



CATC[™] Detective[™]
USB Bus & Protocol Analyzer
User's Manual

Version 2.21

1 October 1998

Copyright © 1996–1998, Computer Access Technology Corporation (CATC)

TABLE OF CONTENTS

1. INTRODUCTION.....	1
1.1 USB OVERVIEW.....	1
2. CATC DETECTIVE USB BUS & PROTOCOL ANALYZER	2
2.1 GENERAL.....	2
2.2 CATC DETECTIVE SYSTEM COMPONENTS	2
2.3 THE CATC DETECTIVE ISA CARD CONFIGURATION.....	3
2.4 THE DETECTIVE USB PROBE	4
2.4.1 External Triggers	5
2.4.1.1 The Manual Trigger Push-Button	5
2.4.1.2 TRG Signal Generation.....	5
2.5 SYSTEM SETUP.....	6
2.5.1 PC Connection	6
2.5.2 USB Connection	7
3. SOFTWARE INSTALLATION (ALL VERSIONS)	8
3.1 GENERAL.....	8
3.1.1 Standard Version (Win 3.1 & Win 95)	9
3.1.2 Standard Version (Win NT).....	9
3.2 RUNNING THE SOFTWARE.....	10
4. THE CATC DETECTIVE SOFTWARE.....	10
4.1 GETTING STARTED.....	10
4.2 THE MAIN DISPLAY WINDOW.....	10
4.2.1 The Status Bar	11
4.2.1.1 Device Class Status	12
4.2.1.2 Recording Options Status	12
4.2.1.3 Search Status.....	12
4.2.1.4 Recording Status	12
4.2.2 USB Traffic Error Displays.....	13
4.3 THE FILE MENU	13
4.3.1 Open.....	14
4.3.2 Close	14
4.3.3 Save As... ..	14
4.3.4 Save As Text... ..	14
4.3.5 Edit Comment.....	14
4.3.6 Printer Setup... ..	15
4.3.7 Print... ..	15
4.3.8 Exit	15
4.4 THE SETUP MENU.....	15
4.4.1 Recording Options... ..	16
4.4.1.1 Trigger Selection.....	16
4.4.1.1.1 Manual Trigger	17
4.4.1.1.2 External Start Trigger	17
4.4.1.1.3 External Stop Trigger.....	17
4.4.1.2 Idle State Recording Selection	17
4.4.1.3 Connection Speed Selection	18
4.4.1.4 File Name.....	18
4.4.1.5 Save... (Recording Options)	18
4.4.1.6 Load... (Recording Options)	18
4.4.1.7 Save As Default (Recording Options).....	18
4.4.1.8 Buffer Size	19
4.4.2 Display Options.....	19
4.4.2.1 View Type.....	20
4.4.2.2 Data Presentation	20

4.4.2.3 Field Formats	21
4.4.2.4 Hidden Elements	22
4.4.2.5 Field Colors	23
4.4.2.6 Save... (Display Options)	23
4.4.2.7 Load... (Display Options)	23
4.4.2.8 Save As Default (Display Options)	23
4.4.2.9 Display Configuration Name	24
4.5 THE RECORD MENU	24
4.5.1 Start	24
4.5.2 Stop	24
4.6 THE REPORT MENU	25
4.6.1 File Information	25
4.6.2 Timing Calculations	26
4.6.3 Packet Error Summary	28
4.6.4 Transaction Error Summary	28
4.6.5 Traffic Summary	29
4.6.6 Saving Summaries as Text Files	30
4.7 THE VIEW MENU	31
4.7.1 Add View	31
4.7.2 Hide SOF	31
4.7.3 Hide NAKed Transactions	32
4.7.4 Zoom In	32
4.7.5 Zoom Out	32
4.7.6 Set Current Zoom Value as Default	32
4.8 THE DECODE MENU	32
4.8.1 Select Device Class...	32
4.8.2 Decode Device Request...	33
4.8.2.1 Decoded Standard Requests	35
4.8.2.2 Decoded Hub Class Requests	40
4.8.2.3 Decoded Requests for Other Device Classes	42
4.9 THE SEARCH MENU	42
4.9.1 Go to Packet...	43
4.9.2 Go To Marker	43
4.9.3 Find...	43
4.9.3.1 Find PID	45
4.9.3.2 Find Error Condition	46
4.9.3.3 Find Frame	46
4.9.3.4 Find ADDR and ENDP	47
4.9.3.5 Find Static Bus Event	47
4.9.3.6 Find Data String	48
4.9.4 Next	48
4.10 THE WINDOW MENU	48
4.11 THE HELP MENU	48
4.12 THE DATA FIELD VIEW POP-UP MENU	49
4.13 THE PACKET MARKER & TIMING POP-UP MENUS	49
4.14 THE DEVICE DECODING POP-UP MENUS	50
4.15 THE I/O OPERATION POP-UP MENU	51
5. HOW TO CONTACT CATC	53
6. WARRANTY AND LICENSE	53

1. INTRODUCTION

The CATC **DETECTIVE** USB Bus & Protocol Analyzer is an invaluable development and test tool for Universal Serial Bus designers. When connected to any point in a USB network, the Detective USB analyzer, like the CATC Inspector™ advanced USB analyzer, continuously monitors all bus activities and alerts the user to any abnormal bus conditions in an easy to use, menu driven, Windows software environment.

Detective Features:

- USB bus & protocol analyzer, compatible with the CATC Inspector advanced USB analyzer and the CATC Traffic Generator™
- external, high impedance probe connects non-intrusively to any branch of a USB system
- captures both full- and low-speed USB traffic
- sophisticated software analyzes all bus transactions, identifies and highlights abnormal bus conditions, and decodes generic device class, hub class, and other standard device class messages
- easy to use Windows environment (Win 3.1, Win 95, and Win NT)
- tested for compliance with the USB specification
- one year warranty and hot-line customer support
- non-recording, view-only version of software available (no hardware required)

This document explains how to install the CATC Detective hardware and software in your PC. It also explains how to connect and activate the analyzer in a USB system environment.

1.1 USB Overview

USB is an open industry standard, providing a simple and inexpensive way to connect up to 127 devices to a single computer port. Keyboards, mice, tablets, digitizers, scanners, bar-code readers, modems, printers, and more can all run at the same time. USB devices plug into any platform that supports the standard, from notebooks to desktop PCs to workstations.

USB is a dynamically reconfigurable serial bus with an elementary data rate of 12,000,000 bits/sec, based on off the shelf, low cost micro-controller technology. Its modular layered software protocol supports sophisticated device drivers and application programs.

Please refer to the USB Specifications for details on the USB protocol. The USB specifications are available from the USB Implementers Forum at:

USB IF

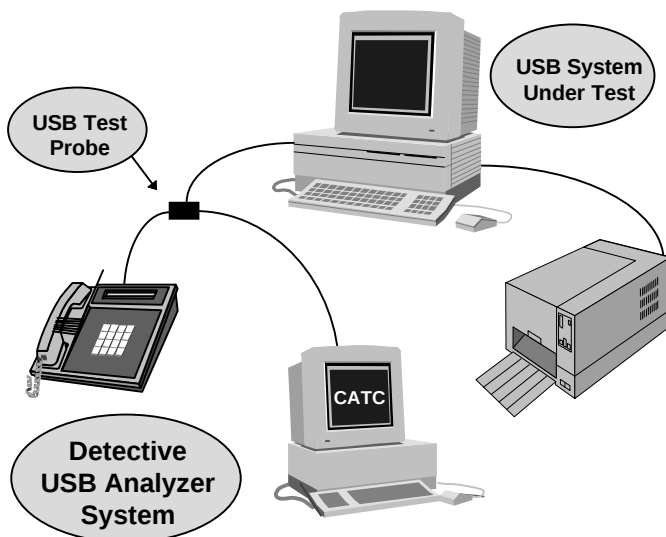
M/S JF2-51
2111 NE 25th Avenue
Hillsboro, OR 97124

Tel: +1/ 503 264 0590
Fax: +1/ 503 693 7975
Web: <http://www.usb.org/>

2. CATC DETECTIVE USB BUS & PROTOCOL ANALYZER

2.1 General

The CATC Detective USB Bus & Protocol Analyzer captures, analyzes, and saves USB traffic data, based on a user-specified trigger signal, which can be supplied manually, programmatically, or via external hardware.



The Detective USB analyzer is designed to turn a 386/486 or Pentium class PC into a USB test station. The PC itself does not need to have a USB interface. The Detective package includes an add-in ISA card, an external Detective Probe, USB and Probe cables, an external trigger cable set, a sophisticated software program running under Microsoft Windows (3.1, 95, and NT versions), and comprehensive product documentation (including on-line help).

The Detective analyzer uses an external high impedance USB Probe to connect to and monitor the two USB wires (D+ and

D-); it translates the raw differential data into a single NRZI bit stream, samples the data with the recovered synchronized clock, and stores the resulting bit stream on disk. The analyzer also detects and reports the static bus conditions Suspend, Resume, Reset, and Idle.

The Detective software scans the collected data and displays it in several meaningful formats. The user can view the data as a continuous stream, or as complete transactions. In continuous mode, the analyzer fills the entire display line with data; in transaction mode, each line is dedicated to one bus transaction, such as token, data, or handshake.

The Detective software provides a powerful search function that enables investigation of particular bus events, with the software identifying and highlighting specific events such as Bad PID, Undefined PID, Bad CRC, Bad Stuffing Bits, Missing Frames, etc.

In addition to immediate analysis, the user can print any part of the data and save all or selected portions of the data on disk for later viewing. The program also provides a variety of timing information.

The Detective USB analyzer comes with a one year warranty and hot-line customer support.

2.2 CATC Detective System Components

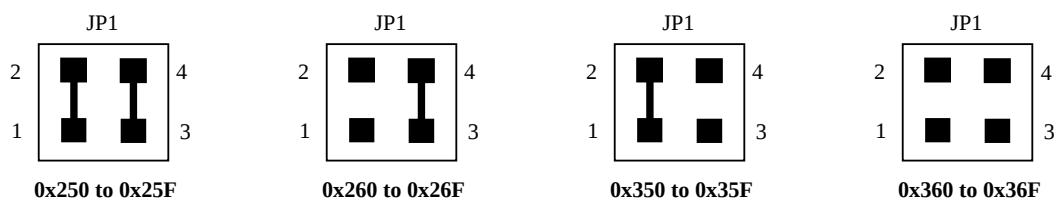
The CATC Detective package includes the following components:

- a CATC Detective ISA add-in card for the PC (approximately 4.2×7-inch printed circuit board with a DB15 connector in a mounting bracket on the side)
- an external, non-intrusive USB Detective Probe (approximately 4.5×2.5×1.5-inch box with a DB15 connector and two USB connectors)

- a six foot, male-to-male DB15 (15-pin) cable to connect the Probe to the ISA card
- a USB cable
- an external trigger cable-set to connect the Probe to a PC parallel port; this is comprised of two cables:
 - a one foot, 10-pin ribbon cable with a 2×5 header connector on one end and a 25-pin DB25 connector on the other
 - a three foot 25-pin cable with DB25 connectors on each end (one male, one female)
- two diskettes with the associated application software program, for operation under Microsoft Windows 95, Windows 3.1, or Windows NT
- comprehensive product documentation, including on-line help

2.3 The CATC Detective ISA Card Configuration

The CATC Detective ISA card uses one of four user defined PC I/O address ranges to communicate with the Detective software. The 2×2 header jumper block, JP1, located at the top of the board next to the 48MHz crystal oscillator, allows selection of one of the four designated I/O address ranges. To select a specific I/O address range, position the two jumpers between pin pairs 1/2 and 3/4 as follows:



I/O Address selection jumpers

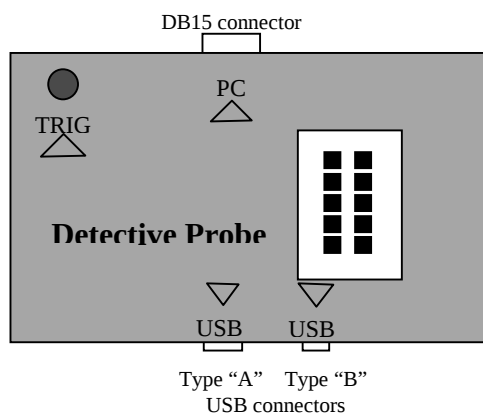
The card is shipped pre-configured with both jumpers installed for addresses 0x250 to 0x25F. After system installation and startup, the CATC Detective software will attempt to communicate with the board. If required, the software may request changing of the jumpers to a different setting. Any of the other three settings above can be tried by removing one or both of the JP1 jumpers. After changing the jumper settings, restarting the Detective software will retry communication with the board. The software will configure itself automatically to the selected jumper settings.

The CATC Detective card uses no interrupt request (IRQ) lines on the ISA bus; no IRQ setting is required.

Note: If none of the four I/O address range settings works properly, please contact CATC.

2.4 The Detective USB Probe

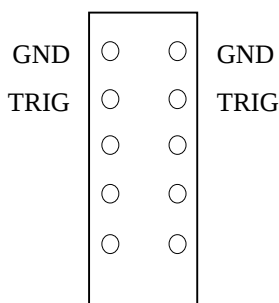
The Detective USB probe is an external box, about 4.5×2.5×1.5 inches, with a female DB15 connector on one side and two USB connectors (one A-type and one B-type) on the other. The probe is designed to connect to any point in the USB system as a passive listening device, without interfering with bus traffic. See the System Setup section for details on connecting the Probe to a system.



In addition to physically connecting the analyzer to the USB system, the Probe includes special circuitry to assist in generating an external trigger signal. Two components are associated with this external trigger mechanism:

- The 10 pin trigger header
- The TRIG push button

Inside the CATC Detective Probe box is a 10-pin external triggering header, arranged in 5 rows of 2 pins each, and easily accessed through an opening in the protective cover of the Probe. The triggering header signal pin assignment is detailed below:



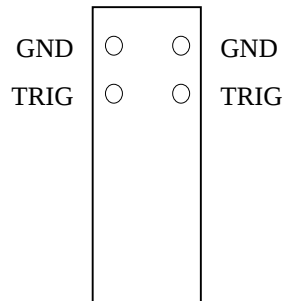
TRIG is an external trigger input to the CATC Detective system, and is duplicated on 2 of the pins as marked. This signal is tied through a 4.7kΩ pull-up resistor to Vcc on the Detective ISA card, and is connected to the input of a FAST logic circuit. To activate the external trigger signal, it must be pulled to a TTL-low level for at least 8 USB bit times (0.67 microseconds for a full speed branch and 5.33 microseconds for a low speed branch). When the Detective software is set to record using an external trigger mode (External Start or External Stop), the low level on this pin will activate either the start or the end of the recording session.

The TRIG push button is located on top of the Detective Probe box, and can be used to manually generate the external trigger signal. To activate this feature, the analyzer must be in either the

“External Start” or the “External Stop” recording mode. Once one of these recording modes has begun, the analyzer waits for an external trigger signal to either start or end the recording session. Manually pushing the TRIG button will assert the external trigger signal and thus affect the operation.

Note: Early versions of the Detective USB Probe have either two A-type USB connectors or two A-type USB connectors and one B-type USB connector.

Note: Early versions of the USB Detective Probe have a 2×2 pin header instead of the 5×2 pin header. This header carries the same TRIG signal described above. The 2×2 triggering header signals pin assignment is illustrated below:



2.4.1 External Triggers

The CATC Detective Probe offers two ways to generate an external trigger to control a recording session: the “Manual Trigger” push-button, and the “TRG” pin in the Probe Triggering Header.

2.4.1.1 The Manual Trigger Push-Button

The simplest way to generate an external trigger (when enabled in the Recording Options dialog box) is by manually activating the Manual Trigger push button located on top of the Probe.

2.4.1.2 TRG Signal Generation

In order to view a particular USB event (to determine—for example—how a particular device behaves during the initialization phase), it is necessary to activate the CATC Detective analyzer to record the bus activities during a specific time period. If the USB host allows manual control of the bus traffic, then in theory the CATC Detective recording could be started manually at the same time. Because of USB speed, correspondingly slow human reaction time, and buffer memory limitations (1 Mbytes), however, manually coordinating the host actions with the Detective recording is generally impractical.

A simple solution is to generate a signal in the USB host PC, or in the USB hub or device under observation, that will be synchronized to the particular event to be recorded. Such a signal can be generated on the PC by calling a small software routine (see sample code below) that uses a standard I/O Write command to a specific pin on an available serial or parallel port.

Alternatively, the TRG signal might be generated by programming one of the general I/O ports on the USB controller in the hub or device.

A short cable connects this (active low) signal to the TRG pin of the Probe Triggering Header.

TRIG Signal Sample software Routine

```
case IOCTL_START_TRIGGER_RTS:

    switch (gTriggerDongle) {
        case SERIAL_PORT_TRIGGER_DONGLE:
            outp (0x3fc, 00);
            break;

        case PARALLEL_PORT_TRIGGER_DONGLE:
            outp (0x378, 00);
            break;
    }//switch
    break;

case IOCTL_STOP_TRIGGER_RTS:

    switch (gTriggerDongle) {
        case SERIAL_PORT_TRIGGER_DONGLE:
            outp (0x3fc, 02);
            break;

        case PARALLEL_PORT_TRIGGER_DONGLE:
            outp (0x378, 0xFF);
            break;
    }//switch
    break;
```

2.5 System setup

The Detective is designed to work on any PC with a (16-bit) ISA slot. The PC does not have to be equipped with a USB interface in order to work with the Detective analyzer. Two steps are involved in the setup of the system hardware: connecting to the PC and connecting to the USB system under test.

2.5.1 PC Connection

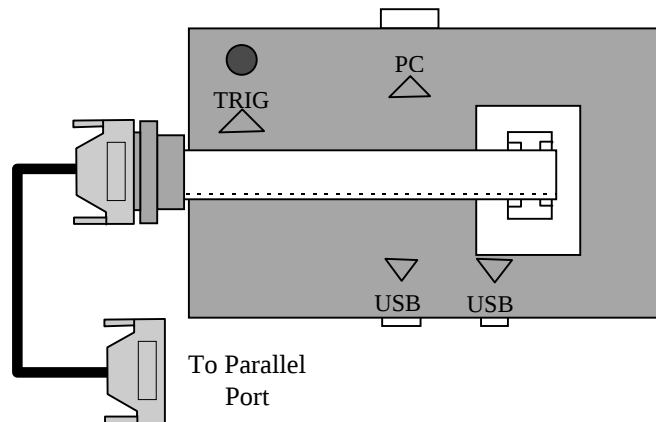
Turn off the PC power, and plug the Detective ISA card into any (16-bit) ISA slot in the PC's motherboard.

Connect the 15-pin cable between the CATC Detective Probe connector and the ISA card. Note that both the USB Detective Probe and the USB Detective card use the same DB15 female connector, which is similar to the standard PC graphic display VGA connector.

When external triggering initiation from the USB host software is desired, connect the external trigger cable set between the USB Detective Probe header and the PC parallel port as follows (see diagrams below):

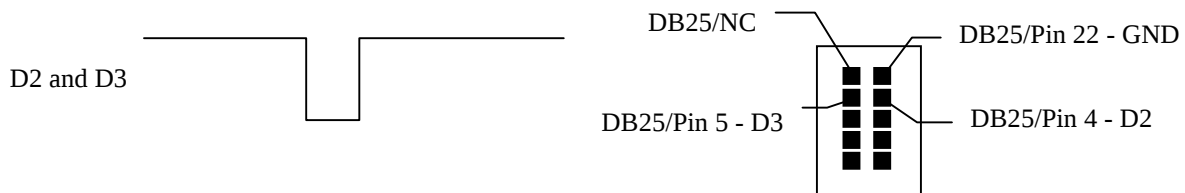
- Plug the 10-pin ribbon cable connector (included with the USB Detective package) into the 2×5 header of the USB Detective Probe.

- Connect the DB25 male connector on the other side of the ribbon cable to the DB25 female connector of the 25-pin cable (included with the USB Detective package).
- Connect the DB25 male connector on the other side of the 25-pin cable to the parallel port of the PC running the USB host software.



Once the Probe trigger pin is connected to the parallel port, a simple write command to the parallel port will trigger the USB Detective recording process (see sample software routine above).

The two trigger pins on the Probe header are shorted together. The external trigger kit cables connect one of the trigger pins to the parallel port D2 signal, and the other pin to the parallel port D3 signal (pins 4 and 5 of the DB25 connector). The Detective trigger is activated by generating a negative pulse simultaneously on both D2 and D3 for at least 8 USB bit times (0.67 microseconds for a full-branch and 5.33 microseconds for a low-speed branch).



PC power may then be restored.

2.5.2 USB Connection

Locate the CATC Detective Probe near the USB system under test.

In the USB system, at a point where USB bus traffic is to be analyzed, open a connection and reconnect the open link through the CATC Detective Probe as follows:

- Connect a USB cable between one side of the open connection and one of the two USB receptacles on the CATC Detective Probe (the two receptacles are functionally identical).
- Connect another USB cable between the other side of the open USB connection and the other USB receptacle of the CATC Detective Probe.

Note: CATC recommends the use of USB cables shorter than 2 meters (6 feet) for all connections to the USB Detective Probe.

Note: The B-type USB connector on the Detective Probe is normally connected to the upstream USB port, while the A-type connector is connected to the downstream port.

Note: Early versions of the USB Detective Probe do not contain the B-type USB receptacle. These Probes have only the two A-type USB connectors..

The CATC Detective Bus & Protocol Analyzer hardware is now ready for operation.

3. SOFTWARE INSTALLATION (ALL VERSIONS)

3.1 General

The CATC Detective software is available in four different versions:

- standard version for Windows 3.1 and Windows 95
- standard version for Windows NT
- view-only version for Windows 3.1, Windows 95, and Windows NT (This version does not require the USB Detective hardware; it is used only for viewing and analyzing previously created USB traffic files. *Information on installing and using this version can be found in the CATC Inspector Advanced USB Bus & Protocol Analyzer User's Manual.*)
- demo version for Windows 3.1, Windows 95, and Windows NT (This version also does not require the Detective USB hardware; it is made available for product demonstration purposes, and can be used only for viewing and analyzing a specific set of USB traffic files. *Information on installing and using this version can be found in the CATC Inspector Advanced USB Bus & Protocol Analyzer User's Manual.*)

The software diskette label identifies the program version. To install the CATC Detective software, run the installation program from the Detective software diskette, and follow the instructions on the screen. Note that to install the standard version on Windows NT systems, it is necessary to log in as administrator.

- For Windows 3.1 and 95 run the 'install.exe' installation program.
- For Windows NT run the 'setup.exe' installation program.

The installation program creates a program group for the Detective application once it has finished copying all the files. The icon for an *Uninstall* program is also placed in the program group. This *Uninstall* program can be run later, if desired, to remove the CATC Detective software from the system.

To run the software, double-click on the Detective icon in the program group created during installation. Section 4 describes the software in detail.

3.1.1 Standard Version (Win 3.1 & Win 95)

The installation program copies the following files to the PC's hard drive.

To the \USBDTCTV directory (or that otherwise specified by the user):

- USBDTCTV.EXE executable code of the CATC Detective program
- USBDTCTV.DLL DLL for the CATC Detective program
- CLS_HID.DLL DLL for HID Class device decoding
- USBDTCTV.HLP CATC Detective help file
- DEFAULT.OPT default DISPLAY function settings
- DEMO.USB sample USB traffic file

to the \WINDOWS\SYSTEM directory:

- USBDTCTV.386 Windows CATC Detective virtual device driver
- CTL3D.DLL Windows 3D Control Library
- CTL3DV2.DLL Windows 3D Control Library

to the \WINDOWS directory:

- CLSDECOD.INI USB Device Class decoding initialization

In the \WINDOWS\SYSTEM.INI file, the installation program adds a reference to the CATC Detective driver in the [386Enh] section.

device=usbdctv.386

3.1.2 Standard Version (Win NT)

The installation program copies the following files to the PC's hard drive.

To \Program Files\CATC\Detective directory (or that otherwise specified by the user):

- USBDTCTV.EXE executable code of the CATC Detective program
- USBDTCTV.DLL DLL for the CATC Detective program
- CLS_HID.DLL DLL for HID Class device decoding
- USBDTCTV.HLP CATC Detective help file
- DEFAULT.OPT default DISPLAY function settings
- DEMO.USB sample USB traffic file

to the \WINDOWS\SYSTEM32 directory:

- CTL3D32.DLL Windows 3D Control Library

to the \WINDOWS directory:

- CLSDECOD.INI USB Device Class decoding initialization

to the \WINDOWS\SYSTEM32\DRIVERS directory:

- USBDTCTV.SYS Windows NT CATC Detective device driver

The installation program modifies the system registry to install the CATC Detective driver.

3.2 Running The Software

The CATC Detective software is a Windows application, and can be run under Windows 3.1, Windows 95, and Windows NT. To start the program, double-click on the file name (located with the Explorer or equivalent service), or on the CATC Detective icon created during the software installation.

The program will start with the main window active.

4. THE CATC DETECTIVE SOFTWARE

4.1 Getting Started

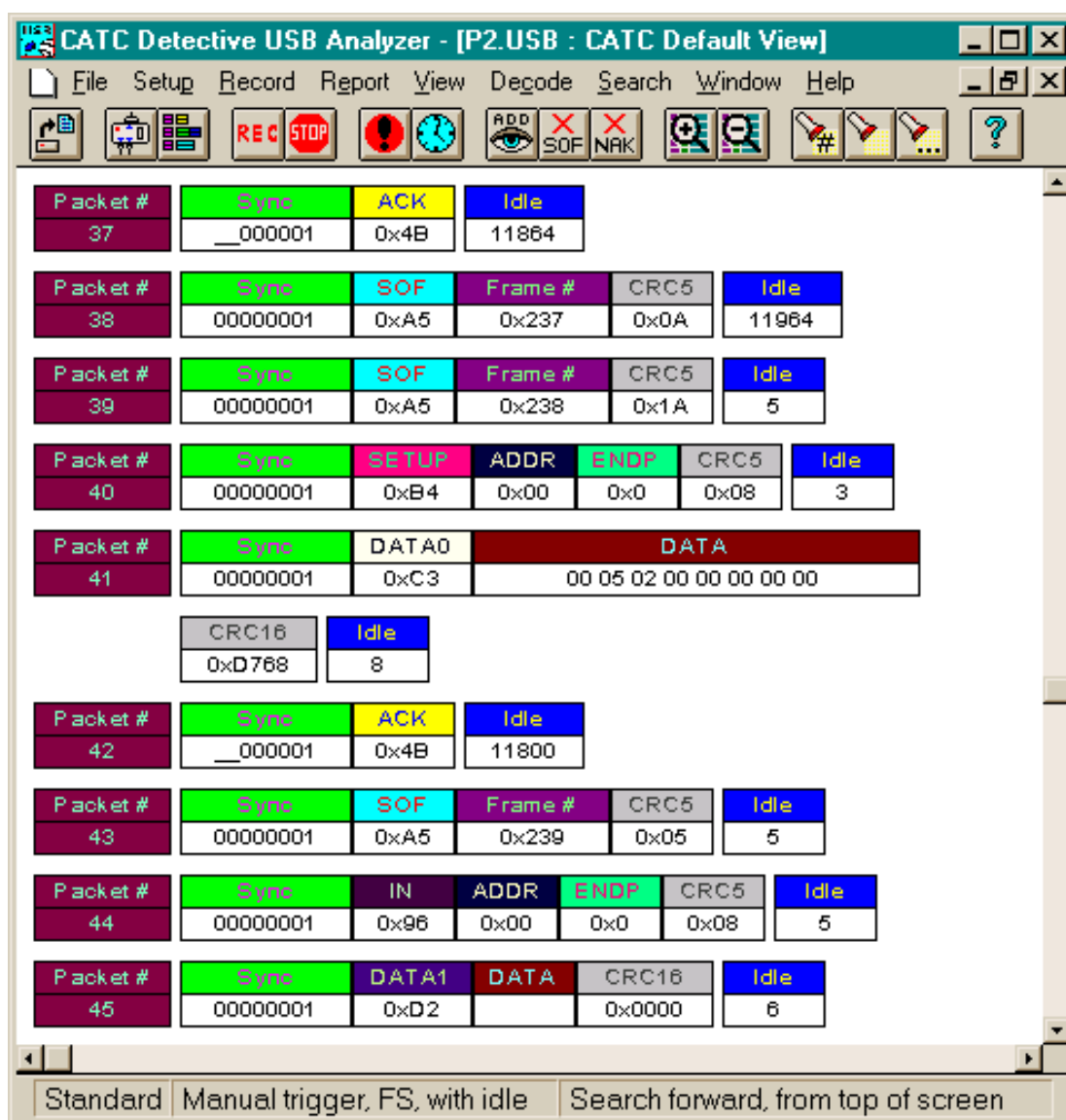
The CATC Detective Bus & Protocol Analyzer continuously monitors all USB activity. At the operator's discretion, the analyzer will record a snap shot view of the bus traffic. It will store the data in a file (initially named "data.usb") on the system hard drive and display the information on the screen. Once the information is captured and is displayed, it can be viewed and analyzed using a variety of tools. The data can be stored permanently, and conveniently viewed on any PC equipped with the CATC Detective software. A view-only version of the software permits subsequent viewing without the need for any Detective hardware.

4.2 The Main Display Window

The CATC Detective analyzer's main display incorporates the following set of Windows pull-down menus:

- File
- Setup
- Record
- Report
- View
- Decode
- Search
- Window
- Help

Clicking on any of these menus will expand it, offering various function selections. Subsequent sections of this document describe the operation of each menu item.



Additionally, several of the most frequently used functions can be activated by specific icons located on the toolbar immediately below the pull-down menus. Each icon's functionality is identified in the left portion of the status bar (at the bottom of the window) when the pointing device cursor moves over the icon. Finally, several operations can be invoked by clicking directly on the affected packet fields (using pop-up menus).

4.2.1 The Status Bar

The status bar is located at the bottom of the Detective main display window. The functionality of each icon and menu item is briefly described in the bar when the pointing device cursor moves over the icon/item. At other times, the bar is divided into three segments, used to display the following:

4.2.1.1 Device Class Status

The center segment displays the currently selected USB Device Class, used when displaying decoded Device Class requests. As described under Recording Status, below, this information will be temporarily overwritten during recording activity.

4.2.1.2 Recording Options Status

The center segment displays the current Recording Options, consisting of trigger state ("Manual", "ExtStart", or "ExtStop"), idle recording state ("with idle" or "no idle"), and connection speed ("FS" or "LS", for full- and low-speed respectively). As described under Recording Status, below, this information will be temporarily overwritten during data-saving operations.

4.2.1.3 Search Status

The rightmost segment displays the current search direction (forward or backward) and start position (from start/end of file, or from last match).

4.2.1.4 Recording Status

During recording activity, the leftmost segment temporarily displays the current recording status. When the user activates the Record function, this segment will flash one of the following messages (depending on the selected Recording Options):

Recording...

Awaiting trigger to start recording...

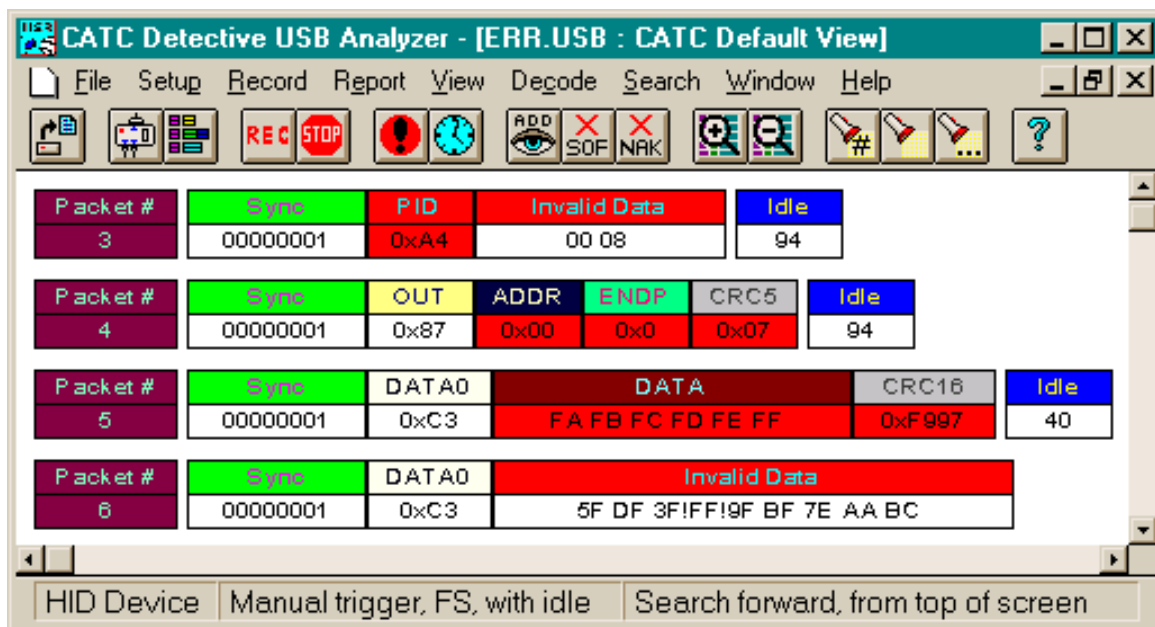
Recording; awaiting trigger to stop...

After the Detective stops recording, the flashing message changes to "Saving data...", which is a multiphase operation. In the first phase, the software scans the recorded data stream, computing the packet boundaries; during this phase, the center segment of the status bar displays the packet number currently being processed by the software. In the second phase, the traffic data is copied to disk, using the default file name "data.usb" (overwriting any previous version of this file).

When the software has finished saving the data, the recorded data file appears in the main display window and the recording status window is cleared. The display will begin with the first packet in the traffic file.

4.2.2 USB Traffic Error Displays

The analyzer detects a variety of USB traffic errors, and displays them as follows:



Packet #3 above has an invalid PID value; the PID value field is colored red, and the rest of the packet is marked as "Invalid Data". Packets #4 and #5 have incorrect CRCs; the CRC value field is colored red, as are the preceding fields associated with the CRC value. Packet #6 has bit stuffing errors; the affected field is marked as "Invalid Data", with any byte containing a bit stuffing error bracketed with exclamation marks ("!"). *When a bit stuffing error occurs, it is no longer possible to determine the correct data byte boundaries; thus all affected data (through the end of the packet) are collected into a field labeled "Invalid Data", displaying the raw data received, from left to right (regardless of the order specified in the Field Format Display Options).*

A related situation is the special case of Sync fields. Occasionally, the analyzer does not synchronize with the data stream until part way through the Sync token; such situations are marked by replacing the missed leading zero bits with underscore ("_") characters. This situation is not considered an error, but the analyzer reports only bits it has actually acquired.

In addition to packet errors, the Detective analyzer also detects a wide variety of transaction errors. Reporting of these and other errors is discussed in section 4.6 ("The Report Menu").

4.3 The File Menu

The file menu behaves as a standard Windows File menu, allowing the operator to open existing analyzer traffic data files from previous sessions, save the data file from the current session, create/edit data file comments, and print all or selected portions of the selected data file.

The File menu includes the following functions:

4.3.1 Open...

Open an existing, previously recorded “*.usb” file (i.e., a CATC Bus & Protocol analyzer USB traffic file).

4.3.2 Close

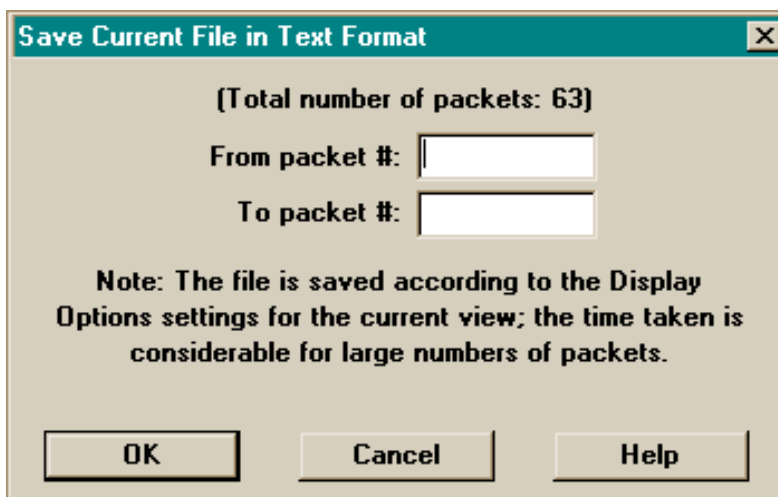
Close an open traffic data file.

4.3.3 Save As...

Save the currently displayed USB traffic data file with a newly-specified file name (more correctly, **Rename...** the file). If this function is not used following the capture of new data (which is recorded in the default file “data.usb”), the next recording will overwrite it. Any file name can be specified, though use of the “.usb” extension is recommended (see “Open”, above); if no extension is specified, “.usb” will be added by default.

4.3.4 Save As Text...

Save all or a selected range of the current USB traffic data file in a text format for further viewing, analysis, and/or printing. Activating this function opens up the following selection box:



Data are saved according to the Display Options settings for the current view. The saved file can be opened with any standard text editor.

4.3.5 Edit Comment

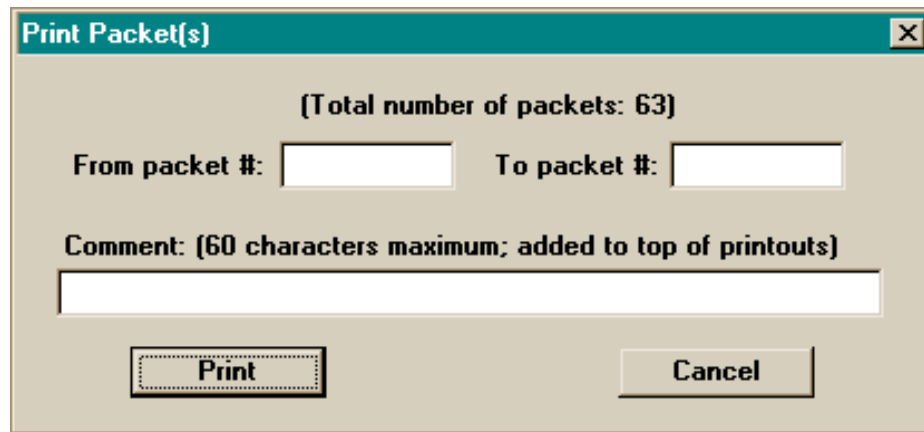
Create, view, and/or edit the 50-character comment field associated with each USB traffic data file.

4.3.6 Printer Setup...

The “Printer Setup...” menu item is a standard Windows function that allows configuring of the printer (paper size, source, orientation, etc.).

4.3.7 Print...

Print all or a selected range of the current USB traffic data file. Activating this function opens up the following selection box:

A screenshot of a Windows-style dialog box titled "Print Packet(s)". The dialog has a light beige background and a dark teal title bar with a close button (X) in the top right corner. Inside the dialog, the text "[Total number of packets: 63]" is centered. Below this, there are two labels: "From packet #:" and "To packet #:", each followed by an empty rectangular text input field. Underneath these fields is a label "Comment: (60 characters maximum; added to top of printouts)" followed by a single-line text input field. At the bottom of the dialog, there are two buttons: "Print" on the left and "Cancel" on the right, both with a 3D effect.

The specified traffic information will be printed as currently displayed, in color or grayscale as supported by the destination printer. Any supplied comment (up to 60 characters in length) will be printed following the current document name at the top of each page.

4.3.8 Exit

Terminate the CATC Detective Windows application.

4.4 The Setup Menu

The CATC Detective software offers many choices for recording, viewing, and analyzing USB traffic. The Setup menu includes “Recording Options” and “Display Options” functions that allow customization of these choices. Both functions are additionally available as individual icons on the toolbar in the main display window.

4.4.1 Recording Options...

The “Recording Options...” menu item enables customization of the recording criteria, using the following dialog box:



This box includes controls for trigger selection, idle state recording, bus speed selection, constraining the memory buffer size, and a variety of file-related functions. Once the desired recording options are specified (by activating the “OK” button), they remain valid until changed again by the Recording Options function.

Note: Selecting the OK button to confirm record option selections does not start recording. To actually record USB traffic, either the “REC” icon or the Record menu’s “Start” item must be activated.

4.4.1.1 Trigger Selection

The CATC Detective supports three modes of data recording triggering:

- Manual
- External Start
- External Stop

The external trigger modes work in conjunction with the trigger (active low) input on the Detective Probe, as previously described under “External Triggers”.

4.4.1.1.1 Manual Trigger

In this mode, the analyzer will start to record when the user activates the “REC” icon or “Start” in the Record Menu, and stop when the CATC Detective on-board buffer memory is full or when the “STOP” icon (or menu function) is activated, whichever comes first.

4.4.1.1.2 External Start Trigger

In this mode, the analyzer **starts** recording when an external trigger signal is detected. This permits recording following a specific point of interest (aided by external decoding).

It is still necessary to “arm” the Detective software by activating the “REC” icon or “Start” in the Record Menu. Actual recording will begin following detection of an external trigger signal, and stop when the CATC Detective on-board buffer memory is full or when the “STOP” icon (or menu function) is activated, whichever comes first.

4.4.1.1.3 External Stop Trigger

In this mode the analyzer **stops** recording when an external trigger signal is detected. This permits recording up to a specific point of interest (aided by external decoding).

The operation is initialized by activating the “REC” icon or “Start” in the Record Menu. At which time the analyzer will start recording immediately, and continuously, until it detects the external trigger signal, or when the “STOP” icon (or menu function) is activated, whichever comes first. The system's buffer memory is filled cyclically until the stop trigger occurs, and thus will hold (a maximum of) the last megabyte of USB data that appeared on the bus prior to the trigger.

4.4.1.2 Idle State Recording Selection

“Idle” is a valid state of the USB physical layer between packets. By default, the CATC Detective analyzer records all bus activity, including the Idle state; in this mode, the available buffer space permits the recording of just under 0.67 second of full-speed (5.36s of low-speed) traffic.



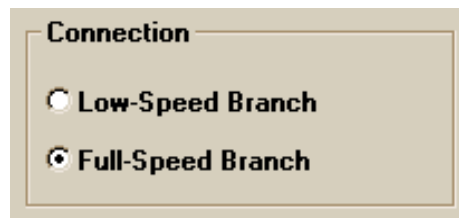
Idle state recording can be disabled by selecting the “Don’t Record” option (in the Idle State panel of the Data Recording Options dialog box, shown above); this will increase the recording time to just under 4 minutes of full-speed traffic (low-speed recording time is traffic-dependent, and could be hours). In this mode the analyzer suspends recording upon detection of the Idle, and resumes upon detection of the start of the next packet (SOP), which is a transition from the J to the K state.

Although this permits greatly increased recording times, there are two associated drawbacks:

1. When bus traffic is at a minimum, it can take a long time to fill the analyzer's recording memory. Once a triggering event has been detected it may still take several minutes before recording stops, due to limited bus traffic filling the memory. This problem can be somewhat alleviated by stopping manually once the trigger has been detected; the analyzer provides an on-screen "triggered" indicator for this purpose.
2. Recording without Idle state eliminates the real-time information, so the CATC Detective software will not be able to support any of the timing related features.

4.4.1.3 Connection Speed Selection

This panel of the Data Recording Options dialog box allows specification of the USB branch where the analyzer is connected. If Low-Speed is specified, the analyzer views the bus traffic as would a low-speed device, switching its internal clock (from the full-speed 12 MHz) to 1.5 MHz clock. Additionally, it inverts the data polarity to provide the software with the correct binary information.



4.4.1.4 File Name...

Use the specified file name when saving the recorded traffic data file; the default name is "data.usb". Any file name can be specified, though use of the ".usb" extension is recommended (see "Open", under "The File Menu", above); if no extension is specified, ".usb" will be added by default.

4.4.1.5 Save... (Recording Options)

Save the currently specified Recording Options for use in future recording sessions. Any file name can be specified, though use of the ".rec" recommended is suggested (see "Load...", following); if no extension is specified, ".rec" will be added by default.

4.4.1.6 Load... (Recording Options)

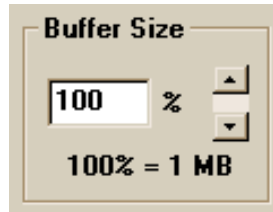
Load a previously saved "*.rec" file, thus restoring a previous set of Recording Options.

4.4.1.7 Save As Default (Recording Options)

The "Save As Default" function is equivalent to the "Save..." function, specifying the file name "default.rec". Whenever the CATC Detective software begins execution, it automatically loads the "default.rec" file, if one exists.

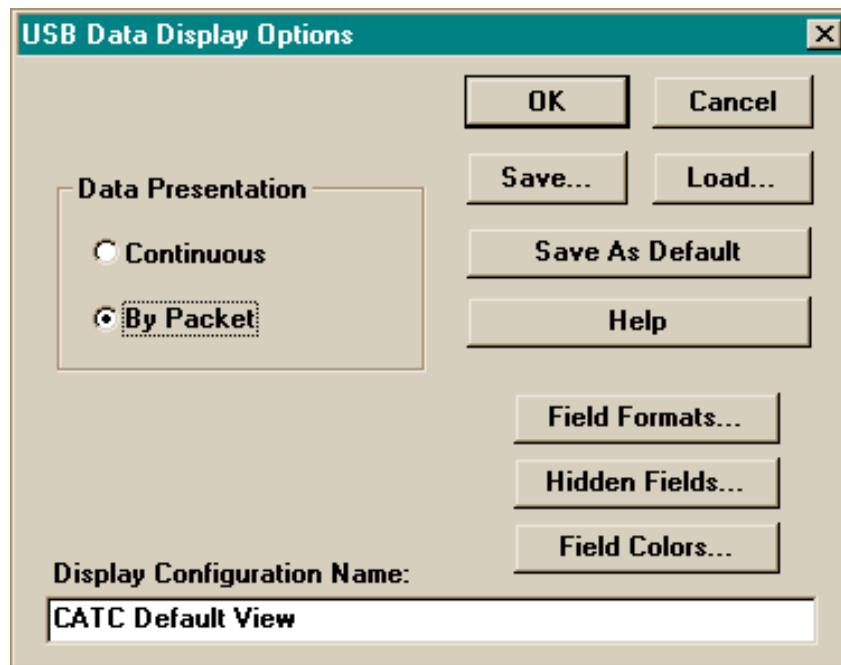
4.4.1.8 Buffer Size

When recording without Idle, or from a low-speed branch, it is often useful to use less than the full buffer space of the Detective analyzer (to save recording time, or reduce the amount of captured data). The “Buffer Size” panel of the Data Recording Options dialog box allows selection of the desired portion (from 10% to 100%) of the buffer memory.



4.4.2 Display Options...

The “Display Options...” menu item allows customization of the way that the recorded USB traffic data files are presented on the screen. The USB Data Display Options dialog box includes control buttons for the selection of data presentation and screen formatting options, plus the ability to save and restore custom display option configurations. The Detective software will display the recorded data as specified, highlighting any packet fields that violate USB specifications (e.g., missing stuff bits, invalid PID type, bad CRC, etc.).



Once the desired options are established (by selecting the OK button), they will remain valid until the Display Options function (which can also be invoked from the Add View function in the Display menu) is used again.

Note: Selecting the “OK” button to confirm the display options selection does not change the current data view. Only newly created views are affected.

4.4.2.1 View Type

The user can choose whether to view recorded data in a “global” fashion (i.e., displaying all of the data) or “by device”. In the latter case, a device is specified by entering its address and, optionally, an endpoint number (if no ENDP is specified, all endpoints are included); subsequently, only SOF (start of frame) packets, and those pertaining to transactions with the specified device will be displayed. Note that the display of SOF and NAKed transaction packets can be independently suppressed (see “Hidden Elements”, below).

4.4.2.2 Data Presentation

Recorded data is displayed either as a “Continuous” stream, or separated “By Packet”, as selected. The following screen duplicates the USB traffic information of the screen shown in section 4.2 (“The Main Display Window”), but uses a continuous mode display:

CATC Detective USB Analyzer - [P2.USB : CATC Default View]

File Setup Record Report View Decode Search Window Help

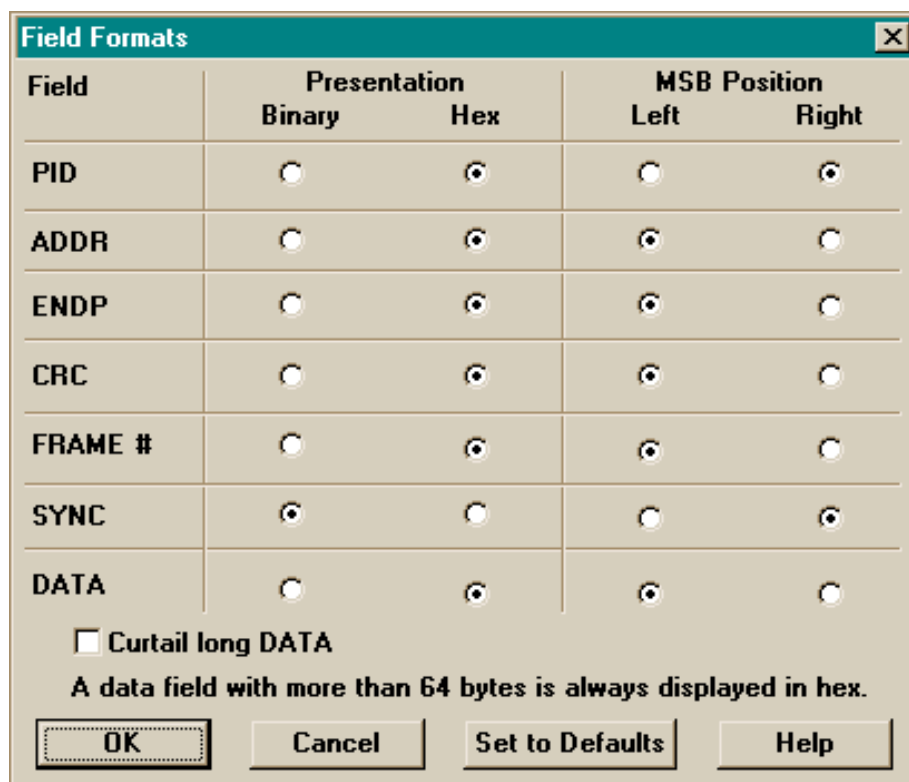
REC STOP ADD SOF NAK

Packet #	Sync	SOF	Frame #	CRC5	Idle	Packet #	
21	00000001	0xA5	0x22F	0x03	11964	22	
Sync	SOF	Frame #	CRC5	Idle	Packet #	Sync	
00000001	0xA5	0x230	0x14	11964	23	00000001	
SOF	Frame #	CRC5	Idle	Packet #	Sync	SOF	
0xA5	0x231	0x0B	11964	24	00000001	0xA5	
Frame #	CRC5	Idle	Packet #	Sync	SOF	Frame #	
0x232	0x09	11964	25	00000001	0xA5	0x233	
CRC5	Idle	Packet #	Sync	SETUP	ADDR	ENDP	CRC5
0x16	5	26	00000001	0xB4	0x00	0x0	0x08
Idle	Packet #	Sync	DATA0	DATA			
3	27	00000001	0xC3	80 06 00 01 00 00 40 00			
CRC16	Idle	Packet #	Sync	ACK	Idle	Packet #	
0xBB29	6	28	00000001	0x4B	11800	29	
Sync	SOF	Frame #	CRC5	Idle	Packet #	Sync	
00000001	0xA5	0x234	0x08	5	30	00000001	
IN	ADDR	ENDP	CRC5	Idle	Packet #	Sync	DATA1
0x96	0x00	0x0	0x08	6	31	_00000001	0xD2

Standard Manual trigger, FS, with idle Search forward, from top of screen

4.4.2.3 Field Formats

The CATC Detective software supports several different formats in which the USB traffic data can be displayed. When the 'Field Formats' button is selected, the following dialog box opens, enabling a choice of viewing mode (either binary or hexadecimal format) for each of the special message fields (Sync, PID, CRC, etc.). In addition, each field can be viewed with the most significant bit (MSB) positioned on its left or right side.



The 'Field Formats' dialog box contains a table with the following structure:

Field	Presentation		MSB Position	
	Binary	Hex	Left	Right
PID	☐	☒	☐	☒
ADDR	☐	☒	☒	☐
ENDP	☐	☒	☒	☐
CRC	☐	☒	☒	☐
FRAME #	☐	☒	☒	☐
SYNC	☒	☐	☐	☒
DATA	☐	☒	☒	☐

Below the table, there is a checkbox labeled 'Curtail long DATA' which is currently unchecked. A note states: 'A data field with more than 64 bytes is always displayed in hex.' At the bottom are four buttons: 'OK', 'Cancel', 'Set to Defaults', and 'Help'.

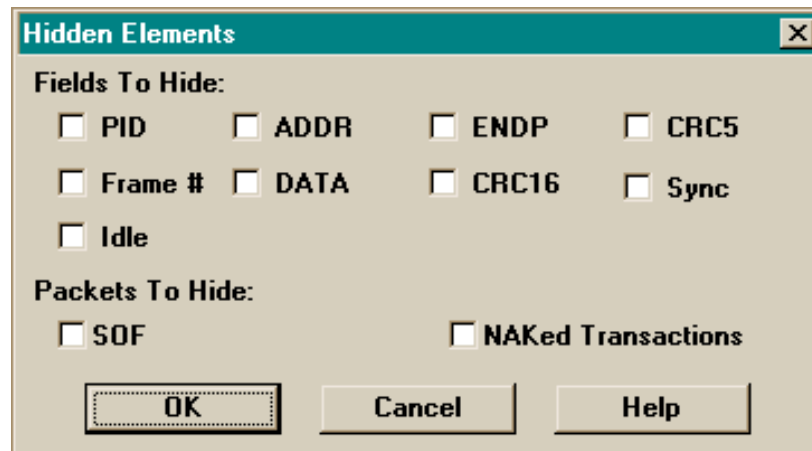
Data fields can sometimes be quite lengthy. To reduce screen clutter, data fields longer than 64 bytes are always displayed in hexadecimal, regardless of the field format specification. In addition, if the "Curtail long DATA" checkbox is marked, data fields longer than 16 bytes will be displayed as their initial two bytes (one byte when in binary mode) plus a remaining byte count. Thus a field that might otherwise occupy several lines of display will be shown as:

DATA
00 01 ... + 254 bytes

It is possible to revert back to the default setting at any time by selecting the 'Set to Defaults' button. After making the desired selections, selecting the OK button will close this dialog box and return to the Display Options dialog box for additional selections.

4.4.2.4 Hidden Elements

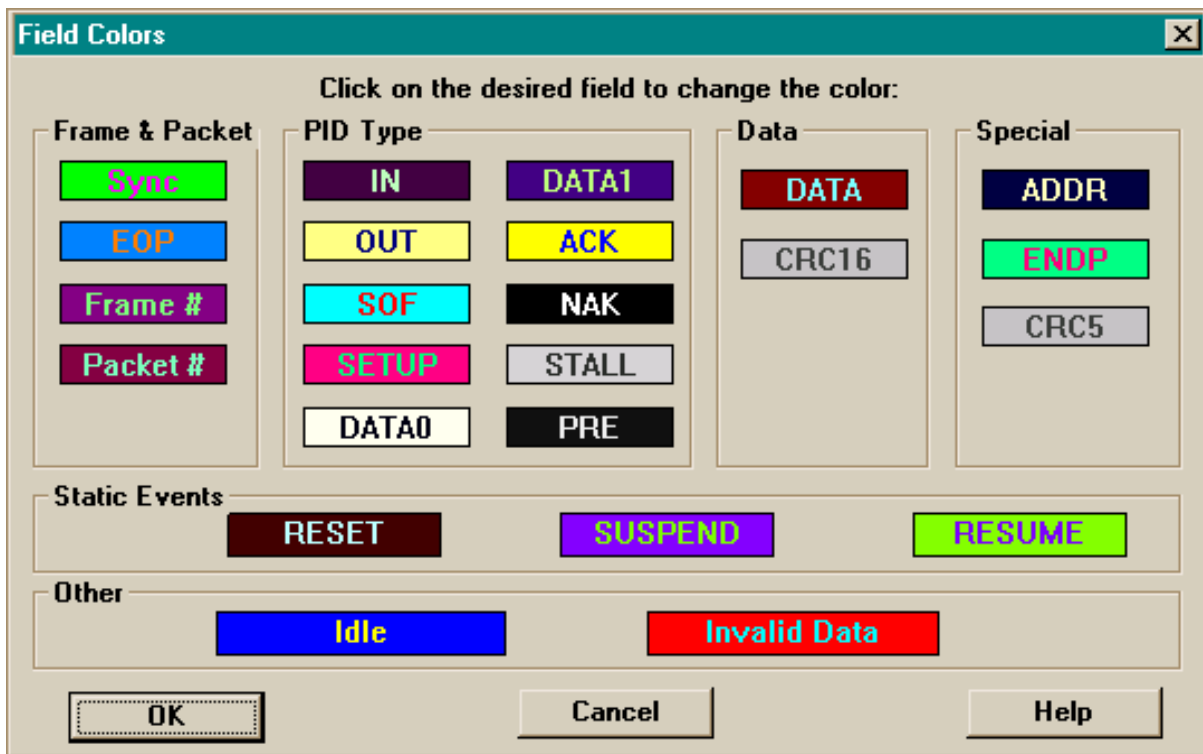
It is occasionally convenient to display only some of the different USB packet fields. For example, eliminating the display of Sync and Idle state fields (in situations where they are not significant) can often simplify, and thus clarify, the traffic display. The Hidden Elements button, which brings up the following dialog box, allows customization of the message fields to be included in the display.



The suppression of certain entire packets may additionally be of benefit; the CATC Detective analyzer enables the removal of all SOF packets, and also those pertaining to any NAKed transaction, from the traffic display. Note that the hiding of SOF and NAKed transaction packets can also be controlled specifically for the current view (see section 4.7, "The View Menu").

4.4.2.5 Field Colors

The Field Colors button allows customization of the color associated with each field in the message, using the following dialog box:



Users may choose to experiment with this option to achieve a color combination that is best suited to a particular graphic system. A brighter color might be appropriate for a specific field that should stand out in the display (e.g. the Setup PID field). Note that the color of an Invalid Data (error) field cannot be changed; it is permanently set to red.

4.4.2.6 Save... (Display Options)

Save the currently specified Display Options for use in future sessions. Any file name can be specified, though use of the ".opt" extension is recommended (see "Load...", following); if no extension is specified, ".opt" will be added by default.

4.4.2.7 Load... (Display Options)

Load a previously saved "*.opt" file, thus restoring a previous set of Display Options.

4.4.2.8 Save As Default (Display Options)

The "Save As Default" function is equivalent to the "Save..." function, specifying the file name "default.opt". Whenever the CATC Detective software begins execution, it automatically loads the "default.opt" file, if one exists.

4.4.2.9 Display Configuration Name

This field is used to enter a text string (30 characters maximum) to be associated with the current set of Display Options. This name will be saved with the option set, and appear as part of the title of the view window that is created using this set of options.

4.5 The Record Menu

The Record menu has two items, “Start” and “Stop”, described below. When the record function is active, the current recording status is displayed in the status bar.

4.5.1 Start

Selecting the Start function instructs the CATC Detective analyzer to begin recording USB traffic data, as specified by the Recording Options.

4.5.2 Stop

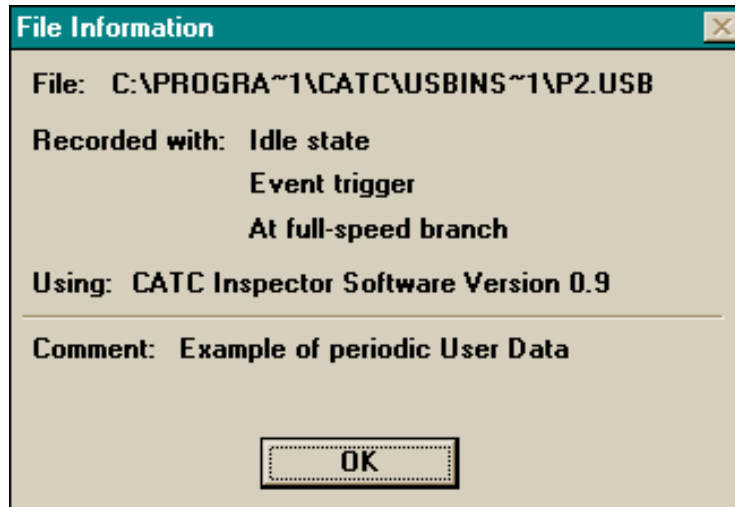
Selecting the Stop function instructs the analyzer to stop the data recording process. This feature is primarily of use when recording low-speed traffic, or not recording Idle states, which could take a long time to fill the recording buffer.

4.6 The Report Menu

The Report Menu contains five items, used to generate information displays concerning the current traffic data view.

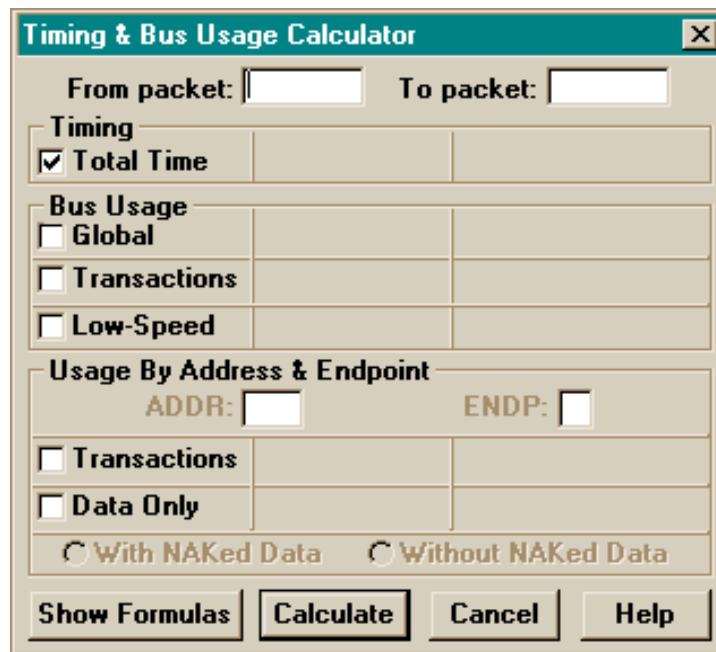
4.6.1 File Information

The File Information menu item displays information about the traffic file currently being viewed, including the recording time and conditions, and any comment line that may have been added to the file.



4.6.2 Timing Calculations

This menu item (enabled only for files recorded with Idle state) opens the following “calculator” display, permitting computation of the time difference between any two packets in the file:



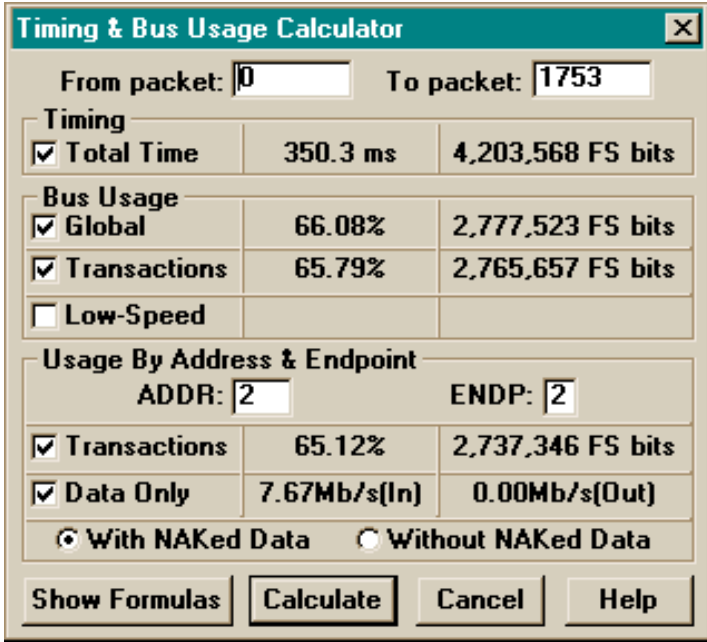
The dialog box is titled "Timing & Bus Usage Calculator" and contains the following fields and controls:

- From packet:** [text box] **To packet:** [text box]
- Timing**
 - ☒ **Total Time**
- Bus Usage**
 - ☐ **Global**
 - ☐ **Transactions**
 - ☐ **Low-Speed**
- Usage By Address & Endpoint**
 - ADDR:** [text box] **ENDP:** [text box]
 - ☐ **Transactions**
 - ☐ **Data Only**
- ☐ **With NAKed Data** ☐ **Without NAKed Data**
- Show Formulas** **Calculate** **Cancel** **Help**

Entering relevant packet numbers and selecting the “Calculate” button results in a display of the packet-to-packet time (measured from start of Sync to start of Sync) in both microseconds (or milliseconds), and bit times. If no packet numbers are entered, the computation is performed over the entire range of packets in the currently displayed file. An appropriate error message is provided if either of the selected packets does not contain a Sync field (i.e., SUSPEND or RESET sequences).

If additional check boxes are marked, further information will be calculated and displayed (note that bus usage computation can take a noticeable amount of time, depending on the range of packets selected). Usage will also be computed for specific addresses (and optionally, endpoints; if ENDP is left blank, all endpoints for the specified address will be included).

The following example shows such a display for a data capture of USB traffic, using isochronous data transfers (the nature of the device—a camera—accounts for the high percentage of bus utilization):



Timing & Bus Usage Calculator

From packet: To packet:

Timing

☒ Total Time	350.3 ms	4,203,568 FS bits
--	----------	-------------------

Bus Usage

☒ Global	66.08%	2,777,523 FS bits
☒ Transactions	65.79%	2,765,657 FS bits
☐ Low-Speed		

Usage By Address & Endpoint

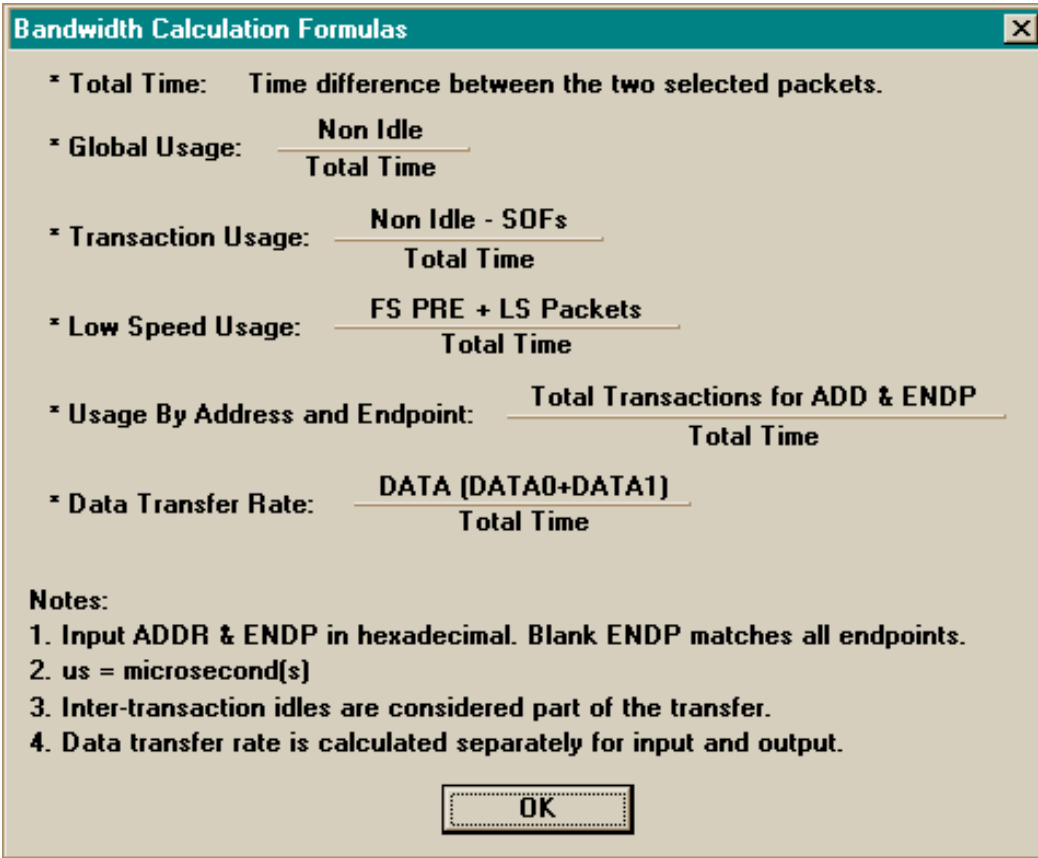
ADDR: ENDP:

☒ Transactions	65.12%	2,737,346 FS bits
☒ Data Only	7.67Mb/s(In)	0.00Mb/s(Out)

☒ With NAKed Data ☐ Without NAKed Data

Show Formulas Calculate Cancel Help

Selecting the “Show Formulas” button presents the following display, summarizing the formulas used to compute bandwidth utilization.



Bandwidth Calculation Formulas

- * Total Time: Time difference between the two selected packets.
- * Global Usage: $\frac{\text{Non Idle}}{\text{Total Time}}$
- * Transaction Usage: $\frac{\text{Non Idle} - \text{SOFs}}{\text{Total Time}}$
- * Low Speed Usage: $\frac{\text{FS PRE} + \text{LS Packets}}{\text{Total Time}}$
- * Usage By Address and Endpoint: $\frac{\text{Total Transactions for ADDR \& ENDP}}{\text{Total Time}}$
- * Data Transfer Rate: $\frac{\text{DATA (DATA0+DATA1)}}{\text{Total Time}}$

Notes:

1. Input ADDR & ENDP in hexadecimal. Blank ENDP matches all endpoints.
2. us = microsecond[s]
3. Inter-transaction idles are considered part of the transfer.
4. Data transfer rate is calculated separately for input and output.

OK

Note: The active file display can be scrolled, and other files opened; the calculator dialog box remains open (and frontmost) until “Cancel” is selected, or all files closed. Computations are always performed on the currently active file.

4.6.3 Packet Error Summary

The Packet Error Summary menu item displays a summary table of abnormal bus conditions detected in the current recorded file, as follows:

Packet Error Summary				
Error Type	Total	In Packets		
Bad PID	47	3	10	17
CRC5	47	4	11	18
CRC16	47	5	12	19
Bit Stuffing	47	6	13	20

Save As... OK Help

For each error type, the summary lists the packet number(s) in which these errors occur. The dialog box remains open (and frontmost) even if the window is no longer active, allowing manipulation of the open data file view while the error summary is visible (for example, scroll or go to an error packet listed in the error summary). Packet error summary data can be saved (with the “Save As...” button) for future use. See “Saving Summaries as Text Files”, below.

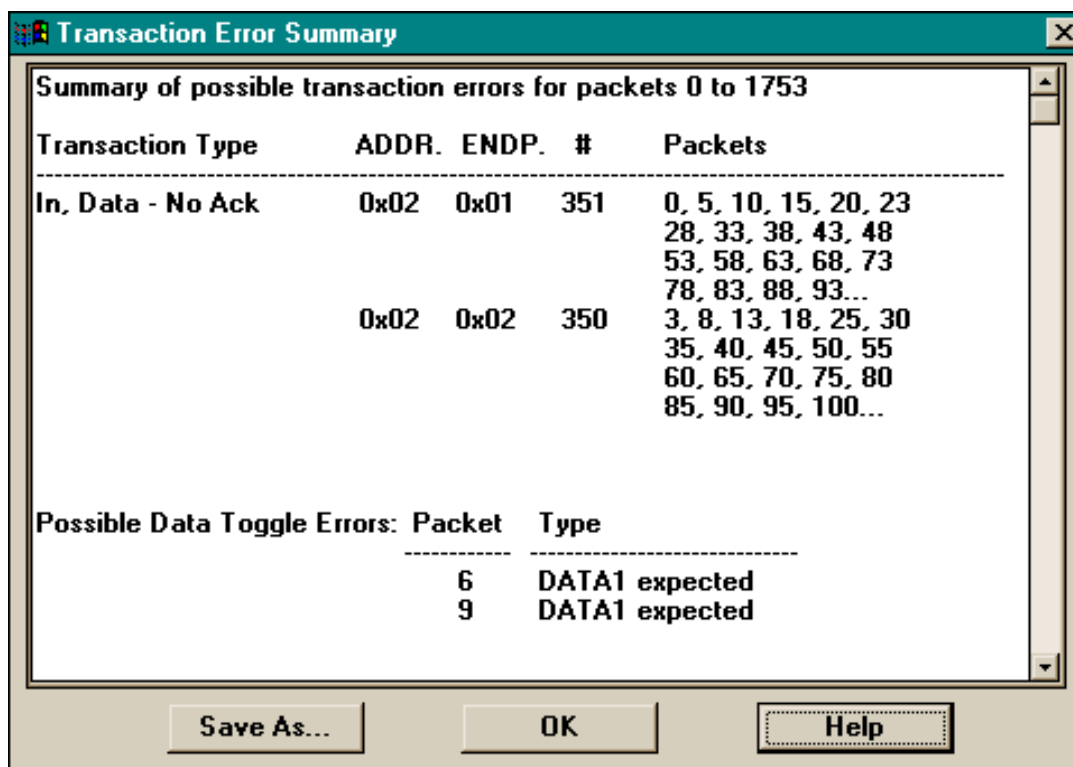
Note: The number of error packets listed in the error summary is limited to a maximum of 200 for each error type.

4.6.4 Transaction Error Summary

Selecting the Transaction Error Summary menu item brings up a dialog box enabling the specification of a range of packets to search for transaction errors (initialized to the complete set of packets in the file), as follows:

Select Packets	
(Total number of packets: 1754)	
From packet #:	To packet #:
0	1753
OK	Cancel

Selecting “OK” in this dialog will subsequently display a listing of possible transaction errors detected in the specified range of packets, such as:



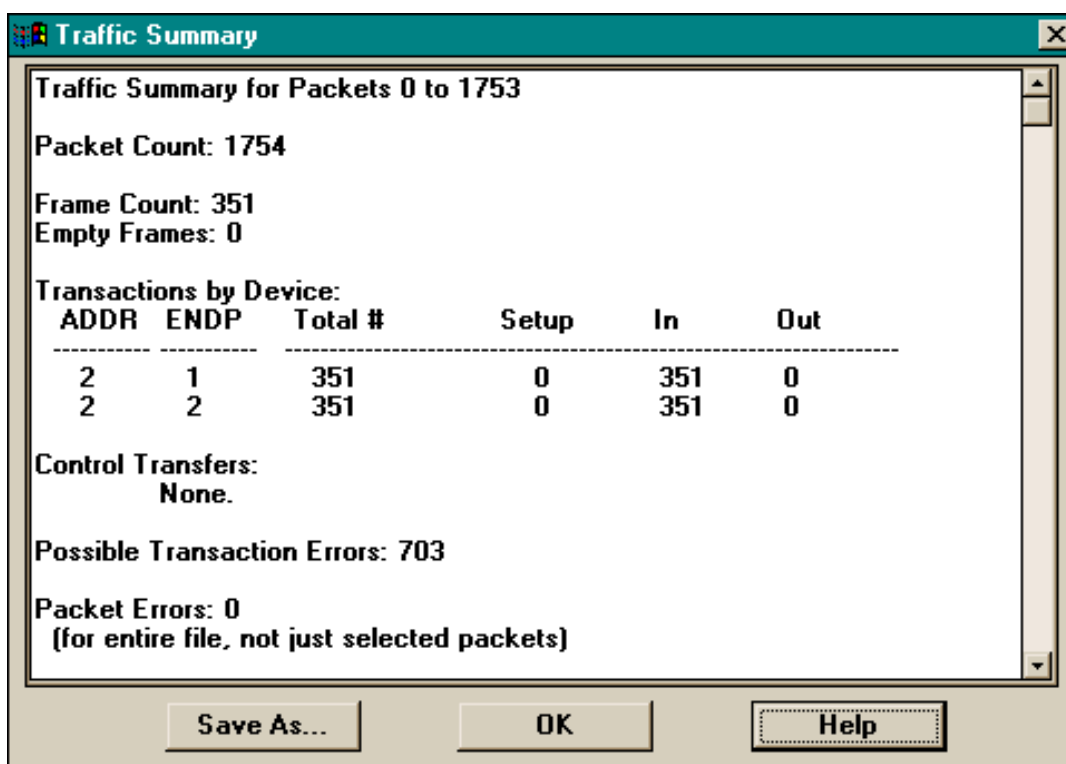
When there are long lists of packets containing the same transaction error (as in the above example), only the first 20 will be shown, followed by an ellipsis (...).

Note that it is not always possible to precisely determine the existence (or lack thereof) of transaction errors, particularly in the presence of isochronous traffic; all suspect occurrences should thus be interpreted as “potential” errors. The above example, for instance, is actually the result of sampled isochronous traffic, and the reported “errors” are merely artifacts of the isochronous data streams.

Transaction error summary data can be saved (with the “Save As...” button) for future use. See “Saving Summaries as Text Files”, below.

4.6.5 Traffic Summary

Selecting this menu item brings up a dialog box enabling the specification of a range of packets over which to accumulate traffic statistics (initialized to the complete set of packets in the file), as with the Transaction Error Summary. Selecting “OK” then generates a summary of a variety of traffic statistics for the currently selected file, including counts of packets, frames, empty frames, transaction errors, and packet errors, plus listings of transactions (ordered by device) and control transfers, such as the following:



Note that—unlike the other statistics—the packet error count is computed for the entire data file, not just for the range of packets selected in the earlier dialog box.

Traffic statistics data can be saved (with the “Save As...” button) for future use. See “Saving Summaries as Text Files”, below.

4.6.6 Saving Summaries as Text Files

Results of the three summary items in the Report Menu (as well as exported I/O data; see “The I/O Operation Pop-Up Menu”, below) can be saved as text files. Any file name can be specified, though use of the “.txt” extension is recommended; if no extension is specified, “.txt” will be added by default.

If the saved file is opened with a text editor using a monospaced type font, the text will not be aligned in the same fashion as it appears in the analyzer’s display window. To most closely approximate this display use the **MS Sans Serif** font in an **8 point** size.

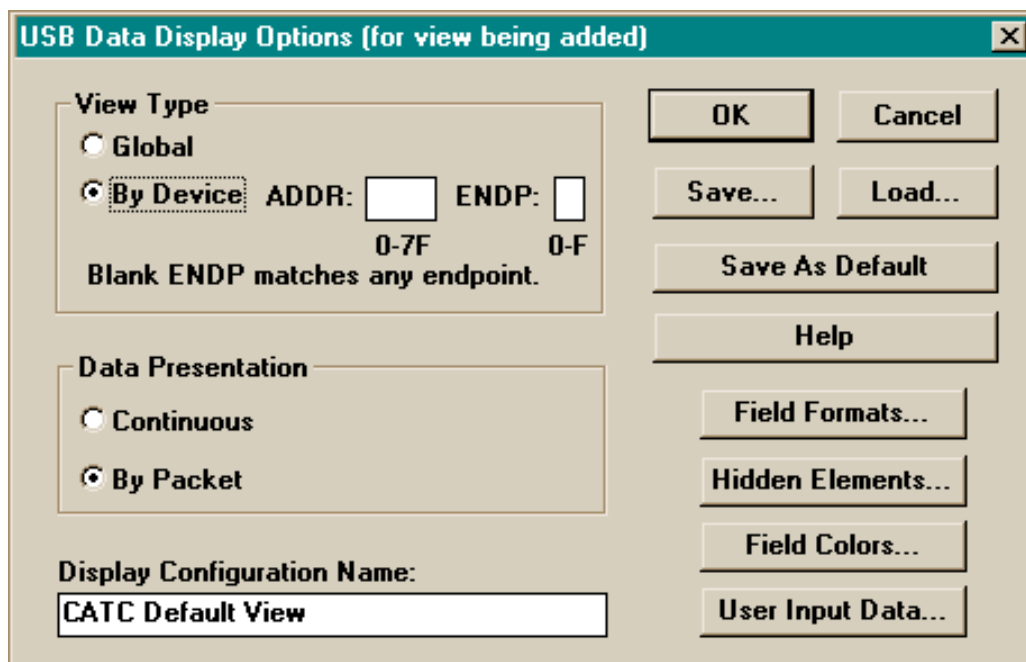
4.7 The View Menu

4.7.1 Add View

The Add View function is used to open a new window with an additional view of the currently selected USB data file. This is useful to:

- view the recorded data in a different format, or
- view (in conjunction with the “Tile Windows” function) two portions of the data file simultaneously.

As the former is the more common usage, the following dialog box is automatically opened to allow modification of the current viewing format.



Note that this is identical to the default Display Options dialog box, except for the title bar (which is intended to remind the user that the options about to be specified are for this particular view only, and will not be retained for subsequent use). The newly specified view of the data file will then be displayed.

Note: The previous display window remains open; the user can switch among display windows, or arrange them for simultaneous viewing, by using the Window menu.

4.7.2 Hide SOF

In order to reduce display “clutter”, this menu item removes the display of all Start of Frame packets from the current view (a new view is not created; the current view is redrawn). The action takes place immediately, unlike the otherwise equivalent operation in the Display Options selection, where it affects *subsequent* presentations.

As with several of the more frequently-used Detective options, the Hide SOF feature is accorded its own toolbar icon; this particular button indicates its current state by appearing depressed (or not, as appropriate) in the toolbar display.

4.7.3 Hide NAKed Transactions

This menu item functions identically to the Hide SOF operation, except that it is used to suppress the display of any packets pertaining to NAKed transactions.

4.7.4 Zoom In

The zoom entries in the View Menu provide an ability to adjust the size of the displayed elements in a USB traffic file, in order to represent more (or less) information on the screen (or printed output). Nine levels of zoom are implemented.

“Zoom In” increases the size of the displayed elements, allowing fewer (but larger) packet fields per screen. This function is also available as an icon in the toolbar.

4.7.5 Zoom Out

This function decreases the size of the displayed elements, allowing more (but smaller) packet fields per screen. This function is also available as an icon in the toolbar.

4.7.6 Set Current Zoom Value as Default

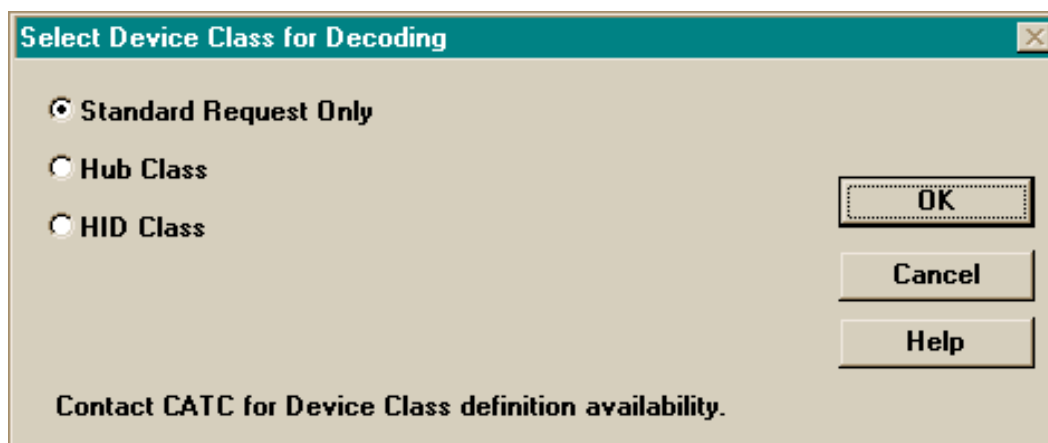
This function causes the current element size to be used as the default value upon subsequent invocations of the CATC Detective analyzer.

4.8 The Decode Menu

If the current file contains class-specific USB device requests, the CATC Detective software can decode the contained information according to the appropriate Device Class specifications.

4.8.1 Select Device Class...

The “Select Device Class...” menu item brings up the following dialog box, allowing selection of a USB Device Class:



Selecting a Device Class will cause future Decode Device Requests to interpret the protocol information according to the specification for the selected class.

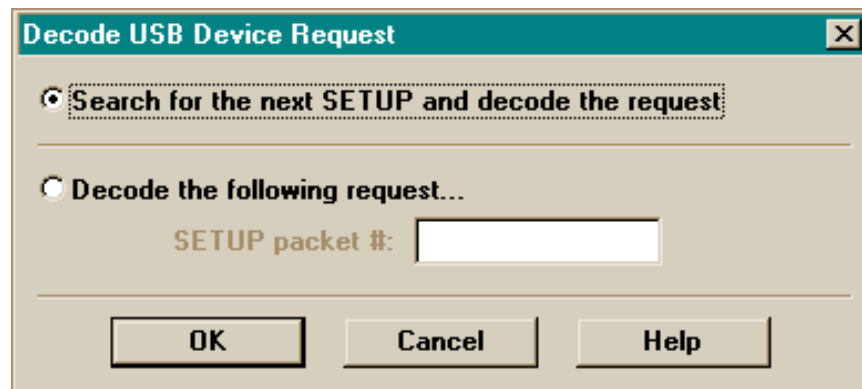
IMPORTANT: If the appropriate Device Class is not supported by the Detective software, the user should select the Standard Request Only option. Applying an improper Device Class specification to class-specific commands will display undefined results!

*Note: A Device Class can also be selected by clicking with the **right** mouse button on the title of any SETUP field on the screen. See “The Device Decoding Pop-Up Menus”.*

Note: The Detective software incorporates support for standard and Hub Class operations directly in the application code. Other classes are added at system startup time, by reading a set of library files (e.g., “CLS_HID.DLL” for the Human Interface Device Class); these additional classes will automatically show up as options on the above dialog box (which here shows an added “HID Class”). Contact CATC for information on the availability of these additional Device Class files.

4.8.2 Decode Device Request...

Control Transfers from the USB host to Endpoint 0 of a specific device are defined by the USB specification as USB Device Requests. The “Decode Device Request...” menu item displays a decoding of such requests (including the naming of the standard requests and descriptor types) according to USB Specification 1.0, using the following dialog box:



Two options are available: letting the software automatically search for the next SETUP and perform the decoding of the associated request, and providing the packet number for the SETUP token that begins the setup stage of the desired request. Selecting the OK button then decodes the specified Device Request.

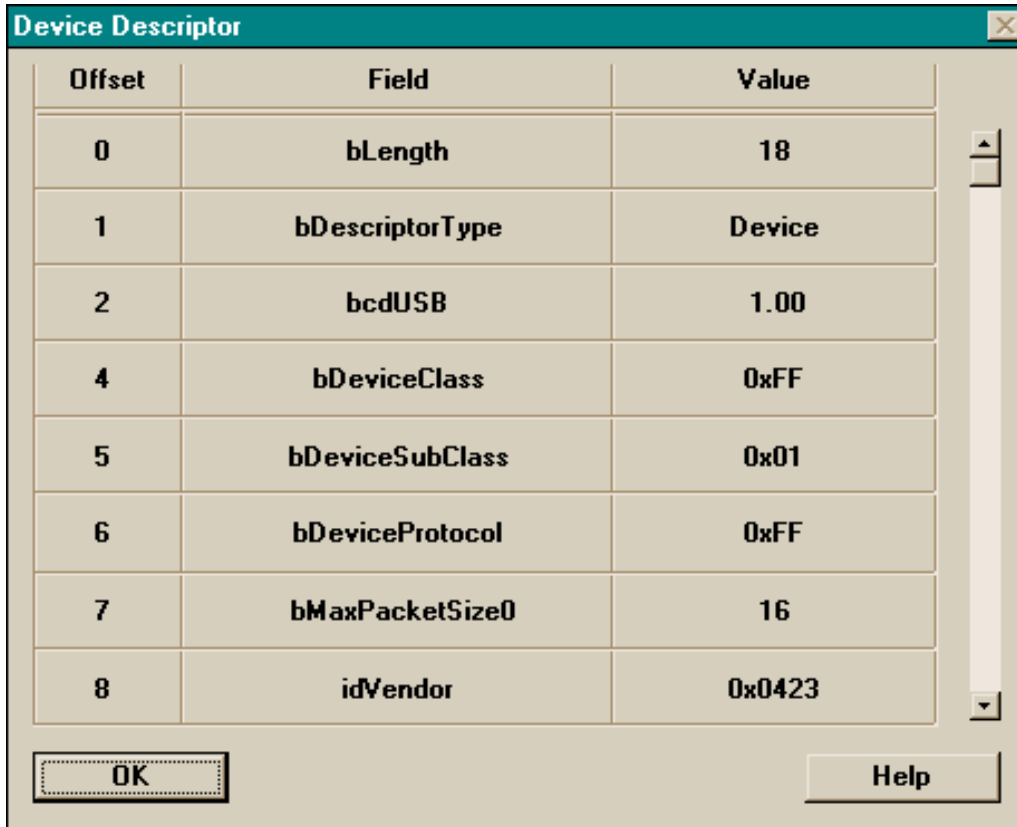
*Note: A specific Device Request can also be decoded by clicking with the **left** mouse button on the title of its SETUP field on the screen. See “The Device Decoding Pop-Up Menus”.*

The following dialog box is displayed following a Decode Device Request operation (The contents of the decoded display depend somewhat upon the Device Class and the specific Device Request):



4.8.2.1 Decoded Standard Requests

If the decoded standard request is GET_DESCRIPTOR and the requested descriptor is DEVICE or CONFIGURATION, or the request is SET_DESCRIPTOR, a button called “Show Descriptor Data” appears in the USB Device Request Data dialog box (as in the above example). Selecting this button brings up a form similar to the following, displaying the descriptor(s) returned by (or sent to) the device, decoded according to USB Specification 1.0:



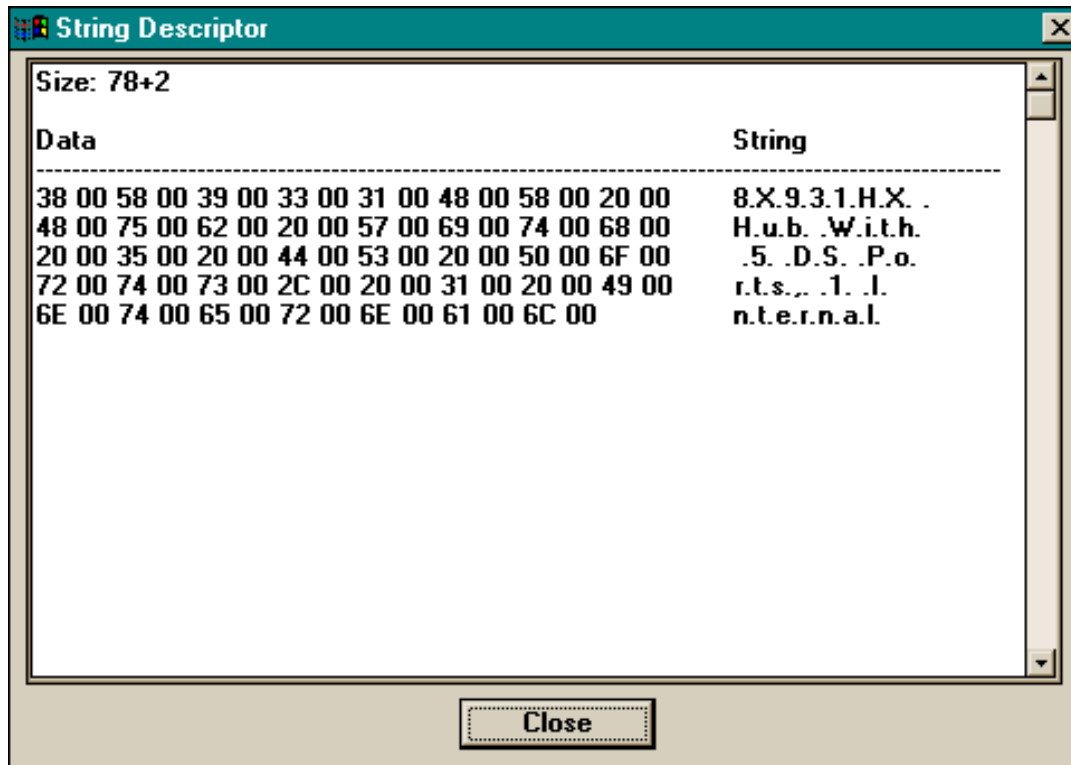
The image shows a dialog box titled "Device Descriptor" with a close button in the top right corner. It contains a table with three columns: "Offset", "Field", and "Value". The table lists the following fields and values:

Offset	Field	Value
0	bLength	18
1	bDescriptorType	Device
2	bcdUSB	1.00
4	bDeviceClass	0xFF
5	bDeviceSubClass	0x01
6	bDeviceProtocol	0xFF
7	bMaxPacketSize0	16
8	idVendor	0x0423

At the bottom of the dialog box, there are two buttons: "OK" and "Help". A scrollbar is located on the right side of the table, indicating that there may be more fields than are currently visible.

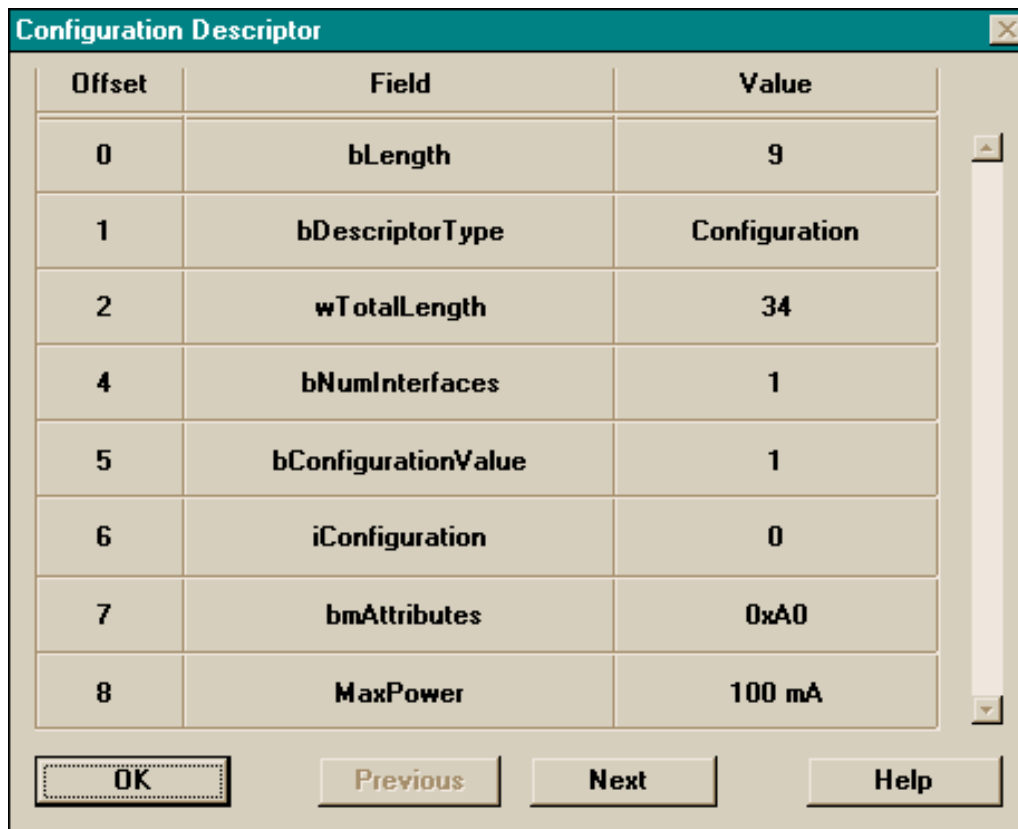
The scrollbar at the right side of the form permits viewing of all descriptor fields. If the device only sends a portion of a descriptor, the Detective software marks missing fields with “N/A”.

If the decoded standard request is GET_DESCRIPTOR and the requested descriptor is STRING, the “Show Descriptor Data” button displays a form similar to the following, showing the string decoded according to USB Specification 1.0:



In the above example, the representation of the string size as “78+2” is intended to remind the user that the total length of the string is comprised of the data portion (78 bytes in this instance) plus two bytes used to store the data length.

If a Configuration request is made, the device is expected to return a configuration descriptor and all interface and endpoint descriptors. In this case, Next and Previous buttons will appear at the bottom of the form, allowing viewing of all the returned descriptors in the order in which they were sent by the device.



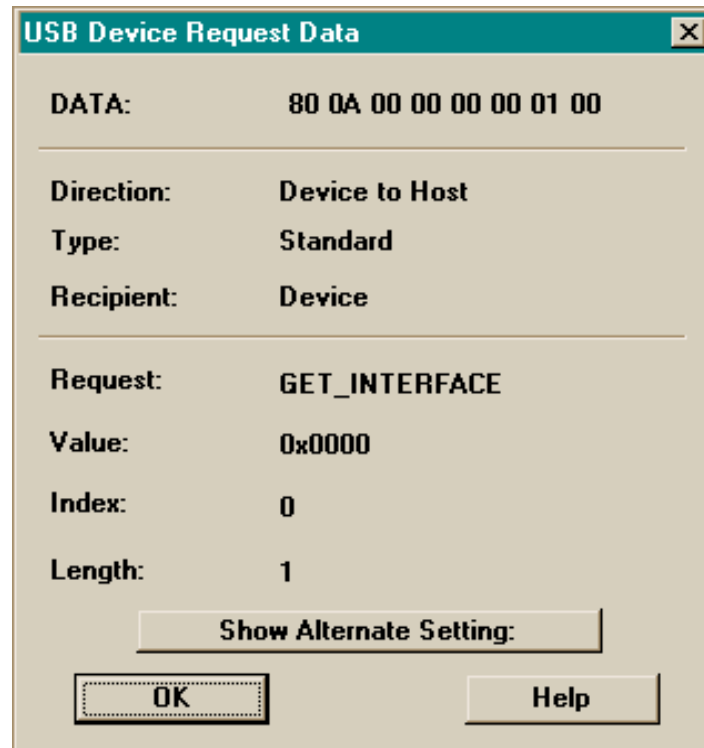
The image shows a software window titled "Configuration Descriptor". It contains a table with three columns: "Offset", "Field", and "Value". The table lists the following data:

Offset	Field	Value
0	bLength	9
1	bDescriptorType	Configuration
2	wTotalLength	34
4	bNumInterfaces	1
5	bConfigurationValue	1
6	iConfiguration	0
7	bmAttributes	0xA0
8	MaxPower	100 mA

At the bottom of the window, there are four buttons: "OK", "Previous", "Next", and "Help". A scrollbar is located on the right side of the table, indicating that there are more entries than are currently visible.

The scrollbar at the right side of the form permits viewing of all the entries. If the device only sends a portion of the data, the Detective software marks missing entries with "N/A".

If the decoded standard request is GET_INTERFACE (or GET_CONFIGURATION), a button called “Show Alternate Setting:” (or “Show Configuration:”) appears in the USB Device Request Data dialog box, as follows:



Selecting this button displays the value that was returned by the device (on the same form, in a small window immediately below the button).

If the decoded standard request is GET_STATUS), a button called “Show Status” appears in the USB Device Request Data dialog box; selecting this button brings up a form similar to the following, displaying the status information returned by the device, decoded according to USB Specification 1.0:

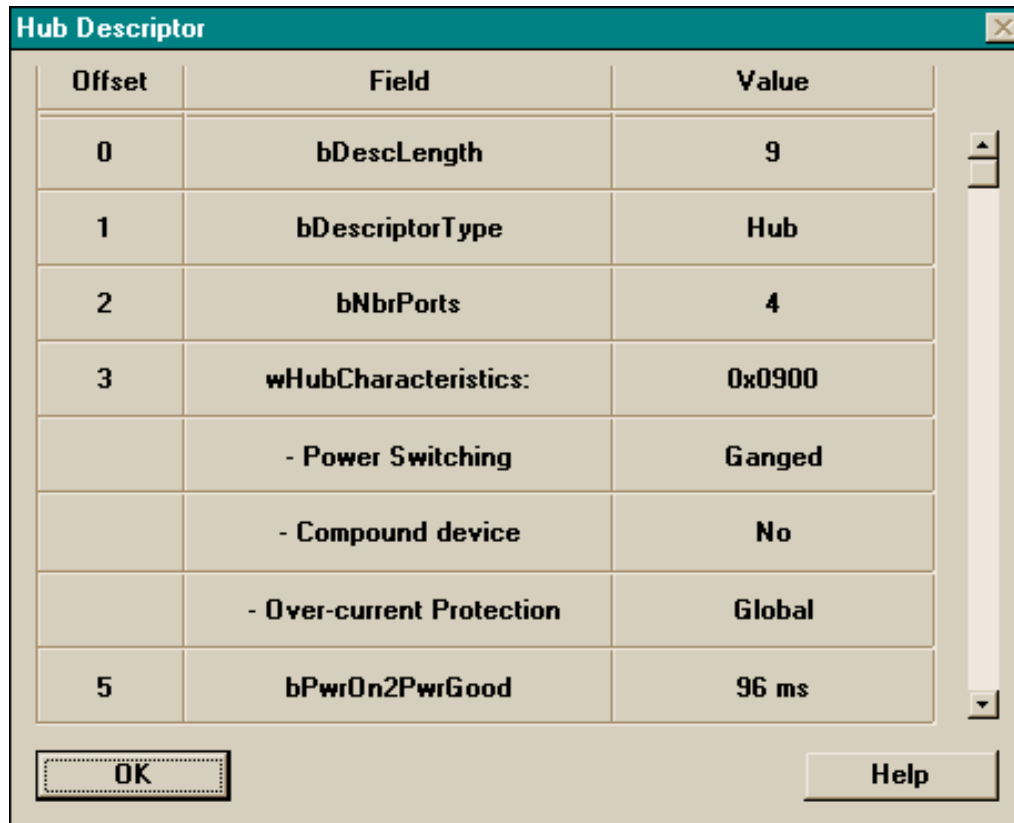
Bit	Field	Value
0	SelfPowered	1
1	RemoteWakeup	1

The form displays the recipient of the request (device, interface, or endpoint) as part of its title. For interface and endpoint recipients, it also displays the corresponding number. The scrollbar at the right side of the form permits viewing of all the entries. If the device only sends a portion of the data, the Detective software marks missing entries with “N/A”.

4.8.2.2 Decoded Hub Class Requests

Decoded USB Hub Descriptor

If the decoded standard request is GET_DESCRIPTOR, a button called “Show Descriptor Data” appears in the USB Device Request Data dialog box (as in the earlier example). Selecting this button brings up a form similar to the following, displaying the returned Hub descriptor, decoded according to USB Specification 1.0:



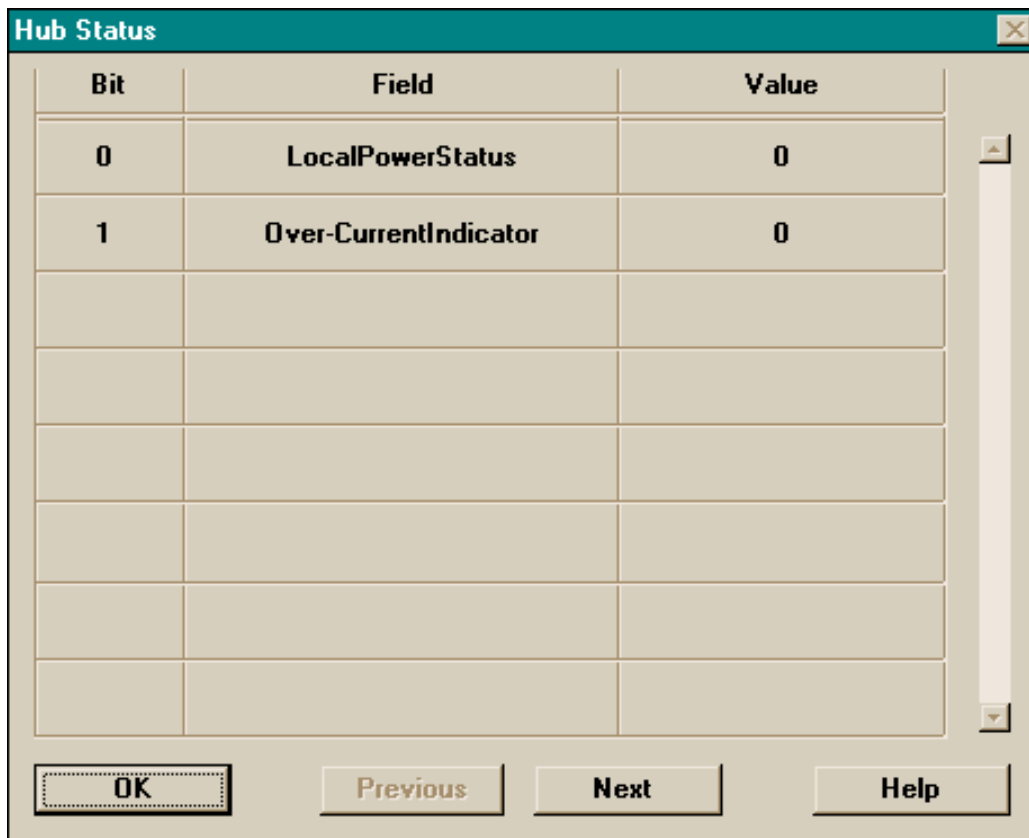
The image shows a dialog box titled "Hub Descriptor" with a table of fields and values. The table has three columns: Offset, Field, and Value. The fields include bDescLength, bDescriptorType, bNbrPorts, wHubCharacteristics (with sub-entries for Power Switching, Compound device, and Over-current Protection), and bPwrOn2PwrGood. The values are 9, Hub, 4, 0x0900, Ganged, No, Global, and 96 ms respectively. There are OK and Help buttons at the bottom.

Offset	Field	Value
0	bDescLength	9
1	bDescriptorType	Hub
2	bNbrPorts	4
3	wHubCharacteristics:	0x0900
	- Power Switching	Ganged
	- Compound device	No
	- Over-current Protection	Global
5	bPwrOn2PwrGood	96 ms

The scrollbar at the right side of the form permits viewing of all the entries. If the device only sends a portion of the data, the Detective software marks missing entries with “N/A”.

Decoded Hub Status/Change for Hub Device

The following form displays the hub status information that was returned by the USB Hub on a hub-class-specific GET_STATUS (GetHubStatus) request, decoded according to USB Specification 1.0:



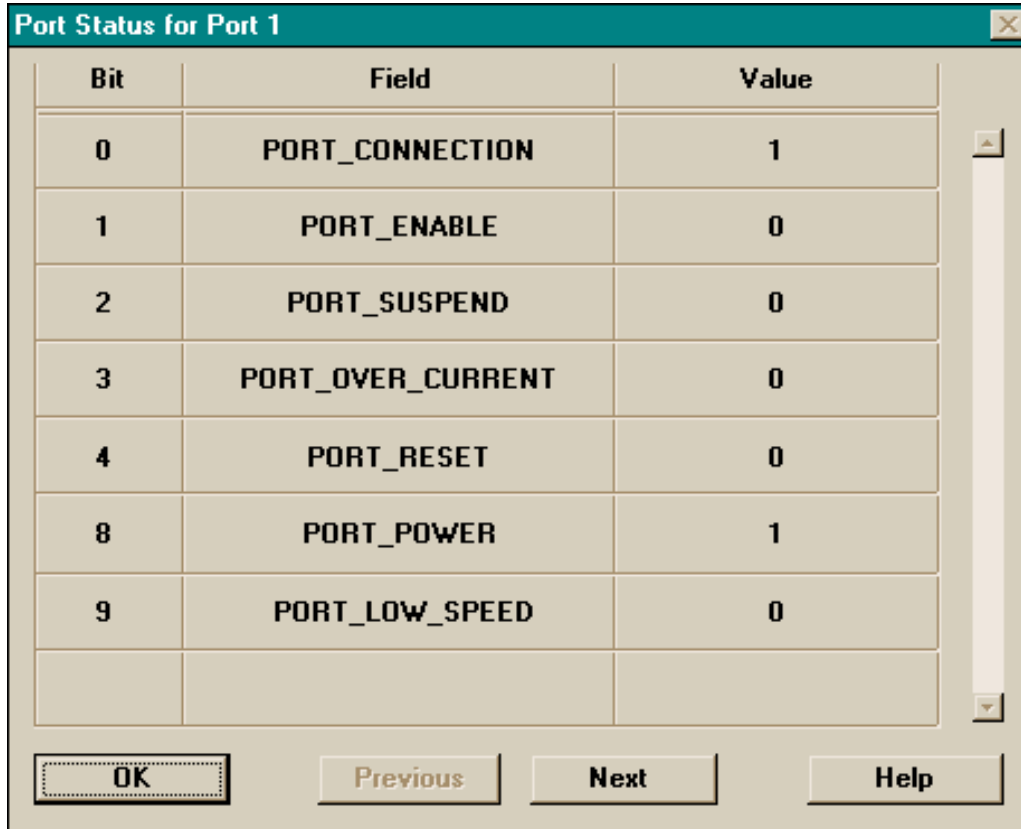
The image shows a Windows-style dialog box titled "Hub Status". It contains a table with three columns: "Bit", "Field", and "Value". The table has two rows of data: Bit 0 with Field "LocalPowerStatus" and Value 0; and Bit 1 with Field "Over-CurrentIndicator" and Value 0. There are five empty rows below these. To the right of the table is a vertical scrollbar. At the bottom of the dialog are four buttons: "OK", "Previous", "Next", and "Help".

Bit	Field	Value
0	LocalPowerStatus	0
1	Over-CurrentIndicator	0

Corresponding change information can be viewed using the Next button at the bottom of the form. The scrollbar at the right side of the form permits viewing of all the entries. If the device only sends a portion of the data, the Detective software marks missing entries with "N/A".

Decoded Port Status/Change for Hub Device

The following form displays the port status information returned by the Hub on a hub-class-specific GET_STATUS (GetPortStatus) request, decoded according to USB Specification 1.0:



Bit	Field	Value
0	PORT_CONNECTION	1
1	PORT_ENABLE	0
2	PORT_SUSPEND	0
3	PORT_OVER_CURRENT	0
4	PORT_RESET	0
8	PORT_POWER	1
9	PORT_LOW_SPEED	0

OK Previous Next Help

The form displays the number of the port for which status information was requested in its title. Corresponding change information can be viewed using the Next button at the bottom of the form. The scrollbar at the right side of the form permits viewing of all the entries. If the device only sends a portion of the data, the Detective software marks missing entries with “N/A”.

4.8.2.3 Decoded Requests for Other Device Classes

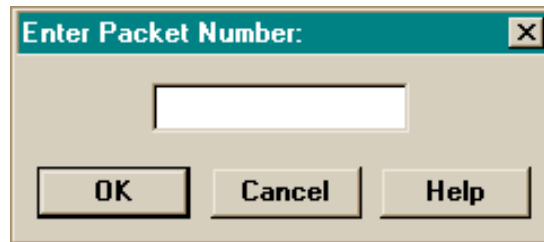
The Detective software incorporates support for standard and Hub Class operations directly in the application code. Other classes are added at system startup time, by reading a set of library files (e.g., “CLS_HID.DLL” for the Human Interface Device Class); these additional classes will automatically show up as options on the “Select Device Class...” dialog box. Contact CATC for information on the availability of these additional Device Class files.

4.9 The Search Menu

The CATC Detective software provides several options for searching through the recorded USB traffic, allowing the user to find specific packets based on packet number, marking, or content. The three most common actions (Go to Packet, Find, and Next) also have their own individual icons on the toolbar.

4.9.1 Go to Packet...

When the “Go to Packet...” menu item (or the associated toolbar icon) is selected, the following dialog box opens. To move quickly to a view of a specific packet, enter the packet number and select OK; the display will be repositioned with the specified packet at the top.



4.9.2 Go To Marker

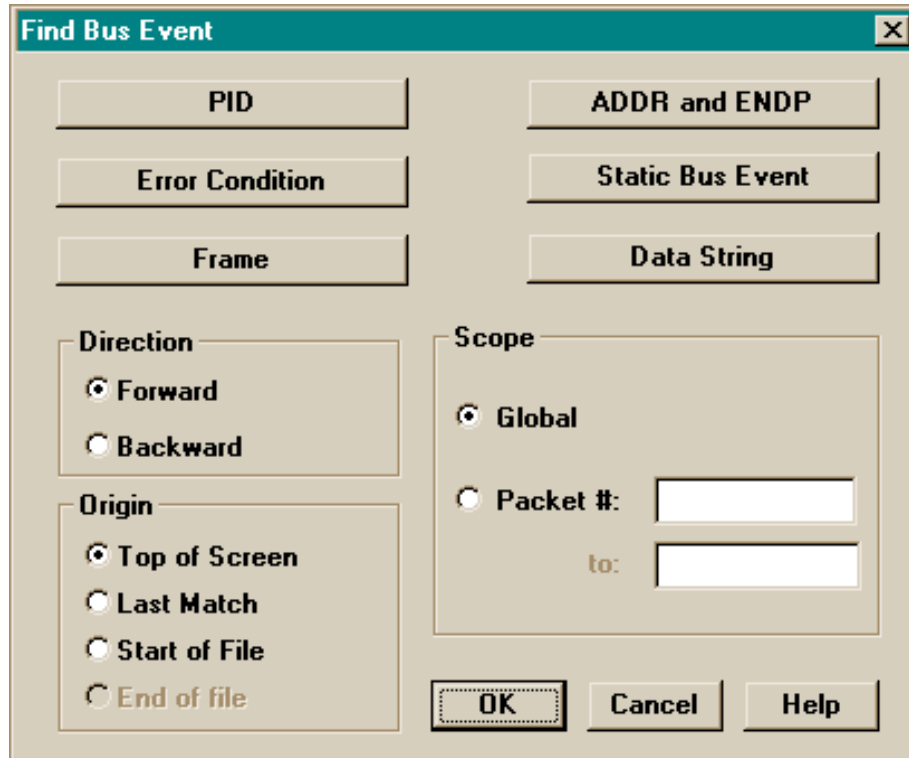
The “Go to Marker” menu item is only enabled when one of the packets in the traffic data file has been marked (using the Packet Marker & Timing pop-up menu, described below). When the item is selected, the display will be repositioned with the marked packet at the top.

4.9.3 Find...

The “Find...” menu item enables searching for specific bus events within the recorded data file. The CATC analyzer will search for:

1. protocol violations:
 - bad PID (check field)
 - undefined PID
 - bad CRC5
 - bad CRC16
 - missing stuff bits
2. packets with specific PIDs (e.g., Setup)
3. bus transactions with specific device Ids
4. specific frame numbers
5. empty frames (with SOF token only)
6. non-empty frames (including one or more non-SOF fields)
7. specific bit strings in data fields
8. transactions with low speed devices (PRE)
9. reset conditions (SE0)
10. suspend & resume conditions

Selecting “Find...” (or the associated toolbar icon) brings up the following dialog box:



The "Find Bus Event" dialog box is a standard Windows-style window with a title bar and a close button. It contains several input fields and radio button groups. On the left side, there are three text boxes labeled "PID", "Error Condition", and "Frame". To their right are three more text boxes labeled "ADDR and ENDP", "Static Bus Event", and "Data String". Below these, there are two groups of radio buttons. The first group, labeled "Direction", has two options: "Forward" (selected) and "Backward". The second group, labeled "Origin", has four options: "Top of Screen" (selected), "Last Match", "Start of File", and "End of file". To the right of these radio button groups is a "Scope" section. It contains a "Global" radio button (selected) and a "Packet #" radio button. The "Packet #" option has two text boxes: one for the packet number and one labeled "to:". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

As a rule, the **general** search parameters (Direction, Origin, and Scope of search) should be selected prior to the **specific** ones (PID, Error Condition, Frame, ADDR & ENDP, Static Bus Event, and Data String), as selecting the “OK” button in the specific event dialogs will launch the search immediately, without returning to this initial setup screen.

Note: The “Start of File” and “End of File” origins are considered temporary in nature; immediately following a search from either location, the origin will be changed to “Last Match”. This convention provides intuitive behavior when the “Search Next” feature is employed.

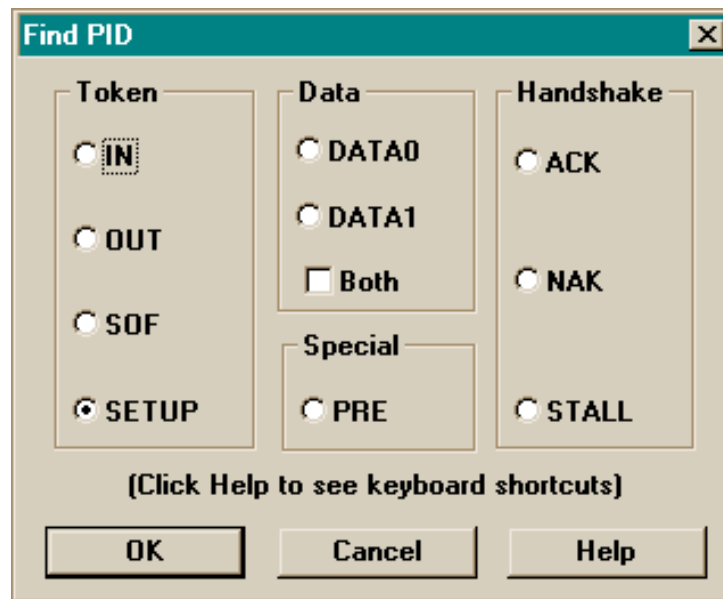
The following keyboard shortcuts can also be used (at any time) to change the direction and origin of searches:

Ctrl-f	direction: <u>f</u> orward
Ctrl-b	direction: <u>b</u> ackward
Ctrl-t	origin: <u>t</u> op of screen
Ctrl-m	origin: last <u>m</u> atch

The current settings for the search direction and origin are always displayed in the right segment of the status bar.

4.9.3.1 Find PID

Selecting the PID button brings up the following dialog box, to allow selection of a specific PID type:



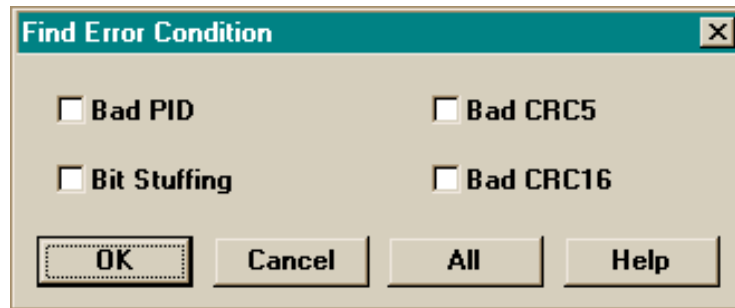
Selecting the “OK” button will then launch the search for the selected PID, using the search direction, origin, and scope previously specified.

The following keyboard shortcuts can also be used (at any time) to search for a specific PID:

Shift-s	<u>S</u> ETUP
Shift-o	<u>O</u> UT
Shift-i	<u>I</u> N
Shift-f	SO <u>F</u>
Shift-0	DATA <u>0</u>
Shift-1	DATA <u>1</u>
Shift-a	<u>A</u> CK
Shift-n	<u>N</u> AK
Shift-l	STA <u>L</u> L
Shift-p	<u>P</u> RE

4.9.3.2 Find Error Condition

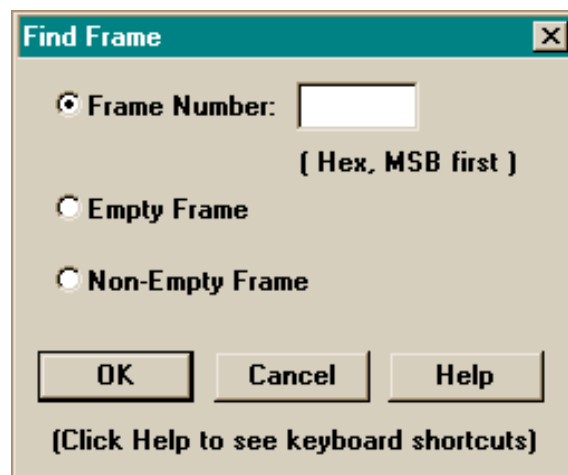
Selecting the Error Condition button brings up the following dialog box, to allow specification of particular error conditions (or, by selecting “All”, any error condition):



Selecting the “OK” button will then launch the search for the selected error condition, using the search direction, origin, and scope previously specified.

4.9.3.3 Find Frame

Selecting the Find Frame button brings up the following dialog box, to allow selection of a specific frame (by Frame ID number), an empty frame (containing only an SOF token), or a non-empty frame (containing one or more fields other than SOF):



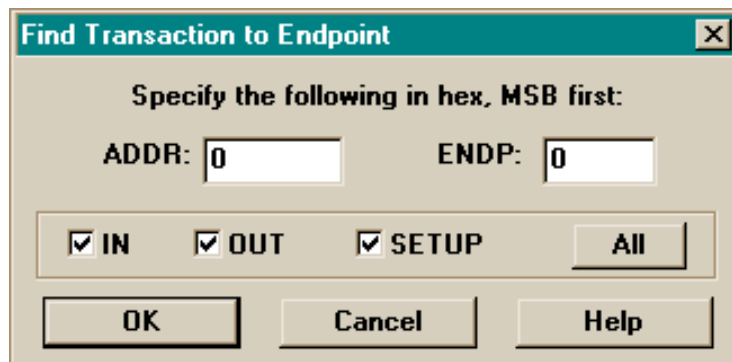
Selecting the “OK” button will then launch the search for the selected frame, using the search direction, origin, and scope previously specified.

The following keyboard shortcuts can also be used (at any time) to search for empty or non-empty frames:

< (Shift-comma)	empty frame
> (Shift-period)	non-empty frame

4.9.3.4 Find ADDR and ENDP

Selecting the ADDR and ENDP button brings up the following dialog box, to allow selection of a specific device address and endpoint:

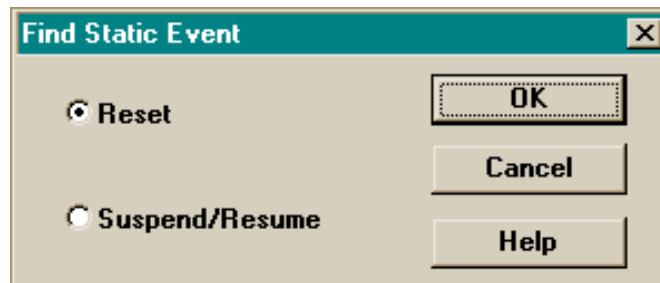


The dialog box is titled "Find Transaction to Endpoint" with a close button (X) in the top right corner. Below the title bar, it says "Specify the following in hex, MSB first:". There are two input fields: "ADDR:" followed by a text box containing "0", and "ENDP:" followed by a text box containing "0". Below these fields is a row of three checkboxes: "IN" (checked), "OUT" (checked), and "SETUP" (checked). To the right of these checkboxes is a button labeled "All". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

The search can be restricted to any combination of In, Out, and Setup packets by marking the appropriate checkboxes. Selecting the "OK" button will then launch the search for a packet with the selected device address and endpoint, using the search direction, origin, and scope previously specified.

4.9.3.5 Find Static Bus Event

The Static Bus Event button is only enabled when the traffic file was recorded with Idle state; it permits searching for the static bus events Reset and Suspend/Resume. Selecting this button brings up the following dialog box, to allow specification of a particular event:

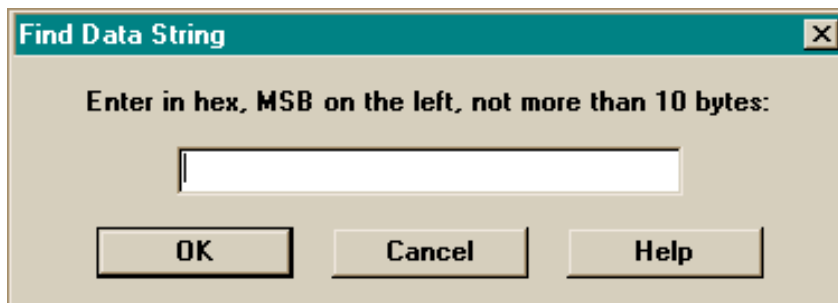


The dialog box is titled "Find Static Event" with a close button (X) in the top right corner. It contains two radio buttons: "Reset" (selected) and "Suspend/Resume". To the right of the radio buttons are three buttons: "OK", "Cancel", and "Help".

Selecting the "OK" button will then launch the search for a packet with the specified static bus event, using the search direction, origin, and scope previously specified.

4.9.3.6 Find Data String

Selecting the Data String button brings up the following dialog box, to allow selection of a specific data pattern within the DATA fields of the traffic file:



Up to 10 bytes of data (hexadecimal notation, MSB of each byte on the left) can be specified. Selecting the "OK" button will then launch the search for a packet with the selected data string, using the search direction, origin, and scope previously specified.

An example: to search for the standard device request "Get Device Descriptor", specify the data string '80060001'.

*Note: Data string searches are performed on a strict bit-by-bit basis; thus, if the specified bit string appears **anywhere** within a data field (whether or not its position-based hexadecimal representation is identical to that entered) it will produce a match.*

4.9.4 Next

Selecting the "Next" menu item (or the associated toolbar icon) will repeat the previous search; that is, it will initiate another search using the previously selected parameters (recall that "start/end of file" origins are automatically converted to "last match"). In keeping with Windows tradition, function key F3 also invokes this function.

4.10 The Window Menu

The Window menu is a standard Windows function that allows the open windows to be viewed and arranged in different ways.

4.11 The Help Menu

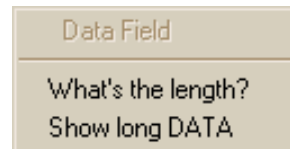
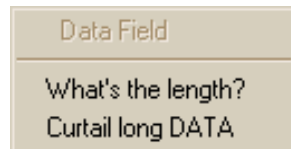
The Help menu is a standard Windows function that supplies additional information on the various functions of the CATC *Detective* program when it is in use.

4.12 The Data Field View Pop-Up Menu

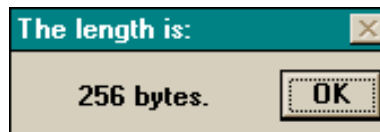
Clicking on the title of any DATA field will bring up the following Data Field menu for short data fields:



or one of the following menus for data fields containing more than 16 bytes:



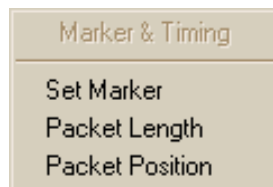
Selecting the single “What’s the length?” menu item will display the length of the associated data field, using the following display box:



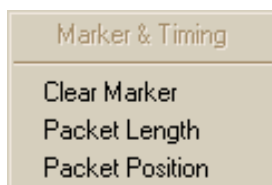
The second menu item enables toggling of the current data display format, between full and curtailed display modes, as previously described under Field Formats. When invoked by the pop-up menu, the display change will take place immediately.

4.13 The Packet Marker & Timing Pop-Up Menus

Clicking on the “Packet #” title of any packet display will bring up the following menu (files recorded without Idle state will not show the timing-related items):

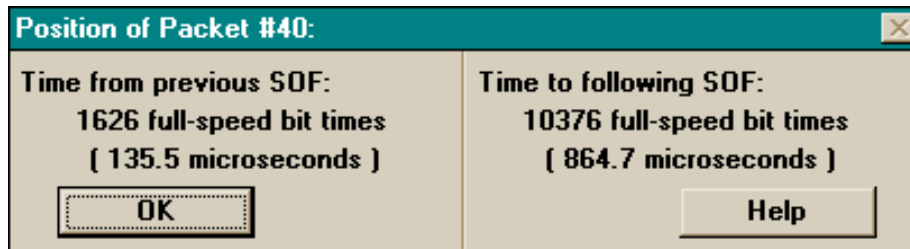


The first menu item is associated with the concept of “marking” a particular packet in the traffic data file (only one packet can be marked at any given time). This marked packet (displayed with a distinctive red outline) can be the target of a Search operation (see above), and also a point of reference for timing measurements. If any packet is marked, subsequent invocation of this pop-up menu will produce one of the following displays:



Selecting the relevant menu item will then either clear the marker or relocate it to the current packet (that which spawned the pop-up menu).

The remaining menu items (displayed only for files recorded with Idle state) are used to compute timing information for the associated packet. Selecting “Packet Length” will display the time taken by the packet, from start of Sync to the end of EOP signaling. Selecting “Packet Position” will display the frame-related position of the packet (the time from the closest previous Start of Frame/keep-alive and the time to the closest following SOF/keep-alive). Both durations are displayed as equivalent bit times and in microseconds, as in the following example:



Appropriate error messages are displayed if the selected packet contains a RESET or SUSPEND/RESUME, or if the lack of an SOF/keep-alive makes the computation of the associated time impossible.

Finally, selecting the “Time From Marker” (or “Time To Marker”, as appropriate) menu item will display the elapsed time from the marked packet, using the “Timing & Bus Usage Calculator” display.

4.14 The Device Decoding Pop-Up Menus

Clicking on the title of any SETUP field with the **right** mouse button will bring up the following menu, allowing the selection of a USB Device Class to be used in subsequent decoding:

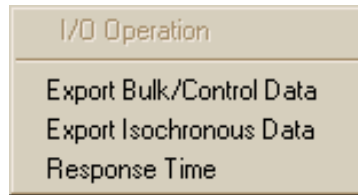


Clicking on the title of any SETUP field with the **left** mouse button will bring up the following single item menu, allowing decoding of its device-specific information, according to the currently selected Device Class:

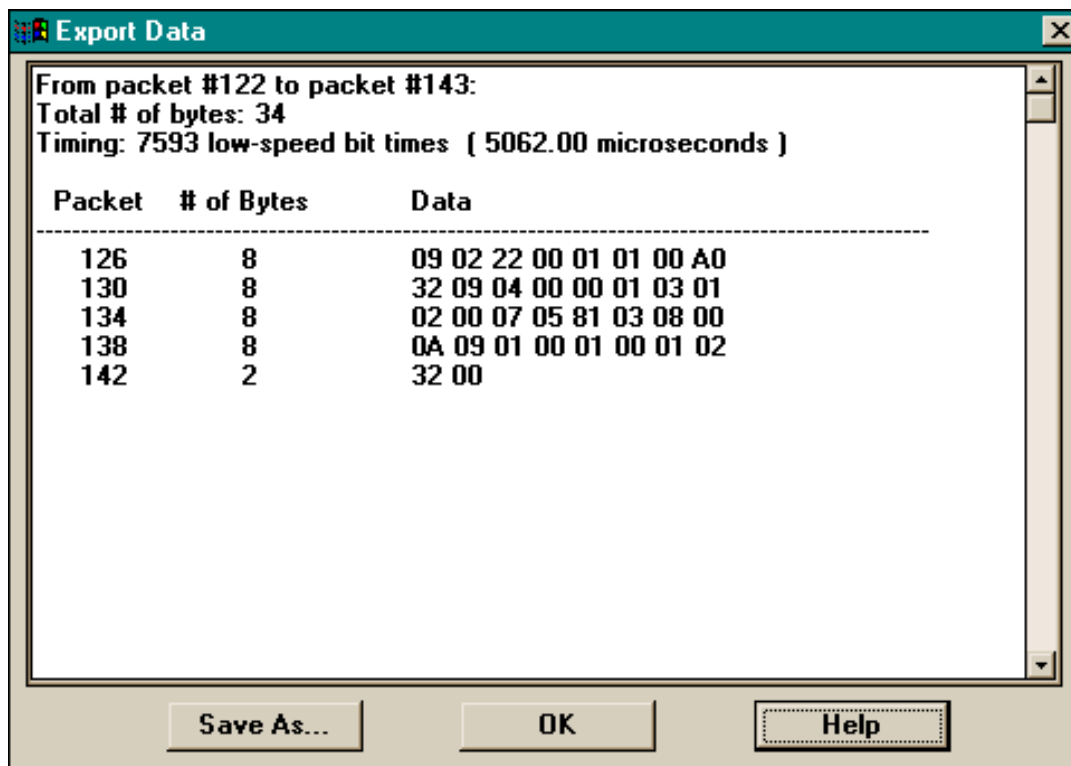


4.15 The I/O Operation Pop-Up Menu

Clicking on the title of any IN or OUT field will bring up the following menu:

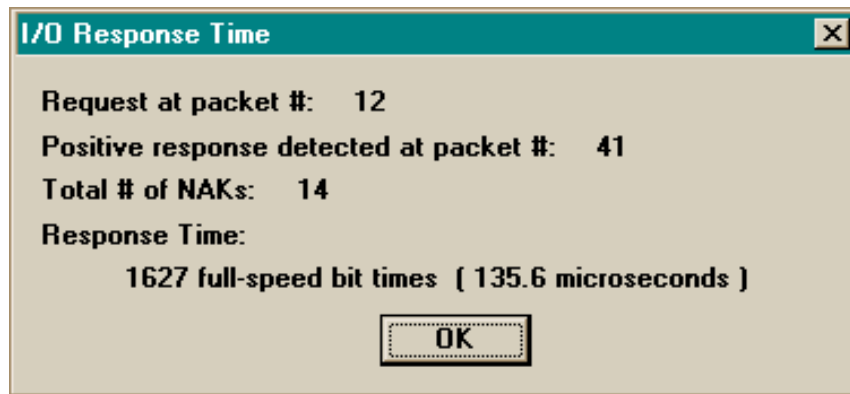


The “Export Bulk/Control Data” and “Export Isochronous Data” menu items are intended for the output of data to a file. The analyzer is not able to determine with certainty the type of data transfer involved, so uses the user’s specification of the associated transfer type (bulk/control or isochronous) to guide its “best effort” attempt to isolate the chosen data transfer. Any NAKed data is not included. The collected data is first displayed in a form such as the following:



The extracted data can now be saved (with the “Save As...” button) for future use. See “Saving Summaries as Text Files”, above.

Selecting the “Response Time” menu item brings up the following display, showing the elapsed time from the selected I/O request and the closest following positive response to same:



5. HOW TO CONTACT CATC

Type of Service	Contact
Call for technical support...	US and Canada: +1/ 800 909 2282 Worldwide: +1/ 408 727 6600
Fax your questions...	Worldwide: +1/ 408 727 6622
Write a letter...	Computer Access Technology Corp. Customer Support 2403 Walsh Avenue Santa Clara, CA 95051-1302
Send e-mail...	support@catc.com
Visit CATC's Website...	http://www.catc.com/

6. WARRANTY AND LICENSE

Computer Access Technology Corporation (hereafter CATC) warrants this product to be free from defects in material, content, and workmanship, and agrees to repair or replace any part of the enclosed unit that proves defective under these terms and conditions. Parts and labor are warranted for one year from the date of first purchase.

The CATC Detective software is licensed for use on a single PC. The software may be copied for backup purposes only.

This warranty covers all defects in material or workmanship. It does not cover accidents, misuse, neglect, unauthorized product modification, or acts of nature. Except as expressly provided above, CATC makes no warranties or conditions, express, implied, or statutory, including without limitation, the implied warranties of merchantability and fitness for a particular purpose.

CATC shall not be liable for damage to other property caused by any defects in this product, damages based upon inconvenience, loss of use of the product, loss of time or data, commercial loss, or any other damages, whether special, incidental, consequential, or otherwise, whether under theory of contract, tort (including negligence), indemnity, product liability, or otherwise. In no event shall CATC's liability exceed the total amount paid to CATC for this product.