fte.com frontline Debug Communications Faster℠

ComProbe® User Manual

Revision Date: 4/17/2014

Contents

List of Figures

Chapter 1: ComProbe Hardware & Software

Frontline Test Equipment ComProbe family of protocol analyzers work with the following technologies.

- Classic Bluetooth
- *Bluetooth* low energy
- Dual Mode *Bluetooth* (simultaneous Classic and low energy)
- *Bluetooth* Coexistence with 802.11
- *Bluetooth* HCI (USB, SD, High Speed UART)
- NFC
- 802.11 (Wi-Fi)
- SD
- USB
- HSU (High Speed UART)

The ComProbe hardware interfaces with your computer that is running our robust software engine called the ComProbe Protocol Analysis System or ComProbe software. Whether you are sniffing the air or connecting directly to the chip Frontline analyzers use the same powerful ComProbe software to help you test, troubleshoot, and debug communications faster.

ComProbe software is an easy to use and powerful protocol analysis platform. Simply use the appropriate ComProbe hardware or write your own proprietary code to pump communication streams directly into the ComProbe software where they are decoded, decrypted, and analyzed. Within the ComProbe software you see packets, frames, events, coexistence, binary, hex, radix, statistics, errors, and much more.

This manual is a user guide that takes you from connecting and setting up the hardware through all of the ComProbe software functions for your ComProbe hardware. Should you have any questions contact the Frontline Technical Support Team.

1.1 What is in this manual

The ComProbe User Manual comprises the following seven chapters. The chapters are organized in the sequence you would normally follow to capture and analyze data: set up, configure, capture, analyze, save. You can read them from beginning to end to gain a complete understanding of how to use the ComProbe hardware and software or you can skip around if you only need a refresher on a particular topic. Use the Contents, Index, and Glossary to find the location of particular topics.

- **Chapter 1 ComProbe Hardware and Software**. This chapter will describe the minimum computer requirements and how to install the software.
- **Chapter 2 Getting Started**. Here we describe how to set up and connect the hardware, and how to apply power. This chapter also describes how to start the ComProbe software in Data Capture Methods. You will be introduced to the Control window that is the primary operating dialog in the ComProbe software.

- **Chapter 3 Configuration Settings**. The software and hardware is configured to capture data. Configuration settings may vary for a particular ComProbe analyzer depending on the technology and network being sniffed. There are topics on configuring protocol decoders used to disassemble packets into frames and events.
- **Chapter 4 Capturing and Analyzing Data**. This Chapter describes how to start a capture session and how to observe the captured packets, frames, layers and events.
- **Chapter 5 Navigating and Searching the Data**. Here you will find how to move through the data and how to isolate the data to specific events, often used for troubleshooting device design problems.
- **Chapter 6 Saving and Importing Data**. When a live capture is completed you may want to save the captured data for future analysis, or you may want to import a captured data set from another developer or for use in interoperability testing. This chapter will explain how to do this for various data file formats.
- **Chapter 7 General Information**. This chapter provides advanced system set up and configuration information, timestamping information, and general reference information such as ASCII, baudot, and EBCDIC codes. This chapter also provides information on how to contact Frontline's Technical Support team should you need assistance.

1.2 Minimum System Requirements

- PC with Windows XP 32 bit, (Service Pack 2 or higher), Windows 7 (32 or 64 bit)
- Pentium 2 GHz processor
- RAM Requirements: 2 GB minimum, 4 GB recommended
- 100 MB free Hard Disk Space
- USB 2.0 High Speed enabled port

1.3 Software Installation

1.3.1 From CD:

Insert the ComProbe installer disc into your DVD drive. Click on the **Install CPAS** shortcut and follow the directions.

1.3.2 From Download:

Download the latest CPAS installer from FTE.com. Once downloaded, double-click the installer and follow the directions.

Chapter 2: Getting Started

In this chapter we introduce you to the ComProbe hardware and show how to start the ComProbe analyzer software and explain the basic software controls and features for conducting the protocol analysis.

2.1 802.11 Hardware

2.1.1 Attaching Antennas

When you remove the ComProbe 802.11 from the box, the first step is to attach the antennas (Figure 1).

Figure 1. Front Panel

1. Attach an antenna to each front panel connector.

Figure 2. ComProbe 802.11 with both antennas attached

2.1.2 Connecting/Powering the ComProbe 802.11

Once you have attached the antennas, the next step is to power up and connect the ComProbe 802.11 to the computer.

1. Insert the power cable (DC connector) from the 12 volt AC adapter into the **Power** port on the ComProbe 802.11 back panel (Figure 3).

Figure 3. Back Panel - Power

2. Plug the 12 volt AC adapter into the AC power source. The front panel **Power** light illuminate (Figure 1).

3. Insert the USB cable into the **USB** port on the ComProbe 802.11 back panel (Figure 4).

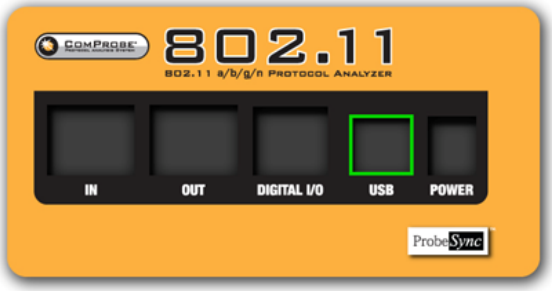


Figure 4. Back Panel - USB

4. Insert the other end of the USB cable into the PC.

5. It may take as long as thirty seconds for Windows to recognize that the ComProbe 802.11 hardware is connected to the PC. The **Activity** light on the ComProbe 802.11 front panel (Figure 1 will blink during this period, when the light is steady, the ComProbe 802.11 hardware is ready to communicate with the ComProbe software.

2.1.3 Setting Up for ProbeSync™

The ComProbe 802.11 hardware has ProbeSync™ which allows for synchronization of ComProbe hardware clocks and timestamping. One ComProbe device will act as the master device by providing the clock to the slave device receiving the clock. Do not confuse "master" and "slave" with Bluetooth device master and slave relationships. When using the ComProbe 802.11 with a ComProbe BPA 600 the BPA 600 must always be the master ProbeSync device. Refer to the following table.

802.11 ProbeSync Relationships

Master	Slave
No. 1 ComProbe 802.11	No. 2 ComProbe 802.11
ComProbe BPA 600	ComProbe 802.11

1. Using a CAT 5 Ethernet cable (less than 1.5 meters (4.9 feet)) insert one end to the master ComProbe device OUT jack.
2. Insert the other end of the cable into the slave ComProbe device IN jack.

Note: The ComProbe BPA 600 device must always be the master node in ProbeSync mode.

Figure 5. Back Panel - ProbeSync with BPA 600

2.2 Data Capture Methods

This section describes how to load Frontline Test Equipment, Inc ComProbe Protocol Analysis System software, and how to select the data capture method for your specific application.

2.2.1 Opening ComProbe® Data Capture Method

On product installation, the installer creates a folder on the windows desktop labeled "Frontline ComProbe Protocol Analysis System <version#>".

1. Double-click the "Frontline ComProbe Protocol Analysis System" desktop folder

This opens a standard Windows file folder window.

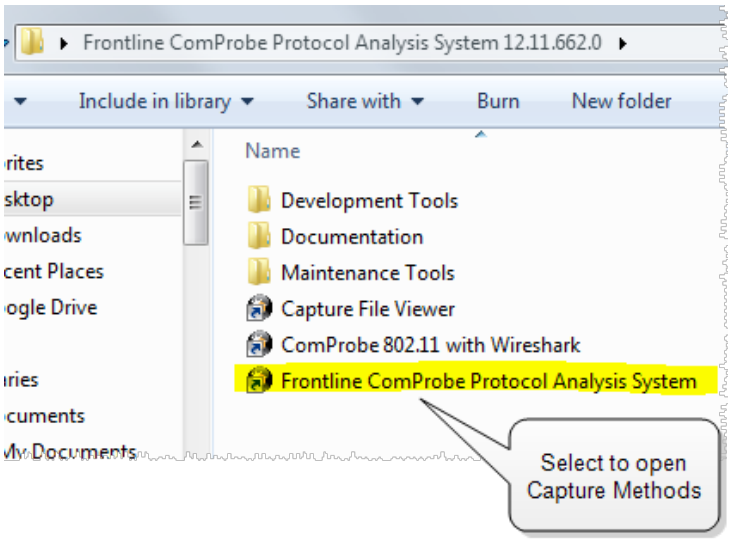


Figure 6. Desktop Folder Link

2. Double-click on **Frontline ComProbe Protocol Analysis System** and the system displays the Select Data Capture Method dialog.

Note: You can also access this dialog by selecting Start > All Programs > Frontline ComProbe Protocol Analysis System (Version #) > Frontline ComProbe Protocol Analysis System

This dialog lists all the methods ComProbe 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).

Run starts the selected protocol stack.

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

Help 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.
4. Click on the Run button and the ComProbe Control Window will openconfigured to the selected capture method.

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

Creating a Shortcut

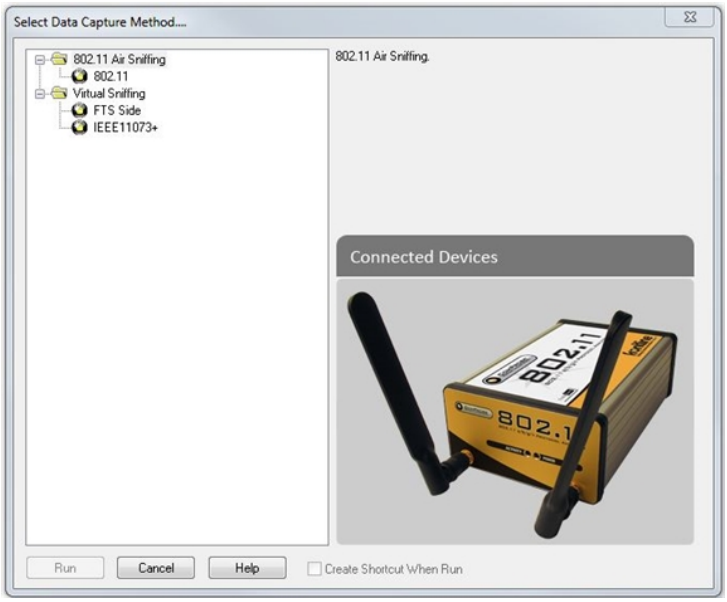
A checkbox labeled Create Shortcut When Run is located near the bottom of the dialog. This box is unchecked by default. Select this checkbox, and the system creates a shortcut for the selected method, and

places it in the "Frontline ComProbe Protocol Analysis System <version#>" 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.

Supporting Documentation

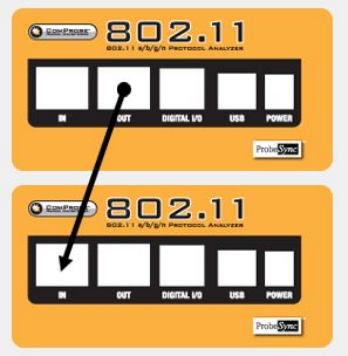
The Frontline ComProbe Protocol Analysis System directory contains supporting doucmentation for development (Automation, DecoderScript, application notes), documentation (Quick Start Guides and User Manual), and maintenance tools.

2.2.2 ComProbe® 802.11 Air Sniffing Data Capture Methods



- 802.11
  - Requires one ComProbe 802.11 hardware.
  - Captures 802.11 data on the selected channel.

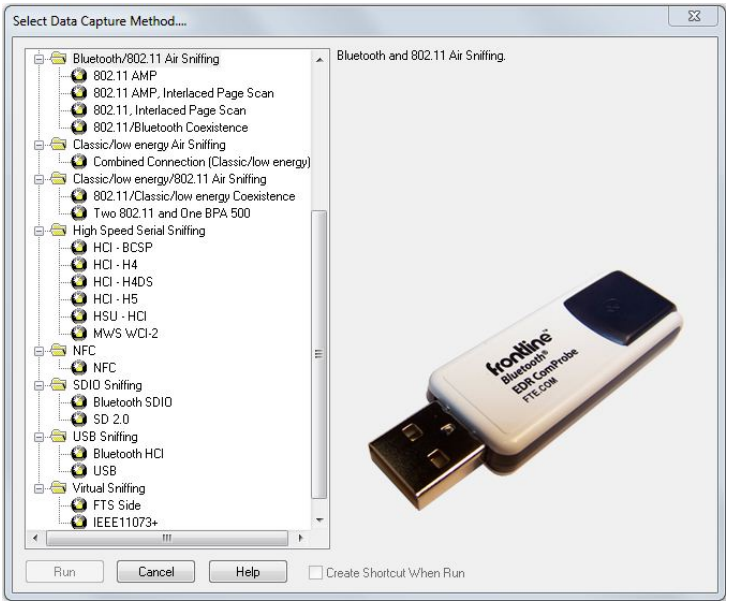
- 802.11 Double
  - Requires two ComProbe 802.11 hardware.



- 802.11 Triple
  - Requires three ComProbe 802.11 hardware.
- 802.11 with USB
  - Requires one ComProbe 802.11 and one ComProbe USB hardware.
- 802.11 with USB and SD
  - Requires one ComProbe 802.11, one ComProbe USB, and one ComProbe SD hardware.

2.2.3 Bluetooth®/802.11 Air Sniffing Data Capture Methods

ComProbe® Protocol Analysis System has different data capture methods to accommodate various applications.



- 802.11 AMP
  - Requires one ComProbe FTS4BT and one ComProbe 802.11 hardware.
  - This method is used for *Bluetooth* v3.0 +HS analysis.
  - Captures *Bluetooth* and 802.11 data, including AMP Manager and displays both in the Frame Display and Coexistence View.
- 802.11AMP, Interlaced Page Scan
  - Requires two ComProbe FTS4BT and one ComProbe 802.11 hardware.
  - This method 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 syncing with chips that employ interlaced page scan.
- 802.11, Interlaced Page Scan
  - Requires two ComProbe FTS4BT and one ComProbe 802.11 hardware.
  - This method 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 syncing with chips that employ interlaced page scan.
- 802.11/Bluetooth Coexistence
  - Requires one ComProbe FTS4BT and one ComProbe 802.11 hardware.
  - This method is for *Bluetooth*/802.11 coexistence analysis.
  - Captures *Bluetooth* and 802.11 data and displays both in the Frame Display and Coexistence View.

2.2.4 Virtual Sniffing

The Virtual Sniffer is a live import facility within ComProbe software 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. Please refer to the “Show Live Import Information“ button on the Virtual Sniffer Datasource window in ComProbe software. More information is available in the Live Import Developer's Kit located in the Development Tools folder in Frontline ComProbe Protocol Analysis System desktop folder, and a white paper is available at Bluetooth Virtual Sniffing

- **FTS Side**
  - No hardware required.
  - ComProbe software acquires data via user-developed software.
- **IEEE 11073+**
  - No hardware required
  - for sniffing data virtually from the continua Enabling Software Library (CESL) IEEE 11073 tester.

2.2.5 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. Afterward a role switch may occur, but the analyzer automatically follows the role switch.

Note: You do not have to identify a Master address if you are using Firmware Version 62 or newer.

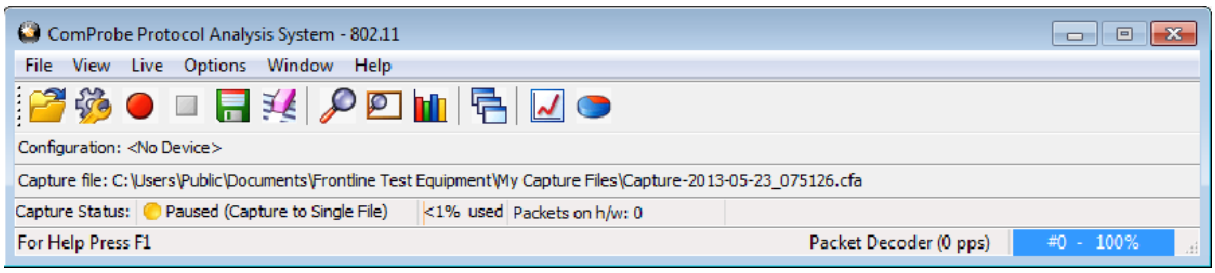
Role Switches

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 link exists between a PC and a keyboard with the PC a master. If the mouse wants to become a member of the link it initiates the connection. Since the mouse initiated the connection, it is the master of a new link and the PC is the slave. The PC is still the master of the link 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 link with two slaves: the mouse and keyboard.

2.3 Control Window

The analyzer displays information in multiple windows, with each window presenting a different type of information. The Control window opens when the Run button is clicked in the Capture Method window. The Control window provides access to each ComProbe analyzer functions and settings as well as a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function. A sample Control Window is shown below.



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.

2.3.1 Control Window Toolbar

Toolbar icon displays vary according to operating mode and/or data displayed. Available icons appear in color, while unavailable icon are not visible. Grayed-out icons are available for the ComProbe hardware and software configuration in use but are not active until certain operating conditions occur. All toolbar icons have corresponding menu bar items or options.


Open File - Opens a capture file.


I/O Settings - Opens settings


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.


Save - Saves the file the capture file.


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.


Cascade - Arranges windows in a cascaded display.


Coexistence View - Opens the Coexistence View dialog.


Wi-Fi Error Statistics - Opens the Wi-Fi Error Statistics dialog.

2.3.2 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.

2.3.3 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. It will also display whether you are capturing to a series of files or capturing to a single file.
  - 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 200 Kb 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.

2.3.4 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.

2.3.5 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, Edit, View, Filter, Bookmarks, Live, Options, Window, and Help. Most of the options are self explanatory.

- Many of the File/Edit menu items are standard Windows type commands: Open, Close, Save, Recent Files, etc. There are, however, several of these menu items that have unique functionality:
- 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 clicked, the plug-ins are reset and received frames are decoded again.

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

- Live contains commands that are used in capturing data.

- Under Options you have opportunities to set/modify various system settings. These include:
  - Hardware Settings
  - I/O Settings
  - System Settings
  - Check for New Releases at Startup: When this is enabled, the application automatically checks for the latest Frontline releases. If a new version is detected, a dialog appears similar to the sample below . The system and version will vary dependent upon the ComProbe® hardware being used.
- The Window menu displays the open Frontline dialogs and standard options like Cascade, Minimize, Tile, etc.

- Within the Help menu you can open the electronic Help file, About <hardware.where <hardware> if the specific ComProbe capture method, e.g. "About BPA 600".

2.3.6 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.

Chapter 3: Configuration Settings

In this section we show how to configure each of the Frontline ComProbe analyzer using the ComProbe software for capturing data .

3.1 802.11 Configuration

3.1.1 ComProbe 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 Frontline devices. To access the Hardware Settings dialog:

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

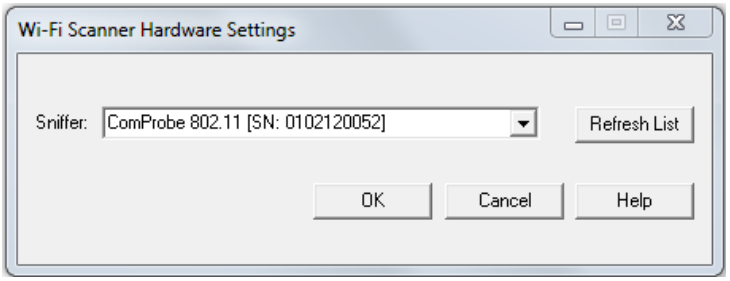


Figure 7. 802.11 Hardware Settings Dialog

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

If no devices are found, the list is blank.

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

3.1.2 802.11 I/O Settings

1. Select I/O Settings from the Options menu on the Control window.

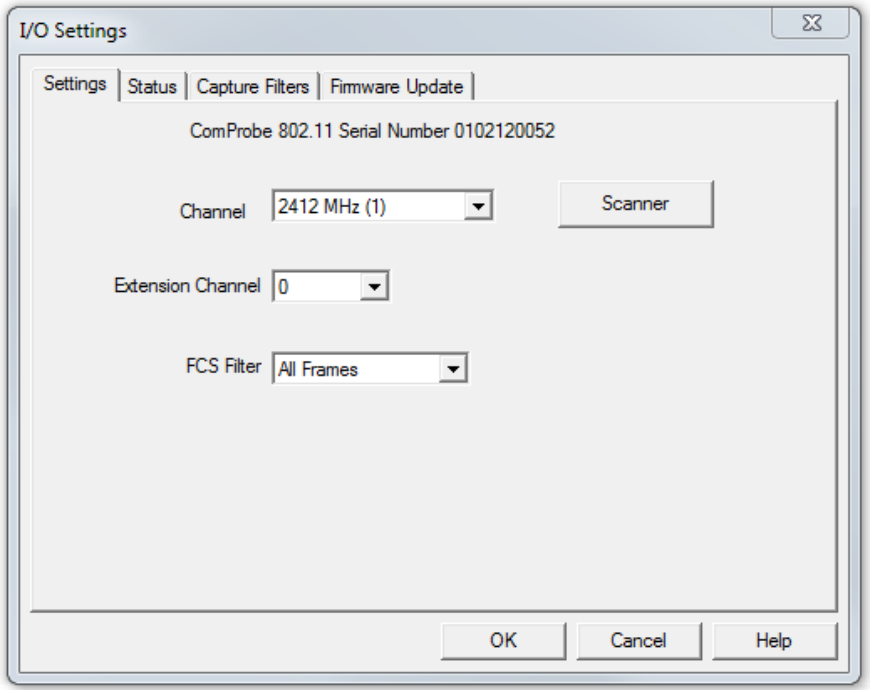


Figure 8. 802.11 I/O Settings Dialog

There are several things to remember about I/O Settings:

- The I/O Settings are specific to the device selected in the Hardware Settings.
- Two 802.11 devices attached to a computer have different settings.
- Changing the settings changes the devices' default settings.
- If a parameter is changed (e.g. Channel 1 is changed to 6), the new setting appears the next time the I/O Settings dialog is opened for the device.
- The settings are saved when the OK button is pressed.

3.1.2.1 Settings

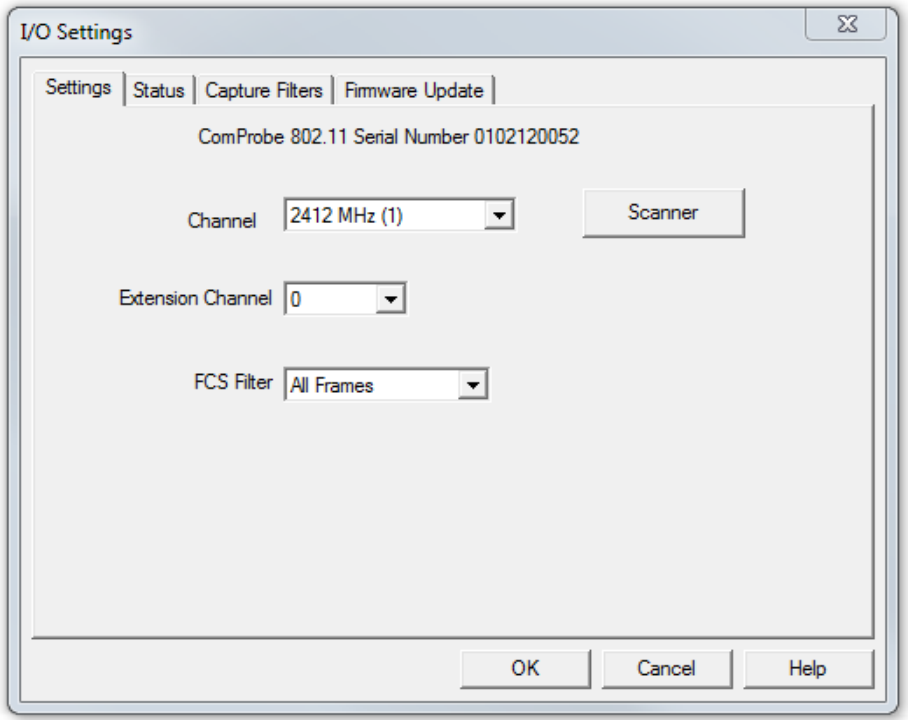


Figure 9. 802.11 I/O Settings Settings Tab

The Settings dialog allows you to change and observe basic configuration values. These include the Channel, Extension Channel, FCS Filter and Capture Type.

- Channel - Select the channel from the drop-down list. Channels have been extended to the 5Ghz range.
- Extension- allows you to extend the range of channels available
  - 0 = Standard 1-14 Wi-Fi channels
  - -1 = Expanded channels below the standard range
  - +1 = Expanded channels above the standard range
- FCS Filter - The Frame Check Sequence filter indicates if the device should capture frames with an invalid FCS. Select All Frames or Valid Frames

Clicking on the Scanner button will open the Wi-Fi Scanner dialog. This action is useful if you do not know the channel to sniff. Once you have selected a channel in the Wi-Fi Scanner dialog and confirmed your selection the selected channel will appear in Channel.

3.1.2.2 Status

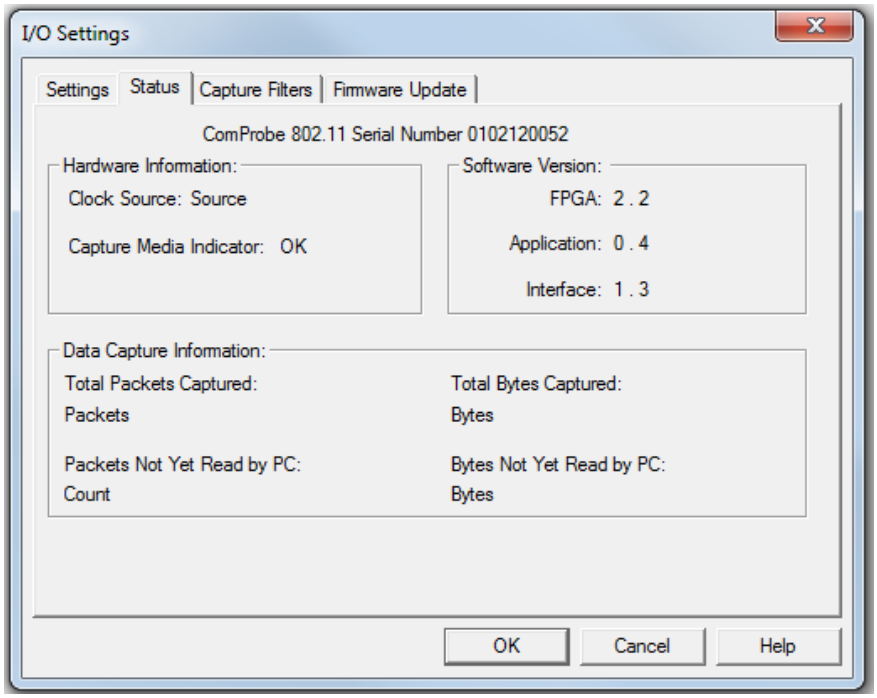


Figure 10. 802.11 I/O Settings Status Tab

The Status dialog provides current information about the ComProbe device. There are no settings for this dialog.

3.1.2.3 Capture Filters

The Capture Filters dialog allows you create, modify, and delete capture filters. The dialog initially displays the existing MAC address Capture Filters.

- To activate the capture filters and to be able to create/modify additional filters, you first must select the Enable MAC Address Capture Filters check box.
- You can select/deselect which filters are active by checking/unchecking the Enable checkbox in the first column in the table.
- You can also select to ignore Management, Control, Data, and Reserved frame types by selecting one or more the checkboxes.

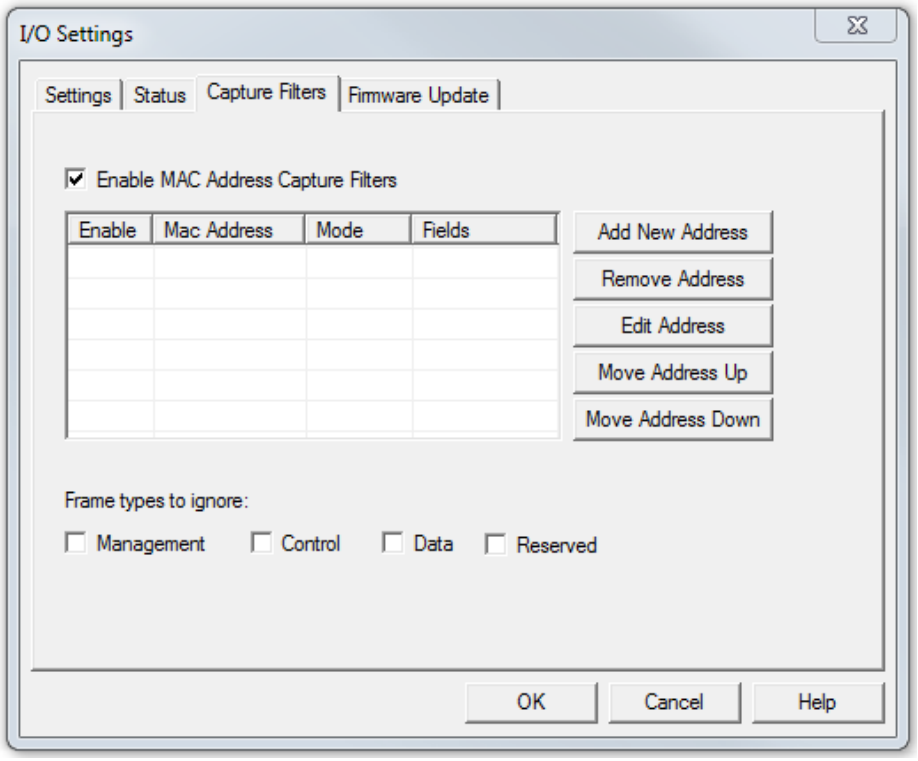


Figure 11. 802.11 I/O Settings Capture Filters Tab

To create a key, select one of the following options:

- Add New Address - displays a text box where you can enter the address

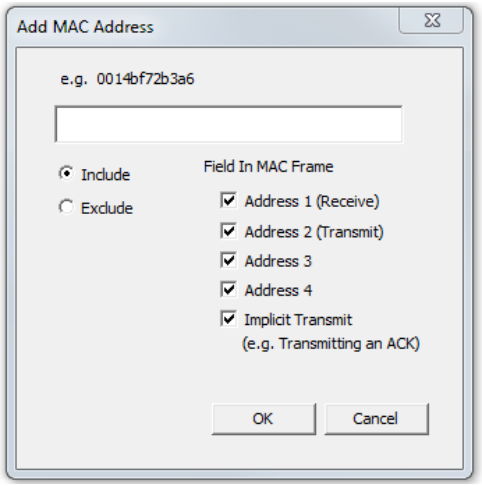


Figure 12. 802.11 I/O Settings Capture Filters Add New Address Dialog

1. Enter a MAC Address in the text field.
2. Select the Include radio button to only capture packets with this MAC address.
3. Select the Exclude radio button to capture packets with other filters, but not ones with this MAC address.
4. Select one or more check boxes to identify which fields in the MAC Frame to include.

   The MAC header for an 802.11 frame can contain up to 4 address fields. Most frames do not have that many. In general, the first address is the intended receiver and the second address is the device that transmits the frame. The third and fourth address fields depend on the context of the frame. Some of the control type frames do not include the transmitter address but they may be determined from previous frames.
5. Select OK to close the dialog.

Once you have MAC addresses on the main dialog, you can modify them using four options.

- Remove Address - Highlight an address that you want to delete and select Remove Address to remove it from the list.
- Edit Address - Highlight an address that you want to edit and select Edit to bring up a dialog where you can edit the address. The address and any of the prior settings may be changes. Click OK to save and close.

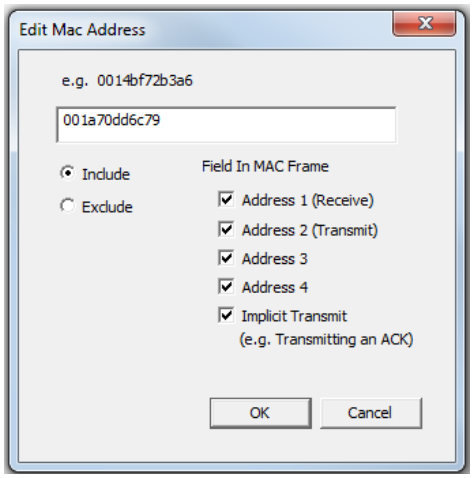


Figure 13. 802.11 I/O Settings Capture Filters Edit MAC Address Dialog

- Move Address Up - moves the selected address up in the queue.
- Move Address Down - moves the selected address down in the queue.

3.1.2.4 Firmware Update

This tab displays the current firmware version in the hardware. You can check for the firmware updates by first noting the current version and then clicking on the Check For Updates button.

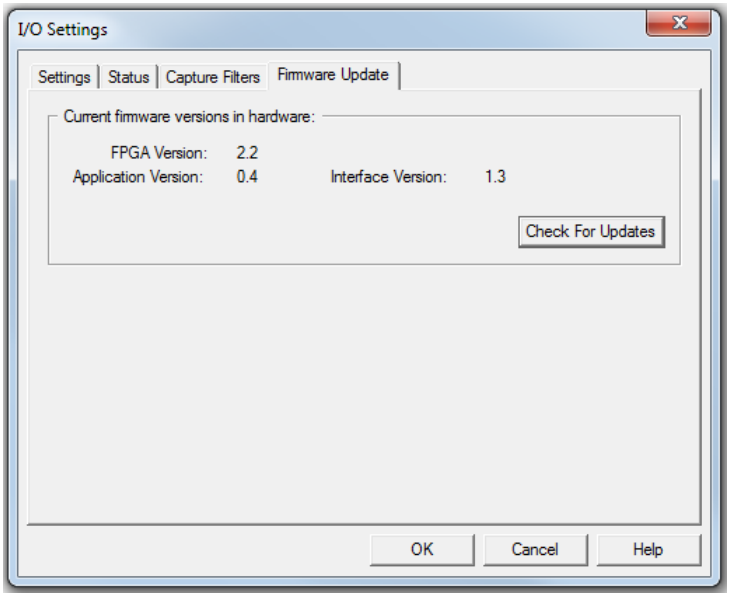


Figure 14. 802.11 I/O Settings Firmware Update Tab

The Check for Updates dialog will open. If an update is available you can install it by clicking on the Start Update button.

The update process will begin and when finished the dialog will show a list of all completed actions. Upon completion of the update you will be notified of successful installation and returned to the Firmware Update dialog.

The I/O Settings dialog Firmware tab will open and show the old firmware version. At this point, the ComProbe 802.11 is rebooting. You will notice the Activity LED blinking on the ComProbe hardware. Click OK on the I/O Settings dialog.

An error message will appear. Ignore the message and click on the Cancel button. Completely exit the ComProbe software by selecting Exit the ComProbe Protocol Analysis System from the Control window File menu.

Wait for a solid Activity LED on the ComProbe hardware .

Important: Remove power from the ComProbe 802.11 hardware, and reapply power. Wait until the Activity LED comes back on and resume normal ComProbe operation.

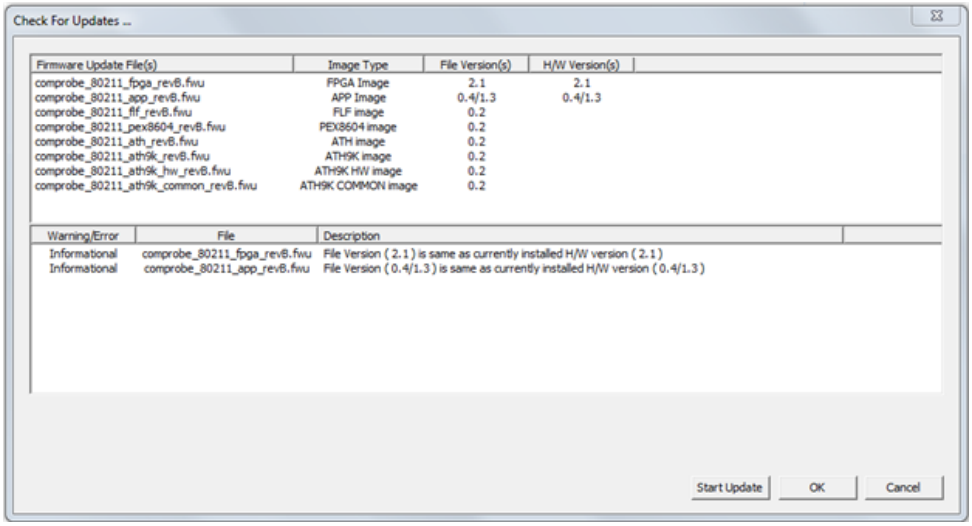


Figure 15. 802.11 I/O Settings Firmware Update Version List

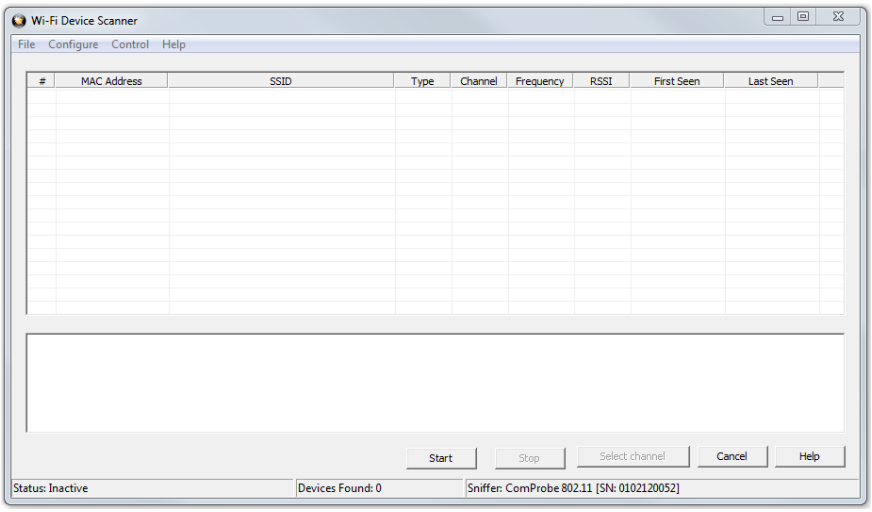
3.1.2.5 Security

Wi-Fi security settings are discussed in detail in the Decoder Parameters section .

3.1.2.6 Device Scanner

3.1.2.6.1 Wi-Fi Device Scanner

1. On the I/O Settings dialog click on the Settings tab, and then click on the Scanner button. The Wi-Fi Device Scanner dialog will open.



802.11 Device Scanner with no Devices Detected

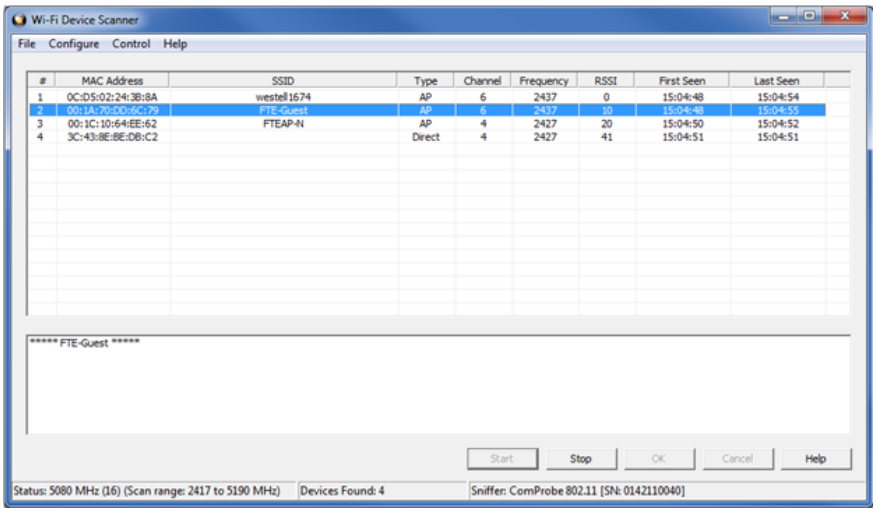
2. On the Wi-Fi Device Scanner dialog Select the Start button or select Start Scanning from the

Control menu to begin populating the list .

The Wi-Fi Device Scanner dialog displays a list of discoverable Wi-Fi devices in a table. The devices are identified by:

- MAC Address
- SSID
- Type
- Channel
- Frequency
- RSSI
- First Seen
- Last Seen

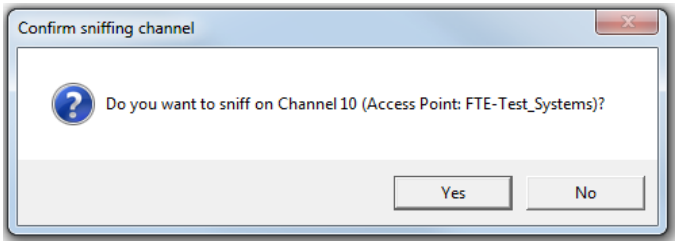
Note: You can select the Stop or Stop Scanning from the Configure menu anytime to stop the device search.



802.11 Device Scanner with Devices Detected

3. Select the device.

4. Click on Select channel <*no*>, where <*no*> is the channel number selected. The Confirm Sniffing Channel confirmation will appear. Click on Yes will close the Wi-Fi Device Scanner and the ComProbe analyzer will used the selected channel.



3.1.2.6.1.1 File Menu

Under the File menu you can select Export to file which converts the information in the table to a text file.

1. Select Export to CSV file. The Save As menu appears
2. Select where you want to save the file in Save in.
3. Enter a File Name.
4. Select Save.

3.1.2.6.1.2 Configure

From the Configure menu you can select , ,Hardware Settings and I/O Settings

3.1.2.6.1.3 ComProbe 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 Frontline devices. To access the Hardware Settings dialog:

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

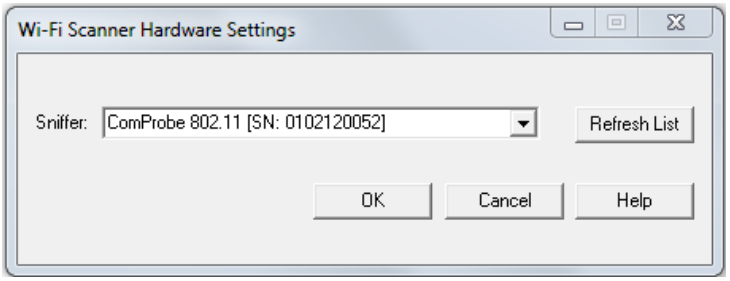


Figure 16. 802.11 Hardware Settings Dialog

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

If no devices are found, the list is blank.

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

3.1.2.6.1.4 Wi-Fi Device Scanner - I/O Settings

The Device Scanner I/O Settings dialog is used to set a listening time and to activate a probe request. To access the I/O Settings dialog:

1. Select I/O Settings from the Configure menu on the Wi-Fi Device Scanner window.

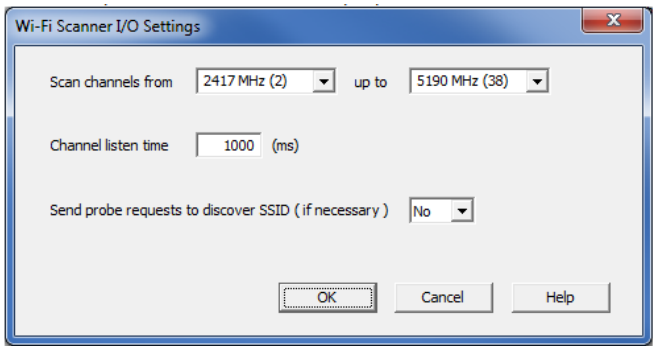


Figure 17. Wi-Fi Device Scanner I/O Settings Dialog

2. Scan Channels from: Pick a lower and upper limit to scan a specific subset of frequencies. By default all channels are selected. Choosing a subset of frequencies to scan saves time and can be used when the user is interested in scanning only a certain range of frequencies.
3. Enter an amount, in msecs, for Channel listen time.

   Channel listen time is how long ComProbe® 802.11 will listen on a channel to discover devices before moving on to the next channel.

4. Select Yes or No to choose whether to send a probe sync request.

   Sometimes an Access Point will intentionally not send it's SSID in a beacon to conceal it's identity. Selecting Yes for this option will send the MAC address, the SSID will be part of the Probe Response it sends back.

5. Select OK to save the options and close the dialog or Cancel to close the dialog without saving your choices.

3.1.2.6.1.5 Device Scanner RSSI Values

The 802.11 specification does not provide a relationship between the RSSI value and the actual power value. Here are the definitions from the specification.

1. RSSI in FHSS PHY: The RSSI is an optional parameter that has a value of 0 through RSSI Max. This parameter is a measure by the PHY of the energy observed at the antenna used to receive the current PPDU. RSSI shall be measured between the beginning of the SFD and the end of the PLCP HEC. RSSI is intended to be used in a relative manner. Absolute accuracy of the RSSI reading is not specified.

2. RSSI in DSSS PHY: The RSSI shall be a measure of the RF energy received by the DSSS PHY. RSSI indications of up to 8 bits (256 levels) are supported.

3. RSSI in OFDM PHY: The allowed values for the RSSI parameter are in the range from 0 through RSSI maximum. This parameter is a measure by the PHY of the energy observed at the antenna used to receive the current PPDU. RSSI shall be measured during the reception of the PLCP preamble. RSSI is intended to be used in a relative manner, and it shall be a monotonically increasing function of the received power.

Different vendors implement these value in their own way. The ComProbe 802.11 uses an Atheros chipset which provides RSSI values in the range of 0 to 128. The radio hardware in the ComProbe 802.11 has two receive chains (one for each antenna). Each received packet has RSSI values for both antennas as well as the combined value.

The hardware provides the following five values:

1. rssi_ant00: Receive signal strength indicator of control channel chain 0.
2. rssi_ant01: Receive signal strength indicator of control channel chain 1.
3. rssi_ant10: Receive signal strength indicator of extension channel chain 0.
4. rssi_ant11: Receive signal strength indicator of extension channel chain 1
5. rssi_combined: Receive signal strenth indicator of combination of all active chains on the control and extension channels.

All five of these values are shown in the PHY layer decoder for every packet. The Wi-Fi scanner shows the combined value.

3.1.2.7 Wi-Fi Device - MAC Address Editor

If you know the MAC Address of the device you can enter it manually.

1. From the I/O Settings dialog select the "Edit" button.
2. On the MAC Address Editor enter the MAC Address for the device.

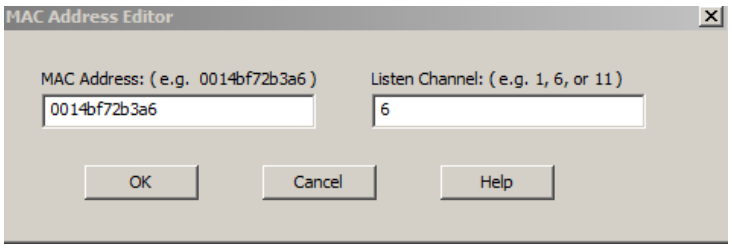


Figure 18. Wi-Fi Direct MAC Address Editor

3. Enter a channel number in Listen Channel.
4. Select "OK".

The MAC Address appears on the I/O Settings dialog.

Once you close the dialog, the last MAC Address shown will appear when you reopen the dialog.

3.2 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.

There may be times when the context for decoding a frame is missing. For example, if the analyzer captures a response frame but does not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters window allows you to supply the context for any frame. The dialog allows you to define any number of parameters and save them in a template for later use

The decoder template function provides the capacity to create multiple templates that contain different parameters. This capability allows you 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.

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 and Frame Display windows.

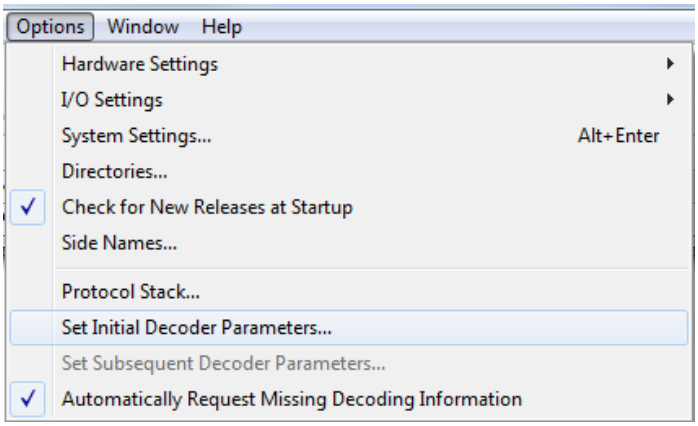


Figure 19. Select Set Initial Decoder Parameters… from Control window

The Set Initial Decoder Parameters window opens with a tab for each decoder that requires parameters.

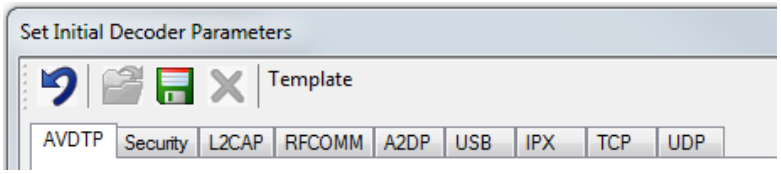


Figure 20. Tabs for each decoder requiring parameters.

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

Override Existing Parameters

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. You can also right-click on the frame to select the same option.

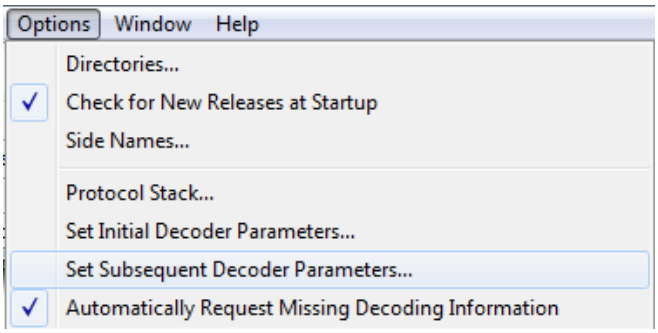


Figure 21. Set Subsequent Decoder Parameters... from Control window

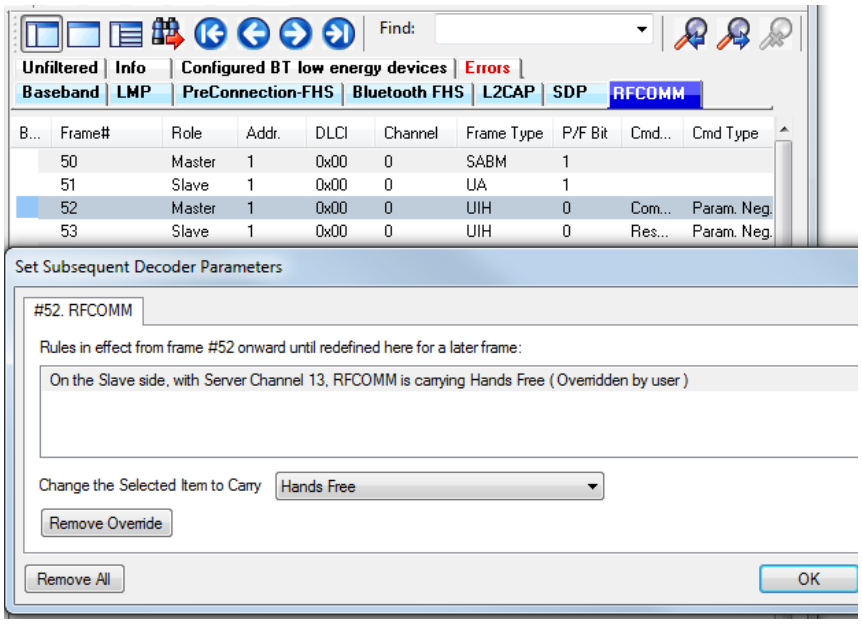


Figure 22. Example: Set Subsequent Decode for Frame #52, RFCOMM

- 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.
- The Remove Override button will remove the selected decode parameter override.
- The Remove All button will remove all decoder overrides.

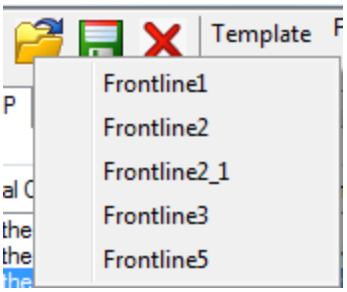
If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

3.2.1 Decoder Parameter Templates

3.2.1.1 Select and Apply a Decoder Template

1. Select Set Initial Decoder Parameters... from the Options menu on the Control window or the Frame Display window.

2. Click the Open Template icon in the toolbar and select the desired template from the pop up list. The system displays the content of the selected template in the Initial Connections list at the top of the dialog



3. Click the OK button to apply the selected template and decoders' settings and exit the Set Initial Decoder Parameters dialog.

3.2.1.2 Adding a New or Saving an Existing Template

Add a Template

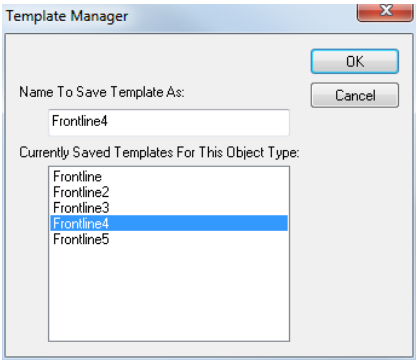
A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

1. Click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Template Manager dialog.

2. Enter a name for the new template and click OK.

   The system saves the template and closes the Template Manager dialog.

3. Click the OK button on the Set Initial Decoder Parameters window 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 window to display the Template Manager dialog.

2. Ensure that the name of the template is listed in the Name to Save Template As text box and click OK.

3. The system displays a dialog asking for confirmation of the change to the existing template. 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 window to apply the template and close the window.

3.2.1.3 Deleting a Template

1. After opening the Set Initial Decoder Parameters window click the Delete button in the tool-bar.

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

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

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

3. Click the OK button to complete the deletion process and close the Delete dialog.

4. Click the OK button on the Set Initial Decoder Parameters window to apply the deletion and close the dialog.

3.2.2 Wi-Fi Security Decoder Parameters

On the Set Initial Decoder Parameters dialog, the security tab allows specifying a key for software decryption of 802.11 frames.

To access this dialog:

1. In 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.

- WPA2 (Wi-Fi Protected Access), and WEP (Wired Equivalent Privacy) data that is transmitted over a 802.11 communications link. There are two values you have to enter for the WPA2 and WEP to be decrypted properly. Click here to see additional WEP settings in the I/O Settings dialog.
- The Bluetooth® alternative MAC/PHY (AMP) enables *Bluetooth* to support data rates up to 24Mbps by using additional wireless radio technologies.
- The third method is to specify the pre-shared key in its raw hex forum a 32-byte hex number.

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

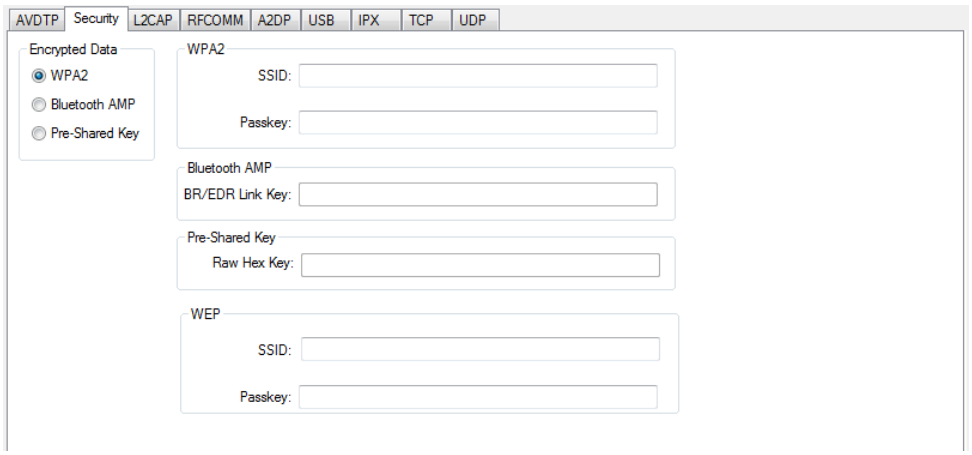


Figure 23. Security (WPA2/WEP) Decoder Tab

Set the WPA2 or WEP parameters.

1. Select the WPA2 radio button. This activates the WPA2 and WEP text boxes.
2. There are two values to set for the WPA2 and WEP keys.
    a. WEP SSID (Service Set Identifiers) - the station ID of the 802.11 communications link.
    b. WEP Passkey - .the shared passkey phrase used in communications.
3. Select OK to save the settings and close the dialog.

Set the Bluetooth AMP parameters.

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

1. Select the Bluetooth AMP radio button to activate Bluetooth AMP and WEP text boxes
2. Enter a hexadecimal value for the BR/EDR Link Key (Basic Rate or Extended Data Rate) .
3. There are two values to set for the WEP key.
    a. WEP SSID (Service Set Identifiers) - the station ID of the 802.11 communications link.
    b. WEP Passkey - .the shared passkey phrase used in communications.

Note: When capturing both *Bluetooth* and 802.11 data using the 802.11 AMP capture selection, Frontline 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.

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

Set the Pre-Shared Key parameters.

The third way to set encrypted data is to specify the pre-shared key in its raw hex forumas a 32-byte hex number.

Note: The other ways of specifying the WPA2 key automatically generate this value.

1. Select the Pre-Shared Key radio button - activates the Pre-Shared Key and WEP text boxes.
2. Enter a 32-byte hex number inthe Pre-Shared Key Raw Hex Key text box.
3. There are two values to set for the WEP key.
    a. WEP SSID (Service Set Identifiers) - the station ID of the 802.11 communications link.
    b. WEP Passkey - .the shared passkey phrase used in communications.

Note: When capturing both *Bluetooth* and 802.11 data using the 802.11 AMP capture selection, Frontline 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.

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

3.2.3 Adding or Changing TCP/UDP Port Assignments

TCP and UDP are Transport layer protocols in the IP protocol suite. These transport layer protocols use ports to establish communication between application layer protocols. For example, all Web traffic uses the HTTP protocol. HTTP is an application layer protocol that uses the standard TCP/UDP port 80. The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the list of standard port numbers and their assignments. For an up-to-date listing of all standard TCP/UDP port assignments, visit www.iana.org.

When the analyzer reads a TCP, UDP or IPX packet, it infers the upper layer protocols by using pre-defined rules of traversal. For example, if the packet has a TCP source or destination port number 80, then the upper layer protocol is HTTP. These rules, which are built in to the software, determine the upper layers of the protocol stack based on the source or destination port numbers in the packet. The built-in rules are based on the standard port assignments. However, it is quite common to come across network systems in which upper layer protocols use user-defined port numbers for both standard and custom protocols. In such cases, the analyzer users can tell the software which port numbers are assigned to which protocols.

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.

3.2.3.1 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
4. Enter the port number in the Port Number box.

5. In the Protocol drop-down list, choose the protocol to traverse to.
6. Click the Add button.

The system adds the new entry to the bottom of the port number list.

3.2.3.2 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. Select the Port Range radio button and specify the starting and ending port numbers. The range is inclusive.
6. Click the Modify button.

The system displays the changes in port assignment.

3.2.3.3 Delete a 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 delete.
4. Select Delete.

The system deletes the port assignment.

3.2.3.4 Move a Port Assignment

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.

3.2.3.5 Port Assignment Considerations

- 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.

Chapter 4: Capturing and Analyzing Data

The following sections describe the various ComProbe software functions that capture and display data packets.

4.1 Capture Data

4.1.1 Capturing Data to Disk

Note: 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.

   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.

   Note: For the Dashboard, when you capture to series of files, the window displays the data from the beginning of the first capture, even when a new file in the series is created. This is because the Dashboard is a "Session Monitor", which means that even if you capture to a series of files, the data from the first file is always displayed. The display does not refresh when a new capture file in a series is created.

2. 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.

3. 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.

4. 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 see how to capture to a single file, choose System Settings from the Options menu on the Control window.

When live capture stops, no new packets are sniffed but there can still be packets that were previously sniffed but not yet read by the ComProbe analyzer. This happens when packets are being sniffed faster than the ComProbe analyzer can process them. These packets are stored either on the ComProbe hardware itself or in a file on the PC. If there are remaining packets to be processed when live capture stops the Transferring Packets dialog below is displayed showing the packets yet to be read by the ComProbe analyzer. The dialog shows the name of each ComProbe hardware device, its process id in square brackets, and the number of packets remaining. These stored packets are read until they're exhausted or the user clicks the Discard button on the dialog.

Unlike 802.11, *Bluetooth* packets never come in faster than the datasource can process them. However, *Bluetooth* packets must still be stored so that they can be read in chronological order with the 802.11 packets.

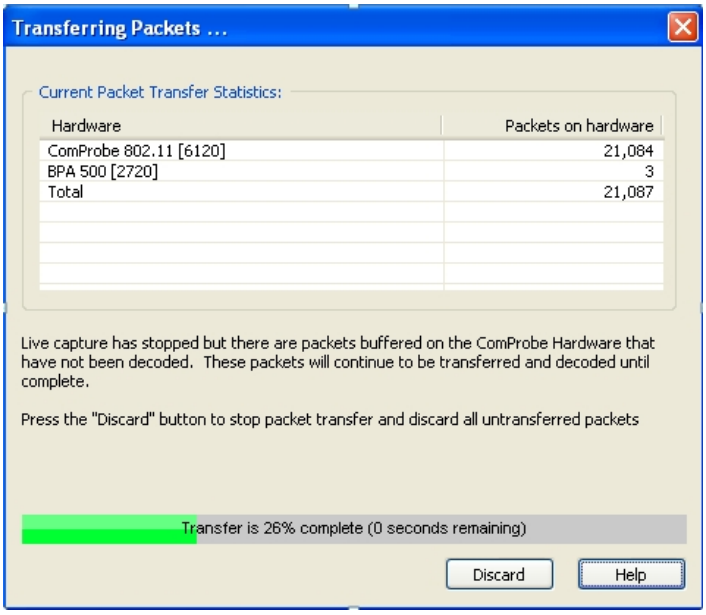


Figure 24. Packet Transfer Dialog

4.1.2 ComProbe® 802.11 with Wireshark®

4.1.3 Capturing Using Frontline Wi-Fi Datasource

Click on the "ComProbe 802.11 with Wireshark" short cut to launch and start capturing the Wi-Fi packets. If you do not see any packets on the Wireshark window then check the status message indication on the Wi-Fi Datasource window to see if sniffing has stopped. Click on the Start  button .

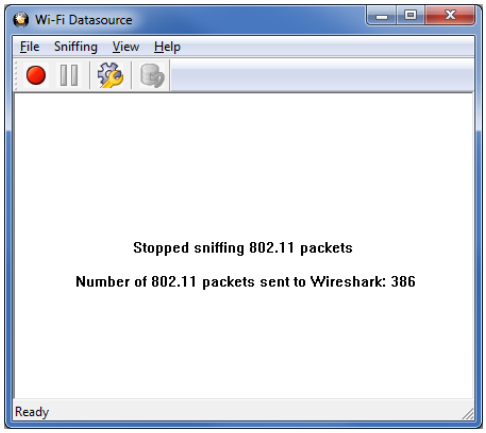


Figure 25. Datasource Stopped Sniffing

When the ComProbe 802.11 is sniffing the datasource will display the following message. Sniffing can be stopped by clicking the Stop button  .

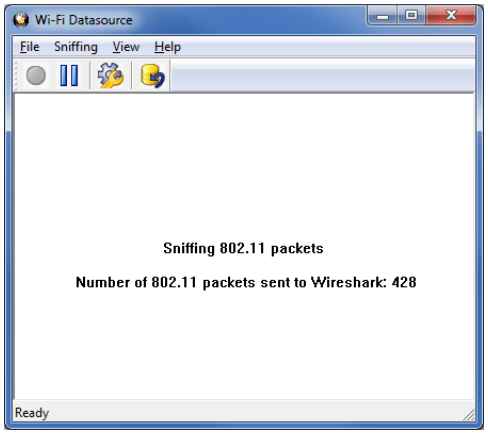


Figure 26. Datasource Sniffing

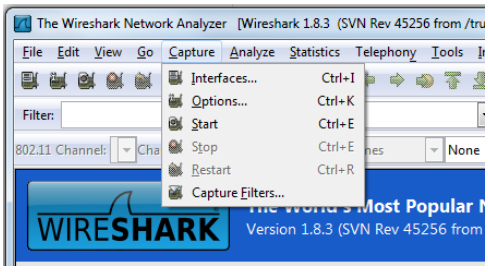


Figure 27. Wireshark Capture Dialog

Note: Whenever you give Start Capture command on Wireshark, the status message on the Wi-Fi Datasource window should display "Please START capturing on the Wireshark." If it is displaying a different message then you can use the Reset button on the Wi-Fi Datasource window or select **Reset** or in the Sniffing menu to get back to this message.

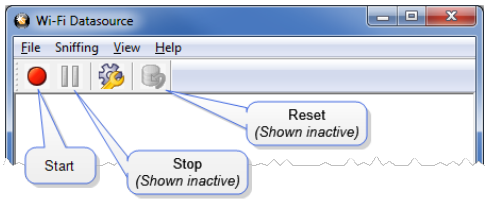


Figure 28. Wi-Fi Datasource Toolbar

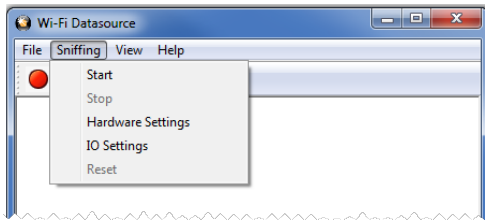


Figure 29. Wi-Fi Datasource Sniffing Menu

Once the Wi-Fi Datasource starts capturing packets and sending them to Wireshark, you can pause and resume capturing using the Stop and Start toolbar buttons on the Wi-Fi Datasource toolbar or the Sniffing menu. Note that the Restart command on the Wireshark window does not function. The workaround is to click Reset on the Wi-Fi Datasource then click Start on the Wireshark Capture menu. Also the Wireshark Capture Filters menu does not function, but you can use IO Settings menu on the Wi-Fi Datasource window or Sniffing menu for setting filters.

4.1.3.1 Known Issues with Wireshark

- In Real Time capture mode (when you select Update list of packets in real time check-box in the Capture Options dialog), if you move the Wireshark window around on the desktop or click on anything on the Wireshark window, it freezes the desktop. You can unfreeze it by bringing up Windows Task Manager by pressing Ctrl+Alt+Delete.

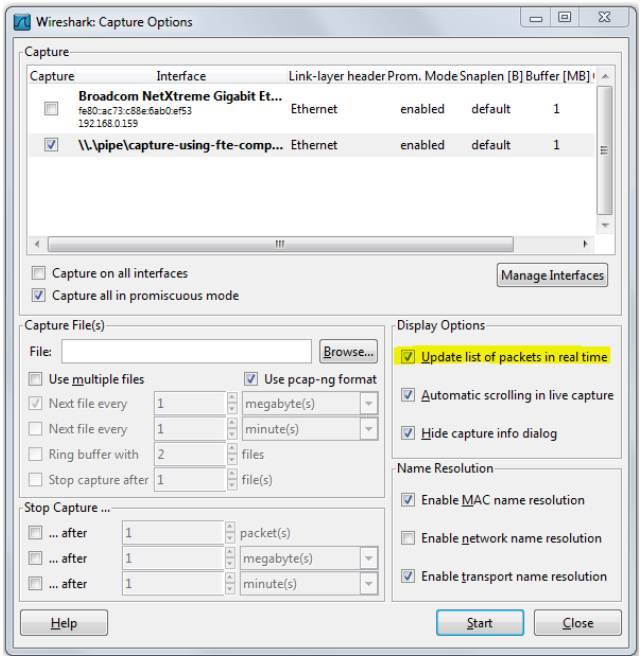


Figure 30. Wireshark Capture Options

- If you capture more than a few millions of packets, e.g. 4 million, Wireshark crashes.

4.1.4 Combining BPA 600, 802.11, and HSU with ProbeSync

ProbeSync™ allows multiple ComProbe analyzers to work seamlessly together and to share a common clock. Clock sharing allows the analyzers to precisely synchronize communications stream and to display resulting packets in a single shared view.

The ComProbe BPA 600, ComProbe 802.11, and ComProbe HSU analyzers have ProbeSync capability allowing timestamp synchronization of captured data. Synchronizing the clock for these ComProbe devices used in combination requires attention to the sequence of hardware connection. It is important to remember the following key points.

- ComProbe devices are connected serially in a daisy-chain fashion. The combined length of all cables in the chain cannot exceed 1.5 meters (4.5 ft.).
- The "master" ComProbe device provides the clock to the other devices. All other ComProbe devices are "slaves" and received the clock from the "master" device.
- On ComProbe devices with an OUT and IN connector, the function of these connectors is dependent on if they are a "master" or a "slave".
    - "master" device: OUT connector provides the clock to all "slave" devices. IN connector is not used.
    - "slave" device: IN connector receives the clock from the OUT connector of the prior device in the chain. The OUT connector is just a pass-through connector on a "slave" device.
- BPA 600 is always the "master" device and the first device in the chain, if being used.

- HSU is always the last "slave" device in the chain, if being used.
- HSU maximum capture data rate is 6 Mbit/sec.

Connecting ComProbe BPA 600, ComProbe 802.11, and ComProbe HSU devices in ProbeSync takes place in the following steps.

1. Connect the ComProbe BPA 600 OUT connector to the ComProbe 802.11 IN connector.
2. Connect the ComProbe HSU Cat 5 cable to the ComProbe 802.11 OUT connector.

Each device datasource is setup individually to sniff their respective link. Should the hardware be connected incorrectly, that is IN to IN or OUT to OUT, an error message will appear. Follow the instructions in error message. To continue click on the OK button. The ComProbe device datasource Status window will also display a warning message suggesting information sources.

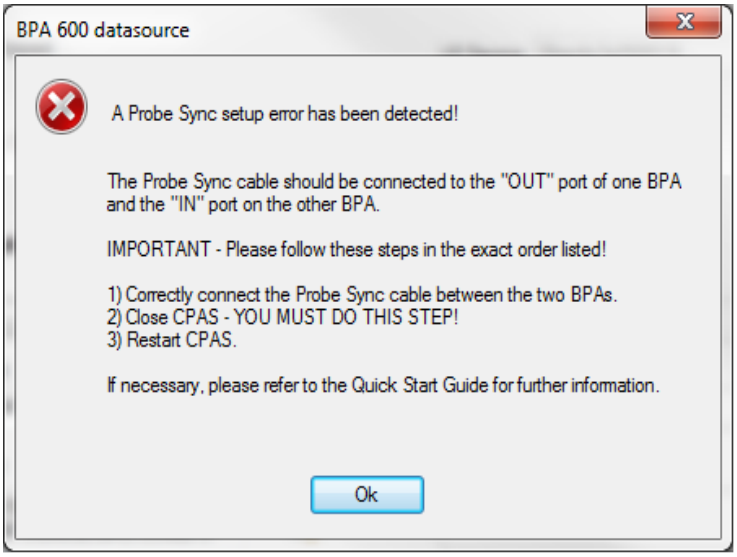


Figure 31. Incorrect ProbeSync Hardware Connection Error

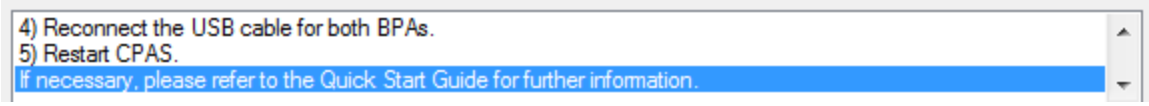


Figure 32. Incorrect ProbeSync Hardware Connection Message In Datasource Status

The BPA 600 datasource dialog Start Sniffing  button initiates the capture for all connected ComProbe 802.11 and HSU devices. On the 802.11 and HSU receiving the clock—cable connected to IN— the Start Sniffing button is disabled when using ProbeSync. In each ComProbe device's Control window status window will announce the synchronizing function.

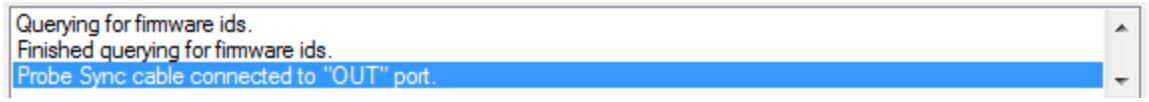


Figure 33. ProbeSync Synchronizing Device Status Message

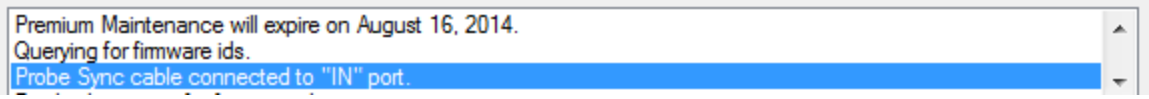


Figure 34. ProbeSync Synchronized Device Status Message

Data captured in the synchronized device will appear in the Frame Display, Event Display, Bluetooth Timeline, Bluetooth low energy Timeline, and Coexistence View. Data saved as a capture file will include data captured on each devices. Within these dialogs the packets identified as link 1, 2, and 3 were captured on the synchronizing device that provides the clock. Those packets captured on the synchronized device carry link 4, 5, and 6 identifiers.

4.1.5 Extended Inquiry Response

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

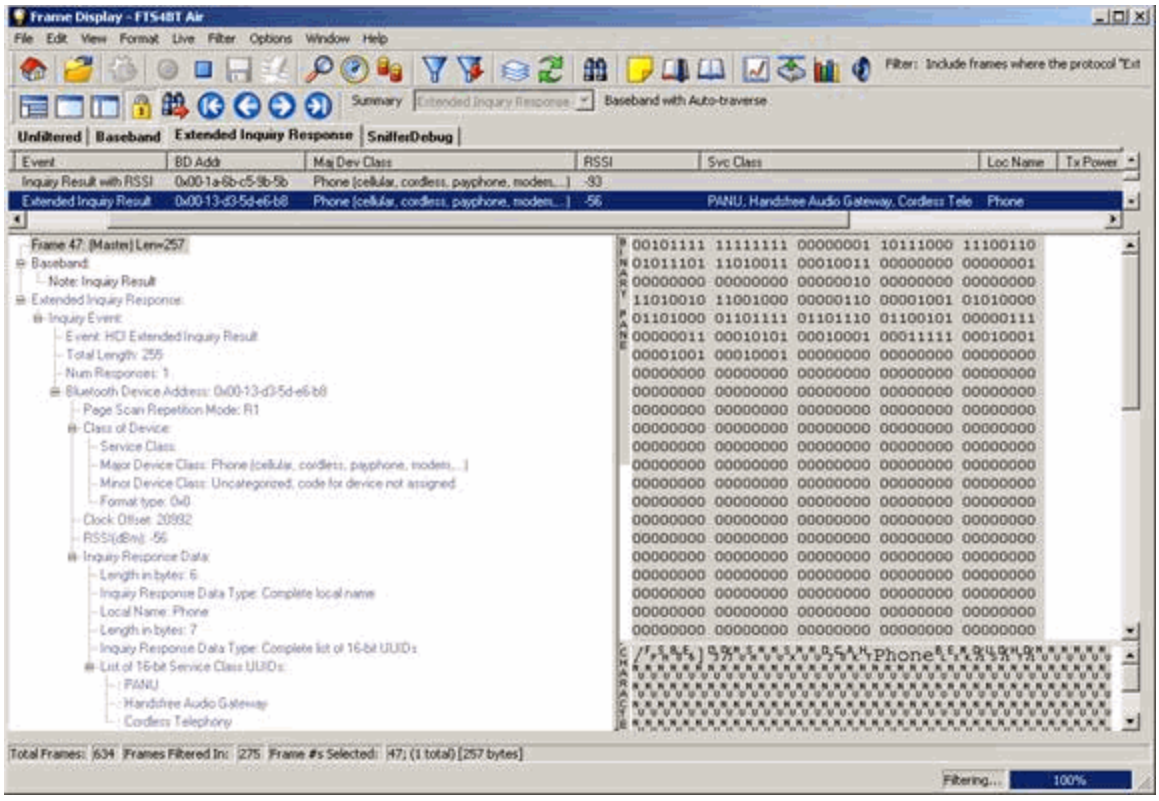


Figure 35. Frame Display Extended Inquire Response

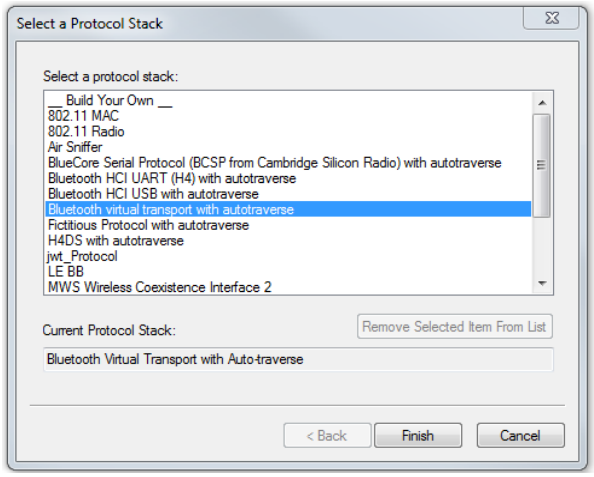
EIR displays extensive information about the Bluetooth devices that are discovered as data is being captured. Before the EIR tab was created, this type of information was not available until a connection was made to a device. Therefore, EIR can be used to determine whether a connection can/should be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

4.2 Protocol Stacks

4.2.1 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.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating and Removing a Custom Stack on page 42.

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 Selected Item From Listbutton 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.

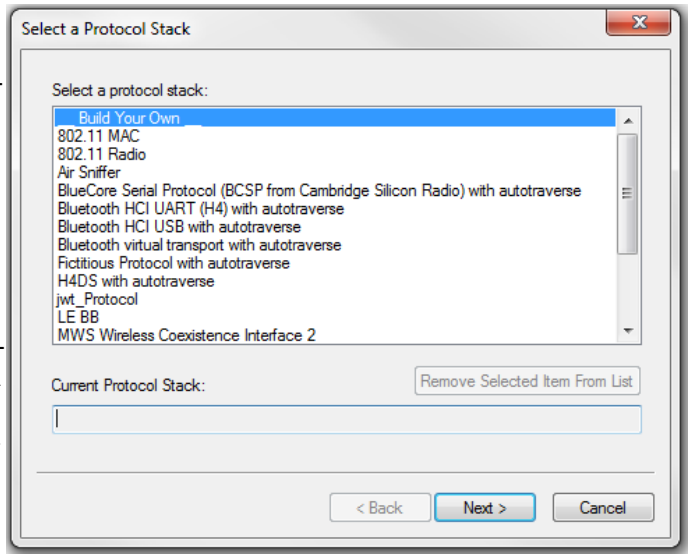
If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing on page 43 for more information.

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.

4.2.2 Creating and Removing a Custom Stack

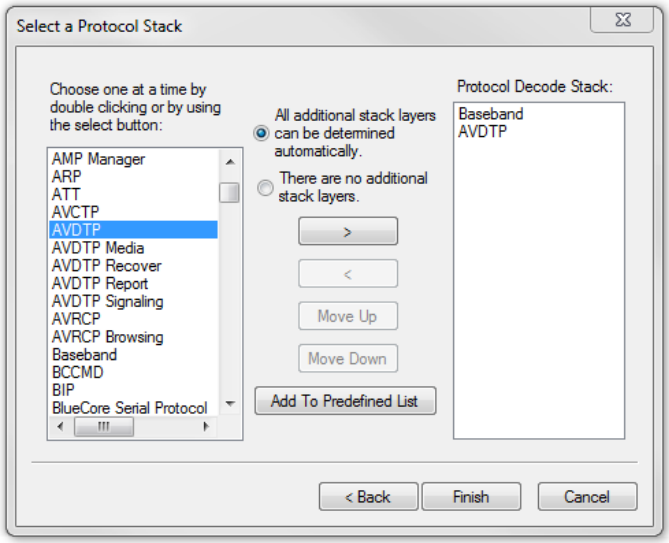
To create a custom stack:

1. Choose Protocol Stack from the Options menu on the Control window or click the Protocol Stack icon on the Frame Display toolbar.
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

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

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.

4.2.3 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 on page 44 for instructions on removing framing from data.

4.2.4 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:

1. 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 by choosing Open from the File menu on the Control window.
2. Select the file to load.
3. Choose Protocol Stack from the Options menu on the Control window
4. Select None from the list
5. Click Finish. The Protocol Stack Wizard asks you if you want to unframe your data and put it into a new file.
6. Choose Yes.

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 on page 43 for instructions on framing unframed data.

4.2.5 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.

4.2.6 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 and the Frame Display window. 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 option 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.

4.3 Analyzing Byte Level Data

4.3.1 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.

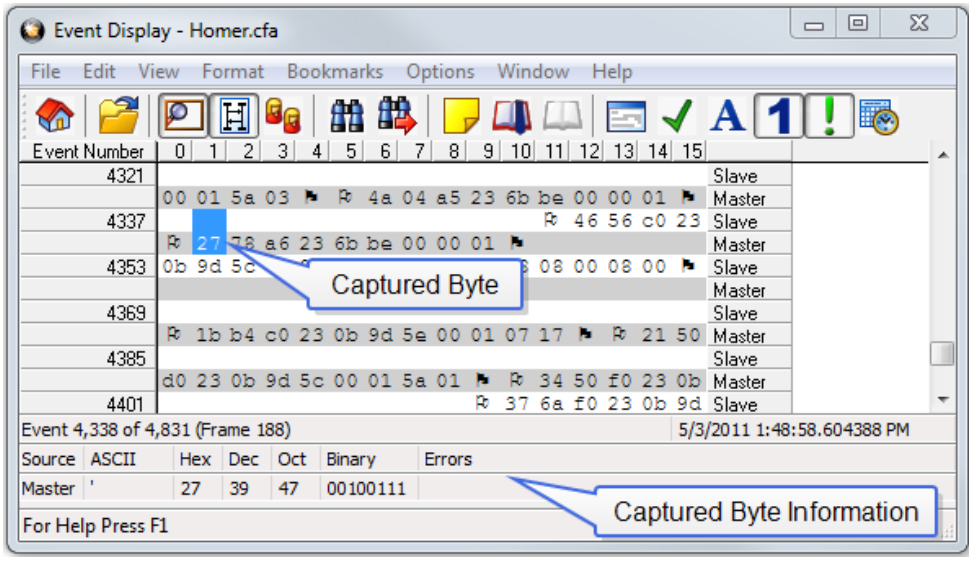


Figure 36. Event Display

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.

Event Display is synchronized with the Frame Display and Mesage Sequence Chart dialogs. Selecting a byte in Event Display will also select the related frame in the Frame Display and the related message in the Message Sequence Chart.

4.3.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Home – Brings the Control window to the front.


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.


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.

4.3.3 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.

4.3.4 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.

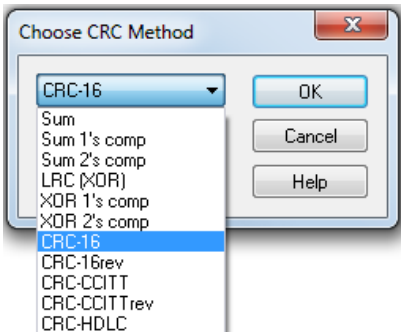
1. Open the Event Display  window.
2. Click and drag to select the data for which you want to generate a CRC.

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.



Calculating CRC for interwoven data

Frontline 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 Frontline calculates the CRC for just the bytes on that side. If the first byte is from the other side, then Frontline 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.

4.3.5 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.

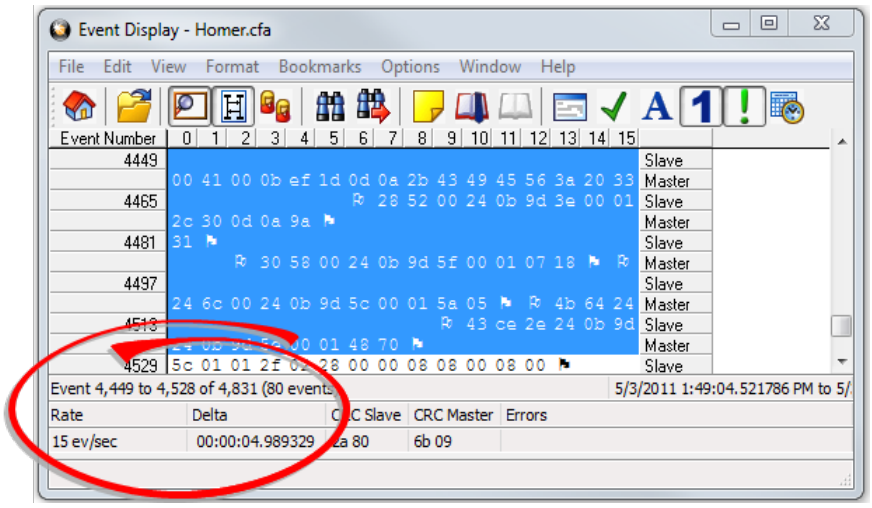


Figure 37. Delta fields

4.3.6 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.

4.3.7 Data Formats and Symbols

4.3.7.1 Switching Between Viewing All Events and Viewing Data Events

By default, the analyzer on the Event Display dialog shows all **events**[1] that include:

[1]An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are I/O Settings changes and Data Capture Paused and Resumed.

- 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 on page 53 for a list of all the special events shown in the analyzer and what they mean.

4.3.7.2 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**[1] used to display data.

Go to the Format menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.

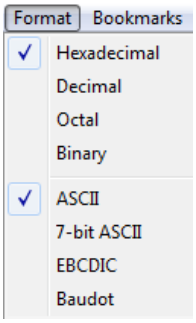


Figure 38. Format Menu

1. Right-click on the data display header labels and choose a different radix.

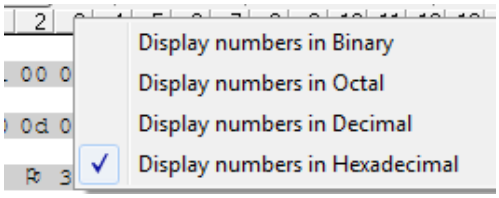


Figure 39. Header labels, right click

2. Or right-click anywhere in the data display and select a different radix.

[1]The base of a number system. Binary is base 2, octal is base 8, decimal is base 10 and hexadecimal is base 16.

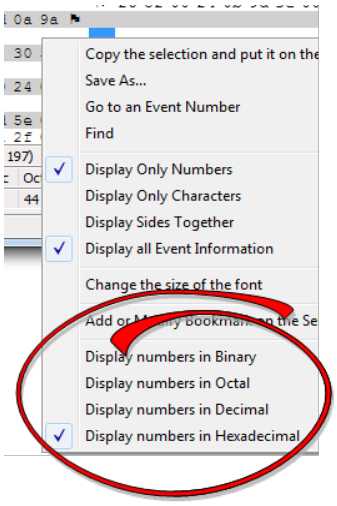


Figure 40. Data display right click menu

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

4.3.7.3 Switching Between ASCII, EBCDIC, and Baudot

On the Event Display window, the analyzer displays data in ASCII by default when you click on the Characters Only icon  . There are several ways to change the character set used to display data.

1. Go to the Format menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. With the data displayed in characters, right-click on the data panel header label to choose a different character set.

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

4.3.7.4 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 (Slave) is shown on a white background and data from the other side (Master)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 in the center of the data display window to change between mixed and side over side modes by selecting Display Sides Together. A check mark is displayed. Click on Display Sides Together to remove the check mark and return to side-by-side display.

4. Right click in the sides panel on the right of the data display and select Display Sides Together. A check mark is displayed. Click on Display Sides Together to remove the check mark and return to side-by-side display.

4.3.7.5 List of all Event Symbols

By default, the Event Display shows all eventsevents[1], 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.

---

[1]An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are I/O Settings changes and Data Capture Paused and Resumed.

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.

I/O Settings Change - A change was made in the I/O Settings window which altered the baud, parity, or other circuit setting.

Long Break

Low Power - The battery in the ComProbe® is low.

Short Break

SPY Event (SPY Mode only) - SPY events are commands sent by the application being spied on to the UART.

Start of Frame - Marks the start of a frame.

Begin Sync Character Strip

End Sync Character Strip

Sync Dropped

Sync Found

Sync Hunt Entered

Sync Lost

Test Device Stopped Responding - The analyzer lost contact with the ComProbe for some reason, often because there is no power to the ComProbe.

Test Device Began Responding - The analyzer regained contact with the ComProbe.

Timestamping Disabled - Timestamping was turned off. Events following this event are not timestamped.

Timestamping Enabled - Timestamping was turned on. Events following this event have timestamps.

Truncated Frame- A frame that is not the same size as indicated within its protocol.

Underrun Error

Unknown Event

4.3.7.6 Font Size

The font size can be changed on several Event Display 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 Event Display menu Options, and select Change the Font Size.

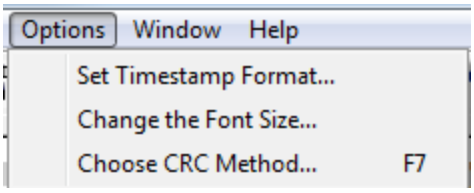


Figure 41. Event Display Options menu

2. Choose a font size from the list.

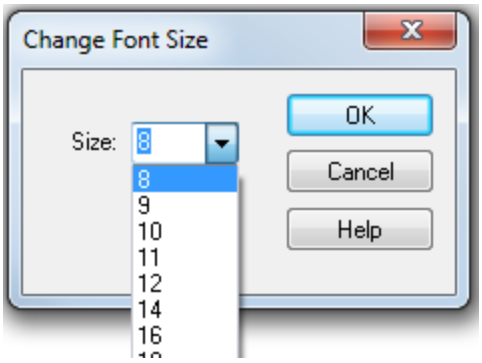


Figure 42. Event Display Font Size Selection

3. Click OK.

4.4 Analyzing Protocol Decodes

4.4.1 Frame Display Window

To open this window

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

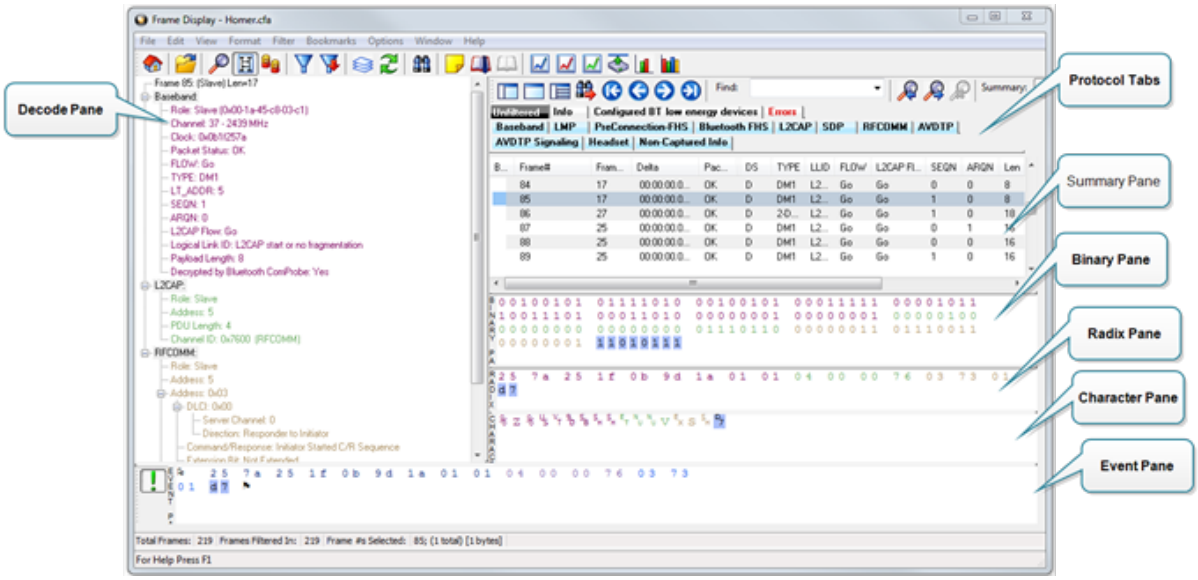


Figure 43. Frame Display with all panes active

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.

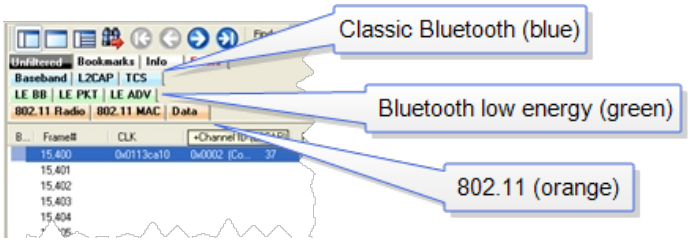
- Summary Pane - The Summary Pane displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.
- Decode Pane - The Decode Pane displays a detailed decode of the highlighted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

Protocol filter tabs are displayed in the Frame Display above the Summary pane.

- These tabs are arranged in separate color-coded groups. These groups and their colors are General (white), Classic Bluetooth (blue), Bluetooth low energy (green), 802.11 (orange), USB (purple), NFC (brown) and SD (teal). The General group applies to all technologies. The other groups are technology-specific.



- Clicking on a protocol filter tab in the General group filters in all packets containing that protocol regardless of each packet's technology.
- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.
- A protocol filter tab appears in the General group only if the protocol occurs in more than one of the technology-specific tab groups. For example, if L2CAP occurs in both Classic Bluetooth and Bluetooth low energy , there will be L2CAP tabs in the General group, the Classic Bluetooth group, and the Bluetooth low energy group.

Select the Unfiltered tab to display all packets.

There are several special tabs that appear in the Summary Pane when certain conditions are met. These tabs appear only in the General group and apply to all technologies. The tabs are:

- Bookmarks appear when a bookmark is first seen.
- Errors appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- Info appears when a frame containing an Information field is first seen.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

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.

Frame Wrapping and Display

In order to assure that the data you are seeing in Frame Display are current, the following messages appear describing the state of the data as it is being captured.

- All Frame Display panes except the Summary pane display "No frame selected" when the selected frame is in the buffer (i.e. not wrapped out) but not accessible in the Summary pane. This can happen when a

tab is selected that doesn't filter in the selected frame.

- When the selected frame wraps out (regardless of whether it was accessible in the Summary pane) all Frame Display panes except the Summary pane display "Frame wrapped out of buffer".
- When the selected frame is still being captured, all Frame Display panes except the Summary pane display "Frame incomplete".

4.4.1.1 Frame Display Toolbar

The buttons that appear in the Frame Display window vary according to the particular configuration of the analyzer. For controls not available the icons will be grayed-out.

Control – 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.

Show Statistics - Opens Statistics 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.

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 re-decoded. 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.

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.

Coexistence View - Opens the Coexistence View

Extract Data - Opens the Extract Data dialog.

Audio Extraction - Opens the Audio Extraction dialog.

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

Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are re-decoded. 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.

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.

Shall All Panes Except Event Pane - Makes the Decode pane taller and the Summary pane narrower.

Toggle Display Lock - Prevents the display from updating.

Go To Frame

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.

Find:

Find on Frame Display only searches the Decode Pane for a value you enter in the text box.

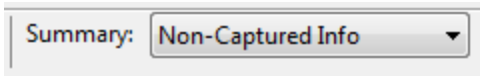
Find Previous Occurrence - Moves to the previous occurrence of the value in the Frame Display Find.

Find Next Occurrence - Moves to the next occurrence of the value in the Frame Display Find.

Cancel Current Search - Stops the current Frame Display Find.

Summary:

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 low energy 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.

Note: 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.

4.4.1.2 Frame Display Status Bar

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

- Frame #s Selected: Displays the frame number or numbers of selected (highlighted) frames, and the total number of selected frames in parentheses
- 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

4.4.1.3 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.

4.4.1.4 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 resulting byte values after escape codes or other character altering codes have been applied (a process called transformation).

As an example, bytes with a value of less than 0x20 (the 0x indicates a hexadecimal value) cannot be transmitted in Async PPP. To get around this, a 0x7d is transmitted before the byte. The 0x7d says to take the next byte and subtract 0x20 to obtain the true value. In this situation, the Event pane displays 0x7d 0x23, while the Radix pane displays 0x03.

4.4.1.5 Sorting Frames

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.

4.4.1.6 Frame Display - Find

Frame Display has a simple Find function that you can use to search the Decode Pane for any alpha numeric value. This functionality is in addition to the more robust Search/Find dialog.

Frame Display Find is located below the toolbar on the Frame Display dialog.

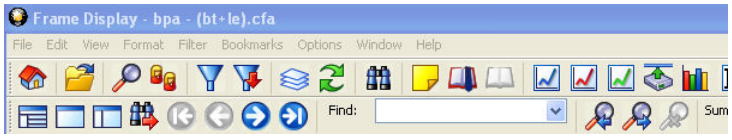


Figure 44. Frame Display Find text entry field

Where the more powerful Search/Find functionality searches the Decode, Binary, Radix, and Character panes on Frame Display using TImestamps, Special Events, Bookmarks, Patterns, etc.,

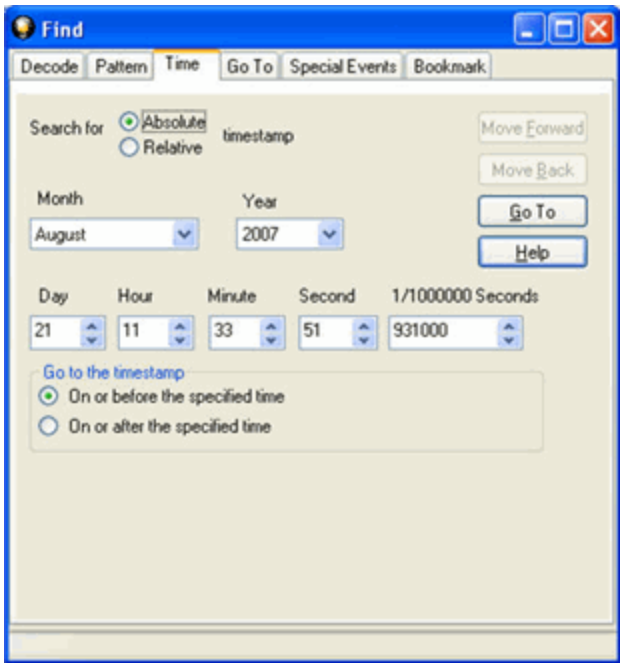


Figure 45. Search/Find Dialog

Find on Frame Display only searches the Decode Pane for a value you enter in the text box.

To use Find:

1. Select the frame where you want to begin the search.

2. Enter a value in the Find text box. 

Note: Note: The text box is disabled during a live capture.

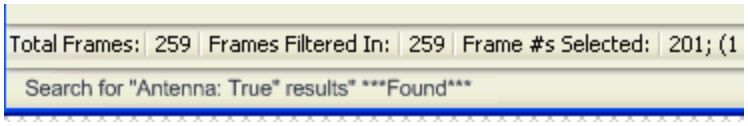
Select Find Previous Occurrence to begin the search on frames prior to the frame you selected, or Find Next Occurrence to begin the search on frames following the frame you selected.

The next occurrence of the value (if it is found) will be highlighted in the Decode Pane.

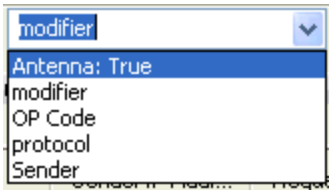
4. Select Find Previous Occurrence or Find Next Occurrence to continue the search.

There are several important concepts to remember with Find.

- When you enter a search string and select Enter, the search moves forward.
- If you select Find Previous Occurrence, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous Occurrence.
- If you select Find Next Occurrence, when the search reaches the last frame it will then cycle to the first frame and continue until it reaches the frame where the search began.
- F3 is a shortcut for Find Next Occurrence.
- You cannot search while data is being captured.
- After a capture is completed, you cannot search until Frame Display has finished decoding the frames.
- Find is not case sensitive.
- The status of the search is displayed at the bottom of the dialog.



- The search occurs only on the protocol layer selected.
- To search across all the protocols on the Frame Display, select the Unfiltered tab.
- A drop-down list displays the search values entered during the current session of Frame Display.



- The search is cancelled when you select a different protocol tab during a search.
- You can cancel the search at any time by selecting the Cancel Current Search  button.

4.4.1.7 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.

4.4.1.8 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.

Note: When you have multiple Frame Display windows open and you are capturing data, you may receive an error message declaring that "Filtering cannot be done while receiving data this fast." If this occurs, you may have to stop filtering until the data is captured.

4.4.1.9 Working with Panes on Frame Display

When the Frame Display first opens, all panes are displayed except the Event pane (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.

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.

To open a pane, right-click on the any pane and select 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.

To re-size a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to re-size the pane.

4.4.1.10 Frame Display - Byte Export

The captured frames can be exported as raw bytes to a text file.

1. From the Frame Display File menu select Byte Export….

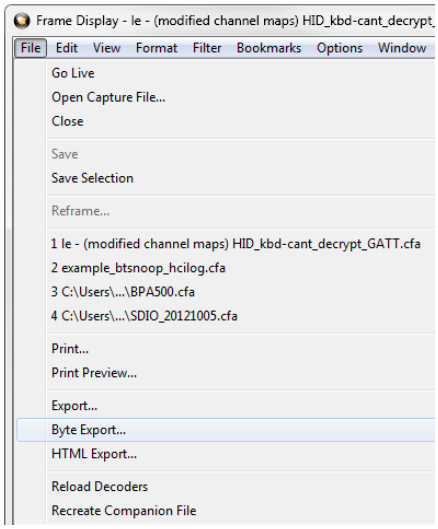


Figure 46. Frame Display File menu, Byte Export

2. From the Byte Export window specify the frames to export.

   - All Frames exports all filtered-in frames including those scrolled off the Summary pane. Filtered-in frames are dependent on the selected Filter tab above the Summary pane. Filtered-out frames are not exported.
   - Selected Frames export is the same as **All Frames** export except that only frames selected in the Summary pane will be exported.

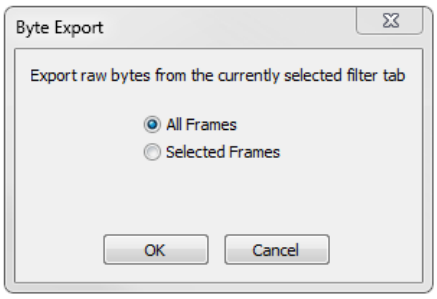


Figure 47. Byte Export dialog

Click the **OK** button to save the export. Clicking the **Cancel** button will exit Byte Export.

3. The Save As dialog will open. Select a directory location and enter a file name for the exported frames file.

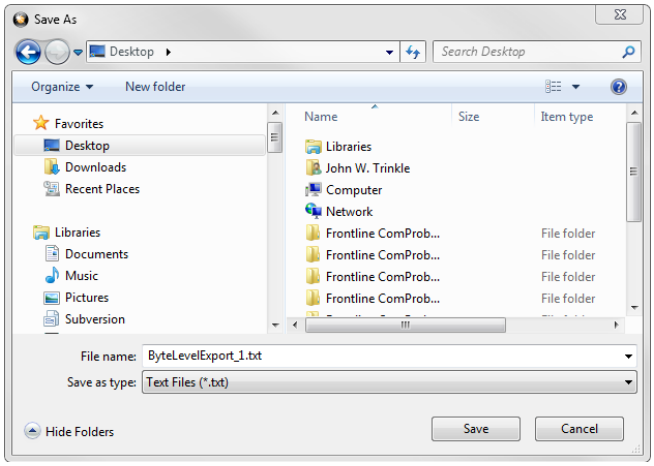


Figure 48. Save As dialog

Click on the Save button.

The exported frames are in a text file that can be opened in any standard text editing application. The header shows the export type, the capture filename, the selected filter tab, and the number of frames. The body shows the frame number, the timestamp in the same format shown in the Frame Display Summary pane, and the frame contents as raw bytes.

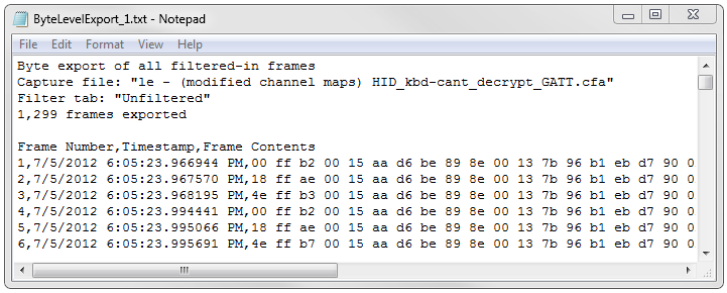


Figure 49. Sample Exported Frames Text File

4.4.1.11 Panes in the Frame Display

4.4.1.11.1 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 ComProbe USB Summary pane in 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.

Protocol Tabs

Protocol filter tabs are displayed in the Frame Display above the Summary pane.

- These tabs are arranged in separate color-coded groups. These groups and their colors are General (white), Classic Bluetooth (blue), *Bluetooth* low energy (green), 802.11 (orange), USB (purple), and SD (brown). The General group applies to all technologies. The other groups are technology-specific.

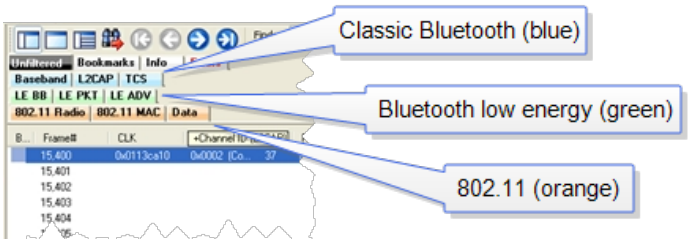


Figure 50. Example Protocol Tags

- Clicking on a protocol filter tab in the General group filters in all packets containing that protocol regardless of each packet’s technology.
- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.

- A protocol filter tab appears in the General group only if the protocol occurs in more than one of the technology-specific tab groups. For example, if L2CAP occurs in both Classic *Bluetooth* and *Bluetooth* low energy , there will be L2CAP tabs in the General group, the Classic *Bluetooth* group, and the *Bluetooth* low energy group.

Select the Unfiltered tab to display all packets.

There are several special tabs that appear in the Summary pane when certain conditions are met. These tabs appear only in the General group and apply to all technologies. The tabs are:

- Bookmarks appear when a bookmark is first seen.
- Errors appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- Info appears when a frame containing an Information field is first seen.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

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.

Placing the mouse pointer on a summary pane header with truncated text displays a tooltip showing the full header text.

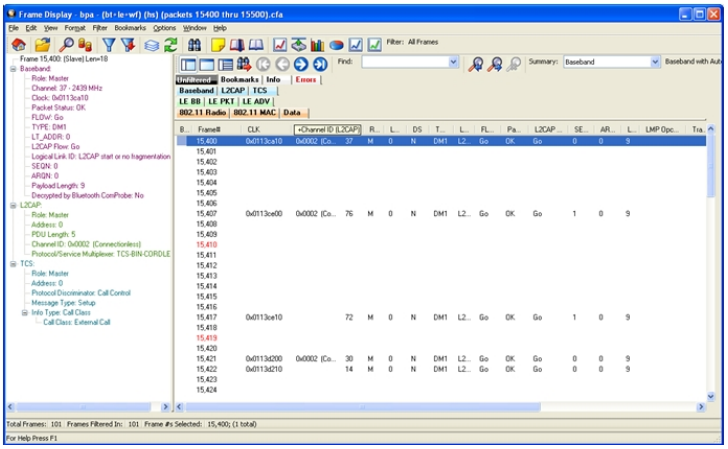


Figure 51. Summay pane (right) with Decoder pane (left)

Sides in *Bluetooth* low energy

A Bluetooth low energy data connection consists of connection events, which are a series of transmissions on the same channel. In each connection event the master transmits first, then the slave, and then the devices take turns until the connection event is finished.

When the data connection is encrypted and the packets are successfully decrypted, the sniffer can determine exactly who sent which packet (only non-empty, encrypted packets – empty packets are never encrypted). These packets are labeled either 'M' for master or 'S' for slave.

When the data connection is unencrypted or when encrypted packets are not successfully decrypted by the sniffer, the sniffer cannot distinguish the two devices' (master and slave) packets by their content, just by the packet timing. In those cases we label each device as side '1' or '2', not as master or slave. In each connection event, packets sent by the device which transmitted first in the connection event are labeled '1', and packets sent by the device which transmitted second are labeled '2'.

If no packets in the connection event are missed by the sniffer, the device labeled '1' is the master and the device labeled '2' is the slave. However, if we do not capture the very first packet in a connection event (i.e. the packet sent by the master) but do capture the packet sent by the slave, we label the slave as side '1' since it is the first device we heard in the connection event. Because there is potential clock drift since the last connection event, we cannot use the absolute timing to correct this error; there would still be cases where we get it wrong. Therefore we always assign '1' to the first packet in a connection event. So even though it is rare, there are connection events where packets sent by the slave device are labeled '1' and packets sent by the master are labeled '2'.

Finally, in a noisy environment it is also possible that the sniffer does not capture packets in the middle of a connection event. If this occurs and the sniffer cannot determine the side for the remaining packets in that connection event, the side is labeled 'U' for "unknown".

4.4.1.11.2 Customizing Fields in the Summary Pane

You can modify the Summary Pane in Frame Display.

Summary pane columns can be reordered by dragging any column to a different position.

Fields from the Decode pane can be added to the summary pane by dragging any Decodepane field to the desired location in the summary pane header. If the new field is from a different layer than the summary pane a plus sign (+) is prepended to the field name and the layer name is added in parentheses. The same field can be added more than once if desired, thus making it possible to put the same field at the front and back (for example) of a long header line so that the field is visible regardless of where the header is scrolled to.

An added field can be removed from the Summary pane by selecting Remove New Column from the right-click menu.

The default column layout (both membership and order) can be restored by selecting Restore Default Columns from the Format or right-click menus.

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.

4.4.1.11.3 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.

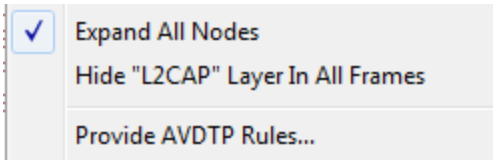
A green circle means the frame was not fully decoded. There are several reasons why this might happen.

- 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.

4.4.1.11.4 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

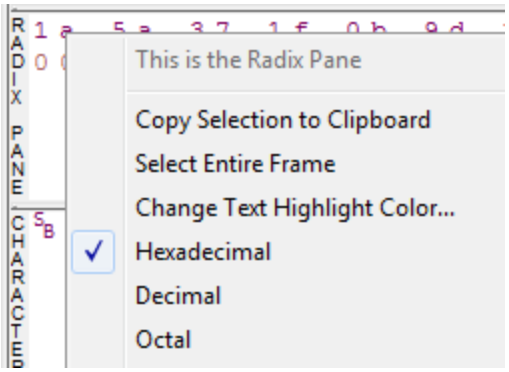
Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the Event, Radix, Binary and Character panes. The colors are not assigned to a protocol, but are assigned to the layer.

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.

4.4.1.11.5 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.



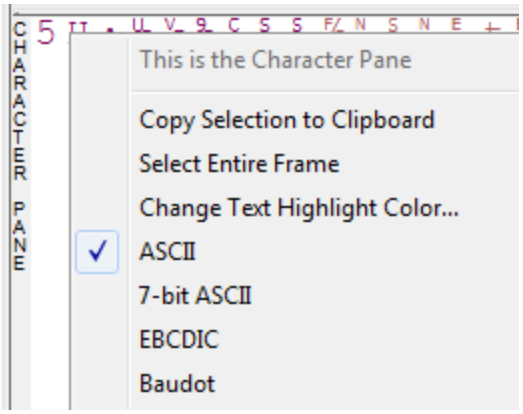
Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

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.

4.4.1.11.6 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.

4.4.1.11.7 Binary Pane

The Binary pane displays the logical bytes in the frame in binary.

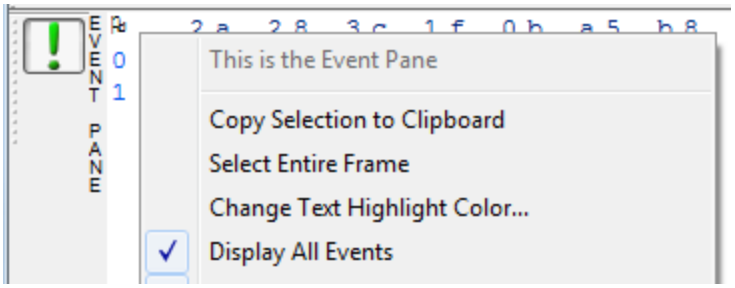
Because the Binary pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

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.

4.4.1.11.8 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.

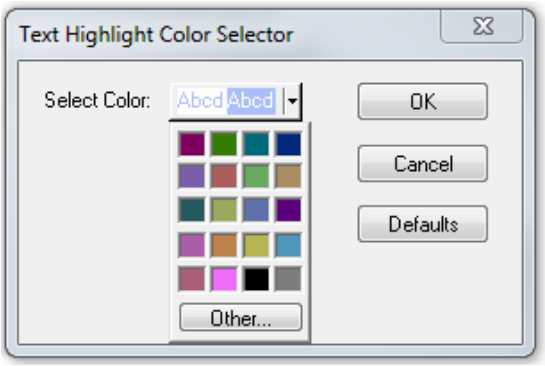
Because the Event pane displays the physical bytes rather than the logical bytes, the data in the Event pane may be different from that in the Radix, Binary and Character panes. See Physical vs. Logical Byte Display for more information.

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.

4.4.1.11.9 Change Text Highlight Color

Whenever you select text in the Binary, Radix, or Character panes in Frame Display, the text is displayed with a highlight color. You can change the color of the highlight.



1. Select Change Text Highlight Color from the Options menu. You can also access the option by right clicking in any of the panes.
2. Select a color from the drop-down menu.
3. Click OK.

The highlight color for the text is changed.

Select Cancel to discard any selection. Select Defaults to return the highlight color to blue.

4.4.1.12 Protocol Layer Colors

4.4.1.12.1 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. Also, the Errors tab is displayed in red. 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.

4.4.1.12.2 Changing Protocol Layer Colors

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

1. Choose Select Protocol Layer Colors from the Options menu to change the colors used.

   The colors for the different layers is displayed.
2. To change a color, click on the arrow next to each layer and select a new color.
3. Select OK to accept the color change and return to Frame Display.

Select Cancel to discard any selection. Select Defaults to return the highlight colors to the default settings.

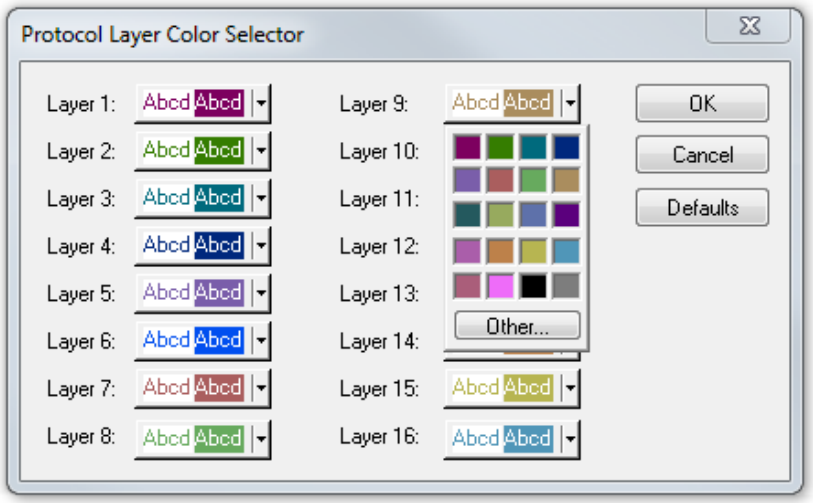


Figure 52. Frame Display Protocol Layer Color Selector

4.4.1.13 Protocol Filtering From the Frame Display

4.4.1.13.1 Quick Filtering on a Protocol Layer

On the Frame Display , click the 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.

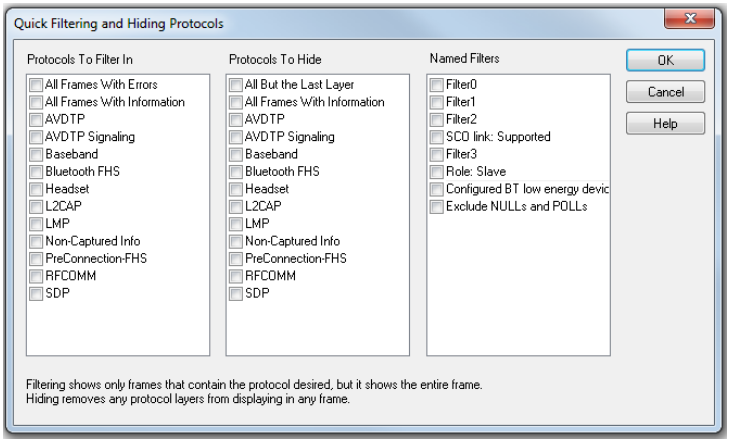


Figure 53. Frame Display Quick Filtering and Hiding Protocols Dialog

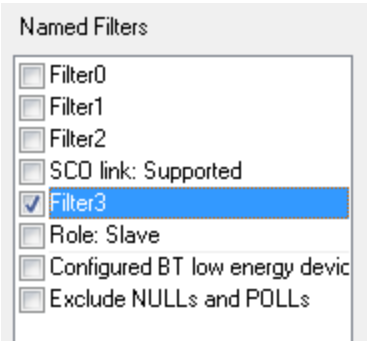
The box on the left is Protocols To Filter In. When you select the checkbox for a protocol in the Protocols to Filter In, the Summary pane will only display those frames that contain data from that protocol.

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. 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.

Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.

Then click OK

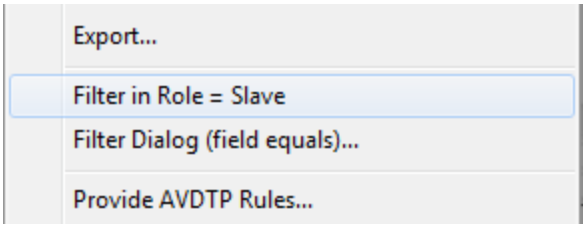
4.4.1.13.2 Frame Display - Right Click Filtering

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, where name is the column name and value is the column-value to filter. For our example "Filter in Role = Slave" appears in the menu.

   The Filtering Results dialog appears.
3. Enter a name for the Filter or use the default name.
4. Click 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.

4.4.1.13.3 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.

4.4.1.13.3.1 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 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.

4.4.1.13.3.2 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 "Errors" that displays the results of the All Frames With Errors filter. 

Note: When you have multiple Frame Display windows open and you are capturing data, you may receive an error message declaring that "Filtering cannot be done while receiving data this fast." If this occurs, you may have to stop filtering until the data is captured.

4.4.2 Coexistence View

The Coexistence View displays Classic Bluetooth, *Bluetooth* low energy, and 802.11 packets and throughput in one view. You access the Coexistence View by clicking its button  in the Control window or Frame Display toolbars, or Coexistence View from the View menus.

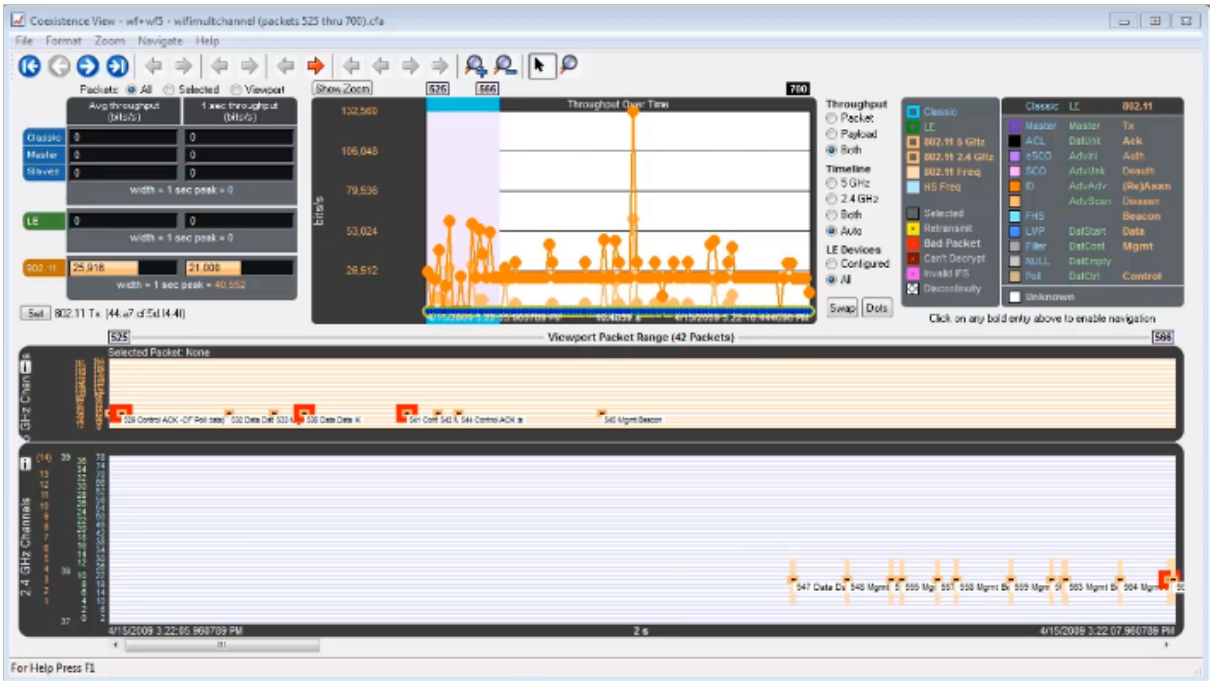


Figure 54. Coexistence View Window

Coexistence View – Toolbar

4.4.2.1 Coexistence View - Toolbar

Figure 55. Coexistence View Toolbar

The toolbar contains the following:


Move to the first packet.


Move to the previous packet.


Move to the next packet.


Move to the last packet.


Move to the previous retransmitted packet.

 Move to the next retransmitted packet

 Move to the previous invalid IFS for *Bluetooth* low energy.

 Move to the next invalid IFS for *Bluetooth* low energy.

 Move to the previous bad packet.

 Move to the next bad packet.

 Move to the first packet of the type selected in the legend.

 Move to the previous packet of the type selected in the legend

 Move to the next packet of the type selected in the legend.

 Move to the last packet of the type selected in the legend.

 Zoom in.

 Zoom out.

 Scroll cursor.

 When selected the cursor changes from scroll  to a context-aware zooming cursor  . Click on normal cursor to remove the zooming cursor.

Scroll Lock/Unlock during live capture mode.

Reset during live capture mode. Clears the display.

Coexistence View - Throughput Indicators

4.4.2.2 Coexistence View - Throughput Indicators

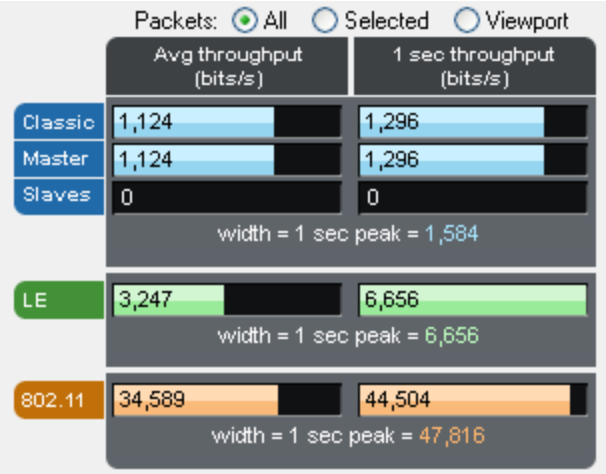


Figure 56. Coexistence View Throughput Indicators

Throughput indicators show average throughput and 1 second throughput for Classic Bluetooth (all devices, master devices, and slave devices are each shown separately), *Bluetooth* low energy, and 802.11.

Throughput

4.4.2.2.1 Throughput

Throughput is total packet or payload size in bits of the included packets divided by the duration of the included packets, where:

- *Packet size* is used if the Packet or Both radio button is selected in the Throughput group.
- *Payload size* is used if the Payload radio button is selected in the Throughput group.
- *Included packets* are defined separately for each of the radio buttons that appear above the throughput indicators.
- *Duration of the included packets* is measured from the beginning of the first included packet to the end of the last included packet.

4.4.2.2.1.1 Radio Buttons

The radio buttons above the throughput indicators specify which packets are *included*. Radio button descriptions are modified per the following:

- *Bluetooth* low energy packets from non-configured devices are excluded if the Configured radio button in the LE Devices group is selected.

- Frame Display filtering has no effect here in that packets that are filtered-out in Frame Display are still used here as long as they otherwise meet the criteria for each radio button as described below.

4.4.2.2.1.2 All radio button

All packets are used for average throughput, and packets occurring in the last 1 second of the session are used for 1 second throughput, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

4.4.2.2.1.3 **Selected radio button**

Selected packets (the selected packet range is shown in the timeline header) are used for average throughput, and packets in the 1 second duration ending at the end of the last selected packet are used for 1 second, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

Figure 57. Timeline Header Showing Selected Packets

4.4.2.2.1.4 Viewport radio button

The viewport is the purple rectangle in the Throughput Graph and indicates a specific starting time, ending time, and resulting duration. Packets that occur within that range of time are used for average throughput,and packets in the 1 second duration ending at the end of the last packet in the viewport time range are used for 1 second throughput, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

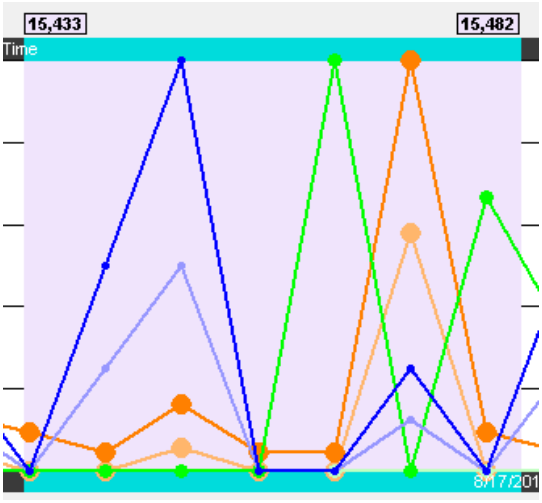


Figure 58. Throughput Graph viewport.

4.4.2.2.2 Indicator width

The width of each indicator is the largest 1 second throughput seen up to that point for that technology (Classic *Bluetooth*, *Bluetooth* low energy, or 802.11), where the 1 second throughput is calculated anew each time another packet is received. The 1 second throughput indicator will never exceed this width, but the average throughput indicator can. For example, the image below has a large average throughput because the Selected radio button was selected and a single packet was selected, and the duration in that case is the duration of the single packet, which makes for a very small denominator in the throughput calculation. When the average throughput exceeds the indicator width, a plus sign (+) is drawn at the right end of the indicator.

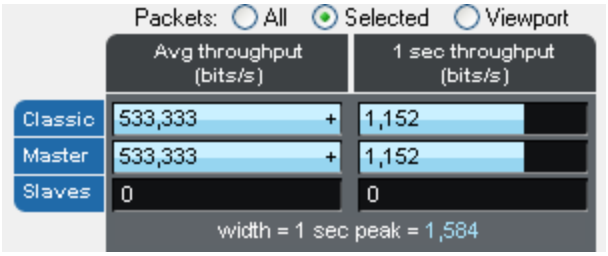


Figure 59. Average throughput indicators show a plus sign (+) when the indicator width is exceeded.

Figure 60. A single selected packet

4.4.2.3 Coexistence View - Set Button

The Set button is used to specify the 802.11 source address, where any packet with that source address is considered a Tx packet and is shown with a purple border in the timelines.

All source MAC addresses that have been seen during this session are listed in the dialog that appears when the Set button is clicked. Also listed is the last source MAC address that was set in the dialog in the previous session. If that address has not yet been seen in this session, it is shown in parentheses.

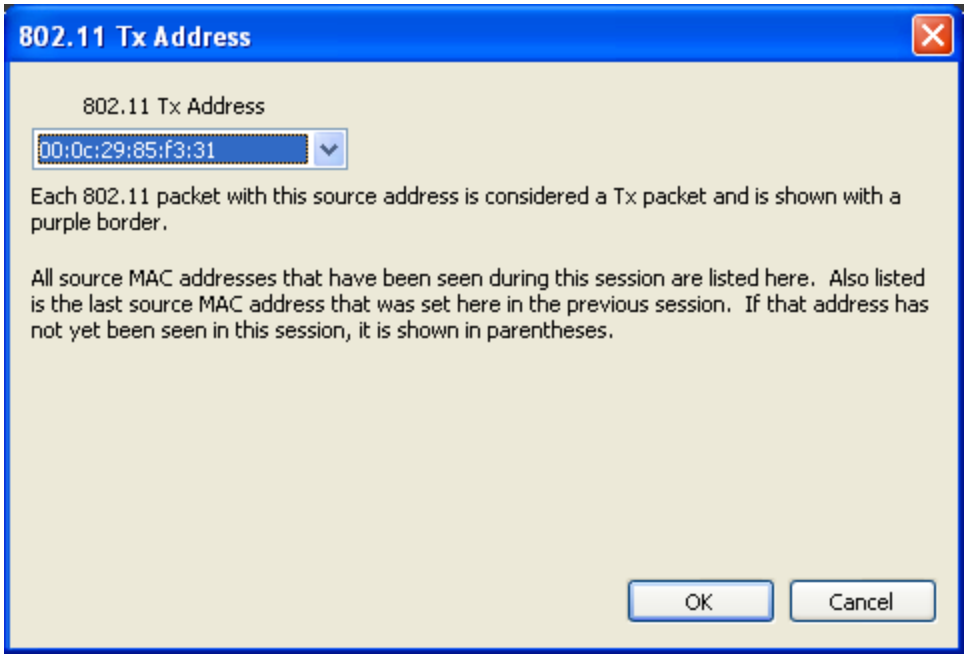


Figure 61. 802.11 Source Address Dialog

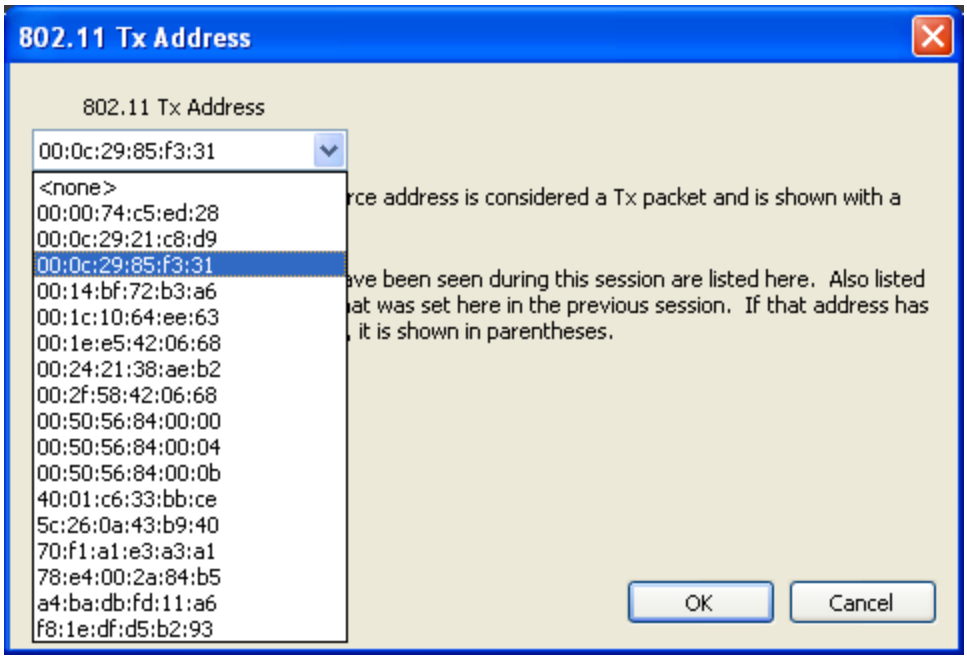


Figure 62. 802.11 Source Address Drop Down Selector

4.4.2.4 Coexistence View - Throughput Graph

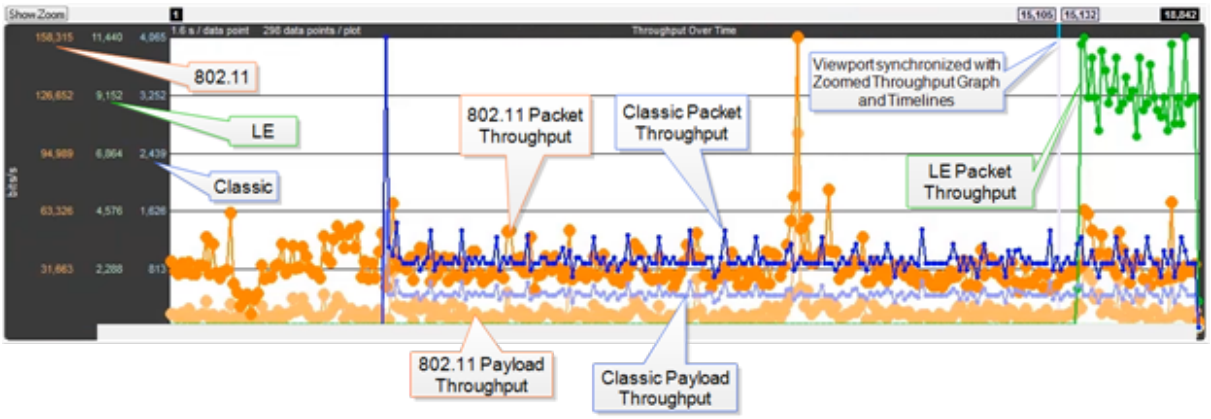


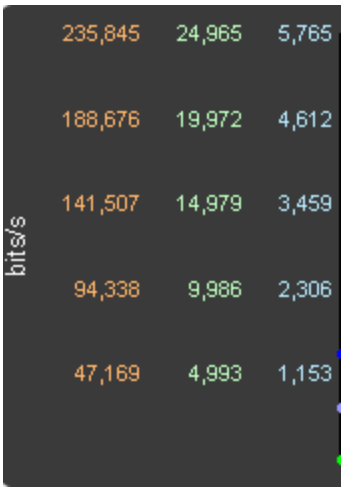
Figure 63. Coexistence View Throughput Graph

The Throughput Graph is a line graph that shows packet and/or payload throughput over time as specified by the radio buttons in the Throughput group. If the Both radio button is selected, packet and payload throughput are shown as two separate lines for each technology. The payload throughput line is always below the packet throughput line (unless both are 0).

The data lines and y-axis labels are color-coded: Blue = Classic Bluetooth, Green = *Bluetooth* low energy, Orange = 802.11. Each data point represents a duration which is initially 0.1 s. Each time the number of data points per line reaches 300, the number of data points per line is halved to 150 and the duration per data point is doubled. The duration per data point thus progresses from 0.1 s to 0.2 s to 0.4 s to 0.8 s and so on.

4.4.2.4.1 Throughput Graph Y-axis labels

The y-axis labels show the throughput in bits per second. From left-to-right the labels are for 802.11, *Bluetooth* low energy, and Classic *Bluetooth*. The duration of each data point must be taken into account for the y-axis label's value to be meaningful. For example, if a data point has a duration of 0.1 s and a bit count of 100, it will have a throughput of 1,000 bits/s, and the y-axis labels will be consistent with this.



Throughput Graph y-axis labels.

4.4.2.4.2 Excluded packets

Retransmitted packets and bad packets (packets with CRC or Header errors) are excluded from throughput calculations.

4.4.2.4.3 Tooltips

Placing the mouse pointer on a data point shows a tooltip for that data point. The tooltip first line shows the throughput, the throughput type (packet or payload), and the technology. Subsequent lines show the bit count, the duration of the data point, the packet range of that duration (only packets of the applicable technology from that packet range are used for the throughput calculation), and the number of the data point (which is 0 for the first data point in each line).

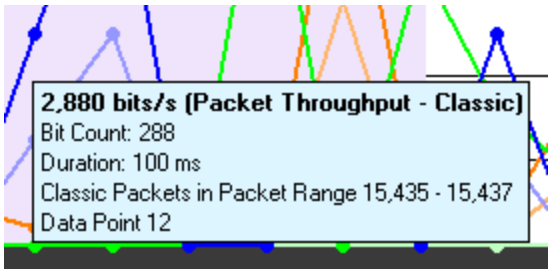


Figure 64. Data point tooltip

The Throughput graph tool tips can be shown in the upper-left corner of your computer screen to provide an unobstructed view. Refer to Relocating Tool Tips.

4.4.2.4.4 Discontinuities

A discontinuity is when the timestamp going from one packet to the next either goes backward by any amount or forward by more than 4.01 s. This value is used because the largest possible connection interval in *Bluetooth* low energy is 4.0 s. A discontinuity is drawn as a vertical dashed line. A discontinuity for a timestamp going backward is called a negative discontinuity and is shown in red. A discontinuity for a timestamp going forward by more than 4.01 s is called a positive discontinuity and is shown in black. A positive discontinuity is a cosmetic nicety to avoid lots of empty space. A negative discontinuity is an error.

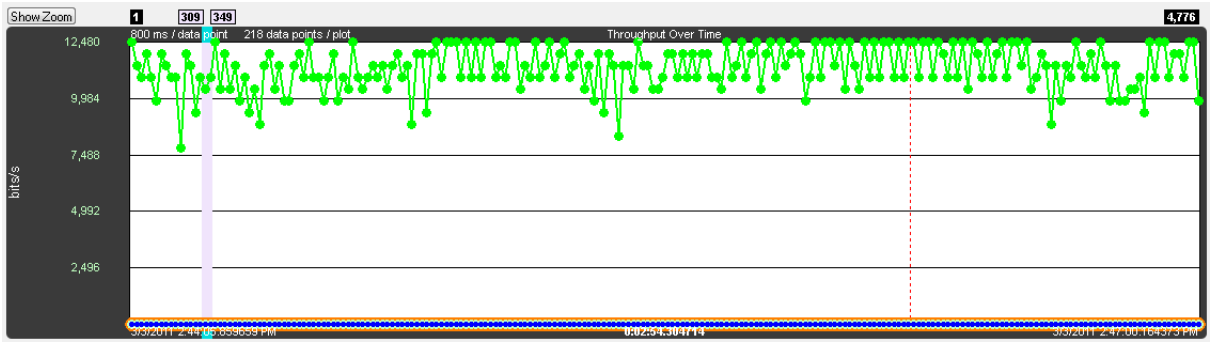


Figure 65. A negative discontinuity.

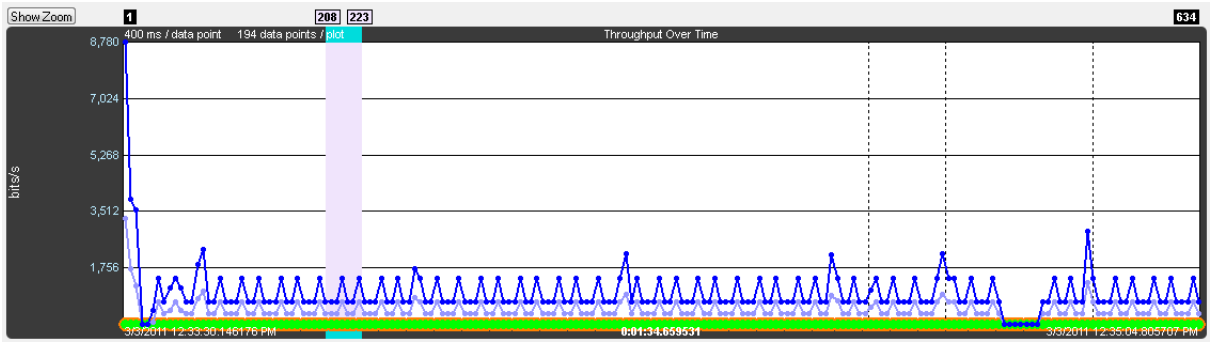


Figure 66. Three positive discontinuities.

4.4.2.4.5 Viewport

The viewport is the purple rectangle in the Throughput Graph. It indicates a specific starting time, ending time, and resulting duration, and is precisely the time range used by the Timeline. The packet range that occurs within this time range is shown above the sides of the viewport.

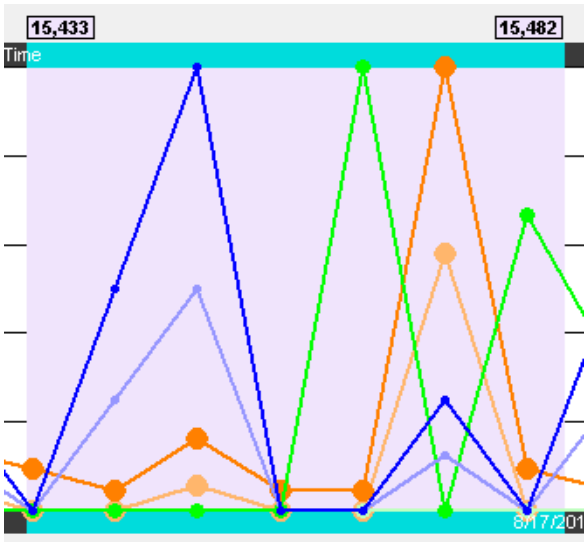


Figure 67. Throughput Graph Viewport

The viewport is moved by dragging it or by clicking on the desired location in the Throughput Graph (the viewport will be centered at the click point).

The viewport is sized by dragging one of its sides or by using one of the other zooming techniques. See the Zooming subsection in the Timeline section for a complete list.

Swap button

The Throughput Graph and Timeline can be made to trade positions by clicking the Swap button.

Clicking the Swap [Swap] button swaps the positions of the Throughput Graphs and the Timelines.

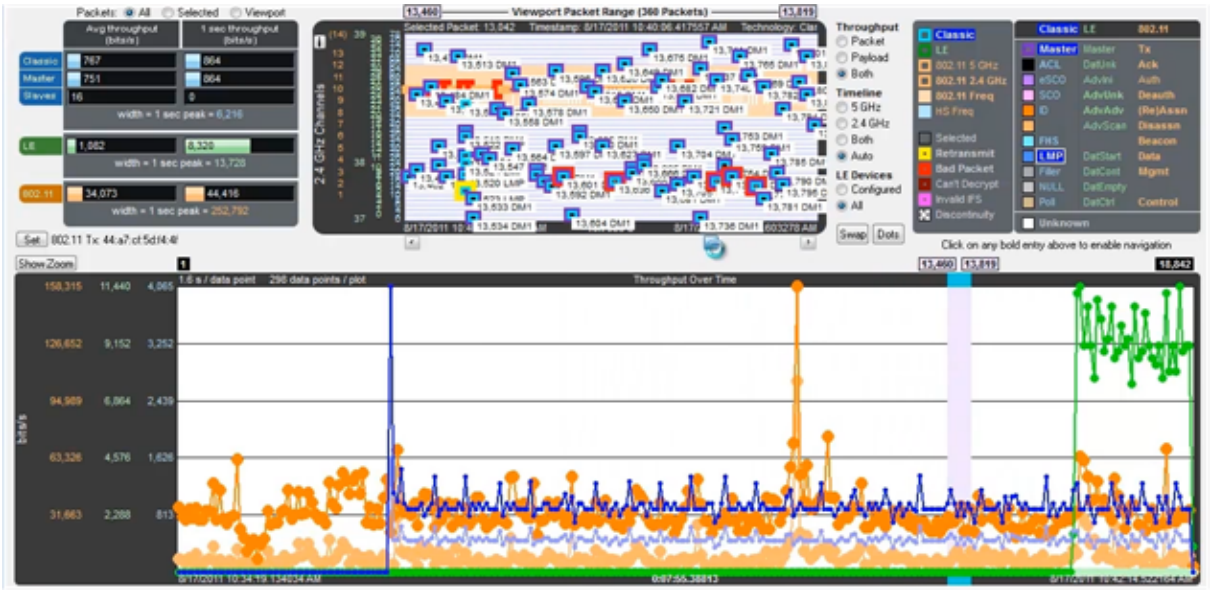


Figure 68. Small Timeline and large Throughput Graph after pressing the Swap button.

4.4.2.4.6 Dots button

The dots on the data points can be toggled on and off by clicking the Dots [Dots] button. Dots are different sizes for each technology so that they reveal overlapping data points which otherwise wouldn't be visible. A tooltip can be displayed for each dot.

Dots can be removed for greater visibility of the plots when data points are crowded together.

Figure 69. Dots Toggled On and Off

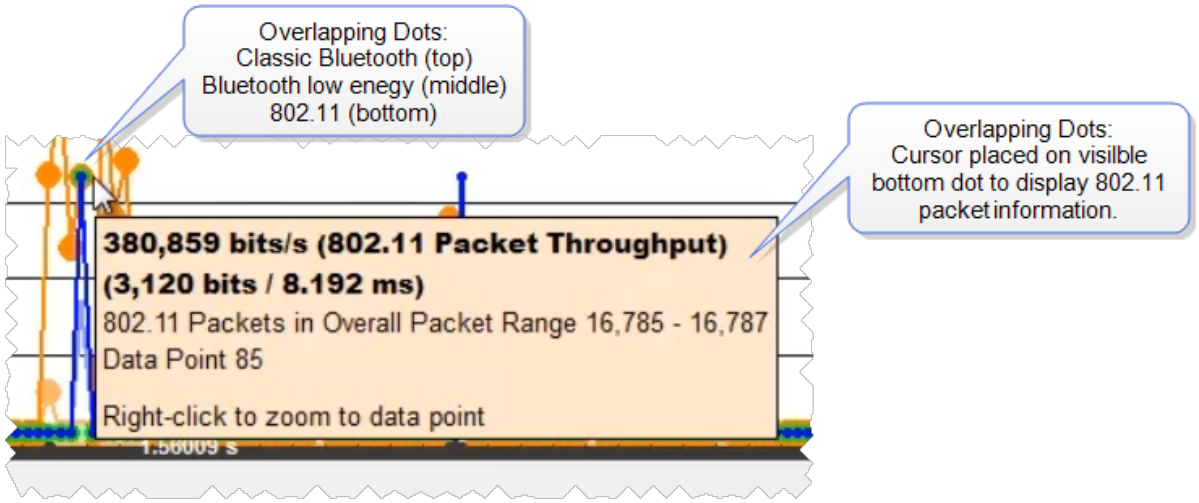


Figure 70. Overlapping Dots Information Display

4.4.2.4.7 Zoomed Throughput Graph

Clicking the Show Zoom button 

displays the Zoomed Throughput Graph above the Throughput Graph. The Zoomed Throughput Graph shows the details of the throughput in the time range covered by the viewport in the Throughput Graph. Both the Zoomed Throughput Graph and the Timelines are synchronized with the Throughput Graph's viewport. The viewport is sized by dragging one of its sides or by using one of the other zooming techniques listed in the Zooming subsection in the Timelines section.

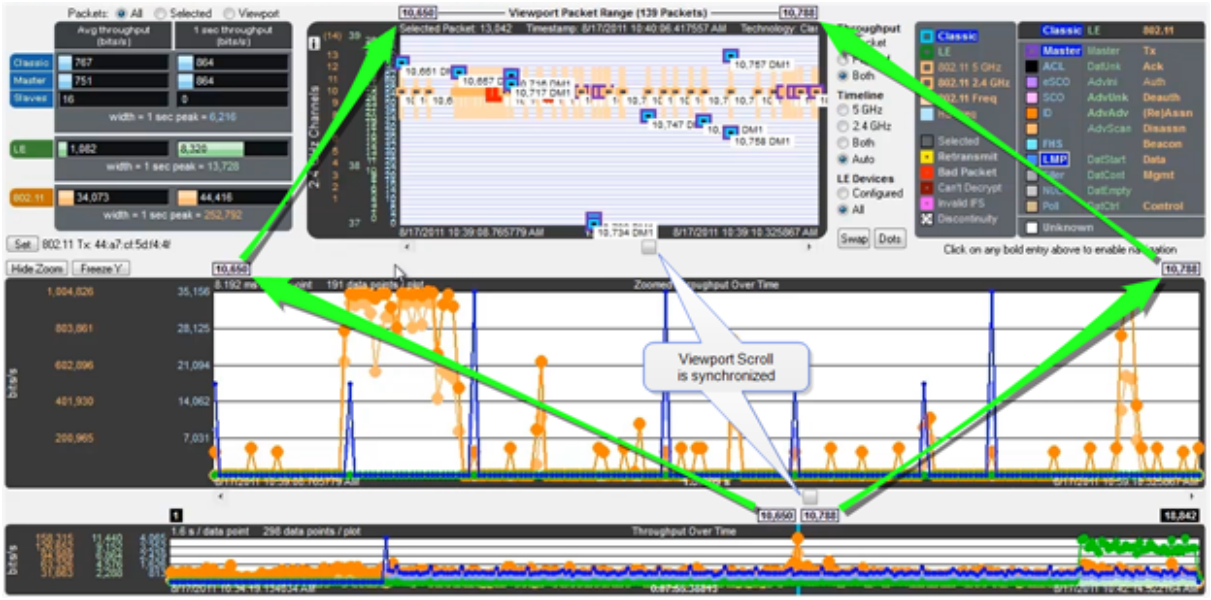
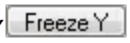


Figure 71. Synchronized Zoomed Throughput Graph and Throughput Graph

The largest value in each technology in the Zoomed Throughput Graph is snapped to the top of the graph. This makes the graph easier to read by using all of the available space, but because the y-axis scales can change it can make it difficult to compare different time ranges or durations. Clicking the Freeze Y 

button freezes the y-axis scales and makes it possible to compare all time ranges and durations (the name of the button changes toUnfreeze Y and aY Scales Frozen indicator appears to the right of the title. Clicking the Unfreeze Y 

button unfreezes the y-axis scales.

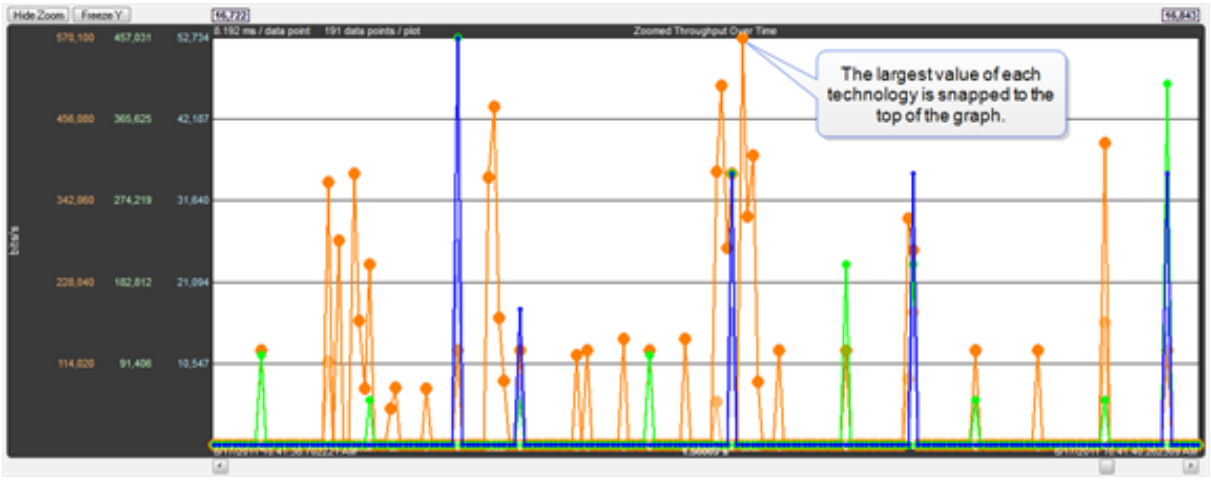


Figure 72. Zoomed Throughput GraphUnfreeze Y- Largest Value Snaps to Top

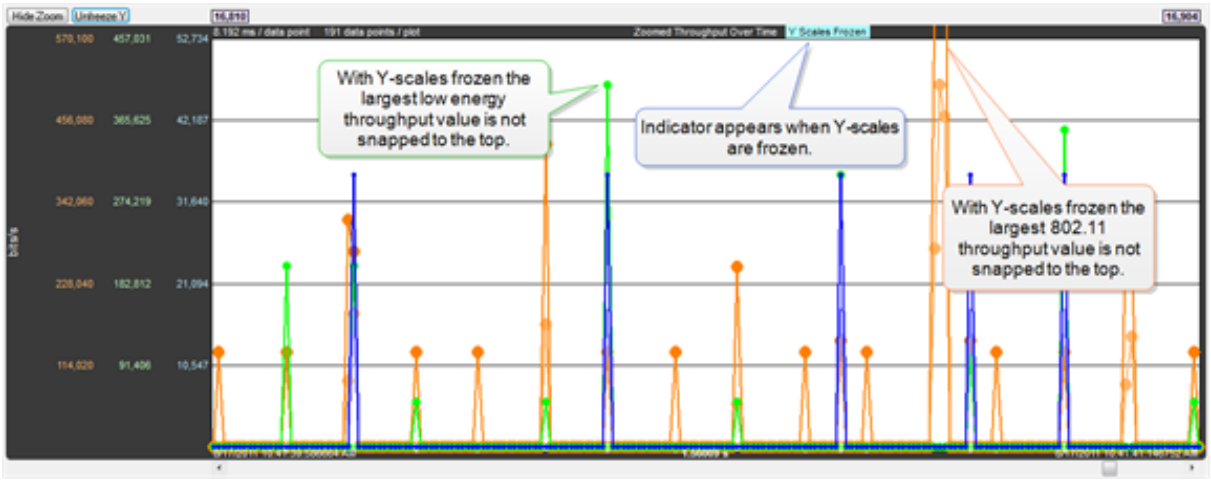


Figure 73. Zoomed Throughput GraphFreeze Y - Largest Value Snaps to Top

4.4.2.4.8 Zoom Cursor

Selecting the Zoom Cursor  button changes the cursor to the zoom cursor  . The zoom cursor is controlled by the mouse wheel and zooms the viewport and thus the Timelines and the Zoomed Throughput Graph. The zoom cursor appears everywhere except the Throughput Graph, which is not zoomable, in which case the scroll cursor is shown. When the zoom cursor is in the Timelines or Zoomed Throughput Graph zooming occurs around the point in time where the zoom cursor is positioned. When the zoom cursor is outside the Timelines and the Zoomed Throughput Graph the left edge of those displays is the zoom point.

4.4.2.4.9 Comparison with the Bluetooth Timeline's Throughput Graph

The Throughput Graphs for Classic *Bluetooth* in the Coexistence View and the *Bluetooth* Timeline can look quite different even though they are plotting the same data. The reason is that the Coexistence View uses timestamps while the *Bluetooth* Timeline uses *Bluetooth* clocks, and they do not always match up exactly. This mismatch can result in the data for a particular packet being included in different intervals in the two Throughput Graphs, and can have a significant impact on the shapes of the two respective graphs. This can also result in the total duration of the two Throughput Graphs being different.

Another factor that can affect total duration is that the *Bluetooth* Timeline's Throughput Graph stops at the last Classic *Bluetooth* packet while the Coexistence View's Throughput Graph stops at the last packet regardless of technology.

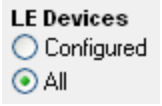
4.4.2.5 Coexistence View - Throughput Radio Buttons

The radio buttons in the Throughput group specify whether to show packet and/or payload lines in the Throughput Graph, and also whether to show packet or payload throughput in the throughput indicators (if the Both radio button is selected, packet throughput is shown in the throughput indicators).

4.4.2.6 Coexistence View - Timeline Radio Buttons

The radio buttons in the Timeline group specify timeline visibility. The first three buttons specify whether to show one or both timelines, while the Auto button shows only timelines which have had packets at some point during this session. If no packets have been received at all and the Auto button is selected the 2.4 GHz timeline is shown.

4.4.2.7 Coexistence View – LE Devices Radio Buttons



The radio buttons in the LE Devices group (where "LE" means Bluetooth low energy) specify both visibility and inclusion in throughput calculations of *Bluetooth* low energy packets. The All radio button shows and uses all *Bluetooth* low energy packets. The Configured radio button shows and uses only *Bluetooth* low energy packets which come from a configured device.

4.4.2.8 Coexistence View – Legend

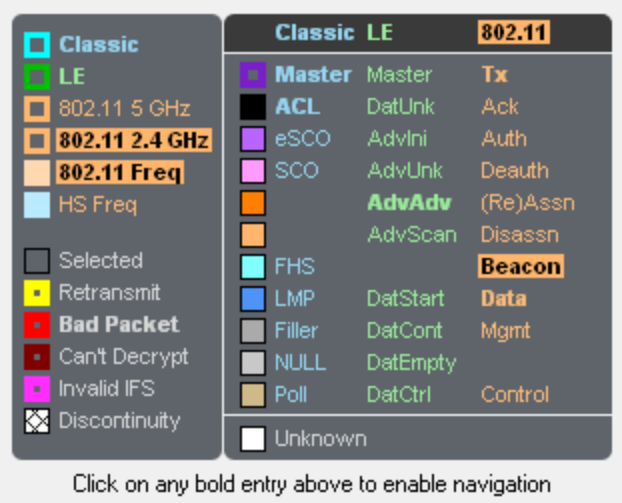


Figure 74. Coexistence View Legend

The legend describes the color-coding used by packets in the timelines. Selecting a packet in a timeline highlights the applicable entries in the legend. An entry is bold if any such packets currently exist. Clicking on a bold entry enables the black legend navigation arrows in the toolbar for that entry.

4.4.2.9 Coexistence View – Timelines

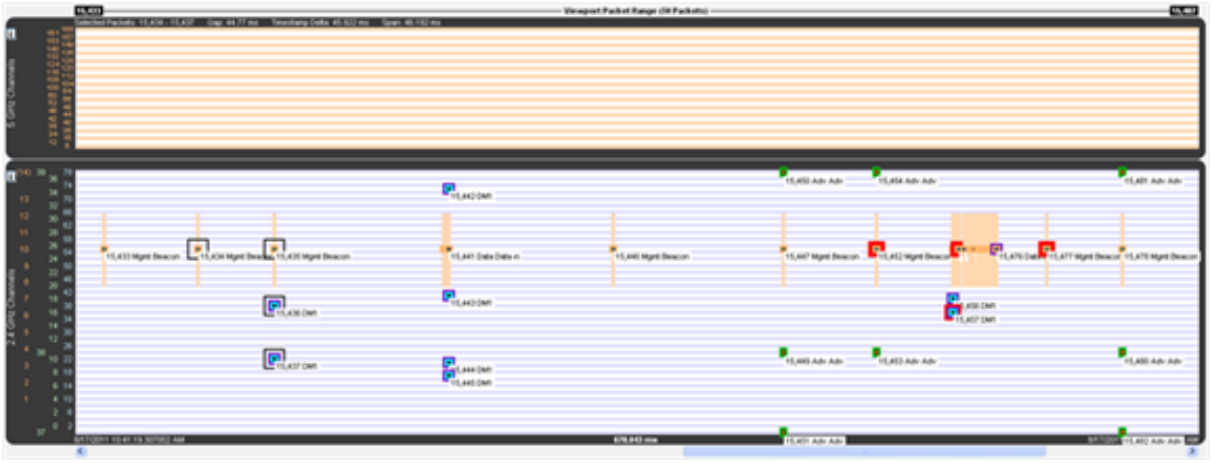


Figure 75. Coexistence View Timelines

The Timelines show Classic Bluetooth, *Bluetooth* low energy, and 802.11 packets by channel and time.

4.4.2.9.1 Packet information

Packet information is provided in various ways as described below.

Packets are color-coded to indicate attribute (Retransmit, Bad Packet, Can't Decrypt, or Invalid IFS), master/Tx, technology (Classic Bluetooth, *Bluetooth* low energy, or 802.11), and category/type.

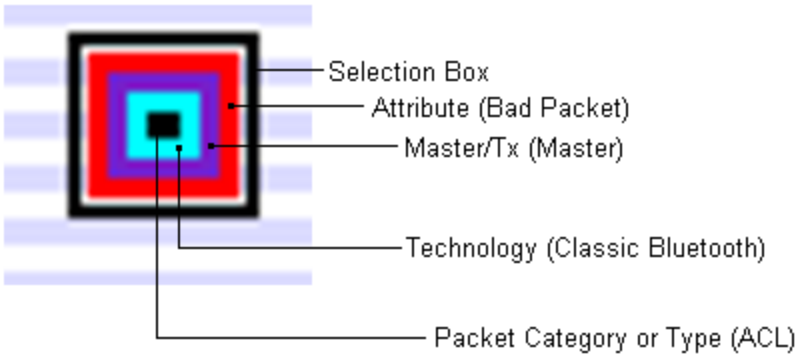


Figure 76. Each packet is color-coded

The innermost box (which indicates packet category/type) is the packet proper in that its vertical position indicates the channel, its length indicates the packet's duration in the air, its left edge indicates the start time, and its right edge indicates the end time.

The height of Classic *Bluetooth* and *Bluetooth* low energy packets indicates their frequency range (1 MHz and 2 MHz respectively). Since 802.11 channels are so wide (22 MHz), 802.11 packets are drawn with an arbitrary 1 MHz height and centered within a separate frequency range box which indicates the actual frequency range.

Selecting a packet by clicking on it draws a selection box around it (as shown above) and highlights the applicable entries in the legend.

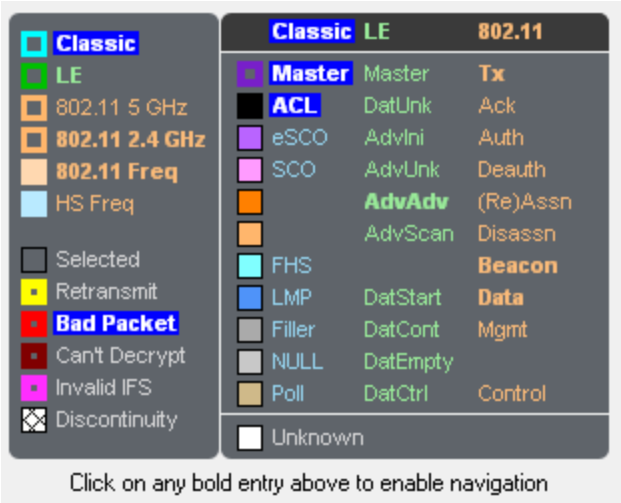


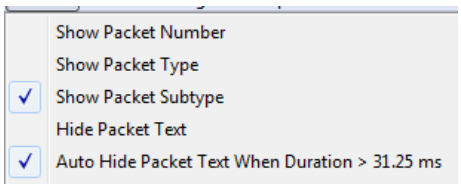
Figure 77. Highlighted entries in the legend for a selected packet.

Summary information for a selected packet is displayed in the timeline header.

Figure 78. Timeline header for a single selected packet.

When multiple packets are selected (by dragging the mouse with the left button held down, clicking one packet and shift-clicking another, or clicking one packet and pressing shift-arrow), the header shows Gap (duration between the first and last selected packets), Timestamp Delta (difference between the timestamps, which are at the beginning of each packet), and Span (duration from the beginning of the first selected packet to the end of the last selected packet).

Figure 79. Timeline header for multiple selected packets



Text can be displayed at each packet by selecting Show Packet Number, Show Packet Type, and Show Packet Subtype from the Format menu.

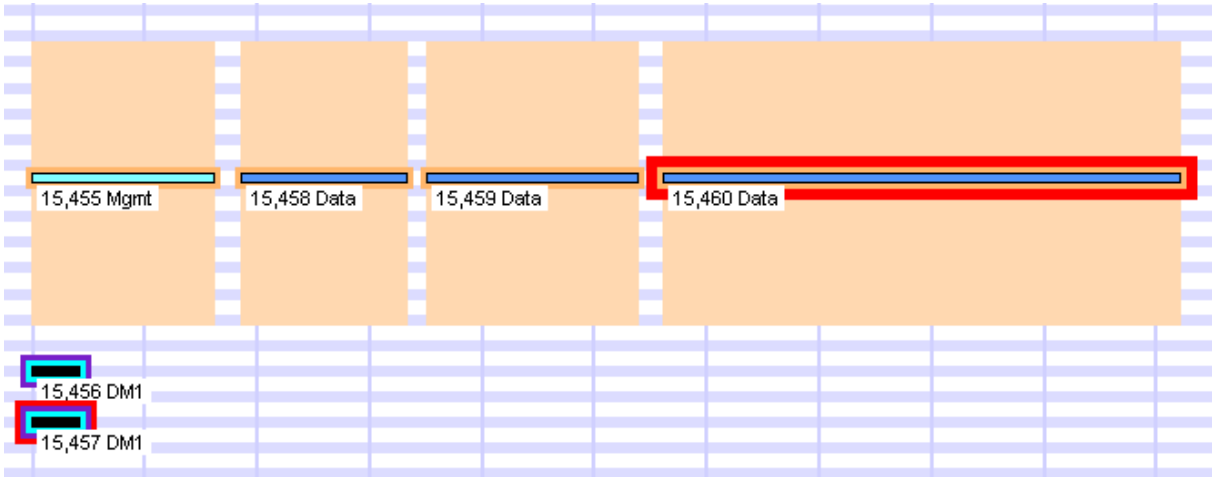


Figure 80. Descriptive text on timeline packets.

Placing the mouse pointer on a packet displays a tooltip (color-coded by technology) that gives detailed information.

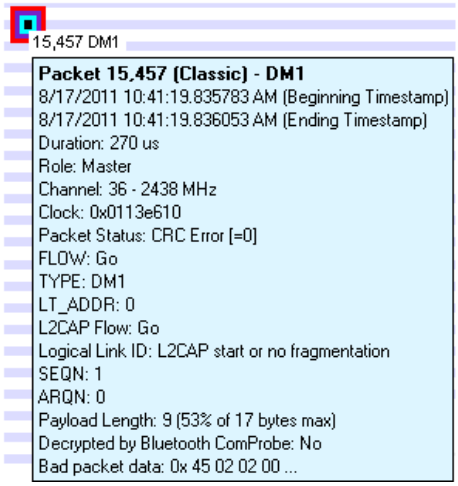


Figure 81. A tool tip for a Classic *Bluetooth* packet.

4.4.2.9.2 Relocating the tool tip

You can relocate the tool tip for convenience or to see the timeline or throughput graph unobstructed while displaying packet information. In the Format menu select Show Tooltips in Upper-Left Corner of Screen, and any time you mouse-over a packet the tool tip will appear anchored in the upper-left corner of the computer screen. To return to viewing the tool tip adjacent to the packets deselect the tool tip format option in the menu.

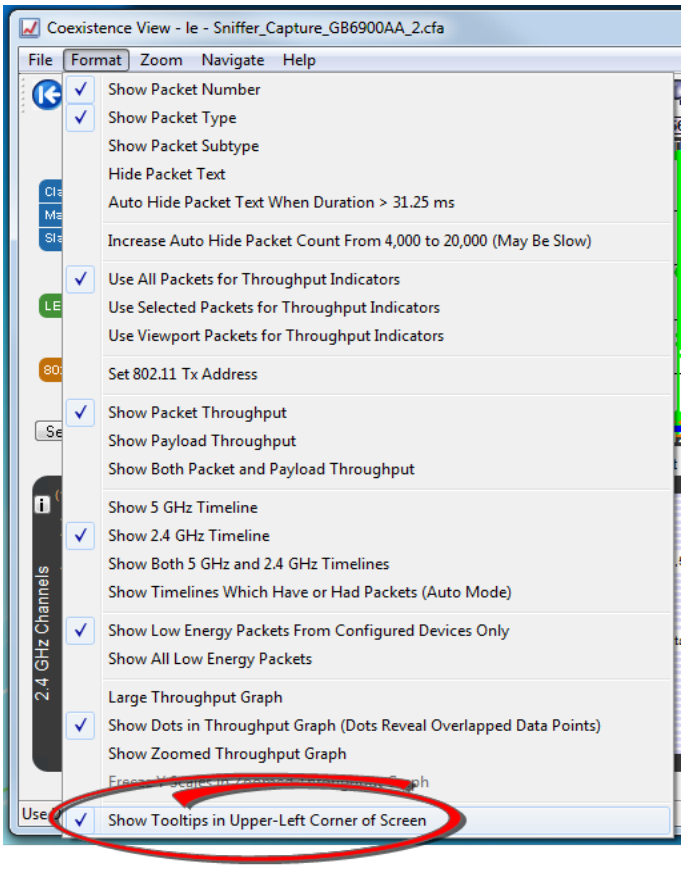


Figure 82. Coexistence View Format Menu - Show Tooltips on Computer Screen

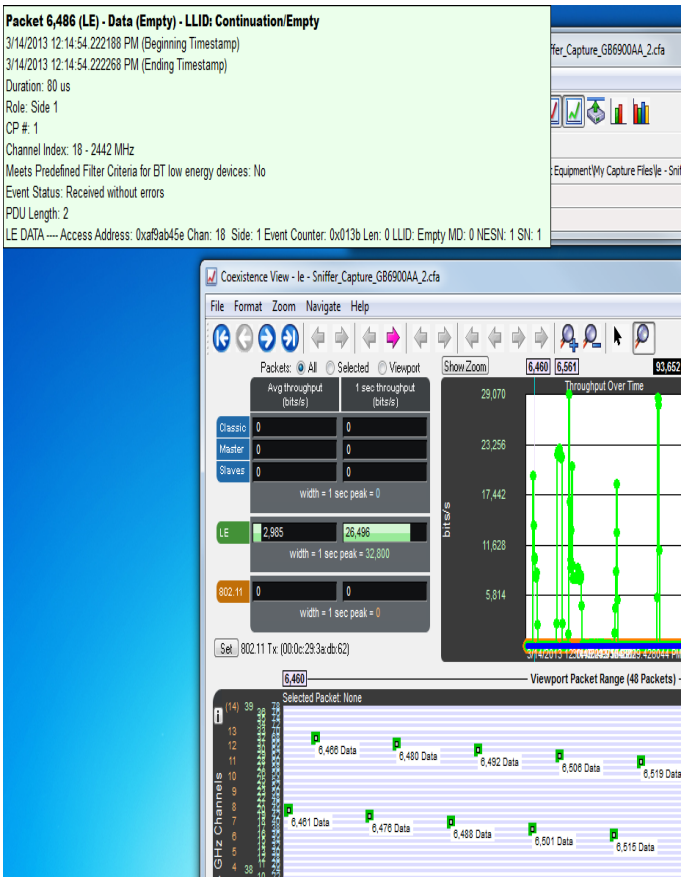


Figure 83. Coexistence View Timeline Tool Tip Shown Anchored to Computer Screen

4.4.2.9.3 The two Timelines

There are two Timelines available for viewing, one for the 5 GHz range and one for the 2.4 GHz range. Classic *Bluetooth* and *Bluetooth* low energy occur only in the 2.4 GHz range. 802.11 can occur in both.

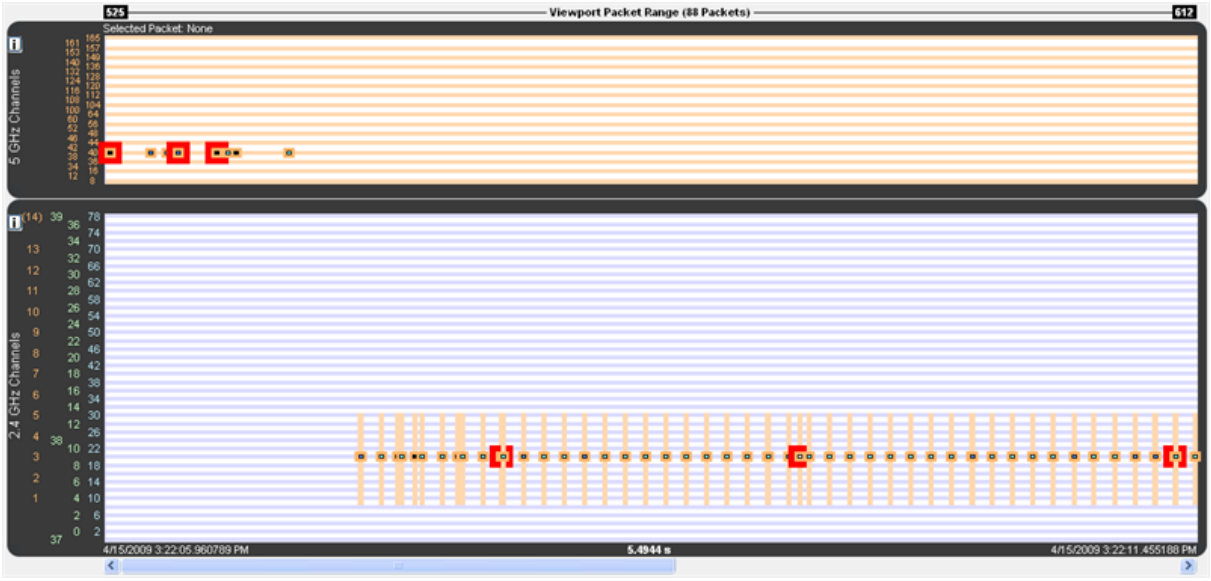


Figure 84. 5 GHz and 2.4 GHz 802.11 packets

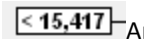
The y-axis labels show the channels for each technology and are color-coded: Blue = Classic *Bluetooth*, Green = *Bluetooth* low energy, Orange = 802.11.

The 5 GHz timeline has only 802.11 channel labels, and the rows alternate orange and white, one row per channel.

The 2.4 GHz timeline has labels for all three technologies. The rows alternate blue and white, one row per Classic *Bluetooth* channel. The labels going left-to-right are 802.11 channels, *Bluetooth* low energy advertising channels, *Bluetooth* low energy regular channels, and Classic *Bluetooth* channels.

The Viewport Packet Range above the timelines shows the packet range and packet count of packets that would be visible if both timelines were shown (i.e. hiding one of the timelines doesn't change the packet range or count). This packet range matches the packet range shown above the viewport in the Throughput Graph, as it must since the viewport defines the time range used by the timelines. When no packets are in the time range, each of the two packet numbers is drawn with an arrow to indicate the next packet in each direction and can be clicked on to navigate to that packet (the packet number changes color when the mouse pointer is placed on it in this case).

An arrow points to the next packet when no packets are in the time range.



An arrowed packet number changes color when the mouse pointer is on it. Clicking navigates to that packet.

The header shows information for packets that are selected.

The footer shows the beginning/ending timestamps and visible duration of the timelines.

The 'i' buttons bring up channel information windows, which describe channel details for each technology. They make for interesting reading.

802.11 5 GHz
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 fixed spacing instead of being spaced relative to its distance from other channels as is done with 2.4 GHz channels (with the exception of 802.11 channel 14).

Figure 85. 5 GHz information window

Bluetooth Classic
There are 79 Classic channels. Each channel is 1 MHz wide and has the indicated center frequency. Channels do not overlap.

0 = 2402 MHz	10 = 2412 MHz	20 = 2422 MHz	30 = 2432 MHz	40 = 2442 MHz	50 = 2452 MHz	60 = 2462 MHz	70 = 2472 MHz
1 = 2403 MHz	11 = 2413 MHz	21 = 2423 MHz	31 = 2433 MHz	41 = 2443 MHz	51 = 2453 MHz	61 = 2463 MHz	71 = 2473 MHz
2 = 2404 MHz	12 = 2414 MHz	22 = 2424 MHz	32 = 2434 MHz	42 = 2444 MHz	52 = 2454 MHz	62 = 2464 MHz	72 = 2474 MHz
3 = 2405 MHz	13 = 2415 MHz	23 = 2425 MHz	33 = 2435 MHz	43 = 2445 MHz	53 = 2455 MHz	63 = 2465 MHz	73 = 2475 MHz
4 = 2406 MHz	14 = 2416 MHz	24 = 2426 MHz	34 = 2436 MHz	44 = 2446 MHz	54 = 2456 MHz	64 = 2466 MHz	74 = 2476 MHz
5 = 2407 MHz	15 = 2417 MHz	25 = 2427 MHz	35 = 2437 MHz	45 = 2447 MHz	55 = 2457 MHz	65 = 2467 MHz	75 = 2477 MHz
6 = 2408 MHz	16 = 2418 MHz	26 = 2428 MHz	36 = 2438 MHz	46 = 2448 MHz	56 = 2458 MHz	66 = 2468 MHz	76 = 2478 MHz
7 = 2409 MHz	17 = 2419 MHz	27 = 2429 MHz	37 = 2439 MHz	47 = 2449 MHz	57 = 2459 MHz	67 = 2469 MHz	77 = 2479 MHz
8 = 2410 MHz	18 = 2420 MHz	28 = 2430 MHz	38 = 2440 MHz	48 = 2450 MHz	58 = 2460 MHz	68 = 2470 MHz	78 = 2480 MHz
9 = 2411 MHz	19 = 2421 MHz	29 = 2431 MHz	39 = 2441 MHz	49 = 2451 MHz	59 = 2461 MHz	69 = 2471 MHz	

The row labels are placed at the center frequency of each channel.

Bluetooth low energy (LE)
There are 40 LE channels. Each channel is 2 MHz wide and has the indicated center frequency. Channels do not overlap.
Channels 0 through 36 are Data channels. Channels 37 through 39 are Advertising channels.

37 = 2402 MHz	4 = 2412 MHz	9 = 2422 MHz	13 = 2432 MHz	18 = 2442 MHz	23 = 2452 MHz	28 = 2462 MHz	33 = 2472 MHz
0 = 2404 MHz	5 = 2414 MHz	10 = 2424 MHz	14 = 2434 MHz	19 = 2444 MHz	24 = 2454 MHz	29 = 2464 MHz	34 = 2474 MHz
1 = 2406 MHz	6 = 2416 MHz	38 = 2426 MHz	15 = 2436 MHz	20 = 2446 MHz	25 = 2456 MHz	30 = 2466 MHz	35 = 2476 MHz
2 = 2408 MHz	7 = 2418 MHz	11 = 2428 MHz	16 = 2438 MHz	21 = 2448 MHz	26 = 2458 MHz	31 = 2468 MHz	36 = 2478 MHz
3 = 2410 MHz	8 = 2420 MHz	12 = 2430 MHz	17 = 2440 MHz	22 = 2450 MHz	27 = 2460 MHz	32 = 2470 MHz	39 = 2480 MHz

The row labels are placed at the center frequency of each channel.

802.11 2.4 GHz
In the 802.11 2.4 GHz frequency range there are 11 channels in the USA, 13 in Europe, and 14 in Japan. Each channel is 22 MHz wide. Channels 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 802.11 channels 1-13 are placed at the center frequency of each channel.
The row label for 802.11 channel 14 is in parentheses because that channel's center frequency is above the top of the graph.

Figure 86. 2.4 GHz information windows

4.4.2.9.4 Bluetooth slot markers

When zoomed in far enough *Bluetooth* slot markers appear in the 2.4 GHz timeline. A *Bluetooth* slot is 625 µs wide.

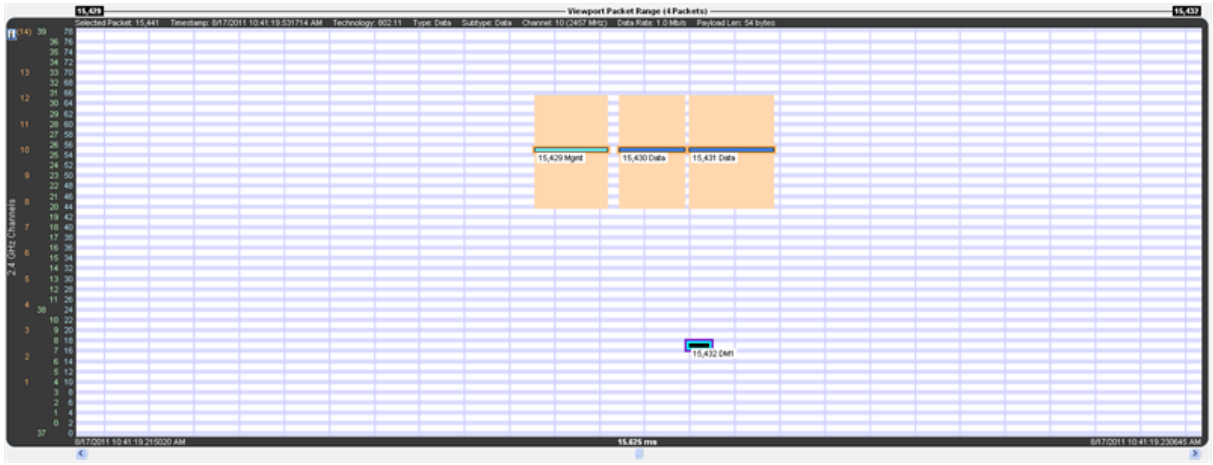


Figure 87. Vertical blue lines are *Bluetooth* slot markers

4.4.2.9.5 Zooming

There are various ways to zoom:

1. Drag one of the sides of the Throughput Graph viewport.
2. Select a zoom preset from the Zoom or right-click menus.
3. Select the Zoom In or Zoom Out button or menu item.
4. Turn the mouse wheel in the Timelines or the Zoomed Throughput Graph while the zoom cursor is selected. The action is the same as selecting the Zoom In and Zoom Out buttons and menu items except that the time point at the mouse pointer is kept in place if possible.
5. Select the Zoom to Data Point Packet Range menu item, which zooms to the packet range shown in the most recently displayed tool tip.
6. Select the Zoom to Selected Packet Range menu item, which zooms to the selected packet range as indicated in the Selected Packets text in the timeline header.
7. Select the Custom Zoom menu item. This is the zoom level from the most recent drag of a view-port side, selection of Zoom to Data Point Packet Range, or selection of Zoom to Selected Packet.

The zoom buttons and tools step through the zoom presets and custom zoom, where the custom zoom is logically inserted in value order into the zoom preset list for this purpose.

4.4.2.9.6 Discontinuities

A discontinuity is when the timestamp going from one packet to the next either goes backward by any amount or forward by more than 4.01 s (this value is used because the largest possible connection interval in *Bluetooth* low energy is 4.0 s). A discontinuity is drawn as a vertical cross-hatched area one *Bluetooth* slot (625 µs) in width. A discontinuity for a timestamp going backward is called a negative discontinuity and is shown in red. A discontinuity for a timestamp going forward by more than 4.01 s is called a positive discontinuity and is shown in black. A positive discontinuity is a cosmetic nicety to avoid lots of empty space. A negative discontinuity is an error.

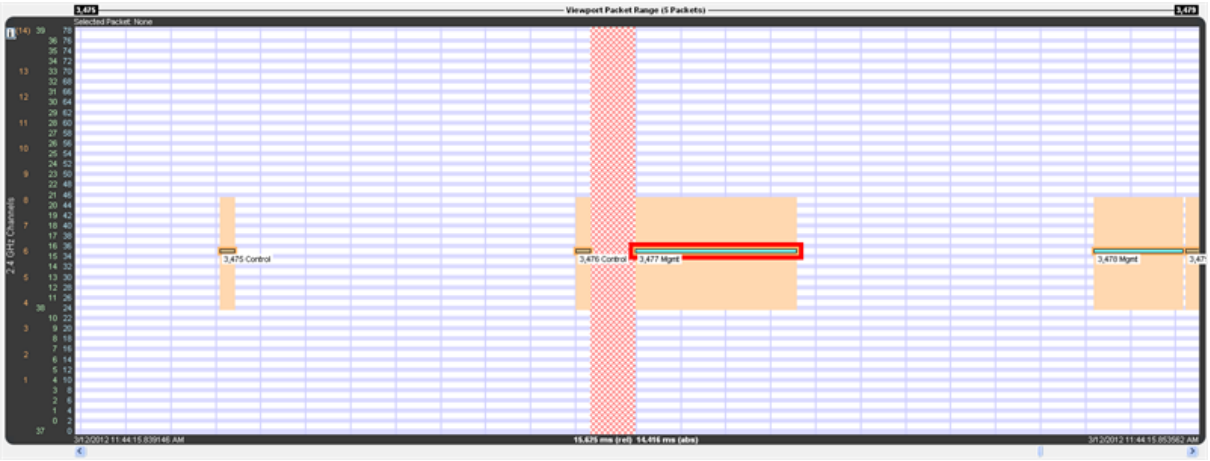


Figure 88. A negative discontinuity

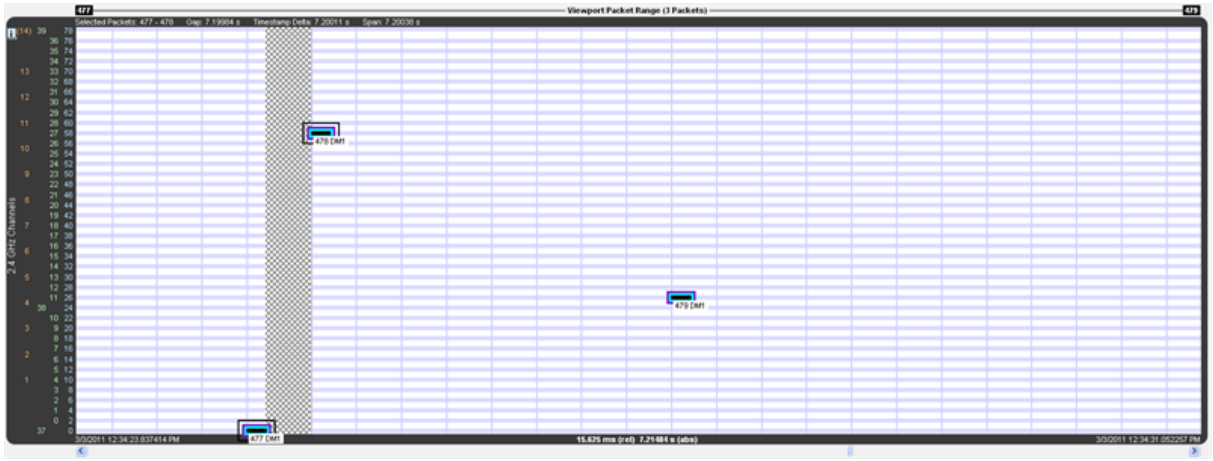


Figure 89. A positive discontinuity

When there are one or more discontinuities the actual time encompassed by the visible timeline differs from the zoom level duration that would apply in the absence of any discontinuities. The actual time, referred to as absolute time, is shown followed by "(abs)". The zoom level duration, referred to as relative time, is shown followed by "(rel)". When there are no discontinuities, relative and absolute time are the same and a single value is shown.

Figure 90. Timeline header with discontinuity

Figure 91. Timeline duration footer with discontinuity

For example, the timeline above has a zoom level duration of 15.625 ms (the relative time shown in the footer). But the discontinuity graphic consumes the width of a *Bluetooth* slot (625 µs), and that area is 7.19984 s of absolute time as shown by the Gap value in the header. So the absolute time is 7.21484 s:

Zoom level duration – *Bluetooth* slot duration + Gap duration =

15.625 ms - 625 µs + 7.19984 s =

0.015625 s – 0.000625 s + 7.199840 s =

0.015000 s + 7.199840 s =

7.214840 s =

7.21484 s

4.4.2.9.7 High-Speed Bluetooth

High-speed *Bluetooth* packets, where *Bluetooth* content hitches a ride on 802.11 packets, have a blue frequency range box instead of orange as with regular 802.11 packets (both are shown below), and the tool tip has

two colors, orange for 802.11 layers and blue for *Bluetooth* layers.

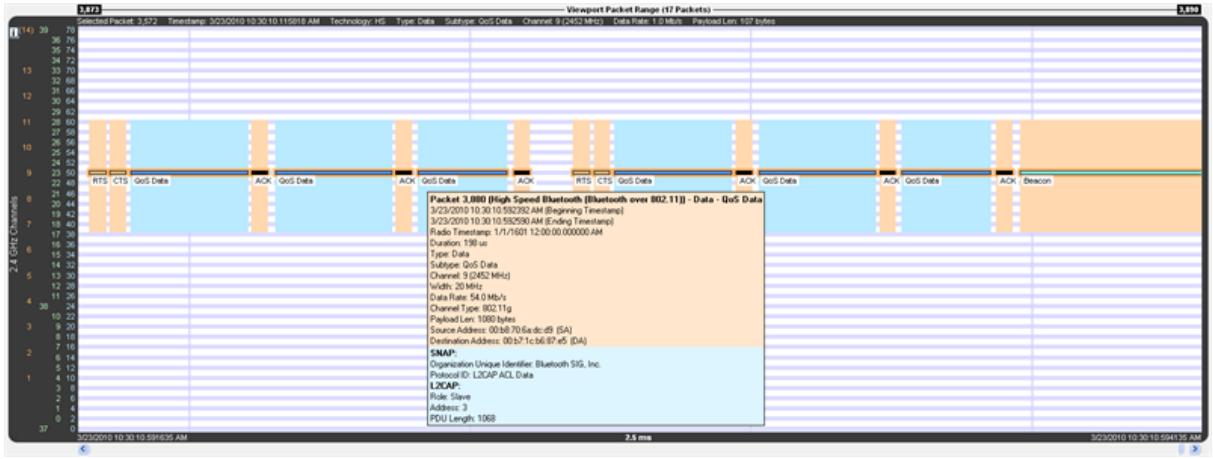


Figure 92. High-speed *Bluetooth* packets have a blue frequency box and a two-tone tool tip

4.5 Data/Audio Extraction

You use Data/Audio Extraction to pull out data from various decoded Bluetooth protocols. Once you have extracted the data, you can save them into different file types, such as text files, graphic files, email files, .mp3 files, and more. Then you can examine the specific files information individually.

1. You access this dialog by selecting Extract Data/Audio from the View menu or by clicking on the icon from the toolbar  .

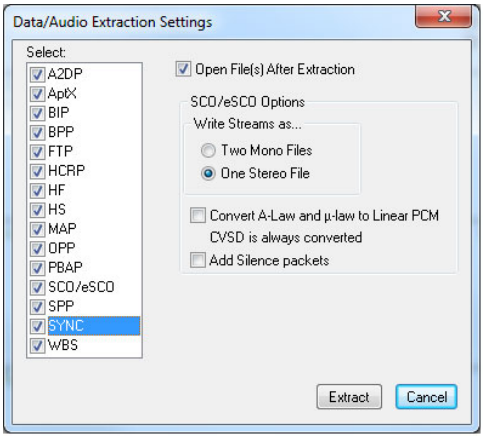


Figure 93. Data/Audio Extraction Settings dialog

2. Choose a checkbox(es) on the left side of the dialog to identify from which profile(s) 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.

3. If you want the file(s) to open automatically after they are extracted, select the Open File(s) After Extraction checkbox.

Note: This does not work for SCO/eSCO.

4. Click on a radio button to write the streams as Two Mono Files or as One Stereo File.

Note: This option is for SCO/eSCO only.

5. Select the checkbox if you want to convert A-Law and µ-law to Linear PCM.
CVSD are always converted to Linear PCM. It's probably a good idea to convert to Linear PCM since more media players accept this format.

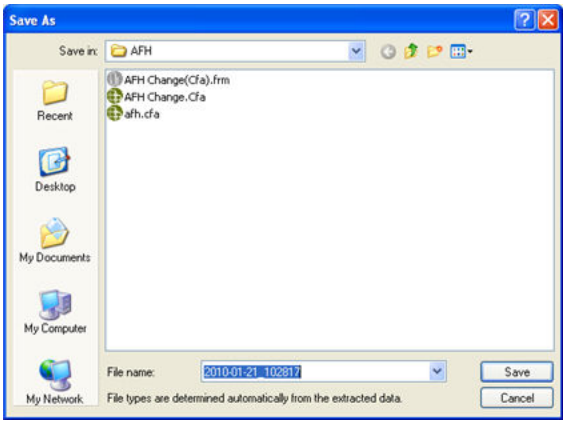
Note: This option is for SCO/eSCO only.

6. 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.

Note: This option is for SCO/eSCO only.

7. 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. The file type varies depending on the original profile. A separate file for each profile will be created, but only for those profiles with available data.

8. Select a location for the file.

9. Click Save.

The Data Extraction Status and Audio Extraction Status dialogs appear. When the process is complete the dialogs display what files have been created and where they are located.

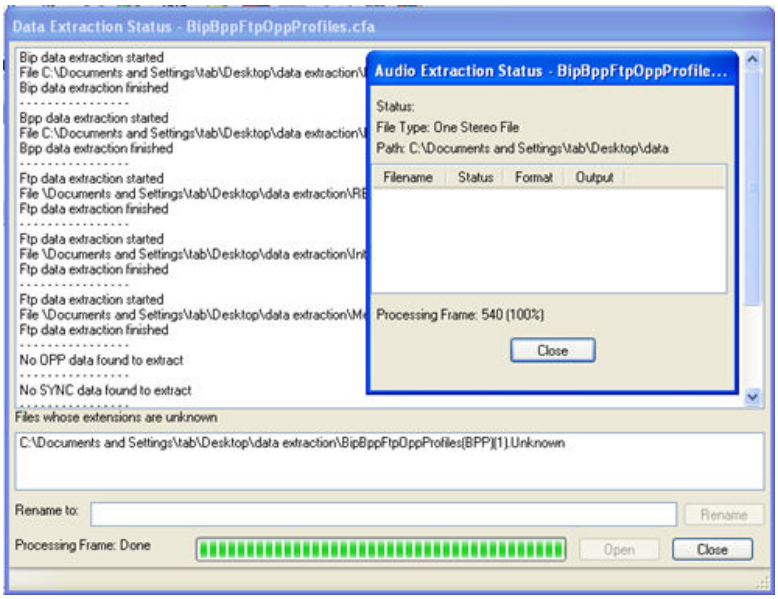


Figure 94. Data and Audio Extraction Status

If you selected Open Files(s) After Extraction, the files open automatically.

10. If you did not select this option, you can open a file by simply double-clicking on the name.

Also, if a file type is unknown, you can select the file and it appears in the Rename to: text box.

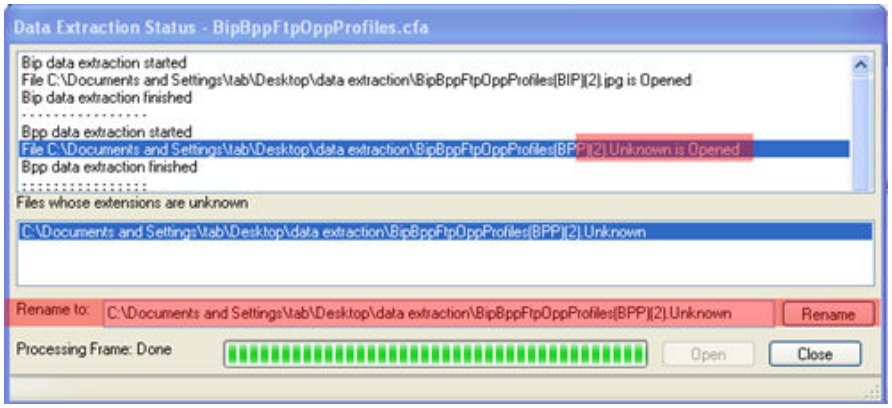


Figure 95. Rename To in the bottom section of Data Extraction Status

Then you can rename the file, adding a file type to attempt to open the file.

When you are finished, select Close to close the dialogs.

4.6 Statistics

4.6.1 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

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.

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 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.

4.6.2 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.

The Capture File tab shows information on the data that is currently in the capture.

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.

4.6.3 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

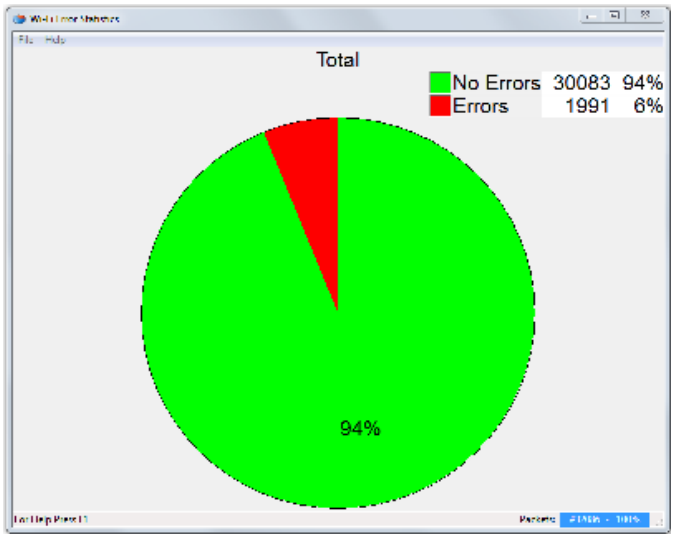
To copy the information from an individual table to the clipboard (where it can be pasted into any application),

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.

4.6.4 802.11 Error Statistics

The Wi-Fi Error Statistics window appears when you select the window from the icon in the Control window toolbar or the Frame Display toolbar.. The dialog is view only; there is no user interaction possible.

The window displays the percentage of packets with and without errors in a pie chart and in a table.



4.6.5 Graphs

4.6.5.1 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  .

4.6.5.2 Printing Graphs

Click the Print icon  to print the graph. The analyzer prints exactly what is shown on the window.

Chapter 5: Navigating and Searching the Data

The following sections describe how to navigate through the data and how to find specific data or packet conditions of interest to the user.

5.1 Find

Capturing and decoding data within the ComProbe® analyzer produces a wealth of information for analysis. This mass of information by itself, however, is just that, a mass of information. There has to be ways to manage the information. ComProbe software provides a number of different methods for making the data more accessible. One of these methods is Find.

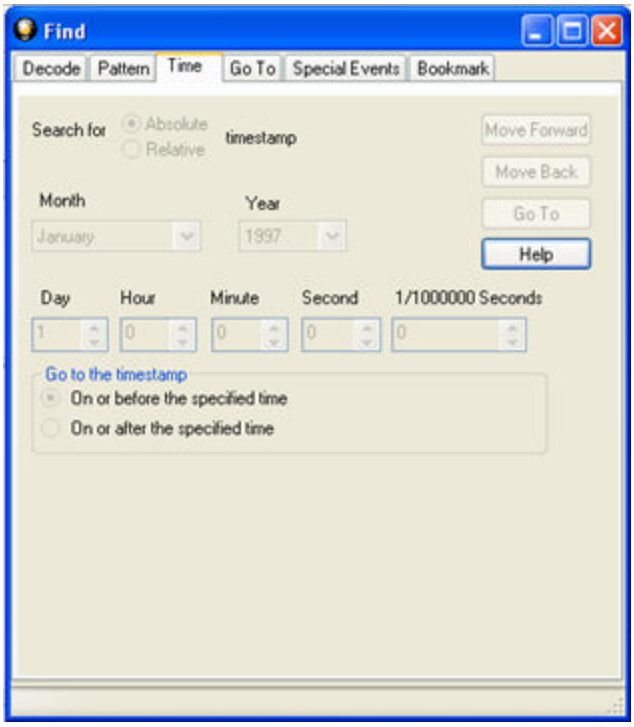


Figure 96. Find Diaglog

Find, as the name suggests, is a comprehensive search function that allows users to search for strings or patterns in the data or in the frame decode. You can search for errors, control signal changes, bookmarks, special events, time, and more. Once the information is located, you can easily move to every instance of the Find results.

5.1.1 Searching within Decodes

Searching within decodes lets you to do a string search on the data in the Decode Pane of the Frame Display window.

To access the search within decodes function:

1. Open a capture file 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. 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.

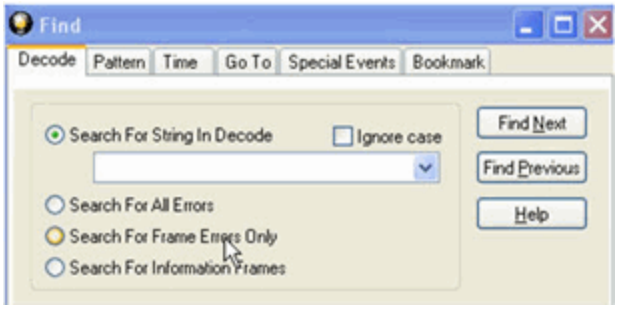


Figure 97. Find Decode Tab Search for String

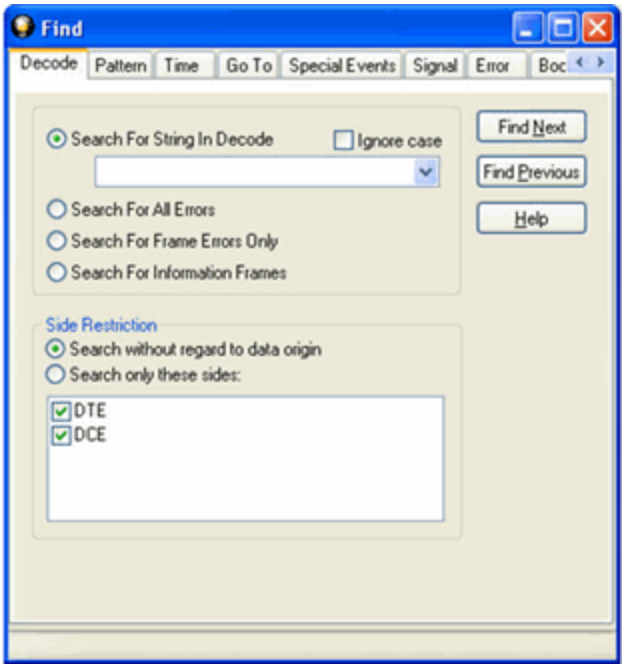


Figure 98. Find Decode Tab Side Restriction

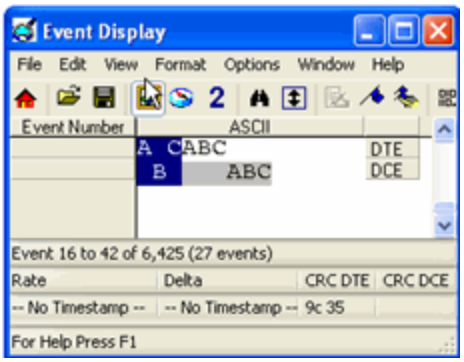
There are several options for error searching on the Decoder tab.

- Search For String in Decoder allows you to enter a string in the text box. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the analyzer saves the search. The next time you open Find, the drop-down list will contain your search parameters.
- 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.

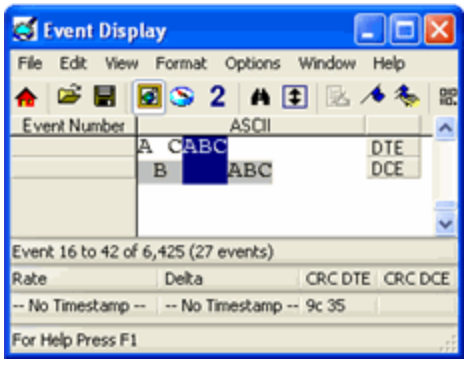
1. Enter the search string.
2. Check Ignore Case to do a case-insensitive search.
3. When you have specified the time interval you want to use, click on the Find Next or Find Previous buttons to start the search from the current event.

The result of the search is displayed in the Decode pane in Frame Display.

Side Restrictions - Side Restriction means that the analyzer looks for a pattern coming wholly from the DTE or DCE side. If you choose to search without regard for data origin, the analyzer looks for a pattern coming from one or both sides. For example, if you choose to search for the pattern ABC and you choose to search without regard for data origin, the analyzer finds all three instances of ABC shown here.



The first pattern, with the A and the C coming from the DTE device and the B coming from the DCE is a good example of how using a side restriction differs from searching without regard to data origin. While searching without regard for data origin finds all three patterns, searching using a side restriction never finds the first pattern, because it does not come wholly from one side or the other.



If you choose to search for the pattern ABC, and you restrict the search to just the DTE side, the analyzer finds the following pattern:

In this example, the analyzer finds only the second pattern (highlighted above) because we restricted the search to just the DTE side. The first pattern doesn't qualify because it is split between the DTE and DCE sides, and the third pattern, though whole, comes from just the DCE side.

If we choose both the DTE and the DCE sides in the above example, then the analyzer finds the second pattern followed by the third pattern, but not the first pattern. This is because each side has one instance in which the whole pattern can be found. The analyzer completely searches the DTE side first, followed by the DCE side.

Note: Side Restriction is available for pattern and error searching.

1. Select one of the two options.
2. Select DTE, DCE, or both.
3. When you made your selections, click on the Find Next or Find Previous buttons to start the search from the current event.

The result of the search is displayed in the Decode pane in Frame Display.

5.1.2 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.

To access the search by pattern function:

1. Open a capture file 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. 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.

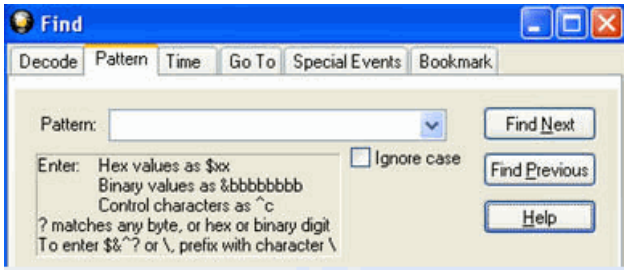


Figure 99. Find Pattern Tab

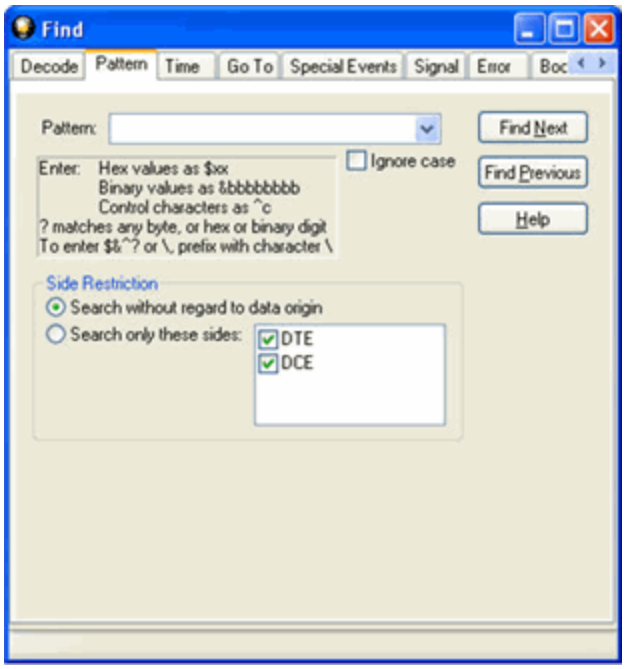


Figure 100. Find Pattern Tab Side Restrictions

Pattern allows you to enter a string in the text box. You can use characters, hex or binary digits, control characters, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the ComProbe analyzer saves the search. The next time you open Find, the drop-down list will contain your search parameters.

1. Enter the search pattern.
2. Check Ignore Case to do a case-insensitive search.
3. When you have specified the pattern you want to use, click on the Find Next or Find Previous buttons to start the search from the current event.

The result of the search is displayed in the in Frame Display and Event Display.

Refer to Searching by Decode on page 108 for information on Side Restrictions

5.1.3 Searching by Time

Searching with Time allows you search on timestamps on the data in Frame Display and Event Display window.

To access the search by time function:

1. Open a capture file 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. 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.

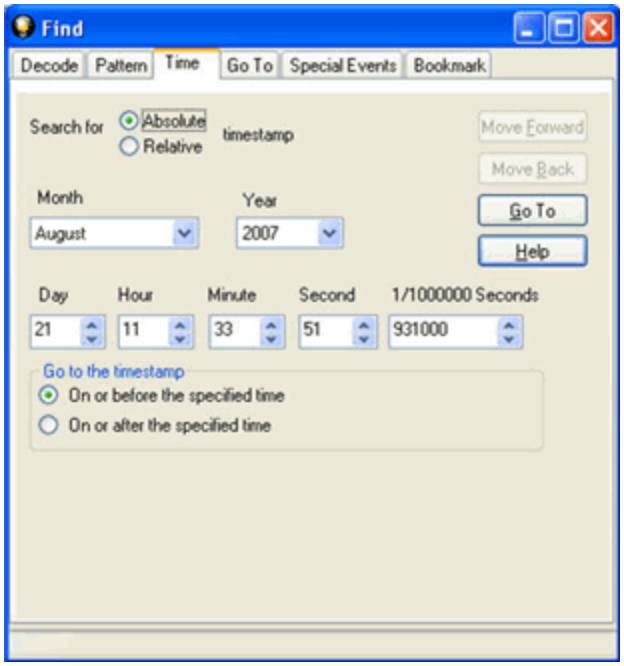


Figure 101. Find by Time tab

The analyzer can search by time in several different ways.

Search for Absolute/Relative timestamp.

- 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.

1. Select Absolute or Relative
2. Select the date and time using the drop-down lists for Month, Year, Day, Hour, Minute, Second, 1/10000000.

Note: Month and Year are not available if you select Relative.

3. When you have specified the time interval you want to use, click on the Go To, Move Forward or Move Backward buttons to start the search from the current event.

Note: When you select Absolute as Search for, Go To is available. When you select Relative as Search for, Move Forward or Move Backwardis available.

Go to the timestamp: On or before/ 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 option. 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.

When you select Absolute as Search for, the radio buttons are On or before the specified time or On or after the specified time. When you select Relative as Search for, the radio buttons are On or before the specified time relative to the first selected item or On or after the specified time relative to the last selected item.

1. Select On or before the specified time or On or after the specified time.
2. When you have specified the time interval you want to use, click on the Go To, Move Forward or Move Backward buttons to start the search from the current event.

   When you select Absolute as Search for, Go To is available. When you select Relative as Search for, Move Forward or Move Backwardis available.

There are a couple of other concepts to understand in respect to searching with timestamps.

- 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.
- 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.
- The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

5.1.4 Using Go To

Searching with Go To 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. Open a capture file 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. Click on the Go To tab of the Find dialog.
5. 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 you are viewing.

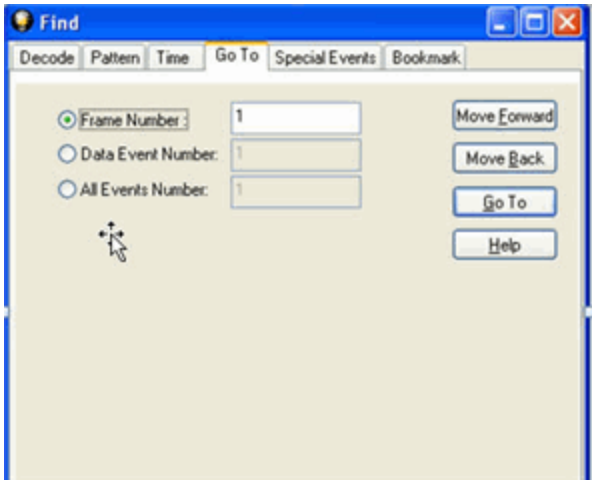


Figure 102. Find Go To tab

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 the 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, Frontline 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.

5.1.5 Searching for Special Events

Frontline 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. You can use Find to locate single or multiple special events.

To access the search for special events function:

1. Open a capture file 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. Click on the Special Events 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.

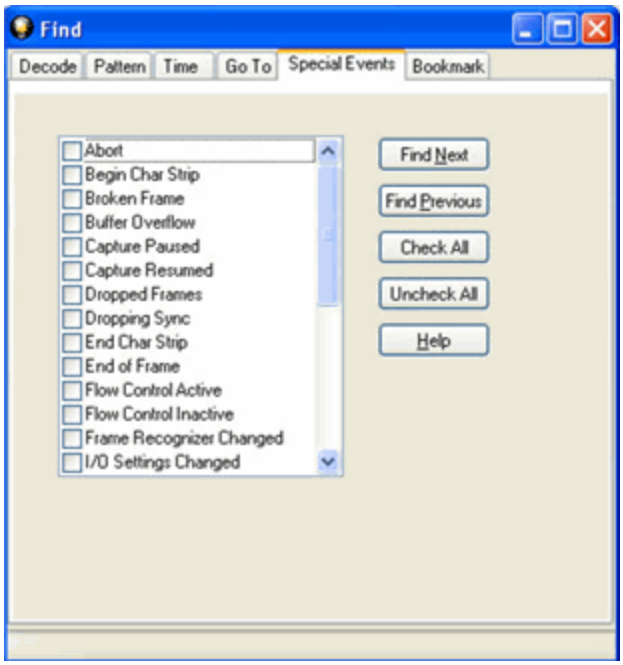


Figure 103. Find Special Events tab

5. Check the event or events you want to look for in the list of special events. Use Check All or Uncheck All buttons to make your selections more efficient.
6. Click Find Next and Find Previous to move to the next instance of the event.

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 on page 53.

5.1.6 Searching by Signal

Searching with Signal 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 search by time function:

1. Open a capture file 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. 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.

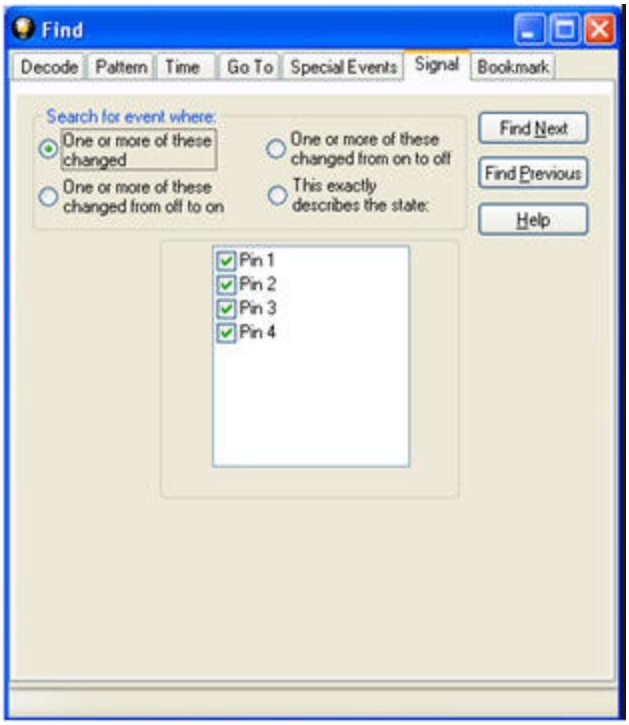


Figure 104. Find Signal tab.

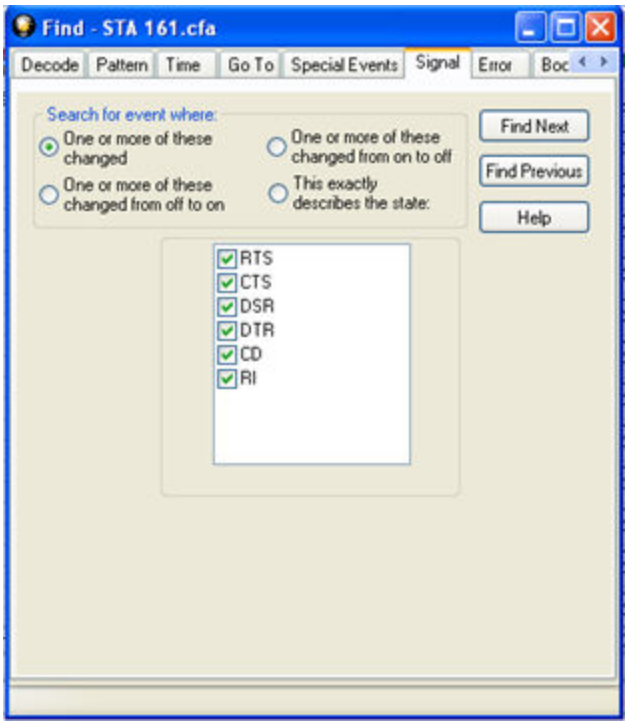


Figure 105. Find Signal Tab

You will choose one qualifier—Searching for event where, then choose one or more control signals

Control Signals

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.

The control signals types include:

- USB - Pin 1
- USB - Pin 2
- USB - Pin 3
- USB - Pin 4

or

- RS232 - Request to Send (RTS)
- RS232 - Clear to Send (CTS)
- RS232 - Data Set Ready (DSR)
- RS232 - Data Terminal Ready (DTR)
- RS232 - Carrier Detect (CD)
- RS232 - Ring Indicator (RI).

Click here to learn more about the Breakout Box and Pins 1 - 4.

Searching for event where:

- 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.
- Select one of the four radio buttons to choose the condition that must be met in the search
- Select one or more of the checkboxes for Pin 1, 2, 3, or 4.
- Or, Select one or more of the checkboxes for Request to Send (RTS), Clear to Send (CTS), Data Set Ready (DSR), Data Terminal Ready (DTR), Carrier Detect (CD), and Ring Indicator (RI).
- Click Find Next to locate the next occurrence of the search criteria or Find Previous to locate an earlier occurrence of the search criteria.

5.1.7 Searching for Data Errors

The analyzer can search for several types of data errors. Searching for data error sallows you to 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 search by time function:

1. Open a capture file 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. Click on the Errors 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.

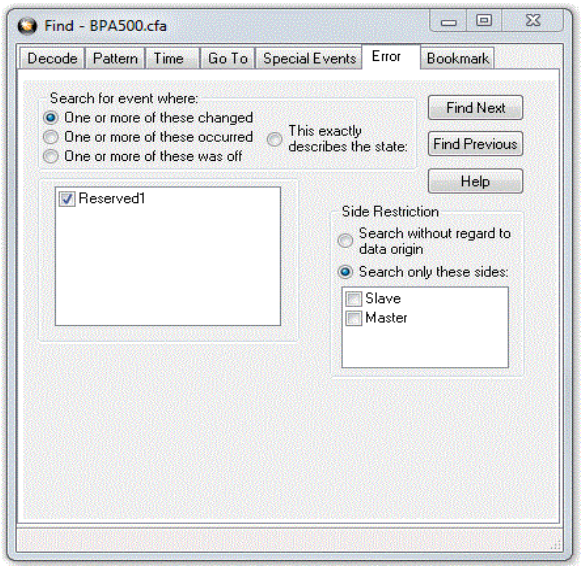


Figure 106. Find Error tab.

Searching for event where

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)

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 box if shown
- un-check the other boxes.

To search for all types of errors

- check all boxes

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.

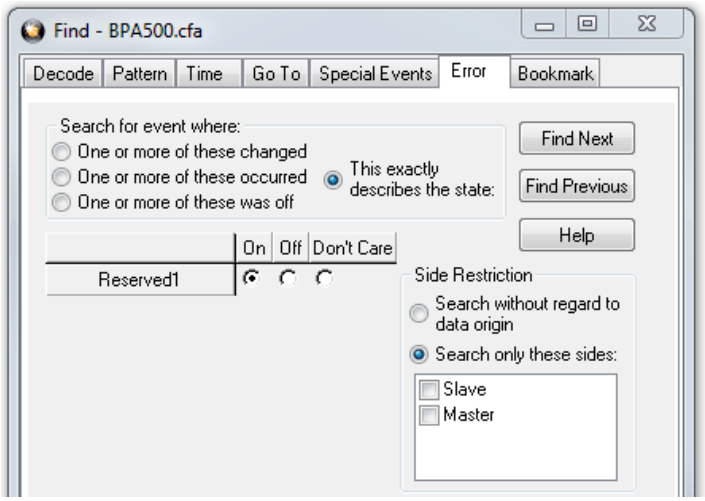
Searching for an event where the error conditions changed means that the analyzer searches the data and stop at every point where the error condition changed from on to off, or off to on.

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. Clicking Find Previous will search backwards from the current postion.

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.

5.1.8 Find - Bookmarks

Searching with Bookmarks allows you search on specific bookmarks on the data in Frame Display and Event Display window. Bookmarks are notes/reminders of interest that you attach to the data so they can be accessed later.

To access the search for bookmarks

1. Open a capture file 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. Click on the Bookmarks 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.

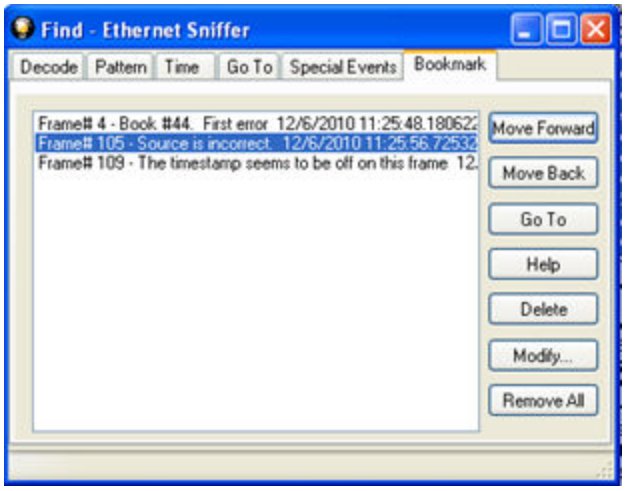


Figure 107. Find Bookmark tab.

There are several ways to locate bookmarks.

- Select the bookmark you want to move to and click the Go To button.
- Simply double-click on the bookmark.
- Click the Move Forward and Move Back buttons to move through the frames to the bookmarks shown in the window. When the bookmark is found it is highlighted in the window.

There are three ways to modify bookmarks:

1. Click on Delete to remove the selected bookmark.
2. Click on Modify... to change the selected Bookmark name.
3. Remove All will delete all bookmarks in the window.

The Find window Bookmark tab will also appear when using functions other than Find such as when clicking on the Display All Bookmarks  icon.

5.1.9 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.

```
[CVEventDisplay]
SelectionOffset=2
```

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\User\Public\Public Documents\Frontline Test Equipment\)
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).

5.1.10 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.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

5.2 Bookmarks

Bookmarks are electronic sticky notes that you attach to frames of interest so they can be easily found later. In Frame Display bookmarked frames appear with a magenta triangle icon next to them.

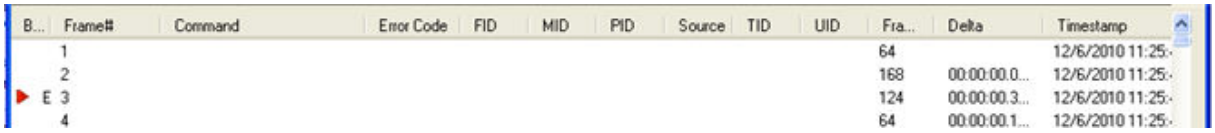
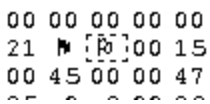


Figure 108. Bookmarked Frame (3) in the Frame Display



In the Event Display bookmarks appear as a dashed line around the start of frame marker.

Bookmarks are easy to create and maintain, and are a very valuable tool for data analysis. When you create or modify a bookmark, you have up to 84 characters to explain a problem, leave yourself a reminder, leave someone else a reminder, etc. Once you create a bookmark it will be saved with the rest of the data in the .cfa file. When you open a .cfa file, the bookmarks are available to you.

Once you have created a bookmark, you can use the Find function or other navigation methods to locate and move among them.

5.2.1 Adding, Modifying or Deleting a Bookmark

You can add, modify, or delete a bookmarks from Frame Display and Event Display

Add:

1. Select the frame or event you want to bookmark.
2. There are three ways to access the Add Bookmark dialog.
    a. Select Add or Modify Bookmark from the Bookmarks menu on the Frame Display and Event Display,
    b. Select the Add or Modify Bookmark  icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing Add Bookmark….
3. In the dialog box, add a comment (up to 84 characters) in the text box to identify the bookmark.
4. Click OK.

Once you create a bookmark it will be saved with the rest of the data in the .cfa file. When you open a .cfa file, the bookmarks are available to you.

Modify

1. Select the frame or event with the bookmark to be edited.
2. There are three ways to access the Add/Modfy Bookmark dialog.
    a. Select Add or Modify Bookmark from the Bookmarks menu on the Frame Display and Event Display'
    b. Select the Add or Modify Bookmark  icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing Modify Bookmark… on the selection.
3. Change the comment in the dialog box
4. Click OK. The edited bookmark will be saved as a part of the .cfa file.
5. You can also select Display All Bookmarks  from the Frame Display and Event Display tool-bar or the Bookmarks menu. the Find window will open on the Bookmark tab. Select the book-mark you want to modify and click the Modify… button. Change the comment in the dialog box, and click OK.

Delete

1. Select the frame or event with the bookmark to be deleted.
2. There are three ways to access the Add/Modfy Bookmark dialog.

a. Select Add or Modify Bookmark from the Bookmarks menu on the Frame Display and Event Display,

b. Select the Add or Modify Bookmark icon on one of the toolbars, or

c. Right-click on the frame/event and choosing Modify Bookmark… on the selection.

3. Click on the Delete button. The bookmark will be deleted.

4. You can also select Display All Bookmarks from the Frame Display and Event Display toolbar or the Bookmarks menu. the Find window will open on the Bookmark tab. Select the bookmark you want to delete and click the Delete button.

5.2.2 Displaying All and Moving Between Bookmarks

There are three ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.
2. Select Go to Next Bookmark from the Bookmarks menu.
3. 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.

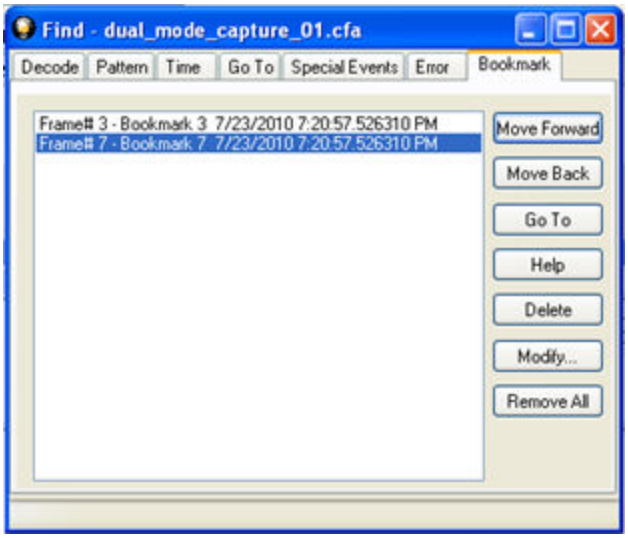


Figure 109. Find Window Bookmark tab Used to Move Around With Bookmarks

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.

5.3 Filtering

5.3.1 About 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. Display filters allow a user to look at a subset of captured data without affecting the capture content. There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filter

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.

5.3.1.1 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 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 is self configuring which means that when you Select each frame under Conditions the following displayed fields depend on your selection. With each subsequent selection the dialog fields will change depending on you selection in that field.

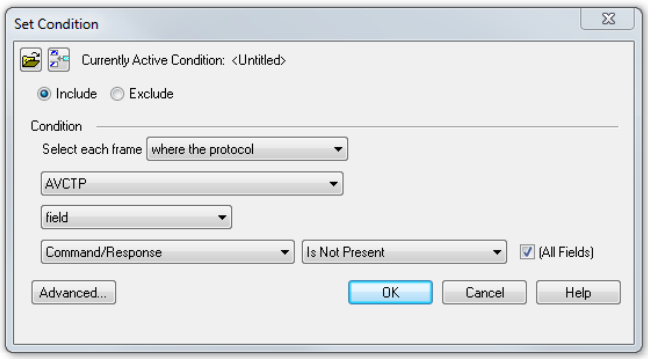


Figure 110. Example: Set Conditions Self Configuring Based on Protocol Selection

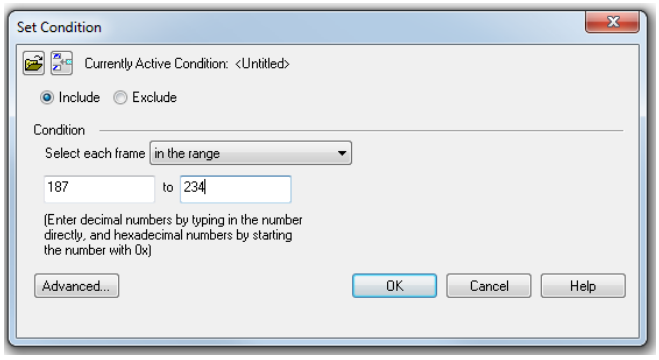


Figure 111. Example: Set Conditions Self Configuring Based on Frame Range

2. Select Include or Exclude to add filtered data or keep out filtered data respectively.
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 also appears in the Quick Filtering and Hiding Protocols dialog.

When a display filter is applied, a description of the filter appears to the right of the toolbar in 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.

5.3.1.2 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.

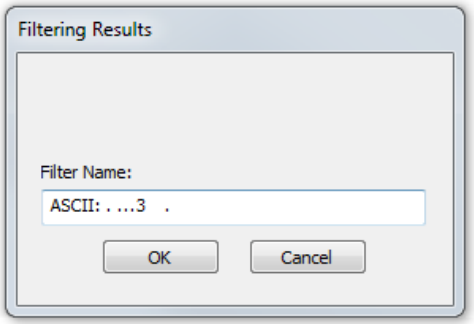
Include: A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

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.

5.3.1.3 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.

5.3.1.4 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.

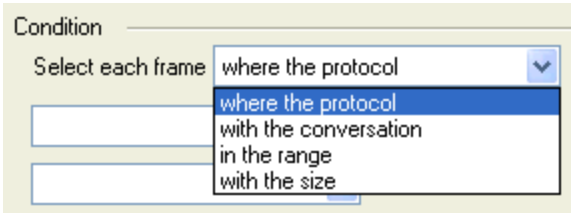
The AND operator narrows the filter, the OR operator broadens the filter, and the NOT operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

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 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 Include or Exclude radio button.

   Now you can set the conditions for the filter.

4. Select the initial condition for the filter from the combo box at the bottom of the dialog for Select each frame.



5. 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.

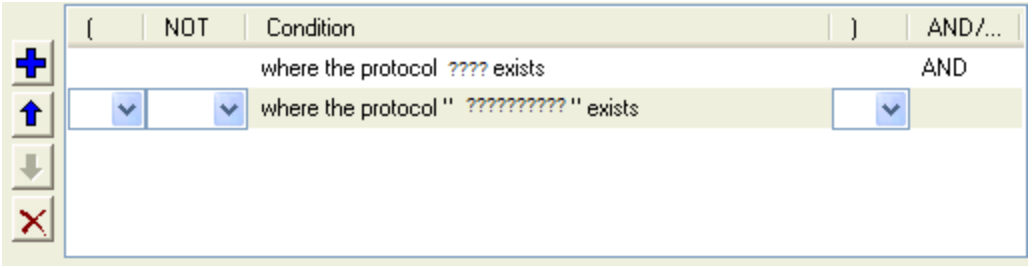


Figure 112. Two Filter Conditions Added with an AND Operator

6. Click the plus icon on the left side of the dialog box and repeat steps 4 and 5 for the next condition. 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.
7. Continue adding conditions until your filter is complete.
8. Include parentheses as needed and set the boolean operators.
9. Click OK.
10. 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.

Figure 113. Save Named Filter Condition Dialog

The Set Condition dialog box closes, creates a tab on the Frame Display with the filter name, and applies the filter.

Filter: Include each frame where the protocol Data exists

When a display filter is applied, a description of the filter appears to the right of the toolbar in the Frame Display windows.

Note: The OK button on the Set Condition dialog box is unavailable (grayed out) until the condition selections are complete.

5.3.1.5 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 the Frame Display window or select Apply/Modify Display Filters… from the filter menu to open the Set Condition dialog box.
2. From the Select each frame combo box choose frames with the conversation as the initial condition.
3. Select an address type—IP, MAC, TCP/UDB—from the Typecombo 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 and continue with step 8.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select a

node address from the second Address combo box..

8. 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 the Frame Display windows.

Note: The OK button is unavailable (grayed out) until the condition selections are complete.

5.3.1.6 The Difference Between Deleting and Hiding Display Filters

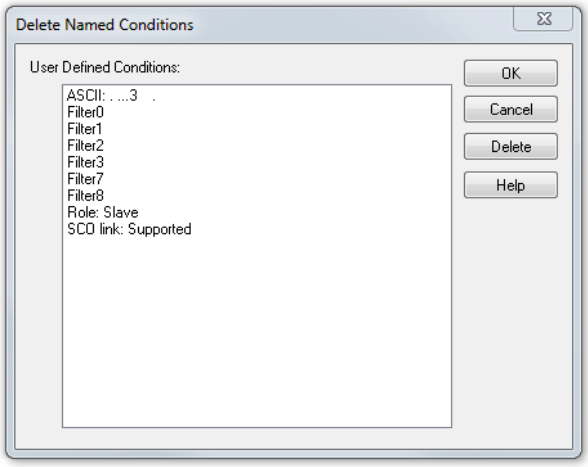
If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

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.

5.3.1.6.1 Deleting Saved Display Filters

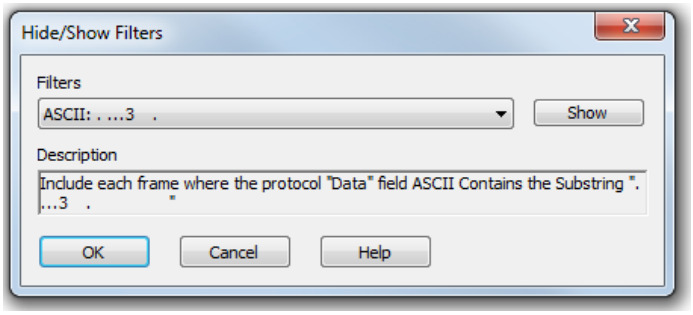
1. Select Delete Display Filters from the Filter menu in the Frame Display window to open the Delete Named Condition dialog. The system displays the Delete Named Condition dialog with a list of all user defined filters.
2. Select the filter to be deleted from the list.
3. Click the Delete button.
4. Click OK. The Delete Named Condition dialog box closes and the system deletes the filter.



5.3.1.6.2 Hiding/Showing a Display Filter

Hiding a Display Filter. If a display filter is showing the following steps will hide that filter but will not delete it.

1. Select Hide/Show Display Filters… from the Filter menu on the Frame Display window to open the Hide/Show Filters dialog. The system displays the Hide/Show Filters 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. The Hide button is only showing if the selected filter is currently showing in the Frame Display.
4. Click OK. The Hide/Show Filters dialog box closes, and the system hides the filter and removes the filter tab from the Frame Display.

Showing a Hidden Display Filter. If a display filter is hidden the following steps will reveal that filter in the Frame Display.

1. Select Hide/Show Display Filters… from the Filter menu in the Frame Display window to open the Hide/Show Filters dialog. The system displays the Hide/Show Filters 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 Filters dialog box closes and the system reveals the filter in the Frame Display.

You can also open the Quick Filter dialog and check the box next to the hidden filter to show or hide a display filter.

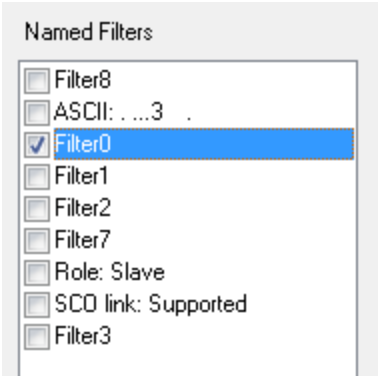
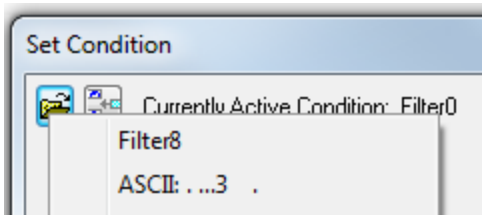


Figure 114. Using Named Filters Section of Quick Filters to Show/Hide Filters

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/Show dialog to display a filter created in one Frame Display in different Frame Display window.

5.3.1.7 Editing Filters

5.3.1.7.1 Modifying a Condition in a Filter



1. Click the Display Filters icon on 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 at the top of the dialog. To display another filter, click the Open icon, and select the filter from the pop-up 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.

5.3.1.7.2 Deleting a Condition in a Filter

If a display filter has two or more conditions you can delete conditions. If there is only one condition set in the filter you must delete the filter using Delete Display Filters… from the Filters menu.

1. Click the Display Filters icon on the Frame Display window or select Apply/Modify Display Filters… from the Filter menu to open the Set Condition dialog box. Click on the Advanced button to show the condition in Boolean format. The dialog box displays the current filter definition. To display another filter, click the Open icon, and select the filter from the pop-up list of all the saved filters.

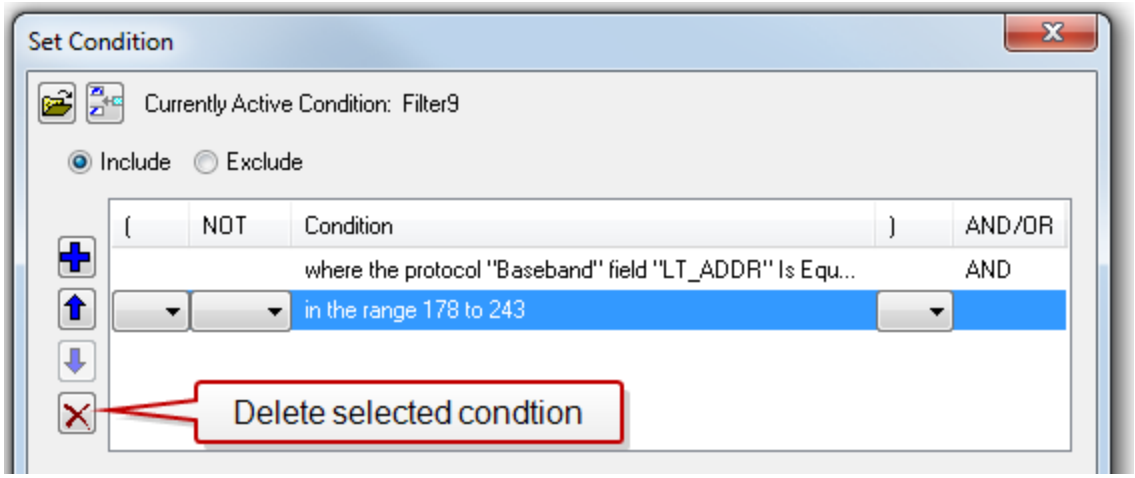


Figure 115. Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.

3. Click the Delete Selected Line 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.

5.3.1.7.3 Renaming a Display Filter

1. Select Rename Display Filters… from the Filter menu in 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 in the Filters combo box.

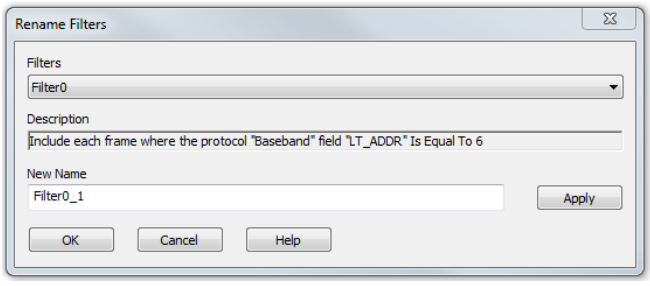


Figure 116. Rename Filters Dialog

2. Select the filter to be renamed from the combo box.

3. Enter a new name for the filter in the New Name box. Optionally click the Apply button and the new name will appear in the Filters combo box and the New Name box will empty. This option allows you to rename several filters without closing the Rename Filter dialog each time.

4. Click OK. The Rename Filter dialog box closes and the system renames the filter.

5.3.2 Protocol Filtering From the Frame Display

5.3.2.1 Quick Filtering on a Protocol Layer

On the Frame Display , click the 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.

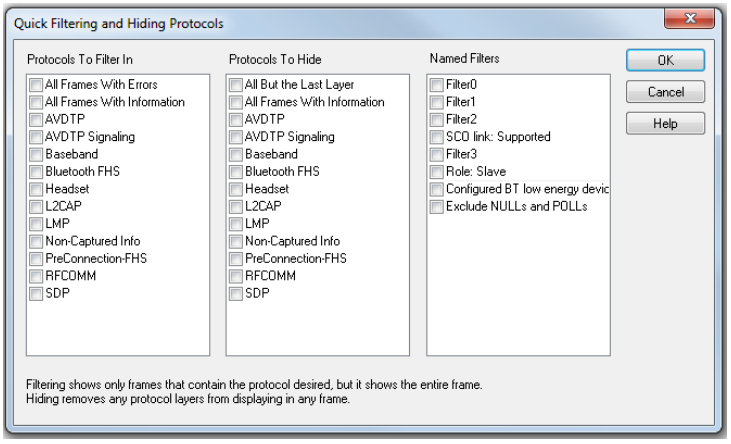


Figure 117. Frame Display Quick Filtering and Hiding Protocols Dialog

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. 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.

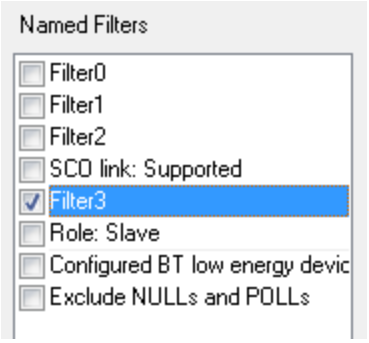
The box in the center is the Protocols To Hide. When you select the checkbox for a protocol in the Protocols To Hide, data for that protocol will not appear in the Decode, Binary, Radix, and Character panes. The frames containing that type data will still appear in the Summary pane, but not in the Decode, 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.

Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.

Then click OK



5.3.2.2 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.

5.3.2.3 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 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.

5.3.2.4 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 "Errors" that displays the results of the All Frames With Errors filter.

Note: When you have multiple Frame Display windows open and you are capturing data, you may receive an error message declaring that "Filtering cannot be done while receiving data this fast." If this occurs, you may have to stop filtering until the data is captured.

Chapter 6: Saving and Importing Data

6.1 Saving Your Data

You can save all or part of the data that you have captured. 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.

6.1.1 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.

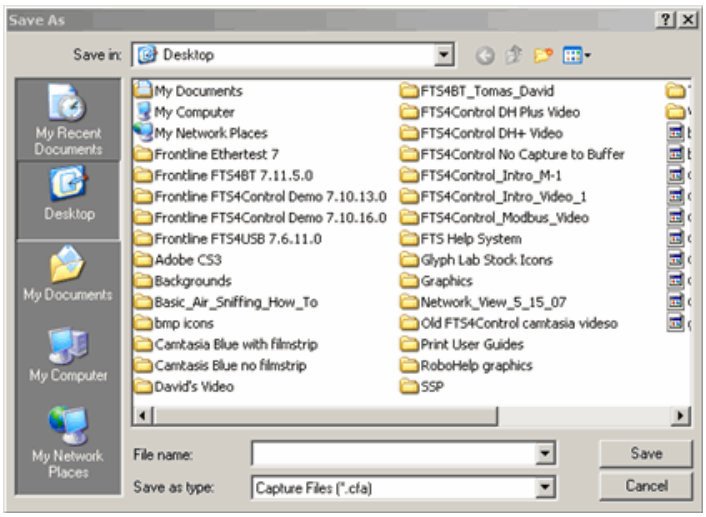
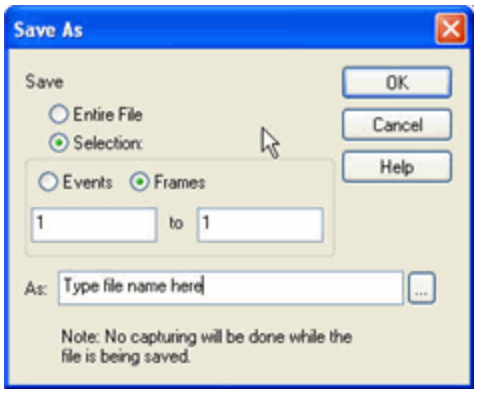


Figure 118. Windows Save dialog

4. Type a file name 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.

6.1.2 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.
5. Click on the radio button labeled Entire File.
6. 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.
7. Type a file name in the 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.

8. When you are finished, click OK.

6.1.3 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

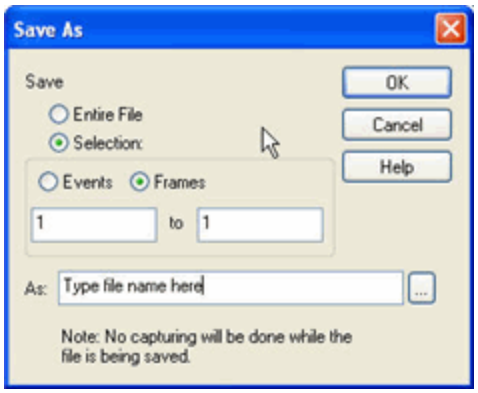
5. Select Save Selection or Save As from the right click menu

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 file name in the 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.



6.1.4 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.

6.1.5 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  , 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 features are supported from Edit menu and the toolbar  when text is selected. Undo and Redo features are all supported from Edit menu and the toolbar  at the current cursor location.
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.

6.2 Loading and Importing a Capture File

6.2.1 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.

6.2.2 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. Left of the File name text box, select from the drop-down list Supported File Types box to All Importable File Types or All Supported File Types (*.cfa, *.log, *.txt, *.csv, *.cap). 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.

6.3 Printing

6.3.1 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.

Frame Display Print

The Frame Display Print feature provides the user with the option to print the capture buffer or the current selection. The maximum file size, however, that can be exported is 1000 frames.

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.

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—No decode section—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.
4. Click on selected layers in the list to de-select, or click the Reset Selected Layers button to de-select all selected layers.

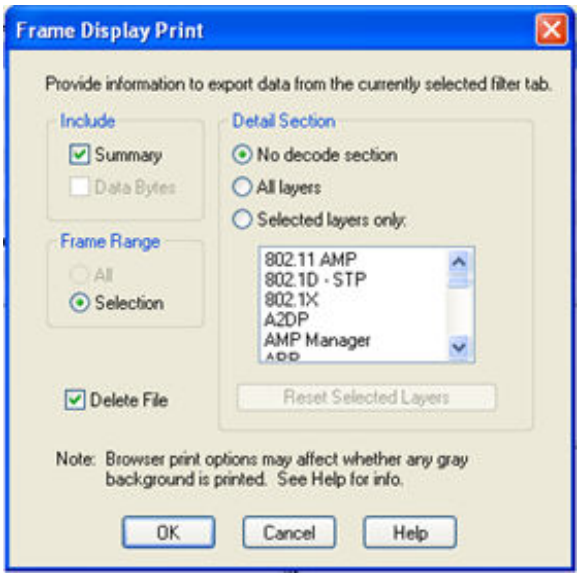


Figure 119. Frame Display Print Dialog

5. Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

   Choosing All prints up to 1000 frames from the buffer.

   Choosing Selection prints only the frames you select in the Frame Display window.

6. Selecting the Delete File deletes the temporary html file that was used during printing

7. 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.

Frame Display HTML Export

The Frame Display HTML Export feature provides the user with the option to export the capture buffer to an .html file. The maximum file size, however, that can be exported is 1000 frames.

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.

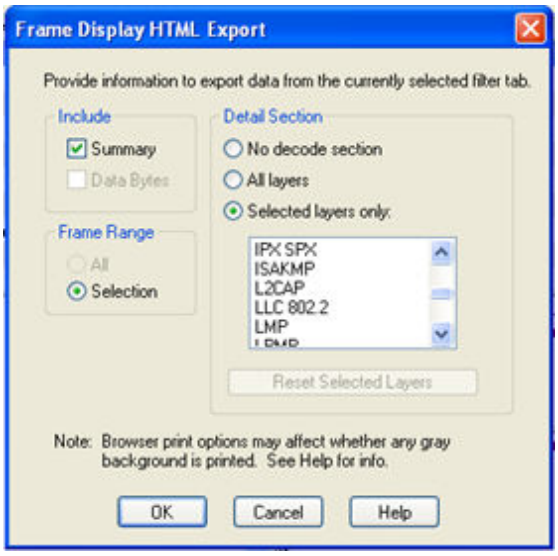


Figure 120. Frame Display HTML Export Dialog

2. From this point the procedure is the same as steps 2 through 5 in "How to Print Frame Display Data" above.
3. Click the OK button.

   The Save As dialog appears

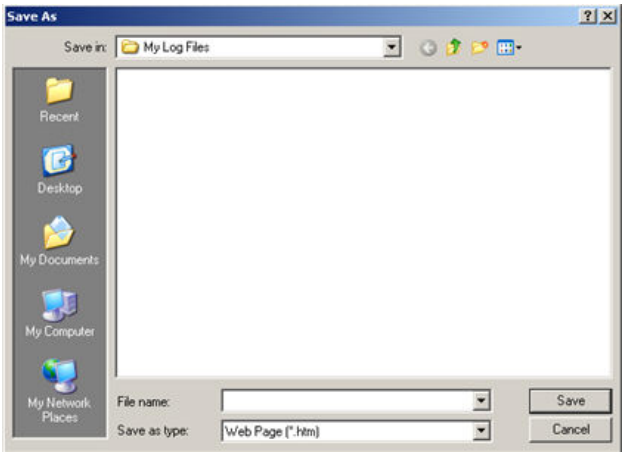


Figure 121. Save As Dialog

4. Enter a name for the file you want to save. The .htm extension is automatically added.
5. Select Save

The file is saved as a .htm file in the file location you chose

6.3.2 Printing from the Event Display

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.

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 , 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: Note: See "Configure the Print File Range in the Event Display Print Dialog" above for an explanation of these selections

Figure 122. Event Display Print Dialog

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.

6.4 Exporting

6.4.1 Frame Display 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 or open the Frame Display File menu.
2. Select the Export… menu item.
3. Select a storage location and enter a File name.
4. Select Save.

6.4.2 Exporting a File with Event Display Export

With the Event Display Export dialog you can export the contents of the Event Display dialog as a test (.txt), CSV (.csv.), HTML (.htm), or Binary File (.bin). You also have the option of exporting the entire capture buffer or just the current selection of the Event Display dialog.

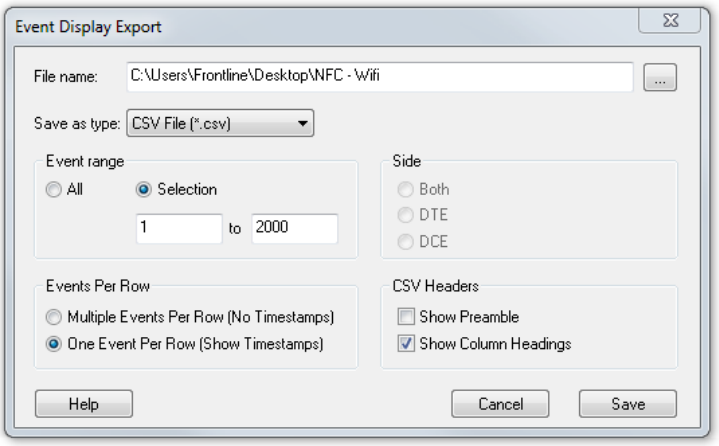


Figure 123. Event Display Export Example: .csv file.

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. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

   Binary File (*.bin)
4. 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.
   - 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.
5. Next you need to select the Side variable for serial communications.
   - is used to determine whether you want to export data from , or both.
   - Choose Host, Function\Control or Both to determine how you want to export the data.
5. Choose Host, Function\Control or Both to determine how you want to export the data.
6. Choose whether you want to display multiple events or single events per row.

Events Per Row: You can choose to display Multiple Events Per Row, but this method contains no timestamps. If you select One Event Per Row, you can display timestamps. multiple events or single events per row.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

.

The timestamp data types displayed in columns for One Event Per Row.

Timestamp

Delta

Event Number

Byte Number

Frame Number

Type

Hex

Dec

Oct

Bin

Side

ASCII | 7-bit ASCII | EBCDIC | Baudot

RTS

CTS

DSR

DTR

CD

RI

UART Overrun

Parity Error

Framing Error

7. If you select .csv as the file type, choose whether you want to hide/display Preambles or Column Headings in the exported file
8. Click Save. The Event Display Export file is saved to the locations you specified in File name.

	A	B	C	D	E	F	G	H	I	J	K
1	Timestamp	Delta	Event Number	Byte Number	Frame Number	Type	Hex	Dec	Oct	Bin	ASCII
632	11/30/2012 12:20:02.895166 PM	0:00:00.00	631	626	3	Data	0	0	0	0	.
633	11/30/2012 12:20:02.895166 PM	0:00:00.00	632	627	3	Data	0	0	0	0	.
634	11/30/2012 12:20:02.895166 PM	0:00:00.00	633	628	3	Data	0	0	0	0	.
635	11/30/2012 12:20:02.895166 PM	0:00:00.00	634	629	3	Data	98	152	230	10011000	.
636	11/30/2012 12:20:02.895166 PM	0:00:00.00	635	630	3	Data	70	112	160	1110000	p
637	11/30/2012 12:20:02.895166 PM	0:00:00.00	636	631	3	Data	94	148	224	10010100	.
638	11/30/2012 12:20:02.895166 PM	0:00:00.00	637	632	3	Data	22	34	42	100010	"
639	11/30/2012 12:20:02.895166 PM	0:00:00.00	638	633	3	Data	21	33	41	100001	!
640	11/30/2012 12:20:02.895166 PM	0:00:00.00	639	634	3	Data	1c	28	34	11100	.
641	11/30/2012 12:20:02.895166 PM	0:00:00.00	640	635	3	Data	80	128	200	10000000	.
642	11/30/2012 12:20:02.895166 PM	0:00:00.00	641	636	3	Data	80	128	200	10000000	.
643	11/30/2012 12:20:02.895166 PM	0:00:00.00	642	637	3	Data	80	128	200	10000000	.
644	11/30/2012 12:20:02.895166 PM	0:00:00.00	643	638	3	Data	80	128	200	10000000	.

Figure 124. Example: .csv Event Display Export, Excel spreadsheet

6.4.2.1 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.

6.4.2.2 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.

Chapter 7: General Information

7.1 System Settings and Progam Options

7.1.1 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.

There are two ways you can capture data: Series of files or Single File.

7.1.1.1 Series of files

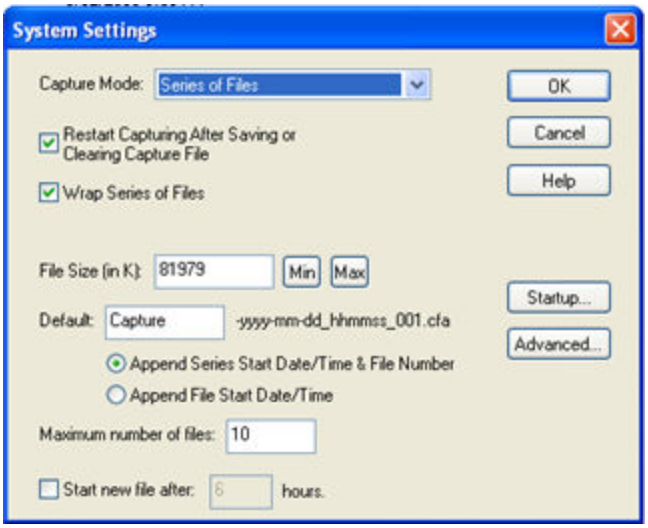


Figure 125. System Settings for defining how to capture data

This option lets you capture to more than one file, based on file size or time.

- Restart Capturing After Saving or Clearing Capture File: the analyzer restarts capture to the file immediately after the file is closed.
- Wrap Series of Files: 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:

  1. Click the Min button to see/set the minimum acceptable value for the file size.

  2. Click the Max button to see/set the maximum acceptable value for the file size.

You can accept these values, or you can enter a unique file size. But if you try to close the dialog after entering a value greater than the maximum or less than the minimum, you will see th1s dialog.

- Default:

  Enter a name for the capture file in the Default text box. Each saved file will begin with this name. 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.

- 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.

- Maximum number of files:

  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.

- Start new file after:

  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 makes a new 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.

7.1.1.2 Single File

This option allows the analyzer to capture data to a file. Each time you capture the file you must provide a file name. The size of each file cannot 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.

7.1.1.3 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.

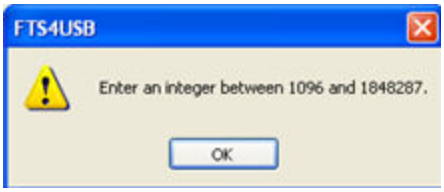
- Wrap File

  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: The size of the file will depend of the available hard disk space.

  1. Click the Min button to see/set the minimum acceptable value for the file size.

  2. Click the Max button to see/set the maximum acceptable value for the file size.



You can accept these values, or you can enter a unique file size. But if you try to close the dialog after entering a value greater than the maximum or less than the minimum, you will see the following dialog.

- 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.

7.1.1.4 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.

7.1.1.5 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.

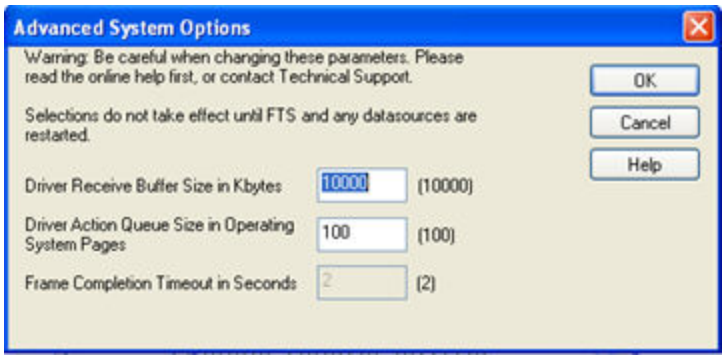


Figure 126. Advanced System Options dialog

- 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.

  The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

Note: This option is currently disabled.

7.1.1.6 Selecting Start Up Options

To open this window:

1. Choose System Settings from the Options menu on the Control window.
2. On the System Settings window, click the Start Up button.
3. Choose one of the options to determine if the analyzer starts data capture immediately on starting up or not.

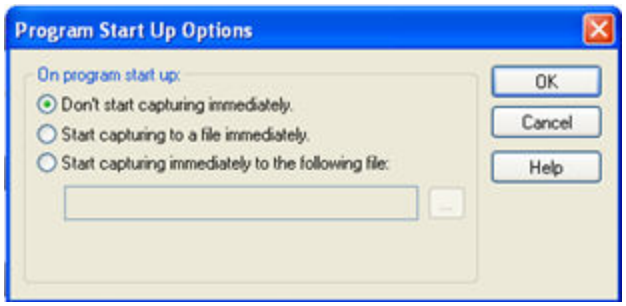


Figure 127. Start Up Options dialog

- Don't start capturing immediately - This is the default setting. The analyzer begins monitoring data but does not begin capturing data until clicking the Start Capture icon on the Control, Event Display or Frame Display windows.
- Start capturing to a file immediately - When the analyzer starts up, it immediately opens a capture file and begins 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 file name 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.

7.1.2 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.

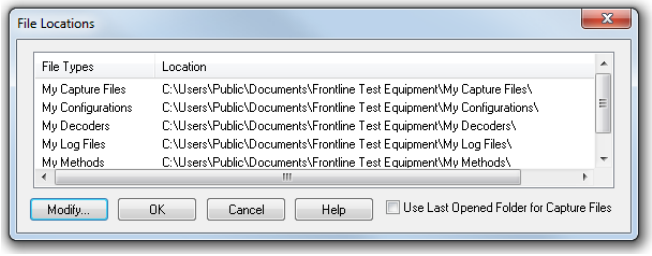


Figure 128. File Locations dialog

2. Select the default location you wish to change.
3. Click Modify.
4. Browse to a new location.

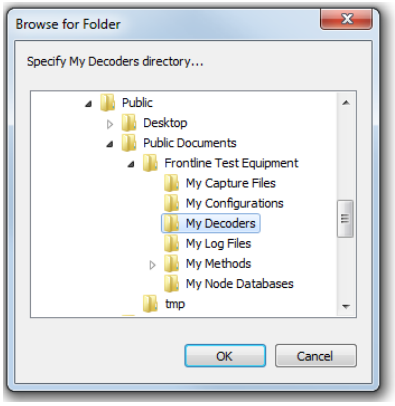


Figure 129. File Locations Browse dialog

5. Click OK.
6. Click OK when finished.

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 Frontline. For example, if an Frontline product is installed at C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\ then "My Decoders" cannot be set to any of the following:

- C:\ My Decoders\
- C:\Users\ My Decoders\
- C:\Users\\Public\My Decoders\
- C:\Users\Public\Public Documents\My Decoders\
- or to any directory that already exists in the path C:\Users\Public\Public Documents\Frontline Test Equipment\My 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 for example. 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. **ComProbe software 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.

7.1.3 Side Names

The Side Names dialog is used to change the names of objects and events that appear in various displays. The Side Names dialog will change depending on the sniffing technology in use at the time the software was loaded.

Changes to the Names are used throughout the program.

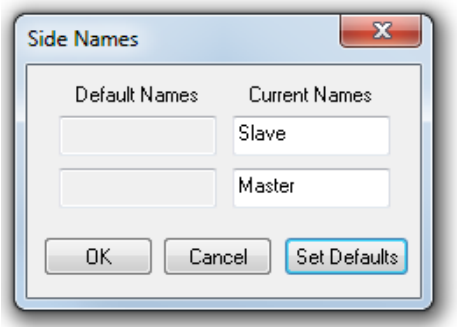


Figure 130. Example: Side Names Where "Slave" and "Master" are current

1. To open the Side Names dialog, choose Side Names… from the Options menu on the Control window.
2. To change a name, click on the name given in the Current Names column, and then click again to modify the name (a slow double-click).
3. Select OK to initiate the changes. The changes that have been made will not fully take effect for any views already open. Closing and reopening the views will cause the name change to take effect.
4. To restore the default values, click the Set Defaults button.

7.1.4 Timestamping

Timestamping is the process of precise recording in time of packet arrival. Timestamps is an optional parameter in the Frame Display and Event Display that can assist in troubleshooting a network link.

7.1.4.1 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:

Choose Set Timestamp Format… from the Options menu on the Frame Display and Event Display window or click on the Timestamping Option  icon in the Event Display toolbar. The Timestamping Options window will open.

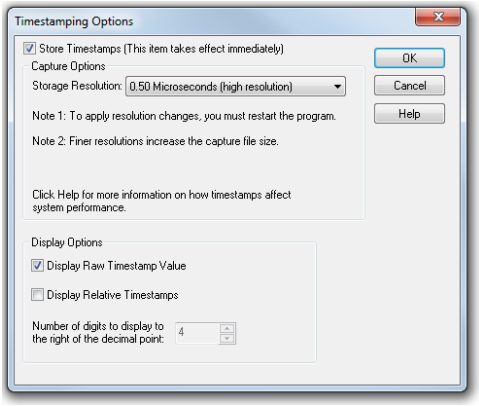


Figure 131. Timestamping Options dialog

7.1.4.1.1 Enabling/Disabling Timestamp

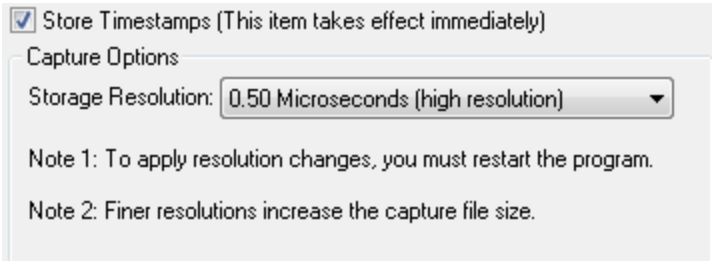
To enable timestamping click to make a check appear in the checkbox Store Timestamps (This time takes effect immediately). Removing the check will disable timestamping.

7.1.4.1.2 Changing the Timestamp 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.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

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. Go to the Capture Options section of the window.
2. Change the resolution listed in the Storage Resolution box.

Note: If you change the resolution, you need to exit the analyzer and restart in order for the change to take effect.

7.1.4.1.2.1 Performance Issues with High Resolution Timestamp

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.

7.1.4.1.3 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 the Event Display 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 Display Relative Timestamp you can set the number of digits to display using the up or down arrows on the numeric list.

7.1.4.1.4 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 the Event Display  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.

7.2 Technical Information

7.2.1 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.

7.2.2 Ring Indicator

The following information applies when operating the analyzer in Spy mode or Source DTE, No FTS Cables mode. When using the cables supplied with the analyzer to capture or source data, Ring Indicator (RI) is routed to a different pin which generates interrupts normally.

There is a special case involving Ring Indicator and computers with 8250 UARTs or UARTs from that family where the state of RI may not be captured accurately. Normally when a control signal changes state from high to low or low to high, an interrupt is generated by the UART, and the analyzer goes to see what has changed and record it. Ring Indicator works a little differently. An interrupt is generated when RI changes from high to low, but not when RI changes from low to high. If Ring Indicator changes from low to high, the analyzer does not know that RI has changed state until another event occurs that generates an interrupt. This is simply the way the UART works, and is not a deficiency in the analyzer software.

To minimize the chance of missing a Ring Indicator change, the analyzer polls the UART every millisecond to see if RI has changed. It is still possible for the analyzer to miss a Ring Indicator change if RI and only RI changes state more than once per millisecond.

UARTs in the 8250 family include 8250s, 16450s, 16550s and 16550 variants. If you have any questions about the behavior of your UART and Ring Indicator, please contact technical support.

7.2.3 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.

7.2.4 Event Numbering

This section provides information 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.

7.2.5 Useful Character Tables

7.2.5.1 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

7.2.5.2 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

7.2.5.3 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						

7.2.5.4 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.

Communications Control Characters

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

Communications Control Characters(continued)

Abbreviation	Control Character	Text
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

7.2.6 The Frontline Serial Driver

ComProbe software uses custom versions of the standard Windows serial drivers in order to capture data. These drivers are usually installed during the routine product installation. However, if you need to install the serial driver after ComProbe software has already been installed, please refer to the instructions available in the Setup folder installed under Start | Programs | [Product Name and version #] | Setup | How to Install the FTS Serial Driver.

7.2.7 DecoderScript Overview

The DecoderScript™ Reference Manual and User Guide is delivered with each Frontline ComProbe® Protocol Analysis System installation package under Developer Tools. The manual is also available on-line at FTE.com.

The main purpose of this manual is to describe DecoderScript™, the language used in writing decoders. DecoderScript allows you to create new decoders or modify existing decoders to expand the functionality of your ComProbe protocol analyzer. DecoderScript displays protocol data, checks the values of fields, validates checksums, converts and combines field values for convenient presentation. Decoders can also be augmented with custom C++-coded functions, called "methods", to extend data formatting, validation, transformations, and so on.

A decoder defines field-by-field how a protocol message can be taken apart and displayed. The core of each "decoder" is a program that defines how the protocol data is broken up into fields and displayed in the Frame Display window of the analyzer software.

This manual provides instruction on how to create and use custom decoders. When reading the manual for the first time, we encourage you to read the chapters in sequence. The chapters are organized in such a way to introduce you to DecoderScript writing step- by- step.

Screenshots of the ComProbe protocol analyzer have been included in the manual to illustrate what you see on your own screen as you develop decoders. But you should be aware for various reasons, the examples may be slightly different from the ones that you create. The differences could be the result of configuration differences or because you are running a newer version of the program. Do not worry if an icon seems to be missing, a font is different, or even if the entire color scheme appears to have changed. The examples are still valid.

Examples of decoders, methods, and frame recognizers are included in this manual. You can cut and paste from these examples to create your own decoders.

A quick note here: Usually the pasted code appears the same as the original in your editor. Some editors, however, change the appearance of the text when it is pasted (something to do with whether it is ASCII or Unicode text). If you find that the pasted text does not appear the same as the original, you can transfer the code into a simple text editor like Notepad, save it as an ANSI (ASCII) file, then use it in your decoder.

These files are installed in the FTE directory of the system Common Files directory. The readme file in the root directory of the protocol analyzer installation contains a complete list of included files. Most files are located in My Decoders and My Methods.

We will be updating our web site with new and updated utilities, etc, on a regular basis and we urge decoder writers to check there occasionally.

7.3 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://fte.com/support/supportrequest.aspx

Email: tech_support@fte.com

If you need to talk to a technical support representative about your ComProbe 802.11 product, support is available between 9 am and 5 pm, U.S. Eastern Time zone, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

7.3.1 Instructional Videos

Frontline provides a series of videos to assist the user and may answer your questions. These videos can be accessed at fte.com/support/videos.aspx. On this web page use the Video Filters sidebar to select instructional videos for your product.

Appendix A: Application Notes

1. Bluetooth Virtual Sniffing

A.1 Bluetooth Virtual Sniffing

A.1.1 Introduction

The ComProbe software Virtual sniffing function simplifies Bluetooth® development and is easy to use. Frontline's Virtual sniffing with Live Import provides the developer with an open interface from any application to ComProbe software so that data can be analyzed and processed independent of sniffing hardware. Virtual sniffing can also add value to other Bluetooth development tools such as Bluetooth stack SDKs (Software Development Kits) and Bluetooth chip development kits.

This white paper discusses:

- Why HCI sniffing and Virtual sniffing are useful.
- Bluetooth sniffing history.
- What is Virtual sniffing?
- Why Virtual sniffing is convenient and reliable.
- How Virtual sniffing works.
- Virtual sniffing and Bluetooth stack vendors.
- Case studies: Virtual sniffing and Bluetooth mobile phone makers.
- Virtual sniffing and you. • Where to go for more information.

A.1.2 Why HCI Sniffing and Virtual Sniffing are Useful

Because the Bluetooth protocol stack is very complex, a Bluetooth protocol analyzer is an important part of all Bluetooth development environments. The typical Bluetooth protocol analyzer "taps" a Bluetooth link by capturing data over the air. For many Bluetooth developers sniffing the link between a Bluetooth Host CPU and a Bluetooth Host Controller—also known as HCI-sniffing—is much more useful than air sniffing.

HCI-sniffing provides direct visibility into the commands being sent to a Bluetooth chip and the responses to those commands. With air sniffing a software engineer working on the host side of a Bluetooth chip has to infer and often guess at what their software is doing. With HCI-sniffing, the software engineer can see exactly what is going on. HCI-sniffing often results in faster and easier debugging than air sniffing.

ComProbe software's Virtual sniffing feature is a simple and easy way to perform HCI-sniffing. Virtual sniffing is not limited to just HCI-sniffing, but it is the most common use and this white paper will focus on the HCI-sniffing application of Virtual sniffing.

It is also important to understand that ComProbe software is a multi-mode product. ComProbe software does support traditional air sniffing. It also supports serial HCI sniffing (for the H4 (HCI UART), H5 (3-wire UART) , and BCSP (BlueCore Serial Protocol) protocols), USB HCI (H2) sniffing, SDIO sniffing, and Virtual sniffing. So with ComProbe software nothing is sacrificed—the product is simply more functional than other Bluetooth protocol analyzers.

A.1.3 *Bluetooth* Sniffing History

Frontline has a strong appreciation for the importance of HCI sniffing because of the way we got involved with *Bluetooth*. Because of our company history, we are uniquely qualified to offer a multi-mode analyzer that

provides many ways to sniff and supports a wide variety of protocols. This brief *Bluetooth* sniffing history should help you understand our approach to *Bluetooth* protocol analysis.

In the early days of *Bluetooth*, there were no commercially available *Bluetooth* protocol analyzers, so developers built their own debug tools and/or used protocol analyzers that weren't built for *Bluetooth*. Many developers built homegrown HCI analyzers—basically hex dumps and crude traces—because they recognized the need for visibility into the HCI interface and because it was too difficult to build air sniffers. Several companies developed air sniffers because they saw a market need and because they realized that they could charge a high price (USD $25,000 and higher).

Two *Bluetooth* chip companies, Silicon Wave and Broadcom were using Frontline's Serialtest® serial analyzer to capture serial HCI traffic and then they would manually decode the HCI byte stream. This manual decoding was far too much work and so, independently, Silicon Wave and Broadcom each requested that Frontline produce a serial HCI *Bluetooth* analyzer that would have all the features of Serialtest. In response to these requests Frontline developed SerialBlue®—the world's first commercially available serial HCI analyzer.

The response to SerialBlue was very positive. When we asked our *Bluetooth* customers what they wanted next we quickly learned that there was a need for an affordable air sniffer that provided the same quality as SerialBlue. We also learned that the ultimate *Bluetooth* analyzer would be one that sniff air and sniff HCI simultaneously.

As work was progressing on our combination air sniffer and HCI sniffer the functional requirements for *Bluetooth* analyzers were changing. It was no longer good enough just to decode the core *Bluetooth* protocols (LMP, HCI, L2CAP, RFCOMM, and OBEX). Applications were beginning to be built on top of *Bluetooth* and therefore application level protocol decoding was becoming a requirement. For example, people were starting to browse the Internet using *Bluetooth*-enabled phones and PDAs therefore a good *Bluetooth* analyzer would need to support TCP/IP, HTTP, hands-free, A2DP, etc.

For Frontline to support for these higher levels protocols was no problem since they were already in use in other Frontline analyzer products. People have been using Frontline Serialtest serial analyzers and Ethertest™ Ethernet analyzer to troubleshoot TCP/IP and Internet problems for many years.

As we continued to work closely with the *Bluetooth* community we also came across one other requirement: sniffing itself had to be made easier. We took a two-pronged approach to this problem. We simplified air sniffing (and we continue to work on simplifying the process of air sniffing) and we invented Virtual sniffing.

A.1.4 Virtual Sniffing—What is it?

Historically, protocol analyzers have physically tapped the circuit being sniffed. For example, an Ethernet circuit is tapped by plugging into the network. A serial connection is sniffed by passively bridging the serial link. A *Bluetooth* air sniffer taps the piconet by synchronizing its clock to the clock of the piconet Master.

Not only is there a physical tap in traditional sniffing, but the sniffer must have some knowledge of the physical characteristics of the link being sniffed. For example, a *Bluetooth* air sniffer must know the BD_ADDR of at least one piconet member to allow it perform clock synchronization. A serial sniffer must know the bit rate of the tapped circuit or be physically connected to the clock line of the circuit.

With Virtual sniffing the protocol analyzer itself does not actually tap the link and the protocol analyzer does not require any knowledge of the physical characteristics of the link.

In computer jargon, "virtual" means "not real". Virtual memory is memory that doesn't actually exist. Virtual reality is something that looks and feels real, but isn't real. So we use the term Virtual sniffing, because there is sniffing taking place, but not in the traditional physical sense.

A.1.5 The Convenience and Reliability of Virtual Sniffing

Virtual sniffing is the most convenient and reliable form of sniffing and should be used in preference to all other forms of sniffing whenever practical. Virtual sniffing is convenient because it requires no setup to use except for a very small amount of software engineering (typically between one and four hours) that is done once and then never again. Once support for Virtual sniffing has been built into application or into a development environment none of the traditional sniffing setup work need be done.

This means:

- NO piconet synchronization.
- NO serial connection to tap.
- NO USB connection to tap.

Virtual sniffing is reliable because there is nothing that can fail. With Virtual sniffing all data is always captured.

A.1.6 How Virtual Sniffing Works

ComProbe software Virtual sniffing works using a feature called Live Import. Any application can feed data into ComProbe software using Live Import. A simple API provides four basic functions and a few other more advanced functions. The four basic Live Import functions are:

- Open a connection to ComProbe software.
- Close a connection to ComProbe software.
- Send an entire packet to ComProbe software.
- Send a single byte to ComProbe software.

All applications that send data to ComProbe software via Live Import use the first two functions. Usually only one of the two Send functions is used by a particular application. When ComProbe software receives data from the application via Live Import, the data is treated just as if it had been captured on a Frontline ComProbe sniffer. The entire protocol stack is fully decoded.

With Virtual sniffing the data can literally be coming from anywhere. ComProbe software does not care if the data being analyzed is being captured on the machine where ComProbe software is running or if the data is being captured remotely and passed into ComProbe software over an Internet connection.

A.1.7 Virtual Sniffing and *Bluetooth* Stack Vendors

As the complexity of the *Bluetooth* protocol stack increases *Bluetooth* stack vendors are realizing that their customers require the use of a powerful *Bluetooth* protocol analyzer. Even if the stack vendor's stack is bug free, there are interoperability issues that must be dealt with.

The homegrown hex dumps and trace tools from the early days of *Bluetooth* just are not good enough anymore. And building a good protocol analyzer is not easy. So stack vendors are partnering with Frontline. This permits the stack vendors to concentrate of improving their stack.

The typical *Bluetooth* stack vendor provides a Windows-based SDK. The stack vendor interfaces their SDK to ComProbe software by adding a very small amount of code to the SDK, somewhere in the transport area, right about in the same place that HCI data is sent to the Host Controller.

If ComProbe software is installed on the PC and the Virtual sniffer is running then the data will be captured and decoded by ComProbe software, in real-time. If ComProbe software is not installed or the Virtual sniffer is not running then no harm is done. Virtual sniffing is totally passive and has no impact on the behavior of the SDK.

One Frontline stack vendor partner feels so strongly about ComProbe software that not only have they built Virtual sniffing support in their SDK, but they have made ComProbe software an integral part of their product offering. They are actively encouraging all customers on a worldwide basis to adopt ComProbe software as their protocol analysis solution.

A.1.8 Case Studies: Virtual Sniffing and *Bluetooth* Mobile Phone Makers

Case Study # 1

A *Bluetooth* mobile phone maker had been using a homemade HCI trace tool to debug the link between the Host CPU in the phone the *Bluetooth* chip. They also were using an air sniffer. They replaced their entire sniffing setup by moving to ComProbe software.

In the original test setup the Host CPU in the phone would send debug messages and HCI data over a serial link. A program running on a PC logged the output from the Host CPU. To implement the new system using Virtual sniffing, a small change was made to the PC logging program and it now sends the data to ComProbe software using the Live Import API. The HCI traffic is fully decoded and the debug messages are decoded as well.

The decoder for the debug messages was written using ComProbe software's DecoderScript feature. DecoderScript allows ComProbe software user to write custom decodes and to modify decodes supplied with ComProbe software. DecoderScript is supplied as a standard part of ComProbe software. In this case, the customer also created a custom decoder for HCI Vendor Extensions.

The air sniffer that was formerly used has been replaced by the standard ComProbe software air sniffer.

Case Study # 2

A second *Bluetooth* mobile phone maker plans to use Virtual sniffing in conjunction with a Linux-based custom test platform they have developed. Currently they capture serial HCI traffic on their Linux system and use a set of homegrown utilities to decode the captured data.

They plan to send the captured serial HCI traffic out of the Linux system using TCP/IP over Ethernet. Over on the PC running ComProbe software they will use a simple TCP/IP listening program to bring the data into the PC and this program will hand the data off to ComProbe software using the Live Import API.

A.1.9 Virtual Sniffing and You

If you are a *Bluetooth* stack vendor, a *Bluetooth* chip maker, or a maker of any other products where integrating your product with ComProbe software's Virtual sniffing is of interest please contact Frontline to discuss your requirements. There are numerous approaches that we can use to structure a partnership program with you. We believe that a partnership with Frontline is an easy and cost-effective way for you to add value to your product offering.

If you are end customer and you want to take advantage of Virtual sniffing, all you need to do is buy any Frontline *Bluetooth* product. Virtually sniffing comes standard with product.

A.1.10 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.

Web: http://www.fte.com, click Support

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

Author: Eric Kaplan

Publish Date: May 2003

Revised: December 2013

Index

D