FRONTLINE TEST SYSTEM™

FTS4BT™

USER MANUAL

Table of Contents

1 Welcome to FTS

Welcome to Frontline Test System (FTS). The design of FTS allows you to conduct data analysis of protocols using your personal computer. The FTS interface is easy to use without training, but we recommend you read the online Help to take maximum advantage of all the features.

We designed the online Help System with complete explanations and easy to use systematic instructions. Access the online Help by choosing Help Topics from the Help menu, or by pressing the F1 key on any window.

2 Getting Started

2.1 Control Window

The analyzer displays information in multiple windows, with each window presenting a different type of information. The *Control* window provides access to each window as well as a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function.

Because the *Control* window can get lost behind other windows, every window has a *Home* icon  that brings the *Control* window back to the front. Just click on the *Home* icon to restore the *Control* window.

When running the *Capture File Viewer*, the *Control* window toolbar and menus contain only those selections needed to open a capture file and display the About box. Once a capture file is opened, the analyzer limits Control window functions to those that are useful for analyzing data contained in the current file. Because you cannot capture data while using *Capture File Viewer*, data capture functions are unavailable. For example, when viewing Ethernet data, the Signal Display is not available. The title bar of the Control window displays the name of the currently open file. The status line (below the toolbar) shows the configuration settings that were in use when the capture file was created.

2.2 The Control Window Toolbar

Available options are in color, while unavailable options are grayed out. All toolbar icons have corresponding menu items. Toolbar icon displays vary according to operating mode and/or data displayed.

 Open File - Opens a capture file.

 I/O Settings - Opens the I/O Settings dialog.

 Start Capture - Begins data capture to disk.

 Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.

 Clear - Clears or saves the capture file.

 Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.


Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.


Protocol Navigator - (framed data only) Opens the Protocol Navigator window, with the currently selected frame highlighted.


Statistics Window - Opens up the Statistics window.


Signal Display - Opens The Signal Display dialog.


Breakout Box - Opens the Breakout Box dialog.


Transmit - Opens the Transmit dialog.


Cascade - Arranges windows in a cascaded display.


Packet Timeline - Opens the Packet Timeline display.


Extract Data - Opens the Extract Data dialog.


Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.


Audio Extraction - Opens the Audio Extraction dialog.

2.3 Drop-Down Menus

The menus that you see on the Control Window and dialogs like Frame Display and Event Display vary depending on whether the data is being captured live or whether you are looking at a .cfa file. You will see File, View, Live, Options, Window, and Help. Most of the options are self explanatory.

- Many of the **File** menu items are standard Windows type commands: Open, Close, Save, Recent Files, etc. There are two exceptions:
    - **Recreate Companion File**. This option is available when you are working with decoders. If you change a decoder while working with data, you can use Recreate Companion File to recreate the .frm file, the companion file to the .cfa file. Recreating the .frm file helps ensure that the decoders will work properly.
    - **Reload Decoders**. When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded.

- Under the **View** menu you can choose which FTS windows are available to open.

- **Live** contains commands that used in capturing data.

- Under **Options** you have opportunities to set/modify various system settings.

- The **Window** menu displays the open FTS dialogs and standard options like Cascade, Minimize, Tile, etc.

- Within the **Help** menu you can open the electronic Help file, About FTS, and access the FTS web site for additional help.

2.4 Configuration Information on the Control Window

The *Configuration* bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc. If the analyzer cannot find the MAC Address, it lists zeroes after the NIC name.

2.5 Status Information on the Control Window

The *Status* bar located just below the *Configuration* bar on the *Control* window provides a quick look at current activity in the analyzer.

- *Capture Status* displays *Not Active*, *Paused* or *Running* and refers to the state of data capture.
    - *Not Active* means that the analyzer is not currently capturing data
    - *Paused* means that data capture has been suspended
    - *Running* means that the analyzer is actively capturing data.

- % Used
    - The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200K capture file, the bar graph tells you how much of the capture file has been used. When the graph reaches 100%, capture either stops or the file begins to

overwrite the oldest data, depending on the choices you made in the System Settings.

- Utilization/Events
    - The second half of the status bar gives the current utilization and total number of events seen on the network. This is the total number of events monitored, not the total number of events captured. The analyzer is always monitoring the circuit, even when data is not actively being captured. These graphs allow you to keep an eye on what is happening on the circuit, without requiring you to capture data.

2.6 Frame Information on the Control Window

Frame Decoder information is located just below the *Status* bar on the *Control* window. It displays two pieces of information.

- **Frame Decoder (233 fps)** displays the number of frames per second being decoded. You can toggle this display on/off with Ctrl-D, but it is available only during a live capture.
- **#132911** displays the total frames decoded.
- **100%** displays the percentage of buffer space used.

2.7 Determining Master and Slave

In *Bluetooth*®, the device that initiates the connection is always the master at connection time. You only need to know the master and slave at connection time when setting up the I/O Settings. Afterwards a role switch may occur, but the analyzer automatically follows the role switch.

Role Switches

After the connection has been made, a role switch can take place. A good example of why this happens would be when a mouse connects to the PC. The mouse initiates the connection, so it is the master. After the connection is made, a role switch occurs so that the PC becomes the master and the mouse becomes a slave. The role switch takes place because the PC may be working with multiple devices at the same time, and as such, the PC would not be a slave of more than one device.

Let us say that a piconet exists between a PC and a keyboard with the PC a master. If the mouse wants to become a member of the piconet it initiates the connection. Since the

mouse initiated the connection, it is the master of a new piconet and the PC is the slave. The PC is still the master of the piconet between the PC and keyboard. A role switch now occurs between the PC and the mouse, and the PC is now the master of a piconet with two slaves: the mouse and keyboard.

2.8 Using more than one additional ComProbe® when sniffing a link

There will be instances when you will want to use one or more additional ComProbe when sniffing an FTS4BT a Low Energy Analyzer link. The procedure for doing that appears below

1. Locate the file **Bluetooth air.personality**, which will be in C:\Program Files\Frontline Test System II\Frontline FTS4BT [version #]\App Data\Decoders\Bluetooth.
2. Find the section titled [Personality`FTS4BT`Generic`Scatternet]
3. Locate the line:CmdLine="/mem=FTS4BT=generic" "/dspath=.\btcpds.exe" "/Mode=Scatternet"
4. On the end of that, add "/dsnum=n", where n is the number of packet sniffers you need to use.

For example, if you wanted to use three packet sniffers, the line would read:

CmdLine="/mem=FTS4BT=generic" "/dspath=.\btcpds.exe" "/Mode=Scatternet" "/dsnum=3"

5. Save the file.

Note: Be sure to include the quotes.

2.9 FTS4BT Data Capture Methods

FTS4BT has different data capture methods to accommodate various applications.

- **Bluetooth Air Sniffing**
  - **Interlaced Page Scan**
    This mode results in two *Bluetooth*® Air datasource instances and requires two ComProbes®. This mode allows you to sync to a piconet when the slave being paged uses interlaced page scanning. Interlaced Page Scan will only work with Slave Inquiry as the synchronization method for both datasources on the I/O Settings dialog.
  - **Multiple Connections**
    This mode is used when multiple link keys are being used in a Piconet and/or when there are multiple masters being sniffed in a Scatternet.
  - **Redundant**

    This mode uses two ComProbes to sniff the same Piconet to ensure that no data is being missed.
  - **Single Connection (Air Basic)**
    This is the standard Air Sniffer using the *Bluetooth* ComProbe (USB dongle) as the hardware interface to *Bluetooth* air traffic.

- **Bluetooth/802.11 Air Sniffing (optional)**
  - **802.11**

    Requires one 802.11 ComProbe.

    An 802.11 ComProbe is included with the Wi-Fi option.

    Captures 802.11 data on the selected channel.
  - **802.11 AMP**

    Requires one Bluetooth ComProbe and one 802.11 ComProbe.

For Bluetooth v3.0 + HS analysis.

Captures Bluetooth and 802.11 data, including AMP Manager and displays both ion the Frame Display and Coexistence View.

- **802.11 AMP, Interlaced Page Scan**

  Requires two Bluetooth ComProbes and one 802.11 ComProbe.

  Captures Bluetooth and 802.11 data, including AMP Manager and displays both in the Frame Display and Coexistence View.

  Syncs to the Bluetooth piconet using interlaced page scan to increase consistency of synching with chips that employ interlaced page scan.

- **802.11, Interlaced Page Scan**

  Requires two Bluetooth ComProbes and one 802.11 ComProbe.

  Captures Bluetooth and 802.11 data and displays both in the Frame Display and Coexistence View.

  Syncs to the Bluetooth piconet using interlaced page scan to increase consistency of synching with chips that employ interlaced page scan.

- **802.11/Bluetooth Coexistence**

  Requires one Bluetooth ComProbe and one 802.11 ComProbe.

  For Bluetooth/802.11 coexistence analysis.

  Captures Bluetooth and 802.11 data and displays both in the Frame Display and Coexistence View.

- **High Speed Serial Sniffing (optional)**

  - **HCI-BCSP**
    Requires embedded ComProbe.
    An embedded ComProbe is included with the FTS4BT HSU option.
    Captures and decodes BlueCord Serial Protocol.

  - **HCI-H4**
    Requires embedded ComProbe.
    An embedded ComProbe is included with the FTS4BT HSU option.
    Captures and decodes HCI commands and events over the H4 transport.

  - **HCI-H4DS**
    Requires embedded ComProbe.
    An embedded ComProbe is included with the FTS4BT HSU option.
    Captures and decodes HCI commands and events over the H4DS transport.

  - **HCI-H5**
    Requires embedded ComProbe.
    An embedded ComProbe is included with the FTS4BT HSU option.
    Captures and decodes HCI commands and events over the H5 transport.

- **HSU**
  Requires embedded ComProbe.
  An embedded ComProbe is included with the FTS4BT HSU option.

- **USB HCI H2 Sniffer**
  - **Internal Tap**
    No hardware needed.
    For sniffing devices plugged into the PC that is running FTS4BT.
  - **Raw USB Packets - USB ComProbe I (optional)**
    Requires one USB ComProbe I.
    Captures and decodes USB, USB Setup data, and Bluetooth.
  - **H2 + Raw USB Packets - USB ComProbe II (optional)**
    Requires one USB ComProbe II.
    Captures and decodes USB, USB Setup data, and Bluetooth.
  - **USB ComProbe I (optional)**
    Requires one USB ComProbe I.
    Captures and decodes Bluetooth data; USB and USB Setup data will be filtered out.
  - **USB ComProbe II (optional)**
    Requires one USB ComProbe II.
    Captures and decodes Bluetooth data; USB and USB Setup data will be filtered out.

The USB HCI Data source dialog allows the user to select which *Bluetooth* device to sniff and to Start and End the sniffing process. The dialog has a list containing the *Bluetooth* Devices connected to your system. If the Show Connected Only checkbox is unchecked, then all USB devices that have ever been connected to your system are listed. If you have connected or disconnected a device while this dialog is open, click on Refresh List to update the list. To sniff a USB device, just select it with your mouse and click on Start Sniffing.

Note: Start USB HCI packet sniffer before you run an application on the USB port.

- **Virtual Sniffer**

The Virtual Sniffer is a live import facility within FTS4BT that makes it possible to access any layer in a stack that the programmer has access to and feed this data into the Virtual Sniffer FTS4BT. Please refer to the “Show Live Import Information“ button on the Virtual Sniffer Datasource window in FTS4BT. More information is available in the Options Folder in FTS4BT Desktop folder, and a white paper is available at

http://www.fte.com/downloads/Datasheets/FTS4BT_Virtual_Sniffing_white_paper.pdf

- **FTS Side**
  No hardware required.
  FTS4BT acquires data via used-developed software.

2.10 Opening FTS4BT

On product installation, the installer creates a folder on the windows desktop labeled **Frontline FTS4BT**.

1. Double-click the Frontline FTS4BT desktop folder 

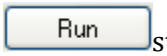
This opens a standard Windows file folder window.

2. Double-click on Frontline FTS4BT and the system displays the *Select Data Capture Method* dialog.

Note: You can also access this dialog by selecting *Start > All Programs > Frontline FTS4BT (Version #) > Frontline FTS4BT*.

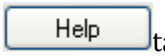
This dialog lists all the methods FTS4BT supports in a tree control. See Protocol List

Three buttons appear at the bottom of the dialog; **Run**, **Cancel**, and **Help**. When the dialog first opens, Cancel and Help are active, and the Run button is inactive (grayed out).



starts FTS using the selected protocol stack.

closes the dialog and exits the user back to the desktop.



takes the user to this help file as does pressing the F1 key.

3. Expand the folder and select the data capture method that matches your configuration.

Note: If you don't need to identify a capture method, then click the Run button to start the analyzer.

Creating a Shortcut

A checkbox labeled **Create Shortcut When Run** is located near the bottom of the dialog. This box is un-checked by default. Select this checkbox, and the system creates a shortcut for the selected method, and places it in the FTS4BT desktop folder and in the start menu when you click the Run button. This function allows you the option to create a shortcut icon that can be placed on the desktop. In the future, simply double-click the shortcut to start the analyzer in the associated protocol.

2.11 Minimizing Windows

Windows can be minimized individually or as a group when the *Control* window is minimized.

To minimize windows as a group:

1. Go to the *Window* menu on the *Control*  window
2. Select *Minimize Control Minimizes All*. The analyzer puts a check next to the menu item, indicating that when the Control window is minimized, all windows are minimized.
3. Select the menu item again to deactivate this feature.
4. The windows minimize to the top of the operating system Task Bar.

3 Configuration Settings

3.1 Hardware Settings

3.1.1 Determining Hardware Settings

Choose a *Bluetooth*® ComProbe® device to use from the drop down list. Click Refresh to update the list if you change or add devices. If you only have one *Bluetooth* ComProbe connected to your PC, that device is used automatically and you don't need to select it.

The dialog also lists information on the current device connection, the *Bluetooth* Device Address (BD_ADDR) of the *Bluetooth* ComProbe, the hardware type, and the firmware version.

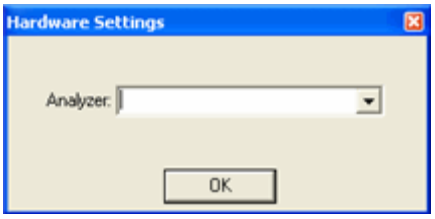
3.1.2 Establishing the Hardware Setup

1. Connect the *Bluetooth*® ComProbe® to an available USB port.
2. Open the FTS4BT folder on your desktop and double-click FTS4BT Air Sniffer. FTS4BT starts and the *Bluetooth* ComProbe icon appears in your system tray (usually found in the lower right corner of your screen) in red. Also, the Data Source Control dialog box appears.
3. Click the Hardware Settings button and select which *Bluetooth* ComProbe to use. Click OK to return to the Data Source dialog.
4. Click the I/O Settings button on the Data Source Control dialog and enter all the necessary *Bluetooth* ComProbe setup information. Click OK when finished to return to the Data Source Control window.
5. On the Control Window, click the red circle  to start data capture. When data begins arriving the analyzer will capture it.
6. Click the Start Sniffing button to begin synchronizing to the piconet.

3.1.3 Establishing the USB Hardware Settings

When establishing USB settings, you must select which device to sniff.

1. Connect the USB ComProbe® to an available USB port.
2. Start the analyzer.
3. Click the Hardware Settings button and select which USB ComProbe to use.



Choose a USB ComProbe device to use from the drop down list. If you just have one USB ComProbe connected to your PC, that device is used automatically and you don't need to select it.

4. Start data capture. On the Control Window, click *Start Capture* icon  .

Check the I/O Settings dialog to select the packet types filtered out of the capture.

3.1.4 FTS4BT/USB Datasource Dialog

FTS4BT USB ComProbe® Datasource

The FTS4BT USB Datasource Dialog allows the user to select a USB sniffer device, and to initiate/terminate the sniffing process. The dialog has a list control containing the USB Devices connected to your system. If you connected or disconnected a device:

1. Click the Refresh List button to update the list
2. Choose a USB ComProbe device to use from the drop down list. If you only have one ComProbe connected to your PC, that device is used automatically and you don't need to select it.
3. Click the *Start* button to start the sniffing process
4. Click on the *Start Capture* button on the Control window to capture data.

3.1.4.1 USB HCI (H2) - USB ComProbe

The *Bluetooth*® Core Specification defines USB endpoint numbers for each of the four HCI packet types.

1. Normally you would never need to change these assignments. However, if you need to change these assignments, then click the *Settings* button and change them as needed.

Note- HCI commands always go out from the host and in to the USB device.

3.1.4.2 USB HCI (H2) + raw USB packets - USB ComProbe

Capture Filters

FTS filters out a number of packet types by default.

If you would like to see these packet types:

1. Click the Capture Filters button.
2. Un-check the box next to the type of packet you wish to include in your results. Some of these packet types can be so numerous that they may make it more difficult to locate data packets in the Frame Display and Protocol Navigator windows.

3.1.4.3 Hardware Installation

Consult the Quick Start Guide for information on installing the USB ComProbe.

To access the PDF version of the Quick Start Guide from your Windows operating system

1. Click Start | Programs | FTS4BT [version #] | Quick Start Guide, or locate it in the FTS4BT desktop folder.

3.1.5 Internal Tap Datasource Dialog

The USB Data Source Dialog allows the user to initiate or terminate the sniffing process on a USB device.

This dialog has a list control containing the USB Devices connected to your system. If the *Show Connected Only* checkbox is unchecked then all USB devices that have ever been connected to your system are listed.

The *Refresh List* button updates the list if you have connected or disconnected a device while this dialog is open.

To initiate the sniffing process:

1. Select the device you wish to sniff then click on the *Start Sniffing* button.
2. Click on the *Start Capture to Disk* icon on the Control window to capture data.

3.1.6 USB HCI Sniffing

The analyzer restarts the USB *Bluetooth*® Device when the *Start Sniffing* button on the Control dialog is pressed. Some USB *Bluetooth* devices are unable to restart if they are connected to another *Bluetooth* Device.

If this is the case, you should:

1. Break the connection between the device you want to sniff and any devices it is communicating with.

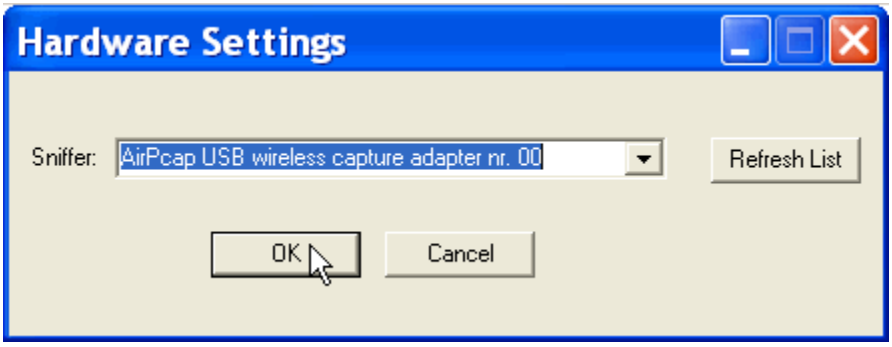
2. Click the *Start Sniffing* button.
3. Reconnect the devices so that you can sniff the connection.

For a specific example here is how to sniff the Microsoft Keyboard and Mouse.

3.1.7 802.11 Hardware Settings

The Hardware Settings dialog provides the ability to select a device to sniff/scan. The dialog only lists devices with a MAC address that match the FTS4BT list. To access the Hardware Settings dialog:

1. Select Hardware Settings from the Options menu on the 802.11 Control window.



2. Select a device from the drop-down list.
3. Select OK

If no devices are found, the list is blank.

Note:

Upon launching FTS4BT Air Sniffer, the first device in the drop-down is the default device.

3.1.8 Troubleshooting USB Communications

Most performance problems such as input buffer overflow are the result of improper connections.

To achieve optimal performance from the USB analyzer, we recommend the following configuration:

- Use two high-speed computers, one for the analyzer and one for the device under test.
- Use USB 2.0 connections.
- Use cables that do not exceed the recommended maximum lengths (the cable connected to the analysis computer should not exceed 15 feet, and the total length of the cables connected to the test computer and the device under test should not exceed 9 feet).

Although it is possible to use one computer as both the analysis and the test computer, this requires that the computer in use is high-speed and has two or more host controllers available. If you attempt to analyze data using one computer with only one host controller, then the system displays an error message informing you of the problem.

If the operating system encountered an error when trying to install a device, simply disconnect the device, then reconnect it and try again.

Negative Timestamp Delta Value

On rare occasions, the system may display a negative delta value. One possible explanation has to do with the Reset function. The timestamp occurs when the Reset is actually sent but perhaps as much as 10 ms might pass before the Reset takes effect. Only then does the Datasource send the Reset up to the analyzer, and thus the negative delta.

USB HCI – Internal Tap FTS4USB Spy Mode

Sniffing USB devices without the aid of a USB ComProbe® can be troublesome. Some of the data, such as file transfers when sniffing flash drives, are often missed when sniffing USB devices directly causing the analyzer to ignore subsequent data. If the analyzer appears to stop processing data from a USB device when running in “Internal TapSpy” mode, then simply install a USB ComProbe, restart the packet sniffer, and the system should function normally.

3.1.9 Sniffing the Microsoft Keyboard and Mouse

To sniff the Microsoft® Keyboard and Mouse, start the USB HCI packet sniffer, select the Wireless Transceiver and select the Start Sniffing button.

On some versions of Windows® the Windows USB driver cannot reset when it is in use. In this case you get an error saying "Invalid Selection – device may be in use". To get around this problem use the following steps to sniff the Keyboard and Mouse.

1. The first thing you need to do is to break the connections from the keyboard and mouse to the Wireless Transceiver. There is a button on the bottom of the keyboard. Press this button and hold for a bit to make sure it took effect. There is a similar button at the bottom of the mouse. Press and hold it too. We need to break all connections to the Wireless Transceiver or we are not able to restart.
2. Start the USB HCI packet sniffer. On the data source find the Microsoft Wireless Transceiver and hit the Start Sniffing button, and hit the Start Capturing button.
3. Go to the Start menu and find the Microsoft Keyboard program and use it to reconnect the keyboard.
4. Go to the Start menu and find the Microsoft Mouse program and use it to reconnect the mouse.
5. All traffic should now be sniffed.

3.2 I/O Settings

3.2.1 Bluetooth® I/O Settings

The I/O Settings window has all the setup information the analyzer needs in order to synchronize with the piconet and capture data. The analyzer requires information on the clock synchronization method and the device address of the device to initially sync to. You may optionally specify an inquiry access code to limit the device addresses the analyzer looks at, choose whether or not to capture certain packet types and specify any encryption information needed to correctly decode data.

- Choosing a Clock Synchronization Method
- Specifying the *Bluetooth*® Device Address (BD_ADDR) to Sync To
- Encryption
- Capture Filtering
- Advanced

3.2.1.1 Bluetooth® Async - I/O Settings Dialog

The I/O settings dialog allows you to configure the analyzer for communication, monitor, and source operating modes. The analyzer requires circuit settings or the protocols present on your circuit to operate properly.

Baud, parity, length and stop settings for DTE and or DCE devices are set in the I/O Settings dialog. The analyzer only allows you to change settings that are relevant to your operating mode. All other settings are grayed out if not applicable. Some settings only apply to specific modes. If a configuration file is being used, the analyzer reverts to its default settings. You can return to the default settings at any time by clicking the Factory Defaults icon.

When using capture file viewer, the only settings accessible in the I/O settings dialog are Custom Protocol Stack and the Names button. The analyzer determines which protocols were used when the file was captured and decodes the data in the file accordingly.

To change the protocols:

1. Click the Custom Protocol Stack  button
2. Select a protocol
3. Click Finish

To change the names of labels for sides, errors and control signals:

4. Click the Names button
5. Click on the item in the Current column
6. Double click (slowly) on the item again to modify.

3.2.2 Selecting a Synchronization Mode

The Bluetooth® analyzer needs to know how to synchronize with the piconet. The analyzer supports two Synchronization Modes.

Standard (Slave Page)

This is the preferred synchronization mode to use.

The analyzer pages the slave device to obtain an estimate of its *Bluetooth* clock; however, the paging process does not get completed so the slave device times out and returns to page scanning. The analyzer then enters continuous page scan mode, using the slave's estimated *Bluetooth* clock and the slave's address to calculate the page scan frequencies. When the master pages the slave, the analyzer switches to the master's *Bluetooth* clock and then follows the master's frequency hopping sequence. This synchronization mode requires that the slave is page scanning prior to being paged by the master. This synchronization mode is considered to be passive because the *Bluetooth* host is never made aware of the page made by the analyzer since the paging process does not get completed.

Note: Since no slave address will have not been specified, clicking on Start Sniffing will generate the message "Cannot start sniffing: the synchronization method that you have selected requires that you select a Slave Device to synchronize with. Please select a Slave Device" in the status window.

Alternate - Slave must be Discoverable (Slave Inquiry)

The analyzer performs an inquiry of the slave device to obtain its *Bluetooth* clock. The analyzer then enters continuous page scan mode, using the slave's *Bluetooth* clock and address to calculate the correct page scan frequencies. When the master pages the slave, the analyzer switches to the master's *Bluetooth* clock and then follows the master's frequency hopping sequence. This synchronization mode requires that the slave has inquiry scan enabled and is page scanning prior to being paged by the master. Interlaced Page Scan is an example of a mode that will only work with Slave Inquiry synchronization.

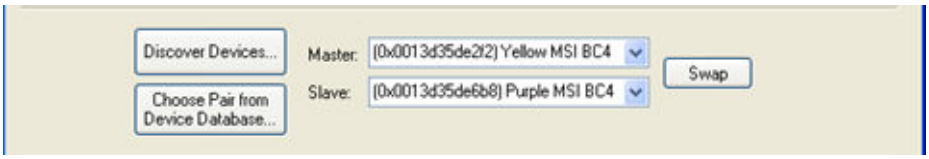
Interlaced Page Scan

For Interlaced Page Scan, there is no choice. The Slave must be discoverable.

1. Select one of the mode radio buttons.

3.2.3 Specifying the Synchronization Device

The analyzer needs to know the *Bluetooth*® Device Address (BD_ADDR) of the synchronizing device. If you have selected Slave Inquiry Mode or Slave Page Mode, you must specify a Slave address. You may optionally specify a Master device if you want to be certain of sniffing a specific piconet. If you have selected Master Inquiry Mode, you must specify a Master address, and may optionally specify a Slave address.



You can specify the *Bluetooth* Device Address in multiple ways.

1. Select the *Bluetooth* Device Address (BD_ADDR) from a list of available devices.

   The list of available devices is stored in the Device Database. To add to the list, press the Discover Devices button. A device inquiry is performed and all discoverable devices (subject to matching up with the Inquiry Access Code) is then available from the drop-down list. If you want to limit the list of devices by access code, select an access code from the Device Discovery combo box located on the Advanced I/O Settings dialog.

   Note: If you click Discover Devices before you start capturing data, FTS will still discover the *Bluetooth* devices, but the device descriptions will not contain any Extended Inquiry Response (EIR) data. To capture EIR data you have to actually start a data capture first, then select Discover Devices.

2. Type in the number as a 12 digit hex number.

   The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.

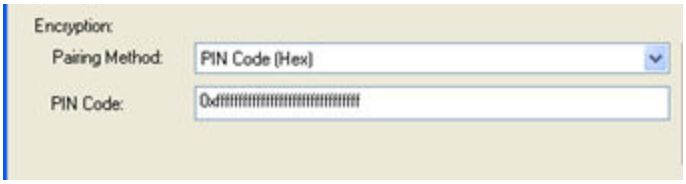
3. Press the Choose Pair button.

   This button takes you to the Device Database Dialog, which allows you select a pair of devices and a Link Key from a list.

Note: Clicking the Swap button switches the Slave and Master addresses.

3.2.4 Encryption

Bluetooth® devices can have their data encrypted when they communicate.



There are five encryption options in the I/O Settings dialog.

- None

- PIN Code (ASCII)
- PIN Code (Hex)
- Link Key
- Secure Simple Pairing

You are able to switch between these methods in the I/O Settings window. When you select a method, a note appears at the bottom of the dialog reminding you what you need to do to successfully complete the dialog.

- **First**, you can choose None as the encryption method when neither of the devices has encryption enabled.

- The **second** and **third ways** are to use a PIN Code to generate the Link Key. The devices generate link Keys during the Pairing Process based on a PIN Code. The Link Key generated from this process is also based on a random number so the security cannot be compromised. If the analyzer is given the PIN Code it can determine the Link Key using the same algorithm. Since the analyzer also needs the random number, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

  Example:

  If the ASCII character PIN Code is *ABC* and you choose to enter the ASCII characters, then select *PIN Code (ASCII)* from the Encryption drop down list and enter *ABC* in the field below.

  If you choose to enter the Hex equivalent of the ASCII character PIN Code *ABC*, then select *PIN Code (Hex)* from the Encryption drop down list and enter *0x414243* in the field. Where *41* is the Hex equivalent of the letter *A*, *42* is the Hex equivalent of the letter *B*, and *43* is the Hex equivalent of the letter *C*.

  Note: When *PIN Code (Hex)* is selected from the Encryption drop down list, the *0x* prefix is entered automatically.

- **Fourth**, if you know the Link Key in advance you may enter it directly. Select *Link Key* in the Encryption list and then enter the Link Key in the edit box. If the link key is already in the database, the Link Key is automatically entered in the edit box after the Master and Slave have been selected. You can also pick *Choose Pair from Device Database* to select a Master, Slave and Link Key from the Device Database.

- **Finally**, you can select *Secure Simple Pairing* (SSP) mode. SSP is the encryption methodology developed in *Bluetooth* Core Specification - 2.1+EDR. This enables sniffing without using a debug mode in the devices under test. SSP requires a Master Private Key and a Slave Private Key. These numbers are used to generate a 6 digit value which the user must confirm, for instance by typing in the same value as is displayed on a screen, or pressing Yes or No when asked if both devices are

displaying the same value. If the devices you are using on in Secure Simple Pairing Debug Mode, FTS4BT will automatically recognizes the debug mode.

If you want to use SSP, you must enter the values for the Private Key.

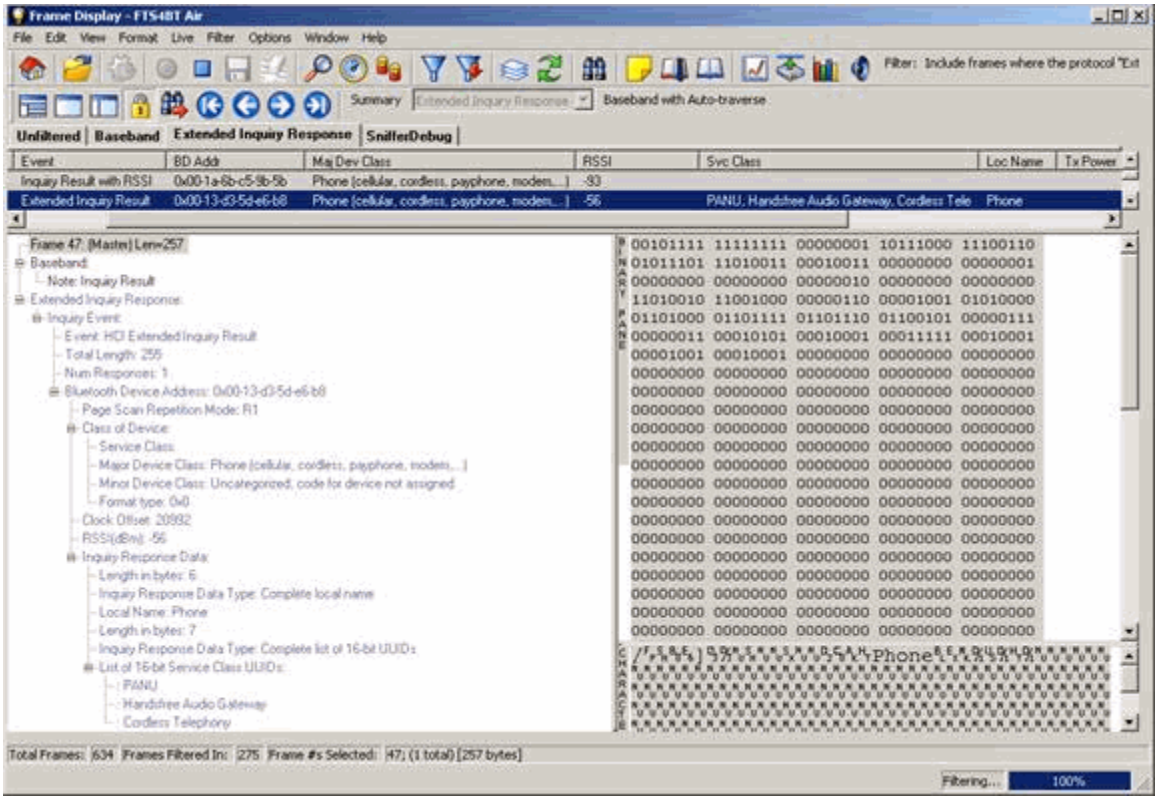
Filtering

- The analyzer filters out a number of packet types by default. If you would like to see these packet types, un-check the box next to the type of packet. Some of these packet types can be so numerous that they may make it more difficult to locate data packets in the Frame Display and Protocol Navigator windows.
- Select the Frame Slicing checkbox if you wish to limit the size of frames sent to the analyzer from the Datasource. When analyzing large frames, often only the first few bytes of a frame are of interest. Frame Slicing allows the user to choose not to process a portion of large frames.

Note: *Current Link Key* is a display only field. This field displays the last known link key, if one exists.

3.2.5 Extended Inquiry Response

Extended Inquiry Response (EIR) is a tab that appears automatically on the Frame Display window when you capture data.



EIR displays extensive information about the Bluetooth® devices that are discovered as data is being captured. Before the EIR tab was created, this type of information was not available until a connection was made to a device. Therefore, EIR can be used to determine whether a connection can/should be made to a device prior to making the connection.

Note: If a Bluetooth® device does not support Extended Inquiry Response, the tab displays Received Signal Strength Indication (RSSI) data, which is less extensive than EIR data.

3.2.6 Advanced Bluetooth I/O Settings

3.2.6.1 Advanced I/O Settings

The Advanced I/O Settings window contains additional options for synchronizing the analyzer with the piconet to capture data.

1. **Automatically initiate Clock Synchronization Options**
   - If you would like to have the analyzer resynchronize when a Link Manager Detach (LMP_Detach) packet is received after a specific period of time or when the Bluetooth ComProbe has not been locked to the Master Clock, you must select the options here.
   - You can adjust the amount of time until re-synchronization if synchronization is lost for more than a specified amount of time for both LMP_Detach and ComProbe/Master Clock. The time is set by default to 30 seconds for the ComProbe/Master Clock and six (6) seconds for the LMP-Detach.

2. **Access Codes**

   Access Codes controls which devices are placed into the selection list when Discover Devices is pushed on the I/O Settings screen. Device Discovery is used for selecting a device address to synchronize to.

3. **ComProbe® Settings**
   - *Sniffer Timeout* should not be changed unless you have contacted technical support first.
   - *Slave Inquiry Clock Offset* allows you to skew the packet sniffer´s clock when using slave inquiry to sync to a piconet. This can improve syncing with some devices. However, this should only be used after consultation with technical support.
   - *Use Hard Resets* is similar to removing and reinserting a device. This option should remain checked unless advised differently by technical support
   - *Drift Compensation* does two inquires on the slave clock and compares the difference between the two clock inquires with our own reference clock. A linear interpolation of the drift is done and applied to the slave's clock.
   - *Prioritized Decryption* can be selected if you are having trouble establishing the correct decryption. This option adjusts the data capture to give priority to

establishing the proper decryption over receiving frames. If you select this option, some frames may be dropped, but establishing the decryption key will be more efficient.

- *Sniffer Diagnostics* - When this is checked, some diagnostic data from the ComProbe® is captured and stored in the .cfa file. This is useful when a .cfa file is sent to Frontline for analysis and diagnosis. Technical support may ask you to check this option when you are experiencing issues with FTS4BT.

4. **Frame Slicing Settings**
   - Frame Slicing Settings allow you to enter the size of the largest frame allowed to pass the analyzer without having any bytes removed. The second field tells the analyzer the number of bytes you would like to capture if the frame is larger than the allowable value indicated in the first field.

5. **Active Member Following**
   - You can use this dialog to change which member the firmware follows. In previous versions, the firmware would decode the low-level information for all members of the piconet. To support AFH, the firmware must only decode this information for one member. All packets are sniffed and decoded at the higher levels but the low-level decoding is followed on the first member of the piconet it sees.
   - There are eight levels of decoding when using Air Sniffer.
   - The default is the First Active LT-ADDR (Same as **First Active Member** in previous versions).
   - You can also choose a number from one to seven that corresponds to an active member (Same as selecting Single Active Member and a number from the drop-down in pervious versions).

6. **AFH Following**

   You can choose to enable or disable this feature by selecting the respective checkbox.

7. **Channel Map**
   - *Clear on Resync* -used to clear the map each time a resynchronization occurs
   - *Send with data*- allows you to send a map each time data is sent instead of just sending a map when changes occur.

Note:

Because of hardware filtering of packets; as selected on the I/O Settings dialog, some packets are not captured and therefore some active channels may not be indicated in the Channel Map Display.

3.2.6.2 Force Adapted Hopping Sequence (AHS)

Adapted Hopping Sequence

If you suspect that the hop sequence changed, and the analyzer missed capturing the new one, then click on the *Force AHS (79)* button. This makes the analyzer hop all 79 channels, thereby eliminating the possibility of missing packets transmitted on channels not included in the earlier channel map. the analyzer remains in the AHS (79) state until a new channel map is received.

The master controls and enables hop sequence adaptation. When communication is initiated, the master, with input from the slave, establishes the hop sequence. The master shares the resulting channel map with the slave. If the analyzer catches the channel map when it is transmitted, then the analyzer adopts the same hop sequence. During the communication session, the master may periodically update the set of used and unused channels, create another channel map, and share the new sequence with the slave. If the analyzer does not capture the new channel map information, then the analyzer may miss packets transmitted on channels included in the new hop sequence that were absent in the old one.

3.2.7 Air Sniffing FTS4BT

3.2.7.1 Air Data Source Dialog

The Data Source Control window provides access to and displays the status of the *Bluetooth*® ComProbe® . As data is being captured, the Status message at the top of the window indicates the synchronization status of the *Bluetooth* ComProbe . Also, the color of the *Bluetooth* ComProbe icon in the system tray changes depending on the synchronization state.

There are five states:

Blue = running and in sync with the piconet.

Green = running and waiting for piconet to form or reform

Yellow = attempts to resynchronize in 5 seconds.

Red = initializing

White = stopped.

The Functions of the Buttons

- **Resync Now** - When you start sniffing, the buttons cycle through Green, Yellow, Red every thirty seconds. When it is red it is resyncing. Selecting the Resync Now button causes it to be red immediately instead of having to wait for the full thirty seconds.
- Force AHS(79) – Forces the analyzer to sniff all 79 channels
- Hardware Settings - opens a dialog box where you can change which *Bluetooth* ComProbe device to use and get information on the *Bluetooth* ComProbe's Device Address (BD_ADDR).
- I/O Settings - opens a dialog box where you can change synchronization mode, device to sync to, and other parameters related to encryption and packet capture.
- **Start Sniffing** - sets up the *Bluetooth* ComProbe using the settings from the I/O Settings window and synchronizes to the piconet. This button changes its name to Stop Sniffing when it is in sniffing mode. If no ComProbe is plugged in, Start Sniffing button will be grayed out and the message "There is no Bluetooth ComProbe plugged in. Please plug in a Bluetooth ComProbe" will be displayed in the status window. All settings are saved automatically when you start sniffing.
- **Stop Sniffing** - stops monitoring data.
- **Channel Map**  Click this button to toggle the display of the Channel Map.

  This display is used to determine which channels are available with Adaptive Frequency Hopping.

- **Green**

  Channel is currently available for use.

- **Red**

  When Adaptive Frequency Hopping is in use; red indicates that the channel has been marked unavailable.

- **Blue**

  Indicates that a packet was captured on the channel.

The *Clear* button resets each indicator back to the green state. The indicators are also reset whenever a new Channel Map goes into effect.

3.2.8 Channel Map Info

On the FTS4BT Datasource dialog you can access the Channel Map info by clicking the arrow on the lower right corner.

This display is used to determine which channels are available with Adaptive Frequency Hopping.

- **Green**

  Channel is currently available for use.

- **Red**

  When Adaptive Frequency Hopping is in use; red indicates that the channel has been marked unavailable.

- **Blue**

  Indicates that a packet was captured on the channel.

The *Clear* button resets each indicator back to the green state. The indicators are also reset whenever a new Channel Map goes into effect.

Note:

Because of hardware filtering of packets; as selected on the I/O Settings dialog, some packets are not captured and therefore some active channels may not be indicated in the Channel Map Display.

3.3 High Speed UART (HSU) Option

3.3.1 HSU Hardware Requirements and Configuration

System requirements for the EB ComProbe®:

- Windows XP SP2
- One USB 2.0 High Speed enabled port. The EB ComProbe does not run on USB 1.1 Full Speed ports.

Connect the EB ComProbe to a Source

The EB ComProbe is designed for use with TTL voltage levels, 0 to 5 volts max (exceeding the 5.0 volts max damages the ComProbe). The ComProbe interprets 0 to 1.9 volts as a logical zero, and 2.0 to 5.0 as a logical one. To ensure accurate data collection and proper operation, connect the ComProbe to the TTL side of any transceivers, line drivers, or line receivers.

Use the table below to determine the connection configuration you need for monitoring signals on the source device. Disconnecting and reconnecting the wires in a different configuration negates the validity of the following table. To avoid confusion, we recommend that you maintain the color code as expressed in this table.

Note: Disconnecting the EB ComProbe from the source while capturing data with FTS4BT may temporarily affect your computers performance. To ensure proper operation of your system, always terminate FTS4BT live capture prior to removing the ComProbe from the circuit under test.

Pin outs for the EB ComProbe:

Wire Label	Label/Wire Color	Signal	Meaning

0	Black	CH 0	Data Connection
1	Brown	CH 1	Data Connection
2	Red	RTS	Request to Send
3	Orange	CTS	Clear to Send
4	Yellow	DSR	Data Set Ready
5	Green	DTR	Data Terminal Ready
6	Blue	CD	Carrier Detect
7	Violet	RI	Ring Indicator
TRG	White	Not Used	N/A
CLK	Gray	Not Used	N/A
GND	Black	Ground	Ground

3.3.2 Identifying HSU Hardware Settings

Select *Hardware Settings* from the *Options* menu on the Control window.

1. Choose a device to use from the drop down list.
2. Click Refresh to update the list if you change or add devices. If you just have one device connected to your PC, that device is used automatically and you don't need to select it.
3. Click the *Performance Test* button to run this test manually. The Performance Test determines the maximum rate at which you can capture data. This rate is tied to the speed of your computer in combination with the capabilities of the selected EB ComProbe®. The result of the test is displayed at the bottom of the I/O Settings dialog.

3.3.3 Identifying HSU I/O Settings

1. Click the *I/O Settings* icon  on the Control window, or select *I/O Settings* from the *Options* menu on the Control window  , the Frame Display  , the Protocol Navigator  , or the Event Display  .

The first time you open the I/O Settings dialog with a new EB ComProbe® connected, the system asks if you want to run a performance test.

2. Click OK, and the system determines the maximum rate at which you can capture data. This rate is tied to the speed of your computer in combination with the capabilities of the selected EB ComProbe. The result of the test is displayed at the bottom of the I/O Settings dialog. This test can be run manually on the Hardware Settings dialog.

The analyzer requires information on Bit Rate, Parity, Length, and number of Stop bits in order to operate properly. If you are capturing framed data, the analyzer needs to know which protocols are present on your circuit to decode them correctly.

There are two rows of settings, the CH 0 (data connection), and the CH 1 (data connection).

To change the bit rate, parity, word length or number of stop bits:

1. Click on the down arrow next to the setting box and choose an option from the list. For bit rate, you can either choose a listed rate or enter a rate.
2. After entering the settings for CH 0, click the *Copy CH 0* button to apply the same settings to the CH 1 row.
3. Check the Invert Control Signals checkbox to invert the interpretation of the voltage on the control signal lines (e.g. zero volts would be interpreted as a binary 1 and voltage would be interpreted as a binary 0).

3.4 Port Assignments

3.4.1 Adding or Changing Port Assignments

The analyzer autotraverses the stack from TCP, UDP and IPX based on the source or destination port number. Many systems use user-defined port numbers for both standard and custom protocols. Here's how to tell the analyzer about a custom port assignment on the system you are monitoring.

Add a New Port Assignment

1. Choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window 
2. Click the *TCP* tab (or UDP or IPX for those protocols).
3. Choose the *Single Port* radio button, and enter the port number in the *Port Number* box.
4. In the *Protocol* drop-down list, choose the protocol to traverse to.
5. Click the *Add* button. The system adds new entry to the bottom of the port number list.

Modify an Existing Port Assignment

1. Choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window.
2. Click the *TCP* tab (or UDP or IPX for those protocols).
3. Select (click on and highlight) the port assignment to modify.
4. Change the port number and/or choose the protocol to traverse to.
5. Click the *Modify* button. The system displays the changes in port number list.
6. You can also specify a range of ports. Select the *Port Range* radio button and specify the starting and ending port numbers. The range is inclusive.
7. To remove an entry, select the entry and click *Delete*.

Two considerations are:

- The analyzer traverses an entry if either the source or destination port match
- The analyzer processes port number entries in order from top to bottom
  If you need to move an entry to ensure it is processed before or after another entry, select the entry in the list and then click the *Move Up* or *Move Down* buttons.

3.5 Decoder Parameters

Some protocol decoders have user-defined parameters. These are protocols where some information cannot be discovered by looking at the data and must be entered by the user in order for the decoder to correctly decode the data. For example, such information might be a field where the length is either 3 or 4 bytes, and which length is being used is a system option.

If you have decoders loaded which require decoder parameters, a window with one tab for every decoder that requires parameters appears the first time the decoder is loaded.

For help on setting the parameters, click the Help button on each tab to get help information specific to that decoder.

If you need to change the parameters later,

- Choose Set Initial Decoder Parameters from the Options menu on the Control, Frame Display or Protocol Navigator windows.
- Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The Set Subsequent Decoder Parameters dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter

- Select the frame where the change should take effect
- Select Set Subsequent Decoder Parameters from the Options menu, and make the needed changes.

- Each entry in the Set Subsequent Decoder Parameters dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

3.5.1 A2DP Decoder Parameters

3.5.1.1 Selecting A2DP Decoder Parameters

The decoding of SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame in detail. You can increase the decoding speed by decoding only the header fields and not all the parts if they are not required. You can select the detail-level of decoding using the **Set Initial Decoder Parameters** dialog.

Note: By default the decoder decodes only the header fields of the frame.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *A2DP* tab.
3. Choose the desired decoding method.
4. Click the *OK* button to apply the selection and exit the *Set Initial Decoder Parameters* dialog.

3.5.2 Security Parameters

3.5.2.1 Security Key

On the Set Initial Decoder Parameters dialog, the security tab allows specifying a key for software decryption of 802.11 frames. One can enter two types of keys. The types are a WPA (Wi-Fi Protected Access) pre-shared key and a WEP (Wired Equivalent Privacy) key.

To access this dialog:

1. Go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters.*
2. Select the *Security* tab.

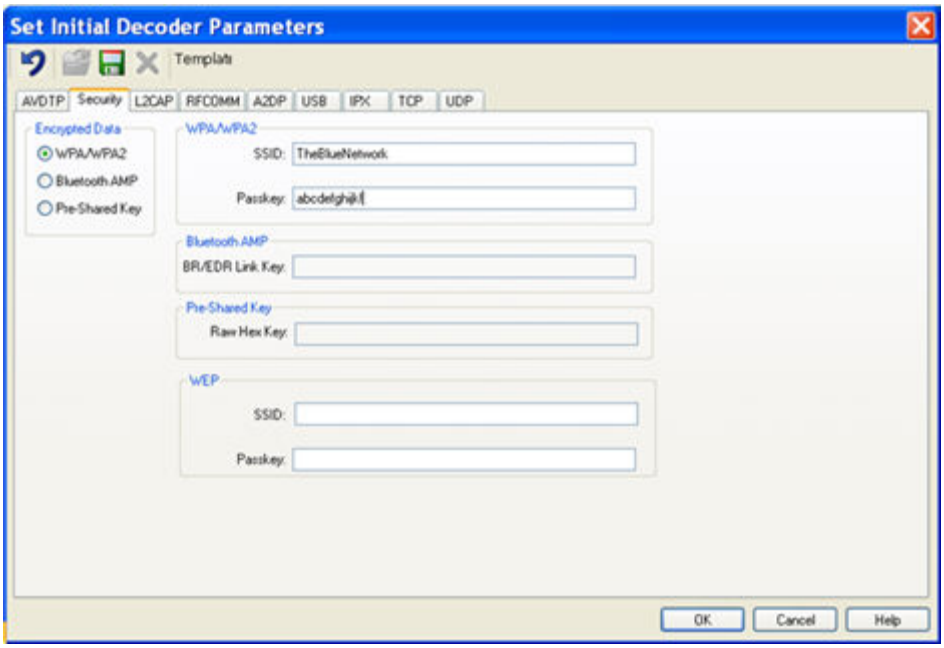
There are three types of types of encrypted data on the security tab, each one selectable via a radio button.

- WPA, WPA2 (Wi-Fi Protected Access), and WEP (Wired Equivalent Privacy) data that is transmitted over a Wi-Fi communications link. There are two values you have to enter for the WPA/WPA2 and WEP to be decrypted properly.

- The Bluetooth® alternative MAC/PHY (AMP) enables Bluetooth to support data rates up to 24Mbps by using additional wireless radio technologies.

- The Pre-Shared Key: The third way is to specify the pre-shared key in its raw hex forum. This is a 32 byte hex number.
  Note: When you use WPA/WPA2, the Pre-Shared key is generated automatically.

Depending on which Encrypted Data type you select, the options for entering data on the rest of the dialog varies.



3.5.2.1.1 TO SET THE WPA/WPA2 VALUES.

1. Select the WPA/WPA2 radio button.

This activates the WPA/WPA2 and WEP text boxes.

There are two values to set for the WPA and WEP keys.

2. Set the WPA/WPA1 and WEP Service Set Identifiers (SSID).

The SSID is the station ID of the Wi-Fi communications link.

3. Set the WPA/WPA2 and WEP Passkeys.

The Passkey field is the shared passkey phrase used in communications.

4. Select *OK* to save the settings and close the dialog.

3.5.2.1.2 TO SET THE BLUETOOTH AMP VALUES.

This is used when capturing 802.11 alternative MAC/PHY (AMP) frames for Bluetooth High Speed.

1. Select the Bluetooth AMP radio button.

This activates the Bluetooth AMP and WEP text boxes.

2. Enter a hexidecimal value for the Basic Rate or Extended Data Rate (BR/EDR) Link Key.

3. Set the WEP Service Set Identifier (SSID).

The SSID is the station ID of the Wi-Fi communications link.

4. Set the WEP Passkey.

The Passkey field is the shared passkey phrase used in communications.

Note: When capturing both Bluetooth and 802.11 data using the 802.11 AMP capture selection, FTS uses the link from the BR/EDR connection. To automatically decode 802.11 AMP frames in this case, select the Bluetooth AMP encryption type but leave the link key blank.

5. Select *OK* to save the settings and close the dialog.

3.5.2.1.3 TO SET THE PRE-SHARED KEY VALUES.

The third way is to specify the pre-shared key in its raw hex forum. This is a 32 byte hex number.
Note: The other ways of specifying the WPA key automatically generate this value.

1. Select the Pre-Shared Key radio button.

This activates the Pre-Shared Key and WEP text boxes.

2. Enter a 32 byte hex number for the Pre-Shared Key.

3. Set the *WEP Service Set Identifier (SSID)*.

The SSID is the station ID of the Wi-Fi communications link.

4. Set the WEP Passkey.

The Passkey field is the shared passkey phrase used in communications.

5. Select *OK* to save the settings and close the dialog.

3.5.3 AVDTP Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame but did not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters dialog provides a means to supply the context for any frame. The dialog allows the user to define any number of parameters and save them in a Parameter Template for later use.

The Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each *Bluetooth*® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. The AVDTP Set Initial Decoder Parameters dialog requires the following user inputs to complete a Parameter:

- Data Source Number
  When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- Device Role
  This identifies the role of the device initiating the frame (master or slave)
- L2CAP Channel
  The channel number 0 through 78
- AVDTP Carries
  Select the protocol that AVDTP traverses to from the following:
  - AVDTP Signaling
  - AVDTP Media
  - AVDTP Reporting
  - AVDTP Recovery
  - -Raw Data-

3.5.3.1 Selecting and Applying an AVDTP Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *AVDTP* tab
   The dialog displays the content of the most recently selected Parameter Template in the

Initial Connections list at the top of the tab. If the template displayed is the desired template, then skip to step 4. If it is not, then continue with step 3.

3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exit the *Set Initial Decoder Parameters* dialog.

3.5.3.2 AVDTP Parameters

3.5.3.2.1 ADDING AN AVDTP PARAMETER

This procedure adds one or more parameters to an existing Parameter Template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *AVDTP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template , then click the Open File button and select the desired template from the Popup list.

3. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source

4. Select the Device Role.
   This identifies the role of the device initiating the frame (master or slave)

5. Enter the L2CAP Channel.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

6. Select the protocol AVDTP Carries.
   Select the protocol that AVDTP traverses to from the list

7. Click the Add button.
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 8 until all desired parameters are added.

8. Click the Save icon at the top of the dialog to display the *Save As* dialog.

9. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template

10. Click the *Yes* button.
    The system saves the new parameter to the template and closes the *Save As* dialog.

11. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.3.2.2 DELETING AN AVDTP PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *AVDTP* tab.
   The dialog displays the most recently selected Parameter Template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the *Set Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.3.3 AVDTP Parameter Templates

3.5.3.3.1 ADDING AN AVDTP PARAMETER TEMPLATE

This procedure adds a Parameter Template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *AVDTP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults button at the top of the dialog to clear the *Initial Connections* list.

4. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

5. Select the Device Role.
   This identifies the role of the device initiating the frame (master or slave).

6. Enter the L2CAP Channel
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

7. Select the AVDTP Carries
   Select the protocol that AVDTP traverses to from the list.

8. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 9 until all desired parameters are added.

9. Click the Save button at the top of the dialog to display the *Save As* dialog.

10. Enter a name for the new template and click *Ok*.
    The system saves the template and closes the *Save As* dialog.

11. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.3.3.2 DELETING AN AVDTP PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *AVDTP* tab
   The dialog displays the most recently selected Parameter Template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete button at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.5.3.4 AVDTP Missing Decode Information

3.5.3.4.1 AVDTP MISSING DECODE INFORMATION

The analyzer usually determines the protocol carried in an AVDTP payload by monitoring previous traffic. However, when this fails to occur, the Missing Decoding Information Detected dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- the capture session started after transmission of the vital information
- the analyzer incorrectly received a frame with the traversal information
- the communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the AVDTP payload of this frame (and other frames with the same channel) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.5.3.5 AVDTP Override Decode Information

3.5.3.5.1 AVDTP OVERRIDE DECODE INFORMATION

The Set *Subsequent Decoder Parameters* dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect
2. Select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Choose the protocol the selected item carries from the drop-down list, and click *OK*.

Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.5.4 L2CAP Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame but did not capture the command frame, then the decode for the response may be incomplete. The **Set Initial Decoder Parameters** dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in a Parameter Template for later use. To access this dialog:

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

For more on setting parameters, see Selecting and Applying an L2CAP Parameter Template.

The Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each *Bluetooth*® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The L2CAP Set Initial Decoder Parameters dialog requires the following user inputs to complete a Parameter :

- Stream
  This identifies the role of the device initiating the frame (master or slave)
- Channel ID
  The channel number 0 through 78
- Connection Handle
  This is the actual physical connection values for the devices
- Data Source Number
  When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- Carries (PSM)
  Select the protocol that L2CAP traverses to from the following:
  - AMP Manager
  - AMP Test Manager
  - SDP
  - RFCOMM
  - TCS
  - LPMP
  - BNEP
  - HCRP Control
  - HCRP Data
  - HID
  - AVCTP
  - AVDTP
  - CMTP
  - MCAP Control
  - IEEE P11073 20601
  - -Raw Data-

3.5.4.1 Selecting and Applying an L2CAP Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab
   The dialog displays the content of the most recently selected Parameter Template in the

Initial Connections list at the top of the tab. If the template displayed is the desired template , then skip to step 4. If it is not, then continue with step 3.

3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exit the *Set Initial Decoder Parameters* dialog.

3.5.4.2 L2CAP Parameters

3.5.4.2.1 ADDING AN L2CAP PARAMETER

This procedure adds one or more parameters to an existing Parameter Template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window  , the Frame Display window  , or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *L2CAP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template , then click the Open File icon and select the desired template from the Popup list.

3. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

4. Enter the Channel ID.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

5. Enter the Connection Handle.
   This is the L2CAP address.

6. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

7. Select the Carries (PSM).
   Select the protocol that L2CAP traverses to from the list.

8. Click the Add button.
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 8 until all desired parameters are added.

9. Click the Save icon at the top of the dialog to display the *Save As* dialog.

10. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
    The system displays a dialog asking for confirmation of the change to the existing template.

11. Click the *Yes* button.
    The system saves the new parameter to the template and closes the *Save As* dialog.

12. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.4.2.2 DELETING AN L2CAP PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab.
   The dialog displays the most recently selected Parameter Template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the *Set Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.4.3 L2CAP Parameter Templates

3.5.4.3.1 ADDING AN L2CAP PARAMETER TEMPLATE

This procedure adds a Parameter Template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *L2CAP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the *Initial Connections* list.

4. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

5. Enter the Channel ID.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

6. Enter the Connection Handle.
   This is the L2CAP address.

7. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

8. Select the Carries (PSM).
   Select the protocol that L2CAP traverses to from the list.

9. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 9 until all desired parameters are added.

10. Click the Save icon at the top of the dialog to display the *Save As* dialog.

11. Enter a name for the new template and click *Ok*.
    The system saves the template and closes the *Save As* dialog.

12. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.4.3.2 DELETING AN L2CAP PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab
   The dialog displays the most recently selected Parameter Template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete button at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.5.4.4 L2CAP Missing Decode Information

FTS4BT usually determines the protocol carried in an L2CAP payload by monitoring previous traffic. However, when this fails to occur, the Missing Decoding Information Detected dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- the capture session started after transmission of the vital information
- the analyzer incorrectly received a frame with the traversal information
- the communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the L2CAP payload of this frame (and other frames with the same LT_ADDR and CID that originate from the same side) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

Most often, the first L2CAP session in a connection is for SDP. If the data you are looking at seems to be in the first connection, selecting SDP in the dialog may yield useful results.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.5.4.5 L2CAP Override Decode Information

The Set *Subsequent Decoder Parameters* dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect
2. Select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Then choose the protocol the selected item carries from the drop-down list, and click *OK*.
5. Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.5.5 RFCOMM Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame, then the decode for the response may be incomplete. The **Set Initial Decoder Parameters** dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in Parameter Templates for later use.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

The Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each *Bluetooth*® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The RFCOMM Set Initial Decoder Parameters dialog requires the following user inputs to complete a parameter:

- Stream
  This identifies the role of the device initiating the frame (master or slave)

- Server Channel
  The channel number 0 through 78
- DLCI
  This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server
- Data Source Number
  When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- Carries (UUID)
  Select from the list to apply the Universal Unique Identifier (UUID) of the application layer that RFCOMM traverses to from the following:
  - OBEX
  - SPP
  - encap asyncPPP
  - Headset
  - FAX
  - Hands Free
  - SIM Access
  - VCP
  - UDI
  - -Raw Data-

3.5.5.1 Selecting and Applying an RFCOMM Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *RFCOMM* tab
   The dialog displays the content of the most recently selected template in the *Initial Connections* list at the top of the tab. If the template displayed is the desired Connection Set , then skip to step 4. If it is not, then continue with step 3.
3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exits the *Set Initial Decoder Parameters* dialog.

3.5.5.2 RFCOMM Parameters

3.5.5.2.1 ADDING AN RFCOMM PARAMETER

This procedure adds one or more parameters to an existing template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *RFCOMM* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template , then click the Open File icon and select the desired template from the Popup list.

3. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

4. Enter the Server Channel.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

5. Enter the DLCI.
   This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server.

6. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

7. Select the Carries (UUID).
   Select the application layer that RFCOMM traverses to from the list to apply the Universal Unique Identifier for the necessary application layer.

8. Click the Add button.
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 8 until all desired parameters are added.

9. Click the Save icon at the top of the dialog to display the *Save As* dialog.

10. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
    The system displays a dialog asking for confirmation of the change to the existing template.

11. Click the *Yes* button.
    The system saves the new parameter to the template and closes the *Save As* dialog.

12. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.5.2.2 DELETING AN RFCOMM PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *RFCOMM* tab.
   The dialog displays the most recently selected template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the S*et Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.5.3 RFCOMM Parameter Templates

3.5.5.3.1 ADDING AN RFCOMM PARAMETER TEMPLATE

This procedure adds a template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *RFCOMM* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the *Initial Connections* list.

4. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

5. Enter the Server Channel.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

6. Enter the DLCI.
   This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server.

7. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

8. Select the Carries (UUID).
   Select the application layer that RFCOMM traverses to from the list to apply the Universal Unique Identifier for the necessary application layer.

9. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 9 until all desired parameters are added.

10. Click the Save icon at the top of the dialog to display the *Save As* dialog.

11. Enter a name for the new template and click *Ok*.
    The system saves the template and closes the *Save As* dialog.

12. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.5.3.2 DELETING AN RFCOMM PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *RFCOMM* tab
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete icon at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.5.5.3.3 RFCOMM MISSING DECODE INFORMATION

FTS4BT usually determines the protocol carried in an RFCOMM payload by monitoring previous traffic. However, when this fails to occur, the Missing Decoding Information Detected dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- The capture session started after transmission of the vital information
- The analyzer incorrectly received a frame with the traversal information
- The communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the RFCOMM payload of this frame (and other frames with the same channel) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.5.5.4 RFCOMM Override Decode Information

3.5.5.4.1 RFCOMM OVERRIDE DECODE INFORMATION

The Set *Subsequent Decoder Parameters* dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect, and select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
2. Select the rule you wish to modify from the list of rules.
3. Choose the protocol the selected item carries from the drop-down list, and click *OK*.
4. Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.5.6 USB Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in templates for later use.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

The USB Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each USB network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. The USB Set Initial Decoder Parameters dialog requires the following user inputs to complete a parameter:

- Function Address (Range: 1-127)
  This is the decimal address of the USB port that connects the device to the computer.
- End Point Address (Range: 1-15)
  This is the decimal address of the operation within the device.

- USB Carrying
  Select from the list to apply the USB application

3.5.6.1 Selecting and Applying a USB Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab
   The dialog displays the content of the most recently selected template in the *Initial Connections* list at the top of the tab. If the template displayed is the desired template, then skip step 3 and go to step 4. If it is not, then continue with step 3.
3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exit the *Set Initial Decoder Parameters* dialog.

3.5.6.2 USB Parameters

3.5.6.2.1 ADDING A USB PARAMETER

This procedure adds one or more parameters to an existing template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *USB* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template, then click the Open File icon and select the desired template from the Popup list.

3. Enter the Function Address (Range: 1-127)
   This is the decimal address of the USB port that connects the device to the computer.

4. Enter the End Point Address (Range: 1-15)
   This is the decimal address of the operation within the device.

5. Select the USB Application from the list of applications.

6. Click the Add button
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 6 until all desired parameters are added.

7. Click the Save icon at the top of the dialog to display the *Save As* dialog.

8. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.

9. Click the *Yes* button.
   The system saves the new parameter to the template and closes the *Save As* dialog.

10. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.6.2.2 DELETING A USB PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab.
   The dialog displays the most recently selected template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the S*et Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.6.3 USB Parameter Templates

3.5.6.3.1 ADDING A USB PARAMETER TEMPLATE

This procedure adds a template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *USB* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the *Initial Connections* list.

4. Enter the Function Address (Range: 1-127).
   This is the decimal address of the USB port that connects the device to the computer.

5. Enter the End Point Address (Range: 1-15).
   This is the decimal address of the operation within the device.

6. Select the USB Application from the USB Carrying drop-down list.

7. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 7 until all desired parameters are added.

8. Click the Save icon at the top of the dialog to display the *Save As* dialog.

9. Enter a name for the new template and click *Ok*.
   The system saves the template and closes the *Save As* dialog.

10. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.5.6.3.2 DELETING A USB PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete icon at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.5.6.4 USB Missing Decode Information

The system usually determines the protocol carried in an USB payload by monitoring previous traffic. However, when this fails to occur, the *Missing Decoding Information Detected* dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- the capture session started after transmission of the vital information
- the analyzer incorrectly received a frame with the traversal information
- the communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the USB payload of this frame (and other frames with the same address) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.5.6.5 USB Override Decode Information

The Set *Subsequent Decoder Parameters* is a selection from the Options menu on the Frame Displays dialog. This option allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter :

1. Select the frame where the change should take effect.
2. Select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Choose the protocol the selected item carries from the drop-down list, and click *OK*.
5. Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.5.7 Decoder Parameter Templates

3.5.7.1 Adding a New or Saving an Existing Template

A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

1. Click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Save As dialog.
2. Enter a name for the new template and click Ok.

The system saves the template and closes the Save As dialog.

3. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the template and close the dialog.

Save Changes to a Template

This procedure saves changes to parameters in an existing template.

1. After making changes to parameter settings in a user defined template, click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Save As dialog.
2. Ensure that the name of the template is listed in the Save As text box and click Ok.

The system displays a dialog asking for confirmation of the change to the existing template.

3. Click the Yes button.

The system saves the parameter changes to the template and closes the Save As dialog.

4. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the template and close the dialog.

3.5.7.2 Deleting a Template

1. After opening the *Set Initial Decoder Parameters* dialog click the Delete button at the top of the dialog.

   The system displays the Delete dialog with a list of saved templates.

2. Select (click on and highlight) the template marked for deletion and click the Delete button on the Delete dialog.

   The system removes the selected template from the list of saved templates.

3. Click the Ok button on the Delete dialog to complete the deletion process and close the Delete dialog.
4. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the deletion and close the dialog. Protocol Stacks

3.6 Protocol Stack Wizard

The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.

To start the wizard:

1. Choose *Protocol Stack* from the *Options* menu on the Control window or click the Protocol Stack icon  on the Frame Display.
2. Select a protocol stack from the list, and click Finish. Click for information on how the analyzer auto-traverses the protocol stack.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating a Custom Stack.

1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the *Remove Selected Item From List* button becomes active.

2. Click the Remove button to remove the stack from the list. You cannot remove stacks provided with the analyzer. If you remove a custom stack, you need to define it again in order to get it back.

If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing for more information.

You cannot select a stack or change an existing one for a capture file loaded into the Capture File Viewer (the Capture File Viewer is used only for viewing capture files and cannot capture data). Protocol Stack changes can only be made from a live session.

Note for BCSP:

If you are using the BCSP protocol stack, you must connect the analyzer to the circuit such that the data on the DTE line comes from the host, and data on the DCE line comes from the controller. Click here

Note for Modbus RTU:

If you are using the Modbus RTU protocol stack, you must select either Modbus RTU Master or Modbus RTU Slave depending on where the analyzer taps into the circuit. Click here for more information.

Note for Modbus TCP:

If you are using Modbus TCP over Ethernet, you need to set up a node database giving the IP addresses for the Master and Slave devices. Click here for more information.

Note for Data Highway Plus (DH+):

There are special hardware and software configuration instructions for setting up the DL3000 DHM device used to tap into the Data Highway Plus network. Click here for more information.

Note for IEC 870-5-101:

You need to give the decoder information on the sizes of some fields and whether or not other fields are present. There are all system configurable options and therefore the decoder has no way of knowing this information from the data. Click here for more information.

Note for DeviceNet

You need to install the DeviceNet card before beginning data capture. Then you need to setup the device in the Hardware Settings window, and optionally select any capture filters.

DeviceNet Card Installation Instructions

DeviceNet Device Setup

DeviceNet Capture Filters

3.7 Information Screen

The second screen of the Protocol Stack Wizard gives information to help you decide if you need to define a custom stack or if a pre-defined stack has what you need.

3.7.1 How the Analyzer Auto-traverses the Protocol Stack

In the course of doing service discovery, devices ask for and receive a Protocol Descriptor List defining which protocol stacks the device supports. It also includes information on which PSM to use in L2CAP, or the channel number for RFCOMM, or the port number for TCP or UDP. The description below talks about how the analyzer auto-traverses from L2CAP using a dynamically assigned PSM, but the principle is the same for RFCOMM channel numbers and TCP/UDP port numbers.

The analyzer looks for SDP Service Attribute Responses or Service Search Attribute Responses carrying protocol descriptor lists. If the analyzer sees L2CAP listed with a PSM, it stores the PSM and the UUID for the next protocol in the list.

After the SDP session is over, the analyzer looks at the PSM in the L2CAP Connect frames that follow. If the PSM matches one the analyzer has stored, the analyzer stores the source channel ID and destination channel ID, and associates those channel IDs with the PSM and UUID for the next protocol. Thereafter, when the analyzer sees L2CAP frames using those channel IDs, it can look them up in its table and know what the next protocol is.

In order for the analyzer to be able to auto-traverse using a dynamically assigned PSM, it has to have seen the SDP session giving the Protocol Descriptor Lists, and the subsequent L2CAP connection using the PSM and identifying the source and channel IDs. If the analyzer misses any of this process, it is not able to auto-traverse. It stops decoding at the L2CAP layer.

For L2CAP frames carrying a known PSM (0x0001 for SDP, for example, or 0x0003 for RFCOMM), the analyzer looks for Connect frames and stores the PSM along with the associated source and destination channel IDs. In this case the analyzer does not need to see the SDP process, but does need to see the L2CAP connection process, giving the source and destination channel IDs.

3.8 Creating and Removing a Custom Stack

To create a custom stack:

1. Choose *Protocol Stack* from the *Options* menu on the Control window or click the Protocol Stack icon  on the Frame Display.
2. Select *Build Your Own* from the list and click *Next*.
3. The system displays an information screen that may help you decide if you need to define your own custom stack. Defining a custom stack means that the analyzer uses the stack for every frame. Frames that do not conform to the stack are decoded incorrectly. Click *Next* to continue.

Select Protocols

1. Select a protocol from the list on the left.
2. Click the right arrow button to move it to the Protocol Decode Stack box on the right, or double-click the protocol to move it to the right.
3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.
4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the *Move Up* and *Move Down* buttons until the protocol is in the correct position.
5. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.

Auto-traversal (Have the analyzer Determine Higher Layers)

If you need to define just a few layers of the protocol stack, and the remaining layers can be determined based on the lower layers:

1. Click the All additional stack layers can be determined automatically button.
2. If your protocol stack is complete and there are no additional layers, click the There are no additional stack layers button.
3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

To save your stack:

1. Click the Add To Predefined List button.
2. Give the stack a name, and click Add.

In the future, the stack appears in the Protocol Stack List on the first screen of the Protocol Stack wizard.

Remove a Stack

To remove the stack:

1. Select it in the first screen and click *Remove Selected Item From List*.
2. If you remove the stack, you must to recreate it if you need to use it again.

Note:

If you do not save your custom stack, it does appear in the predefined list, but applies to the frames in the current session. However, it is discarded at the end of the session.

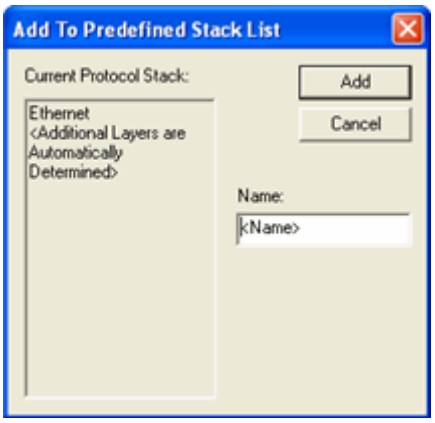
3.9 Saving User Defined Stacks

You can create protocol stacks for one time use that disappear at the end of the session. If you want to use the stack again in a subsequent session, then you need to recreate it.

However, if you save the stack, then it is available every time you start the analyzer, until you delete it.

The *Add To Predefined Stack List* dialog allows the user to save a custom stack for future use.

1. After creating a custom stack using the Protocol Stack Wizard, click the *Add To Predefined List* button on the last screen of the wizard.



Your newly defined stack appears in the *Current Protocol Stack* pane on the left.

2. Simply enter a name for the stack and click *Add*.

The name of the stack now appears as a selection in the *Select a Protocol Stack* dialog.

3.10 Reframing

If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. You can also use Reframe to frame unframed data. The original capture file is not altered during this process.

Note: You cannot reframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To reframe your data, load your capture file, select a protocol stack, and then select Reframe from the File menu on the Control window. Reframe is only available if the frame recognizer used to capture the data is different from the current frame recognizer.

In addition to choosing to Reframe, you can also be prompted to Reframe by the Protocol Stack Wizard.

1. Load your capture file by choosing Open from the File menu on the Control window, and select the file to load.
2. Select the protocol stack by choosing Protocol Stack from the Options menu on the Control window, select the desired stack and click Finish.

3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the Protocol Stack Wizard asks you if you want to reframe your data. Choose Yes.
4. The analyzer adds frame markers to your data, puts the framed data into a new file, and opens the new file. The original capture file is not altered.

See Unframing for instructions on removing framing from data.

3.11 Unframing

This function removes start-of-frame and end-of-frame markers from your data. The original capture file is not altered during this process.

You cannot unframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To manually unframe your data, select Unframe from the File menu on the Control window. Unframe is only available if a protocol stack was used to capture the data and there is currently no protocol stack selected.

In addition to choosing to Unframe, you can also be prompted to Unframe by the Protocol Stack Wizard.

1. Load your capture file. To do this, choose Open from the File menu on the Control window, and select the file to load.
2. Remove the protocol stack. To do this, choose Protocol Stack from the Options menu on the Control window, select None from the list, and click Finish.
3. The Protocol Stack Wizard asks you if you want to unframe your data and put it into a new file. Choose Yes.
4. The system removes the frame markers from your data, puts the unframed data into a new file, and opens the new file. The original capture file is not altered.

See Reframing for instructions on framing unframed data.

3.12 Providing Context For Decoding When Frame Information Is Missing

There may be times when you need to provide information to the analyzer because the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame indicating the command.

The analyzer provides a way for you to supply the context for any frame, provided the decoder supports it. (The decoder writer has to include support for this feature in the decoder, so not all decoders support it. Note that not all decoders require this feature.)

If the decoder supports user-provided context, three items are active on the Options menu of the Control Window, Frame Display and Protocol Navigator windows. These items are *Set Initial Decoder Parameters*, *Automatically Request Missing Decoding Information*, and *Set Subsequent Decoder Parameters*. (These items are not present if no decoder is loaded that supports this feature.)

Set Initial Decoder Parameters is used to provide required information to decoders that is not context dependent but instead tends to be system options for the protocol.

Choose Set Initial Decoder Parameters in order to provide initial context to the analyzer for a decoder. A dialog appears that shows the data for which you can provide information.

If you need to change this information for a particular frame :

1. Right-click on the frame in the Frame Display window
2. Choose Provide <context name>.

Alternatively, you can choose Set Subsequent Decoder Parameter from the Options menu.

3. This brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check *Automatically Request Missing Decoding Information*.
5. When unchecked, the analyzer doesn't bother you with dialogs asking for frame information that you don't have. In this situation, the analyzer decodes each frame until it cannot go further and then simply stop decoding.

4 Capturing Data

4.1 Capturing Data

Note: Data Capture is not available in Viewer mode.

1. Click the Start Capture icon  to begin capturing to a file. This icon is located on the Control  , Event Display  , and Frame Display  windows.
2. Files are placed in My Capture Files by default and have a .cfa extension. Choose Directories from the Options menu on the Control window to change the default file location.
3. Watch the status bar on the Control window to monitor how full the file is. When the file is full, it begins to *wrap*, which means the oldest data will be overwritten by new data.
4. Click the Stop icon  to temporarily stop data capture. Click the Start Capture icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured date remains in the file.
5. To clear captured data, click the Clear icon  .
    - If you select Clear after selecting Stop, a dialog appears asking whether you want to save the data.
        - You can click Save File and enter a file name when prompted .
        - If you choose Do Not Save, all data will be cleared.
        - If you choose Cancel, the dialog closes with no changes.
    - If you select the Clear icon while a capture is occurring:
        - The capture stops.
        - A dialog appears asking if you want to save the capture
        - You can select Yes and save the capture or select No and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
        - If you choose Cancel, the dialog closes with no changes.

To change the size of the capture file, choose System Settings from the Options menu on the Control window.

4.2 USB HCI Internal Software Tap Data Source Dialog

The USB HCI Internal Software Tap Data Source Dialog allows the user to select which *Bluetooth*® device to sniff and to initiate and terminate the sniffing process.

This dialog has a list control containing the *Bluetooth* Devices connected to your system. If the *Show Connected Only* checkbox is unchecked then all USB devices that have ever been connected to your system are listed.

1. Select the device you wish to sniff.
2. Click on the Start Sniffing button. You must click on the *Start Capture*  icon on the Control window to capture data. For more details see USB HCI Sniffing.
3. Click the *Refresh List* button if you have connected or disconnected a device while this dialog is open to update the list.

5 Analyzing Byte Level Data

5.1 Event Display

To open this window

Click the Event Display icon  on the Control window toolbar.

The Event Display window provides detailed information about every captured event. Events include data bytes, data related information such as start-of-frame and end-of-frame flags, and the analyzer information, such as when the Data Capture Was Paused. Data bytes are displayed in hex on the left side of the window, with the corresponding ASCII character on the right.

Click on an event to find out more about it. The three status lines at the bottom of the window are updated with information such as the time the event occurred (for data bytes, the time the byte was captured), the value of the byte in Hex, Decimal, Octal, and Binary, any errors associated with the byte, and more.

Events with errors are shown in red to make them easy to spot.

When capturing data live, the analyzer continually updates the Event Display as data is captured. Make sure the Lock icon  is displayed on the toolbar to prevent the display from updating (Clicking on the icon again will unlock the display). While locked, you can review your data, run searches, determine delta time intervals between bytes, and check CRCs. To resume updating the display, click the Lock icon again.

You can have more than one Event Display open at a time. Click the Duplicate View icon  to create a second, independent Event Display window. You can lock one copy of the Event Display and analyze your data, while the second Event Display updates as new data is captured.

5.2 The Event Display Toolbar

 Home – Brings the Control window to the front.

 Open File - Opens a capture file.

 Start Capture - Begins data capture to disk.

 Stop Capture - Closes a capture file and stops data capture to disk.

 Save - Prompts user for a file name. If the user supplies a name, a .cfa file is saved.

Clear- Discards the temporary file and clears the display.

Lock - In the Lock state, the window is locked so you can review a portion of data. Data capture continues in the background. Clicking on the Lock icon unlocks the window.

Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon locks the window.

Duplicate View - Creates a second Event Display window identical to the first.

Frame Display - (framed data only) Brings up a Frame Display, with the frame of the currently selected bytes highlighted.

Focus Protocol Navigator - (framed data only) Brings up the Protocol Navigator window, with the currently selected frame highlighted.

Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.

Add/Modify Bookmark - Add a new or modify an existing bookmark.

Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Find - Search for errors, string patterns, special events and more.

Go To - Opens the Go To dialog, where you can specify which event number to go to.

CRC - Change the algorithm and seed value used to calculate CRCs. To calculate a CRC, select a byte range, and the CRC appears in the status lines at the bottom of the Event Display.

Mixed Sides - (Serial data only) By default, the analyzer shows data with the DTE side above the DCE side. This is called DTE over DCE format. DTE data has a white background and DCE data has a gray background. The analyzer can also

display data in mixed side format. In this format, the analyzer does not separate DTE data from DCE data but shows all data on the same line as it comes in. DTE data is still shown with a white background and DCE data with a gray background so that you can distinguish between the two. The benefit of using this format is that more data fits onto one screen.

Character Only - The analyzer shows both the number (hex, binary, etc.) data and the character (ASCII, EBCDIC or BAUDOT) data on the same screen. If you do not wish to see the hex characters, click on the Character Only button. Click again to go back to both number and character mode.

Number Only - Controls whether the analyzer displays data in both character and number format, or just number format. Click once to show only numeric values, and again to show both character and numeric values.

All Events - Controls whether the analyzer shows all events in the window, or only data bytes. Events include control signal changes and framing information.

Timestamping Options – Brings up the timestamping options window which has options for customizing the display and capture of timestamps.

5.3 Opening Multiple Event Display Windows

Click the Duplicate View icon  from the Event Display toolbar to open a second Event Display window.

You can open as many Event Display windows as you like. Each Event Display is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

The Event Display windows are numbered in the title bar. If you have multiple Event Displays open, click on the Event Display icon  on the Control window toolbar to show a list of all the Event Displays currently open. Select a window from the list to bring it to the front.

5.4 Calculating CRCs or FCSs

The cyclic redundancy check (CRC) is a function on the Event Display window used to produce a checksum. The frame check sequence (FCS) are the extra checksum characters added to a frame to detect errors.

1. Open the Event Display  window.
2. Click and drag to select the data you want to generate a CRC for.

3. Click on the CRC icon  .
4. In the CRC dialog box, click on the down arrow to show the list of choices for CRC algorithms. Choose an algorithm to use. Choose CRC 32 (Ethernet). Choose CRC 32 (Ethernet) for Ethernet data or the appropriate CRC type for serial data.
5. Enter a seed value in hexadecimal if desired.
6. Click OK to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC using the algorithm you selected is calculated automatically.

"CRC!" in Ethernet data

Ethernet network cards do not normally send the CRC with the frame to the upper layers of the system. The hardware on the card checks that the CRC is correct and then throws it away. FTS marks the place where the CRC would be in the data with "CRC!". When viewing Ethernet capture files made with other programs, the CRC may or may not be included, depending on the specifications of the capturing software/hardware.

Reversed CRCs on the Event Display with Ethernet data

The CRC calculated in the Event Display window is reversed from the CRC shown in the data. CRCs are calculated in network data order from Most Significant Byte (MSB) to Least Significant Byte (LSB). The Ethernet specification says to send data in host data order (LSB to MSB). Therefore the CRC as captured in the data is the reverse of the CRC as calculated.

Example: If the CRC in the data is shown as 00 01 02 03, the Event Display calculated the CRC and show it in the status lines as 03 02 01 00. This is correct.

Calculating CRC for interwoven data

FTS calculates the CRC for either side of the interwoven data. Which side it calculates is determined by the first byte selected. If the first byte is from one side, then FTS calculates the CRC for just the bytes on that side. If the first byte is from the other side, then FTS calculates the CRC for just the bytes on that side.

Incorrect results with CRC16 for serial data

If you are calculating CRCs using the CRC16 algorithm and the CRCs do not match what you know they should be, try CRC16rev. What hardware often calls CRC16 is what software calls CRC16rev.

5.5 Calculating Delta Times and Data Rates

1. Click on the Event Display icon  on the Control window to open the Event Display window.
2. Use the mouse to select the data you want to calculate a delta time and rate for.
3. The Event Display window displays the delta time and the data rate in the status lines at the bottom of the window.

5.6 Switching Between Live Update and Review Mode

The Event Display and Frame Display windows can update to display new data during live capture, or be frozen to allow data analysis. By default, the Event Display continually updates with new data, and the Frame Display is locked.

1. Make sure the Lock icon  is active so the display is locked and unable to scroll.
2. Click the Unlock  icon again to resume live update.

The analyzer continues to capture data in the background while the display is locked. Upon resuming live update, the display updates with the latest data.

You can have more than one Event Display or Frame Display window open at a time. Click the Duplicate View icon  to open additional Event or Frame Display windows. The Lock/Resume function is independent on each window. This means that you can have two Event Display windows open simultaneously, and one window can be locked while the other continues to update.

5.7 Data Formats and Symbols

5.7.1 Switching Between Viewing All Events and Viewing Data Events

By default, the analyzer on the Event Display dialog shows all *events*.

This includes:

- Data bytes
- Start-of-frame
- End-of-frame characters
- Data Captured Was Paused.

Click on the Display All Events icon to remove the non-data events. Click again to display all events.

See List of All Event Symbols for a list of all the special events shown in the analyzer and what they mean.

5.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the *radix* used to display data.

1. Go to the View menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.
2. Right-click on the "Hex" header label and choose a different radix.

If you want to see only the numerical values, click on the Numbers Only icon  on the Event Display toolbar.

5.7.3 Switching Between ASCII, EBCDIC, and Baudot

On the Event Display window, the analyzer displays data in ASCII by default. There are several ways to change the character set used to display data.

1. Go to the View menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. Right-click on the "ASCII" header label and choose a different character set.

If you want to see only characters, click on the Characters Only icon  on the Event Display toolbar.

5.7.4 Viewing Only ASCII (or EBCDIC or Baudot)

On the Event Display toolbar you can choose to view data in ASCII, EBCDIC, or Baudot format only.

1. Click on the Characters Only icon  on the Event Display toolbar.

To add the numerical values back to the display:

1. Click the Characters Only icon again.

5.7.5 Viewing Only Hex (Or Decimal or Octal or Binary)

On the Event Display toolbar you can choose to view data as numeric only.

1. Click on the Numbers Only icon  on the Event Display toolbar.

To display the characters back to the display:

1. Click the Number Only icon again.

5.7.6 Selecting Mixed Channel/Sides

If you want to get more data on the Event Display window, you can switch to mixed sides mode. This mode puts all the data together on the same line. Data from one side is shown on a white background and data from the other is shown on a gray background.

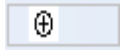
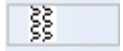
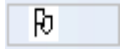
1. Click once on the Mixed Sides icon  to put the display in mixed sides mode.
2. Click again to return to side over side mode.
3. You can right click on the labels in the center of the data display window to change between mixed and side over side modes.
4. Choose Display Sides Together to go to Mixed Sides Mode or Display Sides Separately to go to side over side mode.

5.7.7 List of All Event Symbols

By default, the Event Display shows all *events*, which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button  . Click again to display all events.

Click on a symbol, and the analyzer displays the symbol name and sometimes additional information in the status lines at the bottom of the Event Display window. For example, clicking on a control signal change symbol displays which signal(s) changed.

In addition to data bytes, the events shown are (in alphabetical order):

	Abort
	Broken Frame - The frame did not end when the analyzer expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.
	Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.
	Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.
	Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
	Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
	Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.
	End of Frame - Marks the end of a frame.
	Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.
	Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
	Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.

5.7.8 Font Size

The font size can be changed on several windows. Changing the font size on one window does not affect the font size on any other window.

To change the font size:

1. Click on *Options,* and select Change the Font Size.
2. Choose a font size from the list.
3. Click OK.

6 Analyzing Protocol Decodes

6.1 Frame Display Window

6.1.1 Frame Display Window

To open this window

Click the Frame Display icon  on the Control window toolbar, or select Frame Display from the Window menu.

Frame Display Panes

The Frame Display window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame. The image below gives the name of each pane. Click on the links below the image to learn more about each pane.

- Summary Pane

  The Summary Pane displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.

- Decode Pane

  The Detail Pane displays a detailed decode of the highlighted frame. Fields selected in the Decode pane have the appropriate bit(s) or byte(s) selected in the Radix, Binary, Character and Event panes.

- Radix Pane

  The Radix Pane displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.

- Binary Pane

  The Binary Pane displays a binary representation of the logical data bytes.

- Character Pane

  The Character Pane displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.

- Event Pane

  The Event Pane displays the physical data bytes in the frame, as received on the network.

By default, all panes except the Event pane are displayed when the Frame Display is first opened.

Protocol Tabs

The Frame Display adds a tab to the top of the Summary Pane for every protocol found in the in the data. You can click on these tabs to filter on the protocol. Select the Unfiltered tab to display all protocols. The Unfiltered tab is automatically selected when multiple protocols are being *filtered-in* using other filtering methods.

Comparing Frames

If you need to compare frames, you can open additional Frame Display windows by clicking on the Duplicate View icon  . You can have as many Frame Display windows open at a time as you wish.

6.1.2 Frame Display Toolbar

The buttons that appear in the Frame Display window vary according to the particular configuration of the analyzer.

 Home – Brings the Control window to the front.

 Open File - Opens a capture file.

 I/O Settings - Opens the I/O Settings dialog.

 Start Capture - Begins data capture to a user designated file.

 Stop Capture - Closes a capture file and stops data capture to disk.

 Save - Save the currently selected bytes or the entire buffer to file.

 Clear- Discards the temporary file and clears the display.

 Event Display – Brings the Event Display window to the front.

 Protocol Navigator – Brings the Protocol Navigator window to the front.

 Statistics - Brings the Statistics window to the front. This icon does not display in this location when running the analyzer in Air Sniffer. See Packet Error Rate Statistics below.

 Signal Display - Opens the Signal Display. This icon does not display when running the analyzer in Air Sniffer.


Breakout Box - Opens the Breakout Box dialog.


Duplicate View - Creates a second Frame Display window identical to the first.


Apply/Modify Display Filters - Opens the Display Filter dialog.


Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.


Find - Search for errors, string patterns, special events and more.


Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.


Add/Modify Bookmark - Add a new or modify an existing bookmark.


Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.


Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data


Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.


Packet Timeline – Opens the Packet Timeline display.


Extract Data - Opens the Extract Data dialog.


Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.


Audio Extraction - Opens the Audio Extraction dialog.


Pie Chart - This icon displays a chart that displays the number of frames with and without errors.

Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.

The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.

Show Default Panes - Returns the panes to their default settings.

Show Only Summary Pane - Displays only the Summary pane.

Toggle Expanded Decode Pane - Makes the Decode pane taller and the Summary pane narrower.

Toggle Display Freeze - Prevents the display from updating.

Go To Frame - Opens the Go To dialog, where you can specify which event number to go to.

First Frame - Moves to the first frame in the buffer.

Previous Frame - Moves to the previous frame in the buffer.

Next Frame - Moves to the next frame in the buffer.

Last Frame - Moves to the last frame in the buffer.

Note that if the frames are sorted in other than ascending frame number order, the order of the frames in the buffer is the sorted order. Therefore the last frame in the buffer may not have the last frame number.

Summary drop-down box

Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to the analyzer, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol. When a FBLEA predefined Named Filter (like Nulls and Polls) is selected, the Summary drop-down is disabled.

Text with Protocol Stack

To the right of the Summary Layer box is some text giving the protocol stack currently in use.

6.1.3 Frame Display Status Bar

The Frame Display Status bar appears at the bottom of the Frame Display. It contains the following information:

- Total Frames: The total number of frames in the capture buffer or capture file in real-time
- Frames Filtered In: The total number of frames displayed in the filtered results from user applied filters in real-time
- Frame #s Selected: Displays the frame number or numbers of selected (highlighted) frames, and the total number of selected frames in parentheses

6.1.4 Hiding and Revealing Protocol Layers in the Frame Display

Hiding protocol layers refers to the ability to prevent a layer from being displayed on the Decode pane. Hidden layers remain hidden for every frame where the layer is present, and can be revealed again at any time. You can hide as many layers as you wish.

Note: Hiding from the Frame Display affects only the data shown in the Frame Display and not any information in any other window.

There are two ways to hide a layer.

1. Right-click on the layer in the Decode pane, and choose Hide [protocol name] Layer In All Frames.
2. Click the Set Protocol Filtering button on the Summary pane toolbar. In the Protocols to Hide box on the right, check the protocol layer(s) you want hidden. Click OK when finished.

To reveal a hidden protocol layer:

1. Right-click anywhere in the Decode pane
2. Choose Show [protocol name] Layer from the right-click menu, or click the Set Protocol Filtering button and un-check the layer or layers you want revealed.

6.1.5 Physical vs. Logical Byte Display

The Event Display window and Event Pane in the Frame Display window show the *physical bytes*. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the *logical data*, or the

d

By default, frames are sorted in ascending numerical sequence by frame number. Click on a column header in the Summary pane to sort the frames by that column. For example, to sort the frames by size, click on the *Frame Size* column header.

An embossed triangle next to the header name indicates which column the frames are sorted by. The direction of the triangle indicates whether the frames are in ascending or descending order, with up being ascending.

Note that it may take some time to sort large numbers of frames.

6.1.7 Synchronizing the Event and Frame Displays

The Frame Display is synchronized with the Event Display. Click on a frame in the Frame Display and the corresponding bytes is highlighted in the Event Display. Each Frame Display has its own Event Display.

As an example, here's what happens if the following sequence of events occurs.

1. Click on the Frame Display icon  in Control window toolbar to open the Frame Display.
2. Click on the Duplicate View icon  to create Frame Display #2.
3. Click on Event Display icon  in Frame Display #2. Event Display #2 opens. This Event Display is labeled #2, even though there is no original Event Display, to indicate that it is synchronized with Frame Display #2.
4. Click on a frame in Frame Display #2. The corresponding bytes are highlighted in Event Display #2.
5. Click on a frame in the original Frame Display. Event Display #2 does not change.

6.1.8 Working With Multiple Frame Displays

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset or two filtered subsets against each other.

- To create a second Frame Display, click the *Duplicate View* icon  on the Frame Display toolbar.

This creates another Frame Display window. You can have as many Frame Displays open as you wish. Each Frame Display is given a number in the title bar to distinguish it from the others.

- To navigate between multiple Frame Displays, click on the *Frame Display* icon  in the Control window toolbar.

A drop-down list appears, listing all the currently open Frame Displays.

- Select the one you want from the list and it comes to the front.

Note: When you create a filter in one Frame Display, that filter does not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

6.1.9 Working With Panes

When the Frame Display first opens, all panes are displayed except the Event pane. The panes include:

- To view all the panes, select *Show All Panes* from the *View* menu.
- The *Toggle Expand Decode Pane* icon  makes the decode pane longer to view lengthy decodes better.
- The *Show Default Panes* icon  returns the Frame Display to its default settings.
- The *Show only Summary Pane* icon  displays on the Summary Pane.

1. To close a pane, right-click on the pane and select *Hide This Pane* from the pop-up menu, or de-select *Show [Pane Name]* from the *View* menu.
2. To open a pane, right-click on the any pane and highlight *Show Hidden Panes* from the pop-up menu and select the pane from the fly-out menu, or select *Show [Pane Name]* from the *View* menu.
3. To resize a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to resize the pane.

6.1.10 The Panes in the Frame Display

6.1.10.1 Summary Pane

The Summary pane  displays a one-line summary of every frame in a capture buffer or file, including frame number, timestamp, length and basic protocol information. The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

On a two-channel circuit, the background color of the one-line summary indicates whether the frame came from the DTE or the DCE device. Frames with a white background come from the DTE device, frames with a gray background come from the DCE device.

The Summary pane in FTS4USB displays a one-line summary of every transaction in a capture buffer or file. Whenever there is a transaction it is shown on a single line instead of showing the separate messages that comprise the transaction. The Msg column in that case says "Transaction".

Each message in a transaction contains a packet identifier (PID). All of the PIDs in a transaction are shown in the transaction line.

All IN transactions (i.e. transactions that contain an IN token message) are shown with a purple background. All other transactions and all non-transactions are shown with a white background. IN transactions have special coloring because that is the only place where the primary data flow is from a device to the Host.

The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

Frame numbers in red indicate errors, either physical (byte-level) or frame errors. If the error is a frame error in the displayed protocol layer, the bytes where the error occurred is displayed in red. The Decode Pane gives precise information as to the type of error and where it occurred.

The Summary pane is synchronized with the other panes in this window. Click on a frame in the Summary pane, and the bytes for that frame is highlighted in the Event pane while the Decode pane displays the full decode for that frame. Any other panes which are being viewed are updated accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame is highlighted in the other panes.

Use the navigation icons, keyboard or mouse to move through the frames. The icons  and  move you to the first and last frames in the buffer, respectively. Use the Go To icon  to move to a specific frame number.

6.1.10.2 Customizing Fields in the Summary Pane

You can modify the Summary Pane in Frame Display.

Changing Column Widths

To change the width of a column:

1. Place the cursor over the right column divider until the cursor changes to a solid double arrow.
2. Click and drag the divider to the desired width.
3. To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column:

1. Drag the right divider of the column all the way to the left.
2. The cursor changes to a split double arrow when a hidden column is present.
3. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.
4. The Frame Size, Timestamp, and Delta columns can be hidden by right-clicking on the header and selecting *Show Frame Size Column, Show Timestamp Column,* or *Show Delta Column*. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column :

1. Click and hold on the column header
2. Drag the mouse over the header row.
3. A small white triangle indicates where the column is moved to.
4. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations, their default widths, and show any hidden columns

1. Right-click on any column header and choose *Restore Default Column Widths*, or select *Restore Default Column Widths* from the *Format* menu.

6.1.10.3 Frame Symbols in the Summary Pane

A green dot means the frame was decoded successfully, and the protocol listed in the Summary Layer drop-down box exists in the frame. No dot means the frame was decoded successfully, but the protocol listed in the Summary Layer drop-down box does not exist in the frame.

A green circle means the frame was not fully decoded. There are several reasons why this might happen.

One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for the analyzer to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If the analyzer is busy capturing data, frame compilation may fall behind. When the analyzer catches up, the green circle changes to either a green dot or no dot.

Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has

changed. If the analyzer does not capture the first frame with the complete header, it cannot decode subsequent frames with partial header information.

A magenta triangle indicates that a bookmark is associated with this frame. Any comments associated with the bookmark appear in the column next to the bookmark symbol.

6.1.10.4 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary Pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary Pane using the **Filtering Results** dialog.

Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:

1. Right-click on a value in the Summary Pane. For example, the "S" for Slave under Role
2. On the drop-down list select **Filter in "Name = Value"**

Note: The "Name" and "Value" change depending on the layer.

The Filtering Results dialog appears.

3. Enter a name for the Filter.
4. Select OK.

A new protocol tab with the Filter Name you just created appears in the Summary Pane. The new tab displays data specific to the layer you selected.

6.1.10.5 Decode Pane

The Decode pane (aka detail pane)  is a post-process display that provides a detailed decode of each frame transaction (sometimes referred to as a frame). The decode is presented in a layered format that can be expanded and collapsed depending on which layer or layers you are most interested in. Click on the plus sign to expand a layer. The plus sign changes to a minus sign. Click on the minus sign to collapse a layer. Select Show All or Show Layers from the Format menu to expand or collapse all the layers. Layers retain their expanded or collapsed state between frames.

Protocol layers can be hidden, preventing them from being displayed on the Decode pane. Right-click on any protocol layer and choose Hide [protocol name] from the right-click menu.

In a USB transaction, all messages that comprise the transaction are shown together in the detail pane. The color coding that is applied to layers when the detail pane displays a single

message is applied to both layers and messages when the detail pane displays a transaction. To keep the distinction between layers and messages clear, each header of each message in the detail pane ends with the word “Message” or “Messages”. The latter is used because data and handshake messages are shown as a single color-coded entry

Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the Event, Radix, Binary and Character Panes. The colors are not assigned to a protocol, but are assigned to the layer.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

Click the Toggle Expand Decode Pane icon  to make the Decode pane taller. This allows for more of a lengthy decode to be viewed without needing to scroll.

6.1.10.6 Radix or Hexadecimal Pane

The Radix pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the Format menu, or by right-clicking on the pane and choosing Hexadecimal, Decimal or Octal.

Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

6.1.10.7 Character Pane

The Character pane represents the logical bytes in the frame in ASCII, EBCDIC or Baudot. The character set can be changed from the Format menu, or by right-clicking on the pane and choosing the appropriate character set.

Because the Character pane displays the logical bytes rather than the physical bytes, the data in the Character pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

6.1.10.8 Binary Pane

The Binary pane displays the logical bytes in the frame in binary. This pane is synchronized with the Decode pane so that individual bit fields can be highlighted.

Because the Binary pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

6.1.10.9 Event Pane

The Event pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the All Events icon  .

Displaying all events means that special events, such as Start of Frame/End of Frame and any signal change events, are displayed as special symbols within the data.

The status lines at the bottom of the pane give the same information as the status lines in the Event Display window. This includes physical data errors, control signal changes (if appropriate), and timestamps.

Because the Event pane displays the physical bytes rather than the logical bytes, the data in the Event pane may be different from that in the Radix, Binary and Character panes. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

6.1.11 Protocol Layer Colors

6.1.11.1 Data Byte Color Notation

The color of the data in the panes specifies which layer of the protocol stack the data is from. All data from the first layer is bright blue, the data from the second layer is green, the third layer is pink, etc. The protocol name for each layer in the Decode pane is in the same color. Note that the colors refer to the layer, not to a specific protocol. In some situations, a protocol may be in two different colors in two different frames, depending on where it is in the stack. You can change the default colors for each layer.

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the Radix, Character, Binary and Event panes mean there is a physical error associated with the byte.

6.1.11.2 Red Frame Numbers and Bytes

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the Radix, Character, Binary and Event panes mean there is a physical error associated with the byte.

6.1.11.3 Changing Protocol Layer Colors

You can differentiate different protocol layers in the Decode, Event, Radix, Binary and Character panes.

1. Choose *Select Colors* from the Options menu to change the colors used
2. To change a color, click on the arrow next to each layer and select a new color.

6.1.12 Protocol Filtering from the Frame Display

6.1.12.1 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the *Summary* pane, and the second lets you filter on any protocol discovered on the network so far.

6.1.12.2 Filtering On the Summary Layer Protocol

To filter on the protocol in the *Summary* in the Frame Display window pane:

1. Select the tab of the desired protocol, or open the *Summary Layer* combo box.
2. Select the desired protocol.
3. To filter on a different layer, just select another tab, or change the layer selection in the combo box.

6.1.12.3 Quick Filtering on a Protocol Layer

1. To filter on any protocol layer, open either the *Frame Display* or *Protocol Navigator* window.
2. On the *Frame Display* window, click the starred *Quick Filtering* icon  or select "Quick Filtering" from the *Filter* menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

The box on the left is **Protocols To Filter In**.

- When you select the checkbox for a protocol in the **Protocols to Filter In**, the Summary Pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A Quick Filter tab then appears on the Frame Display labeled Quick Filter. Changing the filter definition on the Quick Filter dialog changes the filter applied on the Quick Filter tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**.

- When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the Decode, Binary, Radix, and Character Panes. The frames containing that type data will still appear in the Summary Pane, but not in the Decode, Binary, Radix, and Character Panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs.

- When you select the checkbox for the Name Filters, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With **FBLEA**, the Configured BT Low energy devices and Exclude NULLSs and POLLs are default named filters.

1. Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.
2. Then click *OK*.

6.1.12.4 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

1. Open the *Frame Display*  window.
2. Click the starred *Quick Filter* icon  or select "Quick Filtering" from the *Filter* menu
3. Check the box for *All Frames With Errors* in the "Protocols to filter in" pane, and click *OK.*
4. The system creates a tab on the *Frame Display* labeled *Quick Filter* that displays the results of the *All Frames With Errors* filter.

6.1.12.5 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary Pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary Pane using the **Filtering Results** dialog.

Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:

1. Right-click on a value in the Summary Pane. For example, the "S" for Slave under Role
2. On the drop-down list select **Filter in "Name = Value"**

Note: The "Name" and "Value" change depending on the layer.

The Filtering Results dialog appears.

3. Enter a name for the Filter.
4. Select OK.

A new protocol tab with the Filter Name you just created appears in the Summary Pane. The new tab displays data specific to the layer you selected.

6.2 Protocol Navigator Window

6.2.1 Protocol Navigator

The *Protocol Navigator* displays the decode for more than one frame at a time, and has several features for controlling which frames and/or parts of frames are displayed. The main part of the window displays the decode for multiple frames. When you first open the window, every protocol layer of every frame is collapsed. By expanding the protocols, the *Protocol Navigator* displays the equivalent of the *Decode* pane on the *Frame Display*, with the added convenience of displaying multiple frame decodes in one place.

Click the *Protocol Navigator* icon  to display the *Protocol Navigator*.

There are three methods for controlling the display in the *Protocol Navigator;* expanding/collapsing protocols, filtering, and hiding.

6.2.2 Protocol Navigator Toolbar

The buttons that appear in the Protocol Navigator window vary according to the particular configuration of the analyzer.


Home – Brings the Control window to the front.


Open File - Opens a capture file.


I/O Settings - Opens the I/O Settings dialog.


Start Capture - Begins data capture to a user designated file.


Stop Capture - Closes a capture file and stops data capture to disk.


Save - Save the currently selected bytes or the entire buffer to file.


Clear- Discards the temporary file and clears the display.


Event Display – Brings the Event Display window to the front.


Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.


Breakout Box - Opens the Breakout Box dialog.


Duplicate View - Creates a second Frame Display window identical to the first.


Apply/Modify Display Filters - Opens the Display Filter dialog.


Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.


Find - Search for errors, string patterns, special events and more.


Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.


Add/Modify Bookmark - Add a new or modify an existing bookmark.


Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data

Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.

Packet Timeline – Opens the Packet Timeline display.

Extract Data - Opens the Extract Data dialog.

Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.

Audio Extraction - Opens the Audio Extraction dialog.

The following icons all change how the panes are arranged on Protocol Navigator. Additional layouts are listed in the View menu.

First Frame - Moves to the first frame in the buffer.

Previous Frame - Moves to the previous frame in the buffer.

Next Frame - Moves to the next frame in the buffer.

Last Frame - Moves to the last frame in the buffer.

6.2.3 Protocol Navigator Status Bar

The Protocol Navigator Status bar appears at the bottom of the Protocol Navigator. It contains the following information:

- Total Frames: The total number of frames in the capture buffer or capture file in real-time
- Frames Filtered In: The total number of frames displayed in the filtered results from user applied filters in real-time
- Frame #s Selected: Displays the frame number(s) of selected (highlighted) frames, and the total number of selected frames in parentheses.

6.2.4 The Difference Between Filtering and Hiding

You can filter on one or more protocol layers. The filter is inclusive, which means that filtering on a protocol means that only frames that contain that protocol are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several. (Filtering on the Protocol Navigator window is display filtering only.)

Hiding means that the selected layer is not displayed in the window, even though it may be present in the frame. This allows you to zoom in on a particular layer by hiding every layer but the one of interest.

An example using the IP stack may help to illustrate the difference. Assume that you only want to see frames that have TCP in them. You create a filter on TCP. The results displayed in the Protocol Navigator (or Frame Display) window have only those frames that carry TCP.

Now you're ready to look at the TCP decode in your frames. You don't care about what has happened at the IP layer or any other layer, so you hide everything but TCP. The window shows just the TCP decode for each frame. With those two steps, you've eliminated looking at any frame that doesn't have TCP in it, and you've narrowed down what you see to just the TCP decode.

6.2.5 Hiding and Revealing Protocol Layers in the Protocol Navigator

Hiding means that the selected protocol is not displayed in the window, even though it may be present in the frame. This allows you to zoom in on a particular protocol by hiding every protocol but the one of interest. This is especially effective when all the layers are expanded.

Note: Hiding affects only the view in the Protocol Navigator  and not the view in any other window.

There are two ways to hide a protocol in the Protocol Navigator window :

1. Right-click on the protocol and choose Hide [Protocol Layer Name].
2. There are three panes on the left side of the window. The middle box is the Hidden From View pane. Check the boxes next to the protocols you want to hide.

To reveal a hidden protocol:

1. Right-click anywhere in the main window
2. Select the protocol you want to show from the right-click menu, or un-check the box next to the protocol name in the Hidden From View pane.

When one or more layers are hidden, a note appears at the top of the Protocol Navigator saying, "Some layers are hidden. Right-click to see." This warns you that some layers are hidden.

Two special options are *All But the Last Layer* and *All Special Information Nodes*.

- *All But the Last Layer* hides all layers in each frame except for the last one, regardless of which protocol is present in the last layer.

- *All Special Information Nodes* hides the information line present in some protocol decoders.

6.2.6 Filtering on a Protocol Layer

You can filter on one or more protocol layers. The filter is inclusive which means only frames matching the filter you select are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several.

On the left side of the Protocol Navigator window are three panes. The top pane is the Frames Filtered In pane. In the pane is a list of all the protocols seen so far on the circuit.

1. Check the boxes next to the names of the protocols you want to filter in.

The data on the right side of the screen matches the filtering selected.

Three additional filters available are:

- All Frames With Bookmarks - filters in all frames with a *bookmark* associated with them.
- All Frames With Errors - filters in all frames with errors.
- All Special Information Nodes - filters in all *special information nodes* .

6.2.7 Filtering on all Frames with Errors from the Protocol Navigator

To filter on all frames with errors :

1. Open the *Protocol Navigator*  window.
2. Check the *All Frames With Errors* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

6.2.8 Expanding and Collapsing Protocol Layers

You can expand any collapsed frame or protocol layer by clicking on the plus sign next to the frame number or protocol name. Expanding a protocol layer in one frame expands it for all frames.

1. To collapse a layer or frame, click on the minus sign next to the frame number or protocol name.

What do you want to see?

Everything	Choose Show All from the Format menu.
Everything for just one frame	Click the plus sign next to the frame you want to see. Then click the plus signs next to each protocol name to see the full decode.
Just the stack for each	Choose Show Frames AND Show Protocol Stack When Frame Is Completely Collapsed from the Format menu. This makes

frame the display look similar to the following:

Frame 1: Len=104 Ethernet -> IP -> TCP

Frame 2: Len=98 Ethernet -> IP -> TCP -> NBSS

Just the stack without summary information Choose Show Layers AND un-check Show Summary Decode When Detailed Decode Is Collapsed on the Format menu. This makes the display look similar to the following:

Frame 1: Len=104
+ Ethernet:
+ IPv4:
+ TCP:

Frame 2: Len=98
+ Ethernet:
+ IPv4:
+ TCP:
+ NBSS:

Just the stack including summary information Choose Show Layers AND Show Summary Decode When Detailed Decode Is Collapsed from the Format menu. This makes the display look similar to the following:

Frame 1: Len=104
+ Ethernet: --- Dest. Address: BROADCAST Source Address: XYZ etc.
+ IPv4: --- Protocol: TCP Length: 80 etc.
+ TCP: --- Source Port: 9988 Destination Port: NETBIOS etc.

Frame 2: Len=98
+ Ethernet: --- Dest. Address: etc.
+ IPv4: --- Protocol: TCP Length: 56 etc.
+ TCP: --- Source Port: NETBIOS Destination Port: 9988 etc.
+ NBSS: --- Length: 23 Fragment: Entire Message

The full decode for a protocol layer Click on the plus sign next to the protocol name. This expands just that protocol in every frame.

The decode for just Choose Collapse All Nodes AND Show Last Layer When

the last layer in each frame	Frame is Completely Collapsed from the Tree menu.

7 Analyzing Control Signal Changes

7.1 Viewing Signal Changes in Real-time

7.1.1 Breakout Box Window

The Breakout Box window provides a real-time graphical view of control signals. The window is customizable based on the control signals you wish to view and your preference of indicators (+/-, 1/0, T/F, arrows, and simulated LEDs). Also included are counters showing the number of times a control signal has changed.

To open this window :

1. Click the Breakout Box icon  on the Control window.

Name - Pin 1, 2, 3, and 4

FTS4USB monitors four control signals.

Digital inputs provide a means for users to insert events into the data stream. There are four digital inputs that can be enabled individually. Whenever an enabled input changes state it will issue an event and be tagged with a timestamp of when the input was interpreted by the analyzer. Digital inputs can not exceed a rate of 30 MHz. Digital inputs that occur faster than that are not guaranteed to be interpreted correctly by the analyzer. Also, only one digital input event may occur per active packet. All other digital input events can only be handled after the packet has completed. Digital inputs, although guaranteed to have the correct timestamp given the previous conditions, have the possibility of being presented out of order because they are provided randomly by the user and have no direct correlation to the bus. It is important to note that the digital inputs are susceptible to cross-talk if they are not being actively driven. A situation like this could occur if a digital input has been enabled, but has not been tied to a signal. Any other nearby signal (i.e., other digital inputs or outputs) could cause the input to activate. It is recommended that all undriven digital inputs be disabled or tied to ground.

FTS monitors six *RS-232* control signals. They are listed below :

DTE Signals

- *DTR - Data Terminal Ready*
- *RTS - Request to Send DCE Signals*

- *CTS - Clear to Send*
- *DSR - Data Set Ready*
- *CD - Carrier Detect*
- *RI - Ring Indicator* (see the special note on capturing Ring Indicator changes)

When monitoring a synchronous circuit, FTS also displays clock signals at the bottom of the window. These signals rotates when clock is present, and has an X over them if clock is not detected.

When using the SST interface cards for analyzing DeviceNet traffic, the following signals are displayed:

- BP - Bus Power
- OL - Online
- BW - Bus warning, either the receive or transmit error counter (incremented and decremented at various rates according to the Bosch CAN specification) has reached 128.
- BO - Bus off, either the receive or transmit error counter has reached 255 and the CAN chip has been forced offline.
- RO - Receive buffer overrun, one or more messages has been lost due to a full queue in the on-card firmware.
- ML - Message lost, one or more messages has been lost due to a slow interrupt response by the on-card firmware.
- ER - Error, one or more CAN error frames has been detected.

Note: The messages received by NetDecoder are still correct when the ER flag shows some activity, as re-transmission is automatic and only error-free frames result in a receive interrupt from the CAN controller.

7.1.2 The Breakout Box Toolbar

Home - brings the Control window to the front.

Reset - resets the Breakout Box window.

Lock - Locks the display. Clicking on the Lock icon, unlocks the window.

Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon, locks the window.

Options - Brings up the Breakout Box Options window. This window allows you to change the window refresh rate and choose which control signals to display. Type topic text here.

7.1.3 Reading the Breakout Box Window

The Breakout Box display is divided into three main parts. The first part (to the far left of the screen) shows the abbreviated name of the control signal being monitored. These names can be changed in the I/O Settings window  by clicking the *Names* button.

The second part shows the control signal counters. The counters show how many times each control signal has changed state. This is useful in situations when signals may be changing state too rapidly to be displayed graphically.

Below the counters are the clock indicators. The indicators rotate when clock is present, and have an X over them when clock is not detected.

The third part of the Breakout Box shows the current states of the control signals. The indicators show the state that the control signal is currently in, and the line graph displays the state of the signal over time. A single line means that the signal is logically off, while a double line means that the signal is logically on. A half-height "tick" means that a signal has gone through one full transition (from off to on to off, or vice versa) since the analyzer last updated the screen.

To change the indicators, hide the clock signals, or change the rate at which the analyzer updates the window, click on the Options icon  .

7.1.4 Selecting Breakout Box Options

To access options

1. Click the Options icon  on the Breakout Box toolbar or choose *Breakout Box options* under the *Options* menu.

Display Signal

This box shows which control signals FTS monitors.

- A check mark next to a control signal name indicates that the breakout box displays the status of that control signal.
- To prevent FTS from displaying the status of a signal, un-check the box next to it.

Display Clocks

Click to place a check mark in this box if you want the Breakout Box window to display the clock indicators. Un-check to hide the clock indicators. (This option is only shown when in synchronous or isochronous mode.)

Window Refresh Rate

The refresh rate is the rate at which FTS updates the window.

- By default, FTS refreshes the display once every 1,000 milliseconds (one second.)
- To change the rate, highlight the number in the box and enter a new number. See item 7 in Performance Notes for information on how Window Refresh Rate can affect performance.

Indicators

You can choose what type of indicators FTS uses.

- The default indicators are a green "+" sign to show a logically high state, and a red "-" sign to show a logically low state.
- To change the indicators, click on the down arrow and choose a pair of indicators from the list.
- As a reminder, FTS gives the definition of the indicators in the top part of the Breakout Box window.

8 Viewing Historical Signal Changes

8.1 Signal Display Window

The Signal Display window provides a graphical view of control signal transitions that you can manipulate. You can zoom in to view the state of control signals for a range of events, or zoom out to view control signal changes over the course of an entire capture session.

To open this window

Click the Signal Display icon  on the Control window toolbar, or choose Signal Display from the Window menu.

The Signal Display window does not provide a real-time view of control signal changes. It is intended to be used as a post-process review screen. Use the Breakout Box window to view real-time control signal changes. Note that if you bring up the Signal Display window while data is being captured, the window shows you the state of the control signals at the time the window was opened. This is called a "snapshot" because it is a picture of the buffer at the time the Signal Display was opened. To update the display to reflect the current state of the buffer, use the New Snapshot icon  .

When you open Signal Display IN FTS4USB you will see Pin Codes 1, 2, 3, and 4. These correspond to the four Digital Input Enabling Options explained in USB I/O Settings.

When using the SST interface cards for analyzing DeviceNet traffic, the following signals are displayed:

- BP - Bus Power
- OL - Online

- BW - Bus warning, either the receive or transmit error counter (incremented and decremented at various rates according to the Bosch CAN specification) has reached 128.
- BO - Bus off, either the receive or transmit error counter has reached 255 and the CAN chip has been forced offline.
- RO - Receive buffer overrun, one or more messages has been lost due to a full queue in the on-card firmware.
- ML - Message lost, one or more messages has been lost due to a slow interrupt response by the on-card firmware.
- ER - Error, one or more CAN error frames has been detected.

Note: The messages received by NetDecoder are still correct when the ER flag shows some activity, as re-transmission is automatic and only error-free frames result in a receive interrupt from the CAN controller.

8.2 Signal Display Toolbar

Home - brings the Control window to the front.

Take New Snapshot - Takes a new "picture" of the capture buffer. If you are capturing data when you open the Signal Display window, the window shows only the state of the control signals that were in the buffer when the window was opened. Click this button to update the window with the contents of the current buffer.

Zoom In - "Zooms in" on the signal display. How much you zoom in is determined by your selection in the Signals menu. You can zoom in by a factor of 2, 4, or 8.

Zoom Out - Reverse of Zoom In.

Zoom to Selection - Zooms to show only the region highlighted on the screen. If the highlighted area contains few events, the Signal Display window may also display additional events in order to fill up the screen.

Display Entire Buffer - Zooms all the way out to display the contents of the entire buffer in the window.

Find - Opens the Find Control Signal change window.

Snap to Nearest Change - Moves the cursor to the nearest signal change whenever you click on the line graphics in the window. Find the line for the control signal whose changes you want to see. Click on that line, and the analyzer moves to the nearest signal change for that control signal. You can

also highlight a range, and the analyzer snaps to the 2 nearest changes on either side of the range.

Timestamping Options - Opens the Timestamping Options window, where you can change the timestamping resolution and how timestamps are displayed.

8.3 Reading the Signal Display

Control signal changes are displayed in a graphical format. On the left side of the screen is a list of the signals currently being displayed, and to the right of each name is a line displaying the state of the signal over time. A single line means that the signal was logically off, while a double line means that the signal was logically on. Dotted lines are used for signals that were not present at the time of capture. For example, if you are monitoring a circuit that does not use CD, that line appears as a dotted line in the control signal display.

The four information lines at the bottom of the window tell you what events are being shown in the window, and where you are in relation to the buffer as a whole.

- The first line tells you what event numbers are in the current snapshot, the total number of events, and the amount of time that passed between the first event in the snapshot and the last event (called Delta).
- The second line gives the same information about the events that are currently visible in the window. Because you can zoom in and out, often the events being shown in the window are not the same as the number of events in the current snapshot.
- The third line gives the same information for the currently selected events. You can highlight a range of events by clicking at any point on the graphical display and dragging the mouse to the left or the right. The third line shows information for the selected range.
- The fourth and last line shows the exact timestamps of the first and last bytes in the currently selected range. Note that this does not tell you the timestamp for the entire snapshot or the events displayed in the window, just the highlighted events.

A single mouse click places the cursor in the window. The analyzer highlights all six signal changes in one color, and uses a different color to specify the control signal line clicked on. You can highlight a range by clicking and dragging the mouse to the right or left. You can also use the arrow keys to move the cursor to the right or left.

The Signal Display window is synchronized with other windows in the analyzer. A range highlighted in the Signal Display window is also highlighted in the Event Display and Frame Display windows.

The Snap to Nearest Change icon  lets you place the cursor on the signal change you want to look at without needing to click on exactly the right spot. Find the line corresponding to the control signal you want to look at. Click on the line, and the analyzer

moves the cursor to the nearest change. If you highlight a range, the analyzer "snaps to" the nearest changes on either side. This feature is active when the Snap To button is pressed, and inactive when the button is not pressed.

Use the Zoom In and Zoom Out buttons to increase and decrease the magnification of the window. The analyzer changes the magnification by a factor of 2, 4 or 8, depending on the option selected in the Signals menu.

If you want to see a range in greater detail, highlight the range you want to view and click on the Zoom to Selection icon  . The analyzer zooms in to show only that range in the window. If the range is small, the analyzer may add additional events to fill up the window.

To view the entire snapshot in the window, click on the Display Entire Buffer icon  .

Note that if you bring up the Signal Display window while data is being captured, the window shows you the state of the control signals at the time the window was opened. To update the display, use the New Snapshot icon  .

8.4 Selecting Signal Display Options

To access Signal Display Options

Click the Signal Display icon  on the Control window toolbar. From the *Options* menu, select Signal Display Options.

To choose which control signals to display in the Signal Display window.

- Click on a box to check or un-check it the control signal name.
- A check mark next to a control signal name means that the signal is displayed.

9 Statistics

9.1 Statistics

Statistics displays vary according product configuration. Select the help topics that apply to the mode you are running.

9.2 Statistics Window

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

To open the Statistics window, click the Statistics icon  on the Control window toolbar, or choose Statistics from the View menu on the Control window.

The Statistics window supplies basic information about the data on the network. When reviewing a capture file, the Statistics window shows a summary of the data in the file.

The analyzer monitors the network and collects statistics all the time, even when data is not actively being captured. Activate the Lock icon  to stop the window from updating.

Click the Unlock icon  again to resume updating. The analyzer continues to monitor network traffic while the Statistics window is locked, so you may see the numbers jump right after updating has resumed, reflecting all the statistics that were gathered while the window was locked.

9.3 Session, Resettable and Capture File Tabs

The Session and Resettable tabs are parts of the Statistics window.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Information about all data collected since the analyzer was started is shown in the Session tab. The Session tab cannot be reset; in this sense, it is like the odometer on a car. The odometer on a car shows you all the miles driven since the car was built, and the Session tab shows you all the data collected since the analyzer was started.

If you think of the Session tab as the odometer, then the Resettable tab is the trip odometer. It can be reset, and allows you to record statistics for a new "trip". In this way you can effectively start a new session without having to restart the analyzer. If the Reset button was pressed during the capture, then the numbers on this tab differs from the numbers on the Session tab.

The Capture File tab shows information on the data that is currently in the capture. If the capture file had become full, the analyzer began to overwrite the oldest data and put new data in its place. This is called "wrapping". If the file wrapped, the numbers on the Capture File tab is smaller than those on the Session tab.

Occasionally some of the statistics read n/a, for Not Available. This happens for various reasons. For example, many of the items on the Capture File tab become not available (n/a) if the buffer becomes full and wraps. When this happens, the analyzer can no longer provide accurate statistics for the data in the file, because some of the data that the statistics are based on has been lost.

9.4 Copying Statistics To The Clipboard

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

To copy the information from an individual table to the clipboard (where it can be pasted into any application),

1. Choose the name of the table from the *Edit* menu.
2. To copy the contents of all the tables, choose *Copy All to Clipboard*.

9.5 Graphs

9.5.1 Statistics Graphs

Open the Statistics window and click on the picture of a graph  on the table header, or choose the graph name from the Graph menu on the Statistics window.

The Frame Sizes Graph window has Session, Resettable and Buffer tabs that correspond to the tabs on the Statistics window. Each tab shows the data that corresponds to the appropriate tab on the Statistics window.

The Frame Sizes Graph window displays the number of frames of each length in either a pie chart or bar graph format. Click the Pie icon  to display a pie chart, and click the Bar icon  to display a bar graph.

For networks with more than one side, the analyzer displays one graph for each side. To view the aggregate of all sides, click the Aggregate icon  .

9.5.2 Printing Graphs

1. Click the Print icon  to print the graph. The analyzer prints exactly what is shown on the window.

9.5.3 Changing the Graph Refresh Rate

The graphs window refreshes once every second.

To change the refresh rate:

1. Click the Options icon  on the *Statistics* window.
2. Enter a new refresh rate in milliseconds in the Time Interval (ms) text box.

9.5.4 Viewing Percentages or Values

On the *Statistics* window you can view data expressed as a percentage.

1. Open the *Statistics* window
2. Select the graph to display.

On the graph window,

3. Click the *Percentages* icon  to view data expressed as a percentage.
4. Click the *Percentages* icon again to view the actual number of items of each type.
5. Click the *Show Data Grid* icon  to view both the number and percentage of the total for each item. The analyzer places a grid in the legend.

9.6 Information on Tables

9.6.1 Statistics Tables

The Statistics Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI

- High Speed UART (HSU)
- USB HCI

The information on the Statistics window is organized into Tables. Fields marked "n/a" are fields for which there is currently no data. This can happen for a variety of reasons. On the buffer tab, fields are n/a when there is no data in the buffer (i.e. no capturing is being done). On the Errors table, some fields may be n/a depending on the statistics supported by your Ethernet card. Some tables are always present, while tables with framing information are present only when capturing framed data.

9.6.2 Frames Per Second Table

The Frames Per Second Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Current The current number of frames per second.

Average The average number of frames per second.

Peak The highest number of frames per second.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

9.6.3 Characters Per Second Table

The Characters/Sec Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Baud The current baud.

Current The current number of characters per second.

Average The average number of characters per second.

Peak The highest number of characters per second.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

9.6.4 Utilization Table

The Utilization Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Current The current number of bits per second divided by the maximum speed of the network, expressed as a percentage.

Average The average number of bits per second divided by the maximum speed of the network, expressed as a percentage.

Peak The highest utilization.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

9.6.5 Data Table

The Data Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

The information in the Data table relates to the amount of data captured by the analyzer. Data information varies depending on the type of data in the capture. When Ethernet data passes through a capture filter, this table displays statistics only for the data kept by FTS, i.e. only the data that passes the filter. The Unfiltered Data table always displays statistics for the entire network, regardless of the state of any capture filter.

Ethernet Data

Frames This includes frames received with and without errors, and frames transmitted by the PC running the analyzer, if the PC is an active node on the network. This field and the Total Frames field in the Unfiltered Data table should be roughly equal, unless a capture filter is active. They are not exactly equal because the counters are updated at different times.

Bytes The total number of bytes.

Events The total number of events captured. Events include data bytes and start-of-frame and end-of-frame markers. For a description of all events and their symbols, see the List of Event Symbols.

Multicast The total number of multicast frames.

Broadcast The total number of broadcast frames.

Serial Data

Frames The total number of frames, if applicable, with a breakdown by DTE and DCE device.

Chars The total number of characters, with a breakdown by DTE and DCE device.

Events The total number of events captured. Events include data bytes, control signal changes, flow control changes, etc. For a description of all events and their symbols, see the List of Event Symbols.

Wireless Data

Frames The total number of frames, if applicable, with a breakdown by device.

Octets The total number of octets, with a breakdown by device.

Events The total number of events captured. Events include data bytes, start and end-of-frame markers, etc. For a description of all events and their symbols, see the List of Event Symbols.

9.6.6 Octets Per Second Table

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Speed	maximum speed of the network expressed in megabits
Current	current number of octets per second
Average	average number of octets per second
Peak	highest number of octets per second

9.6.7 Buffer Information Table

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

These errors do not indicate problems on the network, but rather indicate that FTS was not able to keep up with the amount of incoming data. They usually indicate that a faster PC was needed. See Performance Notes for more information.

Driver Buffer Overflow	The number of times the analyzer lost frames because it could not retrieve them from the driver buffer fast enough.

The remaining three items are for Ethernet data only.

Frames Missed, No Buffer	The number of frames lost because the analyzer driver could not retrieve them from the NDIS buffers before they were overwritten by new, incoming frames.
Receive Overrun	The number of times that frames are lost because NDIS could not retrieve data quickly enough from the buffer on the network card.
Frames Lost	The number of frames lost due to driver buffer overflows.

9.6.8 Errors Table

The Errors Table is found on the Statistics window. The table provides the number of each type of error seen on the network. Error types vary depending on the type of data. When analyzing Ethernet data, not all errors are supported by all NDIS drivers. Errors not supported are marked "n/a".

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- Serial Asynchronous
- High Speed Serial HCI
- High Speed UART (HSU)

To graph, click the bar graph icon  on the Errors table header.

Ethernet Errors

CRC Errors	The number of frames with *CRC* errors. A CRC error occurs when the frame is properly aligned on a byte boundary but does not pass the Cyclic Redundancy Check. The CRC verifies that the data was not corrupted in transit.
Alignment Errors	The number of frames with alignment errors. Alignment errors occur when the frame does not end on a byte boundary. For example, frames may not be 95 and 2 bits long. It must be either 92 or 93 bytes.
Rx Frames With Errors	The total number of frames received with errors (includes frames with CRC and Alignment errors).
Tx Frames With Errors	The total number of frames transmitted with errors.
Tx One Collision	The number of frames successfully transmitted after detecting one collision.
Tx More Collisions	The number of frames successfully transmitted after detecting multiple collisions.
Tx Deferred	The number of frames successfully transmitted after transmission has been deferred at least once.
Tx Max Collisions	The number of frames not transmitted due to excessive collisions.

Tx Underrun	The number of frames not transmitted due to underrun errors.
Tx Heartbeat Failure	The number of frames transmitted without detecting the collision detection heartbeat.
Tx Times CRS Lost	The number of times carrier sense was lost during frame transmission.
Tx Late Collisions	The number of collisions detected after the normal window.

Serial Asynchronous Errors

Overrun	The number of overrun errors broken down by DTE and DCE device.
Parity	The number of parity errors broken down by DTE and DCE device. If you have a large number of parity errors, check your I/O Settings for accuracy.
Framing	The number of framing errors broken down by DTE and DCE device. If you have a large number of framing errors, check your I/O Settings for accuracy.

Serial Synchronous Errors

USART Overrun	The number of overrun errors broken down by DTE and DCE device.
Parity	The number of parity errors broken down by DTE and DCE device. If you have a large number of parity errors, check your I/O Settings for accuracy.
Framing	The number of framing errors broken down by DTE and DCE device. If you have a large number of framing errors, check your I/O Settings for accuracy.
CRC	The number of *CRC* errors detected. CRC counting is done only when monitoring HDLC or SDLC data.
Underrun	The number of underrun errors broken down by DTE and DCE device. Underrun errors occur when FTS is unable to transmit data quickly enough. These errors only occur when transmitting in sync mode.

High Speed Serial HCI and High Speed UART (HSU) Errors

Parity	The number of parity errors broken down by device.
Framing	The number of framing errors broken down by device.

ZigBee Errors

FCS The number of FCS errors detected.

9.7 Packet Error Rate Statistics (PER Stats)

9.7.1 Packet Error Rate

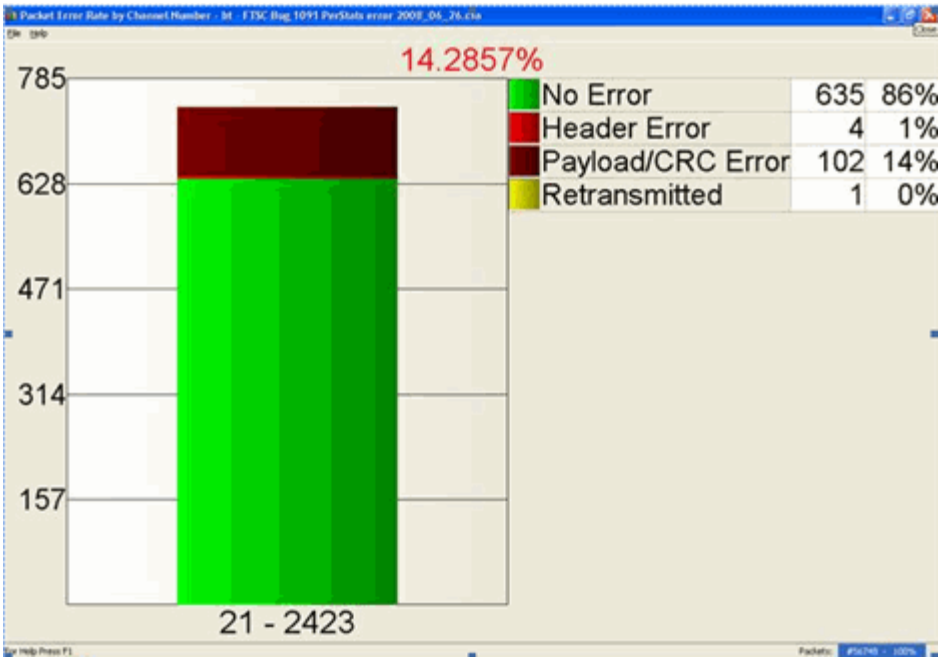
The Packet Error Rate Stats Plug-in provides a dynamic graphical representation of the Packet Error Rate for each channel.

The Packet Error Rate window displays a graph for each channel numbered 0 through 78 and a pie chart summarizing the total of all channels.

Expand individual graphs by clicking on the desired one. The expanded graph displays the percentage of errors (Packet + Header if any) in red text at the top of the graph, and a legend with color-coded statistics in percentages and actual values, by parameter, in tabular format, to the right of the graph. Click the expanded graph to return to the Packet Error Rate window.

Each graph and table display the following parameters:

- Total number of packets (determined by reading the scale to the left of the graph)
- The number of packets with no errors, color-coded green
- The number of packets that have header errors, color-coded red
- The number of payload errors, color-coded dark red
- The number of re-transmits, color-coded yellow



Click on the error rate percentages in the graphic above to learn more about the Packet Error Rate percentages.

The Reset button is available only during live capture and not when viewing a capture file. It resets the Packet Error Rate Stats display to all zeros, and starts displaying data from that point on.

Unavailable channels, due to Adaptive Frequency Hopping (AFH), display the "not" symbol. However, the graph may contain data against transmissions made prior to becoming unavailable.

Data Analysis

Packet Error Rate Stats assist in detecting bad communication connections. When a high percentage of re-transmits, and/or header/payload errors occur, careful analysis of the statistics indicate whether the two devices under test are experiencing trouble communicating, or the packet sniffer is having difficulty listening.

Generally, if the statistics display either a large number of re-transmits with few errors or an equal number of errors and re-transmits, then the two devices are not communicating clearly. However, if the statistics display a large number of errors and a small number of re-transmits, then the packet sniffer is not receiving the transmissions clearly.

Note: The total percentage of the Packet Error Rate can be < or > 100%. The discrepancy can be attributed to the rounding methodology. For example, look at the following numeric values and the resulting rounded values:

- 635/742 = 0.8557 -> 86%
- 4/742 = 0.0053 -> 1%
- 102/742 = 0.1374 -> 14%
- 1/742 = 0.0013 -> 0%

Note that a count of 1 is shown as 0% because the actual percentage rate is 0.0013. 1 is an actual value, but rounding gives it a percentage of 0. Also note that 4 is rounded to 1% even though the actual percentage is 0.0053.

What you can have, then, is a total percentage of 101% and still be correct. You could also have a total percentage of 99% and be correct.

The total percentage of the Packet Error Rate can be < or > 100%. The discrepancy can be attributed to the rounding methodology. For example, look at the following numeric values and the resulting rounded values:

- 635/742 = 0.8557 -> 86%
- 4/742 = 0.0053 -> 1%

- 102/742 = 0.1374 -> 14%
- 1/742 = 0.0013 -> 0%

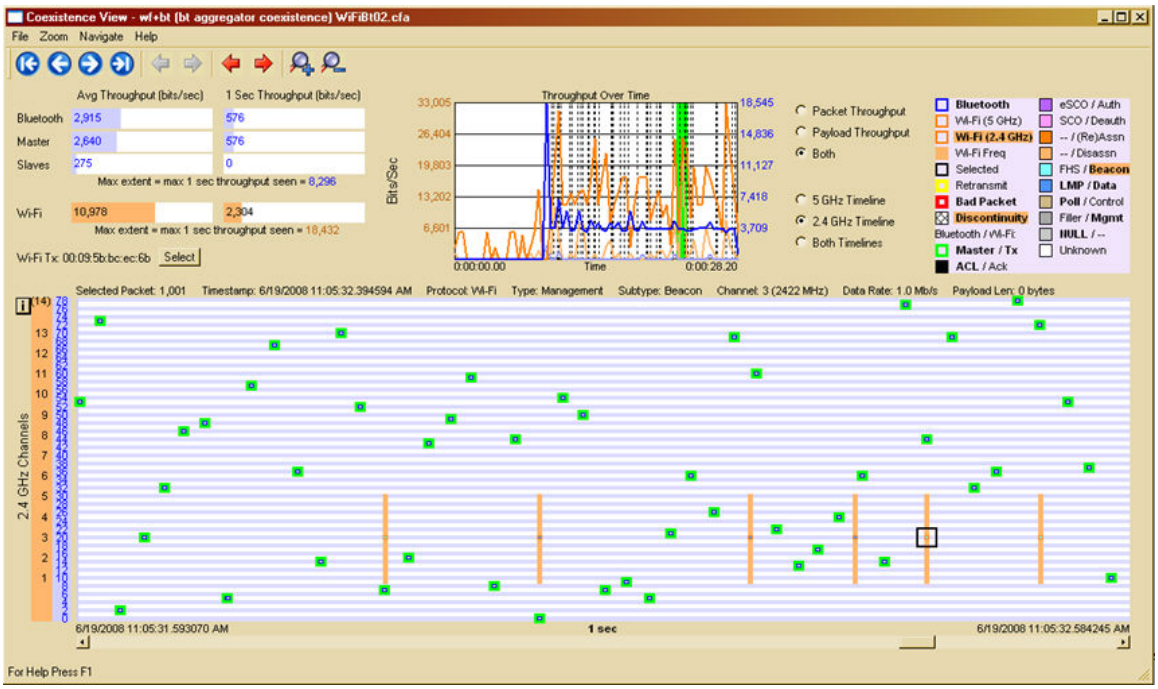
Note that a count of 1 is shown as 0% because the actual percentage rate is 0.0013. 1 is an actual value, but rounding gives it a percentage of 0. Also note that 4 is rounded to 1% even though the actual percentage is 0.0053.

What you can have, then, is a total percentage 0f 99% or 101% and still be correct.

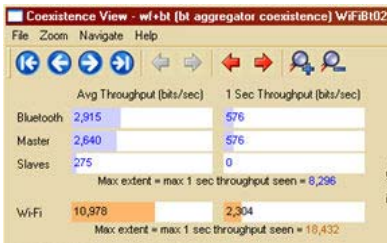
10 Coexistence View

10.1 Coexistence View Introduction

The Coexistence View displays both the Bluetooth® and the Wi-Fi channels frequencies in one view. You access the Coexistence View by selecting the icon from the Control Window, Frame Display, and Protocol Navigator toolbars or from the View menus.



10.1.1 Average Throughput/1 Second Throughput



Bluetooth: Average Throughput/ 1 Second Throughput
This chart displays:

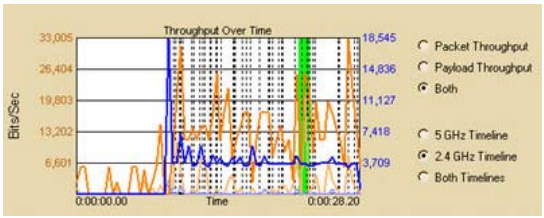
- Average Throughput in bits/seconds for all Bluetooth packets, Bluetooth Master packets, and Bluetooth Slave packets.
- One (1) Second Throughput in bits/seconds for all Bluetooth packets, Bluetooth Master packets, and Bluetooth Slave packets.
    - Average Throughput = total packet/payload size divided by the duration of the entire session

- 1 second Throughput = packet/payload size during the most recent one second of the session

Wi-Fi: Average Throughput/ 1 Second Throughput
This chart displays the

- Average Throughput in bits/second and One (1) Second Throughput in bits/seconds for Wi-Fi.
  - Average Throughput = total packet/payload size divided by the duration of the entire session
  - 1 second Throughput = packet/payload size during the most recent one second of the session

10.1.2 Throughput Graph



The Throughput Graph displays throughput over time.

- Wi-Fi packet throughput is displayed as an orange line with corresponding orange numeric values on the left.
- Bluetooth packet throughput is displayed as a blue line with corresponding blue numeric values on the right.
- When you click anywhere in the graph, the timeline moves to the corresponding position in time.
- To keep the timeline and the throughput graph manageable, big jumps in packet timestamps are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the timestamp goes forward more than 2 seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph.
- You can show Packet Throughput, Payload Throughput, or both depending on which radio button to the right of the graph you select. The Avg Throughput and 1 Sec Throughput indicators are also affected.
- Payload Throughput is always less than Packet Throughput because a packet is never all payload.
- The green area in the throughput graph is called the viewport. Its position and width correspond to the beginning timestamp and duration of the timeline.

10.1.3 Legend

This legend identifies the color coding found in the timeline. When you select a packet in the timeline, its attributes are highlighted in the legend. A bold entry in the legend indicates that such a packet has been seen during the current session.

A Bluetooth packet has a blue outline, and a Wi-Fi packet has an orange outline.

10.1.4 Coexistence View Wi-Fi Tx Address

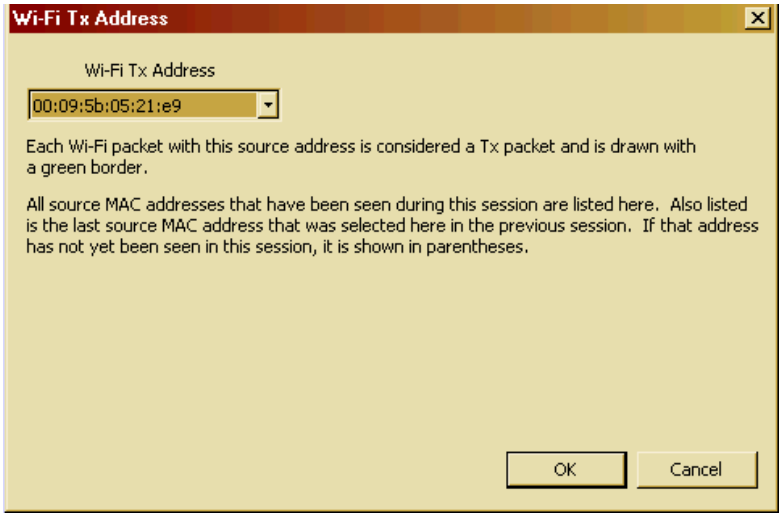
The Wi-Fi Tx Address displays a selected source address that you choose.

The specific address is highlighted with a green border.

To select a specific address:

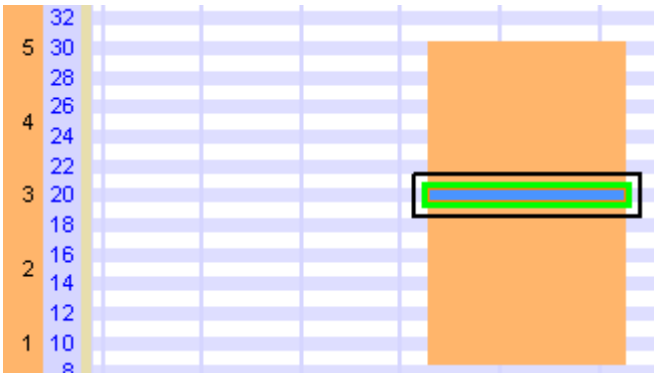
1. Click the **Select** button.

The Wi-Fi Tx Address dialog appears.



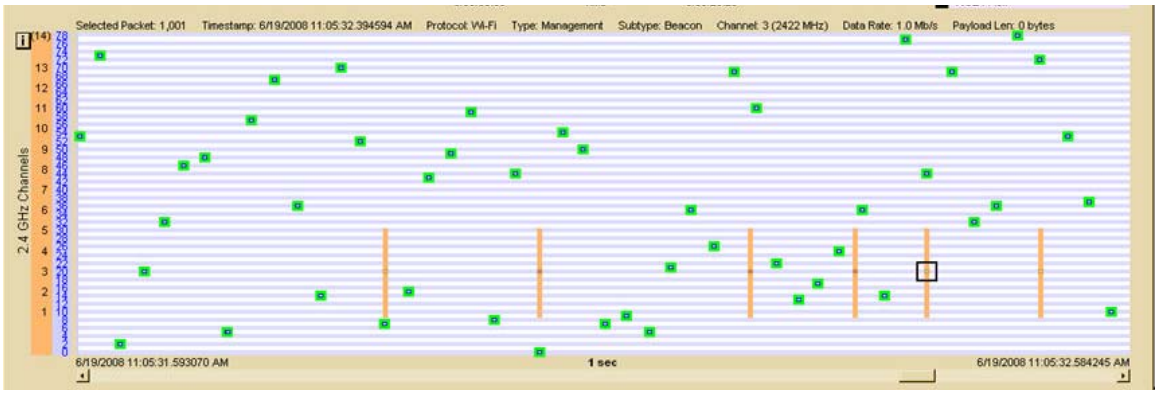
2. Select an address from the **drop-down list**.
3. Select **OK**.

The selected address appears with a green border around it.



4. Click on the links below to learn more about the specific *Bluetooth* and the Wi-Fi channel frequencies.

10.1.5 Timeline



- The timeline shows Bluetooth and Wi-Fi packets within a specific period of time.
- The horizontal lines in the timeline are rows that correspond to Bluetooth and Wi-Fi frequencies.
- The vertical blue lines are Bluetooth slot markers for reference.
- The timeline displays Bluetooth and 2.4 GHz Wi-Fi packets together in the 2.4 GHz range when you select the 2.4 GHz Timeline radio button.
- The timeline displays 5 GHz Wi-Fi packets in the 5 GHz range when you select the 5 GHz Timeline radio button.

- The timeline displays Bluetooth/Wi-Fi packets in the 2.4 GHz range and Wi-Fi packets in the 5 GHz range when you select the Both Timelines radio button.
- The timeline duration is displayed underneath the timeline.
- Placing the mouse pointer on a packet in the timeline displays information about that packet in an information box.
- You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- On the 2.4 GHz Timeline, there are 79 Bluetooth and 14 Wi-Fi channels. Channel numbers are shown on the left side of the timeline. Bluetooth channel numbers have a blue background, and Wi-Fi channel numbers have an orange background.
- On the 5 GHz Timeline, there are 31 Wi-Fi channels. Channel numbers are shown on the left side of the timeline with an orange background. The channel spacing varies from 20 to 40 MHz.
- Each Bluetooth channel is 1 MHz wide with no channel overlap.
- Each Wi-Fi channel in the 2.4 GHz range is 22 MHz wide and overlaps. There is a 5 MHz shift between each of the first 13 channels. There is a 12 MHz shift between channels 13 and 14.The row labels for channels 1-13 are placed at the center frequency of each channel. Channel 14 is in parentheses because that channel's center frequency is above the top of the graph.Due to space limitations, each Wi-Fi channel in the 5 GHz range is drawn with a fixed height instead of being sized and spaced relative to its width and distance from other channels.
- When both timelines are visible, selecting packets by dragging with the mouse applies to packets in both timelines, regardless of which timeline the mouse is in.
- Using the mouse scroll wheel scrolls horizontally in the chart. You can also use the arrow keys and the scroll bar at the bottom of the timeline to move within the timeline.
- Using the mouse scroll wheel + CTRL zooms. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Selecting the Information icons displays information about the Bluetooth and Wi-Fi channels.
- A green border appears around Wi-Fi Tx and Bluetooth Master.

10.2 Coexistence button bar

The button bar contains the following:

Lock - This locks the highlighted area in the display. Data will continued to be captured, but the highlighted area will move along the point where the lock was engaged.

Unlock - This unlocks the highlighted area so it will always remain at the right side of window where the newest data is displayed.

Note:The Lock/Unlock buttons only appears in live mode. Lock is automatically depressed when the user scrolls.

First Packet

Previous Packet

Next Packet

Last Packet

Previous Error Packet - This is active only when there is at least one qualifying packet to move back to. An error in Wi-Fi indicates a bad CRC. An error in Bluetooth indicates any error the data source can pass back.

Next Error Packet - This is active only when there is at least one qualifying packet to move forward to. An error in Wi-Fi indicates a bad CRC. An error in Bluetooth indicates any error the data source can pass back.

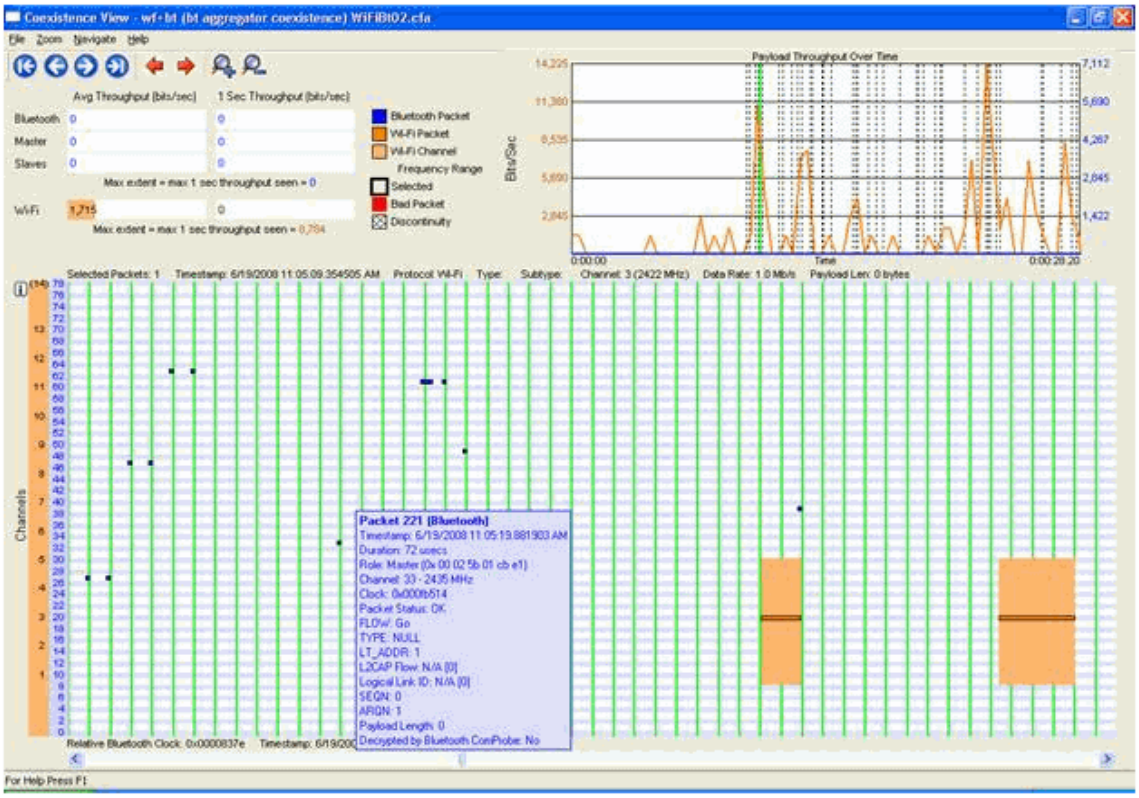
Zoom Tool - Click on the icon each time to zoom in from 4800 slots to 12 slots

Zoom Tool - Click on the icon each time to zoom out from 12 slots to 4800 slots

Reset - This resets the live capture data.

10.3 Bluetooth® Channel Frequencies

There are 79 Bluetooth channels in the 2.4 GHz timeline. The Bluetooth channel numbers appear with a blue background along the left side of the timeline.



Each *Bluetooth* channel is 1 MHz wide with no channel overlap, unlike Wi-Fi channels which do overlap. Selecting the icon displays channel information.

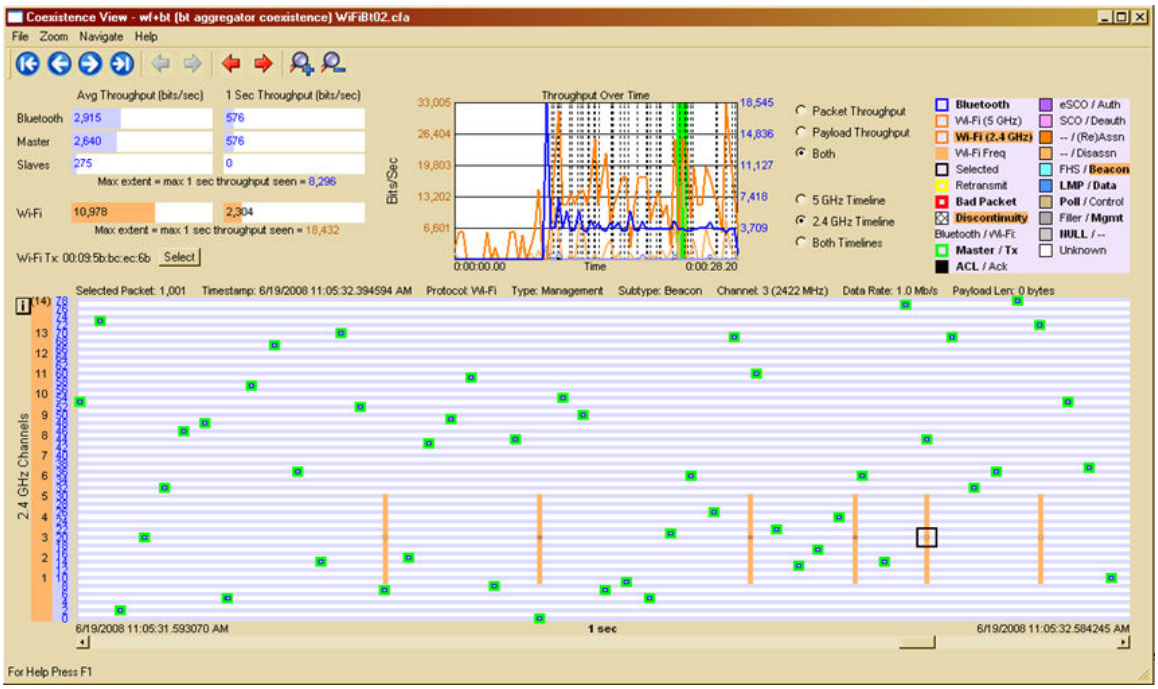
0=2402	12=2414	24=2426	36=2438	48=2450	60=2462	72=2474
1=2403	13=2415	25=2427	37=2439	49=2451	61=2463	73=2475
2=2404	14=2416	26=2428	38=2440	50=2452	62=2464	74=2476
3=2405	15=2417	27=2429	39=2441	51=2453	63=2465	75=2477
4=2406	16=2418	28=2430	40=2442	52=2454	64=2466	76=2478
5=2407	17=2419	29=2431	41=2443	53=2455	65=2467	77=2479
6=2408	18=2420	30=2432	42=2444	54=2456	66=2468	78=2480
7=2409	19=2421	31=2433	43=2445	55=2457	67=2469	
8=24010	20=2422	32=2434	44=2446	56=2458	68=2470	
9=24011	21=2423	33=2435	45=2447	57=2459	69=2471	
10=24012	22=2424	34=2436	46=2448	58=2460	70=2472	
11=24013	23=2425	35=2437	47=2449	59=2461	71=2473	

10.4 Wi-Fi Channel Frequencies - 2.4 GHz Channels

There are 14 Wi-Fi channels in the 2.4 GHz timeline. There are 11 channels available in the USA, 13 in Europe, and 14 in Japan.

The 14 Wi-Fi channels appear with an orange background along the left side of the timeline.

Selecting the icon displays channel information

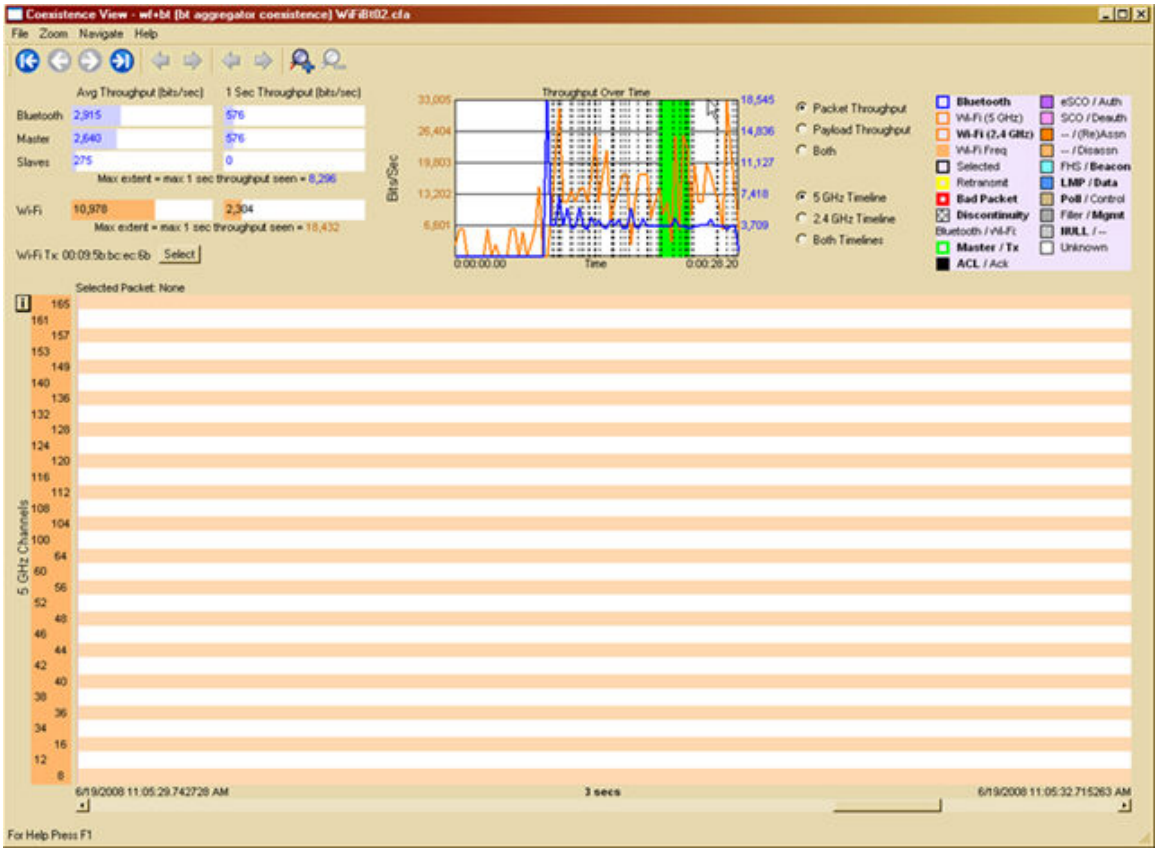


Each Wi-Fi channel is 22 MHz wide and overlap. There is a 5 MHz shift between each of the first 13 channels. There is a 12 MHz shift between channels 13 and 14.

1 = 2401-2423 MHz (centered at 2412 MHz) (USA, Europe, Japan)	8 = 2436-2458 MHz (centered at 2447 MHz) (USA, Europe, Japan)
2 = 2406-2428 MHz (centered at 2417 MHz) (USA, Europe, Japan)	9 = 2441-2463 MHz (centered at 2452 MHz) (USA, Europe, Japan)
3 = 2411-2433 MHz (centered at 2422 MHz) (USA, Europe, Japan)	10 = 2446-2468 MHz (centered at 2457 MHz) (USA, Europe, Japan)
4 = 2416-2438 MHz (centered at 2427 MHz) (USA, Europe, Japan)	11 = 2451-2473 MHz (centered at 2462 MHz) (USA, Europe, Japan)
5 = 2421-2443 MHz (centered at 2432 MHz) (USA, Europe, Japan)	12 = 2456-2478 MHz (centered at 2467 MHz) (Europe, Japan)
6 = 2426-2448 MHz (centered at 2437 MHz) (USA, Europe, Japan)	13 = 2461-2483 MHz (centered at 2472 MHz) (Europe, Japan)
7 = 2431-2453 MHz (centered at 2442 MHz) (USA, Europe, Japan)	14 = 2473-2495 MHz (centered at 2484 MHz) (Japan)
The row labels for Wi-FI channels 1-13 are placed at the center frequency of each channel	The row label for Wi-FI channel 14 is in parentheses because the channel's center frequency is above the top of the graph.

10.5 Wi-Fi Channel Frequencies - 5 GHz Channels

There are 165 Wi-Fi channels in the 5 GHz timeline. You access the 5 GHz Timeline by selecting the 5 GHz radio button.



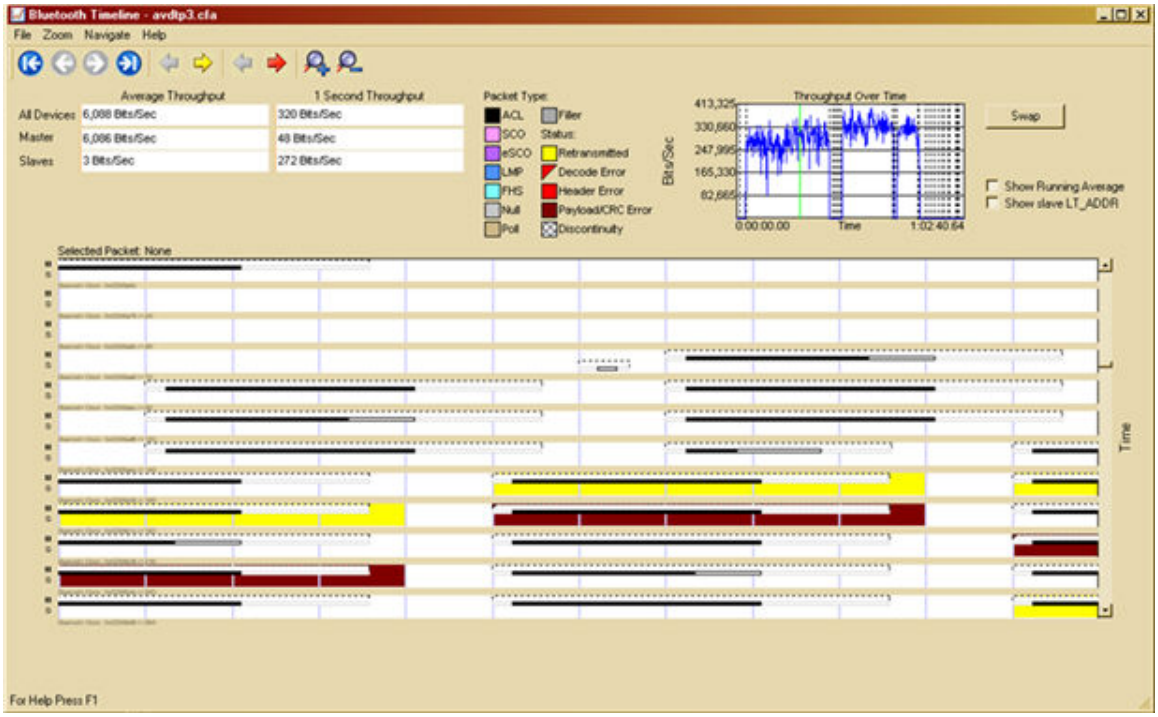
Only channels with a base value of 5 GHz and spacings of either 20 or 40 MHz are shown here. Due to space limitations, each channel is drawn with a fixed height instead of being sized and spaced relative to its width and distance from other channels (unlike the 2.4 GHz channels - both Wi-Fi and Bluetooth® - which are sized and spaced relative to each other with the exception of Wi-Fi channel 14).

11 Bluetooth Timeline

11.1 Bluetooth® Timeline

In addition to the Coexistence View, which displays both *Bluetooth*® and Wi-Fi data together, you can also see more information about *Bluetooth* in a separate dialog. The *Bluetooth* Timeline displays packet information with an emphasis on temporal information and payload throughput. The timelines also provide selected information from the Frame Display and the Protocol Navigator.

The timelines provide a rich set of diverse information about *Bluetooth* packets, both individually and as a range. Information is conveyed using text, color, graphic size, line type, and position.



You access the *Bluetooth* Packet Timeline by selecting **Bluetooth Timeline** from the View menu or by pressing the *Bluetooth* Timeline icon  on the Control Window toolbar, Frame Display, or Protocol Navigator.

Select one of the links below to learn more about the *Bluetooth* Timeline.

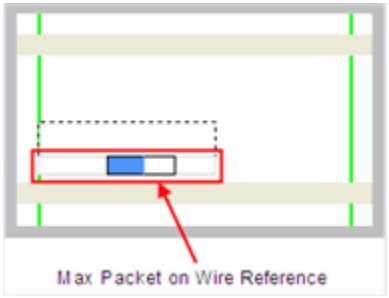
11.2 Bluetooth® Timeline Packet_Depiction

The timeline shows *Bluetooth* packets within a specific period of time.

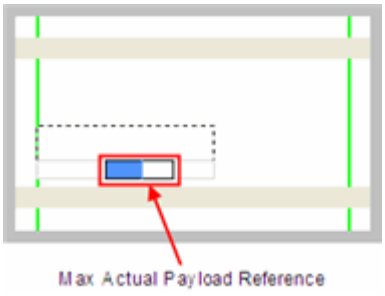
- The timeline shows Bluetooth packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
- Within each row are two divisions: M (master) and S (Slave). Packets are placed on M or S depending on which type of data it is.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet.You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

A packet is drawn using the following components:

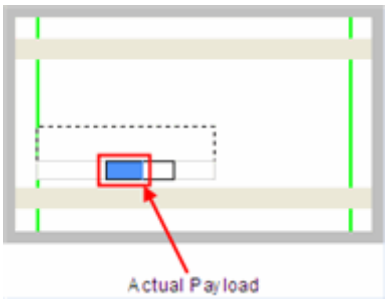
- A "**max packet on wire reference**" rectangle (light solid lines). This indicates the packet on the wire with a max payload.



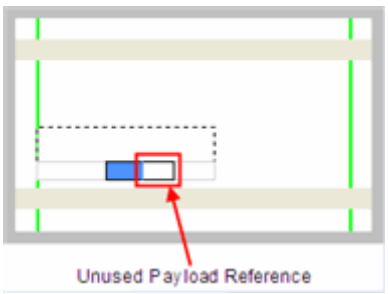
- A "max actual payload reference" rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload on the wire contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates where the payload begins in time.



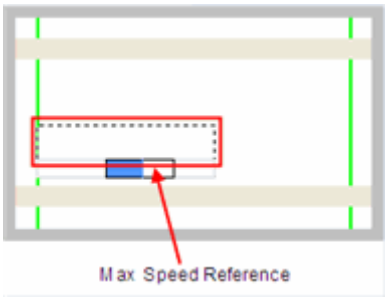
- • An “**actual payload**” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference” rectangle. If the actual payload is of max size, the entire “max actual payload reference” rectangle is colored.



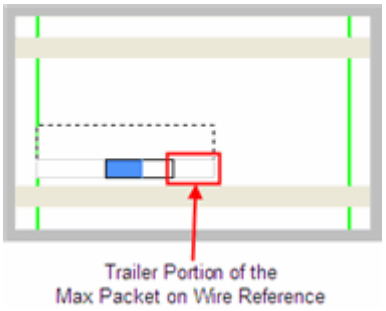
- • An “**unused payload reference**” sub-rectangle (always white). This indicates the unused portion of a maximum payload. It is the remaining portion of the “max actual payload reference” rectangle. The packet on the wire does not leave room for this. It is indicated for reference only.



- • A “**max speed reference**” rectangle (dashed lines). This is used to extend the height to that of a 3 Mbits/sec packet, and appears only for packets whose speed is less than that. The packet shown here has a speed of 1 Mbit/sec because the height of the other rectangles is 1/3 of the total height.



The part of the “max packet on wire reference” rectangle (light solid lines) that trails the “max actual payload reference” rectangle (dark solid lines) is partly packet on the wire (if the payload on the wire contained FEC) and partly trailer (CRC, etc). There is always a trailer, so there is always a little space (subject to round off error and pixel granularity) between the ends of the two rectangles.



This table shows how packets are colored:

Packet Category	Packet Types	Color
ACL	DM1, DM3, DM5 DH1, 2-DH1, 3-DH1 DH3, 2-DH3, 3-DH3 DH5, 2-DH5, 3-DH5 AUX1	Black
SCO	HV1, HV2, HV3, DV	Pink
eSCO	EV3, 2-EV3, 3-EV3, EV4 EV5, 2-EV5, 3-EV5	Purple
LMP*	DM1, DV	Dark blue
FHS	FHS	Light blue
NULL	NULL	Light gray
POLL	POLL	Light brown
Filler	Filler provided by FTS	Dark gray

*LMP is a protocol layer that uses either DM1 or DV packets. If a packet has an LMP layer, the LMP color is used instead of the packet type color.

This table summarizes the various ways in which packet information is presented:

Information	Text	Color	Graphic size	Position
Packet type	x			
Packet category		x		
Protocol	x	x		
Time of occurrence	x			x
Source device	x			x
Duration			x	
Size in bytes	x		x	
Size as a percentage of max size for that packet type	x		x	
Speed			x	
Status	x	x		

Bluetooth Channel Frequencies

11.3 Bluetooth® Timeline Packet Navigation and Selection

- Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous error packet, next or previous retransmitted packet (*Bluetooth* only), and the first or last packet.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the Frame Display.
- Selecting Previous Packet with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).
- Selecting Next Packet with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).
- Selecting Previous/Next for a packet that's currently visible selects it without scrolling.
- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline, it is also becomes selected in the Frame Display. When multiple packets are selected in the timeline, only one of them is selected in the Frame Display.
- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

11.4 Bluetooth® Timeline Button Bar

The button bar contains the following:


Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.


Unlock


First Packet


Previous Packet


Next Packet


Last Packet


Previous Retransmitted Packet


Next Retransmitted Packet


Previous Error Packet


Next Error Packet


Zoom In - Click on the icon each time to zoom in from 4800 slots to 12 slots


Zoom Out - Click on the icon each time to zoom out from 12 slots to 4800 slots


Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in the Frame Display or Protocol Navigator. Resetting the display may be useful when the most recent throughput values are of interest.

11.5 Bluetooth® Timeline Menu Bar

The menu bar contains the following:

File Menu:

Toggle Display Lock
(available only in live mode)

Reset (available only in live mode)

Exit

Zoom Menu:	**Keyboard Shortcuts:**
Zoom In	Ctrl+Plus
Zoom Out	Ctrl+Minus
Zoom In Tool	
Zoom Out Tool	
Selection Tool	
12 Slots (3 X 4)	
36 Slots (6 X 6)	
144 Slots (12 X 12)	
324 Slots (18 X 18)	
576 Slots (24 X 24)	
900 Slots (30 X 20)	
1296 Slots (36 X 36)	
1764 Slots (42 X 42)	
2304 Slots (48 X 48)	
2916 Slots (54 X 54)	
3600 Slots (60 X 60)	
4356 Slots (66 X 66)	
5184 Slots (72 X 72)	

Navigate Menu:	**Keyboard Shortcuts:**
First Packet	Home
Last Packet	End
Previous Packet	Left Arrow
Next Packet	Right Arrow
Previous Retransmitted Packet	
Next Retransmitted Packet	
Previous Error Packet	Ctrl+Left Arrow
Next Error Packet	Ctrl+Right Arrow
Selected Packet	Enter
Toggle Display Lock (available only in live mode)	L

Help Menu:

Help Topics

About

11.6 Bluetooth® Timeline Visual Elements

The *Bluetooth* Timeline consists of the following visual elements:

- **The timeline shows *Bluetooth* packets within a specific period of time.**
  - The timeline shows Bluetooth packets within a specific period of time.
  - The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
  - Within each row are two divisions: M (master) and S (Slave). Packets are placed on M or S depending on which type of data it is.
  - Placing the mouse pointer on a packet displays information about that packet in an information box.

- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet.You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

- **Rows of *Bluetooth* Slots**

  Each slot begins at the left edge of the vertical blue bar. There are two *Bluetooth* clocks per slot. Each slot represents 0.000625 seconds, or 625 µs.

- **'M' and 'S' labels**

  Within each row, master and slave packets are indicated on the left side of the row. By default, all possible slave devices (there can be up to 7) are put on the 'S' sub-row, but checking the "Show slave LT_ADDR" checkbox shows all existing slave device sub-rows with numbered labels (some or all of S1, S2, …, S7).

- ***Bluetooth* Clock**

  The *Bluetooth* clock of the first slot in each row is shown underneath each row.

- **Packet Info Line**

  The packet info line appears just above the timeline and displays information for the currently selected packet(s). If only one packet is selected, this information consists of the packet number, packet type, *Bluetooth* clock (*Bluetooth* only), and Timestamp. If multiple packets are selected, this information consists of the packet range, the *Bluetooth* clock delta (*Bluetooth* only), and the Timestamp delta. Selected packets are bounded by a magenta rectangle. See the Packet Navigation and Selection section.

- **Floating Information Window (aka Tooltip)**

  The information window displays when the mouse cursor hovers on a packet (not slot). It persists as long as the mouse cursor stays on the packet or tooltip. For *Bluetooth*, the tooltip shows the packet number (in bold), the Baseband layer decode from the decode pane of the Frame Display (with the percentage of the Payload Length max added), and the decode of the highest layer (if it's not the Baseband layer) as displayed in the Protocol Navigator.

- **Discontinuities**

  Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.

- **Zoom Tools**

  Zoom tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See the "Zooming" section.

- **Packet Status**

  Packet status is indicated by color codes. A yellow slot indicates a re-transmitted packet, a dark red slot indicates a CRC error, and a small red triangle in the upper-left corner of the packet (not the slot) indicates a decode error.

- **Right-Click Menu**

  The right-click menu provides zooming and tool selection. See the "Zooming" section.

- **Graphical Packet Depiction**
  Each packet within the visible range is graphically depicted. See the "Packet Depiction" section.

- **Swap Button**
  The Swap button switches the position of the Timeline and the Throughput graph.

- **Show Running Average**
  Selecting this check box shows a running average in the Throughput Over Time graph as an orange line

- **Show slave LT_ADDR**

  Selecting this checkbox displays the Slave LT_ADDR in the timeline row labels.

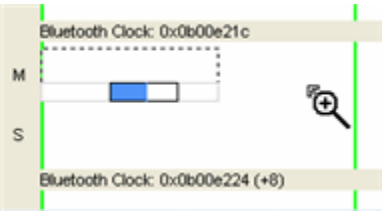
11.7 Bluetooth® Timeline Zooming

Zoom features can be accessed from the Zoom menu, clicking a zoom tool on the toolbar, or by right clicking on the Timeline window.

A couple of things to remember about Zooming.

- Zoom tools accessed using the right click menu allow you to maintain the current position on the screen and precisely zoom in to a specific packet.
- Selecting a Zoom icon (+ or -) on the toolbar does not change the pointer to a Zoom Tool. Each distinct click only zooms in our out.

- Zoom tools accessed from the Zoom Menu have a pointer in the upper-left corner which is useful for specifying the zoom location and bringing up a tool tip of a specific packet.



11.8 Bluetooth® Timeline Throughput Displays

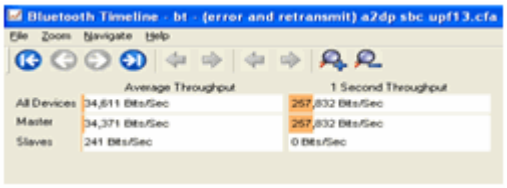
Throughput is payload over time. There are 3 categories of throughput:

- Average
- 1-second
- Graph

In computing throughput, payload is not counted from Bluetooth packets that have a CRC error (dark red slot) or that are a retransmission (yellow slot).

11.9 Bluetooth® Timeline Average Throughput Indicators

The following figure depicts the Throughput display with the Average Throughput indicators in the left column.



Average throughput is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet. In *Bluetooth*, timestamp difference is used instead of *Bluetooth* clock count because timestamp difference is immune to role switches. However, this can result in inaccuracies when the duration is small enough that a coarse timestamp granularity is significant.

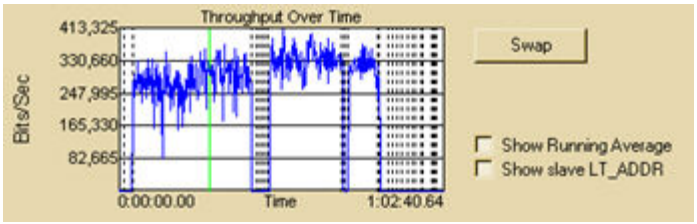
- Average throughput is shown as 0 when there is only one packet, because in that case the timestamp difference is 0 and an average cannot be computed.
- Average throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates percentage of max, and text gives the actual throughput.

11.10 Bluetooth® Timeline One Second Throughput Indicators

- 1-second throughput is the total payload over the most recent one second of duration (This is determined by counting *Bluetooth* clocks). It is cleared after each discontinuity. A discontinuity is when the *Bluetooth* clock goes forward more than two (2) seconds or goes backwards any amount. This is caused by either a role switch or *Bluetooth* clock rollover . The *Bluetooth* clock count is used instead of timestamp difference because the *Bluetooth* clock count is precise; however, if timestamp difference were used it would not be necessary to clear the 1-second throughput after each discontinuity.
- 1-second throughput is not an average. It is simply the total payload over the most recent one second of duration. Since it's not an average, it behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small payload by small time), 1-second throughput is very small (since it counts only what it sees and doesn't try to extrapolate).
- A 1-second throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates percentage of max, and text gives the actual throughput.

11.11 Bluetooth® Timeline Throughput Graph

The following figure depicts the Throughput Graph (Throughput Over Time).



The throughput graph shows total payload for each successive time interval. The time interval is initially 0.1 second. Each time the number of throughput elements reaches 100, they are collapsed into a set of 50 by combining adjacent elements and doubling the duration of each element. Collapsing thus occurs as follows:

Collapse count	Time since beginning of session (seconds)	Element duration after collapse (seconds)
1	10	0.2
2	20	0.4
3	40	0.8
4	80	1.6
5	160	3.2
6	320	6.4

and so on...

The bottom of the graph shows a beginning time and an ending time. The beginning time is relative to the start of the session and initially 0. When packets start wrapping out it becomes the relative time offset of the first available packet. The ending time is always the total time of the session.

Discontinuities are indicated by vertical dashed lines.

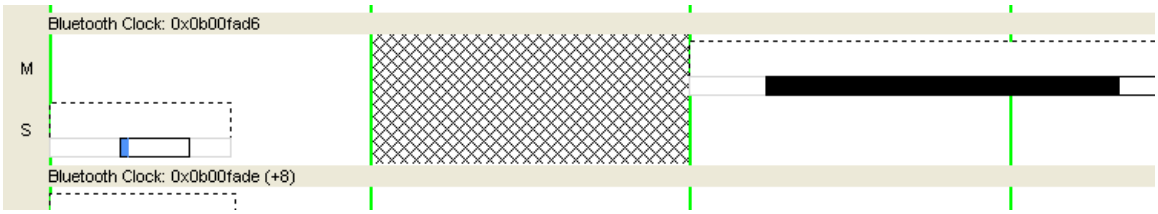
A green view port indicates the time range corresponding to the visible slots in the timeline. The view port can be moved by clicking elsewhere in the graph or by dragging. Whenever it is moved, the timeline scrolls to match. When the slot range in the timeline changes, the view port moves and resizes as necessary to match.

The **Swap** Button
The Swap button switches the position of the Timeline and the Throughput graph.

Show Running Average
Selecting this check box shows a running average in the Throughput Over Time graph as an orange line

11.12 Bluetooth® Timeline Discontinuities

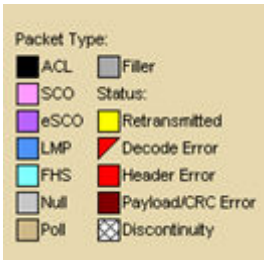
The following figure depicts a Discontinuity between two packets.



To keep the timeline and the throughput graph manageable, big jumps in the Bluetooth clock are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the Bluetooth clock goes forward more than two (2) seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph. The Bluetooth clock can jump forward when capture is paused or when there is a role switch (in a role switch, a different device becomes master, and since each device keeps its own Bluetooth clock, the clock can change radically), and backwards when there is a role switch or clock rollover.

11.13 Legend

This legend identifies the color coding found in the timeline.



12 Data Extraction

12.1 Data Extraction

The Data Extraction  plug-in allows you to extract files that were transferred over various protocols. You can also choose to have the files opened automatically as long as you have applications able to read the files.

To extract data, select the Extract Data menu item from the View menu on the Control window. When you select this item a settings dialog appears that allows you to define how the system extracts the data.

A status dialog displays the progress and important information concerning the extraction.

12.2 Data Extraction Settings

The Data/Audio Extraction  plug-in allows you to extract files that were transferred over *Bluetooth*® profiles.

1. Choose a checkboxe(s) on left side of the dialog to identify from which **profiles** you want to extract data.

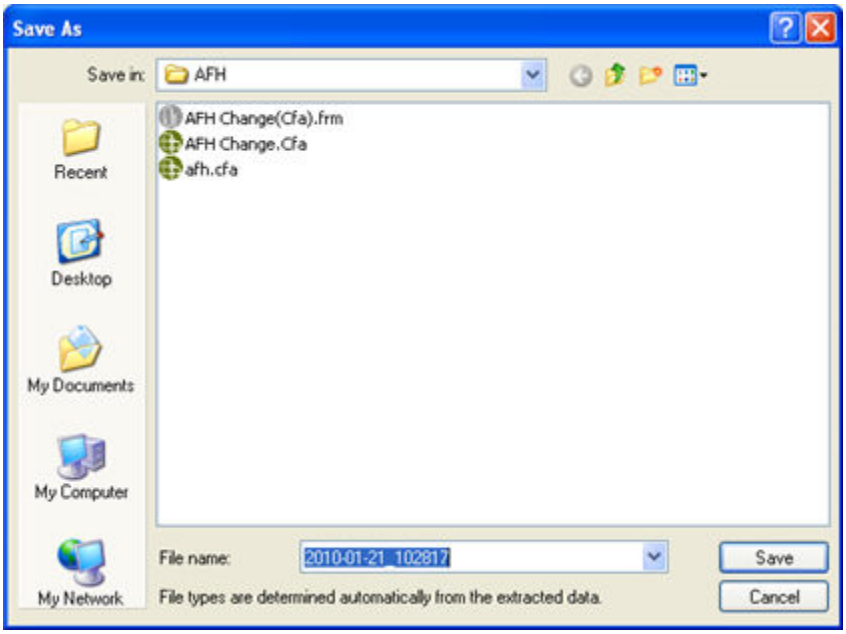
It's important to note that if there is no data for the profile(s) you select, no extracted file is created.

2. If you want to open the file(s) automatically after they are extracted, select the **Open File(s) After Extraction** checkbox.
   Note: This does not work for SCO/eSCO.

3. Click on a radio button to write the streams as **Two Mono Files** or as **One Stereo File**. This is for SCO/eSCO only.
4. Select the checkbox if you want to convert **A-Law and µ-law to Linear PCM.** CVSD are always converted to Linear PCM. You may choose to convert to Linear PCM since more media players accept this format.

5. Select the Add silence packets to insert the silence packets (dummy packets) for the reserved empty slots into the extracted file. If this option is not selected, the audio packets are extracted without inserting the silence packets for the reserved empty slots. *This is for SCO/eSCO only.*
6. Select **Extract.**

A *Save As* dialog appears.



The application will assign a file name and file type for each profile you select in Step 1 above. A separate file for each profile will be created, but only for those profiles with available data.

7. Select a **location** for the file(s).
8. Click **Save**.

13 Find

13.1 Starting a Search

You can search your data in several different ways. Some types of searches are relevant only for framed data and is not offered if the data is not framed. Other types of searches are available depending on the type of data being viewed.

To Begin a Search

1. Open a capture file, or capture some data to search.
2. Open the Event Display  or Frame Display  window.
3. Click on the *Find* icon  or choose *Find* from the *Edit* menu.
4. The Find window has a tab for each type of search. Click on the appropriate tab for the type of search you want to do.
5. Select the parameters for your search, and click *Find Next*. *Find Next* looks for the next occurrence of the search criteria, while *Find Previous* looks for an earlier occurrence of the search criteria.
6. Press F3 to repeat the last search.

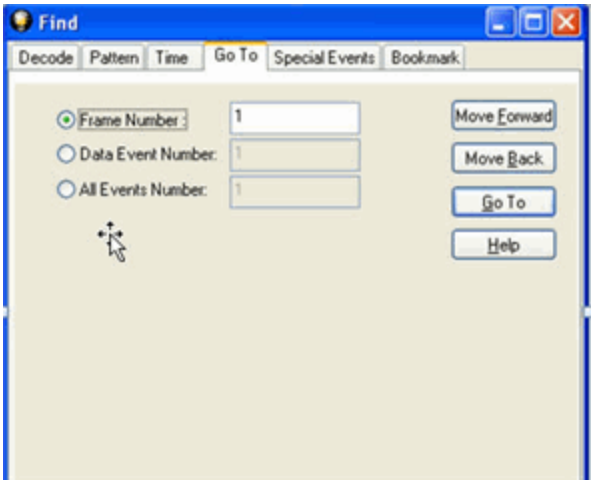
Search results are highlighted in the Event or Frame Displays, or both if appropriate. The selection in the Event Display appears on the third line down from the top of the window by default: this value can be changed.

13.2 Using Go To

This type of search allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To access the Go To function:

1. Select *Go To* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also click the Find icon  on the toolbar
2. The system displays the Find dialog with the Go To tab selected.



Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file or buffer you are viewing.

To go to a particular frame :

1. Select the *Frame Number* radio button
2. Type the frame number in the box.
3. Click the *Go To* button.
4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the *Move Forward* or *Move Back* button.

To go to a particular event :

1. Select the Data Event Number or All Events Number radio button.
2. Type the number of event in the box.
3. Click the Go To button.
4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the Move Forward or Move Backward button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on Move Forward. Each time you click on Move Forward, FTS moves forward 10 events.

See Event Numbering for why the Data Event Number and All Events Number may be different. As a general rule, if you have the Show All Events icon depressed on the Event Display window or Frame Display Event pane, choose All Events Number. If the Show All Events button is up, choose Data Event Number.

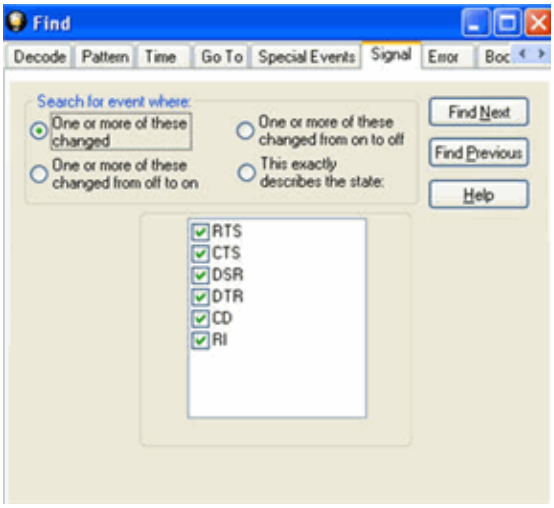
13.3 Searching for Control Signal Changes

Control signal searching allows you to search for changes in control signal states for one or more control signals. You can also search for a specific state involving one or more control signals, with the option to ignore those control signals whose states you don't care about.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where control signals changed.

To access the control signal search function

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to click the Find icon  from one of the toolbars
2. Click on the *Signal* tab of the Find dialog.



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

Selecting Control Signals to Search

The section with the check boxes allows you to specify which control signals the analyzer should pay attention to when doing the search. The analyzer pays attention to any control signal with a check mark.

- Click on a box to place a check mark next to a control signal
- Click again to uncheck the box
- By default, the analyzer searches all control signals, which means all boxes start out checked.

For example, if you are only interested in finding changes in RTS and CTS, you would check those two boxes and uncheck all the other boxes. This tells the analyzer to look only at the RTS and CTS lines when running the search. The other signals are ignored.

Searching for On, Off, or Changed States

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- One or more control signals changed
- One or more control signals changed from off to on
- One or more control signals changed from on to off

Searching for an event where one or more signals changed means that the analyzer looks at every control signal that you checked, and see if any one of those signals changed state at any time.

If you want to look at just one control signal:

- Check the box for the signal.
- Uncheck all the other boxes.
- Choose to search for an event where one or more signals changed.
- The analyzer notes the state of the selected signal at the point in the buffer where the cursor is, search the buffer, and stop when it finds an event where RTS changed state.
- If the end of the buffer is reached before an event is found, the analyzer tells you that no matches were found.

Searching for events where control signals changed state from off to on, or vice versa, is most useful if the signals are usually in one state, and you want to search for occasions where they changed state.

For example,

- If DTR is supposed to be on all the time but you suspect that DTR is being dropped
- Tell the analyzer to look only at DTR by checking the DTR box and unchecking the others
- Do a search for where one or more control signals changed from on to off.
- The analyzer would search the DTR signal and stop at the first event where DTR dropped from on to off.

Searching for an Exact State

To search for an exact state means that the analyzer finds events that match exactly the state of the control signals that you specify.

- First, choose to search for an event where your choices exactly describe the state.
- This changes the normal check boxes to a series of radio buttons labeled On, Off and Don't Care for each control signal.
- Choose which state you want each control signal to be in.
- Choose Don't Care to have the analyzer ignore the state of a control signal.

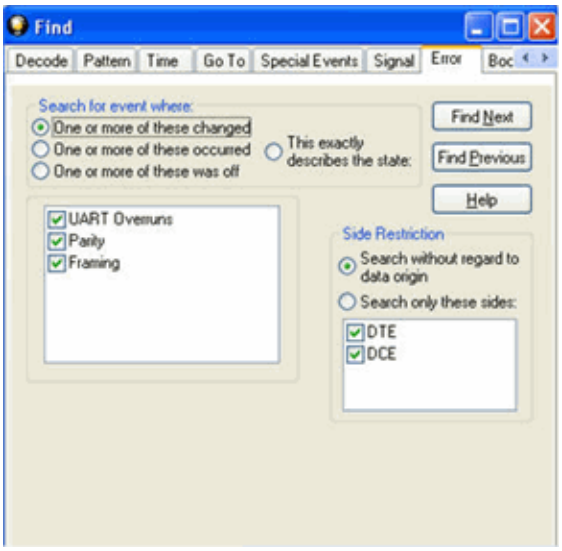
- When you click Find Next, the analyzer searches for an event that exactly matches the conditions selected, beginning from the currently selected event.
- If the end of the buffer is reached before a match is found, the analyzer asks you if you want to continue searching from the beginning.
- If you want to be sure to search the entire buffer, place your cursor on the first event in the buffer.

13.4 Searching for Data Errors

The analyzer can search for several types of data errors. You can choose which errors you want to search for and whether to search the DTE or DCE data or both. Bytes with errors are shown in red in the Event Display window, making it easy to find errors visually when looking through the data.

To access the data errors search function

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars
2. Click on the *Error* tab of the Find dialog.



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

Selecting Which Errors to Search

The section with the check boxes allows you to choose which errors the analyzer should look for. Click on a box to check or un-check it

If you want to search only for overrun errors

- check the overrun box

- un-check the other boxes.

To search for all types of errors

- check all boxes

Searching for Error Conditions

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- one or more error conditions changed
  - one or more error conditions occurred
- one or more error conditions were off (i.e. no errors occurred)

The most common search is looking for a few scattered errors in otherwise clean data.

To do this type of search:

- choose to search for an event where one or more error conditions occurred
- choose which errors to look for
- By default, the analyzer looks for all types of errors.

In contrast, searching for an event where one or more error conditions were off means that the analyzer looks for an event where the errors were not present.

For example, if you have data that is full of framing errors, and you know that somewhere in your 20 megabyte capture file the framing got straightened out, you could choose to search for an event where one or more error conditions were off, and choose to search only for framing. The analyzer searches the file, and finds the point at which framing errors stopped occurring.

Searching for an event where the error conditions changed means that the analyzer searches the data and stop at every point where the error condition changed from on to off, or off to on.

For example, if you have data where sometimes the framing is wrong and sometimes right, you would choose to search framing errors where the error condition changed. This first takes you to the point where the framing errors stopped occurring. When you click Find Next, the analyzer stops at the point when the errors began occurring again.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where error conditions changed. The analyzer searches until it finds an event where error conditions changed or it reaches the end of the buffer, at which point the analyzer tells you that there are no more events found in the buffer. If you are searching for an exact match, the analyzer asks you if you want to continue searching from the beginning of the buffer.

Searching for Exact Error Conditions

To search for an exact state means that the analyzer finds events that exactly match the error conditions that you specify.

- Select the "This exactly describes the state" radio button.

- This changes the normal check boxes to a series of radio buttons labeled On, Off and Don't Care for each error.
- On means that the error occurred
- Off means that the error did not occur
- Don't Care means that the analyzer ignores that error condition.
- Select the appropriate state for each type of error.

Example:

If you need to find an event where just an overrun error occurred, but not any other type of error, you would choose overrun error to be On, and set all other errors to Off. This causes the analyzer to look for an event where only an overrun error occurred.

If you want to look for events where overrun errors occurred, and other errors may have also occurred but it really doesn't matter if they did or not, choose overrun to be On, and set the others to Don't Care. The analyzer ignores any other type of error, and find events where overrun errors occurred.

To find the next error, click the Find Next button. To find an error that occurred earlier in the buffer to where you are, click the Find Previous button.

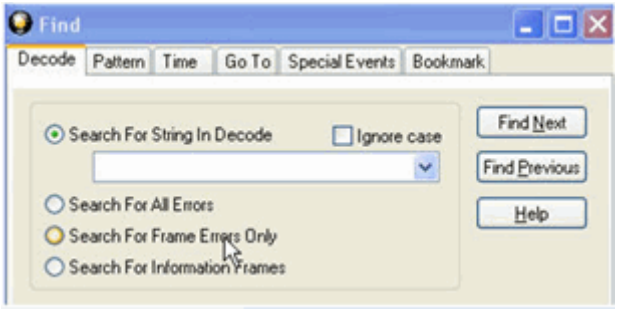
13.5Searching for Frame Errors

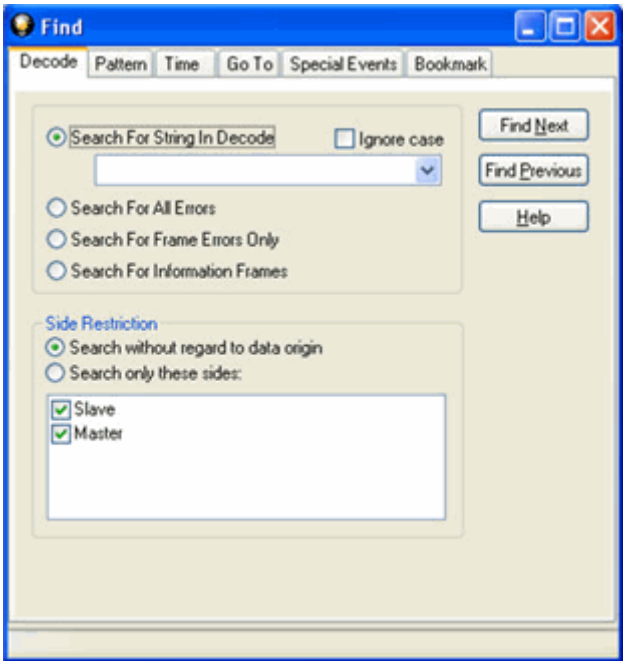
There are several options for error searching:

- Search for All Errors finds frame errors as well as frames with byte-level errors (such as parity or CRC errors).
- Search for Frame Errors Only finds Frame specific errors, such as Frame Check errors.
- Search for Information Frame only searches Information Frames

To access the search within decodes function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars
2. Click on the *Decode* tab of the Find dialog.
3. Click the appropriate radio button for the type of search you want to perform or enter a value
4. Click Find Next.





Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

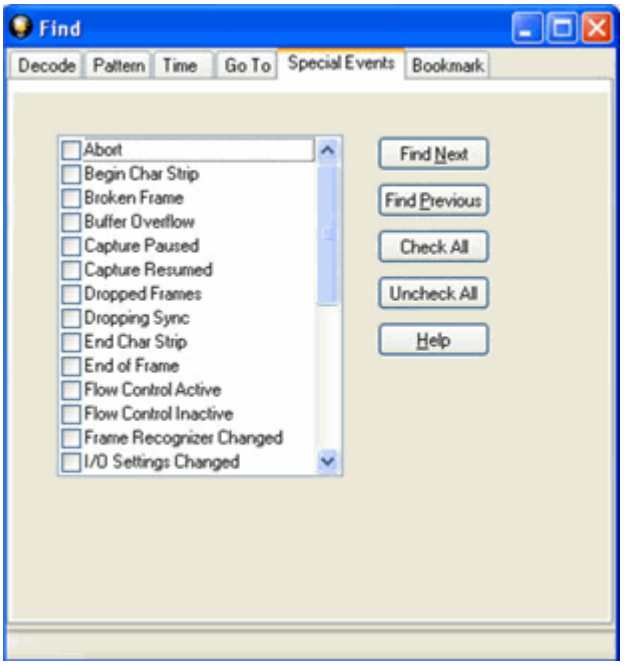
13.6 Searching for Special Events

The analyzer inserts or marks events other than data bytes in the data stream.

For example, the analyzer inserts start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, the analyzer shows this using a special event marker.

To access the search for special events function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars
2. Click on the *Special Events* tab of the Find dialog.



3. Check the event or events you want to look for in the list of special events.
4. Click Find Next.

Note:The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

- Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

For a list of all special events and their meanings, see List of All Event Symbols.

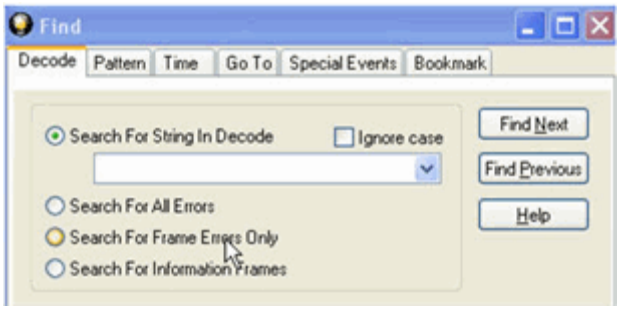
13.7Searching within Decodes

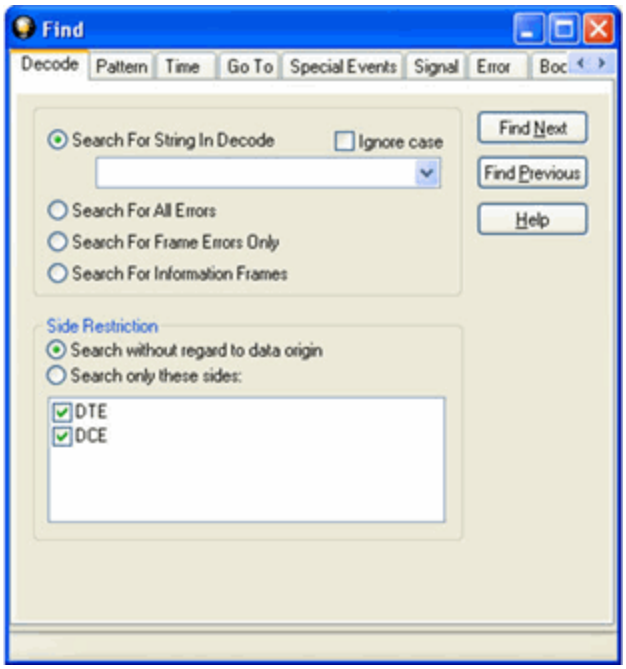
Searching within decodes lets you to do a string search on the data in the Decode Pane of the Frame Display window.

You can search one or both sides of the circuit, and your search can include wildcards. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string.

To access the search within decodes function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars.
2. Click on the *Decode* tab of the Find dialog.





Note:

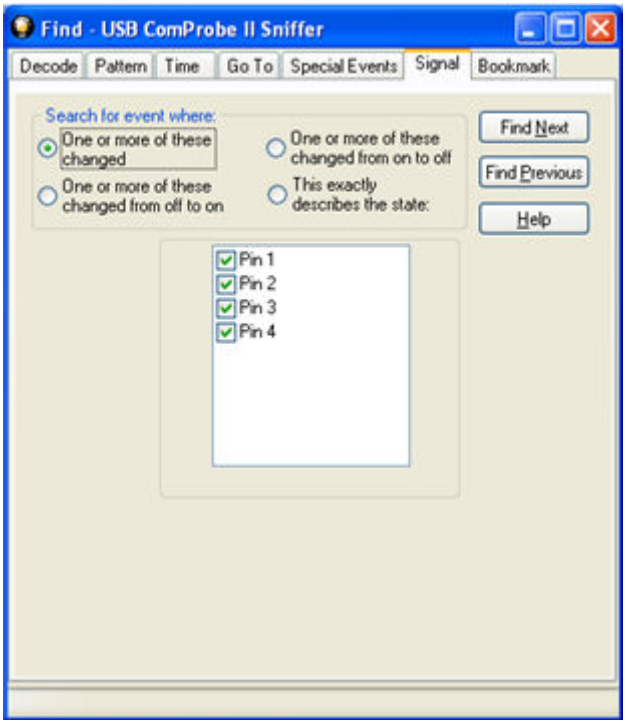
The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

13.8Searching by Signal

You can search using information originating from the Breakout Box.

1. Select one or more of the *checkboxes* for Pin 1, 2, 3, or 4.
   Click here to learn more about the Breakout Box and Pins 1 - 4.

2. Select one of the *four radio buttons* to choose the condition that must be met in the search



3. Click *Find Next* to locate the next occurrence of the search criteria or *Find Previous* to locate an earlier occurrence of the search criteria.

13.9 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the Event Display. The first selected byte appears on the third line of the display.

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\Program Files\Common Files\FTE)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

13.10 Subtleties of Timestamp Searching

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.

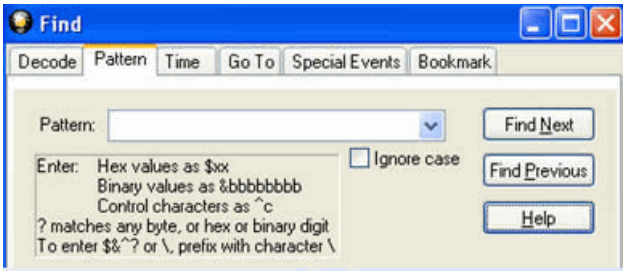
13.11 Entering Search Patterns (String Searches)

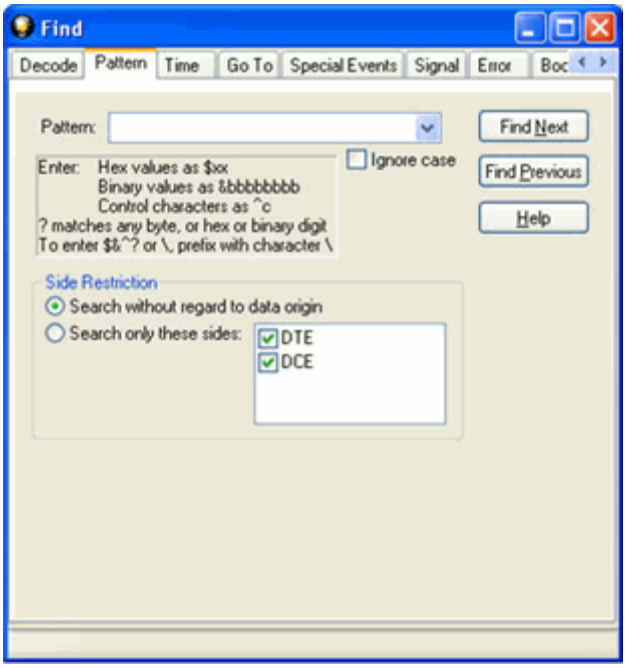
13.11.1 Searching by Pattern

Search by Pattern lets you perform a traditional string search. You can combine any of the formats when entering your string, and your search can include wildcards. You can search one or both sides of a circuit containing interwoven data such as serial communication.

To access the search by pattern function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also click the Find icon  from one of the toolbars.
2. Click on the *Pattern* tab of the Find dialog.





Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

13.11.2 Entering Characters

Various characters are used when creating a search string on the Find dialog. You can enter any character from a character set, with the following exceptions: \$&^?. These characters are used as prefixes to let you to enter hex, binary, control or wildcard characters.

1. Place the cursor in the Pattern box and type in your string.
2. Click Find Next in order to find the next occurrence of the string.
3. Click on Find Next as many times as necessary until the analyzer has searched all the data.
4. Clicking on Find Previous searches the buffer backwards.

The escape character is the backslash \. Use this character when you want to search for one of the above restricted characters. For example, to search for a $, you enter \$. To search for a \, enter \\.

Check Ignore Case to do a case-insensitive search.

13.11.3 Entering Hex or Binary

Hex or Binary values are used when creating a search string on the Find dialog.

To enter a hex value :

1. Enter a $ followed by two hex digits.
2. For example, to search for hex 00 01, enter $00$01.
3. If you need to specify the $ as a character, use \$.
4. The $ symbol tells the analyzer that the following characters are hex digits

To enter a binary value:

- The & symbol tells the analyzer that a binary number comes next. For example, to search for binary 00001111, you would use &00001111.
- If you need to specify the & as a character, use \&.

13.11.4 Control Characters

Various control characters are used when creating a search string on the Find dialog. You can enter any character from a character set, with the following exceptions: \$&^?. These characters are unavailable. The ^ (caret) is used to enter the control characters Ctrl-A through Ctrl-Z and Ctrl-@,[,\,],- when using the ASCII character set. For example, ^A specifies Ctrl-A ($01) and ^@ specifies ASCII NUL ($00).

If you need to specify the ^ as a character, use \^.

Note that neither the ^ character nor control characters exist in Baudot, so attempts to search for the ^ character results in an error message. The ^ character exists in EBCDIC, but

control characters do not. A search for ^A in EBCDIC matches any occurrence of ^A ($5F$C1). You do not need to use the escape character to search for a ^ character in EBCDIC.

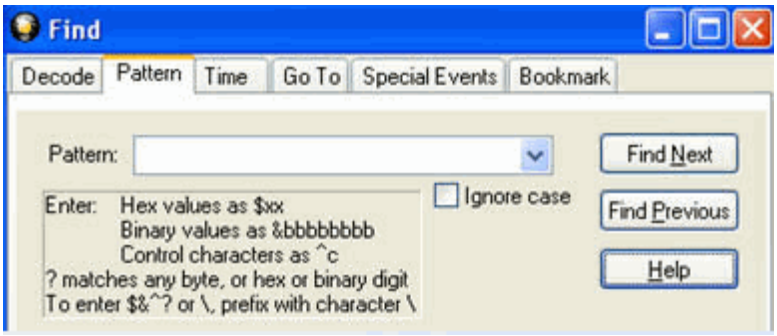
13.11.5 Wildcard Character

A wildcard can be used when creating a search string on the Find dialog.

The wildcard character is the question mark (?). The analyzer supports wildcard searching at the byte, nibble and bit level. Wildcards can be used in place of characters, hex digits, and binary digits. If you need to search for a ?, you can use \?.

13.11.6 Examples of Search Strings

In the Find function on the Frame Display, Event Display, or Protocol Navigator, you can search for any single byte in the range of hex $10 through $1F, type $1?.



&111111?? searches for binary numbers beginning with 111111 and ending with any combination of 1 and 0. 11111100, 11111101, 11111110, and 11111111 are all strings that match the search criteria.

To search for any four character string which starts with an L and ends with an ES, type L?ES.

You can combine formats in one string. For example, another way to specify a search for the string L?ES is $4C&????????&01000101S.

13.12 Searching by Time

13.12.1 Searching by Time

The analyzer can search by time in two different ways.

- **Absolute**

  An absolute timestamp search means that the analyzer searches for an event at the exact date and time specified. If no event is found at that time, the analyzer goes to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.

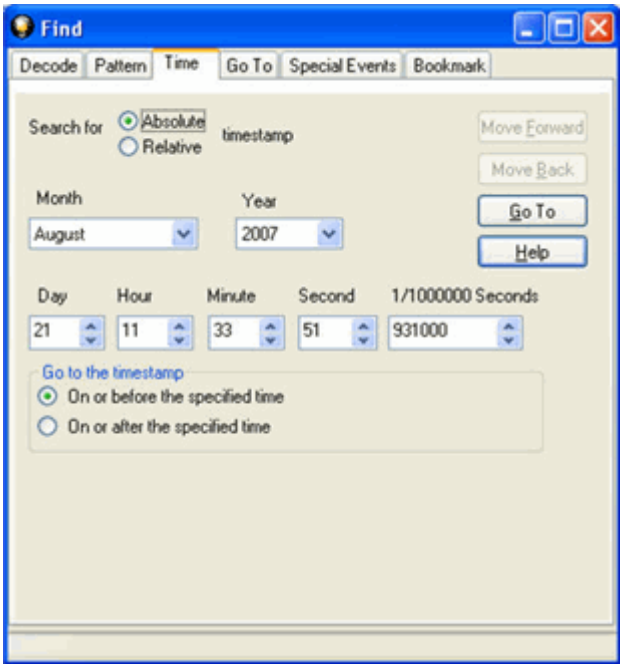
- **Relative**

  A relative search means that the analyzer begins searching from whatever event you are currently on, and search for the next event a specific amount of time away.

Note that the analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars.
2. Click on the *Time* tab of the Find dialog.
3. Use the "Search for" radio buttons at the top of the dialog to indicate the search type



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing

13.12.2 Searching with Absolute Timestamp

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may also select the Find icon  from one of the toolbars
2. Click on the *Time* tab of the Find dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

3. Specify the time to search for by using the counters in the middle of the window.

   - Click on the arrows next to each item to increase or decrease the value of each counter.
   - By default, the counters display the timestamp of the first event in the file

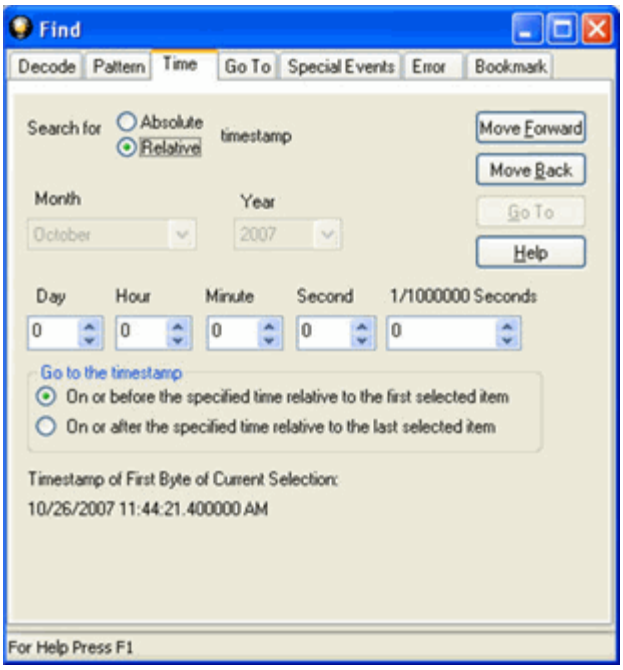
4. After selecting the time, click on the Go To button to start the search.

Sometimes there can be more than one event with the same timestamp. The system highlights all events with the specified timestamp.

13.12.3 Searching with Relative Timestamp

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also select the Find icon  from one of the toolbars.
2. Click on the *Time* tab of the Find dialog.



Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file or buffer you are viewing.

3. Click on the event in the Event Display window that you want to begin the search from. The event must have a timestamp in order for relative timestamp search to work.

4. In the *Find* dialog, use the counters in the middle of the window to specify the time interval you want to jump.
   You can specify intervals in days, hours, minutes, seconds, and fractions of a second, or any combination of these.

5. When you have specified the time interval you want to use, click on the Move Forward or Move Backward buttons to start the search from the current event.

For example, to search for an event occurring 10 seconds after the currently selected event, choose to do a relative timestamp search, use 10 seconds for your time interval, and click on Move Forward.

As with absolute timestamping, the analyzer highlights all events with the specified timestamp.

13.12.4 Choosing "On or Before" or "On or After"

The analyzer searches for an event that matches the time specified. If no event is found at the time specified, the analyzer goes to the nearest event either before or after the specified time. Choose whether to have the analyzer go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the "Go to the timestamp" box.

If you are searching forward in the buffer, you usually want to choose the "On or After" button. If you choose the "On or Before" option, it may be that the analyzer finishes the search and not move from the current byte, if that byte happens to be the closest match.

14 Bookmarks

14.1 Bookmarks

- Bookmarks are a way to mark frames or events in a capture file. You can search for bookmarks and move quickly between bookmarks.
- Bookmarks appear as a magenta triangle next to the frame number in the Frame Display window. Any comment associated with the bookmark appears in the Bookmark column.
- When you add or change a bookmark, you are asked if you want to save your changes when you close the capture file, and given the option of saving the bookmarks to the current file or to a new one. See Confirming CFA Changes for more information.

14.2 Adding, Modifying or Deleting a Bookmark

You can Add, Modify, or Delete a Bookmark from the Add Bookmark dialog from the Frame Display, Event Display, or the Protocol Navigator.

Add:

1. Select the frame or event you want to bookmark.
2. Select *Add or Modify Bookmark* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. Or simply select the *Add or Modify Bookmark*  icon on one of the toolbars.
3. In the dialog box, add a comment if you wish.
4. Click *OK*.

You can also add a bookmark by right-clicking on the frame and choosing Add Bookmark from the right-click menu.

Modify and Delete:

1. Select the frame or event with the bookmark to be edited.
2. Select *Add or Modify Bookmark* from the *Edit* menu on the Frame Display  , Event Display  , or the Protocol Navigator  . Or simply select the *Add or Modify Bookmark*  icon on one of the toolbars.
3. To modify a bookmark, change the comment in the dialog box and click OK.
4. To delete a bookmark, click the Delete button.

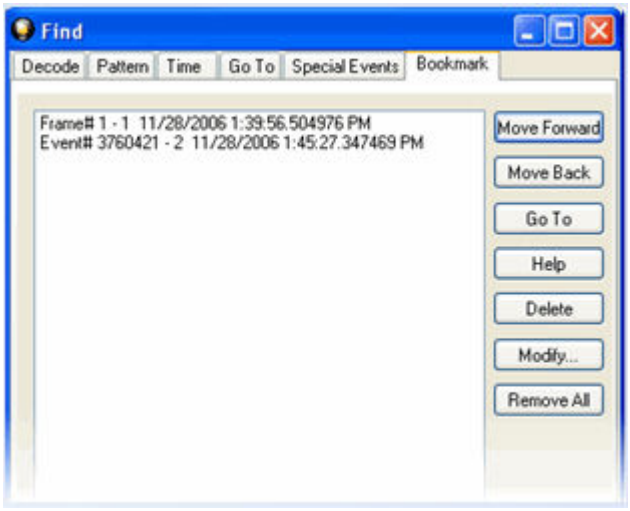
You can also modify or delete a bookmark by right-clicking on the frame and choosing Modify Bookmark from the right-click menu.

14.3 Displaying All and Moving Between Bookmarks

There are two ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.

2. Click the Display All Bookmarks icon  . Select the bookmark you want to move to and click the Go To button, or simply double-click on the bookmark. Click the Move Forward and Move Back buttons to cycle through the bookmarks.



- To delete a bookmark, select it and click the Delete button.
- To modify a bookmark, select it and click the Modify button.
- Click Remove All to delete all the bookmarks.

15 Filtering

15.1 Display Filters

A *display filter* looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Unlike an Ethernet capture filter, where data that does not match is thrown away, all the data is kept when using a display filter. The filter just displays a subset of the data. Multiple display filters can be used simultaneously, and different windows can be displaying data using different filters.

There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filters

Protocol Filters

Protocol filters test for the existence of a specific single layer. The system creates a protocol filter for each decoder that is loaded if that layer is encountered in a capture session.

There are also three special purpose filters that are treated as protocol filters:

- All Frames with Errors
- All Frames with Bookmarks
- All Special Information Nodes

Named Filters

- Named filters test for anything other than simple single layer existence. Named filters can be constructed that test for the existence of multiple layers, field values in layers, frame sizes, etc., as well as combinations of those things. Named filters are persistent across sessions.
- Named filters are user-defined. User-defined filters persist in a template file. User defined filters can be deleted.

Quick Filters

- Quick Filters are combinations of Protocol Filters and/or Named Filters that are displayed on the Quick Filter tab.
- Quick Filters cannot be saved and do not persist across sessions.
- Quick Filters are created on the Quick Filter Dialog or through filter selection on the Protocol Navigator.

15.1.1 Including and Excluding Radio Buttons

All filter dialog boxes contain an "Include" and an "Exclude" radio button. These buttons are mutually exclusive. The "Include/Exclude" selection becomes part of the filter definition, and appears as part of the filter description displayed to the right of the Toolbar.

Include:

A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

Exclude:

A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

15.1.2 Creating a Display Filter

There are two steps to using a display filter. Define the filter conditions, and then apply the filter to the data set. The system combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon  on either the *Protocol Navigator*  or the *Frame Display*  window or select *Apply/Modify Display Filters* from the *Filter* menu to open the *Set Condition* dialog box.
2. Select Include or Exclude to
3. Select the initial condition for the filter from the drop-down list.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the condition statement is complete.
5. Click *OK*. The system displays the *Save Named Condition* dialog. Provide a name for the filter condition or accept the default name provided by the system and click OK. Prohibited characters are left bracket '[', right bracket ']' and equal sign '='. The *Set Condition* dialog box closes, creates a tab on the *Frame Display* with the filter name, and applies the filter.

The filter appears in the Quick Filtering and Hiding Protocols dialog also.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

Notes:

The system requires naming and saving of all filters created by the user.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

15.1.3 Named Display Filters

You can create a unique display filter by selecting a data type on the Frame Display and using a right click menu. When you create a Name Filter, it appears in the Quick Filtering dialog, where you can use it do customize the data you see in the Frame Display panes.

1. Select a frame in the Frame Display Summary Pane.
2. Right click in the one of the data columns in the Summary Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.
3. Select Filter in (data type)

The Filtering Results dialog appears.

4. Enter a name for the filter
5. Select OK.

The filter you just created appears in the Named Filters section of the Quick Filtering dialog.

15.1.4 Using Compound Display Filters

Compound filters use Boolean logic to create complex and precise filters. There are three primary Boolean logic operators: AND, OR, and NOT.

The AND operator narrows the filter, the OR operator broadens the filter, and the NOT operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

There are two steps to using a compound filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon  on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the filter menu to open the *Set Condition* dialog box.
2. Click the *Advanced* button on the *Set Condition* dialog box.
3. Select the initial condition for the filter from the combo box.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.
5. Click the Plus icon  on the left side of the dialog box and repeat steps 3 and 4 for the next condition. Continue adding conditions until your filter is complete.
6. Include parentheses as needed and set the Boolean operators.

7. Click *OK*. The system displays the *Save Named Condition* dialog. Provide a name for the filter condition or accept the default name provided by the system and click *OK*. The *Set Condition* dialog box closes, creates a tab on the Frame Display with the filter name, and applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the Protocol Navigator and the Frame Display windows.

Note:

Use the *Up*  and *Down*  arrow icons on the left side of the dialog box to order your conditions, and the *Delete* button  to delete conditions from your filter.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

15.1.5 Defining Node and Conversation Filters

There are two steps to using Node and Conversation display filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon  on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the filter menu to open the *Set Condition* dialog box.
2. Choose "frames with the conversation" as the initial condition from the *Select* combo box.
3. Select an address type from the *Type* combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first *Address* combo box.
5. Choose a direction arrow from the *Direction* box. The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.
6. If you want to filter on just one node address, skip step 7 & 8, and continue with step 9.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select an address type for the second node address from the *Type* combo box.
8. Select a node address from the second *Address* combo box.
9. Click *OK*. The *Set Condition* dialog box closes and the analyzer applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

Note:

The *OK* button is unavailable (grayed out) until the condition selections are complete.

15.1.6 Using Advanced Display Filtering Techniques

Intermediate to advanced users, with a solid knowledge of filter definition and application may find it useful to create some of the more common filters "on the fly" using the advanced filtering techniques.

Choose one of the panes in either the *Frame Display* or *Protocol Navigator* windows:

1. Place the cursor over a parameter you wish to filter on such as a node address or protocol type, and right click.
2. A pop up menu appears with selections for filtering.
3. Select the filter.
4. The system either closes the menu and applies the filter, or displays the *Set Conditions* dialog box with the known parameters filled in and the additional options available to complete the conditions statement.

15.1.7 Deleting and Hiding Display Filters

15.1.7.1 The Difference Between Deleting and Hiding Display Filters

If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

Deleting a saved filter removes the filter from the current session and all subsequent sessions. In order to retrieve a deleted filter, the user must recreate it using the *Set Conditions* dialog.

Hiding a filter merely removes the filter from the display. A hidden filter can be reapplied using the Show/Hide procedure.

15.1.7.2 Deleting Saved Display Filters

1. Select *Delete Display Filters* from the *Filter* menu in either the *Protocol Navigator*  or the *Frame Display*  window to open the *Delete Named Condition* dialog. The system displays the *Delete Named Condition* dialog with a list of all user defined filters.
2. Select the filter to be deleted from the drop-down list.
3. Click the *Delete* button.
4. Click *OK*. The *Delete Named Condition* dialog box closes and the system deletes the filter.

15.1.7.3 Hiding/Revealing a Display Filter

1. Select "Hide/Show Display Filters" from the filter menu on either the *Protocol Navigator*  or the *Frame Display*  window to open the *Hide/Show* dialog. The system displays the *Hide/Show* dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.
3. Click the *Hide* button.
4. Click *OK*. The *Hide/Show* dialog box closes, and the system hides the filter and removes the filter tab from the *Frame Display*.

15.1.7.4 Revealing a Hidden Display Filter

There are several ways to reveal a hidden filter. One can open the *Quick Filter* dialog and check the box next to the hidden filter, or check the box next the hidden filter in the *Protocol Navigator* display.

Perform the following actions to reveal a hidden filter:

1. Select "Hide/Show Display Filters" from the filter menu in either the *Protocol Navigator*  or the *Frame Display*  window to open the *Hide/Show* dialog. The system displays the *Hide/Show* dialog with a list of all user defined filters.
2. Select the filter to be revealed from the combo box.
3. Click the *Show* button.
4. Click *OK*. The *Hide/Show* dialog box closes and the system reveals the filter and adds the filter tab to the *Frame Display*.

Note: When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

15.1.8 Editing Filters

15.1.8.1 Modifying a Condition in a Filter

1. Click the *Display Filters* icon  on either the *Protocol Navigator*  or the *Frame Display*  window or select "Apply/Modify Display Filters" from the *Filter* menu to open the *Set Condition* dialog box. The *Set Condition* dialog box displays the current filter definition. To display another filter, click the *Open* icon, and select the filter from the Popup list of all the saved filters.
2. Edit the desired parameter of the condition.
   Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.
3. Click *OK*. The system displays the *Save Named Condition* dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click *OK*. (If you choose to

create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click *OK*.) The *Set Condition* dialog box closes, and the system applies the modified filter.

Note:

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

15.1.8.2 Deleting a Condition in a Filter

1. Click the *Display Filters* icon  on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the *Filter* menu to open the *Set Condition* dialog box. The *Set Condition* dialog box displays the current filter definition. To display another filter, click the *Open* icon, and select the filter from the Popup list of all the saved filters.
2. Select the desired condition from the filter definition.
3. Click the Delete icon.
4. Edit the Boolean operators and parentheses as needed.
5. Click *OK*. The system displays the *Save Named Condition* dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click *OK*. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click *OK*.) The *Set Condition* dialog box closes, and the system applies the modified filter.

Note:

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

15.1.8.3 Renaming a Display Filter

1. Select "Rename Display Filters" from the *Filter* menu in either the *Protocol Navigator*  or the *Frame Display*  window to open the *Rename Filter* dialog. The system displays the *Rename Filter* dialog with a list of all user defined filters.
2. Select the filter to be renamed from the combo box.
3. Enter a new name for the filter in the text box.
4. Click *OK*. The *Rename Filter* dialog box closes and the system renames the filter.

15.2 Protocol Filtering from the Frame Display

15.2.1 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the *Summary* pane, and the second lets you filter on any protocol discovered on the network so far.

15.2.2 Filtering On the Summary Layer Protocol

To filter on the protocol in the *Summary* in the Frame Display window pane:

1. Select the tab of the desired protocol, or open the *Summary Layer* combo box.
2. Select the desired protocol.
3. To filter on a different layer, just select another tab, or change the layer selection in the combo box.

15.2.3 Quick Filtering on a Protocol Layer

1. To filter on any protocol layer, open either the *Frame Display* or *Protocol Navigator* window.
2. On the *Frame Display* window, click the starred *Quick Filtering* icon  or select "Quick Filtering" from the *Filter* menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

The box on the left is **Protocols To Filter In**.

- When you select the checkbox for a protocol in the **Protocols to Filter In**, the Summary Pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A Quick Filter tab then appears on the Frame Display labeled Quick Filter. Changing the filter definition on the Quick Filter dialog changes the filter applied on the Quick Filter tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**.

- When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the Decode, Binary, Radix, and Character Panes. The

frames containing that type data will still appear in the Summary Pane, but not in the Decode, Binary, Radix, and Character Panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs.

- When you select the checkbox for the Name Filters, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With **FBLEA**, the Configured BT Low energy devices and Exclude NULLSs and POLLs are default named filters.

3. Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.
4. Then click *OK*.

15.2.4 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

1. Open the *Frame Display*  window.
2. Click the starred *Quick Filter* icon  or select "Quick Filtering" from the *Filter* menu
3. Check the box for *All Frames With Errors* in the "Protocols to filter in" pane, and click *OK.*
4. The system creates a tab on the *Frame Display* labeled *Quick Filter* that displays the results of the *All Frames With Errors* filter.

15.3 Protocol Filtering from the Protocol Navigator

15.3.1 Filtering on a Protocol Layer

You can filter on one or more protocol layers. The filter is inclusive which means only frames matching the filter you select are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several.

On the left side of the Protocol Navigator window are three panes. The top pane is the Frames Filtered In pane. In the pane is a list of all the protocols seen so far on the circuit.

1. Check the boxes next to the names of the protocols you want to filter in.

The data on the right side of the screen matches the filtering selected.

Three additional filters available are:

- All Frames With Bookmarks - filters in all frames with a *bookmark* associated with them.
- All Frames With Errors - filters in all frames with errors.
- All Special Information Nodes - filters in all *special information nodes* .

15.3.2 Filtering on all Frames with Bookmarks

To filter on all frames with bookmarks:

1. Open the *Protocol Navigator*  window.
2. Check the *All Frames With Bookmarks* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

15.3.3 Filtering on all Frames with Errors from the Protocol Navigator

To filter on all frames with errors :

1. Open the *Protocol Navigator*  window.
2. Check the *All Frames With Errors* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

15.3.4 Filtering on all Frames with Special Information Nodes

To filter on all frames with special information nodes:

1. Open the Protocol Navigator  window.
2. Check the All Special Information Nodes box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

15.3.5 Named Filters

You can create, modify, and delete filters using the Filter menu items on the Protocol Navigator and Frame Display dialogs.

If you create a *Named* filter using the *Filters* dialog, the filter appears in the *Named Frame Filters* pane in the bottom left corner of the *Protocol Navigator* window.

1. Check the boxes next to the names of the filters you want to use.

Note that using a named filter affects the contents of the *Frame Display* window as well.

16 Saving Data

16.1 Saving Your Data

You can save all or part of a capture file. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.

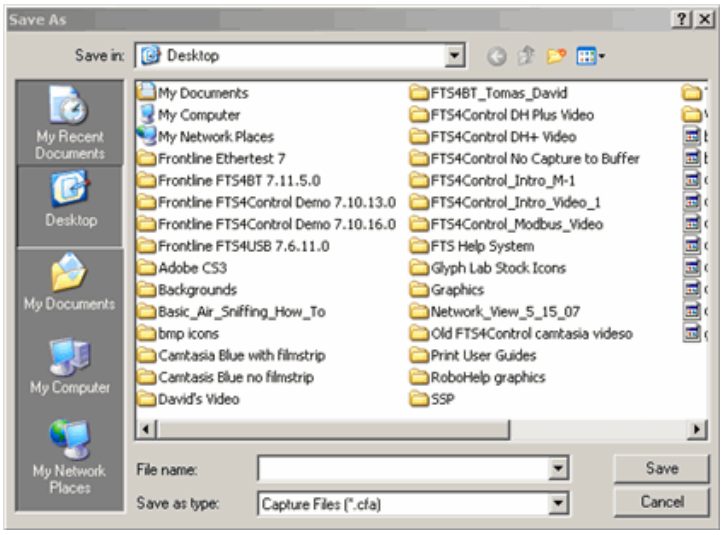
On the Control toolbar you can set up to capture a single file or series of files. Click here to see those settings.

There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data.

16.2 Saving the Entire Capture File using File > Save or the Save icon

This option is only available when you select Single File from the Capture Mode on System Settings. Click here to learn more about selecting Save options from System Settings.

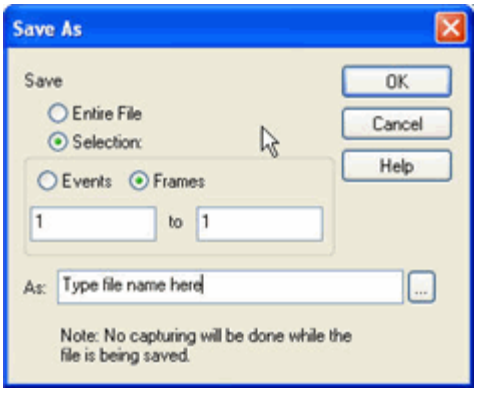
1. If you are capturing data, click on the *Stop* icon  to stop data capture. You cannot save data to file while it is being captured.
2. Open the *Event Display*  or *Frame Display*  window.
3. Click the *Save* icon, or select *Save* from the *File* menu.



4. Type a filename in the *File name* box at the bottom of the screen.
5. Browse to select a specific directory. Otherwise your file is saved in the default capture file directory.
6. When you are finished, click *OK*.

16.3 Saving the Entire Capture File with Save Selection

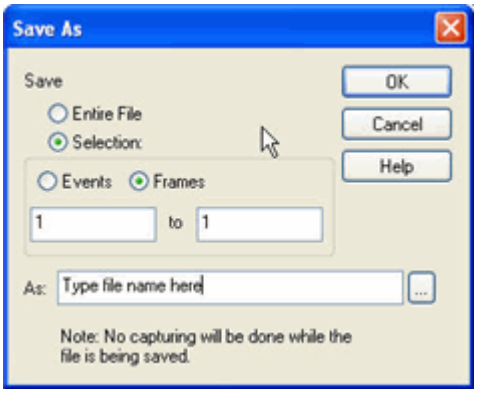
1. If you are capturing data, click on the *Stop* icon  to stop data capture. You cannot save data to file while it is being captured.
2. Open the *Event Display*  or *Frame Display*  window.
3. Right click in the data
4. Select *Save Selection* or *Save As* from the right click menu



1. Click on the radio button labeled *Entire File*.
2. Choose to save *Events* or *Frames.* Choosing to save *Events* saves the entire contents of the capture file. Choosing to save *Frames* does not save all events in the capture file.
3. Type a filename in the *Save As* box at the bottom of the screen. Click the *Browse* icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
4. When you are finished, click *OK*.

16.4 Saving a Portion of a Capture File

1. If you are capturing data, click on the *Stop* icon  to pause data capture. You cannot save data to a file while it is being captured.
2. Open the *Event Display*  or *Frame Display* window  , depending on whether you want to specify a range in bytes or in frames.
3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range, or use the Shift key with the keyboard arrows or the navigation icons in the Frame Display toolbar. If the range you want to save is too large to select, note the numbers of the first and last item in the range.
4. Right click in the data
5. Select *Save Selection* or *Save As* from the right click menu



6. Click on the radio button labeled *Selection*. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes.
7. Select either *Events* or *Frames* to indicate whether the numbers are event or frame numbers.
8. Type a filename in the *Save As* box at the bottom of the screen. Click the *Browse* icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
9. Click *OK* when you are finished.

16.5 Confirm Capture File (CFA) Changes

This dialog appears when you close a capture file after changing the Notes, the protocol stack, or bookmarks. The dialog lists information that was added or changed and allows you to select which information to save, and whether to save it to the current file or to a new one.

Changes made to the file appear in a list in the left pane. You can click on each item to see details in the right pane about what was changed for each item. You simply check the boxes next to the changes you want to keep. Once you decide what changes to keep, select one of the following:

- Save To This File – Saves the changes you have made to the current capture file.
- Save As – Saves the changes to a new file.
- Cancel the Close Operation – Closes the file and returns you back to the display. No changes are saved.
- Discard Changes – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

16.6 Adding Comments to a Capture File

The *Notes* feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the Notes window :

1. Click the Show Notes icon  . This icon is present on the toolbars of the *Frame Display*  , the *Protocol Navigator*  , as well as the *Event Display*  . *Notes* can be selected from the *Edit* menu on one of these windows.
2. Type your comments in the large edit box on the Notes window. The Cut, Copy, Paste, Undo and Redo features are all supported.
3. Click the thumbtack icon  to keep the Notes window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

17 Loading and Importing Capture Files

17.1 Loading a Capture File

From the Control Window:

1. Go to the File menu.
2. Choose a file from the recently used file list.
3. If the file is not in the File menu list, select *Open Capture File* from the File menu or simply click on the *Open* icon  on the Toolbar.
4. Capture files have a .cfa extension. Browse if necessary to find your capture file.
5. Click on your file, and then click Open.

17.2 Importing Capture Files

1. From the Control Window  , go to the File menu and select *Open Capture File* or click on the *Open* icon on the Toolbar.
2. Change the Files of Type box to All Importable File Types or All Supported File Types. Select the file and click Open.

The analyzer automatically converts the file to the analyzer's format while keeping the original file in its original format. You can save the file in the analyzer's format, close the file without saving it in the analyzer's format, or have the analyzer automatically save the file in the analyzer's format (see the System Settings to set this option). All of these options keep your original file untouched.

When you first open the file, the analyzer brings up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for the analyzer to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

At present, the analyzer supports the following file types:

- **Frontline Serialtest* Async and Serialtest ComProbe® for DOS** – requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- **Greenleaf ViewComm* 3.0 for DOS** - requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- **Frontline Ethertest* for DOS** – requires 3 files: filename.cap, filename.ca0 and filename.ca1.
- **Sniffer Type 1** – supports files with the .enc extension. Does not support Sniffer files with a .cap extension.
- **Snoop or Sun Snoop** – files with a .cap extension based on RFC 1761. For file format, see http://www.faqs.org/rfcs/rfc1761.html.

- **Shomiti Surveyor files in Snoop format** – files with a .cap extension. For file format, contact Technical Support.
- **CATC Merlin** - files with a .csv extension. Files must be exported with a specific format. See File Format for Merlin Files for information.
- **CATC Chief** - files with a .txt extension.

17.3 Converting Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. The analyzer always uses Greenwich Mean Time (also known as Universal Time Coordinates).

When importing a Serialtest for DOS file, the analyzer must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for the analyzer to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

17.4 Adding Comments to a Capture File

The *Notes* feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the Notes window :

1. Click the Show Notes icon  . This icon is present on the toolbars of the *Frame Display*  , the *Protocol Navigator*  , as well as the *Event Display*  . *Notes* can be selected from the *Edit* menu on one of these windows.
2. Type your comments in the large edit box on the Notes window. The Cut, Copy, Paste, Undo and Redo features are all supported.
3. Click the thumbtack icon  to keep the Notes window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

17.5 File Format for Merlin Files

FTS imports Merlin's export files that have been exported with Merlin's default settings. These files should have an extension of ".csv".

It is possible with the Merlin software to hide or change a field's format. If you do this before exporting the Merlin file then FTS may have trouble importing the file.

If you are experiencing problems importing Merlin files, then check to make sure that no fields were hidden and that the default field formats were being used, when the file was exported from Merlin.

18 Printing

18.1 Printing from the Frame Display/HTML Export

The Frame Display Print dialog and the Frame Display HTML Export are very similar. This topic discusses both dialogs.

The **Frame Display Print** dialog is directly below. The **Frame Display HTML Export** is located midway in this discussion.

About Frame Display Print

The Frame Display Print feature provides the user with the option to print the entire capture buffer or the current selection. When *Print Preview* is selected, the output displays in a browser print preview window, where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

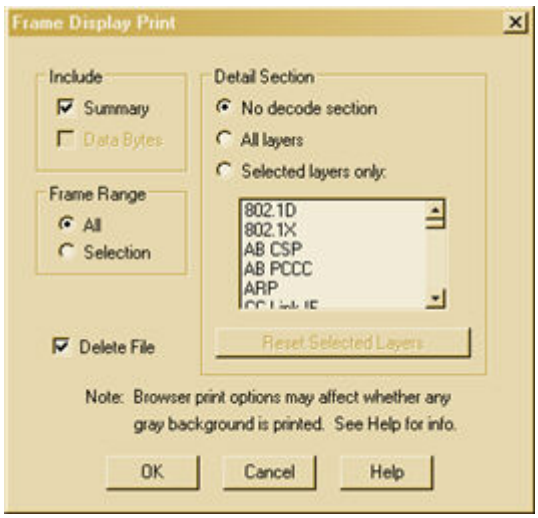
Configure the Print File Range in the Frame Display Print Dialog

Selecting more than one frame in the Frame Display window defaults the radio button in the Frame Display Print dialog to *Selection* and allows the user to choose the *All* radio button. When only one frame is selected, the *All* radio button in the Frame Display Print dialog is selected.

How to Print Frame Display Data

1. Select *Print* or *Print Preview* from the *File* menu on the Frame Display window to display the Frame Display Print dialog. Select *Print* if you just want to print your data to your default printer. Select *Print Preview* if you want access to printer options.
2. Choose to include the Summary Pane (check the box) in the print output. The summary Pane appears at the beginning of the printed output in tabular format. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.

CAUTION: Decode layers printout expanded regardless of the state of the Detail Pane in the Frame Display at the time of the request to print. This can produce a print output consisting of hundreds of pages or more. We recommend that you use *Print Preview* to determine the number of pages in your print output prior to printing.



Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

Choosing *All* prints all of the frames in the capture file or buffer. If more than 1000 frames in the Frame Range, All will be disabled. You can still select more than 1000 frames using the Selection option, but when printing more than 1000 frames, there is the possibility that Print will not work properly.

Choosing *Selection* prints only the frames you select in the Frame Display window.

Note: Selecting the **Delete File** deletes the temporary html file that was used during printing..

4. Click the OK button.

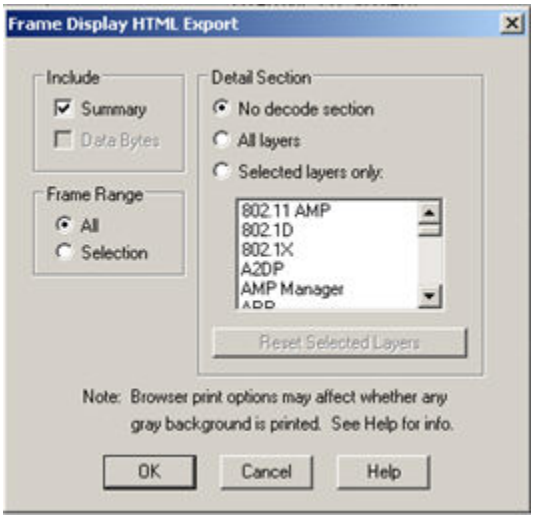
If you chose *Print Preview*, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

18.2 Frame Display HTML Export

The Frame Display **HTML Export** feature provides the user with the option to export the entire capture buffer to an .html file.

How to export display data to an .html file

1. Select *HTML Export* from the *File* menu on the Frame Display window to display the **Frame Display HTML Export**.



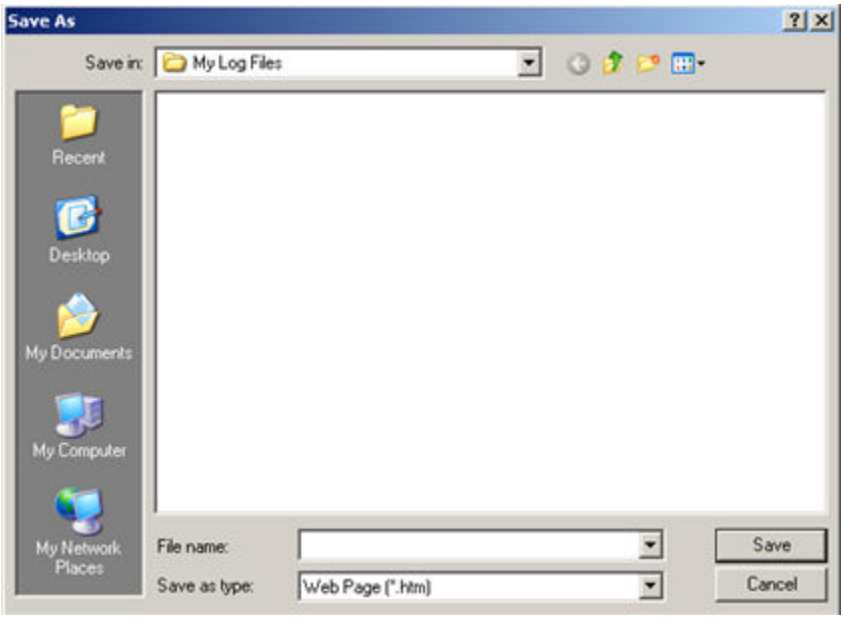
2. Choose to include the Summary Pane (check the box) in the .html output. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.
4. Select the range of frames to include *All* or *Selection* in the Frame Range section of the dialog.

   Choosing *Selection* includes only the frames you select in the Frame Display window.

Note: If the file size is too big, the Frame Range, **All**, will not be available. It will be grayed out.

5. Click the OK button.

The *Save As* dialog appears.



6. Enter a name for the file you want to save.

Note: There is no need to choose a file type. The file is saved as a .htm.

7. Select Save

The file is saved as a .htm file in the file location you chose.

18.3 Printing from the Event Display

About Event Display Print

The Event Display Print feature provides the user with the option to print either the entire capture buffer or the current selection. When *Print Preview* is selected, the output displays in a browser print preview window where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

The Event Display Print feature uses the current format of the Event Display as specified by the user.

Note: See About Event Display for an explanation on formatting the Event Display prior to initiating the print feature.

Configure the Print File Range in the Event Display Print Dialog

Selecting more than one event in the Event Display window defaults the radio button in the Event Display Print dialog to Selection and allows the user to choose the All radio button. When only one event is selected (can't have None selected), the *All* radio button in the Event Display Print dialog is selected.

How to Print Event Display Data to a Browser

1. Select *Print* or *Print Preview* from the *File* menu on the Event Display window to display the Event Display Print dialog. Select *Print* if you just want to print your data to your default printer. Select *Print Preview* if you want access to printer options.
2. Select the range of events to include from either *All* or *Selection* in the Event Range section of the Event Display Print dialog. Choosing *All* prints all of the events in the capture file or buffer. Choosing *Selection* prints only the selected events in the Event Display window.

   Note: In order to prevent a Print crash, you cannot select* All *if there are more than 100,000 events in the capture buffer.

Note: See Configure the Print File Range in the Event Display Print Dialog above for an explanation of these selections

3. Click the OK button.

If you chose *Print Preview*, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

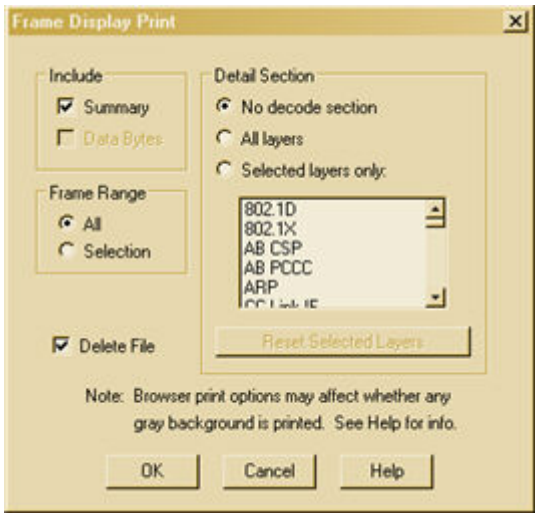
18.4 Print Preview

Print Preview gives a preview of how the data looks printed. You can scroll through the pages and zoom in on the data to get a closer look. The line of buttons across the top of the window controls the functions of the window.

To open the Print Preview window:

1. Choose Print Preview from the File menu in any window that supports printing.
2. Choose to include the Summary Pane (check the box) in the print output. The summary Pane appears at the beginning of the printed output in tabular format. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.

CAUTION: Decode layers printout expanded regardless of the state of the Detail Pane in the Frame Display at the time of the request to print. This can produce a print output consisting of hundreds of pages or more. We recommend that you use *Print Preview* to determine the number of pages in your print output prior to printing.



4. Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

   Choosing *All* prints all of the frames in the capture file or buffer. If there are more than 1000 frames in the capture file or buffer, **All** will not be available.

   Choosing *Selection* prints only the selected frames in the Frame Display window.

Note: See Configure the Print File Range in the Frame Display Print Dialog above for an explanation of these selections.

Note: Selecting the **Delete File** deletes the temporary html file that was used during printing..

5. Click the OK button.

You can print directly from the Print Preview window.

- Next Page shows you how the next page in your data looks
- Prev Page takes you back to the previous page.
- Two Page changes the display to show two pages of data. When in the Two Page display, the button reads One Page. Click on the One Page button to return to viewing one page.
- Zoom In and Zoom Out allow you to change the magnification of the pages. Click on Zoom In to increase the magnification, and on Zoom Out to decrease the magnification. When you have reached the limit in either direction, the buttons is grayed out.
- You can also zoom in and out by clicking on the page itself. When the cursor looks like a magnifying glass, you can click on the page to increase the magnification. When you have reached the top level of magnification, the cursor changes back to an arrow. Click on the page to return to normal magnification.
- Click on the Close button to return to the regular display.

19 Exporting

19.1 Export

You can dump the contents of the Summary pane on the Frame Display into a Comma Separated File (CSV).

To access this feature:

1. Right click on the Summary Pane
2. Select the Export menu item
3. Enter a file name
4. Select Save

Another option to access quick export is :

1. Click on the File menu
2. Choose Export
3. Enter a file name
4. Select Save

19.2 Export Filter Out

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the Filter Out box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Non-printable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the non-printable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between $20 and $7e.

19.3 Exporting Event Display to a File

About Event Display Export

The Event Display Export feature provides the following options:

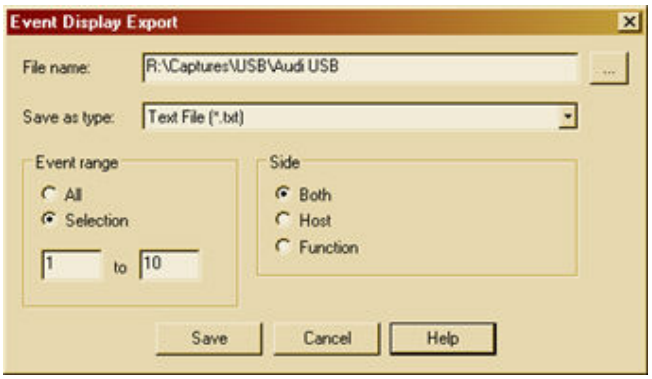
- Export either the entire capture buffer or the current selection
- Output file format as text, CSV, html, or bin.

The Event Display Export feature uses the current format of the Event Display as specified by the user.

Note: See About Event Display for an explanation on formatting the Event Display prior to initiating the export feature.

Accessing the Event Display Export Dialog

Selecting Export Events… from the File menu in the Event Display brings up the following dialog:



Configure the Export File Range in the Event Display Export Dialog

- Selecting more than one event in the Event Display window defaults the radio button in the Event Display Export dialog to Selection and allows the user to choose the All radio button.
- When only one event is selected (something must be selected), the All radio button in the Event Display Export dialog is selected by default.
- Side is used to determine whether you want to export data from a DCE/DTE, Slave/Master, Host/Function device or both.

How to Export Event Display Data to a File

1. Select Export Events… from the File menu on the Event Display window to display the Event Display Export dialog.

2. Enter a file path and name, or click the browser button to display the Windows Save As dialog and navigate to the desired storage location.
3. Select a file type from the Save as type: drop-down List Menu on the Event Display Export dialog.
4. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

   Binary File (*.bin)

5. Select the range of events to include in the file from either All or Selection in the Event Range section of the Event Display Export dialog.
   Note: See Configure the Export File Range in the Event Display Export Dialog above for an explanation of these selections.
6. Select a Side, either Host, Function, or Both
7. Click Save.

19.4 Exporting Baudot

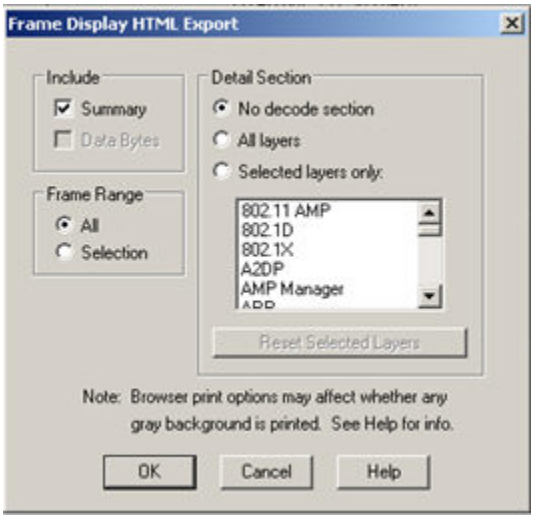
When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field shows letters and vice versa.

19.5 HTML Export

The Frame Display **HTML Export** feature provides the user with the option to export the entire capture buffer to an .html file.

How to export display data to an .html file

1. Select *HTML Export* from the *File* menu on the Frame Display window to display the **Frame Display HTML Export**.



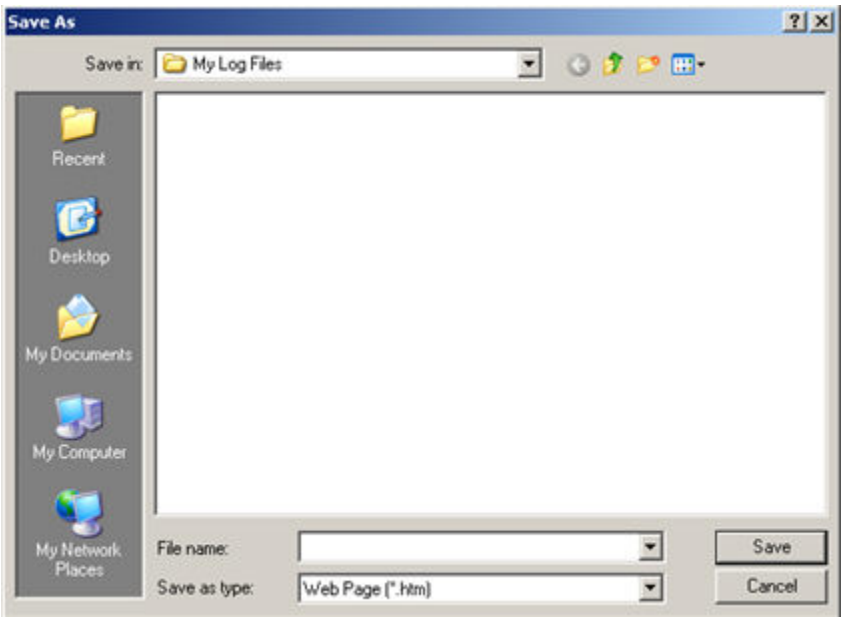
2. Choose to include the Summary Pane (check the box) in the .html output. If you select All layers in the Detail Section, the Data Bytes option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the Reset button to de-select all selected layers.
4. Select the range of frames to include All or Selection in the Frame Range section of the dialog.

Choosing *Selection* includes only the frames you select in the Frame Display window.

Note: If the file size is too big, the Frame Range, **All**, will not be available. It will be grayed out.

5. Click the OK button.

The *Save As* dialog appears.



6. Enter a name for the file you want to save.

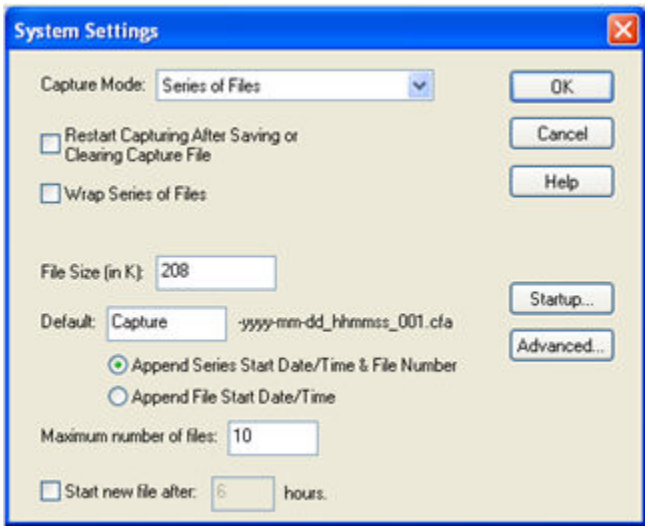
Note: There is not need to choose a file type. The file is saved as a .htm.

7. Select Save

20 System Settings and Program Options

20.1 System Settings

Open the System Settings window by choosing System Settings from the Options menu on the Control window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.



Capture Mode

- **Series of files**

  This option lets you capture to a series of files. The size of each file is no larger than the number given in File Size (in K),which has a maximum limit of approximately 176,000KB (1.7 GB) or 1/2 of the available hard disk space, whichever is **smaller**. The name of each file is the name you give it in the Name box followed by the date, time and a number. The date and time are when the series was opened. The number increments with each file. This guarantees unique file names are created.

  Set the maximum number of files in the series in the **Maximum number of files** box. The next file starts when the currently open file is full. If you want to start a new file on a periodic basis, check the box for **Start new file after** and put in the number of hours after which a new file is started. Note that if the currently open file becomes full before the time limit has been reached, a new file is opened immediately rather than lose data.

  Capturing stops if the maximum number of files has been used unless Wrap Files has been checked. If Wrap Files has been checked the analyzer erases the oldest file in the series and make a new file.

- **Single File**

This option allows the analyzer to capture data to a file without prompting you for a file name each time. The size of each file is not larger than the number given in File Size (in K). The name of each file is the name you give it in the Name box followed by the date and time. The date and time are when the series was opened.

Common Options

- **Restart Capturing After Saving or Clearing Capture File**

  If the Automatically Restart feature is enabled, the analyzer restarts capture to the file immediately after the file is closed.

- **Wrap File**

  When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.

- **File Size (in K)**

  Enter the maximum size of the capture file, which is 176,000 KB, or 1/2 of the available hard drive space, whichever is **smaller**. If you enter a number larger than the maximum allowable size, the analyzer will display the allowable size.

- **Default**
  Enter a name for the capture file in the Default text box. Each saved file will begin with this name.

- **Append Series Start/Date & File Number**
  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) and file number (001) when capturing a series of files.

- **Append File Start Date/Time**
  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) when capturing a single file.

- **Start up**

  Opens the Program Start up Options window. Start up options let you choose whether to start data capture immediately on opening the analyzer.

- Advanced

  Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

20.2 System Settings - Disabled/Enabled Options

Some of the **System Settings** options are disabled depending upon the status of the data capture session.

- As the default, all the options on the System Settings dialog are enabled.
- Once the user begins to capture data by selecting the Start Capture button, some of the options on the System Settings dialog are disabled until the user stops data capture and either saves or erases the captured data.
- The user can go into the Startup Options and Advanced System Options on the System Settings dialog and make changes to the settings at any time.

20.3 Bluetooth ComProbe Maintenance

The Bluetooth® ComProbe® Maintenance Utility is used to configure Bluetooth ComProbes and to upgrade the firmware. Bluetooth ComProbes should be upgraded to the newest firmware release to take advantage of new features and fixes.

Upgrading Your Bluetooth ComProbe

To start the Bluetooth ComProbe Maintenance Utility:

1. Open the FTS4BT desktop folder > Setup folder.
2. Double click the shortcut to the utility.

OR

1. From your Windows operating system click Start > Programs > FTS4BT [version#] > Setup > Bluetooth ComProbe Maintenance Utility.

The main dialog appears.

2. Connect the **ComProbe** to the PC
3. Click on the **Select Device** button.

To avoid mistakes, we recommended that only one ComProbe be connected at a time. Also, it is very important that you do not remove any connections to the ComProbe while the firmware update is in progress!

4. Select **Yes.**

Older ComProbes will display an error indicating the ComProbe is older and needs replacing. Note that when you do this, the [Device Information], [Check Configuration] and [Update Firmware] buttons should become available. [Update Firmware] will not be accessible if you are using an older ComProbe®.

5. Select the **Update Firmware** button.

The utility will display a dialog titled "Select the firmware file to download". There may be more than one firmware file with extension ".dfu" in the directory. The version number of the firmware will be in the name of the file.

6. Please **select the version you want** (typically you should choose the highest version number).
7. Then press the **Open** button.

When the update is complete, a dialog appears confirming the download.

8. Press the **OK** button.

20.4 Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box.

Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of the analyzer, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options:

1. Go to the Control  window.
2. Choose *System Settings* from the *Options* menu.
3. On the System Settings window, click the *Advanced* button.

- **Driver Receive Buffer Size in Kbytes**

  This is the size of the buffer used by the driver to store incoming data. This value is expressed in Kbytes.

- **Driver Action Queue Size In Operating System Pages**

  This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages.

- **Frame Completion Timeout in Seconds**

  This is the number of seconds that the analyzer waits to receive data on a side while in the midst of receiving a frame on that side.

If no data comes in on that side for longer than the specified number of seconds, an "aborted frame" event is added to the Event Display and the analyzer resumes decoding incoming data. This can occur when capturing interwoven data (DTE and DCE) and one side stops transmitting in the middle of a frame.

Aborted frames (just like broken frames and regular frames) are decoded and displayed in the Frame Display. If you experience aborted frames and suspect that your framed data may have pauses in it that exceed the specified timeout time, then you may want to increase that value.

The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

20.5 Changing Default File Locations

The analyzer saves user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. These locations are set at installation.

Follow the steps below to change the default locations.

1. Choose Directories from the Options menu on the Control  window to open the File Locations window.
2. Select the default location you wish to change.
3. Click Modify.
4. Browse to a new location.
5. Click OK.
6. Click OK when finished.

Note: If a user sets the **My Decoders** directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch FTS. For example, if an FTS product is installed at **C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z**, then "My Decoders" cannot be set to any of the following:

- C:\
- C:\FTS Stuff
- C:\FTS Stuff\My Products
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data\Decoders

- or to any directory that already exists under C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data\Decoders

Default Capture File Folder Checkbox

If the "Use Last Opened Folder for Capture Files" checkbox is checked, then the system automatically changes the default location for saving capture files each time you open a file from or save a file to a new location. For example, let's say the **default** location for saving capture files is **Drive A > Folder A**. Now you select the "Use Last Opened Folder for Capture Files" checkbox. The next time, however, you open a capture file from a different location, **Folder B > Removable Flash Drive**. Now when you save the capture file, it will be saved to **Folder B > Removable Flash Drive**. Also, all subsequent files will be saved to that location. This remains true until you open a file from or save a file to a different location.

There is one caveat to this scenario, however. Let's say you have selected "Use Last Opened Folder for Capture Files" and opened a file from a location other than the default directory. All subsequent capture files will be saved to that location. Suppose, however, the next time you want to save a capture file, the new file location is not available because the directory structure has changed: a folder has been moved, a drive has been reassigned, a flash drive has been disconnected, etc. In the case of a "lost" directory structure, subsequent capture files will be saved to the default location. FTS will always try to save a file to the folder where the last file was opened from or saved to, if "Use Last Opened Folder for Capture Files" is checked. If, however, the location is not accessible, files are saved to the default directory that is set at installation.

If the checkbox is unchecked, then the system always defaults to the directory listed in the File Locations dialog.

20.6 Selecting Start Up Options

1. To open this window:
2. Choose *System Settings* from the *Options* menu on the Control  window.
3. On the System Settings window, click the *Start Up* button.
4. Choose one of the options to determine if the analyzer starts data capture immediately on starting up or not.

Don't start capturing immediately.

This is the default setting. The analyzer begins monitoring data but does not begin capturing data until the *Start Capture*  icon on the Control, Event Display or Frame Display windows is clicked.

Start capturing to a file immediately.

When the analyzer starts up, it immediately opens a capture file and begin data capture to it. This is the equivalent of clicking the *Start Capture*  icon. The file is given a name based on the settings for capturing to a file or series of files in the System Settings window.

Start capturing immediately to the following file:

Enter a filename in the box below this option. When the analyzer starts up, it immediately begins data capture to that file. If the file already exists, the data in it is overwritten.

Use this capture filter:

The drop down box lists all named filters. Select one that you want to use immediately on start up.

20.7 Names

The Names dialog is used to change the names of objects and events that appear in various displays.

1. To open the Names dialog, choose *Names* from the *Options* menu on the Control window. Changes to the Names are used throughout the program.

To change a name, click on the name given in the current column, and then click again to modify the name (a slow double-click). To restore the default values, click the Defaults button. The names used in the system fall into one of three general categories.

Because of variations associated with different types of communications, the Names dialog may display all or only a subset of the following categories:

- **Sides**

  The Sides section allows you to give each side on a network more descriptive names. This is useful on network with more than one side.

- **Errors**

  This section allows you to change the error names. The errors listed are appropriate for the type of circuit/network you are monitoring.

- **Signals**

  Signals refers to the six control signals used in RS-232 data communications, and may not apply to the type of communications you are monitoring.

  FTS4USB has four Control Signals: Pin 1, Pin 2, Pin 3, and Pin 4.

  Default Labels and their Meaning

Label	Control Signal
RTS	Request to Send
CTS	Clear to Send

DSR Data Set Ready

DTR Data Terminal Ready

CD Carrier Detect

RI Ring Indicator

If you are used to different abbreviations for the same signals, you can change them in this section. For example, if you normally refer to Carrier Detect as DCD, highlight CD and type in DCD.

20.8 Timestamping

20.8.1 Timestamping Options

The Timestamping Options window allows you to enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.

To open this window:

1. Choose *System Settings* from the *Options* menu on the Control window.
2. Click the *Set Timestamp Format* button.

OR

1. Click the Timestamping Options icon from either the Event Display or Statistics window.

OR

1. Click the Timestamping Options icon from the Event Display window.

20.8.2 Enabling/Disabling Timestamping

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Statistics  window.
2. Check the *Store Timestamps* box to enable timestamping. Remove the check to disable timestamping. If you disable timestamping, you are not able to do delta or rate calculations.

20.8.3 Switching Between Relative and Absolute Time

With Timestamping you can choose to employ Relative Time or Absolute time.

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Statistics  window.
2. Go to the *Display Options* section at the bottom of the window and find the *Display Relative Timestamps* checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

Note: The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

- *Display Raw Timestamp Value* shows the timestamp as the **total time in hundred nanoseconds** from a specific point in time.
- *Display Relative Timestamps* shows the timestamp as the **amount of time that has passed since the first byte was captured**. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.
- *Selecting both values* displays the **total time in nanoseconds from the start of the capture** as opposed to a specific point in time.
- *Selecting neither value* displays the **actual chronological time**.

When you select Relative Timestamp, you can set the number of digits to display using the up or down arrows on the numeric list.

20.8.4 Changing the Timestamping Resolution

This option affects the resolution of the timestamp stored in the capture file. The default timestamp is 10 milliseconds. This value is determined by the operating system and is the smallest "normal" resolutions possible.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked by an asterisk as high resolution in the drop down list. To change timestamping resolutions:

1. Choose *System Settings* from the *Options* menu on the Control  window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Statistics  window.

2. Go to the *Capture Options* section of the window.
3. Change the resolution listed in the *Storage Resolution* box. Note that if you change the resolution, you need to exit the analyzer and restart in order for the change to take effect.

20.8.5 Displaying Fractions of a Second

1. Choose *System Settings* from the *Options* menu on the Control  window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Statistics  window.
2. Go to the *Display Options* section at the bottom of the window, and find the *Number of Digits to Display* box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

The options in this section affect only how the timestamps are displayed on the screen, not the resolution used to capture the data.

20.8.6 Converting Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. The analyzer always uses Greenwich Mean Time (also known as Universal Time Coordinates).

When importing a Serialtest for DOS file, the analyzer must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for the analyzer to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

20.8.7 Performance Issues For High Resolution Timestamps

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions. The second issue is that using high resolution timestamping may affect performance on slower machines

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file has more data events in it, because less room is used to store timestamps.

You can increase the size of your capture file in the System Settings.

21 Technical Information

21.1 Contacting Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

On the Web: http://www.fte.com/support/default.asp

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

21.2 Technical Information

The following information is provided to assist you with troubleshooting problems with this analyzer.

Performance Notes

Ethernet Performance Notes

Synchronous Serial Performance Notes

Asynchronous Serial Performance Notes

Ring Indicator

The FTS Serial Driver

Contacting Technical Support

Contacting Technical Support

Miscellaneous Helpful Information

ASCII Codes

EBCDIC Codes

Baudot Codes

Communication Control Characters

21.3 Performance Notes

As a software-based product, the speed of your computer's processor affects the analyzer's performance. Buffer overflow errors are an indicator that the analyzer is unable to keep up with the data. The information below describes what happens to the data as it arrives, what the error means, and how various aspects of the analyzer affect performance. Also included are suggestions on how to improve performance.

The analyzer's driver takes data from the driver and counts each byte as they are put into the driver's buffer. The analyzer's driver tells the user interface that data is ready to be processed. The analyzer takes the data from the driver's buffer and puts the data into the capture buffer.

Driver Buffer Overflows occur when the user interface does not retrieve frames from the driver quickly enough. Buffer overflows are indicated in the Event Display window by a plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost.

There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by the analyzer. (Ethernet Only)
- Close all other programs that are doing work while the analyzer is running. Refrain from doing searches in the Event Display window or other processor intensive activities while the analyzer is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the file. Try turning off timestamping from the Timestamping Options window.
- For Driver Buffer Overflows, change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value Driver Receive Buffer Size in Operating System Pages. Take the number listed there and double it.
- The analyzer's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause the analyzer to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. The analyzer can capture data with no windows other than the Control window open.
- If you are still experiencing buffer overflows after trying all of the above options, then you need to use a faster PC.

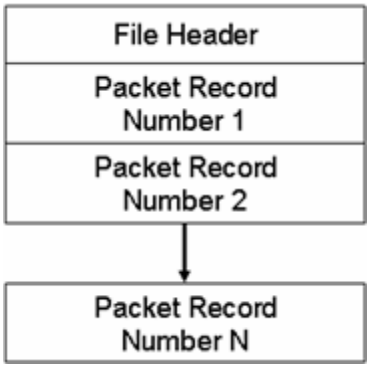
21.4 BT Snoop File Format

Overview

The BT Snoop file format is suitable for storing *Bluetooth*® HCI traffic. It closely resembles the snoop format, as documented in RFC 1761.

File Format

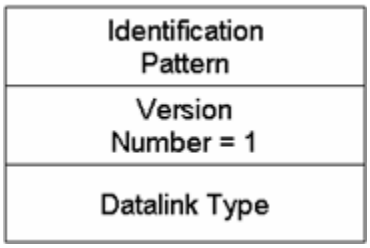
The snoop packet capture file is an array of octets structured as follows:



The File Header is a fixed-length field containing general information about the packet file and the format of the packet records it contains. One or more variable-length Packet Record fields follow the File Header field. Each Packet Record field holds the data of one captured packet.

File Header

The structure of the File Header is as follows:



Identification Pattern:

A 64-bit (8 octet) pattern used to identify the file as a snoop packet capture file. The Identification Pattern consists of the 8 hexadecimal octets:

62 74 73 6E 6F 6F 70 00

This is the ASCII string "btsnoop" followed by one null octets.

Version Number:

A 32-bit (4 octet) unsigned integer value representing the version of the packet capture file being used. This document describes version number 1.

Datalink Type:

A 32-bit (4 octet) field identifying the type of datalink header used in the packet records that follow. The datalink type codes are listed in the table below. Values 0 - 1000 are reserved, to maximize compatibility with the RFC1761 snoop version 2 format.

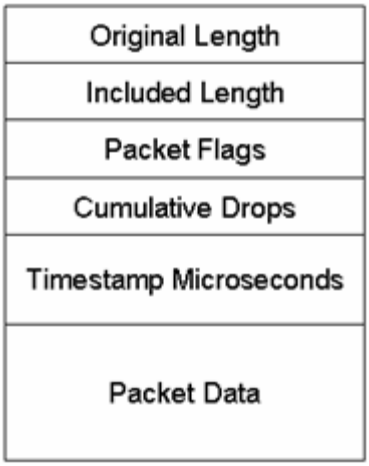
Datalink Type	Code
Reserved	0 - 1000
Un-encapsulated HCI (H1)	1001
HCI UART (H4)	1002
HCI BCSP	1003
HCI Serial (H5)	1004
Unassigned	1005 – 4294967295

Packet Record Format

Each packet record holds a partial or complete copy of one packet as well as some descriptive information about that packet. The packet may be truncated in order to limit the amount of data to be stored in the packet file.

Each packet record holds 24 octets of descriptive information about the packet, followed by the packet data, which is variable-length, and an optional pad field. The descriptive information is structured as six 32-bit (4-octet) integer values.

The structure of the packet record is as follows:



Original Length

A 32-bit unsigned integer representing the length in octets of the captured packet as received via a network.

Included Length

A 32-bit unsigned integer representing the length of the Packet Data field. This is the number of octets of the captured packet that are included in this packet record. If the received packet was truncated, the Included Length field is less than the Original Length field.

Packet Flags

Flags specific to this packet. Currently the following flags are defined:

Bit no	Definition
0	Direction flag. 0 = Sent; 1 = Received
1	Command flag. 0 = Data; 1 = Command/Event
2 – 31	Reserved.

Bit 0 is the least significant bit of the 32-bit word.

Direction is relative to host / DTE. i.e. for *Bluetooth* controllers, Send is Host->Controller, Receive is Controller->Host.

Note: Some Datalink Types already encode some or all of this information within the Packet Data. With these Datalink Types, these flags should be treated as informational only, and the value in the Packet Data should take precedence.

Cumulative Drops

A 32-bit unsigned integer representing the number of packets that were lost by the system that created the packet file between the first packet record in the file and this one. Packets may be lost because of insufficient resources in the capturing system, or for other reasons.

Note: some implementations lack the ability to count dropped packets. Those implementations may set the cumulative drops value to zero.

Timestamp Microseconds

A 64-bit signed integer representing the time of packet arrival, in microseconds since midnight, January 1st, 0 AD nominal Gregorian.

In order to avoid leap-day ambiguity in calculations, note that an equivalent epoch may be used of midnight, January 1st 2000 AD, which is represented in this field as 0x00E03AB44A676000.

Packet Data

Variable-length field holding the packet that was captured, beginning with its datalink header. The Datalink Type field of the file header can be used to determine how to decode the datalink header. The length of the Packet Data field is given in the Included Length field.

Note that the length of this field in not necessarily rounded to any particular multi-octet boundary, as might otherwise be suggested by the diagram.

Data Format

All integer values are stored in "big-endian" order, with the high-order bits first.

21.5 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the Event Display. The first selected byte appears on the third line of the display.

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\Program Files\Common Files\FTE)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

21.6 Progress Bars

The analyzer uses progress bars to indicate the progress of a number of different processes. Some progress bars (such as the filtering progress bar) remain visible, while others are hidden.

The title on the progress bar indicates the process underway.

21.7 Event Numbering

This section talks about how events are numbered when they are first captured and how this affects the display windows in the analyzer. The information in this section applies to frame numbering as well.

When the analyzer captures an *event*, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are *wrapped* out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague's file use the same event numbers that your file does.

21.8 File Format for Merlin Files

FTS imports Merlin's export files that have been exported with Merlin's default settings. These files should have an extension of ".csv".

It is possible with the Merlin software to hide or change a field's format. If you do this before exporting the Merlin file then FTS may have trouble importing the file.

If you are experiencing problems importing Merlin files, then check to make sure that no fields were hidden and that the default field formats were being used, when the file was exported from Merlin.

21.9 Flag and Sync Character Subtleties

The chip used by the ComProbe® hides some details relating to HDLC/SDLC flags (hex 7e) and the sync character in Bisync and Monosync.

In HDLC and SDLC, the analyzer does not know how many flag characters were actually present between frames. The analyzer inserts a 7e at the start and end of each frame to indicate that at least one flag was present on the link. What FTS shows is:

<7e><start-of-frame marker><data><crc><end-of-frame marker><7e><7e><start-of-frame marker><data><etc.>

However, there may have been many flags between frames or just one, but the analyzer has no way to know this.

In Bisync and Monosync, the chip hides the characters used as sync characters. The analyzer displays at least two syncs in Bisync and one in Monosync to show that sync characters were present, but the analyzer does not know how many syncs actually occurred. One result of this is that the timestamps on the sync characters may not be correct since the analyzer only knows that the sync characters occurred when data comes in.

21.10 Known Issues with the Source BD_ADDR Field

The data contained in the Source BD_ADDR field has the potential to be inaccurate.

A number of factors associated with wireless communication such as complex usage scenarios, or dropped data packets due to poor RF reception contribute to incorrect information periodically appearing in this field. Due to the nature of wireless communication, it is not always possible for the analyzer, or any device, to determine the BD_ADDR of the communicating devices on the network.

Users should keep in mind that the data contained in the Source BD_ADDR field should be used as a guide and not an absolute.

21.11 Useful Character Tables

21.11.1 ASCII Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

21.11.2 Baudot Codes

DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L	)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

21.11.3 EBCDIC Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(	+	
5x	&										!	$	*	)	;	^
6x	-	/									|	,	%	_	>	?
7x										`	:	#	@	'	=	"
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[		
Bx														]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

21.11.4 Communication Control Characters

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and two-character system abbreviation for each one. Some abbreviations have forward slash characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Abbreviation	**Control Character**	**Text**
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of

		Medium
EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed
FS	FS	File Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle

US	US	Unit Separator
VT	VT	Vertical Tabulation

21.12 Frame Decoder

Frame Decoder is for the development of add-on components to extend the functionality of your FTS protocol analyzer. Those add-on components are generally used to decode existing or custom protocols. The core of each such "decoder" is a program that defines how the protocol data are to be broken up into fields and displayed in the Frame Display window of the analyzer software. The DecoderScript Manual provides instruction on how to create custom decoders and use them just like any of the decoders supplied with the protocol analyzer. You can also apply this knowledge to modify decoders supplied with the protocol analyzer.

For more information about Frame Decoder, consult the DecoderScript Manual located in the desktop folder under Optional Components, or simply select *Start | Programs | Frontline [Product Name and Version Number] | Optional Components | DecoderScript Manual*.

22 Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z