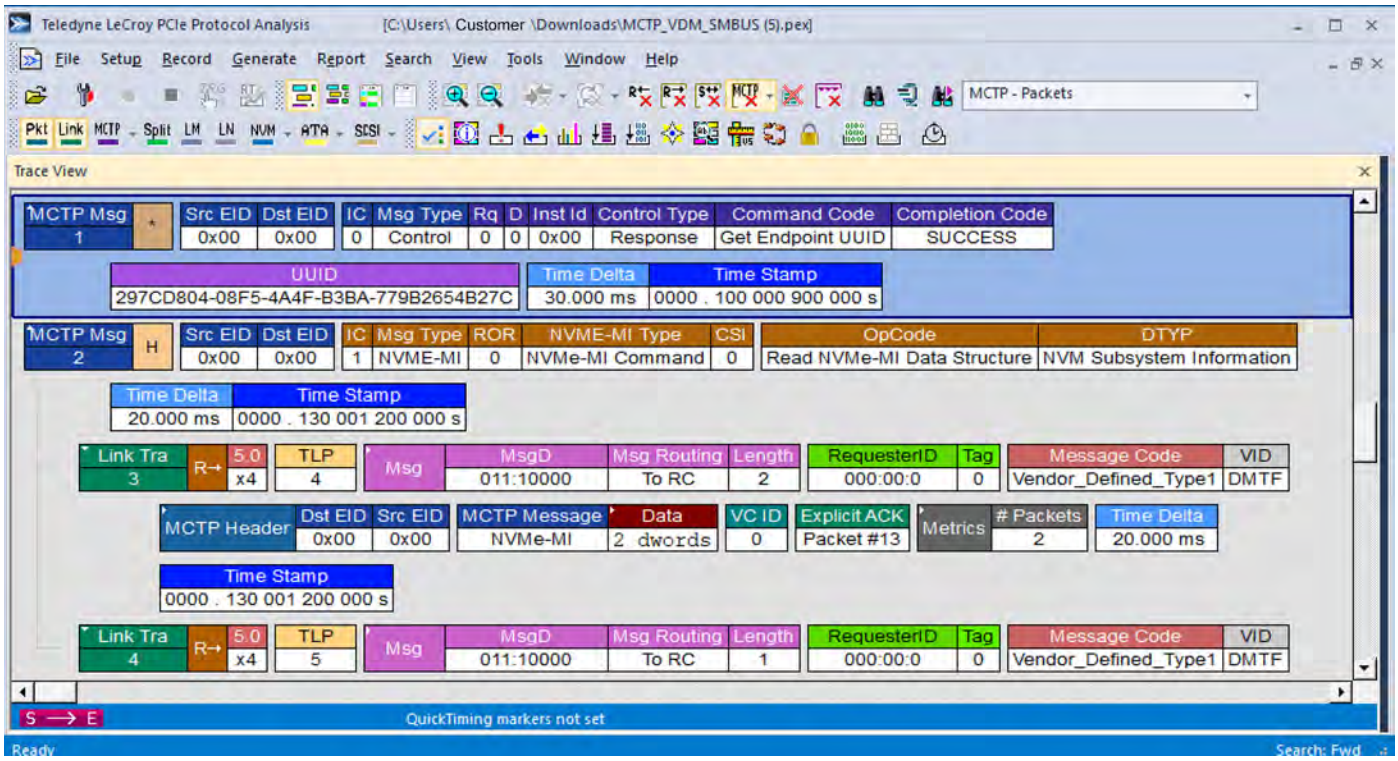


Figure 9.154: MCTP SMBus Traffic: Hidden

9.11.27.3 MCTP Message Type and IC Cells

You can decode MCTP Messages and IC cells. See Figure 9.155.

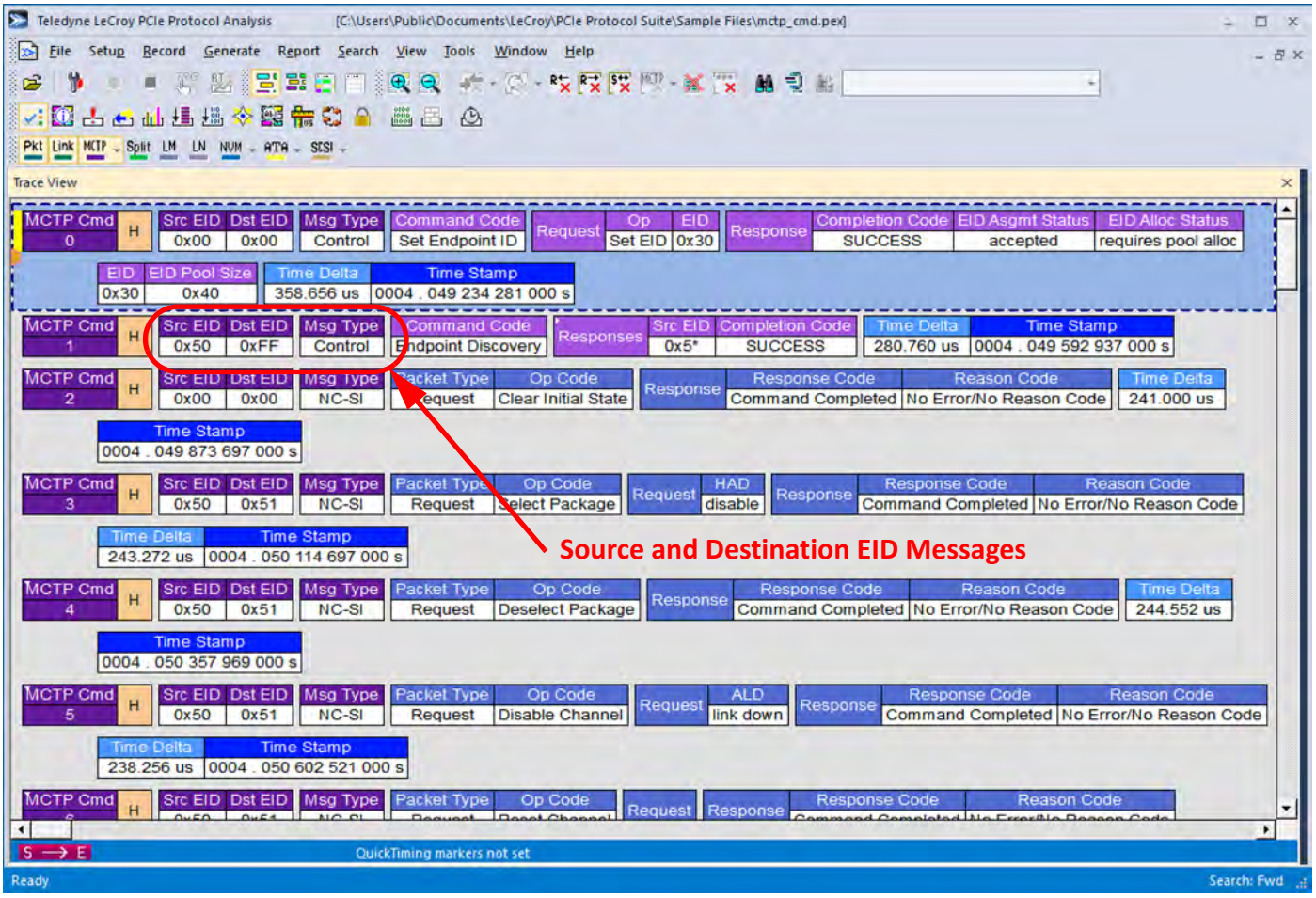


Figure 9.155: MCTP Messages Types and IC Cells Decoded

The colors of the MCTP Messages can be seen in the Display Options. See Figure 9.156 on page 657

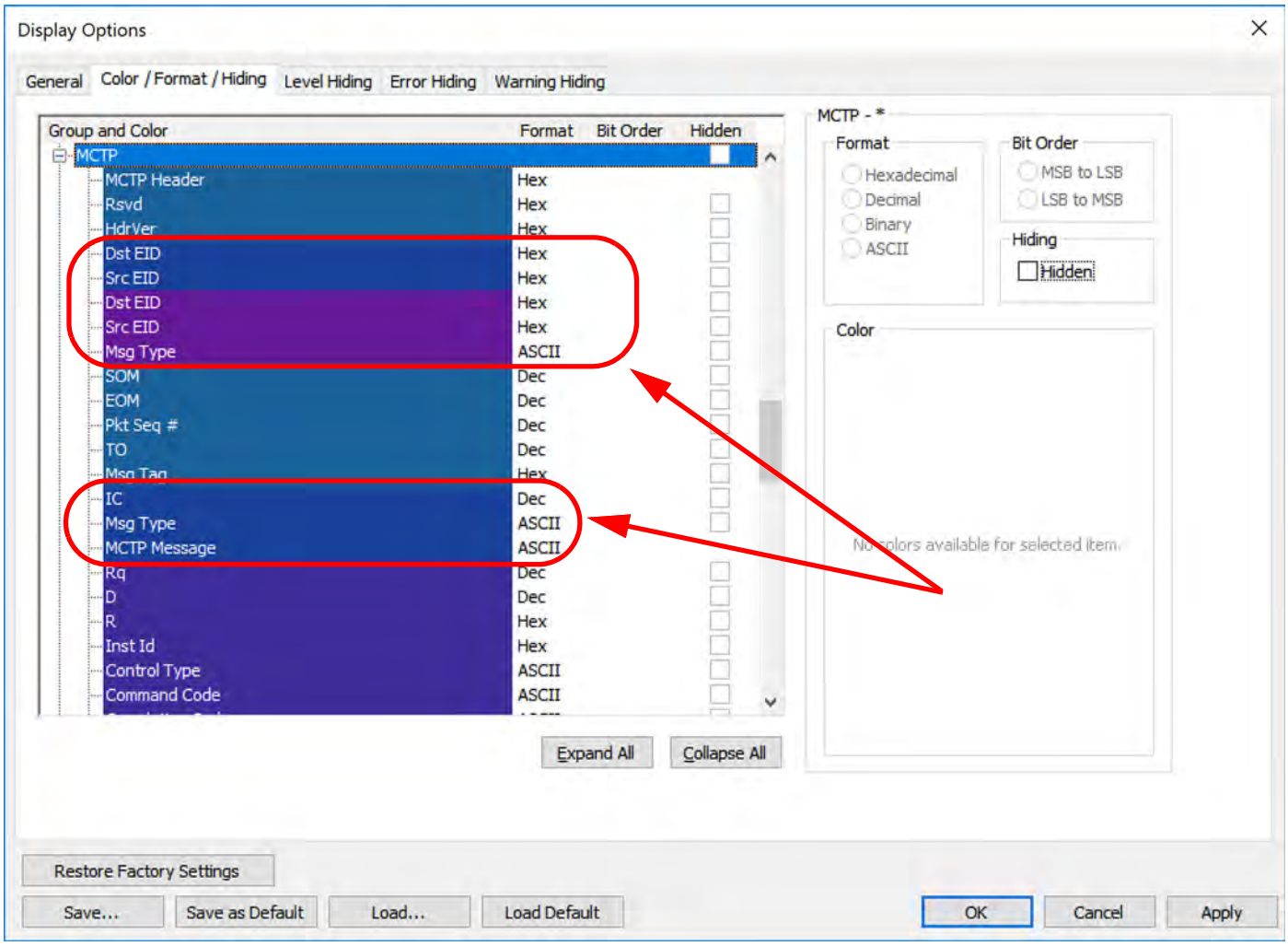


Figure 9.156: MCTP Commands and Transaction Colors from Display Options

9.11.28 Decoding NVME-MI Version 1.1

The PCIe Protocol Analysis software can decode NVME-MI Version 1.1 traffic. See Figure 9.157.

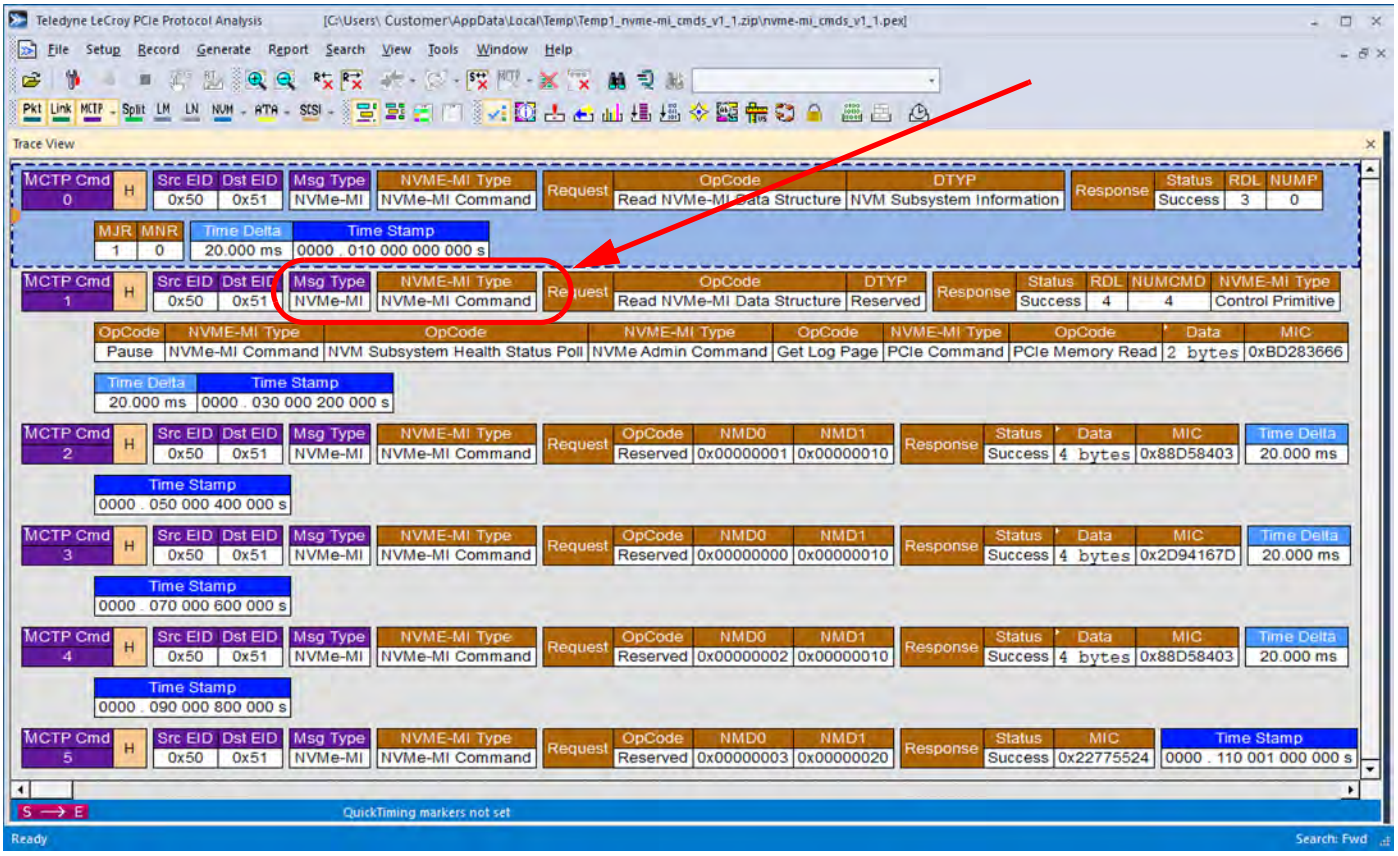


Figure 9.157: Decoding NVME-MI Version 1.1

9.11.29 Swapping Direction of Recorded Traffic Data

Swapping Upstream/Downstream direction of traffic gives you the ability (in a recorded trace) to reverse the direction of the traffic which was recorded. See Figure 9.158.

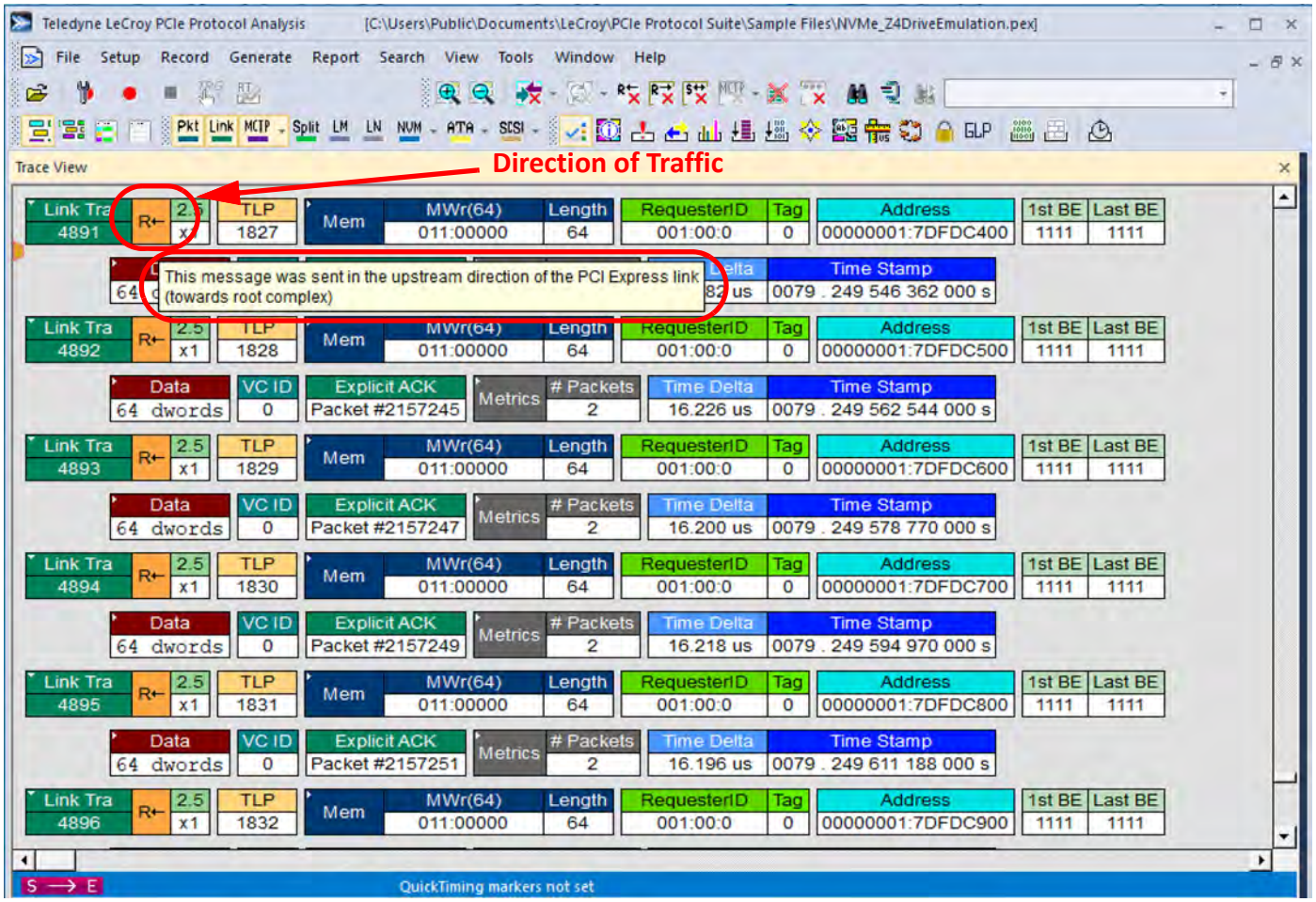


Figure 9.158: Recorded Trace: Traffic Flows in Direction it was Recorded

If you hover over the direction box (just to the right of the Link Transaction number) and perform a right click a context menu will pop up. See Figure 9.159 on page 660.

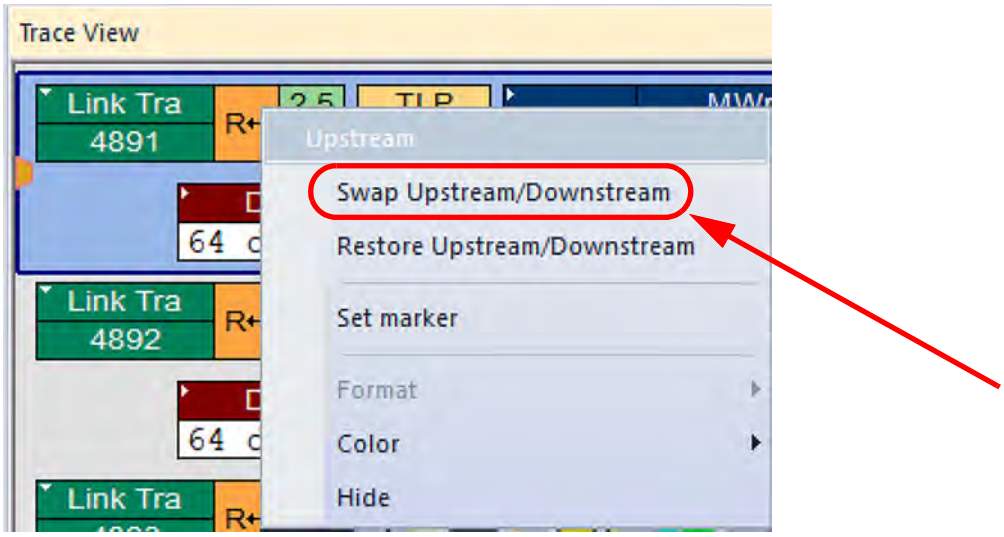


Figure 9.159: Context Menu Showing Traffic Direction

If you select Swap Upstream/Downstream the direction of the traffic will change and the tooltip will reflect that change. The color of the direction block will also change. See Figure 9.160 on page 661.

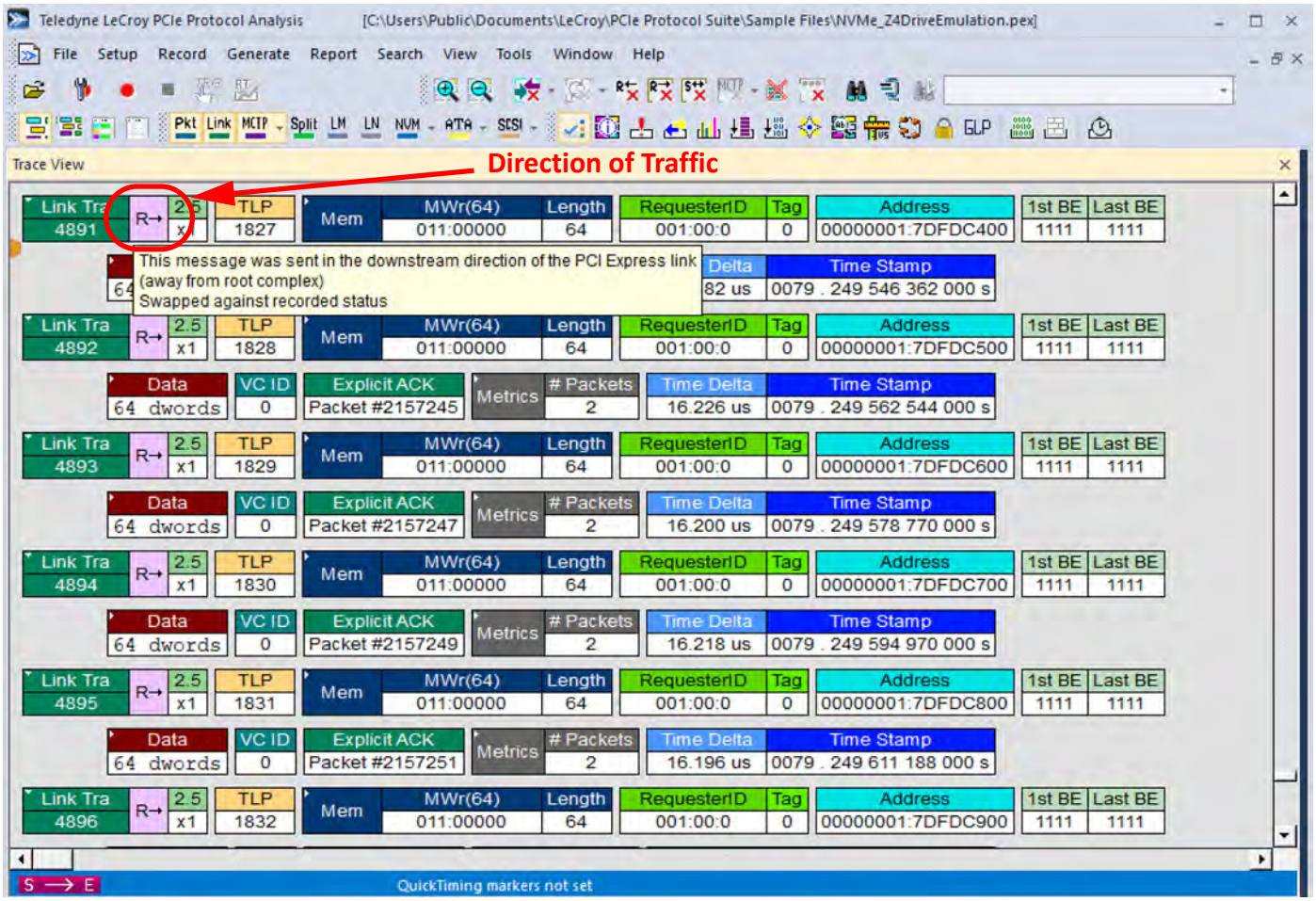


Figure 9.160: Direction of Traffic has been Swapped

If you want to swap the traffic direction back to the way it was originally recorded simply bring up the context menu (left click in the direction block) and select “Restore Upstream/ Downstream”. See Figure 9.161.

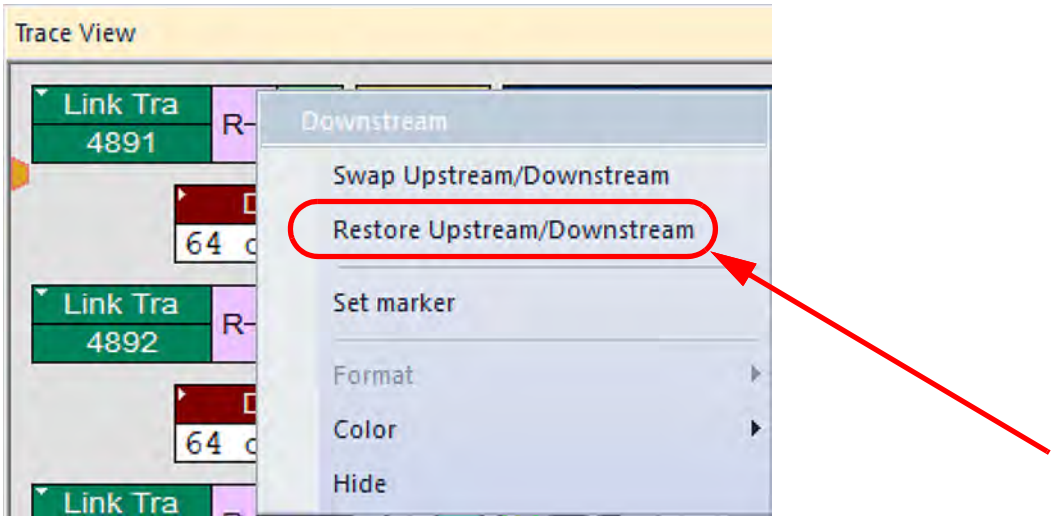


Figure 9.161: Context Menu Showing Traffic Direction: Downstream with Restore Option

9.11.30 Decoding Traces Exported from USB4 Traces with Tunneled PCIe Traffic

The PCIe Protocol Analysis Suite software is capable of decoding traces exported from USB4 traces which have tunneled PCIe Traffic.

A sample USB4 trace with PCIe tunneled traffic is shown in Figure 9.162. The highlighted Packets #6 and #7 contain Tunneled PCIe traffic with a timestamps of 7.848357050 and 7.848357082 containing DLLP types UpdateFC_Cpl and UpdateFC_NP.

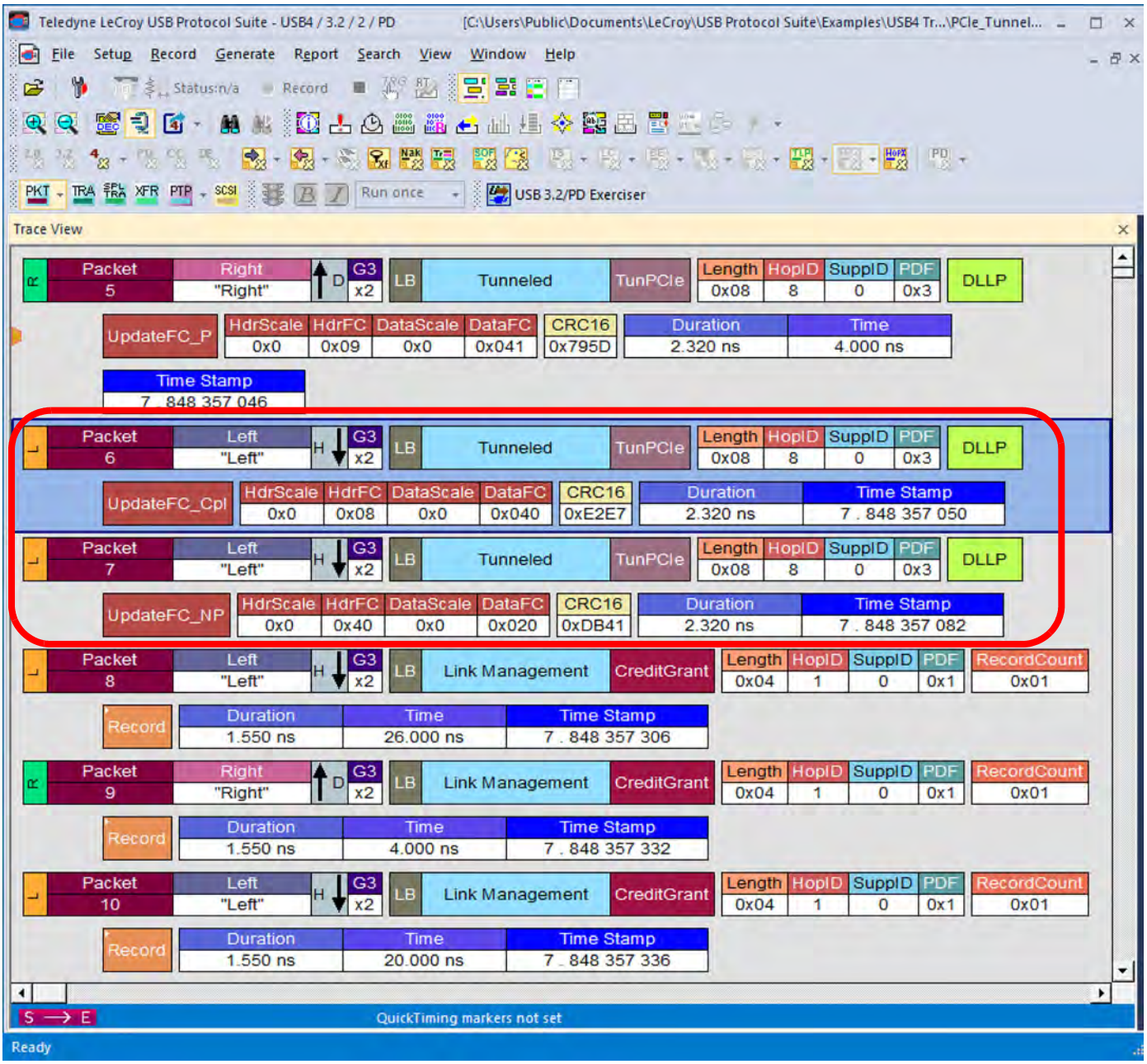


Figure 9.162: USB4 Trace with PCIe Tunneled Traffic

The PCIe Tunneled Traffic from the USB4 trace can be exported to a PCIe trace and decoded and analyzed with the PCIe Protocol Analysis software. See Figure 9.163 on page 663.

The highlighted Packets #4 and #5 contain Tunneled PCIe traffic with a timestamps of 7.848357050 and 7.848357082 containing DLLP types UpdateFC_Cpl and UpdateFC_NP.

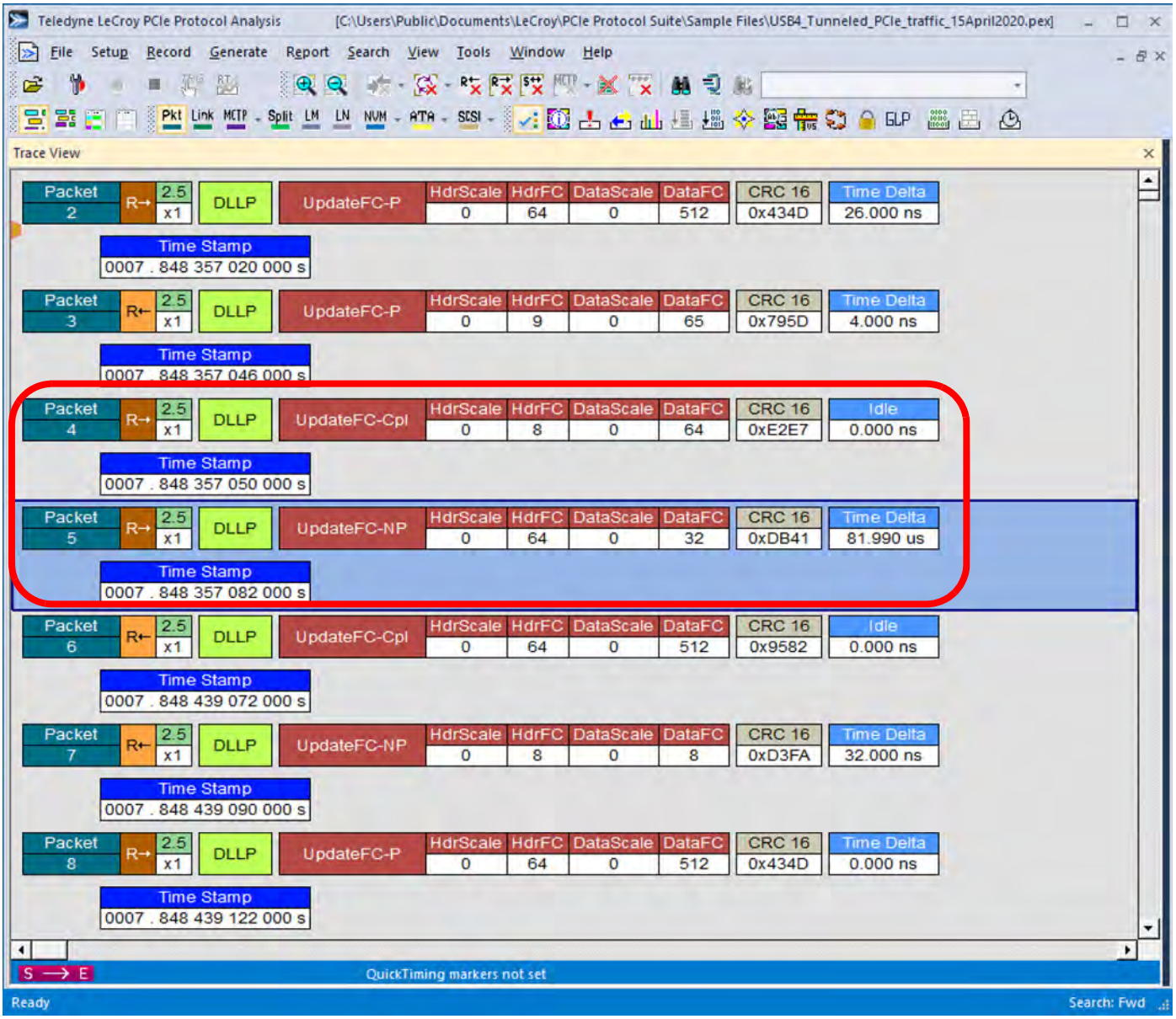


Figure 9.163: PCIe Tunneled Traffic from USB4 Trace Decoded and Analyzed by the PCIe Protocol Analysis software

Note: Link Tracker is disabled for tunneled PCIe packets intentionally, because there is no information about the PCIe link (Link Width, etc.) in USB4 tunnel.

9.11.31 Decoding CXL Traffic

The PCIe Protocol Analysis Suite software is capable of decoding traces with CXL traffic. See Figure 9.164 and Figure 9.165 on page 665.

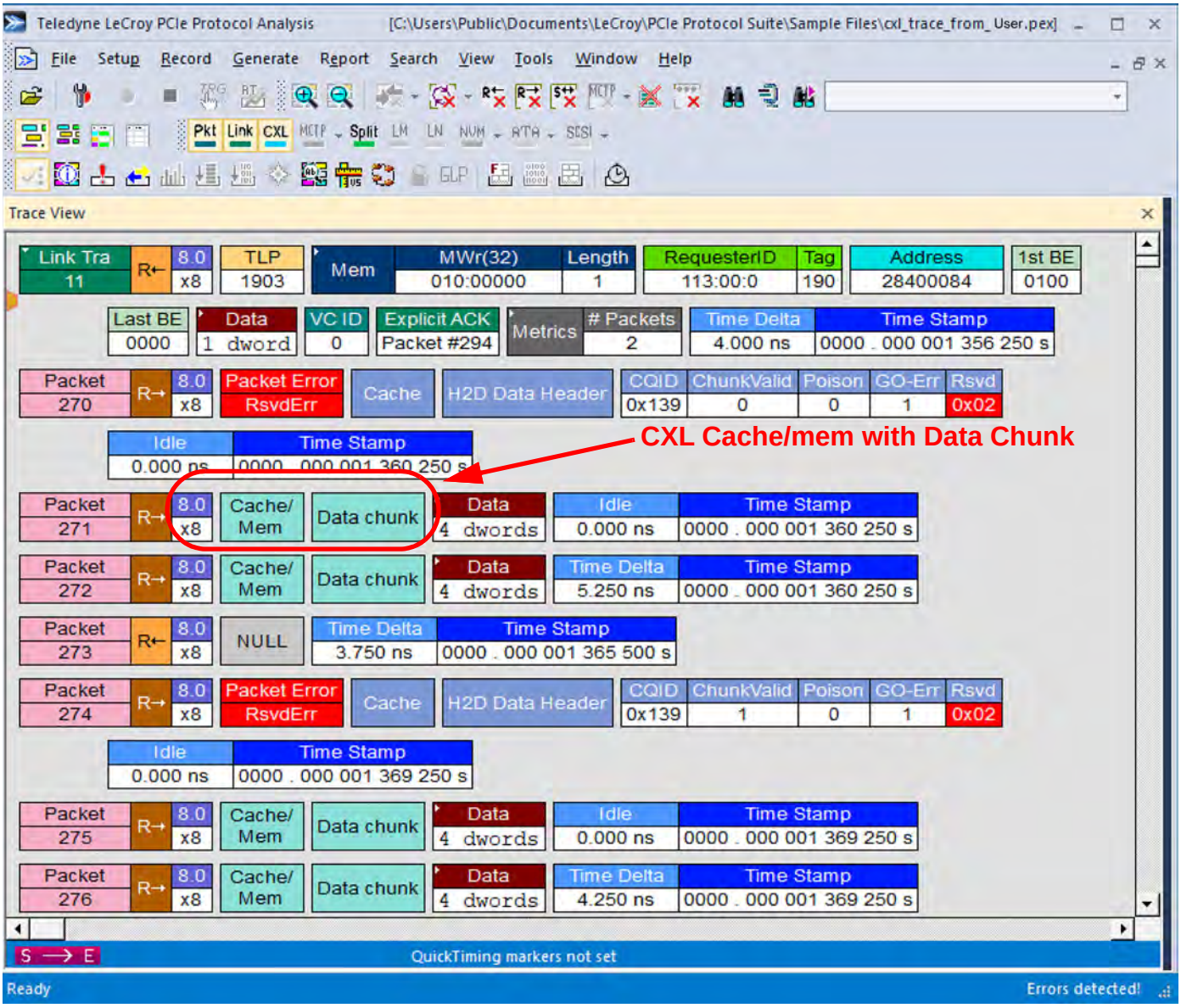


Figure 9.164: Decoding CXL Traffic

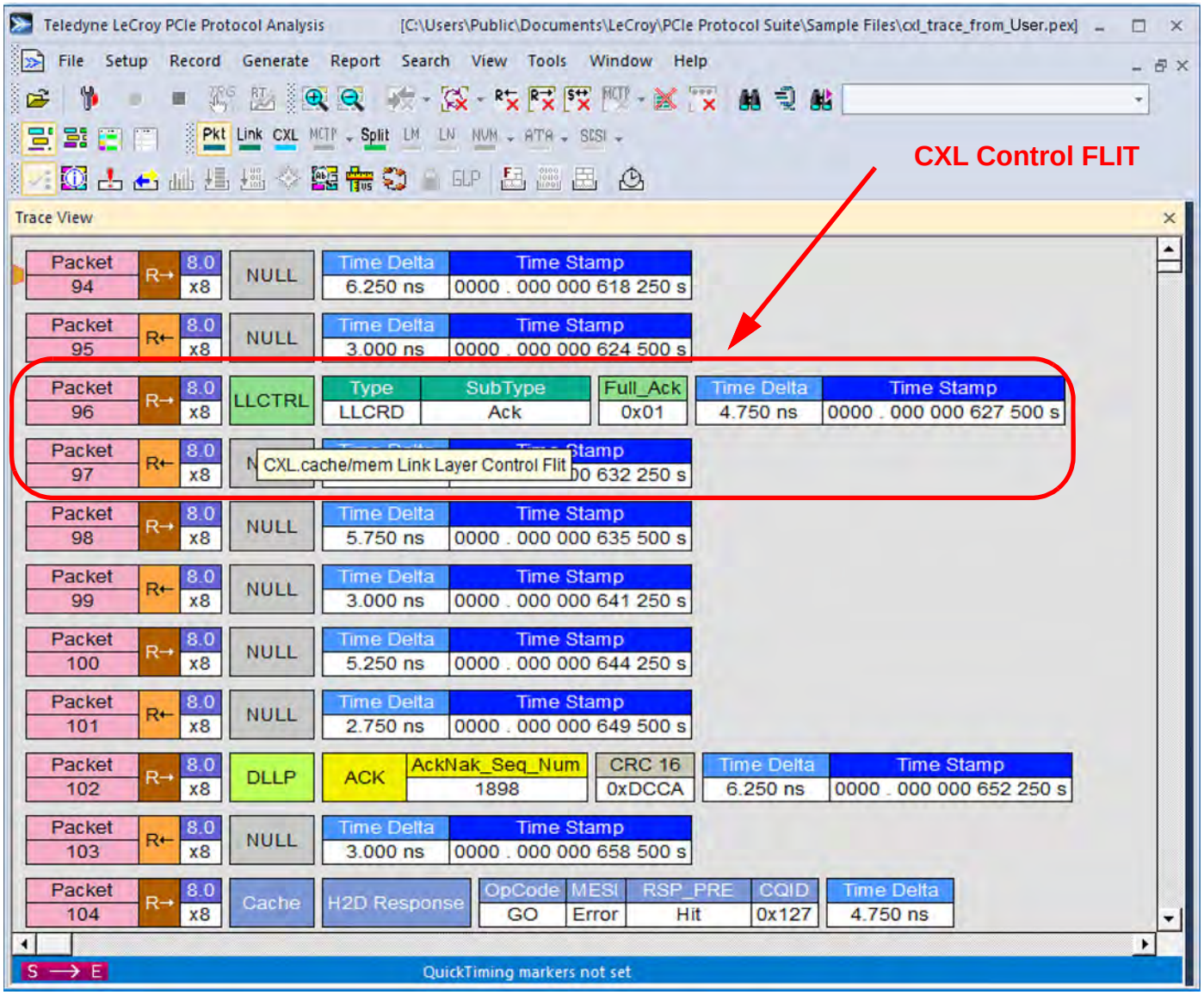


Figure 9.165: CXL Traffic: CXL.cache/mem Link Layer Control FLIT

Chapter 10

Searching CATC Traces

This chapter describes how to search for CATC Trace events.

10.1 CATC Trace Search Overview

Several search commands let you navigate a CATC Trace view to search for key events, such as errors and triggers.

To view the search options, click **Search** in the Menu bar. See Figure 10.1 on page 660.

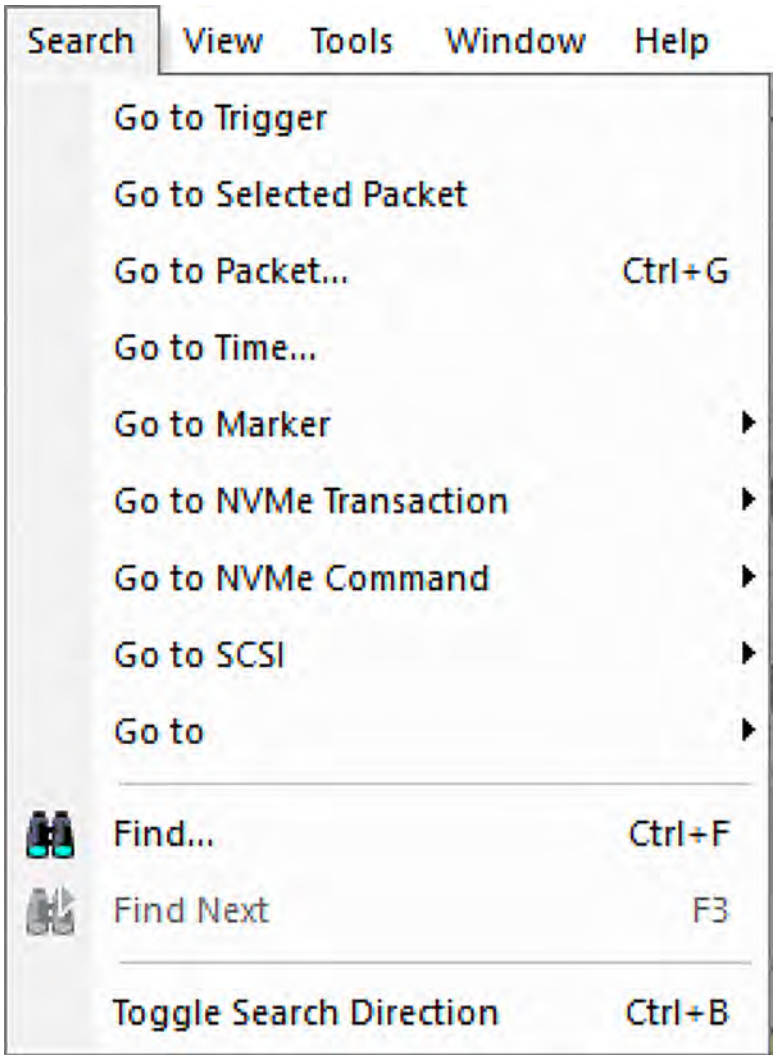


Figure 10.1: Search Menu Options

10.2 Go to Trigger

To position a trigger packet at the top of the screen:

Select **Search > Go to Trigger**.

10.3 Go to Selected Packet

To position a selected packet at the top of the screen:

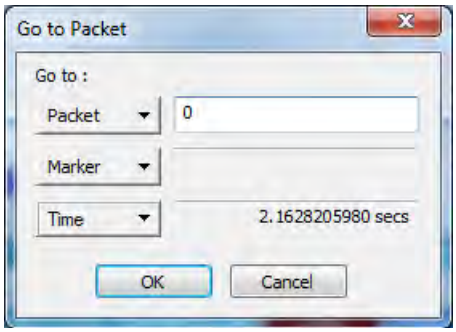
Select the packet and Select **Search > Go to Selected Packet**.

10.4 Go to Packet

To position a specific packet at the top of the screen:

1. Select **Go to Packet** from the Search menu. A pop-up menu prompts you for the packet number, marker, or time (see the following figure).

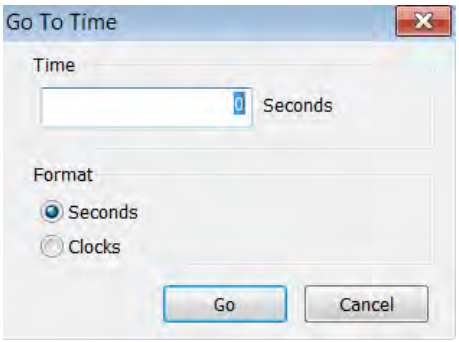
2. Choose the needed transaction level from the Packet drop-down list and enter the transaction number. Please note that transaction levels is added to list if corresponding level is decoded for current trace file.
3. Click **OK**.



10.5 Go to Time

To position a specific time at the top of the screen:

1. Select **Go to Time** from the Search menu. A pop-up menu prompts you for the time in Seconds or Clocks.



2. Enter the time and format (seconds or clocks).
3. Click **Go**.

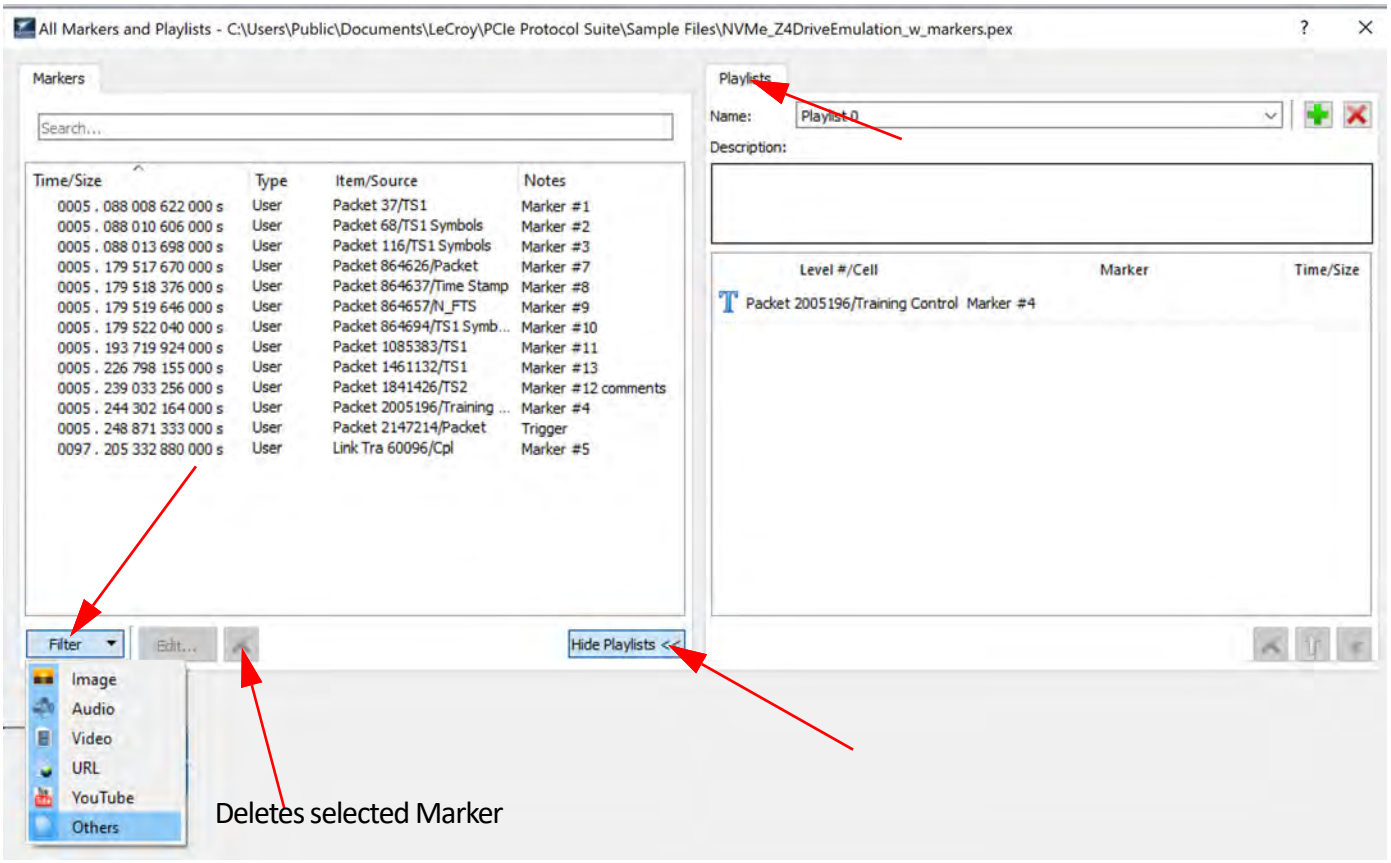
10.6 Go To Marker

Use this operation to go directly to a specific packet or transaction that has been marked with a unique marker by the Set Marker operation.

To go to a marker:

1. Select **Go To Marker** from the Search Menu.

2. Select the marker you want from the fly-out menu.
   Alternatively, select **All Markers** to display the All Markers and Playlists dialog, then select a marker and click **OK** (see figure on next page).



10.6.1 Markers

This section explains the features of Markers. A marker is an entity that flags a physical or logical item of interest within a trace file. A marker contains one or more attachments. You can add a marker to a trace file or unmark a trace file by removing the marker.

Markers are represented graphically in a different way in the application.You can not only add markers to the packets but it is granular enabling you to also add markers to individual cells.

Markers Overview

This functionality provides the user an easy way to navigate through attachments which is a discrete piece of information or data added to a marker, for example, a text description or file, an attachment of a trace file by a predefined order, video or audio files, URL links or any other files.

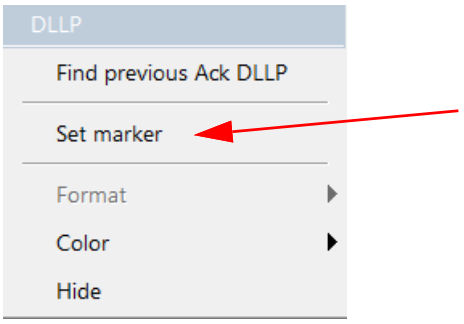
Functionality of Markers

The markers functionality allows you to add markers to:

- Whole packets or frames
- Specific Cells
- Specific values within a cell: Bytes, words, etc.
- The Timestamp of a Packet

You can add attachments to markers.

Right-click on any cell of a packet and select **Set Marker** from the menu as shown below.



The Create Marker dialog displays (see Figure 10.2 on page 664).

Set New Marker

Markers are useful to identify specific points in the data. By default markers follow a numbering convention but can be renamed. Markers can also be inserted by using the keyboard (see Figure 10.2 on page 664):

- Hover your mouse pointer over a packet and press **Ctrl+K** to insert a marker for that packet.
- Click a packet to select it and press **Ctrl+L** to insert a marker for that packet.

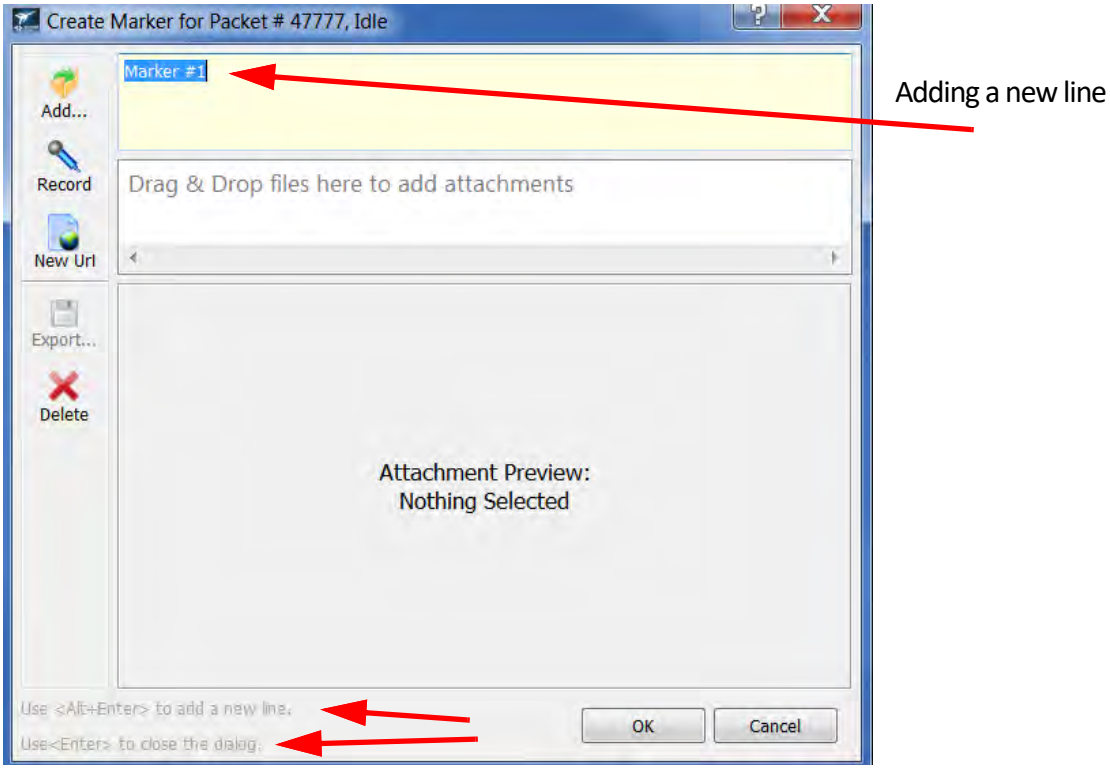


Figure 10.2: Create Marker for Packet Dialog

Click **Enter** to close the Marker dialog.

Click **ALT > Enter** to add a new line.

As shown above you can:

Add...	Add icon. Click on this icon to add any file. See “Adding an Attachment” on page 665.	Export...	Export icon. Click on this icon to export an attachment.
Record	Record icon. Click on this icon to record audio. See “Recording an Audio File” on page 665.	Delete	Delete icon. Click on this icon to delete an attachment
New Url	New URL icon. Click on this icon to add any URL.		

10.6.2 Attaching Markers

You can attach a discrete piece of information/data to a marker, for example, a text description or file, an attachment of a trace file by a predefined order, video or audio files, URL links or any other files. You can also remove an attachment from a Marker.

10.6.3 Adding an Attachment

Perform the following steps to add an attachment to a marker:

1. Right-click on any cell in the trace and select **Set Marker.**
   The Create Marker window displays (see Figure 10.3 on page 665).
2. Click on the **Add** icon.
   The **Add File to the Marker** dialog displays.
3. Go to the file and select it to add it to the marker as an attachment.
4. Click **Open**.
   The file will appear in the Create Marker for Packet... dialog. The Marker # appears in the top panel, the icons are displayed in the second panel and you can click on the icon on the third panel to view the file you are about to attach.
5. Click **OK** to add the attachments.

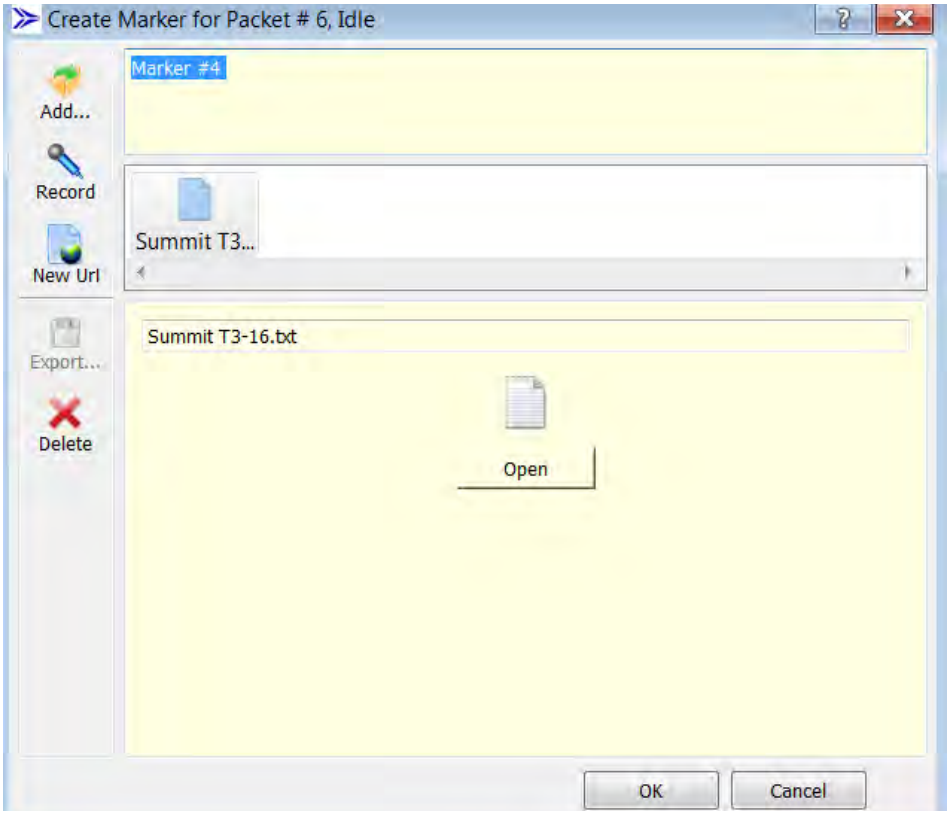


Figure 10.3: Create Marker for Packet Dialog

10.6.4 Recording an Audio File

The audio quality supports voice attachment and is not designed for high-quality audio Playback of audio content is not limited and depends on the formats supported by the installed playback engine.

Click the record icon and speak into the microphone to record an audio file.

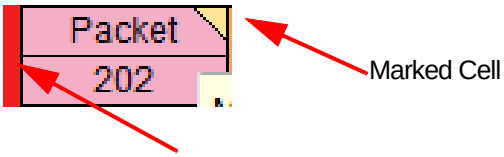
Note: This functionality is disabled if a microphone is not installed.

10.6.5 Video Files Supported

The user can attach video clips to the trace file ("add to the marker"). The playback of the Video clips is limited to the formats that are supported by the video codecs installed in the system.

10.6.6 Attachment Types and Visualization

The markers are represented graphically by a yellow triangle at the top right of the marked item and a red vertical bar at the left-most cell of a packet as shown below.



A marker may comprise any number of attachments of any types.

10.6.7 Embedded Attachments to a Marker

Embedded files are attached to the item marked and transported with the trace. You can embed the following types of files to a marker:

- Audio Files
- Video Files
- Image Files
- YouTube Files
- Web Pages
- Text Attachments
- Other Attachments

Attachments are embedded in the marker and saved in the trace file. Once attachments are placed in a marker, the marker can then be presented to a user in a story structured form. On opening the marker the window resembles the marker editing dialog.

Note: The use of Audio and Video markers is limited to the file types supported on a user's system. CATC Walk has been tested with .mp3 and .wmv files, which are supported by Windows as installed. If additional codecs are installed, they should also work, but it is the user's responsibility to choose formats that will work for whomever they intend to exchange CATC trace files (no different than email attachments in this regard). Because of this dependency on installed codecs, there are situations where bugs in the codecs supplied by Microsoft or third-party applications can prevent proper operation of the Teledyne LeCroy PCIe Protocol Analysis application. See the Teledyne LeCroy PCIe Protocol Analysis Application Read-Me file for more information if you have problems with application crashes, etc.

10.6.8 Viewing Attachments of a Marker

If you hover over the marked cell (yellow triangle at the top right of the marked item), refer to "Attachment Types and Visualization" on page 666, a window pops up displaying the contents of the marked cell (see Figure 10.4 on page 667).

While hovering over the marked cell, it can start playing the start of the audio or video file, but it will stop after a short time due to the Analyzer's host system timeout for Tooltips. You must click on it to open the audio or video attachment for further listening or viewing.

To view an attachment you can click on any of the icons in the attachment bar and or you can double-click on the icon itself to open the attachment.

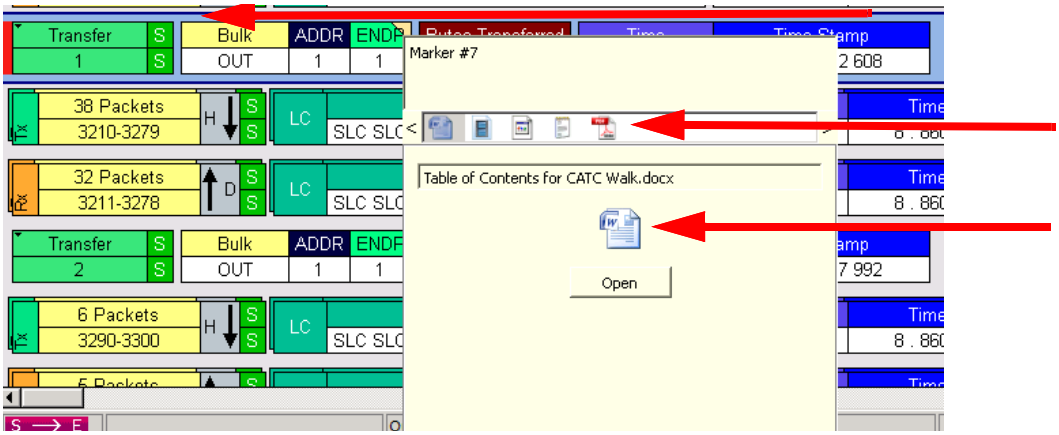


Figure 10.4: Pop-up Displaying Marker Contents

Text

The text attachment is displayed in the icon bar and in the main pop-up window. Text attachments are always shown at the top. The attachment file name is displayed in the field as shown below.

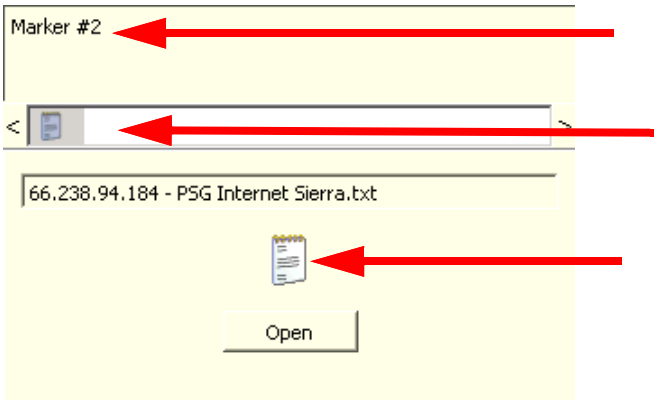


Figure 10.5: Text Attachment Pop-up Window

If there is no attachment, **No Attachments** displays in the status bar at the bottom.

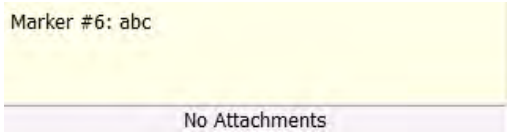


Figure 10.6: No Attachments Pop-up Window

If there are attachments, the status bar is hidden. You can move the cursor to an attachment icon in the list view and a preview of the attachment starts (see Figure 10.7 on page 668).

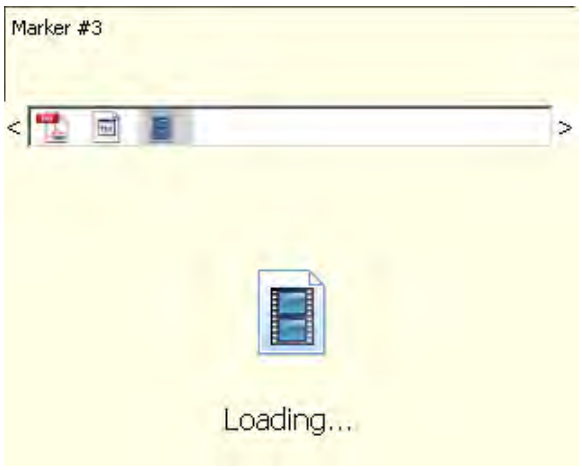


Figure 10.7: Preview Attachments Pop-up Window

Audio

Audio snippets that are recorded and attached to certain point of interest in a trace can be played. The basic Play, Start, Stop, Pause buttons are displayed to listen to the audio file.

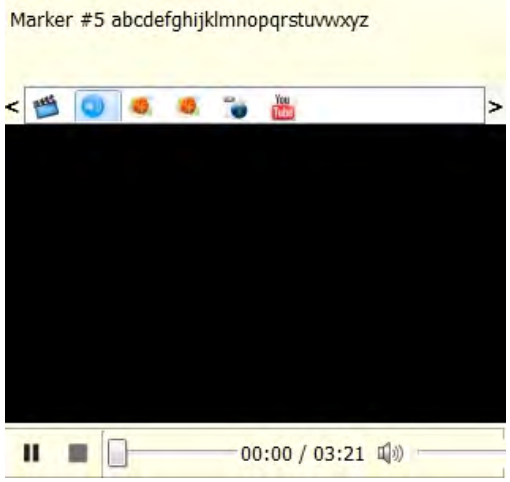


Figure 10.8: Adding a Marker that is an Audio Snippet

Video

Video clips that are recorded and attached to certain point of interest in a trace can be played. The video is embedded in the tooltip with simple playback controls.



Figure 10.9: Adding a Marker that is a Video Clip

File Attachment

You can attach any kind of file, including images, PDFs, documents, media files, etc.

URL Link

You can specify a URL that links to a web page (i.e., YouTube), a network location, or a local file-system location. See Figure 10.10.

Web Link

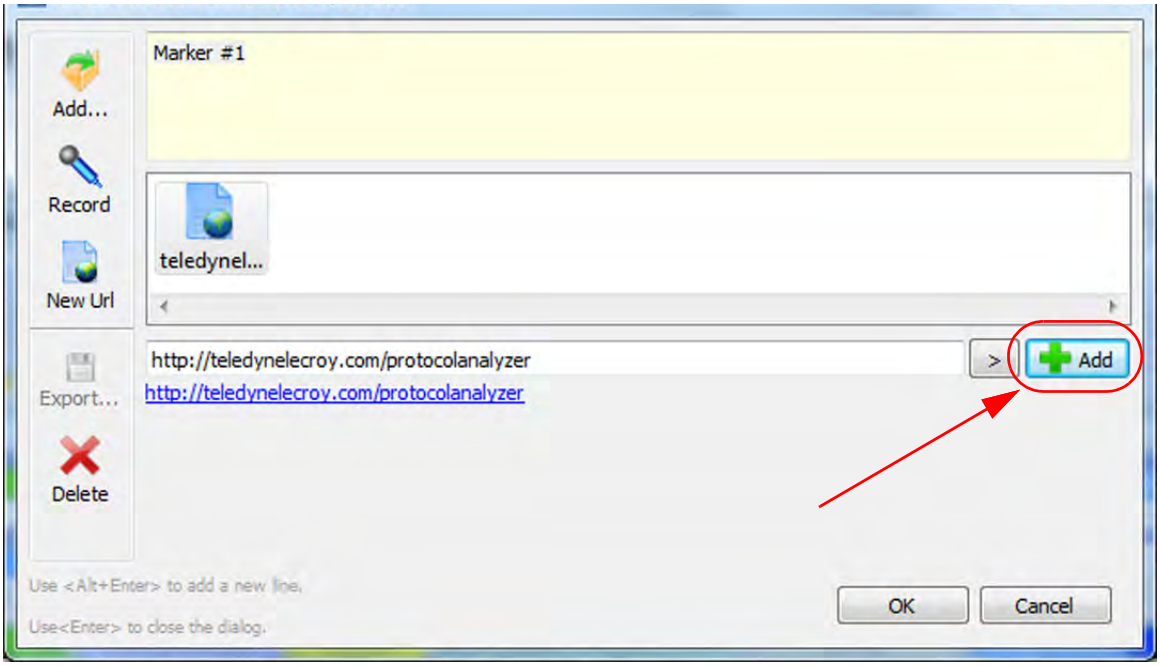


Figure 10.10: Marker: URL Link

After you add the URL marker to the Packet, when you click on the URL it will open in a separate browser window. See Figure 10.11.

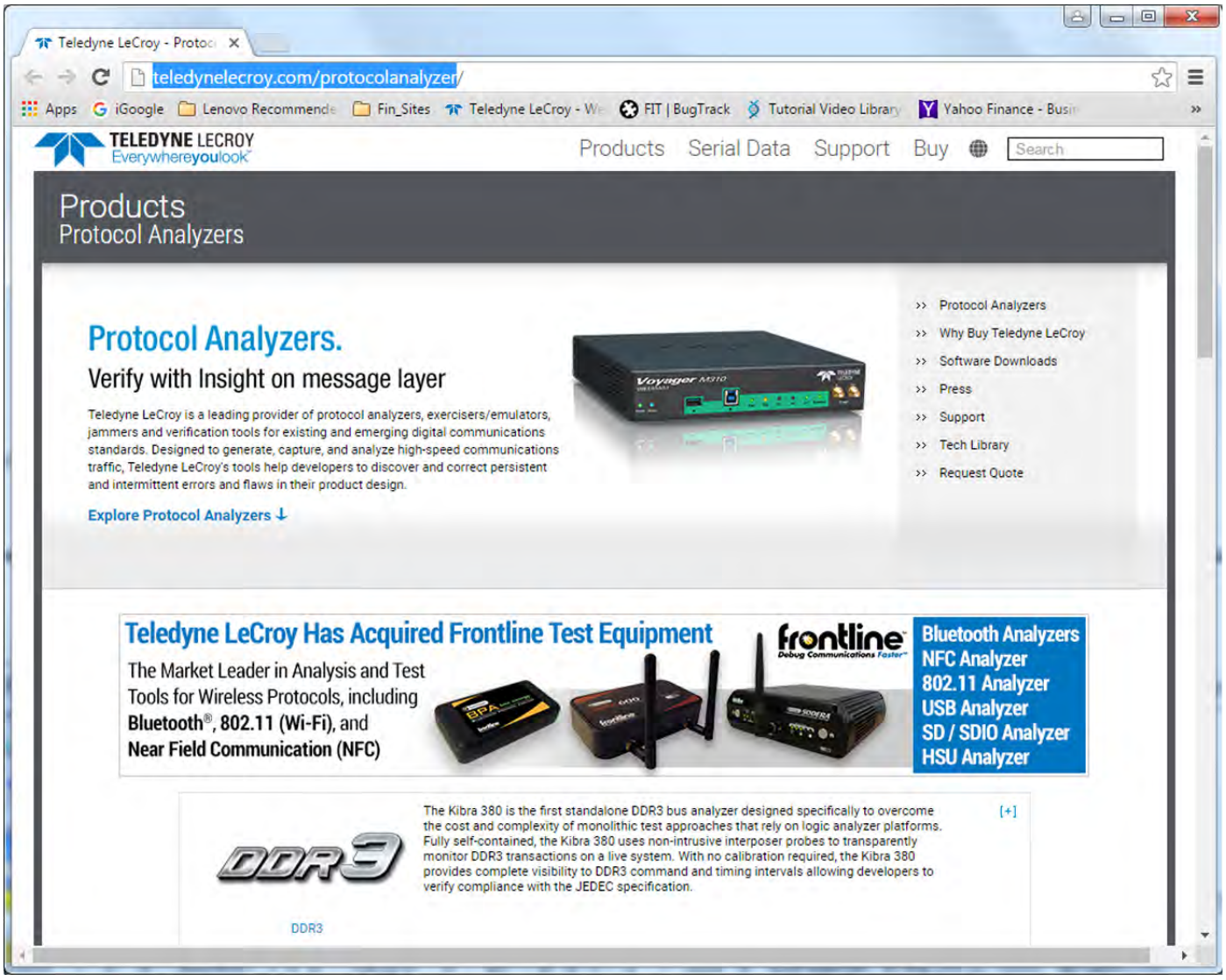


Figure 10.11: Opening a URL Marker in a Separate Window

YouTube Video

YouTube's video player is embedded for YouTube Video playback. See Figure 10.12.



Figure 10.12: Adding a Marker that is a YouTube Video

Images

The image is embedded in the trace. See Figure 10.13.



Figure 10.13: Adding a Marker that is an Image

Other Attachments

Click the **Open** button to open the attachment file with the system's default application for that file type. See Figure 10.14

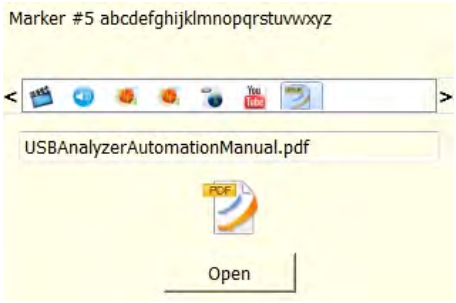


Figure 10.14: Adding a Marker: System Default

10.6.9 Edit Marker

To edit a marker, right-click on the marked item and select **Edit marker** from the menu or **Ctrl + L**. The Edit Marker dialog displays. This Edit Marker window can be used to edit one marker at a time.

You can do the following in the Edit Marker dialog:

- Edit text attachment.
- Record audio attachment.
- Add URL link attachment
- Add a file attachment. Click on **File** and click the **Open** button or drag and drop the file.
- Preview audio/video/image/URL/YouTube attachment or open other files with system default application.
- Save an attachment to a file.
- Remove attachment.



Figure 10.15: EDIT Marker for Packet Dialog

10.6.10 All Markers Dialog

Select **Search > Go to Marker > All Markers** or press **Ctrl + M** to display a list of all the markers in the file. The dialog uses a tree structure to show packets, fields and markers (see Figure 10.16 on page 674). The features of the Markers dialog are:

- ❑ All Markers are displayed.
- ❑ All attachments within the marker are displayed. Hovering over the marker displays a tool-tip displaying the size of all the attachments.
- ❑ You can collapse or expand the item marked to view the attachments.
- ❑ The Time and size of audio and video files are displayed.
- ❑ You can edit Playlists from this window.
- ❑ You can edit, delete a marker or delete all markers from this location.
- ❑ You can filter attachments within the marker.
- ❑ You can select a range of markers by clicking **Shift** and selecting a range.
- ❑ You can select multiple markers by clicking **Ctrl** and selecting individual markers.
- ❑ Double-click on a marker to go to that marker in the trace and close the dialog.
- ❑ You can sort by Timestamps (or any other displayed title) in ascending or descending order. See Figure 10.17 on page 675.

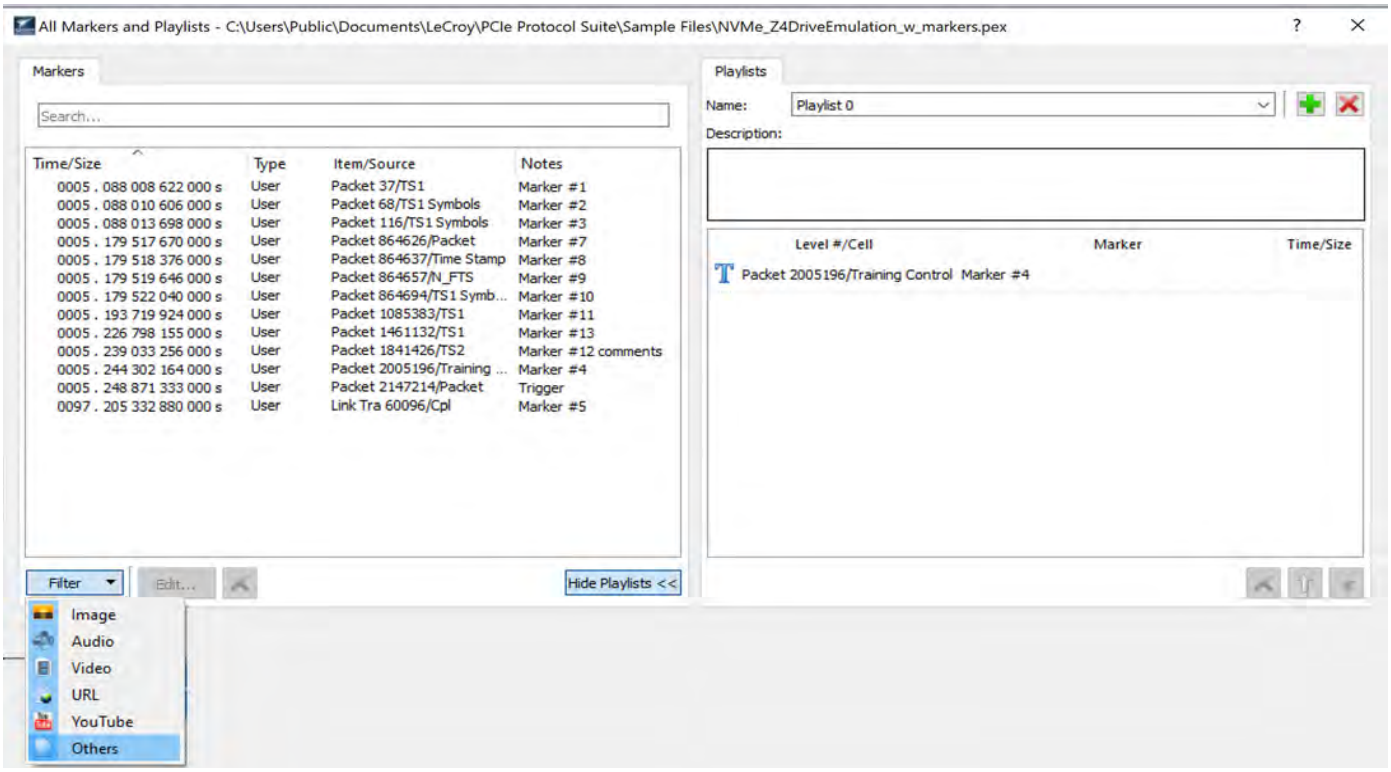


Figure 10.16: All Markers and Playlists Dialog

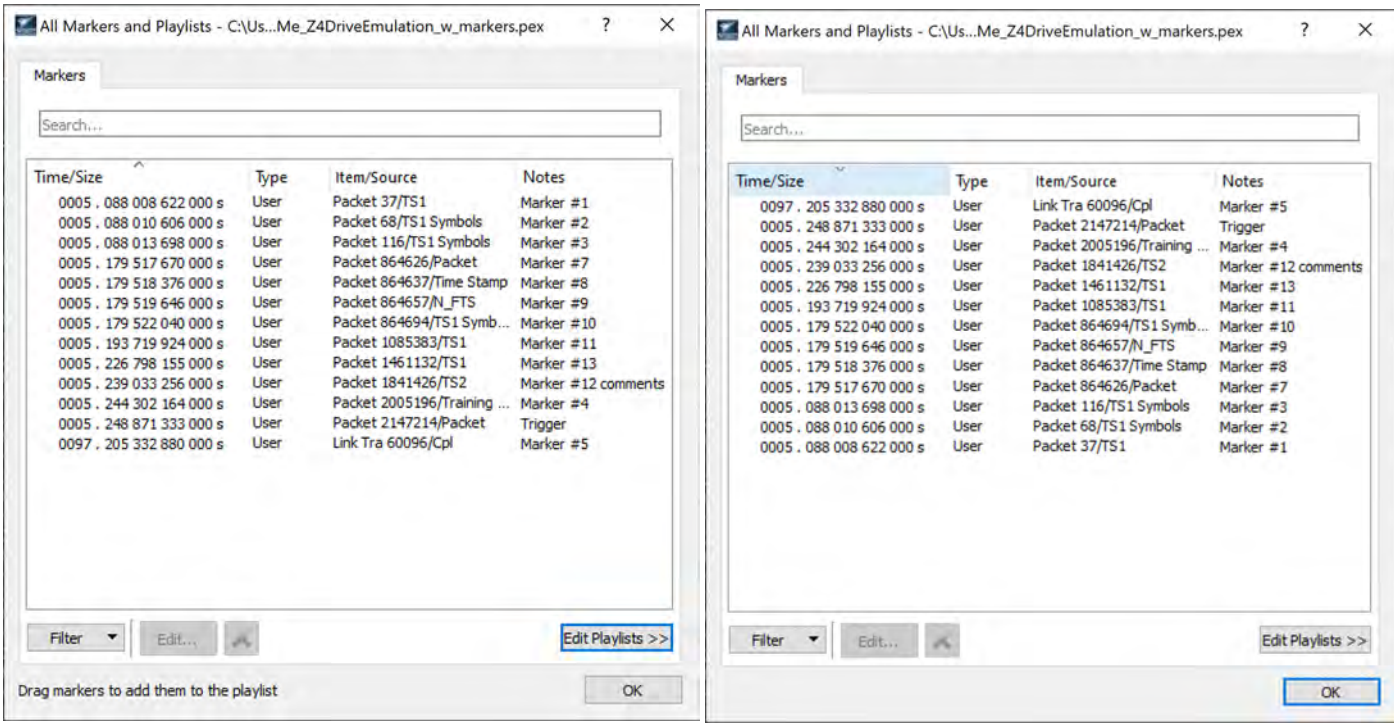


Figure 10.17: Markers Sorted by Timestamps in Ascending and Descending Order

You can filter to show or hide text, image, audio, video, URL, YouTube videos and other files.

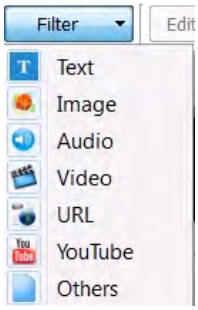


Figure 10.18: Filter Dialog

Clicking delete on markers to delete markers with attachments displays the Delete Marker(s) dialog. Checking the “Don’t ask again” checkbox will not display this confirmation dialog again.

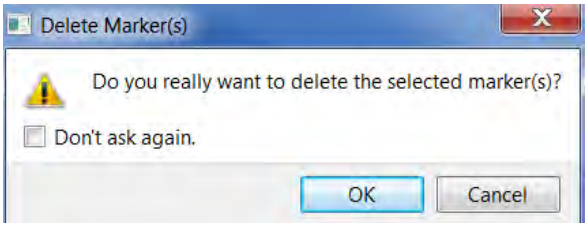


Figure 10.19: Confirmation Dialog

10.6.11 CATC Walk Playlist

This feature allows users to configure sequences of attachments into playlists. Any arbitrary order of attachments are allowed, and there are no limits on the number of playlists supported. This feature can be used for collaborating among developers as well for training, support and marketing purposes.

To access a playlist click on the **View** menu in the top toolbar of application, select **CATC Walk** and then select **Manage Playlists** as shown below.

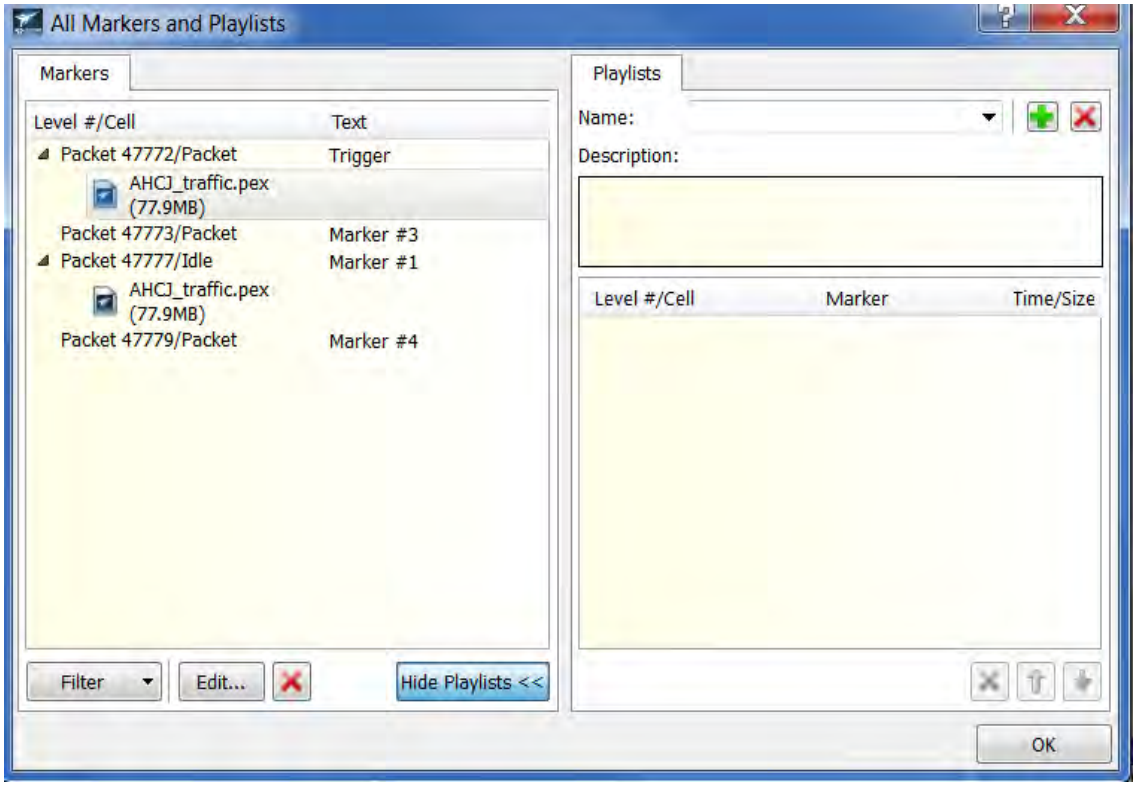


Figure 10.20: Edit CATC Walk Playlists Dialog

10.6.12 Playlist Functionality

You can do the following to manage playlists:

- Remove or edit current playlists
- Edit the playlist name
- Edit the playlist description
- List the sequence of attachments in current playlist
- List of all available attachments and drag/drop to a playlist.

As shown in the previous figure the Playlist window lists the markers with their attachments on the left and the playlist on the right.

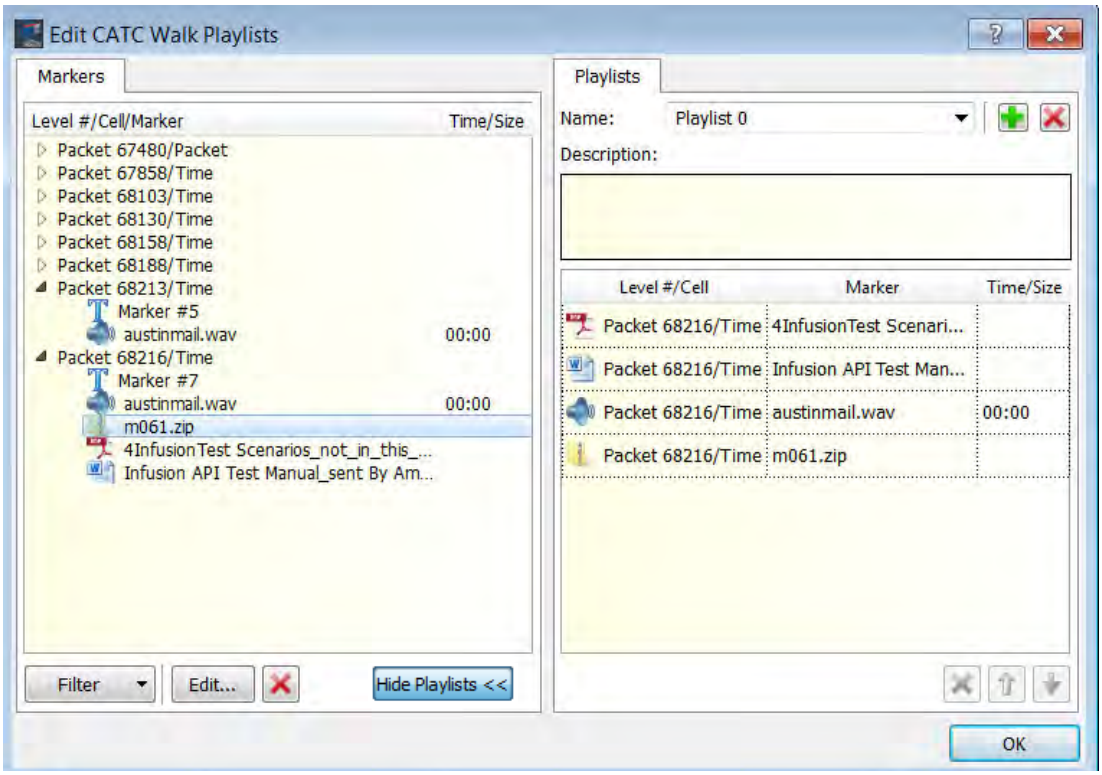


Figure 10.21: Edit CATC Walk Playlists Dialog

You can drag and drop and item or attachment from the **Marker** panel into the **Playlist** panel and build a story. Give a description of the playlist in the **Description** field and you can give a name to the playlist in the **Name** field.

You can add a new playlist by clicking on the green plus sign (+) on the right top corner of the Playlist panel, or delete a playlist by clicking the red (x) button.

If you have more than one playlist saved click on the Name drop-down arrow to select it. The drop-down menu lists all the available playlists

10.6.13 Playback Window

To playback a playlist, click on the **View** menu in the top toolbar of application, select **CATC Walk** and then select **Play > Playlist 1** as shown below.

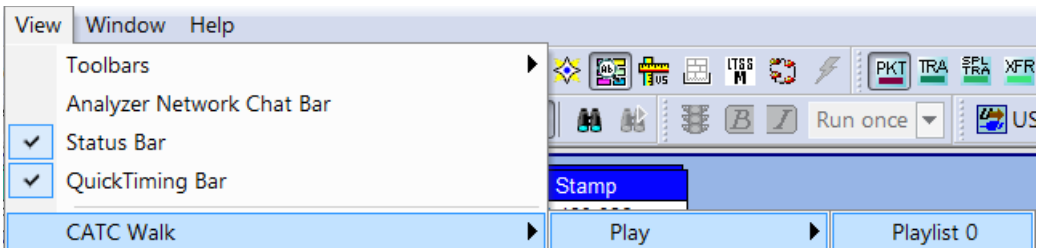


Figure 10.22: View Dialog

The attachment item starts to play in the Playback window (see Figure 10.23).



Figure 10.23: Playback Window

The playback window is re-sizable. The close button at the top right corner and the size grip for resizing at the bottom right corner will hide automatically when moving the cursor out of the window.

Users can provide commentary to a captured trace, converting it into a script or a story and can transfer this meta-information to others.

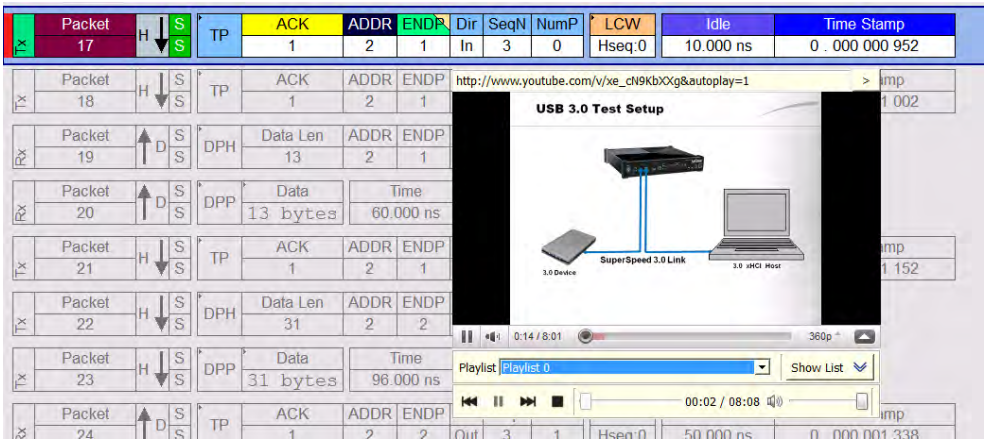
Playlist Playback Controls

The playlist playback control buttons are (see the screen capture on the next page):

- Play/Pause
- Stop
- Jump to Next attachment
- Jump to Previous attachment
- Seek slider for seeking to positions in media streams
- Volume slider
- Playback speed slider (for text attachments)

As a playlist is played back, the playback window is displayed in close proximity to the marked area, just like a regular tooltip window.

As the playback progresses, the view jumps to the element corresponding to the current attachment being played and the marked element is highlighted. During playback the user is prevented from interacting with the trace. To reinforce this restriction, the trace view is grayed-out visually, and only the packet with the item corresponding to the current attachment is colorized.



Playlist Playback View

10.7 Go to NVMe Transactions and Commands

The Go to NVMe Transaction and NVMe Command tabs in the Search menu provides a quick way to search for both NVMe Transactions and NVMe Commands.

10.7.1 NVMe Transaction

The NVMe search capability can also search for the following types of NVMe Transactions:

- Controller Registers
- Other NVMe Entities
- Doorbell Registers
- Admin Submission Command Set
- NVM Submission Command Set
- Completion Queue Entry
- NVMe Errors

As shown in Figure 10.24 on page 680

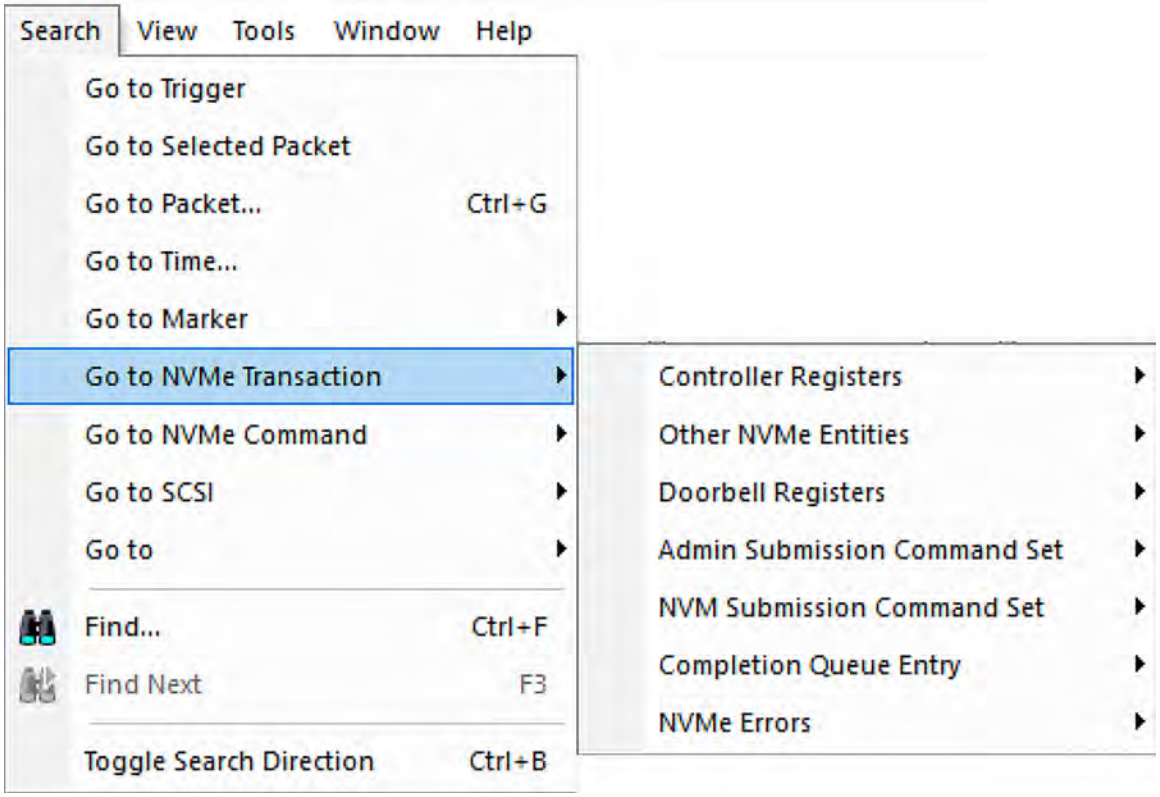


Figure 10.24: Search: NVMe Transaction Types

10.7.2 NVMe Command

The NVMe search capability can also search for the following types of NVMe Commands:

- Admin Command Set
- NVM Command Set
- Status
- Errors
- TCG Types
- TCG Method
- TCG Invoker
- TCG Com ID
- TCG Ext Com ID

As shown below in Figure 10.25 on page 681.

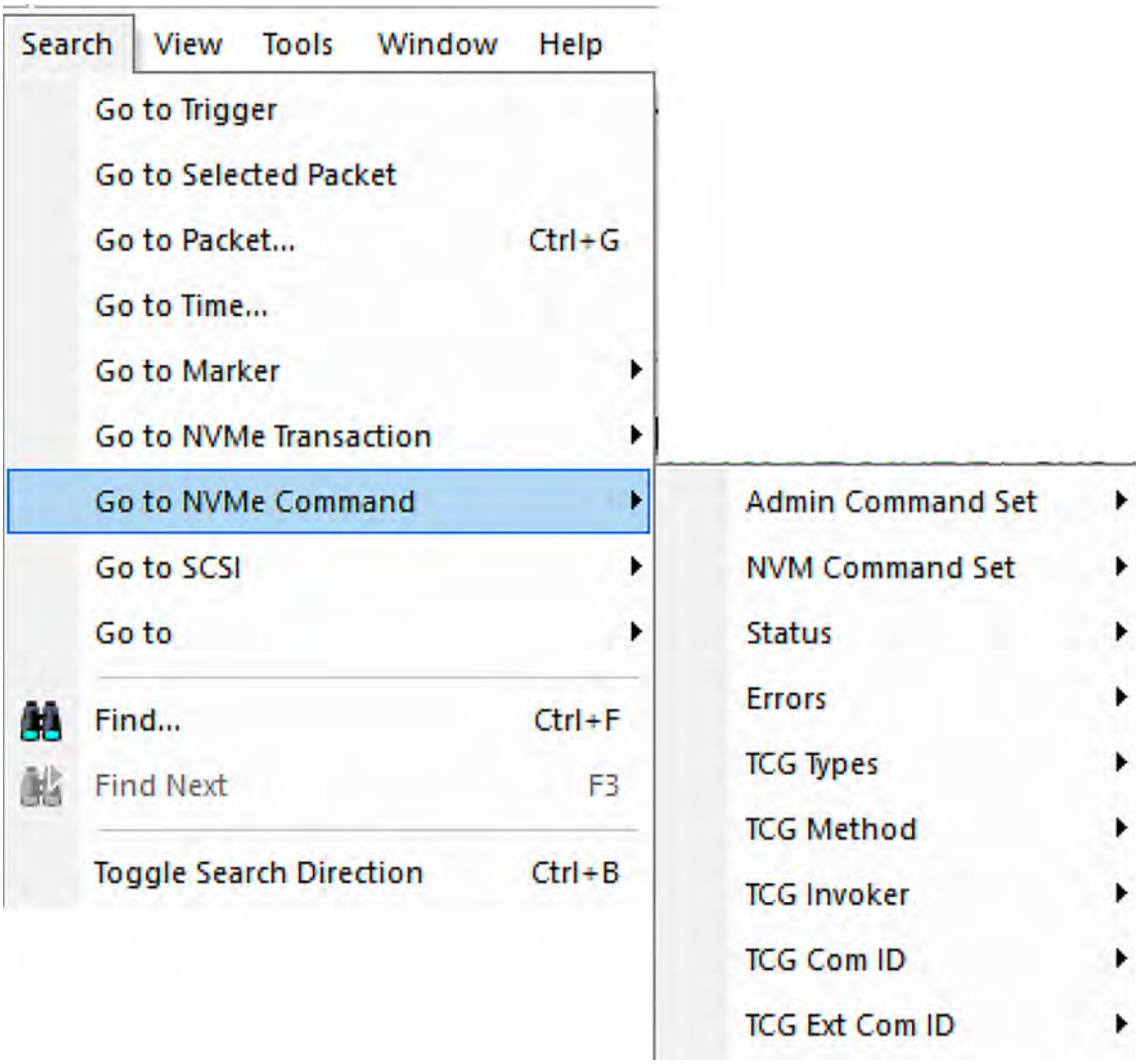


Figure 10.25: Search: NVMe Command Types

10.8 Go To SCSI Menu

The **Go To SCSI** menu in the Search menu provides a quick way to search for a packet based on a SCSI commands and sub-commands. You can search for the following types of events:

- SCSI Operation
- Command Status
- Task Management
- Task Management Response
- Error
- SCSI Logical Unit Number

10.9 Go To Menu

The **Go To menu** in the Search menu provides a quick way to search for a packet based on a simple condition. You can search for the following types of events:

- TLP Type
- DLLP Type
- Ordered Set
- Link Event
- OBFF Message
- Traffic Class
- DLLP Virtual Channel
- TLP Virtual Channel
- Direction
- Speed
- Link Width
- Requester ID
- Completer ID
- Data Lengths
- Errors

10.9.1 Example: Search -> Go to -> Link Event -> Link Up/Link Down

Use the Search -> Go to function to find Link Event: Link Up or Link Down.

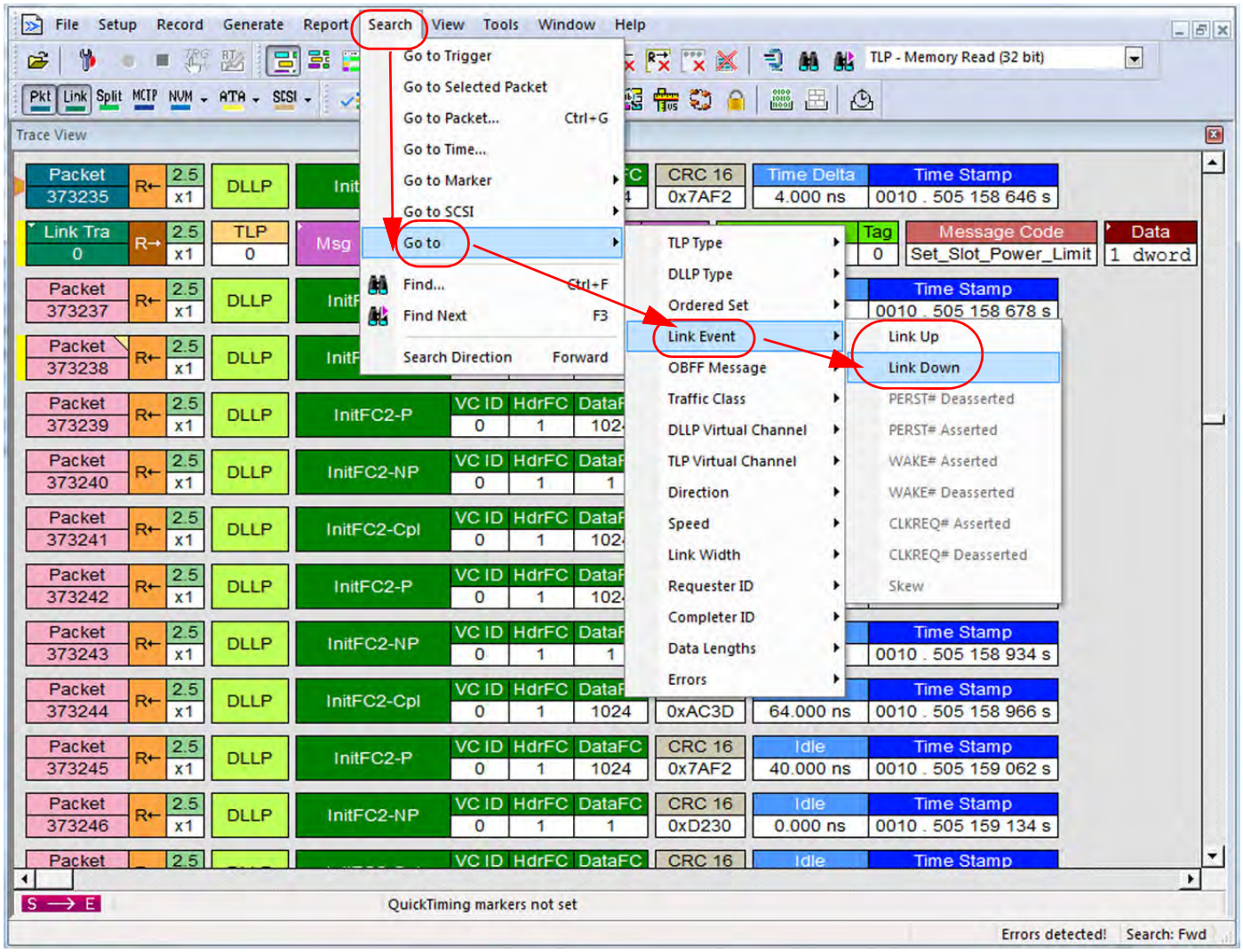


Figure 10.26: Search -> Go to -> Link Event -> Link Up / Link Down: Set Up Search

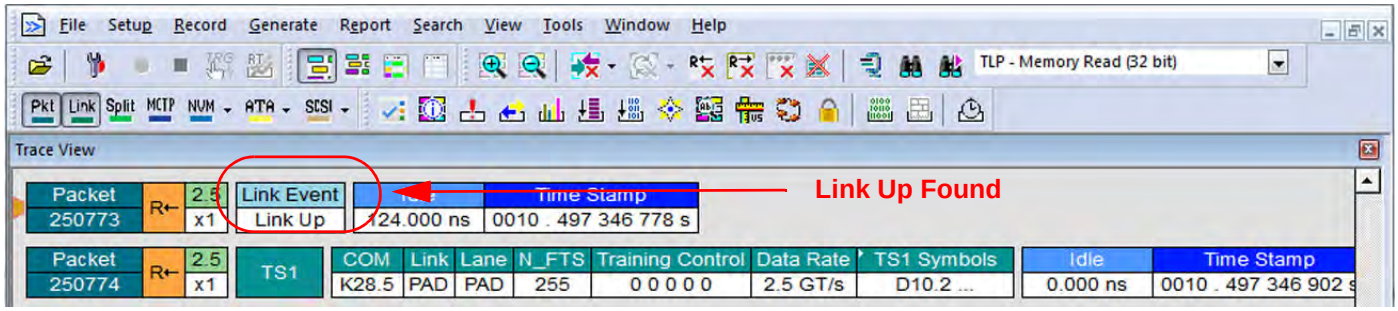


Figure 10.27: Search -> Go to -> Link Event -> Link Up: Found

10.9.2 Example: Go To CXL

Another example of the Search capability is Search -> Go to -> CXL Type. See Figure 10.28

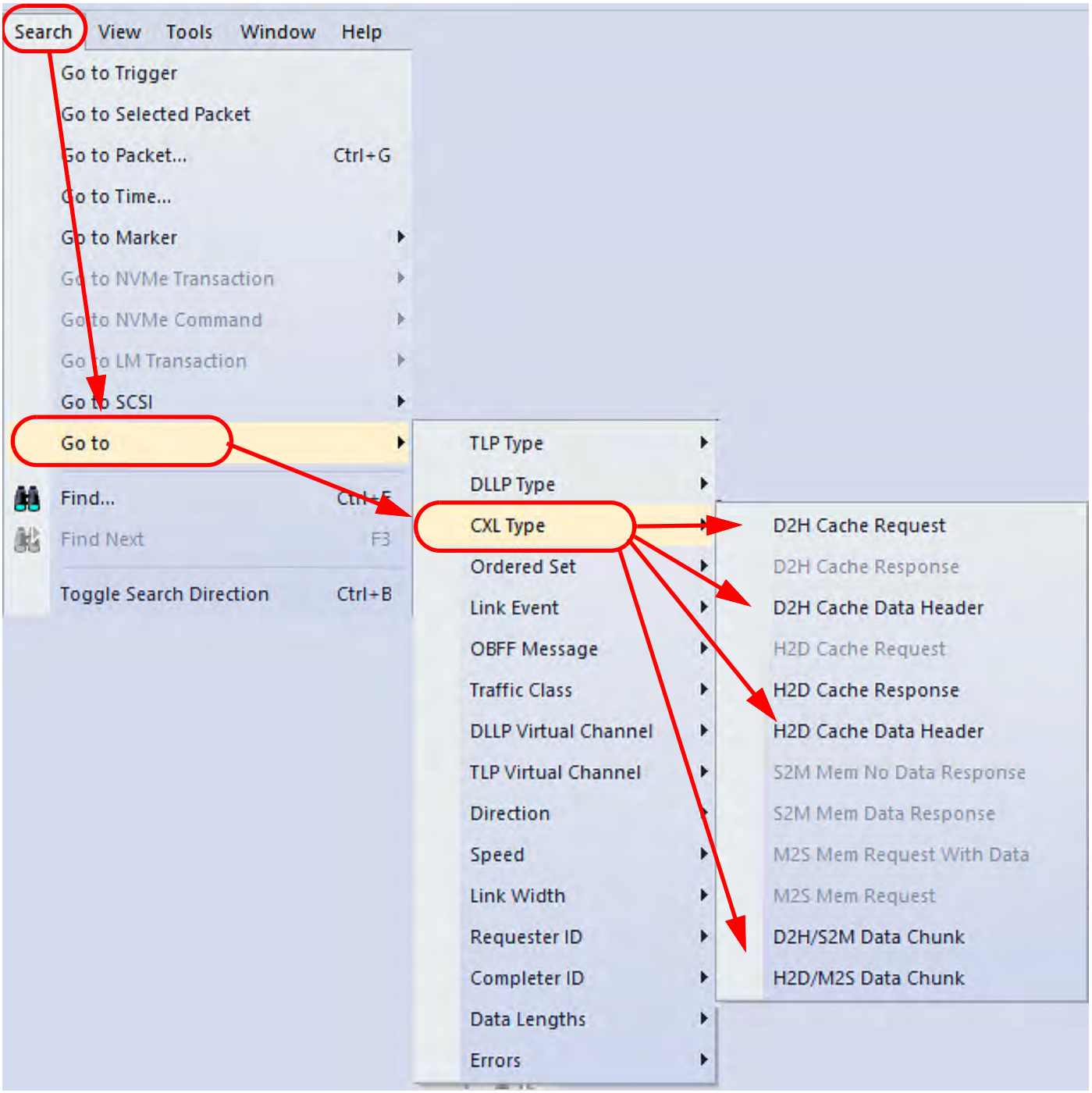


Figure 10.28: Search -> Go to -> CXL Type

10.10 Find

Find allows you to conduct complex searches in a CATC Trace. You can search by protocol level (Packets, Link Transactions, Split Transactions, NVMe, PQI, AHCI, ATA) as shown in Figure 10.29.

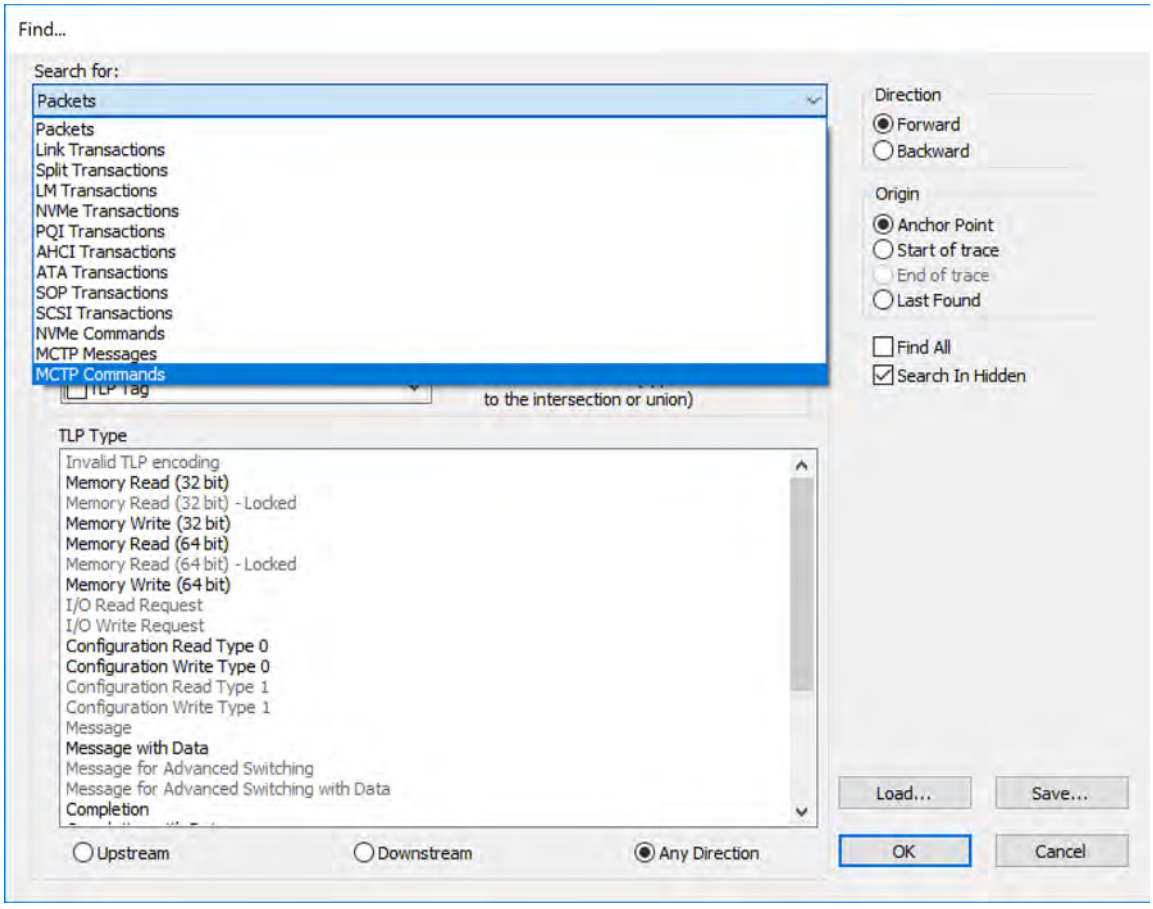


Figure 10.29: Find: Search for

You can search for packets by Event Group: TLP Type, TLP Header, TLP Prefix, TLP Requester ID, TLP Completer ID, TLP Data Pattern, TLP Data Lengths, TLP Tag, TLP Sequence Number, PMUX Channel ID, DLLP Type, DLLP Header, DLLP Virtual Channel, ACK/NAK Seq Number, Ordered Sets, Link Event, OBFF Code, Direction, Errors, TS1 Data, TS2 Data.

You can search for link transactions by Event Group: TLP Type, Traffic Class, Virtual Channel, Direction, Requester ID, Completer ID, Status, Tag.

You can search for split transactions by Event Group: TLP Type, Traffic Class, Virtual Channel, Direction, Requester ID, Completer ID, Status, Tag, Address.

You can search for Lane Margining transactions by Event Group: Margin Commands, Margin Type, Receiver Number or Errors. Each of these Event Groups has a numbers of different event types. See Figure 10.49 on page 703.

You can search for NVMe transactions by the following Event Groups: Controller Registers, Queue IDs, Command IDs, Doorbell Registers, Admin Submission Command Set, NVMe Submission Command Set, Completion Queue Entry, and PRP.

You can search for PQI transactions by Event Group: TLP Type, Traffic Class, Virtual Channel, Direction, Requester ID, Completer ID, Status, Tag, Address.

You can search for AHCI transactions by Event Group: AHCI Register ID, AHCI Port Number, AHCI Slot Number, AHCI Port Multiplier Port, AHCI Raw Address AHCI Direction and, AHCI Errors.

You can search for ATA transactions by Event Group: ATA Register Type, ATA Port Number, ATA Slot Number, ATA Raw Address, ATA port Multiplier Port, ATA Interruption Reason, ATA Error Type ATA Input/Output, ATA Payload Portion, ATA CFIS Fields, ATA RFIS Device to Host Fields, ATA DSFIS Fields, ATA PSFIS Fields, ATA SDBFIS Fields.

You can search for SOP transactions by Event Group: SOP Information Unit ID, SOP Errors.

You can search for SCSI transactions by Event Group: SCSI Operation, Command Status, Task Management, Task Management Response, Errors, SCSI Logical Unit Numbers.

You can search for NVMe Commands by Event Group: Admin Command Set, NVM Command Set, Submission QID, Completion QID, Status, Errors, NVM Command, NVM Payload Portion, TCG Types, TCG Method, TCG Invoker, TCG Com ID or TCG Ext Com ID. See “Example: Search for NVMe Command” on page 705.

The options Union, Intersection, and Exclusion allow you to create complex searches such as “Find x OR y” or “Exclude all x or y.”

To find an item:

1. Open a CATC Trace.
2. Open Find by selecting **Search > Find** from the menu or clicking  (see the following screen capture).

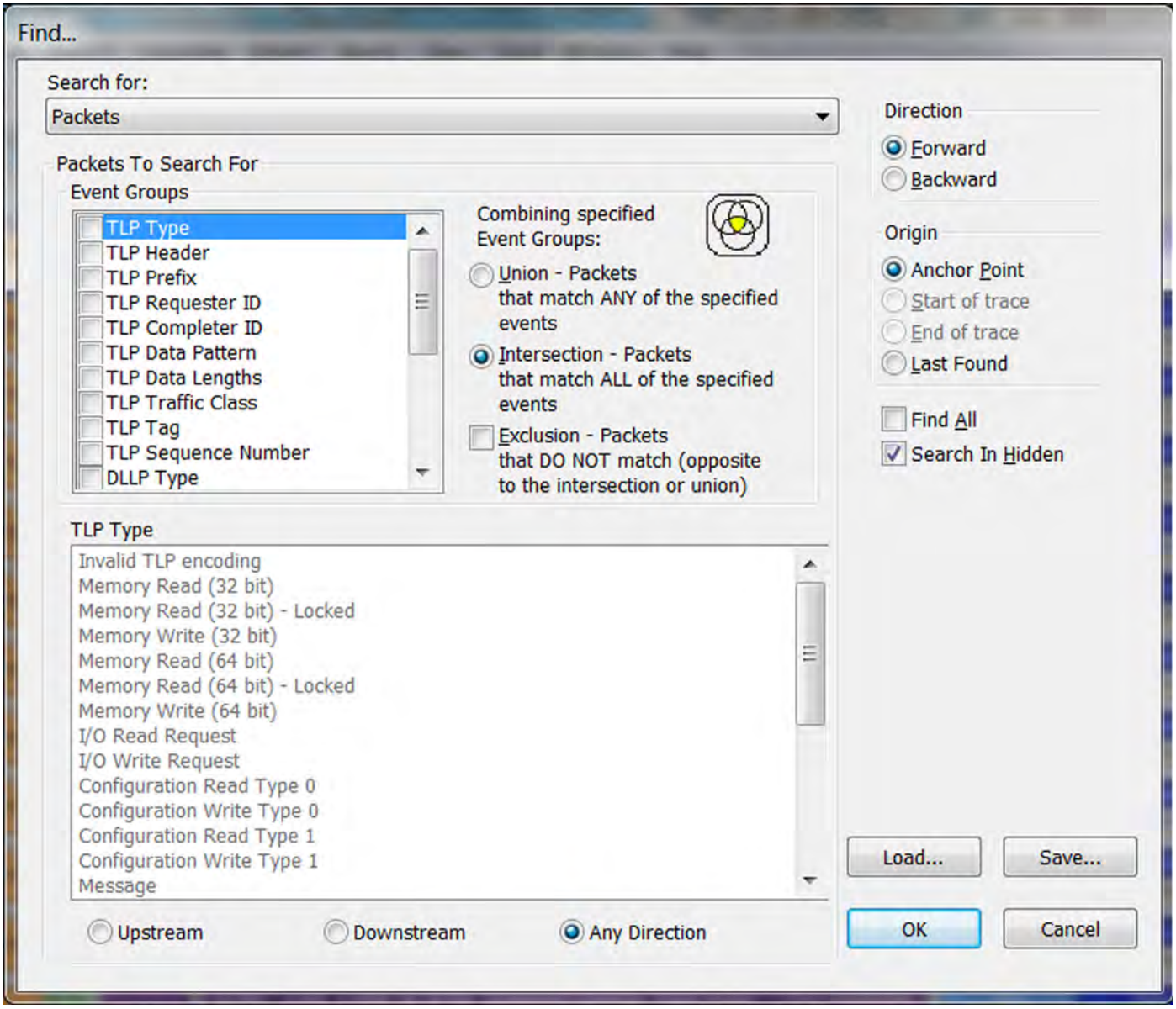
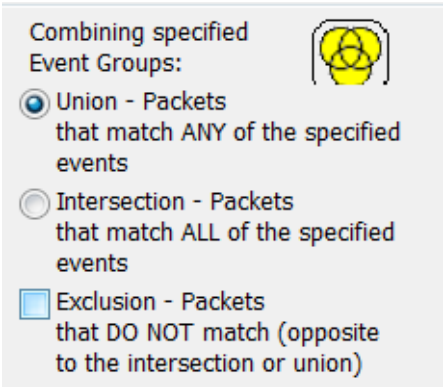


Figure 10.30: Find Dialog

3. From the Search For menu, select a display level such as **Packets**. To search multiple levels, finish steps 3 to 9, and then repeat 3 to 9 for each additional display level.
4. From the Event Groups menu, select an **Event Group**. The menu in the far right of the dialog is context sensitive and changes to reflect the options for that group.
5. In the menu in the far right, select one or more items.
6. Repeat Step 5 for each Event Group of interest for the selected display level.

7. Under Scope, select Current Segment or All Segments to reduce the scope of the search. This applies to old segmented traces, for newer traces leave this option in Current Segment.
8. Under Direction, select **Forward** or **Backward** to select a search direction.
9. Under Origin, select a starting point for the search.
10. Under **Combining Specified Event Groups**, select an option.



The options Union, Intersection, and Exclusion let you set conditions on your searches:

- **Union**: To search for **any** of the selected criteria.
  Example: “Find packets with ANY of the following characteristics …”
- **Intersection**: To search for **all** of the selected criteria.
  Example: “Find packets with ALL of the following characteristics …”
- **Exclude**: To **exclude** items from a search. This option works in conjunction with Union and Intersection. You select Union and Exclude to exclude any of the specified traffic. You select Intersection and Exclude to exclude all of the specified traffic.
  Example: “Exclude packets with ANY of the following …” or
  “Exclude packets with ALL of the following …”

11. Repeat Steps 3 through 9 for additional display levels.
12. **Find All** displays all matching packets or transactions in a separate view.
    NOTE: When **Find All** is checked, the reports display the information for the main trace, however, they do not include Search results.
13. **Search in Hidden** includes hidden packets or transactions in the search.
14. Click **OK**.

10.10.1 Event Groups for Packets

The Event Groups for Packets are:

- TLP Type
- TLP Header
- TLP Prefix
- TLP Requester ID
- TLP Completer ID
- TLP Data Pattern
- TLP Data Lengths
- TLP Traffic Class
- TLP Tag
- TLP Sequence Number
- PMUX Channel ID
- DLLP Type
- DLLP Header
- DLLP Virtual Channel
- ACK/NAK Seq Number
- Ordered Sets
- Link Event
- OBFF Code
- Direction
- Errors
- TS1 Data (see “Example: TS1 and TS2 Event Groups” on page 690)
- TS2 Data (see “Example: TS1 and TS2 Event Groups” on page 690)
- Message Code

Example: TS1 and TS2 Event Groups

Selecting TS1 Data or TS2 Data options allows further definition of the exact field contents to match via the three dialogs show below. The search algorithm will find the specified TS ordered set on any lane.

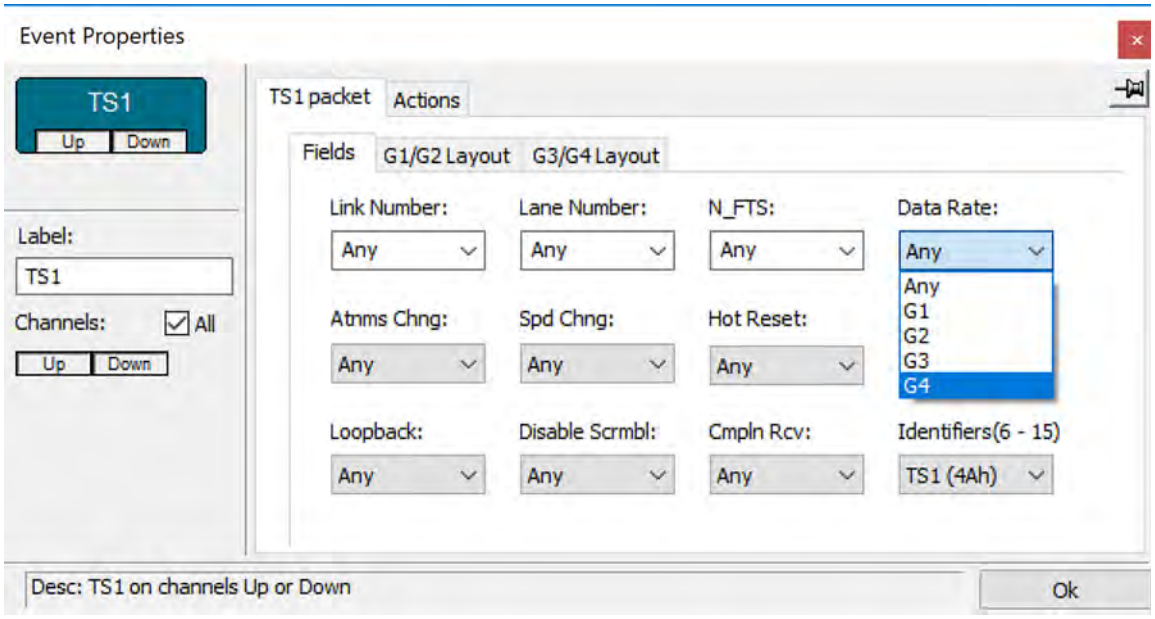


Figure 10.31: TS Data Fields Tab

Select parameters from the drop-down lists to use.

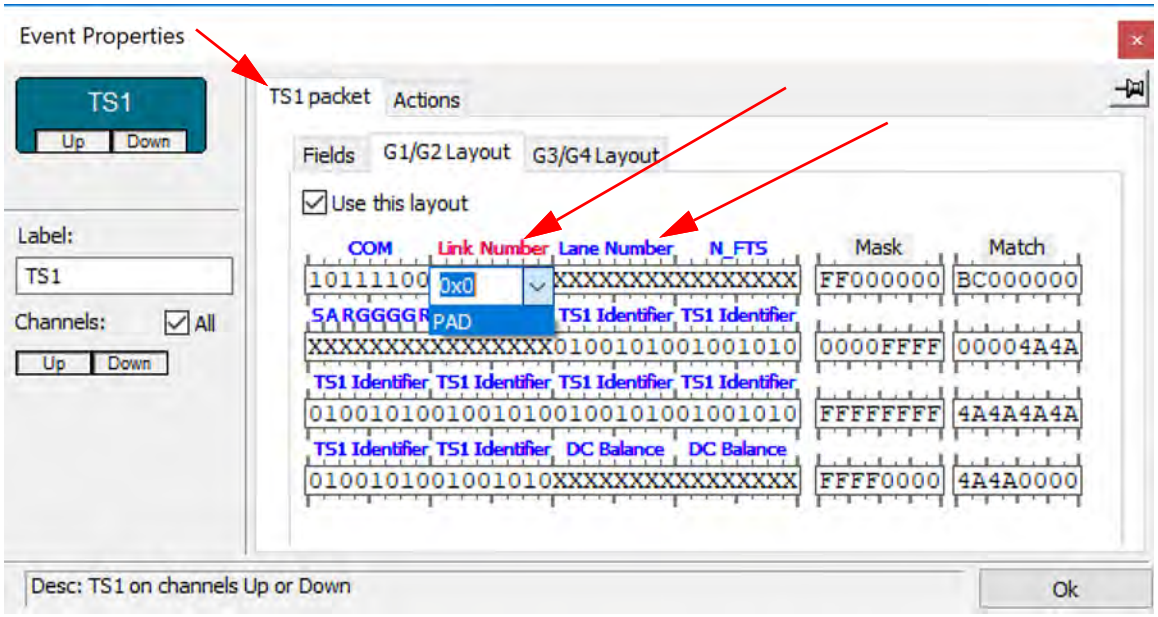


Figure 10.32: TS G1/G2 Layout Tab

Select parameters from the links to use and enter the mask and match values.

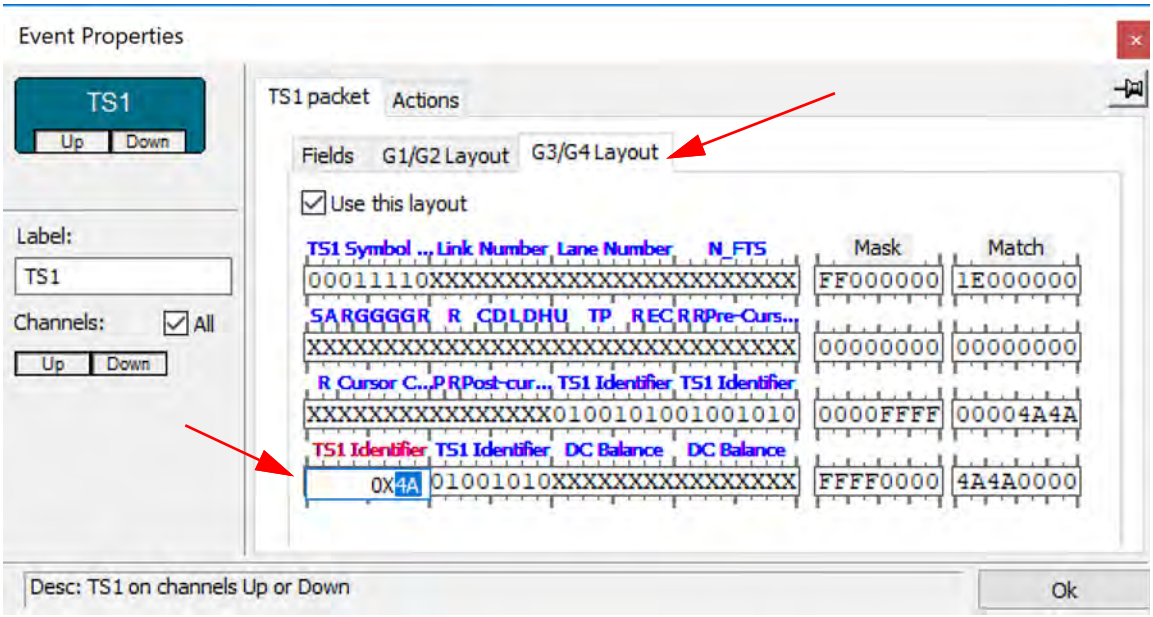


Figure 10.33: TS G3/G4 Layout Tab

Select parameters from the links to use and enter the mask and match values.

Example: TS1 Packet with G3 Speed and G3 Data Rate

In order to select TS1/TS2 packets for search/triggering on G3/G4 speed you need to set data for search/triggering to G3 (see Figure 10.34).

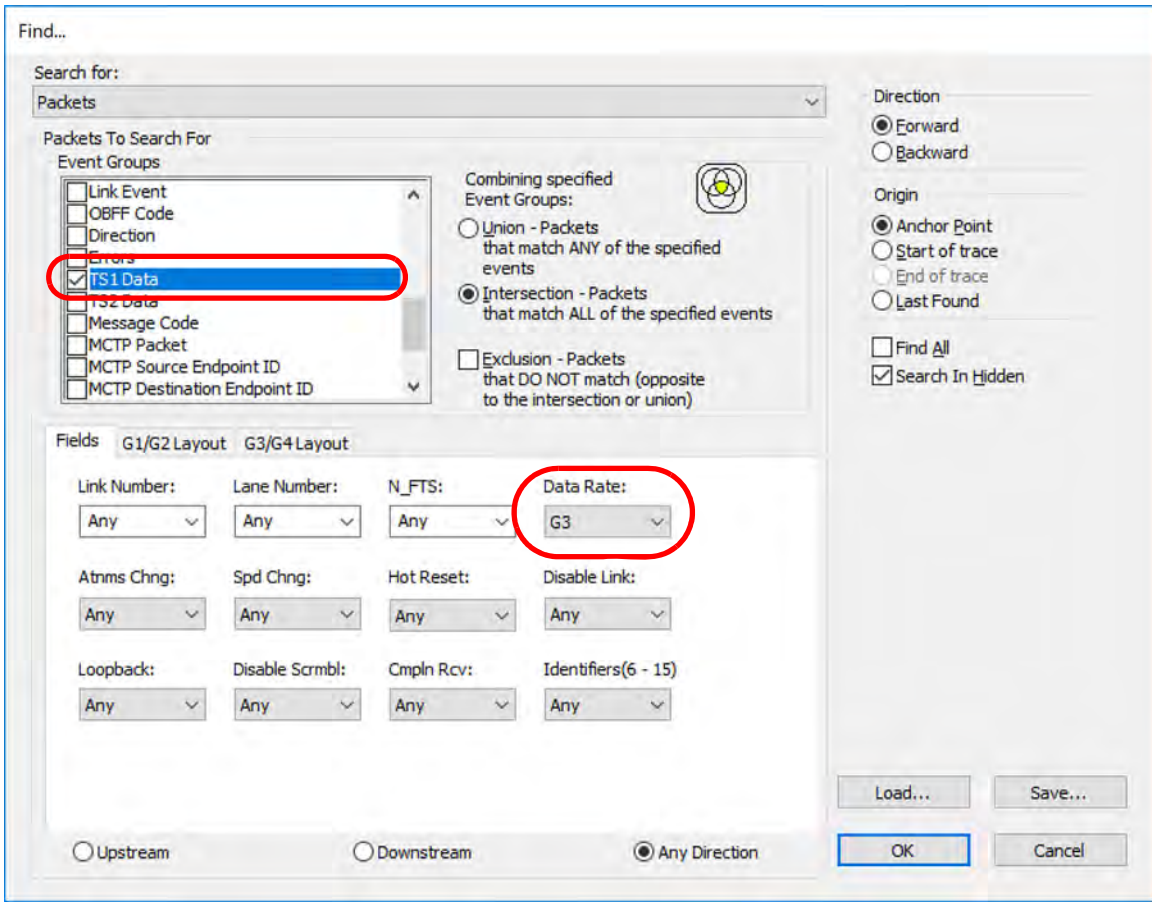


Figure 10.34: Set Search for: Packets -> TS1 Data and Data Rate G3

Set the Recording Options -> TS1 -> Event Properties with the same options. See Figure 10.35 on page 693.

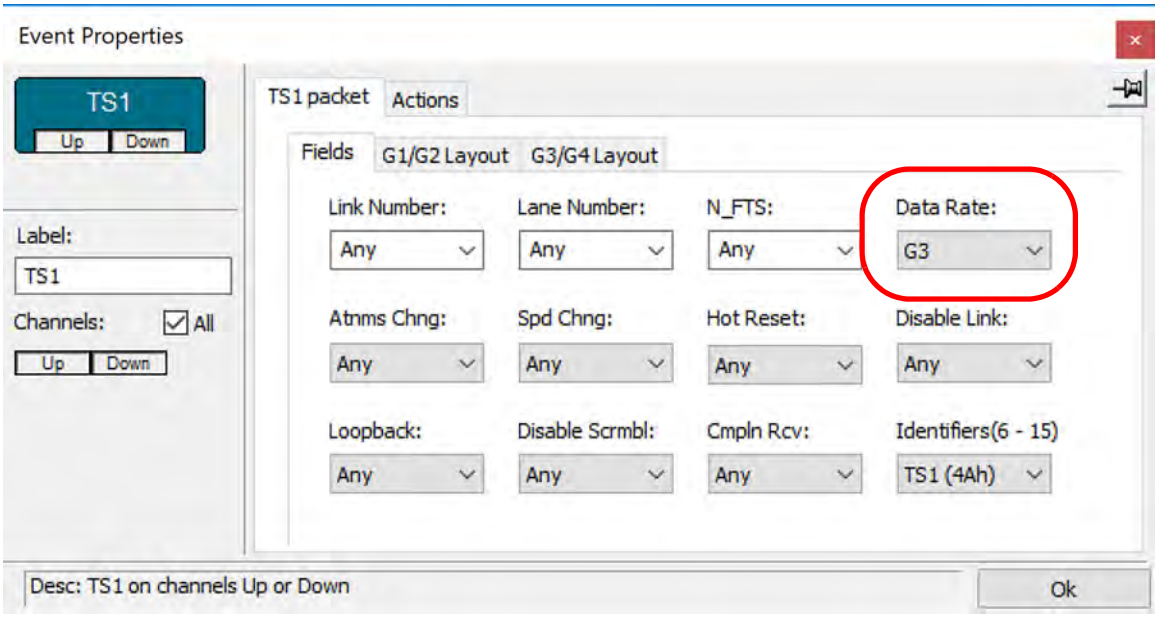


Figure 10.35: Recording Options: Event Properties -> TS1 Data Rate = G3

Uncheck the checkbox “Use this layout” in G1/G2 Layout tab (see Figure 10.36 on page 693).

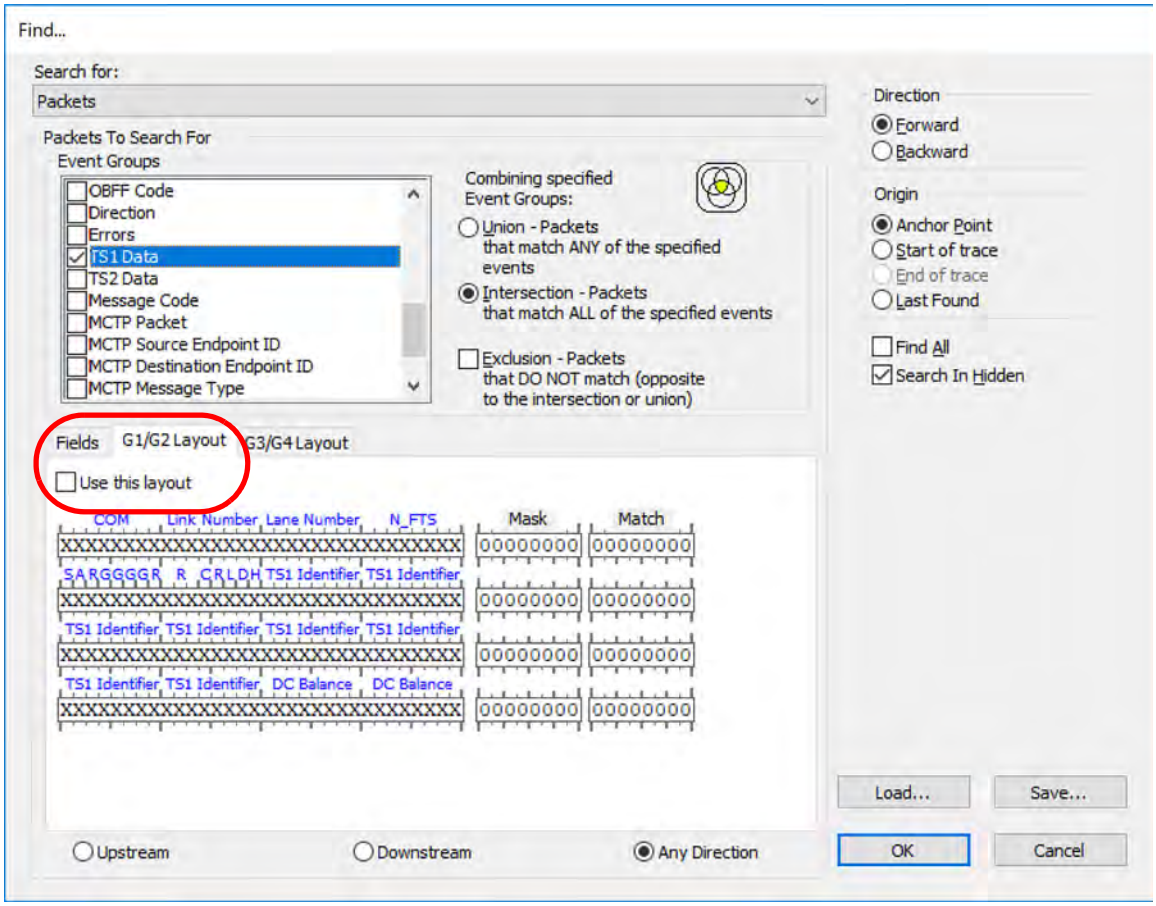


Figure 10.36: Find: Search for Packets -> TS1 G1/G2 Layout

Set the Recording Options -> TS1 packet -> Event Properties with the same options (see Figure 10.37).

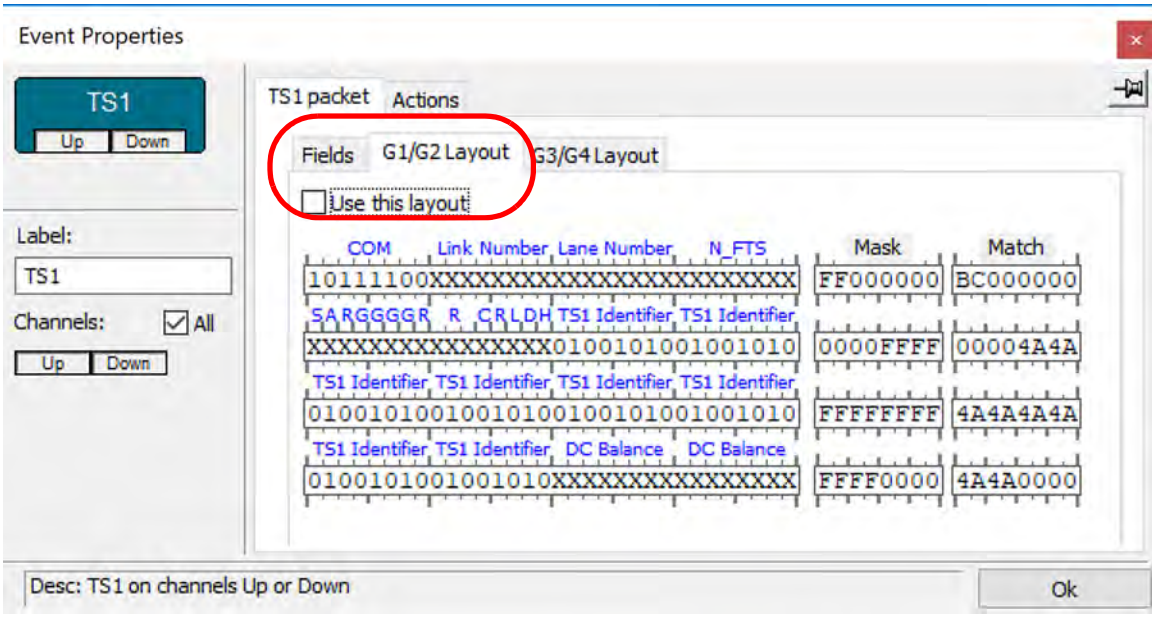


Figure 10.37: Set Recording Options: TS1 Event Properties

Keep the checkbox "Use this layout" in G3/G4 Layout tab checked. See Figure 10.38.

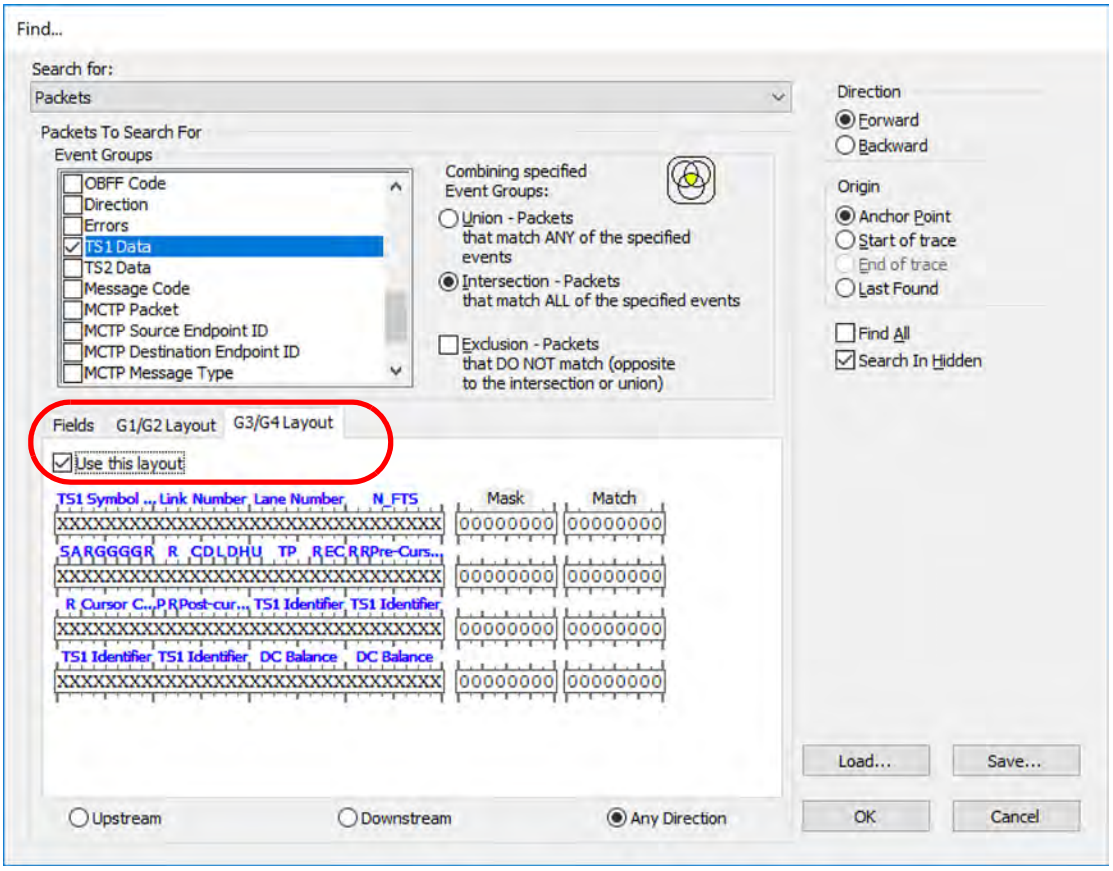


Figure 10.38: Find: TS1 Data -> G3/G4 Layout

Set the Recording Options, TS1 Event Properties with the same options. See Figure 10.39.

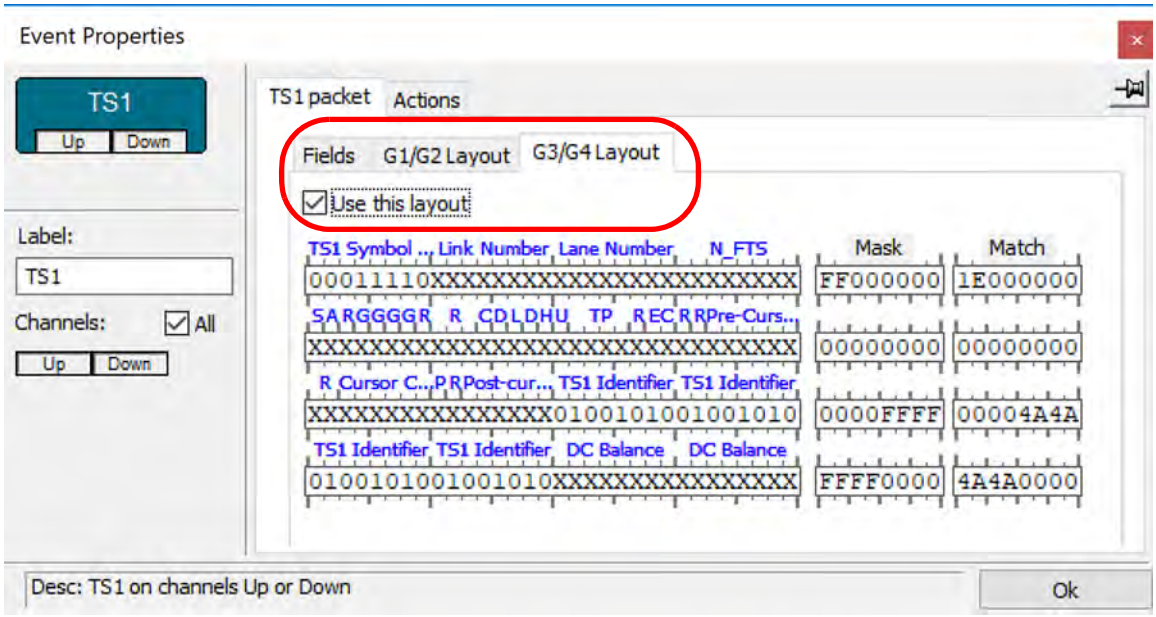


Figure 10.39: Recording Options; TS1 -> Event Properties

Search results example is shown in Figure 10.40.

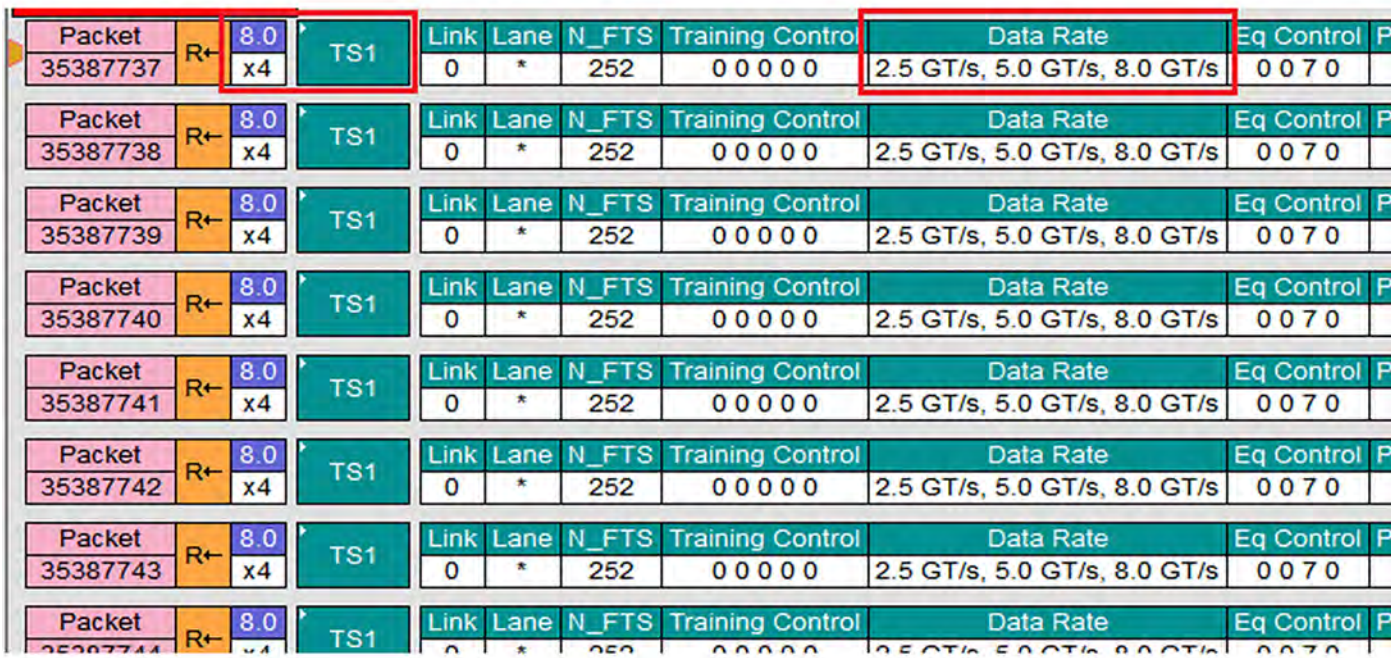


Figure 10.40: Example of Finding TS1 Packet with G3 Speed and G3 Data Rate

Example: TS1 Packet with G1 Speed and G3 Data Rate

In order to select TS1/TS2 packets for search/triggering on G1/G2 speed you need to set the data rate for searching/triggering to G3. See Figure 10.41.

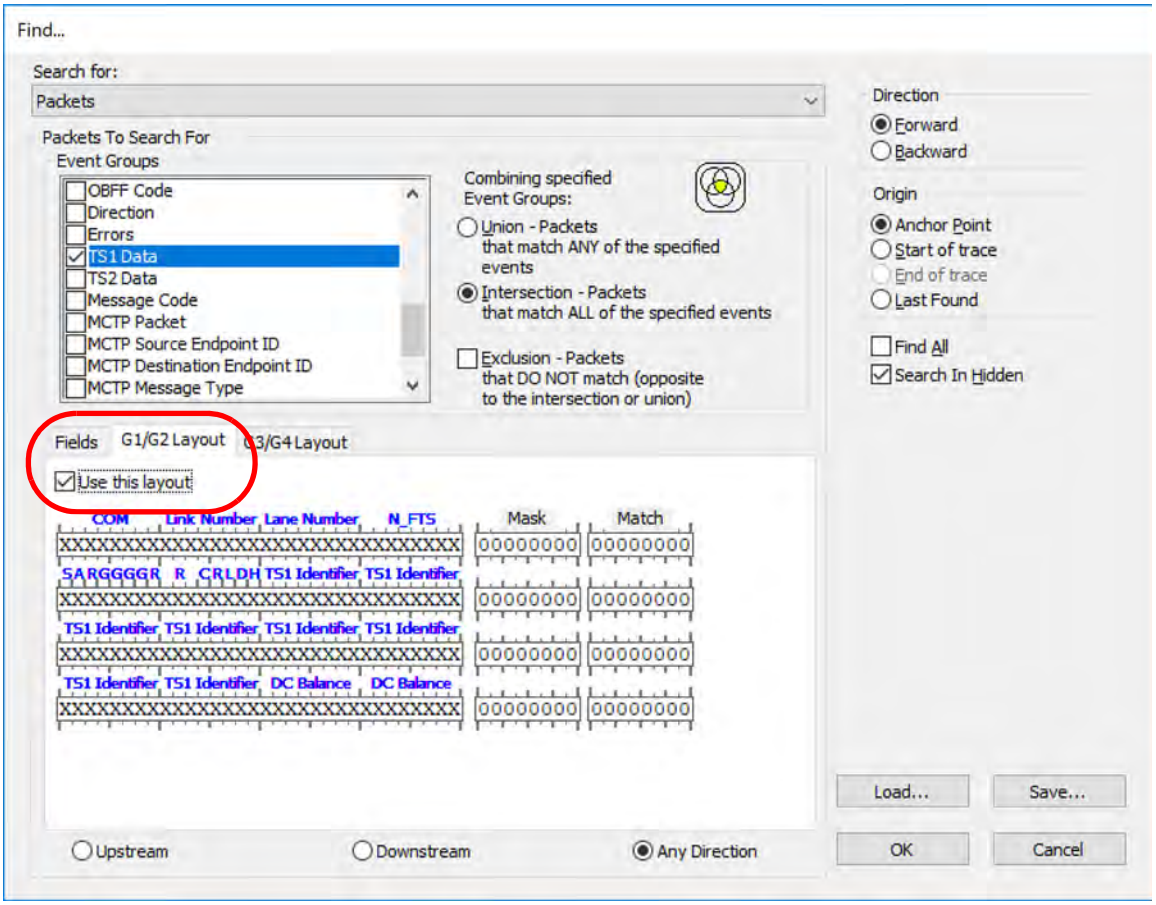


Figure 10.41: Find: TS1 Data -> G1/G2 Layout

Set the Recording Options with the same options. See Figure 10.42 on page 697.

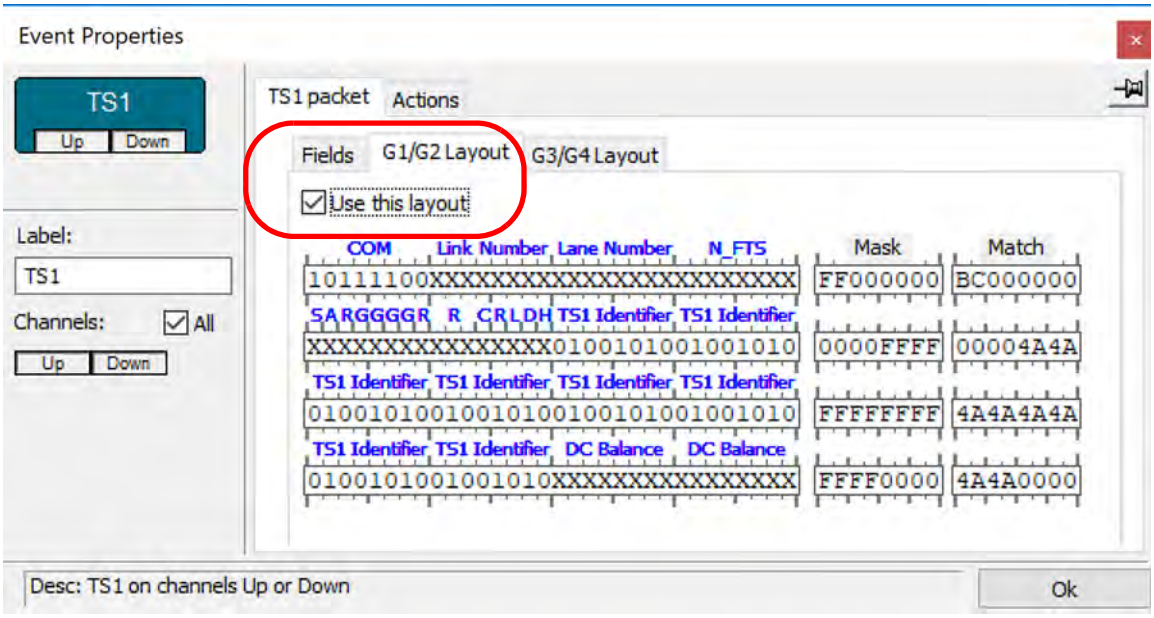


Figure 10.42: Recording Options: TS1 -> Event Properties

Uncheck the checkbox “Use this Layout” in the G3/G4 tab in the Find -> Search for dialog box. See Figure 10.43.

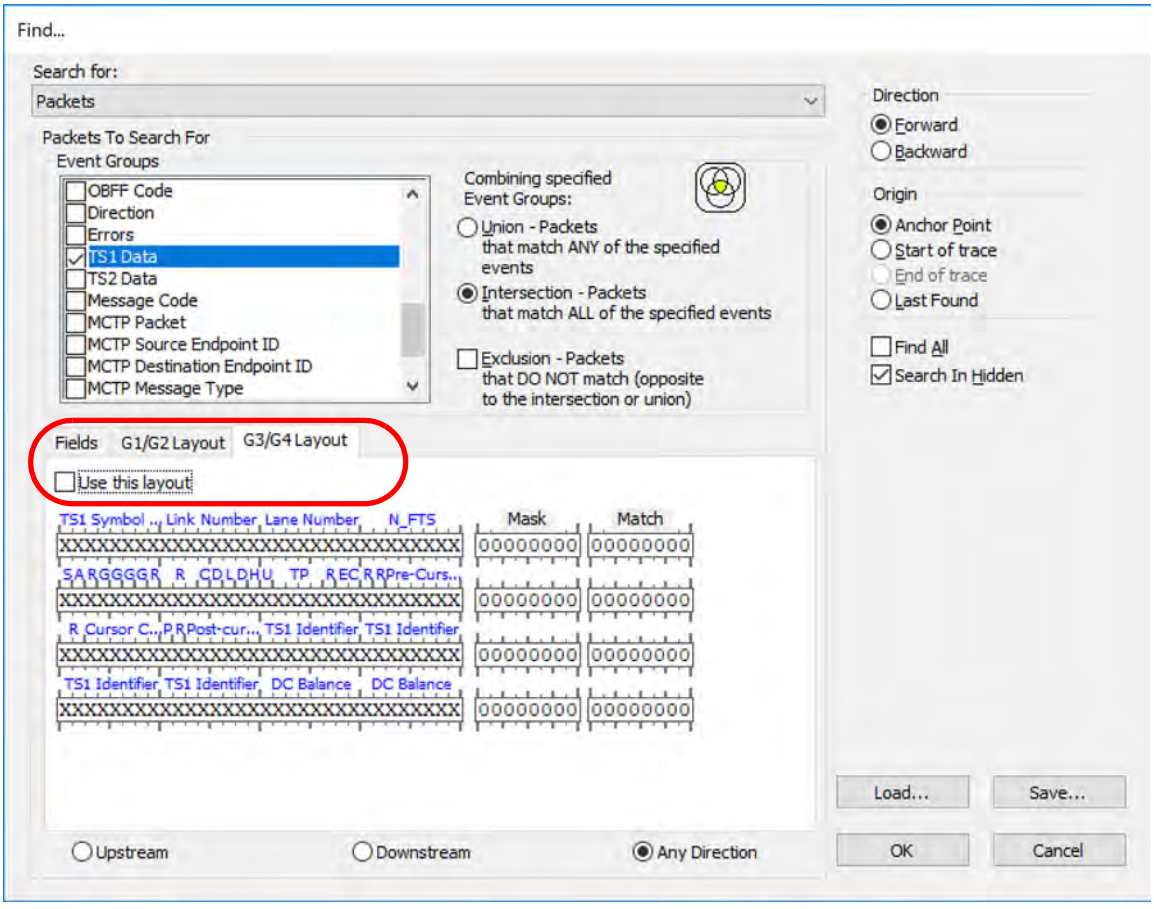


Figure 10.43: Find: TS1 Data -> G3/G4 Layout

In a similar fashion uncheck the checkbox in Recording Options, TS1, Event Properties. See Figure 10.44.

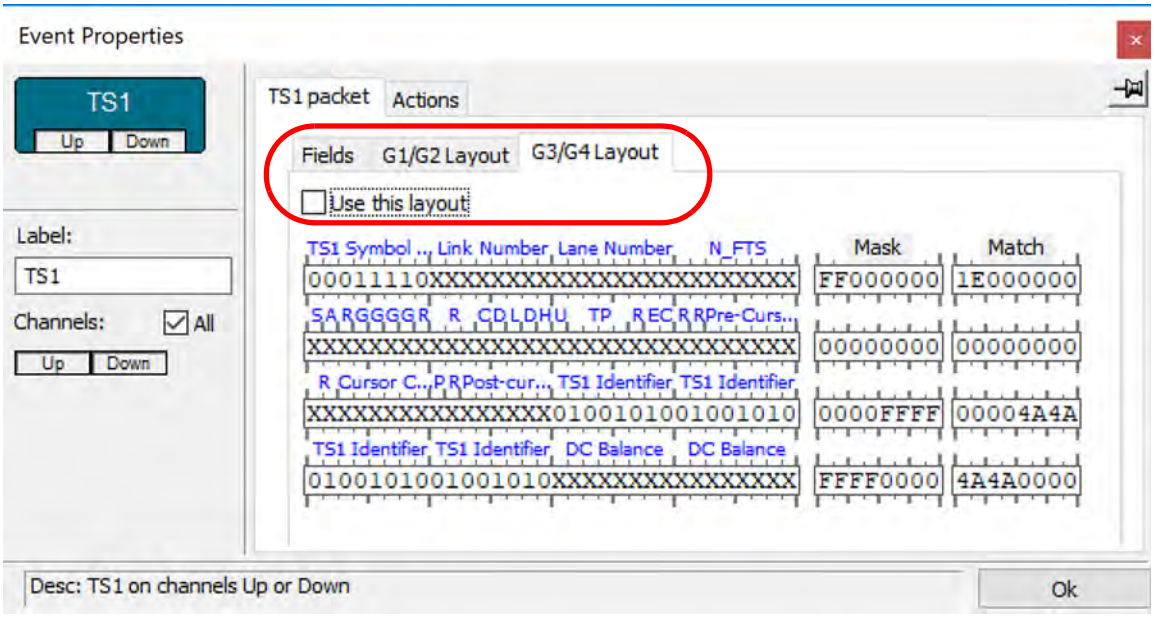


Figure 10.44: Recording Options: TS1 -> Event Properties

An example of a captured trace with TS1 at G1 speed and Data at Gen3 Data Rate is shown below. See Figure 10.45.

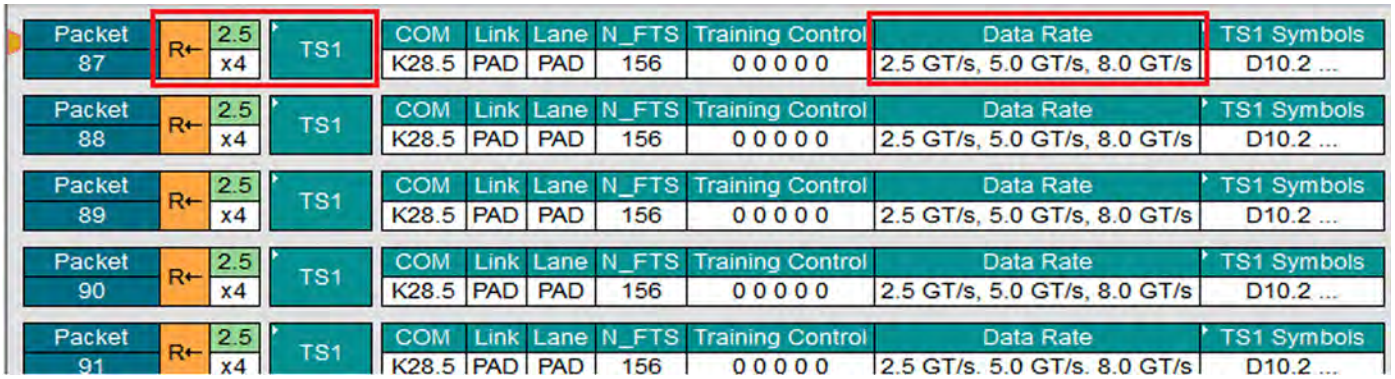


Figure 10.45: TS1 Packet with G1 Speed and G3 Data Rate

Example: Search for PMUX Channel ID

In this case, we are searching for the following event:

- PMUX Channel ID (see Figure 10.46)

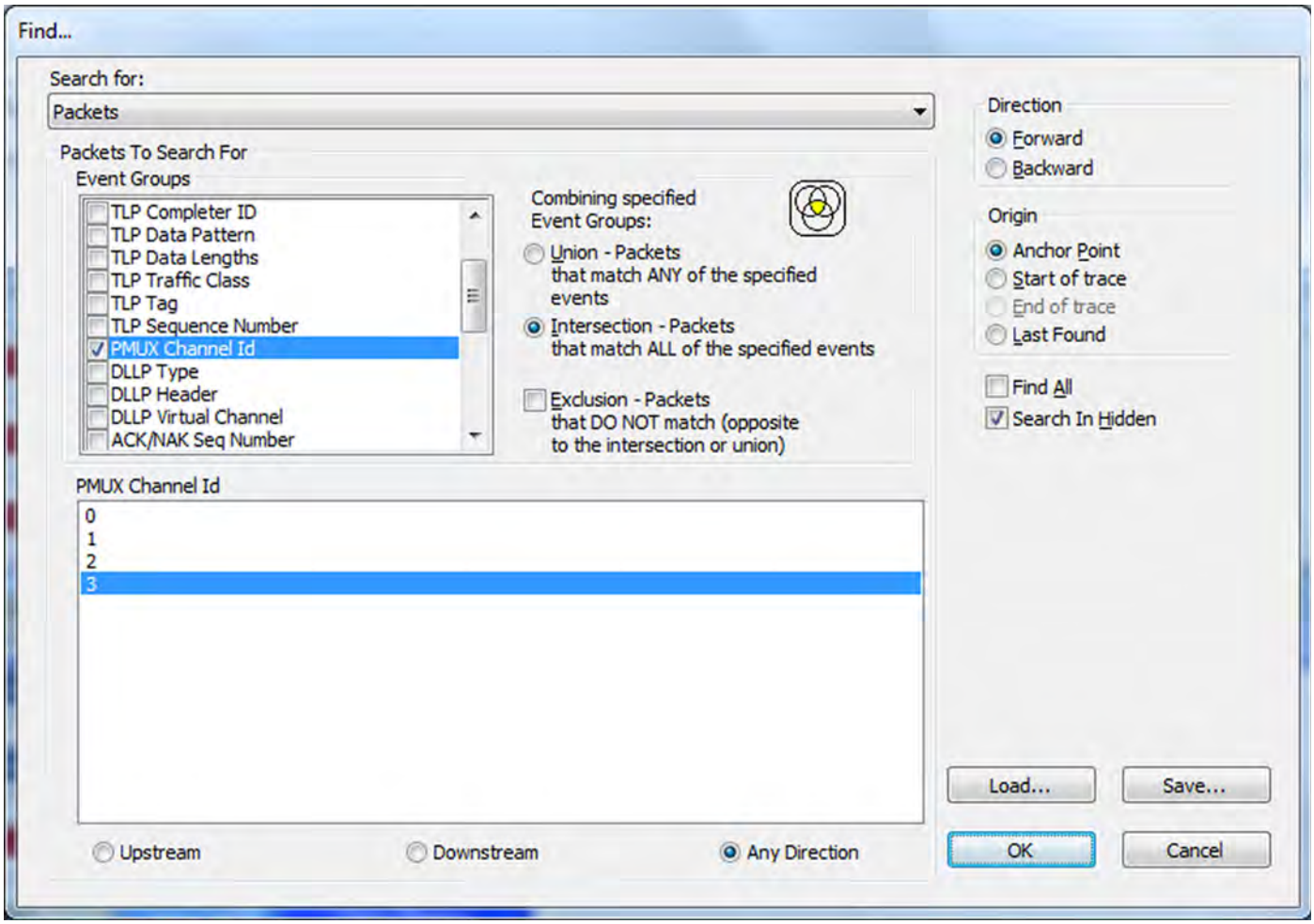


Figure 10.46: Search for: PMUX Channel ID (3)

PMUX Channel ID Found and PMUX Packet Error Decoded in Trace

In the trace both the PMUX Channel ID was found and a Packet PMUX Error was decoded. See Figure 10.47.

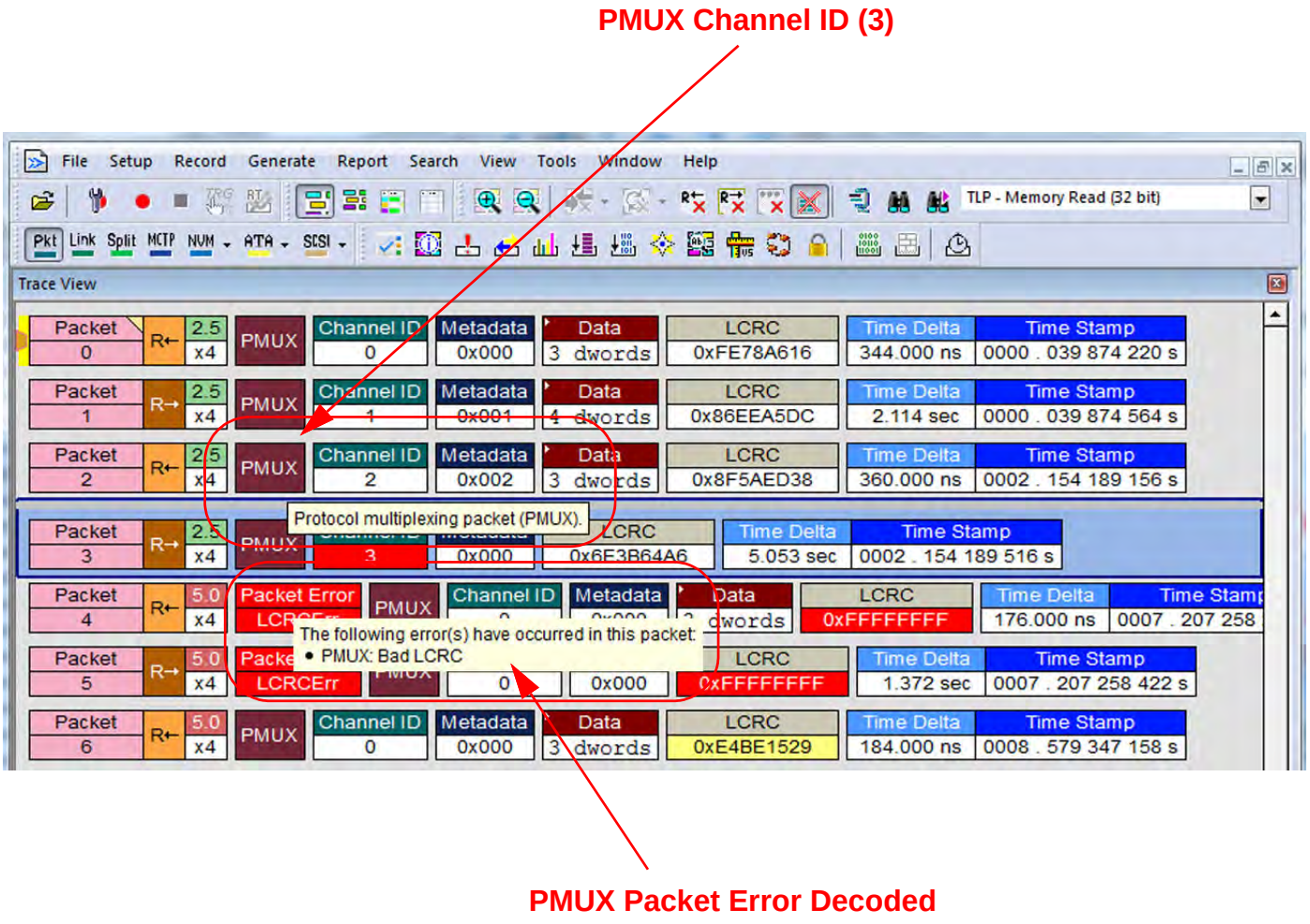


Figure 10.47: PMUX Channel ID (3) Found in Trace and Packet Error Decoded

10.10.2 Find Function and CXL Packets

The Find function includes CXL packets. See Figure 10.48

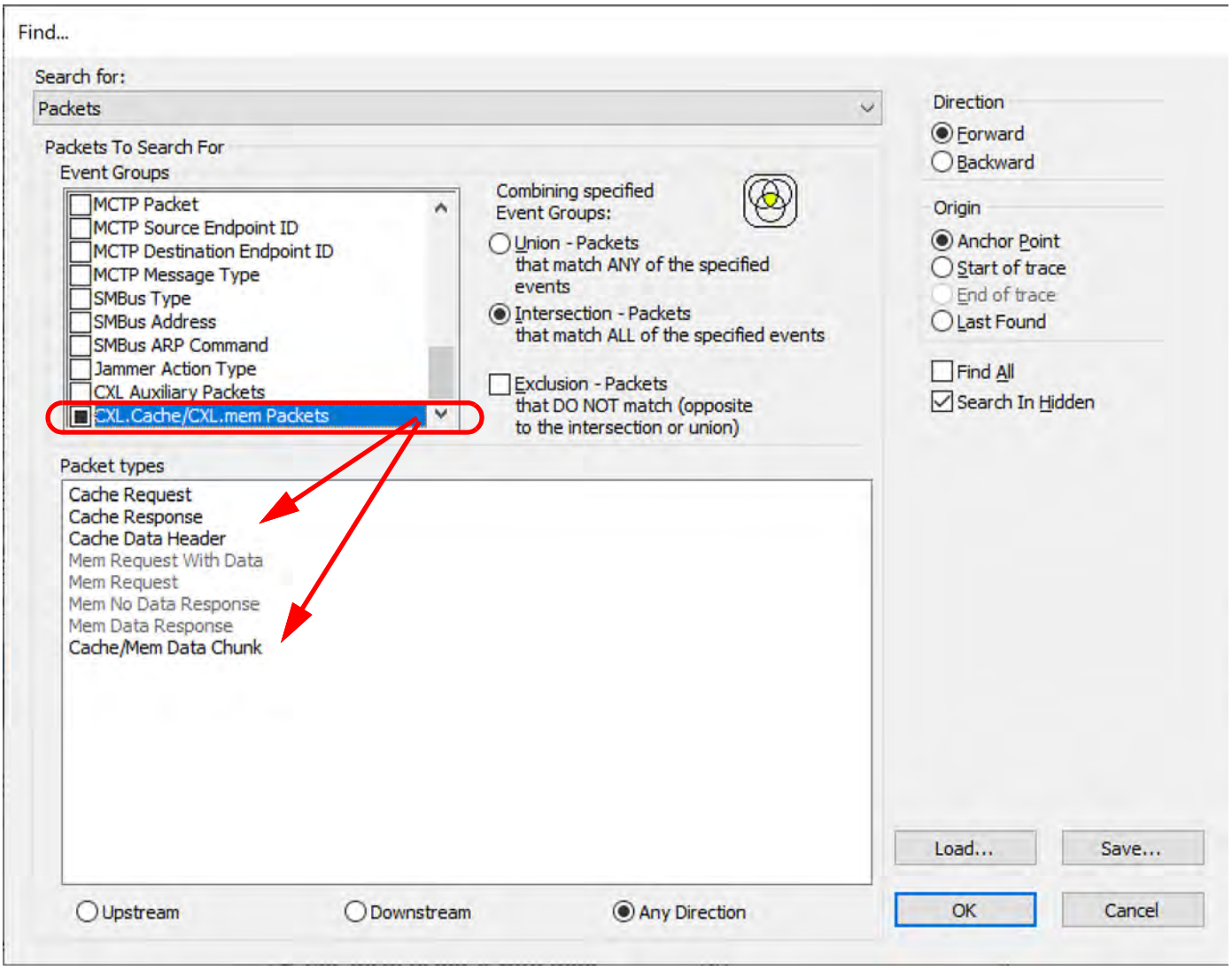


Figure 10.48: Find CXL Packet types

10.10.3 Event Groups for Link Transactions:

- TLP Type
- Traffic Class
- Virtual Channel
- Direction
- RequesterID
- CompleterID
- Status
- Tag

10.10.4 Event Groups for Split Transactions:

- TLP Type
- Traffic Class
- Virtual Channel
- Direction
- Requester ID
- Completer ID
- Status
- Tag
- Address

10.10.5 Event Groups for LM Commands

- Margin Command
- Margin Type
- Receiver Number
- Errors

Example: Search for Lane Margining Command: ReportLM_SamplingRateVoltage (see Figure 10.49 on page 703).

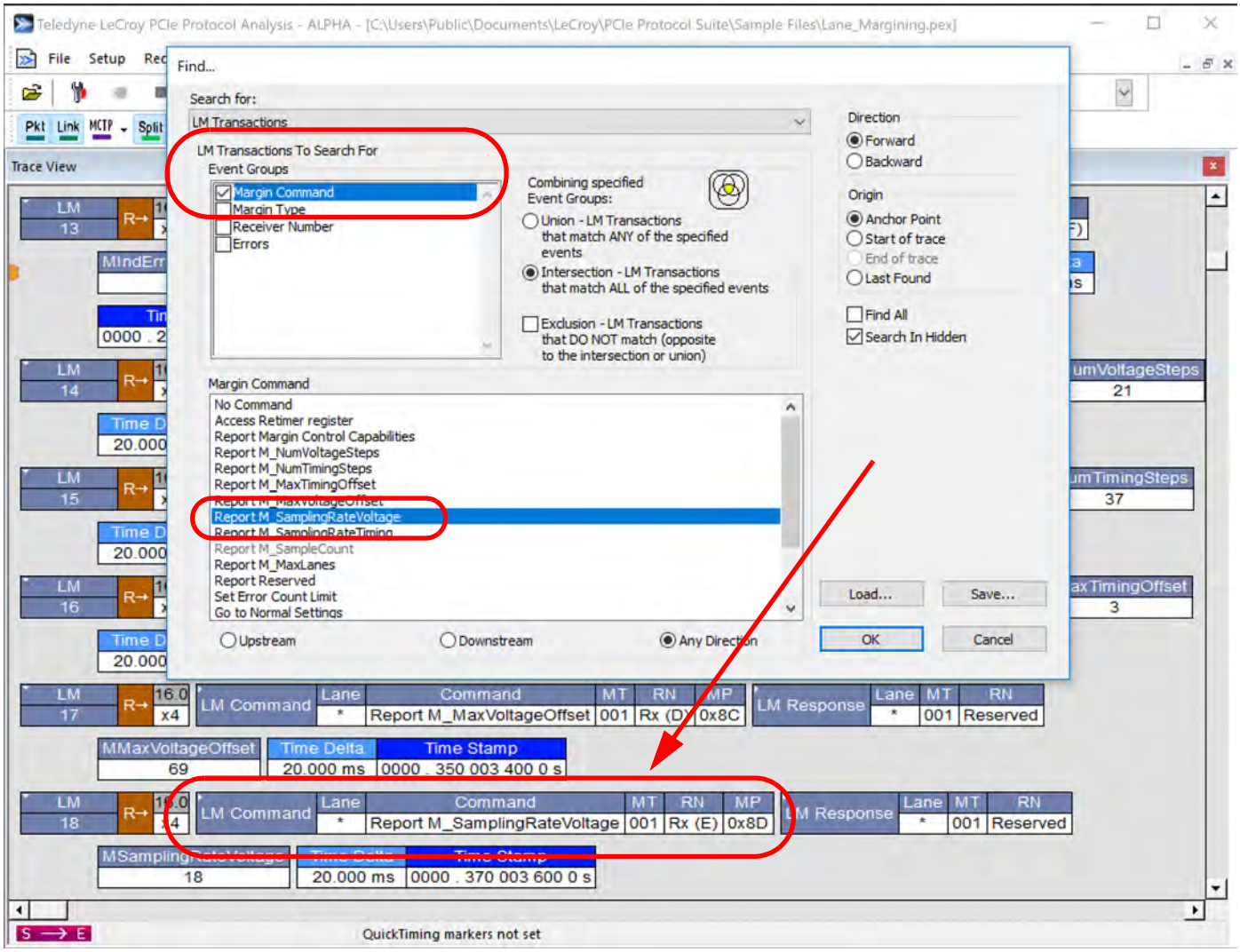


Figure 10.49: Find: Lane Margining Transaction -> Margin Command -> ReportLM_SamplingRateVoltage

10.10.6 Event Groups for NVMe transactions:

- Controller Registers
- Other NVMe Entities
- Queue IDs
- Command IDs
- Doorbell Registers
- Admin Submission Command Set
- NVMe Submission Command Set
- Completion Queue Entry
- PRP
- Submission Command
- NVMe Errors

10.10.7 Event Groups for PQI Transactions:

- PQI Register ID
- PQI Admin Functions
- PQI Errors

10.10.8 Event Groups for AHCI Transactions:

- AHCI Register ID
- AHCI Port Number
- AHCI Slot Number
- AHCI Port Multiplier Port
- AHCI Raw Address
- AHCI Direction
- AHCI Errors

10.10.9 Event Groups for ATA transactions:

- ATA Register Type
- ATA Port Number
- ATA Slot Number
- ATA Raw Address
- ATA Port Multiplier Port
- ATA Interruption Reason
- ATA Error Type
- ATA Input/Output
- ATA Payload Portion
- ATA CFIS Fields
- ATA RFIS Device to Host Fields
- ATA DSFIS Fields
- ATA PSFIS Fields
- ATA SDBFIS Fields

10.10.10 Event Groups for SOP Transactions:

- SOP Information Unit ID
- SOP Errors

10.10.11 Event Groups for SCSI Transactions:

- SCSI Commands
- Command Status
- Task Managements
- Task Management Responses
- Errors
- SCSI Logical Unit Numbers

10.10.12 Event Groups for NVMe Commands:

- Admin Command Set
- NVM Command Set
- Submission QID
- Completion QID
- Status
- Errors
- LBA
- NVM Command
- NVM Payload Portion
- TCG Types
- TCG Method
- TCG Invoker
- TCG Com ID
- TCG Ext Com ID
- RPMB

Note: When searching for a LBA range, it find commands with LBAs that intersect with the selected address range.

Example: Search for NVMe Command

In this case, we are searching for the following event (see Figure 10.50 on page 706):

- NVMe Command
- Event Group NVM command
- Command = 0x02, Read
- Value = 1
- Fields = SQID [SELECTED: 1]

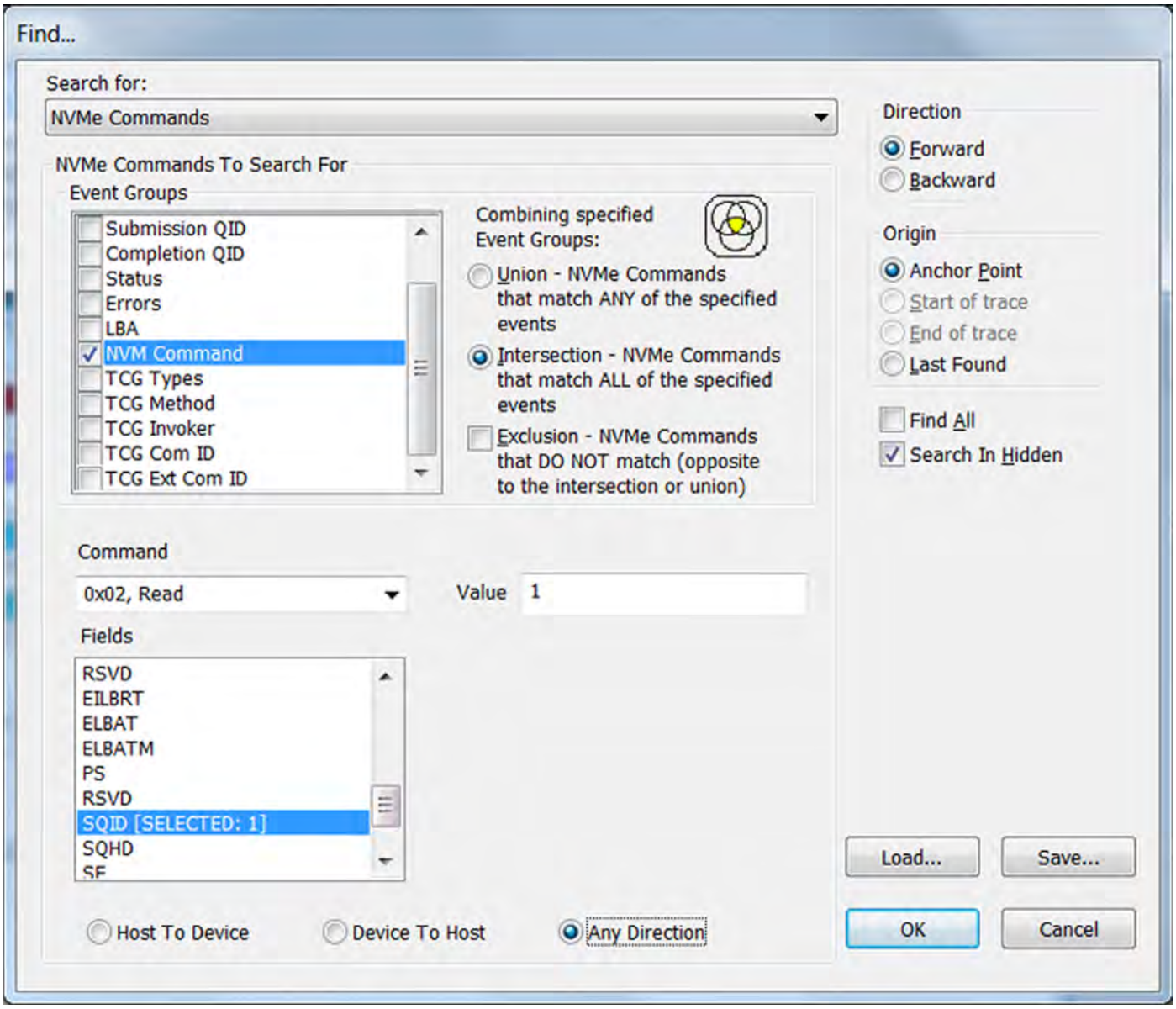


Figure 10.50: Find: Search for NVMe Command

Select OK.

Figure 10.51 on page 707 shows that NVMe Command #67 is a Read Command that has an SQID value of 1.

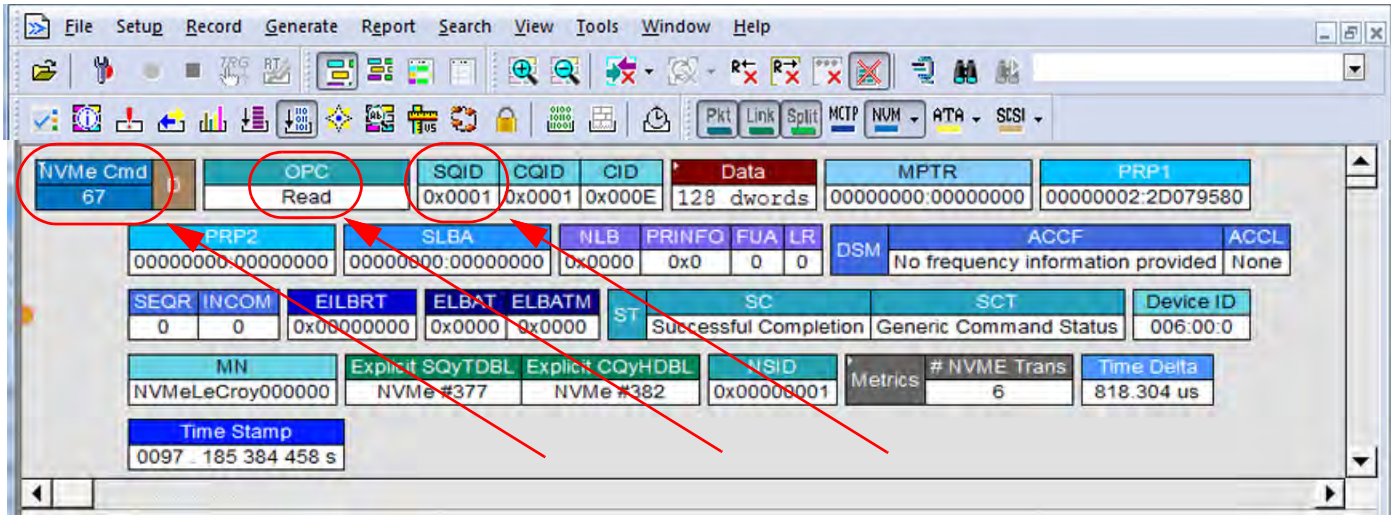


Figure 10.51: Find => Search for NVMe Command => Found

Example: Search for NVMe Command: NVM Payload Portion

The Find -> Search for: NVMe Commands -> Event Groups -> NVM Payload Portion will search the currently loaded trace for an NMV Payload. See Figure 10.52.

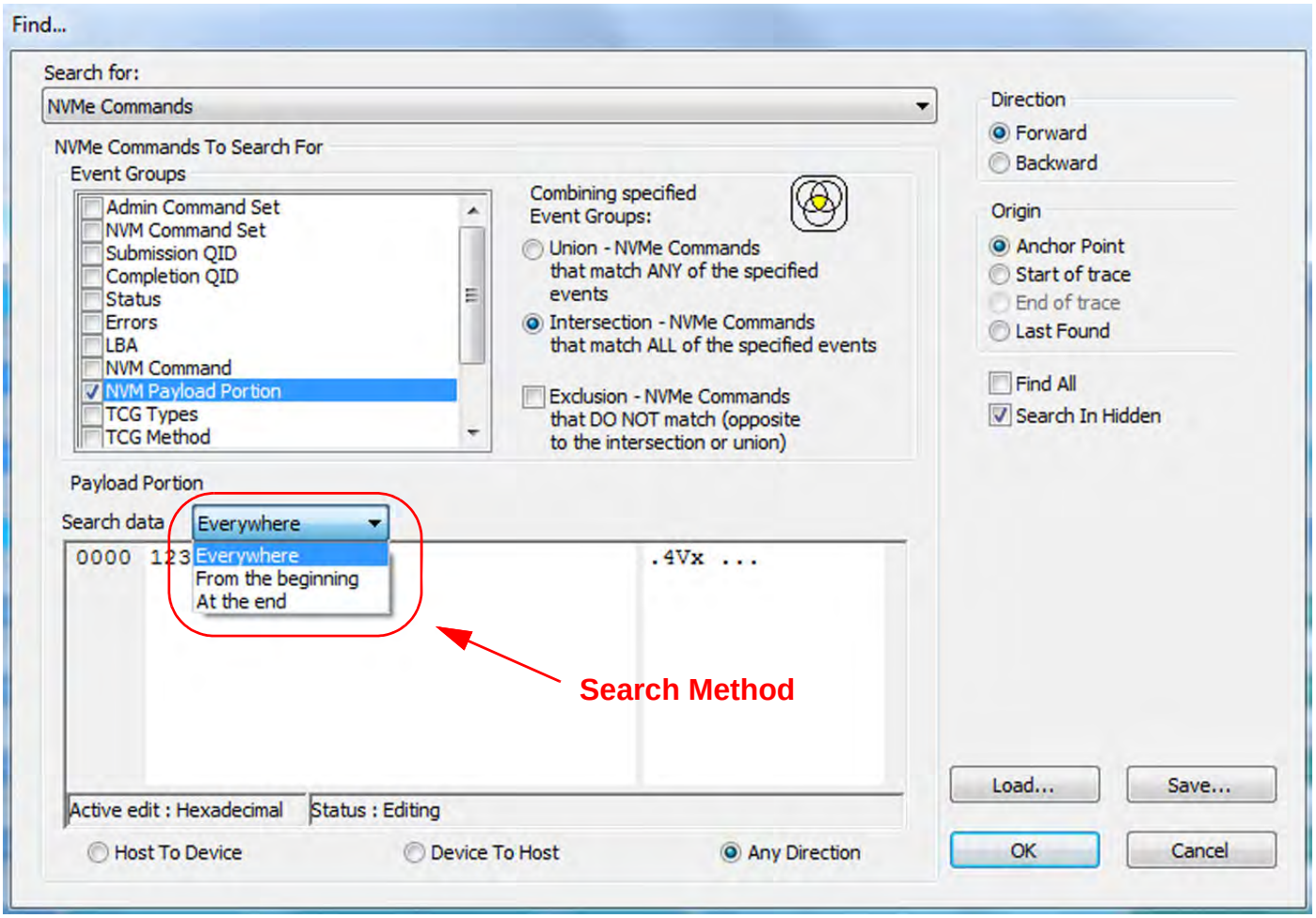


Figure 10.52: Find: Search for NVMe Commands -> NVM Payload Portion

There are several methods which can be used to search the NVM Payload for a particular data pattern:

- Everywhere - matching the set pattern anywhere in the payload
- From the beginning - matching the set pattern in the payload at offset 0
- At the end - matching the set pattern with the offset calculated by the length of the pattern from the end of the payload.

The different search methods are illustrated in Figure 10.53 on page 709.

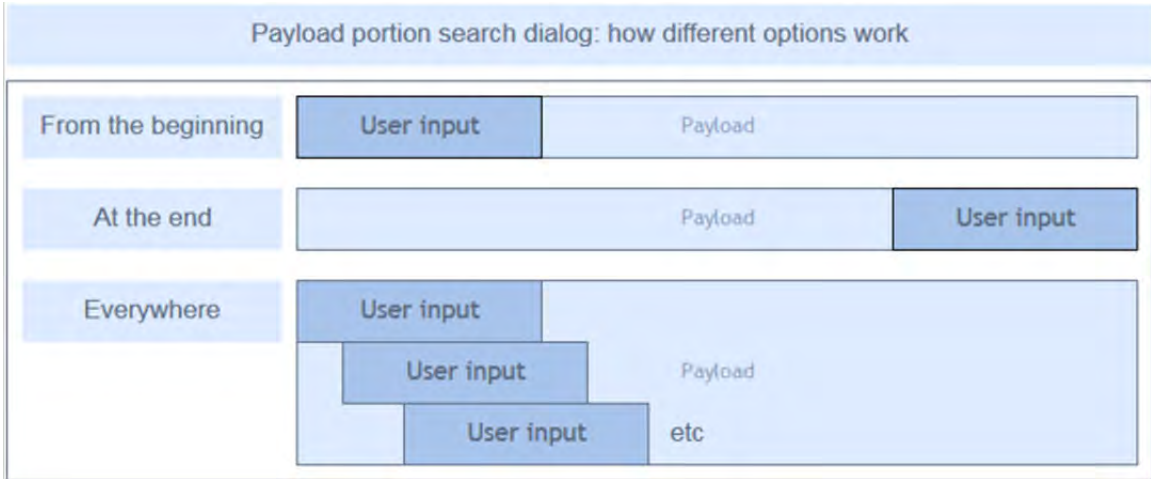


Figure 10.53: Search NVM Payload: Different Methods

10.10.13Example: Search for DLLP Header -> Flow Control Feature

In this case, we are searching for the following event:

- DLLP Header -> Data Link Feature -> Flow Control Packet: Fields and Layout (see Figure 10.54 and Figure 10.55 on page 711)

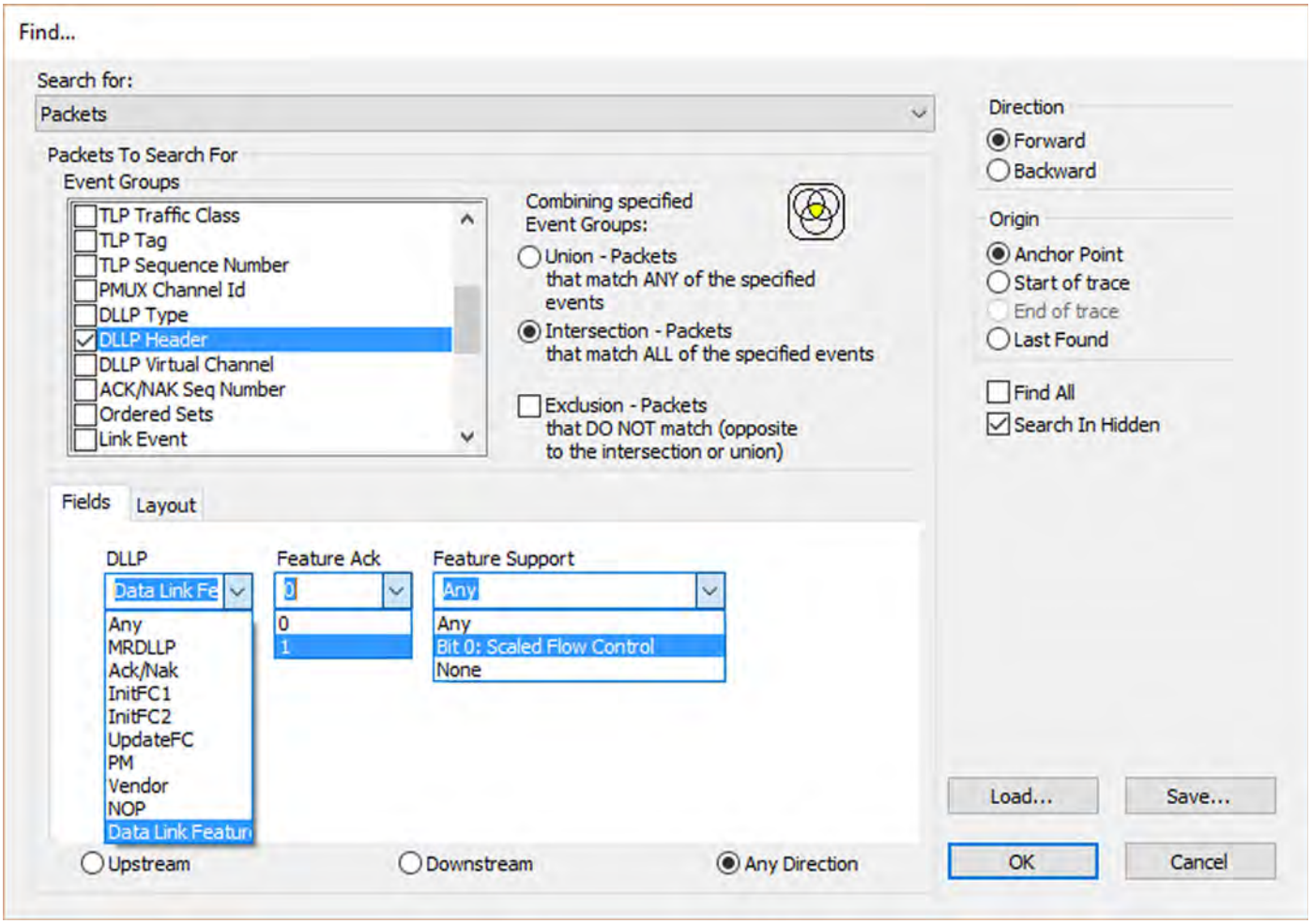


Figure 10.54: Search for: Flow Control Packet -> Fields

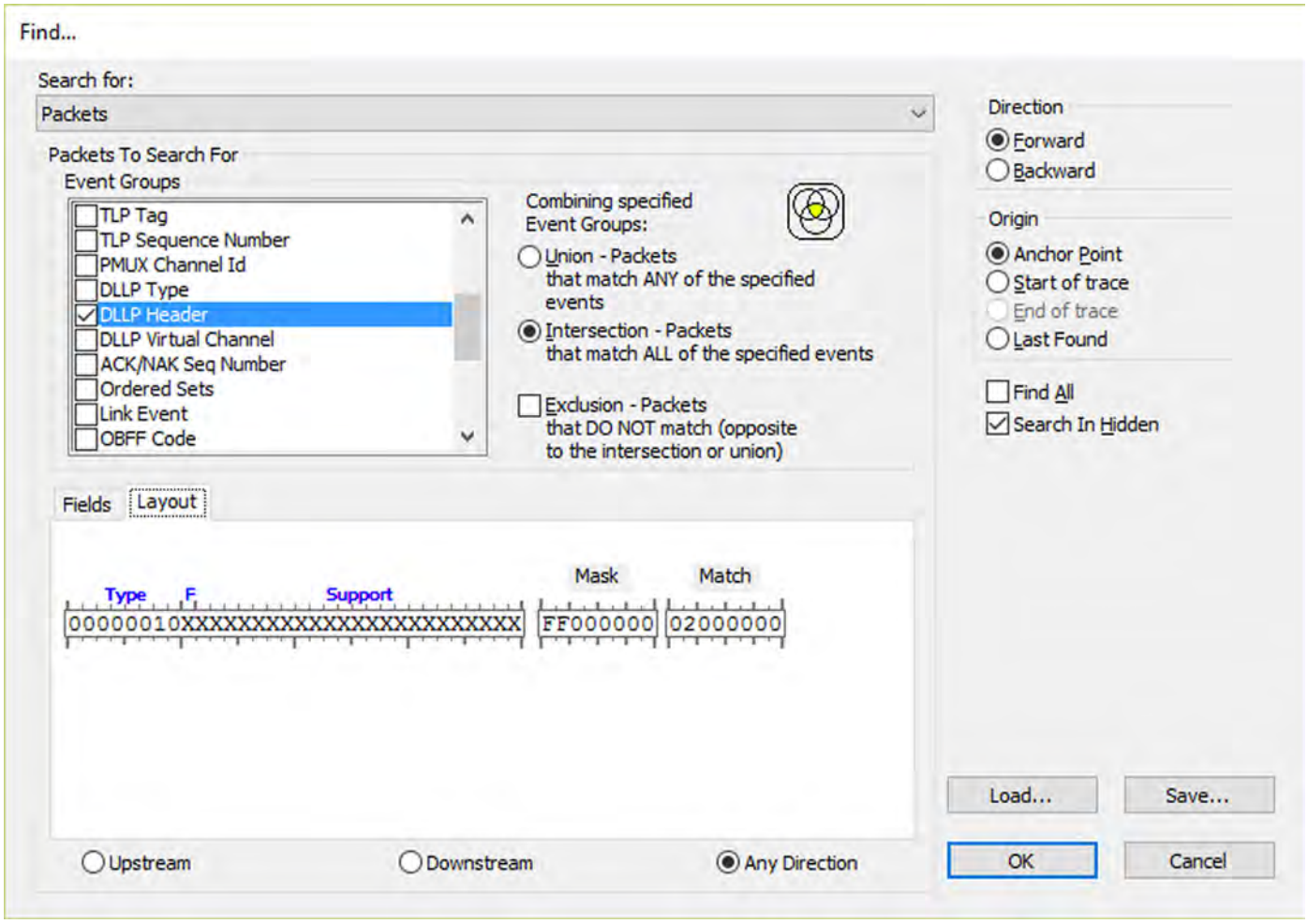


Figure 10.55: Search for: Search for: Flow Control Packet -> Layout

10.11 Find Next Packet Type

Use Find Next or click  to search for the next packet meeting the search criteria.

10.11.1 Quick Search Feature

As an example, the NVMe_Z3DriveEmulation Trace has been loaded from the C:\Users\Public\Documents\LeCroy\PCIe Protocol Suite\Sample Files (see Figure 10.56).

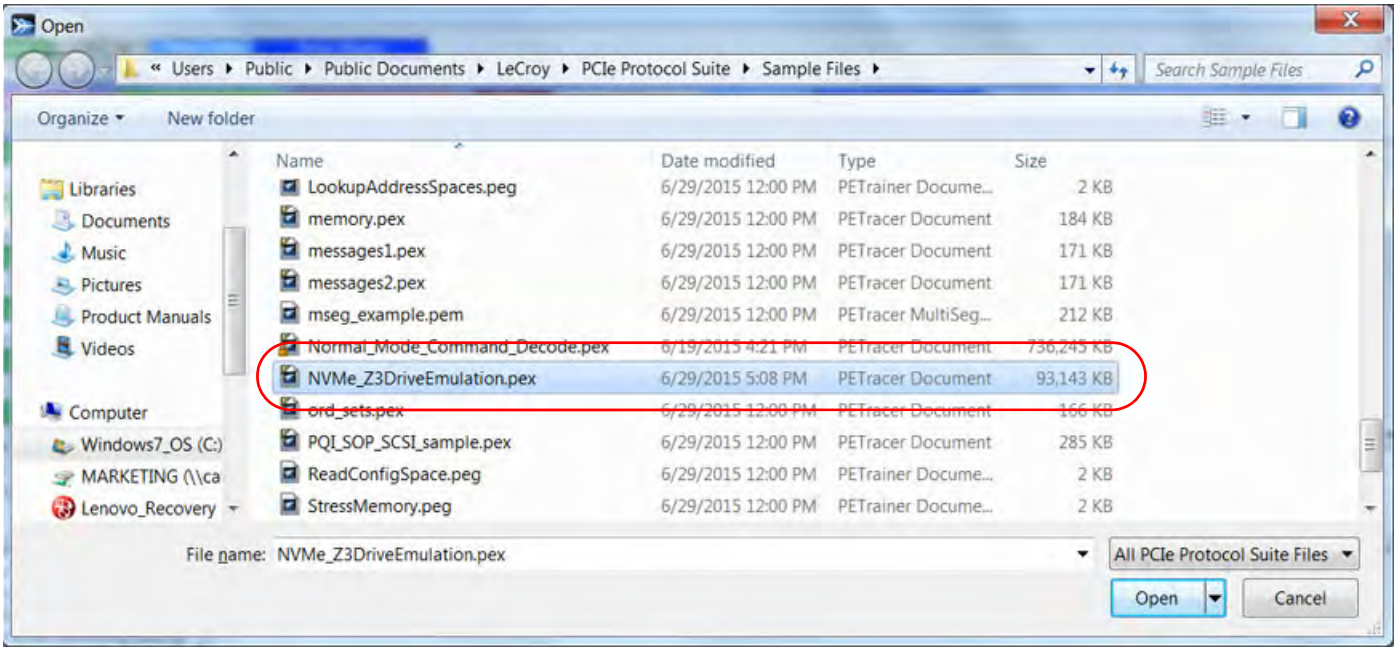


Figure 10.56: Location of Trace File to be Loaded

Select the NVMe_Z3DriveEmulation.pex file and click on Open.

The Main Menu will look like Figure 10.57 after you chosen to look for NVMe commands and removed unrelated traffic.

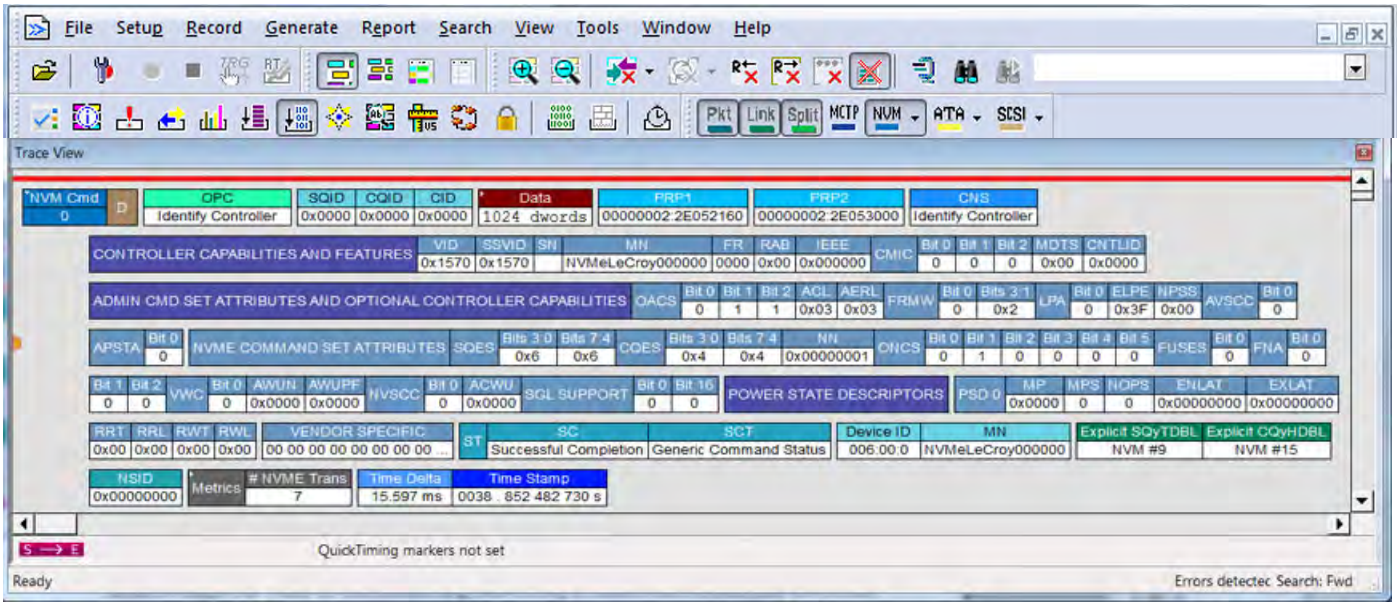


Figure 10.57: Main Menu with NVMe_Z3DriveEmulation Trace Loaded

Enter a term to search for in the Search Window.

In this case, we chose “NVM #66  .

Place the cursor inside the Search Window and click the Enter key. The results are shown below (see Figure 10.58).

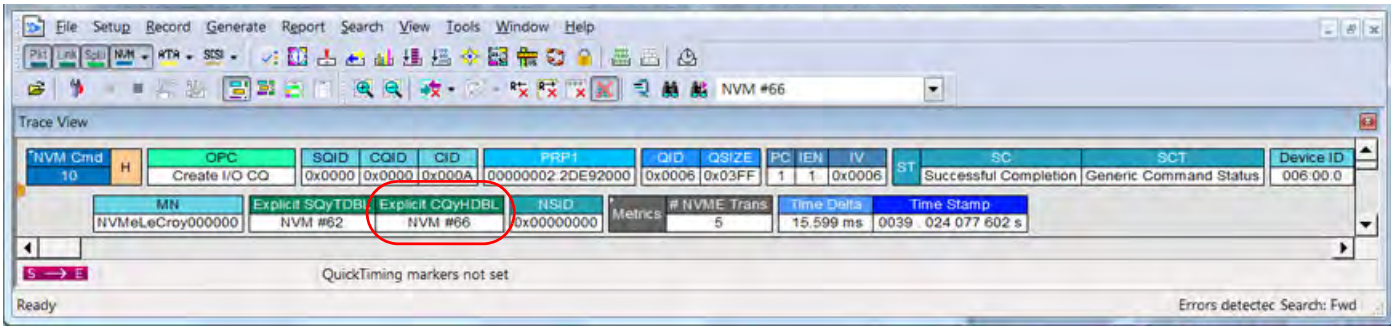


Figure 10.58: Search for NVM #66

Once the packet in the Trace has been found, the NVM #66 can be seen to be part of a doorbell event (Explicit SQyTDBL: NVM #62 with the response of Explicit CQyHDBL NVM #66).

This was just an example, you can search for any of the pre-defined terms (Figure 4.3 on page 73) or chose your own term or event to search for.

If you started Searching in the middle of the Trace the following windows will pop up:

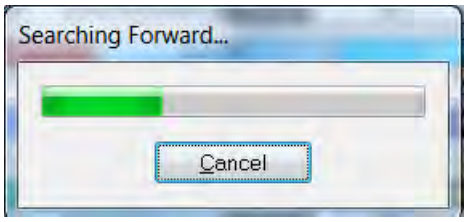


Figure 10.59: Search Progress Window

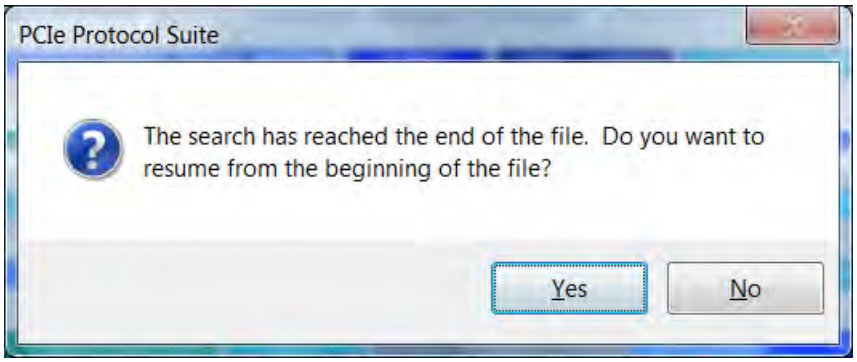


Figure 10.60: Resume Searching From Beginning of Trace

If you select Yes, the tool will continue searching from the start of the Trace, then the following window will pop up:

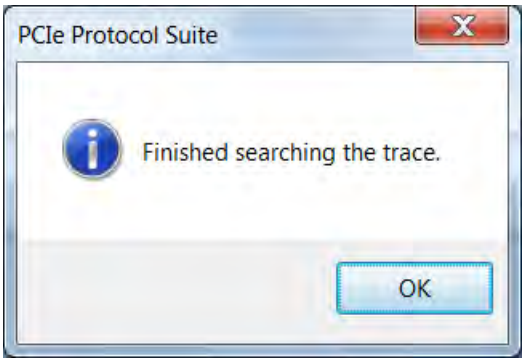


Figure 10.61: Finished Searching Trace

If the tool hasn't moved to a new Packet, the term being Searched for was not found.

10.12 Toggle Search Direction

Search direction can be toggled back and forth by using the command under the Search menu. Search Direction controls the direction of the search. Each time Toggle Search Direction is selected, the search order is reversed. For example, if the previous search was **forward**, choosing **Toggle Search Direction** toggles the current search to **backward**.

To verify the direction of a search look at the lower right corner of the screen. **Search: Bwd** or **Search: Fwd** should appear. If a direction is not indicated, it means that the status bar is turned off.

To turn on the Status bar, select from the menu **View > Status Bar**.

Keyboard shortcuts can also be used to control search direction: Ctrl+b toggles the search direction.

Chapter 9

Display Options

Use **Display Options** to customize the colors, formats, and hiding options of displayed traffic.

To open **Display Options**, select **Setup -> Display Options** or, click the **Display Options** button  on the toolbar.

9.1 Display Options: General Tab

Figure 9.1 shows the 'General' tab of **Display Options.**

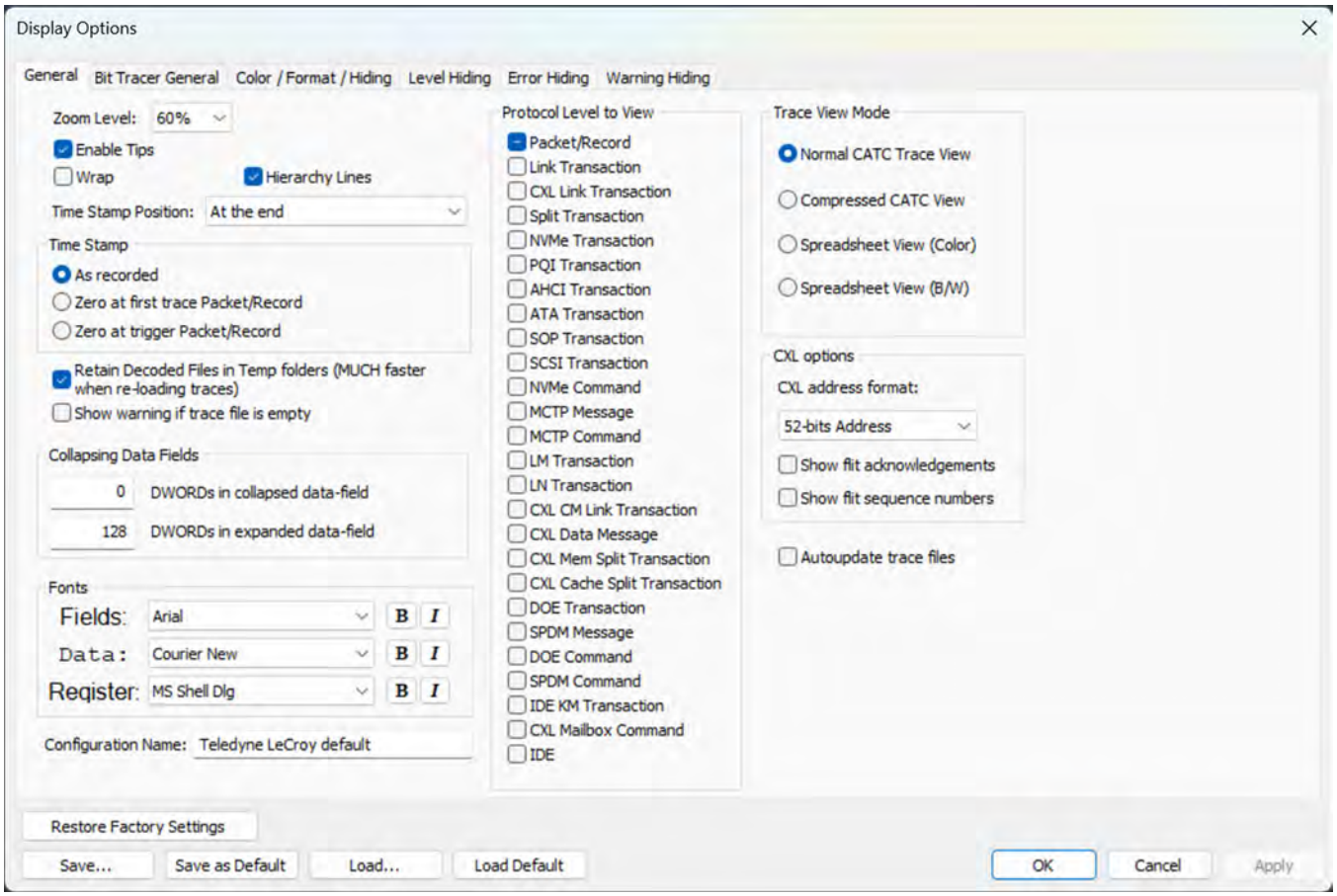


Figure 9.1: Display Options: General

The features of the **Display Options**, 'General' tab are shown in Table 9.1.

TABLE 9.1: General Display Options Features

Feature	Description
Zoom Level	Defines the size of packet fields in the packet view. Zoom level is adjustable as 10, 20, 40, 60, 80, 100, 120, 140, 160, 180 and 200 percent.
Enable Tips	Allows hover text to display on a packet by resting your mouse pointer over it.
Wrap	Allows packets, Link Transactions, and Split Transactions to wrap within the display.
Hierarchy Lines	Adds lines to the trace view indicating relations between packets, Link Transactions, and Split Transactions.
Timestamp position	Moves timestamp location from end of packet to beginning of packet, or merges it with the packet number.
Time Stamp	Options for setting the timestamp to zero for either the first CATC Trace packet or the trigger packet or for leaving the stamp unchanged as it was originally recorded.
Retain Decoded Files	Decoded Files are retained in Temp folders, which makes re-loading the trace much faster.
Show Warning if trace file is empty	Select if a warning message is desired for when recording conditions result in an empty trace (no traffic is recorded).
Protocol Level to View	Allows the CATC Trace to be displayed in different hierarchical levels, such as: Packets, Link Transactions, Split Transactions, CXL, PQI, AHCI, ATA, SOP, SCSI command, NVMe Commands, RRAP, MCTP and LM transactions.
Collapsing Data Fields	0 in the collapsed field means no data will be shown. 128 in the expanded field means 128 DWords will be shown when the data field is expanded. See "Collapsing Data Fields" on page 393.
Fonts	Changes the appearance of field text and/or data text as well as registers.
Configuration Name	Enter a text string to be associated with the current set of Display Options. This name is saved with the Display Options file, and appears as part of the title of the packet view window that uses this set of Display Options.
Trace View Mode	Displays Normal CATC Trace View, Compressed CATC View, Spreadsheet View (Color), and Spreadsheet View (B/W).
CXL Options	CXL Adress format: Sets the CXL address to either 52-bits or 46-bits. Show flit acknowledgements: Check to show. Show flit sequence numbers: Check to show.
Autoupdate Trace Files	Check to automatically update trace files.

9.1.1 Collapsing Data Fields

Using the collapse feature affects the “Data” field in the TLP packets. 0 in the collapsed field means no data will be shown. 128 in the expanded field means 128 DWords will be shown when the data field is expanded. See Figure 9.2 on page 393.

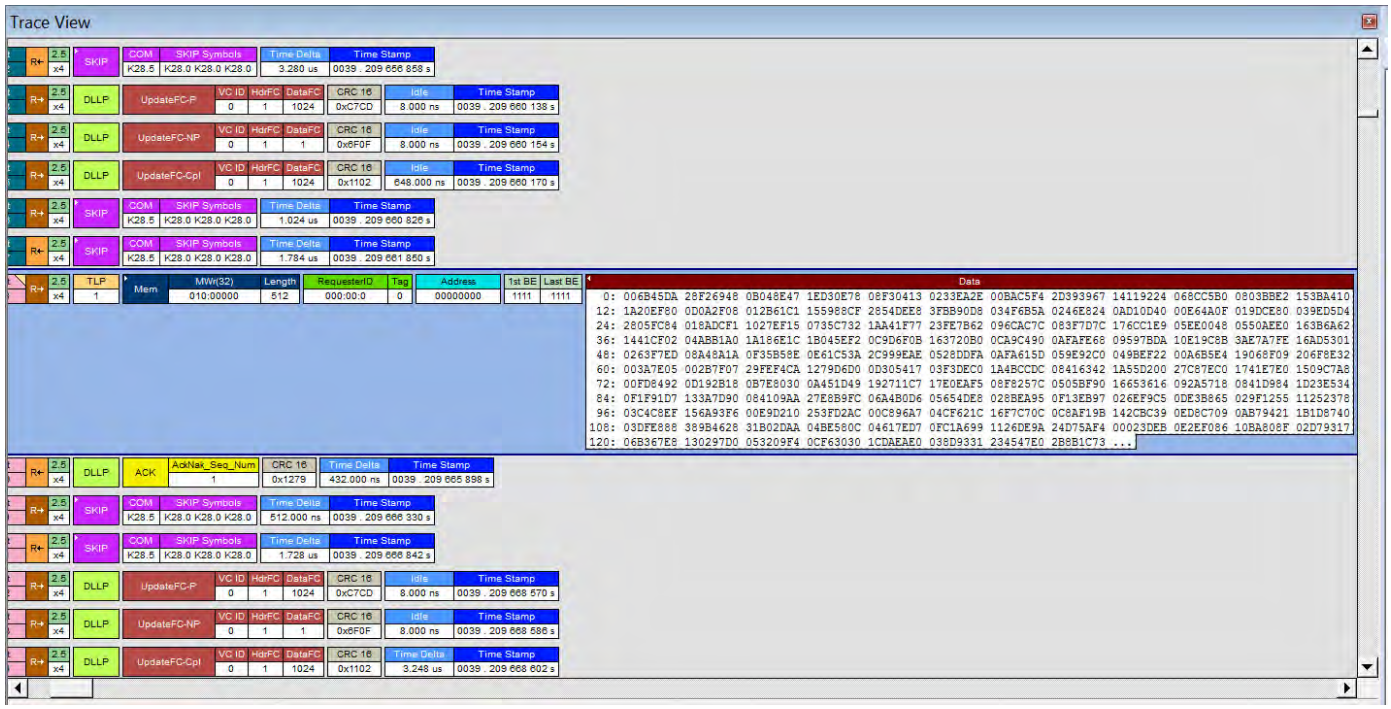


Figure 9.2: Expanded Data Field

9.2 Display Options: BitTracer General

The ‘BitTracer General’ tab is used with Summit T3 - T5 analyzers.

9.3 Display Options: Color/Format/Hiding

The ‘Color/Format/Hiding‘ tab customizes colors and formats associated with each field in the CATC Trace. It also has options to:

- set the data format (binary, hex, decimal, ASCII),
- set the bit order (LSB to MSB or MSB to LSB), and
- hide selected fields from the display.

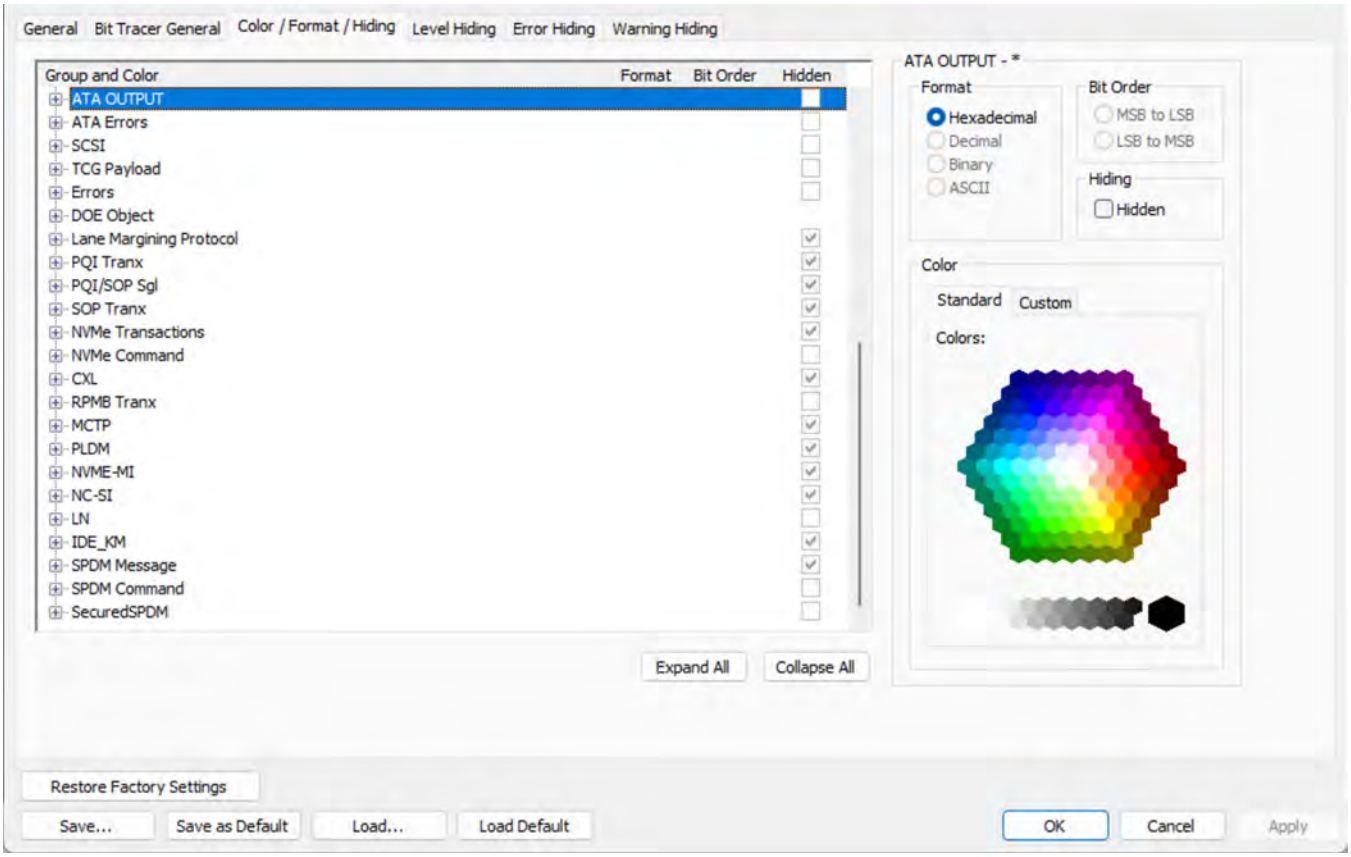
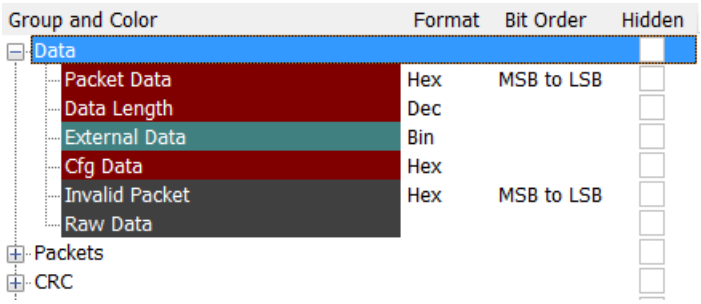


Figure 9.3: Display Options: Color/Format/Hiding

9.3.1 Setting Colors

1. Under the Group and Color column, click the **plus** symbol (**+**) next to the group to reformat. The group expands to show the individual fields within the group. Each field has a color, as shown below:



2. Click the cell to change the color. Note that some cells cannot be changed.
3. Click a color in the Color palette, then click **Apply** to save or **OK** to save changes and exit.

Note: The colors of the Invalid Data (frame error) field (red) and the Softbit Errors (yellow) following Frame types cannot be changed.

9.3.2 Changing Formats and Bit Order

The Field Formats tab allows you to define the way various numeric fields are shown in the packet display. You can select Hexadecimal, Decimal, Binary, or ASCII for certain fields or groups of fields.

To change a field's format, click the plus sign (+) next to a field in the list. This causes the selected item to expand so you can see its sub-fields. Select a sub-field, and then choose the format from the formatting choices that appear at the bottom right of the window (see Figure 9.4 on page 395).

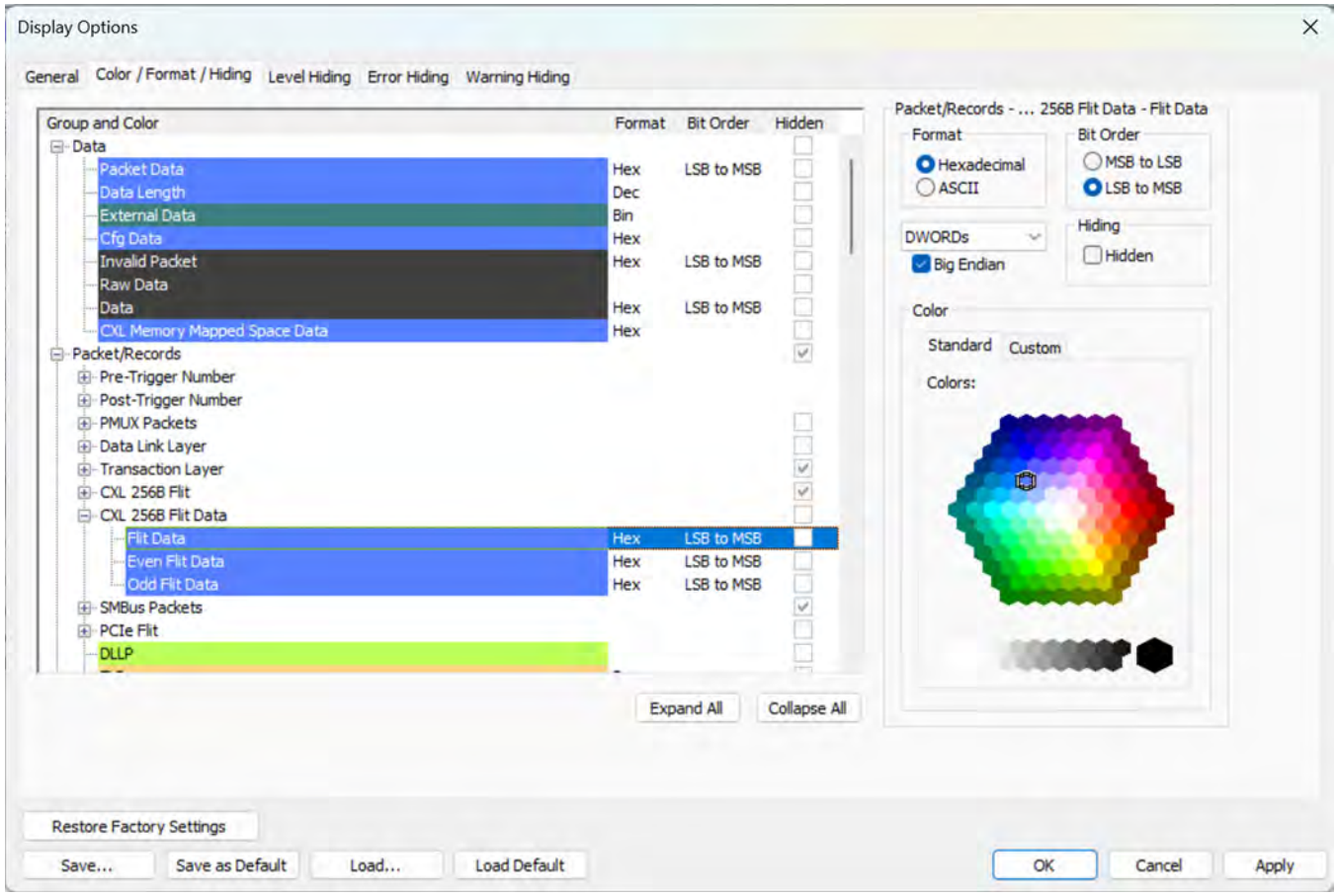
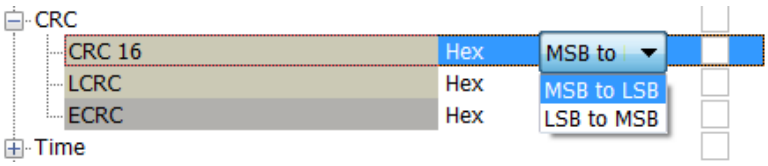


Figure 9.4: Display Options: Color/Format/Hiding Format and Bit Order

To change the format:

1. Under the **Group and Color** column, select the plus symbol (**+**) next to the group to reformat. The group expands to show the individual fields within the group .
2. Select the row representing the field to reformat. If the field can be reformatted, the format options become active.



3. Select the **Format**, either from the **Format** section or by using the drop down list.

4. Specify the bit order in the displayed fields by checking/unchecking the **MSB > LSB** checkboxes or by using the drop down list.
5. Select **Apply** or **OK**.

9.3.3 Hiding Fields

To hide a field:

1. Under the Group and Colors column, click the plus symbol (**+**) next to the group that has the field(s) to hide. The group expands to show the individual fields within the group.
2. Check the checkbox in the row representing the field to hide.
3. Select **Apply** or **OK**.

9.4 Display Options: Level Hiding

The 'Level Hiding' tab hides or shows traffic by Event Group. See Figure 9.5 and Table 9.2 on page 397. Select one or more event types from the Event Group list. The selected types are hidden (or shown) in the CATC Trace.

The **Advanced Hiding** button  goes directly to Display Options: Level Hiding.

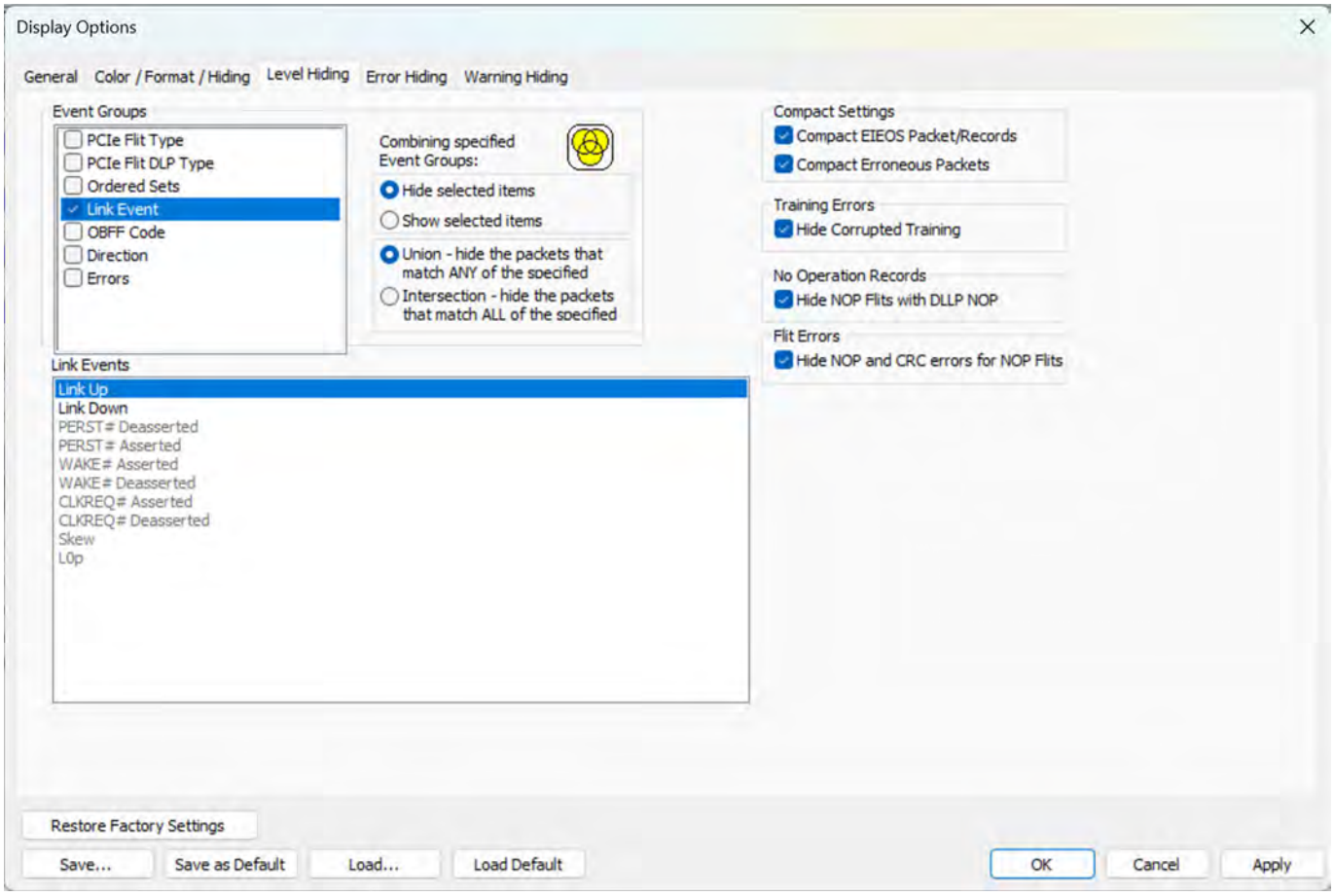


Figure 9.5: Display Options: Level Hiding

TABLE 9.2: Display Options: Level Hiding Features

Feature	Discription
Event Groups	Select one or several event groups to show/hide in the trace. This list varies depending upon the trace contents (i.e., shows CXL content when a CXL trace is open).
Event Groups categories	After selecting event group(s), this section allows further selections. Only items that appear in the trace can be selected.
Combining Specified Event Groups	Hide Selected Items: Hides the items selected in event groups and its categories.
	Show Selected Items: Shows the items selected in event groups and its categories.
	Union: Hide/Show the packets that match ANY of the specified for hiding when selecting several event groups and their categories.
	Intersection: Hide/Show the packets that match ALL of the specified for hiding when selecting several event groups and categories.
Compact Settings	Compact EIEOS Packets/Records: compacts EIEOS packets/ records when selecting compact view.
	Compact Erroneous Packets: Compacts OS packets with errors when selecting compact view.
Training Errors	Hide Corrupted Training: Hides Invalid packets, OS with errors, PMUX and TLP packets inside training.
No Operation Records	Hide NOP Flits with DLLP NOP: Applicable only for Flit mode traces.
Flit Errors	Hide NOP and CRC Errors with NOP Flits: Applicable only for Flit mode traces.

9.4.1 Hiding Levels

1. Select an Event Group from **Event Groups**.
2. Select a subset from ***<event group name>***, where **<event group name>** represents the name of the selected event group, such as Link Events.
3. Select whether to **Hide selected items** or **Show selected items**.
4. Select whether to perform a **union** or **intersection** of specific groups.
5. (Optional) In **Event Groups**, select Direction and choose **Upstream**, **Downstream**, or **Sideband.**
6. (Optional) Select **Compact EIEOS Packets/Records** and/or **Compact Erroneous Packets**.

7. (Optional) Select **Hide Corrupted Training**.
8. (Optional) Select **Hide NOP Flits with DLLP NOP.**
9. (Optional) Select **Hide NOP and CRC Errors for NOP Flits.**
10. Select **Apply** to save the selections. If changes are made, select **Apply** again to save the changes.
11. Click **OK** to save the selections and return to the trace. The trace now shows/hides the selections.

9.4.2 Non-Flit Trace Event Groups

The Event Groups for Non-Flit traces are:

- TLP Type
- TLP Header
- TLP Address/Register
- TLP Prefix
- TLP Requester ID
- TLP Completer ID
- TLP Data Pattern
- TLP Data Lengths
- TLP Traffic Class
- Direction
- TLP Tag
- TLP Sequence Number
- DLLP Type
- DLLP Header
- DLLP Virtual Channel
- ACK/NAK Seq Number
- Ordered Sets
- Link Event
- OBFF Code
- Errors
- IDE Errors
- Message Code
- CXL Auxiliary Packets
- CXL Cache/Mem Protocol Packets
- CXL Cache/Mem LLCTRL Packets
- TLP Decrypted Data Pattern
- IDE Message Code
- IDE Streams

9.4.3 Flit Trace Event Groups

The Event Groups for Flit traces are:

- PCIe Flit DLP Type
- Ordered Sets
- Link Event
- OBFF Code
- Direction
- Errors

9.5 Display Options: Error Hiding

The ‘Error Hiding’ tab hides errors by transaction types (see Figure 9.6). Selecting one or more transaction types from the list results in hiding all these items from the CATC Trace.

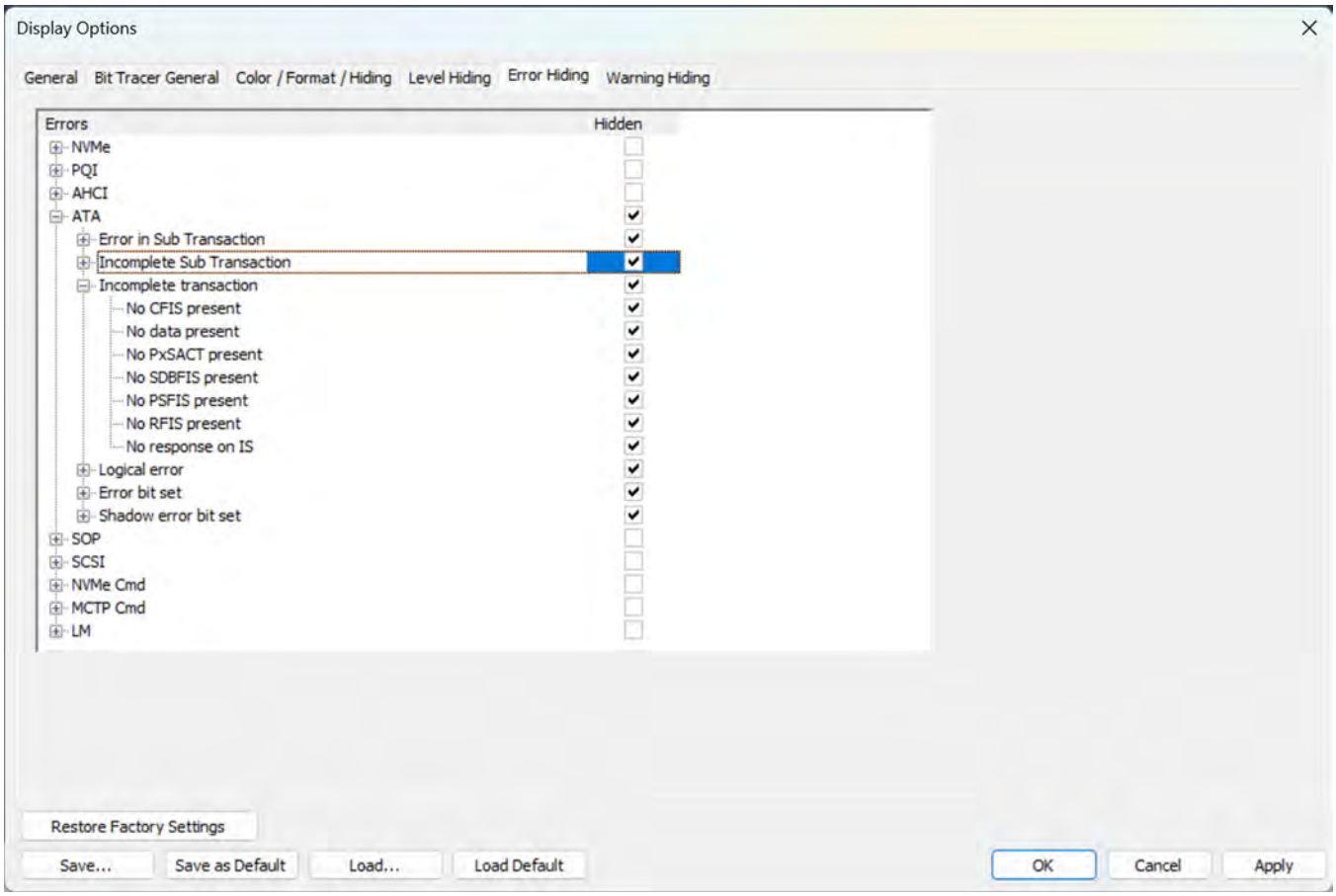


Figure 9.6: Display Options: Error Hiding

9.5.1 Transaction Types

Error Hiding hides a large selection of transaction type errors, including: :

- NVMe
- PQI
- AHCI
- ATA
- SOP
- SCSI
- NVMe Cmds
- LM

9.6 Display Options: Warning Hiding

The 'Warning Hiding' tab hides warnings by transaction type. (see Figure 9.7). Select one or more transaction types from the list to hide them on the CATC Trace.

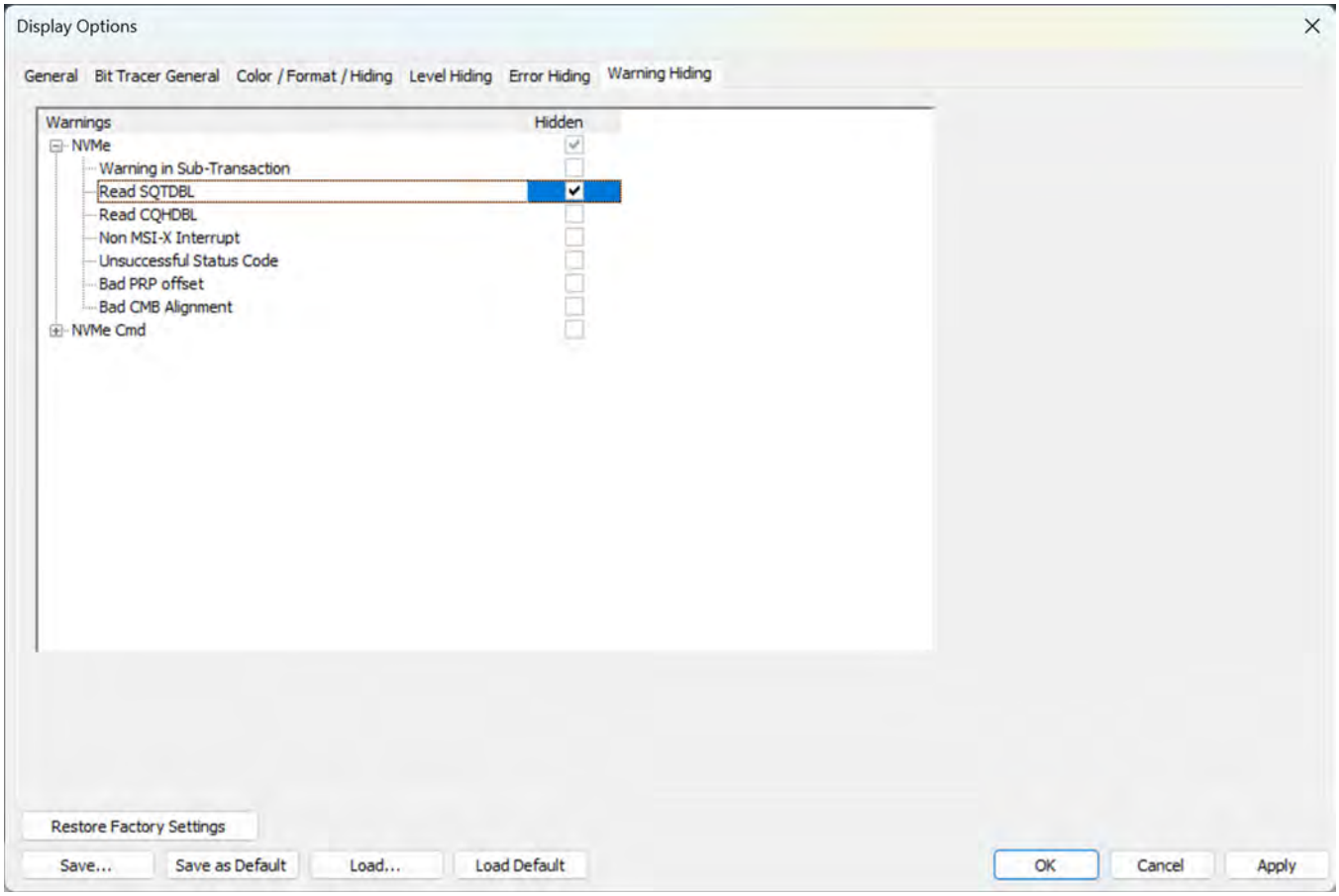


Figure 9.7: Display Options: Warning Hiding

9.6.0.1 Transaction Types

Warning Hiding hides the following transaction types::

- NVMe
- NVMe Cmd

9.7 Load a Previously Saved Display Options File

To open a previously saved **Display Options** file:

1. Select **Load** to use a previously defined display options file. The Open File dialog displays.
2. Select or type the name of the file to load and click **Open**.
3. When the PCIe Protocol Analysis™ returns to **Display Options**, select **OK** to activate the file.

9.8 Saving Display Options

To save customized display options, select the **Save** button. Enter a unique file name. The **.opt** extension is added by default.

9.9 Save as Default

To save the currently specified Display Options to the default file (**default.opt**), select **Save As Default.** When the Analyzer software begins execution, it automatically loads the **default.opt** file, if one exists.

9.10 Load Default

To load the default file (**default.opt**), if one exists, select **Load As Default.** The default display options are applied to the open CATC trace file.

Chapter 12

Reports and Tools

Reports assist you in analyzing traffic recorded by the Analyzer. See Figure 12.1.

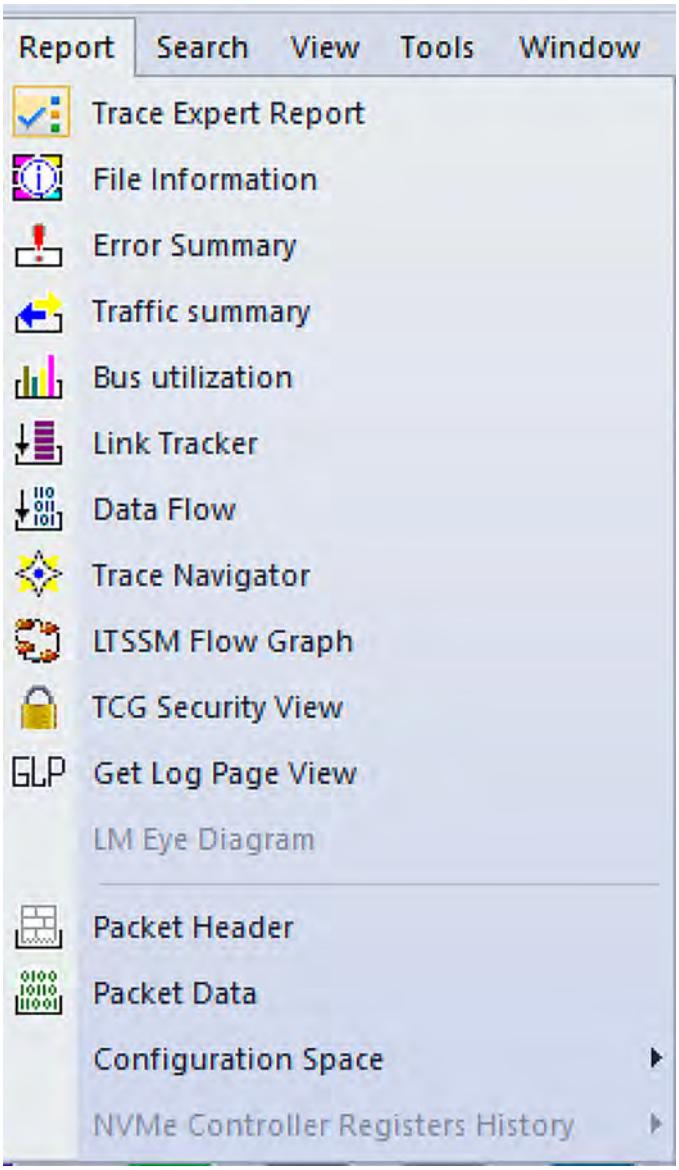


Figure 12.1: Reports Pull Down Menu

The available reports are:

- **Trace Expert**: Generates reports on Performance Analysis, Trace Analysis Statistics, Error Reports and Trace Information. See “NVMe Performance Script Verification” on page 864.
- **Trace Information**: To view general information about the CATC Trace file. See “Trace Expert” on page 736.
- **Error Summary**: To view a count of errors in a CATC Trace file. See “Error Summary” on page 746.
- **Traffic Summary**: To view a summary of protocol-related information in the CATC Trace file summary information about a selected group of items in the CATC Trace file (such as a count of particular frame or packet types). See “Traffic Summary” on page 754.
- **Bus Utilization**: To display information on bandwidth usage for the transmit and receive channels. See “Bus Utilization” on page 767.
- **Link Tracker**: Displays a detailed chronological view of events. See “Link Tracker” on page 775.
- **Data Flow**: Shows marker, packet, direction, type, length, address, payload, handshake, and timestamp information. See “Data Flow Window” on page 781 and “Flow Control Tracking” on page 783.
- **Trace Navigator**: Navigates within the CATC Trace to view the location of errors and triggers, narrow the range of traffic on display, and jump to any point in the CATC Trace. See “Using the CATC Trace Navigator” on page 784.
- **Detail View**: Shows the detail view of the selected packet. See“Detail View” on page 790.
- **LTSSM Flow Graph**: Shows a state diagram of bus activity. See “LTSSM Flow Graph” on page 791
- **TCG Security View:** Shows the Trusted Commuting Group. See “TCG Security View” on page 795.
- **Get Log Page View:** Shows the Log Page View window. See “Get Log Page View” on page 797.
- **LM Eye Diagram:** Displays the samples taken during Lane Margining. See “Lane Margining: Eye Diagram” on page 798
- **Packet Header**: Shows packet header information. See “Packet Header Bar” on page 801
- **Packet Data**: Shows packet or transaction payload. See “Packet Data Window” on page 802.
- **Configuration Space**: Displays a Configuration Space. See “Configuration Space View” on page 803.
- **Metrics**: Measures key operating parameters. See “Using Unit Metrics” on page 808 through “Show Metrics in the Bus Utilization Window” on page 813.
- **Real Time Statistics**: To display statistical information for the channels. See “Real-Time Statistics Window” on page 817.
- **Memory I/O Space Editor**: Displays the Memory I/O Space Editor dialog. See “Tools -> Memory I/O Space Editor” on page 827.
- **TC to VC Mapping**: To display how Traffic Classes are mapped to Virtual Channels (to simplify navigation) and how the CATC Trace display was changed (for example, in Split Transactions). See “Tools -> TC to VC Mapping” on page 838.

- **Timing Calculations**: To view timing measured between two events set within the CATC Trace file. See “Tools -> Timing and Bus Usage Calculations” on page 839.
- **PCIe SSD Base Mapping**: Displays the PCIe SSD Base Address dialog. See “Tools -> PCIe SSD Base Address Mapping” on page 850.
- **Run Verification Scripts**: Allows you to check errors, link transactions, split transactions, metrics, ordered sets, replays, DLLPs, and TLPs. See “Tools -> Running Verification Scripts” on page 861.

Note: In addition to these Reports and Tools, if you select the CXL Flit Data View  a detailed view of the select CXL packet will be shown below the trace view see “CXL Flit Data View” on page 762.

Reports are available from the Report menu and buttons on the Tool bar. Tools are available from the Tools menu.

12.1 Trace Expert

Trace Expert is a reporting tool that is used to create a portable, customized summary and report of a PCI express trace. The generated report groups the selected data and statistics into four groups:

- Performance Analysis
- Trace Analysis Statistics
- Error Reports
- Trace File Information

After a Trace has been loaded, Trace Expert is available from the Main Toolbar as shown in Figure 12.2.

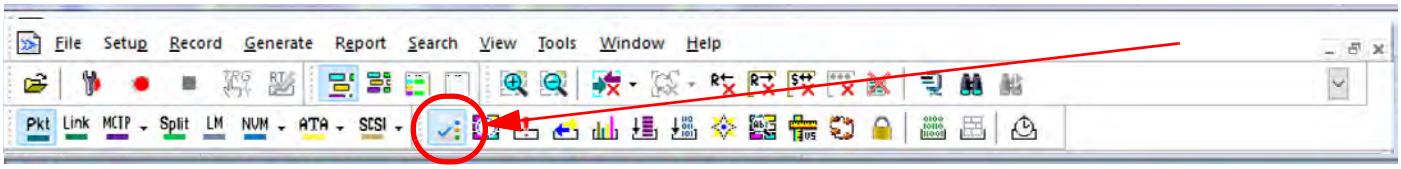


Figure 12.2: Main Toolbar: Trace Expert

To launch the Trace Expert dialog click on the icon. Different report sections can be selected for inclusion into the final report using the dialog. The path where the report will be generated can be set at the bottom of the dialog (see Figure 12.3 on page 737). Any additional decoding required to generate the report will be done automatically.

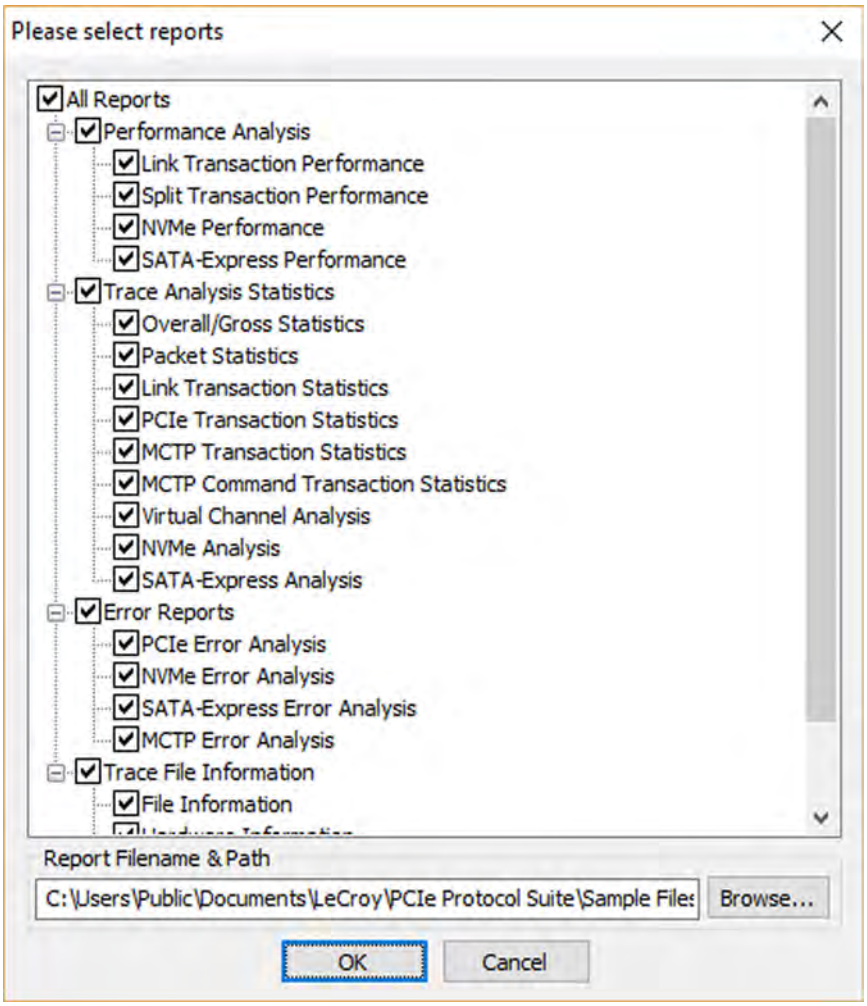


Figure 12.3: Trace Expert Report Types and Path

The generated report (see Figure 12.4 on page 738) has sections which can be expanded to show the associated data. The generated file is self-contained and portable so it can be safely emailed or archived. It will open automatically in the default browser once it is successfully generated. Icons on the top right can be used to:

- Save All (Saves to User's Download folder)
- Expand All
- Collapse All
- Print All of the currently displayed view.

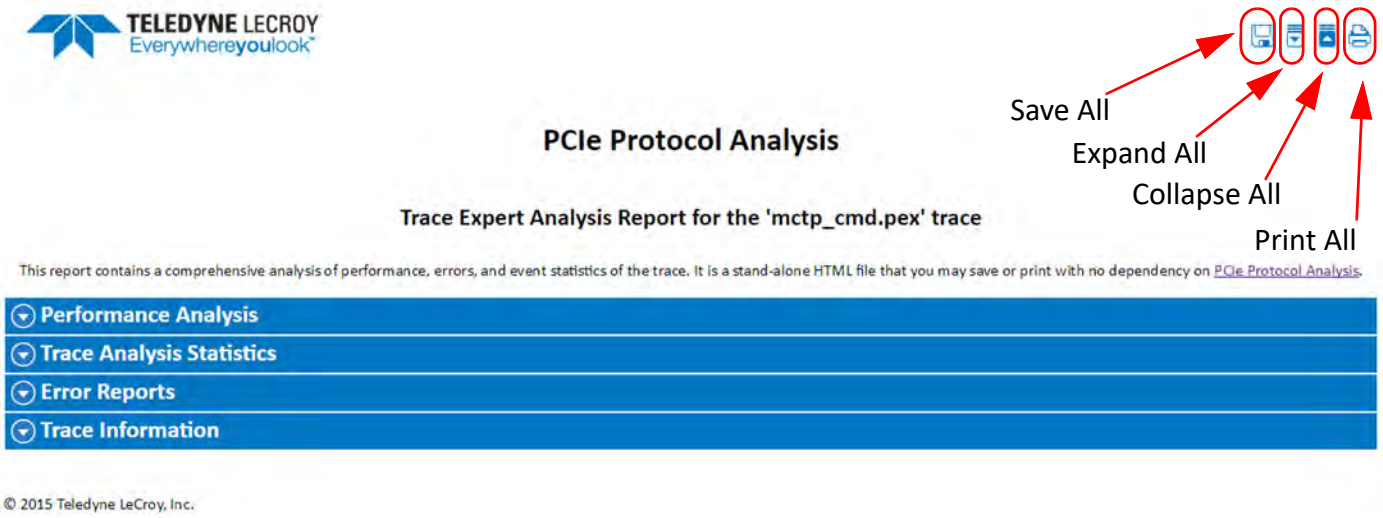


Figure 12.4: Trace Expert Main Menu

Select “Performance Analysis” on page 739 to bring up the respective dialog.

Select “Trace Analysis Statistics” on page 740 to bring up the respective dialog.

Select “Error Reports” on page 741 to bring up the respective dialog.

Select “Trace Information” on page 742 to bring up the respective dialog.

12.1.1 Performance Analysis

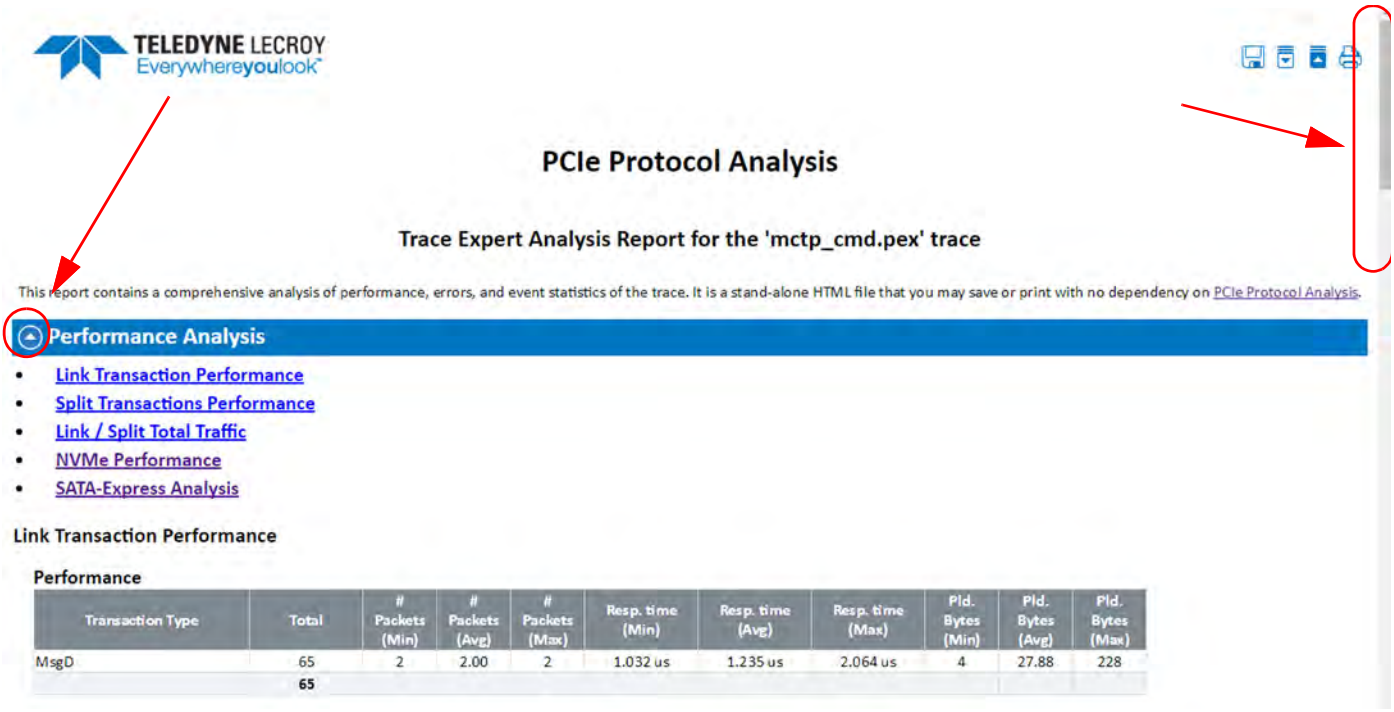


Figure 12.5: Trace Expert - Performance Analysis

You can select other types of transactions to see the other reports.

- Link Transaction Performance
- Split Transaction Performance
- Link / Split Total Traffic
- NVMe Performance
- SATA-Express Analysis

Scroll down to see the other reports and information.

12.1.2 Trace Analysis Statistics

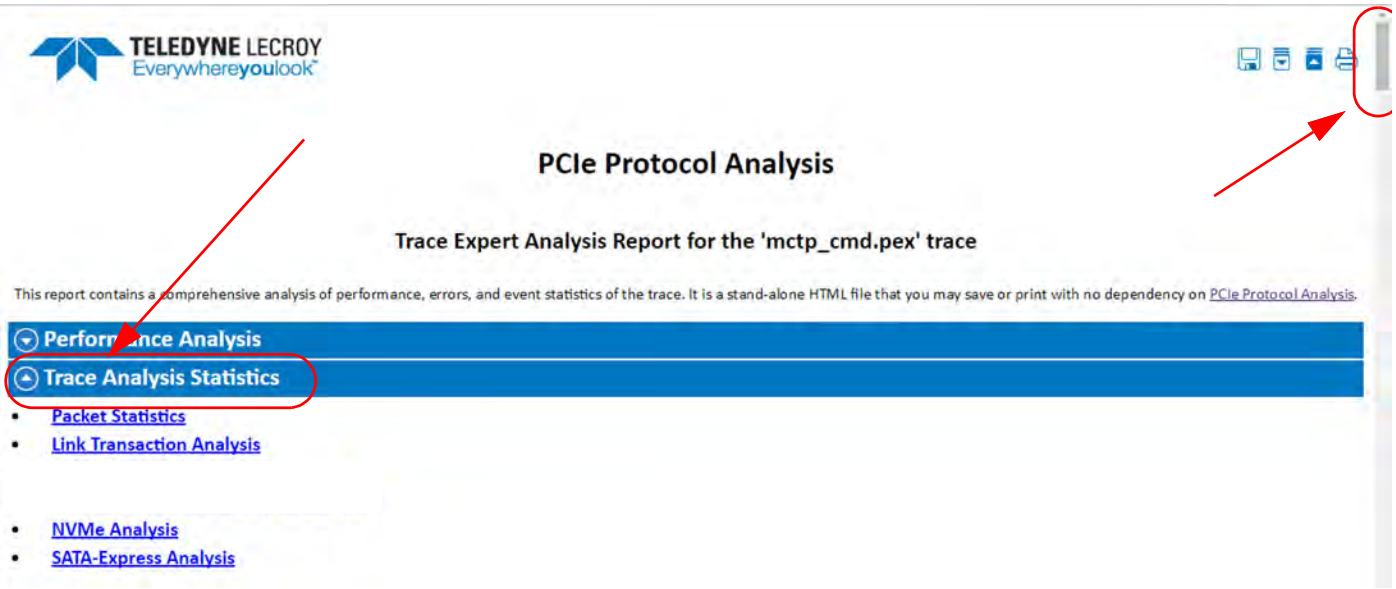


Figure 12.6: Trace Analysis Statistics

Selecting Trace Analysis Statistics will produce the following reports:

- Packet Statistics
- Link Transaction Analysis
- NVMe Analysis
- SATA-Express Analysis

Scroll down to see the other reports and information.

12.1.3 Error Reports

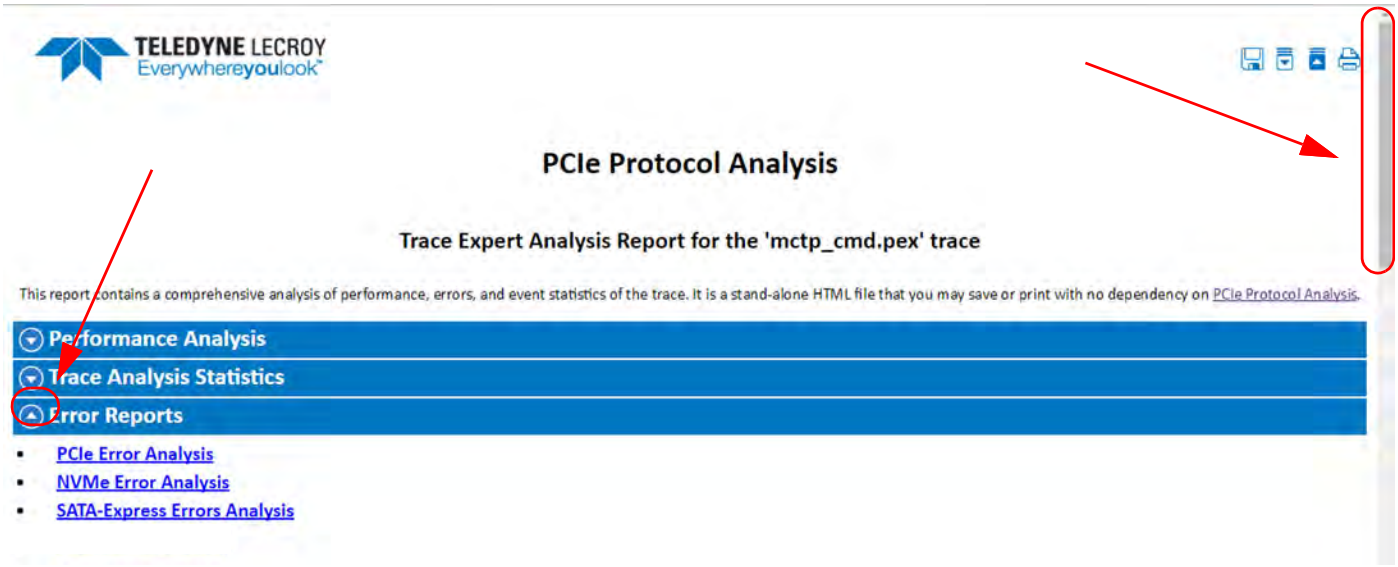


Figure 12.7: Error Reports

Selecting Error Reports generates the following reports:

- PCIe Error Analysis
- NVMe Error Analysis
- SATA-Express Errors Analysis

Scroll down to see the other reports and information.

12.1.4 Trace Information

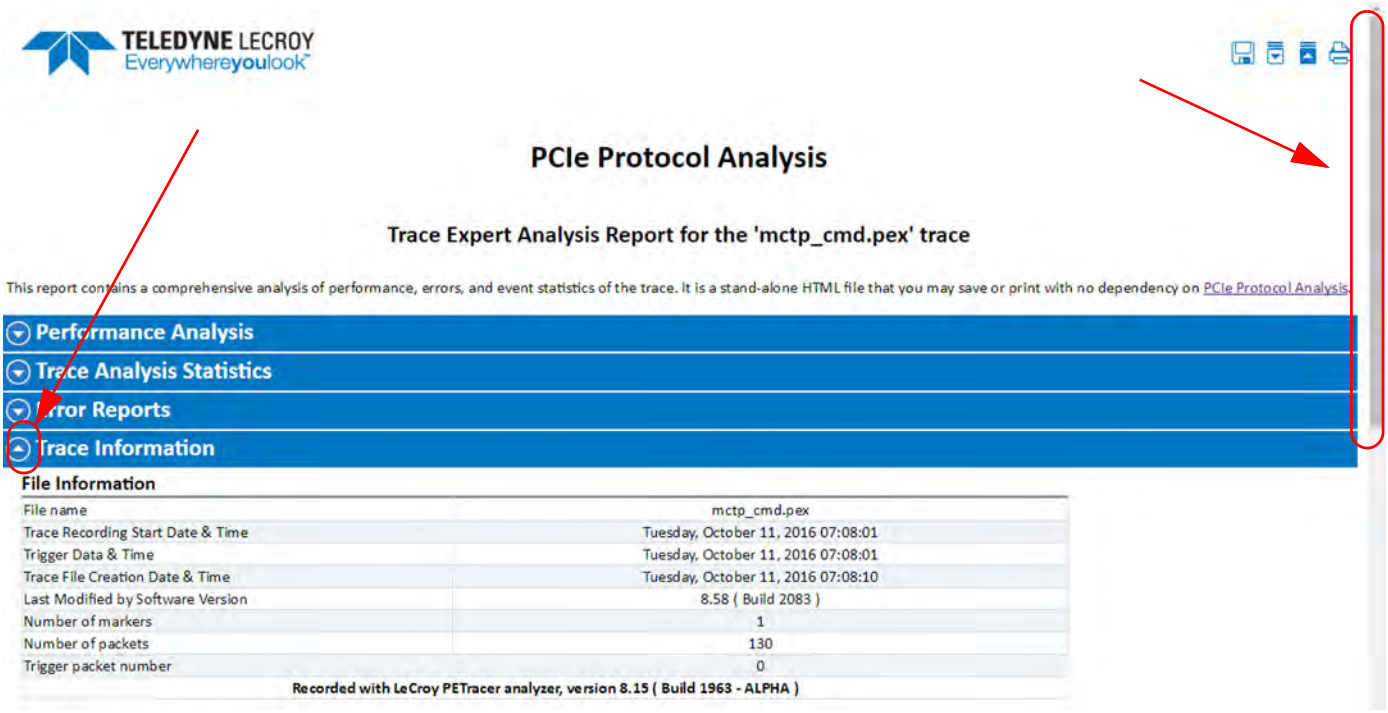


Figure 12.8: Trace Information

Selecting Trace Information generates the following reports:

- File Information
- Hardware Information
- Recording Options
- License Information
- IDE Keys—shown only for IDE Traces

Scroll down to see the other reports and information.

12.2 Trace Information

The Trace Information window provides a summary on the currently displayed file.

Select **Reports > Trace Information**  to display the Trace Information window.

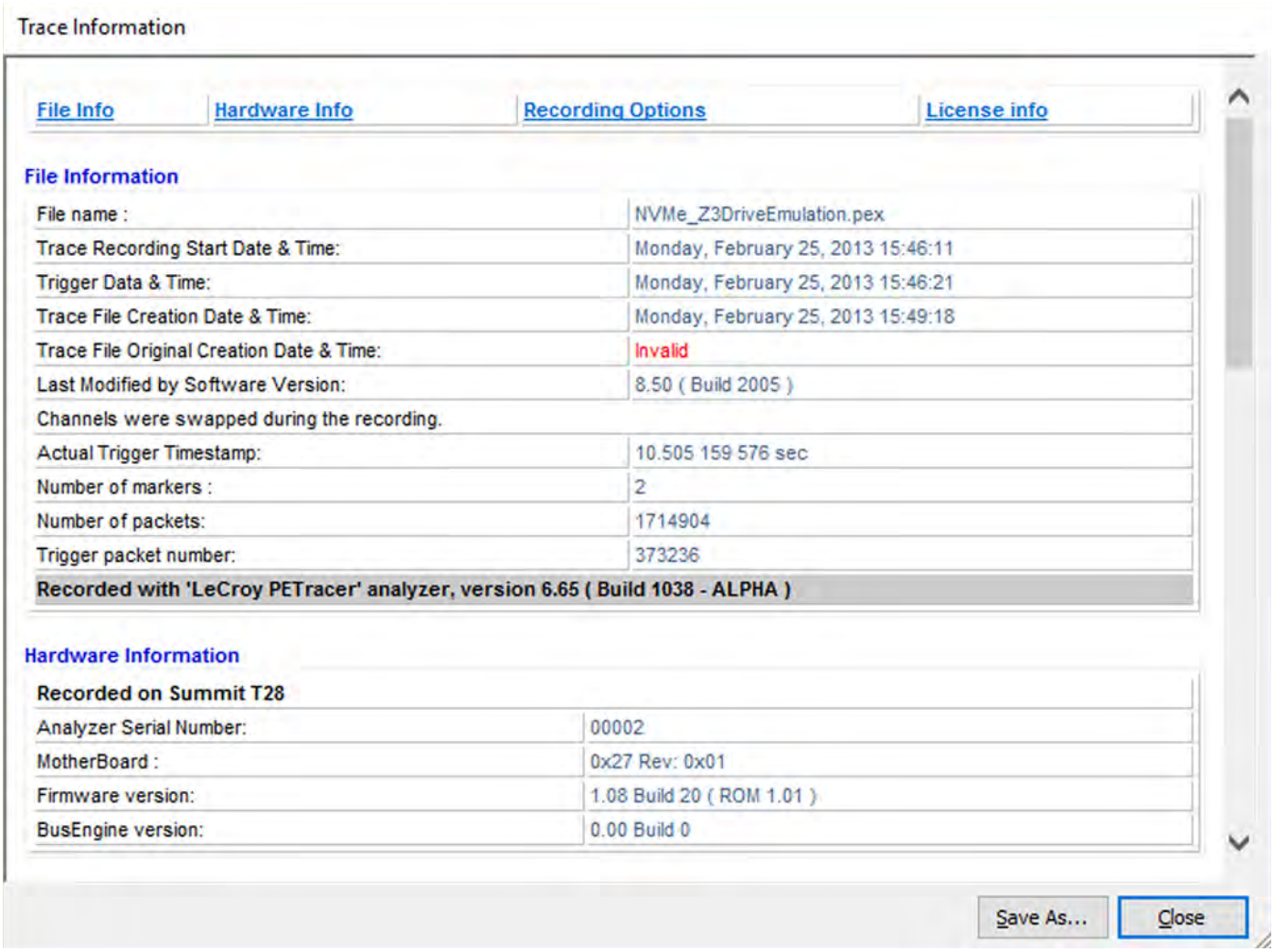


Figure 12.9: Trace Information Part 1

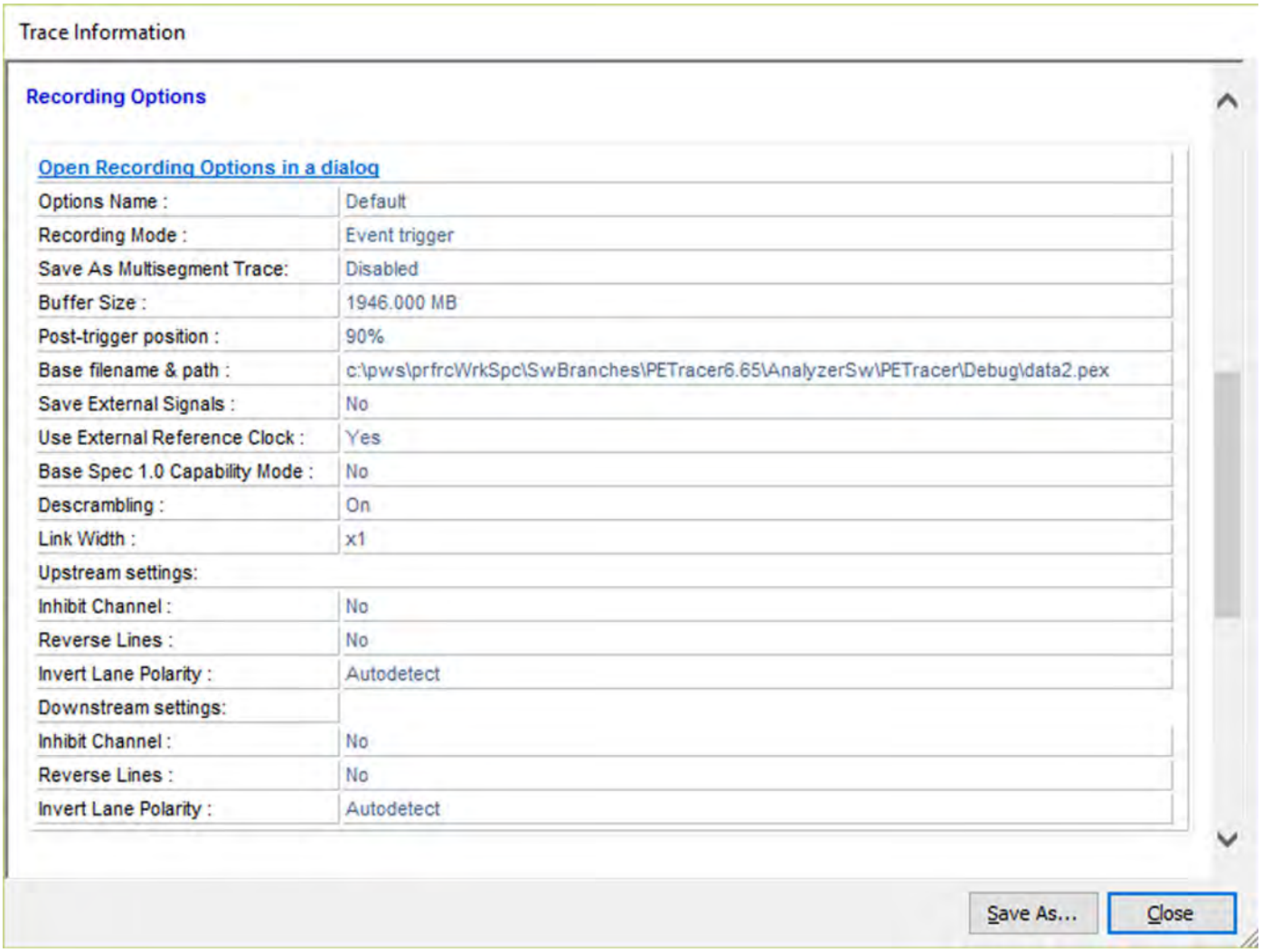


Figure 12.10: Trace Information Part 2

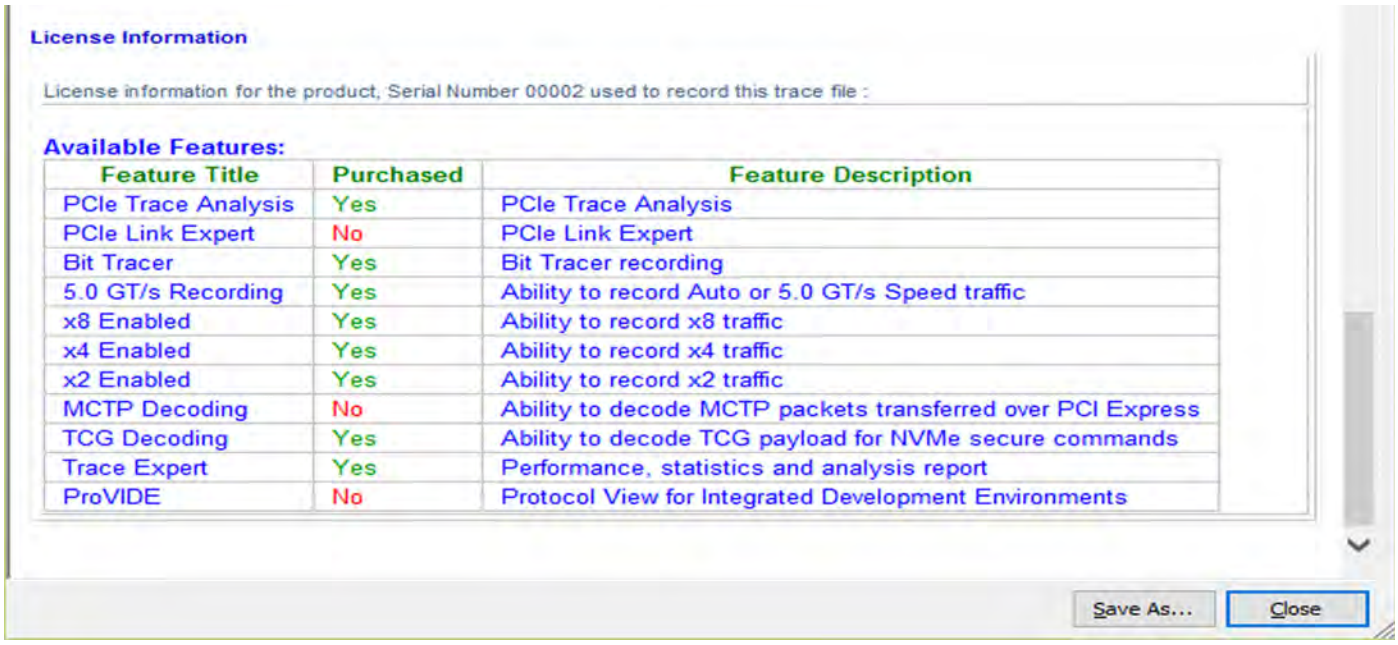


Figure 12.11: Trace Information Part 3

12.3 Error Summary

The Error Summary dialog displays the number of errors for each event and the packet containing the errors.

Select **Reports > Error Summary** or click  to open the Error Summary dialog (see Figure 12.12 on page 746).

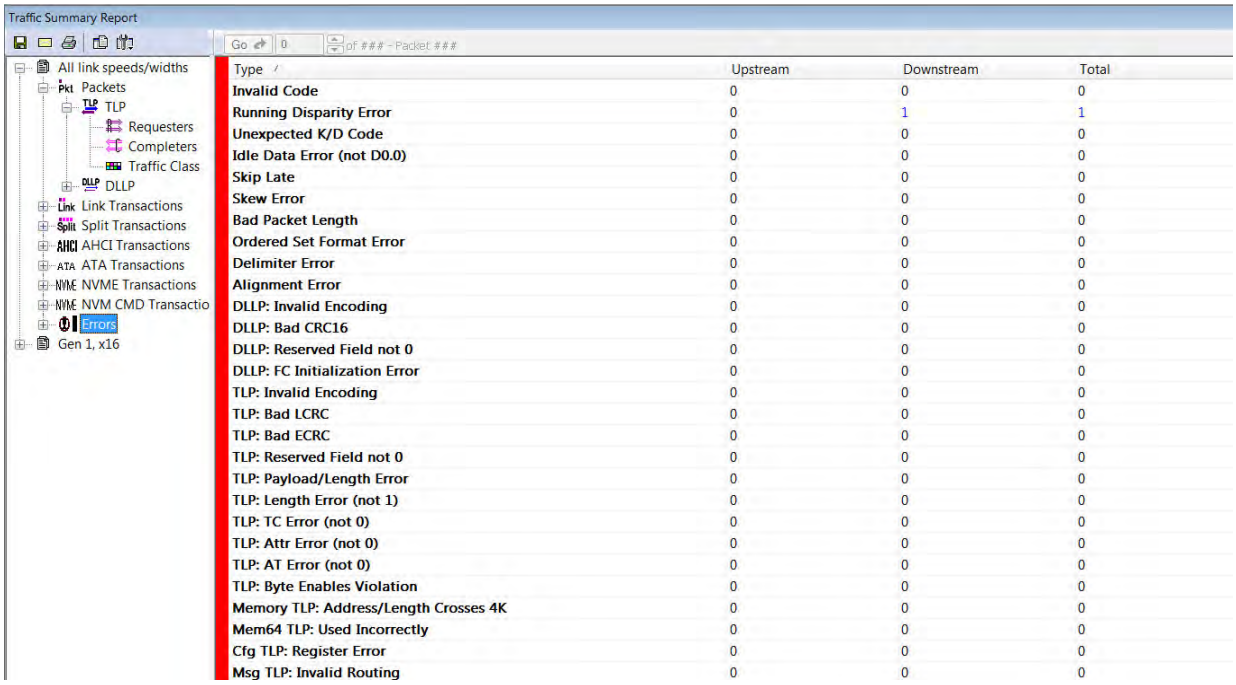


Figure 12.12: Error Summary Dialog.

12.3.1 Error Summary for Storage Protocols

After decoding a trace for the corresponding storage protocol, the CATC Trace will have a summary ready of the errors found for the trace. Example: The AHCI Error Summary dialog is a sub-entry for the main Error Summary dialog. It displays the number of errors for each AHCI transaction containing the errors.

Select **Reports > Error Summary** to open the Error Summary dialog.

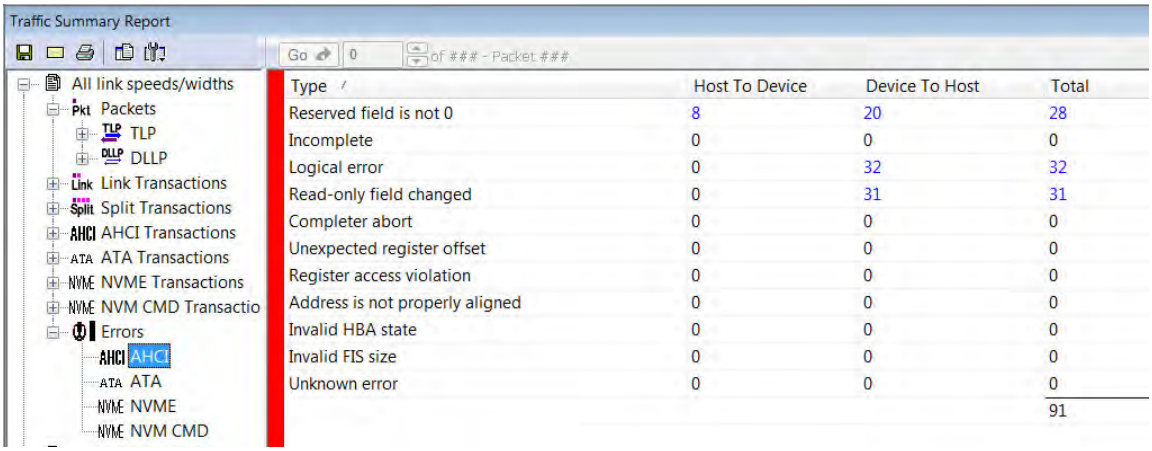


Figure 12.13: AHCI Error Summary Dialog.

The five types of AHCI errors are describe below:

Reserved Field not Zeroes

One or more fields inside the AHCI transaction are not filled with all 0s. The AHCI specification states that all reserved fields and registers must be filled with 0s.

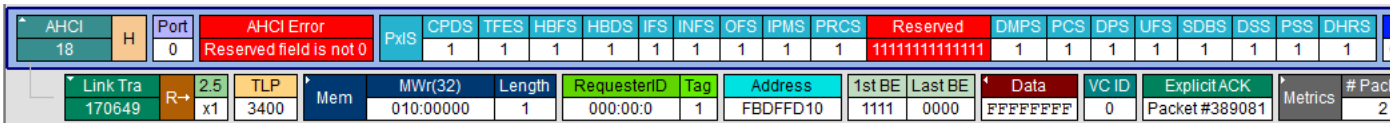


Figure 12.14: Reserved Field Not Filled With Zeroes

Note: Reserved fields for AHCI level are not displayed when filled with all 0s.

Incomplete

The AHCI transaction does not contain enough data or lower-level transactions (Link or Split) are marked as incomplete.

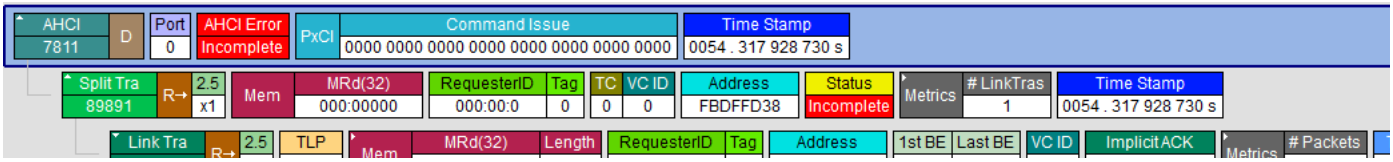


Figure 12.15: Incomplete

Logical Error

One or more fields are in an inconsistent state relative to the other fields in the same or other registers.

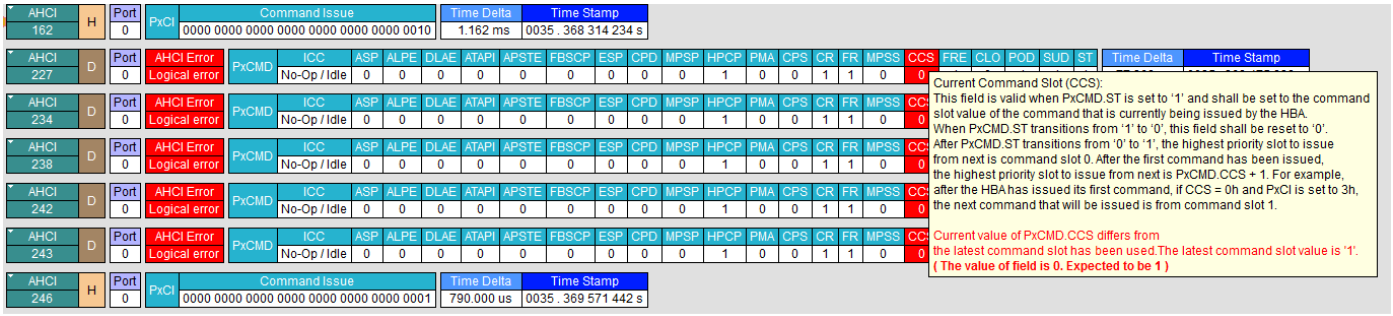


Figure 12.16: Logical Error

Read-only Field Changed

The value of the read-only field differs from the previous one.

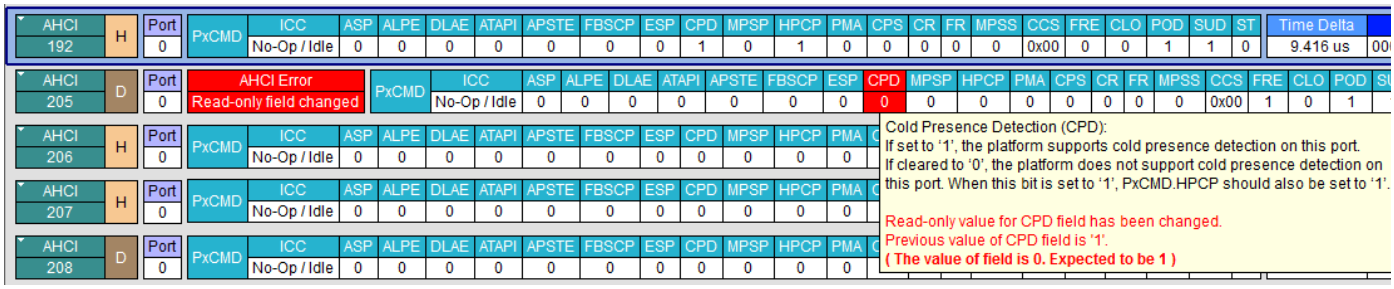


Figure 12.17: Read-only Field Changed

Unknown

The AHCI decoder is unable to decode a particular transaction correctly. This can be caused by missing base address information. Make sure the enumeration phase has been recorded in the trace or provide base address information by selecting **Tools > PCIe SSD Base Address Mapping**.

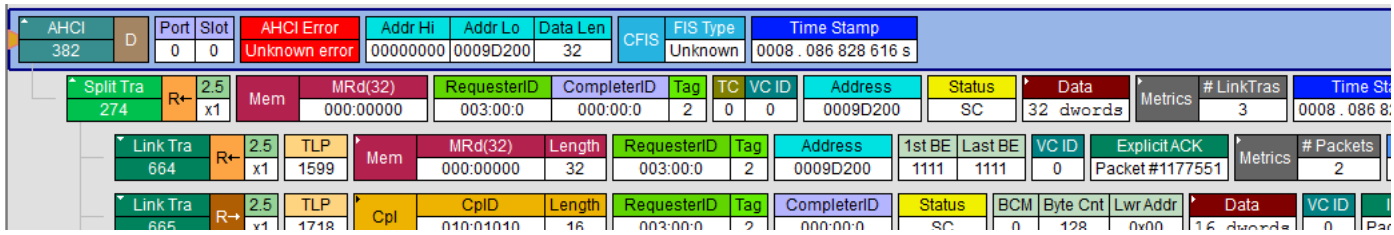


Figure 12.18: Unknown

Checks for Logical error and Read-only field depending on the values obtained from previous registers. It can result in false-positive or false-negative detections in case of partially saved trace file. The AHCI transaction can be marked as incomplete in case of saving a portion.

12.3.2 Error Summary for Storage Protocols -- NVMe

The NVMe sub-entry of the Error Summary dialog displays the number of NVMe errors found while decoding the trace at the NVMe level as shown in Figure 12.19, Figure 12.20 and Figure 12.21.

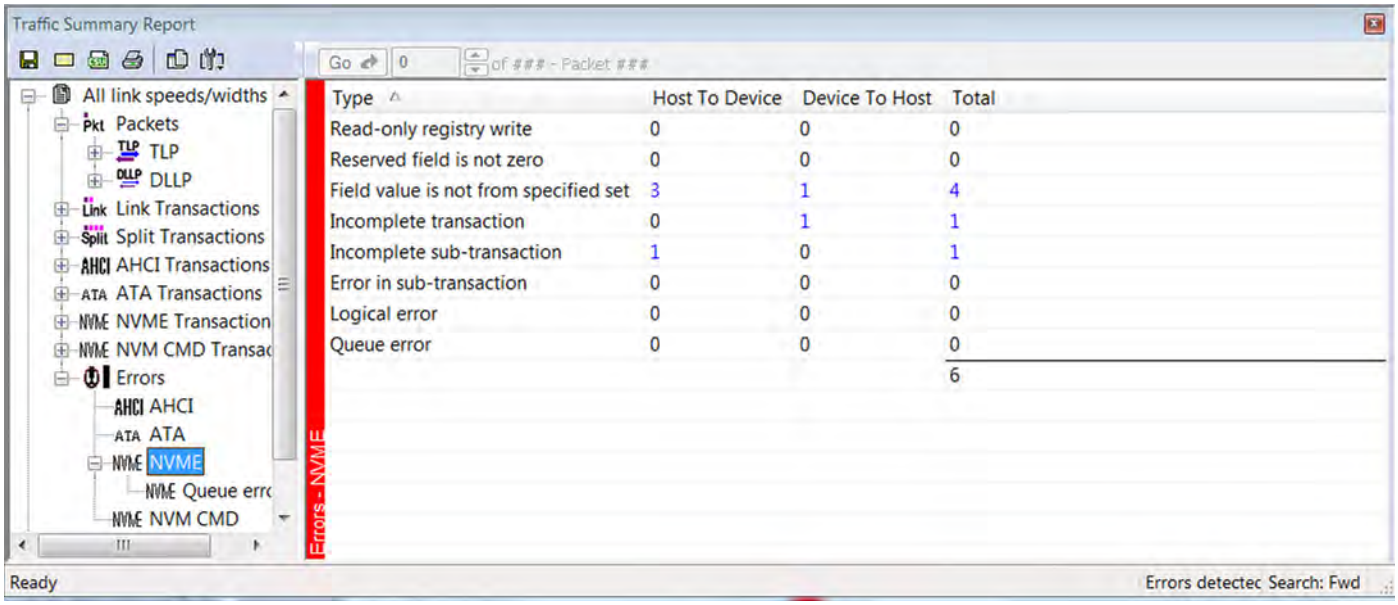


Figure 12.19: NVMe Errors After Decoding the Trace

12.3.2.1 Types of NVMe Errors:

1. Read-only register write: An attempt to write to a read only register was made.
2. Reserved field is not zero: One (or more) of the fields set as reserved in the current spec revision is not zero - this could indicate a problem such as reversed bit ordering, or it could be intentional such as working with unreleased version of the next specification or user debug bits.
3. Field values is not from specified set: There is a value used in the indicated field that is not used in the currently released specification. If working with an early release of the next specification, or a proprietary feature this could be valid otherwise it would normally indicate a problem.
4. Incomplete transaction: One or more of the steps for a NVMe transaction is missing eg no completion queue entry after submission queue submission.
5. Incomplete sub-transaction: Some NVMe transactions have sub states and this indicates that within a substate part of the expected sequence is missing.
6. Error is sub-transaction: Some NVMe transactions have sub states and this indicates that within a substate an error in the sequence or value was detected.
7. Logical error: Groups any potential logic errors, such as declaring a payload of 64 bytes (0) but sending 0 bytes.
8. Queue error: There was an error in writing to the queue. Eg writing to a queue before it was created or trying to write additional entries to a queue that was full. There are a series of specific errors available on the NVMe Queue error report.

12.3.3 NVMe Queue Errors

The NVMe Queue Error sub-entry of the Error Summary dialog lists NVMe errors which are specific to interacting with the NVMe queues.

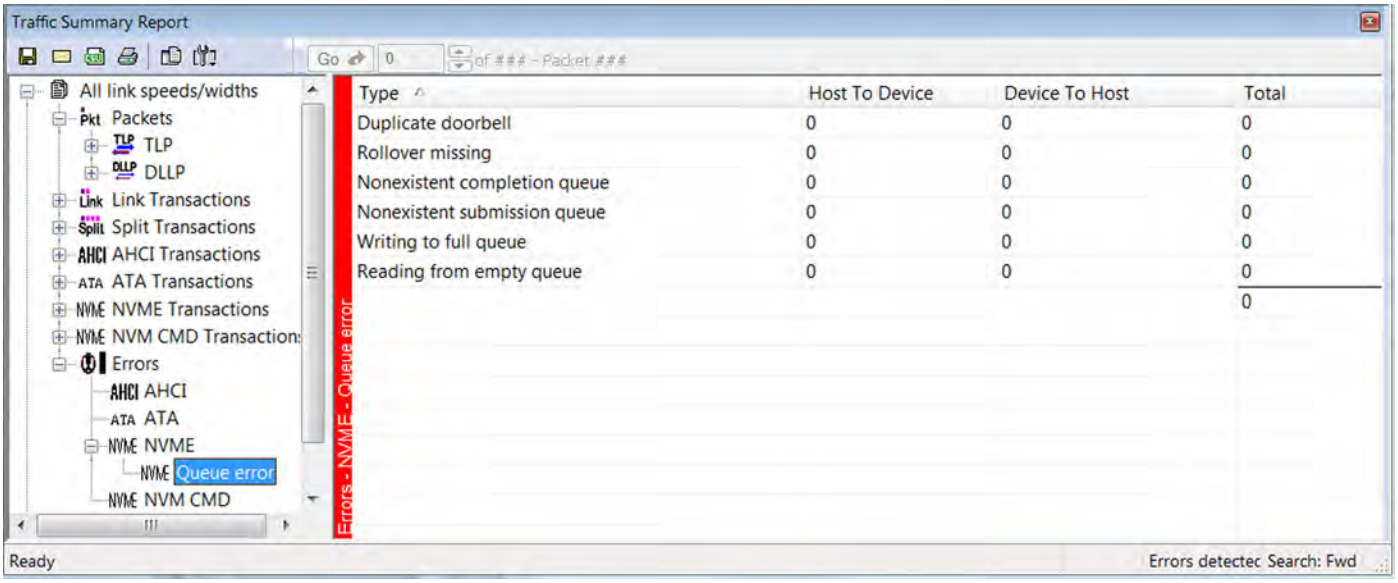


Figure 12.20: NVMe Errors Specific to NVMe Queues

12.3.3.1 Types of NVMe Queue Errors

1. Duplicate doorbell: The same doorbell was used consecutively.
2. Rollover missing: The queue rollover was missed.
3. Nonexistent completion queue: A completion queue was attempted to be used before it had been created.
4. Nonexistent submission queue: A submission queue was attempted to be used before it had been created.
5. Writing to full queue: All possible entries in the queue were previously filled and have not been cleared yet and the current write would add more entries than the declared size of the queue.
6. Reading from empty queue: A queue has had no entries submitted or all previous entries have already been read such that there are no entries in the queue to be read, however a read was attempted even though there are no entries.

12.3.4 NVMe CMD Errors

The NVMe CMD sub-entry of the Error Summary dialog lists errors which are specific to NVMe command decoding. See Figure 12.21

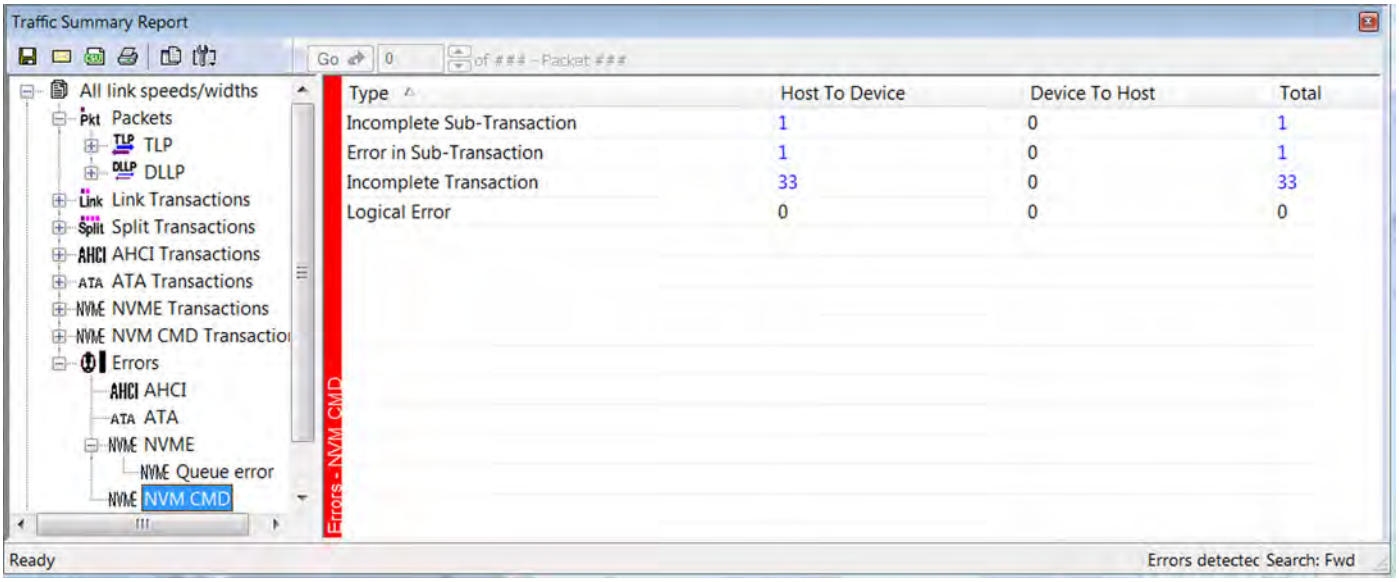


Figure 12.21: NVMe Errors Specific to NVMe Commands

12.3.4.1 Types of NVMe CMD Errors

1. Incomplete Sub-Transaction: Some NVMe transactions have sub states and this indicates that within a substate the required sequence was not completed.
2. Error in Sub-Transaction: Some NVMe transactions have sub states and this indicates that within a substate an error in the sequence or value was detected.

3. Incomplete Transaction: One (or more) of a transactions steps are missing, example shows a transaction missing the doorbell and the preceding one that has all the transaction steps. See Figure 12.22.

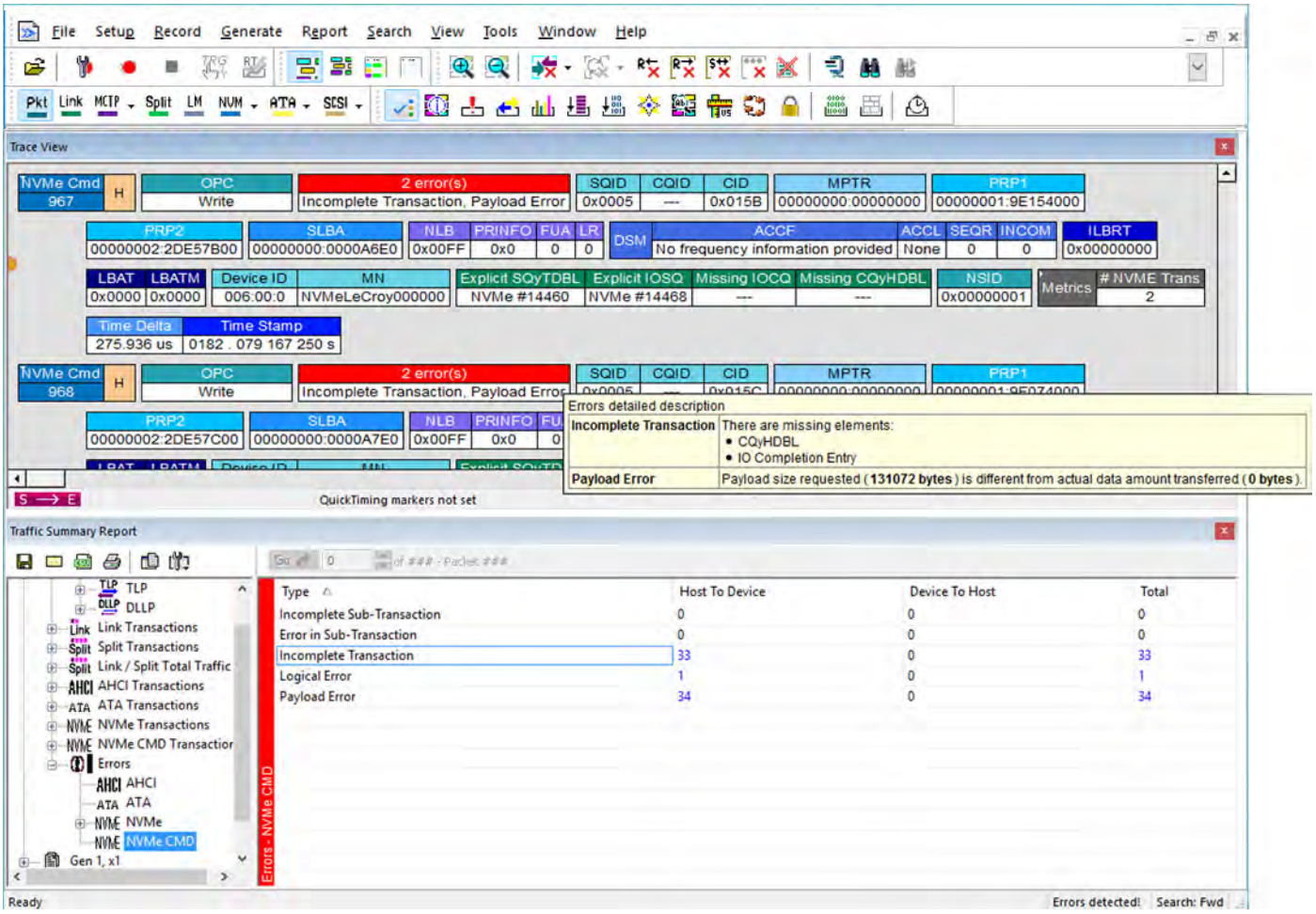


Figure 12.22: NVMe CMD Error -> Incomplete Transaction with Tooltip

4. Logical Error: Groups any potential logic errors, such as declaring a payload of 64 bytes (0) but sending 0 bytes. See Figure 12.23.

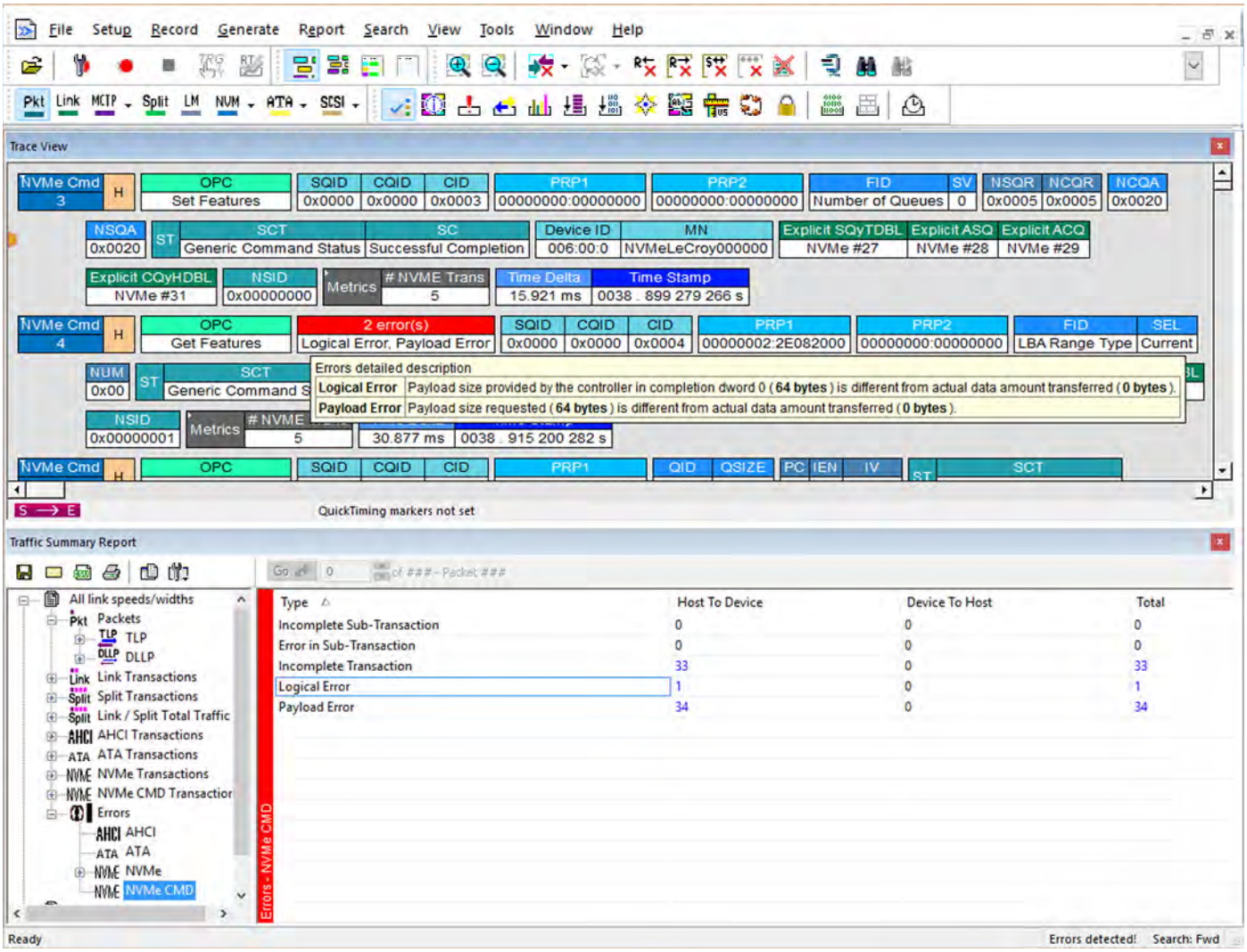
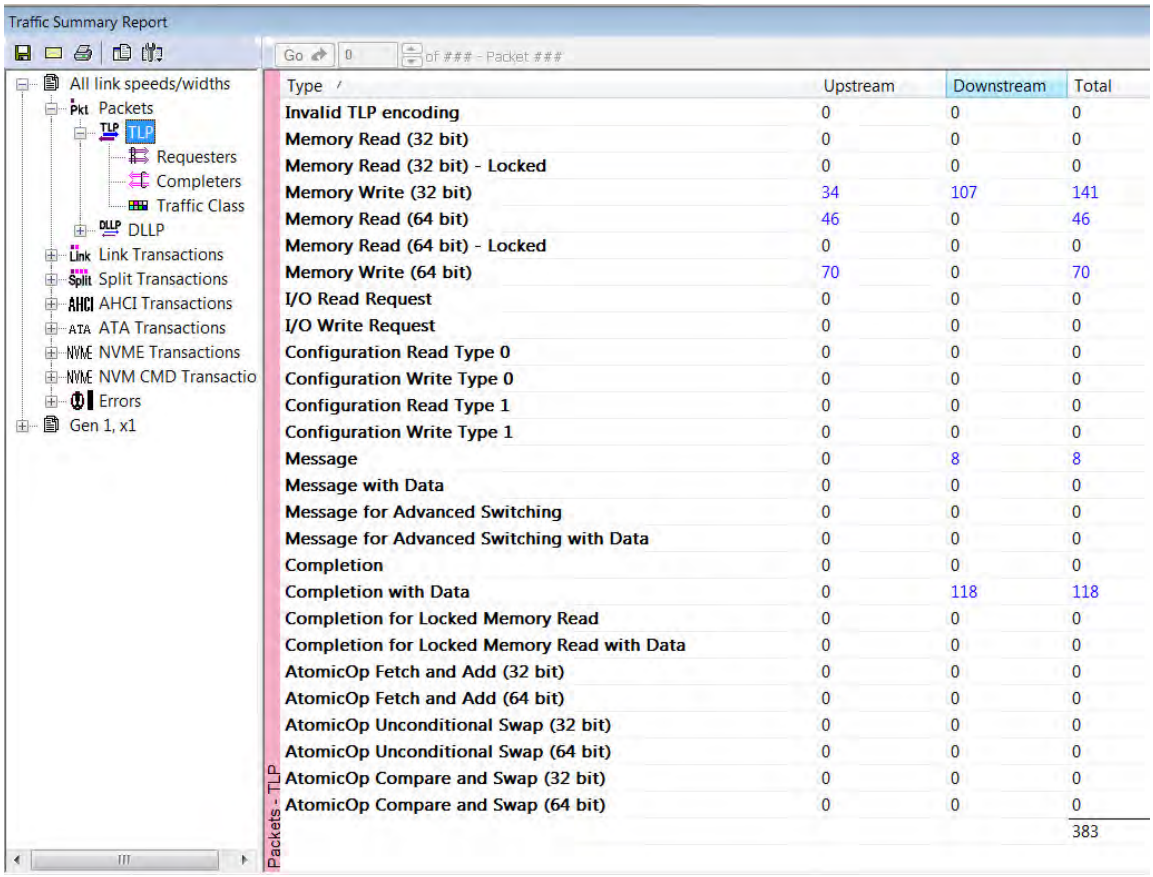


Figure 12.23: NVMe CMD Error -> Logical Error with Tooltip

12.4 Traffic Summary

The Traffic Summary window summarizes the traffic in the current CATC Trace. The left side of the window displays a tree of protocol levels. The right side displays a summary of traffic for the displayed levels.

Select **Reports > Traffic Summary** or click  to display the Traffic Summary window.



Type	Upstream	Downstream	Total
Invalid TLP encoding	0	0	0
Memory Read (32 bit)	0	0	0
Memory Read (32 bit) - Locked	0	0	0
Memory Write (32 bit)	34	107	141
Memory Read (64 bit)	46	0	46
Memory Read (64 bit) - Locked	0	0	0
Memory Write (64 bit)	70	0	70
I/O Read Request	0	0	0
I/O Write Request	0	0	0
Configuration Read Type 0	0	0	0
Configuration Write Type 0	0	0	0
Configuration Read Type 1	0	0	0
Configuration Write Type 1	0	0	0
Message	0	8	8
Message with Data	0	0	0
Message for Advanced Switching	0	0	0
Message for Advanced Switching with Data	0	0	0
Completion	0	0	0
Completion with Data	0	118	118
Completion for Locked Memory Read	0	0	0
Completion for Locked Memory Read with Data	0	0	0
AtomicOp Fetch and Add (32 bit)	0	0	0
AtomicOp Fetch and Add (64 bit)	0	0	0
AtomicOp Unconditional Swap (32 bit)	0	0	0
AtomicOp Unconditional Swap (64 bit)	0	0	0
AtomicOp Compare and Swap (32 bit)	0	0	0
AtomicOp Compare and Swap (64 bit)	0	0	0
			383

Figure 12.24: Traffic Summary Dialog

Buttons at the top of the Traffic Summary window change the display format and enable data to be exported to email, file, or the printer.

12.4.1 Traffic Summary for Storage Protocols

After decoding a trace for the corresponding storage protocol, the CATC Trace will have a summary ready of the commands existing in the trace. Example: The AHCI Traffic Summary window summarizes the AHCI traffic in the current CATC Trace. The right side displays a summary of AHCI transactions and errors.

Select **Reports > Traffic Summary** to open the Traffic Summary dialog.

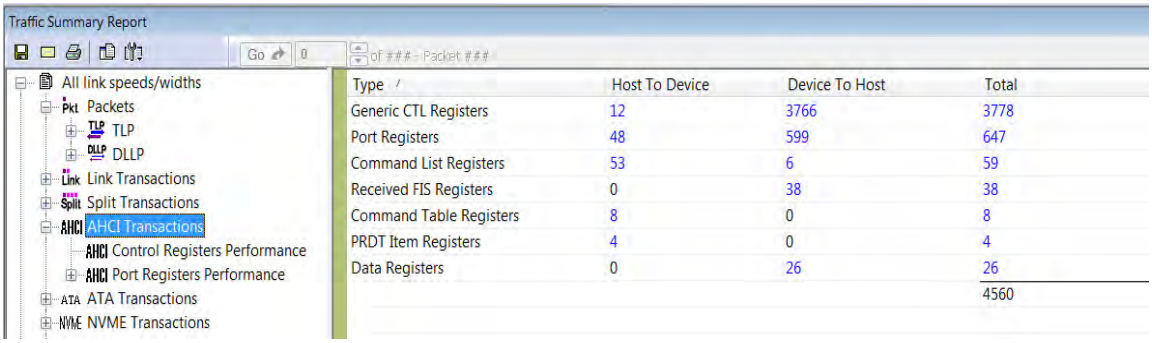


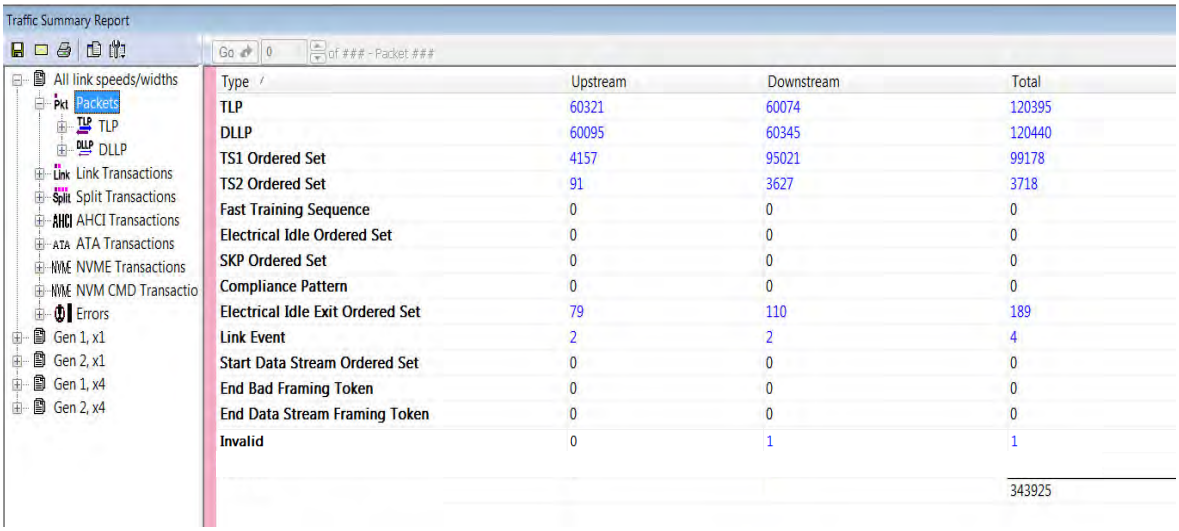
Figure 12.25: AHCI Traffic Summary Dialog

12.4.2 Using the Traffic Summary Window to Search the CATC Trace

You can use the Traffic Summary window to move the CATC Trace to packets of interest:

1. Click one of the numbers in the right side of the Traffic Summary window (see the following figure).

   The CATC Trace jumps to the first instance of the selected protocol.



2. Click the **up** or **down** arrows  . The CATC Trace jumps forward or backward through the display to the next instance of selected protocol level.

12.4.3 NVMe Queue Time Metrics

NVMe Queue Time Metrics can be seen in the Traffic Summary, which includes all of the Doorbell Metrics (see Figure 12.26).

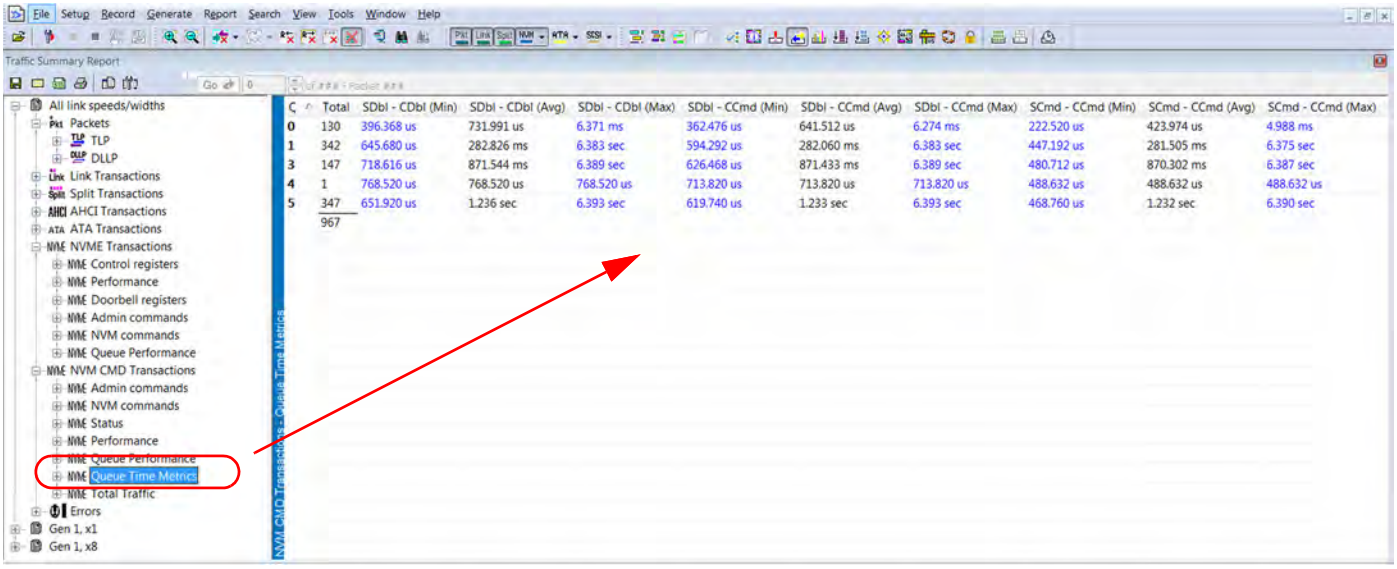


Figure 12.26: NVMe Queue Time Metrics for Doorbell Operations

NVMe Queue Time Metrics Defined (Commands/Transactions)

TABLE 12.15: NVMe Queue Time Metrics (Commands/Transactions)

NVMe Queue Time Metrics	Definition
# NVME Trans	Number of NVME Transactions - the total number of NVME Transactions that compose this NVME Command
# Link & Split Trans	Number of Link & Split Transactions - the total number of Link & Split Transactions that compose this NVME Transaction
Response Time	Time it took to transmit this NVME Command/Transaction on the link, from the beginning of the first packet in the NVME Command/Transaction to the end of the last packet in the NVME Command/Transaction
Latency Time	Time measured from the end of transmission of the NVMe submission command to start of transmission of the NVMe completion command
Pld. Bytes	Payload: Number of payload bytes this NVME Command transferred
Thrpt MB/s	Data Throughput: Payload divided by response time, expressed in megabytes (MB = 1024*1024 bytes) per second (applies to both Commands and Transactions)
IOPS	Input/Output Operation per Second: Calculated as weighted total of all transactions that overlap with the current one, divided by duration of the current transaction
SDbl - CDbl	Time measured between Submission Doorbell and Completion Doorbell
SDbl - CCmd	Time measured between Submission Doorbell and Completion Command
SCmd - CCmd	Time measured between Submission Command and Completion Command

These definitions are readily available by loading an NVMe Trace, Decoding the NVMe Commands or Transaction, locating the Metrics block in the Trace View and hovering the cursor over each of the NVMe Queue Time Metrics to bring up the Tool Tip.

NVME Command Example

As an example for NVMe Command: For SDbl - CDbl see Figure 12.27.

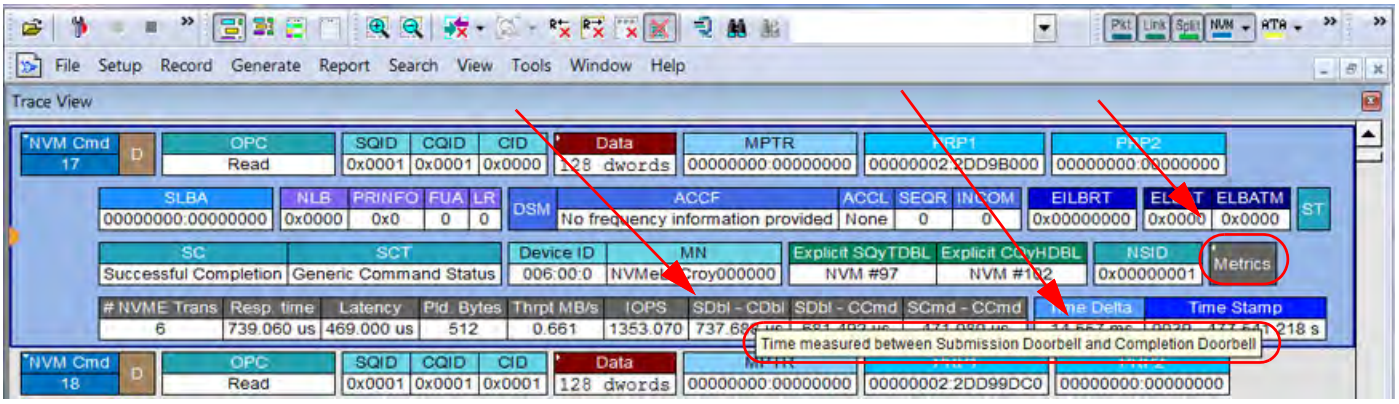


Figure 12.27: NVMe Queue Time Metrics Defined: SDbl - CDbl

NVME Transaction Example

As an example for NVMe Transactions: For Resp time: see Figure 12.28.

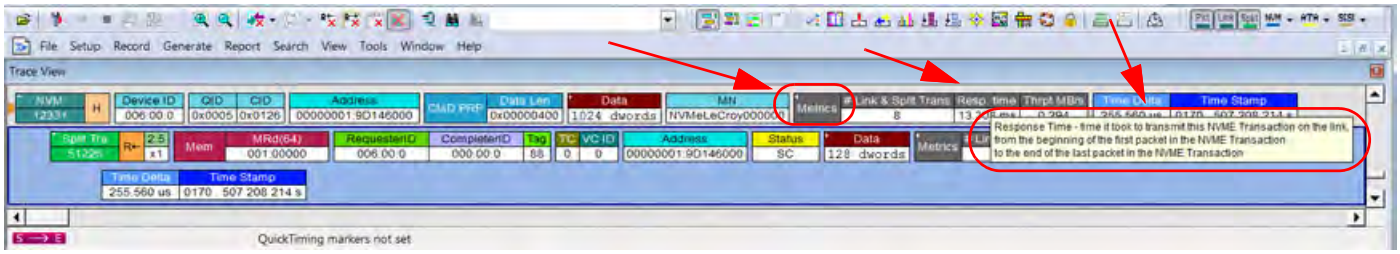


Figure 12.28: NVMe Transactions Metrics: Response Time

12.4.4 Traffic Summary Buttons

Buttons at the top of the Traffic Summary dialog provide options for exporting the data or formatting its appearance:

	Save. Saves Traffic Summary results into an HTML format.
	Email. Attaches an HTML file of the results to a new email.
	Print. Prints results.
	Text. Displays results in HTML format.
	Options. Opens a drop-down menu with the following options: **Grid Lines**: Displays/Hides grid lines **Row Selection**: Allows entire rows to be selected **Tight Columns**: Reformats column widths to match data **Event Navigation**: Skip Hidden Items Show Hidden Items Prompt each time

12.4.5 Traffic Summary for Flow Control

After loading a trace with Flow Control packets in it, you can display the packets which have flow control data and the associated trace as shown below (see Figure 12.29).

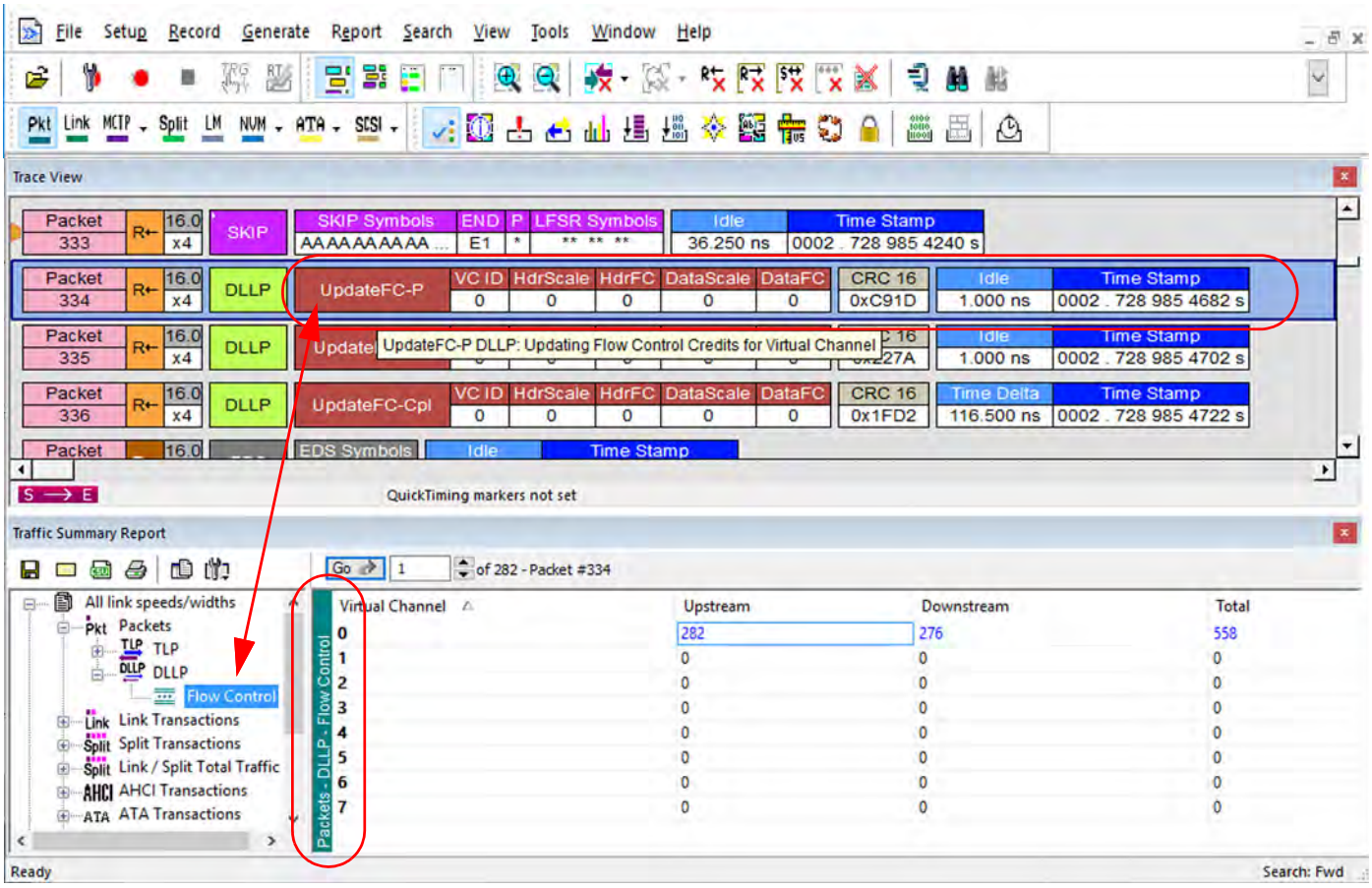


Figure 12.29: Flow Control Trace Showing Traffic Summary

12.4.6 Example: CXL in Traffic Summary

When you have a trace with CXL traffic, you can see that traffic in the Traffic Summary Report. See Figure 12.30.

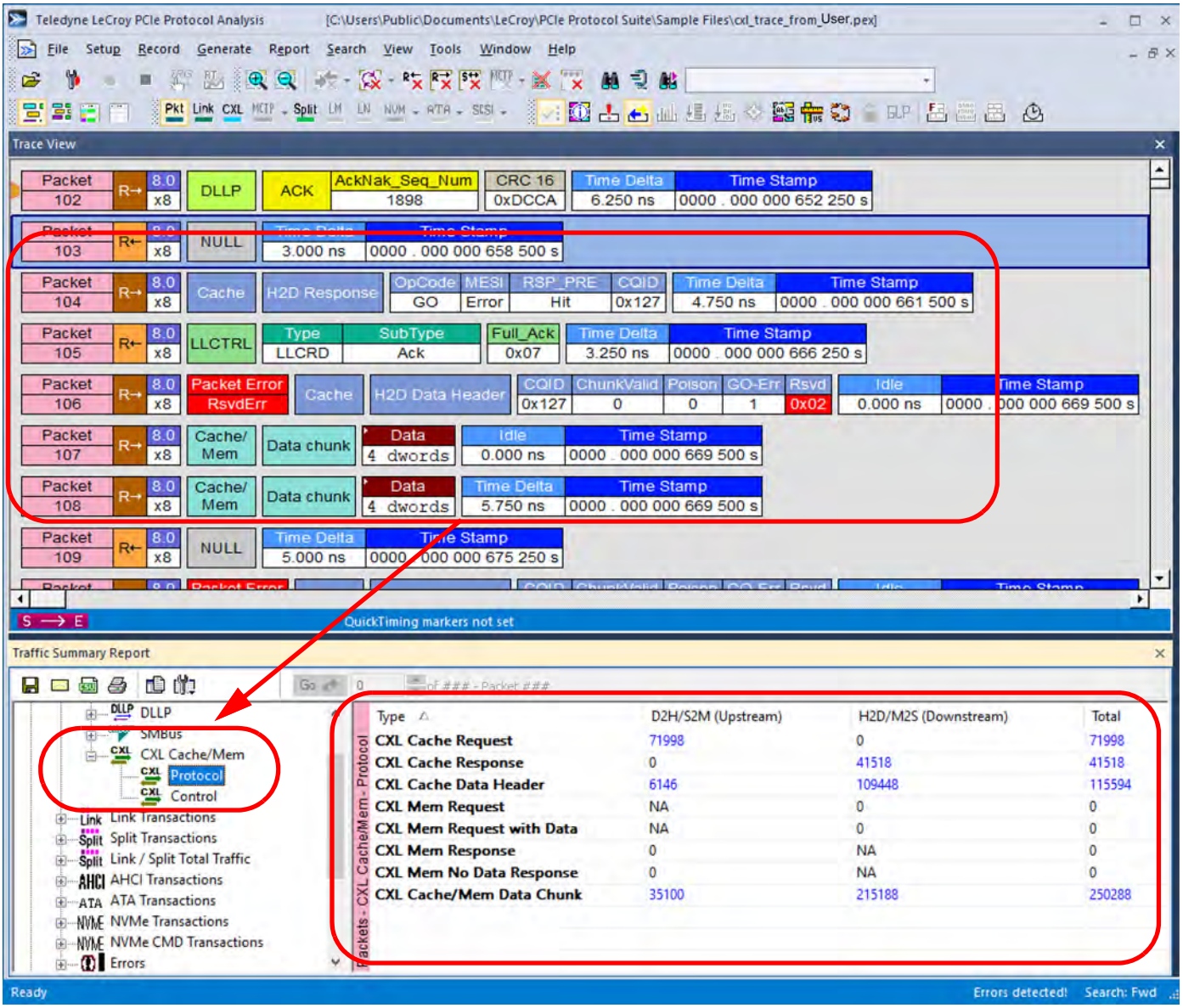


Figure 12.30: Traffic Summary: CXL traffic

12.4.7 Example: CXL Errors Shown in Traffic Summary Report

The PCIe Protocol Analysis software can decode and display a wide variety of CXL errors in the Traffic Summary Report. See Figure 12.31.

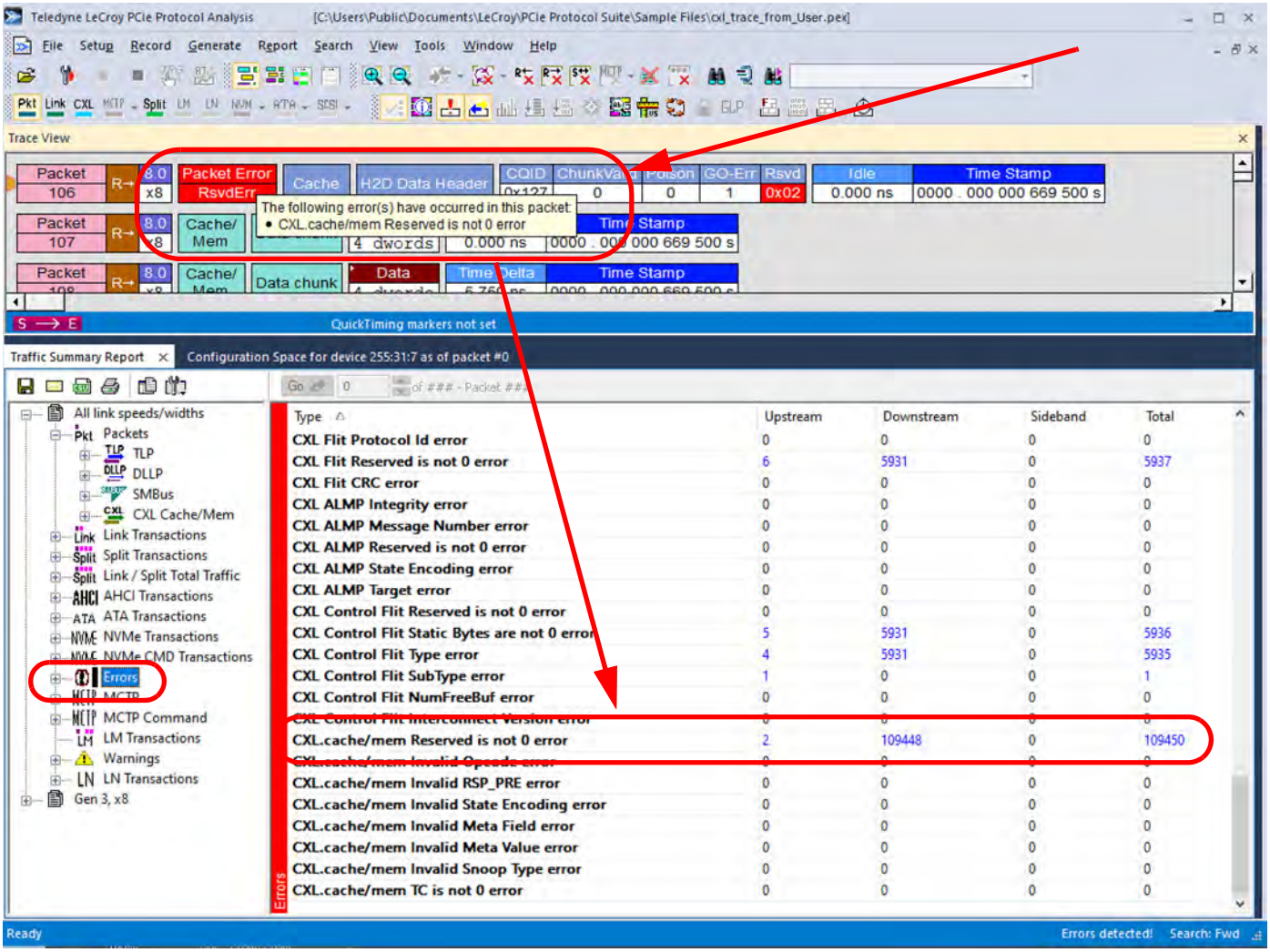


Figure 12.31: CXL Errors: Shown in Traffic Summary Report

12.4.8 CXL Flit Data View

If you select the CXL Flit Data View icon from the main toolbar you'll get a detailed view of the CXL Flit data. See Figure 12.32 and Figure 12.33 on page 763.

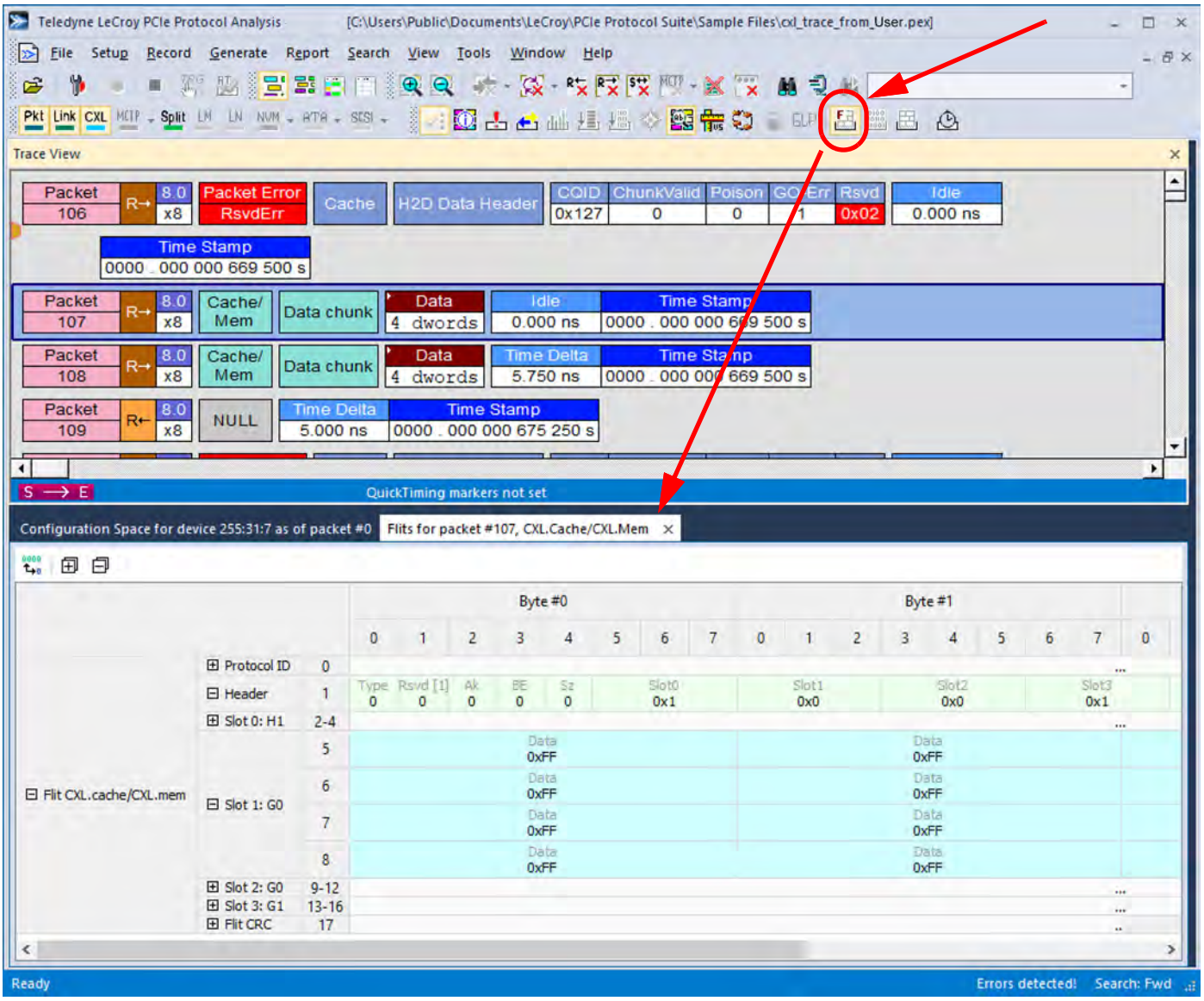


Figure 12.32: CXL Flit Data View: Close Up View Left side of Display

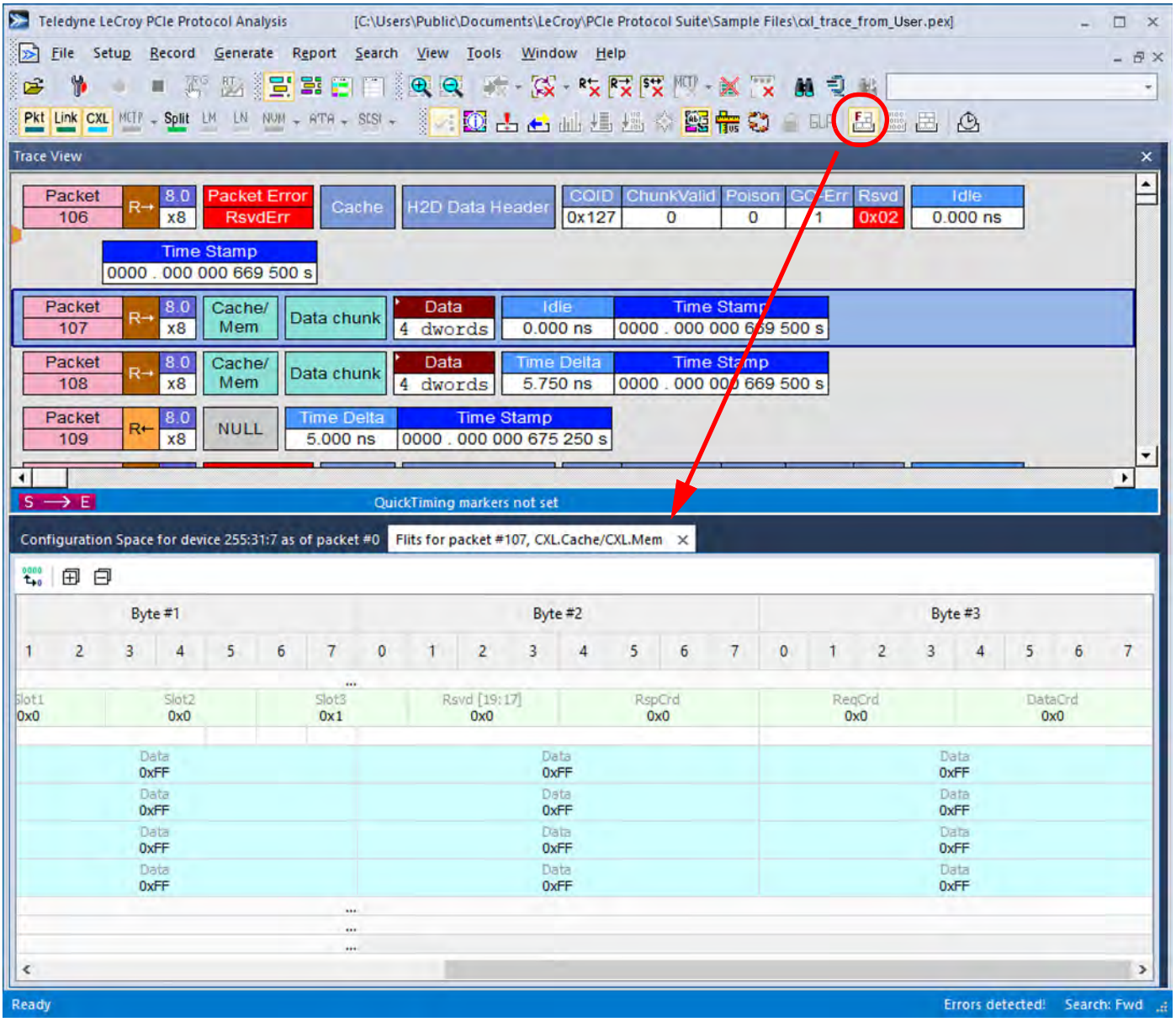


Figure 12.33: CXL Flit Data View: Close Up View Right side of Display

A second way to show the CXL Flit Data view is to select a CXL as shown below and the packet Flit view can also be opened from the menu "Show Flit Fields" once one does a right-click at the packet carried by a flit. See Figure 12.34.

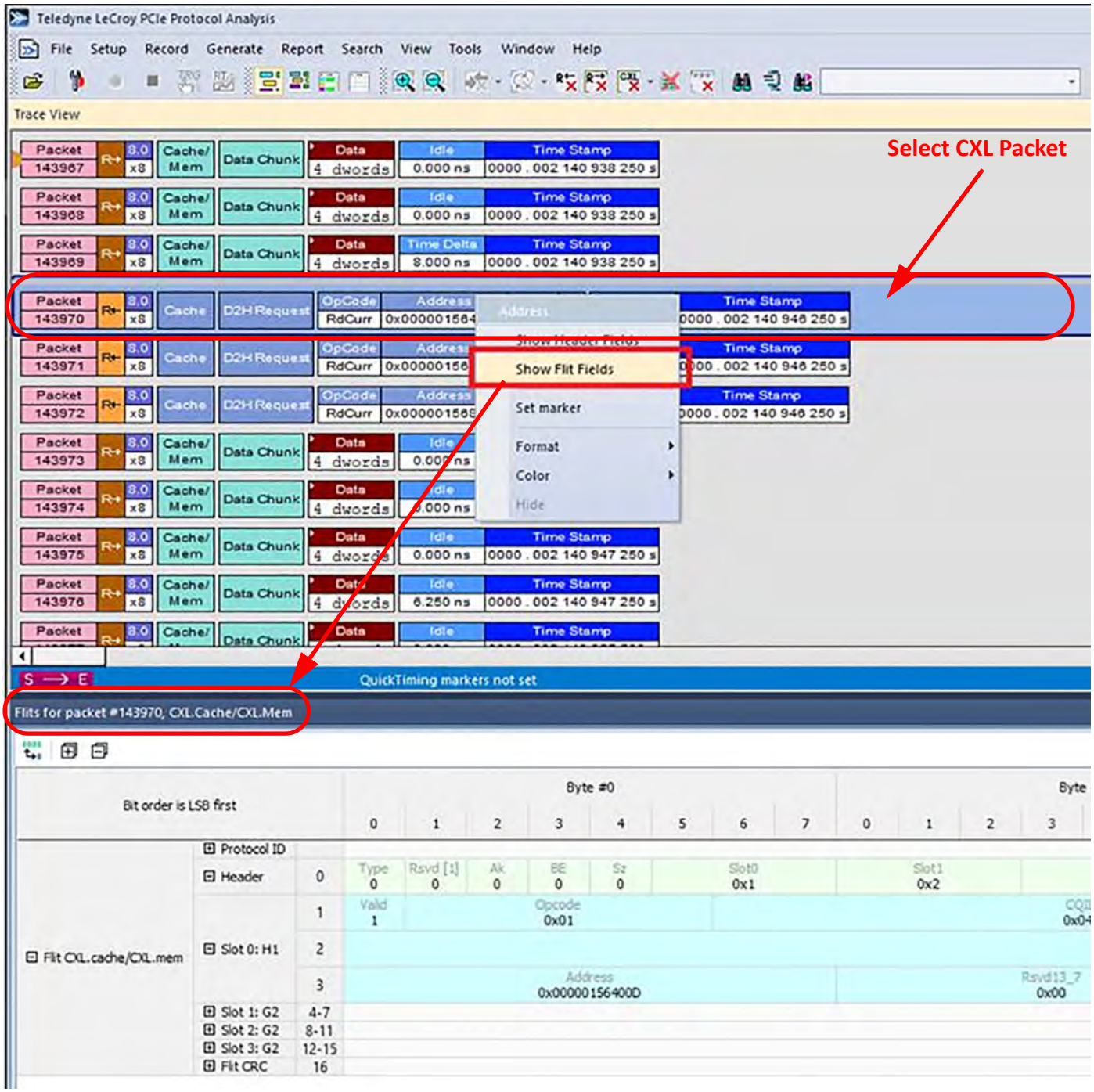


Figure 12.34: CXL Flit Data View from selecting packet and right-click

The CXL Flit Data view can be toggled from DWORD view to Byte view by clicking on the icon at the far left of the screen. See Figure 12.35.

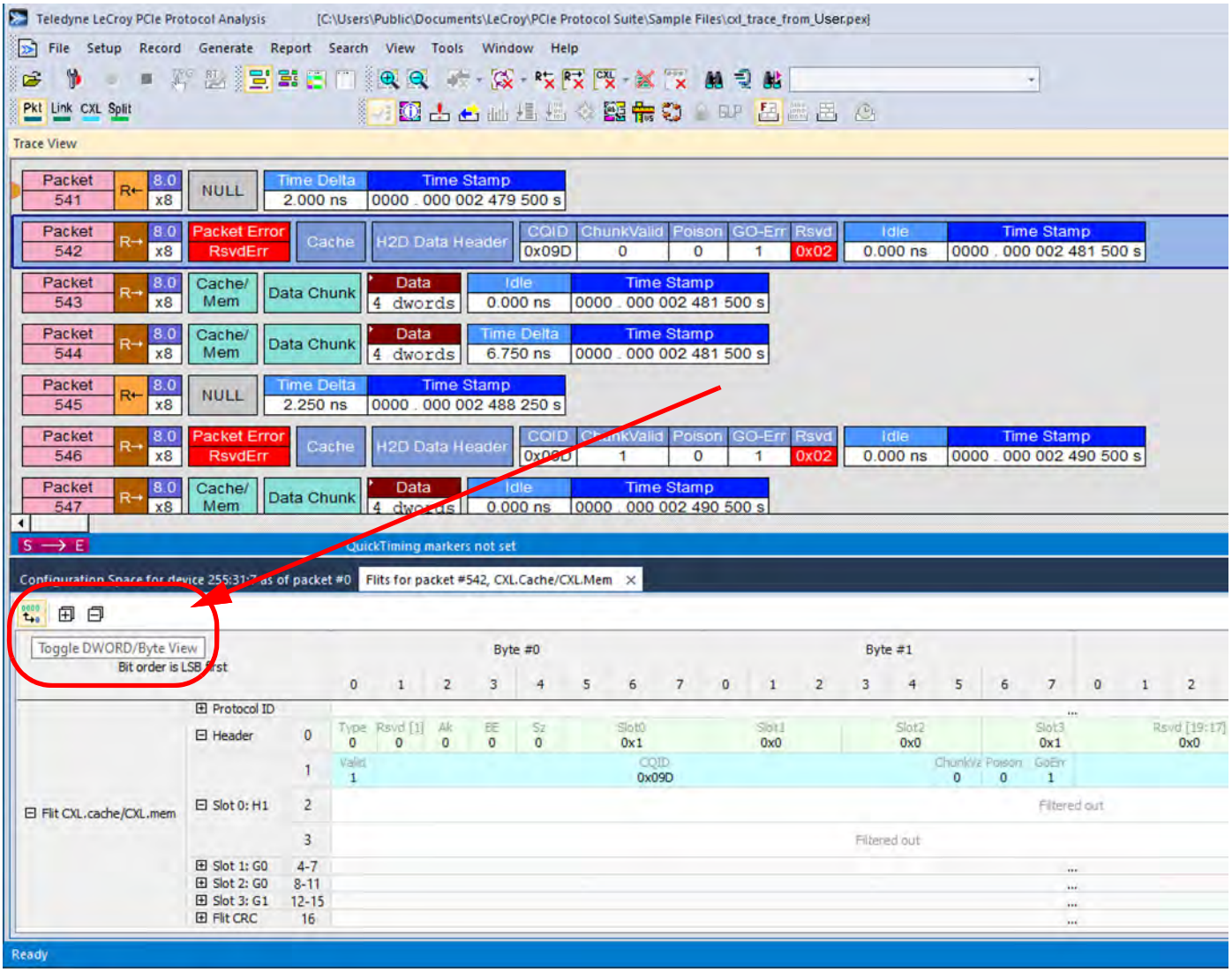


Figure 12.35: Toggle Display from DWORD to Byte View

Tooltips are available in the trace display by scrolling the cursor over a cell in the packet. See Figure 12.36.

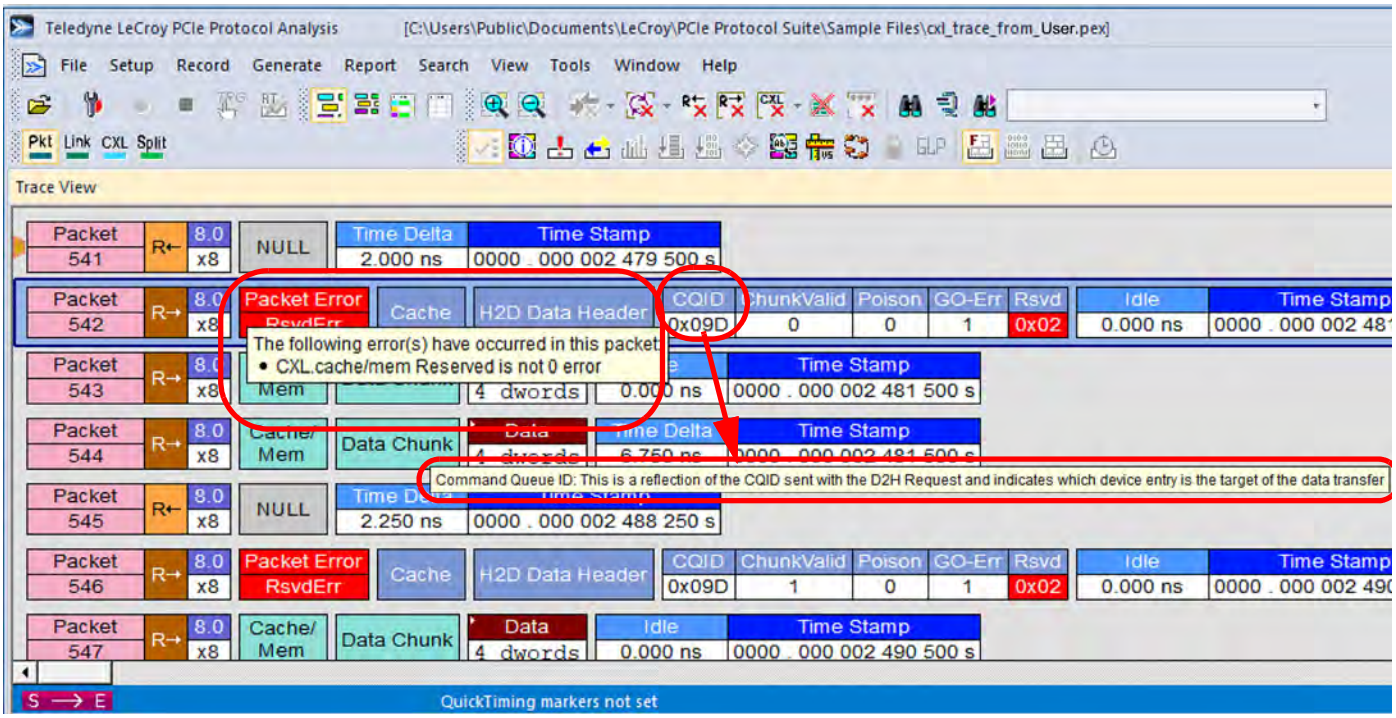


Figure 12.36: Tooltip for CXL Error

12.5 Bus Utilization

Select **Report > Bus Utilization** from the menu or press  to open the Bus Utilization dialog.

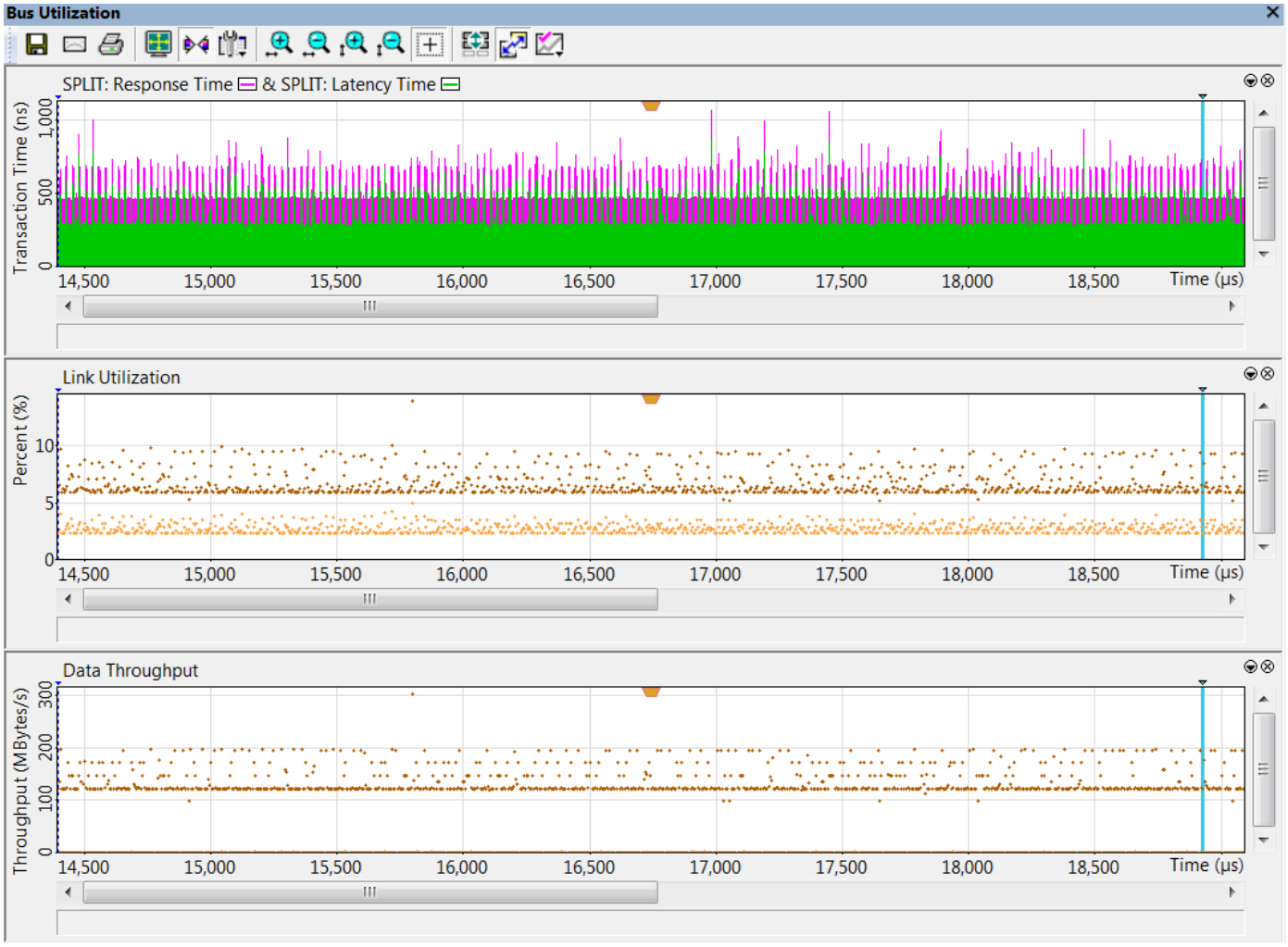


Figure 12.37: Bus Utilization Dialog

The Bus Utilization window displays information on bandwidth use for the transmit and receive channels.

12.5.1 Bus Utilization Pop-up Menu

You can reformat the display by right-clicking a graph and making a selection from the Bus Utilization pop-up menu.

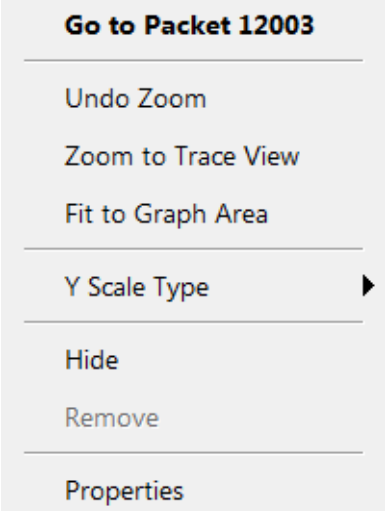


Figure 12.38: Bus Utilization Menu

Go to Packet #: Relocates the CATC Trace to the selected packet number.

Undo Zoom: If you have zoomed in, this command undoes the zoom.

Zoom to Trace View: Zooms in on graph to show traffic currently displayed in the CATC Trace screen.

Fit to Graph Area: Redisplays graph so that the entire CATC Trace fits inside graph area.

Y Scale Type:

- **Linear**: Converts display to linear format
- **Logarithmic**: Converts display to logarithmic format

Hide: Hides the selected graph

Remove: Allows you to add any graph that you created via the **Graph areas**  command.

Properties: Opens a dialog with options for changing the Title, Type, Appearance, Color and Properties of the graphs (see Figure 12.39 on page 769).

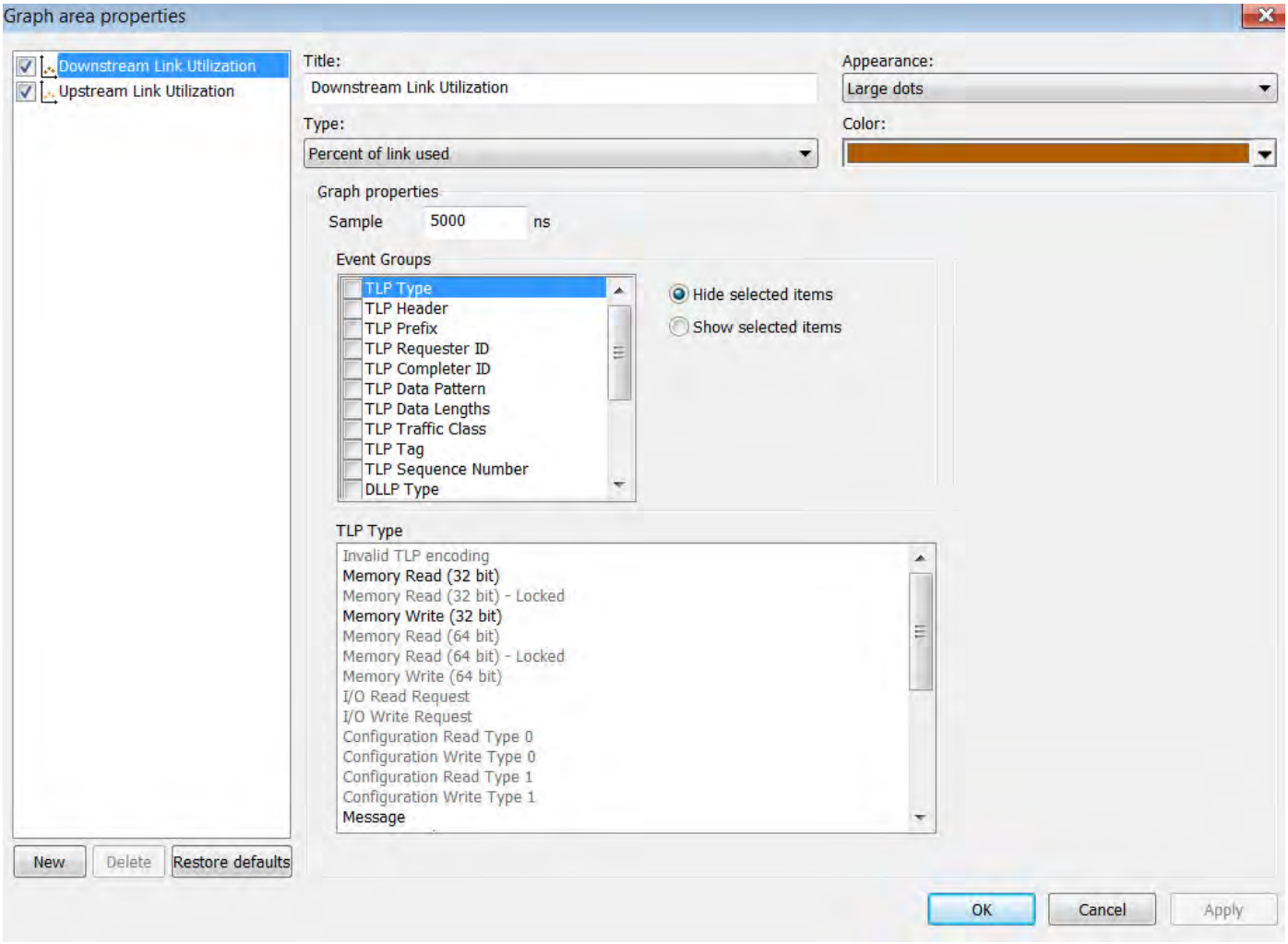


Figure 12.39: Graph Area Properties Dialog

12.5.2 Bus Utilization Buttons

The Bus Utilization window buttons allow you to reformat the display and export data.



Button	Function
	Save. Saves Bus Utilization data to a bitmap file (***.bmp**).

	Email. Opens an email and attaches a bitmap file of the Bus Utilization data.
	Print. Prints the Bus Utilization data.
	Full Screen. Maximizes the Bus Utilization window.
	Synchronize Views.Synchronize the current view with other open views.
	View Settings. Opens a sub-menu with the following choices: • Orient Horizontally • Tile Vertically • Show Markers • Show Plumb Line • Status >> • Bar • Tool tips • None • Grid Lines >> • Both Axes • X Axis • Y Axis • No Grid • Grid on Top • Fonts & Colors
	Horizontal zoom in
	Horizontal zoom out
	Vertical zoom in
	Vertical zoom out
	Click and Drag zoom. Click and drag to zoom in on a part of the graph.

	Select Range. Displays a dialog for selecting a packet range.
	Synchronize Graph Areas. If two or more graphs are displayed, this button synchronizes the graphs to one another. Once synchronized, the positioning slider of one graph moves the other graphs.
	Graph Areas. Provides options for creating and displaying additional graphs of data lengths, packet lengths, and percentage of bus used (see Graph Area Options below).

Graph Area Options

The available graphs are shown in Figure 12.40:

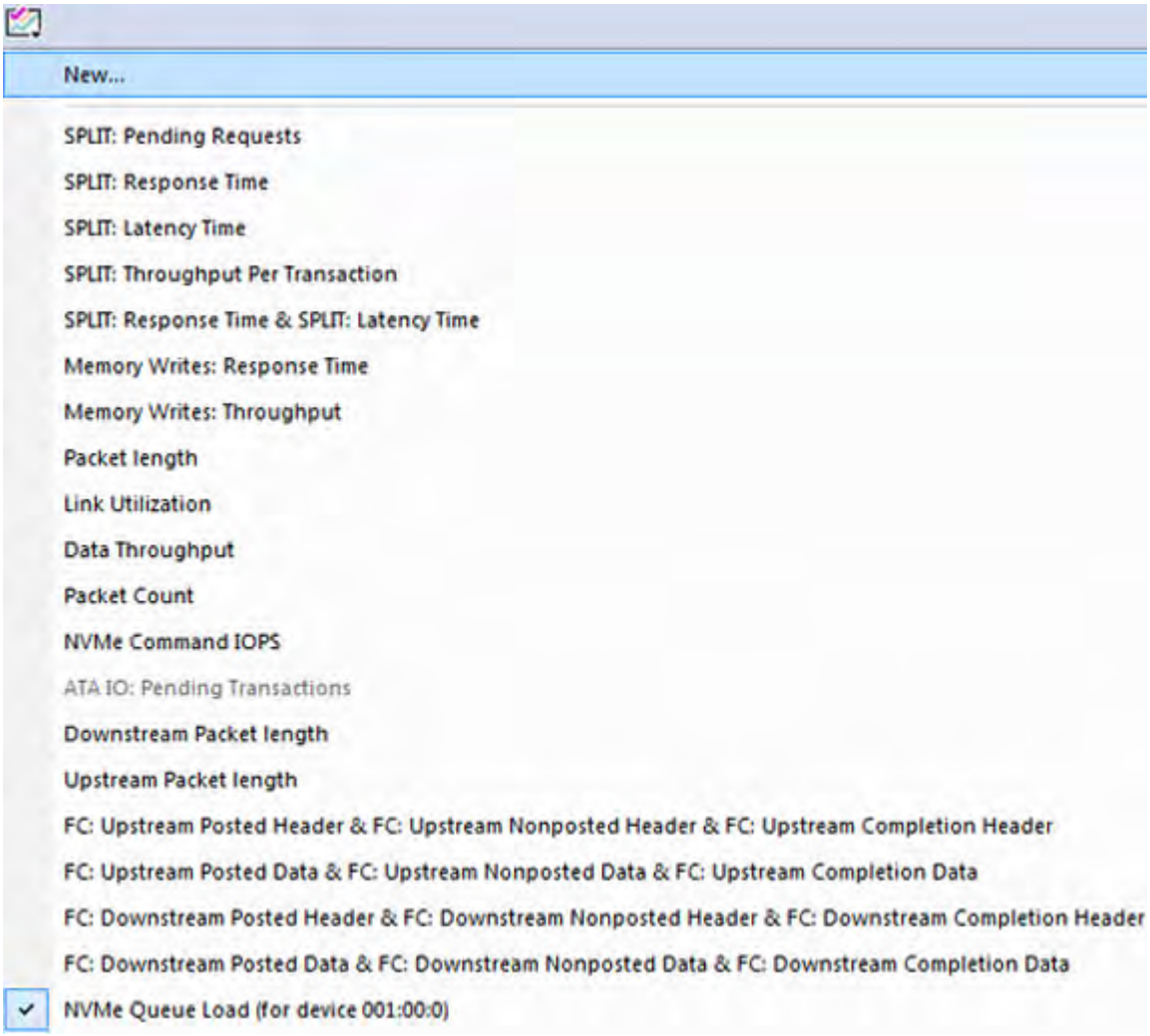


Figure 12.40: Graph Area Options Dialog

- New - Opens Graph Area Properties dialog to specify a new graph
- SPLIT: Pending Requests
- SPLIT: Response Time

- SPLIT: Latency Time
- SPLIT: Throughput Per Transaction
- SPLIT: Response Time & SPLIT: Latency Time
- Memory Writes: Response Time
- Memory Writes: Throughput
- Packet Length
- Link Utilization
- Data Throughput
- Packet Count
- NVMe Command IOPS
- ATA IO: Pending Transactions
- Downstream Packet Length
- Upstream Packet Length
- FC: Upstream Posted Header & FC: Upstream Nonposted Header FC: Upstream Completion Header
- FC: Upstream Posted Data & FC: Upstream Nonposted Data FC: Upstream Completion Data
- FC: Downstream Posted Header & FC: Downstream Nonposted Header FC: Downstream Completion Header
- FC: Downstream Posted Data & FC: Downstream Nonposted Data FC: Downstream Completion Data
- NVMe Queue Load

Example: NVMe Queue Load Graph Feature

This enhancement adds new Bus Utilization graph that indicates how many NVMe queue slots are occupied through the trace. There are separate graphs for each device, present in a trace, each queue is represented by a line. User can select queues to show. See Figure 12.41.

This graph can only be built after the NVMe level is decoded. Trace has to contain doorbells and submission/completion queues. If any of these conditions is not fulfilled, "Graph Areas" popup menu will have "NVMe Queue Load" item disabled. If required transactions are filtered out (for instance, using NVMe Enhanced Mode), user will be additionally prompted in popup menu entry.

Note: If trace with the graph is re-opened with persistent decoding disabled, empty graph area will be shown. After NVMe level decoding graph area gets deselected. Showing graph right after required levels are decoded should be considered as enhancement.



Figure 12.41: Bus Utilization: NVMe Queue Load

Graph Legend

Graph legend can be viewed by moving mouse pointer over graph title. See Figure 12.42 on page 774.

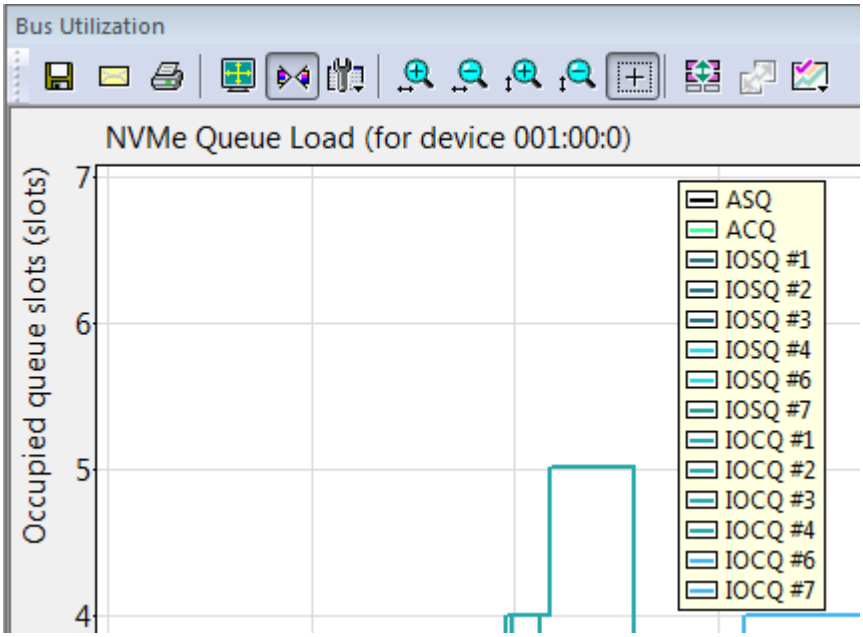


Figure 12.42: Bus Utilization: Graph Legend Details

Graph Properties

Queues to show can be selected in Graph Properties (as well as line colors). See Figure 12.43.

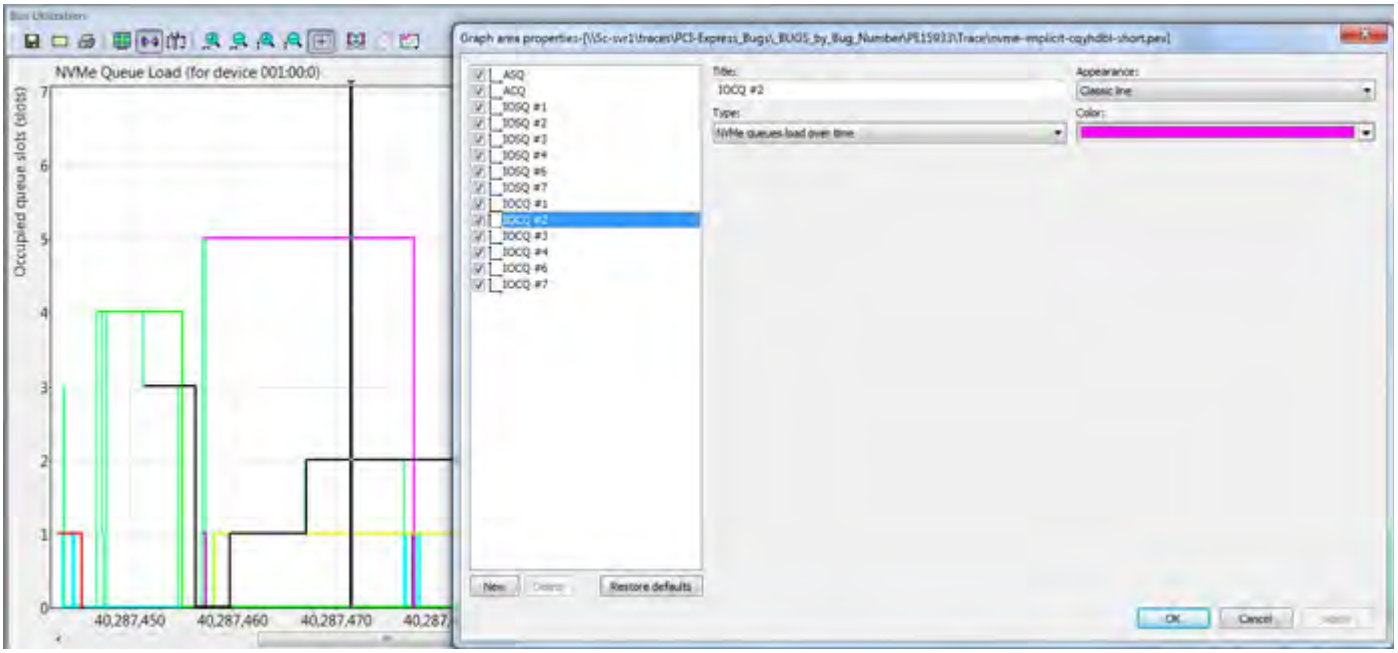


Figure 12.43: Bus Utilization: NVMe Queues => Selected in Graph Properties

12.6 Link Tracker

Open the Link Tracker window by selecting the Link Tracker Icon (to the right of the Bus Utilization Icon in the main toolbar)  .

The Link Tracker window displays a detailed chronological view of events. Events are shown on a channel-by-channel basis in columns within the window.

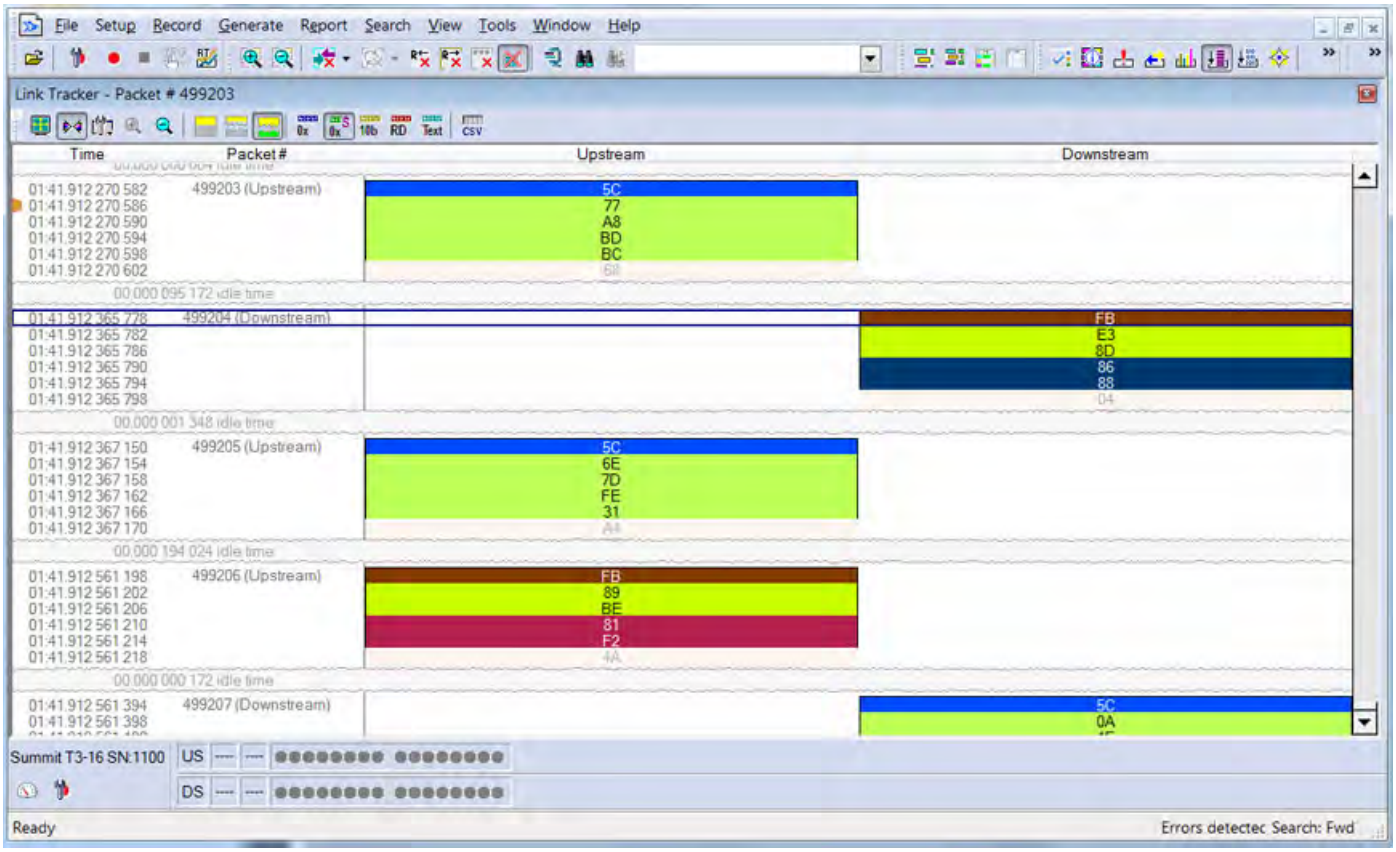


Figure 12.44: Link Tracker Window

Each time slot in the vertical axis represents the minimum time that a DWORD requires to traverse the bus.

Toolbar: Presents buttons for changing the format of the Link Tracker window.

Main Display Area: Displays traffic chronologically as it occurred in the recording. The window divides into columns: the first column shows time and traffic is shown on a channel-by-channel basis in the columns on the right.

12.6.1 Using the Link Tracker Window

The Link Tracker window can be reformatted in several ways.

12.6.2 Zooming In and Out

Zooming out can give you a quick, high-level view of a CATC Trace. A fully zoomed out CATC Trace only shows columns and colored lines. Using the colors, you can see what types of traffic run through the CATC Trace.

Further information can be obtained on any point of interest in the CATC Trace by positioning your mouse pointer over it. Tool tips provide detailed description of events.

When fully zoomed out, the smallest graphical unit is the DWORD, represented by a single line. Zooming out makes the CATC Trace appear smaller and increases the time scale in the first column.

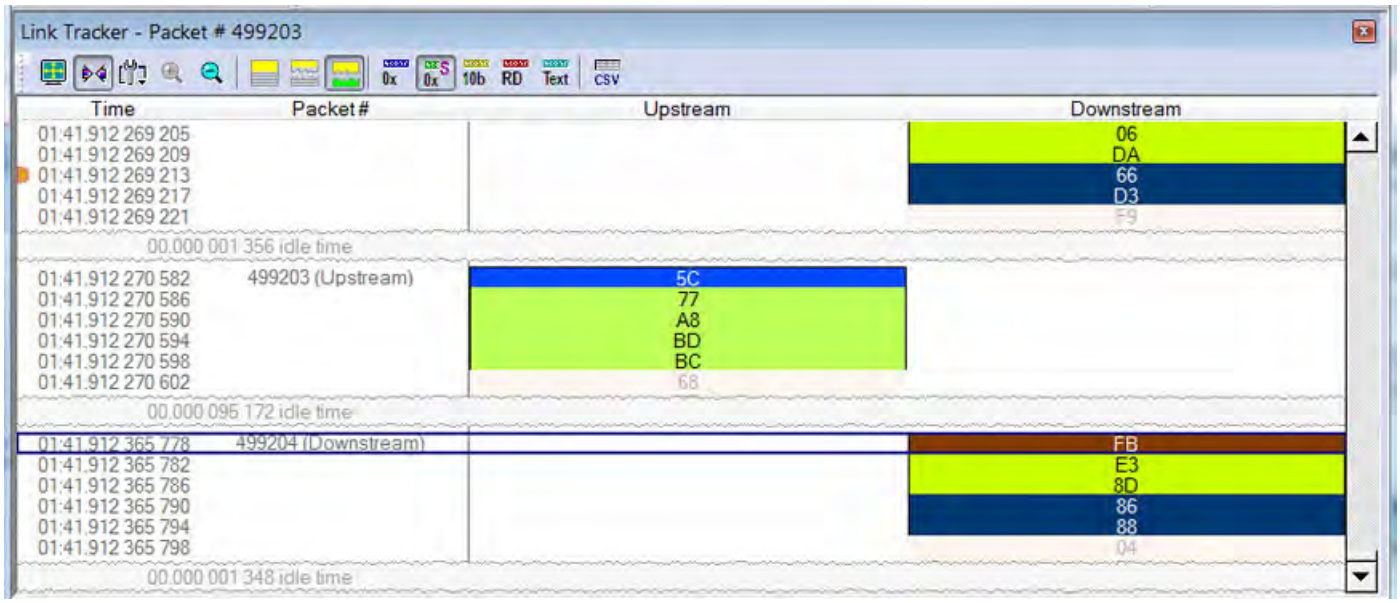


Figure 12.45: Link Tracker: Zoomed Out

12.6.3 Collapsing Idle Time, Enabling Tool tips, and Resetting Column Widths

Click the **View Options** button  to open a menu with options for formatting the display. Three options are presented:

Collapsible Idle Time: Opens a dialog box for setting the Idle time value. Setting a value tells the Analyzer when to collapse Idle times and display them as grayed out strips within the Bus View window.

Tooltip Display: Opens a menu with options for adding content to Tooltips. Tooltips display when you position the mouse pointer over an item in the Bus View window. The options are:

- Tooltips Display Values
- Tooltips Display Scrambled Values
- Tooltips Display 10-bit Codes
- Tooltips Display Symbols

Time Format: Seconds or Clock

Reset Column Widths: This option resets column widths to their defaults and enables columns to resize themselves automatically any time the application window is resized. Normally, columns automatically resize themselves if the application window is made larger or smaller. However, if you manually resize any columns in the Bus View window, column widths become static. Thereafter, if you resize the application window, the Bus View columns do not adjust automatically. Reset Column Widths re-enables the automatic resizing capability.

Reset Columns Order: Return to default column sequence.

12.6.4 Docking and Undocking the Window

You can undock the Link Tracker window by double-clicking the blue title bar along the left side of the window. Once undocked, the window can be dragged anywhere in the application. To re-dock double-click again on the title bar.

12.6.5 Setting Markers

Markers can be set on any event within the Link Tracker window.

To set a marker, right-click an event, then select **Set Marker** from the pop-up menu.

Once marked, you can navigate to events with the **Go to Marker** command in the Search menu.

Markers set in the Link Tracker window display the packet number and DWORD number. In contrast, markers set in the CATC Trace window just show the packet number.

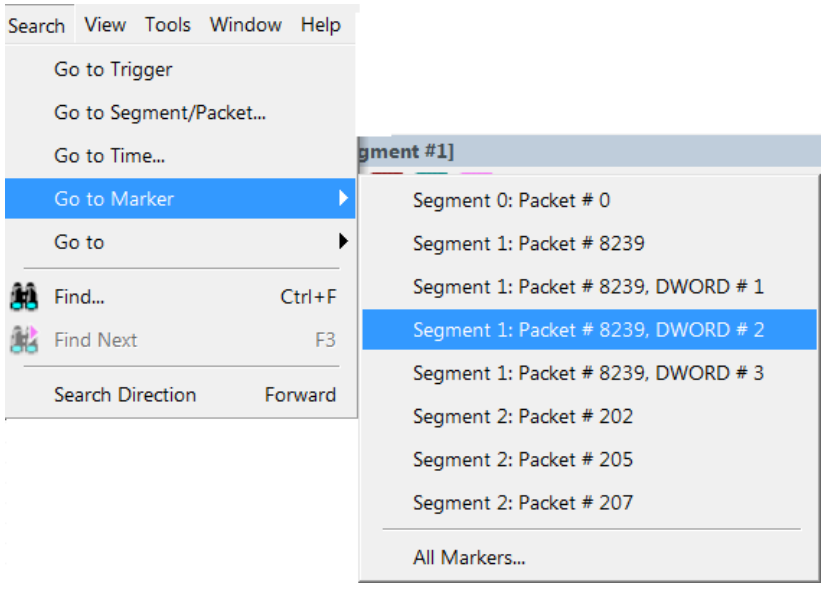


Figure 12.46: Selecting the Go to Marker Option

12.6.6 Calculating Time between DWORDs

You can calculate time between DWORDs by clicking an event and then positioning your mouse pointer over a second event and reading the ensuing Tool tip.

Click the **time value** for the first event. Scroll down through the CATC Trace to the second event and position the mouse pointer above its time value. A Tool tip appears showing the time interval between the first and second events.

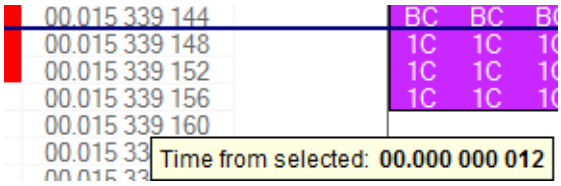


Figure 12.47: Viewing Time Values

12.6.7 Hiding Traffic

You can hide Idles and other data from the Link Tracker window by clicking the **Hide** buttons on the toolbar.

12.6.8 Link Tracker Buttons

The Link Tracker window has a row of buttons for changing the format of the displayed data and for exporting data: The buttons have the following functions:

	Full Screen. Expands the Link Tracker window to fill the entire screen.
	Synchronize Trace View. Synchronizes the Trace View and Link Tracker windows so that a move in one window repositions the other. Because of the differences in scale and logic between the Link Tracker and Trace view window, scrolling produces different effects depending on which window is being scrolled. Scrolling in the CATC Trace window causes the Link Tracker window to rapidly jump from event to event. Long periods of idle time are thus skipped. Scrolling in the Link Tracker window, in contrast, produces modest movements within the CATC Trace window. Scrolling in the Link Tracker window causes the CATC Trace window to pause until the beginning of a packet is displayed. At that point, the CATC Trace window repositions itself. While scrolling long Idle periods or through the contents of a packet, the CATC Trace window does not move.

	View Options. Opens a menu with three options: • **Collapsible Idle Time** (Collapse Idle Bigger Than **n** nanoseconds. **Note:** Does not affect Collapse Idle Plus.) • **Tooltip Display** (Values, Scrambled Values, 10-bit Codes, Symbols) • **Time Format** (Seconds, Clock) • **Reset Columns Widths** (return to default widths) • **Reset Columns Order** (return to default column sequence) See "Using the Link Tracker Window" on page 775 for further details.
	Zoom In
	Zoom Out
	Continuous Time Scale. No collapsing.
	Collapse Idle. Do not show some periods of Link being idle.
	Collapse Idle Plus. Do not show periods of Link being idle.
	Show Descrambled Bytes
	Show Scrambled Bytes
	Show 10b Codes
	Show Symbols
	Show Text
	Show Binary values
	Export to CSV file

Exporting to CSV File

To export trace file information to a CSV file, select the variables you want in the file and select the CSV Icon. A window with your variables will pop up that also shows you the file name and path. See Figure 12.48.

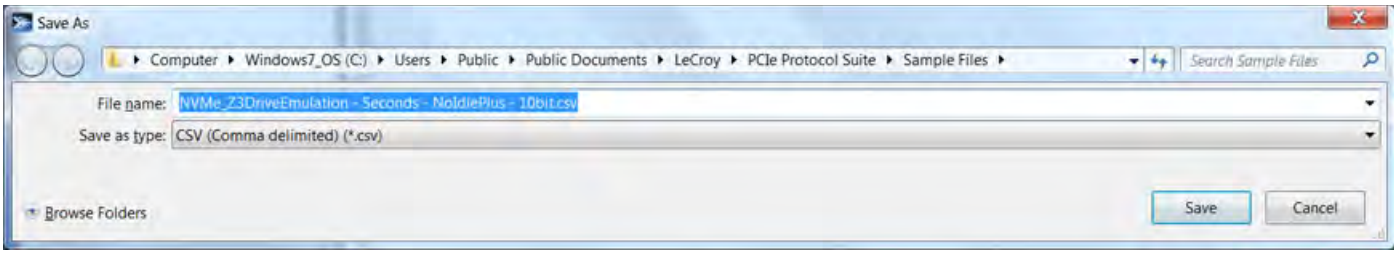


Figure 12.48: Link Tracker: CSV File to be Saved and Location

Select Save and the tool will start. See Figure 12.49.

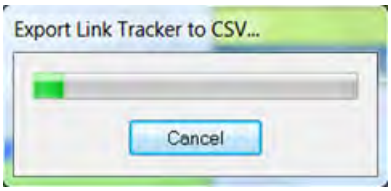


Figure 12.49: Tool Exporting Link Tracker Data to CSV File

The generated CSV file can be viewed in Excel.

12.7 Data Flow Window

The Data Flow window shows marker, packet, direction, type, length, address, payload, handshake, and timestamp information.

To obtain the Data Flow window, select **Report > Data Flow**

or click the  Data Flow toolbar icon.

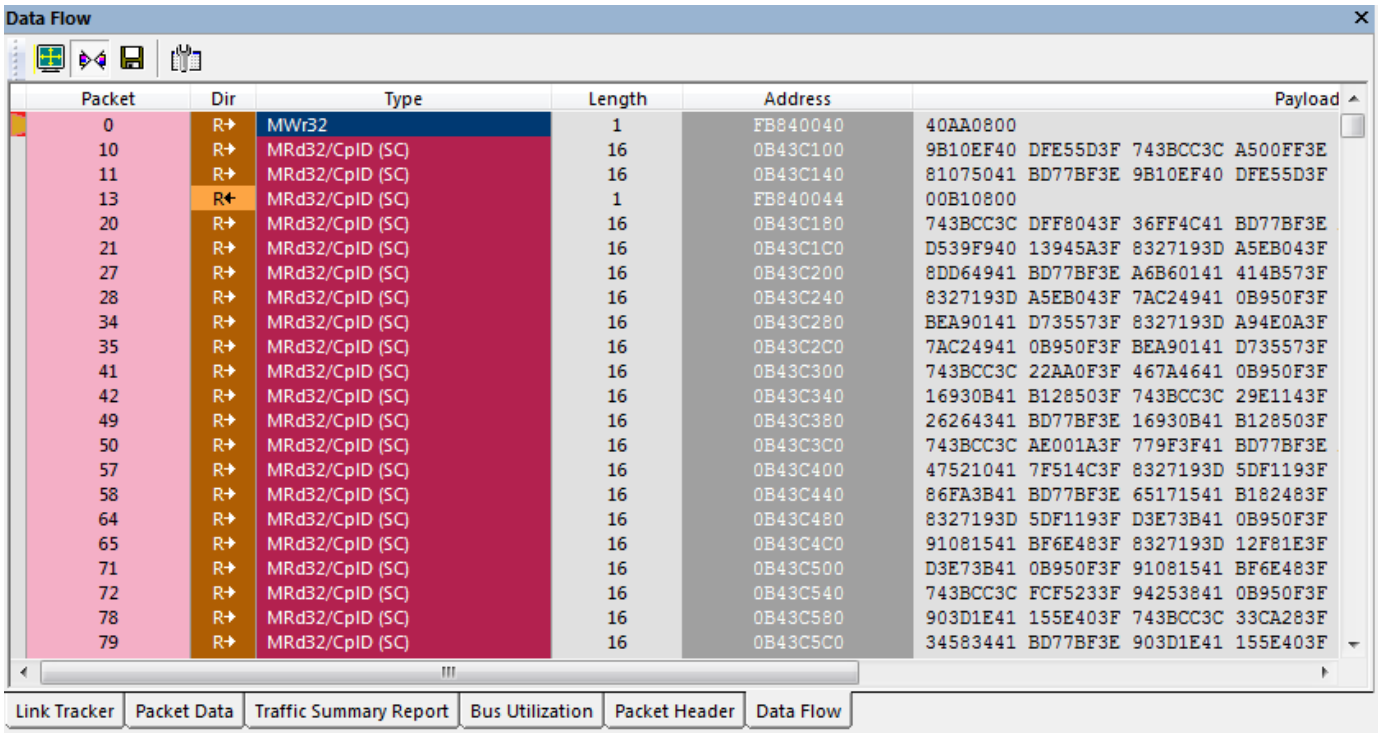
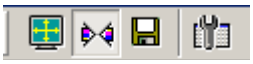


Figure 12.50: Data Flow Window



The toolbar allows you to (see Figure 12.51 on page 782):

- Expand the window to full screen or Collapse to a smaller window.
- Synchronize.
- Save.
- Select Data Flow columns to display and their widths:
  - Marker
  - Packet
  - Direction
  - Type
  - Length
  - Address
  - Payload
  - Handshake
  - Time Stamp

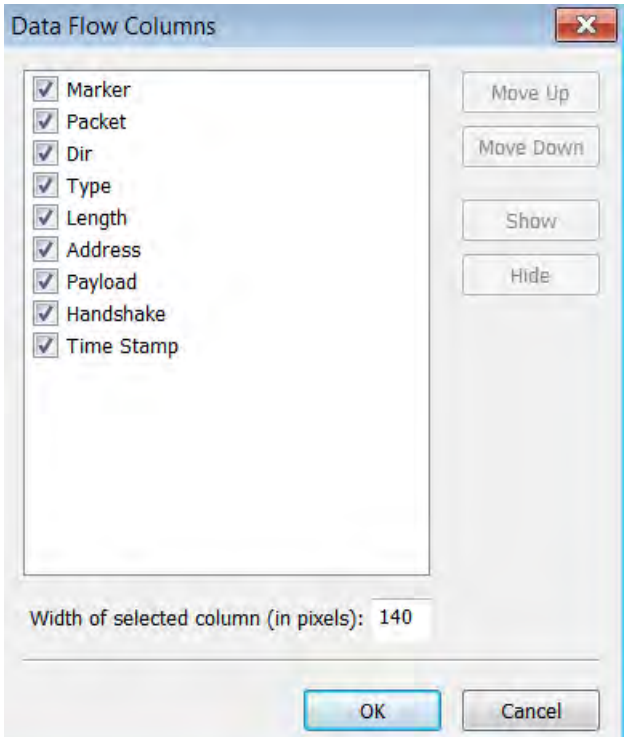


Figure 12.51: Data Flow Columns Dialog

12.8 Flow Control Tracking

The Flow Control View mode highlights portions of the packets that affect flow control and displays flow control values. Flow control values shown at the beginning of Link Transaction display the credit values that were available prior to TLP transmission. Flow control values shown at the end of the Link Transaction display the credit values that were available after TLP was transmitted. Hover the mouse over the field to display tool-tips. Refer to the following screen capture.

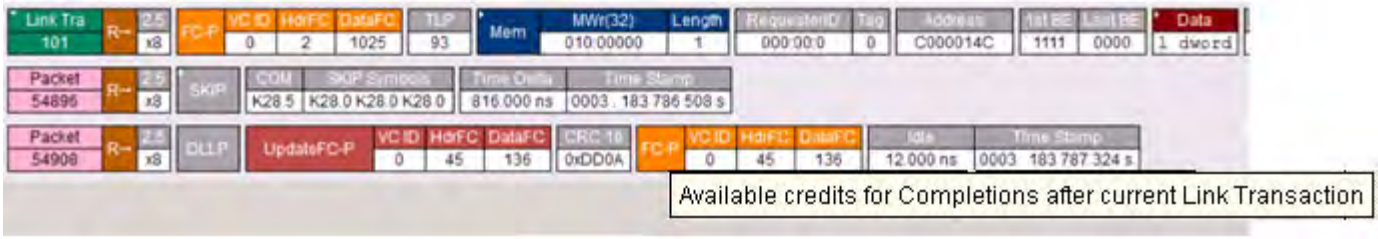


Figure 12.52: Flow Control Display

If the trace includes Flow Control initialization, PCIe Protocol Analysis detects the amount of available credits based on the values advertised in InitFC packets. If the InitFC packets are not in the trace, the amount of available credits can be set using the FC Credit Setup dialog. Select **View > FC Credits Setup...** displays the FC Credit Setup dialog (see the following screen capture).

For each virtual channel that is present in the trace you need to specify the amount of available credits before the beginning of the trace. You can also specify the values of credit fields for UpdateFC packets before the beginning of the trace. If the values of the UpdateFC credit fields are different than the values in the first UpdateFC packet, Flow Control tracking view will show that the first UpdateFC packet is releasing appropriate amount of credits. By default, PCIe Protocol Analysis sets these values to match the first UpdateFC packets in the trace.

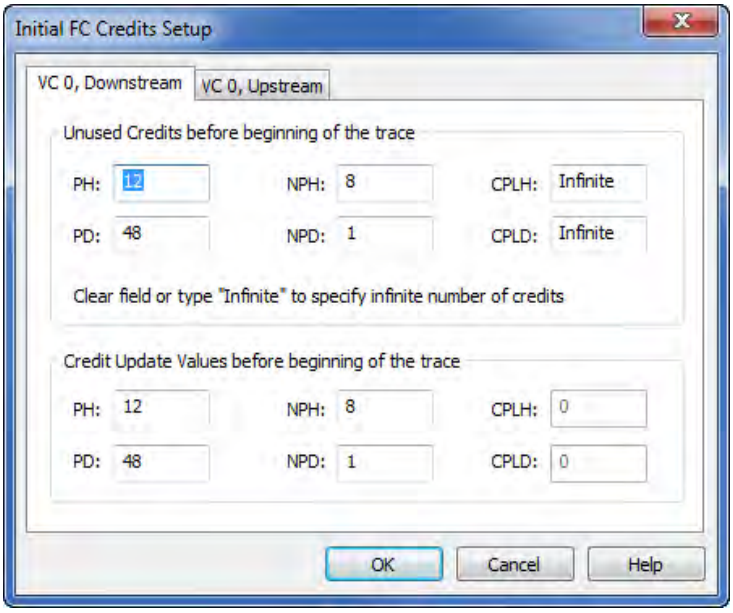


Figure 12.53: Flow Control Setup Dialog

12.9 Using the CATC Trace Navigator

The CATC Trace Navigator is a tool for navigating within the CATC Trace. It allows you to view the location of errors and triggers in a CATC Trace and to narrow the range of traffic on display. It also allows you to quickly jump to any point in the CATC Trace.

12.9.1 Displaying the Navigator

Click  in the toolbar to display the Navigator. The Navigator appears on the right side of the Main window. It has a two-button toolbar and a vertical slider bar. It also has colored panes for navigating the CATC Trace in different ways. You set which panes are displayed through Navigator pop-up menus (see Figure 12.54 on page 784).



Figure 12.54: Navigator Dialog

12.9.2 Navigator Toolbar

The Navigator toolbar lets you quickly set Navigator features. The toolbar has two buttons.





Navigator Ranges: This button brings up a pop-up menu that lets you reset the Navigator range. The range determines what packets are viewable in the CATC Trace display.



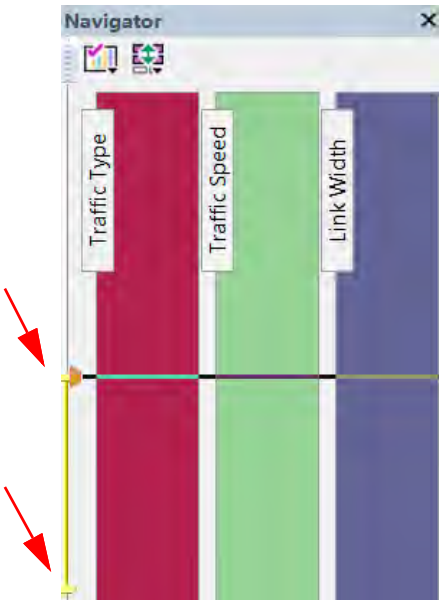
Navigator Panes: This button has two purposes: To select which Navigator panes appear and to bring up the Navigator legend. The legend determines how information is shown in the panes.

12.9.3 Navigator Ranges

You set the viewing range by dragging the **yellow range delimiters** along the slider. To set the lowest packet viewable, drag the **top delimiter up**. As you do so, a tool tip appears to indicate the current range. Stop dragging when you reach the desired lowest packet.

To set the highest packet viewable, drag the **bottom delimiter down**. Stop when the tool tip indicates you are at the desired highest packet.

.



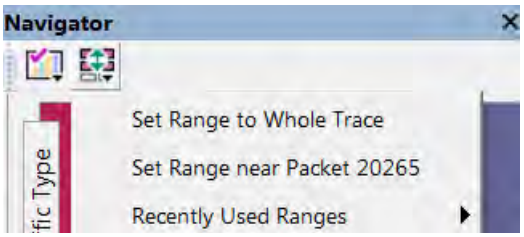
12.9.4 To Determine Current Position

In addition to the two range delimiters, the slider has a **blue current-position** indicator (see above). The current-position indicator shows where you are in the CATC Trace display with respect to the possible viewing range.

For example, suppose you set viewing range to packet 0 through packet 500 (the top range delimiter is at packet 0, and the bottom range delimiter is at packet 500). If you then move the current-position indicator on the slider to midway between the top and bottom delimiters, then packet 250 appears in the middle of the CATC Trace display.

12.9.5 To Reset Navigator Range

You can reset the Navigator range using the toolbar **Navigator Range** button. Press the button to bring up the Navigator Range drop-down menu.



The menu has the following options:

- **Set Range to Whole Trace**: Allows you to reset the range to include the entire CATC Trace file contents. The top range delimiter is placed at the lowest packet number in the CATC Trace. The bottom range delimiter is placed at the highest packet number in the CATC Trace.
- **Set Range Near Packet xxx**: Allows you to collapse the range so that only the packets immediately above and below the xxx packet are displayed. The xxx packet is whatever packet is currently at the top in the CATC Trace display.
- **Recently Used Ranges**: Allows you to reset the range to any of a number of recently used (previously set) ranges.

12.9.6 Navigator Panes

You can display any combination of CATC Trace Navigator panes.



From left to right, the panes are: Pre/Post Trigger, Errors, Traffic Type, Traffic Speed, and Link Width. Each pane represents the entire CATC Trace with respect to different types of information. The top of each pane represents the start of the CATC Trace file, and the bottom represents the end of the CATC Trace file.

- **Pre/Post Trigger:** To view the trigger event in the CATC Trace and the relative size of pre-trigger and post-trigger portions of the CATC Trace. The two portions are set apart as different colors. The trigger event occurs at the point the two colors meet.
- **Errors:** To view any errors in the CATC Trace. A thin red line represents each error in the pane.

- **Traffic Type:** To view the types of packets that occur in the CATC Trace. A different color represents each packet type in the pane. The relative size of colored portions in the pane corresponds to the amounts of the various packet types in the CATC Trace. As described below, you can use the Navigator legend to change the types of packets that take precedence in the display.
- **Traffic Speed:** To view the speed that occurs in the CATC Trace.
- **Link Width:** To view the link width that occurs in the CATC Trace.

12.9.7 To Show/Hide Nav55igator Panes

You can show/hide any of the panes using pop-up menus accessible through left-click the **Navigator Panes** button or by right-click anywhere in any CATC Trace Navigator pane.

12.9.8 Navigator Slider

The Navigator slider appears at the left of Navigator panes. The slider has **yellow upper and lower range delimiters** and a **blue current-position** indicator.

The Navigator slider lets you to set the range of packets viewable in the CATC Trace display. In other words, it sets scrolling range of the display. You can scroll the display up to the lowest packet number in the viewing range. You can scroll the display down to the highest packet number in the viewing range.

12.9.9 CATC Trace Navigator Legend

The Navigator legend lets you control the display of content in Navigator panes.

You bring up the legend through the Navigator Pane's drop-down menu. Press the toolbar **Navigator Panes** button to access the menu. Select the **Legend** option to bring up the Navigator Legend dialog (see Figure 12.54 on page 784).

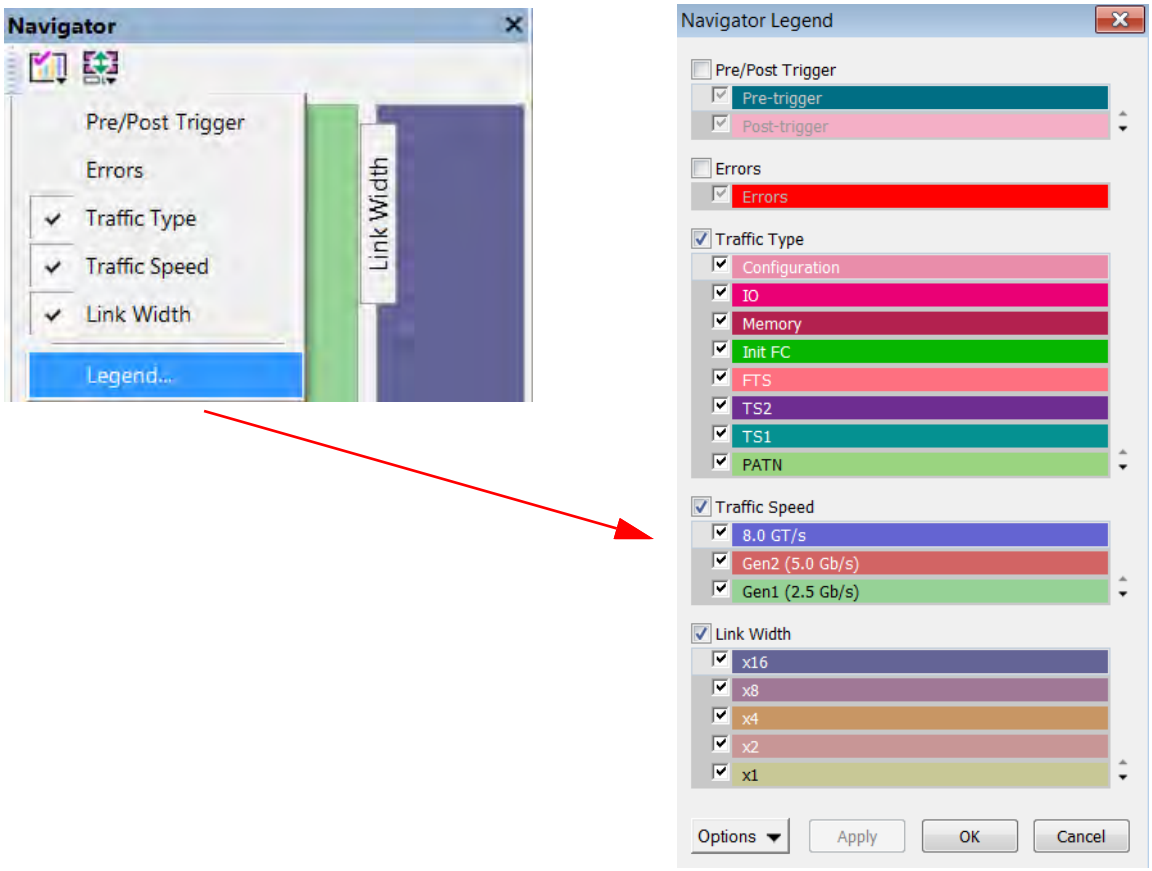


Figure 12.55: Navigator Pane and Navigator Legend Dialog

The Navigator Legend dialog has areas corresponding to each of the panes. Each area has check boxes that allow you to hide/display information in the pane. You can set the priority of information displayed in the panes using the up and down triangles on the right.

12.9.10 Using the Legend to Show/Hide Navigator Panes

To use the legend to show/hide an entire pane, use the **checkbox** next to the name of each pane in the legend.

In the case of the Pre/Post Trigger and Errors areas, the action of show/hide in the legend is identical to that provided by CATC Trace Navigator pop-up menus.

In the case of the Traffic Types pane, there is no equivalent show/hide available through the pop-up menus.

12.9.11 Using the Legend to Set the Priority of Information Display

You can use the legend to set the priority of information displayed in the Pre/Post Trigger Traffic Type panes. This is a two-step process.

1. For a particular item in a pane, click the **column next to the checkbox** for the item. That labels the item as currently active.

2. Next, use the **up-down** at the lower-right of the area to move the item higher or lower in priority.

In the case of the Traffic Type pane, priority determines display priority of each packet type. For portions of the CATC Trace that are dominated by a particular packet type, this setting no effect: only the color corresponding to that packet type is displayed in that portion of the pane. Suppose, however, that part of the CATC Trace includes equal or near equal numbers of several types of packets. In that case, you can use the legend to select which among those types is represented in that portion of the Traffic Types pane. This allows you to view only packets of interest in crowded portions of the CATC Trace display.

12.10 Detail View

Click  to show the Detail View of the selected packet.

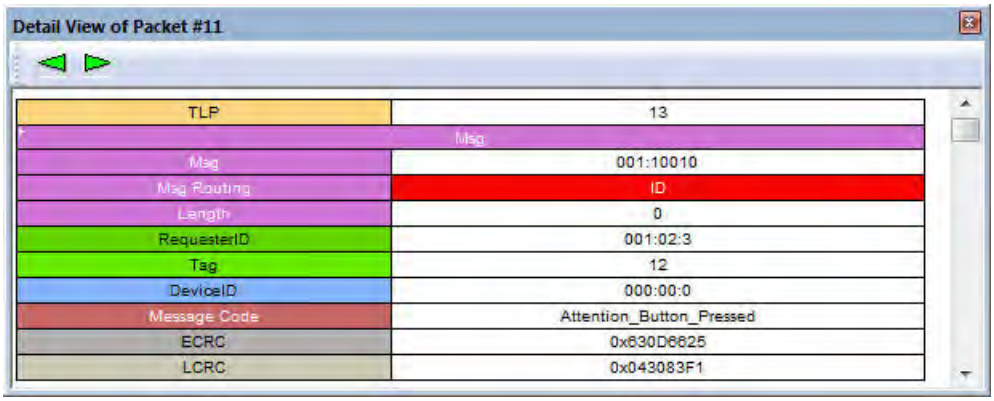


Figure 12.56: Detail View

12.11 LTSSM Flow Graph

The LTSSM Flow Graph shows link state transitions that the link goes through, as recorded in the CATC Trace file.

To obtain the LTSSM Flow Graph (see Figure 12.57 on page 791), select **Report > LTSSM Flow Graph.**

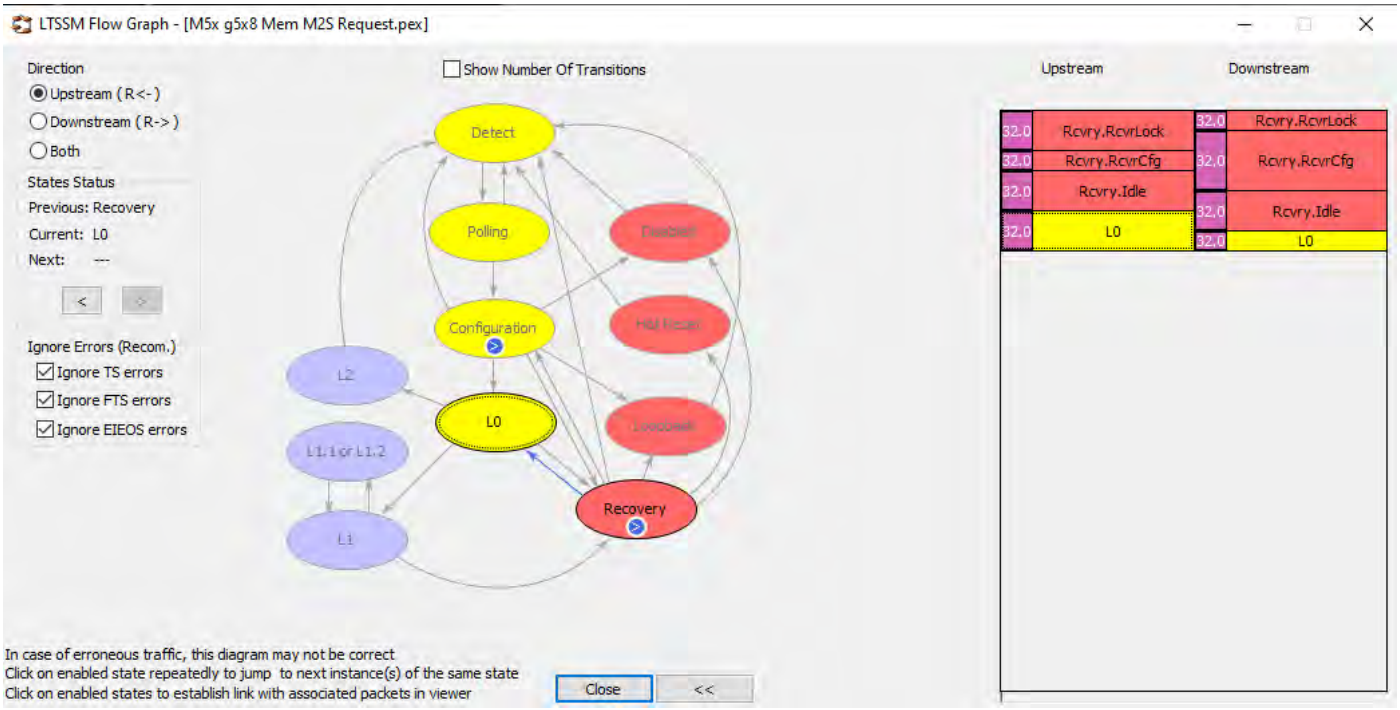


Figure 12.57: LTSSM Flow Graph Dialog

You can enable or disable ignoring of TS/FTS/EIEOS packets with errors so they will not affect the diagram if enabled.

You can display the following directions:

- Upstream
- Downstream
- Both

You can **Show Number of Transitions**.

12.11.1 LTSSM Dynamic Equalization

You can review the PreCursor, Cursor and PostCursor values that the analyzer has used during the dynamic equalization phase of the LTSSM process by selecting the LTSSM icon on the toolbar and checking the following steps: See Figure 12.58.

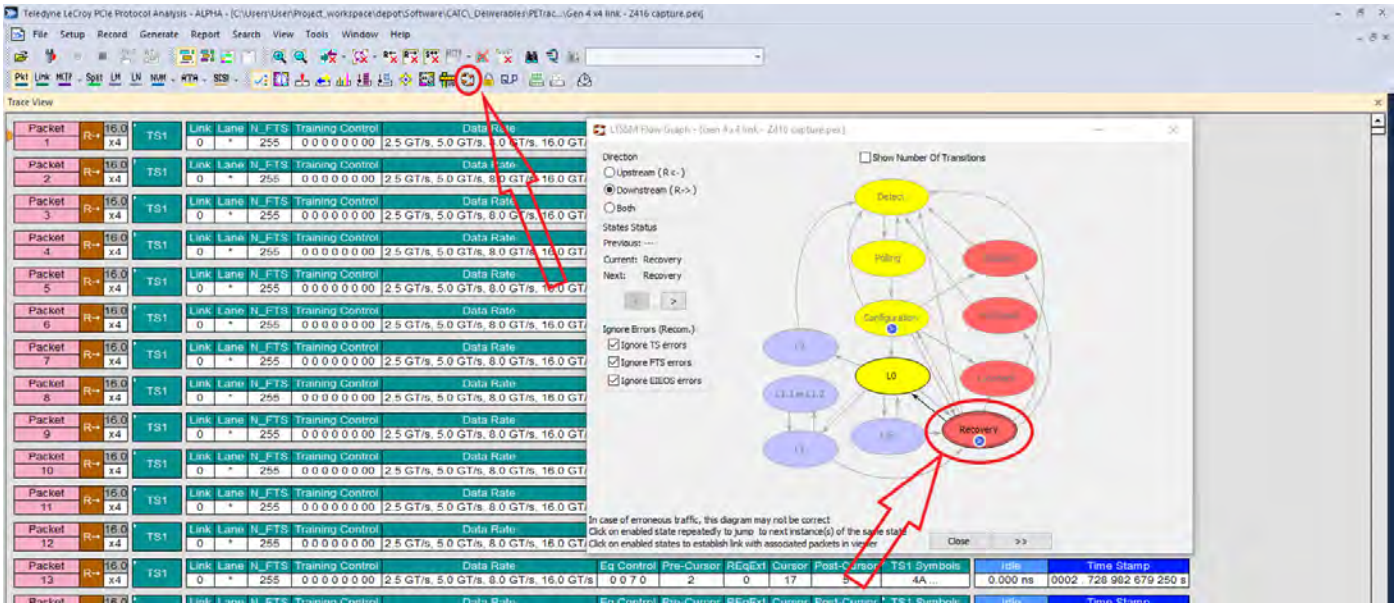


Figure 12.58: Recovery Phase of LTSSM

Click on the arrow in the blue circle in the Recovery state to see more detail. See Figure 12.59 on page 793.

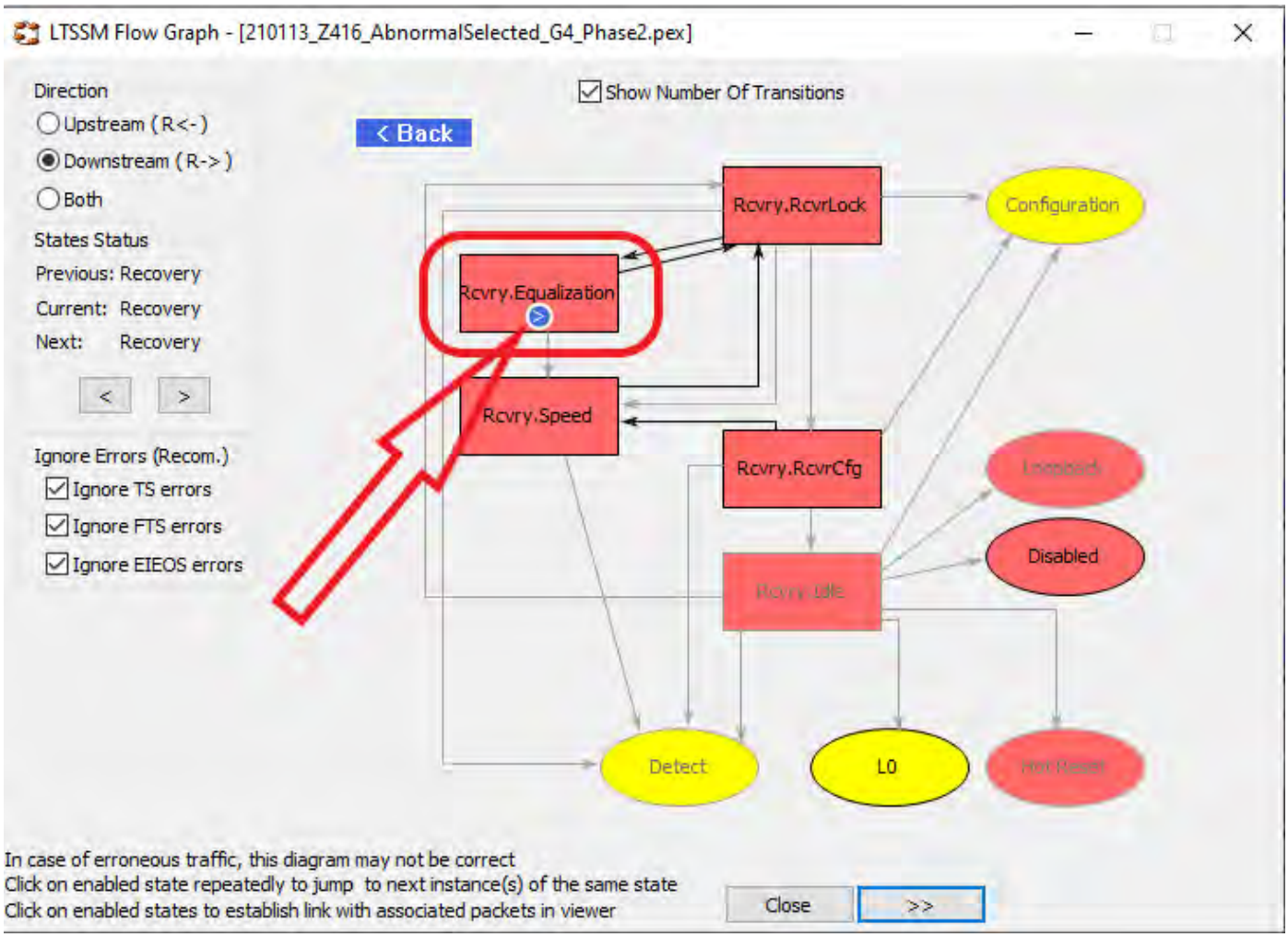


Figure 12.59: Recovery Equalization State

Click on the blue circle with the white arrow in the Recovery.Equalization state to review the PreCursor, Cursor and PostCursor values. See Figure 12.60 on page 794.

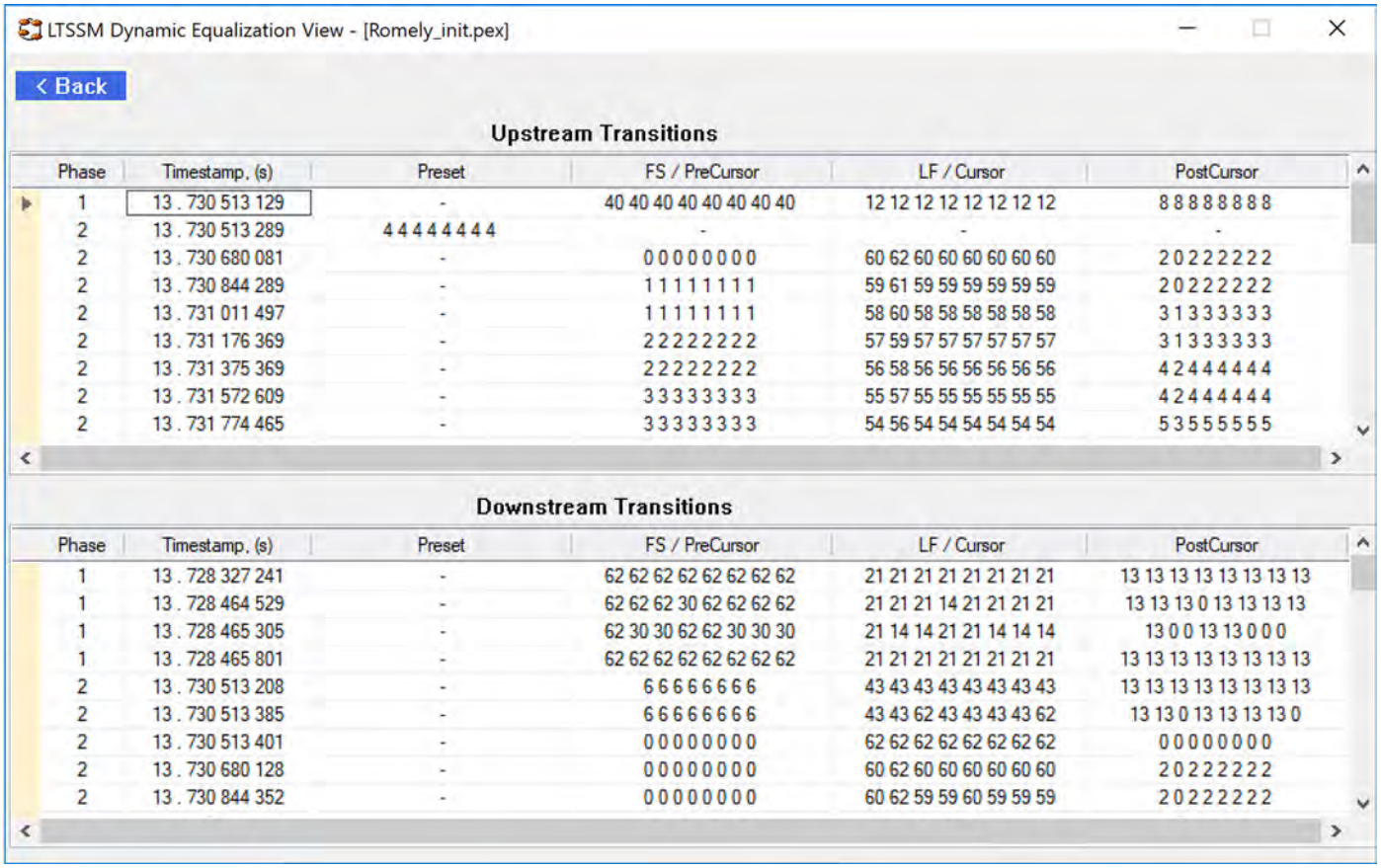


Figure 12.60: LTSSM Dynamic Equalization: PreCursor, Cursor and PostCursor Values

12.12 TCG Security View

The PCIe Protocol Software can decode and display TCG fields. See Figure 12.61.

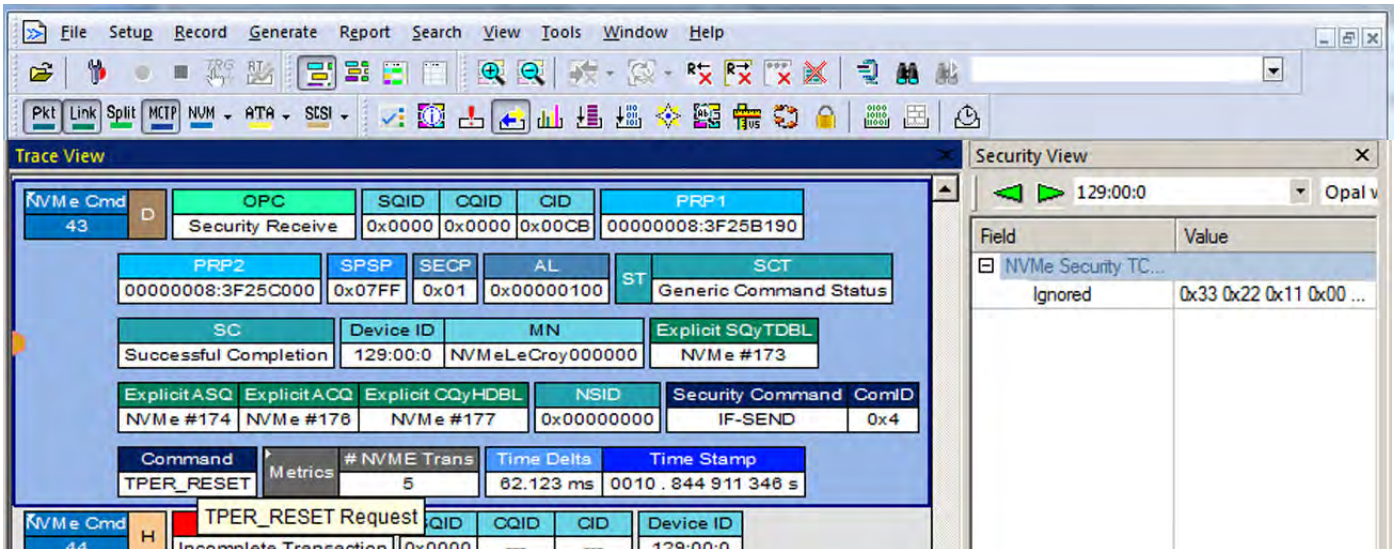


Figure 12.61: NVMe Trace: TCG Security Fields Decoded

A more detailed view of the security field is shown in Figure 12.62 on page 796.

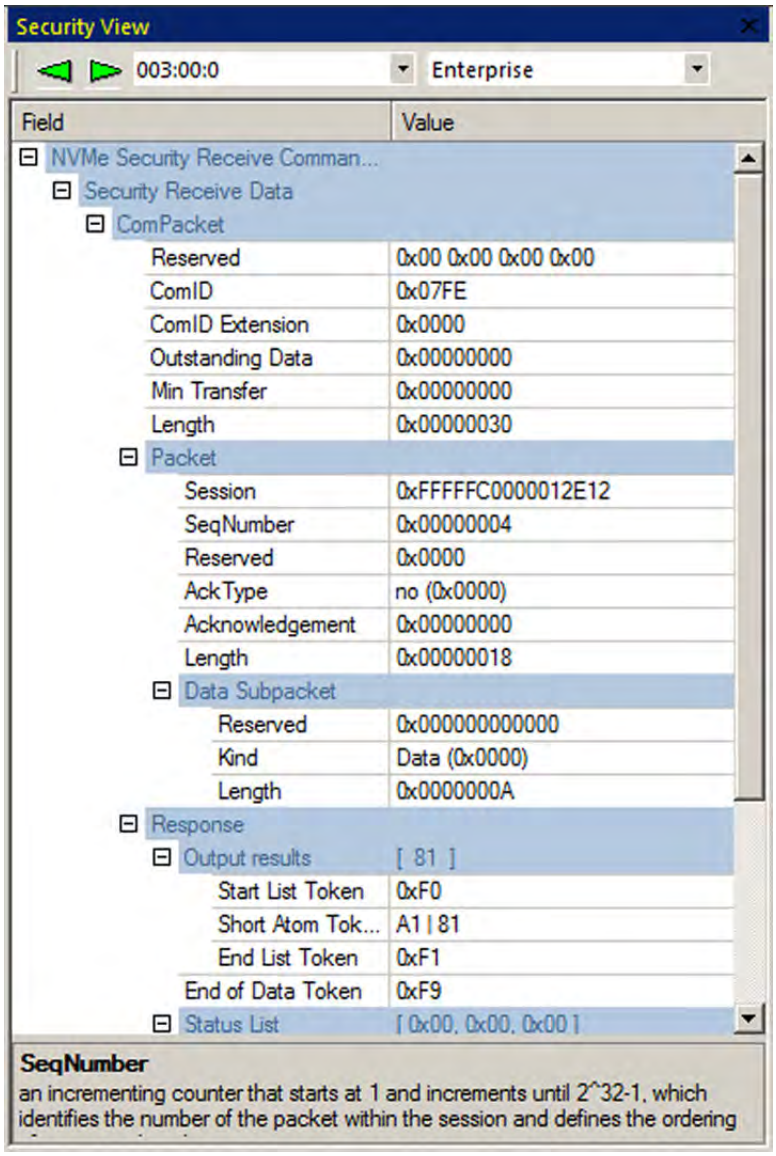


Figure 12.62: NVMe Trace: TCG Security Fields Decoded in Detail

12.13 Get Log Page View

Selecting the Get Log Page View will display the Log File Page View window. See Figure 12.63.

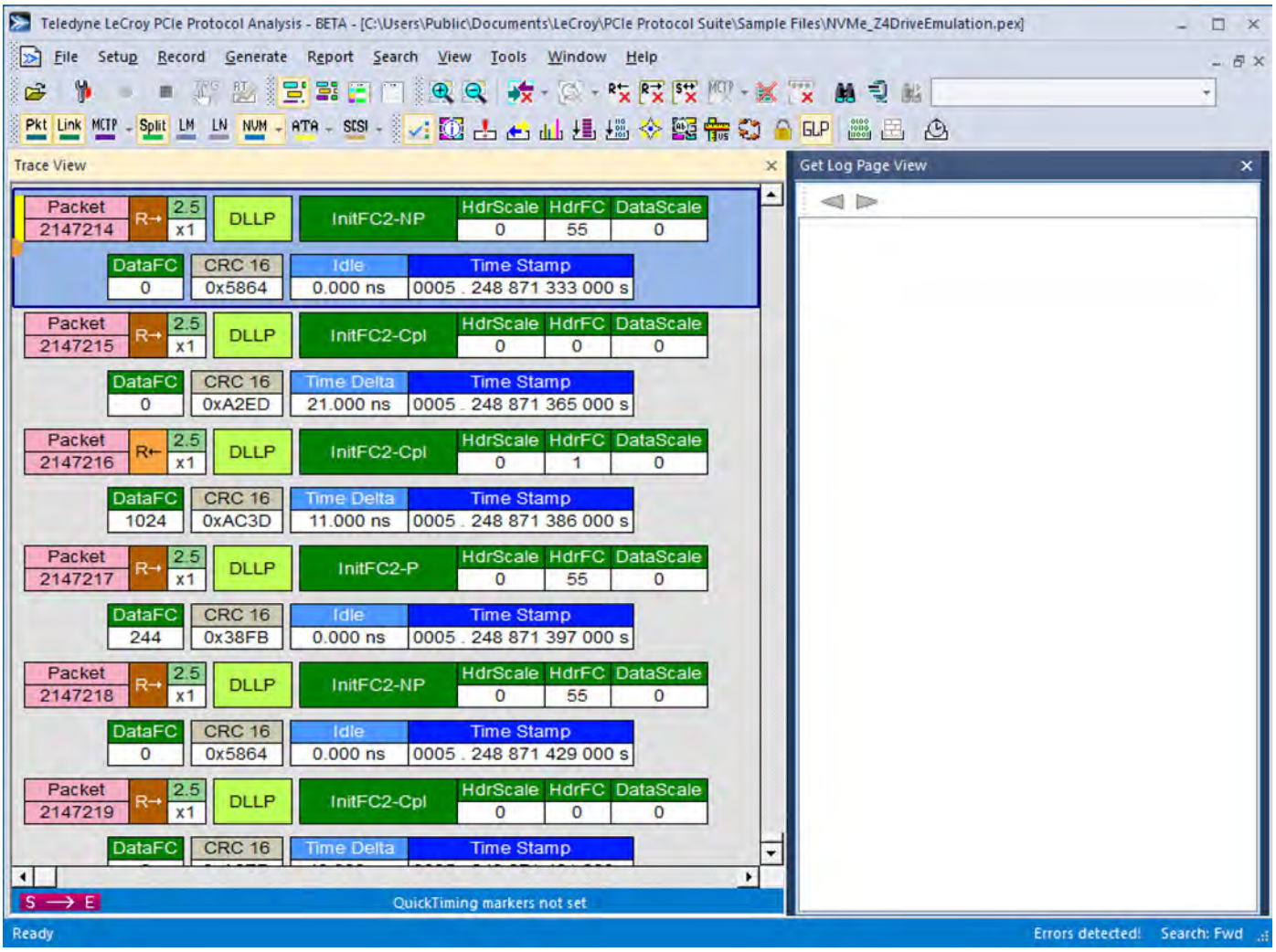


Figure 12.63: Report: Get Log Page View

12.14 Lane Margining: Eye Diagram

A simulated eye diagram for Gen4 analyzers can be generated using the Rx Lane margining parameters delivered through CSR accesses and control skips.

To margin a Receiver, Software moves the target Receiver to a voltage/timing offset from its default sampling position. Simulated eye diagram will help follow stepping through the margin settings and tracking lane margin changes, using right/left offset timing margin steps and up/down offset voltage margin Steps relative to default.

After the trace has been generated select **Report -> LM Eye Diagram** and the following display will pop up. See Figure 12.64.

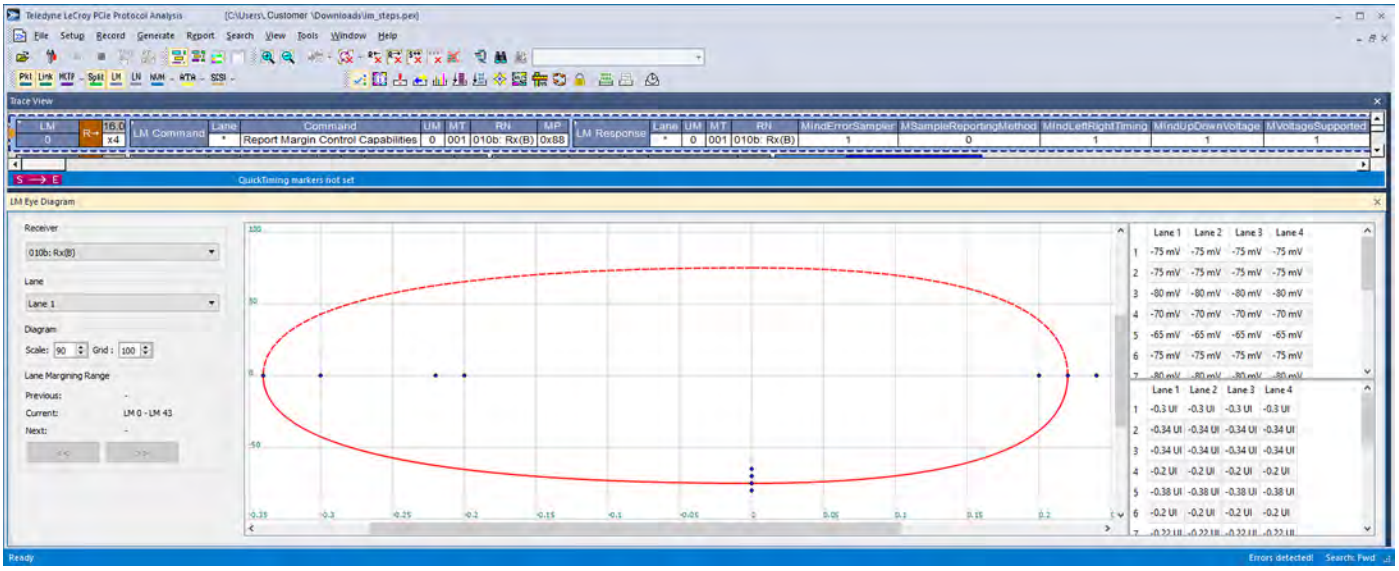


Figure 12.64: Decoded Lane Margining Trace: Eye Diagram

There are a number of controls to manipulate the “Eye Diagram”. Each one has a tooltip to explain it use. On the left side of the Eye Diagram there are the following options:

- Receiver: Choose receiver to be shown in Eye Diagram view and Timing and Voltage tables
- Lane: Choose lane to be shown in Eye Diagram view
- Diagram: Scale Factor -> Set scale factor for Eye Diagram
- Diagram: Grid -> Change grid size of Eye Diagram
- Lane Margining Range: Navigate over existing L0 states in trace

See Figure 12.65 on page 799.

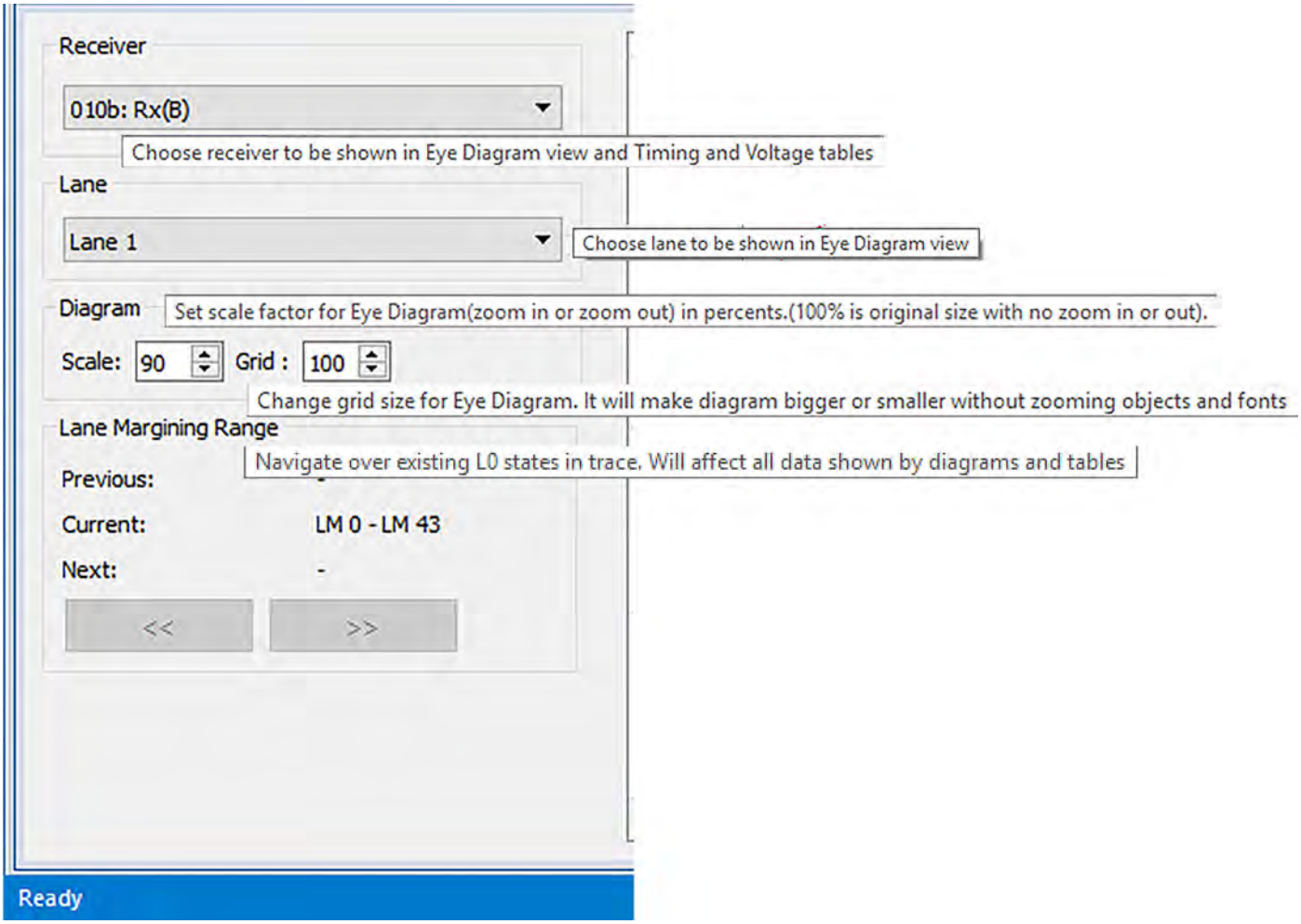


Figure 12.65: Options and Tooltips: Left side of Eye Diagram

On the right side of the Eye Diagram there are the following options:

- Lane 1 - Lane 4: Shows voltage transactions for given receiver
- Lane 1 - Lane 4: Shows timing transactions for given receiver

See Figure 12.66 on page 800.

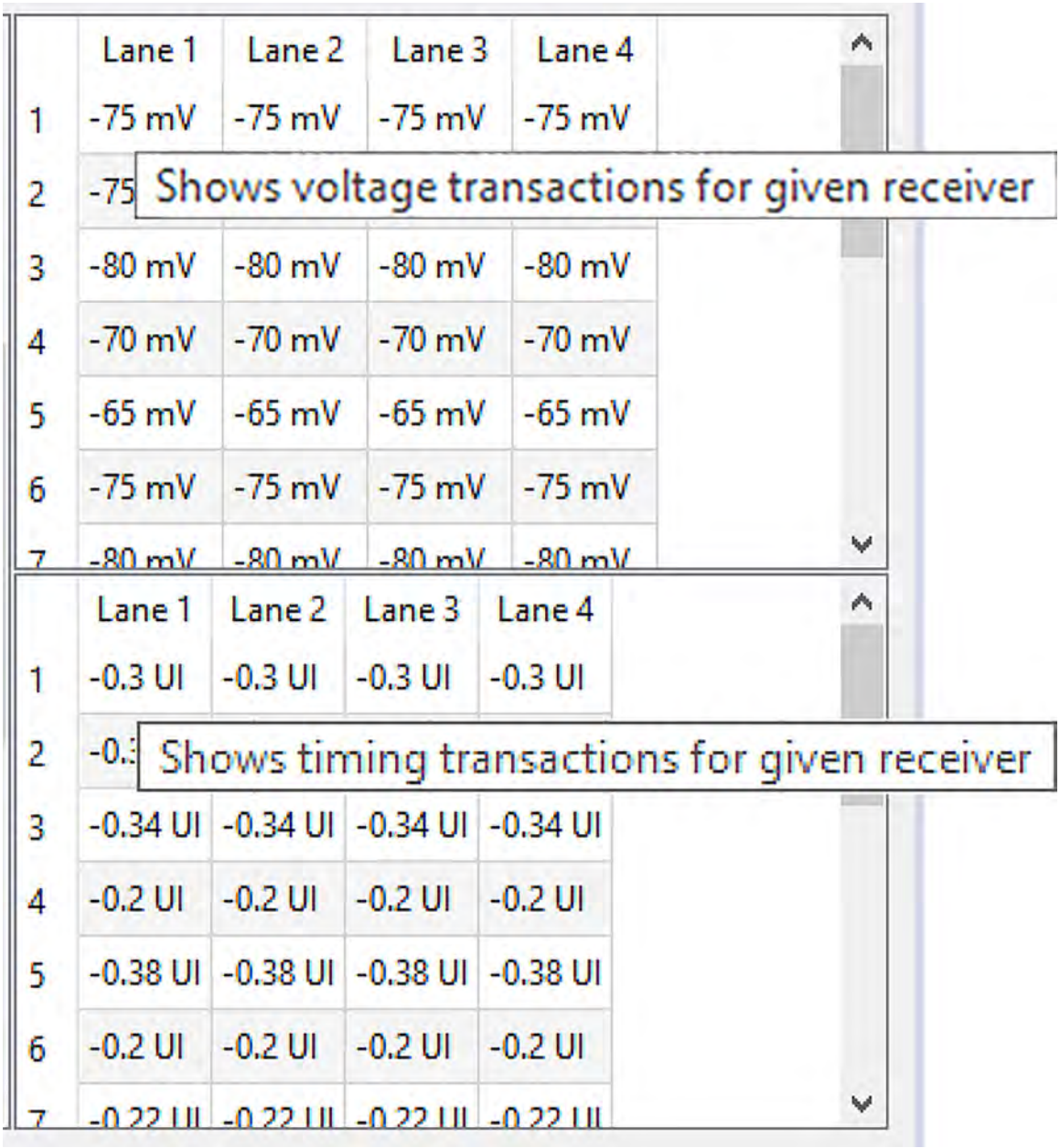


Figure 12.66: Options and Tooltips: Right side of Eye Diagram

12.15 Packet Header Bar

The Packet Header bar shows packet header information.

To display the Packet Header bar (see Figure 12.67 on page 801), select **Report > Packet Header** or click the  toolbar icon.

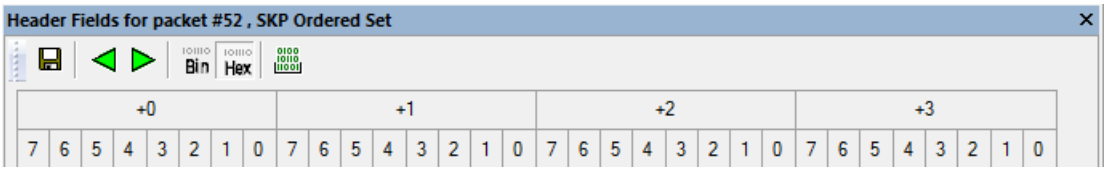


Figure 12.67: Packet Header Bar

The toolbar allows you to Save, go to Previous or Next, display Hexadecimal or Binary, and show the Packet Data window.



12.16 Packet Data Window

The Packet Data window shows packet or transaction payload.

To display the Packet Data window, select **Report > Packet Data**

or click the  toolbar icon.

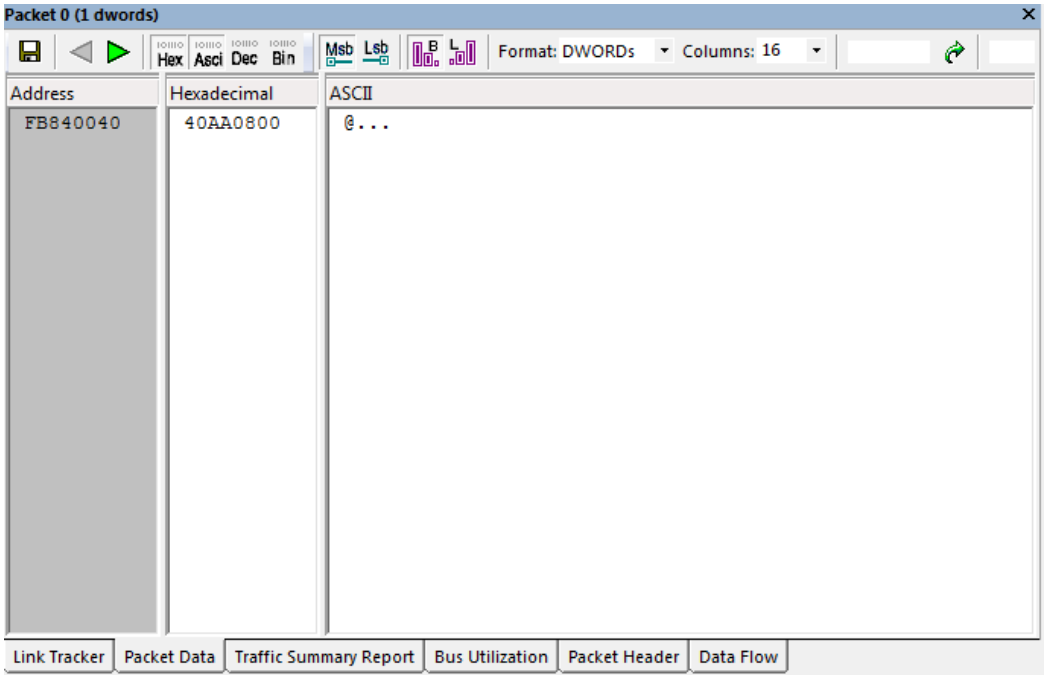
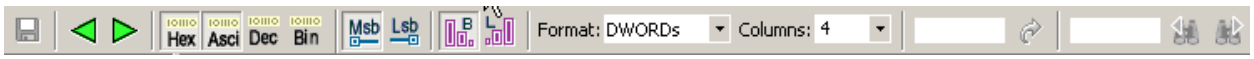


Figure 12.68: Packet Data Window

The toolbar allows you to Save; go to Previous or Next; display Hexadecimal, ASCII, Decimal, or Binary; use MSB Format or LSB Format; and use Big Endian or Little Endian.



Format and Columns allows you to enter the number of bytes, words, or dwords per line.

You can enter an Offset and scroll to it.

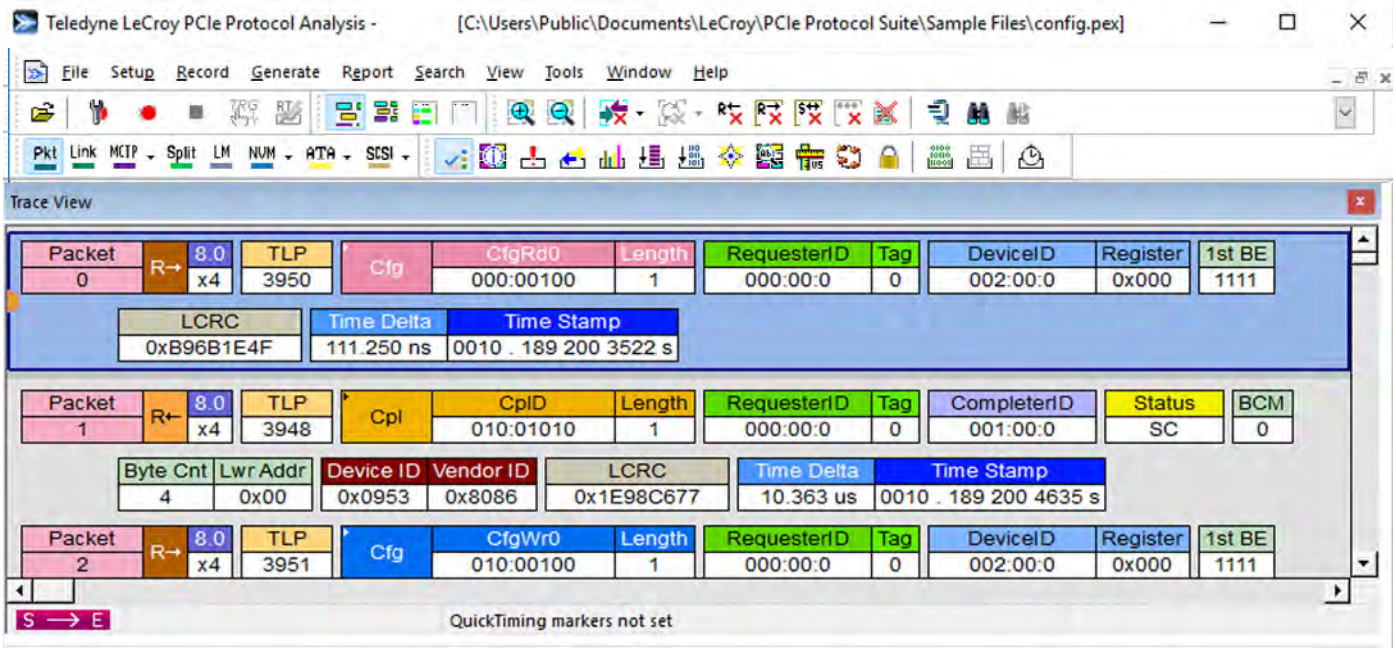
You can enter text and Search Previous or Search Next.

12.17 Configuration Space View

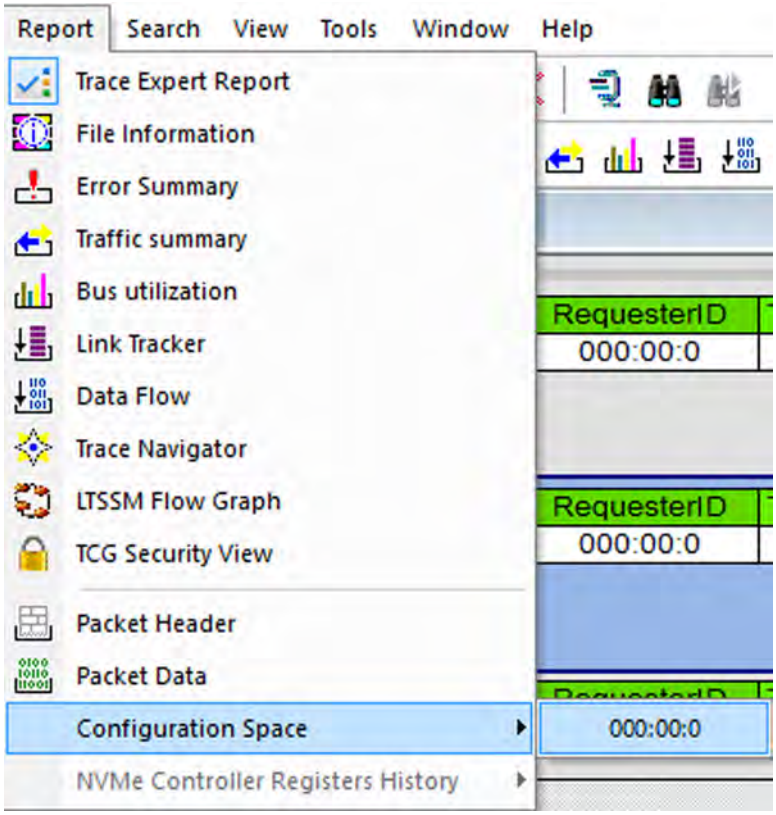
The Configuration Space View displays information about the Configuration Space state as of the current packet of the currently selected device. The view shows the Configuration Space Header and the PCI-compatible or PCI Express Capability Structures.

To display the Configuration Space View for a device at a packet:

1. Open a CATC Trace, such as the sample file **config.pex**.
2. Scroll to a packet with a Configuration header.



3. Select **Report > Configuration Space > <device>** to display the Configuration Space View.



Select **Show Configuration Space for xxxx** from the menu, where **xxxx** is the device number. The Configuration Space View displays (see Figure 12.69 on page 805).

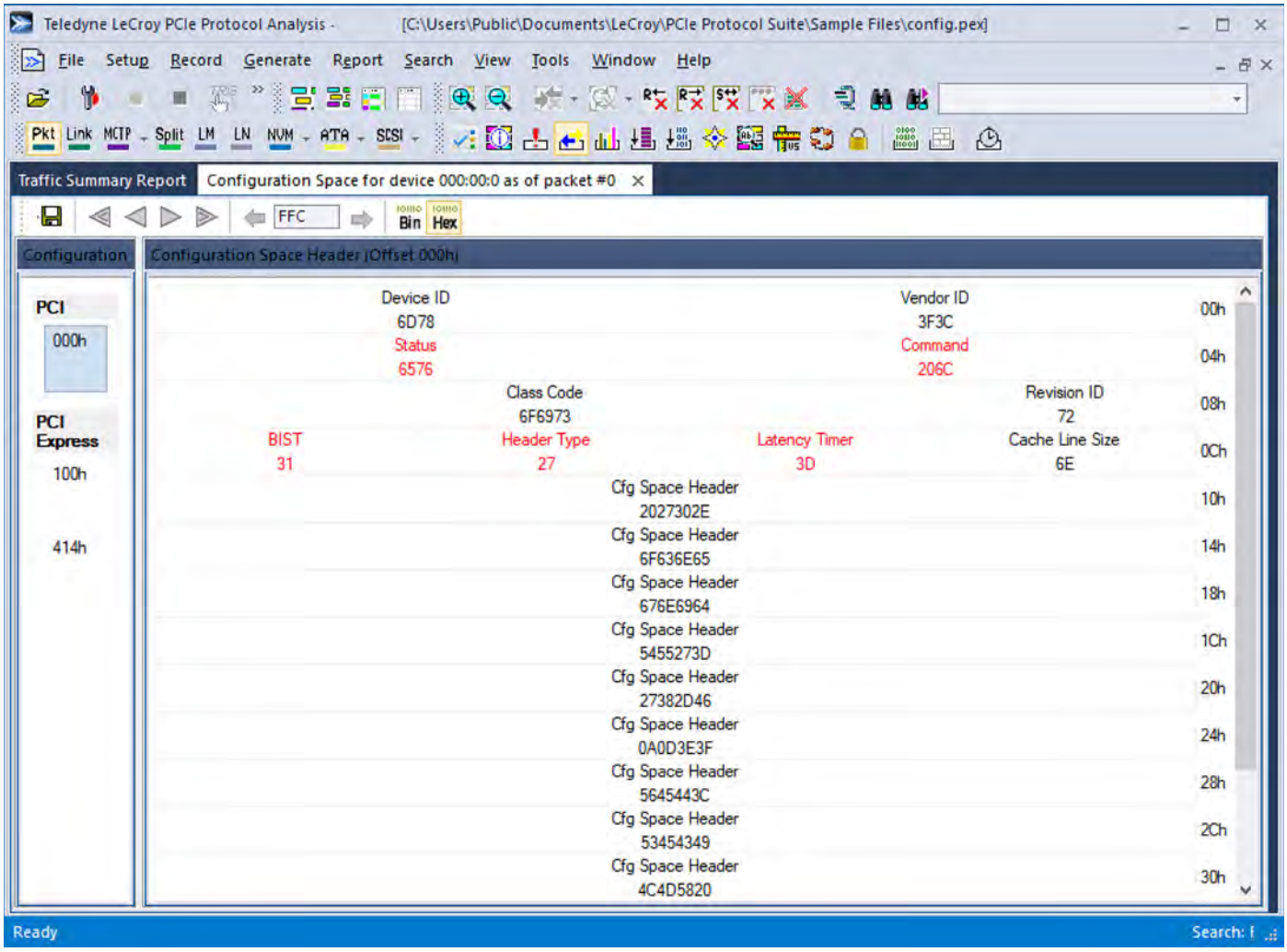


Figure 12.69: Configuration Space View

On the left, the view displays the Configuration Space for the selected CompleterID or DeviceID at the current packet. You can select **Configuration Space Header** or a **Capability Structure.**

The right displays the decoded data of the selected Configuration Space Header or a Capability Structure, up to the current packet. (The decoding builds while navigating through the next packets.)

The Configuration Space View toolbar allows you to save, go to First, go to Previous, go to Next, go to Last, go to Previous Access to Selected Configuration Space Register, go to Next Access to Selected Configuration Space Register, and display Hexadecimal or Binary. See Figure 12.79 on page 825.

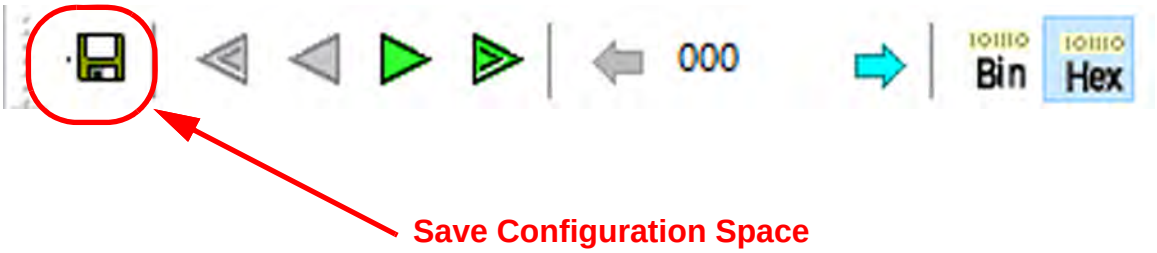


Figure 12.70: Saving Configuration Space File

If you select to Save the Configuration Space file, a dialog box will pop-up and you can save the file for future use in either of two formats:

- PCIe Trainer Configuration Space files
- HTML files

See Figure 12.71.

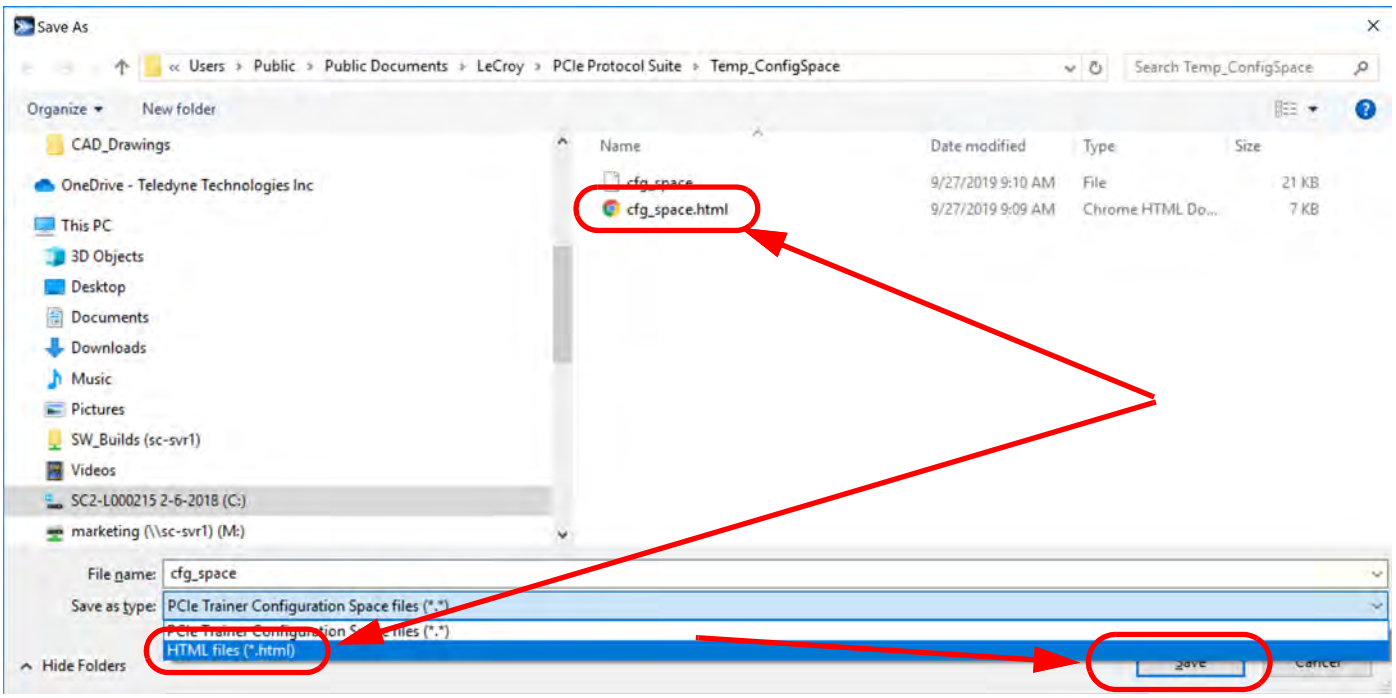
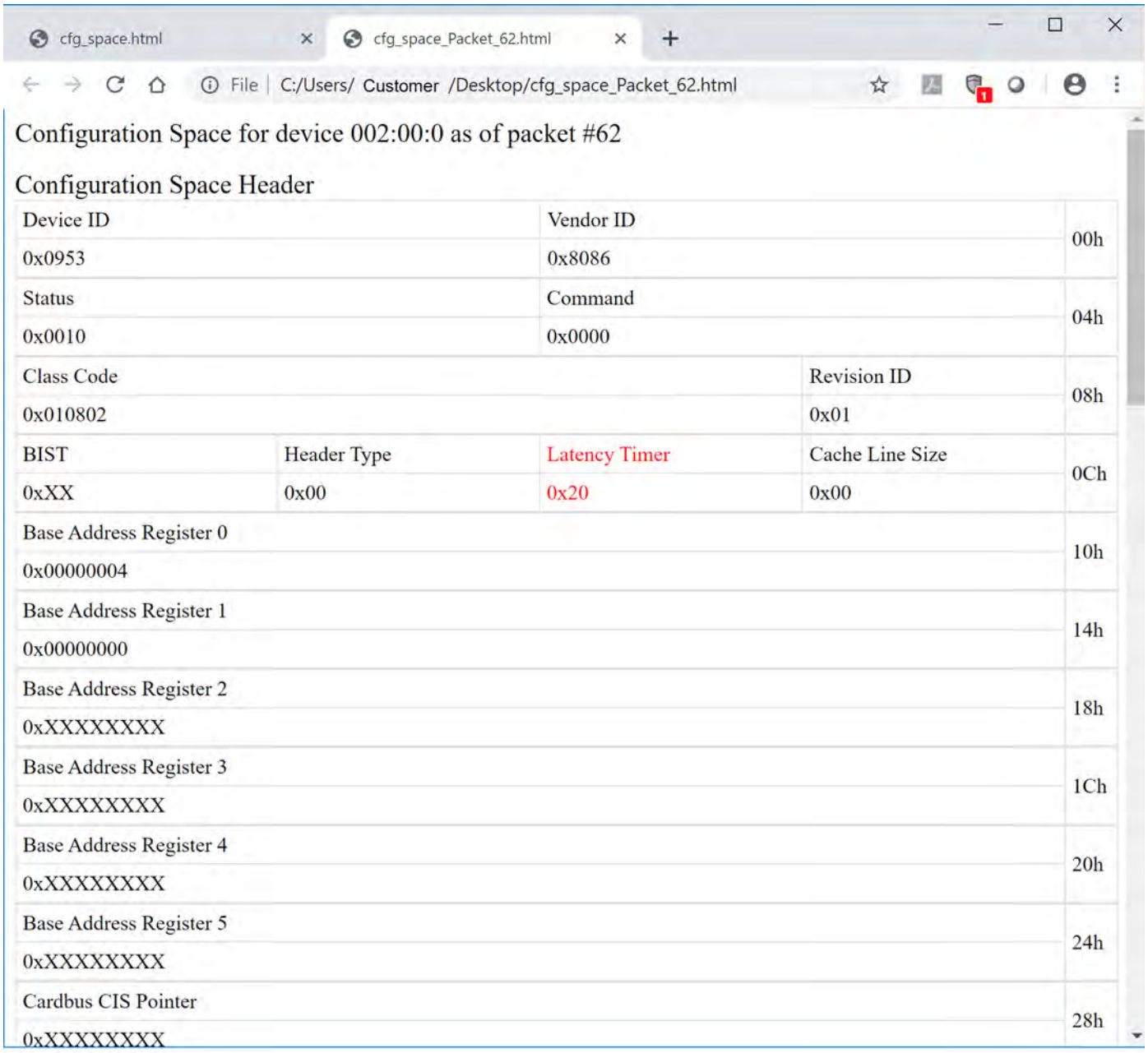


Figure 12.71: Location of Configuration Space File: PCIe Protocol Suite/Temp

Click on the **Save** button to save the file.

If you had selected Saving As -> HTML and you open that file, you will see the following information about the Configuration Space in HTML format. See Figure 12.72 on page 807.



Configuration Space for device 002:00:0 as of packet #62

Configuration Space Header

Device ID		Vendor ID		00h
0x0953		0x8086		
Status		Command		04h
0x0010		0x0000		
Class Code			Revision ID	08h
0x010802			0x01	
BIST	Header Type	Latency Timer	Cache Line Size	0Ch
0xXX	0x00	0x20	0x00	
Base Address Register 0				10h
0x00000004				
Base Address Register 1				14h
0x00000000				
Base Address Register 2				18h
0xXXXXXXXX				
Base Address Register 3				1Ch
0xXXXXXXXX				
Base Address Register 4				20h
0xXXXXXXXX				
Base Address Register 5				24h
0xXXXXXXXX				
Cardbus CIS Pointer				28h
0xXXXXXXXX				

Figure 12.72: Saving Configuration Space File As: HTML

12.18 Using Unit Metrics

For every protocol unit at the Link or Split transaction level, PCIe Protocol Analysis™ calculates and displays a set of metrics. Metrics are measurements of key operating parameters. You can use metrics to evaluate performance of traffic in the CATC Trace stream.

You can view metrics information in the CATC Trace display, the Traffic Summary window, and the Bus Utilization window.

PCIe Protocol Analysis defines different metrics for Link and Split transactions.

12.19 Metrics Defined for Link Transactions

- **Number of Packets**: The total number of packets that compose this Link transaction.
- **Payload**: The number of data payload bytes this Link transaction transferred.
- **Response Time**: The time it took to transmit this Link transaction on the PE link, from the beginning of the first packet in the transaction to the end of the last packet in the transaction.
- **Data Throughput**: The payload divided by response time, expressed in megabytes (MB) per second (MB = 1024*1024 bytes).

Note: Usually, the Number of Packets metric for a link transaction is two (in case of explicit acknowledge) or one (in case of implicit acknowledge). However if Naks/link level retries are involved, this metric might be higher. As a result, the Number of Packets metric is useful in highlighting unusual link transactions.

12.19.1 Metrics Defined for Split Transactions

The following types of metrics currently are defined for Split transactions:

Number of Link Transactions: The total number of Link transactions that compose this Split transaction.

Payload: The number of payload bytes this Split transaction transferred.

Response Time: The time it took to transmit this Split transaction on the PE link, from the beginning of the first packet in the Split transaction to the end of the last packet in the Split transaction;

Data Throughput: The transaction payload divided by response time, expressed in megabytes (MB) per second (MB = 1024*1024 bytes).

Latency Time: The time measured from the end of the request transaction to the first completion transmitted in response to the request within this Split transaction.

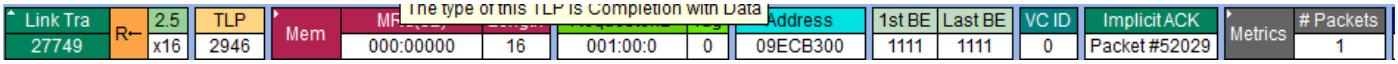
Note: The Number Of Link Transactions metric for a Split Transaction usually is two for a Configuration or IO request. It can be bigger then two for a Memory Read request.

12.20 Show Metrics in the CATC Trace Display

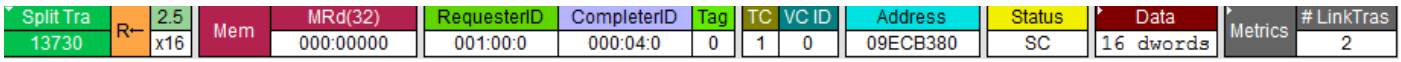
In the CATC Trace view display of Link Transaction or Split Transaction levels, all metrics information applicable to a specific protocol unit is displayed in a Metrics header. The header is located close to the end of the unit, in front of the Time cell. You can expand and collapse the header to show or hide the metrics information.

12.20.1 Collapsed Metrics Header Display

Following is a collapsed metrics display for a unit of Link Transaction. The collapsed header display shows only the metrics cell representing the Number of Packets.

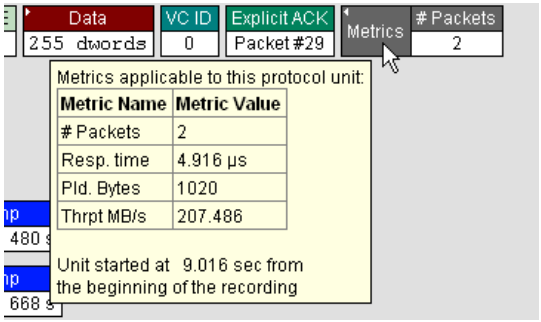


Following is a collapsed metrics display for a unit of Split Transaction. The collapsed header display shows only the metrics cell representing Number of Link Transactions.



12.20.2 Metrics Tool Tip Display

In both CATC Trace level views, you can view the summary of all the unit metrics in the Metrics header tool tip. To view the tool tip, simply place the mouse cursor over the Metrics header. Following is the tool tip for a unit in the Link Transaction view.



Note: The tool tip also presents information for time passed from the start of the recording till the beginning of this Link or Split Transaction.

12.20.3 Expanded Metrics Header Display

When you expand the Metrics header, the display creates a separate cell for each applicable metric:

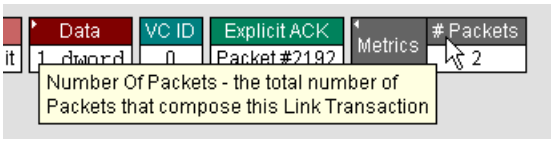
The following is the expanded Metric header for a unit in the Split Transaction view.

Metrics	# LinkTras	Resp. time	Latency	Thrpt MB/s	Pld. Bytes
	2	7.460 µs	6.736 µs	2.145	16

The following is the expanded Metric header for a unit in the Link Transaction view.

Metrics	# Packets	Resp. time	Pld. Bytes	Thrpt MB/s
	2	536.000 ns	64	119.403

Note: Each of the metric cells pops up a tool tip window with the explanation of what the metric means.

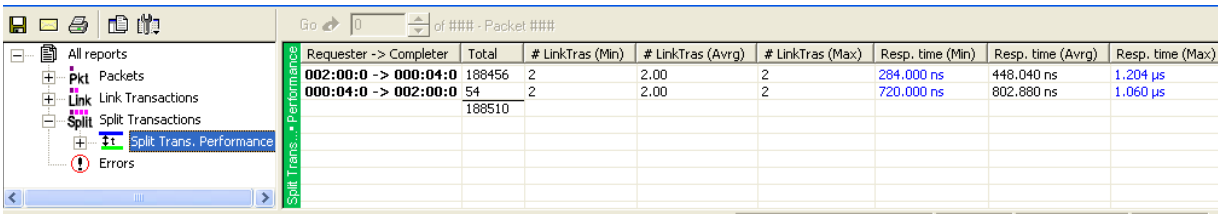


12.21 Show Metrics in the Traffic Summary Window

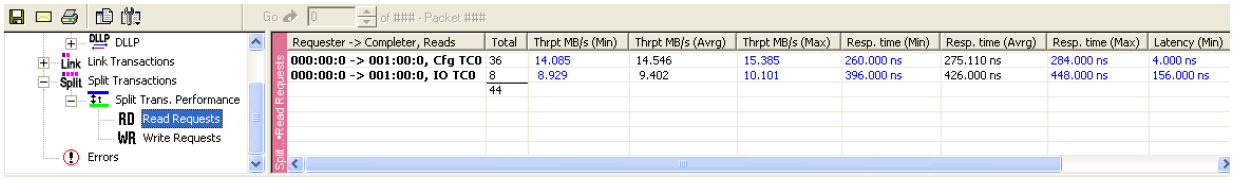
Some of the Traffic Summary reports at the Link and Split Transaction levels are based on metrics collected for the corresponding protocol units in the CATC Trace.

12.21.1 Reports at Split Transaction Level

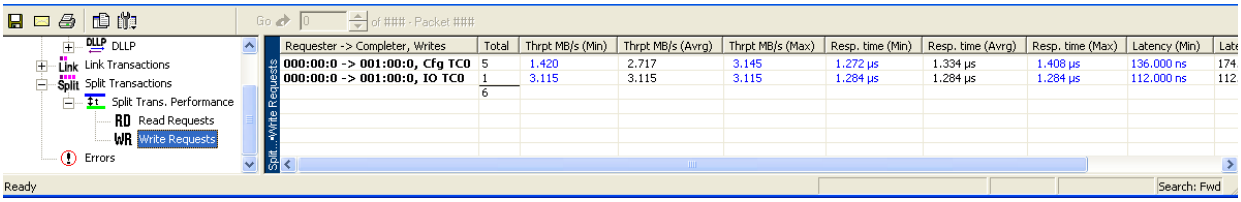
Split Transaction Performance: This report table groups the Split Transactions by Requester-Completer pair and displays Minimum/Average/Maximum data for Number Of Link Transactions and Response Time metrics.



Read Requests Performance: This report table includes only the Split Transactions that present Read Requests (Configuration, IO and Memory). It groups them by the combination of Requester-Completer pair, request type, and Traffic Class and displays Minimum/Average/Maximum data for Throughput, Response Time, and Latency metrics (see the following figure).



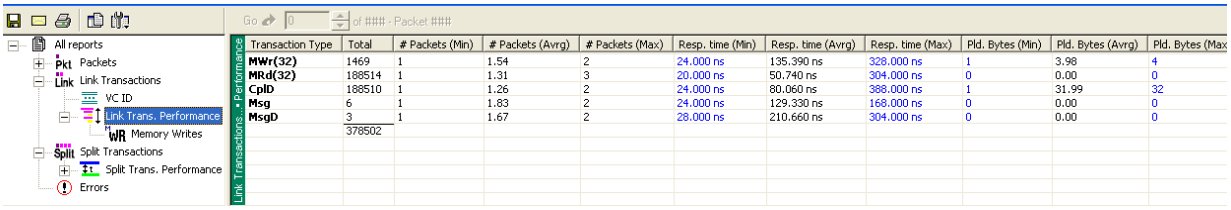
Write Requests Performance: This report table includes only the Split Transactions that present Write Requests (Configuration and IO). It groups them by the combination of Requester-Completer pair, request type, and Traffic Class and displays Minimum/Average/Maximum data for Throughput, Response Time, and Latency metrics.



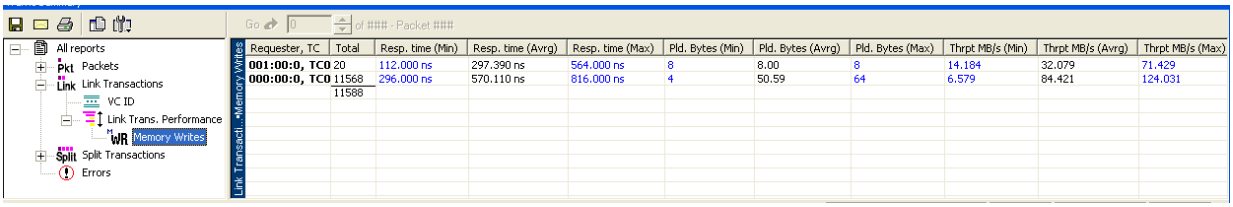
12.21.2 Reports at the Link Transaction Level

The following metric-based reports are displayed at the Link Transaction level:

Link Transaction Performance: This report table groups the Link Transactions by TLP Type and displays Minimum/Average/Maximum data for Number Of Packets, Response Time and Payload Bytes metrics.



Memory Writes: This report table includes only the Link Transactions that present Memory Write Requests. Memory Writes are the only (posted) requests that don't get promoted to the Split transaction level, therefore their performance should be viewed at the Link transaction level. The table groups Memory Writes by the combination of Requester ID and Traffic Class and displays Minimum/Average/Maximum data for Response Time, Payload and Throughput metrics.



The following features apply to all of the report tables described above for the Split Transaction and Link Transaction levels:

- Each report row for the defined tables contains the total number of units in this group for the CATC Trace (total number of units for Split Transaction performance, Read Requests performance, Memory Writes, and so on).
- In many cases, the Maximum and Minimum values in the report tables are navigable. By clicking table cells, you reposition the corresponding CATC Trace view to the Split or Link Transaction that has yielded this maximum or minimum value. This can help you to find specific units in the CATC Trace, such as transactions that produced spikes in Response Time or Throughput.

12.22 Show Metrics in the Bus Utilization Window

The Bus Utilization window provides graphs for packet-level information in the CATC Trace. The window also provides graphs for information on Split and Link Transaction levels, plotted over time. The graphs for Split and Link Transaction levels are based on metrics collected for the transactions throughout the CATC Trace.

The seven graphs related to Split and Transaction levels are:

1. Pending Requests at Split Transaction level.
2. Response Time at Split Transaction level.
3. Latency Time at Split Transaction level.
4. Throughput Per Transaction at Split Transaction level.
5. Response Time and Latency Time at Split Transaction level (combined graph).
6. Response Time at Link Transaction level, for Memory Writes only.
7. Throughput at Link Transaction level, for Memory Writes only.

The following is an example of Bus Utilization window display of graph numbers 1, 4, 5, 6 and 7 (see the following figure):



12.22.1 Unit-Based Averaging

The Analyzer builds metric graphs using unit-based averaging (as opposed to time-based averaging). For the total duration of a certain request (or Memory Write transaction), the graph value is assumed equal to the corresponding metric for this request (transaction). If there are

overlapping operations for a certain time period, then the value is calculated as an average of metric values for all the overlapped requests (transactions).

It is important to remember that the Analyzer uses unit-based averaging rather than time-based averaging. Time-based averaging can be misleading in some situations. For example, consider the Throughput Per Transaction graph. Sometimes, while many outstanding requests are in progress, latency (and response time) grows for each of the transactions, resulting in a lower throughput per transaction over time (which is reflected in the graph). This happens even though aggregated throughput across all the transactions is constant.

12.22.2 Bus Utilization Window Features

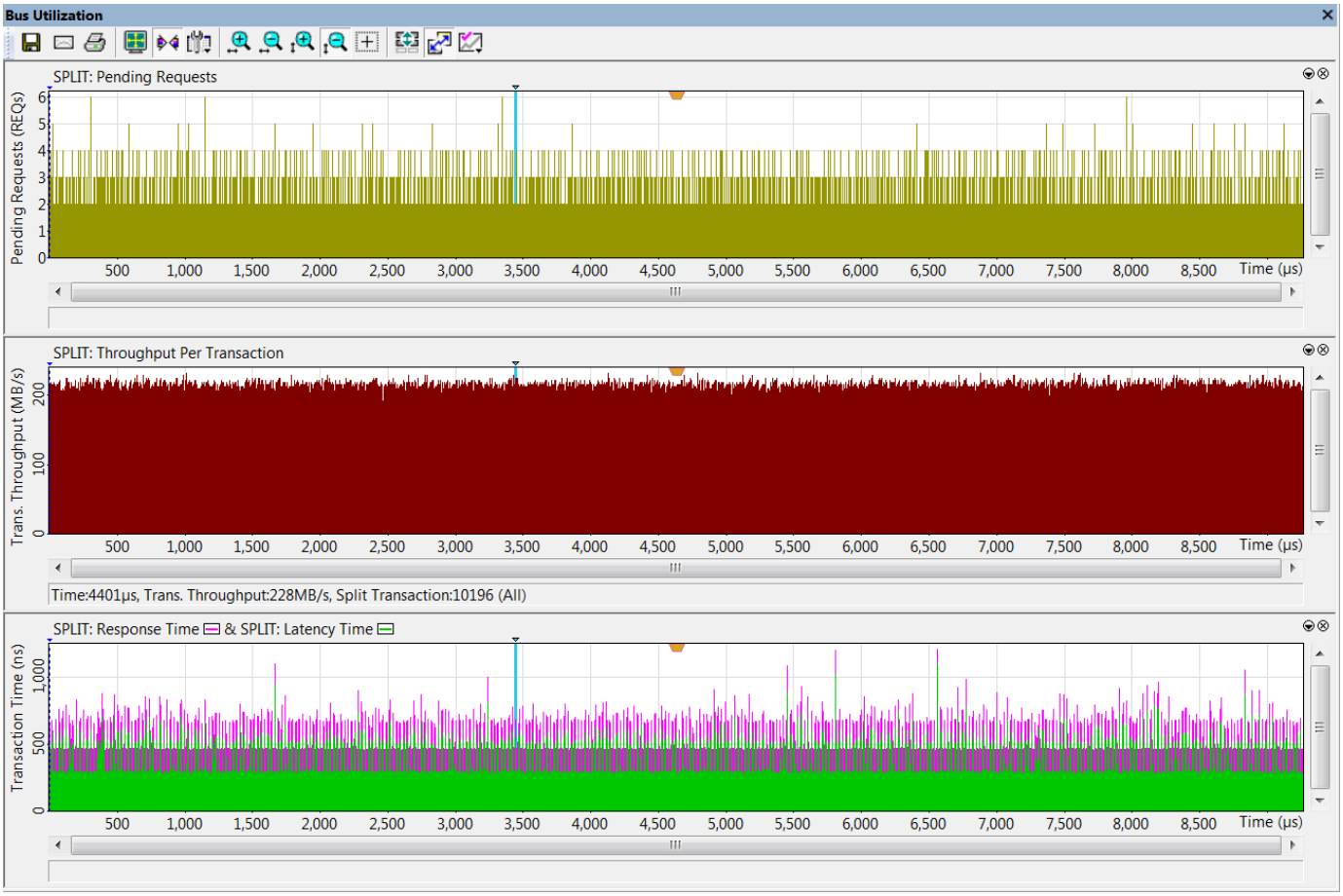
For the seven Split- and Transaction-level graphs listed, all Bus Utilization window features are available, such as zooming in/out, changing scale type, scrolling, context-sensitive status, and graph synchronization. See Bus Utilization and Bus Utilization Buttons for more on these features.

Note: Clicking a certain place within a graph area repositions the CATC Trace display at the Link or Split transaction level to the transaction that was in progress at that time.

12.22.3 Split Transaction Level Graphs

Transactions at the Split level combine all the non-posted requests with corresponding completions. This includes Configuration and IO Read and Write requests, as well as Memory Read requests.

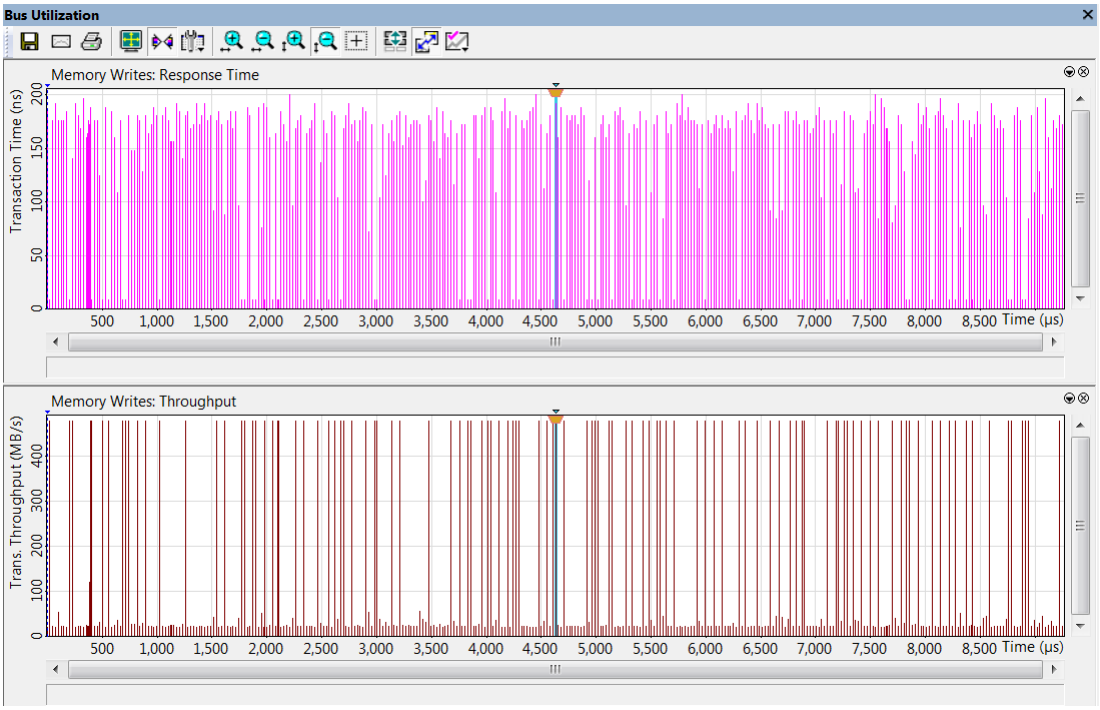
The following shows the graphs for the Split level:



Note: The Pending Requests graph is not directly defined by metrics, but it is useful when considering metrics. The Pending Requests graph presents the unit-averaged number of requests that were pending (in progress) at any moment of time. It allows you to correlate the number of requests posted to a completer with other performance metrics.

12.22.4 Link Transaction Level Graphs

Memory Writes are the only (posted) requests that do not get promoted to the Split transaction level. Therefore, Memory Write performance should be viewed at the Link Transaction level. That is the reason graphs at the Link level only present the Memory Write-related metrics and are titled **Writes: Response Time:** and **Writes: Throughput** (see the following figure).


Bus Utilization
Memory Writes: Response Time
Transaction Time (ns)
0
50
100
150
200
500
1,000
1,500
2,000
2,500
3,000
3,500
4,000
4,500
5,000
5,500
6,000
6,500
7,000
7,500
8,000
8,500
Time (µs)
Memory Writes: Throughput
Trans. Throughput (MB/s)
0
100
200
300
400
500
1,000
1,500
2,000
2,500
3,000
3,500
4,000
4,500
5,000
5,500
6,000
6,500
7,000
7,500
8,000
8,500
Time (µs)

12.23 Real-Time Statistics Window

The Real-Time Statistics Window displays Link Utilization, performance measurements, and statistical values for a PCI Express link plotted in real time.

Click  to open the Real-Time Statistics window (see Figure 12.79 on page 825).

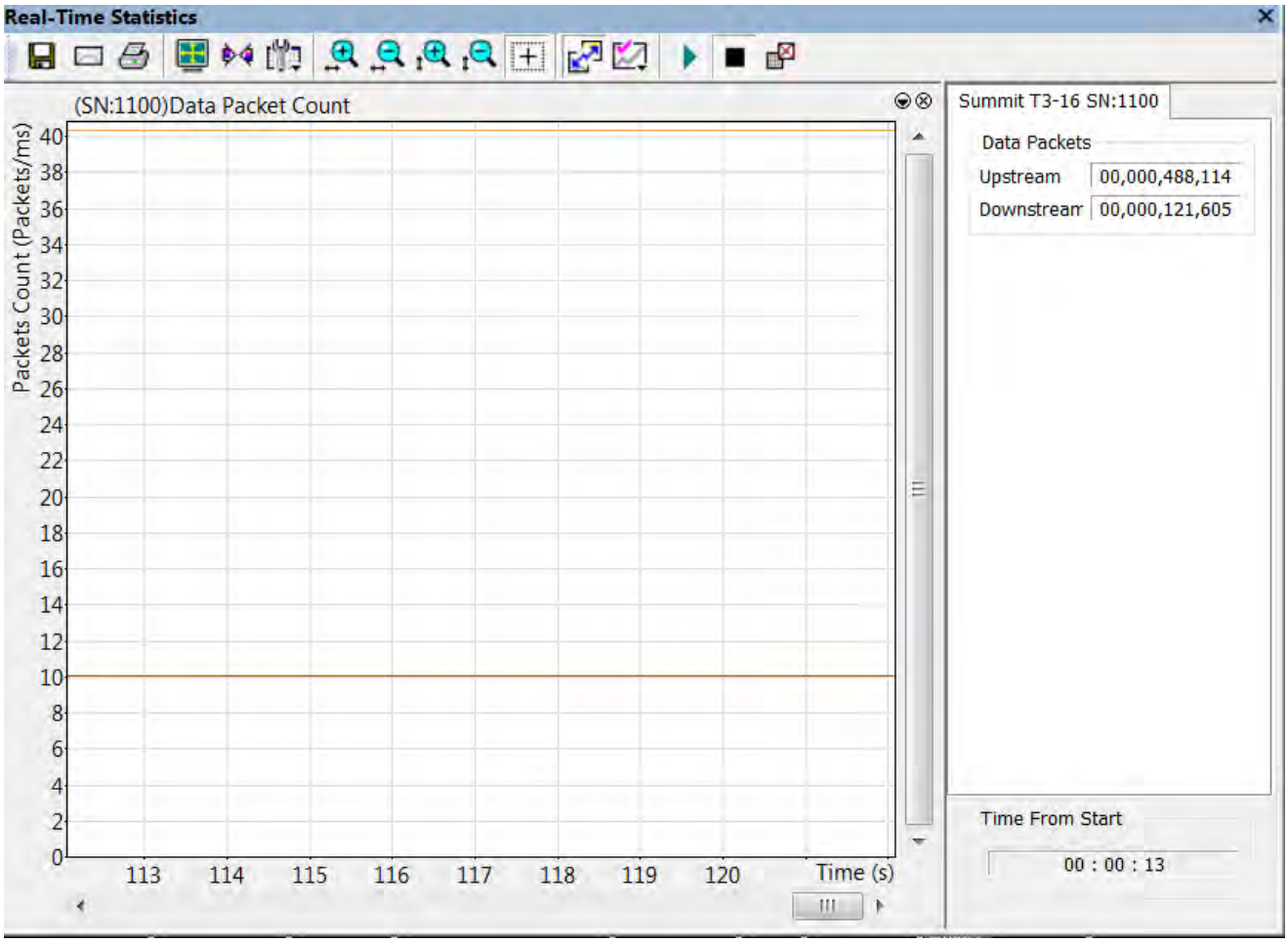


Figure 12.73: Real-Time Statistics Dialog

Start **PCI Express™** link activity.

To start the monitor, press  .

To stop the monitor, press  .

The remaining Real-Time Statistics buttons provide options for changing the format of the display.

Additional formatting options are available through the Real-Time Statistics pop-up menu and the Real-Time Statistics toolbar.

12.23.1 Real-Time Statistics Buttons

Additional formatting options are available through the Real-Time Statistics toolbar.

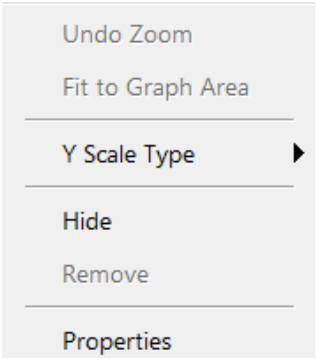


Button	Function
	Save. Saves Real-Time Statistics data to bitmap file (*.bmp).
	Email. Opens an email and attaches a bitmap file of the Real-Time Statistics data.
	Print. Prints the Real-Time Statistics data.
	Full Screen. Maximizes the Real-Time Statistics window.
	Synchronize Views.Synchronize the current view with other open views.
	View Settings. Opens a sub-menu with the following choices: • Orient Horizontally • Tile Vertically • Show Markers • Show Plumbline • Status >> • Bar • Tool tips • None • Grid Lines >> • Both Axes • X Axis • Y Axis • No Grid • Grid on Top • Fonts & Colors

	Horizontal zoom in
	Horizontal zoom out
	Vertical zoom in
	Vertical zoom out
	Click and Drag Zoom. Click and drag to zoom in on a part of the graph.
	Synchronize Graph Areas. If two or more graphs are displayed, this button synchronizes the graphs to one another. Once synchronized, the positioning slider of one graph moves the other graphs.
	Graph Areas. Allows you to hide or display the graphs and the counters. You can toggle Statistics Accumulation, Link Utilization, Data Payload Throughput, and Data Packet Count.
	Start real-time statistics. Starts the real-time statistical monitor.
	Stop real-time statistics. Stops the real-time statistical monitor.
	Reset Graphs. Resets the graphs.

12.23.2 Real-Time Statistical Monitor Pop-up Menu

Additional formatting options are available through the Real-Time Statistics pop-up menu. Right-click a graph in the Real-Time Statistical Monitor window to display a pop-up menu with options for changing the format of the display.



Undo Zoom: If you have zoomed in, this command undoes the zoom.

Fit to Graph Area: Redisplays graph so that the entire CATC Trace fits inside graph area.

Y Scale Type:

- **Linear**: Converts display to linear format.
- **Logarithmic**: Converts display to logarithmic format.

Hide: Hides the selected graph

Properties: Opens a dialog box with options for changing the Title, Appearance, and Color of the graph.

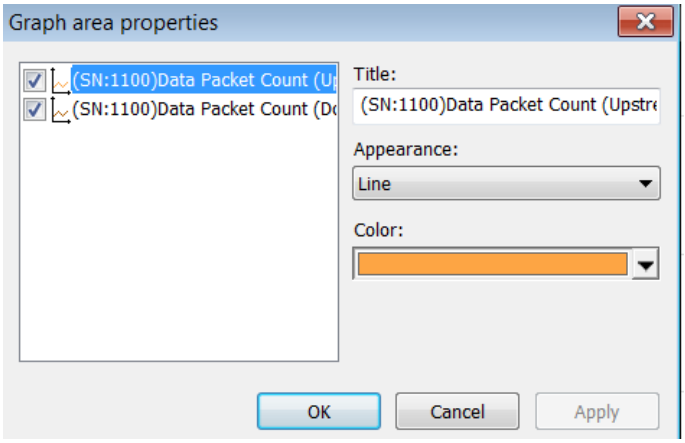


Figure 12.74: Graph Area Properties Display

12.23.3 Real-Time Statistics Graph Areas

The Real-time Statistics window has three graph areas:

- Link Utilization
- Data Payload Throughput

Data Packet Count

Each graph area has Upstream and Downstream graphs for a device (if connected to a host machine), plus as many graphs as Exerciser devices connected to the host machine.

The Statistics Accumulation area shows the PCIe Protocol Analysis statistics tab, plus as many tabs as Exerciser devices connected (see Figure 12.75 on page 821):

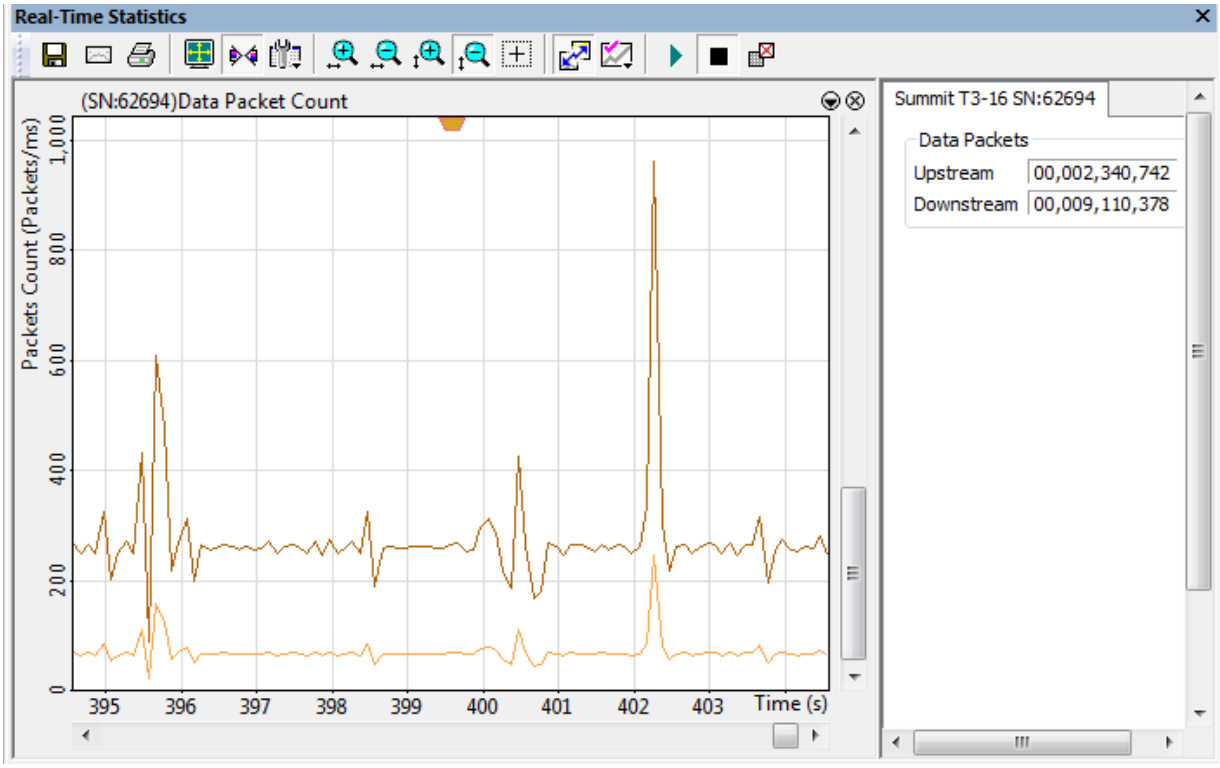


Figure 12.75: Real-Time Statistics Graph Display

For each Exerciser device, the following information is displayed:

- Number of data packets
- Payload size
- **InitFC complete status**: Yes/No
- **Link State**: Possible states are:
  - DETECT_QUIET
  - DETECT_ACTIVE
  - POLLING_ACTIVE
  - POLLING_CONFIG
  - CONFIG_LINKWIDTH_START
  - CONFIG_LINKWIDTH_ACCEPT
  - CONFIG_LANENUM_WAIT
  - CONFIG_LANENUM_ACCEPT
  - CONFIG_COMPLETE
  - CONFIG_IDLE
  - L0
  - L0S_IDLE
  - L0S_FTS
  - L1
  - RECOVERY_RCVRLOCK
  - RECOVERY_RCVRCFG
  - RECOVERY_IDLE
  - HOT_RESET

- DISABLED

12.24 Tools -> Import Configuration Space File

Import Configuration Space dialog can be launched from Tools menu after PCIe trace file is opened. See Figure 12.76.

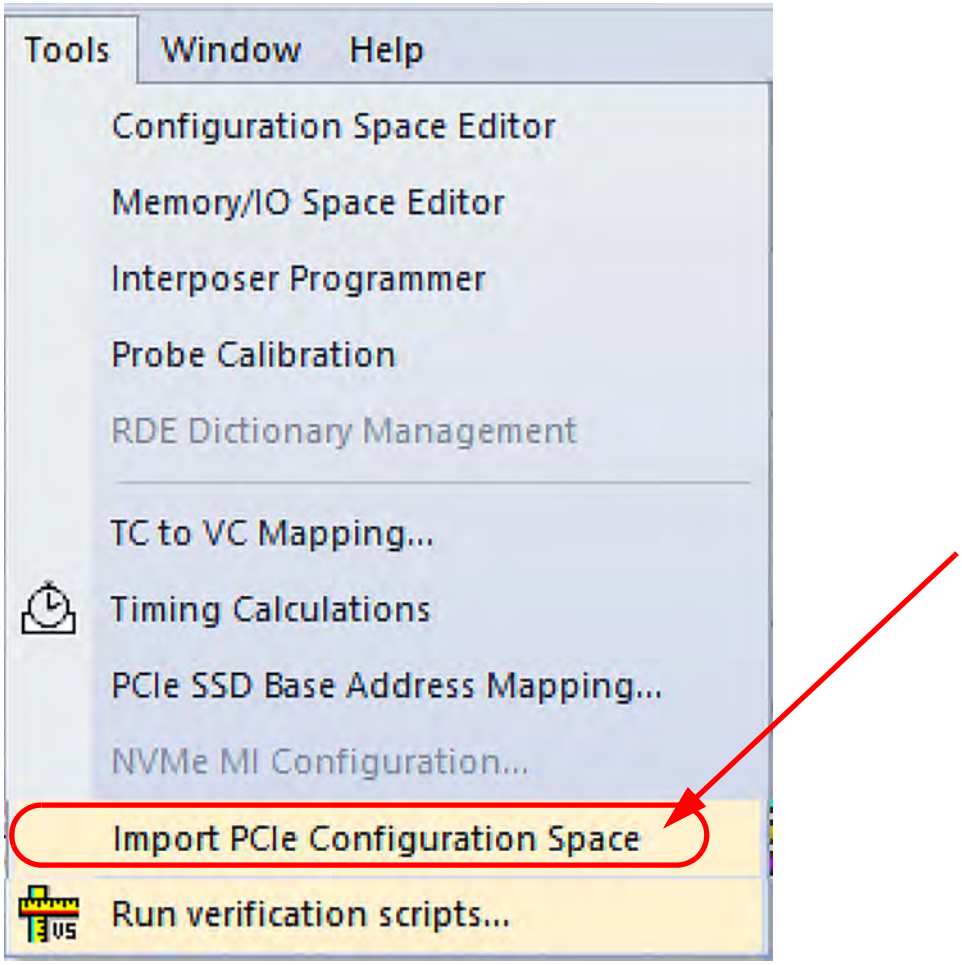


Figure 12.76: **Tools -> Import PCIe Configuration Space**

The main purpose of importing a configuration space is to overwrite existing configuration space or to add configuration space information to a trace without it in order to help decoding.

Select Import PCIe Configuration Space and the following window pops up with previously saved Configuration Space files. See Figure 12.77.

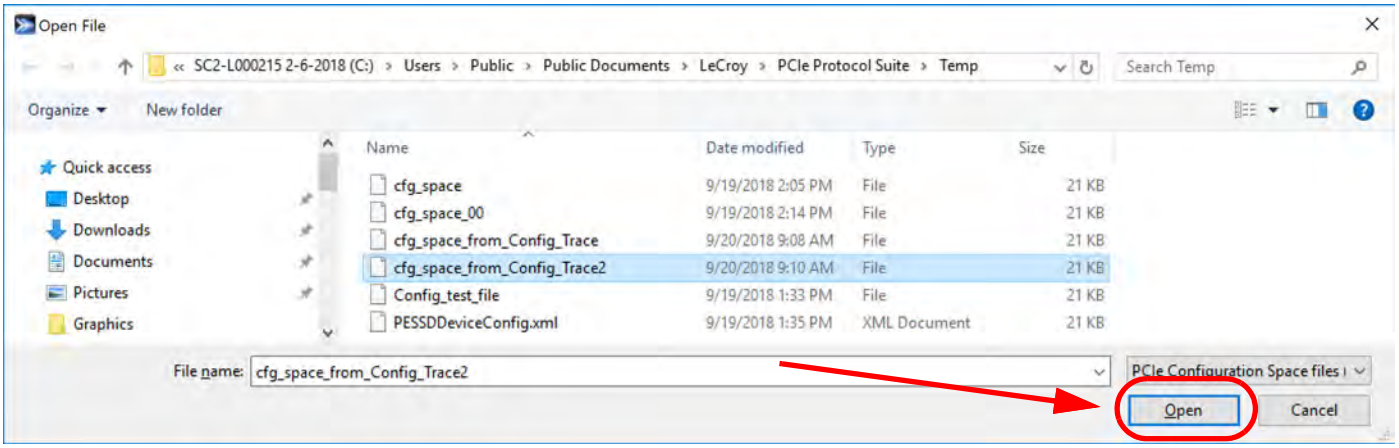


Figure 12.77: Saved Configuration Space files

Select **Open** and the Import PCIe Configuration Space dialog pops up. See Figure 12.78.

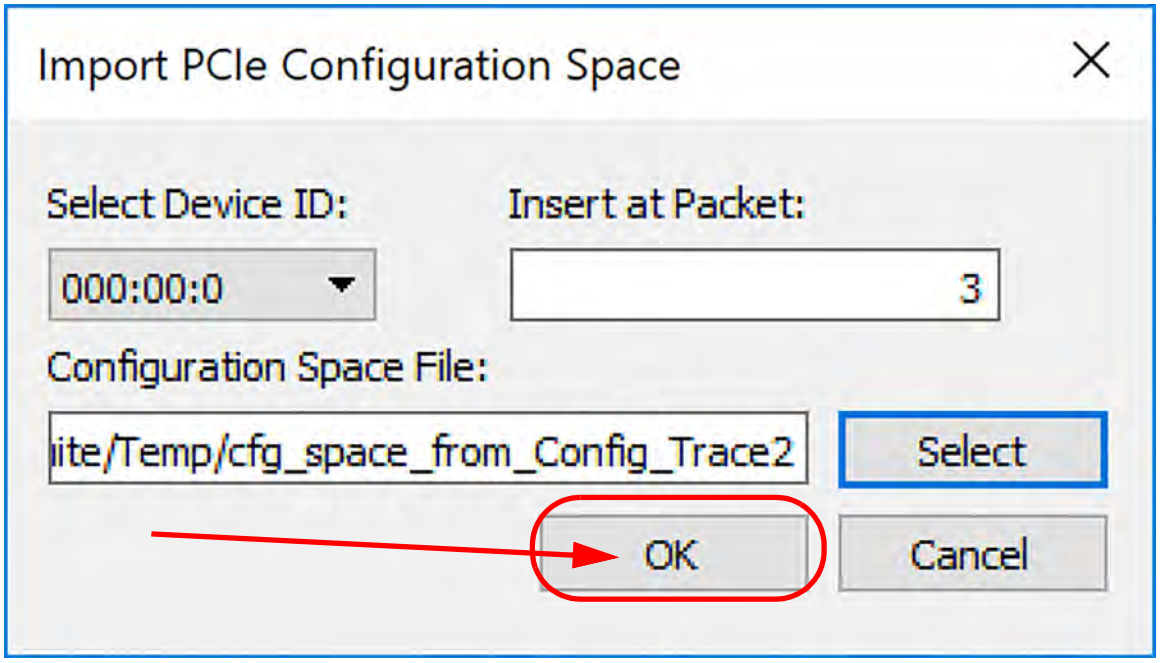


Figure 12.78: Import PCIe Configuration Space Dialog

In this dialog box you can select the following options:

- Device TD
- Insert at Packet
- Select the Configuration Space File you want to use

After making your choices, click on OK and the Configuration File will be inserted into the Trace you have open at the before the Packet you have chosen.

The next section shows how to edit a Configuration Space

12.25 Tools -> Configuration Space Editor

The Configuration Space Editor allows you to create a new Configuration space file or open an existing Configuration Space file. It is used in conjunction with Teledyne LeCroy Trainer products. Select **Tools > Configuration Space Editor** to display the Configuration Space Editor dialog (see Figure 12.79 on page 825).

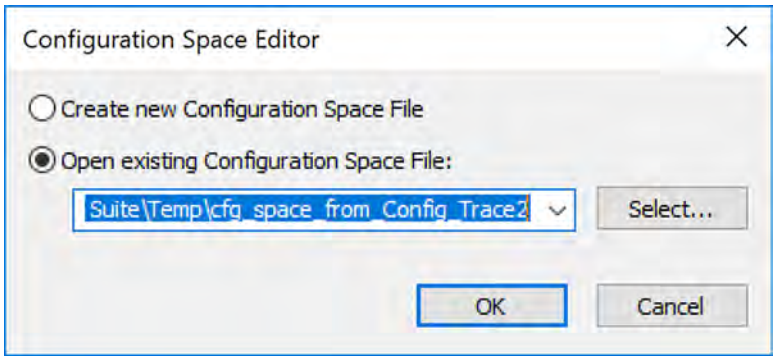


Figure 12.79: Configuration Space Editor Dialog

Click on **OK** and the Editor will popup and you can edit the Configuration Space file manually and then save it and import it. See Figure 12.80.

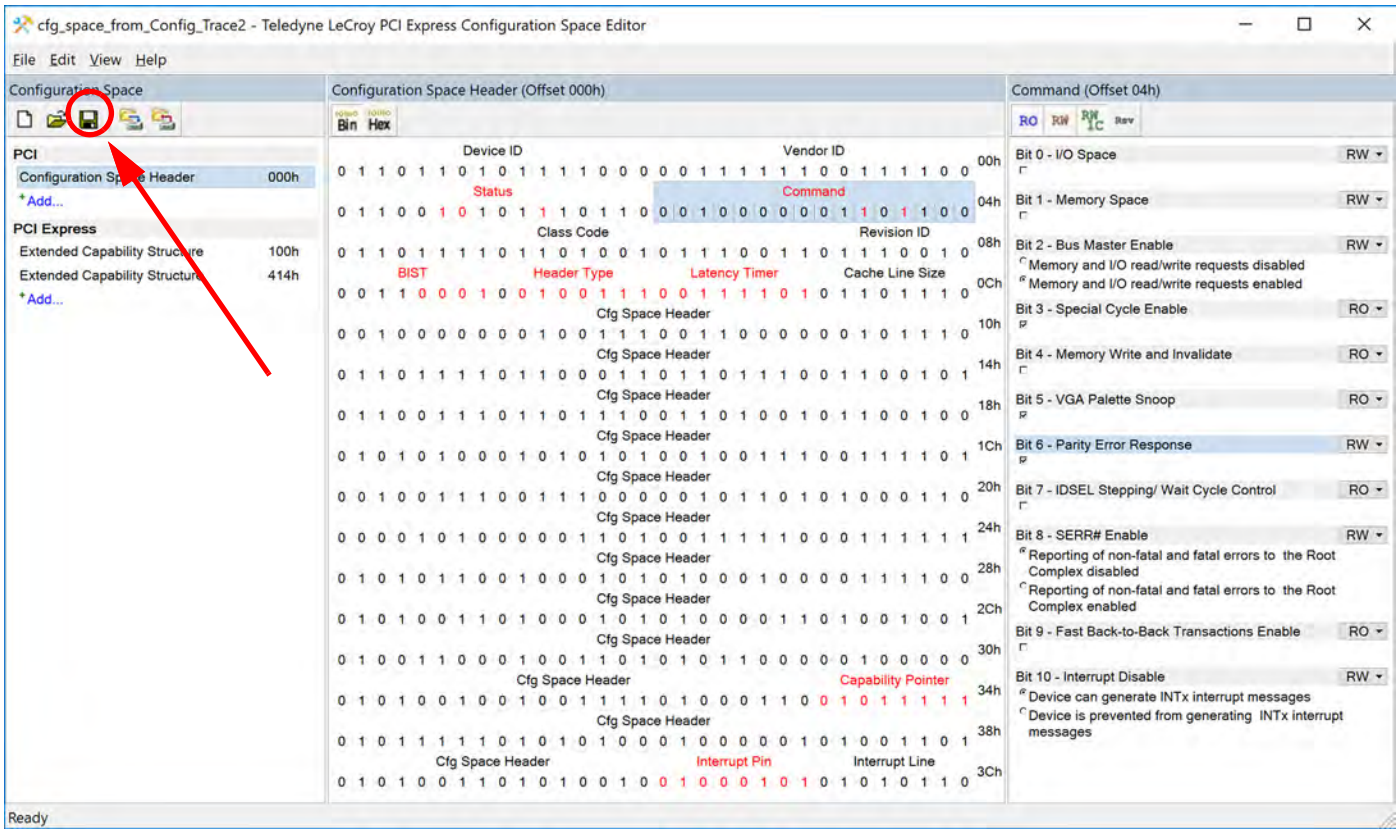


Figure 12.80: Configuration Space File: Example

Note: See “Configuration Space Decoding” on page 875 for details of the Configuration Space file.

12.26 Tools -> Memory I/O Space Editor

The Memory I/O Space Editor allows you to create a new Memory I/O Space file or open an existing Memory I/O Space file. It is used in conjunction with Teledyne LeCroy Trainer products. Select **Tools > Memory I/O Space Editor** to display the Memory Space Editor dialog.

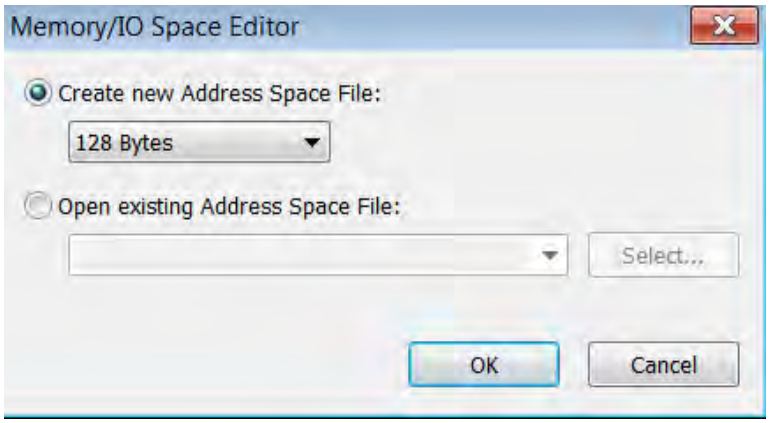


Figure 12.81: Memory I/O Space Editor Dialog

12.27 Tools -> Interposer Programmer

12.27.1 Installing the FTDI Serial Cable

Install the Interposer per instructions in the appropriate User Manual or Quick Start Guide.

To use the Utility you must connect a special FTDI cable (Teledyne LeCroy PN: 929278-00) attached from the interposer to your laptop. The steps to install the cable follow:

- ❑ Ensure the interposer is powered down
- ❑ Locate the 3 pin connector for the ASIC Programming cable near the SW4 switch upper left section of the interposer (see Figure 12.82 on page 828)
- ❑ Align the cable so the SCL wire is located near the top pin, the SDA wire is located near the middle pin and the GND wire is located near the bottom pin (see Figure 12.82 on page 828)
- ❑ Push the FTDI connector onto the pins on the Interposer (see Figure 12.83 on page 829)

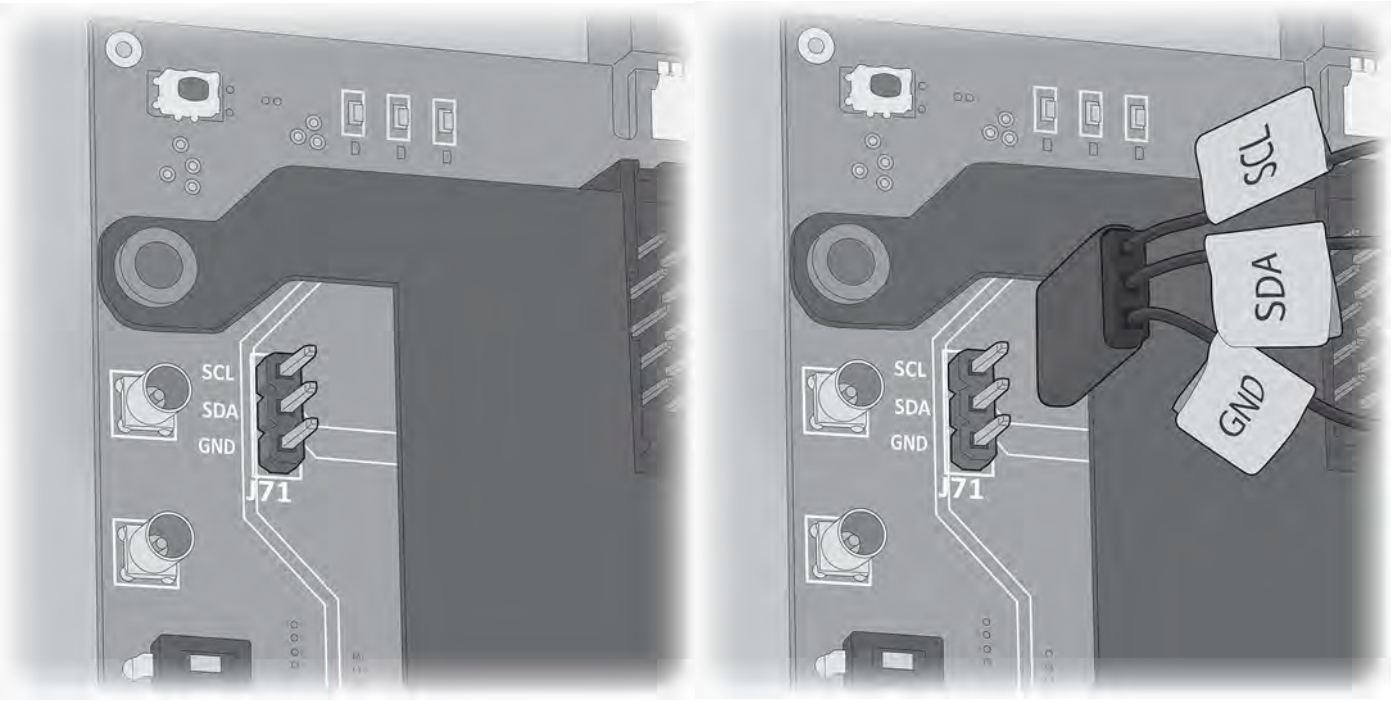


Figure 12.82: Typical Interposer: Programming Pins and Cable Ready to Attach

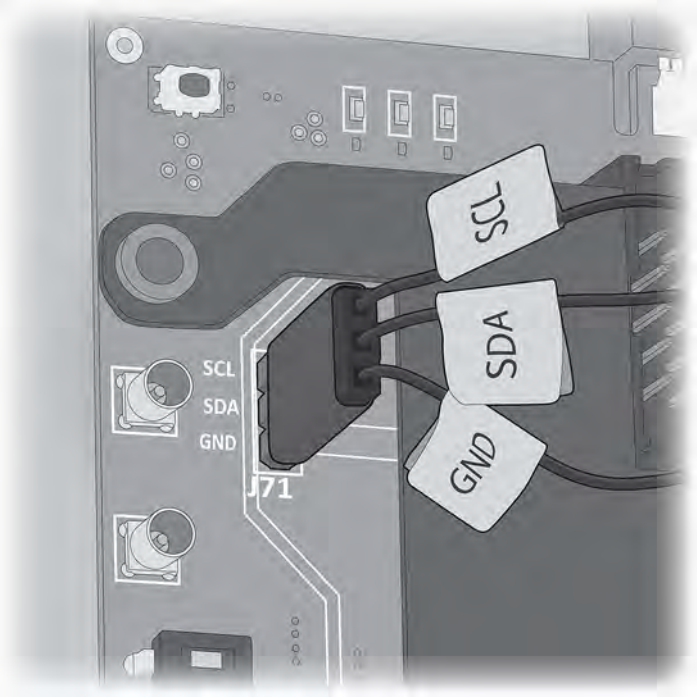


Figure 12.83: Typical Interposer: Programming Cable Attached

- ❑ After the cable has been attached to the Interposer, plug the other end of the cable into a USB connection on your laptop or computer.
- ❑ Power up the interposer.

12.27.2 Installing USB Type-C Serial Cable

- ❑ Ensure the interposer is powered down.
- ❑ Install the Type-C end of the USB cable into the corresponding USB Type-C connector on the interposer. See Figure 12.84.

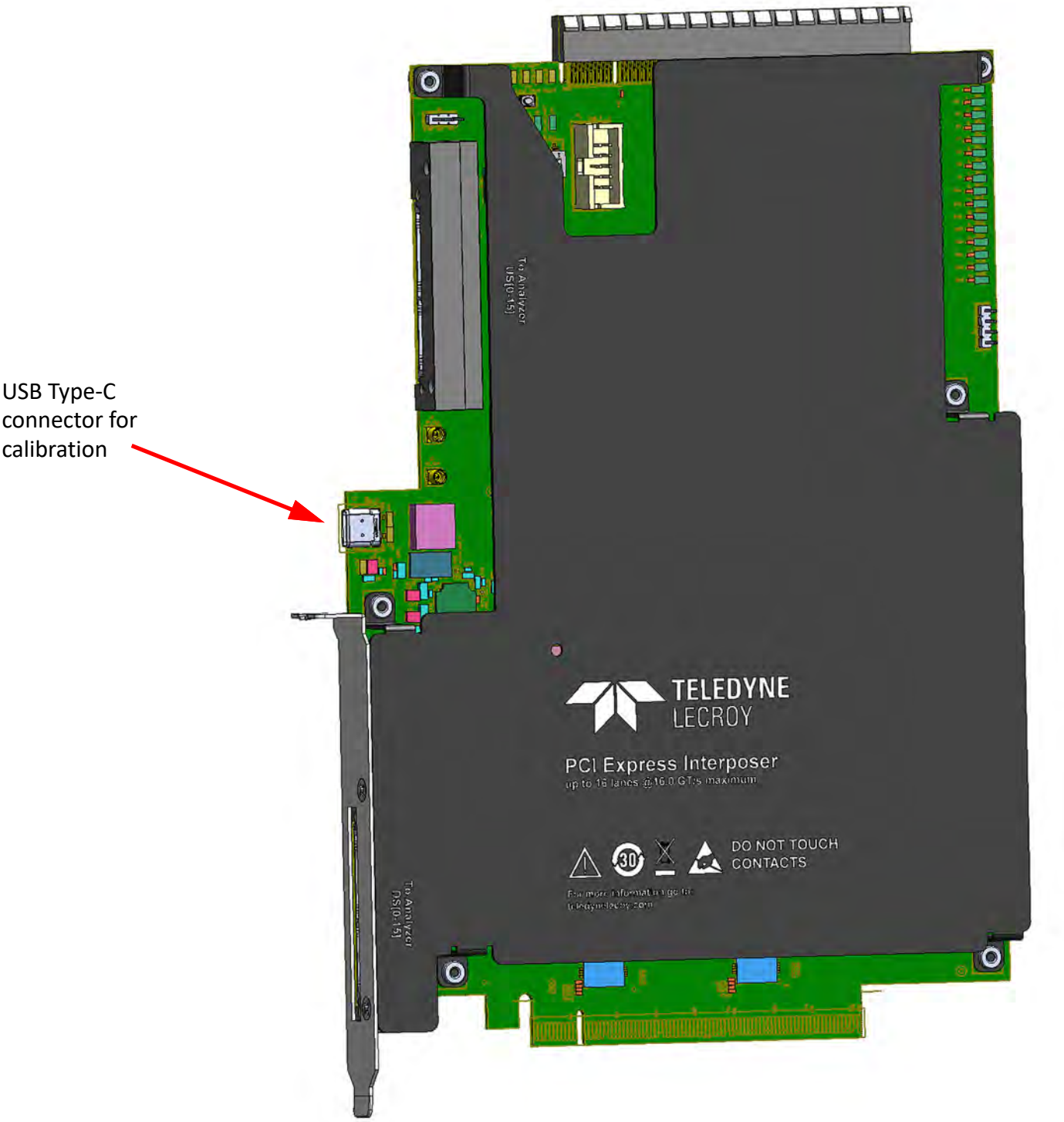


Figure 12.84: Gen4 Interposer with USB Type-C connector for calibration

- After the cable has been attached to the Interposer, plug the other end of the cable into a USB connection on your laptop or computer.
- Power up the interposer.

12.27.3 Running the PCIe Interposer ASIC Programmer Utility

The PCIe Analysis software is capable of programming Continuous Time Linear Equalization (CTLE) and DC Gain values for any interposer attached to the T4 Analyzer. To access this functionality in the Toolbar select **Tools -> Interposer Programmer**. See Figure 12.85.



Figure 12.85: Tools: Interposer Programmer

Selecting Interposer Programmer will pop up the PCIe Interposer ASIC Programmer Utility. See Figure 12.86.

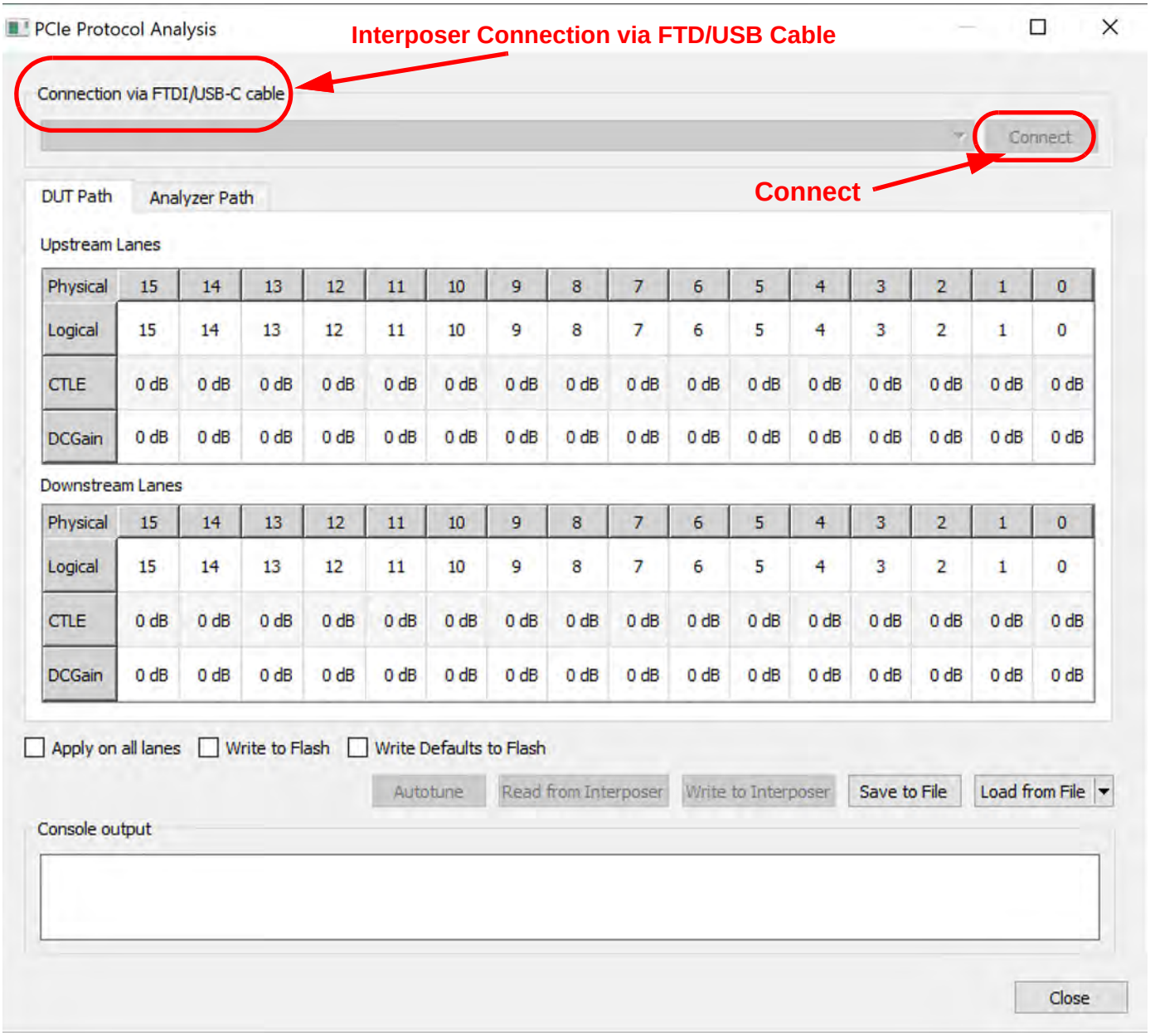


Figure 12.86: PCIe Interposer ASIC Programmer Utility

- Power on the Interposer (if not already powered up).
- Select the Connect button on the right side of the dialog box. See Figure 12.86.

The PCIe Interposer Utility will respond by detecting the Interposer and displaying the number of lanes to be programmed. See Figure 12.87 on page 833.

12.27.4 PCIe Interposer ASIC Programmer Utility Functionality

The functionality of the programmer is explained below:

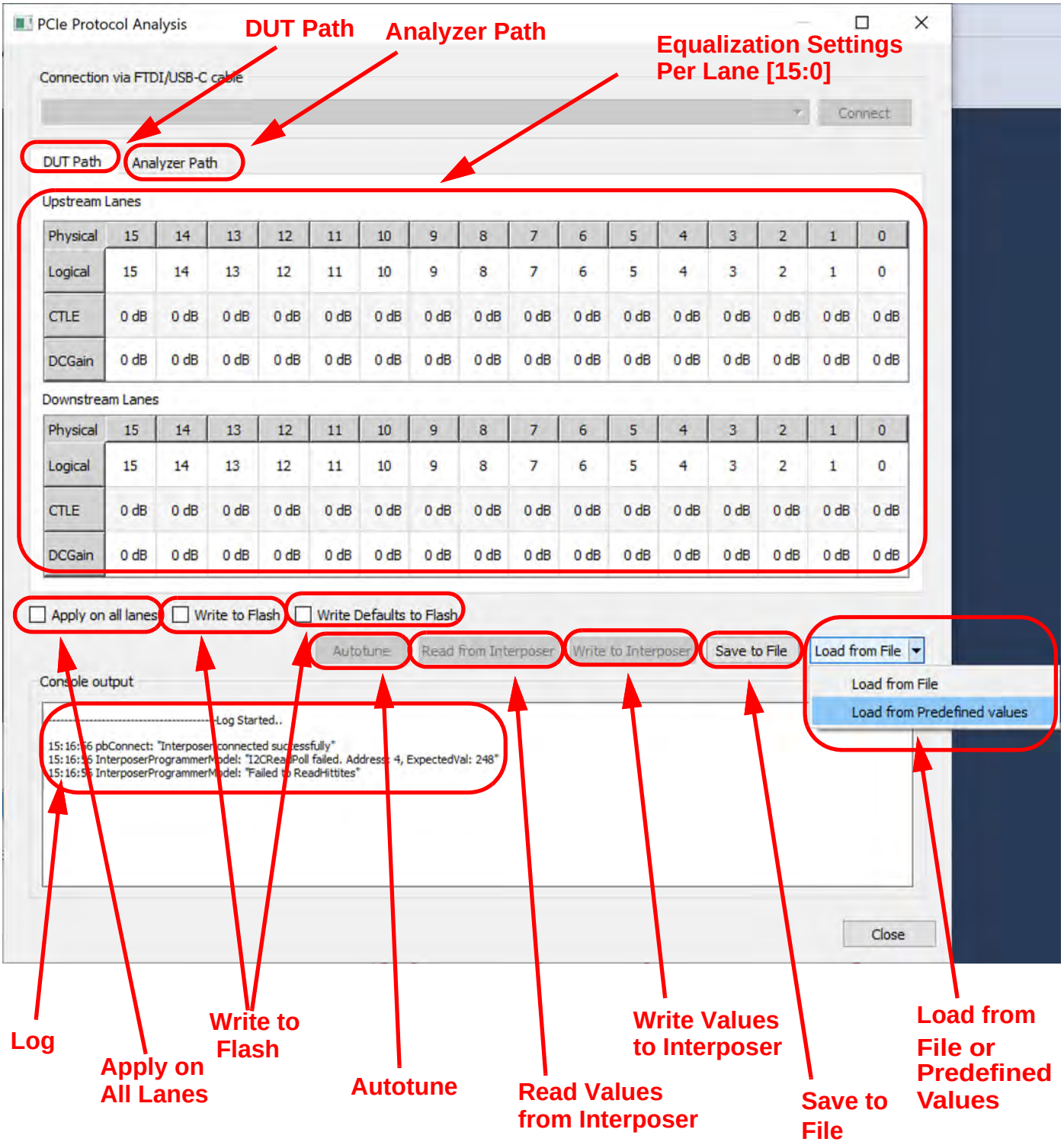


Figure 12.87: PCIe Interposer ASIC Programmer Utility Up and Running

12.27.4.1 Equalization Settings

The Equalization settings are populated for the first time when powering on.

Choose your settings for both CTLE and DC Gain for each lane and click "Write to Interposer" to write the settings to the interposer.

To read the current settings back from the interposer, click "Read from Interposer".

All settings would be reset on power-cycling the device, unless you write to flash.

Values range from 0.0 db to 6.2dB in increments of 0.2dB.

12.27.4.2 Write to Flash

Check "Write to Flash" before pressing "Write to Interposer" to write the settings and save them into Flash Memory on the interposer.

These setting would remain on the interposer even after power-cycling it.

If writing to Flash, you may optionally choose "Defaults" to write the defaults to the Flash Memory. This would restore the interposer to its default settings.

Note: Writing to Flash takes several minutes to complete. While writing is in progress, the Application title bar may show "Not Responding". This is normal and will go away after writing is complete.

12.27.4.3 Write to Interposer

Press this button to write equalization settings to the interposer.

Note: While writing is in progress, the Application title bar may show "Not Responding". This is normal and will go away after writing is complete.

12.27.4.4 Read from Interposer

Press this button to read the equalization settings from the interposer.

Note: While reading is in progress, the Application title bar may show "Not Responding". This is normal and will go away after reading is complete.

12.27.4.5 Set All Lanes

Check this box and change the values in Lane 0 to change all the values in the corresponding column.

12.27.4.6 Log

This log would also be saved in the same location as the ".exe" file. The log should provide some preliminary information about connection and display values read /written.

12.27.4.7 Save to File

You can save your settings to a file.

12.27.4.8 Load from File/Preset

You can load CTLE and DC Gain values from a file or load CTLE and DC Gain values from a Preset list of values for a specific configuration of hardware. Either from:

- Load from File: Opens a dialog box to choose a file from
- Load from Preset: Opens a dialog box with a specific configuration of hardware

See Figure 12.88 on page 835.

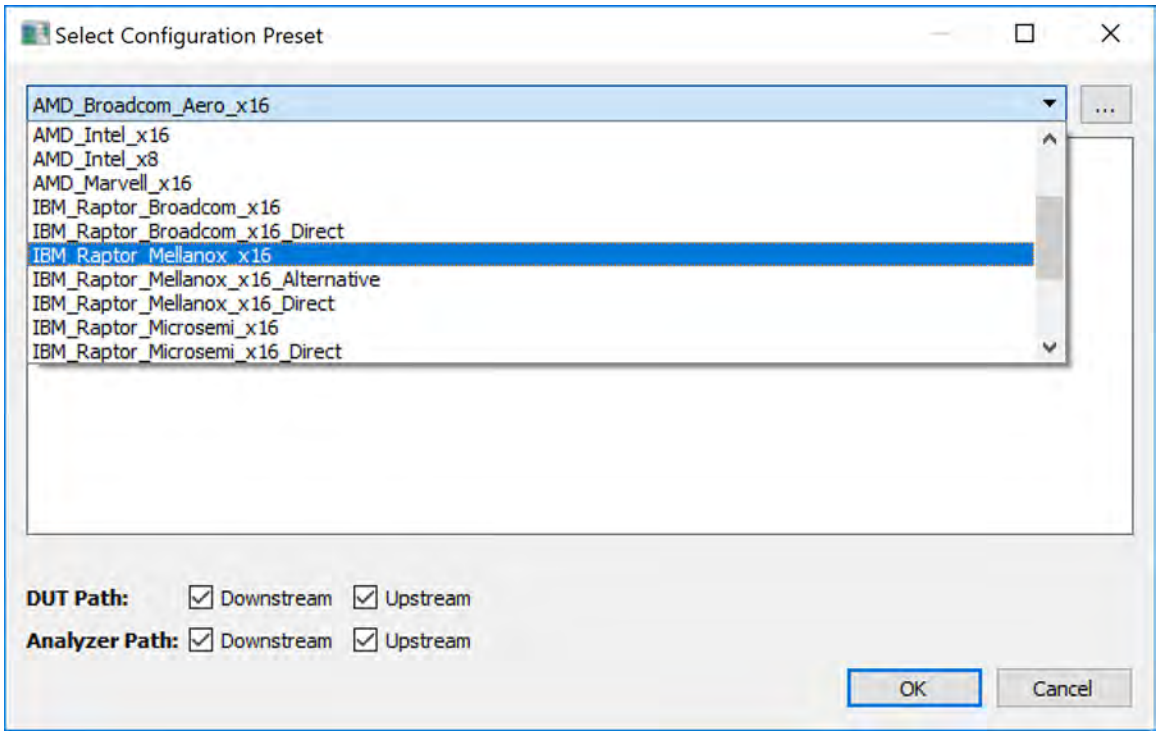


Figure 12.88: Load from Presets

In addition to setting the Equalization Values for the DUT path you can perform the same operations for the Analyzer path. See Figure 12.89 on page 836.

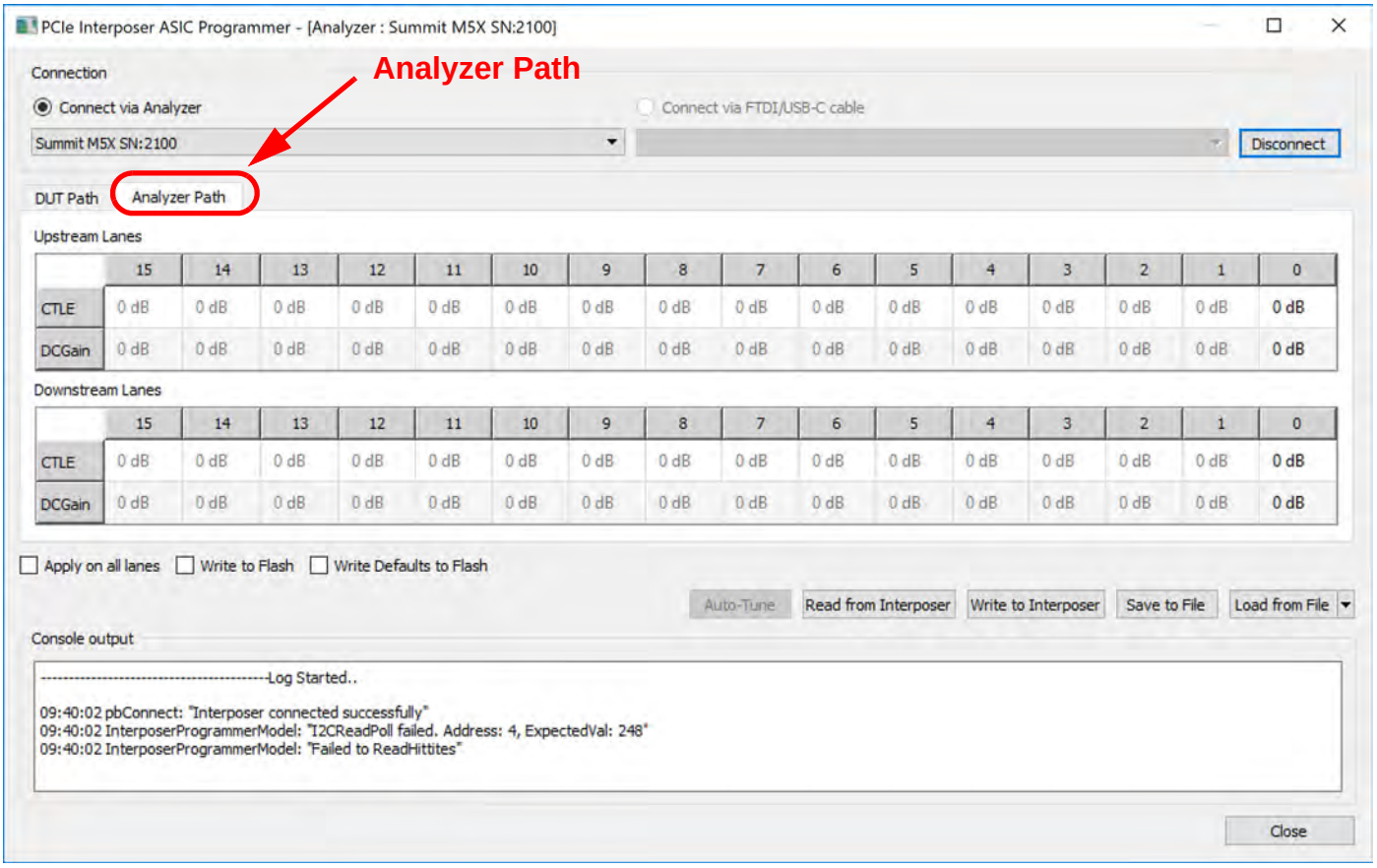


Figure 12.89: PCIe Interposer Programmer Utility for Analyzer Path

12.28 Tools -> Probe Calibration

See “Using the Autotune and Probe Calibration Wizard” on page 414.

12.29 Tools -> TC to VC Mapping

Select **Tools > TC to VC Mapping** displays how Traffic Classes are mapped to Virtual Channels (to simplify navigation) and how the CATC Trace display was changed (for example, in Split Transactions).

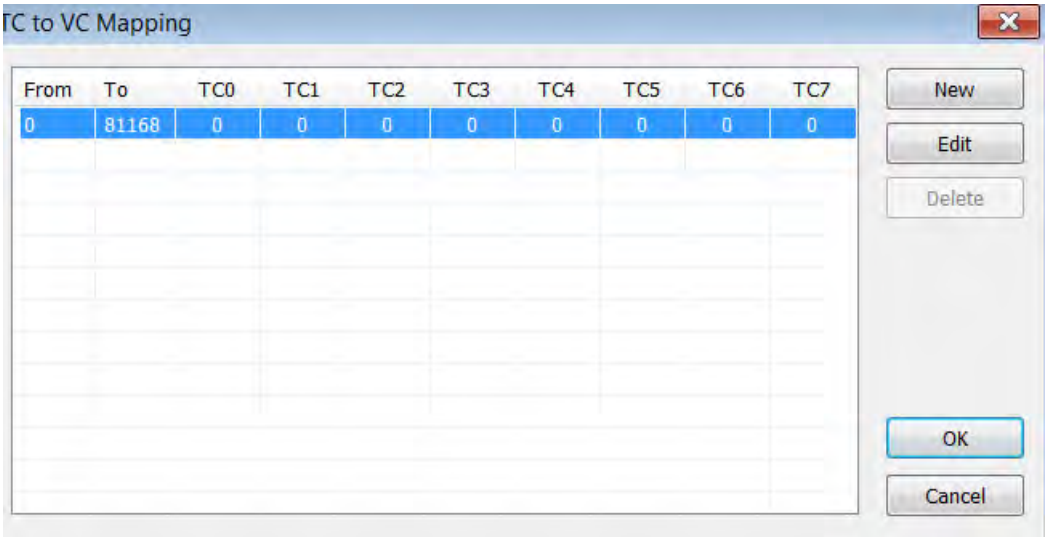


Figure 12.90: TC to VC Mapping Dialog

12.30 Tools -> Timing and Bus Usage Calculations

12.30.1 Timing Calculator

Select **Tools > Timing Calculations** to obtain the Timing Calculator dialog.

The Timing and Bus Usage Calculator calculates PCIe timings, Queue Utilization and Total Input / Output. You can decide how much of a Trace you want analyzed. You can select the segment of the Trace you want analyzed by Packet (beginning to ending), Markers (chosen from the drop down) or Time (in seconds or clocks).

In this first case, we have an NVMe Trace loaded and are looking at the entire trace from the beginning of Packet 0 to the end of Packet 1714903. See Figure 12.91.

PCIe Timing Information: Entire Trace



Figure 12.91: Timing Calculator for Entire Trace

The major portions of the PCIe Timings are discussed below:

Bus Utilization

This portion of the Timing Calculator window gives values that are cumulative for all packets during the timing period. For example, throughput is combined throughput of all packets during the timing period.

Upstream is from endpoint devices to the root complex. Downstream is from the root complex to endpoint devices.

Link Utilization: Percentage of non-idle symbols in total number of symbols transferred.

Time Coverage: Percentage of non-idle symbol times in total number of symbol times. (Non-idle symbol time occurs when at least on one of the lanes there were non-idle symbols transferred.)

Bandwidth: Number of non-idle symbol bits transferred per second.

Data Throughput: Number of TLP payload bytes transferred per second, expressed in MB per second (MB = 1024*1024 bytes).

Packets/second: Number of packets transferred per second.

Split Transaction Performance

This portion of the Timing Calculator window gives minimum, maximum, and average values for all Split transactions during the timing period. For example, minimum throughput is throughput of the Split transaction that passes the least amount of data. Maximum throughput is throughput of the Split transaction that passes the most amount of data. Average throughput is the average calculated for all Split transactions during the timing period.

Response Time: The time it took to transmit this Split transaction on the PE link, from the beginning of the first packet in the Split transaction to the end of the last packet in the Split transaction.

Latency: The time measured from the end of the request transaction to the first completion transmitted in response to the request within this Split transaction.

Throughput: The transaction payload divided by response time, expressed in megabytes per second, expressed in MB per second (MB = 1024*1024 bytes).

Memory Writes Performance

This portion of the Timing Calculator window gives minimum, maximum, and average values for all Memory Write transactions during the timing period. For example, minimum throughput is throughput of the Memory Write transaction that passes the least amount of data. Maximum throughput is throughput of the Memory Write transaction that passes the most amount of data. Average throughput is the average calculated for all Memory Write transactions during the timing period.

Response Time: The time it took to transmit this Memory Write on the PE link, from the beginning of the first packet in the Memory Write to the end of the last packet in the Memory Write.

Throughput: The Memory Write payload divided by response time, expressed in megabytes (MB) per second (MB = 1024*1024 bytes).

The Timing Calculator also has tabs for Queue Utilization and Total Input/Output. For the entire Trace the results are displayed below:

Queue Utilization

The Queue Utilization tool allows you to visualize the traffic on the submission queues (SQ) and command queues (CQ) within a time interval. The default interval is the entire trace. The graph is generated using the Calculate button at the bottom of the dialog (see Figure 12.92) below.

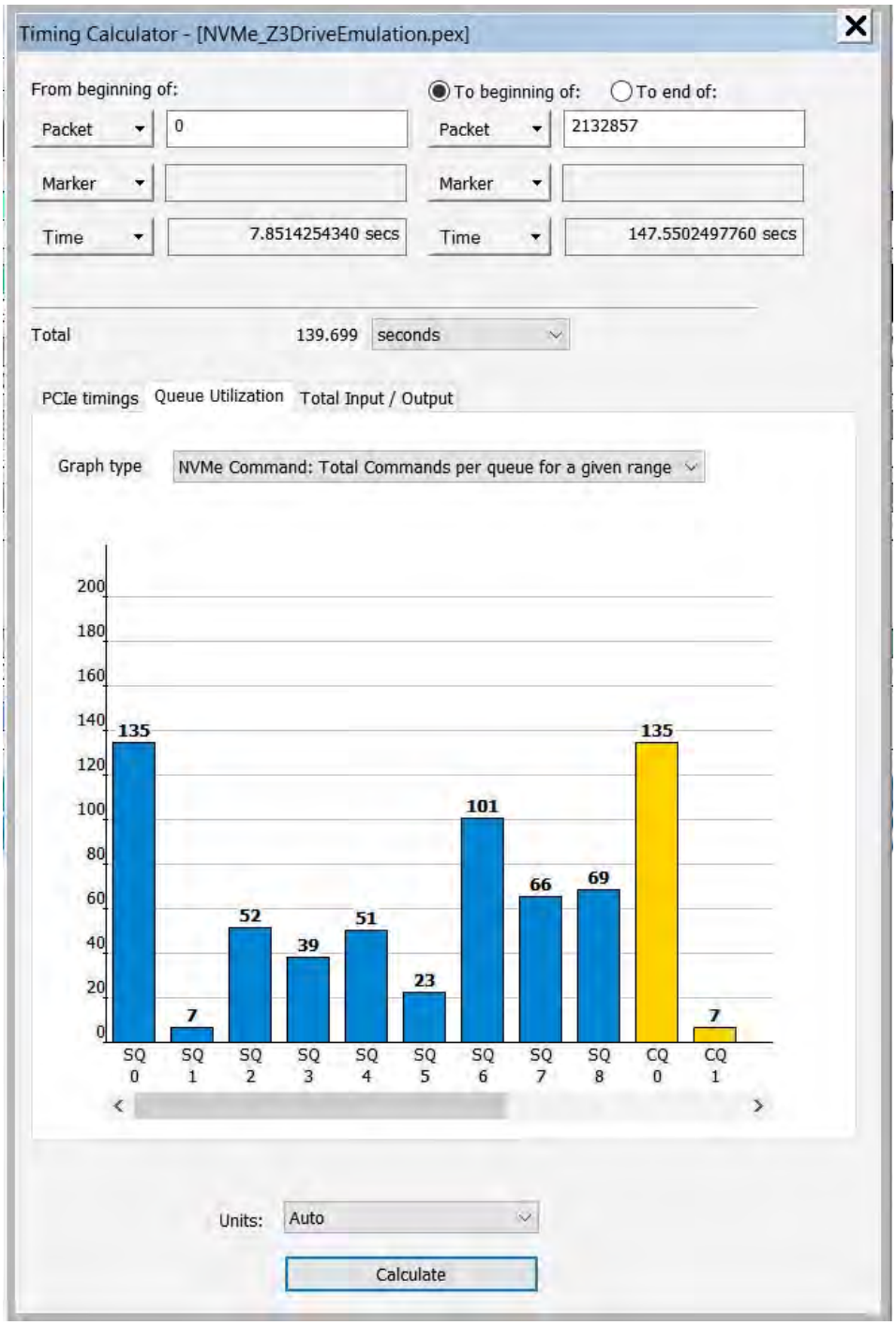


Figure 12.92: Timing Calculator: Queue Utilization

Total Input/Output

The Total Input / Output has two sections:

- Link/Split Total Traffic
- NVMe Command Total Traffic

See Figure 12.93

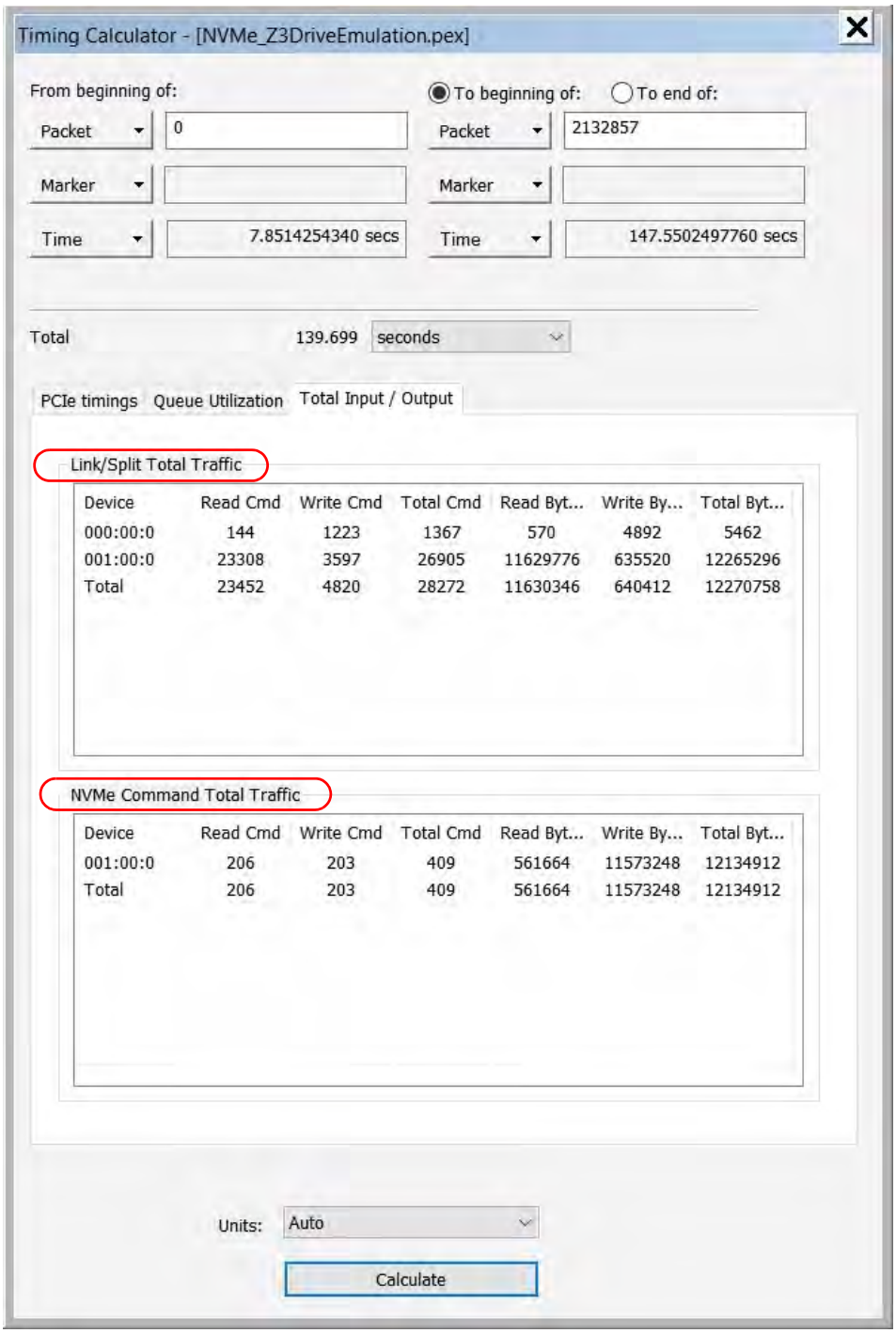


Figure 12.93: Timing Calculator: Total Input / Output

Timing Calculator Display units

The Timing Calculator can display data in several different units by selecting the appropriate combo box value and hitting the Calculate button (see Figure 12.94).

Each unit type is described in bytes or bits value, to be comparable. Auto mode will select MB or GB automatically depending on result value so that values are more readable.

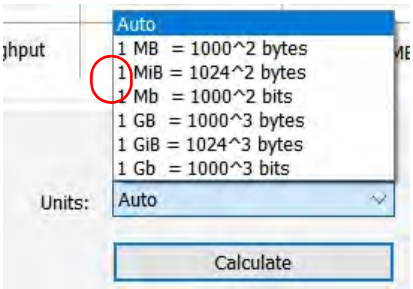


Figure 12.94: Unit selection

The results are displayed as shown below in Figure 12.95.

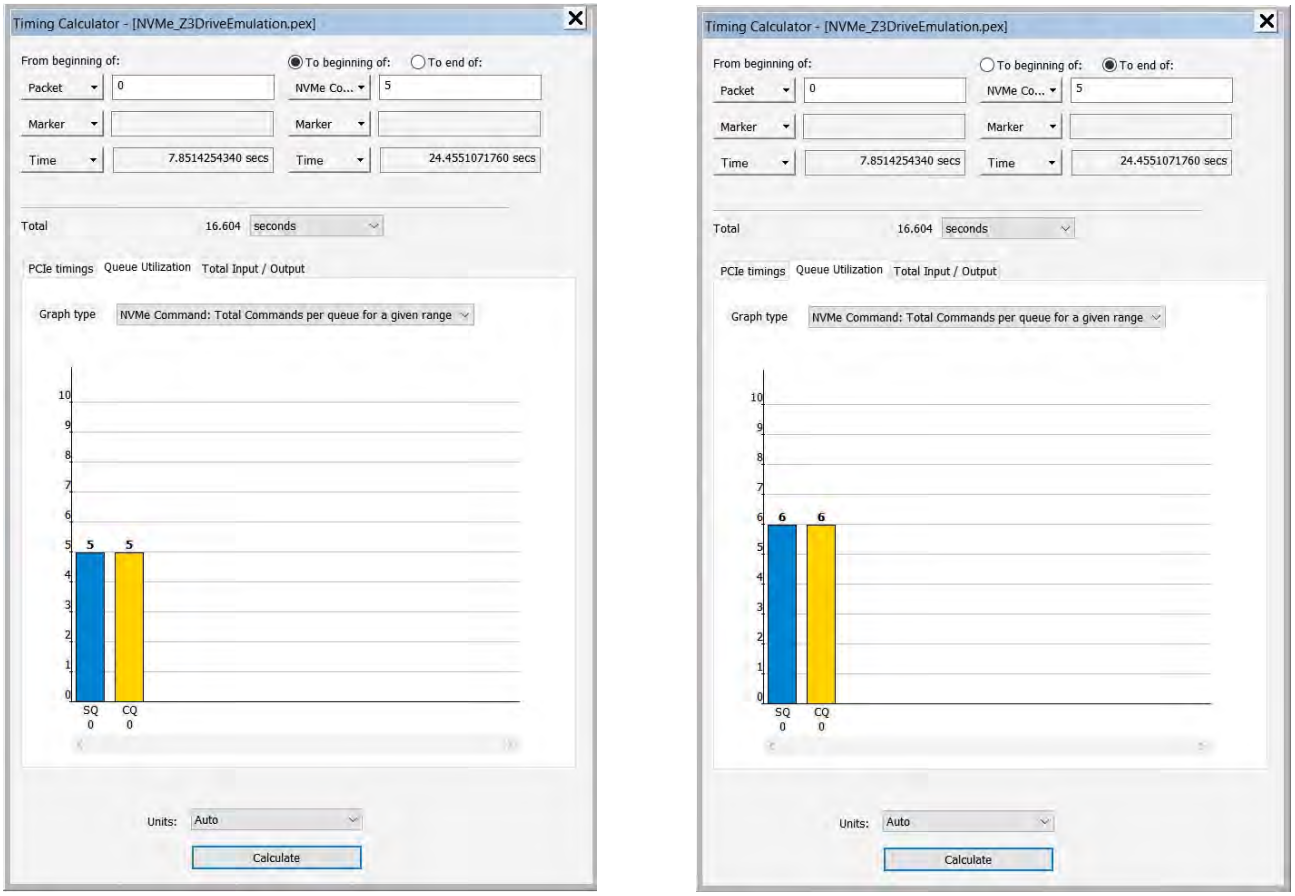


Figure 12.95: Timing Calculator: PCIe Timing Displayed in MB and Mb

12.30.2 Details of Timing Calculations

Timing From Beginning of Event to Beginning of Event or to End of Event

The Timing Calculator can calculate trace timing from the beginning of an event to either the beginning of another event or to the end of another event. See Figure 12.96.

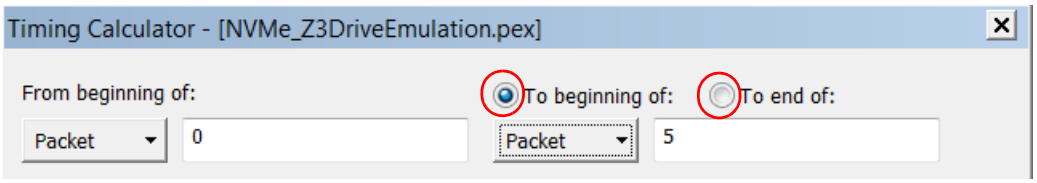


Figure 12.96: Timing Calculator: Beginning of Event to Beginning of Event or to End of Event

Types of Events

The Timing Calculator can also be used to look at specific events in more detail and has a variety of commands to help you parse the entire trace into segments of interest. The Timing Calculator can look at just Packets, Link Transactions, Split Transactions, NVMe Transactions or NVMe Commands. In this case, we have chosen NVMe Commands to explore in detail. See Figure 12.97.

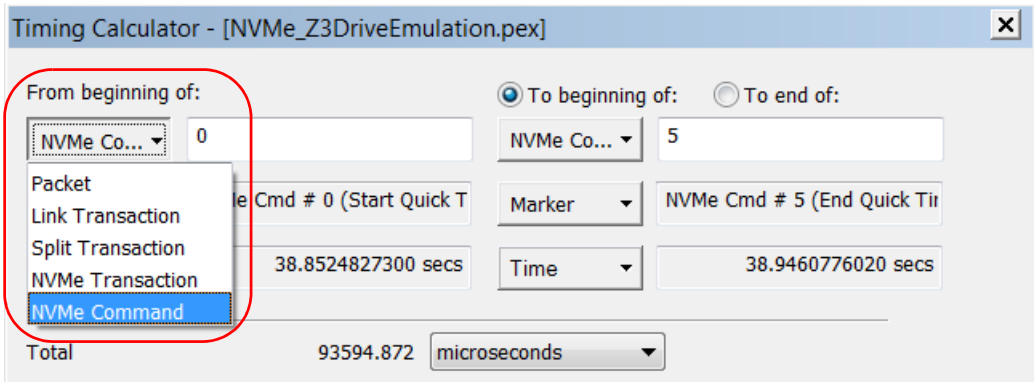


Figure 12.97: Timing Calculator: Types of Events

Displaying Time

The time can be displayed in nanoseconds, microseconds, milliseconds and seconds. See Figure 12.98.

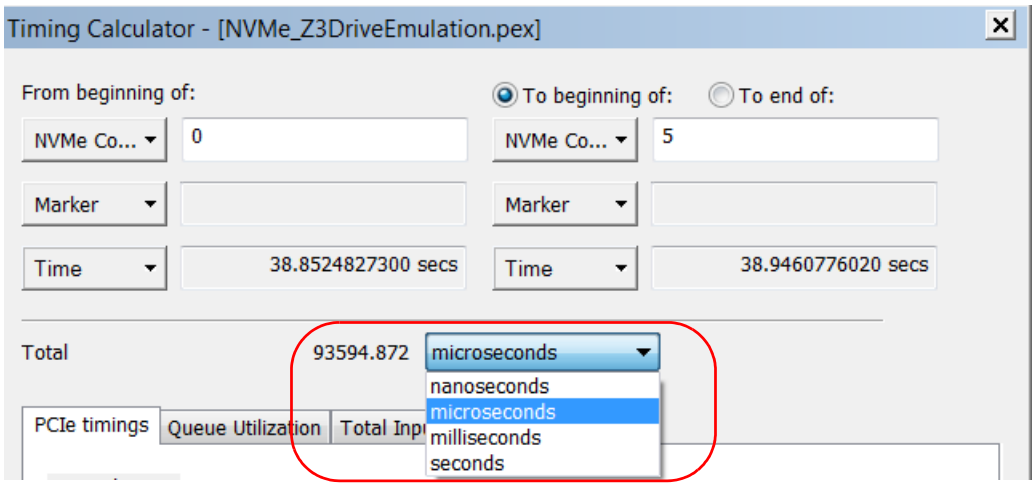


Figure 12.98: Timing Calculator: Timing Units

Markers

If Markers were set, they would be visible in the Marker pull-down (see Figure 12.99).

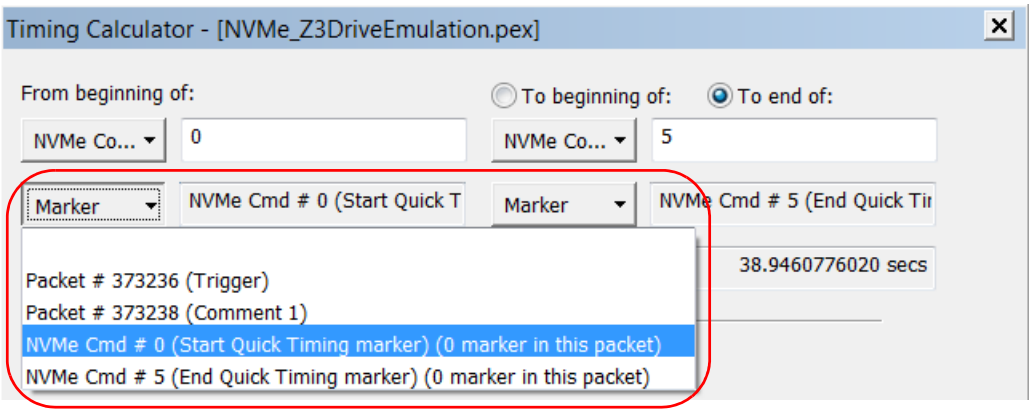


Figure 12.99: Timing Calculator: Markers Set

If the Trigger and Comment 1 Markers were chosen, the Timing Calculator would come up with the following results: see Figure 12.100 on page 846. As you can see from the results, the markers were only two packets apart.

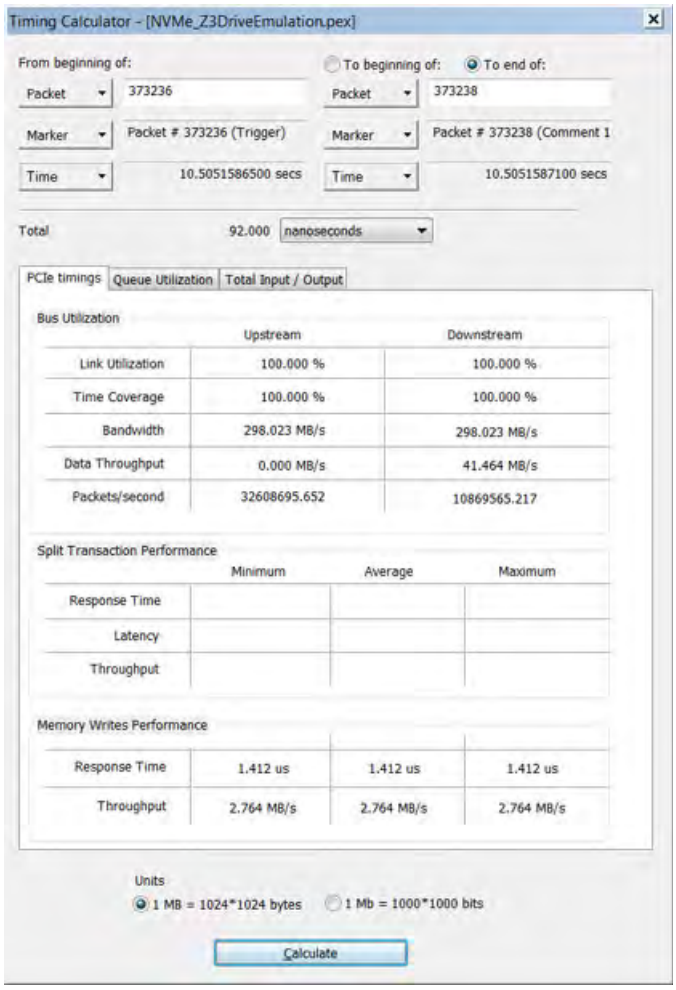


Figure 12.100: Timing Calculator: Results Between Markers

Timing To Beginning of NVMe Command

If NVMe Commands are selected the tool calculates timing information from the beginning of NVMe Command 0 to the beginning of NVMe Command 5. You can see that Total time is 93594.872 microseconds. See Figure 12.101.

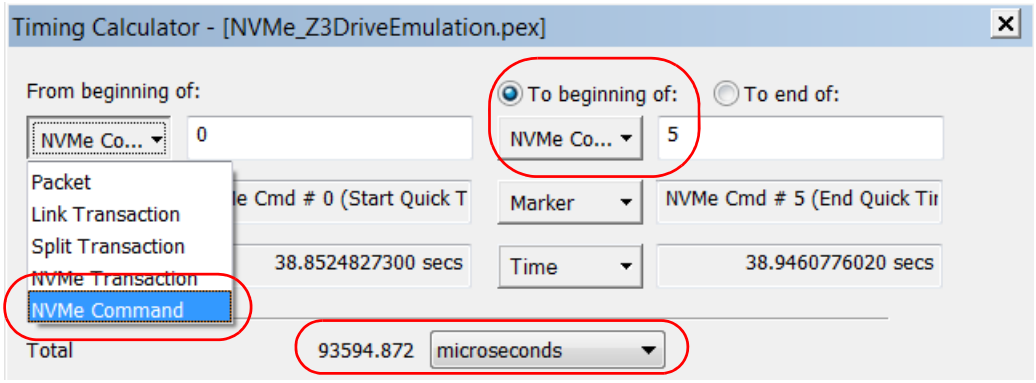


Figure 12.101: Timing Calculator: Selections for Timing Calculations

Timing To End of NVMe Command

If we had chosen to calculate the timing parameters "To end of": NVMe Command 5, the Total time would have included the NVMe Command 5 and the Total time is 93594.968 microseconds. See Figure 12.102 on page 847.

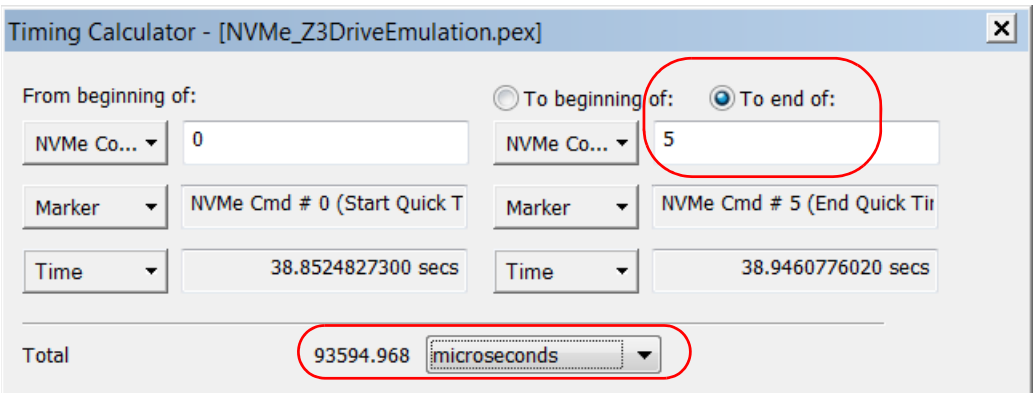


Figure 12.102: Timing Calculator: To end of NVMe Command 5

Results from Timing Calculator

The differences between the Timing Calculator results from the beginning of NVMe Command 0 to the beginning of NVMe Command 5 and to the end of NVMe Command 5 can be seen in Figure 12.103.

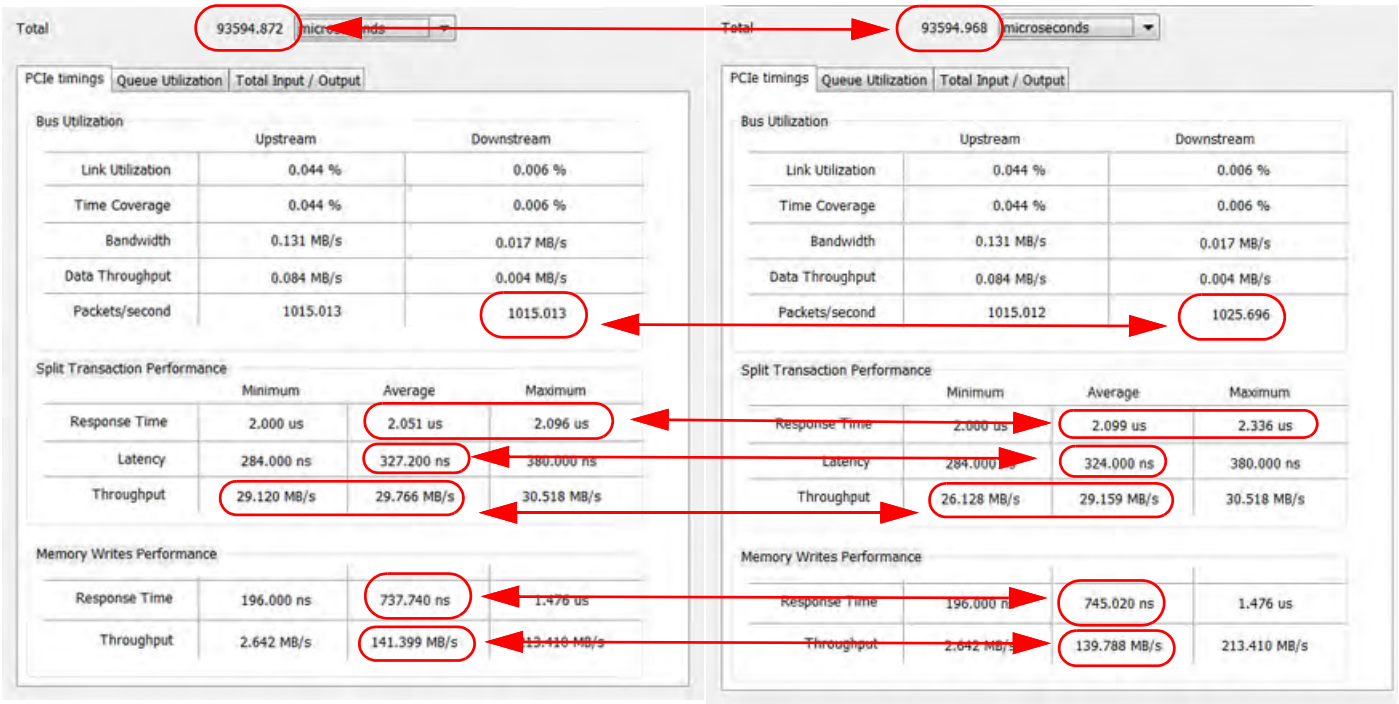


Figure 12.103: Timing Calculator: Beginning of NVMe Cmd 5 and Ending of NVMe Cmd 5 (MB)

Most of the results are the same except for Total time, Downstream Packets/second, Split Transaction Performance (Response Time, Latency and Throughput) and Memory Write Performance (Response Time: Average and Throughput: Average).

Timing to Beginning and End of Events: Effect on Queue Utilization

If we look at the differences between the Queue Utilization from the beginning of NVMe Command 0 to the Beginning of NVMe Command 5 and to the Ending of NVMe Command 5 you'll see one more NVMe Command in the Queue. See Figure 12.104.

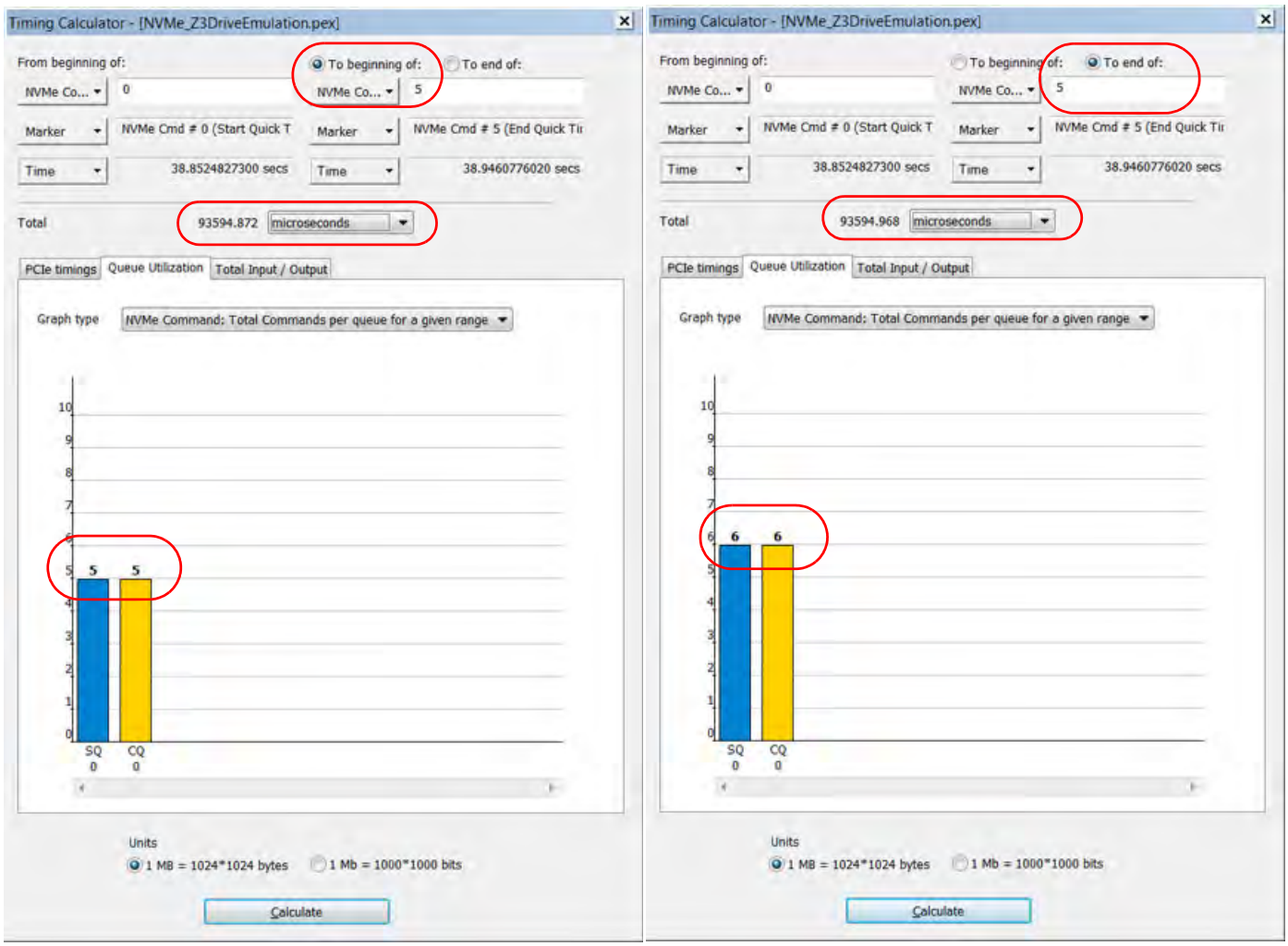


Figure 12.104: Timing Calculator: Queue Utilization

Timing to Beginning and End of Events: Effect on Total Input / Output

If we look at the differences between the Total Input / Output graphs from the beginning of NVMe Command 0 to the Beginning of NVMe Command 5 and Ending of NVMe Command 5 you'll see one more Write Command. See Figure 12.105.

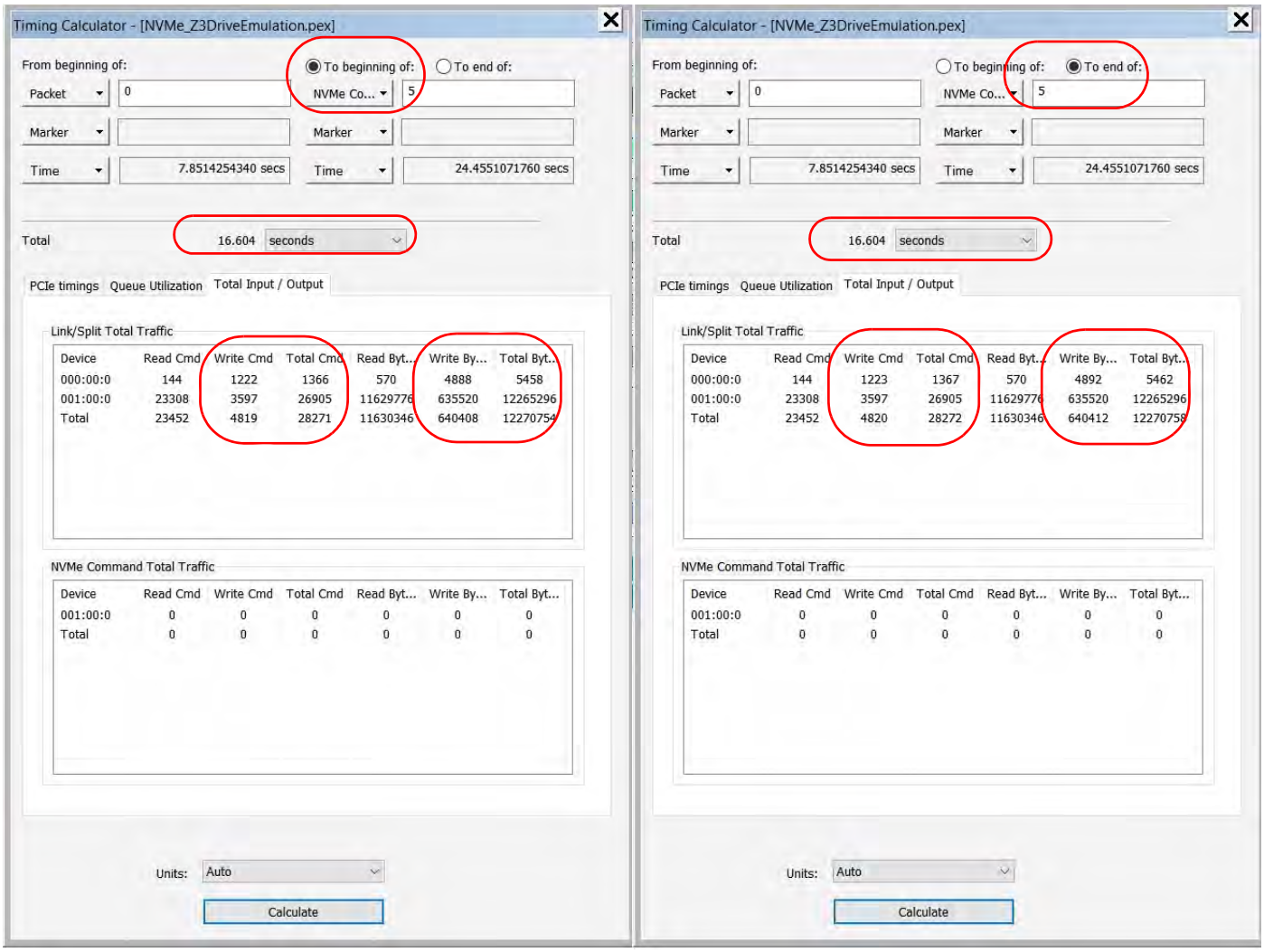


Figure 12.105: Timing Calculator: Differences in Total Input / Output

The two displays show that including NVMe Command 5 adds one more Write Command and it's associated number of bytes.

12.31 Tools -> PCIe SSD Base Address Mapping

In order for NVMe, PQI, AHCI, ATA, SOP and SCSI decoding to work correctly, the PCIe Protocol Analysis needs to know the Memory Base Address of the device.

If the Base Address assignment is not present in the trace, you can specify the values manually using this dialog. You need to select the type of the device (NVMe, PQI, AHCI, ATA, SOP or SCSI) and set the value of the Base Address by selecting **Tools > PCIe SSD Base Address Mapping.** See Figure 12.106.

12.31.1 Base Address Not Recorded in Trace

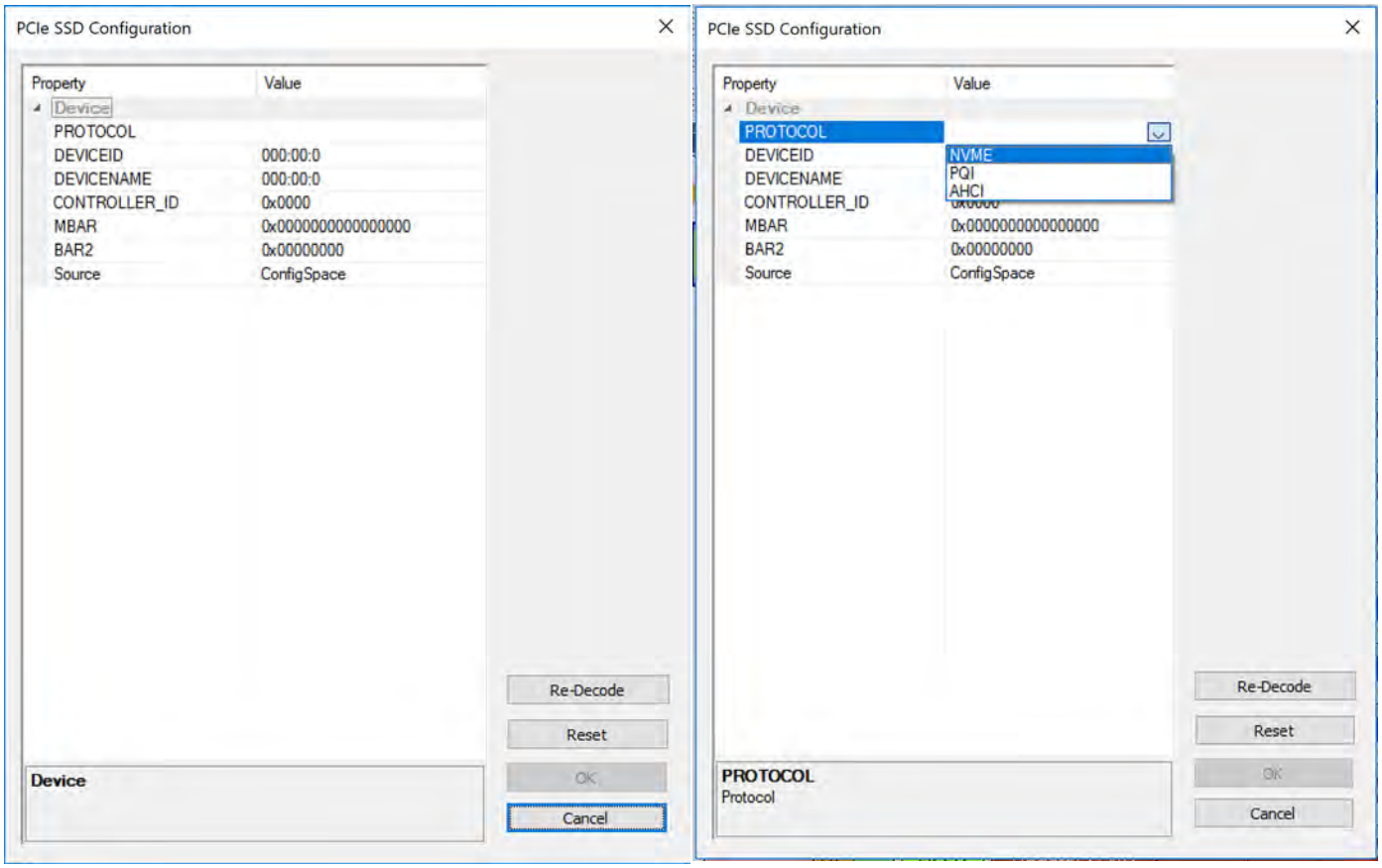


Figure 12.106: Trace without Protocol Type Specified

You must select the type of trace your recorded. In this case we selected NVME and the PCIe SSD Configuration dialog box is fully populated with all the NVME. See Figure 12.107 on page 851.

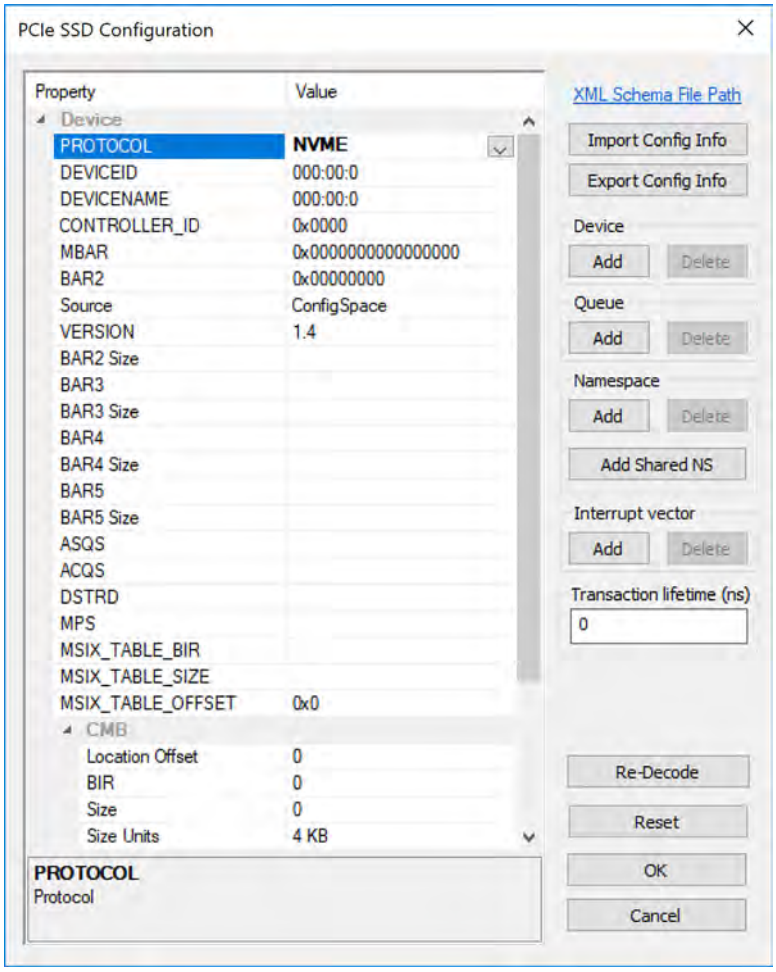


Figure 12.107: PCIe SSD Configuration dialog box populated with NVME options

12.31.2 Base Address Recorded in Trace

In cases when Base Address assignment is recorded in the trace, the software will determine all the values automatically. The PCIe SSD Configuration dialog displays (see Figure 12.108 on page 854).

Note: From software release 6.63 onwards, users are able to decode NVMe/PQI traces which are lacking configuration space and administration information, from release 6.70 this is applicable to AHCI traces, from release 7.00 this is applicable to ATA traces and from release 7.10 this is applicable to SOP and SCSI traces.

Note: From software release 7.30 onwards, multiple NVMe devices can be decoded from the same trace.

Note: From software release 7.34 onwards, the SSD Dialog displays the Device Name as read in the configuration accesses.

Note: From software release 7.38 onwards, while the SSD Dialog is open, the Trace View is scrollable.

Follow the steps below to perform the applicable storage decoding:

1. Record the trace for NVMe, PQI, AHCI, ATA, SOP or SCSI device boot and decode it.
   This saves the configuration space and administration information in .xml format, which is used to decode traces that do not include configuration and administration commands.
2. Record the trace of the same NVMe, PQI, AHCI, ATA SOP or SCSI device without rebooting and the application will decode it.

You can keep recording and decoding until rebooting. On reboot repeat steps 1 and 2 above.

12.31.3 NVMe PCIe SSD Device Configuration

The PCIe SSD Configuration dialog is used to add missing information to decode the trace without the configuration space and queue administration information. See Figure 12.108 on page 854 for NVMe PCIe SSD Device Configuration.

Prior to decoding, if all the required information is available in Configuration Space then the Source field in the PCIe SSD Configuration will be set to "Config Space" (see Figure 12.108 on page 854). The description for important fields and buttons are given below:

1. DEVICE ID: Represents the device ID in the bus/device/function address from the PCIe specification (ID Based routing).
2. DEVICENAME: Device Name
3. MBAR: The MBAR field in this dialog is required and editable. Make sure that the information entered is correct. Click on any field and the description displays in the bottom read-only box. The 64-bit main address bar (i.e. BAR1:BAR0). Without this value decoding cannot be done. It should be in "0x" hex format.
4. BAR2:
5. PROTOCOL: Displays the current storage protocol decoded.
6. ASQS: Defines the size of the Admin Submission Queue in entries. Refer to the controller registers section of the NVMe specification. The minimum size of the Admin Submission Queue is two entries. The maximum size of the Admin Submission Queue is 4096 entries. This is a 0’s based value.
7. ACQS: Defines the size of the Admin Completion Queue in entries. Refer to the controller registers section of the NVMe specification. The minimum size of the Admin Completion Queue is two entries. The maximum size of the Admin Completion Queue is 4096 entries. This is a 0’s based value.
8. DSTRD: This register indicates the stride between doorbell registers. The stride is specified in bytes. This may be used to separate doorbells by a number of bytes in memory space. It may be useful in software emulation of an NVMe Express controller. For hardware implementations of NVMe Express, the expected doorbell stride value is 4.
9. LBASIZE: Size for Logical Block Addressing.

10. MPS: This field indicates the host memory page in bytes.
11. IOCQES: I/O Completion Queue Entry Size. This field defines the I/O Completion Queue entry size that is used for the selected I/O Command Set. The required and maximum values for this field are specified in the Identify Controller data structure for each I/O Command Set. The value is in bytes and is specified as a power of two (2^n).
12. IOSQES: I/O Submission Queue Entry Size. This field defines the I/O Submission Queue entry size that is used for the selected I/O Command Set. The required and maximum values for this field are specified in the Identify Controller data structure for each I/O Command Set. The value is in bytes and is specified as a power of two (2^n).
13. MQES: Maximum Queue Entries Supported. Defines the maximum individual queue size that the controller supports. This is a 0's based value. The minimum value is 1h, indicating two entries.
14. Source: Source of the data.
15. Queues: Under this node the user can add more missing nodes to decode the current trace. Click the **Add Queue** or **Delete Queue** button to add or delete a queue node. Type based on the user selection.
16. XML Schema File Path: Selecting this link pops up a window with the location of the XML Schema File. It is also available in TechBrief_Use_of_NVMe_xml_schema.pdf in the installation AppNotes\ directory (or installation path).
17. Import Config Info: Click to Import configuration information.
18. Export Config Info: Click to Export configuration information.
19. Add Device/Delete Device: Click to add/delete device (NVMe/PQI only).
20. Add Queue/Delete Queue: Click to add/delete queue (NVMe/PQI only).
21. Add Namespace/Delete Namespace: Click to add/delete a new namespace if this information is not present in a trace file (NVMe/PQI only).
22. Interrupt Vector: Add/Delete an Interrupt Vector to a selected Device (see "Interrupts" on page 855).
23. Re-Decode: Click to re-decode.
24. Reset: Click to reset.
25. OK: Click to accept the settings.
26. Cancel: Click to cancel the settings.

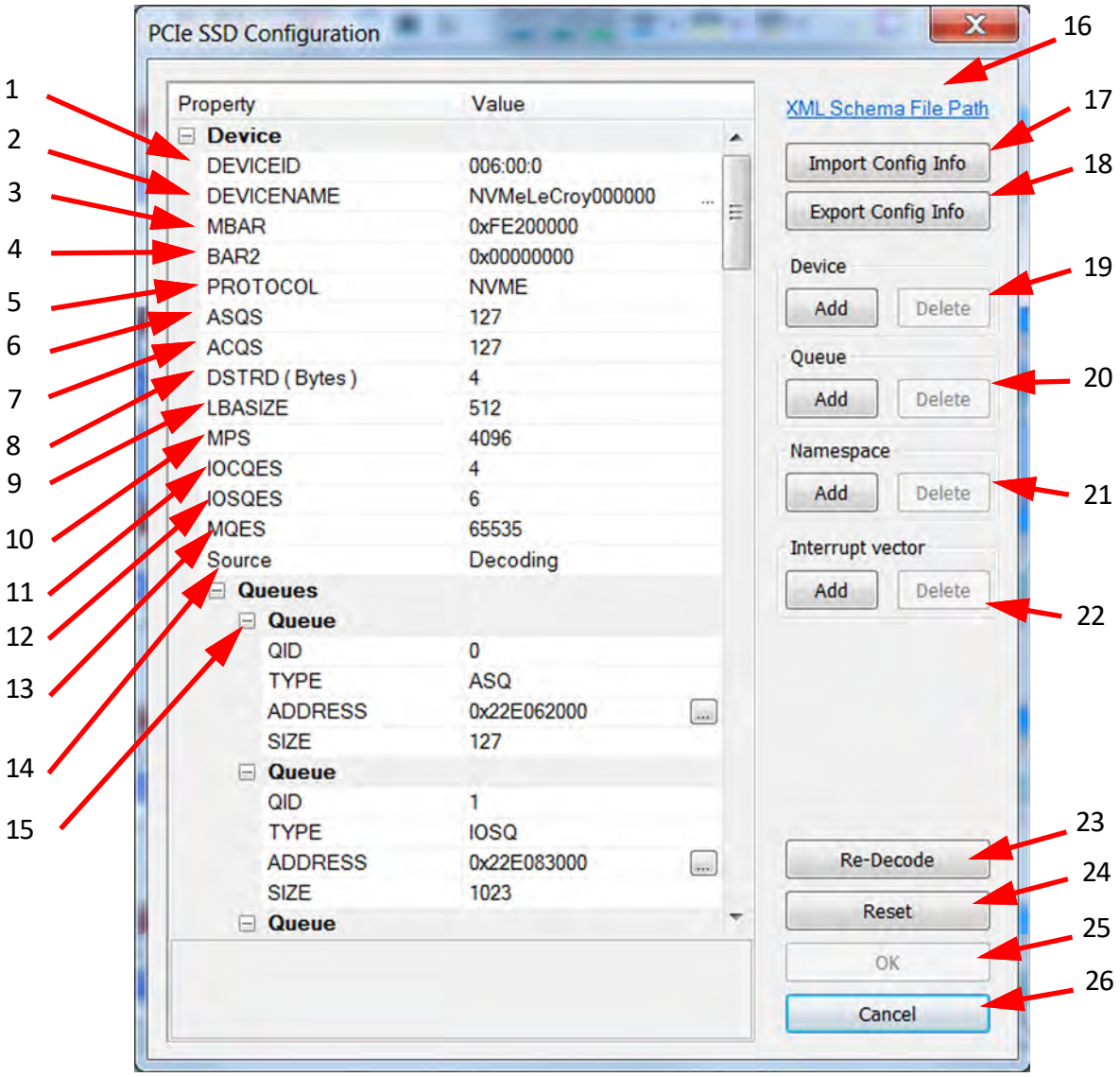


Figure 12.108: PCIe SSD Configuration Dialog Pre-decoding

Select any of the options in the 

drop down menu item to decode the trace and select **Tools > PCIe SSD Base Address Mapping** (see Figure 12.110).

Note: When opening a trace file created with 7.0X or older versions of PCIe Protocol Analysis, these new fields are not present and the application tries to export the configuration information to XML before decoding NVMe transaction level. In this case a message box will show claiming that a value for this field is required.

Note: In case of problems when opening older traces try the following: a) Decode NVMe transaction level before exporting XML file. This will apply the default value for the new fields and export can be performed. b) Manually enter the values for the new fields. c) In case the trace contains submission entries which are not decoded, add a new Queue and set the corresponding address in the PCIe SSD Configuration dialog.

Interrupts

MSI and MSI-x interrupts are decoded at configuration time and include the vector offset and address. These values can be added/deleted/modified by the user to add data that may not have been captured in the trace.

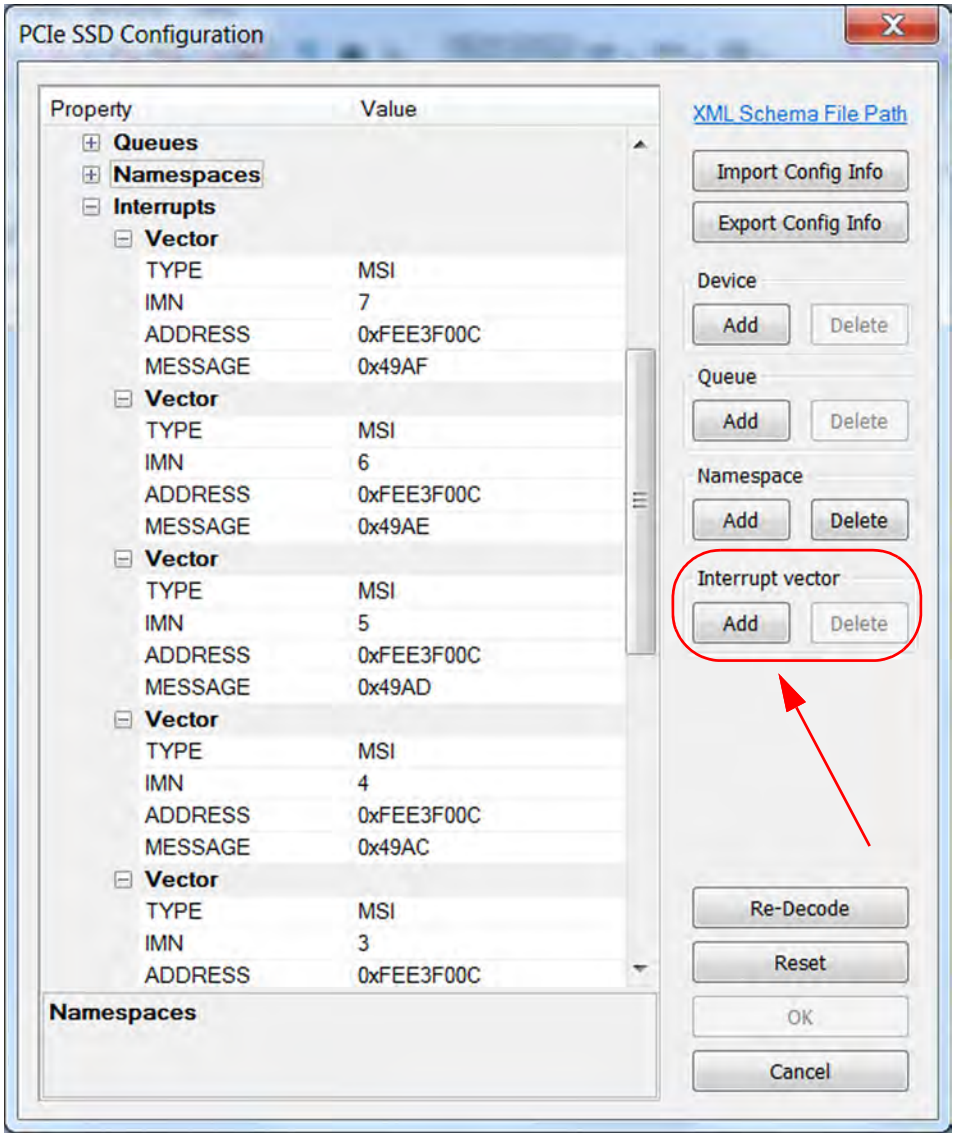


Figure 12.109: MSI and MSI-x Interrupts

12.31.4 AHCI PCIe SSD Device Configuration

The PCIe SSD Configuration dialog is used to add missing information to decode the trace without the configuration space and queue administration information. See Figure 12.110 for AHCI PCIe SSD Device Configuration.

Prior to decoding if every thing is available in Configuration Space then Source equals Config Space (see Figure 12.110).

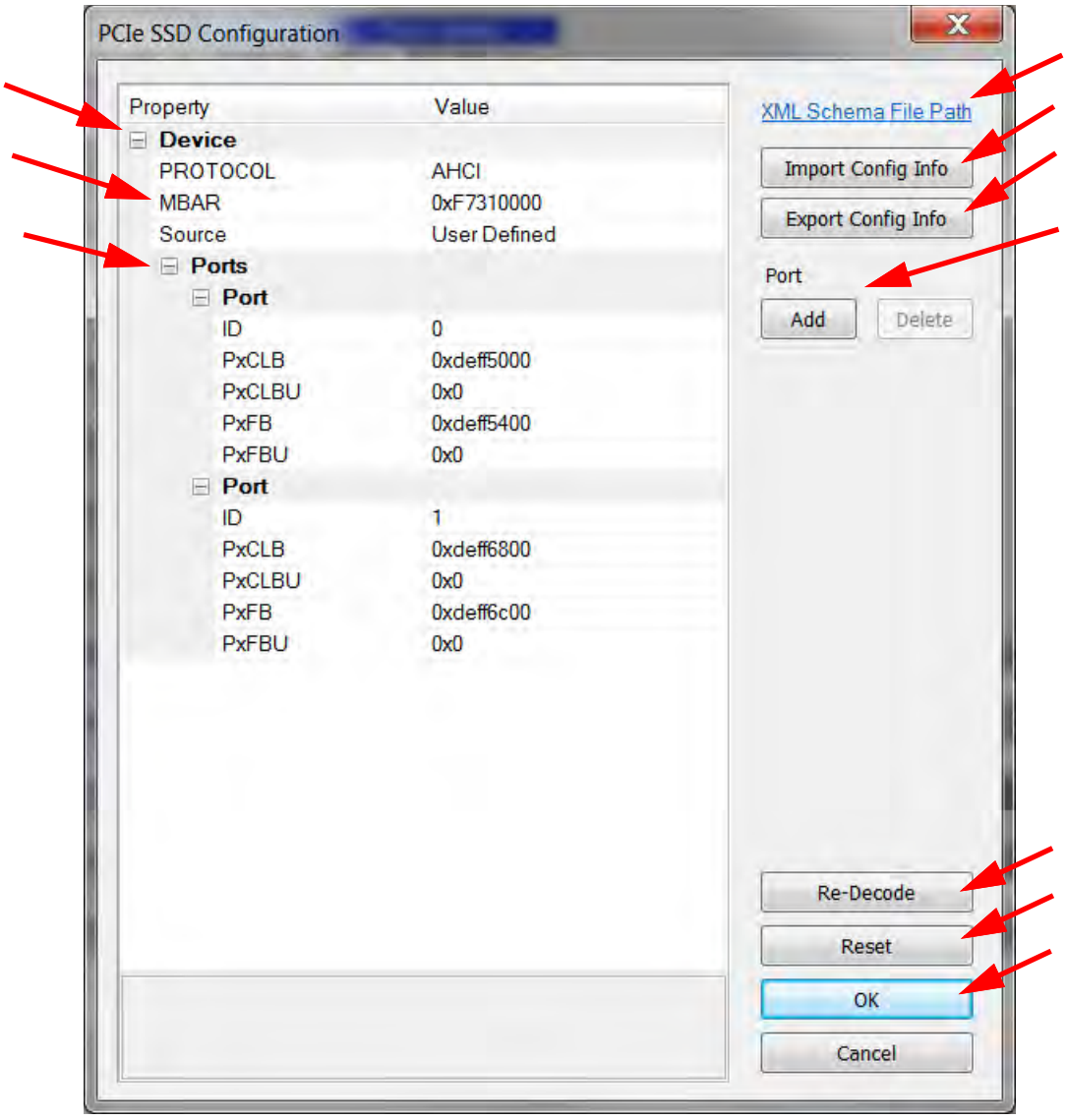


Figure 12.110: AHCI PCIe SSD Configuration Dialog

The MBAR field in this dialog is required and editable. Make sure that the information entered is correct. Click on any field and the description displays in the bottom read-only box (see Figure 12.112 on page 859). Some important fields are described below:

- Device: There is only one device node, (support for multiple device trace decoding will be available in a later release).
- MBAR: The 64-bit main address bar (i.e. BAR1:BAR0). Without this value decoding cannot be done. It should be in "0x" hex format.
- Ports: Under this node the user can add more missing nodes to decode the current trace. Click the **Add Port** or **Delete Port** button to add or delete a port node. Enter CLB, CLBU and FB, FBU address fields. The address is 32 bit and should be in "0x" hex format. Please use the right value for size as it is an important attribute. Consult the AHCI specifications for the correct value.

Clicking the **Re-Decode** button erases the current configuration from this dialog box and attempts to re-decode based on the information present in the open trace and/or saved on the disk with the last decode.

Click the **Import Config Info** button to import the configuration information as an .xml file, instead of adding it individually. Click the hyper-link **XML Schema File Path** to access the required format to generate the .xml file. This schema provides the detailed format for the imported file. All modern languages are equipped to generate an .xml file on a specific xml schema. The driver software accepts this schema and generates the .xml file with all the required information.

Click the **Export Config Info** button to export the configuration information as an .xml file.

Click the **Reset** button to reset the values to the original values. Press the **OK** button to save all the values.

12.31.5 PQI PCIe SSD Device Configuration

The PCIe SSD Configuration dialog is used to add missing information to decode the trace without the configuration space and queue administration information. See Figure 12.111 for PQI PCIe SSD Device Configuration.

Prior to decoding if every thing is available in Configuration Space then Source equals Config Space (see Figure 12.111).

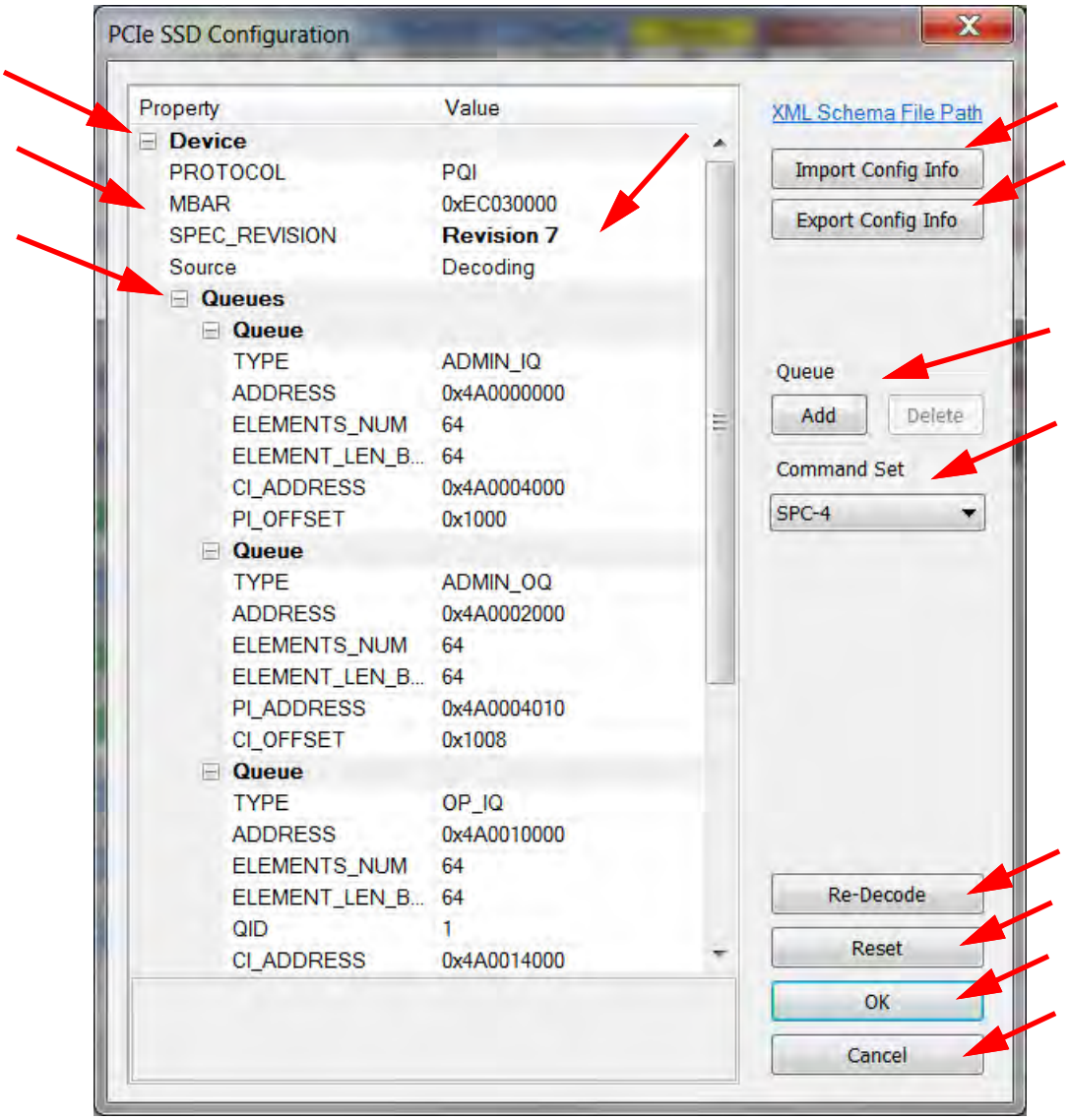


Figure 12.111: PQI PCIe SSD Configuration Dialog Pre-decoding

All the fields in this dialog are required and editable. Make sure that the information entered is correct. Click on any field and the description displays in the bottom read-only box (see Figure 12.112). Some important fields are described below:

- **Device**: There is only one device node, (support for multiple device trace decoding will be available in a later release). You can choose the spec revision from the drop down list.
- **MBAR**: The 64-bit main address bar (i.e. BAR1:BAR0). Without this value decoding cannot be done. It should be in "0x" hex format.
- **Queues**: Under this node the user can add more missing nodes to decode the current trace. Click the Add Queue or Delete Queue button to add or delete a queue node. Type based on the user selection. The following Node types are known.

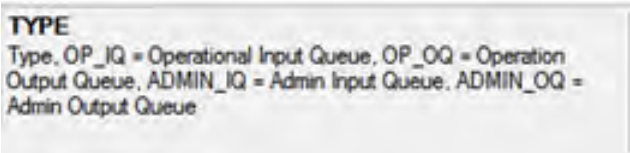


Figure 12.112: Node Types

The address is 64-bit and should be in "0x" hex format. Please use the right value for each size as it is an important attribute. Consult the NVMe specifications for the correct value. Clicking the **Re-Decode** button erases the current configuration from this dialog box and attempts to re-decode based on the information present in the open trace and/or saved on the disk with the last decode.

Click 

button to decode the trace and select **Tools > PCIe SSD Base Address Mapping** (see Figure 12.111 on page 858).

The two figures figure below show the BAR information for PQI and AHCI. If this information is present in the trace then it is not editable, otherwise it can be edited. Decoding is done only when configuration space and administration information is available.

Note: Only one device should be marked with the appropriate BAR, multiple BARs do not work.

12.31.6 SCSI PCIe SSD Device Configuration

The PCIe SSD Configuration dialog is used to add missing information to decode the trace without the configuration space and queue administration information. See Figure 12.113 on page 860 for SCSI PCIe SSD Device Configuration. The base is the same as PQI Device Configuration but you can additionally choose the SCSI Command Set.

Prior to decoding if every thing is available in Configuration Space then Source equals Config Space (see Figure 12.113 on page 860).

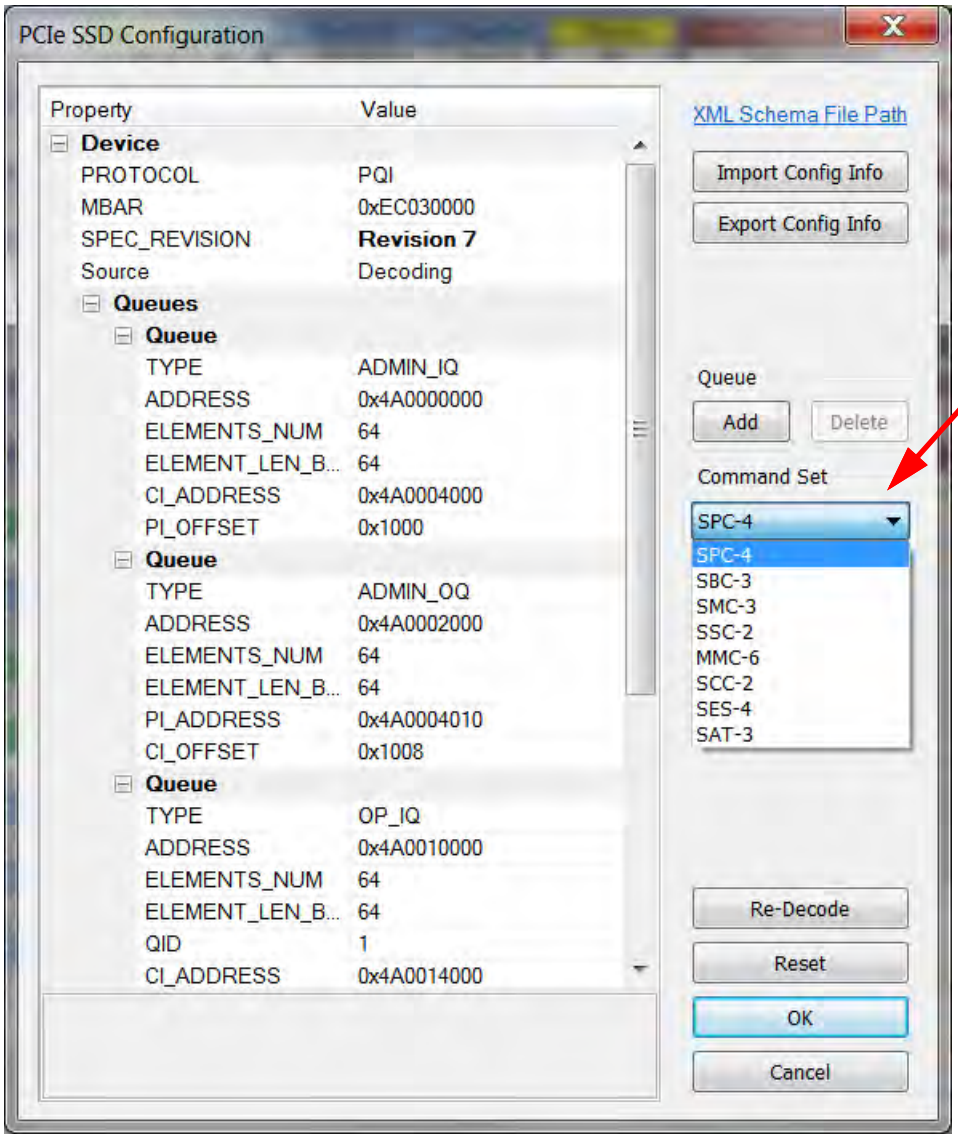


Figure 12.113: PCIe SSD Configuration Dialog - SCSI

See “Example of XML File Format for SSD Decodes” on page 879 for a template of the XML files.

12.32 Tools -> Running Verification Scripts

You can run verification scripts to check errors, link transactions, split transactions, metrics, ordered sets, replays, DLLPs, and TLPs.

To display the Verification Script dialog (see Figure 12.114 on page 861), select **Tools > Run verification scripts**

or click the  icon.

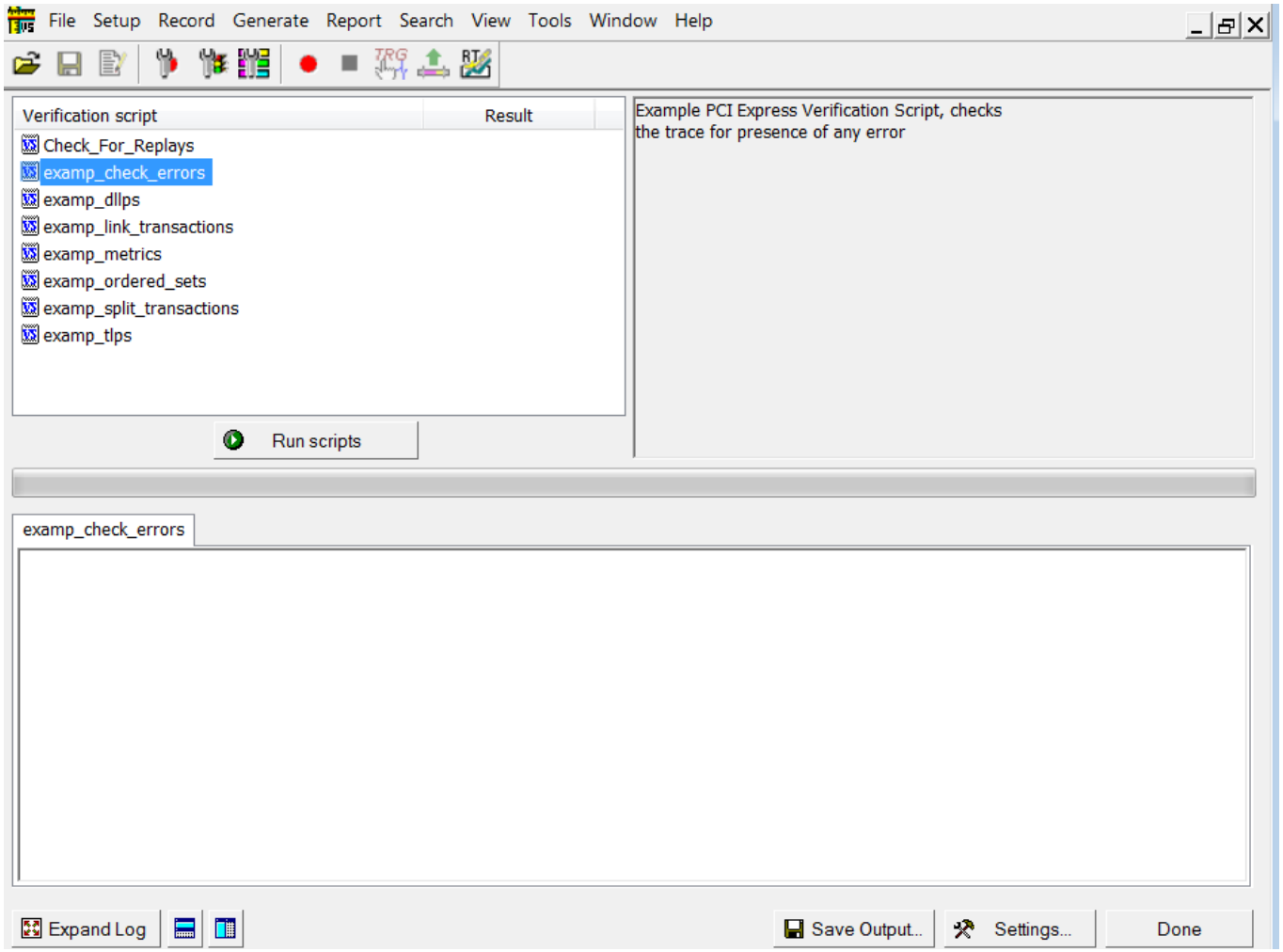


Figure 12.114: Verification Scripts Dialog

If you select examp_ltssm you'll get the following output. See Figure 12.115.

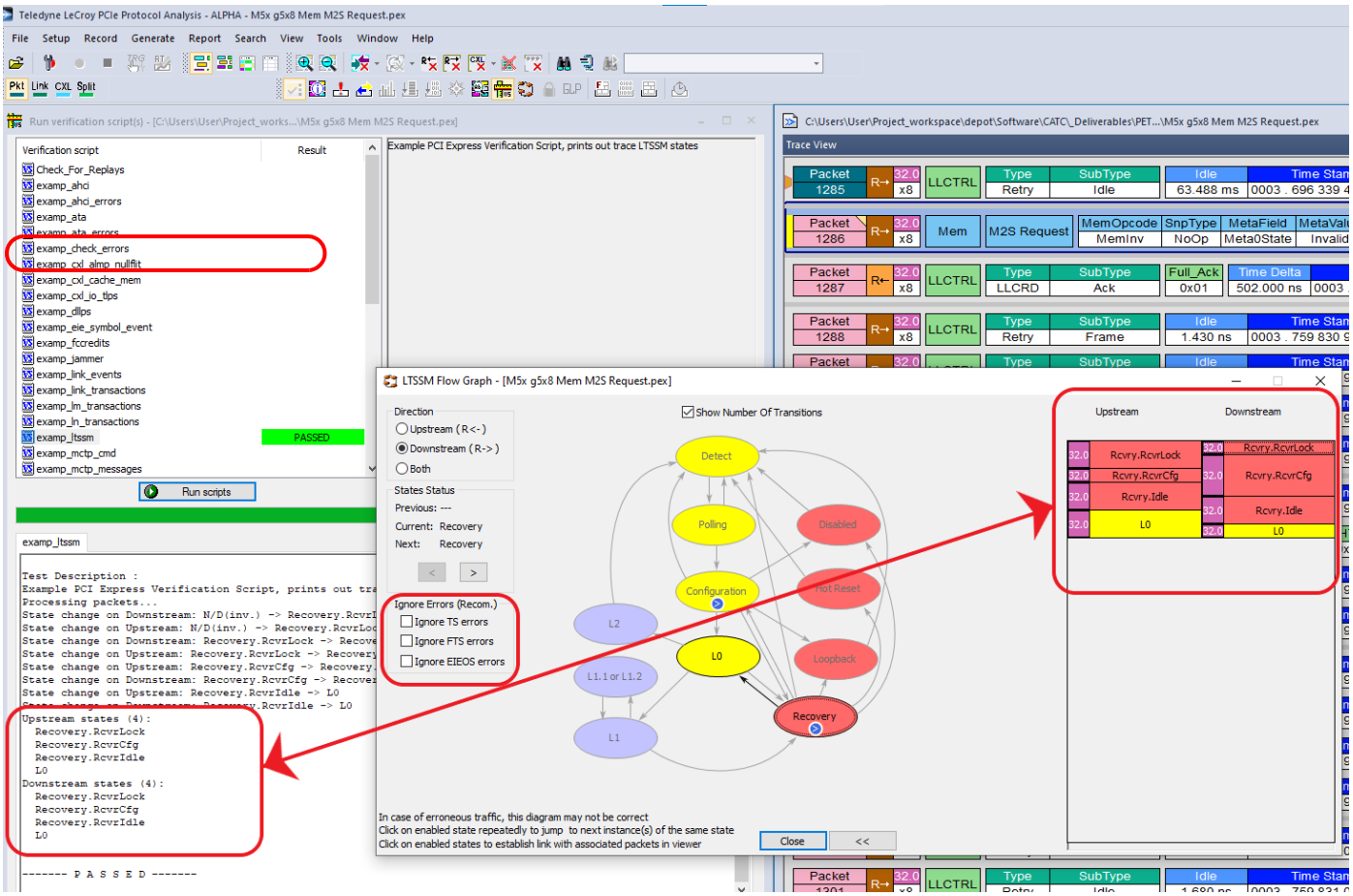
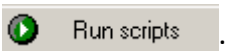


Figure 12.115: Run Verification Script: examp_ltssm

The available verification scripts are in the Verification script section.

To run a script, select it, then click the **Run Scripts** button 

.

The results appear in the bottom window. You can expand or collapse this window. You find a view related to the CATC Trace and place this window under or to the right of it. Click **Save** to save the results.

Click the **Settings** button to display the Settings Dialog (see Figure 12.116 on page 863).

Note: Verification scripts are not ignoring TS/FTS/EIEOS errors so values may be different if some of ignore options are enabled

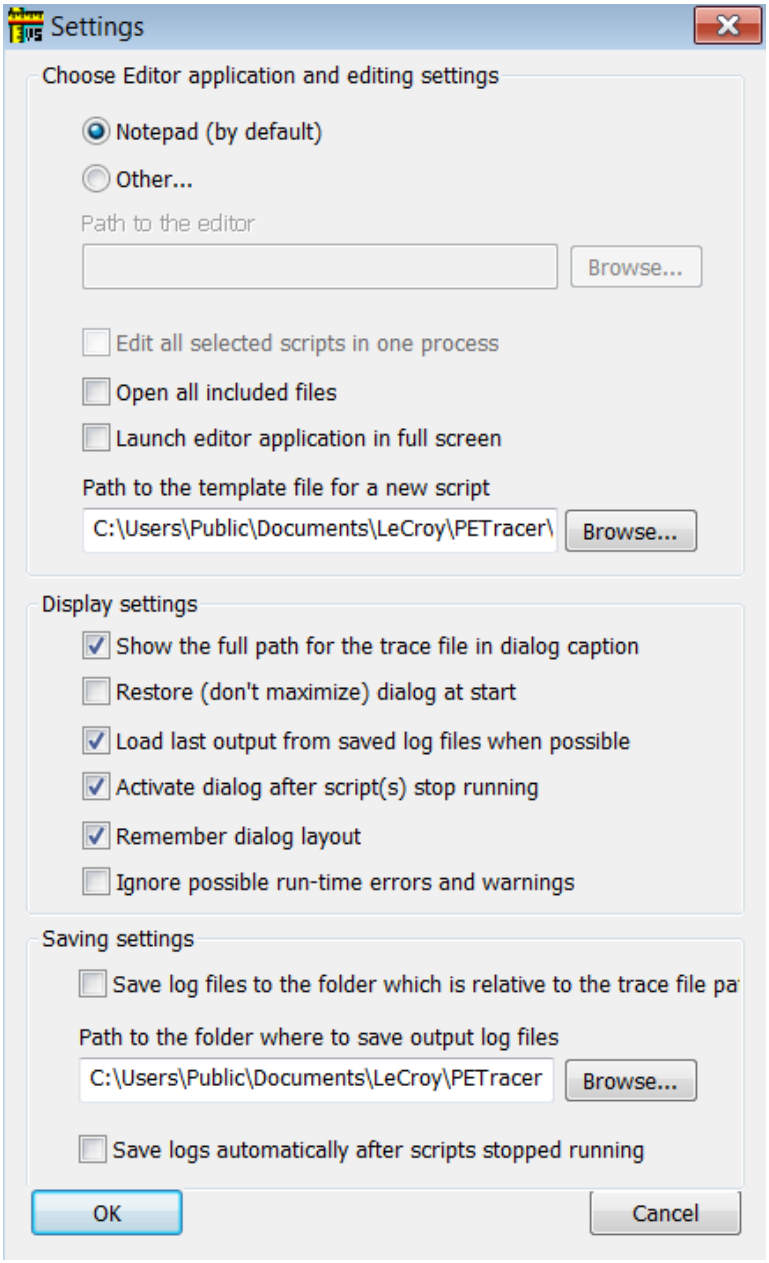


Figure 12.116: Settings Dialog

You can choose the editor, display settings, and saving settings.

12.32.1 NVMe Performance: Doorbell Timing

You can run verification scripts to determine Doorbell performance, see Figure 12.117.

The Doorbell statistics include:

- SQdoorbell to CQdoorbell,
  (time from Submission Doorbell to Completion Doorbell)
- SQDoorbell to CQentry,
  (time from SQ doorbell to command completion)
- SQentry to CQentry,
  (time from submission command to command completion

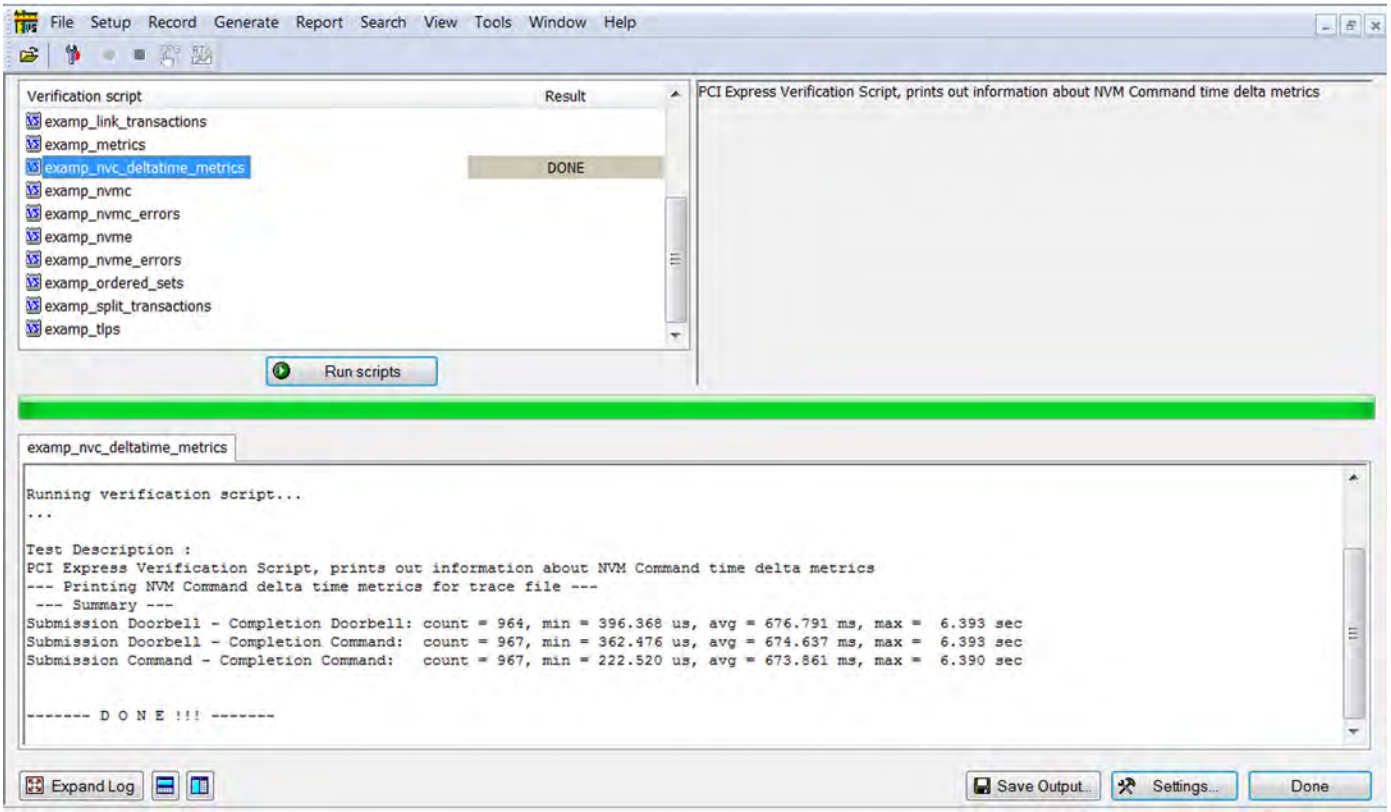


Figure 12.117: NVMe Performance Script Verification

Chapter 13

Updates and Licensing

13.1 Updating the Analyzer

BusEngine™ and/or Firmware updates are now automatic processes that run anytime a new version of the PCIe Protocol Analysis™ is installed that is incompatible with the currently installed BusEngine or Firmware. The update process generates on screen instructions.

If, however, you need to manually perform BusEngine or Firmware updates, follow these steps:

1. Select **Setup > Update Device** … from the menu to display the Update Analyzer dialog box for **Summit M5x™.**
2. Select the appropriate file locations for the Firmware and/or BusEngine, using Browse, if necessary.
3. Check the appropriate options (if in doubt, check all options).
4. Click **Update** to initiate the updating of the Analyzer.

13.2 License Keys

A License Key is necessary to enable software maintenance. If you attempt to record with the Analyzer without an installed License Key, a message appears to indicate that a License Key is necessary in order to record traffic.

A License Key must be obtained from Teledyne LeCroy for each Analyzer.

After you obtain the License Key, follow these steps to install it:

1. Select **Setup > All Connected Devices > Update License** from the menu bar. to display the Select License Key File dialog box.
2. Enter the **path** and **filename** for the License Key or use the Browse button to navigate to the directory that contains the License Key.
3. Select the **.lic** file, and then click **Update Device**.

13.3 License Information

You can view Licensing information for your Analyzer by selecting **Help > Display License Information**… from the menu bar. The License Information window displays data about the maintenance expiration and purchased features.

Appendix A

How to Contact Teledyne LeCroy

Send e-mail to Support	psgsupport@teledyne.com
Contact Support	teledynelecroy.com/support/contact
Visit Teledyne LeCroy's website	teledynelecroy.com
Tell Teledyne LeCroy	Report a problem to Teledyne LeCroy Support via e-mail by selecting **Help > Tell Teledyne LeCroy** from the application toolbar. This requires that an e-mail client be installed and configured on the host machine.

Appendix B

China Restriction of Hazardous Substances Table

The following tables are supplied in compliance with China's Restriction of Hazardous Substances (China RoHS) requirements:

	有毒有害物质和元素					
部件名称	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
PCBAs	X	O	X	X	X	X
机械硬件	O	O	X	O	O	O
金属片	O	O	X	O	O	O
塑料部件	O	O	O	O	X	X
电源	X	X	X	O	X	X
电源线	X	O	X	O	X	X
保护外壳(如有)	O	O	O	O	X	X
电缆组件(如有)	X	O	X	O	X	X
风扇(如有)	X	O	X	O	X	X
交流滤波器和熔丝组件(如有)	X	O	X	O	O	O
外部电源(如有)	X	X	X	O	X	X
探头(如有)	X	O	X	O	X	X

O: 表明该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T11363-2006 标准规定的限量要求之下。

X: 表明该有毒有害物质至少在该部件的某一均质材料中的含量超过 SJ/T11363-2006 标准规定的限量要求。

EFUP (对环境友好的使用时间) 使用条件：
温度：5摄氏度到40摄氏度
湿度：5% - 95%最大相对湿度 (无冷凝)
高度：最高2000米

	Toxic or Hazardous Substances and Elements					
Part Name	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr^{6+})	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCBAs	X	O	X	X	X	X
Mechanical Hardware	O	O	X	O	O	O
Sheet Metal	O	O	X	O	O	O
Plastic Parts	O	O	O	O	X	X
Power Supply	X	X	X	O	X	X
Power Cord	X	O	X	O	X	X
Protective Case (if present)	O	O	O	O	X	X
Cable Assemblies (if present)	X	O	X	O	X	X
Fans (if present)	X	O	X	O	X	X
AC Filter/Fuse Assy (if present)	X	O	X	O	O	O
Ext Power Supply (if present)	X	X	X	O	X	X
Probes (if present)	X	O	X	O	X	X

O: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement specified in SJ/T11363-2006.

X: Indicates that this toxic or hazardous substance contained in at least one of the homogenous materials used for this part is above the limit requirement specified in SJ/T11363-2006.

EFUP (Environmental Friendly Use Period) Use Conditions:

Temperature	5C to 40C
Humidity	5% to 95% max RH (non-condensing)
Altitude	Up to 2000 meters

Appendix C

Quick Search Feature

C.1 Quick Search Feature: Pre-Defined Terms

The Quick Search feature allows you to either search for a pre-defined term within a loaded Trace by clicking on the down arrow  or by typing your own term into the search window  and then moving the cursor into the window and hitting the Enter key.

A complete list of pre-defined terms is shown in Table 1.

TABLE C.1: Pre-Defined Searchable Terms

TLP - Memory Read (32 bit)	Error - TLP: Payload/Length Error
TLP - Memory Read (32 bit) - Locked	Error - TLP: Length Error (not 1)
TLP - Memory Write (32 bit)	Error - TLP: TC Error (not 0)
TLP - Memory Read (64 bit)	Error - TLP: Attr Error (not 0)
TLP - Memory Read (64 bit) - Locked	Error - TLP: AT Error (not 0)
TLP - Memory Write (64 bit)	Error - TLP: Byte Enables Violation
TLP - I/O Read Request	Error - Memory TLP: Address/Length Crosses 4K
TLP - I/O Write Request	Error - Mem64 TLP: Used Incorrectly
TLP - Configuration Read Type 0	Error - Cfg TLP: Register Error
TLP - Configuration Write Type 0	Error - Msg TLP: Invalid Routing
TLP - Configuration Read Type 1	Error - Msg TLP: Invalid Function Number field
TLP - Configuration Write Type 1	Error - Gen3 TLP: Bad Len CRC/Parity
TLP - Message	Error - Invalid Packet
TLP - Message with Data	Error - FC: Invalid Advertisement
TLP - Message for Advanced Switching	Error - FC: Insufficient Credits
TLP - Message for Advanced Switching with Data	Error - Training Sequence Format Error
TLP - Completion	Error - Training Sequence Parity Error
TLP - Completion with Data	Error - RRAP Command Aborted Error

TLP - Completion for Locked Memory Read	Error - RRAP Packet Parity Error
TLP - Completion for Locked Memory Read with Data	Error - RRAP Packet Reserved Fields Not Nullified Error
TLP - AtomicOp Fetch and Add (32 bit)	Controller Register - CAP
TLP - AtomicOp Fetch and Add (64 bit)	Controller Register - VS
TLP - AtomicOp Unconditional Swap (32 bit)	Controller Register - INTMS
TLP - AtomicOp Unconditional Swap (64 bit)	Controller Register - INTMC
TLP - AtomicOp Compare and Swap (32 bit)	Controller Register - CC
DLLP - Ack	Controller Register - Reserved
DLLP - Nak	Controller Register - CSTS
DLLP - PM	Controller Register - NSSR
DLLP - Vendor	Controller Register - AQA
DLLP - InitFC1-P	Controller Register - ASQ
DLLP - InitFC1-NP	Controller Register - ACQ
DLLP - InitFC1-Cpl	Controller Register - CMBLOC
DLLP - UpdateFC-P	Controller Register - CMBSZ
DLLP - UpdateFC-NP	Controller Register - Reserved
DLLP - UpdateFC-Cpl	Controller Register - Reserved Command Set Specific
DLLP - MRIOV	NVMe I/O Cmd - Flush
DLLP - InitFC2-P	NVMe I/O Cmd - Write
DLLP - InitFC2-NP	NVMe I/O Cmd - Read
DLLP - InitFC2-Cpl	NVMe I/O Cmd - Write Uncorrectable
DLLP - NOP	NVMe I/O Cmd - Compare
Link Events - Link Up	NVMe I/O Cmd - Write Zeroes
Link Events - Link Down	NVMe I/O Cmd - Dataset Management
Link Events - PERST# Deasserted	NVMe I/O Cmd - Reservation Register
Link Events - PERST# Asserted	NVMe I/O Cmd - Reservation Report
Link Events - WAKE# Asserted	NVMe I/O Cmd - Reservation Acquire
Link Events - WAKE# Deasserted	NVMe I/O Cmd - Reservation Release
Link Events - CLKREQ# Asserted	NVMe I/O Cmd - Vendor Specific
Link Events - CLKREQ# Deasserted	NVMe ADMIN Cmd - Delete I/O Submission Queue
Link Events - Skew	NVMe ADMIN Cmd - Create I/O Submission Queue
Error - Invalid Code	NVMe ADMIN Cmd - Get Log Page
Error - Running Disparity Error	NVMe ADMIN Cmd - Delete I/O Completion Queue

Error - Unexpected K/D Code	NVMe ADMIN Cmd - Create I/O Completion Queue
Error - Idle Data Error (not D0.0)	NVMe ADMIN Cmd - Identify
Error - Skip Late	NVMe ADMIN Cmd - Abort
Error - Skew Error	NVMe ADMIN Cmd - Set Features
Error - Bad Packet Length	NVMe ADMIN Cmd - Get Features
Error - Ordered Set Format Error	NVMe ADMIN Cmd - Asynchronous Event Request
Error - Delimiter Error	NVMe ADMIN Cmd - Firmware Activate
Error - Alignment Error	NVMe ADMIN Cmd - Firmware Image Download
Error - DLLP: Invalid Encoding	NVMe ADMIN Cmd - Format NVM
Error - DLLP: Bad CRC16	NVMe ADMIN Cmd - Security Send
Error - DLLP: Reserved Field not 0	NVMe ADMIN Cmd - Security Receive
Error - DLLP: FC Initialization Error	NVMe ADMIN Cmd - I/O Command Set specific
Error - TLP: Invalid Encoding	NVMe ADMIN Cmd - Vendor specific
Error - TLP: Reserved Field not 0	

Appendix D

Configuration Space Decoding

The decoded capability structures in the Configuration Space Viewer and Editor are based on programmed definitions in the PCIe Protocol Analysis and on Configuration Space Decode Scripts.

Configuration Space Decode Scripts are tools to define capability structures and instruct the Configuration Space Viewer or Editor how to decode them. These scripts are in the **\CfgSpaceScripts** sub-directory below the **\Scripts** directory in the application directory.

You can write Configuration Space Decode Scripts using the CATC Scripting Language (CSL). See the *Teledyne LeCroy Analyzers File Based Decoding Manual* for reference.

PCI Express Configuration Space Decode Scripts have the file extension **.pecfgdec**.

D.1 Mandatory Definitions

Configuration Space Decode Scripts must set the following reserved variables.

- **CapabilityName**: Name of the capability structure
- **CapabilityID**: ID of the capability structure
- **ExtAddSpace**: Set to 1 if Extended Configuration Space. Else, set to 0 for PCI.

D.2 Mandatory Module Functions

Modules are collections of functions and data dedicated to decoding a specific capability structure. Each module has one primary Configuration Space Decode Script file (extension **.pecfgdec**) and optionally has include files (**.inc**).

A module function is an entry-point into a decoding module. To help display a capability structure, the application calls a module function.

The Configuration Space Editor and Viewer support only the **DecodeRegister(offset)** and **GetSize( )** functions.

D.2.1 DecodeRegister(offset)

The application calls this function while decoding a specific DWORD offset of the specified CapabilityID. The offset is the decoding entry point, where the decoding path starts.

The Configuration Space Editor calls this function to determine how to decode the assigned configuration space. The **offset** parameter is the DWORD to decode.
An offset of 0 indicates bytes 00h-03h, an offset of 1 indicates bytes 04h-07h, and so on.

Note: The Configuration Space Editor can only decode one DWORD at a time.

D.2.2 GetSize()

This function returns the size of the capability structure specified by CapabilityID.

D.3 Configuration Register Types

The following reserved variables are defined global constants.

- CFGREG_UNDEFINED
- CFGREG_HWINIT
- CFGREG_RO
- CFGREG_RW
- CFGREG_RW1C
- CFGREG_ROS
- CFGREG_RWS
- CFGREG_RW1CS
- CFGREG_RSVDP
- CFGREG_RSVDZ

Note: These reserved variables match the Configuration Register Types of Table 7-2 in Section 7.4 of the PCI Express Base Specification, Rev. 2.1.

D.4 Primitives

Decoding uses the following primitives.

D.4.1 GetRegisterField

GetRegisterField(dword_offset, bit_offset, field_length)

This function returns a register field of length **field_length**, starting at bit position **bit_offset** in DWORD **dword_offset**.

- **dword_offset**: DWORD offset of the register field location
- **bit_offset**: Bit offset of the register field location
- **field_length**: Length of the register field

For example, **GetRegisterField(1, 9, 2);** means: Go to DWORD 1, bit offset 9, and returns 2 bits.

D.4.2 AddField

AddField(field_name, field_length, configuration_reg_type, tooltip, encoding_table = NULL)

This function adds a register field to the Capability View and returns a pointer to the field, for adding subfields.

- **field_name**: Name of the register field to display in the Capability View
- **field_length**: Length of the register field
- **configuration_reg_type**: Configuration register type of the register field. Note: If subfields are defined, their configuration register types override this setting for their specified bits.
- **tooltip**: Tooltip displayed for the register field in the Capability View
- **encoding_table**: Optional. Displays encodings as lists for select values.
- For example, user input becomes a combo box for the field in the Field View.

As examples:
AddField("PCI Express Extended Capability ID", 16, CFGREG_RO, "");
means: Add the field “PCI Express Extended Capability ID” with length 16 and cfg register type CFGREG_RO.

capability_reg = AddField("Capability Register", 32, CFGREG_RW, "");
means: Added the field “Capability Register” with length 32 and cfg register type CFGREG_RW and stored a pointer to this field in variable capability_reg, which can be used to add subfields to this field.

D.4.3 AddSubField

AddSubField(parent_field, subfield_name, subfield_length, configuration_reg_type, tooltip, encoding_table = NULL);

This function adds a subfield to a register field in the Capability View. Subfields are modifiable and visible in the Field View and appear in the tooltips of register fields.

- **parent_field**: Pointer to a register field in the Capability View
- **subfield_name**: Name of the subfield, displayed in the Field View
- **subfield_length**: Length of the subfield
- **configuration_reg_type**: Configuration register type of the subfield field. Note: This overrides the configuration_reg_type of the parent field.
- **tooltip**: Tooltip displayed for the subfield in the Capability View
- **encoding_table**: Optional. Displays encodings as lists for select values.
- For example, user input becomes a combo box for the field in the Field View.

For example,
AddSubField(capability_reg, "Mode Supported", 4, CFGREG_RO, "Indicates the Function modes,"), ModeEncodings);
means: Add the subfield "Mode Supported" to the parent field "capability_reg" with length 4, type CFGREG_RO, a tooltip in the Capability View, and a combo box displaying "mode encodings" for input in the Field View.

D.5 Helper File

ConfigSpaceCommon.inc include file contains useful functions for script decoding.

Appendix E

Example of XML File Format for SSD Decodes


```
<DEVICES XML_FORMAT_VERSION="1.0">
<DEVICE ENABLE="0x1" VENDORID="0" CLASSCODE="67586" GUID="{9C9654A1-B693-4F30-912F-125059814C42}"
  DEVICEID="000:00:0">
<BARS>
<MBAR ID="0" VALUE="0xF0000000"/>
<BAR ID="2" VALUE="0x00000000"/>
<BAR ID="3" VALUE="0x00000000"/>
<BAR ID="4" VALUE="0x00000000"/>
<BAR ID="5" VALUE="0x00000000"/>
</BARS>
<PROTOCOL ASQS="64" DSTRD="4" ACQS="16" LBASIZE="512" PROTOCOL="NVME" MPS="4096"
  ADDEDBY="DECODING"/>
<Queues>
<Queue SIZE="10" QID="2" TYPE="IOSQ" ADDRESS="0x11B210300" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="3" TYPE="IOSQ" ADDRESS="0x11B210340" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="5" TYPE="IOSQ" ADDRESS="0x11B210380" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="7" TYPE="IOSQ" ADDRESS="0x11B2103C0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="9" TYPE="IOSQ" ADDRESS="0x11B210400" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="11" TYPE="IOSQ" ADDRESS="0x11B210E80" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="14" TYPE="IOSQ" ADDRESS="0x11B210E40" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="16" TYPE="IOSQ" ADDRESS="0x11B210E00" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="6" TYPE="IOSQ" ADDRESS="0x11B233040" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="8" TYPE="IOSQ" ADDRESS="0x11B233080" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="10" TYPE="IOSQ" ADDRESS="0x11B233B40" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="12" TYPE="IOSQ" ADDRESS="0x11B233B00" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="13" TYPE="IOSQ" ADDRESS="0x11B233AC0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="15" TYPE="IOSQ" ADDRESS="0x11B233A80" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="17" TYPE="IOSQ" ADDRESS="0x11B233A40" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="1" TYPE="IOSQ" ADDRESS="0x11B25F080" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="4" TYPE="IOSQ" ADDRESS="0x11B28B040" ADDEDBY="DECODING"/>
```

<Queue SIZE="10" QID="3" TYPE="IOCQ" ADDRESS="0x11B2200C0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="5" TYPE="IOCQ" ADDRESS="0x11B2200E0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="7" TYPE="IOCQ" ADDRESS="0x11B2200F0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="9" TYPE="IOCQ" ADDRESS="0x11B220100" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="11" TYPE="IOCQ" ADDRESS="0x11B2203A0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="14" TYPE="IOCQ" ADDRESS="0x11B220390" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="16" TYPE="IOCQ" ADDRESS="0x11B220380" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="6" TYPE="IOCQ" ADDRESS="0x11B243010" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="8" TYPE="IOCQ" ADDRESS="0x11B243020" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="10" TYPE="IOCQ" ADDRESS="0x11B2432D0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="12" TYPE="IOCQ" ADDRESS="0x11B2432C0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="13" TYPE="IOCQ" ADDRESS="0x11B2432B0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="15" TYPE="IOCQ" ADDRESS="0x11B2432A0" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="16" TYPE="IOCQ" ADDRESS="0x11B243290" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="1" TYPE="IOCQ" ADDRESS="0x11B26F020" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="2" TYPE="IOCQ" ADDRESS="0x11B26F030" ADDEDBY="DECODING"/>
<Queue SIZE="10" QID="4" TYPE="IOCQ" ADDRESS="0x11B29B010" ADDEDBY="DECODING"/>
</Queues>
</DEVICE>
</DEVICES>

Appendix F

Expandability

F.1 Expandability

- Summit M5x: CATC SYNC Expansion Card functionality is built-in
- Summit T416: CATC SYNC Expansion Card functionality is built-in
- Summit T48: CATC SYNC Expansion Card functionality is built-in
- Summit T34: CATC SYNC Expansion Card functionality is built-in
- Summit T316: CATC SYNC Expansion Card is separate
- Summit T38: CATC SYNC Expansion Card is separate

You can time correlate different analyzers by daisy-chaining multiple Summit M5x, Summit T416, Summit T48 and Summit T316 analyzers or connect to other Teledyne LeCroy protocol analyzers with the CATC SYNC Expansion Cards (ACC-EXP-002-X).

Note: More combinations of analyzers are possible, contact psgsupport@teledynelecroy.com for more details.

Note: The following steps only apply to the Summit T316, T3-8, T28 and T24.

When purchased with the analyzer, this card is typically installed in the analyzer at the factory but it can be purchased separately. There are both extraction and insertion instructions below depending on which operation you need to perform.

The expansion slot can be located on either the front panel or the rear panel, so the first step is to find the expansion slot.

If you are inserting an expansion card see “Installation of Expansion Cards” on page 886. If you are removing an expansion card continue with the steps below.

You can remove expansion cards with two simple tools.

F.1.1 Removal of Expansion Cards

You can remove expansion cards using two tools:

- Standard (flat blade) 3/16” screwdriver
- Teledyne LeCroy Extraction Tool (part number 230-0160-00)

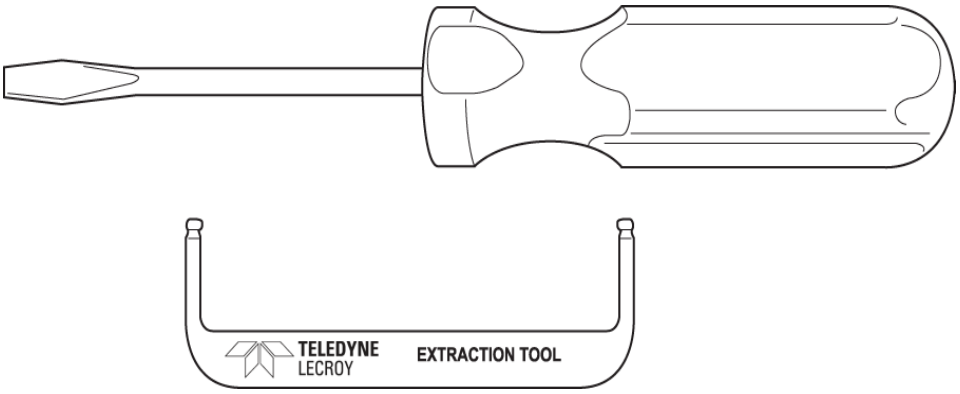


Figure F.1: Tools needed to Remove the Expansion Cards

To remove an expansion card, follow these steps:

1. Unplug the system from AC power and turn the system so the expansion port is facing you.

Note: There are two retaining screws and the holes for the extraction tool that are located on the panel of the expansion card. See Figure F.2.

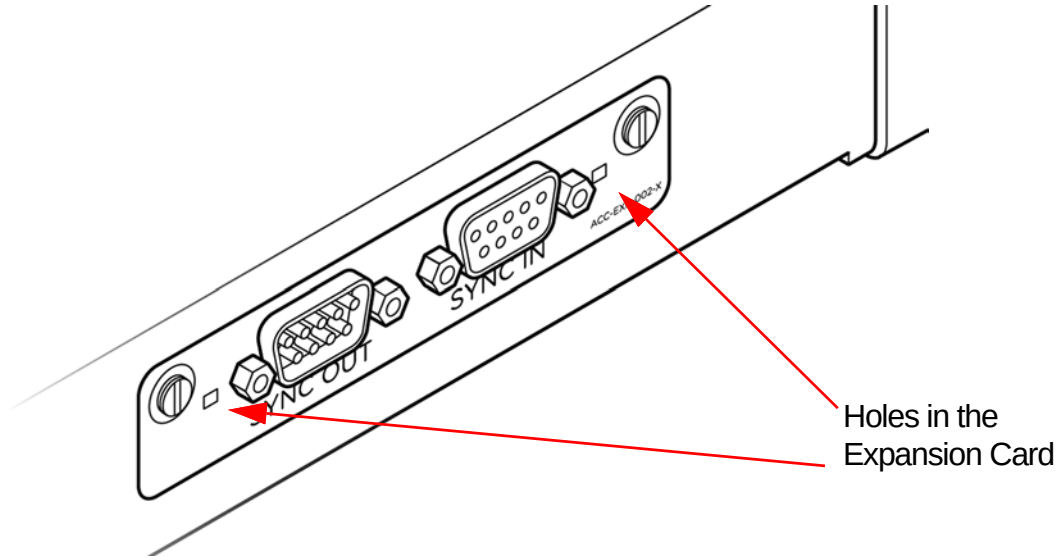


Figure F.2: Holes in the Expansion Card Panel

2. Using the screwdriver, loosen both retaining screws by rotating them counter-clockwise approximately two full turns, until feeling slight resistance. **Do not force the retaining screws** after two turns.

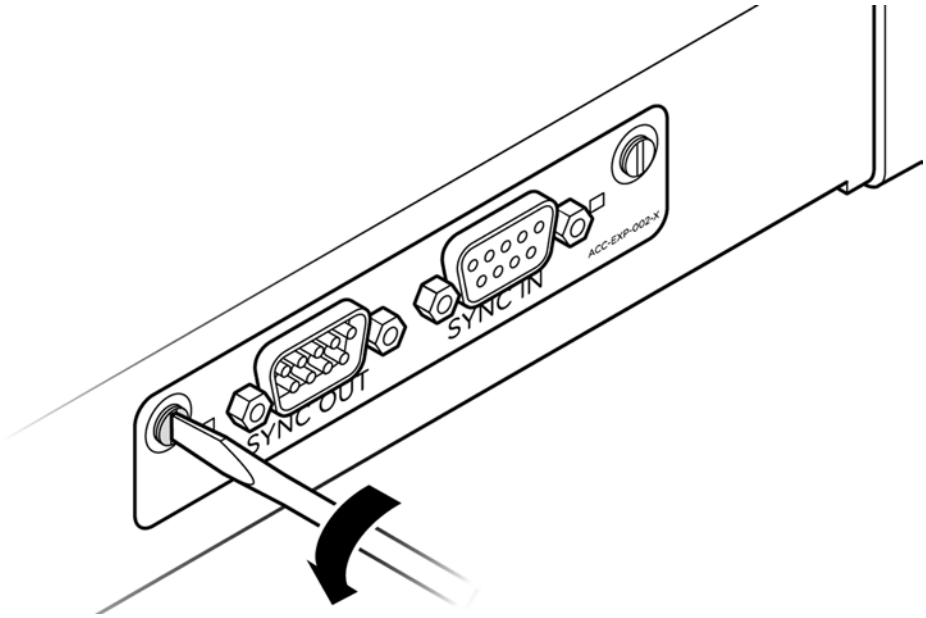


Figure F.3: Loosen Retaining Screws on CATC Card

3. Insert the extraction-tool prongs into the holes in the expansion card panel.

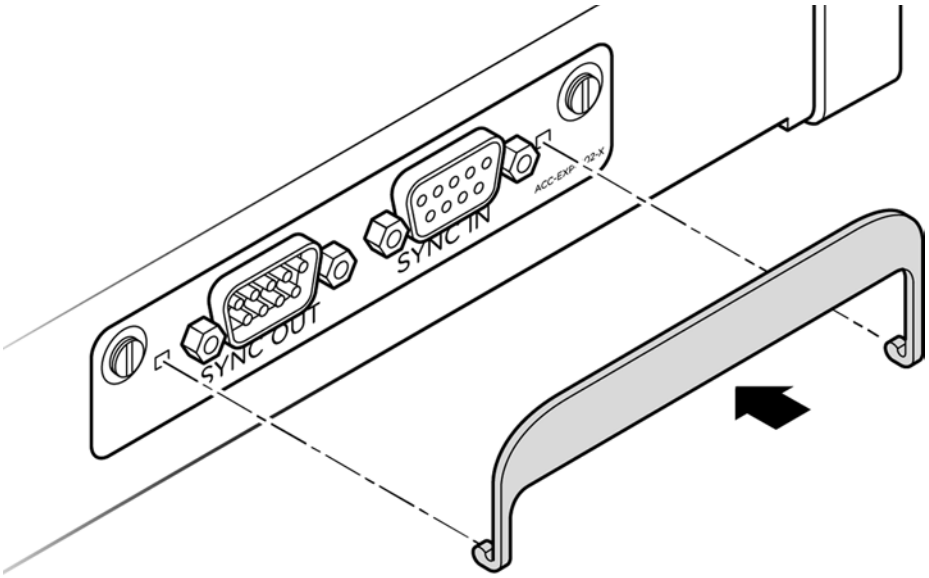


Figure F.4: Insert Extraction Tool

Note: If the prongs do not slip easily into the holes, use a small nail file or similar device to remove paint from the prongs

4. Rotate the extraction tool to a horizontal position to lock the prongs into place and make a handle.

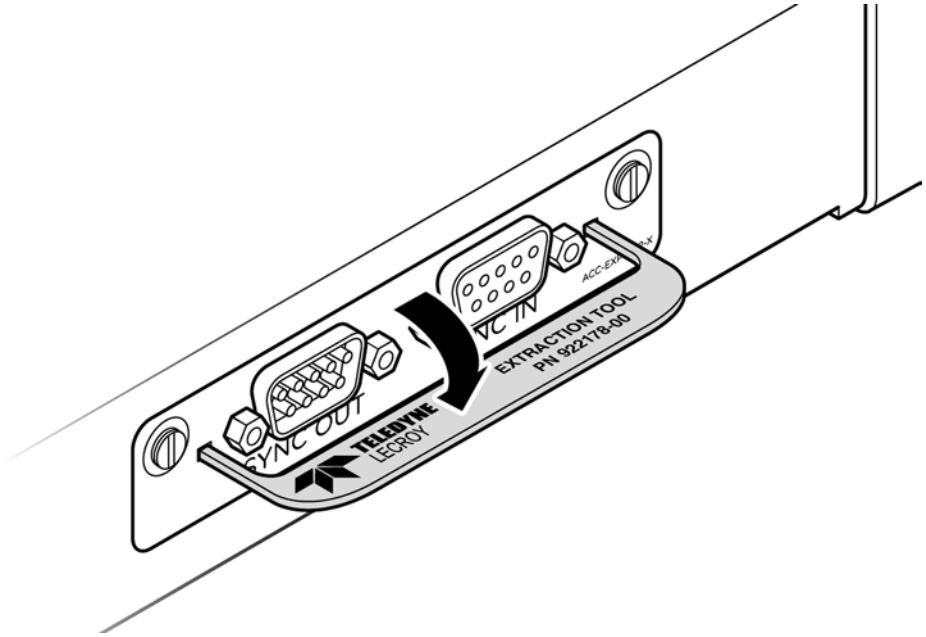
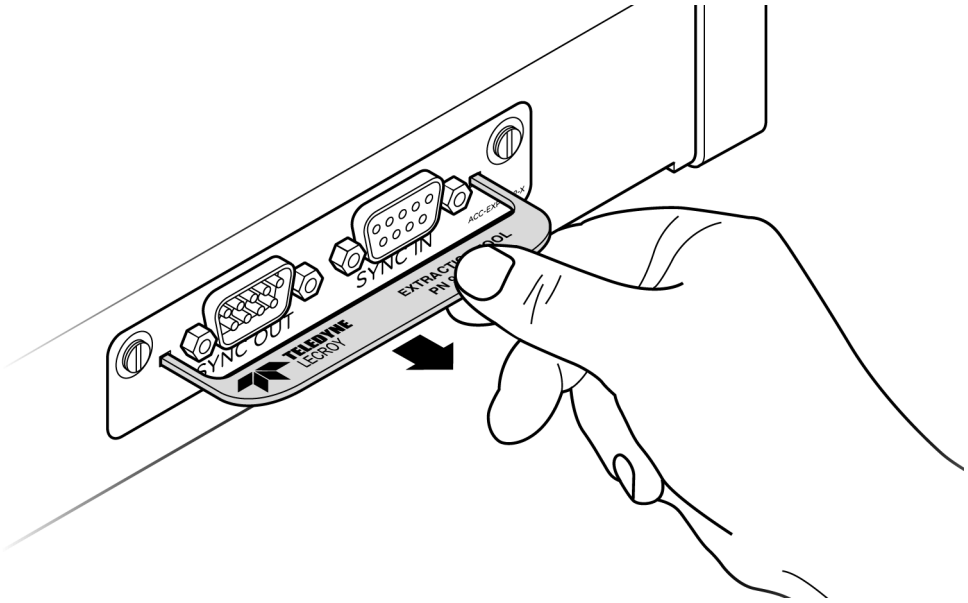


Figure F.5: Insertion of Handle/Tool into Expansion Card Panel

5. Using the extraction tool as a handle, gently wriggle the expansion card forward about 1/8”.



6. Repeat step 5 approximately three times, until the card is free from the retaining screws and you can remove the card from the system.
7. Replace the CATC Expansion Card with a blank panel and tighten the retaining screws. See Figure F.6.

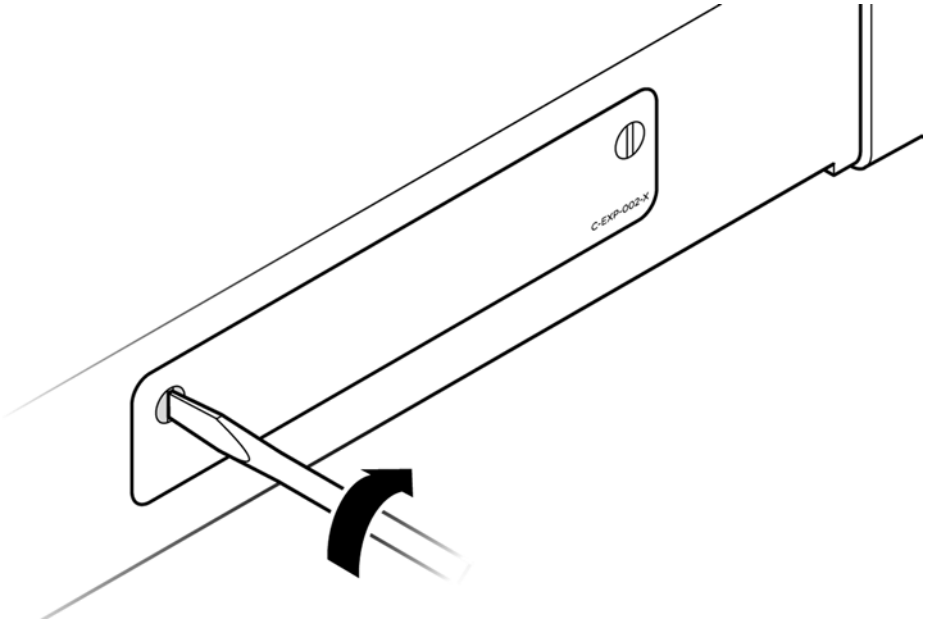


Figure F.6: Replace Retaining Screws in Blank Panel and Tighten

F.1.2 Installation of Expansion Cards

1. Locate the blank expansion panel on either the front or the rear of the analyzer and then continue with the steps below.

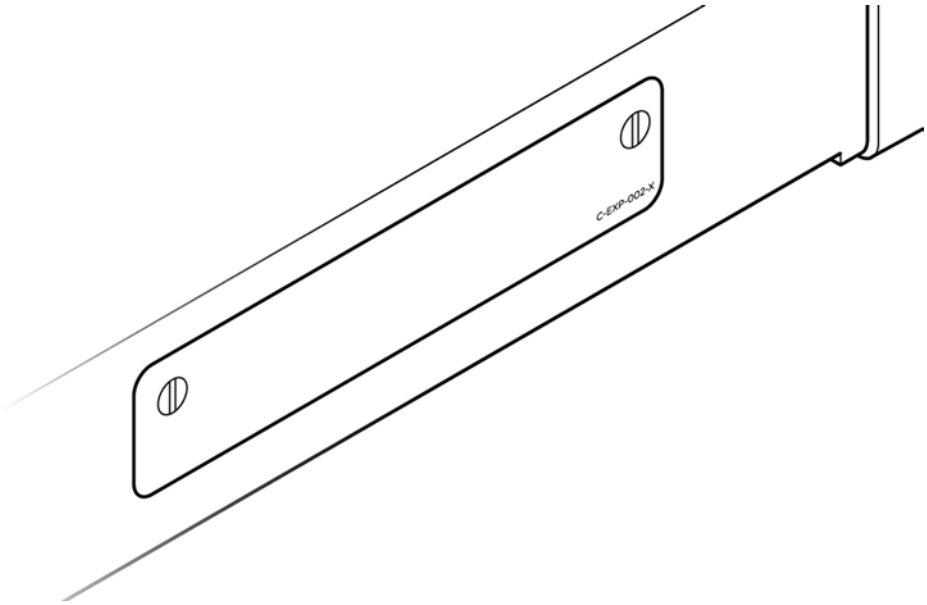


Figure F.7: Front or Rear of Analyzer: Blank Panel

2. Using a flat bladed screw driver, loosen the two retaining screws.

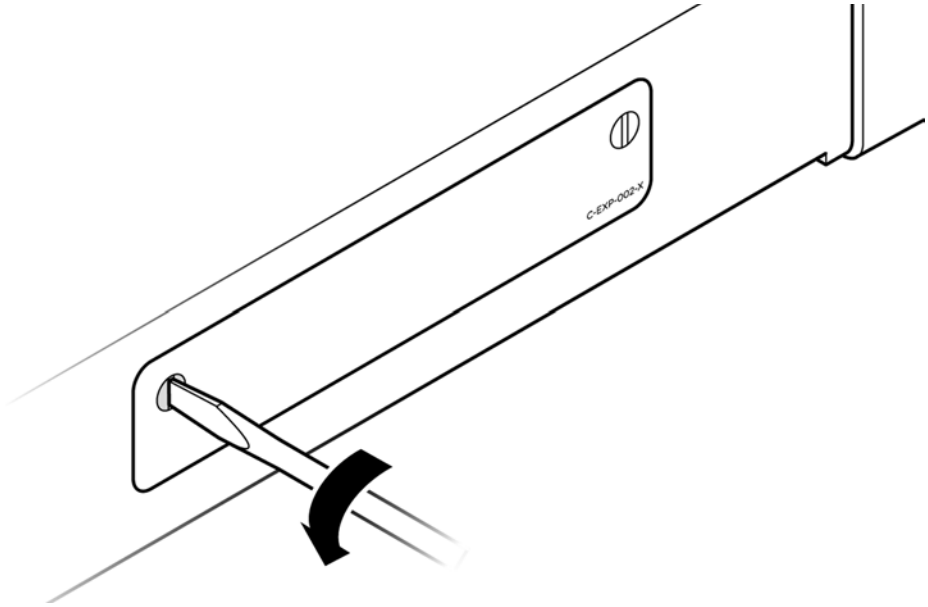


Figure F.8: Loosen Retaining Screws from Blank Panel

3. Remove the retaining screws and blank panel, exposing the inside of the analyzer.

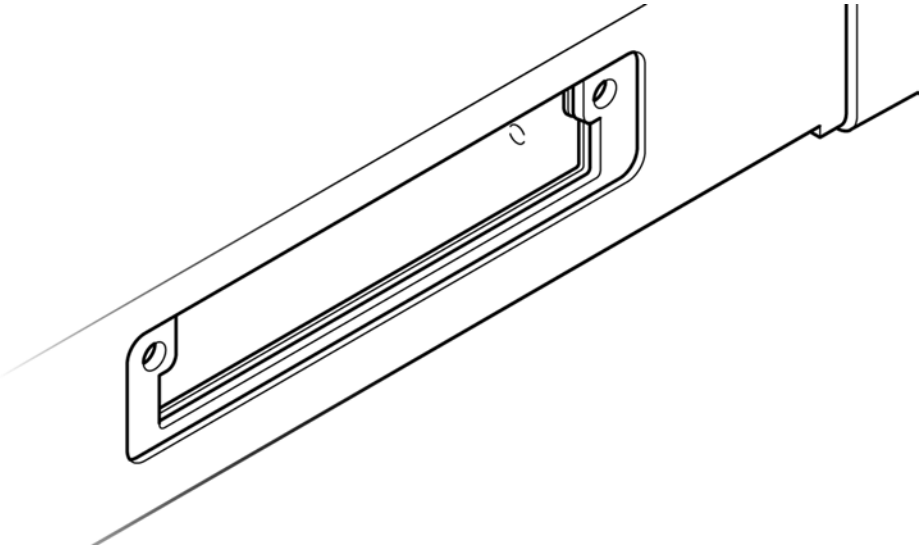


Figure F.9: Rear of Analyzer with Blank Plate Removed

4. Insert the CATC card into the rear of the Analyzer. Gently push on the back panel of the card until you feel the card seat with the internal connector.

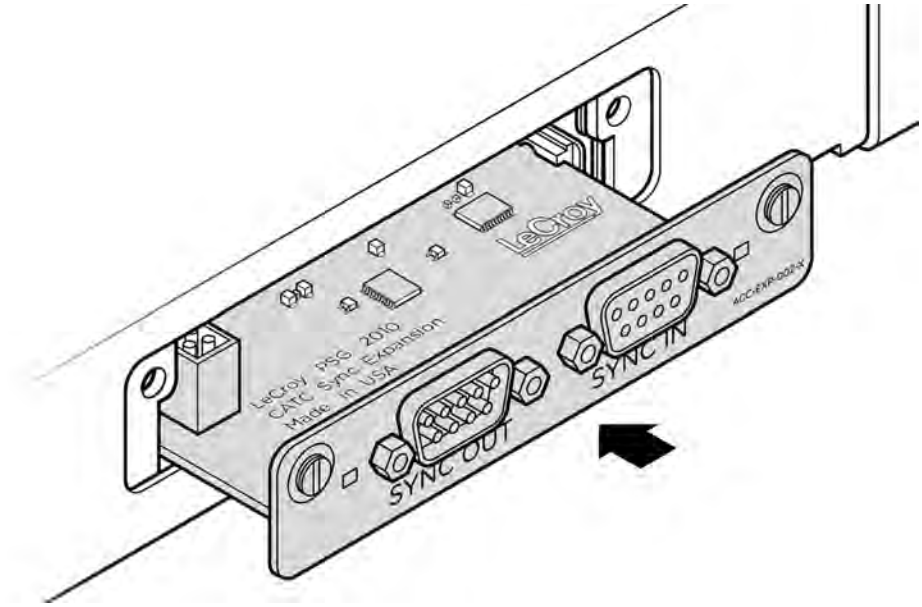


Figure F.10: CATC Card Being Inserted into Rear of Analyzer

5. After the card is seated, tighten the retaining screws.

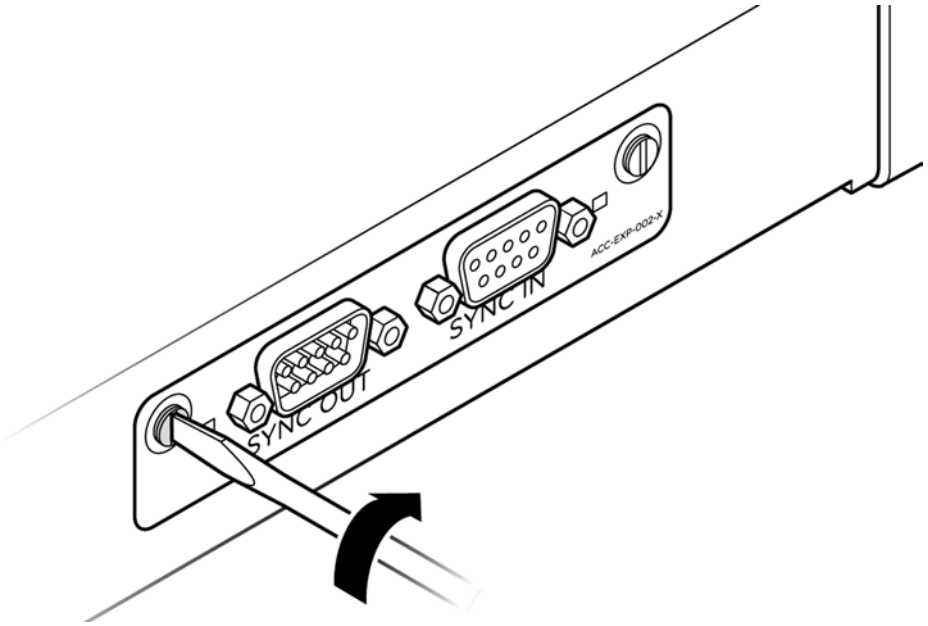


Figure F.11: Tighten the Retaining Screws on the CATC Card

6. The CATC card can now be connected to other CATC cards in other analyzers. As described in the next section (“Daisy-Chaining with CATC SYNC Expansion Cards” on page 889).

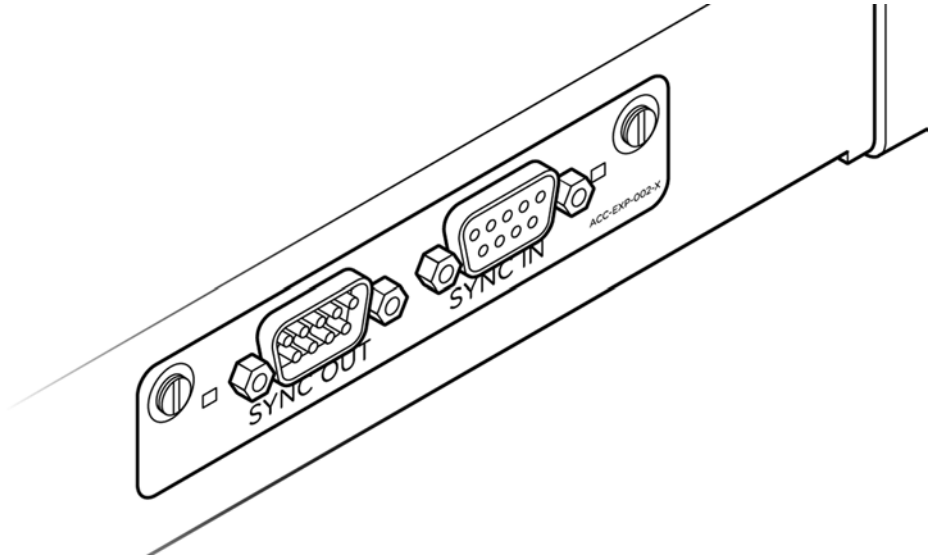


Figure F.12: Analyzer with CATC Card Installed

F.1.3 Daisy-Chaining with CATC SYNC Expansion Cards

You may daisy-chain up to eight analyzer units by connecting the units through the optional CATC SYNC Expansion Card on the analyzer back.

Daisy-chained analyzer units will have their timestamping, recording, and triggering functions synchronized to +/- 100ns. In this example, we daisy-chain the following analyzers:

- Summit M5x
- Summit T416
- Summit T48
- Summit T3-8

Note: More combinations of analyzers are possible, contact psgsupport@teledynelecroy.com for more details.

Perform the following steps to connect the CATC Sync ports between two or more analyzers:

1. Make sure to stop any recordings in progress.

Note: You may plug/unplug the sync cable while the analyzer unit is powered on.

2. Connect the female end of the sync cable to the SYNC OUT port of one Analyzer.
3. Connect the male end of the sync cable to the SYNC IN port of the other Analyzer (see Figure F.13 on page 890.)
4. Repeat steps 2-3 to connect additional units (up to eight total) as needed.
5. DO NOT create a closed loop from the last unit back to the first unit.

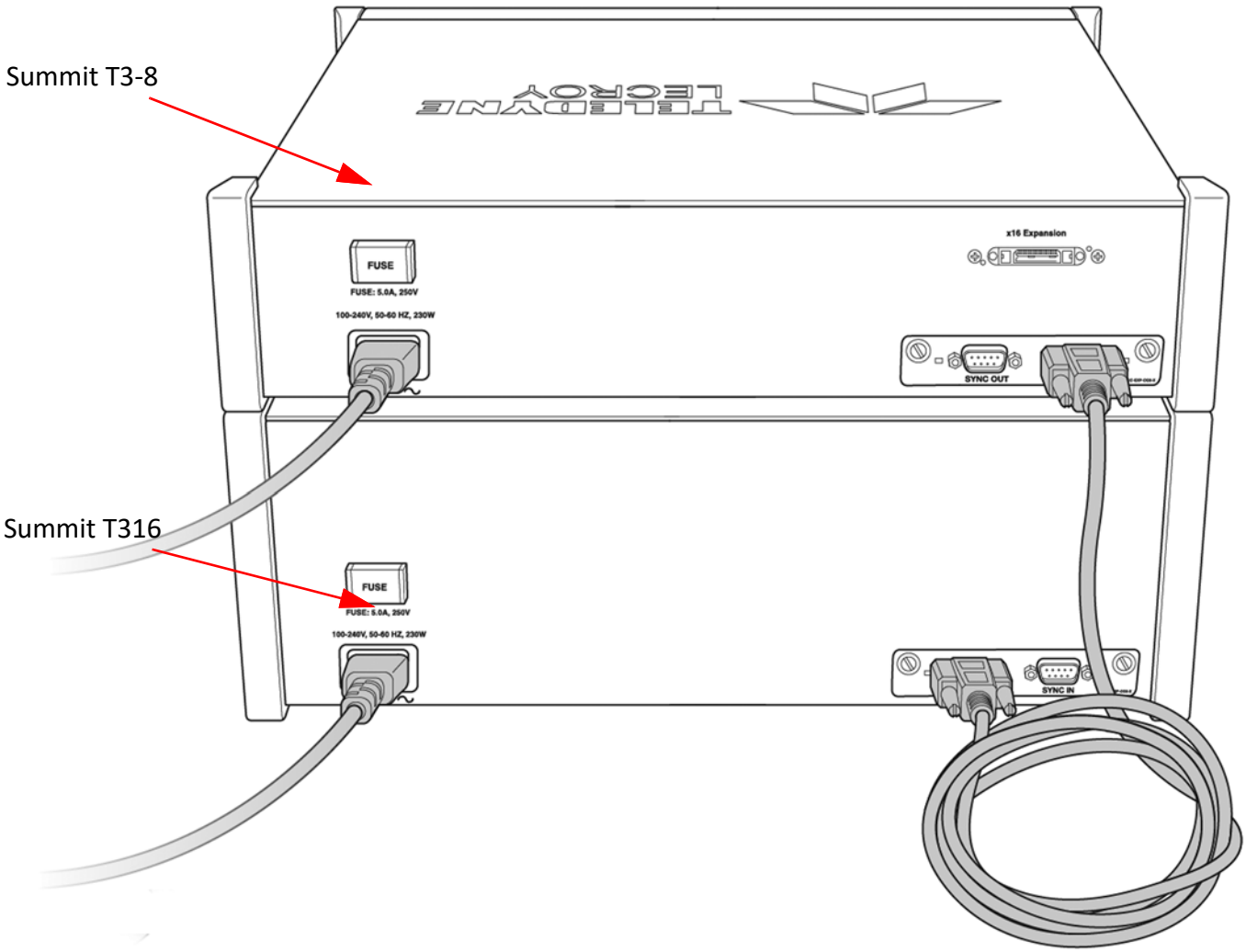


Figure F.13: An Example of Connecting a Summit T3-8 to a Summit T316 Analyzer

Other analyzers are connected in a similar manner.

Index

Symbols

.crec 149
.lic files 881
.opt files 746
.peraw file extension 453
.pex files 111
.rec files 111
*.pem 152, 357
+ sign 440

Numerics

10b errors 438
10-bit code format 434

A

Accessing the Properties Dialog 186
Actions Properties Dialog 207
Activity 105
Adding an Attachment 685
Advanced Hiding Options 79
AHCI level decode 605
All Connected Devices 127
All Markers Window 694
Analyzer
  license 881
  update 881
Analyzer Devices 127
Analyzer Network Chat Bar command 128
application 47
ATA level decode 605
Attaching Markers 684
Auto De-Skew command 433
Auto-Configure Lane Polarity 160, 366
Available Events area 171
  169
averaging 829

B

Bandwidth 856
Base Spec 1.0 Rev Compatibility Mode 154, 358
Binary code format 434
BitTracer
  color-coding 434
  compressing data view 453
  data capture mode 431
  data display 434
  Data Display toolbar. 434
  decoding 442
  de-skewing 433
  enabling 431
  Errors window 438
  expanding data view 453
  exporting 446
  link configuration 444
  logical links 446
  markers 436
  recording mode 431
  report windows 435
  saving 453
  search 443
  Symbol window 440
  timing 435
  Timing window 437
  trigger 432
  views 432
  zooming 453
BitTracer mode 28
blue current-position indicator 803
Both directions 807
Buffer Size 145, 345
Bus Utilization 783, 856, 866
  buttons 785
  features 830
  metrics 829
  pop-up menu 784

BusEngine update 881

C
calculating time between DWORDs 793
CATC Trace 27
CATC Trace View 554
CATC Walk Playlist 696
cells 532
  resizing 532
  states 180
Change Counter Value command 240
changing
  markers 550
Changing the Value of the Counter 237
Changing the Value of the Timer 240
Channel 241
Channels 187
Chat session 128
Chat window 127
Clear Marker command 550
Clocks radio button 681
Collapse Idle 795
Collapse Idle Plus. 795
Collapsible Idle Time 792
collapsing 531
Color Format Hiding tab 739
Combining Specified Event Groups 708
Combo box 821
Comma Separated Value files 116
Comment field 549
comment string 548
Compressed CATC Trace 554
Configuration Space 819
Configuration Space dialog box 819
Configuration Space Header 821
Configuration Space View 819, 820
configuring
  Recording Options 107
Connecting the Analyzer to Power 59
Contact Support 883
Contact Teledyne LeCroy 883
context menus 532
Continue option 110
Continuous Time Scale 795
Control-b command 735
controls
  Analyzer Summit M5x 33
Count action 173
Counters 233
CrossSyncTM Control Panel 29, 86
CSV files 116
current-position indicator 803

D
daisy-chain 905
Data Block window 534
data cells 532
Data Field 531
Data Flow command 797
Data Flow window 797
Data Throughput 824, 856
data.pex file 110, 111
decode levels 561
decoding 561
Decoding window 442
default options file 149, 356
default.opt file 747
default.rec file 149, 356
Defining Recording Rules 170
Deleting a Counter 237
Deleting a Timer 241
delimiters 803
descrambled format 434
Description String 187
descriptive label 150, 357
Detail View and Spreadsheet View 561
Direction 122
Direction field 708
Disable Descrambling 366
disparity errors 438
Display area 72
Display License Information command 881
Display Options 737
  command 737
  fFiles 111
  loading 746
Display Options button 737
DLLP Packet Properties dialog 197, 199
Do not export hidden packets 122
Do not export Idle packets 123
Do not save hidden packets option 113
Downstream 155, 362
DOWNSTREAM 1 connector 33
DOWNSTREAM 2 connector 33
Downstream direction 807
Downstream LED 33
Drag an event here to create a new sequence 182
DS Ref Clk In 33
DWORDs
  timing 793

E
Edit Comment command 127
Edit Marker 693
Edit Marker command 550
Edit Marker for Packet # pop-up 549
e-mail 883
Enable Tool tips 738
Error Hiding tab 745
Error Properties dialog box 196
Error Summary dialog box 762
errors
  10b 438
  disparity 438
Errors pane 802
Errors window 438
ETHERNET 34
Event Groups menu 707
Event Icon Preview 186
Event Navigation 774
Event Trigger recording type 138, 341
events
  searching 679
Events report window 440
Event-specific Settings 187
Exclude option 708
Expand Data command 531
Expansion Slot 38
Export command
  BitTracer 446
Export to Compressed Archive command 453
Export Wait for ACK from upstream 123
Export Wait for Cpl from upstream 123
exporting 116

F
field
  hiding 742
Field Formats tab 741
File Export dialog box 121
file formats 116
File Menu 80
filter 208
Filter action 173
Filter In button 210
Filter Out button 210
Find command 705
Find dialog box 707
Find Next command 732
finding 707
Firmware update 881
First, Prev, Next, and Last buttons 821
Fit to Graph Area 784, 836
Flush option 110
format
  field 741
From 122
From packet # field 127
From Packet field 113
front panel 33
Functionality of Markers 683

G
Gen4 PCI Express 16-lane advanced verification system 25, 335
Generator file format 116
Global State 180
Global State and Sequence States 180
Global State Cell 172
Go To Marker command 681
Go to Marker command 793
Go To menu 701, 702
Go to Packet # 784
Go to Packet command 680, 681
Go to Trigger command 680
Grid Lines 774
Group and Colors column 740, 741

H
header fields 537
Help Menu 100
Hexadecimal vs. Binary tabs 821
Hide 784, 836
Hide buttons 77, 794
Hide Downstream button 78
Hide Sideband button 78, 79
Hide SKIP and Update FC button 78
Hide Training button 78
Hide Upstream button 78
hiding 742
  Idles 794
Hiding tab 742
Hierarchy Lines 738
host machine requirements 31
How to Increment or Reset a Counter 235
How to Set a Counter 234
How to Set a Timer 238
How to Start or Reset a Timer 239

I
Icon Label 187
information
  priority 804

InitFC complete status 837
interface 47
Intersection option 708

K
K/D symbol format 434
Key
  License 881
keyboard shortcuts 104
keystrokes 104

L
label 150, 357
lane swizzling 28
Latency 856
Latency Time 824
Launching the CrossSync Control Panel 129
layout 72
LCD display 34
LCD Display and Button Functions 34
LCD Display and Button Functions for Configuring the Analyzer 34
LCD Menu Navigation Buttons 33
LCD Menus 33
LEDs
  Analyzer Summit M5x 33
Legend option 803
Level Hiding tab 742
levels 561
LFSR value 434
license files 881
License Information window 881
License Key 881
licensing information 881
Linear 784, 836
Link 153, 357
Link Configuration dialog 444
Link level decode 564
Link section 108
Link Settings 153, 357
Link State 837
Link State Dialog 187
Link Tracker
  buttons 794
  toolbar 791
Link Tracker window 791
  docking 793
  markers 793
  reformat 791
link training 109
Link Transaction
  metrics 827
Link Transaction Level graphs 831
Link Transaction Performance 827
Link Utilization 856
Link Width 154, 358, 360
Link Width pane 802
Load button 151, 356, 746
Load command 150, 356, 746
loading 150, 356, 746
Loading Recording Options 356
Logarithmic 784, 836
logical links
  BitTracer 446
Logical view 442
long format 531
LTSSM Flow Graph 807
LTSSM Flow Graph command 807

M
Main Display Area 791
Main display area 170
Manual Trigger
  recording type 138, 340
Markers 682
  Adding an Attachment 685
  Attachment Types and Visualization 686
  Embedded Attachments to a Marker 686
  Recording an Audio File 685
  Video Files supported 686
markers 548
  BitTracer 436
  deleting 550
  editing 550
  setting 548, 793
  user-defined 436
Markers Overview 682
Markers window 437
Memory Writes 828
Memory Writes Performance 856
Menu bar 72
menus 80
  pop-up 532
metrics 824
  Bus Utilization 829
  Link Transaction 827
  Link Transactions 824
  Split Transaction 827
  Split Transactions 824
  trace 825
  Traffic Summary 827
  unit-base averaging 829

Metrics Header 825
Metrics Tooltip 825
Microsoft® Windows®-based host machine 47
Msb -> Lsb checkboxes 742
Multi-Segment Toolbar 77, 80

N

navigating 800
Navigating Recording Rules 183
Navigator 800
  displaying 800
  legend 803
  panes 801, 802
  range 801, 802
  ranges 801
  slider 803
  toolbar 800
Navigator Legend dialog box 804
Navigator Panes button 803
Navigator Range button 802
New Event button 171
New Events button 186
Number of data packets 837
Number of Link Transactions 824
Number of Packets 824
NVMe level decode 569
NVMe PCIe SSD Device Configuration 868

O

opening
  program 57
operating system 47
options files 149, 356
Options Name box 150, 357
Ordered Set Properties Dialog 196
Origin field 708

P

Packet # field 549
Packet Data command 818
Packet Data window 818
Packet Directionality Cell 553
Packet Header bar 817
Packet Header Cell 553
Packet Header command 817
Packet Heading Cell 539
Packet level decode 561
Packet Match Resource 174
Packets report window 441
Packets/second 856
pane checkbox 804
Pattern Format section 444
Payload 824
Payload size 837
PCI Express Spec 4.0 28
PCIe Protocol Analysis Files 111
PCIe Protocol Analysis SN message 105
PCIe Protocol Analysis T3-16
  opening 57
pem 152, 357
PHY layer problems 28
Pin Button 187
Playback Window 697
Playlist Functionality 696
Playlist Playback Control 698, 699
plus symbol 740, 741
polarity checkbox 445
pop-up menus 532
Power Switch 33
PQI level decode 609
PQI PCIe SSD Device Configuration 871, 873
Pre/Post Trigger pane 802
Print command 127
Printer button 127
printing 127
Probe Settings 244, 409
Properties 784, 836
Properties button 186
Properties command 172
Properties dialog 186
Properties dialog box 172, 186
Protocol Level to View 738
protocol unit 824

R

range delimiters 803
Raw 10b Codes 537
Read Requests Performance 827
reading 531
Ready message 105
Real-Time Statistical Monitor window 835
Real-Time Statistics
  buttons 834
  pop-up menu 835
  toolbar 834
Real-Time Statistics window 833
Real-time Statistics window 836
Recently Used Ranges 802
Record button 109
Record Menu 87, 88
recorded activity 107
recording 131, 335

stopping 110
Recording button 173
Recording Options 131, 335
command 131, 149, 150, 335
dialog box 131, 335
files 111
Filter Out 146
Jammer Action 146
loading 356
saving 149, 355
settings 149, 357
Simple Mode 133, 336
Recording Options command 108
recording progress 105
Recording Progress Bar 105
Recording Rules
buttons 170
toolbar 170
Recording Rules Events 183
recording status 105
Recording Type 152, 357
Remove 784
Report Menu 88
Report menu 751
reports 750
Reset Column Widths 793
resizing 532
Resources 173
Response Time 824, 856
Retain Decoded Files 738
Row Selection 774
Run verification scripts command 877
Running Disparity 434

S

Save As command 111
Save As Default 356, 747
Save button 746
Save packet range command 113
saving 111, 746
BitTracer 453
Saving Recording Options 151, 357
scrambled format 434
SCSI level decode 610
Search 105
command 679
Search Bwd message 735
search direction 107
Search For menu 707
Search Fwd message 735
Search Menu 89
Search On section 444
Search Order section 444
Search Pattern window 444
Search window
BitTracer 443
searching 679
Seconds radio button 681
Send command 128
Sequence Cell 172
Sequence State 175, 180, 181, 182
set IP Configuration 35
Set IP Mode Static 35
Set Marker command 549, 793
Set Marker with Text command 436
Set Range Near Packet xxx 802
Set Range to Whole Trace 802
Setting Default Recording Options 149, 355
setting markers 548
Settings button 878
Settings window 878
Setup Menu 86
short format 531
shortcuts 104
Show Configuration Space for xxxx 820
Show Header Fields command 538
Show Header Fields dialog box 537
Show Number of Transitions checkbox 807
Show Packet in Raw Trace 446
Show Raw 10b Codes command 537
Simple and Advanced Mode 140
small triangle 531
Snapshot recording type 138, 340
software 71
installation 47
update 881
SOP and SCSI PCIe SSD Device Configuration 875
SOP level decode 609
Specification view 442
Specify Action command 172
Speed LEDs
33
Split level decode 564
Split Transaction
metrics 827
Split Transaction Level graphs 830
Split Transaction Performance 827, 856
Spreadsheet View 555
StandardSettings.rec file 150, 356
Start menu 57
Statistics Accumulation area 836
Status Bar 105

Status bar 72
Stop button 110
Stop option 110
stopping recording 110
Summit M5x 25, 28, 335
Summit M5x front panel 33
Summit M5x rear panel 38
Swap Recording Channels 154, 358
Swizzling Config... 168
Symbol window 440

T
text files 116
Throughput 856
Tight Columns 774
time between DWORDs 793
Time Coverage 856
Time Stamp 738
time value 794
time-based averaging 829
Timer 237
Timestamp at the beginning 738
Timing and Bus Usage Calculator 855
Timing Calculations command 854, 855
Timing Calculator dialog box 855
Timing measurement
  BitTracer 435
Timing window 437
Title bar 72
TLP Header Properties dialog box 199
TLP Prefix Packet Properties dialog 200
To 122
to Generator File Format 121
To packet # field 127
To Packet field 113
Toggle Search Direction command 735
Tool tip Display 792
Toolbar 72, 169
  72
Tools Menu 98
Tools menu 751
Tooltips 104
trace
  cells 532
  exporting 116
  files 111
  metrics 825
  saving 111
Trace Filename and Path 148, 355
Trace View Mode 738
Trace Viewer 57
traces
  searching 679
traffic 531
  analyzing 749
Traffic Speed pane 802
Traffic Summary
  buttons 774
  metrics 827
Traffic Summary window 770
  moving to packets 771
Traffic Type pane 802
triangle 531
Trigger 33
Trigger action 172
Trigger marker 436
Trigger Position 146, 345
Triggering 168
Triggering On (Advanced Mode) 244
Triggering On (Simple Mode) 168

U
Undo Zoom 784, 836
Union option 708
unit 824
unit-based averaging 829
Update Analyzer dialog 881
Update command 881
Update Device command 881
Update License command 881
Update License dialog box 881
updates 881
Uploading 105
Upstream 155, 362
UPSTREAM 1 connector 33
UPSTREAM 2 connector 33
Upstream direction 807
Upstream LED 33
US Ref Clk In 33
USB 34
Use External Reference Clock 156, 362
user-defined markers 436

V
Verification Script dialog box 877
View Data Block command 534, 537
View Menu 96
View Options 795
View Options button 792
View Settings 786
Viewer 57
Viewing Attachments of a Marker 687

W
web site 883
Window Menu 98
Windows® based host machine 71
Wrap 738
Write Requests Performance 827
Writes Response Time 831
Writes Throughput 831

X
X marker 436

Y
Y marker 436
Y Scale Type 784, 836
yellow range delimiters 803

Z
zoom 792
Zoom Level 738
Zoom to Trace View 784