TELEDYNE LECROY
Everywhereyoulook™

frontline SODERA™

WIDEBAND BLUETOOTH® PROTOCOL ANALYZER

Hardware and Software User Manual

ProbeSync

ES Audio Expert System

Revision Date: 3/17/2017

Contents

Chapter 1 Frontline Hardware & Software

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

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

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

Frontline software is an easy to use and powerful protocol analysis platform. Simply use the appropriate Frontline hardware or write your own proprietary code to pump communication streams directly into the Frontline software where they are decoded, decrypted, and analyzed. Within the Frontline 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 Frontline software functions for your Frontline hardware. Should you have any questions contact the Frontline Technical Support Team.

1.1 What is in this manual

The Frontline 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 Frontline 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 Frontline 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 Frontline software in Data Capture Methods. You will be introduced to the Control window that is the primary operating dialog in the Frontline software.
- **Chapter 3 Configuration Settings**. The software and hardware is configured to capture data. Configuration settings may vary for a particular Frontline 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 Computer Minimum System Requirements

Frontline supports the following computer systems configurations:

- Operating System: Windows 7/8/10
- USB Port: USB 2.0 High-Speed or or later

The Frontline software must operate on a computer with the following minimum characteristics.

- Processor: Core i5 processor at 2.7 GHz
- RAM: 4 GB
- Free Hard Disk Space on C: drive: 20 GB

1.3 Software Installation

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

Use this link: http://www.fte.com/sodera-soft.

Chapter 2 Getting Started

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

2.1 Sodera™ Hardware

2.1.1 Front Panel Controls

Frontline Sodera™ front panel is shown below. The panel provides controls to power up and shut down the Frontline Sodera hardware, and it provides indicators to show the power, battery, and capture status.

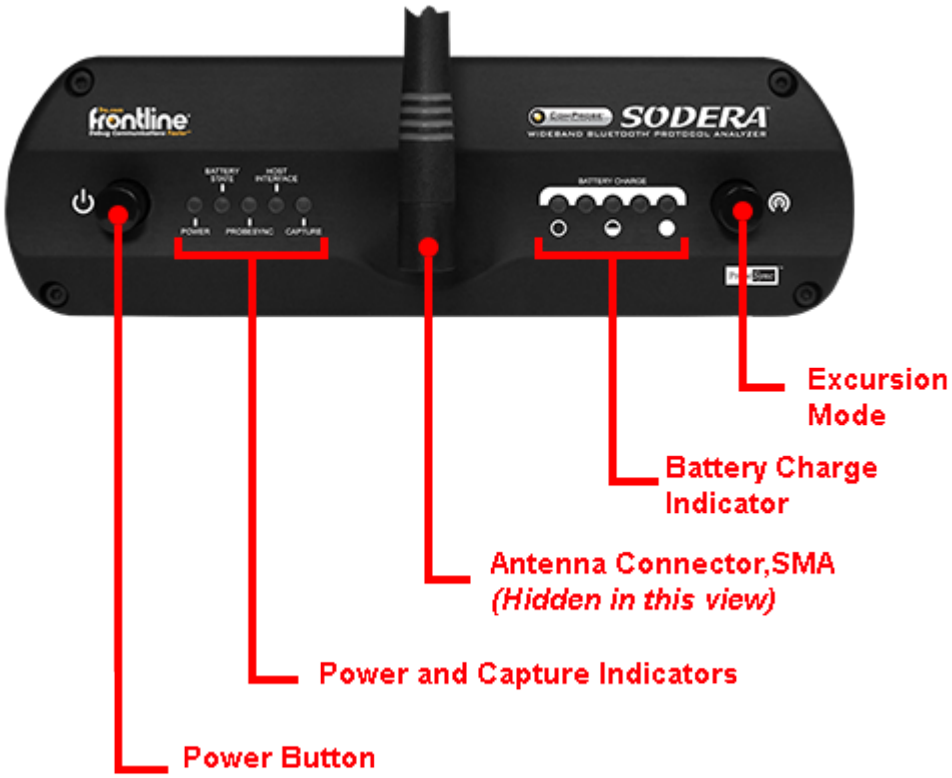


Figure 2.1 - Sodera Front Panel Controls and Indicators

Power On/Off Button: Press and hold the button for at least 1/2 second, and then release the button to power on or power off the system.

Pressing and holding the button for at least five seconds will initiate an **emergency shut down** sequence.

Status Indicators: Colored LEDs show the status of power and capture.

Table 2.1 - Sodera Front Panel Status Indicators

Indicator	Color	State	Status Indicated
Power	None	Off	Unit is powered off
	Green	Constant	Unit is switched on
	Red	Blinking	Unit is approaching its maximum thermal load and should be shut down.
		Constant	Unit has been automatically disabled due to thermal overload.
	Amber	Constant	Unit is powering down.
Battery State	None	Off	No battery present
	Green	Constant	Battery present and is at normal operating voltage
		Slow Flash	Battery charging
	Amber	Fast Flash	Battery fault

Table 2.1 - Sodera Front Panel Status Indicators(continued)

Indicator	Color	State	Status Indicated
Host Interface	None	Off	No host interface is connected.
	Green	Constant	Host interface is connected.
	Amber	Constant	Internal error
Capture	None	Off	Unit is not actively capturing data
	Green	Constant	Unit is capturing data
	Red	Constant	Unit has engaged RF overload protection; the RF signal is too strong.

Antenna SMA Connector: Antenna attaching point.

Battery Charge : The following table shows the charge state of the installed battery. When the battery is not installed, all LEDs are off except when the unit is in the process of powering up. In that case they repeatedly light up in sequence.

Table 2.2 - Sodera Battery Charge State LED Indicators

Indicator LEDs	Charge Status
●●●●●	Greater than 80%
●●●●○	Between 60 and 80%
●●●○○	Between 40 and 60%
●●○○○	Between 20 and 40%
●○○○○	Less than 20%
○○○○○	Not Active

Excursion Mode: When configured for Excursion mode, pressing this button will begin data capture—the same as the Record/Recording button on the Sodera Window Capture Toolbar. The **Excursion Mode** button is inactive when Sodera is connected to a computer . To operate in the Excursion mode, the Sodera hardware must have been previously configured from the Frontline software prior to disconnecting from the computer. The Sodera hardware will retain those configuration settings when disconnected from the computer. See Capture Options Dialog on page 38.

2.1.2 Rear Panel Connectors

The rear panel is shown below. The panel provides connectors for external power, ProbeSync™, HCI, and for connection to the computer hosting the Frontline software.

Figure 2.2 - Sodera Rear Panel Connectors

+12VDC: Connection to the Frontline supplied AC-to-DC power adapter, or a 12 VDC auxiliary vehicle outlet system can be used.

ProbeSync™ **IN/OUT**: Used for synchronizing multiple capture devices. Sodera can act as a clock source (master) device providing the clock to synchronize timestamping with connected target (slave) devices. When operating as a master device the **OUT** RJ-45 connector provides the synchronizing clock. The synchronizing clock can be attached to a slave Frontline Sodera or a Frontline 802.11, for example. When operating as a slave device, the **IN** RJ-45 connector receives the synchronizing clock from a master Sodera unit.

HCI USB 1/HCI USB 2:USB Type B and a USB Type A connectors allow capture of HCI USB data. HCI USB 1 and HCI USB 2 are independent groupings of the Type A and Type B connectors. The HCI USB 1 connectors use the same Sodera unit internal interface as the Sodera HCI POD1 UART pins. Likewise the HCI USB 2 connectors use the same internal interface as the Sodera HCI POD2 UART pins. Therefore you cannot simultaneously capture USB and UART on the "1" interface or on the "2" interface. Refer to Connecting for USB Capture on page 17 and to Connecting for HCI/WCI-2 & Logic Capture on page 14.

PC HOST : USB 2.0 port for connecting Sodera to the host computer where the Frontline software resides. This connector provides host computer command, control, and data transfer.

Note: At this time all other rear panel connectors are inactive.

2.1.3 Attach Antenna

Figure 2.3 - Antenna Attachment Point

Remove the Frontline Sodera™ hardware from the box and attach the antenna to the SMA connector on the front panel.

2.1.4 Applying Power

The Sodera hardware is powered by three methods: the Frontline supplied AC-to-DC adapter, an external DC power source that can include power from an automobile auxiliary power source and an optional internal battery.

To apply power to Sodera use one of the three methods:

1. Connect the provided AC-to-DC power adapter to the **+12VDC** connector on the rear panel and then connect the adapter into an AC source.
2. Connect a DC power source supplying +12 VDC directly to the **+12VDC** connector on the rear panel.
3. Install the battery.

To start Sodera , depress the Power button on the front panel for at least 1/2 second and then release . This action will provide a clean start for Sodera hardware. The battery charge state indicator LEDs will repeatedly flash in sequence while the unit powers up.

The front panel **Power** indicator LED will be green.

Should the front panel **Power** indicator begin blinking red, the Sodera hardware is approaching thermal overload temperature between 50 °C and 60 °C (122 °F and 140 °F) and should be shut down. When the hardware reaches thermal overload it will automatically shut down and the **Power** indicator will be a constant red.

2.1.5 Battery Power

Frontline Sodera™ has an internal battery power option that allows the user to extend the range of the analyzer to include locations without easy access to external power sources. The battery installation is not necessary to operate Sodera with an external AC or DC power source.

The battery is an intelligent lithium rechargeable battery. Frontline Sodera hardware will operate solely on battery power for at least one hour. The battery is charged with an external charging unit or can be charged when installed provided Sodera is connected to an external power source.

2.1.5.1 Battery Install

Turn off power and disconnect the external power source.

Figure 2.4 - Sodera Battery Compartment with Cover Opened

To change or install a battery, start by opening the battery compartment by turning the fastener counterclockwise. The cover is held in place by two tabs on the side opposite the fastener. Slide the cover towards the rear connector panel.

Figure 2.5 - Sodera Battery Removal Using the Tab

If changing the battery, remove the battery from the compartment by lifting on the tab attached to the battery and carefully lifting it upwards until free of the contacts.

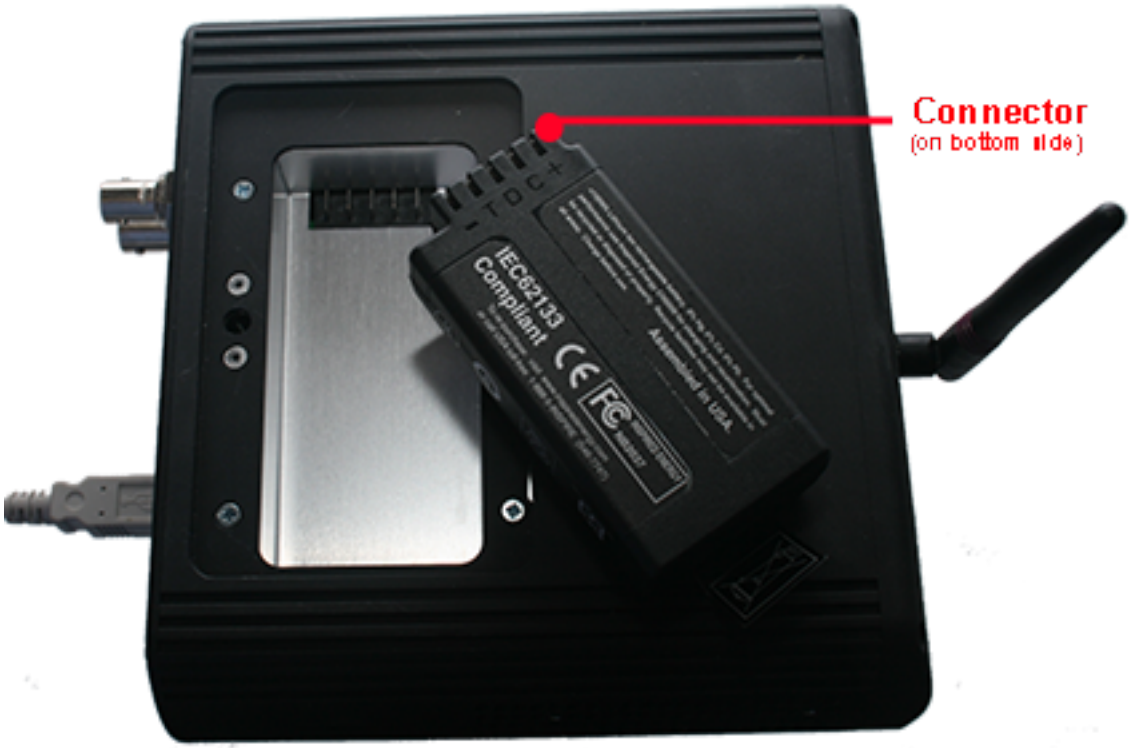


Figure 2.6 - Sodera Battery Connectors, bottom side shown.

To install the battery, position the battery connectors over the connecters in the Sodera battery compartment. Gently press down until the battery makes firm contact.

Figure 2.7 - Sodera Battery: Press to Make Contact

Insert the battery cover tabs in the slots towards the Sodera front panel. Lower the cover and use a screw driver to turn the fastener clockwise until it is firmly engaged.

Figure 2.8 - Sodera Battery Cover: Insert Tabs

Sodera Battery Cover, turn clockwise to secure

After installing the battery, apply power to the Sodera and power it up. Check the battery charge on the front panel **Battery Charge** LEDs. If a charge is necessary, keep the Sodera connected to an external power source until the battery is fully charged.

> **Note:** When using the Sodera in Excursion mode and powered by the battery, it is recommended to have a fully charged battery before beginning data capture.

2.1.6 Connecting for ProbeSync™

ProbeSync allows a Frontline Sodera unit and a 802.11 hardware to be connected together to run off of a common clock, ensuring precise timestamp synchronization while capturing *Bluetooth* and WiFi technologies.. One device will act as the *master* device by providing the clock to the *slave* device receiving the clock. The devices are connected in a daisy-chain configuration. The Sodera unit must be the *master* device. Refer to the following tables, to Rear Panel Connectors on page 5, and to the 802.11 rear panel image below.

Table 2.3 - Sodera Synced to 802.11

Sodera	802.11	Sodera		802.11	
		PROBESYNC OUT	PROBESYNC IN	OUT	IN
Master	Slave	X			X

Using a CAT 5 Ethernet cable, less than 1.5 meters (4.9 feet), insert one end into the master device connector. Insert the other end into the slave device connector.

Each master/slave device will have a separate datasource window open. The *Bluetooth* and WiFi packets can be viewed in the Coexistence View for either datasource.

Figure 2.9 - ComProbe 802.11 Back Panel

2.1.7 Connecting for HCI/WCI-2 & Logic Capture

To capture UART data at the *Bluetooth* Host Controller processor interface using a wired connection:

> **Note:** SPI and SDIO capture is currently not available.

- Connect an HCI Pod to the bottom of the Sodera unit in **POD 1** or **POD 2**.

Figure 2.10 - HCI Pods Installed on Sodera

- Attach the HCI Flying Lead assembly to the end of the HCI Pod. The connector is keyed to ensure proper installation.

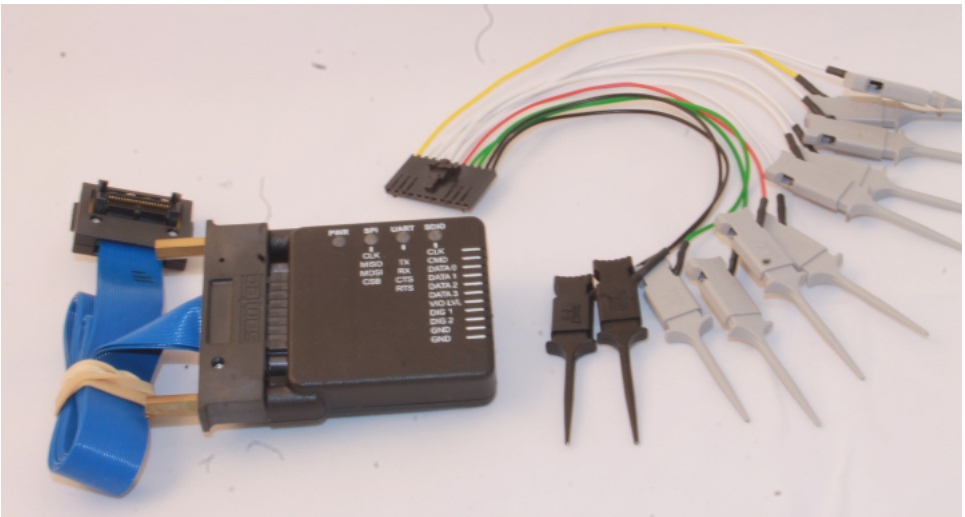


Figure 2.11 - HCI Pod with Flying Lead Assembly

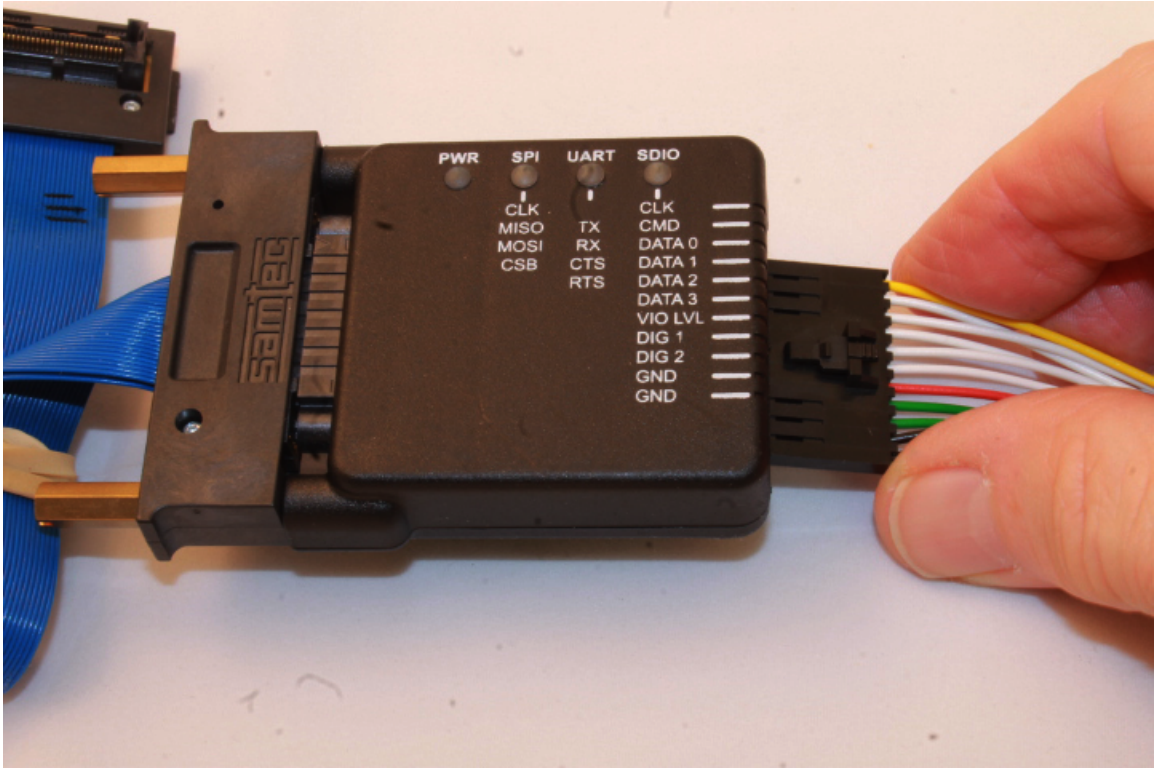


Figure 2.12 - Installing the Flying Lead Assembly on the HCI Pod

- Attach an appropriate Flying Lead Assembly micro-clip to the *Bluetooth* HCI signal test point in accordance with the following table.

Table 2.4 - Sodera HCI Interface Pins

Transport Layer			Pin	Wire Color
SPI	**UART**	**SDIO**		
CLK		**CLK**	1	Yellow
MISO	**TX**	**CMD**	2	White
MOSI	**RX**	**DATA 0**	3	White
CSB	**CTS**	**DATA 1**	4	White
	RTS	**DATA 2**	5	White
		DATA 3	6	White
	VIO LVL	**VIO LVL**	7	Red
		DIG 1	8	Green
		DIG 2	9	Green
	GND	**GND**	10	Black
	GND	**GND**	11	Black

- To remove the Flying Lead Assembly from the HCI Pod, depress the release key on the Flying Lead Assembly.

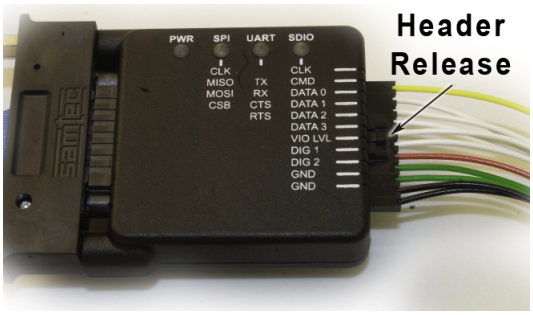


Figure 2.13 - Flying Lead Assembly Header Release

UART Capture Configuration

Successful HCI UART capture requires the following Pod connections.

Table 2.5 - Required UART Layer Connections

Signal Name	Pin	Wire Color	Comment
TX	2	White	Connect to the Device Under Test (DUT) TX pin.
RX	3	White	Connect to the DUT RX pin.
VIO LVL	7	Red	I/O voltage reference that designates the threshold for a logic level "1".. The VIO LVL minimum voltage is 1.65 Vdc. The supplied voltage needs to be the DUT logic signal level that designates a logic level "1". Some DUTs will have a VIO signal/tap. If a VIO tap is not available, use the DUT rail/power supply (Vcc/Vdd). If an I/O reference tap is a available, use that as the VIO LVL source.
GND	10	Black	Either one of these pins can be used to connect the DUT ground to the HCI pod.
GND	11	Black	

2.1.8 Connecting for USB Capture

The HCI USB connectors are located on the Sodera rear panel connectors (see Rear Panel Connectors on page 5). USB testing is normally performed by capturing the USB traffic between a USB device and a host computer or controlling device. In the image below we see the normal configuration of a *Bluetooth* dongle connected to the USB port of a laptop computer. To capture the USB traffic, the Sodera unit is placed between the dongle and laptop computer. Any traffic between the devices is captured through the Sodera HCI interface.

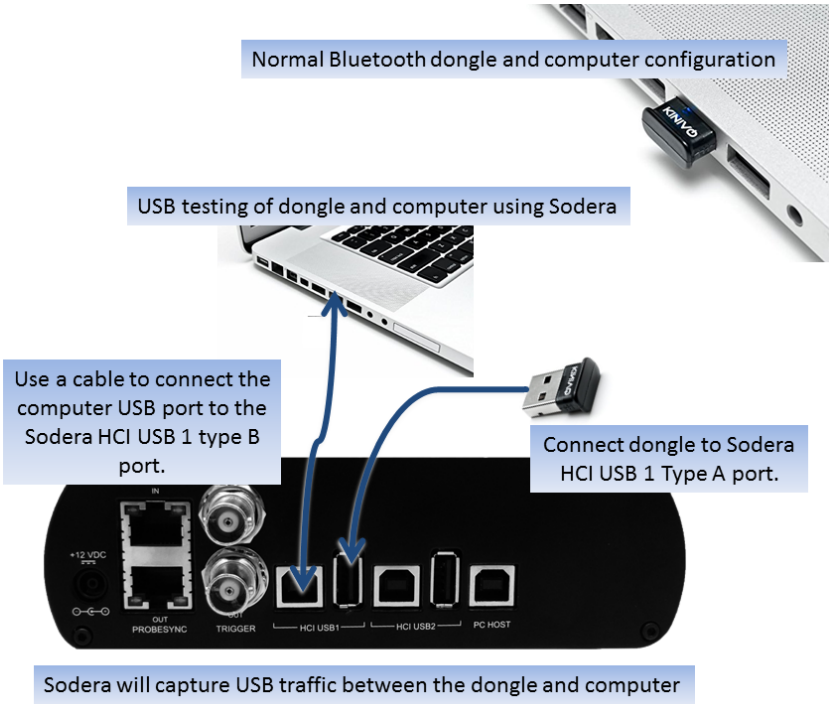


Figure 2.14 - Example: Sodera HCI USB Capture Setup

The HCI USB 1 connectors use the same Sodera unit internal interface as the Sodera HCI POD1 UART pins. Likewise the HCI USB 2 connectors use the same internal interface as the Sodera HCI POD2 UART pins. Therefore you cannot simultaneously capture USB and UART on the "1" interface or on the "2" interface. You can simultaneously capture from the HCI USB 1 connectors and the HCI POD2 UART pins and vice versa. Refer to Menu on page 33.

2.2 Data Capture Methods

This section describes how to load TELEDYNE LECROY Frontline Protocol Analysis System software, and how to select the data capture method for your specific application.

2.2.1 Opening Data Capture Method

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

1. Double-click the " Frontline <*version #*>" desktop folder

This opens a standard Windows file folder window.

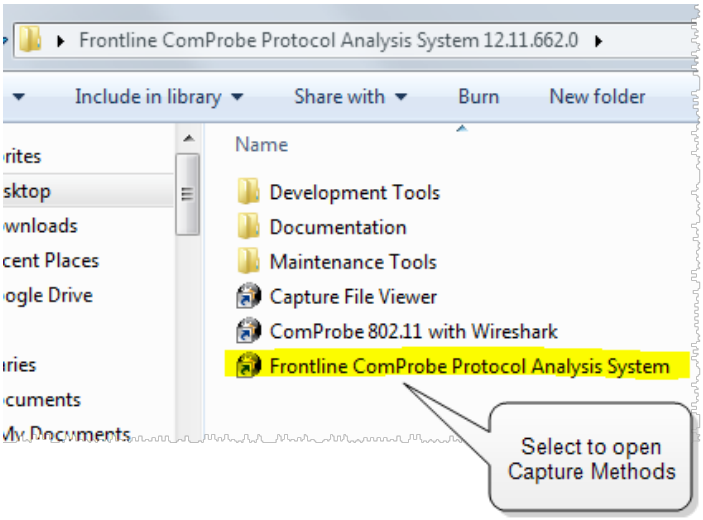


Figure 2.15 - Desktop Folder Link

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 (Version #) > Frontline ComProbe Protocol Analysis System

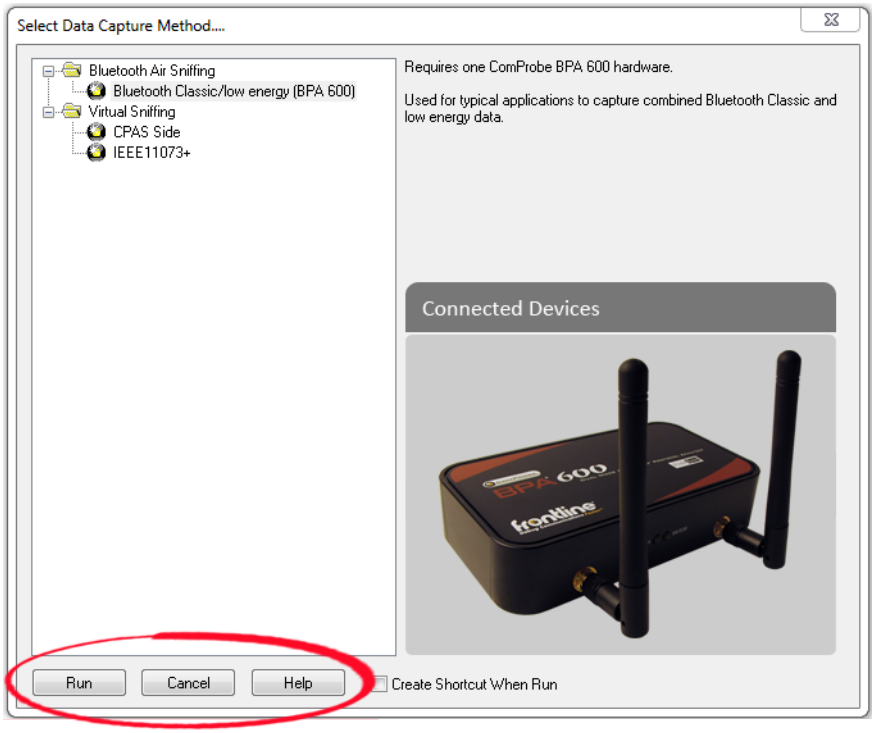


Figure 2.16 - Example: Select Data Capture Method..., BPA 600

Three buttons appear at the bottom of the dialog; **Run**, **Cancel**, and **Help**.

Select Data Capture Method dialog buttons

Button	Description
Run	Becomes active when a capture method is selected. Starts the selected capture method.
Cancel	Closes the dialog and exits the user back to the computer desktop.
Help	Opens Frontline Help. Keyboard shortcut: F1.

3. Expand the folder and select the data capture method that matches your configuration.
4. Click on the Run button and the Frontline Control Window will open configured 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 un-checked 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 <*version #*>directory contains supporting documentation for development (Automation, DecoderScript™, application notes), user documentation (Quick Start Guides and the Frontline User Manual), and maintenance tools.

2.2.2 Sodera Data Capture Method

When the Frontline Sodera is connected to the Host PC running Frontline Protocol Analysis System software the **Select Data Capture Method...** window will display the Sodera options.

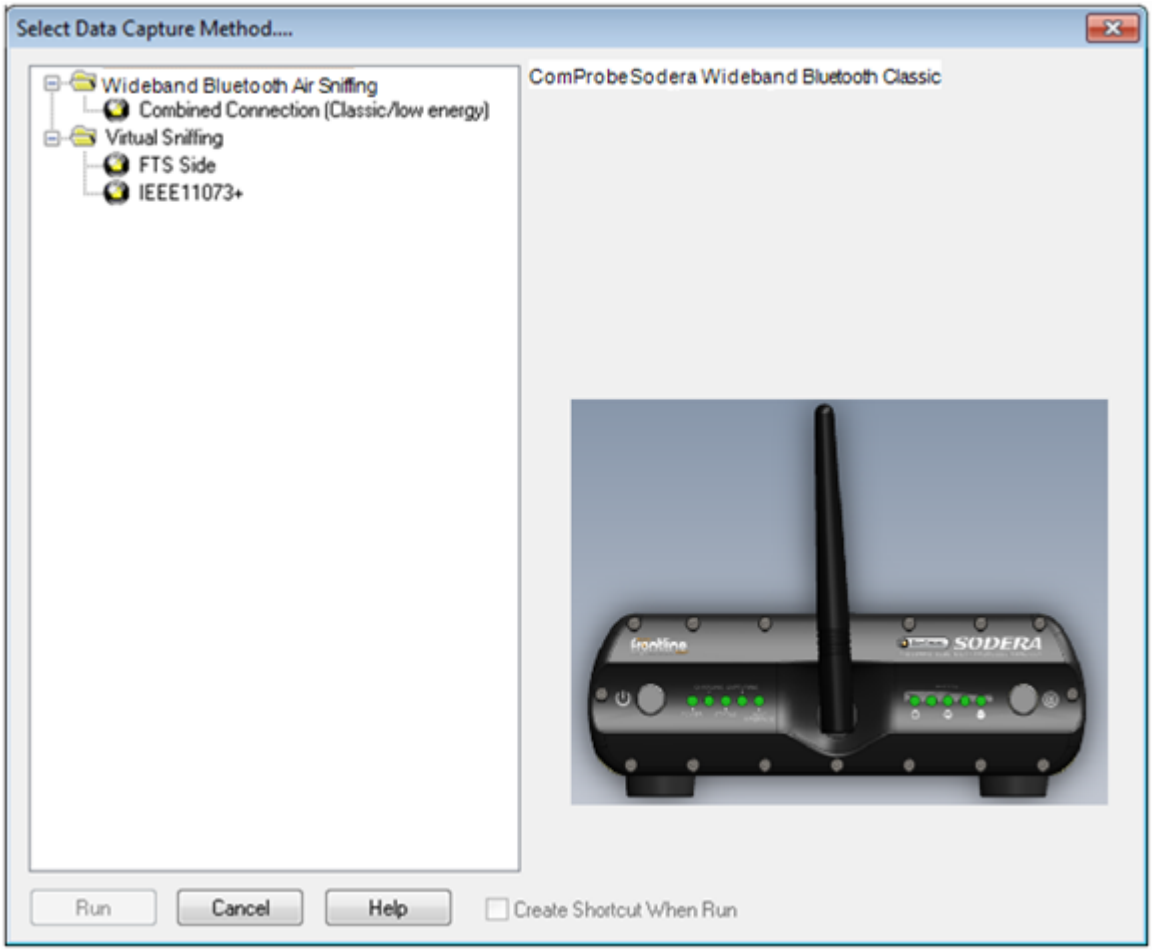


Figure 2.17 - Sodera Data Capture Method

Select **Wideband *Bluetooth*, *Bluetooth* Classic/low energy (Frontline Sodera)**

Click on **Run**. The Frontline software will display the Sodera **Control** window.

2.2.3 Frontline ProbeSync™ for Coexistence and Multiple Frontline Device Capture

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

- Classic and low energy *Bluetooth* sniffing, and 802.11
- ProbeSync configurations include
  - One Sodera unit and an 802.11 unit
  - Two Sodera units

Refer to the Frontline product for specific information on using ProbeSync.

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 **Select Data Capture**

Method window. The Control window provides access to each Frontline 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.

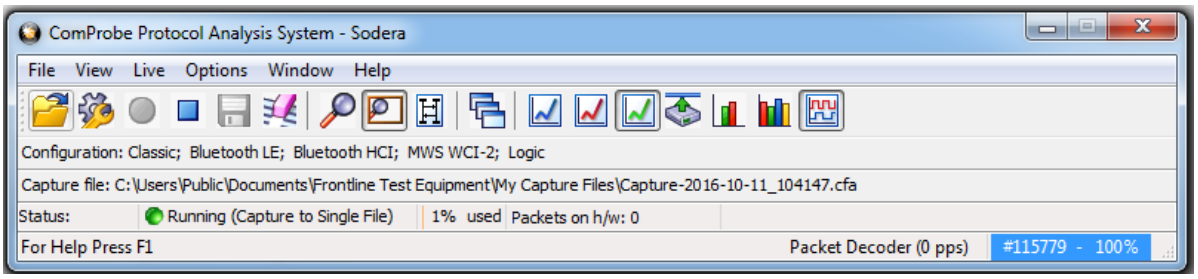


Figure 2.18 - Control Window

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

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

2.3.1 Control Window Toolbar

Toolbar icon displays vary according to operating mode and/or data displayed. Available icons appear in color, while unavailable icons are not visible. Grayed-out icons are available for the Frontline 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.

Table 2.6 - Control Window Toolbar Icons

Icon	Description
	Open File - Opens a capture file.
	I/O Settings - Opens settings
	Start Analyze - data is being decoded from selected wireless devices. Performs the same function as setting the Sodera datasource **Capture Toolbar Analyze/Analyzing** button to **Analyzing**. Changing the **Analyze/Analyzing** button will change the state of this button.
	Stop Analyze- stops decoding data from selected wireless devices. Performs the same function as setting the Sodera datasource **Capture Toolbar Analyze/Analyzing** button to **Analyze**. Changing the **Analyze/Analyzing** button will change the state of this button.
	Save - Saves the capture file.
	Clear - Clears or saves the capture file.

Table 2.6 - Control Window Toolbar Icons (continued)

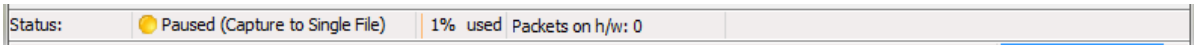
Icon	Description
	Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.
	Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.
	Notes - Opens the Notes dialog.
	Cascade - Arranges windows in a cascaded display.
	Bluetooth Packet Timeline - Opens the Packet Timeline dialog.
	Low energy - Opens the low energy Timeline dialog.
	Extract Data/Audio - Opens the Extract Data/Audio dialog.
	MSC Chart - Opens the Message Sequence Chart
	Bluetooth low energy Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.
	Bluetooth Classic Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.
	Logic Analyzer - Opens the logic analyzer used for logic signal and packet timing analysis.
	Protocol Expert System - Opens *Bluetooth* Protocol Expert System window
	Audio Expert System - Opens Audio Expert System window

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.



- Status displays Not Active, Paused or Running and refers to the state of data analysis.
  - 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 Control Window Menus

The menus appearing on the **Control** window vary depending on whether the data is being captured live or whether you are looking at a .cfa file. The following tables describe each menu.

Table 2.7 - Control Window **File** Menu Selections

Mode	Selection	Hot Key	Description
Live	**Close**		Closes Live mode.

Table 2.7 - Control Window File Menu Selections (continued)

Mode	Selection	Hot Key	Description
Capture File	**Go Live**		Returns to Live mode
	Reframe		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. See Reframing on page 109
	Unframe		Removes start-of-frame and end-of-frame markers from your data. SeeUnframing on page 109
	Recreate Companion File		This option is available when you are working with decoders. If you change a decoder while working with data, you can 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		The plug-ins are reset and received frames are decoded again.
Live & Capture File	**Open Capture File**	Ctrl--O	Opens a Windows Open file dialog. at the default location "...\Public Documents\Frontline Test Equipment\My Capture Files\". Capture files have a .cfa extension.
	Save	Ctrl-S	Saves the current capture or capture file. Opens a Windows Save As dialog at the default location "...\Public Documents\Frontline Test Equipment\My Capture Files\".
	Exit ComProbe Protocol Analysis System		Shuts down the ComProbe Protocol Analysis System and all open system windows.
	Recent capture files		A list of recently opened capture files will appear.

The **View** menu selections will vary depending on the Frontline analyzer in use.

Table 2.8 - Control Window **View** Menu Selections

Mode	Selection	Hot key	Description
Live & Capture File	**Event Display**	Ctrl-Shift-E	Opens the Event Display window for analyzing byte level data.
	Frame Display	Ctrl-Shift-M	Opens the Frame Display window for analyzing protocol level data
	Bluetooth Timeline		Opens the Bluetooth Timeline window for analyzing protocol level data in a packet chronological format and in packet throughput graph.
	Coexistence View		Opens the Coexistence View window that can simultaneously display Classic *Bluetooth*, *Bluetooth* low energy, and 802.11 packets and thourghput.
	Bluetooth low energy Timeline		Opens the Bluetooth low energy Timeline window for analyzing protocol level data in a packet chronological format and in packet throughput graph.
	Extract Data Audio...		Opens the Data/Audio Extraction dialog for pulling data from decoded *Bluetooth* protocols.
	Bluetooth low energy Packet Error Rate Statistics		Opens the *Bluetooth* low energy PER Stats window to show a dynamic graphical representation of the error rate for each low energy channel.
	Classic Bluetooth Packet Error Rate Statistics		Opens the Classic *Bluetooth* PER Stats window to show a dynamic graphical representation of the error rate for each channel.
	Bluetooth Protocol Expert		Opens the Bluetooth Protocol Expert System window to assist in the analysis of Bluetooth protocol issues.
	Audio Expert System		Opens the Audio Expert System window for the purpose of detecting and reporting audio impairments.

Table 2.9 - Control Window **Edit** Menu Selections

Mode	Selection	Hot-key	Description
Capture File	**Notes**	Ctrl-Shift-O	Opens the Notes window that allows the user to add comments to a capture file.

Table 2.10 - Control Window **Live** Menu Selections

Mode	Selection	Hot-Key	Description
The following two rows apply only to Sodera			

Table 2.10 - Control Window Live Menu Selections (continued)

Mode	Selection	Hot-Key	Description
Live	**Start Analyze**	Shift-F5	Data is being decoded from selected wireless devices. Performs the same function as setting the Sodera datasource Capture Toolbar **Analyze/Analyzing** button to **Analyzing**.
	Stop Analyze	F10	Stops decoding data from selected wireless devices. Performs the same function as setting the Sodera datasource Capture Toolbar **Analyze/Analyzing** button to **Analyze**. .
The following rows apply to all Frontline products			
Live	Clear	Shift-F10	Clears or saves the capture file.

Table 2.10 - Control Window Live Menu Selections (continued)

Mode	Selection	Hot-Key	Description
Live & Capture File	**Hardware Settings**		0 - Classic 1 - *Bluetooth* low energy
	I/O Settings		0 - Classic 1 - *Bluetooth* low energy
	System Settings	Alt-Enter	Opens the System Settings dialog for configuring capture files.
	Directories...		Opens the File Locations dialog where the user can change the default file locations.
	Check for New Releases at Startup		When this selection is enabled, the program automatically checks for the latest Frontline protocol analyzer software releases.
	Side Names...		Opens the Side Names dialog used to customize the names of the slave and master wireless devices.
	Protocol Stack...		Opens the Select a Stack dialog where the user defines the protocol stack they want the analyzer to use when decoding frames.
	Set Initial Decoder Parameters...		Opens the Set Initial Decoder Parameters window. There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in templates for later use.Each entry in the window takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. This selection is not present if no decoder is loaded that supports this feature.
	Set Subsequent Decoder Parameters...		Opens the Set Subsequent Decoder Parameters dialog where the user can override an existing parameter at any frame in the capture. Each entry takes effect from the specified frame onward or until redefined in this dialog on a later frame. This selection is not present if no decoder is loaded that supports this feature.
	Automatically Request Missing Decoder Information		When checked, this selection opens a dialog that asking for missing frame information. When unchecked, the analyzer decodes each frame until it cannot go further and it stops decoding. This selection is not present if no decoder is loaded that supports this feature.
	Enable/Disable Bluetooth Protocol Expert		When enabled, the Bluetooth Protocol Expert is active, otherwise it is not available. Only available when a Bluetooth Protocol Expert licensed device is connected.

Table 2.10 - Control Window Live Menu Selections (continued)

Mode	Selection	Hot-Key	Description
	Enable/Disable Audio Expert System		When enabled, the Audio Expert System is active, other wise it is not available. Only available when an Audio Expert System licensed device is connected.

The **Windows** menu selection applies only to the **Control** window and open analysis windows: **Frame Display**, **Event Display**, **Message Sequence Chart**, **Bluetooth Timeline**, **Bluetooth low energy Timeline**, and **Coexistence View**. All other windows, such as the datasource, are not affected by these selections.

Table 2.11 - Control Window **Windows** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Cascade**	Ctrl-W	Arranges open analysis windows in a cascaded view with window captions visible.
	Close All Views		Closes Open analysis windows.
	Minimize Control Minimizes All		When checked, minimizing the Control window also minimizes all open analysis windows.
	Frame Display and **Event Display**		When these windows are open the menu will display these selections. Clicking on the selection will bring that window to the front.

Table 2.12 - Control Window **Help** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Help Topics**		Opens the Frontline Help window.
	About Frontline Protocol Analysis System		Provides a pop-up showing the version and release information, Frontline contact information, and copyright information.
	Support on the Web		Opens a browser to fte.com technical support page.

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 the Frontline software is used to configure an analyzer for capturing data .

3.1 Sodera™ Configuration and I/O

3.1.1 User Configuration Overview

Frontline® Sodera™ is capable of simultaneously capturing and demodulating all RF channels and packet types defined in all *Bluetooth* specification versions up to and including 4.2. The user is not required to specify the addresses of the devices to be captured or their roles (master or slave) during the connection lifetime. Prior to capturing data the user does not need to enter any information (PIN, OOB, long term key, link key) used to encrypt or decrypt data. Sodera provides live simultaneous capture of all 79 Classic *Bluetooth* channels and 40 *Bluetooth* low energy channels storing data for both live and post-capture analysis.

Sodera™ uses a two-stage capture-analysis process. First, **Record** will activate the Sodera™ datasource to begin capturing data from all *Bluetooth* devices in range. In the **Analyze** stage, the user selects one or more wireless or wired devices for analysis and Sodera™ will begin sending captured data that is to/from those devices to the Frontline analysis software. The data appears in the **Frame Display**, **Message Sequence Chart**, **Coexistence View**, ***Bluetooth* Timeline**, **low energy *Bluetooth* Timeline**, **PER Stats**, **Event Display** etc.

If any keys needed for decryption are known from past captures those keys are automatically applied to the devices under test. Prior to protocol analysis the user can enter any unknown keys. Sodera will identify the specific key necessary for data decryption, for example Link Key, Passkey, PIN, Temporary Key.

3.1.1.1 Standard Capture Scenario

In the standard capture scenario, Sodera™ is connected to a host computer via the rear panel **PC HOST** interface and captures live “over the air” data exchanged between two *Bluetooth* devices.

3.1.1.2 Coexistence Capture Scenario

Coexistence capture scenario is an extension of the standard capture scenario with the addition of a Frontline 802.11 Wi-Fi analyzer through the use of ProbeSync™ technology. Frontline Sodera operates in conjunction with Frontline 802.11 to capture transmissions from their respective technologies. ProbeSync™ synchronizes the Frontline hardware clocks to ensure that the captured data timestamping is synchronized for analysis on

the host computer. ProbeSync™ connection are available on the rear panel **PROBESYNC IN/OUT** connectors.

During live or post-capture analysis the *Bluetooth* and Wi-Fi may be simultaneously viewed in the Coexistence View accessible from the **Control** window.

3.1.2 Sodera Datasource Window

When the Frontline software is loaded and started on the host computer the Frontline **Control** window and **Frontline Sodera** datasource window will open. The Sodera window provides controls and panes to

- open or save captured data files, change the datasource window layout, and to configure the capture conditions.
- start and stop data recording and analysis and control the piconet display
- display the wireless and wired devices, setup decryption , and log session events.

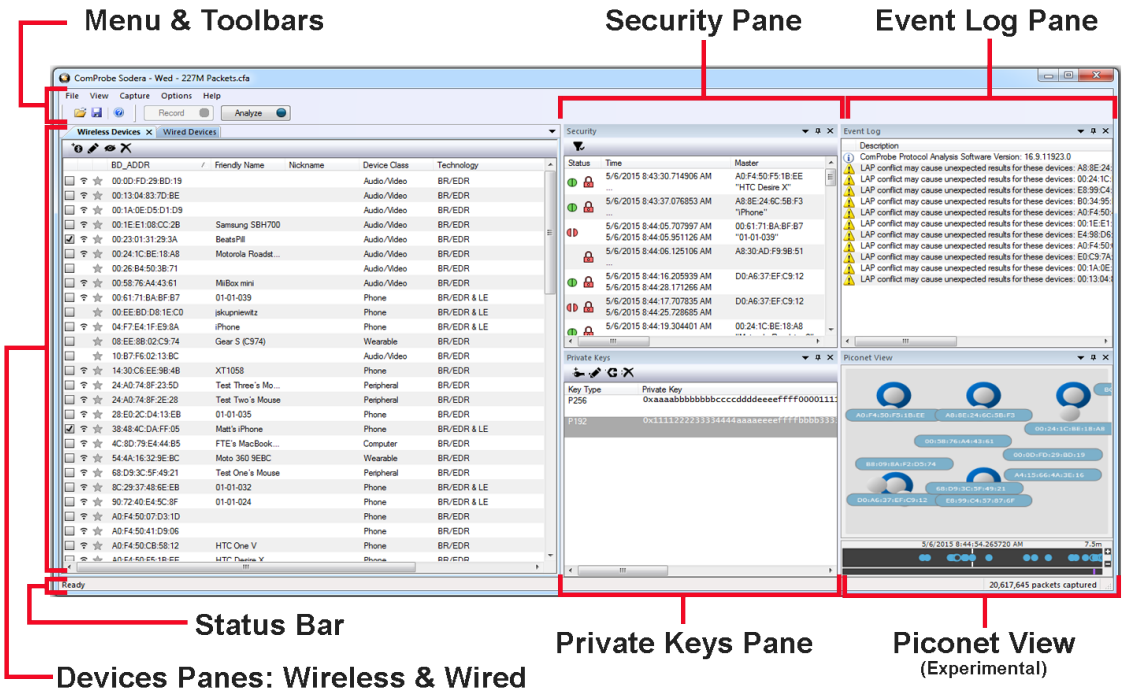


Figure 3.1 - Sodera Window

The Menus and Toolbars provide control of the window's views, starts and stops recording and analysis, sets capture options, and provides file control.

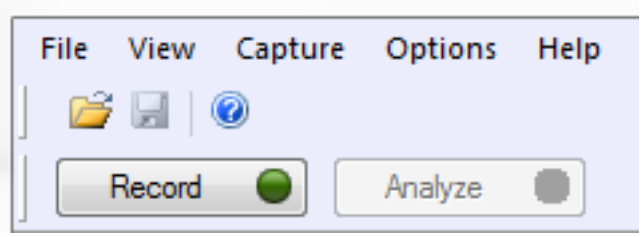
The Devices Pane is always visible and cannot be docked, however if the other panes are docked or not visible the Devices Pane can be expanded to fill the window pane area.

The **Wired Devices**, **Security**, **Private Keys**, **Piconet View**, and **Event Log** Panes can be arranged or collapsed to suit individual preferences. To relocate the pane click on the pane header where the title appears and drag it to a new position. By default the **Piconet View** and **Private Keys** pane are not shown, and must be opened using the **View** menu. When the **Private Keys** pane is shown, it will initially appear as a tab in the **Security** pane. The other open panes will automatically rearrange to suit the user's changes to the layout. These Panes can be configured to **Auto Hide** by clicking on in the pane header or by right-clicking on the pane header to reveal a view option pop-up menu. The pane will collapse and only the header is

visible on one of the window borders. To expand the pane hover the mouse cursor over the hidden pane header and it will expand to its original size and location. Moving the cursor off the header or out of the pane will hide the pane again. If you move the cursor off the header and into the pane the pane will remain unhidden as long as the cursor stays in the pane. To unhide the pane, hover over the pane to expand it and click on ; the pane will remain in its original position and size.

The **Wired Devices**, **Security**, **Private Keys**, **Piconet View**, and **Event Log** Panes can be re-sized by hovering over the pane edge until a double headed arrow appears. Click and hold, dragging it to change the pane size.

3.1.2.1 Menu & Toolbars



At the top of the Sodera window appears the Menu, the Standard Toolbar, and the Capture Toolbar. The Menu is fixed in position and always in view. The Standard Toolbar and Capture Toolbar visibility is optional and is set in the Menu **View** selections. The position of these toolbars can be changed by dragging them, although, the position range is limited to the vicinity of the Menu.

3.1.2.1.1 Menu

The Menu provides the user with the ability to save and open files and to set preferences, change the datasource window layout, and configure the data capture settings.

Table 3.1 - Menu Selections

Option	Selection	Description
File	**Open Capture File (Ctrl-O)**	Opens a Windows Open dialog. Select the location, File name, and .cfa file to analyze. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.
	Save (Ctrl-S)	Opens a Windows Save dialog. Select a file location and name for a recorded and analyzed file. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.
	Manage excursion mode captures...	Record or delete captures from the Sodera hardware that were created using excursion mode. Opens the **Manage excursion mode captures** dialog. This selection is disabled during live capture.
	Exit	Closes Frontline software

Table 3.1 - Menu Selections(continued)

<table>
<tr><th>Option</th><th>Selection</th><th>Description</th></tr>
<tr><td rowspan="8">View</td><td>Toolbars</td><td><table><tr><th>Selection</th><th>Description</th></tr><tr><td>Capture</td><td>When checked the Capture Toolbar is visible. Checked is the default.</td></tr><tr><td>Standard</td><td>When checked the Standard Toolbar is visible. Checked is the default.</td></tr><tr><td>Status</td><td>When checked the Status Bar is visible. Checked is the default.</td></tr></table></td></tr>
<tr><td>Wireless Devices</td><td>When checked the Wireless Devices tab is visible in the Devices pane. Selecting the tab will display the Wireless Devices.</td></tr>
<tr><td>Wired Devices</td><td>When checked the Wired Devices tab is visible in the Devices pane. Selecting the tab will display the Wired Devices connected to POD 1 and POD 2.</td></tr>
<tr><td>Security</td><td>When checked the Security pane is visible. Checked is the default.</td></tr>
<tr><td>Event Log</td><td>When checked the Event Log pane is visible. Checked is the default.</td></tr>
<tr><td>Piconet View (Experimental)</td><td>When checked, the Piconet View is visible. Not-checked is the default.

At this time the Piconet View is experimental and in development.</td></tr>
<tr><td>Private Keys</td><td>When checked, the Private Keys pane is visible. The Private Keys pane displays user entered Private/ Public key pairs for Bluetooth low energy legacy and secure connection pairing. By default, this pane is not displayed. When it is displayed it will be docked as a tab in the same area as the Security pane.

When Debug key is not used during pairing, the datasource will look for a matching Public key in the set of Private/Public key pairs. If a match is found, the datasource will use the corresponding Private Key to compute the Diffe-Hellman Key.</td></tr>
<tr><td rowspan="2">Capture</td><td>Record/Recording</td><td>Starts and stops the capture of data. Performs the same function as the Capture Toolbar Record/Recording button.</td></tr>
<tr><td>Analyze/Analyzing</td><td>Starts and stops the analysis of recorded data. Performs the same function as the Capture Toolbar Analyze/Analyzing button.</td></tr>
</table>

Table 3.1 - Menu Selections(continued)

Option	Selection	Description
Options	**Capture Options...**	Opens the Capture Options dialog where the attached Sodera hardware can be configured for *Bluetooth* technologies and other capture modes. For additional information see Capture Options Dialog on page 38.
	LE Test Mode Filters...	Allows filtering in or out LE Test Mode PDUs and will allow filtering in selective LE Test Mode PDUs by channel number. For additional information see LE Test Mode Channel Selection dialog on page 38.
	Analyze Inquiry Process Packets	When checked will include inquiry packets in the analysis. Inquiry packets are normally ignored, so not-checked is the default.
	Analyze Paging Without Connection	Includes traffic from all failed BR/EDR connection attempts.
	Analyze NULL and POLL packets	When checked will include NULL and POLL packets. NULL and POLL packets are normally ignored, so not-checked is the default.
	Analyze LE Empty Packets	When checked will include *Bluetooth* low energy empty packets. Empty packets are normally ignored, so not-checked is the default.
	Analyze Anonymous/Unknown Adv. Packets	When checked the Frontline software identifies *Bluetooth* low energy anonymous advertising packets. An anonymous advertising packet does not contain the AdvA field and its corresponding auxiliary packet also does not contain an AdvA field. With no address, there is nothing to select for analysis in the **Wireless Devices** pane. The Frontline software groups anonymous packets and this option allows the user to include or exclude those packets for analyzing. If the Frontline system captures either the extended advertising packet or its corresponding auxiliary packet but not both and the AdvA field is not present in the captured packet, the system categorizes the packet as unknown. The default setting is unchecked. Settings are persistent.
Help	**Help Topics**	Opens Frontline help
	About Sodera...	Opens a pop-up window with version and configuration information

Manage excursion mode captures dialog

This dialog provides the user with a means to record or delete captures previously created and saved on the Sodera hardware using excursion mode.

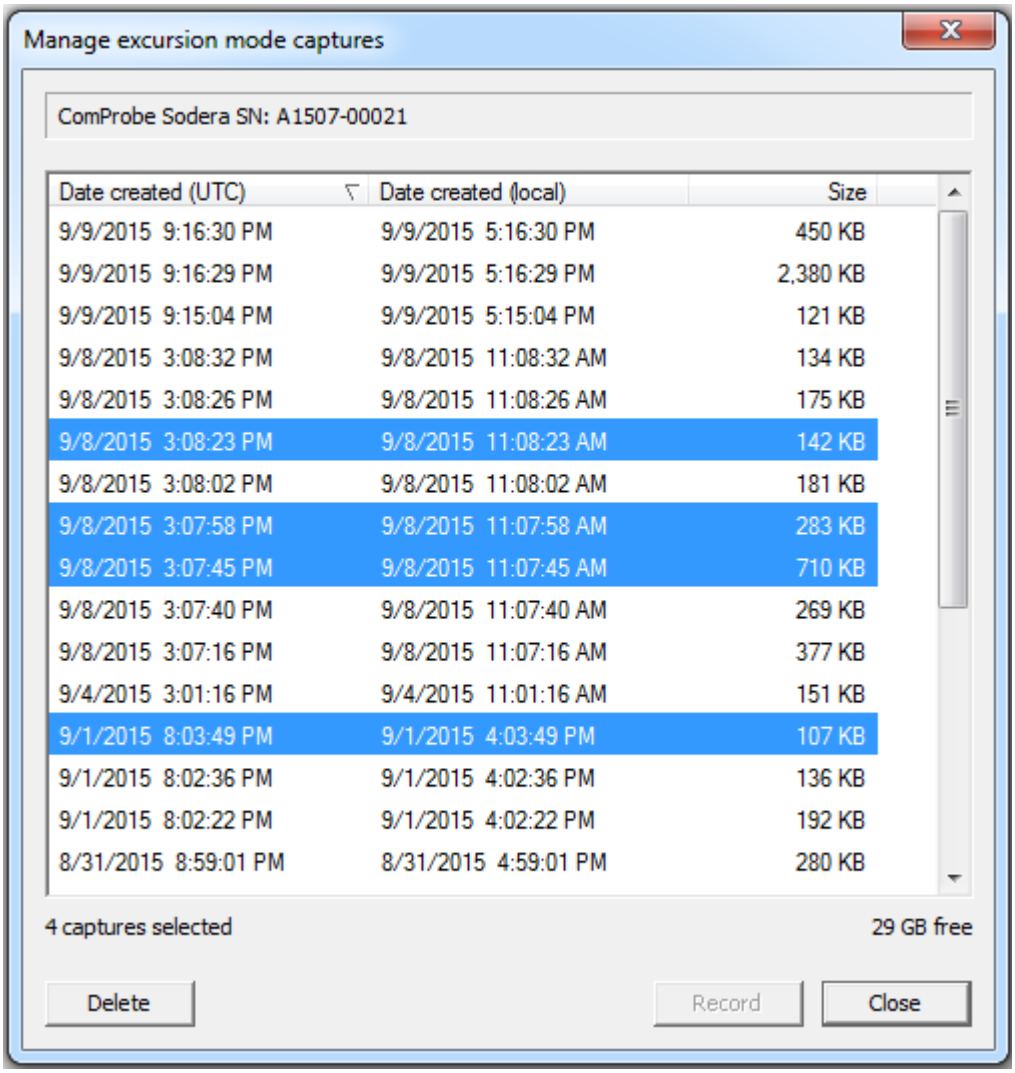


Figure 3.2 - Manage excursion mode captures Dialog

If a Sodera hardware unit is connected to the computer the dialog displays

- The serial number of the Sodera hardware.
- A listing of all Excursion mode capture files stored on the currently connected Sodera hardware. If no files are stored, the list will be empty.

The listed files display the following information.

- **Date Created (UTC)** - the date and time in the UTC time zone that the excursion mode capture was started.
- **Date Created (local)** - The capture's starting date and time in the local time zone of the user's computer.
- **Size** - the size of the excursion mode capture.

Select Excursion mode capture files by

- Click to select a single file.
- Shift-click to select a contiguous range of files starting with the most recently selected file.

- Ctrl-click to select an additional file or non-contiguous file to the selection.
- Select all files by:
  - right-clicking and selecting **Select All Ctrl-A** from the context menu, or.
  - Typing Ctrl-a.

Delete selected files from the connected Sodera hardware by

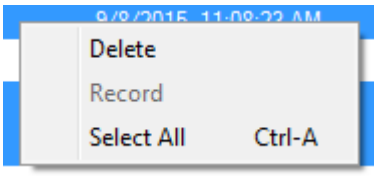
- Pressing the Delete key, or
- Right-clicking and selecting **Delete** from the context menu, or
- Clicking the dialog **Delete** button.

A delete operation will display a confirming dialog that requires the user to confirm the operation before the files are actually deleted. Clicking on **Yes** will permanently delete the files from the connected Sodera hardware. Clicking on **Cancel** will abort the delete operation.

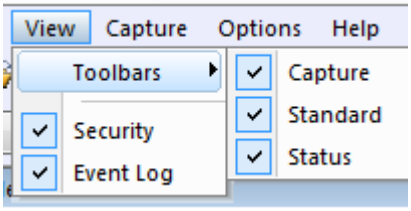
Record - Selecting a single file will enable the **Record** button and the **Record** right-click pop-up menu item. Clicking the **Record** button or menu item will close the dialog and start recording the selected excursion mode capture to the user's computer.

Right-click pop-up menu

Right-clicking on any file will open a pop-up menu with options to **Delete**, **Record**, or **Select All**.

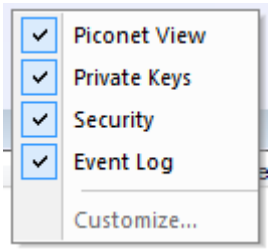


View Menu



The **View** menu offers options to display or hide panes, toolbars, and the status bar to suit the user's preferences.

View Pop-Up Menu

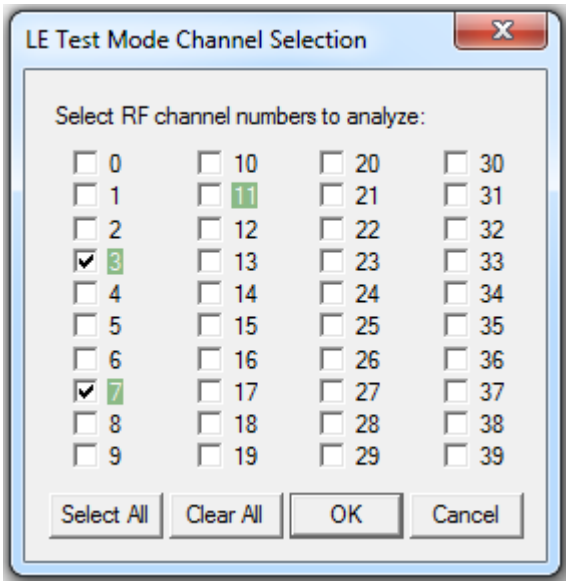


Right-clicking in the toolbar any of the following window/panes will display a pop-up View menu that performs the same as the main View menu:

- Sodera window menu and toolbars area
- **Private Keys** pane toolbar area (lower half of pane header)

The order of the panes shown in the pop-up menu will vary depending on the layout of the user's Sodera Window.

LE Test Mode Channel Selection dialog



In this image , three channels have detected LE Test Mode PDUs and the channels are highlighted: channel 3, 7, and 11. Channels 3 and 7 are checked, so their PDUs are filtered "in" for analysis. Channel 11 has not been checked, so its PDUs are filtered "out" from the analysis.

These channel filter selections are persistent for the current session. Another **Record** action in this same session can be performed and the same channel filter selection will be applied unless changed.

Table 3.2 - LE Test Mode Channel Sellection Buttons

Button	Description
Select All	Selects all 40 low energy channels
Clear All	Deselects all 40 low energy channels
OK	Active once a channels selection is made. When clicked the selected channels are saved for analysis, and the dialog closes.
Cancel	Closes the dialog without saving any changes.

3.1.2.1.1.1 Capture Options Dialog

The Capture Options dialog is used to configure the Sodera unit prior to data capture. The capture options are stored on the Sodera hardware and these setting will persist until changed. The Capture Options dialog is only active when a Sodera unit is connected to the computer running the Frontline software.

> **Note:** if a Sodera hardware unit is not connected then these settings can neither be viewed nor changed.

Wireless tab

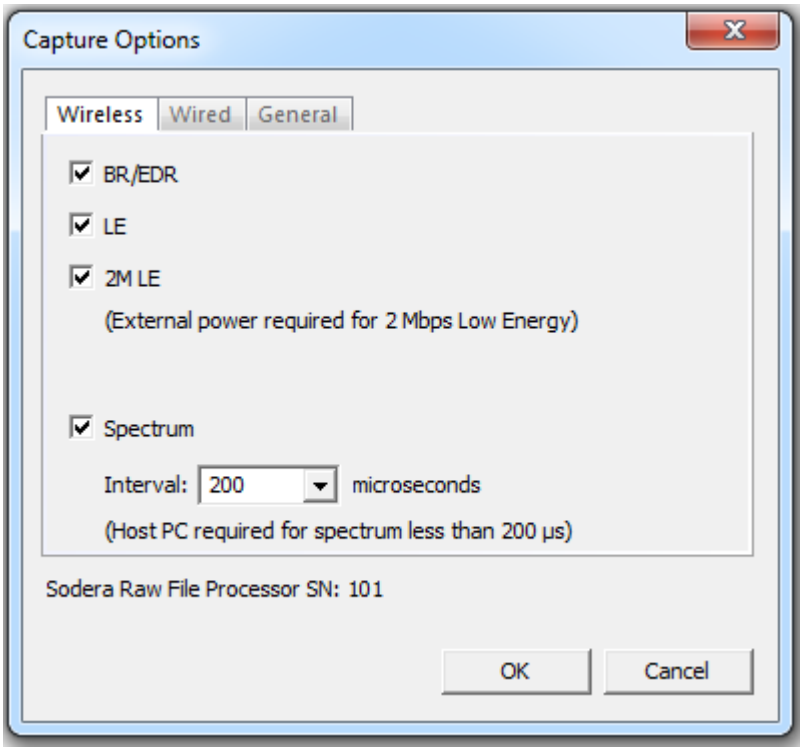


Figure 3.3 - Sodera Capture Options - Wireless tab.

Table 3.3 - Capture Options Wireless Tab Selections

Selection	Description
BR/EDR	When checked, will capture data from Classic *Bluetooth* devices
LE	When checked, will capture data from *Bluetooth* low energy devices.
2M LE	When checked captures *Bluetooth* low energy 2 Mbps data rate. When this option is selected the Sodera unit must be connected to an external power source. Refer to Applying Power on page 7.
Spectrum	When checked, this selection provides the user with the ability to capture samples of the 2.4 GHz RF present at the Sodera antenna. The spectrum data represents the RSSI and it is automatically saved when the capture is saved. It can be optionally viewed in the **Coexistence View**. Spectrum sampling is set at 20, 50, 100, or 200 microsecond intervals. Capturing spectrum data will use additional memory, and the smaller the sample interval, the more memory that is used, So when using sample rates less than 200 microseconds the Sodera unit must be connected to a computer and not being used in Excursion Mode. See Sodera: Spectrum Analysis on page 102 and Coexistence View - Spectrum on page 209 for more information.
Enable Excursion mode captures	When checked the Sodera hardware will support Excursion mode captures where the hardware can capture data without being connected to a computer. The *Bluetooth* traffic is captured for later upload and analysis using a computer running the Frontline Protocol Analysis System software.

Wired tab

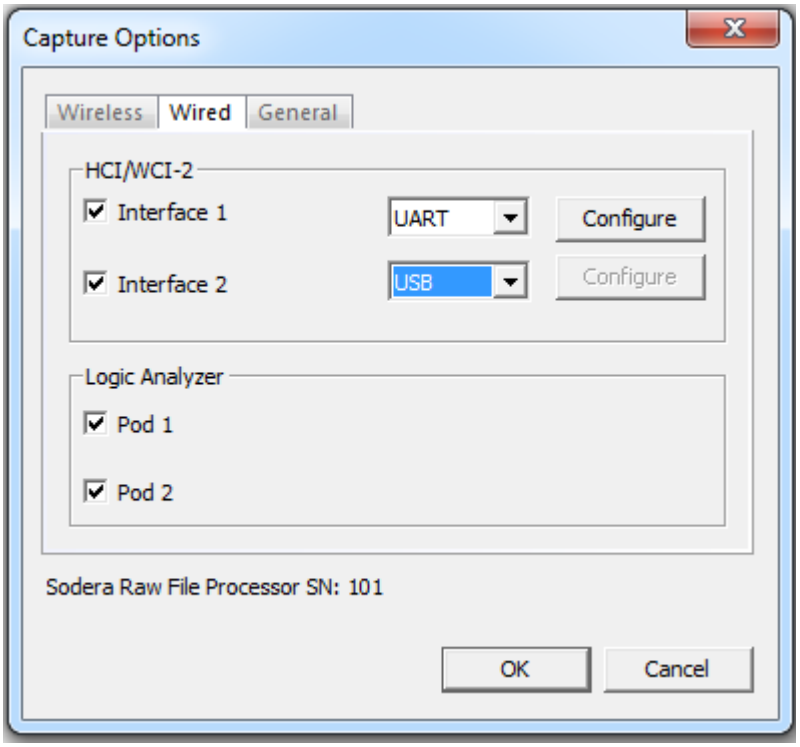


Figure 3.4 - Sodera Capture Options - Wired tab.

Table 3.4 - Capture Options Wired Tab Selections

Section	Selection	Description
HCI/WCI-2	**Interface 1**	Control whether or not HCI traffic on **POD1** will be captured. Available options are: • UART. See UART Capture Configuration on page 17. Click on the **Configure** button to setup the HCI UART capture parameters for **POD 1**. See HCI UART I/O Settings on the facing page. • USB. See Connecting for USB Capture on page 17.
	Interface 2	Control whether or not HCI traffic on **POD2** will be captured. Available options are: • UART. See UART Capture Configuration on page 17. Click on the **Configure** button to setup the HCI UART capture parameters for **POD 1**. See HCI UART I/O Settings on the facing page. • USB. See Connecting for USB Capture on page 17.

HCI UART I/O Settings

After clicking on the **Configure** button, the I/O Settings for UART can be configured without an HCI pod being connected to the Sodera. When you click on the OK button the configuration information is saved, but is not stored on the Sodera hardware.

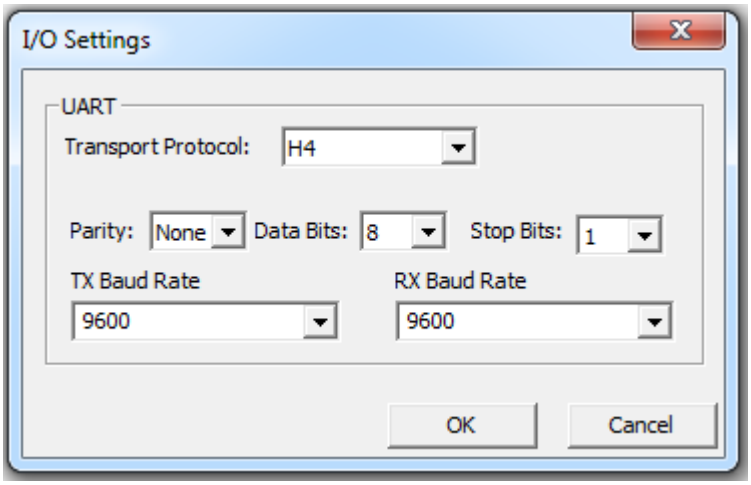


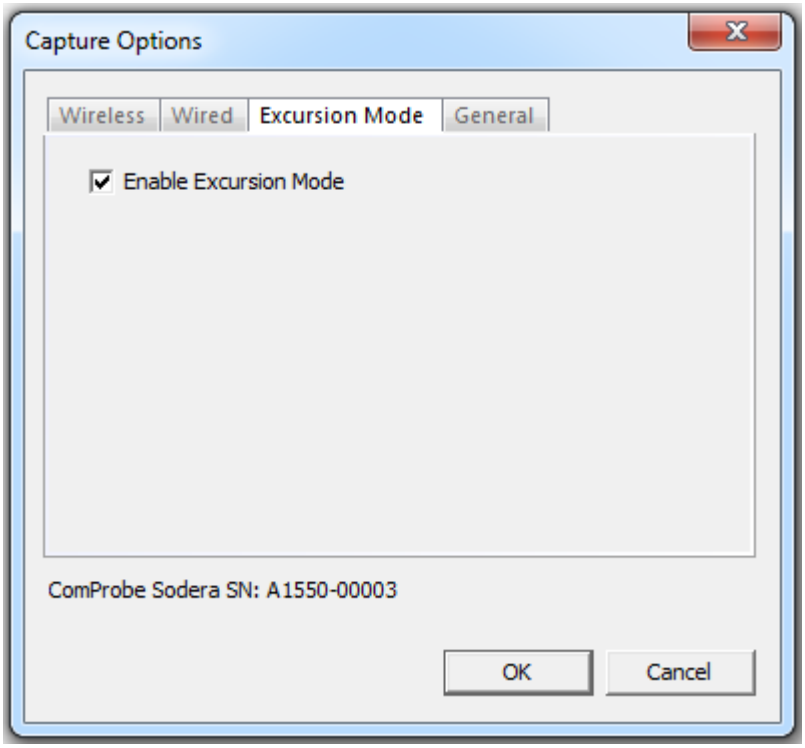
Table 3.5 - HCI I/O Settings for UART

Setting	Value	Description
Transport Protocol	**H4**	The simplest protocol designed to operate over RS-232 with no parity in a 5-wire configuration.
	BCSP	BlueCore Serial Protocol, developed by CSR, provides a more reliable alternative to H4. The protocol is defined to run a 3-wire connection, and can optionally use a 5-wire UART connection with two flow control lines.
	3-Wire (H5)	A 3-wire protocol that provides error detection and correction.
	MWS WCI-2	The Wireless Coexistence Interface (WCI) is a full duplex UART carrying logic signals framed as UART characters.
Parity	**None**	No parity check occurs
	Even	The count of bits set is an even number.
	Odd	The count of bits set is an odd number.
Data Bits	**8**	The number of data bits in the expected packet.
	7	
	6	
	5	
Stop Bits	**1**	The number of data bits held in the mark (logic 1) condition at the end of the expected packet.
	1.5	
	2	

Table 3.5 - HCI I/O Settings for UART (continued)

Setting	Value	Description
TX Baud Rate	**Disabled**	
	9600	
	14400	
	19201	
	28801	
	38402	
	57603	
	115207	
	230414	
	460829	
	925925	
	1000000	
	1250000	
	1515151	
	1754385	
	2000000	
	2272727	
	2500000	
	2777777	
	3030303	
	3333333	
	3571428	
	3846153	
	4000000	
RX Baud Rate		Value selections same as **TX Baud Rate**.

Excursion Mode



Sodera Capture Options - Excursion Mode Tab

Table 3.6 - Capture Options Execution ModeTab Selections

Selection	Description
Enable Execution Mode	When **Enable Excursion Mode** is checked the Sodera hardware will support Excursion mode captures where the hardware can capture data without being connected to a computer. The *Bluetooth* traffic is captured for later upload and analysis using a computer running the Frontline software. Refer to Excursion Mode on page 70 for more information about the Excursion Mode.

General Tab

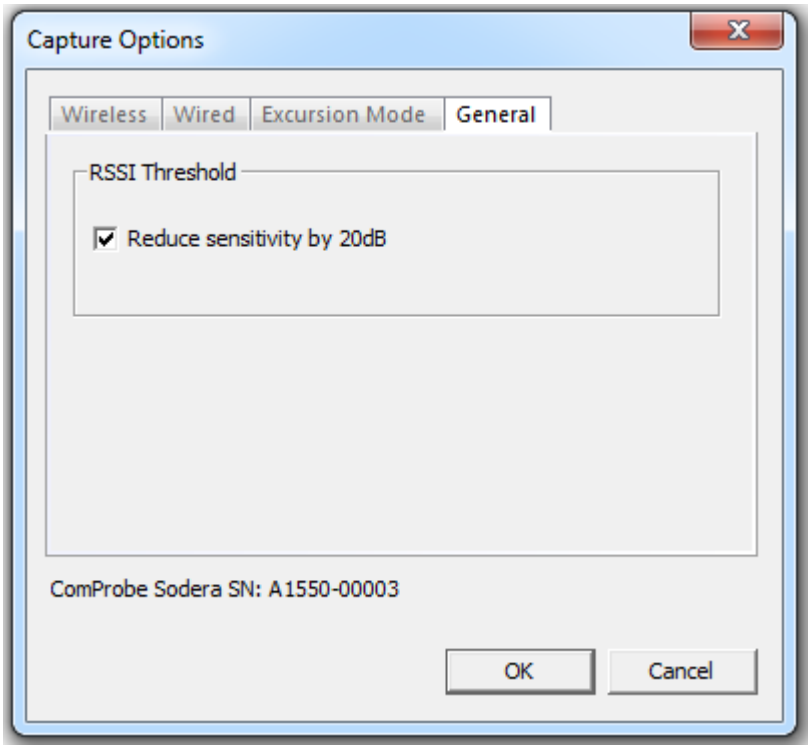


Figure 3.5 - Sodera Capture Options - General Tab

Table 3.7 - Capture Options General Tab Selections

Section	Selection	Description
RSSI Threshold	**Reduce RF Sensitivity (20 dB reduction)**	When checked, Low gain is enabled on the Sodera hardware. The received RF signals are reduced by approximately 20 dB compared to the normal gain setting. For more information, see Sodera Baseband Layer Signal Strength on page 148. When unchecked, normal gain is enabled on the Sodera hardware.

3.1.2.1.2 Standard Toolbar

The Standard Toolbar provides quick one-click access to the same options that appear in menu **File** selection. This toolbar may be hidden by selecting from the menu View Toolbars selection and removing the check from Standard Toolbar selection.

The Standard Toolbar can be positioned to another location by moving the mouse cursor to the left of the menu until a double-headed arrow appears. Click, hold, and drag the menu to another position in the window header.

Table 3.8 - Standard Toolbar Selections

Icon	Description
	Open (Ctrl-O) - Opens a Windows Open dialog. Select the location, File name, and .cfa file to analyze. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.

Table 3.8 - Standard Toolbar Selections(continued)

Icon	Description
	Save (Ctrl-S) - Opens a Windows Save dialog. Select a file location and name for a recorded and analyzed file. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.
	Help Topics - Opens Frontline help, specifically the Sodera Window topic.

3.1.2.1.3 Capture Toolbar

The Frontline Sodera window Capture toolbar provides controls to start and stop data capture, and to start and stop analysis of selected wireless and wired devices.

The toolbar can be hidden by removing the check from **Capture** in the **Toolbars** option of the **View** menu. The toolbar default view is not hidden (checked).

The **Capture Toolbar** can be positioned to another location by moving the mouse cursor to the left of the menu until a double-headed arrow appears. Click, hold, and drag the menu to another position in the window header.

Table 3.9 - Capture Toolbar Buttons

Button	View	Description
Record / Recording	**Record**	When this button view is active Sodera is not capturing data. Clicking this button view will begin data capture from wireless devices within range and wired devices connected to the Sodera unit and the view will change to **Recording**. The default capture is both Classic *Bluetooth* and *Bluetooth* low energy, but if the **Capture Options...** in the **Options** menu settings have been changed from the default the capture session will use those settings. **Note:** The last session **Capture Options...** settings are remembered as the new preferred default settings.
	Recording	When this button view is active Sodera is capturing data. Clicking this button view will stop the data capture process, and the button view will change to **Record**.

Table 3.9 - Capture Toolbar Buttons(continued)

Button	View	Description
Analyze / Analyzing	**Analyze**	This button is grayed-out until a filter is set. When this button view is active Frontline software is not analyzing captured data. Clicking this button will begin protocol analysis, and the button will change to **Analyzing**. This button can be clicked while actively capturing data. Clicking this button view will disable any further filter selection.
	Analyzing	When this button view is active Frontline software is analyzing captured data. The protocol analysis can be on while actively **Recording** data. Clicking in this button will stop the protocol analysis, and the button view will change to **Analyze**.

Filter Selection

The **Analyze** button is available when a filter has been selected. Filters are selected in two ways:

1. Selecting devices in the **Wireless Devices** or **Wired Devices** pane.
2. Enabling inquiry packets by selecting **Analyze Inquiry Process Packets** in the **Options** menu.

3.1.2.2 Wireless Devices Pane

The Sodera Wireless Devices pane provides the user with information on active, inactive, and previously detected *Bluetooth* devices within range of the Sodera wide band receiver. In performing analysis the user will filter the captured data by selecting which devices the Frontline software will use.

The **Wireless Devices** pane is a list populated by wireless devices that are:

- active,
- remembered from previous sessions, or
- added by the user.

A new device/BD_ADDR is automatically added to the Device Pane when:

- For BR/EDR, the full BD_ADDR encapsulated in the **FHS Packet**[1] is added to the **Wireless Devices** pane when Sodera captures an FHS packet that is successfully dewhitened with the CRC checked.
- A partial BD_ADDR—just the Lower Address Part (LAP) and Upper Address Part (UAP)—may be added when we do not observe paging such as when a conversation is already ongoing at the time capturing is started. If Sodera is able to successfully dewhiten a BR/EDR packet using the payload CRC to check repeated dewhitening attempts, then the partial BD_ADDR will be added.
- For Bluetooth low energy, the full BD_ADDR is always displayed.

Added devices are retained by the Frontline software. When devices are added and appear in the **Wireless Devices** pane they must be removed by the user or, in the case of a subsequent session, the devices will appear again. If not used in the current session the devices will be inactive, otherwise it will be active.

[1]The FHS packet is a special control packet containing, among other things, the Bluetooth device address and the clock of the sender. The payload contains 144 information bits plus a 16-bit CRC code.

Retaining past added devices allows the user to select devices prior to starting a session with the **Record** button.

When using a .capture file, e.g. using the Viewer, the set of devices shown will only be the devices in that capture file. Any device changes made can be saved to that file, but do not affect the “live capture” database of devices.

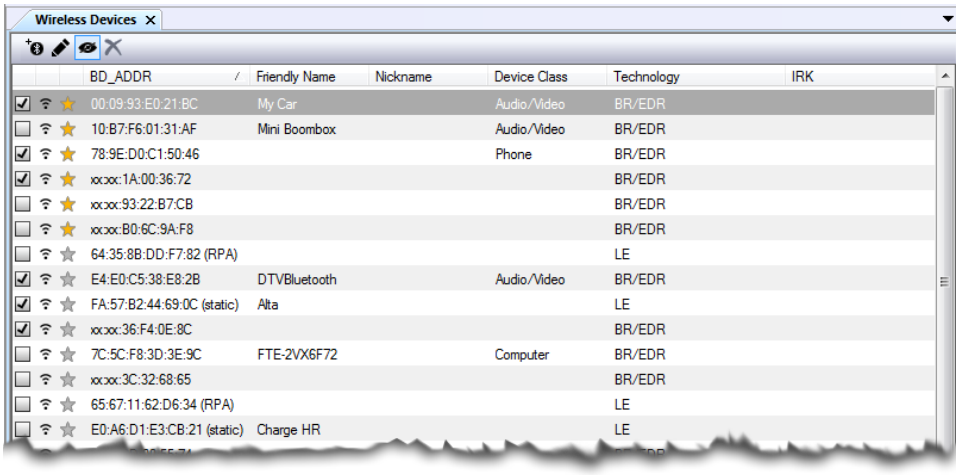


Figure 3.6 - Sodera Wireless Devices Pane

Table 3.10 - Wireless Devices Pane Columns

Column	Description
Filter Selection ☐/☑	The filter is an on/off selection . When checked , the device is selected for data analysis, that is the data is filtered into the Frontline protocol analyzer when the Standard Toolbar **Analyze** button is clicked.
Traffic Captured	If the a "traffic captured" icon is present traffic has been captured that involves the device. If the icon is not present then Sodera has not captured any traffic that involves that device. Only wireless devices with traffic captured can be used for Frontline protocol analysis.
Favorites ☆/★	When a star is activated by clicking on it, the device is designated as a "favorite". A "favorite" device will have a gold star. The "favorites" serve to identify devices key to the user's analysis. Favorite devices are always displayed regardless of their active/inactive status.
BD_ADDR	The device’s *Bluetooth* address.
Friendly Name	The device name. This field is blank if no friendly name has been observed.
Nickname	Users can type in their own custom name for the device.
Device Class	A general use-classification for the wireless device. _ list the classes by *Bluetooth* technology

Table 3.10 - Wireless Devices Pane Columns(continued)

Column	Description
Technology	Device technology to include one of the following. • BR/EDR • Smart(LE) • Smart Ready (LE & BR/EDR)
IRK	*Bluetooth* low energy only, allows the user to determine which devices are actually the same physical device. The Identity Resolving Key allows peer devices to determine their identities when using random addresses to maintain privacy.

Table 3.11 - Device Classes

Class	BR/EDR	low energy
Audio/Video	X	
Barcode Scanner		X
Barcode Scanner		X
Blood Pressure		X
Blood Pressure: Arm		X
Blood Pressure: Wrist		X
Card Reader		X
Clock		X
Computer	X	X
Cycling		X
Cycling: Cadence Sensor		X
Cycling: Cycling Computer		X
Cycling: Power Sensor		X
Cycling: Speed Cadence Sensor		X
Cycling: Speed Sensor		X
Digital Pen		X
Digitizer Tablet		X
Display		X
Eye-Glasses		X
Gamepad		X
Glucose Meter		X
Health	X	
Heart Rate Sensor		X

Table 3.11 - Device Classes (continued)

Class	BR/EDR	low energy
Heart Rate Sensor: Heart Rate Belt		X
Human Interface Device (HID)		X
Imaging	X	
Joystick		X
Keyboard		X
Keyring		X
LAN/Network Access Point	X	
Media Player		X
Miscellaneous	X	
Mouse		X
Outdoor Sports Activity		X
Outdoor Sports: Location and Navigation Display		X
Outdoor Sports: Location and Navigation Pod		X
Outdoor Sports: Location Display		X
Outdoor Sports: Location Pod		X
Peripheral	X	
Phone	X	X
Pulse Oximeter		X
Pulse Oximeter: Fingertip		X
Pulse Oximeter: Wrist		X
Remote Control		X
Reserved	X	
Running Walking Sensor		X
Running Walking Sensor : On Shoe		X
Running Walking Sensor: In Shoe		X
Running Walking Sensor: On Hip		X
Sports Watch		X
Tag		X
Generic Thermometer		X
Thermometer: Ear		X
Toy	X	
Uncategorized	X	

Table 3.11 - Device Classes (continued)

Class	BR/EDR	low energy
Unknown		X
Watch		X
Wearable	X	
Weight Scale		X

Sorting Wireless Devices columns

Any column in the **Wireless Devices** pane can be used to sort the entire table. Each column is sortable in ascending or descending order, but only one column at-a-time can be used to sort.

Clicking on the column header will initiate the sort. An arrow head will appear on the right of the column. An upward pointing arrow head indicates that the sort is in ascending order top to bottom. Clicking the column header again will toggle the sort to descending order top to bottom.

> **Note:** Devices added after a sort will not appear in the last sort order, and are appended to the current list. The sort process must be repeated to place the new devices in sorted order.

Favorite devices will always grouped together at the top of the Wireless Devices pane in sorted order. Non-favorite devices will appear immediately below the favorite devices in sorted order.

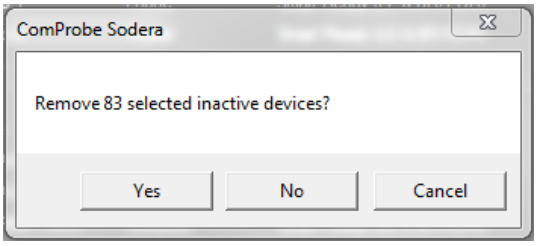
Device Management Tools

At the top of the Wireless Devices pane are three tools for managing the devices in the pane. You can add and edit devices, and delete inactive devices. During Analyzing this toolbar is not available for use.

Table 3.12 - Wireless Devices Management Tools

Tool	Icon	Description
Add New Device,		Clicking this tool will open the **Edit Device Details** dialog. Enter the new device's *Bluetooth* address and other related data and press **OK**.
Edit Selected Device		Allows the user to edit partially known BD_ADDRs, Technology type, Identity Resolving Key (IRK), Device Class, and Friendly Name discovered during capture, and for entering a custom Nickname. Clicking this tool will open the **Edit Device Details** dialog. This tool is inactive until a device is selected.
Hide/Show Inactive Devices		Hide Inactive Devices. All inactive devices are hidden. Favorite devices are always displayed without regard to their active/inactive status. If an inactive devices are selected and the control is toggled to Hide, the selected devices are deselected.
		Show Inactive Devices. Inactive devices are shown. If several active devices are selected and the control is toggled to Show, any inactive device that is inserted between two currently active devices will be shown but not selected.

Table 3.12 - Wireless Devices Management Tools (continued)

Tool	Icon	Description
Remove Selected Inactive Devices,		This tool is grayed-out until an inactive device is selected. Once a device is selected by clicking anywhere in the device row, you can delete the device by clicking on this tool. When this tool is clicked, a warning appears asking for confirmation of the action.  If a device is marked as a Favorite, it will not be deleted even if it is inactive. If Hide Inactive Devices is active, this tool is grayed out and is not active.

Edit Device Details

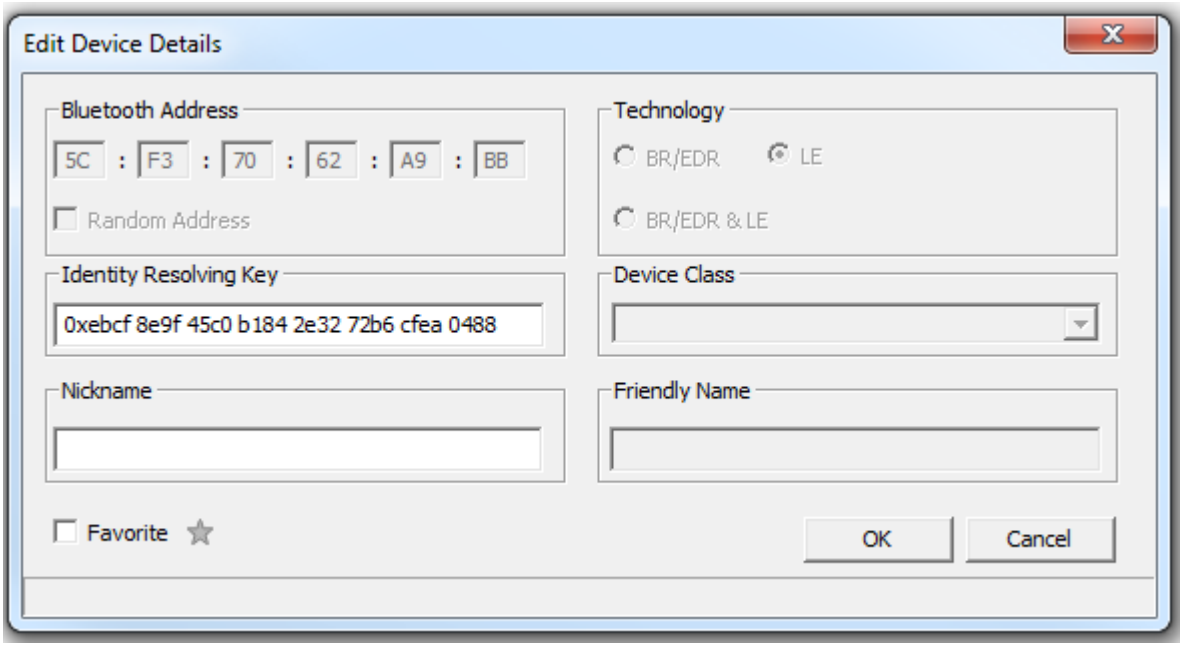


Figure 3.7 - Edit Device Details Dialog

When a device is selected in the window and the **Edit Device Details** tool is selected, a dialog opens showing all the editable fields. Double clicking on a selected field will also open the dialog. If a dialog field is grayed-out, the field is not editable.

Note: Editing of device details is not allowed during Analyzing.

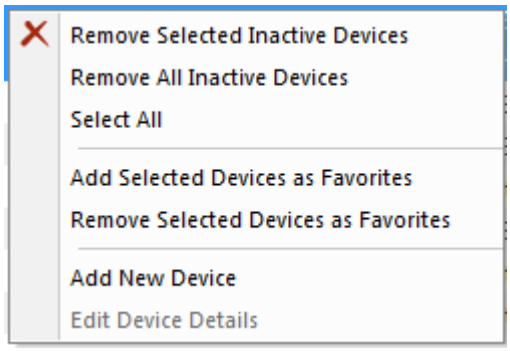
The **Favorite** designation can be changed in this dialog in addition to directly clicking on the star in the table or by using the right-click pop-up menu.

Identity Resolving Key (IRK) Field:

- This field is enabled for devices with a random resolving address or public address. These devices are either Smart (LE) or Smart Ready (LE & BR/EDR) technology. The **Bluetooth Address** will be enabled and checked.
- This field is disabled if the device selected for edit has a valid IRK.
- For random resolving address, entered IRK values are validated against the BD_ADDR. User entered IRK values are automatically reordered when the a secure connection is validated using the IRK. Refer to Reorder Identity Resolving Key (IRK) on page 53 for details on reordering.
- Entering an invalid IRK results in an error message and the field background displays red. The **OK** button is disabled.
- Entering a valid IRK displays a green background and the **OK** button is enabled.
- Valid IRK entries are persisted to the Sodera devices database.

Nickname Field: User defined name or identification, which may be useful for organizing analysis projects.

Right-Click Pop-Up Menu



After selecting a device or devices, right-clicking the mouse will open a pop-up menu that includes functions identical to the Device Management Tools and other functions. The menu active selections will vary depending on the status of the selected devices. For example, selecting inactive devices will activate the inactive devices menu selections.

Table 3.13 - Right-Click Pop-Up Menu Selections

Selection	Description
Remove Selected Inactive Devices	Deletes the selected inactive devices from the wireless devices list. Only active when inactive devices are selected. Same function as the tool in the Device Management Tools. If a device is marked as a Favorite, it will not be deleted even if it is inactive. If Hide Inactive Devices is active , this menu selection is inactive.
Remove All Inactive Devices	Deletes all selected inactive devices from the wireless devices list. Only active when inactive device is selected. If a device is marked as a Favorite, it will not be deleted even if it is inactive. If Hide Inactive Devices is active , this menu selection is inactive.
Select All	Selects all active and inactive devices in the list.

Table 3.13 - Right-Click Pop-Up Menu Selections (continued)

Selection	Description
Add Selected Devices as Favorites	Used to globally designate a group of selected devices as Favorites. If devices in the selection are already designated as Favorites, their designation will not change.
Remove Selected Devices as Favorites.	Used to globally change the Favorite designation for a group of selected devices. If devices in the selection are already not designated as Favorites, their designation will not change.
Add New device	Clicking this tool will open the **Edit Device Details** dialog. Enter the new device's *Bluetooth* address and other related data and press **OK**. Same function as the tool in the Device Management Tools.
Edit Device Details	Active when a single device has been selected. Allows the user to edit partially known BD_ADDRs, Technology type, Identity Resolving Key (IRK), Device Class, and Friendly Name discovered during capture, and for entering a custom Nickname. and Clicking this tool will open the **Edit Device Details** dialog. Same function as the tool in the Device Management Tools.

3.1.2.2.1 Reorder Identity Resolving Key (IRK)

When editing a *Bluetooth* low energy device from the **Wireless Devices** pane using the Edit Device Details dialog, the Frontline software will automatically reorder the user entry. When the user provides an IRK that is in reverse order, the software applies the correct order when validating a secure connection using the IRK.

A reversed IRK is defined as the original IRK value with its endianness reversed. For example, the IRK *0xf31c 22ea a9cb 0422 f9b8 3e03 2305 27e2* in reverse order is *0xe227 0523 033e b8f9 2204 cba9 ea22 1cf3*.

When the user enters a complete IRK in the **Identity Resolving Key** field, a validation of the reversed IRK will occur under the following conditions:

- The device BD_ADDR is a random resolvable private address (RPA), and
- Validation of the IRK in the user-entered order has failed.

The IRK field is also enabled for *Bluetooth* low energy devices with public address, however automatic validation does not occur

If the reversed IRK validates successfully, the **Identity Resolving Key** field turns green and becomes inactive (read only). The status bar at the bottom of the dialog displays "Identity Resolving Key: Valid (Reordered) - Properly resolves the random address". In the Wireless Devices pane, the IRK will now appear for the selected device with "(Reordered)" applended.

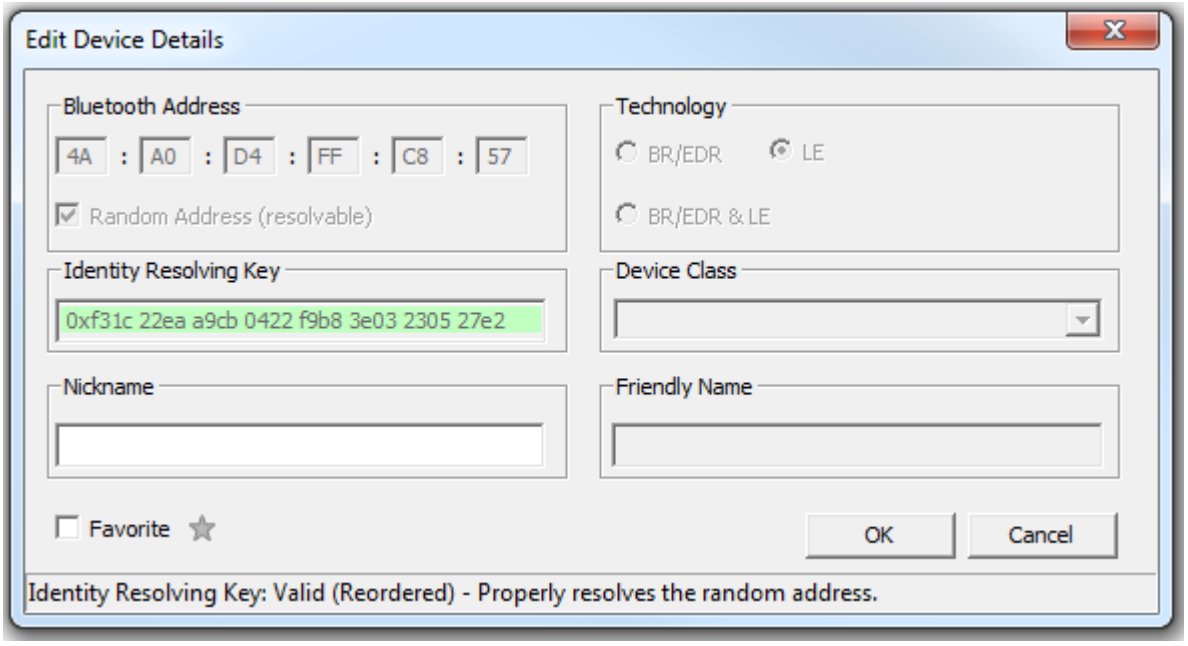
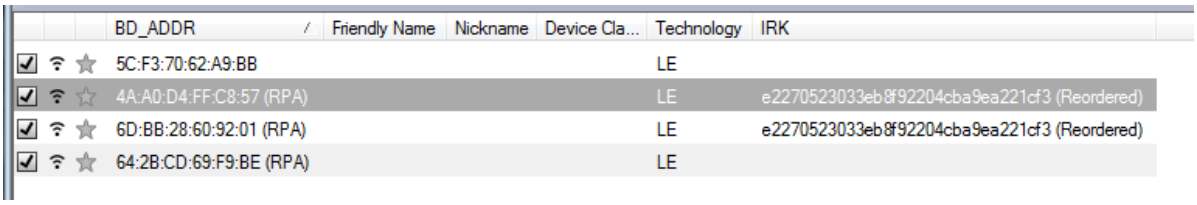


Figure 3.8 - RPA Device IRK Valid and Reordered



BD_ADDR	Friendly Name	Nickname	Device Cla...	Technology	IRK
5C:F3:70:62:A9:BB				LE	
4A:A0:D4:FF:C8:57 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3 (Reordered)
6D:BB:28:60:92:01 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3 (Reordered)
64:2B:CD:69:F9:BE (RPA)				LE	

Figure 3.9 - RPA Wireless Device IRK Reordered and Matched

In the **Wireless Devices** pane, when the user selects a device for filtering for analysis, if that device has an IRK, other devices will also be selected if they match. Two devices match if they satisfy any of the following conditions:

- If two devices have equal IRKs, they are considered to match.
- If one device has a user-entered IRK and its BD_ADDR is not a random resolvable private address (i.e., it is not either a public address or a random static address, and therefore the IRK cannot be validated), it matches if either its IRK is equal or the reverse of its IRK is equal to the other device.

In this next example, we have selected a device with a public address. Entering the IRK in the **Edit Device Details** dialog will indicate "Identity Resolving Key: Complete - Unable to determine if valid." and the **Identity Resolving Key** field remains white and editable but the **OK** button is active. Clicking OK closes the dialog, and the reordered IRK appears in with the public address device with "(Reordered)" appended and matching addresses will display the same reordered IRK.

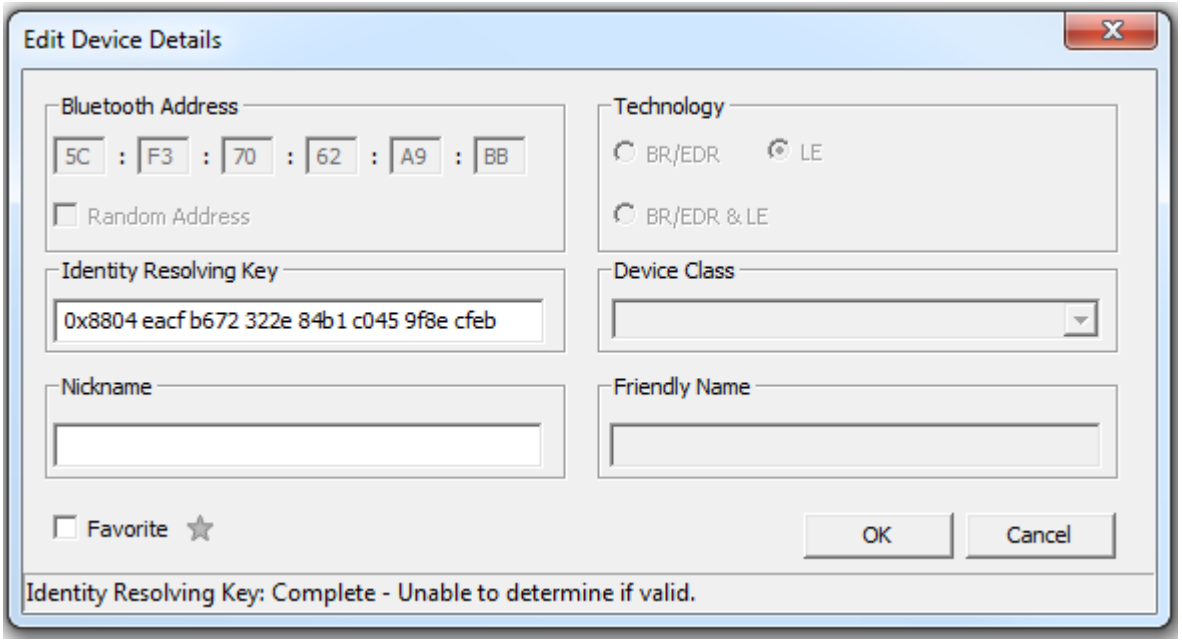


Figure 3.10 - Public Address Device IRK: Unable to Determine if Valid

BD_ADDR	Friendly Name	Nickname	Device Class	Technology	IRK
5C:F3:70:62:A9:BB				LE	ebcf8e9f45c0b1842e3272b6cfea0488 (Reordered)
4A:A0:D4:FF:C8:57 (RPA)				LE	
6D:BB:28:60:92:01 (RPA)				LE	
64:2B:CD:69:F9:BE (RPA)				LE	ebcf8e9f45c0b1842e3272b6cfea0488 (Reordered)

Public Address Device IRK Reordered

Open the **Security** pane. In the first security context for the public address device, enter the LTK into the **Link Key** field. If valid, the IRK for the public address device will appear with "(Reordered)" removed.

Status	Time	Master	Slave	PIN / TK	Link Key
	1/20/2017 7:28:41.334597 AM 1/20/2017 7:28:42.894620 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	n/a	0xccc768dec829ade50842ba3021df44ce Valid
	1/20/2017 7:28:42.894620 AM 1/20/2017 7:28:43.236106 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	Just Works	0xccc768dec829ade50842ba3021df44ce Valid
	1/20/2017 7:28:43.333376 AM 1/20/2017 7:28:44.942150 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	n/a	0xf08bf51a54efb35405d4f4ba07c95ea7 Valid STK
	1/20/2017 7:28:45.429657 AM 1/20/2017 7:28:46.989680 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	n/a	0x7b230f446efe2fadaee1388ac9a53c26 Valid
	1/20/2017 7:28:47.574689 AM 1/20/2017 7:28:49.037211 AM	64:2B:CD:69:F9:BE (RPA)	6D:BB:28:60:92:01 (RPA)	n/a	0x7b230f446efe2fadaee1388ac9a53c26 Valid

Figure 3.11 - Public Address Device: LTK Entered in Security pane to Validate IRK

BD_ADDR	Friendly Name	Nickname	Device Class	Technology	IRK
5C:F3:70:62:A9:BB				LE	ebcf8e9f45c0b1842e3272b6cfea0488
4A:A0:D4:FF:C8:57 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3
6D:BB:28:60:92:01 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3

Figure 3.12 - Public Address Device: IRK Reordered and Validated

3.1.2.3 Wired Devices Pane

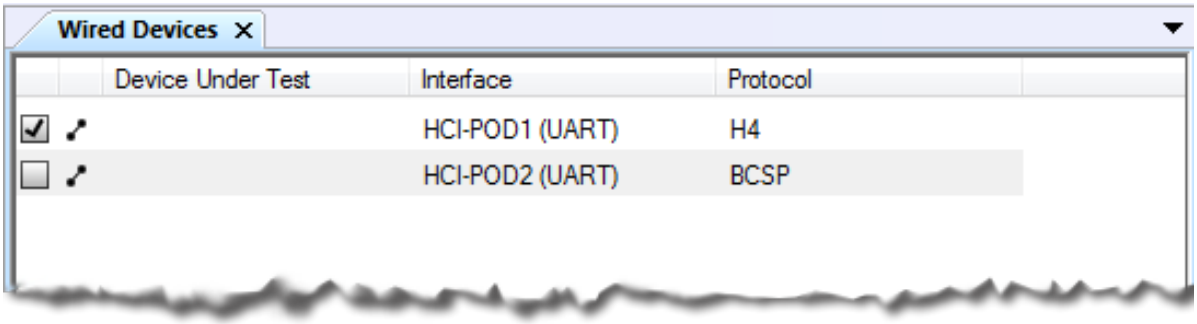


Figure 3.13 - Sodera Wired Devices Pane

The **Wired Devices** pane is selected by selecting the tab in the Devices pane. The Wired Devices tab will appear when **Wired Devices** is checked in the **View** menu. The Wired Devices tab can be hidden from view by unchecking the selection in the **View** menu or by clicking on the ✕ on the **Wired Devices** tab.

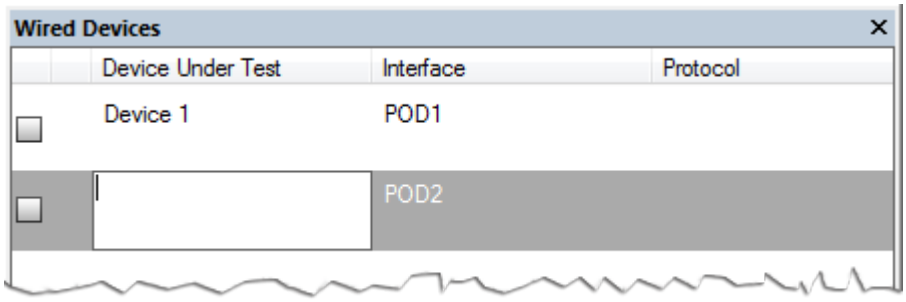
The Wired Devices pane provides information about devices connected to **POD 1** and **POD 2**, on the bottom of the Sodera unit. These connectors are used to capture Host Controller Interface traffic through a direct wired connection. The **HCI UART** will capture Protocol Transports H4, BCSP, and 3-wire (H5).

The Wired Devices pane contains five columns. Their functions are listed below.

Table 3.14 - Sodera Wired Devices Pane Columns

Column	Description
Filter Selection ☐/☑	The filter is an on/off selection . When checked , the device is selected for data analysis, that is the data is filtered into the Frontline protocol analyzer when the Standard Toolbar **Analyze** button is clicked.
Traffic Captured	If the a "traffic captured" icon is present traffic has been captured that involves the device. If the icon is not present then Sodera has not captured any traffic that involves that device. Only wired devices with traffic captured can be used for Frontline protocol analysis.
Device Under Test	The is an area where the user can optionally document which device they were connected to at the time of the capture.
Interface	For each device, this column lists the Sodera interface connection and the protocol configured for that connection.
Protocol	For each device, this column lists the configured interface protocol transport.

Naming the Device Under Test



In the **Device Under Test** column, you can optionally document which device they were connected to at the time of the capture. To do this, click in the **Device Under Test** field in a device row.
Type an identifying name, and press Enter on the keyboard to click in another field.

For more information on configuring the wired devices, see Menu on page 33.

3.1.2.4 Piconet View Pane (Experimental)

> **Note:** At this time the **Piconet View** is in experimental. This topic provides a description of the anticipated **Piconet View** functionality.

Devices and connections detected by the Frontline hardware are displayed graphically on the **Piconet View** pane for further configuration and selection for analysis by the user. Devices and connections are displayed on the **Piconet View** pane only when data to or from those devices or connections has been detected by the Frontline hardware, while the appearance of devices in the **Wireless Devices** pane includes detected devices, user entered devices, and remembered devices.

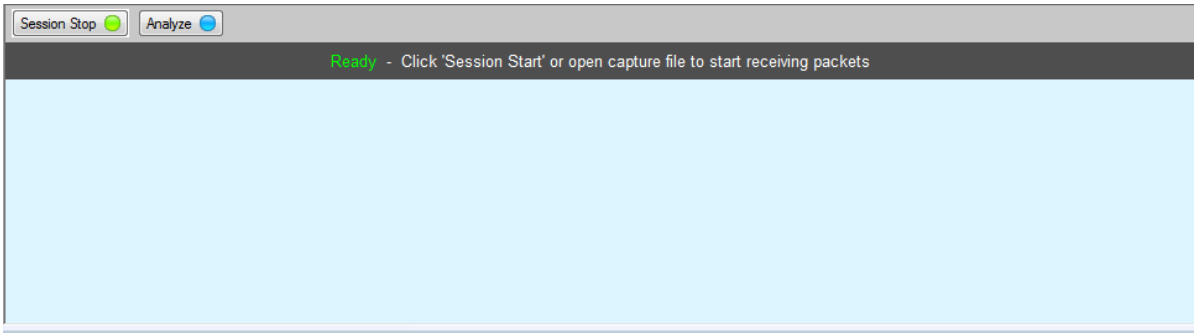
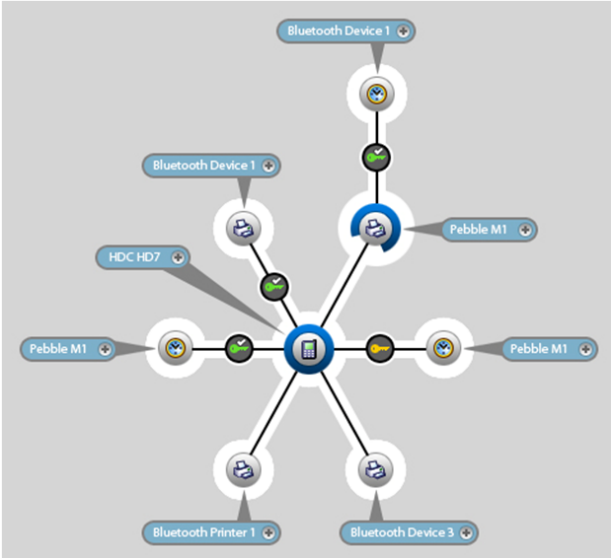


Figure 3.14 - **Piconet View**

Adjacent to each device in the view is the devices BD_ADDR

Attached to each dot is a label that displays BD_ADDR . The tab is colored either blue or green to indicate that the related device is Classic or low energy *Bluetooth*.

A blue ring surrounds the device that is either paging or serving as the master device in the piconet. In the event of a role switch, this blue ring will shift position to the new piconet master.



In the event of scatternet where one piconet master that is also a slave of a secondary piconet, the blue ring is “broken” in that roughly 25% of the ring is cut away to accommodate the slave’s position in primary piconet. The remaining 75% of the blue ring connects to the secondary piconet slave device.

Within the **Piconet View**, rolling the mouse over an icon will highlight that device or security information in the **Wireless** and **Security** panes.

Timeline

Figure 3.15 - **Piconet View** Timeline

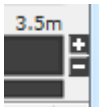
As device connections appear over time, the Timeline on the bottom of the **Piconet View** displays circles representing events over time where the piconet view has changed. Classic *Bluetooth* events appear as blue circles and *Bluetooth* low energy events appear as green circles. These events appear when devices:

- Connects - solid circles
- Role Switches - sold circles
- Disconnects - hollow circles

Select an event on the time line by clicking on an event circle.

The display on the **Piconet View** will change to the piconet configuration active at the selected event time allowing the user to trace piconet activity. A timeline cursor—a white vertical line—will appear behind the selected timeline event. Above the timeline cursor appears the event capture date and time.

> **Note:** The timeline event cursor is always positioned in the center of the display. A selected event will move to the cursor, thus the selected event is always position in the center of the **Piconet View**.



On the timeline right end is the timeline duration and the zoom controls. The current duration of the visible timeline is shown in minutes (m) or seconds (s). The "+" and "-" controls will zoom in and zoom out the timeline, respectively. To show less of the timeline (more detail) click on the "+", and to show more of the timeline (less detail) click on the "-".

3.1.2.5 Security Pane

The Security pane is where the Frontline software identifies devices with captured traffic ( ) that contain pairing, authentication, or encrypted data. The pane will show fields for entering keys, and will show if the keys are valid or invalid.

Successful decryption of captured data requires datasource receipt of all the critical packets and either :

- be given the link key by the user, or
- observe the pairing process and determine the link key.

See Sodera: Critical Packets and Information for Decryption on page 102 for a description of the critical packets. The Security pane will identify the type of key required for decryption.

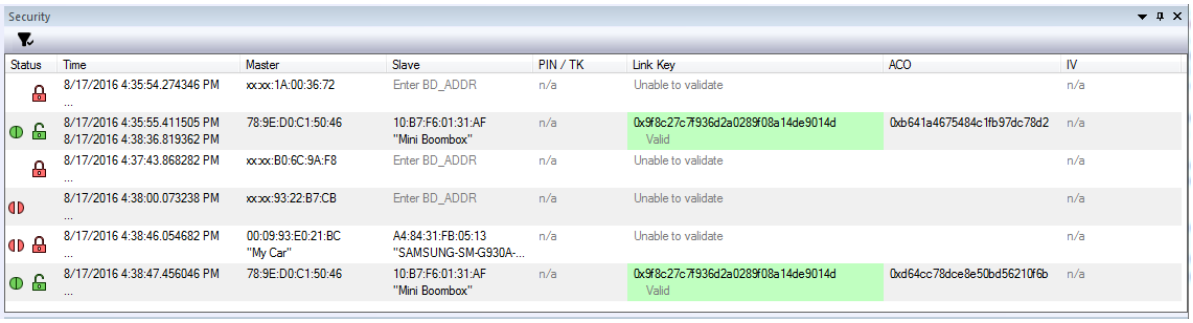
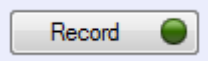


Figure 3.16 - Sodera Datasource Security Pane

The **Security** pane shows events in the current capture. When the **Record** button is clicked, all devices with active traffic that require decryption are shown. Security events appear in starting time order with the most recent event at the bottom.



- **Status**: displays icons showing the pairing and encryption/decryption status.

Icon	Description
	Pairing/Authentication attempt observed but was unsuccessful
	Devices successfully Paired/Authenticated.
	Encrypted: traffic is encrypted but there is insufficient information to decrypt. See Sodera: Critical Packets and Information for Decryption on page 102 for a description of the critical packets.
	Decrypted

- **Time**: Beginning and end time of the security context. No end time is indicated by an "...". Beginning time is shown in the first row of the grouping. End time is shown in the second row.
- **Master**: The BD_ADDR of the master device in the link. If the friendly name is available it will show on the second line.
- **Slave**: The BD_ADDR of the slave device in the link. If the friendly name is available it will show on the second line.

> **Note:** If the **Master** and **Slave** switch roles another entry will appear in the **Security** pane

Status	Time	Master	Slave	PIN / TK	Link Key	ACO
	12/1/2014 12:35:12.797571 PM 12/1/2014 12:35:16.400090 PM	00:88:65:61:B7:27	00:07:62:0F:00:00 "T515"	Not needed	0x5d306875603c4f1e065a052923f4d8ba Valid	0xf67b04b7eb01b38eb55eb3cb
	12/1/2014 12:35:16.610163 PM ...	00:07:62:0F:00:00 "T515"	00:88:65:61:B7:27	n/a	0x5d306875603c4f1e065a052923f4d8ba Valid	0xf67b04b7eb01b38eb55eb3cb

Figure 3.17 - Role Switch Example

- **PIN/TK**:
  - Classic Bluetooth® :
    - Legacy Pairing PIN: 1 to 16 alphanumeric character PIN
  - Bluetooth low energy
    - PIN: 6 digit numeric passkey (000000 - 999999)
    - Out-of-Band Temporary Key (OOB TK): 32 digit hexadecimal number
- **Link Key**
  - Classic Bluetooth® , 32 digit hexadecimal number
  - Bluetooth low energy, 32 digit hexadecimal number
  - The **Link Key** cell displays "*Enter link key*" in gray when the link key is unknown. When a link is invalid the cell has a light red background and indented gray text under the link key says "*Invalid*". When a link key is valid the cell has a light green background and indented gray text under the link key says "*Valid*" (if the link key was transformed from the entered link key the text is "*Valid (Reordered)*".
  - If Sodera is **Analyzing** and a link key has not been entered, "Stop analyzing to enter link key" appears in the device **Link Key** cell. Click the **Analyzing** button to stop the analysis, and type or paste in the link key.
  - Users can enter the device security information by typing directly on the device fields **PIN/TK** and **Link Key**. An invalid entry will display a red background and a warning **Invalid**.
- **ACO**: Authenticated Ciphering Offset is used by the devices for generation of the encryption key in Classic *Bluetooth*.
- **IV**: Initialization Vector is displayed for both *Bluetooth* low energy encryption and Classic *Bluetooth* Secure Connections/AES encryption.. The slave will use the IV in starting the encrypted communications.

3.1.2.5.1 Classic *Bluetooth* Encryption

To decrypt a Classic *Bluetooth* link there are two options in the **Security** pane.

1. PIN : Enter into the **PIN/TK** field; legacy pairing only.

> **Note:** The only time a PIN can be used is when the datasource has captured Legacy Pairing in the current trace. The datasource uses information transferred during the Legacy Pairing process to calculate a Link Key.

2. Link Key: Enter into the **Link Key** field.

Passkey/PIN

The first option uses a PIN to generate the Link Key. If the analyzer is given the PIN and has observed complete pairing it can determine the Link Key. Since the analyzer also needs other information exchanged

between the two devices, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

The **PIN/TK** can be up to a maximum of 16 alphanumeric ASCII characters or a hexadecimal value that the user enters. When entering a hexadecimal value it must include a “0x” prefix, for example, “0x1234ABCD”.

Link Key

If you know the Link Key in advance you may enter it directly. To enter the Link Key click on the device row **Link Key** field and enter the Link Key in hex followed by the keyboard Enter key. If the link key has previously been entered it is automatically entered in the edit box after the Master and Slave have been selected. Once the Link Key is entered the ACO automatically appears in the **Security** pane for the devices in the link.

> **Note:** The Link Key does not have to be prefixed with "0x" because the Link Key field will only accept hex format, and the "0x" prefix is added automatically. Entering "0x..." will result in an invalid entry result.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO
	11/20/2014 2:34:57.115571 PM 11/20/2014 2:35:00.754965 PM	00:88:65:61:B7:27	00:07:62:0F:00:00 "T515"	n/a		
	11/20/2014 2:35:00.928163 PM ...	00:07:62:0F:00:00 "T515"	00:88:65:61:B7:27	n/a	Enter link key	

Figure 3.18 - Classic Bluetooth Link Key Entry

Status	Time	Master	Slave	PIN / TK	Link Key	ACO
	11/20/2014 2:34:57.115571 PM 11/20/2014 2:35:00.718090 PM	00:88:65:61:B7:27	00:07:62:0F:00:00 "T515"	n/a	0x5d306875603c4f1e065a052923f4d8ba Valid	0xf67b04b7eb01b38eb55eb3cb
	11/20/2014 2:35:00.928163 PM ...	00:07:62:0F:00:00 "T515"	00:88:65:61:B7:27	n/a	0x5d306875603c4f1e065a052923f4d8ba Valid	0xf67b04b7eb01b38eb55eb3cb

Figure 3.19 - Classic Bluetooth Valid Link Key Entered and ACO Automatically Calculated

If the Link Key is correct the **Link Key** field for the devices in the encrypted link will appear green with "valid" below the link key. If the Link Key is not correct the **Link Key** field will appear red with "invalid" below the link key. To re-enter the Link Key click on the **Link Key** field and follow the procedure above.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO
	11/20/2014 4:00:51.934571 PM 11/20/2014 4:00:55.573965 PM	00:88:65:61:B7:27	00:07:62:0F:00:00 "T515"	n/a	0x123456789abc Invalid	
	11/20/2014 4:00:55.747163 PM ...	00:07:62:0F:00:00 "T515"	00:88:65:61:B7:27	n/a	Enter link key	

Figure 3.20 - Classic Bluetooth Invalid Link Key Entered

SSP Debug Mode

If one of the *Bluetooth* devices is in SSP Debug Mode then the Frontline Sodera analyzer can automatically figure out the Link Key, under certain conditions. To obtain the information for figuring out the Link Key, the software must actively observe the SSP pairing process in the capture. If the SSP pairing previously took place and encrypted data is later captured the software does not have the necessary information to figure out the Link Key. The only alternatives are

- to again pair the devices in SSP Debug Mode, or
- to independently determine the Link Key and enter it directly..

> **Note:** Only one device in the link must be in SSP Debug Mode.

If the Bluetooth devices do not allow Debug Mode activation, enter the Link Key as described above.

3.1.2.5.2 *Bluetooth* low energy Encryption

Long Term Key

The Long Term Key (LTK) in *Bluetooth* low energy is similar to the Link Key in Classic Bluetooth. It is a persistent key that is stored in both devices and used to derive a fresh encryption key each time the devices go encrypted. In the Sodera Security pane the LTK is entered in the **Link Key** field so the following discussion will use Link Key instead of LTK.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 8:28:06.087692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	Enter link key	n/a	0x67adbde4d857d...

Figure 3.21 - Bluetooth low energy Static Address Link Key Required

In this example a low energy device requires Link Key entry for the Frontline software to decrypt the data. To enter the Link Key click on **Enter link key** and type or paste in the Link Key in hex format.

> **Note:** It is not necessary to precede the Link Key with "0x" to signify a hex format. The software will automatically add "0x" to the front of the Link Key.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 7:14:06.119692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a		n/a	0x67adbde4d857d...

Figure 3.22 - Bluetooth low energy Enter Link Key

Press the Enter key or click outside the Link Key box. If the Link Key is valid the box will be green, beneath the Link Key will appear "Valid, and the Status will show an open, green lock indicating that decryption is enabled.

If the Link Key is not valid the box will be red, beneath the entered Link Key will appear "Invalid", and the Status will show a closed, red lock indicating that decryption is not enabled.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 8:15:16.868692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	0xe26e121986ca19c1a169d4be9... Valid	n/a	0x67adbde4d857d...

Figure 3.23 - Bluetooth low energy Valid Link Key

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 8:28:06.087692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	0x123456adfe Invalid	n/a	0x67adbde4d857d...

Figure 3.24 - Bluetooth low energy Invalid Link Key

Legacy Just Works Pairing

In this example the devices under test useLegacy Just Works pairing to calculate a Short-Term Key (STK) in order to securely transfer the device's Long-Term Key (LTK). The LTK is then used to encrypt the subsequent security contexts.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 8:43:20.557499 AM 11/13/2014 8:43:22.458777 AM	5C:F3:70:62:A9:BB	5C:F3:70:62:B2:E7	Just Works	0x9619dfcec26ee3bf686... Valid	n/a	0x9b032fb0151c0d...
	11/13/2014 8:43:22.995034 AM 11/13/2014 8:43:24.652559 AM	5C:F3:70:62:A9:BB	52:0E:A1:9B:A7:3E (rand)	n/a	0xccc768dec829ade508... Valid	n/a	0x3f45d462fb8d18af
	11/13/2014 8:43:25.091315 AM 11/13/2014 8:43:26.553837 AM	64:2B:CD:69:F9:BE (rand)	4A:A0:D4:FF:C8:57 (rand)	n/a	0xccc768dec829ade508... Valid	n/a	0x2c8edd00ed9c8...

Figure 3.25 - Bluetooth low energy Piconet Public Key and Private Key Encryption

Legacy Passkey Pairing

PIN is a six-digit decimal number. If a passkey is required by the device "Enter passkey" will appear in the device's **PIN/TK** field.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 9:07:10.139572 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	Enter passkey	Enter link key	n/a	0xe0efb01d9705d8...
	11/13/2014 9:13:27.746147 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	Enter passkey	Enter link key	n/a	0xd5a2c01d0c23b...

Figure 3.26 - Bluetooth low energy Passkey Decryption Not Enabled

This example uses Passkey Pairing to enable decryption. The user clicks on "Enter passkey" in the device **PIN/TK** field.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 9:07:10.139572 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	000000	Enter link key	n/a	0xe0efb01d9705d8...
	11/13/2014 9:13:27.746147 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	Enter passkey	Enter link key	n/a	0xd5a2c01d0c23b...

Figure 3.27 - Bluetooth low energy Passkey Entry

Press Enter or click outside the field. If the Passkey is correct it will appear in the **PIN/TK** field with "Valid" appearing below the passkey, **Link Key** field will automatically fill with the Link Key that will show "Valid" and appear green. The **Status** field will show an open, green lock to show that encryption is enabled and the analyzer can show decrypted data.

If the entered Passkey is incorrect, the **PIN/TK** field will be red and "Invalid" will appear below the entered PIIN. The **Status** field will show a closed, red lock to indicate that encryption is not enabled.

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 9:07:10.139572 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	000000 Valid	0x5f66b668de1cddebf4... Valid	n/a	0xe0efb01d9705d8...
	11/13/2014 9:13:27.746147 AM 11/13/2014 9:13:55.406063 AM	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	000000 Valid	0xa398832560f22f9a2c... Valid	n/a	0xd5a2c01d0c23b...

Figure 3.28 - Bluetooth low energy Passkey Decryption Enabled

Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
	11/13/2014 9:30:51.608572 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	111111 Invalid	Enter link key	n/a	0xe0efb01d9705d8...
	11/13/2014 9:37:09.215147 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	Enter passkey	Enter link key	n/a	0xd5a2c01d0c23b...

Figure 3.29 - Bluetooth low energy Passkey Invalid

Legacy Out-of-Band(OOB) Pairing

Out-of-Band (OOB) data is a 16-digit hexadecimal code preceded by "0x" which the devices exchange via a channel that is different than the le transmission itself. This channel is called OOB. For off-the-shelf devices we cannot sniff OOB data, but in the lab you may have access to the data exchanged through this channel.

If a device requires OOB data the device Link Key field will show "Enter OOB TK".

3.1.2.6 Private Keys Pane

For Sodera captures that include Bluetooth low energy Secure Connections Pairing between one or more pairs of devices, users will be able to manually enter Private Keys for both legacy and Secure Connections. The Private/Public keys are stored for use by discovered *Bluetooth* low energy devices. Duplicate keys cannot be stored.

When Debug key is not used during pairing, the datasource will look for a matching Public key in the set of Private/Public key pairs. If a match is found, the datasource will use the corresponding Private Key to compute the Diffe-Hellman Key.

The **Private Keys** pane can be viewed or hidden from the **View** menu and can be docked like the other optionally viewable panes. While operating in live mode, Private Keys are saved to persistent storage when the **Frontline Sodera** window is closed . When the window is opened while in live mode, saved Private Keys are loaded from persistent storage.

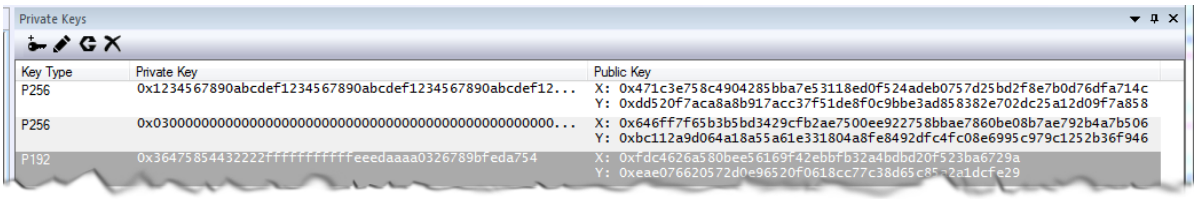


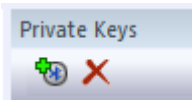
Figure 3.30 - Private Keys Pane

The **Private Keys** pane has three columns that list one entry for each unique key.

Table 3.15 - Private Keys pane Columns

Column	Description
Key Type	P192 if the key is used for Legacy pairing. P256 if the key is used for Secure Connection pairing.
Private Key	The key entered by the user. 24 octets for P192 (Legacy) 32 octets for P256 (Secure Connection)
Public Key	The two parts of the public key automatically generated when the complete Private Key is entered. X - the first half of the Public Key y - the second half of the Public Key

Private Key management tools



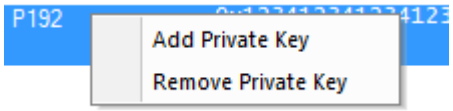
In the header of the **Private Keys** pane is a toolbar for adding or deleting keys.

Table 3.16 - Private Keys Management Tools

Tool	Icon	Descriptioin
Add Private Key		Used to add a Private Key to the pane. When clicked, it opens the **Private Keys Entry** dialog. See Private Key Entry dialog on page 65
Edit Selected Private Key		Enabled when a private key in the pane is selected. When clicked, it opens the **Private Keys Entry** dialog with the selected Private and Public Key filled in. See Private Key Entry dialog on page 65
Reverse Private Key		Enabled with a private key in the pane is selected. When checked, it allows the user to switch between big endian and little endian format. The public key will be updated to reflect the changes made to the private key.

Table 3.16 - Private Keys Management Tools (continued)

Tool	Icon	Descriptioin
Remove Private Key		Enabled when a private key in the pane is selected. When clicked the selected key row is removed from the pane.



Right-clicking on a selected Private Key entry in the pane or right clicking anywhere in the pane will open a Private Key Management tools menu. The menu selections perform the same functions as the Private Key Management tools.

Private Key Entry dialog

The **Private Key Entry** dialog opens when the user selects **Add Private Key** from the Private Keys Management Tools or from the right-click menu.

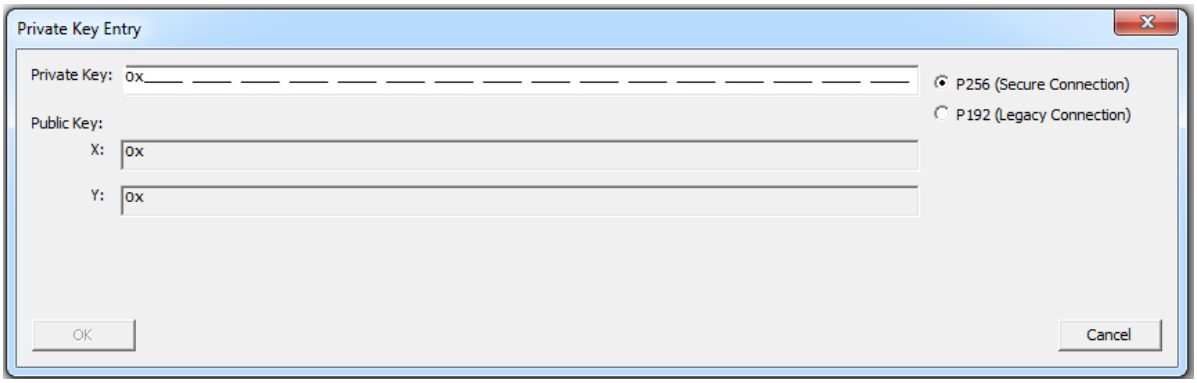


Figure 3.31 - Private Key Entry Dialog

Table 3.17 - Private Key Entry Dialog Fields

Section	Field	Description
Key Type	**P256 (Secure Connection)**	Make this selection if using Secure Connection pairing.
	P192 (Legacy Connection)	Make this selection if using Legacy pairing.
Private Key		Enter the Private Key in hex. The size of this field will vary with the Key Type, P256 or P196.
	Reverse	Allows the user to switch the Private Key between little endian and big endian format. The public key will be updated to reflect the changes made to the private key.
Public Key	**X:**	The Public Key is calculated automatically when the Private Key is completely entered. X: - first half of the key.
	y:	The Public Key is calculated automatically when the Private Key is completely entered. Y: - second half of the key.

To Add a Private Key:

1. Select one of the following connection types to set the length of the **Private Key** field:
   a. **P256 (Secure Connection)**, or
   b. **P192 (Legacy Connection)**
2. Enter the Private Key, in hexadecimal, into the **Private Key** field.
   a. P256 field type takes 64 hexadecimal characters.
   b. P196 field type takes 48 hexadecimal characters.

   > **Note:** If after entering the private key you change the Key Type from P256 to P192, the Private and Public key fields will truncate to the correct length for P192 key type. However, this does not work in the reverse direction.

   The **Private Key** may also be pasted in. The copied key pasted in may have been in either big endian or little endian format. The **Reverse** button allows the user to reverse the format for use with their particular device.
3. Once the **Private Key** field is completely filled in, the **Public Key X:** and **Y:** fields are automatically calculated and filled in.
4. Click the **OK** button, the dialog will close, and the added Private and Public keys appear in the Private Keys pane.

   If the key enterd already matches a key in the local storage, a dialog will be displayed indicating the issue and the window will not close.

To Remove a Private Key:

1. In the **Private Keys** pane, click on the Private Key to be remove to select it.
2. Remove the Private Key by one of the following methods:
   a. Click on the **Remove Private Key** tool in the Private Key Management toolbar. The key is removed from the list.
   b. Right-click on the selected Private Key, and select **Remove Private Key** from the Private Key Management tools pop-up menu. The key is removed from the list.

3.1.2.7 Event Log Pane

The Event Log is a record of significant events that occurred at any time the Sodera datasource software is running. The log is recorded in time sequence using the computer clock. Log event descriptions provide information, warnings, and error notifications. The Event Log provides the user with a history of their analysis process. This history may be useful for process documentation or for troubleshooting capture issues and problems.

Information messages can include the starting and stopping of recording and the time that this event took place. Warnings in the log could be notifying the user that the capture file just opened contains unsupported content. Event Log error events include, for example, telling the user that the capture file is invalid.

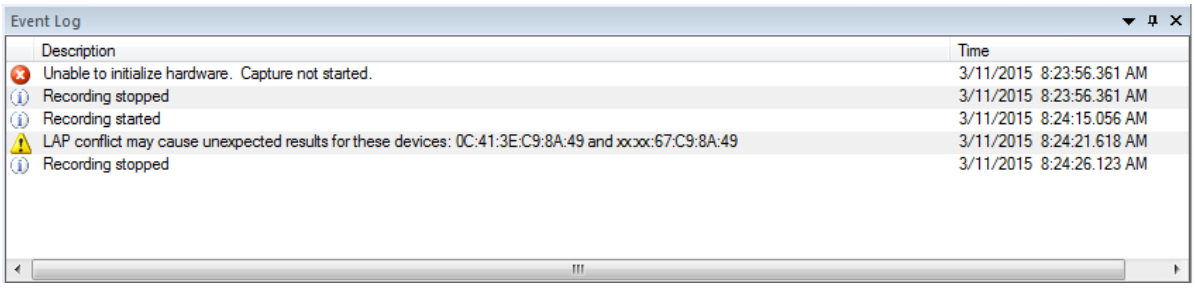


Figure 3.32 - Sodera Event Log Pane

The **Event Log** pane contains event icons in the first column (no heading), event descriptions in the second column (**Description**), and the time the event occurred in the third column (**Time**).

A description of each **Event Log** column is in the following table.

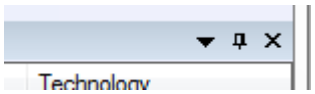
Table 3.18 - Event Log Columns

Heading	Icon	Description
Event		Information: Events related to the normal flow of the capture process, e.g. "Start Capture", "Stop Capture", "Sodera hardware not found"
		Warning: Events that raise concern about the capture process integrity
		Error: Events that compromise the capture process or that may invalidate some of the captured data.
Description	—	Description of the event with additional information related to the Event icon.
Time	—	The actual time of the event in live capture mode, or the recorded time when running a previously captured file. The recorded time is based on the clock of the computer running the ComProbe software.

Saving the Event Log

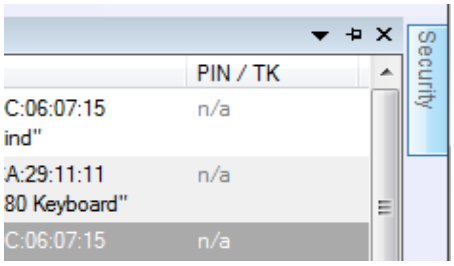
The Event log is automatically saved to "%appdata%\Frontline Test Equipment\Sodera\Logs\" as a .txt file. Logs are retained for each session.

3.1.2.8 Pane Positioning and Control



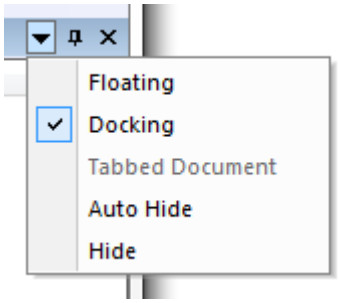
The Sodera window **Wired Devices**, **Security**, **Private Keys**, **Piconet View**, and **Event Log** panes can be customized to suit the user's requirements. At the top of each pane, on the right, is a set of pane positioning controls.

- Clicking on **Close** will close the pane. Once the pane is closed, it can be displayed again by selecting the pane in the **View** menu.
- Clicking on **Auto Hide** will pin the pane to the right border as a tab. The title of the hidden/pinned pane will appear at the border.



Hovering over the hidden pane title will expand the pane and the **Auto Hide** icon appears rotated . Clicking on the **Auto Hide** will unhide or unpin the pane.

- Clicking on **Window Position** opens a menu of positioning options. The currently selected option is shown with a check mark. Right-clicking in the pane header will also bring up the **Window Position** menu.



  - **Floating**: The pane operates as an independent window on the screen allowing it to be positioned anywhere on the screen. Once the pane is floating it can be repositioned within the boundaries of the Sodera datasource window using Positioning by Cursor, below.
  - **Tabbed Document**: A tab for the pane is created adjacent to the **Wireless Devices** tab.
  - **Docking**: The pane is positioned to its last docked position. A new docked position can be selected by using Positioning by Cursor, below.
  - **Auto Hide**: Operates the same as **Auto Hide** discussed above, collapsing the pane and docking.
  - **Hide**: Operates the same as **Close** discussed above.

- You can repeat this process with other panes open and the control will highlight the available area

Positioning by Cursor

Changing the size of pane

To change the size of a pane, position the cursor on an edge of the pane (the cursor will change to a two-way arrow), left-click, hold, and drag the pane to the desired size. Release the mouse button.

If the pane is floating, the cursor can also be positioned on a corner of the pane, which permits two-way resizing.

Changing the position of a pane

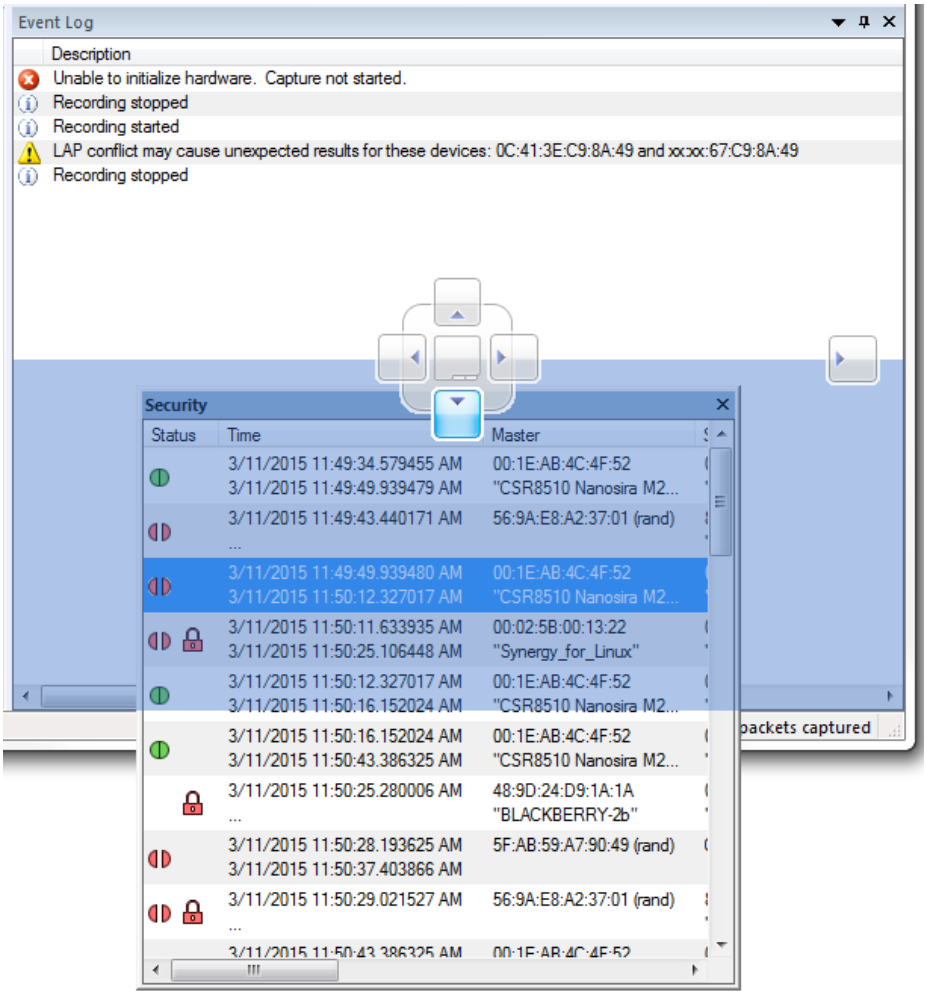


Figure 3.33 - Positioning by Cursor

This pane positioning method works whether the pane is docked or floating.

Position the cursor on the title bar of the pane. Left-click, hold, and start dragging the pane. Eight positioning controls (each with its own arrow) will appear at various locations on the main window. Drag the pane such that the mouse cursor is positioned on the desired positioning control. The positioning control will turn blue and the new position of the pane will be indicated in blue. Release the mouse button. The pane will move to the new position.

Creating a tabbed pane

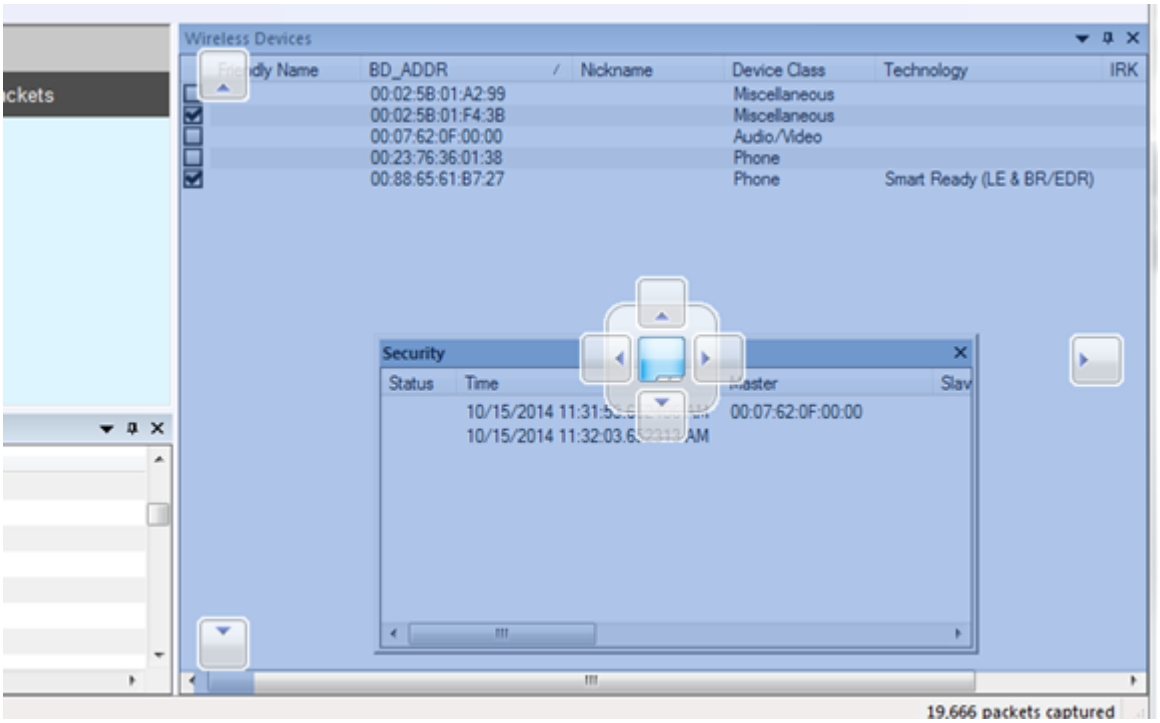
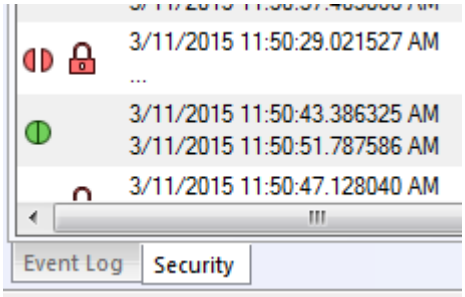


Figure 3.34 - Position Control for Setting Tabbed Security Pane



Move the cursor until the middle position indicator turns blue and release the mouse key. The pane will appear as a tab at the bottom of the target pane.

Changing the position of a tabbed pane

This is the same as changing the position of a non-tabbed pane except that the cursor is positioned on the tab itself, not the title bar.

To set a tabbed pane to full view left-click and drag the tab outside the target pane. The cursor positioning control will appear. Position the pane using the positioning control and release the mouse key.

Using the View Menu

The Sodera window **View** menu can be used to close or open the panes.

3.1.3 Excursion Mode

Excursion Mode allows the user to capture *Bluetooth* data while untethered from a computer. This feature can make it easier to capture data while in a moving vehicle, to capture data in places where a laptop cannot readily be used, or to capture data in confined spaces, for example. Sodera's internal battery complements Excursion mode by providing sufficient power to capture data for up to an hour without being connected to an external power source

Enable Excursion mode

1. Connect the Sodera hardware to a computer with a USB cable and start the Frontline software.
2. In the Sodera window, select **Capture Options...** from the **Options** menu.
3. Verify that the status message on the pop-up indicates the serial number of the connected hardware.
4. Check the box next to **Enable Excursion mode captures** and press **OK**. The pop-up will close and the **Capture Options** are saved to the connected Sodera hardware. The saved **Capture Options** will travel with that specific Sodera hardware module and affect all subsequent captures performed with that unit, regardless of whether they are performed using Excursion mode or using a connected computer.

Disable Excursion mode

1. Connect the Sodera hardware to a computer with a USB cable and start the ComProbe Protocol Analysis System.
2. In the Sodera window, select **Capture Options...** from the **Options** menu.
3. Verify that the status message on the pop-up indicates the serial number of the connected hardware.
4. Uncheck the box next to **Enable Excursion mode captures** and press **OK**. The pop-up will close and the **Capture Options** are saved to the connected Sodera hardware.

Start Capturing Data in Excursion mode

1. With the Sodera hardware disconnected from a computer, hold for at least 1/2 second and then release the Power button on the front panel. The battery charge state indicator LEDs will repeatedly flash in sequence while the unit powers up.
2. Once the unit is powered up, press the Capture button on the front panel (right side). The Capture LED will be a constant green when capturing data.

Stop Capturing Data in Excursion mode

1. Press the Capture button on the front panel (right side). There may be a brief delay, and the Capture LED will turn off.

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.

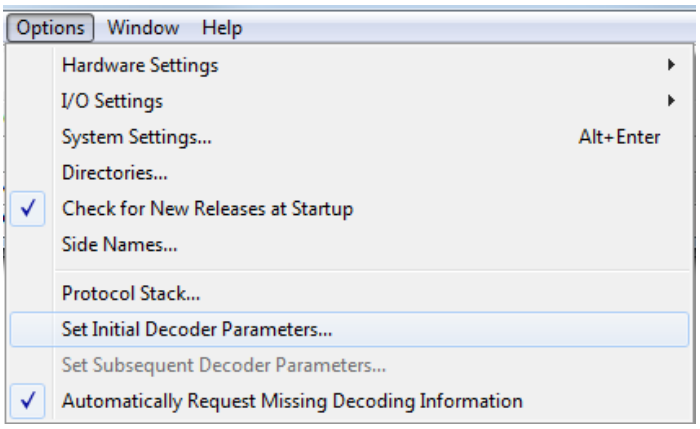


Figure 3.35 - Select **Set Initial Decoder Parameters...** from **Control** window

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

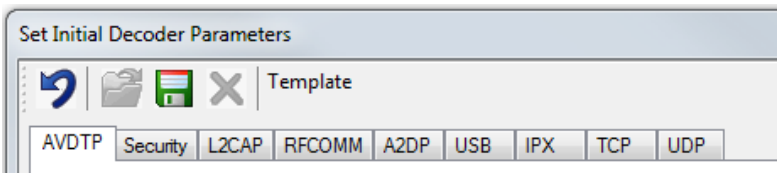


Figure 3.36 - Tabs for each decoder requiring parameters.

- 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.

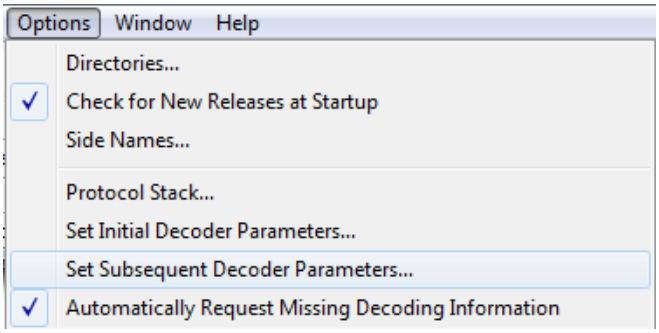


Figure 3.37 - **Set Subsequent Decoder Parameters...** from **Control** window

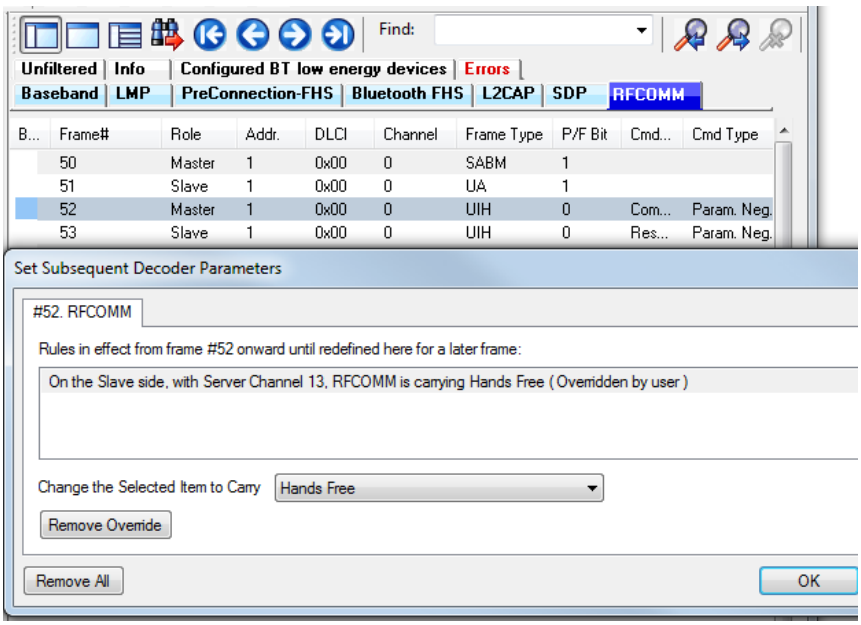


Figure 3.38 - Example: Set Subsequent Decode for Frame #52, RFCOMM

- 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.

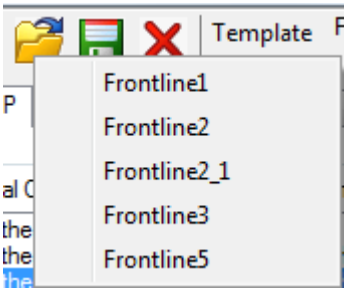
3.2.1 Decoder Parameter Templates

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

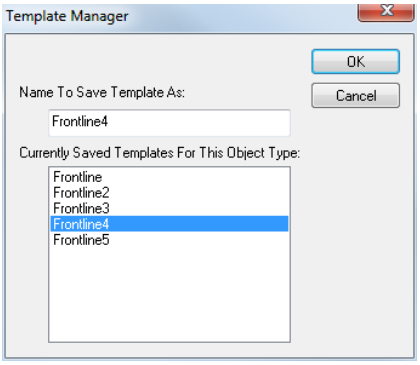
A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

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 toolbar.

   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 Selecting A2DP Decoder Parameters

Decoding SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame. You can increase the decoding speed by decoding only the header fields and disregarding other parts. You can select the detail-level of decoding using the **Set Initial Decoder Parameters** window.

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

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

2. Click on the **A2DP** tab.

3. Choose the desired decoding method.

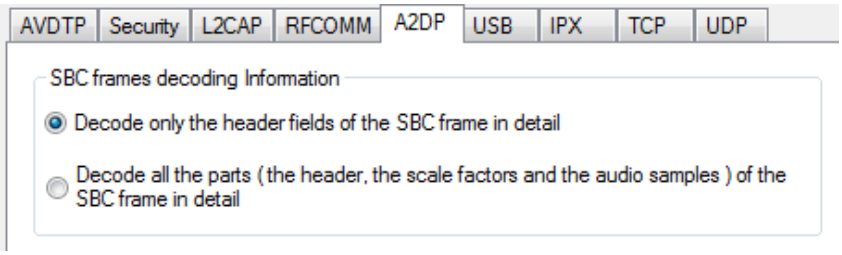


Figure 3.39 - A2DP Decoder Settings

4. Follow steps to save the template changes or to save a new template.

5. Click the **OK** button to apply the selection and exit the **Set Initial Decoder Parameters** window.

3.2.3 AVDTP Decoder Parameters

3.2.3.1 About AVDTP Decoder 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** window.

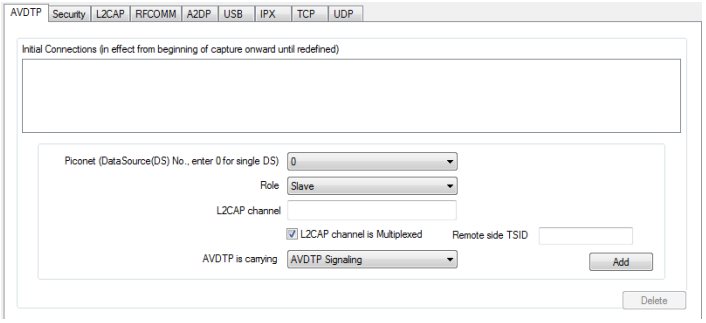


Figure 3.40 - AVDTP parameters tab

The **AVDTP** tab requires the following user inputs to complete a parameter:

- **Piconet (Data Source (DS) No.)** - When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired number of data sources.
- **Role** - This identifies the role of the device initiating the frame (**Master** or **Slave**)
- **L2CAP Channel** - The channel number 0 through 78.
  - **L2CAP channel is Multiplexed** - when checked indicates that L2CAP is multiplexed with upper layer protocols.
- **AVDTP is carrying** - Select the protocol that AVDTP traverses to from the following:
  - AVDTP Signaling
  - AVDTP Media
  - AVDTP Reporting
  - AVDTP Recovery
  - -Raw Data-

Adding, Deleting, and Saving AVDTP Parameters

1. From the **Set Initial Decoder Parameters** window, click on the **AVDTP** tab.
2. Set or select the **AVDTP** decoder parameters.
3. Click on the **ADD** button. The Intial Connection window displays the added parameters.

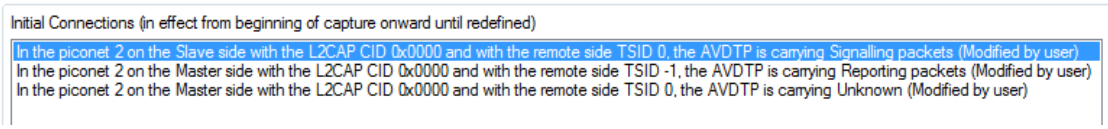


Figure 3.41 - Parameters Added to Decoder

4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and selections and then click on the **Add** button.
6. AVDTP parameters are saved when the template is saved as described in on page 1 on page 1

3.2.3.2 AVDTP Missing Decode Information

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

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

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

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

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

If you are not sure of the payload carried by the subject frame, look at the raw data shown "data" in the **Decoder** pane on the **Frame Display**. You may notice something that hints as to the profile in use.

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

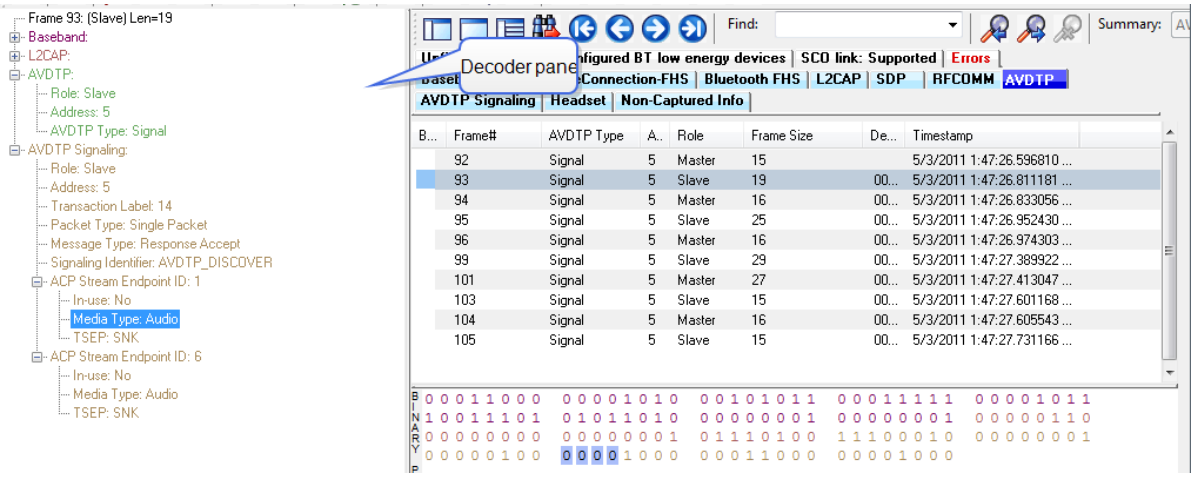


Figure 3.42 - Look in Decoder pane for profile hints

3.2.3.3 AVDTP Override Decode Information

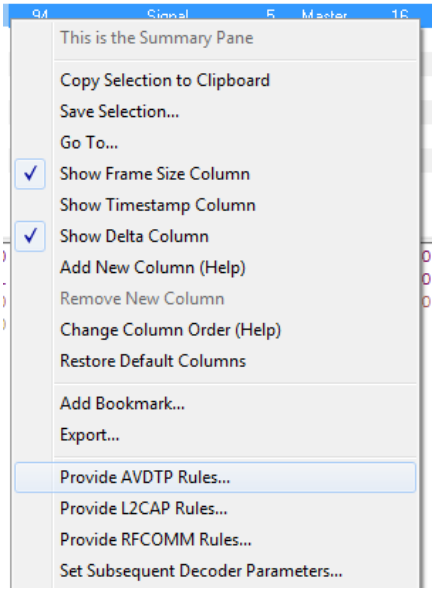
The Set **Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

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

1. Select the frame where the change should take effect.
2. Select **Set Subsequent Decoder Parameters** from the **Options** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.

3. Select the rule you wish to modify from the list of rules.
4. Choose the protocol the selected item carries from the drop-down list, and click **OK**.

If you do not have any previously overridden parameters, you may set parameters for the current frame and onwards by right-clicking the desired frame and choosing **Provide AVDTP Rules...** from the right-click pop-up menu.



If you have a parameter in effect and wish to change it, there are two parameters that may be overridden for AVDTP: **Change the Selected Item to Carry**, and if AVDTP Media is selected. the codec type. Because there are times when vital AVDTP configuration information may not be transferred over the air, we give users the ability to choose between the four AVDTP channel types for each L2CAP channel carrying AVDTP as well as codec type. We attempt to make our best guess at codec information when it is not transferred over the air, but we realize we may not always be correct. When we make a guess for codec type, we specify it in the summary and decode panes by following the codec with the phrase '(best guess by analyzer). This is to let you know that this information was not obtained over the air and that the user may wish to alter it by overriding AVDTP parameters.

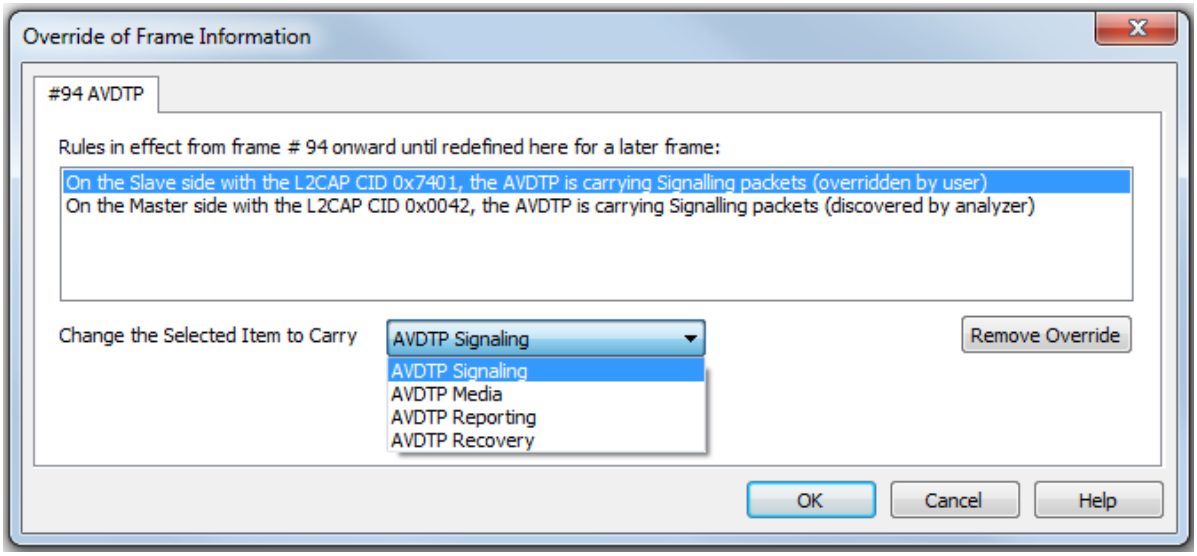


Figure 3.43 - AVDTP Override of Frame Information, Item to Carry

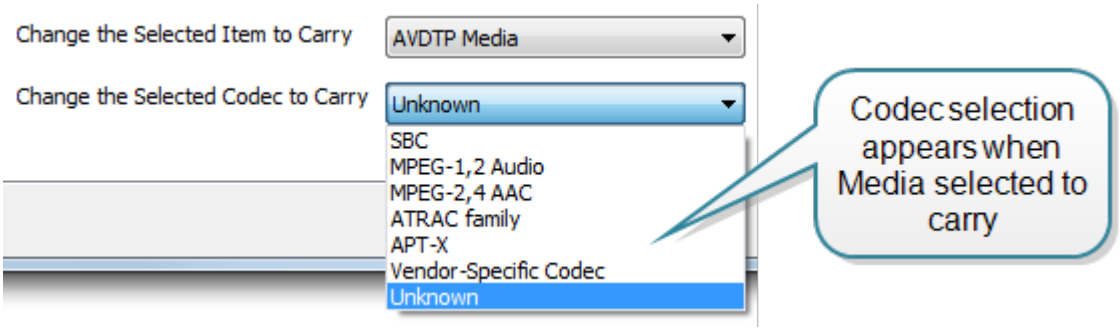
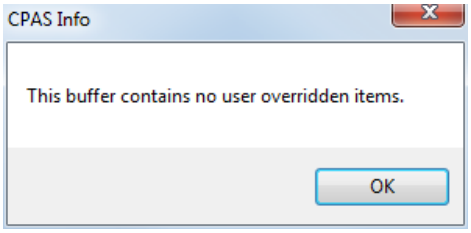


Figure 3.44 - AVDTP Override of Frame Information, Media Codec Selection

Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame. If you are unhappy with your changes, you can undo them by simply choosing your override from the dialog box and pressing the 'Remove Override' button. After pressing 'OK,' the capture file will recompile as if your changes never existed, so feel free to experiment with desired changes if you are unsure of what configuration to use.



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

3.2.4 L2CAP Decoder Parameters

3.2.4.1 About L2CAP Decoder Parameters

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

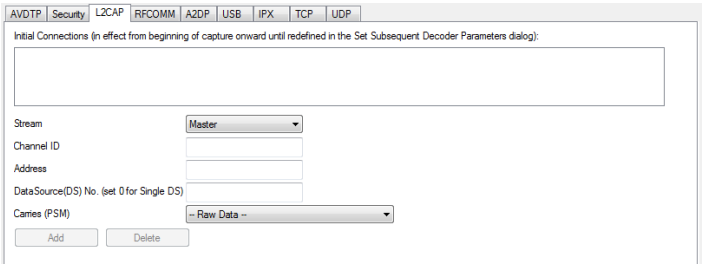
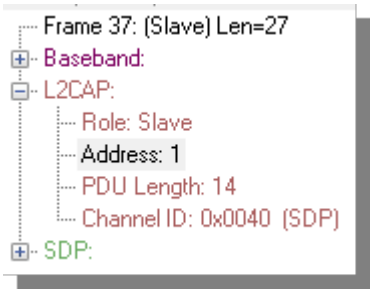


Figure 3.45 - L2CAP Decoder parameters tab

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

- **Stream** - This identifies the role of the device initiating the frame (master or slave)
- **Channel ID** - The channel number 0 through 78

- **Address** - This is the physical connection values for the devices. Each link in the net will have an address. A piconet can have up to seven links. The **Frame Display** can provide address information.



- **Data Source (DS) No.** -When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source number.

Carries (PSM) - Select the protocol that L2CAP traverses to from the following:

- AMP Manager
- AMP Test Manager
- SDP
- RFCOMM
- TCS
- LPMP
- BNEP
- HCRP Control
- HCRP Data
- HID
- AVCTP
- AVDTP
- CMTP
- MCAP Control
- IEEE P11073 20601
- -Raw Data-

Adding, Deleting, and Saving L2CAP Parameters

1. From the **Set Initial Decoder Parameters** window, click on the **L2CAP** tab.
2. Set or select the **L2CAP** decoder parameters.
3. Click on the **ADD** button. The Initial Connection window displays the added parameters.

Initial Connections (in effect from beginning of capture onward until redefined in the Set Subsequent Decoder Parameters dialog):

```
On the Slave side, with CID 0x0000, Address 0, and DataSource 1, L2CAP is carrying AMP Test Manager
On the Master side, with CID 0x0000, Address 0, and DataSource 2, L2CAP is carrying SMP
On the Master side, with CID 0x004e, Address 0, L2CAP is carrying -- Raw Data --
```

Figure 3.46 - Parameters Added to Decoder

4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.

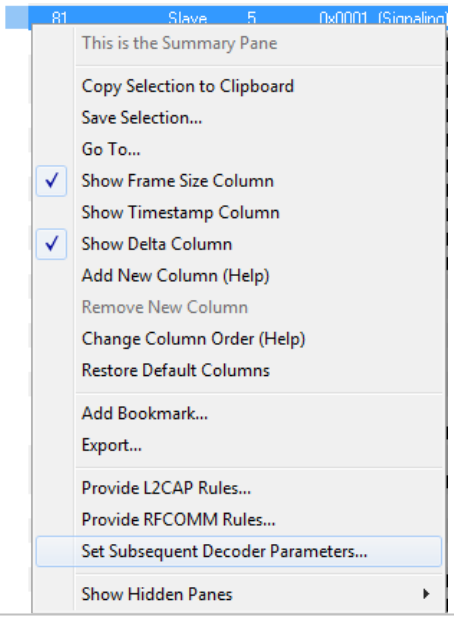
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and selections and then click on the **Add** button.
6. **L2CAP** parameters are saved when the template is saved.

3.2.4.2 L2CAP Override Decode Information

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

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

1. Select the frame where the change should take effect
2. Select **Set Subsequent Decoder Parameters** from the **Options** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes. Refer to
3. Change the L2CAP parameter by selecting from the rule to change, and click on the listed parameters.
4. If you wish to remove an overridden rule click on **Remove Override** button. If you want to remove all decoder parameter settings click on **Remove All**.
5. Click **OK**.



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

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

3.2.5 RFCOMM Decoder Parameters

3.2.5.1 About RFCOMM Decoder Parameters

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

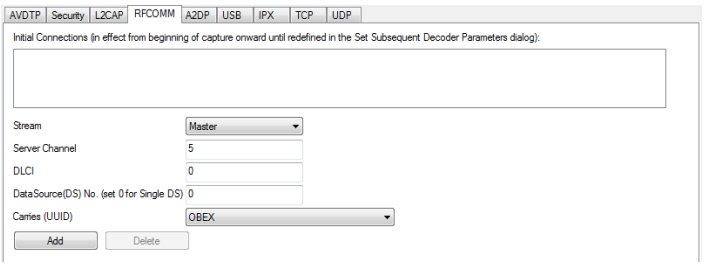


Figure 3.47 - RFCOMM parameters tab

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

- **Stream** - Identifies the role of the device initiating the frame (master or slave)
- **Server Channel** - The Bluetooth® channel number 0 through 78
- **DLCI** - This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server
- **Data Source (DS) No**.- When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- **Carries (UUID)** - Select from the list to apply the Universal Unique Identifier (UUID) of the application layer that RFCOMM traverses to from the following:
    - OBEX
    - SPP
    - encap asyncPPP
    - Headset
    - FAX
    - Hands Free
    - SIM Access
    - VCP
    - UDI
    - -Raw Data-

Adding, Deleting, and Saving RFCOMM Parameters

1. From the **Set Initial Decoder Parameters** window, click on the **RFCOMM**tab.
2. Set or select the **RFCOMM**decoder parameters.
3. Click on the **ADD** button. The Initial Connection window displays the added parameters.

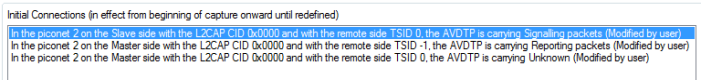


Figure 3.48 - Parameters Added to Decoder

4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and selections and then click on the **Add** button.
6. RFCOMM parameters are saved when the template is saved as described in on page 1

3.2.5.2 RFCOMM Missing Decode Information

ComProbe software usually determines the protocol carried in an RFCOMM payload by monitoring previous traffic. However, when this fails to occur, the **Missing Decoding Information Detected** dialog appears

and requests that the user supply the missing information.

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

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

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

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

If you are not sure of the payload carried by the subject frame, look at the raw data shown under **data** in the **Decode** pane in the **Frame Display**. You may notice something that hints as to the profile in use.

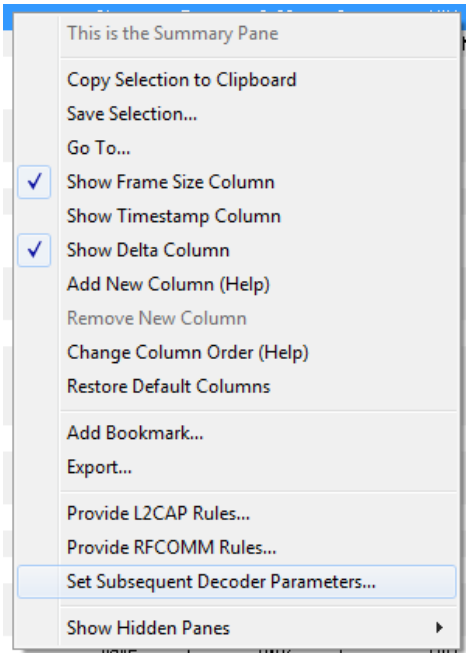
In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.2.5.3 RFCOMM Override Decode Information

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

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

1. Select the frame where the change should take effect, and select **Set Subsequent Decoder Parameters** from the **Options** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
2. Change the RFCOMM parameter by selecting from the **Change the Selected Item to Carry** drop down list.
3. If you wish to remove an overridden rule click on **Remove Override** button. If you want to remove all decoder parameter settings click on **Remove All**.
4. Choose the protocol the selected item carries from the drop-down list, and click **OK**.



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

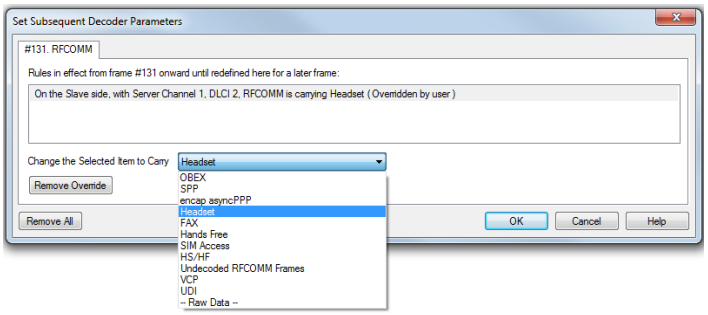


Figure 3.49 - Set Subsequent Decoder Parameters selection list

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

3.3 Mesh Security

Note: The *Bluetooth* SIG is currently in the process of developing specifications for use of *Bluetooth* technology with mesh networking. Any reference to "Smart Mesh" contained herein is only in the context of Frontline software and does not represent SIG approved terminology.

Decryption of *Bluetooth* low energy using mesh networking requires a key or key sets. This information must be manually entered into the MeshOptions.ini file located in the system My Decoders folder. Refer to Changing Default File Locations on page 332 for information on folder locations.

Open a text editor program, such as Windows Notepad, and make the following changes to the MeshOptions.ini file.

For *Bluetooth* technology using mesh networking,

Table 3.19 - *Bluetooth* technology using mesh networking Keys Format

Name	Enter as	Description
Technology Identifier	[mesh]	Identifies the beginning of a set of mesh keys.
Friendly Name		string, 2 word maximum.
IV Index		8 bytes, hexadecimal
Application Key		16 bytes, hexadecimal
Network Key		16 bytes, hexadecimal
Device Key (Optional)		16 bytes, hexadecimal

Note: The Application Key will be substituted for the Device Key when the AFK bit is not set and the Device Key is absent in the MeshOptions.ini file. AKF is the Application Key Flag and is a single bit.

Enter the fields in the order shown and separated by commas. The following code is an example of *Bluetooth* technology using mesh networking decryption key entry. Three mesh keys shown. Note that "Sample5" and "Sample6" keys do not use the optional Device Key.

```
[mesh]
// Key Format - FriendlyName, IV-Index, App Key, Net Key, Dev Key (Optional)
```

Sample1, 00000002, 63964771734fbd76e3b40519d1d94a48,
7dd7364cd842ad18c17c2b820c84c3d6, 63964771734fbd76e3b40519d1d9
Sample5, 01020304, f1a24abea9b86cd33380a24c4dfbe743, efb2255e6422d330088e09bb015ed707
Sample6, 01020304, f1a24abea9b86cd33380a24c4dfbe744, efb2255e6422d330088e09bb015ed708

The Friendly Name is displayed in the summary column of the Mesh tab in the **Frame Display**. This will help the user to filter based on the Friendly Name.

> **Note:** "Unknown Network" will be displayed when the given key set(s) defined in MeshOptions.ini is unable to decrypt a certain frame.

For CSRmesh,

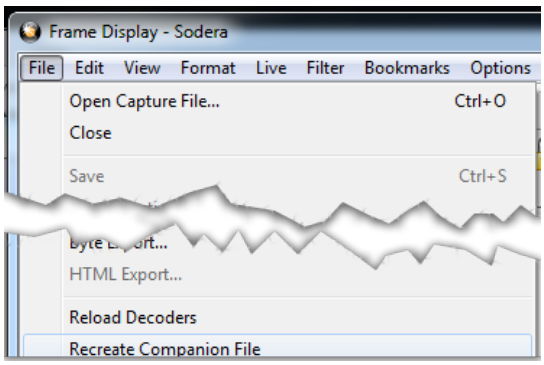
Table 3.20 - CSRmesh Key Set Format

Name	Enter as	Description
Technology Identifier Tag	[CSRmesh]	Required to differentiate from [mesh]. Software will only look for keys after this tag, ignoring comments. Case insensitive within the brackets.
Key set	Name, passphrase	Comma separated: Name = the network name. passphrase = the network key. If not present a key is not necessary.

The following code is an example of CSRmesh decryption key set entry.

```
[csrmesh]
// Format: My Network, My Password //My Comments
MySampleHome, Password
test
Test Home 1, test1
TestHome2, test2
BT, bluetooth
BT1, bluetooth1
BT2, bluetooth2
```

Loading keys or key sets



When the Frontline software is initially loaded, keys or the key sets will be automatically read from the MeshOptions.ini file. If the keys or the key sets are modified while the Frontline software is running, decoders must be reloaded and the companion files must be recreated for the change to take effect. Follow these steps to reload the decoders.

1. In the Frame Display, click on the Reload Decoders icon , or select **Reload Decoders** from the **File** menu.
2. From the **File** menu, select **Recreate Companion Files**.

CSRmesh in Sodera

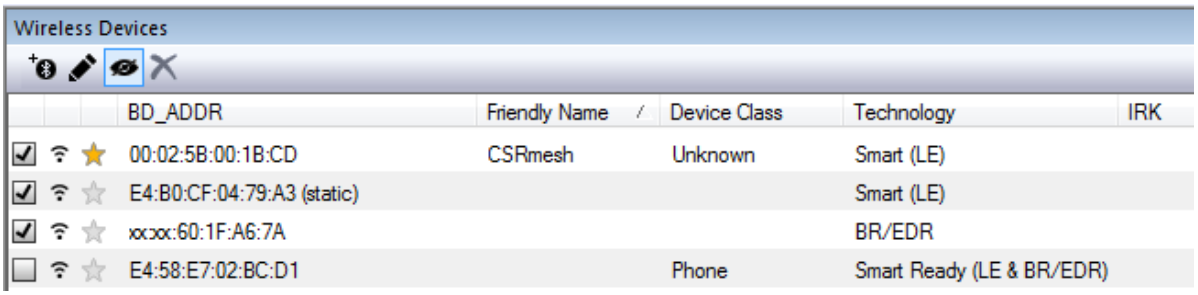
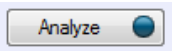


Figure 3.50 - Sodera Wireless Devices pane with CSRmesh device

CSRmesh bridge address usually has a Friendly Name of “CSRmesh”.

Many phone stacks ignore repeated adverts from the same BD_ADDR. To ensure reception, In CSRmesh, BD_ADDR changes after every transmission. The new BD_ADDR used is random and a Non Resolvable Private Address .

A live capture cannot decode CSRmesh information contained in the random BD_ADDR. However, they can be reanalyzed by selecting the CSRmesh device for analysis by checking the check box and clicking on the **Analyze** button 

.

CSRmesh over GATT

ATT maintains a database which maps handles & UUIDs. When there is a connection request the mappings will be loaded to the initiator and/or advertiser sides of the database.

Phones can bypass pairing process for pre-paired devices. In this case, handle/UUID can be mapped by brute force using ATT_Handle_UUID_PreLoad.ini file. This file is to be placed in the root of My Decoders Folder.

For additional information refer to Bluetooth low energy ATT Decoder Handle Mapping on page 342.

Mesh in the Frame Display

In the **Frame Display** Summary pane, Mesh tabs appear for MTP, MASP, and MCP. The **CSRMesh MTP** tab displays the MASP and MCP protocols in the Summary pane.

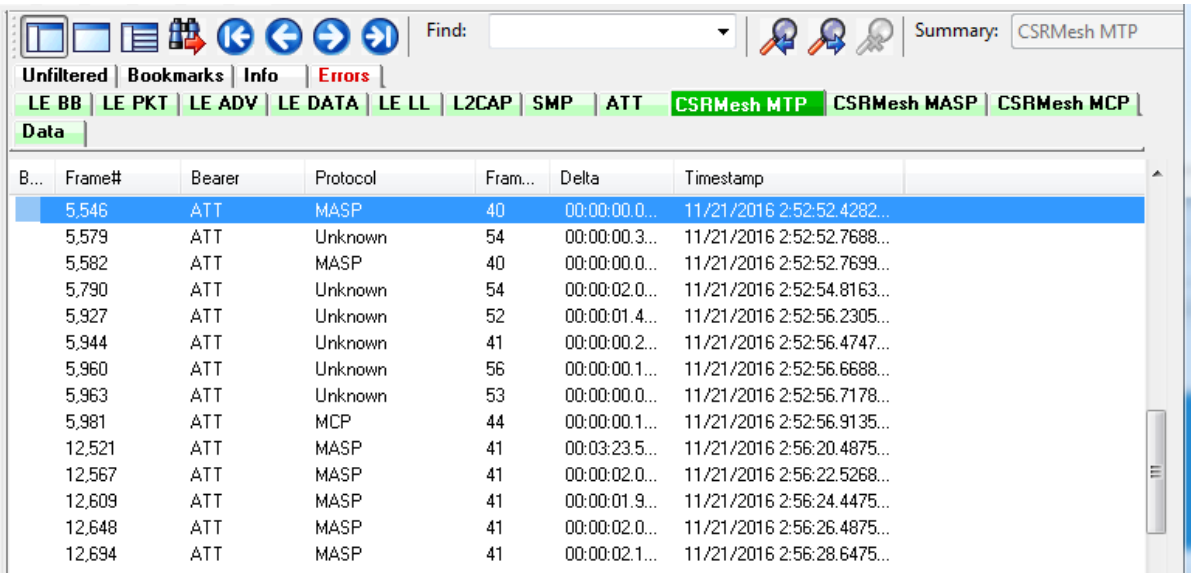


Figure 3.51 - CSRMesh MTP tab Summay pane display

The bearer can be "ATT" or "LE", and the protocols detected can be "MASP", "MCP", or "Unknown". When the MTP tab displays "Unknown" in the **Protocol** column it means

- that the Generated MAC does not match the Received MAC in the packet,
- that there is not a key set to decrypt the payload.

The CSRMesh MASP tab is shown in CSRMesh MSRP tab with Decoder pane inset on page 87 shows the Decoder pane (inset) with the "Network Info" passphrase and network key shown but there is no network name.

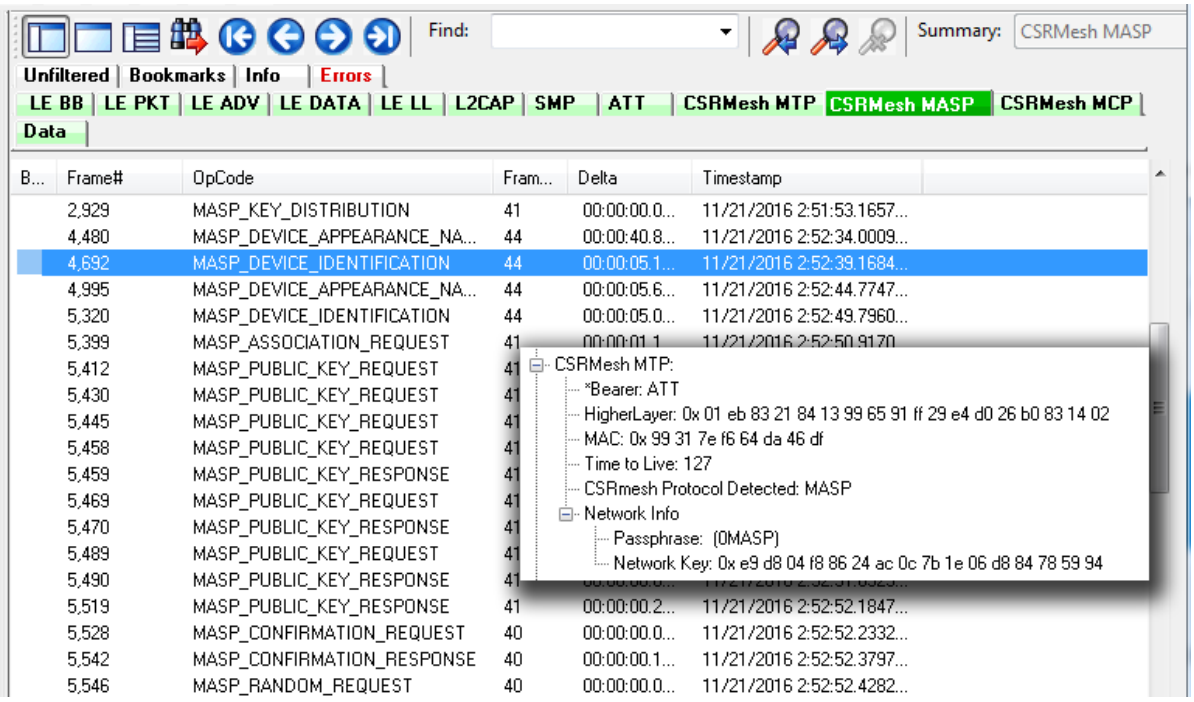


Figure 3.52 - **CSRMesh MSRP** tab with Decoder pane inset

The CSRMesh MCP tab is shown in CSRMesh MCP tab with Decoder pane inset on page 88 shows the Decoder pane (inset) with the "Network Info" passphrase and network key and network name shown. The network name appears in the Network column of the Summary pane.

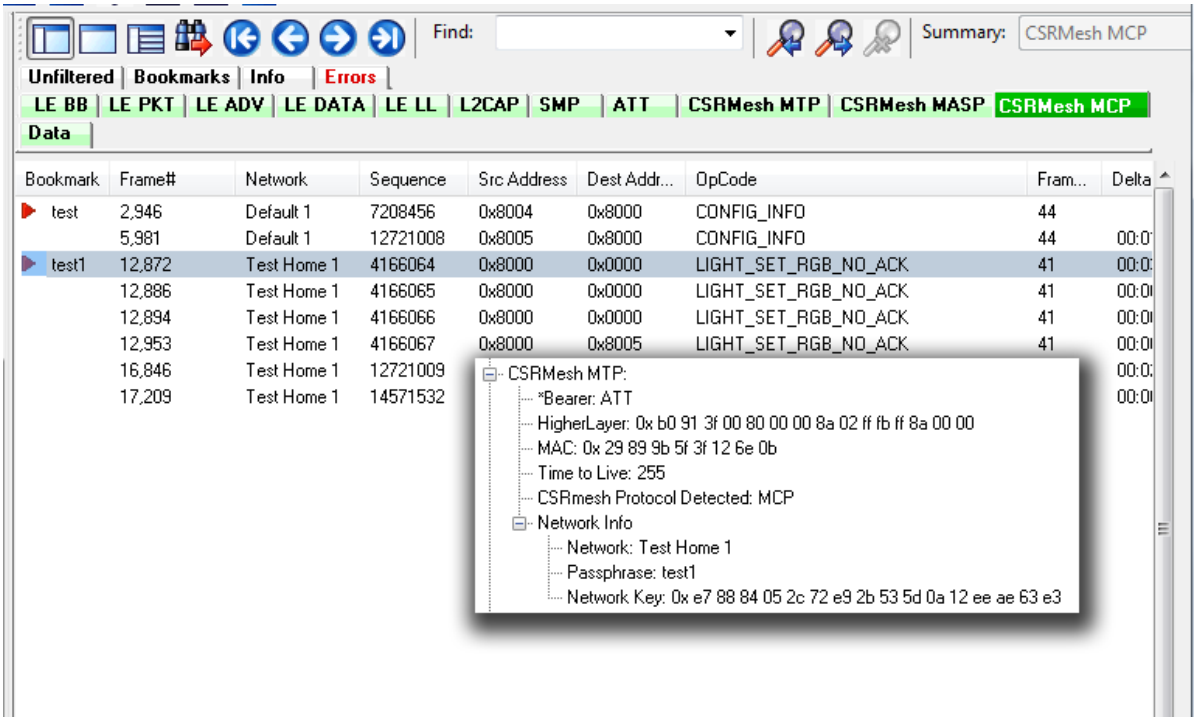


Figure 3.53 - **CSRMesh MCP** tab with Decoder pane inset

Troubleshooting Tips

MeshOptions.ini Errors

Table 3.21 - Errors Associated with MeshOptions.ini

Error Displayed	Descripton
Error: IV Index should be 8 bytes	The IV Index read from MeshOptions.ini is not 8 bytes.
Error: App Key should be 16 bytes	The App Key read from MeshOptions.ini is not 16 bytes
Error: Net Key should be 16 bytes	The Net Key read from MeshOptions.ini is not 16 bytes
Error: Bad Format. Expected (Name, IVI, App, Net, Dev)	Something is wrong with formatting (Can be missing Friendly Name or missing IV Index, missing App Key,r missing Net key, or missing commas ‘,’).
Error: MeshOptions.ini file not found	The file cannot be located

CSRmesh Errors

a. Incorrect key set

- When the key set entered in MeshOptions.ini is incorrect, most of the Mesh Transport Protocol frames will contain *Mesh Protocol Detected: Error*.
- The term “Most” is used because it excludes Mesh Association Protocol (MASP) packets. MASP packets use a constant Passphrase of 0x00 || MASP.

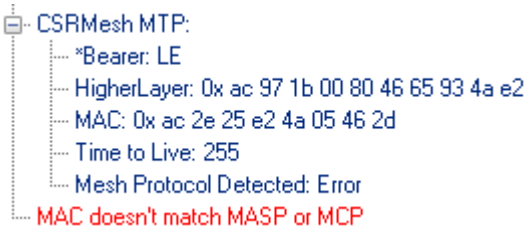


Figure 3.54 - CSRmesh Bad MAC

- An error message will also be displayed, saying “MAC doesn’t match MASP or MCP”.

  This error simply means that the generated MAC does not match the received MAC. This error will also be generated in the case of a bad packet

b. Decryption Error

- The error message associated with a decryption error will say "Decryption Error".

c. Payload Size

- MTL payload<=9 bytes (MAC+TTL)
  - This error is implying that the Mesh Transport Layer (MTL or MTP) has a payload of less than 9 bytes.
  - Message Authentication Code (MAC) is 8 bytes and Time to live (TTL) is 1 byte.
- HML payload is not available
  - This error indicates that MTP payload contains MAC and TTL but HLM payload is missing or is 0 bytes.
- MCP data has no encrypted payload
  - This error indicates that the MCP payload contains the nonce (sequence number and source address) but encrypted payload is missing from the packet.

Bluetooth technology using mesh networking Errors

Table 3.22 - Errors: Bluetooth technology using mesh networking

Error	Description
"Reserved" Opcode	This is most likely the scenario when incorrect keys have been entered. Correct the keys in the MeshOptions.ini file and reload decoders.
Possible error in net decryption	Possible error in net decryption
Possible error in app decryption	Possible error in app decryption

3.4 Conductive Testing

Conductive testing could be used for many reasons, but the most common use is to isolate the Set in Target test setup from the surrounding environment. Interference from radio frequency (RF) sources is the most common reason for isolating the test from the environment. This is especially important when the environment contains RF sources using the industrial, scientific, and medical (ISM) radio bands from 2.4 to 2.485 GHz that are the bands used for Set in Target.

“Conductive” in this context means that you are not “air sniffing”, that is, capturing Set in Target transmissions on the Frontline analyzer's antenna. The conductive test setup uses coaxial cable to directly connect the

Device Under Test (DUT) to the analyzer's antenna connectors. The coaxial cable provides the isolation from the environment through shielding.

3.4.1 Classic *Bluetooth* Transmitter Classes

Classic *Bluetooth* transmitters are categorized by power classes, that is, by the amount of RF power output. A *Bluetooth* Class maximum operating range is directly related to the power output. The class is important in conductive testing because the DUTs and the Frontline unit are connected directly to each other, usually over small distances. The absence of power loss , which occurs during over-the-air transmission, means that larger than normal power levels may be present at the receiving port. Attenuation may be necessary to protect both the DUT and the Frontline unit from excessive power input and to ensure reliable operation.

Classic Bluetooth Power Classes below lists the maximum power and operating range for each Classic *Bluetooth* Class.

Table 3.23 - Classic *Bluetooth* Power Classes

Class	Maximum Power	Operating Range
1	100 mW (20 dBm)	100 meters
2	2.5 mW (4 dBm)	10 meters
3	1 mW (0 dBm)	1 meter

Caution: Good engineering judgment is essential to protecting both the Frontline low energy protocol analyzer and the devices under test from power levels that could cause damage. The procedures contained here are general guidelines for connecting the equipment for conductive testing.

3.4.2 *Bluetooth* low energy Transmitter

A *Bluetooth* low energy device maximum operating range is directly related to the power output. The power output is important in conductive testing because the DUTs and the Frontline unit are connected directly to each other, usually over small distances. The absence of power loss, which occurs during over-the-air transmission, means that larger than normal power levels may be present at the receiving port. Attenuation may be necessary to protect both the DUT and the Frontline unit from excessive power input and to ensure reliable operation.

Bluetooth low energy Transmitter below lists the maximum power and operating range for *Bluetooth* low energy transmitters.

Table 3.24 - *Bluetooth* low energy Transmitter

Bluetooth SIG Specification	Maximum Power	Operating Range
Up to 4	10 dBm (5 mW)	50 meters

Caution: Good engineering judgment is essential to protecting both the Frontline low energy protocol analyzer and the devices under test from power levels that could cause damage. The procedures contained here are general guidelines for connecting the equipment for conductive testing.

3.4.3 Sodera Conductive Testing

Test Equipment

While exact conductive test setups are dependent on the specific circumstances surrounding the DUT (Device Under Test) RF interface, the following equipment is required for most testing situations.

1. Coaxial cable with adapter for connecting to DUT 1.
2. Coaxial cable with adapter for connecting to DUT 2.
3. Coaxial T-connector.
4. SMA adapters for connecting coaxial cable or attenuators to the ComProbe antenna connectors.
5. Attenuators, values depending on the *Bluetooth* technology or DUT power output levels.
6. Sodera Wideband *Bluetooth* Protocol Analyzer.
7. Personal computer for running Frontline software.

Configure the Sodera Unit

To protect the DUTs and the Sodera hardware, it is essential to understand the DUT power output. As a starting point for conductive testing the Sodera hardware should be configured for a lower sensitivity.

1. With the Sodera unit connected to the personal computer with Frontline software running, select **Capture Options** from the **Options** menu.
2. In the **Capture Options** Settings check the **Radio** section box **Reduce RF sensitivity (20 dB reduction)**. This selection will place a 20 dB attenuator in the path of the antenna jack.

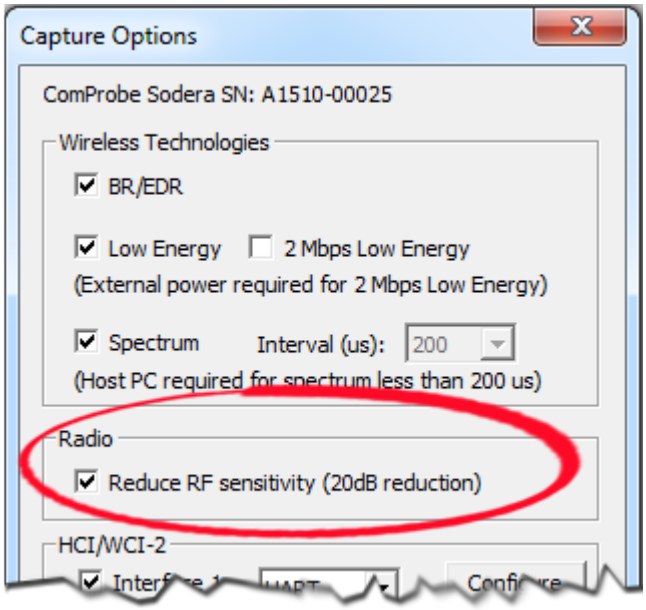


Figure 3.55 - Sodera **Capture Options** dialog **Radio** setting option

3. Click the **OK** button and the settings will be saved to the connected Sodera hardware.
4. This is a cautionary first step, but reducing the Sodera hardware sensitivity may place too much attenuation in the signal path. Should the capture results prove to be ineffective try removing the attenuator to increase the Sodera hardware sensitivity.

Test Setup

Figure 3.56 on the next page shows the conductive test setup. The values of AT1, AT2, and AT3 depend on the power transmitted by DTU 1 and DTU 2. If the Sodera unit was configured for reduced sensitivity, then AT3 may not be necessary.

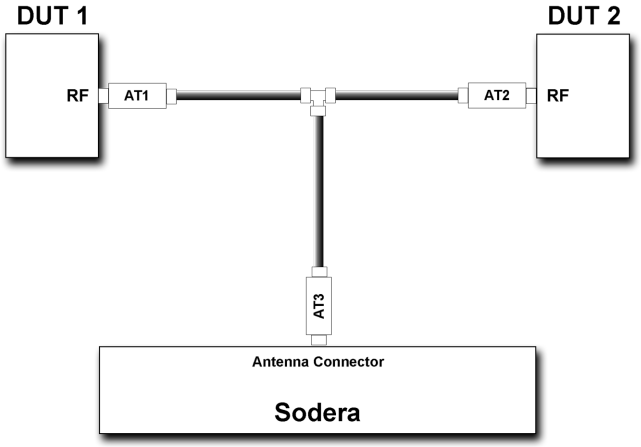


Figure 3.56 - Sodera Conductive Test Setup

The AT1 through AT3 attenuator values will depend on the DUT1 and DUT2 transmitter Class or the transmit power from each device. At higher power levels all three attenuators may be needed. In all cases, use good engineering practices to protect the devices under test and the Sodera hardware from damage, and to ensure reliable operation.

For example, assume that there is no attenuation in the test setup:

- At the T-connector the power will split in half. For example, if DUT1 is a Class 1 device transmitting +20 dBm (100 mW), at the T-connector it will split with +17 dBm (50 mW) going to DUT2 and +17 dBm (50 mW) going to the Sodera antenna connector. Adding additional attenuation with AT1, AT2, AT3, and the **Capture Options Radio** selection will further reduce theinput power level to the Sodera.radio.
- If DUT1 or DUT2 is a Class 2 device, +10 dBm (12.5 mW) will reach the Sodera antenna connector. If they are Class 3 devices, -3 dBm (0.5 mW) will reach the antenna connector.

If the protocol analysis results prove to be unreliable, adjust the AT1, AT2, or AT3 values and the Sodera **Capture Options Radio** settings to achieve reliable results.

3.4.4 *Bluetooth* Conductive Test Process

After connecting DUT1, DUT2, and the Frontline *Bluetooth* protocol analyzer hardware, follow these steps to capture *Bluetooth* data.

1. Pair DUT 1 and DUT 2.
2. Establish data transmission between DUT 1 and DUT 2.
3. Begin capture of the data with the Frontline protocol analyzer.
4. Conduct protocol analysis with the Frontline software on the personal computer or save the capture file for future analysis.

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 Air Sniffing: Positioning Devices

When capturing over the air packets, proper positioning of the Frontline hardware and the Devices Under Test (DUTs) will result in the best possible captures and will mitigate sources of path loss and interference. The following procedures will help optimize the capture process especially if you are have problems obtaining reliable …captures.

Problems with indoor radio propagation

Even in free space, it is well understood that radio frequencies attenuate over distance. The free-space rule-of-thumb dictates that radio energy decreases in strength by 20 dB by each 10-to-1 increase in range. In the real-world, the effects of objects in an outdoor environment cause reflection, diffraction, and scattering resulting in greater signal losses. Indoors the situation can be worse. Reflections occur from walls and other large flat surfaces. Diffraction occurs from objects with sharp edges. Scattering is produced from objects with rough surfaces and from small objects. Also any object directly in the path of the radiation can present a hard or soft partition depending on the partition's material properties. Path losses from partitions are difficult to estimate.

Estimating indoor propagation loss

One estimate of indoor path loss, based on path loss data from a typical building, provides a $\frac{1}{range^{3.5}}$ power rule. At 2.4 GHz, the following relationship provides an approximate estimate of indoor path loss:

$$\text{Indoor Path Loss (in dB)} = 40 + 35Log_{10}(\text{range, in meters})$$

This approximation is expected to have a variance of 13 dB.

Mitigating path loss and interference

Bluetooth device design contributes to mitigating environmental effects on propagation through spread spectrum radio design, for example. However, careful planning of the testing environment can also contribute to reliable data capture process.

The first step to ensuring reliable air-sniffing data capture is to understand the RF characteristics of the Devices Under Test (DUTs). The *Bluetooth* Class, antenna types, and radiation patterns are all important factors that can affect the placement of the DUTs and the Frontline hardware. Radiation patterns are rarely spherical, so understanding your device's radiation patterns can greatly enhance successful data capture. Position devices to avoid radiation attenuation by the surroundings.

This step is optional: Consider conductive testing to establish a baseline capture. Conductive testing isolates the DUTs and analyzer from environmental effects.

The next step is to ensure that the testing environment is as clutter-free as possible.

- Line-of-sight obstructions should be eliminated between the Frontline hardware and the DUTs because they cause a reduction in signal strength. Obstructions include, but are not limited to: water bottles, coffee cups, computers, computer screens, computer speakers, and books. A clear, unobstructed line-of-sight is preferred for DUT and Frontline hardware positioning.
- If using an analyzer connected to a computer, position the computer on an adjacent table or surface away from the analyzer and DUTs, taking advantage of the cables' length. If this is not possible, position the computer behind the analyzer as far away as possible. If using the Frontline FTS4BT, which is a dongle, either use an extension USB cable or position the computer such that the dongle is positioned towards the DUTs.
- The preferred placement is positioning the DUTs and the Frontline hardware at the points of an equilateral triangle in the same horizontal plane, i.e. placed on the same table or work surface. The sides of the triangle should be between 1 and 2 meters for *Bluetooth* transmitter classes 1 and 2. The distance for transmitter class 3 should be 1/2 meter.

Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane

Finally, eliminate other RF sources.

- Wi-Fi interference should be minimized or eliminated. *Bluetooth* shares the same 2.4 GHz frequency bands as Wi-Fi technology. Wi-Fi interference can cause loss of packets and poor captures. In a laboratory or testing environment do not place the DUTs and Frontline hardware in close proximity with Wi-Fi transmitting sources such as laptops or routers. Turning off Wi-Fi on the computer running the Frontline software is recommended.

Positioning for wideband capture

Frontline's Wideband Bluetooth Protocol Analyzer, Sodera, can capture from multiple devices, which requires a different approach to position the DUTs and the analyzer. When testing more than two devices arrange the DUTs on the perimeter of a circle 1-2 meters in diameter for Bluetooth transmitter Class 1 and 2 devices. For transmitter Class 3 DUTs, the circle should be 1/2 meter in diameter. Equally space the DUTs on the perimeter. Place the Sodera in the center of the circle. If not using the Sodera Excursion mode, connect the computer and place it outside the circle as far away from the DUTs as possible.

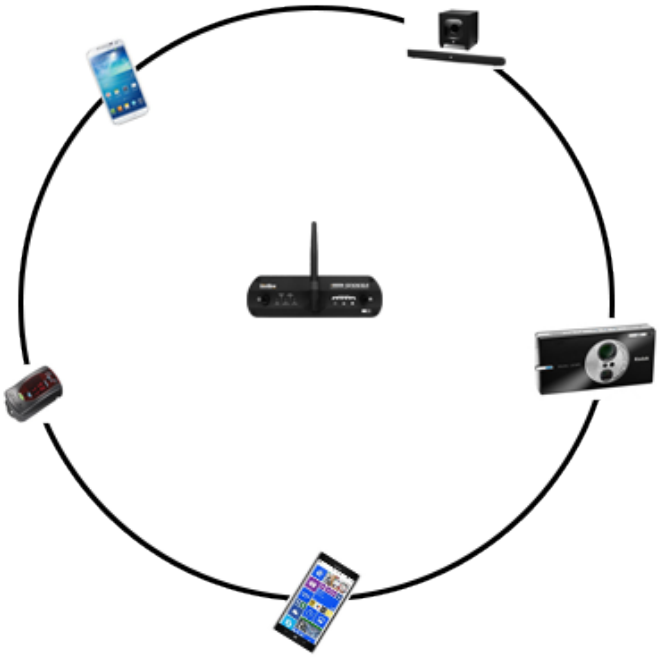


Figure 4.2 - Wideband Capture: Devices Equally Spaced in the Same Horizontal Plane

Positioning for audio capture

The Bluetooth Audio Expert System provides analysis of audio streams and can assist in identifying problems with capture methods including positioning and environment because it will point out missing frames. For hands-free profile data captures both DUTs send and receive data. Therefore, position the devices following the equilateral triangle arrangement as mentioned above.

However, in A2DP data capture scenario, the equilateral positioning of devices is not optimum because, normally, only one device is sending data to the other. It is recommended that the Frontline hardware be positioned closer to the device receiving data so that Frontline better mimics the receiving DUT. Position the DUTs 1 -2 meters apart for Class 1 and 2 transmitters, and 1/2 meter apart for Class 3 transmitters.

Figure 4.3 - For Audio A2DP, Position Closer to SINK DUT

Poor Placement

A poor test configuration for the analyzer is placing the DUTs very close to each other and the analyzer far away. The DUTs, being in close proximity to each other, reduce their transmission power and thus make it hard for the analyzer to hear the conversation. If the analyzer is far away from DUTs, there are chances that the analyzer may miss those frames, which could lead to failure in decryption of the data.

Obstacles in close proximity to or in between the analyzer and the DUTs can interfere and cause reduction in signal strength or interference. Even small objects can cause signal scattering.

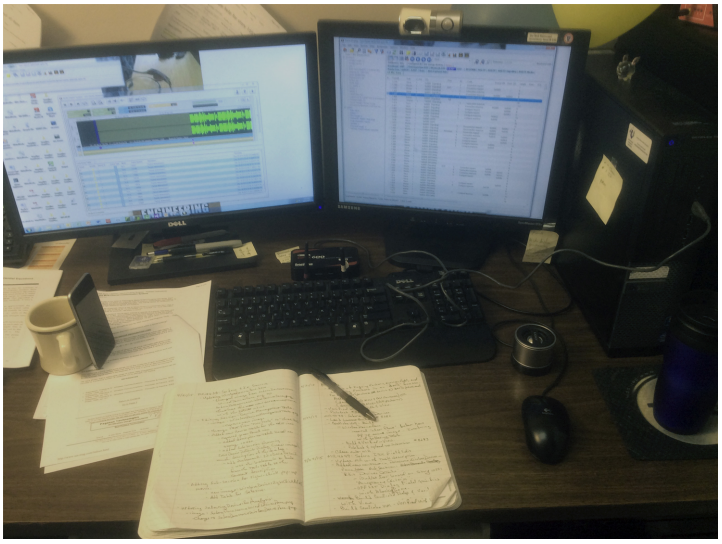


Figure 4.4 - Example: Poor Capture Environment

4.1.2 Sodera Capturing Data: Introduction

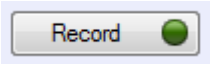
Data capture using Sodera hardware will capture data from all devices with active connections within range of the analyzer. Once a session is started, the capture is initiated and the data is recorded. The analysis mode can begin. The user must select specific devices. The user can select from all devices that are actively

communicating. The user can also select devices from a prior capture, when available, before recording. The data captured only from selected devices is sent to the Frontline software for event- and protocol-level analysis.

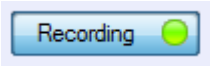
4.1.2.1 Sodera: Record—Begin Capture

When starting a capture session

- the active status of all devices is cleared in the **Wireless Devices** and **Wired Devices** panes ,
- the **Security** pane is emptied, and
- the **Event Log** pane retains all prior logged events.



On the Capture Toolbar, click on the **Record** button, or select **Record** from the **Capture** menu option. When the **Record** button changes to **Recording**, Sodera hardware is capturing data from all active *Bluetooth* devices within range and is recording data on the PC.



On the Capture Toolbar, clicking on the **Recording** button, or selecting **Recording** from the Capture menu options will halt live capture.

The **Wireless Devices** and **Wired Devices** pane populates with any newly discovered devices. Selecting devices for analysis can be done while recording.

> **Note:** The Capture Toolbar **Analyze** button will be grayed out until some wireless devices have been selected for analysis.

The **Security** pane will show all encrypted *Bluetooth* links.

The **Event Log** pane will begin to populate with information, warnings, and error messages.

The **Status Bar** will show a running total of captured packets.

> **Note:** Starting a new capture session will clear all unsaved data from both the Sodera hardware and the Frontline software. If it has not been saved, then a pop-up warning message will appear.

4.1.2.2 Sodera: Selecting Devices for Analysis

Once a Sodera capture session starts by clicking on **Record** on the Capture Toolbar, data from all active devices within range or data from wired connections is being captured. To analyze the data using the Frontline software, you select specific devices of interest to include in the analysis.

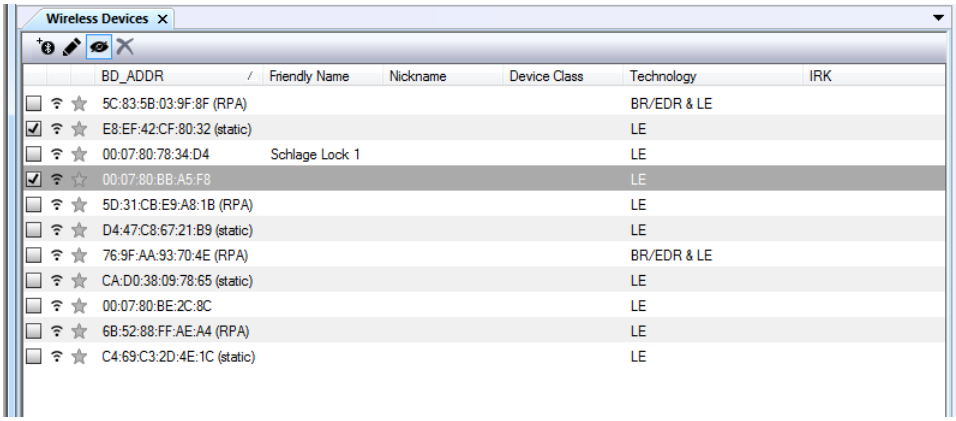


Figure 4.5 - Sodera Wireless Devices Pane

In the **Wireless Devices** and **Wired Devices** pane, place a check in the row of each active device / to be analyzed. Active devices can also be selected while the recording is in process.

> **Note:** Data filtered by the device selection is an "OR" function, not an "AND" function. When selecting device1, device2, device3,… the recorded data filtered into the analyzer is data involving device1 OR device2 OR device3 OR …. However, if in the Options menu, analysis if LE Empty packets is selected an AND function is included. For example: (device2 AND LE Empty packets) OR (device3 AND LE Empty packets).

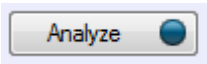
The following table lists some common data capture and device selection scenarios.

Table 4.1 - Common Data Capture and Device Selection Scenarios

Scenario	Wireless Devices Pane Selection
Analyzing traffic between a slave Device Under Test (DUT) and its master.	Select only the slave DUT for analysis
Analyzing all traffic on a piconet	Select the Master for analysis
Analyzing all traffic involved in Inquiries	In the **Sodera** Options menu select **Analyze Inquiry Process Packets** in the **Options** menu

The Sodera is now ready to begin protocol- and event-level analysis.

4.1.2.3 Sodera: Starting Analysis



The analysis begins by clicking on the **Analyze** button, or selecting **Analyze** from the **Capture** menu. Alternatively, click on the **Start Analyze** button In the **Control** window. The Sodera hardware will begin sending captured packets involving the selected device to the Frontline software.

Once analysis has begun, you cannot change the device selection. All device rows in the **Wireless Devices** and **Wired Devices** pane are grayed-out. To stop the analysis, click on the **Analyzing** button. You can then change your device selection and restart analysis by clicking on the **Analyze** button.

To stop the Analysis click on the **Analyzing** button or click on the **Control** window **Stop Analyze** button .

Conducting analysis from a capture file is identical to the live capture method.

4.1.2.4 Sodera: Hardware Signal Too Strong Indication

When the Frontline software has detected an RF signal that is *too strong*, warnings will appear in several places.

- Event Log Pane on page 66 - Displays "Received Signal too Strong" with a Warning icon . The event is added to the log as soon as the conditions for a *too strong* signal have been detected. A signal that is *too strong* can cause errors in the decoding process.

  Caution: The Sodera unit will continue to capture after a *too strong* signal detection, which may compromise the decoded packet integrity.

- Status Bar (see Sodera Datasource Window on page 32) - Displays "SIGNAL TOO STRONG".

> **Note:** These warnings will occur only in live capture mode. No visual indications will occur in capture file playback or in excursion mode playback.

Conditions for "too strong" RF signal

For the Sodera hardware, the Frontline software will determine that a received signal is *too strong* based on the following conditions.

- Normal Gain **Capture Options** setting (see Menu on page 33)- 5 or more packets with RSSI greater than or equal to -20 dBm within the past 5 seconds.
- Reduced Gain **Capture Options** settings (see Menu on page 33) - 5 or more packets with RSSI greater than or equal to -0.5dBm or higher within the past 5 seconds.

Signal too Strong reset

When the Frontline software has determined that the RF signal has returned to a *safe* condition from a *too strong* condition, the following will occur.

- Event Log Pane on page 66 - Displays "Received Signal Strength OK" with an Information icon .

  The event is added to the log as soon as the conditions for a *safe* signal have been detected.

- Status Bar - No display of signal strength.

Conditions for Signal too Strong reset

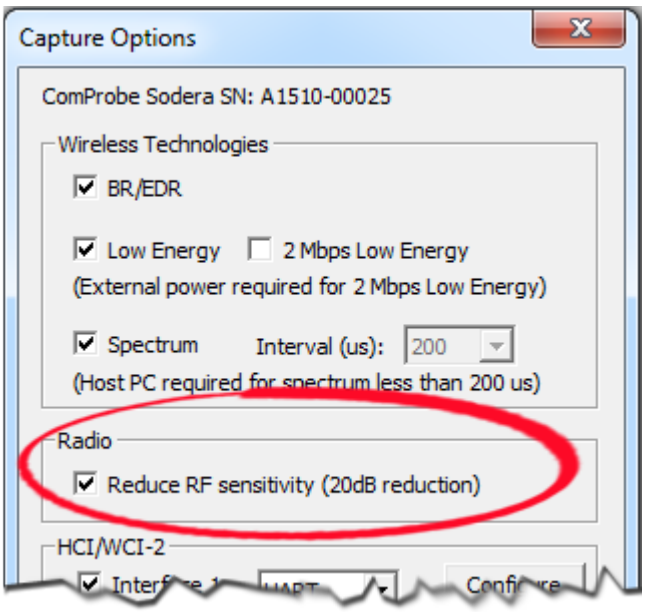
The software will determine that a *too strong* signal has returned to a *safe* status based on the following conditions.

- Normal Gain **Capture Options** setting (see Menu on page 33)- No packets with RSSI greater than -24 dBm within the last 5 seconds.
- Reduced Gain **Capture Options** settings (see Menu on page 33) - No packets with RSSI greater than -4.5 dBm within the last 5 seconds.

Suggested Corrective Action

The device under test (DUT) may be too close to the Sodera unit. Try moving the DUT further away from the Sodera antenna. Try capturing again.

With a persistent Signal too Strong indication, try checking the **Radio Reduced RF Sensitivity (20 db reduction)** from the **Capture Options...** selection of the **Options** menu. This selection will reduce the incoming RF level at the Sodera unit by 19.5 dB. Try capturing again.



4.1.2.5 Sodera: Excursion Mode Capture & Analysis

Capturing data in Excursion mode is accomplished without the Sodera hardware being connected to a computer. The captured data is stored on the Sodera hardware for later access and analysis when connected to a computer.

The Sodera hardware must be configured for Excursion mode while connected to a computer running the ComProbe Protocol Analysis System. Refer to Menu on page 33

Excursion mode Data Capture

To capture in Excursion mode, disconnect the Sodera hardware from the computer.

1. Apply power to Sodera with external power or using the internal battery power. See Applying Power on page 7.
2. Press the Capture button on the Sodera front panel (right side). The **Capture** LED will illuminate a steady green light when capturing data.

To stop capturing data,

1. Press the Capture button on the Sodera front panel.
2. After a brief delay, the **Capture** LED will turn off. The capture file is saved to the Sodera hardware.

Starting a new capture will save the captured data in a new capture file.

Limitations to Excursion mode Capture

The only limitations to Excursion mode capture are:

- Battery life - the internal battery has a one-hour operating life. In the case of capture periods exceeding one hour, connect the Sodera hardware to an external power source.
- Internal memory - the Sodera hardware has 32 GBytes of internal storage that is used to hold Excursion mode captures. This storage can be managed using the ComProbe Protocol Analysis System on a computer.

- Number of Excursion mode captures - there can be no more than 255 Excursion mode captures stored on the Sodera hardware. Refer to Manage excursion mode captures dialog on page 35 for instruction on how to delete Excursion mode capture files from the Sodera unit.

Analyzing Data from Excursion mode Capture

The procedure for protocol analysis of data captured in Excursion mode involves connecting the Sodera hardware to a computer, recording a capture that was previously stored on that hardware unit, and analyzing the data using the ComProbe Protocol Analysis System.

1. Connect the Sodera hardware that contains the excursion mode capture to be analyzed, to a computer.
2. Apply power to the Sodera hardware.
3. Open the ComProbe Protocol Analysis System.
4. When the **ComProbe Sodera** window opens, select **Manage excursion mode captures...** from the **File** menu.
5. When the **Manage excursion mode captures...** dialog opens, select a capture to analyze. Click on the **Record** button, and the dialog will close. Sodera will begin behaving identically to how it handles a live capture. The ComProbe Sodera window Wireless Devices and Security pane will populate with information from the selected Excursion mode capture.
6. Follow the procedures in Sodera: Selecting Devices for Analysis on page 97.
7. Follow the procedures in Sodera: Record—Begin Capture on page 97.

4.1.2.6 Sodera & 802.11: Capturing with ProbeSync

ProbeSync allows Frontline Sodera and 802.11 hardware to work seamlessly together and to share a common clock. Clock sharing allows the analyzers to precisely synchronize communications streams and to display resulting packets in a single shared view.

When configured for synchronization through ProbeSync, one Sodera device provides the clock to the other device. The clock is provided by a provided CAT 5 cable between the master Sodera **PROBESYNC OUT** connector—sending the synchronizing clock—to the slave device hardware ProbeSync **IN** connector—receiving the clock.

When the Frontline software runs in ProbeSync mode, only the Sodera Control window and Sodera datasource window will appear. Should the hardware be connected incorrectly, that is **IN** to **IN** or **OUT** to **OUT**, an error message will appear in the Event Log pane.

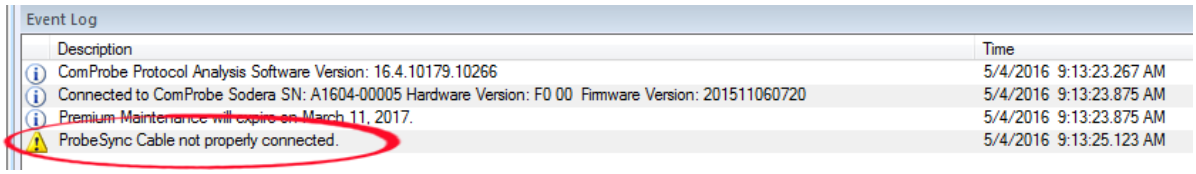


Figure 4.6 - Incorrect ProbeSync Hardware Connection Message

The Sodera datasource window **Record** button initiates the capture for both devices.

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 during analysis will include data captured on both devices.

4.1.2.7 Sodera: Spectrum Analysis

Sodera has the option to sample the 2.4 GHz RF spectrum at the Sodera unit antenna connector. The spectrum data represents the Received Signal Strength Indicator (RSSI) and is automatically saved when the capture is saved.

The spectrum data is synchronized in time to the received packets and is displayed in the Coexistence View 2.4 GHz Timeline when **Show Spectrum** is selected in the **Spectrum** menu on the **Coexistence View**. The spectrum power level is shown as a "heat map" behind the timeline packets. The "heat map" appears in shades of blue with darker blues representing higher power levels and lighter blues representing lower power levels (white represents the lowest power level). The darkest shade of blue represents -15dBm and above, while white represents -100 dBm and below.

> **Note:** Too strong of a signal level is detected and noted in the Events Log pane. See Sodera: Hardware Signal Too Strong Indication on page 99 for more information.

Spectrum data appearing in the **Coexistence View Timeline** that is not synchronized to a packet may indicate the presence of RF interference. Interference has the potential to degrade the *Bluetooth* signal.

The spectrum can be sampled at 20, 50, 100, or 200 microseconds. The Spectrum option and sample rate is set in the **Capture Options...** of the **Options** menu. Refer to Menu on page 33 for information on capture settings. Smaller sample rate will cause an increase in memory used. However, identifying potential sources of interference may require more samples to avoid missing a signal.

> **Note:** For Spectrum sample intervals less than 200 microseconds, the Sodera unit must be connected to a computer.

The spectrum data is saved automatically when the capture is saved. The saved spectrum data file has the file extension .swsd with the same basename as the .cfa file and in the same directory. (See Changing Default File Locations on page 332 for information on default file locations.)

Currently, if a user opens a capture file and chooses to save the capture under a different name, a new.swsd file will not be created (this will change in an upcoming release).

When copying capture files (.cfa, .scap, etc.) to a different directory, the user must also copy the spectrum data file (.swsd). If the spectrum data file is not present at the time the capture file is opened, spectrum data will not be available in the **Coexistence View**.

4.1.2.8 Sodera: Critical Packets and Information for Decryption

After two Bluetooth devices are paired and Sodera has captured data, the Frontline software requires certain packets and information for successful post capture decryption.

BR/EDR Legacy Encryption (E0)

The following information and packets are needed to follow decryption:

- Link Key
- Full Master BD_ADDR, Full Slave BD_ADDR
- All packets from the last authentication (master or slave) before encryption starts (LMP_au_rand, and LMP_sres)
- LMP_en_rand, negotiated LMP_encryption_key_size,

- LMP_start_encryption_req, LMP_accepted(LMP_start_encryption_req)
- LMP_stop_encryption_req, LMP_accepted(LMP_stop_encryption_req)

BR/EDR Secure Encryption (AES)

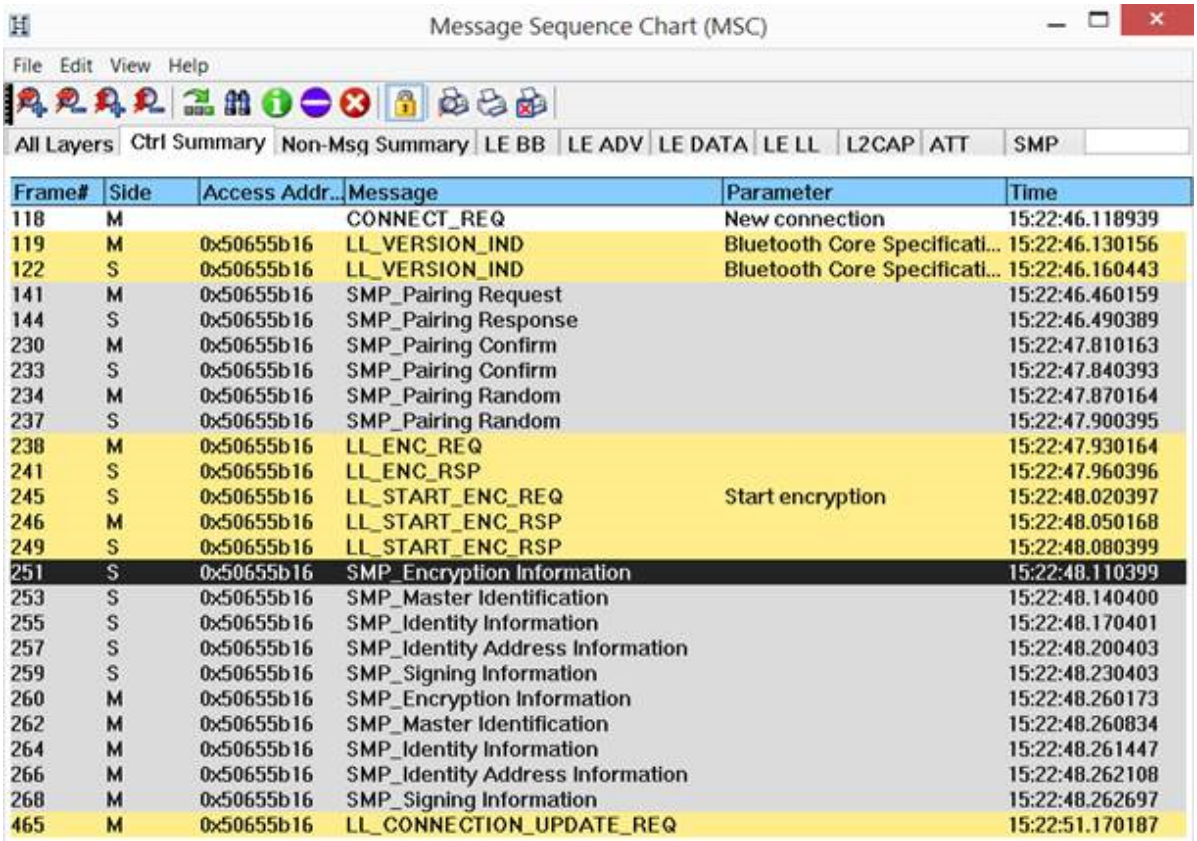
The following information and packets are needed to follow decryption:

- Link Key
- Full Master BD_ADDR, Full Slave BD_ADDR
- Complete mutual authentication (LMP_au_rand from the master and slave as well as LMP_sres from the master and slave)
- Negotiated LMP_encryption_key_size
- LMP_start_encryption_req, LMP_accepted(LMP_start_encryption_req)
- LMP_pause_encryption_aes_req (if pausing and resuming AES encryption)
- LMP_stop_encryption_req, LMP_accepted(LMP_stop_encryption_req)

Bluetooth low energy Encryption (AES)

The following information and packets are needed to follow decryption:

- Long-Term Key (LTK)
- LL_ENC_REQ, LL_ENC_RSP
- LL_START_ENC_REQ, LL_START_ENC_RSP
- LL_PAUSE_ENC_REQ, LL_PAUSE_ENC_RSP



Frame#	Side	Access Addr...	Message	Parameter	Time
118	M		CONNECT_REQ	New connection	15:22:46.118939
119	M	0x50655b16	LL_VERSION_IND	Bluetooth Core Specificati...	15:22:46.130156
122	S	0x50655b16	LL_VERSION_IND	Bluetooth Core Specificati...	15:22:46.160443
141	M	0x50655b16	SMP_Pairing Request		15:22:46.460159
144	S	0x50655b16	SMP_Pairing Response		15:22:46.490389
230	M	0x50655b16	SMP_Pairing Confirm		15:22:47.810163
233	S	0x50655b16	SMP_Pairing Confirm		15:22:47.840393
234	M	0x50655b16	SMP_Pairing Random		15:22:47.870164
237	S	0x50655b16	SMP_Pairing Random		15:22:47.900395
238	M	0x50655b16	LL_ENC_REQ		15:22:47.930164
241	S	0x50655b16	LL_ENC_RSP		15:22:47.960396
245	S	0x50655b16	LL_START_ENC_REQ	Start encryption	15:22:48.020397
246	M	0x50655b16	LL_START_ENC_RSP		15:22:48.050168
249	S	0x50655b16	LL_START_ENC_RSP		15:22:48.080399
251	S	0x50655b16	SMP_Encryption Information		15:22:48.110399
253	S	0x50655b16	SMP_Master Identification		15:22:48.140400
255	S	0x50655b16	SMP_Identity Information		15:22:48.170401
257	S	0x50655b16	SMP_Identity Address Information		15:22:48.200403
259	S	0x50655b16	SMP_Signing Information		15:22:48.230403
260	M	0x50655b16	SMP_Encryption Information		15:22:48.260173
262	M	0x50655b16	SMP_Master Identification		15:22:48.260834
264	M	0x50655b16	SMP_Identity Information		15:22:48.261447
266	M	0x50655b16	SMP_Identity Address Information		15:22:48.262108
268	M	0x50655b16	SMP_Signing Information		15:22:48.262697
465	M	0x50655b16	LL_CONNECTION_UPDATE_REQ		15:22:51.170187

Figure 4.7 - Bluetooth low energy Critical Decryption Packets, Message Sequence Chart

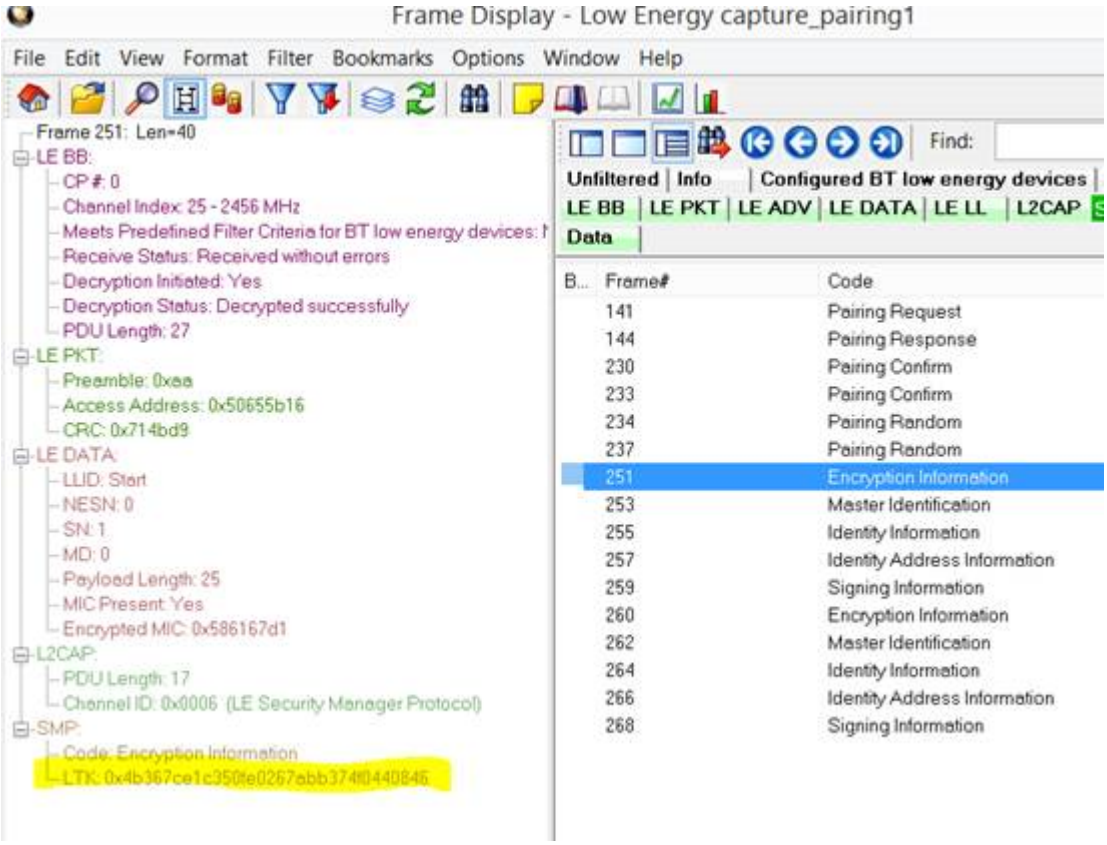


Figure 4.8 - Bluetooth low energy Critical Decryption Packets, Frame Display

4.1.2.9 Capturing Sodera Analyzed Data to Disk

> **Note: Record** is not available in Viewer mode. **Analyze/Analyzing** is available in Viewer mode, allowing different analyses to be performed on previously recorded and saved captures.

1. Click the **Record** Record button on the Standard Toolbar. Sodera will begin capturing data from all wireless devices within range and from all connected wired devices.
2. In the **Wireless Devices** and **Wired Devices** pane select the active devices for analysis
3. Click on **Analyze** Analyze button , or click the **Start Analyze** button to begin capturing to a file. This **Start Analyze** button is located on the **Control** window, **Event Display**, and **Frame Display**.
4. 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.
5. 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.
6. Click the **Analyzing** button, or click the **Stop Analyze** button to stop analyzing. .

7. To clear captured data, click the **Clear** icon .

- If you select **Clear** after stopping analysis, 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.

4.1.3 Extended Inquiry Response

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

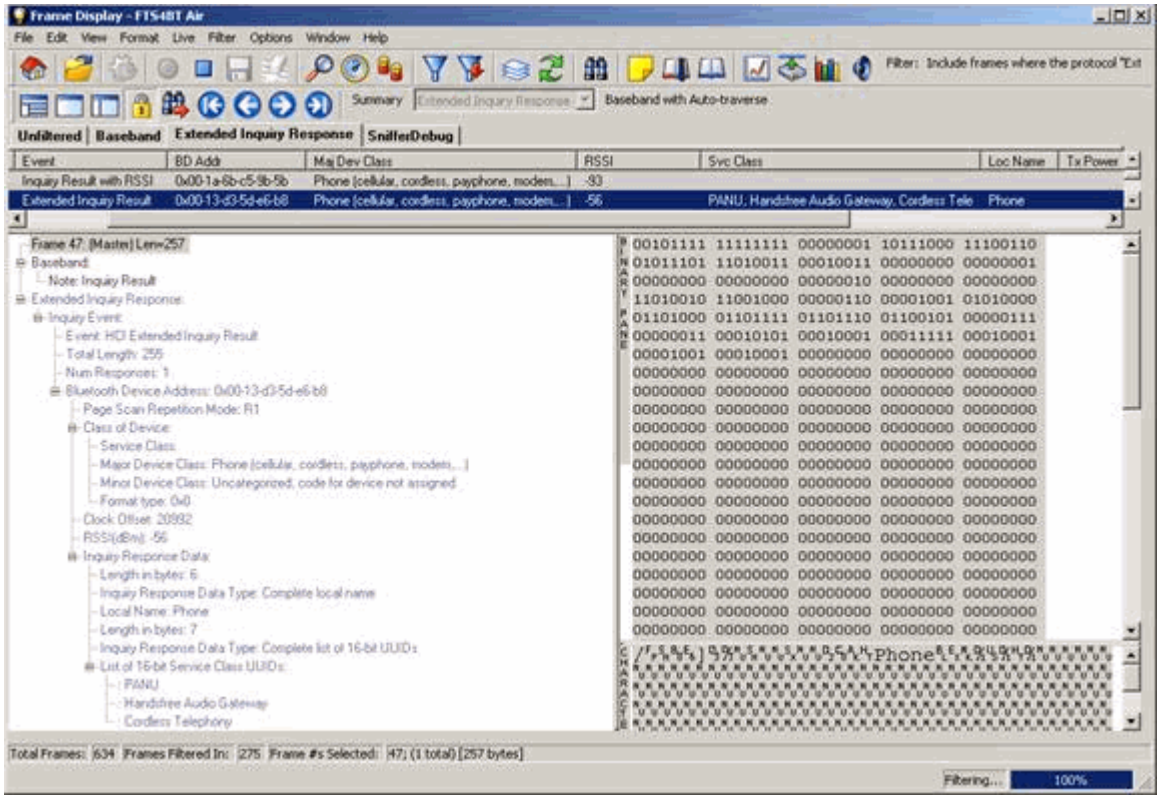


Figure 4.9 - Frame Display Extended Inquire Response

EIR displays extensive information about the Bluetooth® devices that are discovered as data is being captured. EIR provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode. Before the EIR

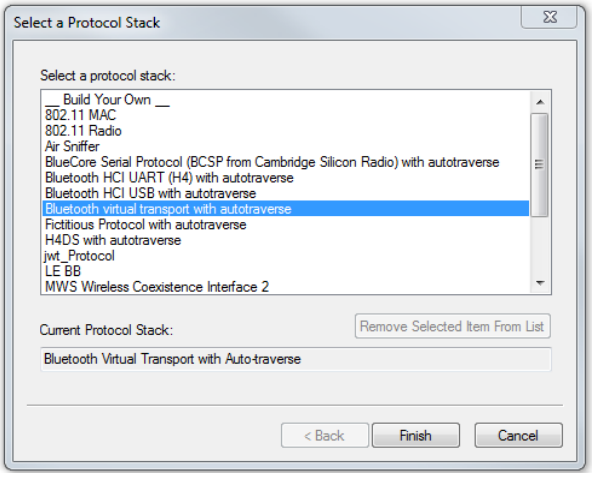
tab was created, this type of information was not available until a connection was made to a device. Therefore, EIR can be used to determine whether a connection can/should be made to a device prior to making the connection.

> **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 108.

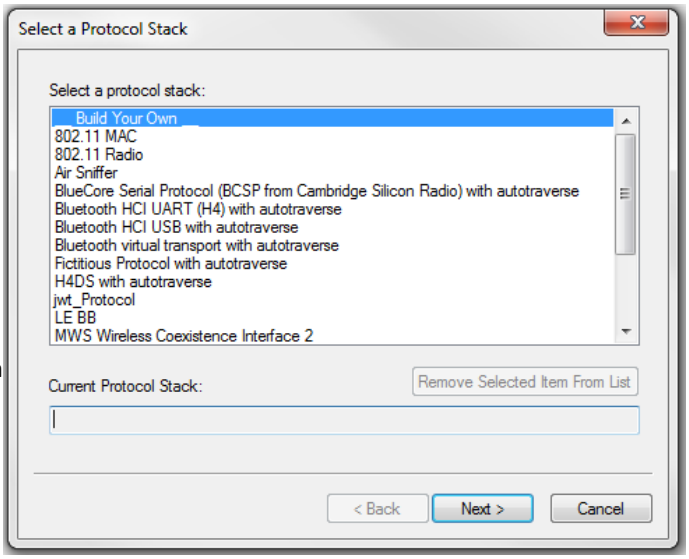
1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the **Remove Selected Item From List** button becomes active.
2. Click the **Remove Selected Item From List**button to remove the stack from the list. You cannot remove stacks provided with the analyzer. If you remove a custom stack, you need to define it again in order to get it back.

If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing on page 109 for more information.

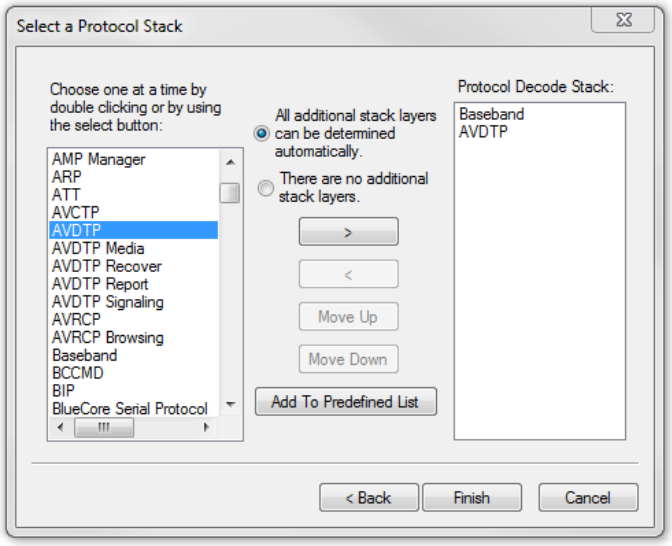
You cannot select a stack or change an existing one for a capture file loaded into the Capture File Viewer (the Capture File Viewer is used only for viewing capture files and cannot capture data). Protocol Stack changes can only be made from a live session.

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 .

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 109 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 109 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 Protocol Decodes

4.3.1 The Frame Display

To open this window

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

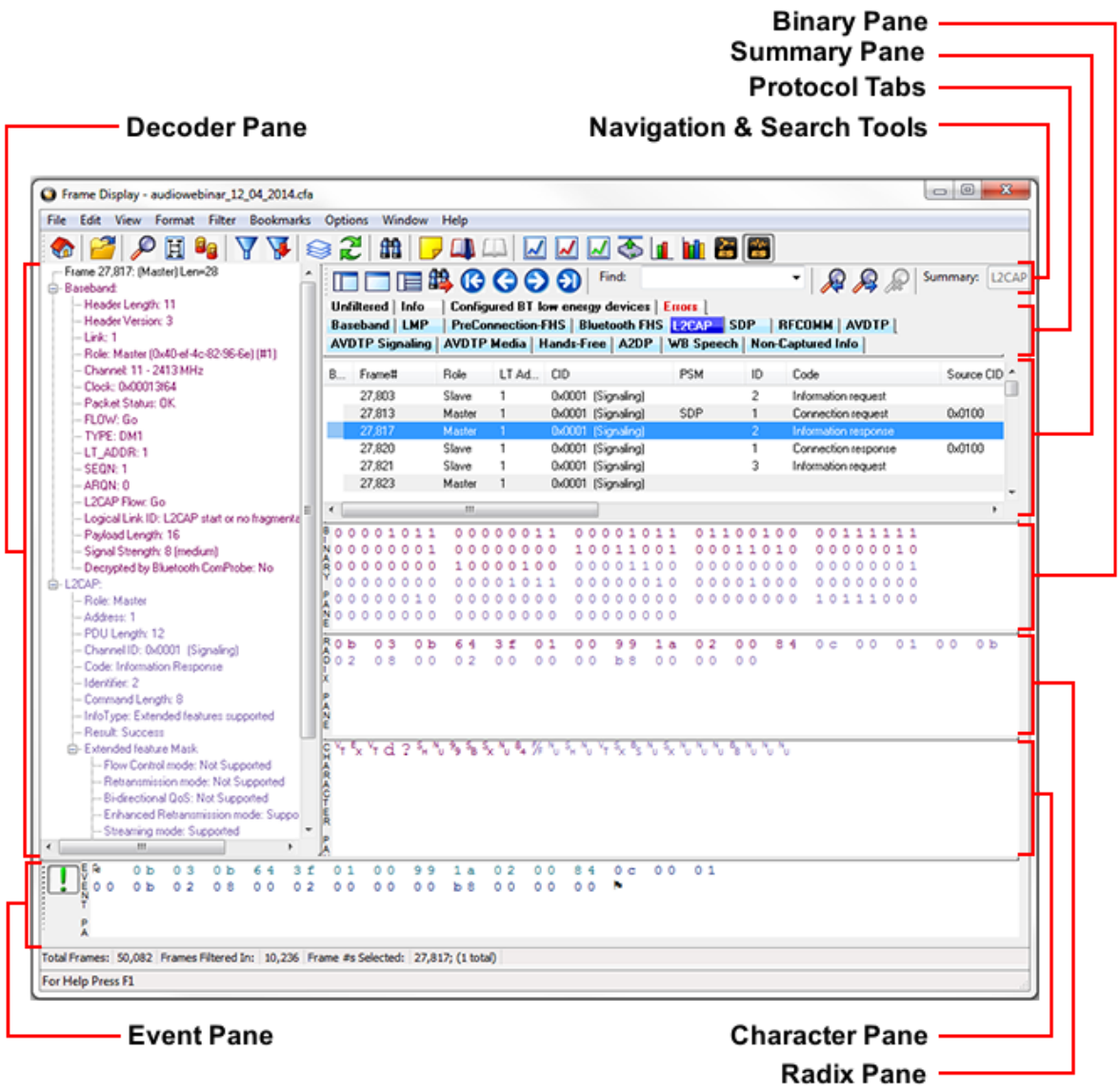


Figure 4.10 - Frame Display with all panes active

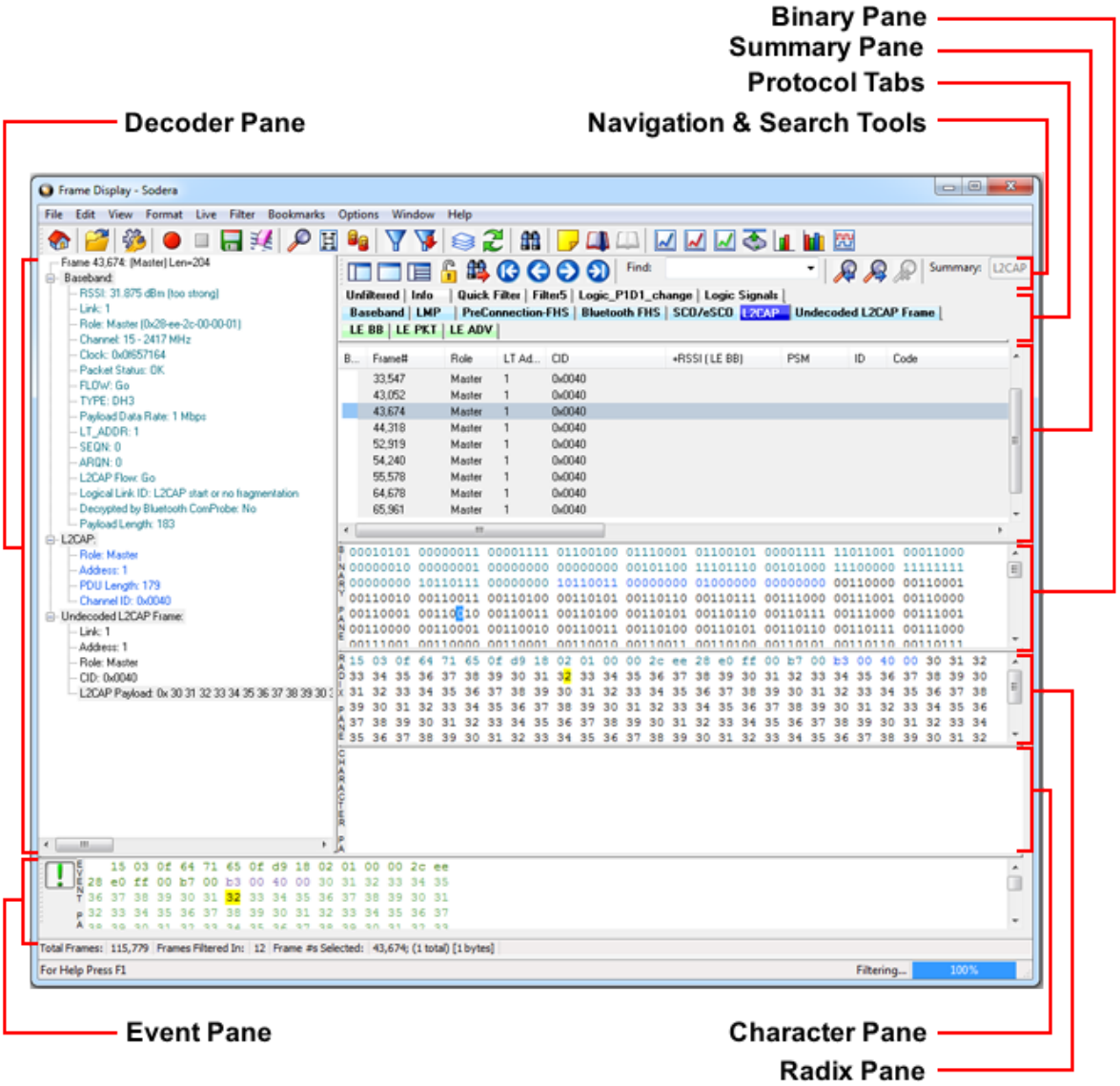


Figure 4.11 - Frame Display with all panes active

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.

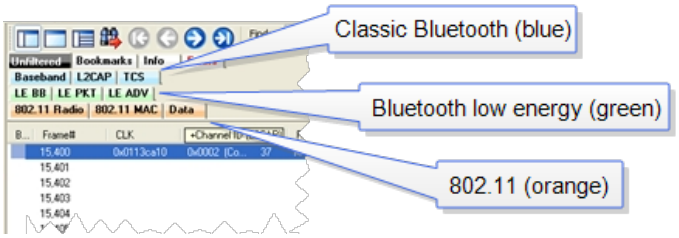
- Character Pane - The **Character Pane** displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.
- Event Pane - The Event Pane displays the physical data bytes in the frame, as received on the network.

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".

4.3.1.1 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.

Table 4.2 - Frame Display Toolbar Icons

Icon	Description
	Control – Brings the Control window to the front.
	Open File - Opens a capture file.
	I/O Settings - Opens the I/O Settings dialog.
	Start Analyze- Begins data analysis..
	Stop Analyze- Stops the analysis and clears the data from the ComProbe analyzer.
	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.
	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

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
	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.
	Bluetooth Expert System - Opens Bluetooth Expert System window
	Audio Expert System - Opens Audio Expert System Window
	Logic Analyzer - Opens the logic analyzer used for logic signal and packet timing analysis.
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:	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.

Table 4.2 - Frame Display Toolbar Icons(continued)

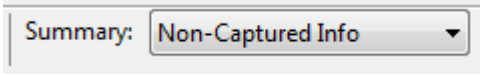
Icon	Description
	Shall All Panes Except Event Pane - Makes the Decode pane taller and the Summary pane narrower.
	Toggle Display Lock - Prevents the display from updating.
	Go To Frame
	First Frame - Moves to the first frame in the buffer.
	Previous Frame - Moves to the previous frame in the buffer.
	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. 

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
	Text with Protocol Stack: To the right of the Summary Layer box is some text giving the protocol stack currently in use. Summary: Non-Captured Info Baseband with Auto-traverse

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.

4.3.1.2 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

4.3.1.3 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 S**et Protocol Filtering** button and un-check the layer or layers you want revealed.

4.3.1.4 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.

4.3.1.5 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.

4.3.1.6 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.

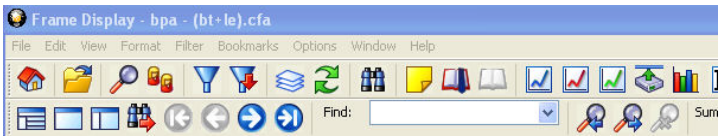


Figure 4.12 - Frame Display Find text entry field

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.,

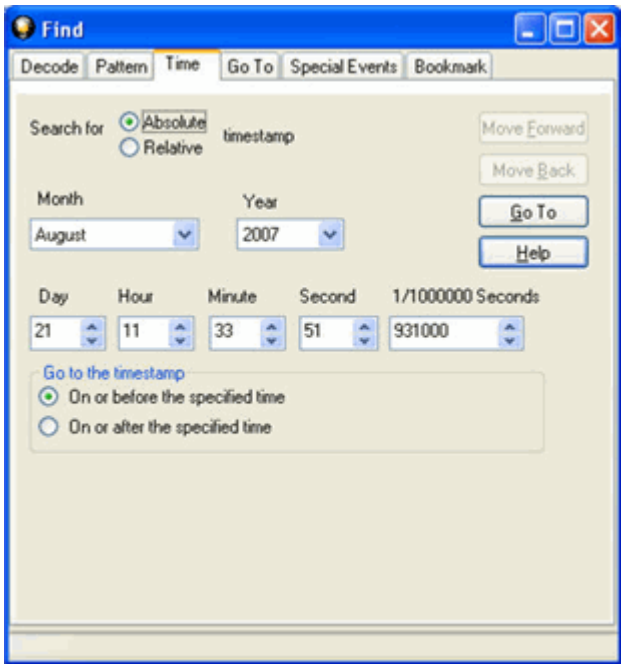


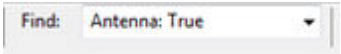
Figure 4.13 - Search/Find Dialog

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

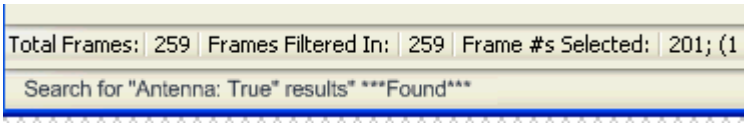
Select **Find Previous Occurrence** to begin the search on frames prior to the frame you selected, or **Find Next Occurrence** to begin the search on frames following the frame you selected.

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

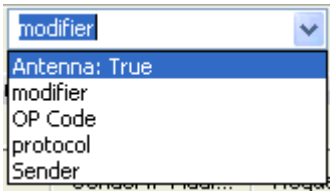
4. Select **Find Previous Occurrence** or **Find Next Occurrence** to continue the search.

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.

4.3.1.7 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.

4.3.1.8 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 the other **Frame Display**. You must use the Hide/Reveal feature to display a filter created in one Frame Display in another.

> **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.

4.3.1.9 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.

4.3.1.10 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...**.

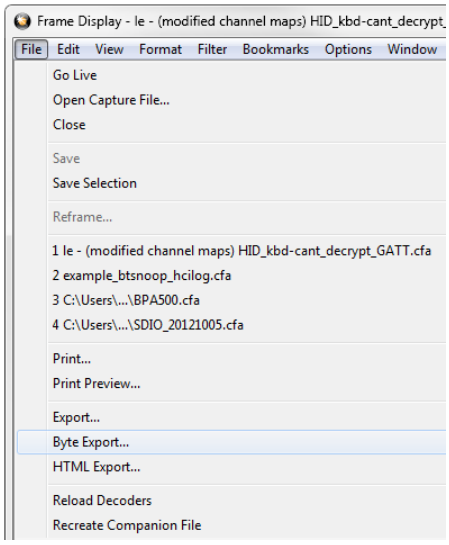


Figure 4.14 - Frame Display File menu, Byte Export

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.

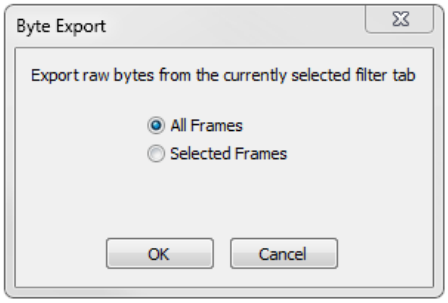


Figure 4.15 - Byte Export dialog

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.

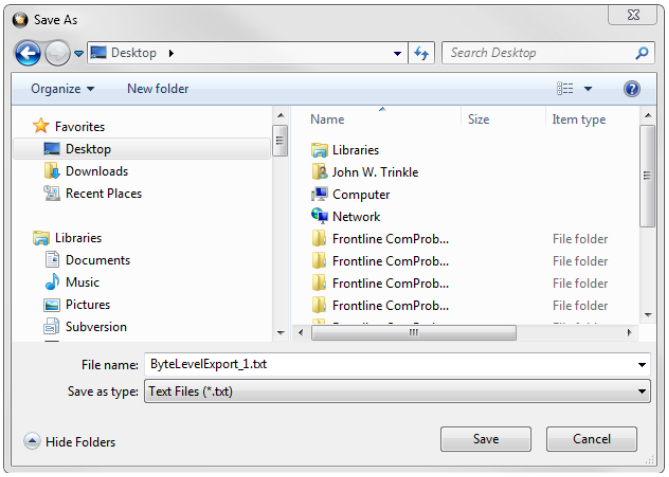


Figure 4.16 - Save As dialog

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 file name, 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.

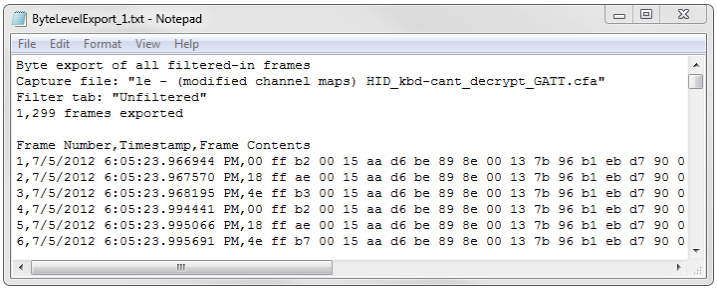


Figure 4.17 - Sample Exported Frames Text File

4.3.1.11 Panes in the Frame Display

4.3.1.11.1 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.

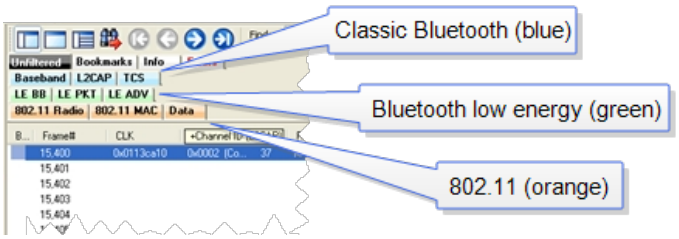


Figure 4.18 - Example Protocol Tags

- 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.

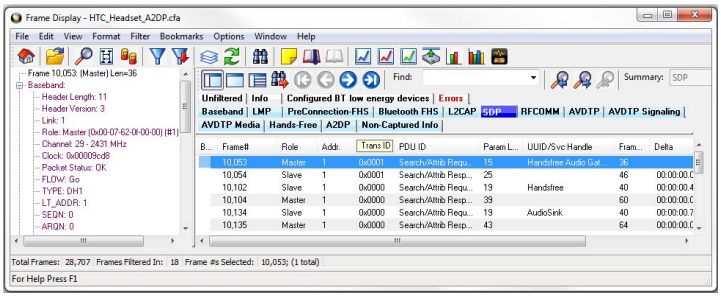


Figure 4.19 - Summary pane (right) with Tooltip on Column 5 (Tran ID)

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".

4.3.1.11.2 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 **Decode**pane 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.

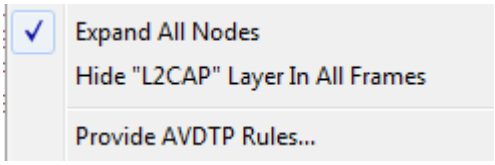
4.3.1.11.3 Frame Symbols in the Summary Pane

Table 4.3 - Frame Symbols

Symbol	Description
	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.

4.3.1.11.4 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

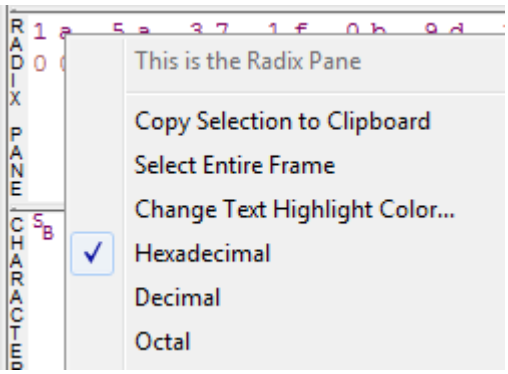
Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the **Event**, **Radix**, **Binary** and **Character** panes. The colors are not assigned to a protocol, but are assigned to the layer.

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.

4.3.1.11.5 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**.



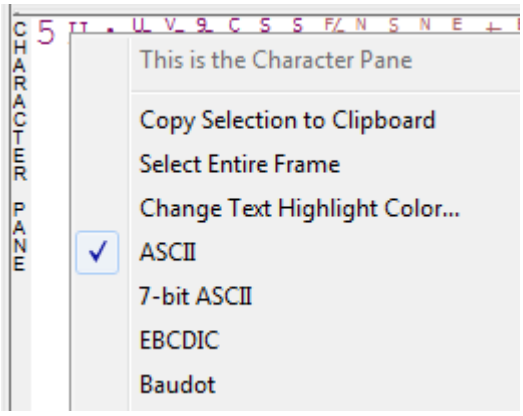
Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

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.

4.3.1.11.6 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.

4.3.1.11.7 Binary Pane

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

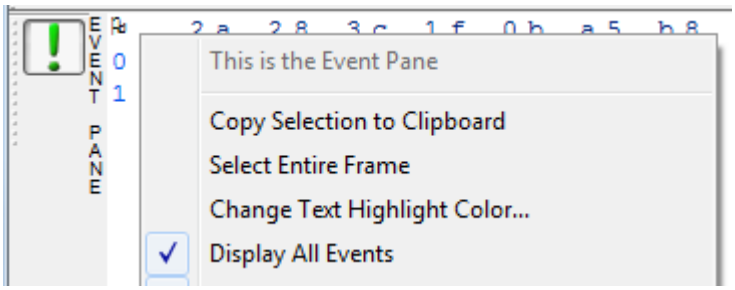
Because the **Binary** pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the **Event** pane. See Physical vs. Logical Byte Display for more information.

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.

4.3.1.11.8 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.

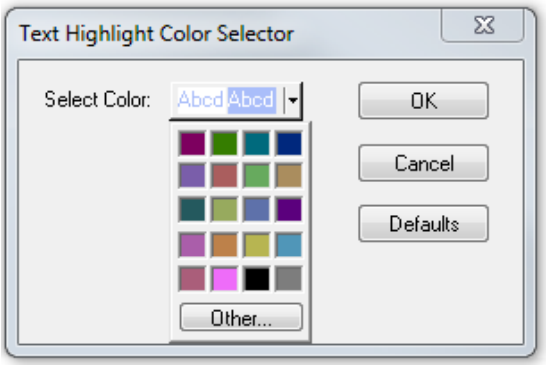
Because the **Event** pane displays the physical bytes rather than the logical bytes, the data in the **Event** pane may be different from that in the **Radix**, **Binary** and **Character** panes. See Physical vs. Logical Byte Display for more information.

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.

4.3.1.11.9 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.

4.3.1.12 Logic Signals in the Frame Display

When analyzing **Logic Signals** captured using the Sodera HCI pods, the Frame Display presents in the Summary pane a frame that contains one packet with two logic signals from HCI POD 1, followed by a frame

with containing one packet from with two logic signals from HCI POD2, if used. The timestamp for these two frames is identical.

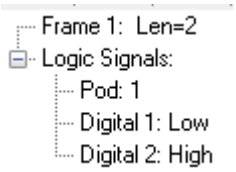
In Figure 4.20 below, Frame# 1 shows logic levels for P1:D1 and P1:D2 but P2:D1 and P2:D2 contain no data. This first frame contains a packet with logic data for POD1. In the next frame—Frame# 2—note that P1:D1 and P1:D2 contain the same logic as in Frame#1, and this data is a copy of the preceding Logic Signals frame—Frame 1—providing continuity in the Summary pane display. New data, P2:D1 and P2:D2, appear having been captured from HCI POD2.

This sequence will continue: Frame# 4 P1:D1 and P1:D2 contains new data from POD1 with P2:D1 and P2:D2 containing data from the preceding frame—Frame#2.

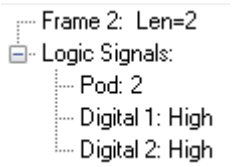
Unfiltered | Info | Logic Signals
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | SCO/eSCO | L2CAP | Undecoded L
LE BB | LE PKT | LE ADV

B...	Frame#	P1:D1	P1:D2	P2:D1	P2:D2	Fram...	Delta	Timestamp
	1	L	H			2		00:00:03.032841
	2	L	H	H	H	2	00:00:00.0...	00:00:03.032841
	4	H*	L*	H	H	2	00:00:00.0...	00:00:03.032996
	5	H	L	H	H	2	00:00:00.0...	00:00:03.032996
	6	H	L	H	H	2	00:00:00.0...	00:00:03.033221
	7	H	L	H	L*	2	00:00:00.0...	00:00:03.033221
	9	L*	L	H	L	2	00:00:00.0...	00:00:03.033783
	10	L	L	H	L	2	00:00:00.0...	00:00:03.033783
	13	L	H*	H	L	2	00:00:00.0...	00:00:03.034796
	14	L	H	H	L	2	00:00:00.0...	00:00:03.034796
	16	H*	L*	H	L	2	00:00:00.0...	00:00:03.035467
	17	H	L	H	L	2	00:00:00.0...	00:00:03.035467

Figure 4.20 - Example: Logic Signals Starting Sequence



When viewing Frame#1 data in the Decoder pane, only POD1 data is shown.



As explained above, in Frame# 2, only new data from POD2 is contained in this packet, and the preceding frame POD1 data is a copy for Summary pane display only. Frame#2 contains only POD2 data.

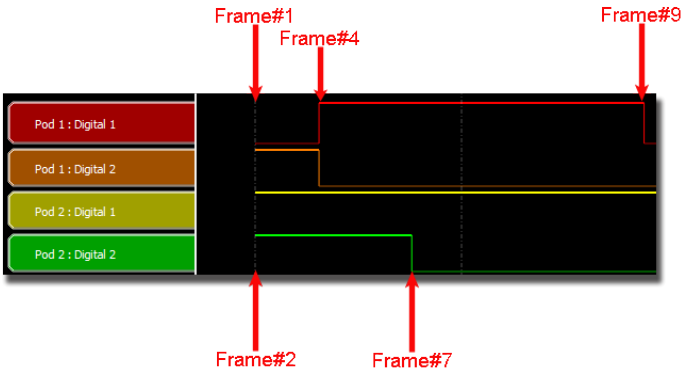


Figure 4.21 - Example: Logic Signals from Frame Display Frame#1 to Frame#9

In Figure 4.21 above, logic signals from Frame#1 through Frame#9 are shown with the signal labels on the left. The first signal transition occurs on both signal lines for POD1 at Frame# 4. The second transition occurs at Frame# 7 on Pod2:Digital 2 (P2:D2). The last transiton occurs at Frame# 9.

4.3.1.13 Protocol Layer Colors

4.3.1.13.1 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.

4.3.1.13.2 Red Frame Numbers and Bytes

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

4.3.1.13.3 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.

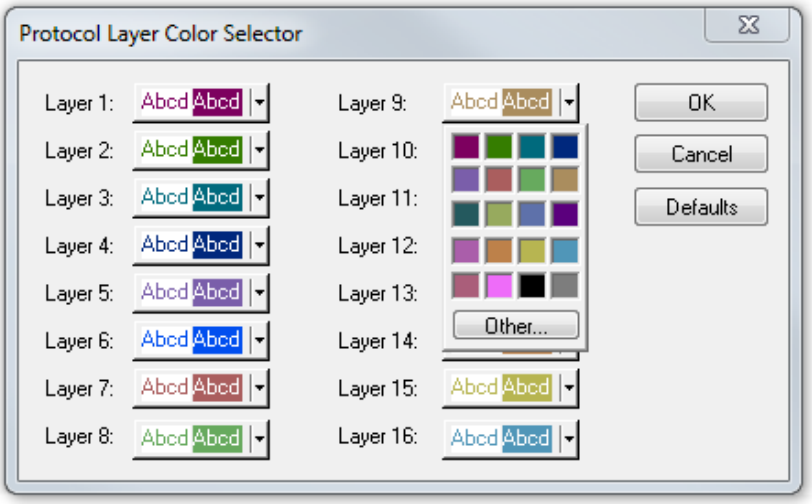


Figure 4.22 - Frame Display Protocol Layer Color Selector

4.3.1.14 Filtering

Filtering allows the user to control the display which capture frames are displayed. Filters fall into two general categories:

1. **Display filters** allow a user to look at a subset of captured data without affecting the capture content. Frames matching the filter criteria appear in the **Frame Display**; frames not matching the criteria will not appear.

2. **Connection filters** Two options are available.

   a. A Bluetooth connection: Displays only the frames associated with a Classic *Bluetooth* link or a *Bluetooth* low energy access address. A new **Frame Display** will open showing only the protocol tabs, frames, summary, and events associated with that particular *Bluetooth* connection.

   b. A specific wireless or wired technology. Displays all of the frames associated with:

      - Classic *Bluetooth*
      - *Bluetooth* low energy
      - 802.11
      - HCI

      A new Frame Display will open showing only the protocol tabs, frames, summary and events associated with the selected technology.

4.3.1.14.1 Display Filters

A display filter looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. 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.

4.3.1.14.1.1 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.

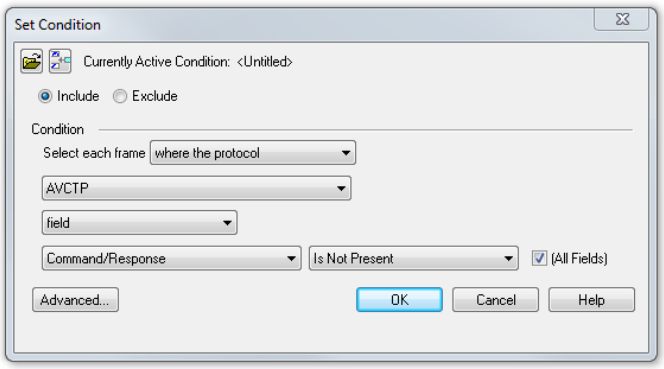


Figure 4.23 - Example: Set Conditions Self Configuring Based on Protocol Selection

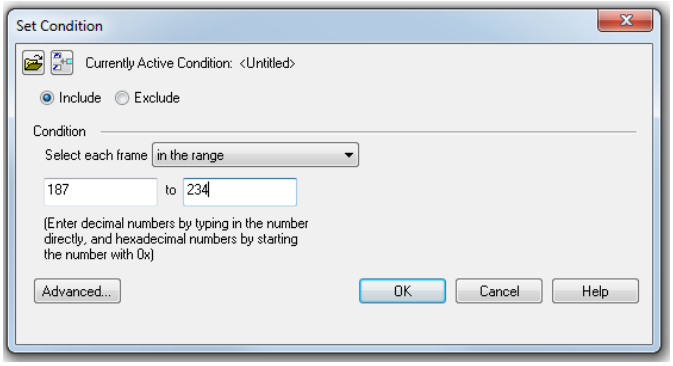


Figure 4.24 - Example: Set Conditions Self Configuring Based on Frame Range

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.

4.3.1.14.1.2 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.

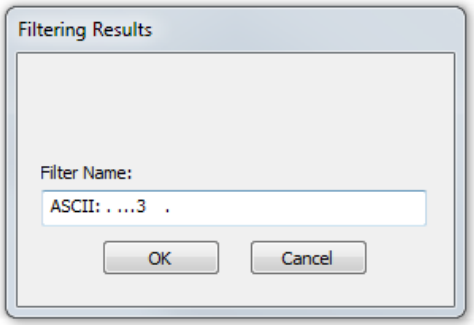
Include: A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

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.

4.3.1.14.1.3 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.

4.3.1.14.1.4 Using Compound Display Filters

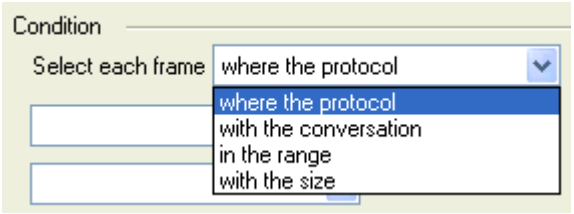
Compound filters use boolean logic to create complex and precise filters. There are three primary Boolean logic operators: **AND**, **OR**, and **NOT**.

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.



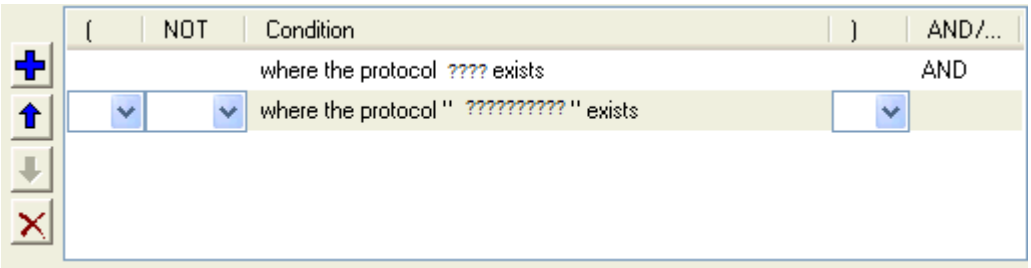


Figure 4.25 - Two Filter Conditions Added with an AND Operator

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**.

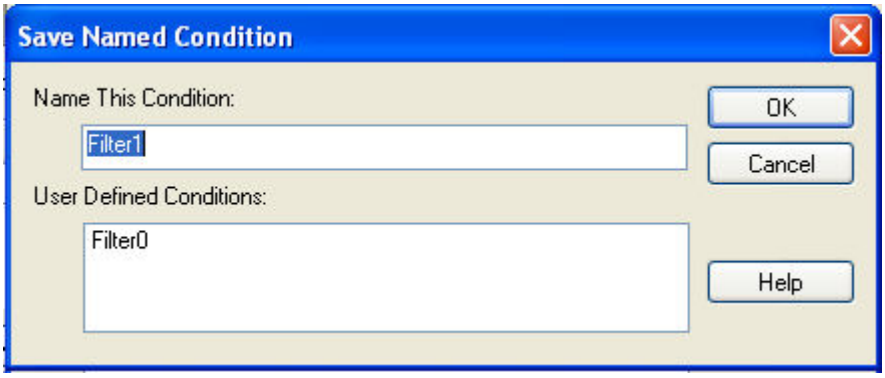


Figure 4.26 - Save Named Filter Condition Dialog

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.

4.3.1.14.1.5 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 **Type**combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first **Address** combo box.

5. Choose a direction arrow from the direction box . The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.

6. If you want to filter on just one node address, skip step 7 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.

4.3.1.14.1.6 The Difference Between Deleting and Hiding Display Filters

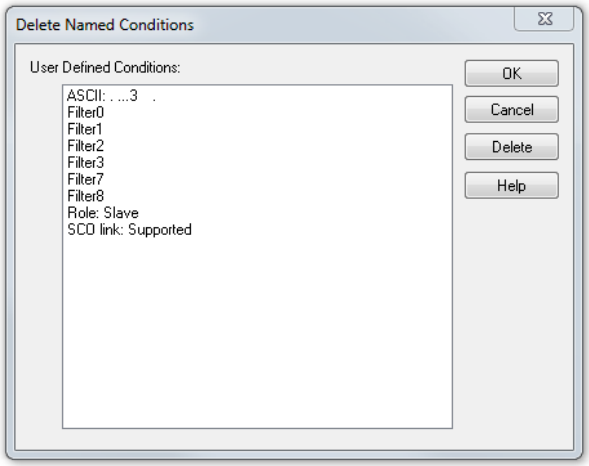
If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

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.

Deleting Saved Display Filters

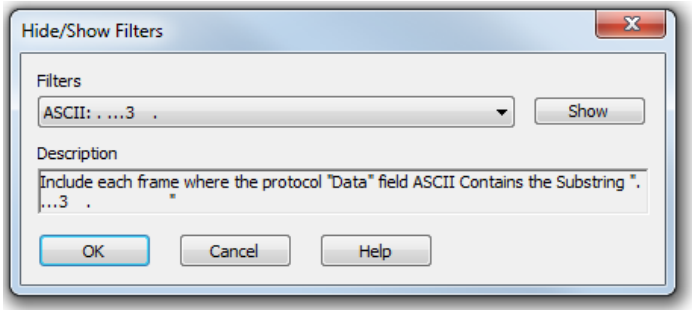
1. Select **Delete Display Filters** from the **Filter** menu in the **Frame Display** window to open the **Delete Named Condition** dialog. The system displays the **Delete Named Condition** dialog with a list of all user defined filters.
2. Select the filter to be deleted from the list.
3. Click the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



Hiding and Revealing Display Filters

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.

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.

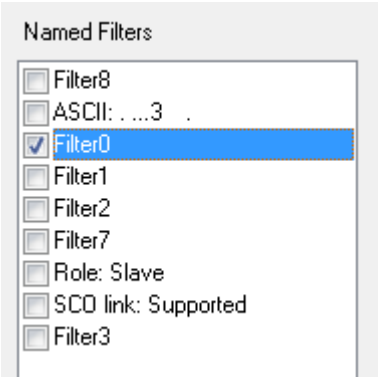
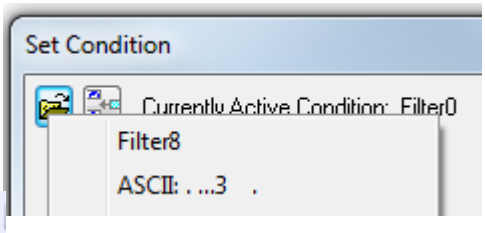


Figure 4.27 - Using Named Filters Section of Quick Filters to Show/Hide Filters

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.

4.3.1.14.1.7 Editing Filters

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.

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

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.

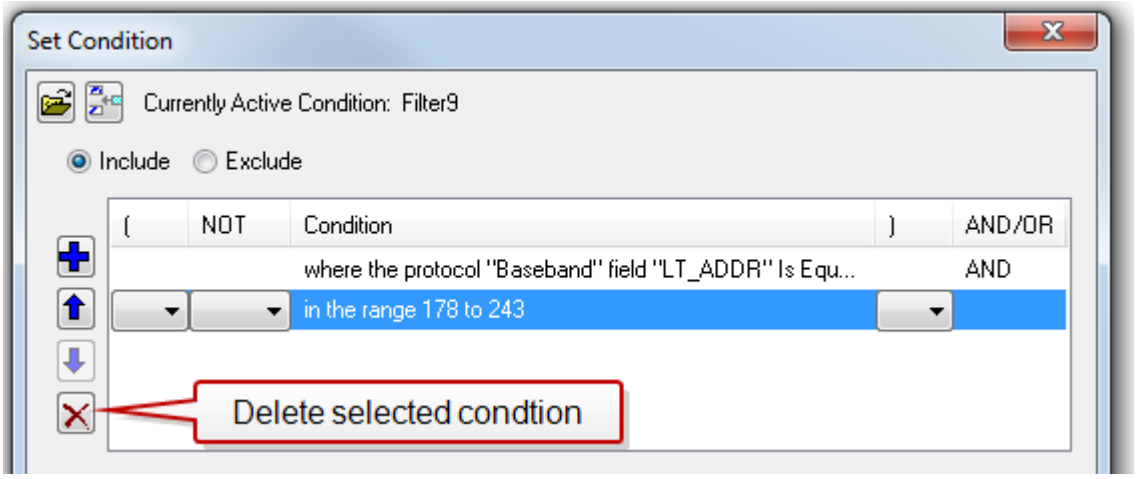


Figure 4.28 - Set Condition Dialog in Advanced View

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.

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

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.

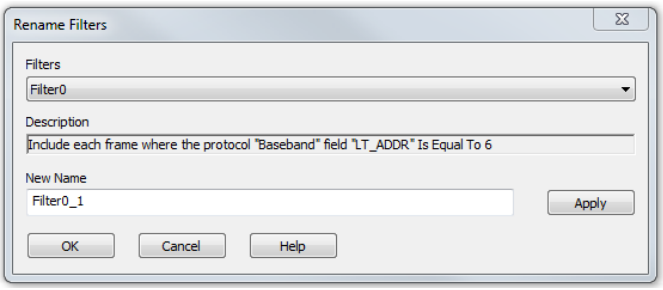


Figure 4.29 - Rename Filters Dialog

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.

4.3.1.14.2 Connection Filtering

Connection Filtering allows the user to view a subset of the total available packets within the **Frame Display**. The subset can include data from a single *Bluetooth* connection, or all of the BR/EDR packets, all of the low energy packets, all of the 802.11 packets, or all of the HCI packets.

Bluetooth Applicability

A connection (device pair) is identified by

1. A Link for Classic *Bluetooth*,
2. An Access Address for *Bluetooth* low energy.

The link ID is a number that the ComProbe software assigns to identify a pair of devices in a BR/EDR connection. In the **Frame Display** details pane, the Baseband layer contains the link ID field if the field's value is not 0.

An Access Address is contained in every *Bluetooth* low energy packet. The Access Address identifies a connection between a slave and a master or an advertising packet.

Connection filtering displays only the frames, protocols, summary, details, and events for the selected connections.

> **Note:** Connection Filters are not persistent across sessions.

4.3.1.14.2.1 Creating a Connection Filter

In the Frame Display there are four ways to create a connection filter.

From the Frame Display Filter menu

Click on the **Frame Display Filter** menu **Connection Filter** selection. From the drop down menu, select **Classic** or **Bluetooth low energy**. The options are

- Classic *Bluetooth*:
  - **All** will filter in all Classic *Bluetooth* frames. You are in effect filtering out any *Bluetooth* low energy frames and are selecting to filter in all the Classic *Bluetooth* links.
  - **Links** displays all the master-slave links. You can select only one link to filter in. The selected link will filter in only the frames associated with that link.
- *Bluetooth* low energy:
  - **All** will filter in all Bluetooth low energy frames. You are in effect filtering out any Classic Bluetooth frames and are selecting to filter in all Bluetooth low energy access addresses.
  - **Access Addresses** displays all the low energy slave device's access address. You can select only one access address to filter. The selected link will filter in only the frames associated with that access address.
- 802.11:
  - **All** will filter in all 802.11 frames. You are in effect filtering out any other technology frames.

- HCI:
  - **All** will filter in all HCI frames. You are in effect filtering out any other technology frames.

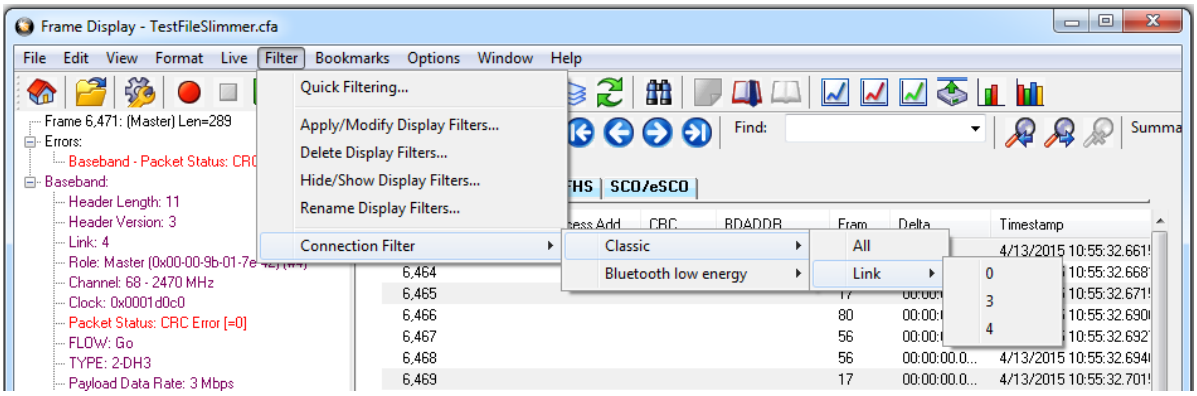


Figure 4.30 - Connection Filter from the Frame Display Menu

From the Frame Display toolbar

Right-click anywhere in the toolbar and select **Connection Filter** from the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

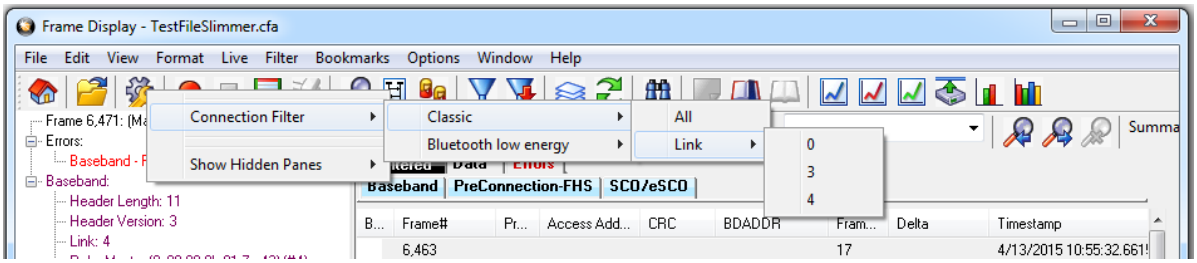


Figure 4.31 - Connection Filter from the Frame Display Toolbar right-click

From the Frame Display panes

Right-click anywhere in a Frame Display pane and select **Connection Filter** in the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

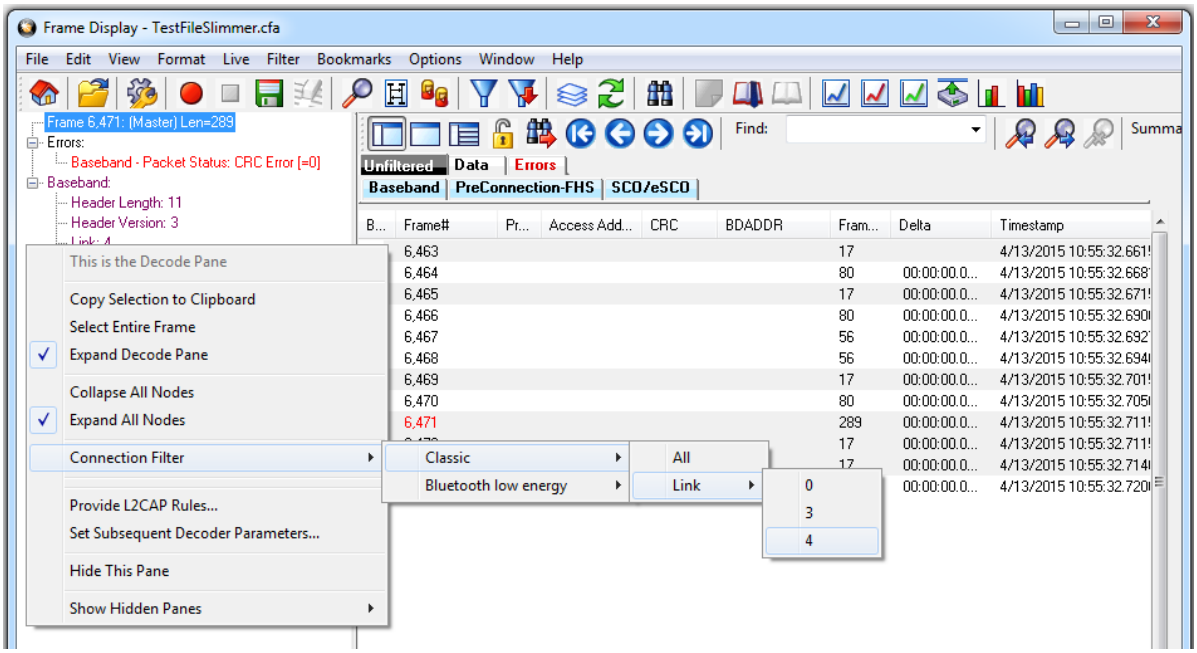


Figure 4.32 - Connection Filter from the Frame Display Pane right-click

From the Frame Display frame selection

Select a frame in the summary pane. Right-click and select **Connection Filter** in the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

If the frame you have selected is associated with a Classic *Bluetooth* link or a *Bluetooth* low energy access address, an additional pop-up menu item will appear as shown in the example image below. This selection is a predetermined filter based on your selection. In the example, frame "6471" is associated with "Link 4", so the predetermined filter assumes that you may want create a connection filter for that link. Clicking on **Connection Filter Link = 4** will filter in "Link 4" frames without opening all the drop-down menus.

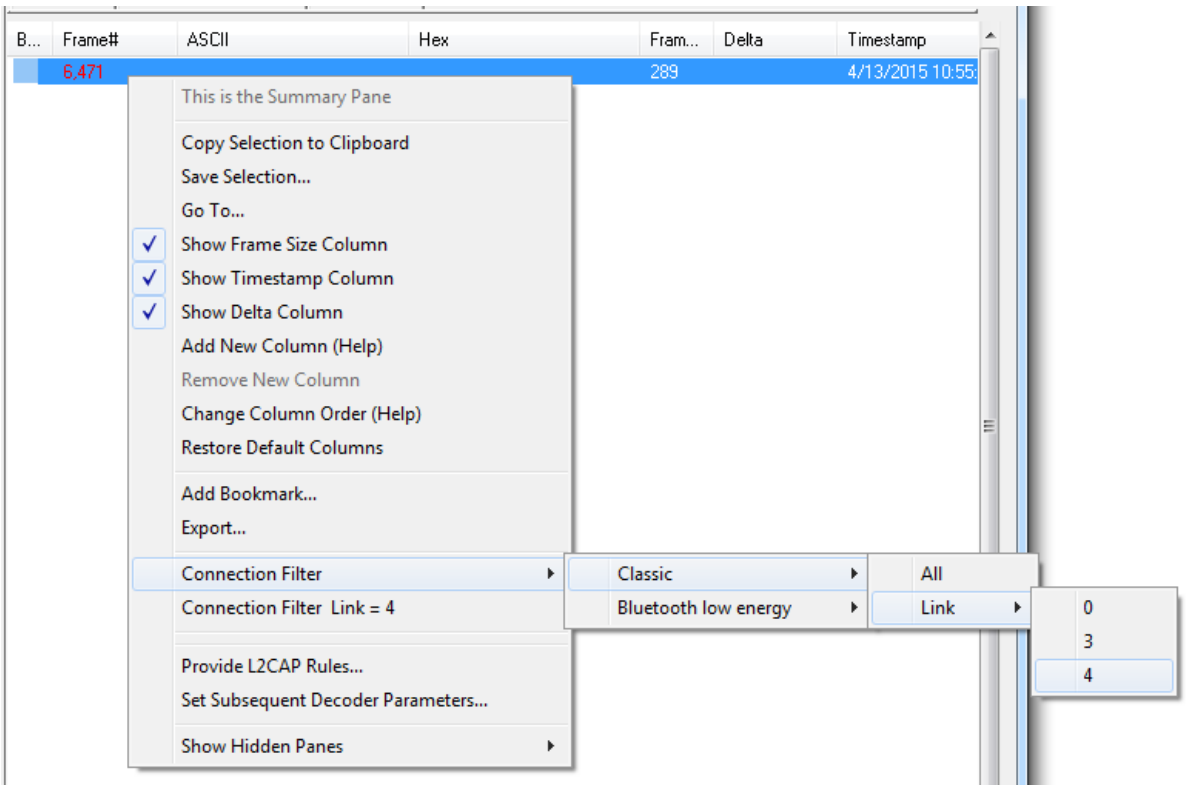


Figure 4.33 - Connection Filter from frame selection right-click

Creating from any Frame Display window

A Connection Filter can be created from any open Frame Display window, and the filtering will always be applied to the original captured data set.

4.3.1.14.2.2 Connection Filter Display

Once you have selected which connections to filter in, another Frame Display will open. The original Frame Display will remain open, and can be minimized.

> **Note:** The system currently limits the number of frame displays to 5. This limit includes any Frame Displays opened using Duplicate View from the Toolbar (see Working with Multiple Frame Displays on page 121)

The new Frame Display with the filtered connection frames will only contain the data defined by the filter criteria. That is, the criteria could be a single link or data for a particular technology.

Display Example 1: Bluetooth low energy Access Address selected

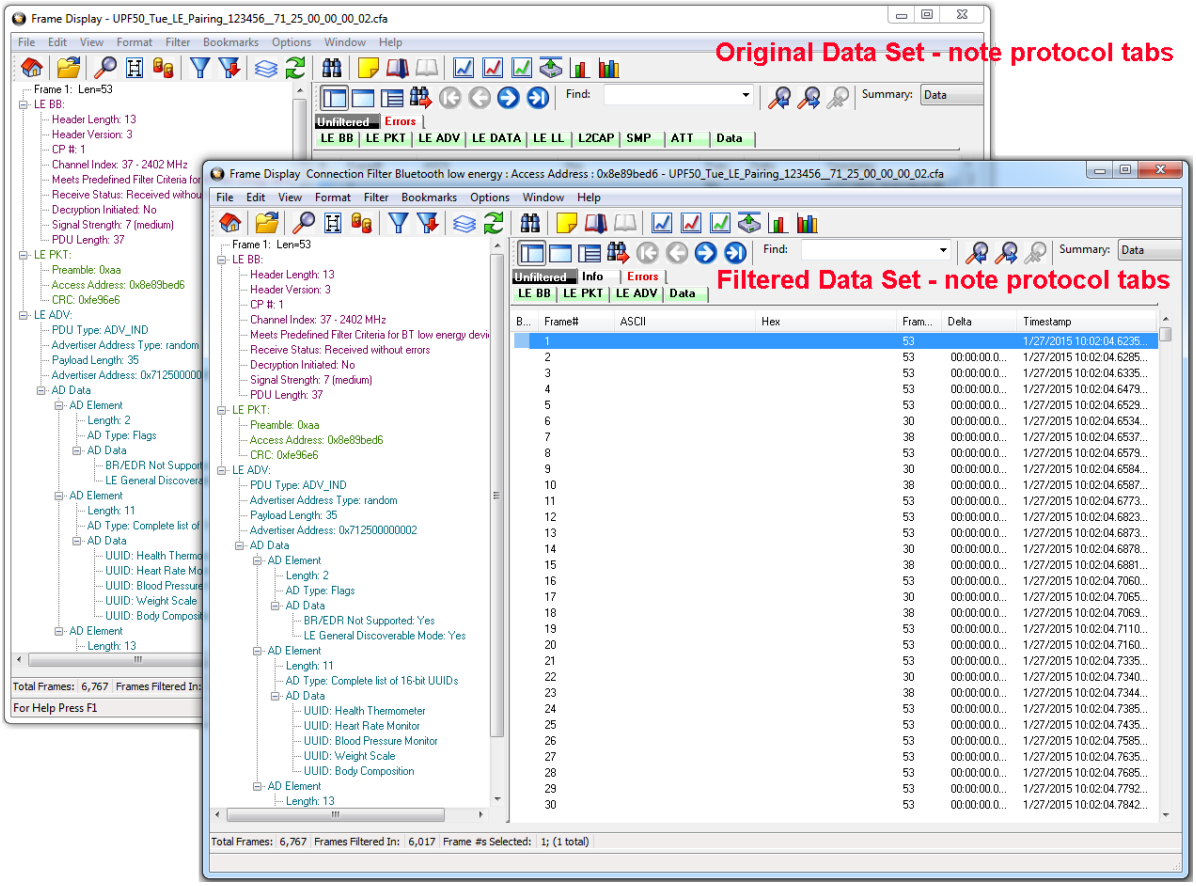


Figure 4.34 - Front Display: Filtered on Access Address 0x8e89bed6

In the figure above is an example Bluetooth low energy data set connection filtered on Access Address = 0x8e89bed6. The Frame Display in the front is the filtered data set. One way to note the difference between the original and the filtered display is to observe the Protocol Tabs. In the filtered display there are four low energy protocol tabs as compared to nine in the original display. This access address connection is not using five of the protocols.

From any open Frame display the user can set another Connection Filter based on the original data set.

Display Example 2: All 802.11 data filtered in

In this example, there is a capture file with Classic *Bluetooth*, *Bluetooth* low energy, and 802.11. To view just the 802.11 data set, 802.11 = All is selected from the right-click pop up menu.

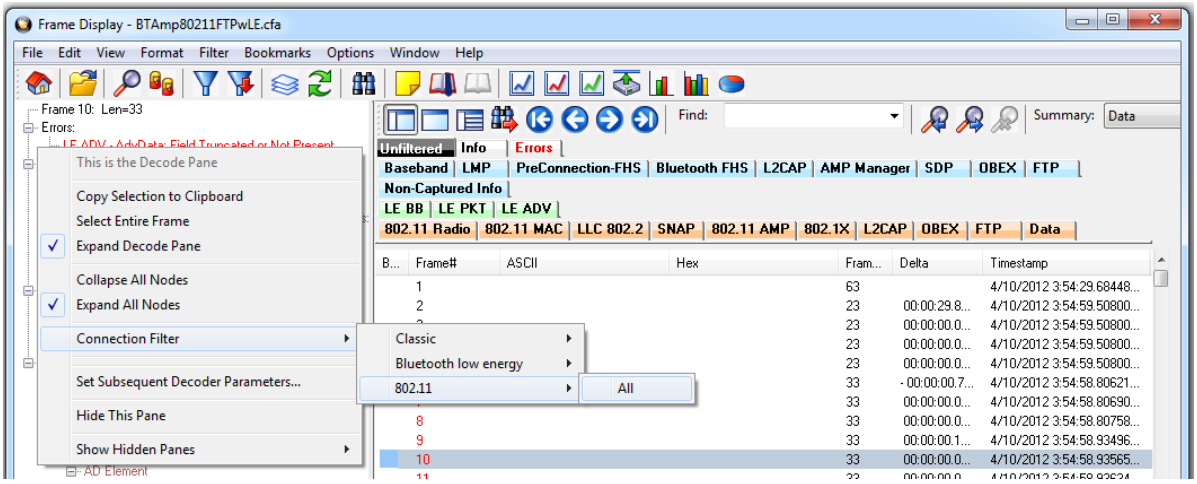


Figure 4.35 - Unfiltered: Capture File with Classic, low energy, and 802.11

When the Frame Display with the filtered 802.11 data set appears, only the Protocol Tabs for 802.11 are present and the tabs for Classic *Bluetooth* and *Bluetooth* low energy have been filtered out.

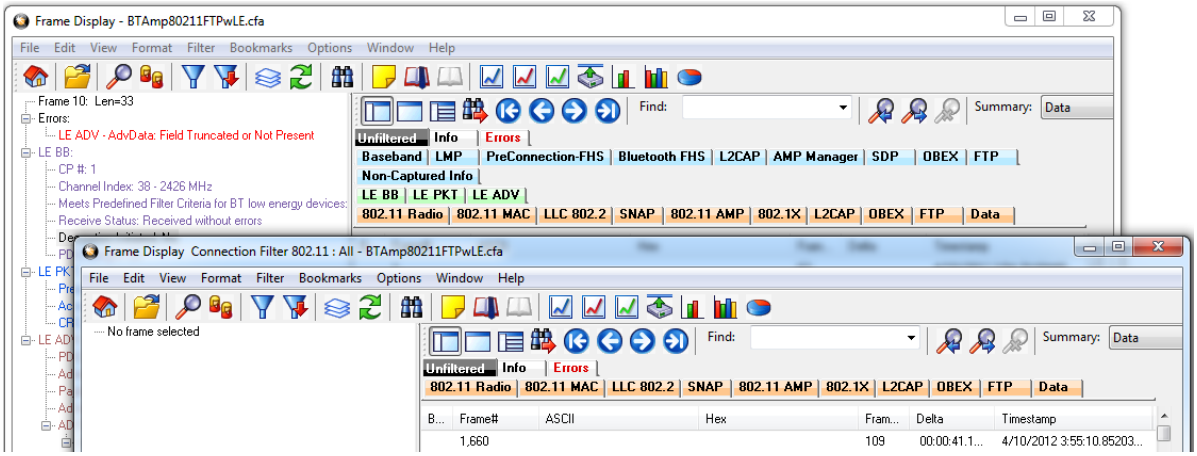


Figure 4.36 - Connection Filter selecting All 802.11 frames, front

4.3.1.14.3 Protocol Filtering from the Frame Display

4.3.1.14.3.1 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.

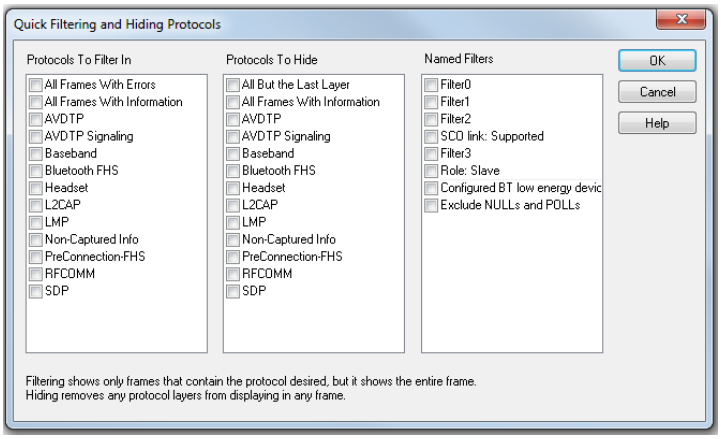


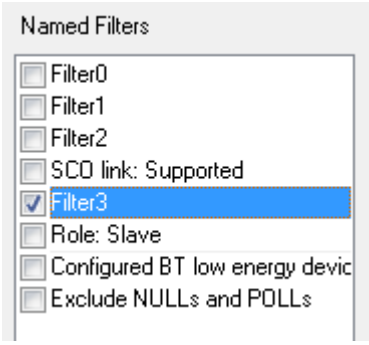
Figure 4.37 - Frame Display Quick Filtering and Hiding Protocols Dialog

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**

4.3.1.14.3.2 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.

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.

Filtering on all Frames with Errors

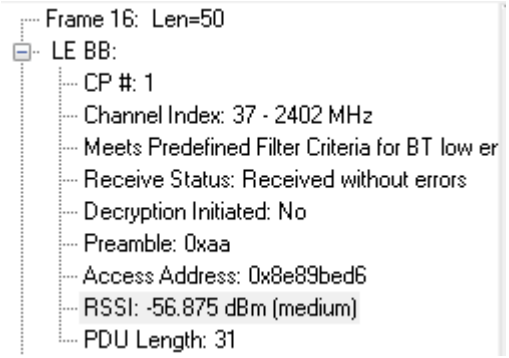
To filter on all frames with errors:

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.

Errors

> **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.

4.3.1.15 Sodera Baseband Layer Signal Strength



The Sodera calculates the RSSI (Receiver Signal Strength Indicator) value, a representation of the radio signal strength at the Sodera receiver, for every *Bluetooth* packet that it captures. RSSI is shown in dBm with a relative signal strength in parentheses. The RSSI value is shown as a decoded field in the **Frame Display** Detail pane Baseband layer .

The Sodera firmware uses the built-in radio firmware features to calculate the RSSI value of the signal received at the antenna.

4.3.2 *Bluetooth* Timeline

In addition to the Coexistence View, which displays both Bluetooth® and 802.11 data together, you can also see more information about *Bluetooth* in a separate dialog. The *Bluetooth* **Timeline** displays packet information with an emphasis on temporal information and payload throughput. The timelines also provide selected information from Frame Display.

The timelines provide a rich set of diverse information about *Bluetooth* packets, both individually and as a range. Information is conveyed using text, color, graphic size, line type, and position.

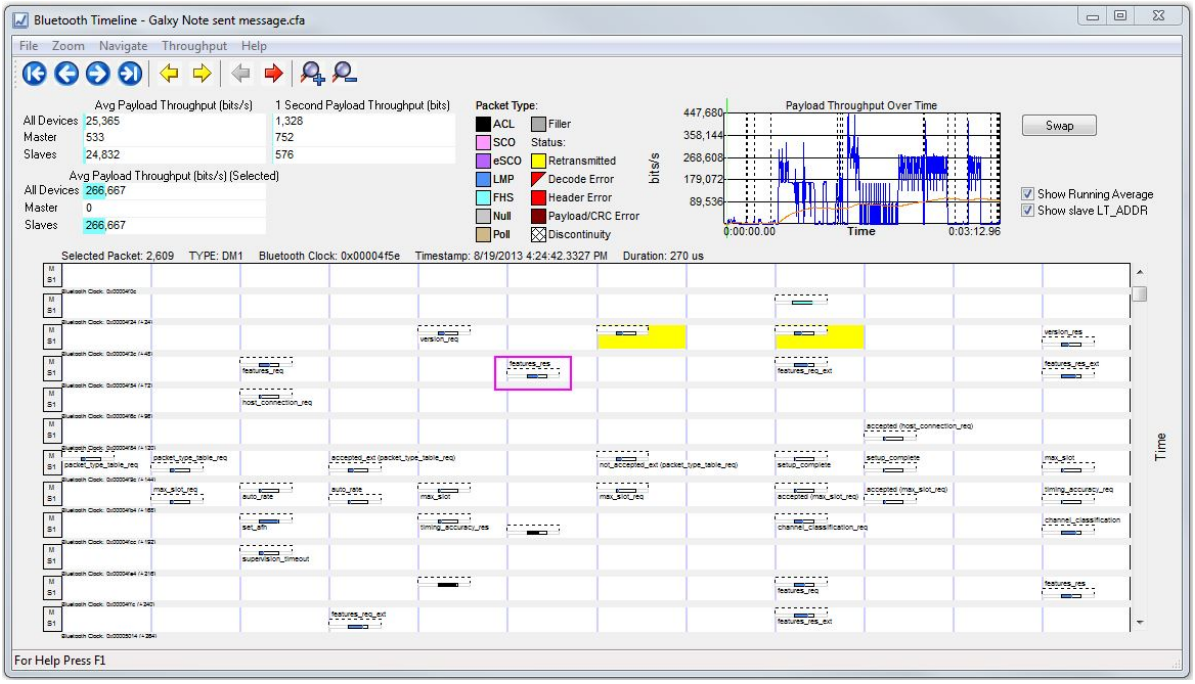


Figure 4.38 - Bluetooth Timeline window

You access the **Bluetooth Timeline** by selecting **Bluetooth Timeline** from the **Control** window **View** menu or by clickingthe **Bluetooth Timeline** icon on the **Control** window toolbar or **Frame Display**.

4.3.2.1 *Bluetooth* Timeline Packet Depiction

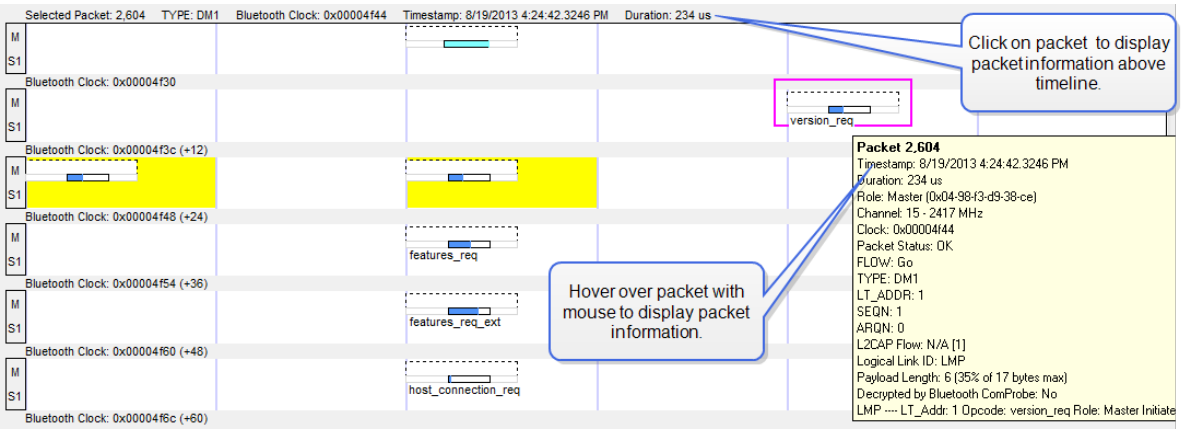


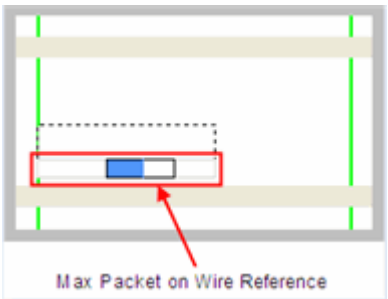
Figure 4.39 - Bluetooth Timeline Packet Depiction with Packet Information Shown

- The timeline shows *Bluetooth* packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
- Within each row are two divisions: **M** (master) and **S** (Slave). Packets are placed on **M** or **S** depending on the data's role.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.

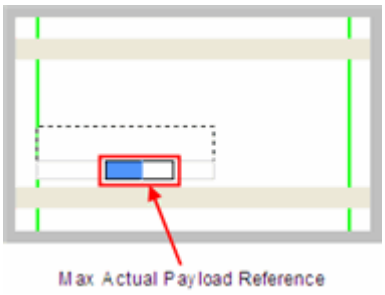
- You can use the arrow keys to move to the next or previous packet. You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

A packet is drawn using the following components:

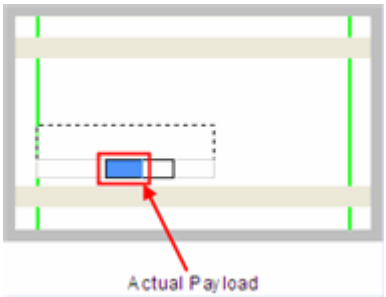
- A “max packet on wire reference” rectangle (light solid lines). This indicates the packet in the air with a max payload.



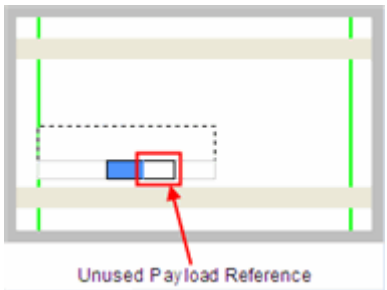
- A “max actual payload reference” rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload in the air contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates where the payload begins in time.



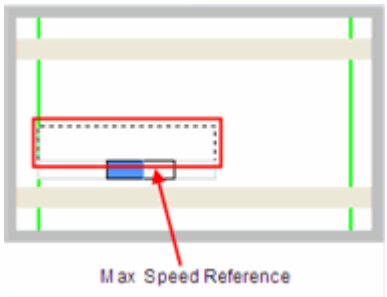
- An “actual payload” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference” rectangle. If the actual payload is of max size, the entire “max actual payload reference” rectangle is colored.



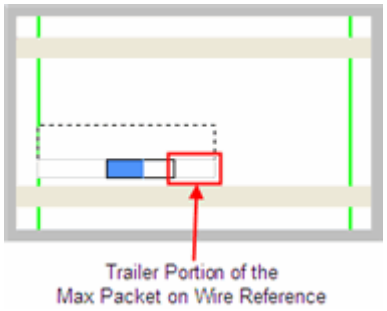
- An “unused payload reference” sub-rectangle (always white). This indicates the unused portion of a maximum payload. It is the remaining portion of the “max actual payload reference” rectangle. The packet in the air does not leave room for this. It is indicated for reference only.



- A “max speed reference” rectangle (dashed lines). This is used to extend the height to that of a 3 Mbits/sec packet, and appears only for packets whose speed is less than that. The packet shown here has a speed of 1 Mbit/sec because the height of the other rectangles is 1/3 of the total height.



- The part of the “max packet on wire reference” rectangle (light solid lines) that trails the “max actual payload reference” rectangle (dark solid lines) is partly packet in the air (if the payload on the wire contained FEC) and partly trailer (CRC, etc). There is always a trailer, so there is always a little space (subject to round off error and pixel granularity) between the ends of the two rectangles.



This table shows how packets are colored:

Table 4.4 - Packet Type Colors

Packet Category	Packet Types	Color
ALC	DM1, DM3, DM5, DH1, 2-DH1, 3-DH1, DH3, 2-DH3, 3-DH3, DH5, 2-DH5, 3-DH5, AUX1	Black
SCO	HV1, HV2, HV3, DV	Pink

Table 4.4 - Packet Type Colors (continued)

Packet Category	Packet Types	Color
eSCO	EV3, 2-EV3, 3-EV3, EV4, EV5, 2-EV5, 3-EV5	Purple
LMP*	DM1, DV	Dark Blue
FHS	FHS	Light Blue
NULL	NULL	Light Gray
POLL	POLL	Light Brown
Filler	Filler provided by ComProbe software	Dark Gray
*LMP is a protocol layer that uses either DM1 or DV packets. If a packet has an LMP layer, the LMP color is used instead of the packet type color.		

This table summarizes the various ways in which packet information is presented:

Table 4.5 - Packet Information Presentation

Information	Text	Color	Graphic size	Position
Packet Type	X			
Packet Category		X		
Protocol	X	X		
Time of occurence	X			X
Source device	X			X
Duration			X	
Size in bytes	X		X	
Size as a percent of max size for that packet type	X		X	
Speed			X	
Status	X		X	

4.3.2.2 *Bluetooth* Timeline Packet Navigation and Selection

- Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous error packet, next or previous retransmitted packet (Bluetooth only), and the first or last packet.
- If there is no selected packet in the timeline, **First Packet** , **Next Packet** , and **Last Packet** are enabled, but **Previous Packet** is not.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the **Frame Display**. Selecting a packet activates **Previous Packet**.

- Selecting **Previous Packet** with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).
- Selecting **Next Packet** with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).
- Selecting **Previous Packet** or **Next Packet** for a packet that's currently visible selects it without scrolling.
- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline, it is also becomes selected in the **Frame Display**. When multiple packets are selected in the timeline, only one of them is selected in the **Frame Display.**
- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

4.3.2.3 *Bluetooth* Timeline Toolbar

The toolbarbar contains the following:


Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.


Unlock


First Packet


Previous Packet


Next Packet


Last Packet


Previous Retransmitted Packet


Next Retransmitted Packet


Previous Error Packet


Next Error Packet


Zoom In - Click on the icon each time to zoom in from 4800 slots to 12 slots


Zoom Out - Click on the icon each time to zoom out from 12 slots to 4800 slots


Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in Frame Display. Resetting the display may be useful when the most recent throughput values are of interest.

4.3.2.4 *Bluetooth* Timeline Menu Bar

The **Bluetooth Timeline** menu bar contains the following:

Table 4.6 - Bluetooth Timeline Menus

Menu	Selection	Description
File	Reset	Resets Timeline to display beginning at current frame. Available only in Live mode.
	Exit	Closes the timeline window

Table 4.6 - Bluetooth Timeline Menus (continued)

Menu	Selection	Description
Zoom	Zoom In	Displays less of the timeline, but in greater detail. Keyboard Shortcut: (Ctrl +)
	Zoom Out	Displays more of the timeline, in less detail. Keyboard Shortcut: (Ctrl -)
	Zoom In Tool	Displays a magnifying glass icon with a + and an arrow that allows for precise positioning on the timeline. Clicking will show less of the timeline around the point where the tools is clicked.
	Zoom Out Tool	Similar to the Zoom In Tool except with a "-" sign in the magnifying glass, and clicking will show more of the timeline around the point where the tool is clicked.
	Selection Tool	
	12 Slots (3x4)	Display 12 timeline slots arranged in (*row* x *time slots*), that is, three row with 4 time slots.
	36 Slots (6x6)	Displays 36 slots.
	144 Slots (12x12)	Displays 144 slots
	324 Slots (18x18)	Displays 324 slots
	576 Slots (24x24)	Displays 576 slots
	900 Slots (30x30)	Displays 900 slots
	1296 Slots (36x36)	Displays 1296 slots
	1764 Slots (42x42)	Displays 1764 slots
	2304 Slots (48x48)	Displays 2304 slots
	2916 Slots (54x54)	Displays 2916 slots
	3600 Slots (60x60)	Displays 3600 slots
	4356 Slots (66x66)	Displays 4356 slots
	5184 Slots (72x72)	Displays 5184 slots

Table 4.6 - Bluetooth Timeline Menus (continued)

Menu	Selection	Description
Navigate	First Packet	Goes to the first packet. Keyboard Shortcut: Home
	Last Packet	Goes to the last packet. Keyboard Shortcut: End
	Previous Packet	Goes to the packet prior to the currently selected packet. Keyboard Shortcut: Left Arrow
	Next Packet	Goes to the next packet after the currently selected packet. Keyboard Shortcut: Right Arrow
	Previous Retransmitted Packet.	Goes to the previous retransmitted packet from the currently selected packet. If there is no previous retransmission this item is not active.
	Next Retransmitted Packet	Goes to the next retransmitted packet from the currently selected packet. If there are no retransmitted packets following the current selection, this item is not active.
	Previous Error Packet	Goes to the first error packet prior to the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Left Arrow
	Next Error Packet	Goes to the first error packet following the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Right Arrow
	Toggle Display Lock	Available only in Live mode. To prevent timeline scrolling during capture, click on this time and the display will lock in its current position. Capture will continue but the displays will remain static. To resume scrolling during capture, click again on this menu item.
Throughput	Export Payload throughput over time.	Save a comma-separated values (.csv) file that contains information about the **Payload Throughput Over Time** graph
	Export Object Throughput Stats	Save a comma-separated values (.csv) file that contains information about objects in the timeline. Assumes at most one object transfer per capture.
Help	Help Topics	Displays *Bluetooth* Timeline help topics.

4.3.2.5 *Bluetooth* Timeline Visual Elements

The *Bluetooth* Timeline consists of the following visual elements:

- The timeline shows *Bluetooth* packets within a specific period of time.
- The timeline shows *Bluetooth* packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
- Within each row are two divisions: **M** (master) and **S** (Slave). Packets are placed on **M or S** depending on source of the data withing the link.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet.You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).
- Rows of *Bluetooth* Slots: Each slot begins at the left edge of the vertical blue bar. There are two *Bluetooth* clocks per slot. Each slot represents 0.000625 seconds, or 625 µs.
- **M** and **S** labels: Within each row, master and slave packets are indicated on the left side of the row. By default, all possible slave devices (there can be up to 7) are put on the **S** sub-row, but checking the **Show slave LT_ADDR** checkbox shows all existing slave device sub-rows with numbered labels (some or all of S1, S2, …, S7).
- *Bluetooth* Clock: The *Bluetooth* clock of the first slot in each row is shown underneath each row.
- Packet Info Line: The packet info line appears just above the timeline and displays information for the currently selected packet(s). If only one packet is selected, this information consists of the **packet number**, **packet type**, *Bluetooth* **clock** (*Bluetooth* only), **Timestamp**, and **Duration**. **Duration** is shown as "Unknown" when the selected packet has an error.

  If multiple packets are selected, this information consists of the packet range, the *Bluetooth* **clock delta** (*Bluetooth* only), the **Timestamp delta**, and **Span**. **Span** is shown as "Unknown" when the last packet in the selected range has an error since its duration is unknown. A user can use these to verify the average throughput calculations.

  Selected packets are bounded by a magenta rectangle. See the Bluetooth Timeline Packet Navigation and Selection on page 152 .
- Floating Information Window (aka Tooltip): The information window displays when the mouse cursor hovers on a packet (not slot). It persists as long as the mouse cursor stays on the packet or tooltip. For Bluetooth, the tooltip shows the packet number (in bold), the Baseband layer decode from the decode pane of the Frame Display (with the percentage of the Payload Length max added).

  Discontinuities are indicated by cross-hatched slots. See the Bluetooth Timeline Discontinuities on page 162 section.
- Zoom Tools: **Zoom** tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See Bluetooth Timeline Zooming on page 158 .

- Packet Status: Packet status is indicated by color codes. A yellow slot indicates a re-transmitted packet, a dark red slot indicates a CRC error, and a small red triangle in the upper-left corner of the packet (not the slot) indicates a decode error.
- Right-Click Menu: The right-click menu provides zooming and tool selection. See the Bluetooth Timeline Discontinuities on page 162 .
- Graphical Packet Depiction: Each packet within the visible range is graphically depicted. See the Bluetooth Timeline Packet Depiction on page 149.
- Swap Button: The Swap button switches the position of the Timeline and the Throughput graph.
- Show Running Average: Selecting this check box shows a running average in the Throughput Over Time graph as an orange line.
- Show slave LT_ADDR: Selecting this checkbox displays the Slave LT_ADDR in the timeline row labels

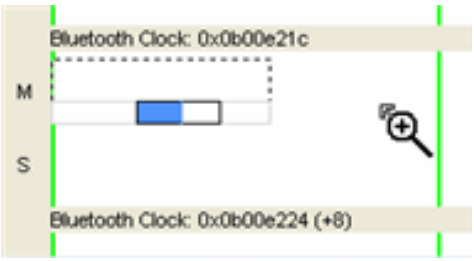
> **Note:** The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

4.3.2.6 *Bluetooth* Timeline Zooming

Zoom features can be accessed from the Zoom menu, clicking a zoom tool on the toolbar, or by right clicking on the **Timeline** window.

A couple of things to remember about Zooming.

- **Zoom** tools accessed using the right click menu allow you to maintain the current position on the screen and precisely zoom in to a specific packet.
- Selecting a **Zoom** icon (+ or -) on the toolbar does not change the pointer to a **Zoom** tool. Each distinct click only zooms in our out.
- **Zoom** tools accessed from the **Zoom** menu have a pointer in the upper-left corner which is useful for specifying the zoom location and bringing up a tool tip of a specific packet.



4.3.2.7 *Bluetooth* Timeline Throughput Displays

In computing throughput, payload is not counted from *Bluetooth* packets that have a CRC error (dark red slot) or that are a retransmission (yellow slot).

4.3.2.7.1 *Bluetooth* Timeline Average Payload Throughput

The figure depicts the **Throughput** display with the **Average Throughput** indicators in the left column.

	Avg Payload Throughput (bits/s)
All Devices	3,668
Master	1,710
Slaves	1,958

Average Throughput is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet. In *Bluetooth*, timestamp difference is used instead of *Bluetooth* clock count because timestamp difference is immune to

role switches. However, this can result in inaccuracies when the duration is small enough that a coarse timestamp granularity is significant.

- **Average Throughput** is shown as 0 when there is only one packet, because in that case the timestamp difference is 0 and an average cannot be computed.
- **Duration** is the beginning of the first packet to the end of the last packet.
- **Duration** for average throughput is beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- **Average Throughput** is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates relative percentage. Text displays the throughput value.

4.3.2.7.2 *Bluetooth* Timeline 1 Second Throughput Indicators

1 Second Payload Throughput (bits)
3,312
1,544
1,768

- 1-Second Payload Throughput is the total payload over the most recent one second of duration (This is determined by counting *Bluetooth* clocks). It is cleared after each discontinuity. A discontinuity is when the Bluetooth clock goes forward more than two (2) seconds or goes backwards any amount. This is caused by either a role switch or Bluetooth clock rollover . The Bluetooth clock count is used instead of timestamp difference because the Bluetooth clock count is precise; however, if timestamp difference were used it would not be necessary to clear the 1-second throughput after each discontinuity. Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.
- 1-second throughput is not an average. It is simply the total payload over the most recent one second of duration. Since it's not an average, it behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small payload by small time), 1-second throughput is very small (since it counts only what it sees and doesn't try to extrapolate).
- A 1-second throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates percentage of max, and text gives the actual throughput.

4.3.2.7.3 Average Payload Throughput (bits/s) (Selected)

The following figure depicts the **Throughput** display with the **Average Payload Throughput (bits/sec) (Selected)** indicators in the left column. This portion of the dialog displays average throughput for a selected packet range when you select a packet from the Timeline.

	Avg Payload Throughput (bits/s) (Selected)
All Devices	0
Master	0
Slaves	0

Average throughput is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet. In *Bluetooth*, timestamp difference is used instead of *Bluetooth* clock count because timestamp difference is immune to role switches. However, this can result in inaccuracies when the duration is small enough that a coarse timestamp granularity is significant.

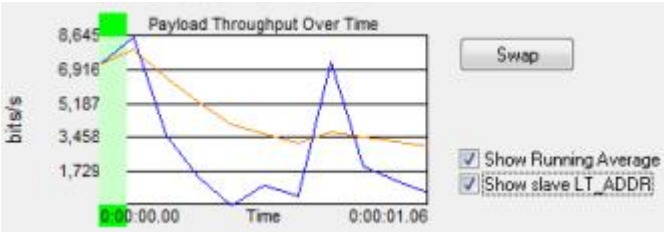
- Duration for average throughput is beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- Average throughput can be nonzero when a single packet is selected.

- Average throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates relative percentage. Text displays the throughput value

4.3.2.7.4 *Bluetooth* Payload Throughput Over Time Graph

The following figure depicts the Payload Throughput Over Time graph.

The Payload Throughput Over Time graph shows total payload for each successive time interval. The time interval is initially 0.1 second. Each time the number of throughput elements reaches 100, they are collapsed into a set of 50 by combining adjacent elements and doubling the duration of each element. Collapsing thus occurs as follows:



Collapse count	Time since beginning of session (seconds)	Element duration after collapse (seconds)
1	10	0.2
2	20	0.4
3	40	0.8
4	80	1.6
5	160	3.2
6	320	6.4

and so on...

- The bottom of the graph shows a beginning time and an ending time. The beginning time is relative to the start of the session and initially 0. When packets start wrapping out it becomes the relative time offset of the first available packet. The ending time is always the total time of the session.
- Discontinuities are indicated by vertical dashed lines.
- A green view port indicates the time range corresponding to the visible slots in the timeline. The view port can be moved by clicking elsewhere in the graph or by dragging. Whenever it is moved, the timeline scrolls to match. When the slot range in the timeline changes, the view port moves and resizes as necessary to match.
- The **Swap** button - switches the position of the Timeline and the **Throughput** graph.
- **Show Running Average** - Selecting this check box shows a running average in the **Throughput Over Time** graph as an orange line.
- **Show slave LT_ADDR** - Selecting this checkbox displays the **Slave LT_ADDR** in the timeline row labels.

Comparison with the Coexistence View 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.

4.3.2.8 Export Payload Throughput Over Time

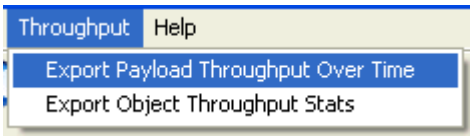
In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about the **Payload Throughput Over Time** graph. The file contains the following information:

- Sequence Number
- Beginning Packet
- Ending Packet
- Bit Count
- Duration (Secs)
- Bits/Sec
- Running Average (Bits/Sec)

To create the file:

1. Select **Export Payload Throughput Over Time** from the Throughput menu.

   The **Save As** menu appears.



2. Select a location where you want to save the file.

> **Note:** In live mode, default path name is *C:\Users\Public\Public Documents\Frontline Test Equipment\My Log Files\PayloadThroughputOverTime.csv*. In view mode, default path name is *cfa basepathname with " (PayloadThroughputOverTime).csv"* appended.

3. Enter a **File Name.**
4. Select **Save.**

   The file is saved and you can open it in a simple text editor or database application.

4.3.2.9 Object Throughput Stats File

In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about objects in the timeline. The file contains the following information:

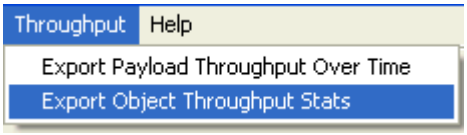
- Name
- Length (bytes)
- Connection Packet Number
- Begin Transfer Packet Number
- End Transfer Packet Number
- Disconnection Packet Number
- Connection Duration
- (Fractional Seconds)

- Transfer Duration
- (Fractional Seconds)
- Connection Throughput (bits/s)
- Transfer Throughput (bits/s)
- Transfer Duration Percentage of Connection Duration
- No Errors Packet Count (Includes Decode Errors) (While Connected)
- Retransmitted Packet Count (While Connected)
- Header Errors Packet Count (While Connected)
- Payload/CRC Errors Packet Count (While Connected)

To create the file:

1. Select **Export Object Throughput Stats** from the Throughput menu.

   The **Save As** menu appears.



2. Select a location where you want to save the file.

   Note: In live mode, the default path name is *C:\Users\Public\Publick Documents\Frontline Test Equipment\My Log Files\ObjectThroughputStats.csv.* In view mode, default path name is *cfa basepathname with " (ObjectThroughputStats).csv"* appended.

3. Enter a **File Name.**
4. Select **Save.**

   The file is saved and you can open it in a simple text editor or database application

4.3.2.10 *Bluetooth* Timeline Discontinuities

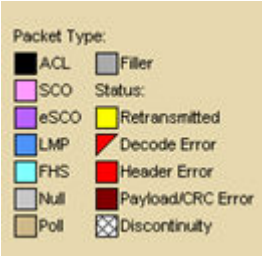
The following figure depicts a discontinuity between two packets.

Figure 4.40 - *Bluetooth* Timeline Packet Discontinuity, cross-hatched area.

To keep the timeline and the throughput graph manageable, big jumps in the *Bluetooth* clock are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the *Bluetooth* clock goes forward more than two (2) seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph. The *Bluetooth* clock can jump forward when capture is paused or when there is a role switch (in a role switch, a different device becomes master, and since each device keeps its own *Bluetooth* clock, the clock can change radically), and backwards when there is a role switch or clock rollover

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

4.3.2.11 Legend



This legend identifies the color coding found in the timeline.

4.3.2.12 *Bluetooth* Timeline: Packets Missing *Bluetooth* Clock

Captured data that is missing the *Bluetooth* clock, such as HCI and BTSnoop, will not display packets. In an instance when the data is missing the clock the *Bluetooth* Timeline will display a message in the Throughput Graph and the Timeline: "Packets without a Bluetooth clock (such as HCI) won't be shown."

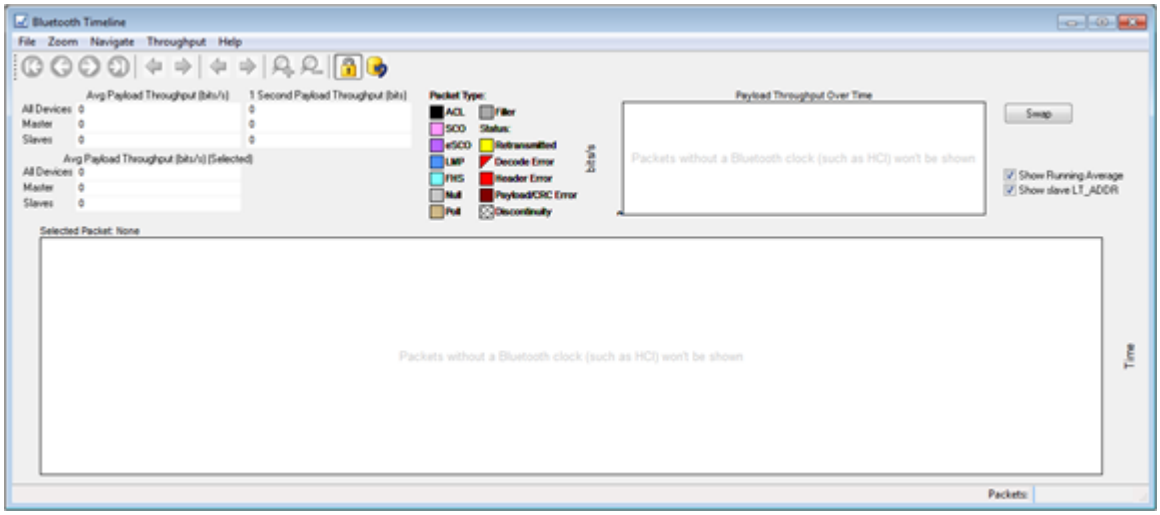


Figure 4.41 - Missing packets message in timeline pane.

4.3.3 low energy Timeline

The **Bluetooth low energy Timeline** displays packet information with an emphasis on temporal information and payload throughput. The timeline also provides selected information from **Frame Display**.

The timeline provides a rich set of diverse information about low energy packets, both individually and as a range. Information is conveyed using text, color, packet size, and position.

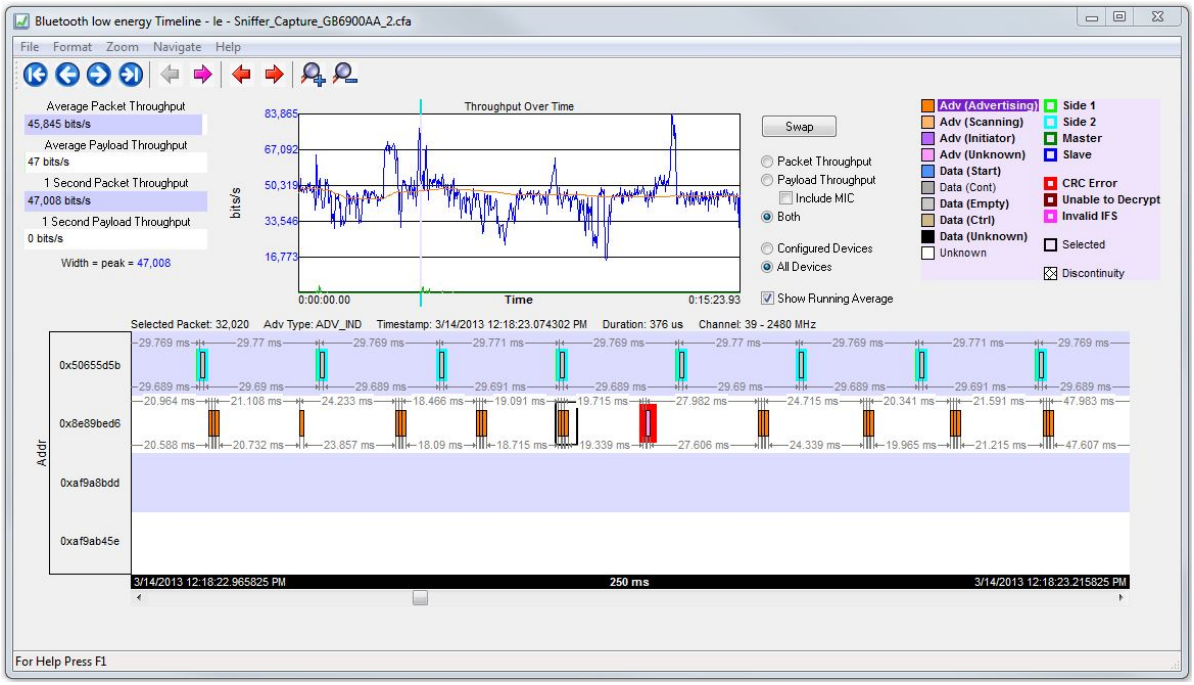


Figure 4.42 - *Bluetooth* **low energy Timeline**

You access the Timeline by selecting **Bluetooth low energy Timeline** from the **View** menu or by pressing the *Bluetooth* low energy Timeline icon on the **Control** window toolbar and **Frame Display** toolbar.

In computing throughput, packets that have a CRC error are excluded.

4.3.3.1 low energy Timeline Toolbar

The toolbar contains the following:

Table 4.7 - *Bluetooth* low energy Timeline Toolbar

Icon	Description
	Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.
	Unlock
	First Packet
	Previous Packet
	Next Packet
	Last Packet

Table 4.7 - Bluetooth low energy Timeline Toolbar (continued)

Icon	Description
	Previous Interframe Spacing (IFS) Error • Interframe Spacing is considered valid if it is within 150 µs + or – 2us • If the Interframe Spacing is less than 148 us or greater than 152 us but less than or equal to 300 µs, it is considered an IFS error.
	Next Interframe Spacing (IFS) Error • Interframe Spacing is considered valid if it is within 150 µs + or – 2us • If the Interframe Spacing is less than 148 us or greater than 152 µs but less than or equal to 300 us, it is considered an IFS error.
	Previous Error Packet
	Next Error Packet
	Zoom In
	Zoom Out
	Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in Frame Display. Resetting the display may be useful when the most recent throughput values are of interest.

4.3.3.2 low energy Timeline Menu Bar

The ***Bluetooth* low energy Timeline** menu bar contains the following:

Table 4.8 - Bluetooth low energy Timeline Menus

Menu	Selection	Description
File	Reset	Resets Timeline to display beginning at current frame. Available only in Live mode.
	Exit	Closes the timeline window
Format	Show Device Address Rows	Displays rows of packets from sending devices. The source device address will appear on the left of each row.
	Show Radio Rows	Displays rows packets received on radios 0,1, or 2. The radio number will appear on the left of each row.

Table 4.8 - Bluetooth low energy Timeline Menus (continued)

Menu	Selection	Description
Zoom	Zoom In	Displays less of the timeline, but in greater detail. Keyboard Shortcut: (Ctrl +)
	Zoom Out	Displays more of the timeline, in less detail. Keyboard Shortcut: (Ctrl -)
	Zoom In Tool	 Displays a magnifying glass icon with a + and an arrow that allows for precise positioning on the timeline. Clicking will show less of the timeline around the point where the tools is clicked.
	Zoom Out Tool	Similar to the Zoom In Tool except with a "-" sign in the magnifying glass, and clicking will show more of the timeline around the point where the tool is clicked.
	Selection Tool	
	Single Segment Zoom: Each selection defines the time displayed, "1" segment, and number of 1.25 ms markers withing the segment.	
	2.5 ms (1x2)	Displays one 2.5 ms segment with 2 markers.
	11.25 ms (1x9)	Displays one 11.25 ms segment with 9 markers.
	33.75 ms (1x27)	Displays one 33.75 ms segment with 27 markers.
	125 ms (1x100)	Displays one 125 ms segment with 100 markers.
	437.5 ms (1x350)	Displays one 437.5 ms segment with 350 markers.
	1.875 s (1x1500)	Displays one 1.875 s segment with 1500 markers.
	3.75 s (1x3000)	Displays one 3.75 ms segment with 3000 markers.
	Multiple Segment Zoom: Each selection defines the timeline view port, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "7.5 ms (6 1.25 ms time intervals (3x2))" will display "7.5 ms" of the total timeline in "3" segments of with "2" markers per segment for a total of "6" markers.	
	7.5 ms (6 1.25 ms time intervals (3x2))	3 segments, 2 markers per segment: 1.25 ms x 6 = 7.5 ms total; 1.25 ms x 2 = 2.5 ms per segment.
	22.5 ms (18 1.25 ms time intervals (6x3))	6 segment, 3 markers per segment
	90 ms (72 1.25 ms time intervals (12x6))	12 segments, 6 markers per segment
	202.5 ms (162 1.25 ms time intervals (18x9))	18 segments, 9 markers per segment
	360 ms (288 1.25 ms time intervals (24x12))	24 segments, 12 markers per segment

Table 4.8 - Bluetooth low energy Timeline Menus (continued)

Menu	Selection	Description
	562.5 ms (450 1.25 ms time intervals (30x15))	30 segments, 15 markers per segment
	810 ms (648 1.25 ms time intervals (36x18))	36 segments, 18 markers per segment
	1.1025 s (882 1.25 ms time intervals (42x21))	30 segments, 15 markers per segment
	1.44 s (1152 1.25 ms time intervals (48x24))	48 segments, 24 markers per segment
	1.8225 s (1458 1.25 ms time intervals (54x27))	45 segments, 27 markers per segment
	2.25 s (1800 1.25 ms time intervals (60x30))	60 segments, 30 markers per segment
	2.7225 s (2178 1.25 ms time intervals (66x33))	66 segments, 33 markers per segment
	3.24 s (2592 1.25 ms time intervals (72x36))	72 segments, 36 markers per segment
	3.8025 s (30421.25 ms time intervals (78x39))	78 segments, 39 markers per segment
	4.41 s (3528 1.25 ms time intervals (84x42))	84 segments, 42 markers per segment
	5.0625 s (4050 1.25 ms time intervals (90x45))	90 segments, 45 markers per segment

Table 4.8 - Bluetooth low energy Timeline Menus (continued)

Menu	Selection	Description
Navigate	First Packet	Goes to the first packet. Keyboard Shortcut: Home
	Last Packet	Goes to the last packet. Keyboard Shortcut: End
	Previous Packet	Goes to the packet prior to the currently selected packet. Keyboard Shortcut: Left Arrow
	Next Packet	Goes to the next packet after the currently selected packet. Keyboard Shortcut: Right Arrow
	Previous Invalid IFS Packet.	Goes to the previous invalid IFS packet from the currently selected packet. If there is no previous invalid IFS packet this item is not active.
	Next Invalid IFS Packet	Goes to the next invalid IFS packet from the currently selected packet. If there are no invalid IFS packets following the current selection, this item is not active.
	Previous Error Packet	Goes to the first error packet prior to the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Left Arrow
	Next Error Packet	Goes to the first error packet following the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Right Arrow
	Selected Packet	Keyboard Shortcut: Enter
	Toggle Display Lock	Available only in Live mode. To prevent timeline scrolling during capture, click on this time and the display will lock in its current position. Capture will continue but the displays will remain static. To resume scrolling during capture, click again on this menu item.
Help	Help Topics	Displays *Bluetooth* low energy Timeline help topics.

4.3.3.3 low energy Timeline Legend

This legend identifies the color coding found in the timeline.

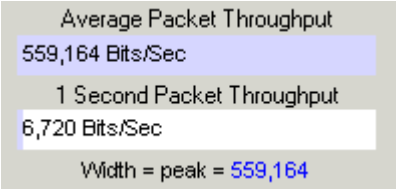
- When you select a packet in the timeline, items in the legend that relate to the packet are highlighted.
- Bold text indicates that the type of packet has been seen in the timeline.

4.3.3.4 Throughput Displays

Throughput is payload over time. There are 3 categories of throughput:

4.3.3.5 Average and 1 Second Packet Throughput

The figure depicts the **Average** and **1 Second Packet Throughput** displays. This display appears when you select the **Packet Throughput** radio button.



- **Average Packet Throughput** is the total packet size over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet.
- **1-Second Packet Throughput** is the total packet size over the most recent one second.
- **Width = peak =**: This displays the maximum throughput seen so far.
- A horizontal bar indicates percentage of max seen up to that point, and text gives the actual throughput.

4.3.3.6 Average and 1 Second Payload Throughput

The figure depicts the **Average** and **One Second Payload** Throughput display. This display appears when you select the **Payload Throughput** radio button.

- **Average Payload Throughput** is the total payload over the entire session divided by the total time.
- **1-second Payload Throughput** is the total payload over the most recent one second.
- **Width = peak =:** This displays the maximum throughput seen so far.

> **Note:** 1-second throughput behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small packet or payload size by small time), 1-second throughput can be very small since it divides by an entire one second.

4.3.3.7 Throughput Graph

The following figure depicts the Throughput Graph.

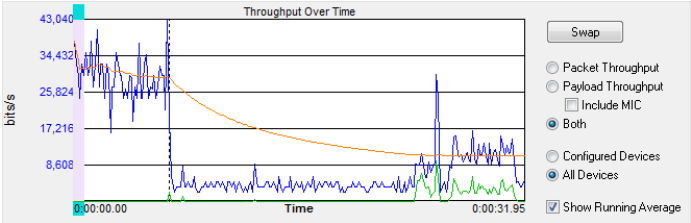


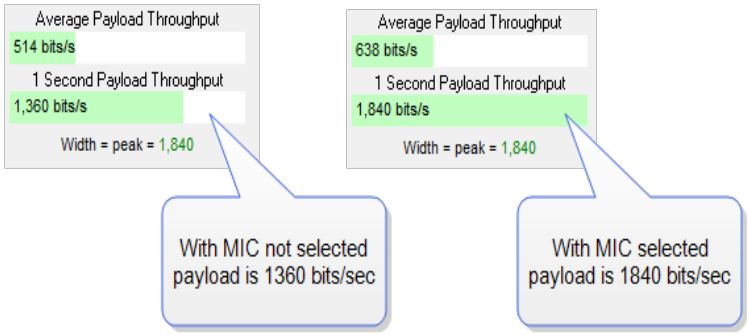
Figure 4.43 - *Bluetooth* low energy Timeline Throughput Graph

The **Swap** button switches the position of the Timeline and the Throughput graph.

Selecting Throughput Display

- Selecting **Packet Throughput** displays just the **Packet Throughput** in graph form and displays the Average and Average and 1 Second Packet Throughput on the left side of the dialog. The y-axis numbers appear in blue.
- Selecting **Payload Throughput** displays just the **Payload Throughput** in graph form and displays the Average and Average and 1 Second Payload Throughput on the left side of the dialog.. The y-axis numbers appear in green.
- Selecting **Include MIC** will include the transmitted 32 bit Message Integrity Check data in the throughput.

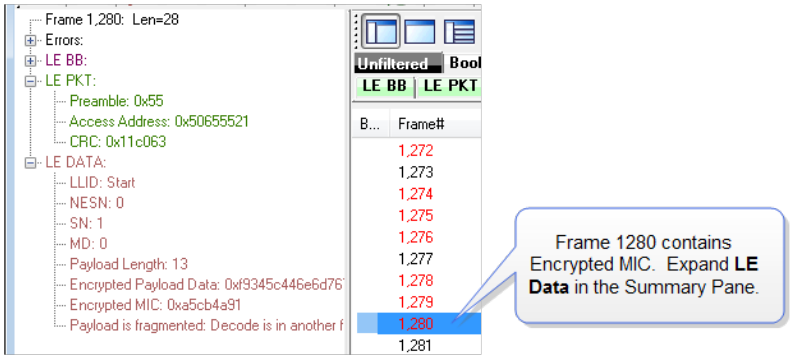
You may want to include Message Integrity Checks in your throughput even though MIC is not application data. MICs are transmitted and you may want to included in the throughput as a measure of how active your radio was.



In this example the 1 Second Payload Throughput is 1,360 bits/sec when **Include MIC** is not checked. By checking the **Include MIC** box the **MIC** data is included in the throughput data and **1 Second Payload Throughput** increases to 1,840 bits/sec. This capture file has 15 MICs in the last second of the file. A MIC is 32 bits for a total of 32 bits X 15 MICs = 480 bits.

The easiest way to view MIC data is to use the **Frame Display**.

1. Using the **Decoder** pane scroll through the frames until LE Data shows "Encrypted MIC".
2. Place the cursor on the Encrypted MIC data and while holding the



left mouse button drag the field to the **Summary** pane.

3. An **Encrypted MIC** column is added to the **Summary** pane.

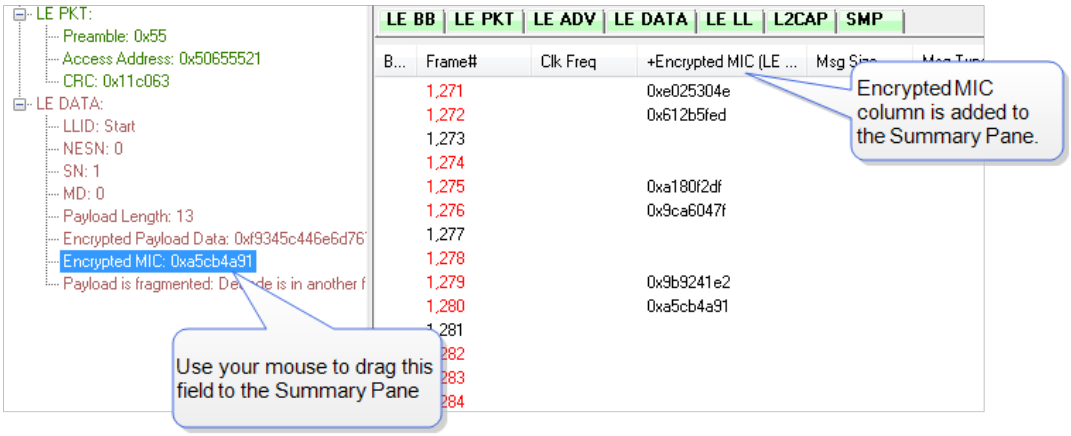


Figure 4.44 - Creating Encrypted MIC in Frame Display Summary pane

4.3.3.8 The Timeline

The **low energy Timeline** shows *Bluetooth* packets within a specific period of time. Time is shown as one or more contiguous segments. Within each segment are one or more source access address or radio rows.

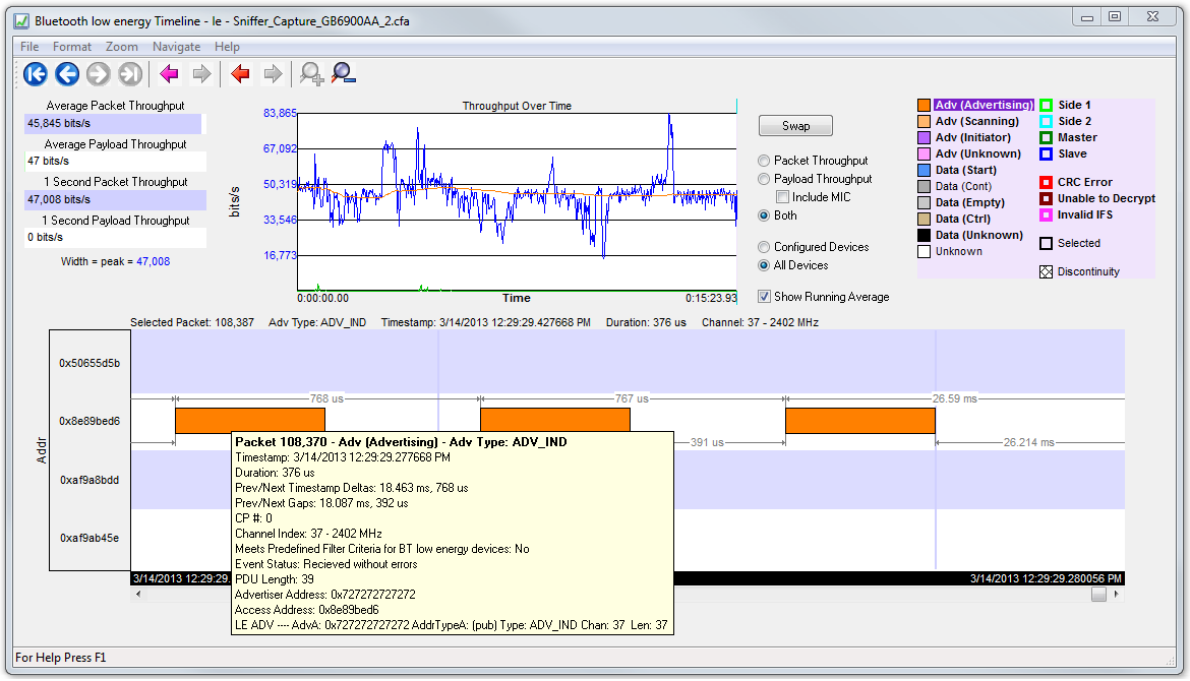


Figure 4.45 - *Bluetooth***low energy Timeline**

4.3.3.9 How Packets Are Displayed

Bluetooth low energy packets are displayed in the low energy timeline in Segments and Rows.

- Segments are "pieces" of the timeline. You can zoom in to show just one segment, or you can zoom out to show multiple segments. In multiple segment displays the segments are contiguous from top to bottom. Refer to the diagram below. The top-most segment contains the beginning timestamp on the left. The timeline proceeds from left to right in a segment, and continues in the next segment down beginning on the left of that segment. If you zoom out to show two segments the viewable timeline appears in those two segments. You will use the scroll bar on the right to scroll through the timeline.

  In a one-segment display the viewable timeline appears in that one segment. You will scroll through the timeline using the scroll bar appearing at the bottom of the timeline display.

- Rows show either the access address of the configured devices or of all discovered devices. Because the segments are contiguous in multiple segment displays, the rows in each segment are identical.

In the following diagram we see a three segment display showing the timeline flow.

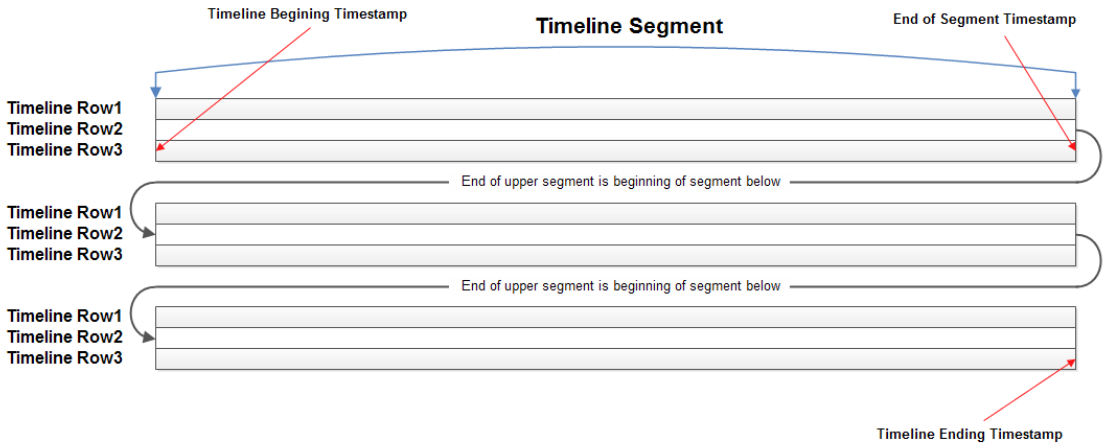
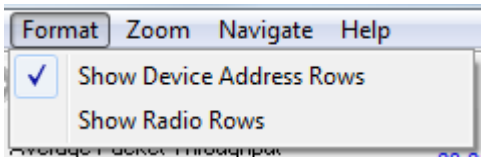


Figure 4.46 - Diagram of low energy Timeline Flow with Segment and Row Relationship

- Rows can display either source device access addresses or the three radios receiving the data..You choose with methods by selecting **Show Device Address Rows** or **Show Radio Rows** from the **Format** menu.

4.3.3.10 Format Menu



Show Device Address Rows will display rows of packets from sending devices. The source device address will appear on the left of each row.

Show Radio Rows will display rows packets received on radios 0,1, or 2. The radio number will appear on the left of each row.

- The **Addr** rows display packets sent by that access address for all devices or configured devices. You select **All Devices** or **Configured Devices** using the radio buttons.The address shown is the access address for the device.

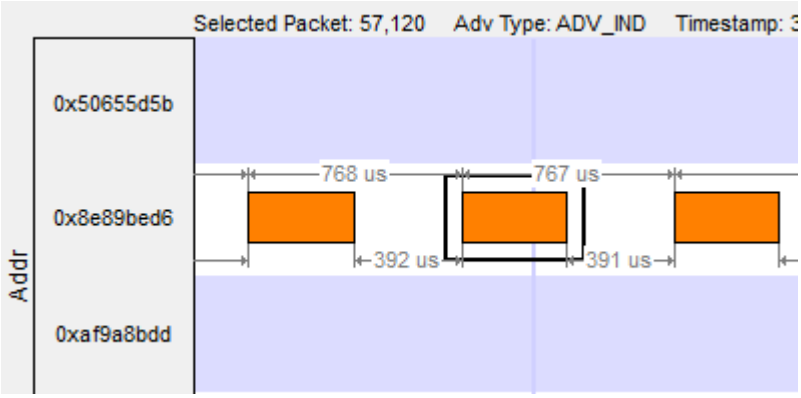


Figure 4.47 - Device Address Rows

- The **Radio** rows display packets received by that radio (0, 1, or 2).

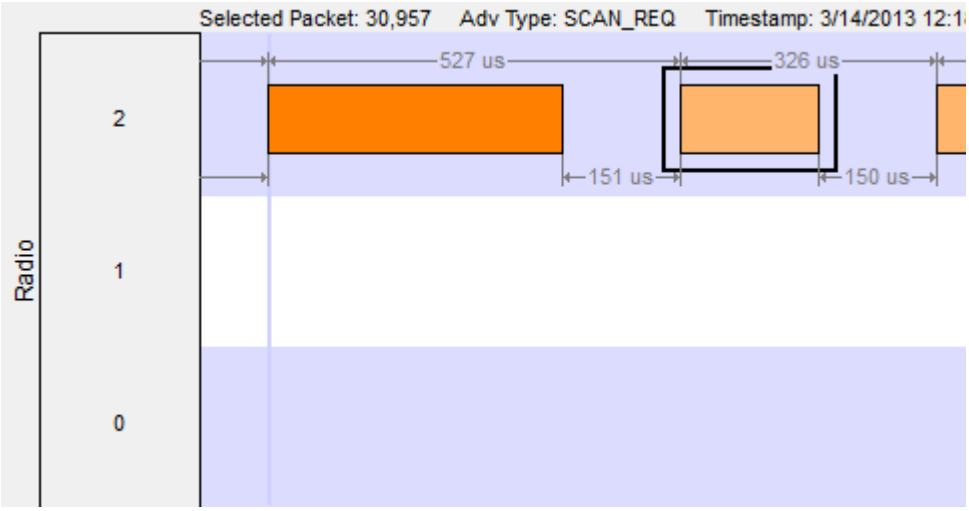


Figure 4.48 - Radio Rows

- The mouse wheel scrolls the timeline horizontally when displaying a single segment, and scrolls vertically when displaying multiple segments
- You can also zoom by using the right-click menu (which displays magnification values), using the + and - Zoom buttons on the toolbar, or by selecting a value from the Zoom menu.
- Packet length indicates duration
- The **Timeline** and **Frame Display** are synchronized so the packet range selected by the user in one is automatically selected in the other. For the selected packet range, the **Timeline** shows various duration values (**Gap**, **Timestamp Delta**, and **Span**), but only if both the first and last packet in the range are available in the **Timeline**. If not, those values are shown as “n/a”. Packets that are not displayed in the **Timeline** are Sniffer Debug packets, non-LE packets (e.g. WiFi), and packets that are not from a **Configured Device** the **Configured Devices** radio button is checked.

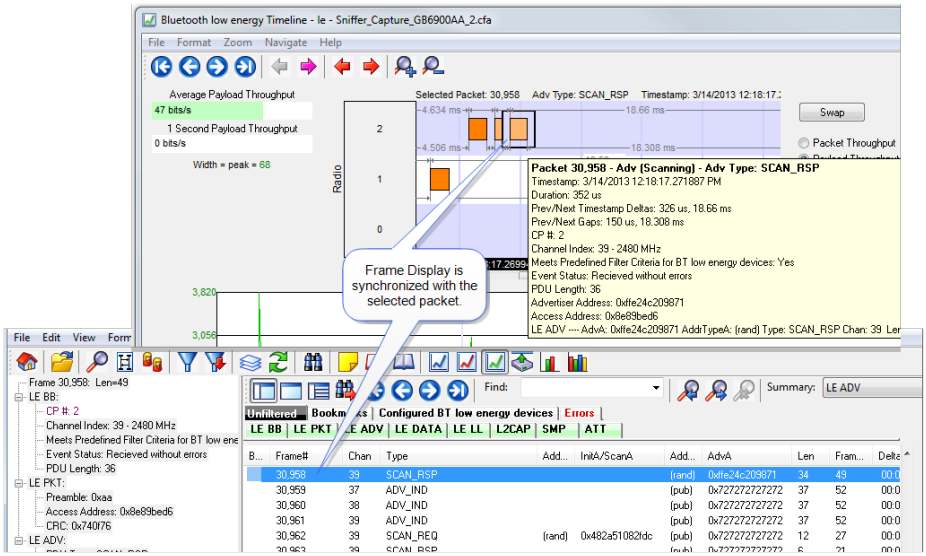


Figure 4.49 - **low energy Timeline** and **Frame Display** Packet Synchronization

4.3.3.11 low energy Timeline Visual Elements

The low energy Timeline consists of the following visual elements:

- Time Markers - Time markers indicated by vertical blue lines are shown at 1.25 ms intervals. The markers are provided to help visualize the timescale and are also useful when using dual-mode chips that do BR/EDR and LE at the same time. Time markers snap to the beginning of the first data packet by default, but they can be snapped to the beginning or end of any packet by right-clicking on a packet and selecting **Align Time Marker to Beginning of Packet** or **Align Time Marker to End of Packet**. All other markers will shift relative to that new reference point.

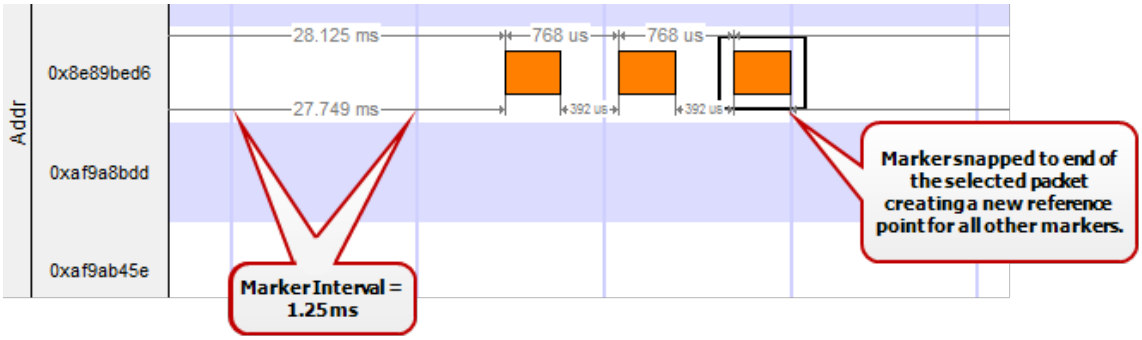


Figure 4.50 - Timeline Markers Shown Snapped to End of Packet

- Timestamp - The beginning and ending timestamp for each segment is displayed beneath each segment. When showing multiple segments the beginning timestamp is the same as the ending timestamp of the previous segment.

  In addition to the timestamps the segment information bar shows the zoom value in the center of the bar.

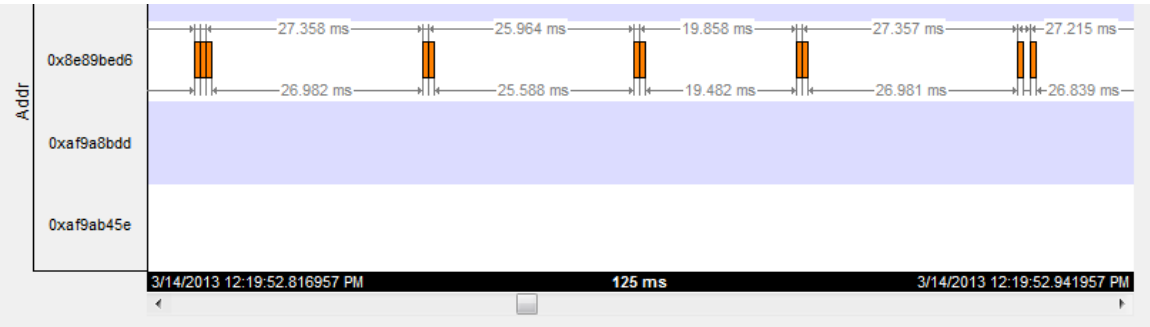


Figure 4.51 - Bluetooth le Timeline Segment Timestamp and Zoom Value

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

- Packet Info Line - The packet info line appears just above the timeline and displays information for the currently selected packet.

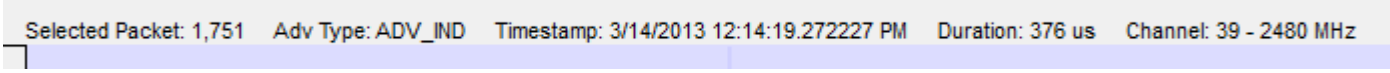


Figure 4.52 - Bluetooth le Timeline Packet Info Line

- When you select multiple packets, the info line includes:
  - Gap - duration between the end of the first selected packet and the beginning of the last selected packet.
  - Timestamp Delta - Duration between the beginnings of the first and last packets selected.
  - Span - Duration between the beginning of the first selected packet and the end of the last selected packet

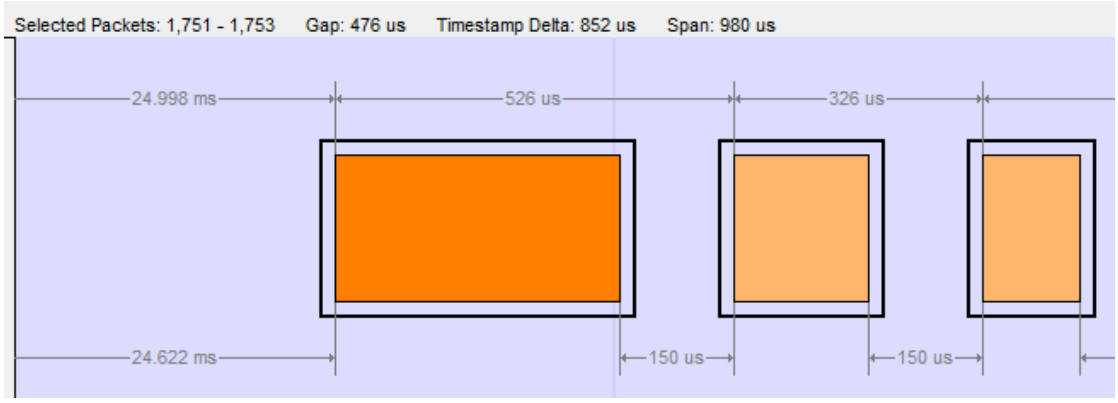


Figure 4.53 - Bluetooth le Timeline Packet Info Line for Multiple Selected Packets

- Floating Information Window (aka Tooltip) - The information window displays when the mouse cursor hovers on a packet. It persists as long as the mouse cursor stays on the packet.
- Discontinuities - Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.
- Packet Status - Packet status is indicated by color codes. Refer to low energy Timeline Legends.
- Right-Click Menu. - The right-click menu provides zooming and time marker alignment.

- Graphical Packet Depiction - each packet within the visible range is graphically depicted. See the Packet Depiction section.
- Swap Button - The Swap button Swap switches the position of the Timeline and the Throughput graph.
- Show Running Average - -Selecting this check box shows a running average in the Throughput Over Time graph as an orange line Show Running Average .

4.3.3.12 low energy Packet Discontinuities

The following figure depicts a discontinuity between two packets.

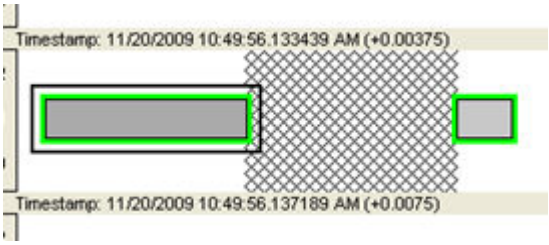


Figure 4.54 - Bluetooth® low energy Packet Discontinuity

To keep the timeline and the throughput graph manageable, big jumps in the timestamp are not represented linearly. Instead, they are shown as discontinuities. A discontinuity exists between a pair of packets when the timestamp delta (the timestamp of the second packet minus the timestamp of the first packet) is (1) more than 4.01 seconds or (2) is negative. The reason that the discontinuity trigger is set at 4.01 seconds is because the maximum connection interval time is 4 seconds.

A discontinuity is indicated by a cross-hatched pattern drawn between two packets and a corresponding vertical dashed line in the throughput graph. When the timestamp delta is greater than 4.01 seconds, the discontinuity is a cosmetic convenience that avoids excessive empty space. When the timestamp delta is negative, the discontinuity is necessary so that the packets can be drawn in the order that they occur.

4.3.3.13 low energy Timeline Navigating and Selecting Data

Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous invalid interframe spacing (IFS), next or previous error packet, and the first or last packet.

- If there is no selected packet in the timeline, **First Packet** , **Next Packet** , and **Last Packet** are enabled, but **Previous Packet** is not.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the **Frame Display**.
  - Single Segment Navigation:
    - Selecting **Previous Packet** will select the next packet in time (moving back in time to the left) regardless of which row it is on. If the previous packet is not in the display or if a portion of the packet is visible, the display will scroll to the next packet and it will appear selected on the left of the display. The timestamp will change with the scrolling of the display.

    - Selecting **Next Packet** will select the next packet in time (moving forward in time to the right). If the next packet is not in the display, the display will scroll to the next packet and it will appear selected on the right of the display. The timestamp will change with the scrolling of the display.

  - Multiple Segment Navigation:

    - Selecting **Previous Packet** will select the next packet moving back in time (to the left) on the segment and will select the previous packet regardless of which or segment it is in.

      If the selected packet overlaps with the previous segment, the display will show the packet selected in both segments.

      If the previous packet is not shown in the timeline display or a portion of the packet is displayed,the display will move the view port back in time and will display the selected packet in the top segment on the left edge. Each segment's timestamps will synchronously change as the view port scrolls backwards in time.

    - Selecting Next Packet will select the next packet moving forward in time (to the right)on the to the next packet regardless of which row or segment it is in.

      If the next packet overlaps on a following segment, the display will show the packet selected in both segments.

      If the next packet is not shown in the timeline display on any segment or a portion of the packet is displayed, the display will move the view port forward in time and will display the selected packet in the bottom segment on the right edge. Each segment's timestamps will synchronously change as the view port scrolls forward in time. All subsequent selected next packets will appear on the right of the bottom segment.

- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline it is also becomes selected in the **Frame Display**. When multiple packets are selected in the timeline, only one of them is selected in the **Frame Display**.
- The keyboard left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.
- The mouse scroll wheel will scroll the timeline as long as the cursor is in the dialog.

4.3.3.14 low energy Timeline Zooming

Zoom features can be accessed from the **Bluetooth low energy Timeline Zoom** menu by right-clicking on the **Timeline** window.

A couple of things to remember about Zooming.

- Zooming using the toolbar buttons in a single segment display is relative to the center of the display. That is as you zoom out those packets on the left and right halves will move closer to the center. If you zoom in, those packets in the left and right halves will move towards the left and right edges respectively.
- Zooming using the toolbar buttons in a multiple segment display is relative to the number of segments. If you have a single display and zoom out they will become two segments, then three segments, then six, and so forth.
- Selecting a Zoom icon (+ or -) on the toolbar zooms in our out.
- The current Zoom setting is shown in the center of the timeline segment information bar at the bottom of each timeline segment.

- If you are in multiple segments the segment information bar will show the zoom level with the text " (Contiguous time segment *x/n*)" where "*x*" is 1,2, 3… segment and "*n*" is the total number of segments. For example: :"(Contiguous time segment 2/3)".

4.3.3.15 Zoom menu

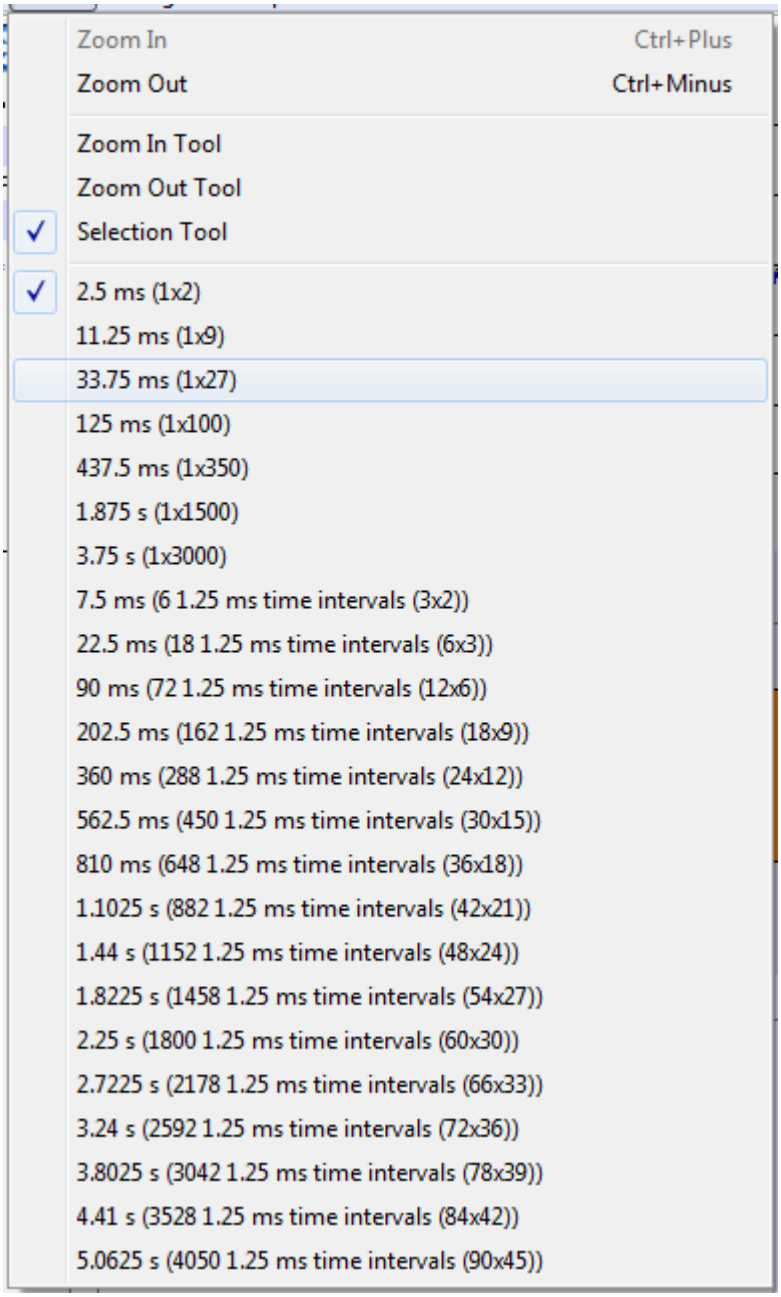
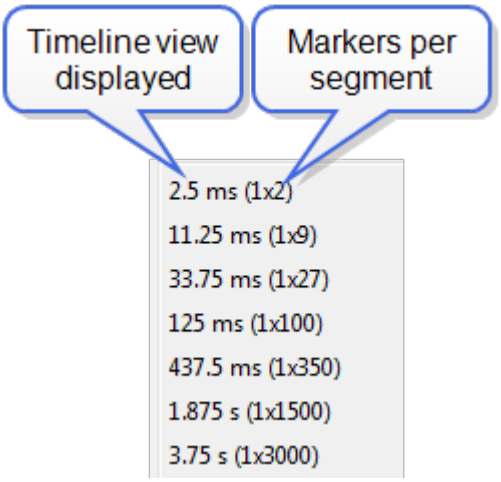


Figure 4.55 - low energy Timeline Zoom menu

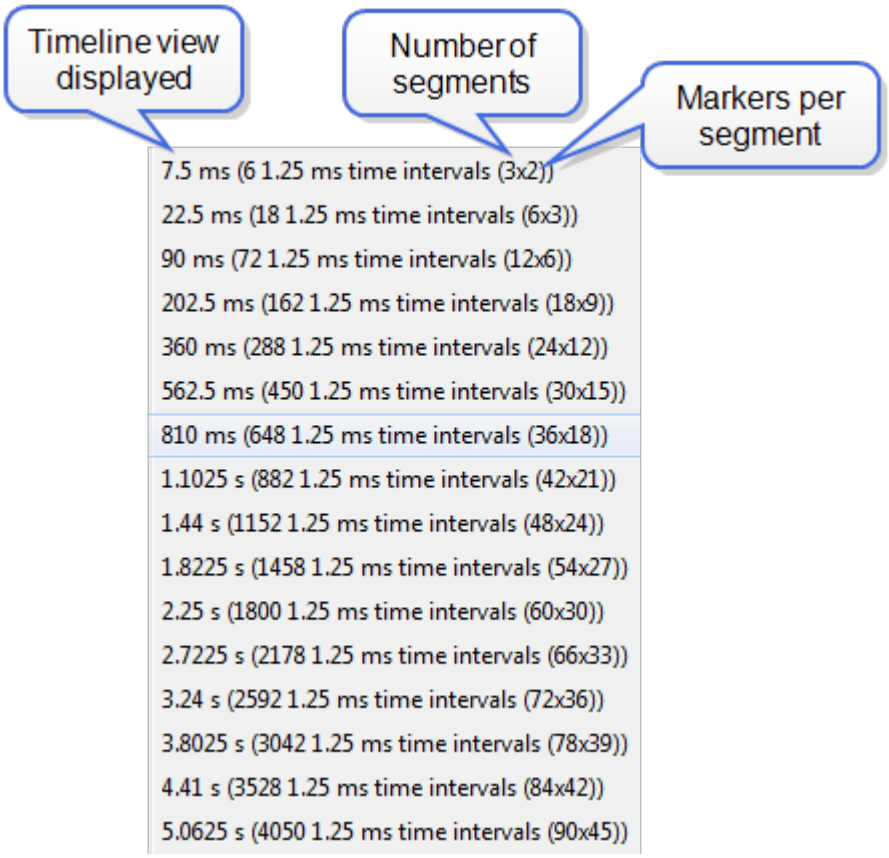
4.3.3.16 Single Segment Zoom



Zoom Menu Single Segment: Each selection defines the timeline displayed, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "33.75 ms (1x27)" will display "33.75 ms" of the throughput graph in "1" segment with "27" markers.

The scroll bar at the bottom of the segment will scroll the throughput graph view port.

4.3.3.17 Multiple Segments



Zoom Menu Multiple Segment: Each selection defines the timeline view port, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "7.5 ms (6 1.25 ms time intervals

(3x2))" will display "7.5 ms" of the total timeline in "3" segments of with "2" markers per segment for a total of "6" markers.

The scroll bar at the left of the segments will scroll the view through the timeline.

4.3.4 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.

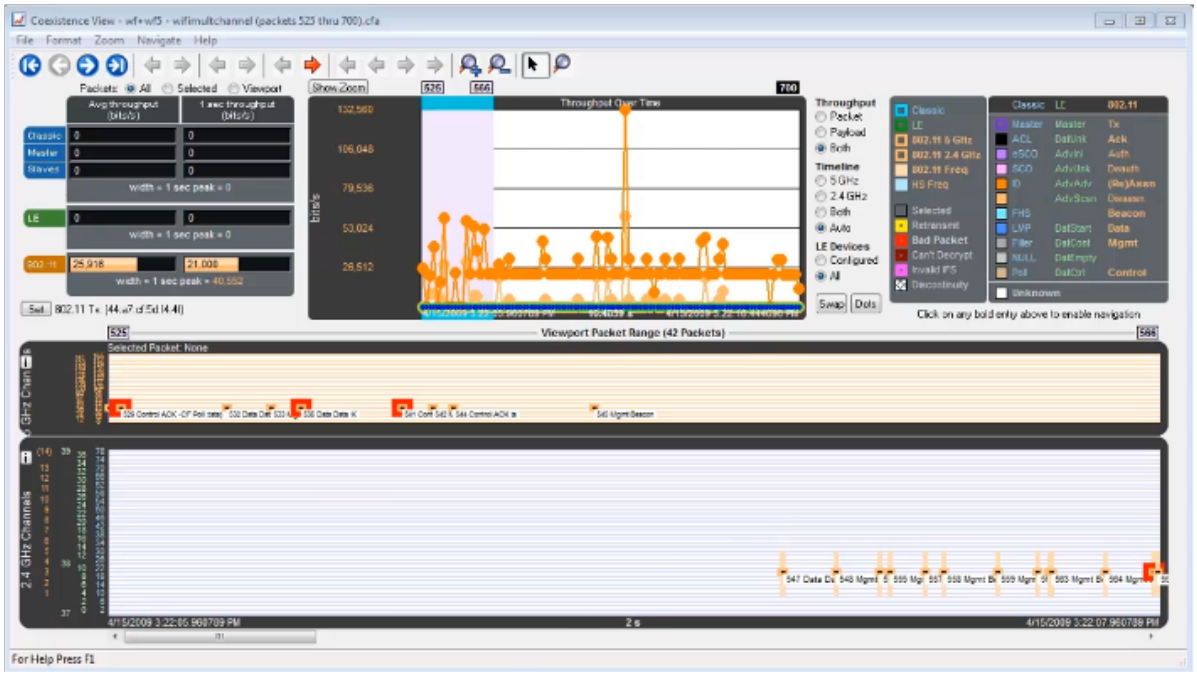
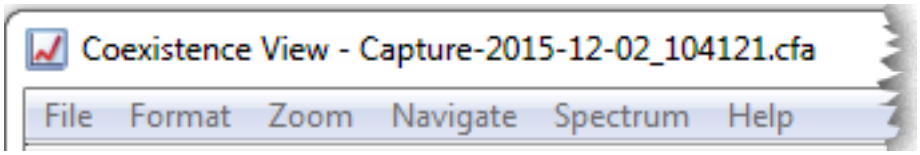


Figure 4.56 - Coexistence View Window

4.3.4.1 Coexistence View Menus



The following tables describe each of the Coexistence View Menus.

Table 4.9 - Coexistence View File Menu Selections

Selection	Description
Reset	Resets the Coexistence View window to its default settings.
Exit	Closes the Coexistence View window.

Table 4.10 - Coexistence View Format Menu Selections

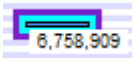
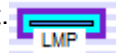
Selection	Description
Show Packet Number	When checked, the packet number shows below the packet in the Viewport. 
Show Packet Type	When checked, the packet type shows below the packet in the Viewport. 
Show Packet Subtype	When checked, the packet subtype shows below the packet in the Viewport, if applicable.
Hide Packet Text	When checked, hides any text shown below the packet in the Viewport. Applies the text shown by the Show Packet Number, **Show Packet Type**, and **Show Packet Subtype** menu selections.
Auto Hide Packet Text When Duration > 31.25 ms.	When checked, automatically hides any text shown below the packet in the Viewport when the Viewport duration exceeds 31.25 ms. Applies the text shown by the Show Packet Number, **Show Packet Type**, and **Show Packet Subtype** menu selections. The Viewport duration is shown at the bottom of the Viewport. This selection reduces display clutter when viewing a larger timeline section.
Increase Auto Hide Packet Count from 4,000 to 20,000 (May Be Slow)	When not checked, the default, the packets in the viewport are hidden if the number of visible packets exceeds 4,000. When checked, the default count increased from 4,000 to 20,000 packets before the packets are hidden. Choosing this selection may slow down the displaying of the packets.
The following three selections are mutually exclusive.	
Use All Packets for Throughput Indicators	When checked, all captured packets are used for average throughput calculations and all packets in the last one second of the capture session are used for the 1 sec throughput. See on page 189 for more information. Performs the same function as the throughput indicator **All** radio button.
Use Selected Packets for Throughput Indicators	When checked, the packets selected in the Viewport are used for average throughput calculations, and selected packets in the one second before the last selected packet are used for the 1 sec throughput. See on page 189 for more information. Performs the same function as the throughput indicator **Selected** radio button.
Use Viewport Packets for Throughput Indicators	When checked, all packets appearing in the Viewport are used for average throughput calculations, and all packets in the one second before the last packet in the Viewport are used for the 1 sec throughput. See on page 189 for more information. Performs the same function as the throughput indicator **Viewport** radio button.
Set 802.11 Tx Address	When checked, this selection 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. Performs the same function as the SET button. Refer to on page 197
The following three selections are mutually exclusive.	

Table 4.10 - Coexistence View Format Menu Selections (continued)

Selection	Description
Show Packet Throughput	When checked, the Throughput Graph and Throughput Indicator shows data based on packet throughput. Performs the same function as the **Throughput Packet** radio button.
Show Payload Throughput	When checked, the Throughput Graph and Throughput Indicator shows data based on payload throughput. Performs the same function as the **Throughput Payload** radio button.
Show Both Packet And Payload Throughput	When checked, the Throughput Graph will graph both the data based on packets throughput in darker colors and payloay throughput in lighter colors. The Throughput Indicator will show calculations based on packet throughput. Performs the same function as the **Throughput Both** radio button.
The following four selections are mutually exclusive.	
Show 5 GHz Timeline	When checked, the 5 GHz Timeline is visible and the 2.4 GHz Timeline is not visible. Only 802.11 5 GHz packets are shown. Performs the same function as the **Timeline 5 GHz** radio button.
Show 2.4 GHz Timeline	When checked, the 2.4 GHz Timeline is visible and the 5 GHz Timeline is not visible. The timeline will show Classic Bluetooth, Bluetooth Low Energy, and 802.11 2.4 GHz packets. Performs the same function as the **Timeline 2.4 GHz** radio button.
Show Both 2.4 GHz and 5 GHZ Timelines	When checked, the 2.4 GHz Timeline and the 5GHZ Timeline is visible. Performs the same function as the **Timeline Both** radio button.
Show Timelines Which Have or Had Packets (Auto Mode)	When check,shows only timelines which have had packets at some point during this session. If no packets are present, the 2.4 GHz Timeline is visible. Performs the same function as the **Timeline Auto** radio button.
The following two selections are mutually exclusive.	
Show Low Energy Packets From Configurated Devices Only	When checked, shows in the 2.4 GHz Timeline only packets from *Bluetooth* low enegry devices configured for this session, and uses these packets for throughput calculations. Performs the same function as the **LE Devices Configured** radio button.
Show All Low Energy Packets	When checked, shows in the 2.4 GHz Timeline all Bluetooth low energy packets captured in this session, and uses these packets for throughput calculations. Performs the same function as the **LE Devices All** radio button.
Large Throughput Graph	When checked, the Throughput Graph appears in the bottom half of the window, swapping position with the timeline. When not checked, the Throughput Graph appears in its default position at the top of the window. Performs the same function as clicking the **Swap** button. See on page 193.

Table 4.10 - Coexistence View Format Menu Selections (continued)

Selection	Description
Show Dots in Throughput Graph (Dots Reveal Overlapped Data Points)	When checked, displays dots on the Throughput Graph. 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. Performs the same function as the **Dots** button. See on page 194.
Show Zoomed Throughput Graph	When checked, dispalys a 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. Performs the same function as the **Show Zoom** button. When not checked, the Zoomed Throughput Graph is hidden. Performs the same function as the **Hide Zoom** button. See on page 194 .
Freeze Y Scales in Zoom Throughput Graph	Only active when the Zoomed Throughput Graph is visible. When checked, it freezes the y-axis scales and makes it possible to compare all time ranges and durations. Performs the same fuction as the **Freeze Y** button, which appears with the Zoomed Throughput Graph. When not checked, the y-axis scales are unfroozen. Performs the same function as the **Unfreeze Y** button, which appears with the Zoomed Throughput Graph. See on page 194
Show Tooltips in Upper-Left Corner of Screen	When checked, Timeline and Throughput Graph tooltips will appear in the upper-left corner of your computer sceen. You can relocate the tool tip for convenience or to see the timeline or throughput graph unobstructed while displaying packet information. See on page 201.

Table 4.11 - Coexistence View Zoom Menu Selections

Selection	Description	Hot Key
Zoom In	When clicked, Viewport time duration decreased.	Ctrl+Plus
Zoom Out	When clicked, Viewport time duration increases	Ctrl+Minus
The following two selectioins are mutually exclusive.		
Scroll Tool (Mouse Wheel Scrolls - Ctrl Key Switches to Zoom Tool)	When checked, sets the mouse wheel to scroll the Viewport. Pressing the Ctrl key while scrolling switches to zooming the Viewport.	
Zoom Tool (Mouse Wheel Zooms- Ctrl Key Switches to Scroll Tool)	When checked, sets the mouse wheel to zoom the Viewport. Pressing the Ctrl key while zooming switches to scrolling the Viewport.	

Table 4.11 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
Zoom To Time Range of Selected Packets	Active only when packets are selected. When clicked, the Viewport duration changes to the time range covered by the selected packets.	
Zoom To Throughput Graph Data Point	When clicked, the Viewport duration changes to the time range of the Throughput Graph selected data point.	
Custom Zoom (Set by Zoom To Time Range of Selected Packets, Zoom To Throughput Graph Data Point, or dragging Viewport Slide)	Automatically checked when taking any zoom action other than the fixed Viewport zoom durations listed below.	
The following 21 selections are mutually exclusive.		
150 usec	Each of these Zoom selections sets the Viewport and the Timeline to a fixed time duration.	
300 usec		
625 usec (1 Bluetooth slot)		
1.25 msec (2 Bluetooth slots)		
1.875 msec (3 Bluetooth slots)		
2.5 msec (4 Bluetooth slots)		
3.125 msec (5 Bluetooth slots)		
6.25 msec (10 Bluetooth slots)		
15.625 msec (25 Bluetooth slots)		
31.25 msec (30 Bluetooth slots)		
62.5 msec (100 Bluetooth slots)		
156.255 msec (250 Bluetooth slots)		
31.25 msec (500 Bluetooth slots)		
625 msec (1,000 Bluetooth slots)		
1 sec (1,600 Bluetooth slots)		
2 sec (3,200 Bluetooth slots)		
3 sec (4,800 Bluetooth slots)		
4 sec (6,400 Bluetooth slots)		
5 sec (8,000 Bluetooth slots)		
10 sec (16,000 Bluetooth slots)		
20 sec (32,000 Bluetooth slots)		

Note: Right-clicking anywhere in the **Coexistence View** window will open the **Zoom** menu in a pop-up.

Table 4.12 - Coexistence View Navigate Menu Selections

Selection	Description	Hot key
First Packet	When clicked, the first packet in the session is selected and displayed in the Timeline. Performs the same function as the First Packet button.	Home
Last Packet	When clicked, the last packet in the session is selected and displayed in the Timeline. Performs the same function as the Last Packet button.	End
Previous Packet	When clicked, the first packet occurring in time prior to the currently selected packet is selected and displayed in the Timeline. Performs the same function as the Previous Packet button.	Left Arrow
Next Packet	When clicked, the first packet occurring next in time from the currently selected packet is selected and displayed in the Timeline. Performs the same function as the Next Packet button.	Right Arrow
Previous Retransmitted Packet	When clicked, selects the first prior retransmitted packet from the current selection and displays it in the Timeline.. Performs the same function as the Previous Retransmitted Packet button.	
Next Retransmitted Packet	When clicked, selects the next retransmitted packet from the current selection and displays it in the Timeline.. Performs the same function as the Next Retransmitted Packet.	
Previous Invalid IFS Packet	When clicked, selects the first prior invalid *Bluetooth* low energy IFS packet from the current selection and displays it in the Timeline. Performs the same function as the Previous Invalid IFS Packet button.	
Next Invalid IFS Packet	When clicked, selects the next invalid *Bluetooth* low energy IFS packet from the current selection and displays it in the Timeline. Performs the same function as the Next Invalid IFS Packet button.	
Previous Error Packet	When clicked, selects the first prior packet with an error from the current selection and displays it in the Timeline. Performs the same function as the Previous Error Packet button.	Ctrl+Left Arrow

Table 4.12 - Coexistence View Navigate Menu Selections (continued)

Selection	Description	Hot key
Next Error Packet	When clicked, selects the next packet with an error from the current selection and displays it in the Timeline. Performs the same function as the Next Error Packet button.	Ctrl+Right Arrow
First Legend Packet	When clicked, selects the first legend packet in the session and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 198. Performs the same functions as the First Legend Packet button.	
Previous Legend Packet	When clicked, selects the first prior legend packet in time from the current selection and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 198. Performs the same functions as the Previous Legend Packet button.	
Next Legend Packet	When clicked, selects the next legend packet in time from the current selection and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 198. Performs the same functions as the Next Legend Packet button.	
Last Legend Packet	When clicked, selects the last legend packet in the session and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 198. Performs the same functions as the Last Legend Packet button.	
Toggle Display Lock	This selection is active during Live capture mode only. Checking this selection will lock the Throughput Graph and the Timeline in its current position, however the capture will continue. Not checking this selection will cause the Throughput Graph and the Timeline to scroll as data is collected.	

Note: Navigate menu selections are context sensitive. For example, If the first packet is selected, the **Next Packet** and the **Last Packet** selections are active, but the **Previous Packet** selection is inactive.

4.3.4.2 Coexistence View - Toolbar

Figure 4.57 - Coexistence View Toolbar

The toolbar contains the following selections:

Table 4.13 - Coexistence View Toolbar icons

Icon	Description
	Move to the first packet.

Table 4.13 - Coexistence View Toolbar icons (continued)

Icon	Description
	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.
	Zooming cursor.
	Scroll Lock/Unlock during live capture mode.

Table 4.13 - Coexistence View Toolbar icons (continued)

Icon	Description
	Reset during live capture mode. Clears the display.

4.3.4.3 Coexistence View - Throughput Indicators

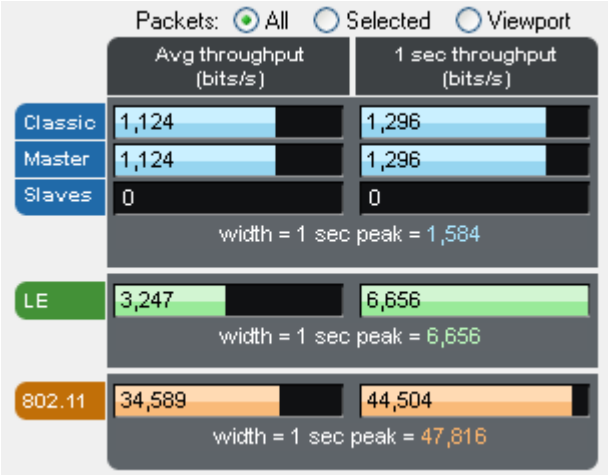


Figure 4.58 - Coexistence View Throughput Indicators

Throughput indicatorsshow 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.

4.3.4.4 Throughput

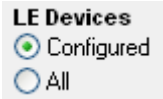
Throughput is total packet or payload size in bits of the included packets divided by the duration of the included packets, where:

- *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.

4.3.4.5 Radio Buttons

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

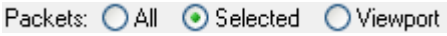
- *Bluetooth* low energy packets from non-configured devices are excluded if the **Configured** radio button in the LE Devices group is selected.
- **Frame Display** filtering has no effect here in that packets that are filtered-out in **Frame Display** are still used here as long as they otherwise meet the criteria for each radio button as described below.



4.3.4.6 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.

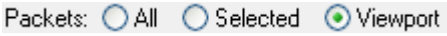
4.3.4.7 Selected radio button



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 4.59 - Timeline Header Showing Selected Packets

4.3.4.8 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.

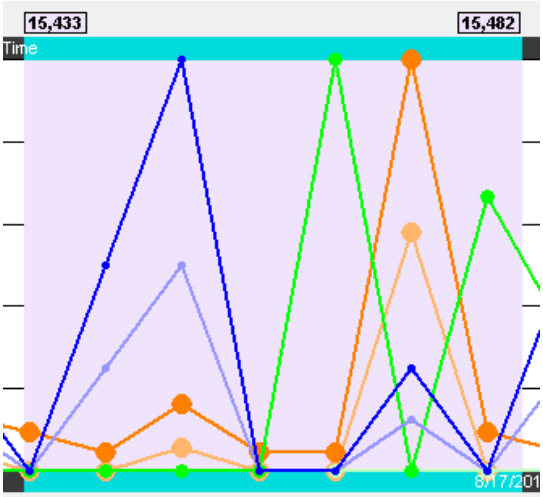


Figure 4.60 - **Throughput Graph** viewport.

4.3.4.9 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.

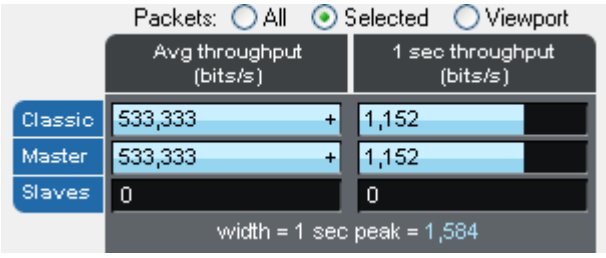


Figure 4.61 - Average throughput indicators show a plus sign (+) when the indicator width is exceeded.

Figure 4.62 - A single selected packet

4.3.4.10 Coexistence View - Throughput Graph

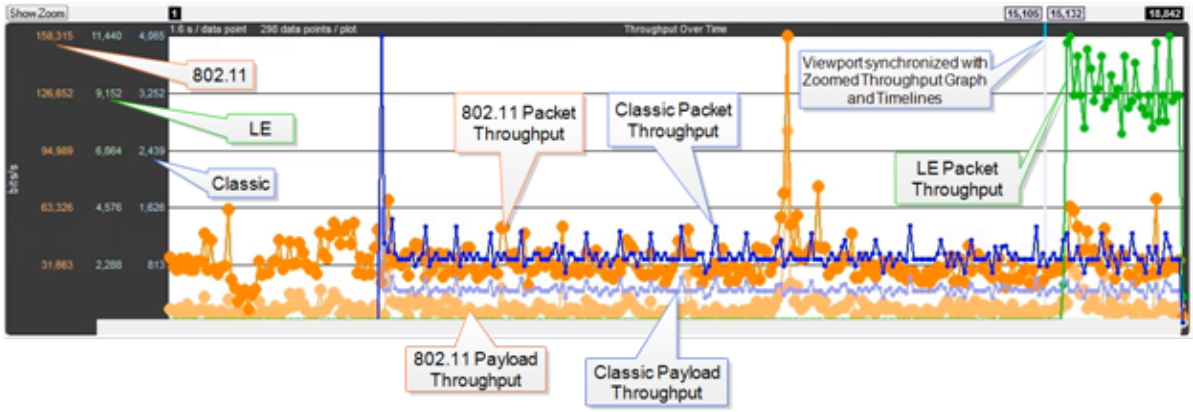


Figure 4.63 - Coexistence View Throughput Graph

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.

4.3.4.11 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.

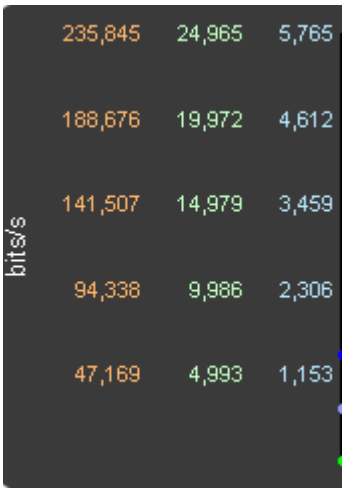


Figure 4.64 - **Throughput Graph** y-axis labels.

4.3.4.12 Excluded packets

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

4.3.4.13 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).

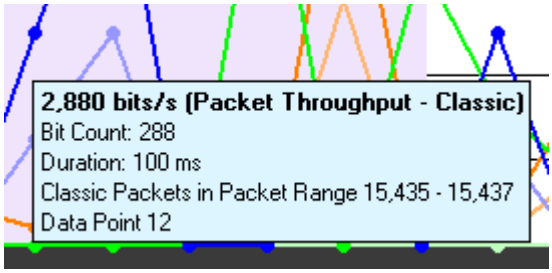


Figure 4.65 - Data point tooltip

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.

4.3.4.14 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.

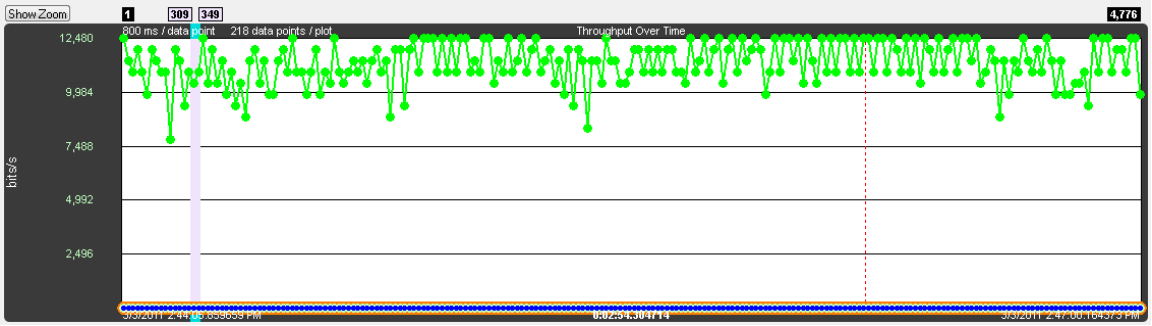


Figure 4.66 - A negative discontinuity.

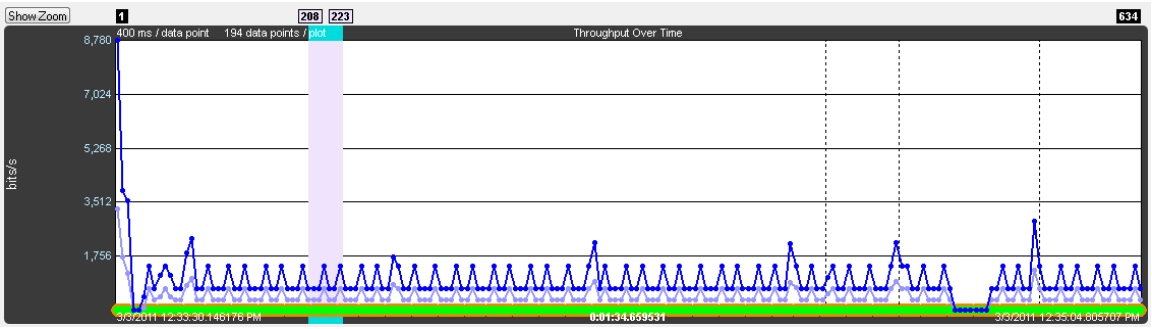


Figure 4.67 - Three positive discontinuities.

4.3.4.15 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.

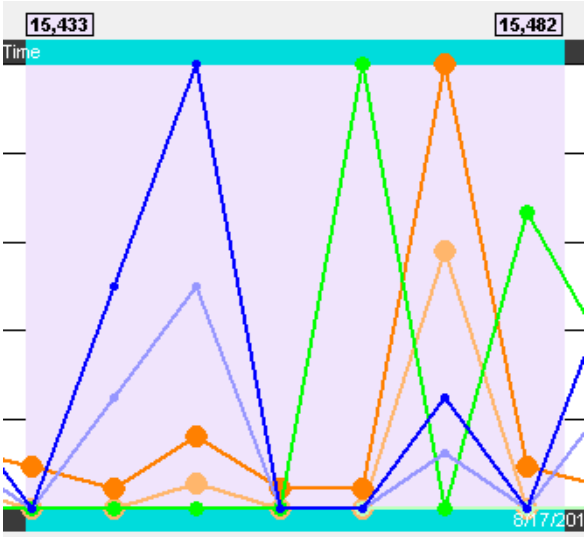


Figure 4.68 - **Throughput Graph** Viewport

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.

4.3.4.16 Swap button

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

Clicking the Swap 

button swaps the positions of the **Throughput Graph**s and the **Timeline**s.

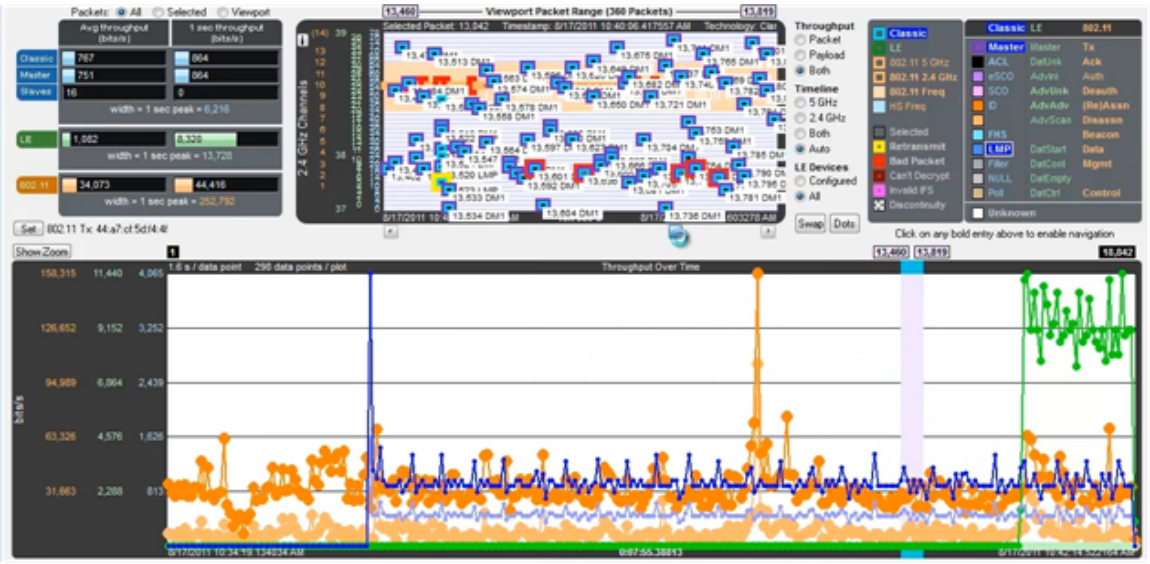


Figure 4.69 - Small Timeline and large Throughput Graph after pressing the Swap button.

4.3.4.17 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 4.70 - Dots Toggled On and Off

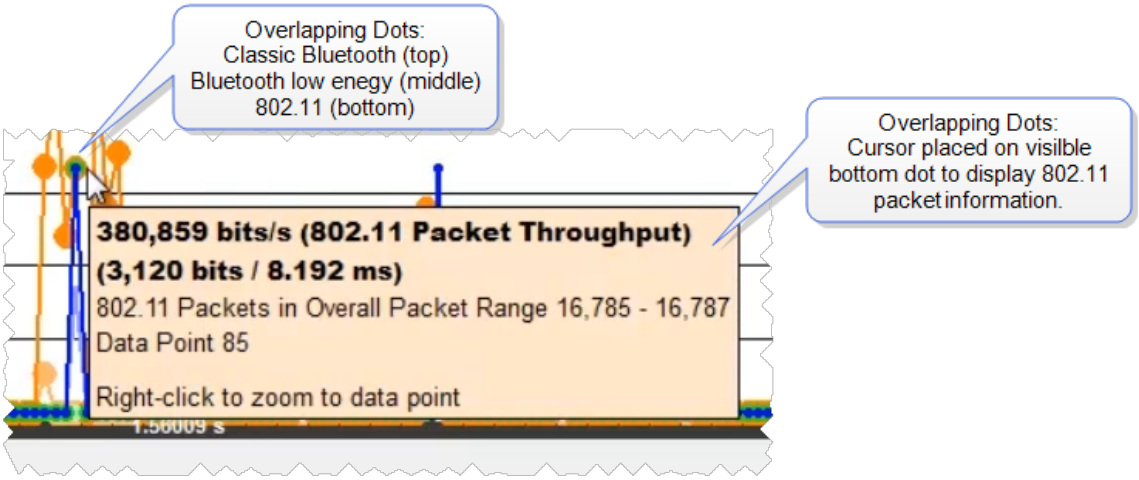


Figure 4.71 - Overlapping **Dots** Information Display

4.3.4.18 Zoomed Throughput Graph

Clicking the **Show Zoom** button Show Zoom 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.

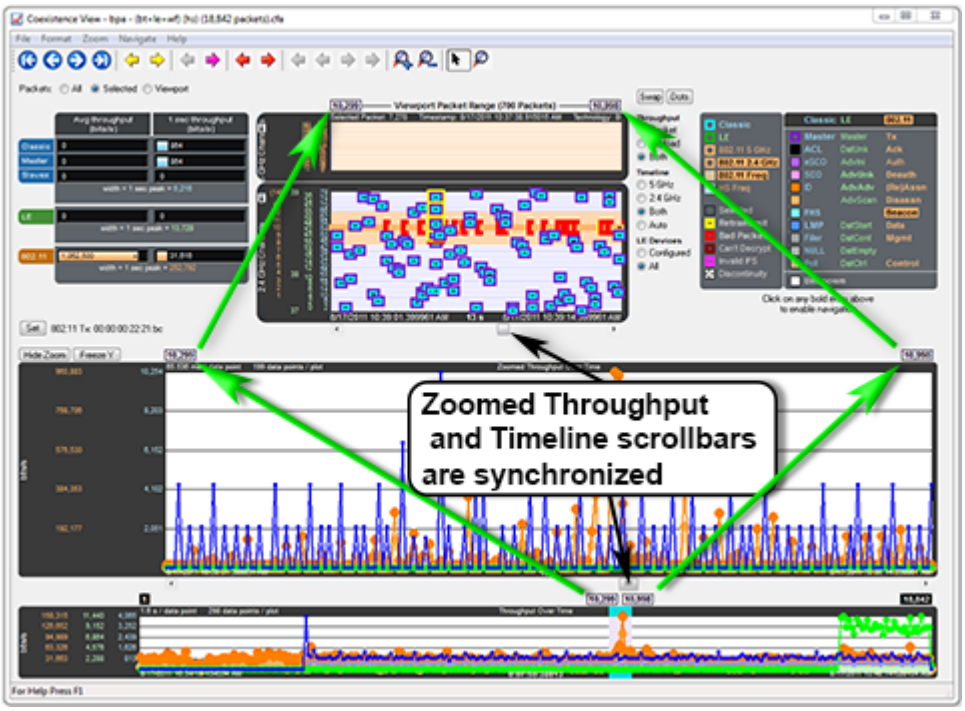


Figure 4.72 - Synchronized Zoomed Throughput Graph and View Port

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** 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 to **Unfreeze Y** and a **Y Scales Frozen** indicator appears to the right of the title. Clicking the **Unfreeze Y** Unfreeze Y button unfreezes the y-axis scales.

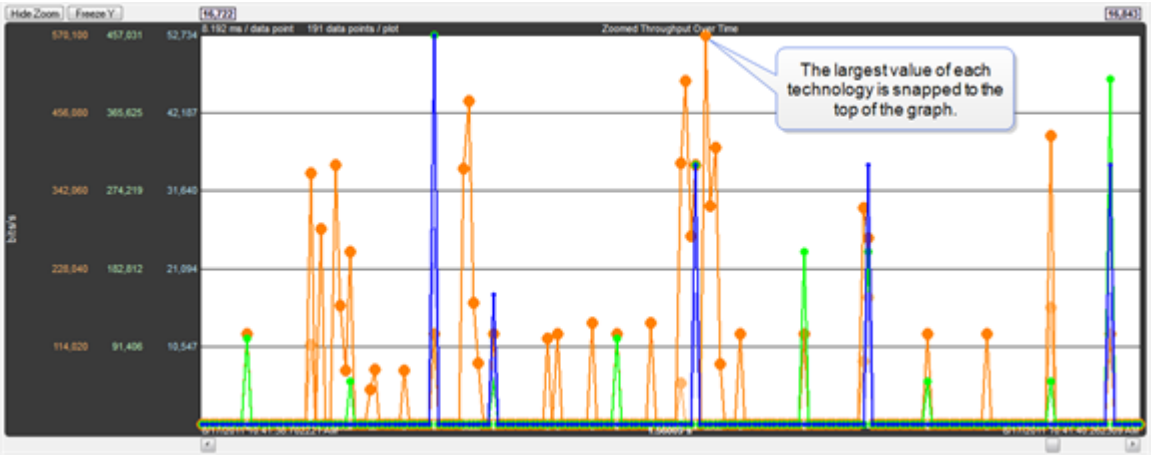


Figure 4.73 - **Zoomed Throughput Graph**- Largest Value Snaps to Top

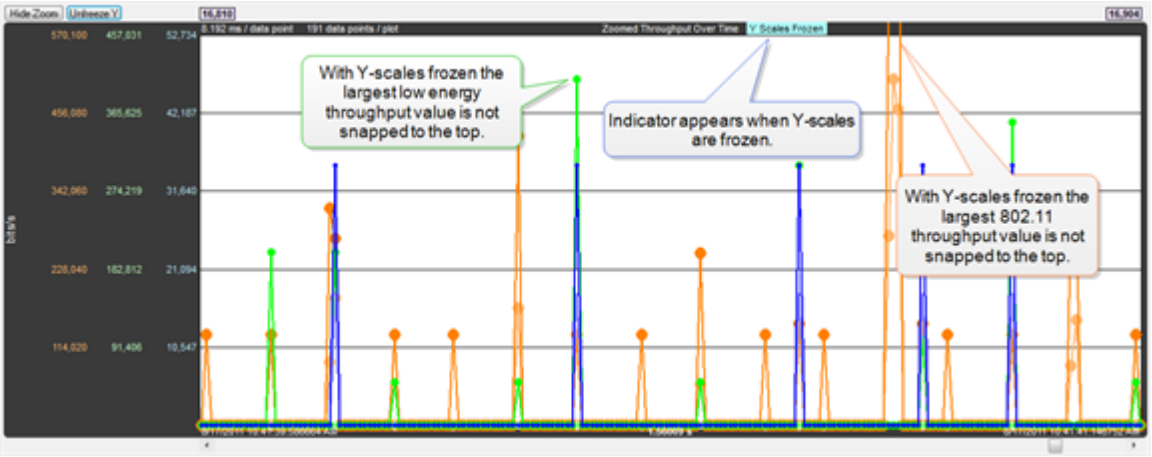
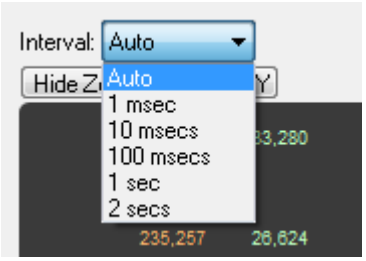


Figure 4.74 - **Zoomed Throughput Graph** - **Freeze Y** keeps the y-axis constant

Interval Menu



The **Interval** drop-down menu is used to set the duration of each data point in the Zoomed Throughput graph. The default setting is **Auto** that sets the data point interval automatically depending on the zoom level. The other menu selections provide the ability to select a fixed data point interval. Selecting from a larger to a smaller interval will display more data points. Should the number of data points exceed 30,000, no data is displayed and a warning will appear in the graph area.

4.3.4.19 Zoom Cursor

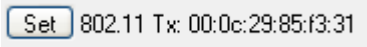
Selecting the **Zoom Cursor**  button changes the cursor to the zoom cursor  . The zoom cursor is controlled by the mouse wheel and zooms the viewport and thus the Timelines and the Zoomed Throughput Graph. The zoom cursor appears everywhere except the **Throughput Graph**, which is not zoomable, in 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.

4.3.4.20 Comparison with the *Bluetooth* Timeline's Throughput Graph

The **Throughput Graph**s 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 Graph**s, 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 Graph**s 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.

4.3.4.21 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.

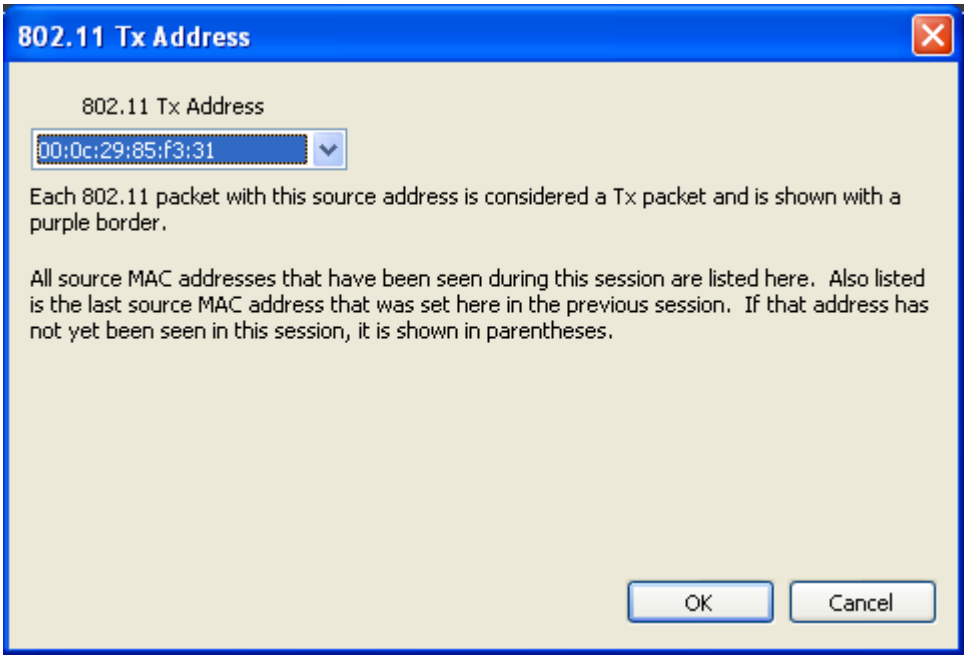


Figure 4.75 - 802.11 Source Address Dialog

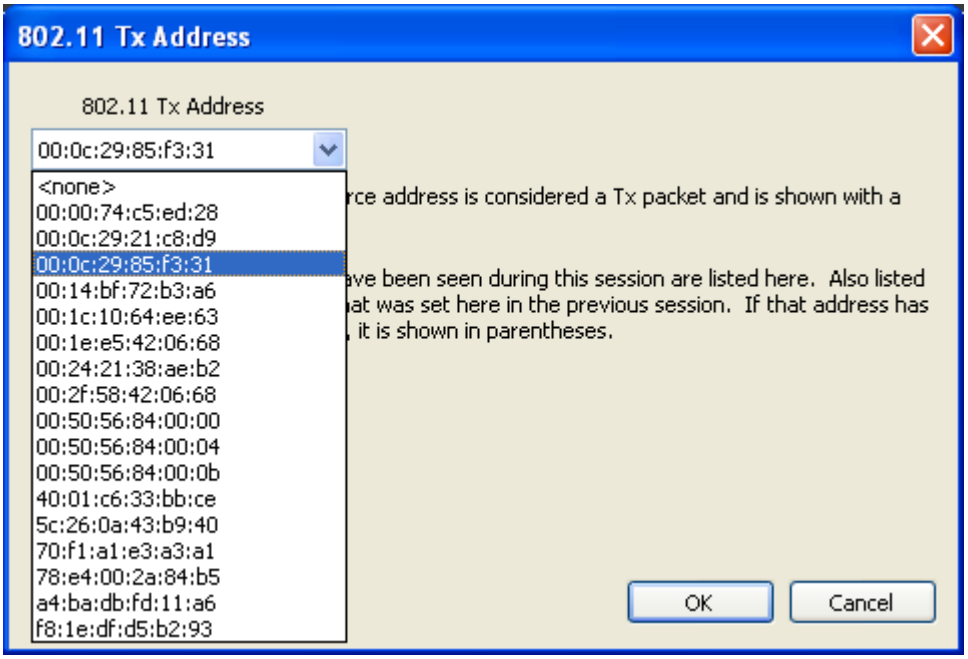
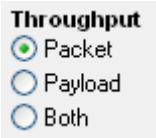


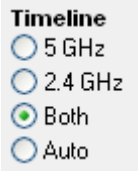
Figure 4.76 - 802.11 Source Address Drop Down Selector

4.3.4.22 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).

4.3.4.23 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.

4.3.4.24 Coexistence View – low energy 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.

4.3.4.25 Coexistence View – Legend

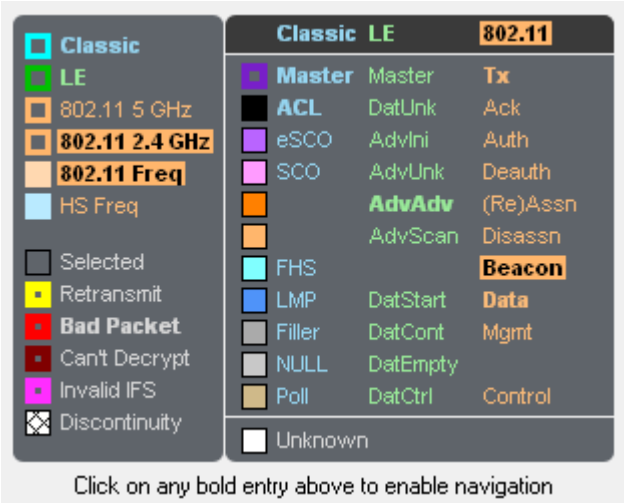


Figure 4.77 - Coexistence View Legend

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.

4.3.4.26 Coexistence View – Timelines

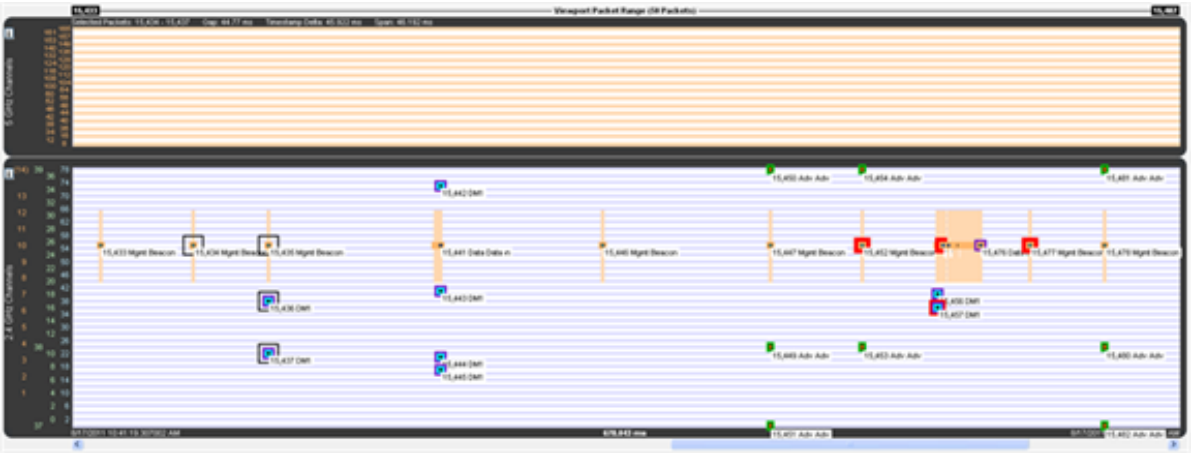


Figure 4.78 - Coexistence View Timelines

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

4.3.4.27 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.

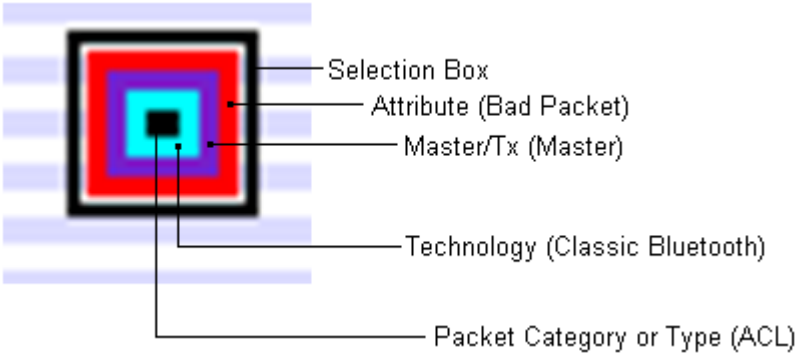


Figure 4.79 - Each packet is color-coded

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.

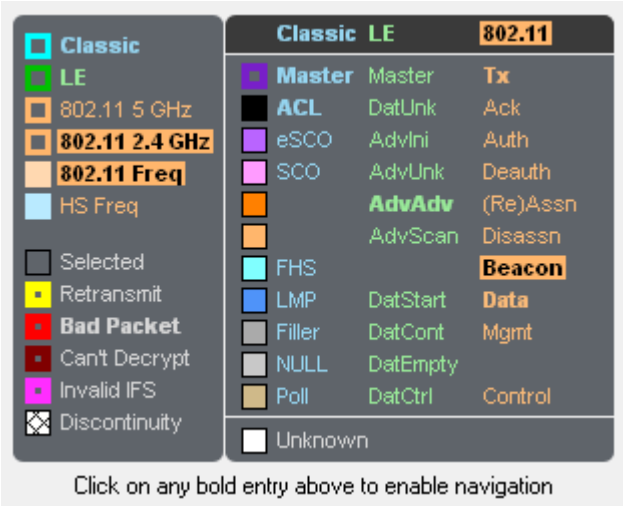


Figure 4.80 - Highlighted entries in the legend for a selected packet.

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

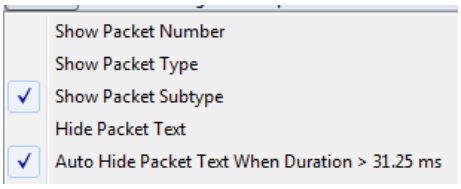
Selected Packet: 15,457 Timestamp: 8/17/2011 10:41:19.835783 AM Technology: Classic Type: DM1 Bluetooth Clock: 0x0113e610 Payload Len: 9 bytes

Figure 4.81 - **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).

Selected Packets: 15,434 - 15,437 Gap: 44.77 ms Timestamp Delta: 45.922 ms Span: 46.192 ms

Figure 4.82 - **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.

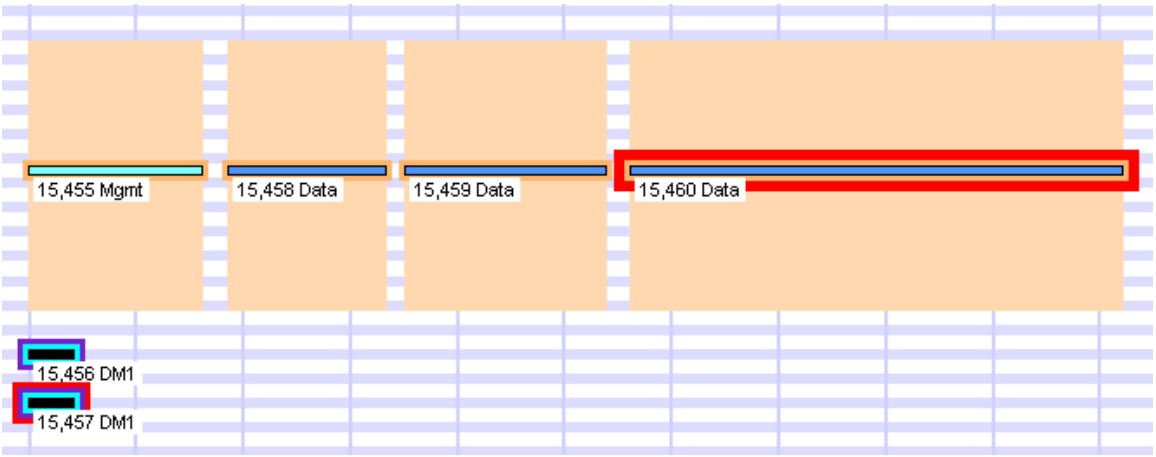


Figure 4.83 - Descriptive text on timeline packets.

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

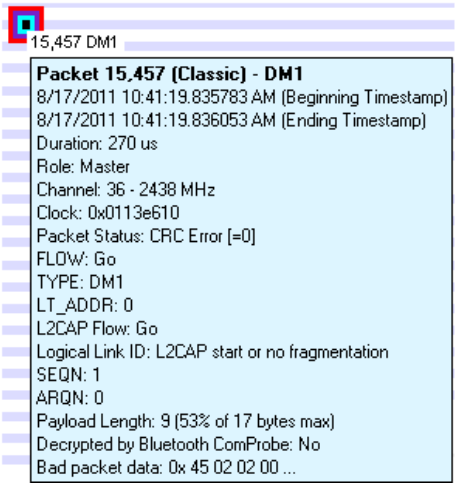


Figure 4.84 - A tool tip for a Classic *Bluetooth* packet.

4.3.4.28 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.

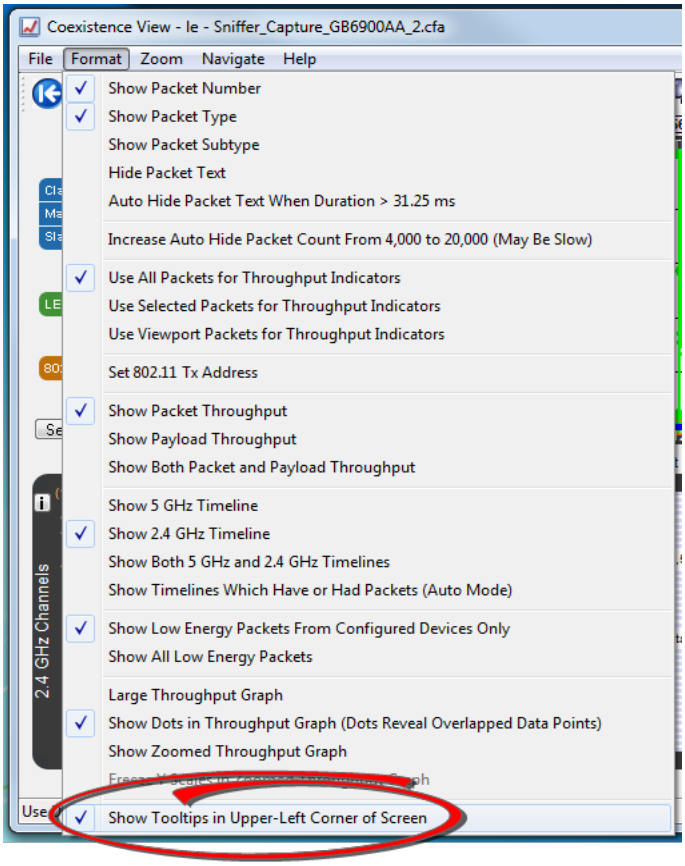


Figure 4.85 - Coexistence View Format Menu - Show Tooltips on Computer Screen

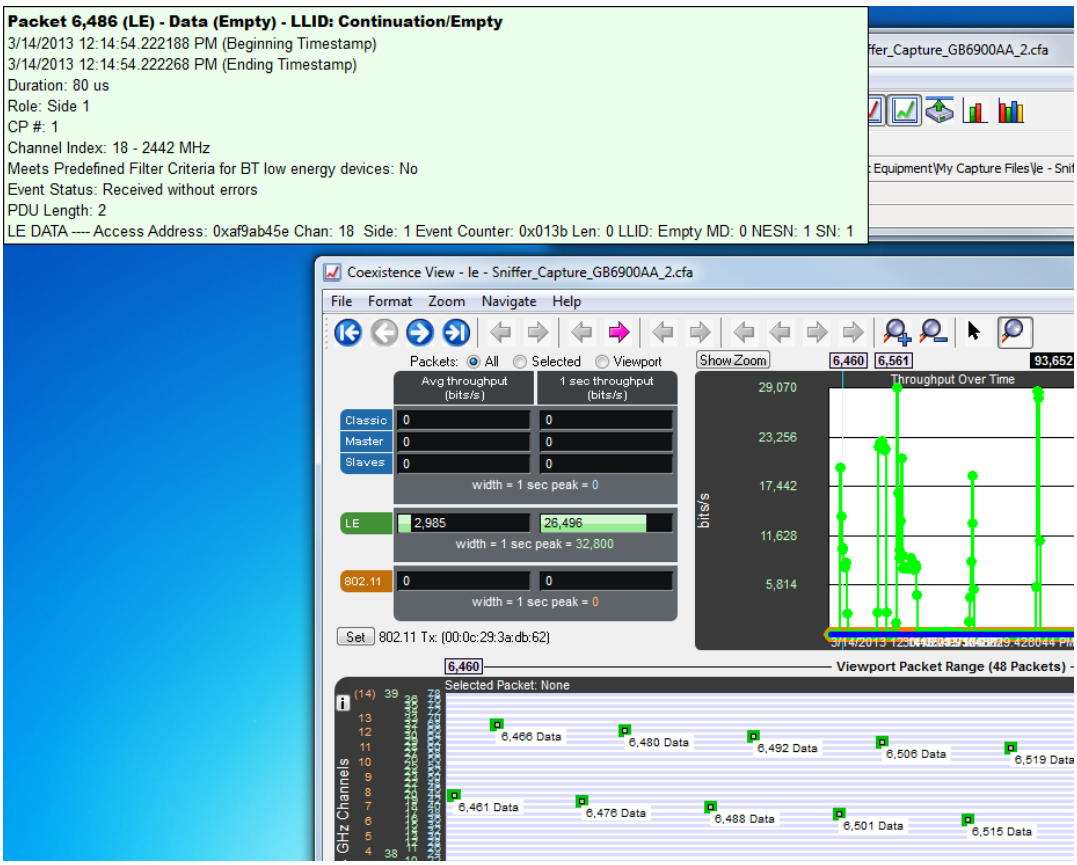


Figure 4.86 - Coexistence View Timeline Tool Tip Shown Anchored to Computer Screen

4.3.4.29 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.

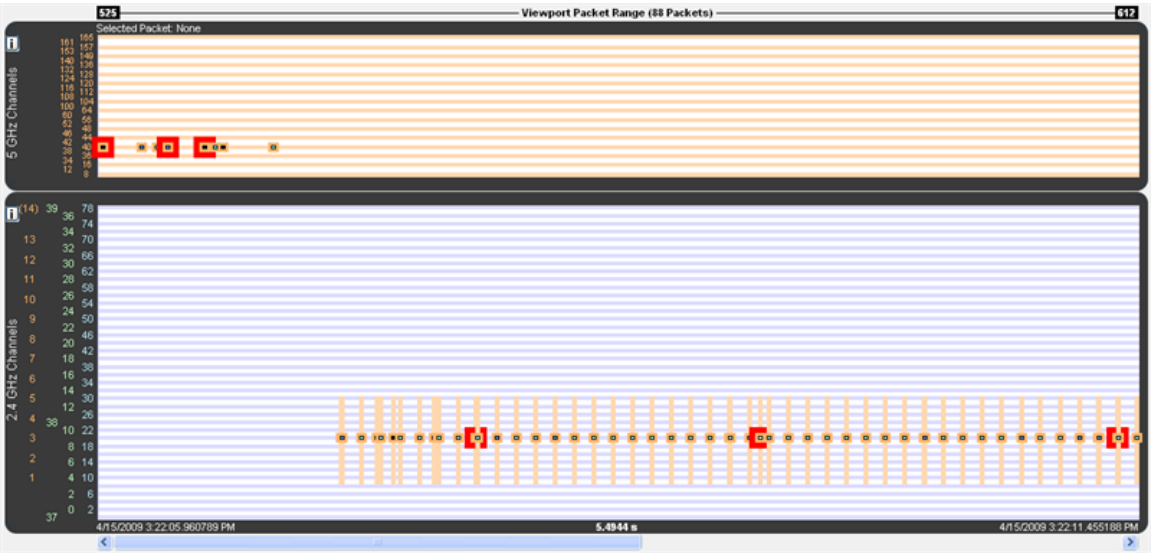


Figure 4.87 - 5 GHz and 2.4 GHz 802.11 packets

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).

< 15,417 An arrow points to the next packet when no packets are in the time range.

< 15,417 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 4.88 - 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 4.89 - 2.4 GHz information windows

4.3.4.30 *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.

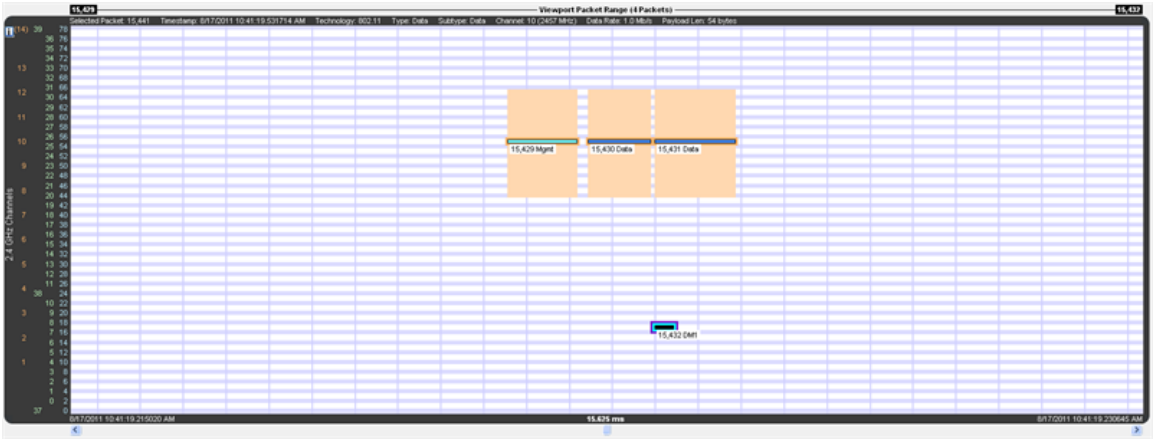


Figure 4.90 - Vertical blue lines are *Bluetooth* slot markers

4.3.4.31 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 viewport 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.

4.3.4.32 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.

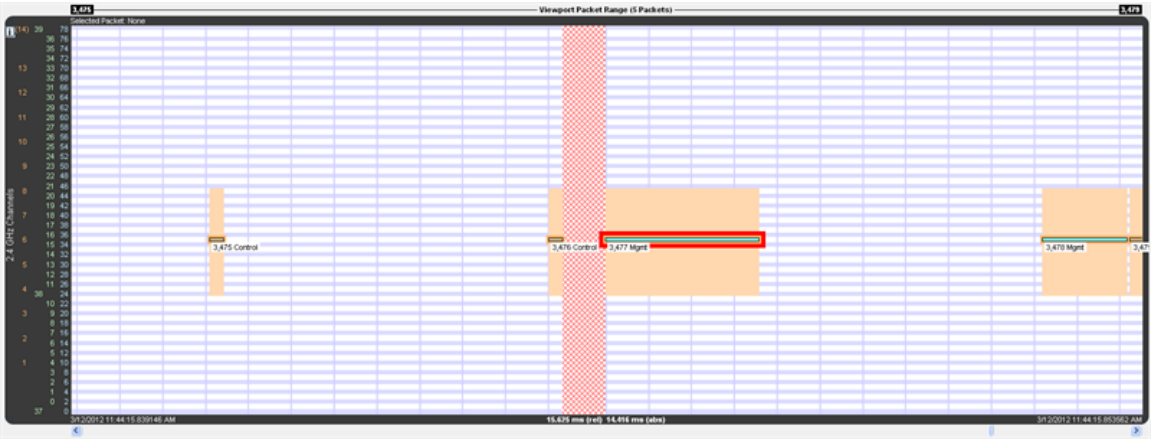


Figure 4.91 - A negative discontinuity

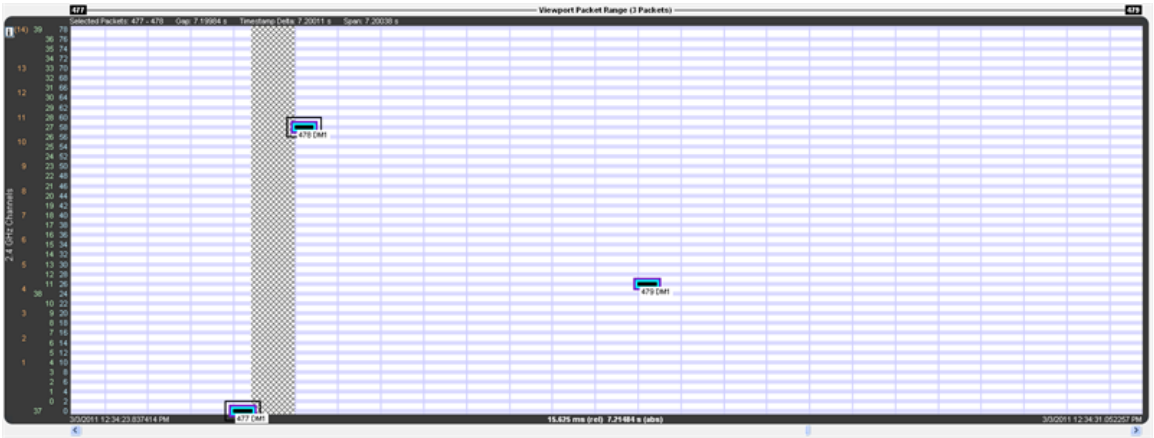


Figure 4.92 - A positive discontinuity

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.

Selected Packets: 477 - 478 Gap: 7.19984 s Timestamp Delta: 7.20011 s Span: 7.20038 s

Figure 4.93 - Timeline header with discontinuity

15.625 ms (rel) 7.21484 s (abs)

Figure 4.94 - 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

4.3.4.33 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.

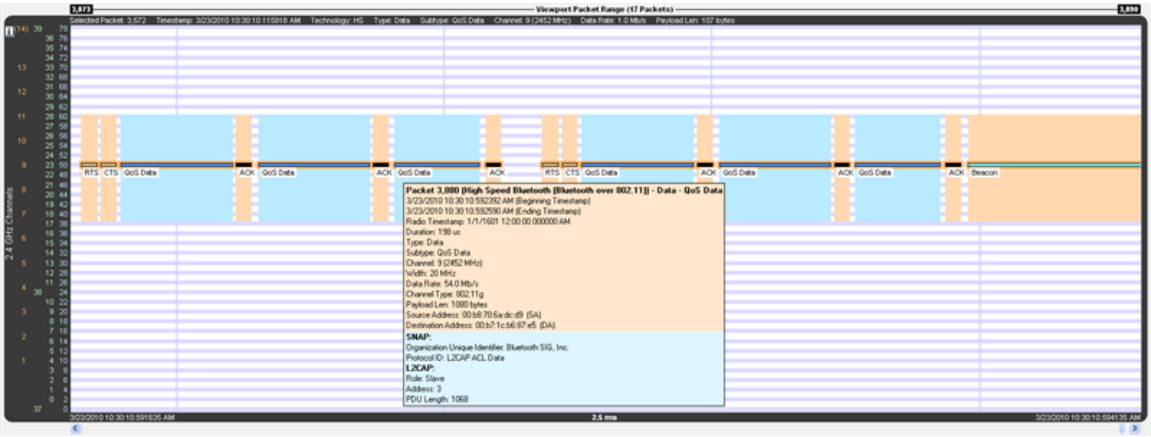


Figure 4.95 - High-speed *Bluetooth* packets have a blue frequency box and a two-tone tool tip

4.3.4.34 Coexistence View - No Packets Displayed with Missing Channel Numbers

> **Note:** This topic applies only to Classic *Bluetooth*.

Captured packets that don't contain a channel number, such as HCI and BTSnoop, will not be displayed. When no packets have a channel number the **Coexistence View Throughput Graph** and **Timelines** will display a message: "Packets without a channel number (such as HCI) won't be shown."

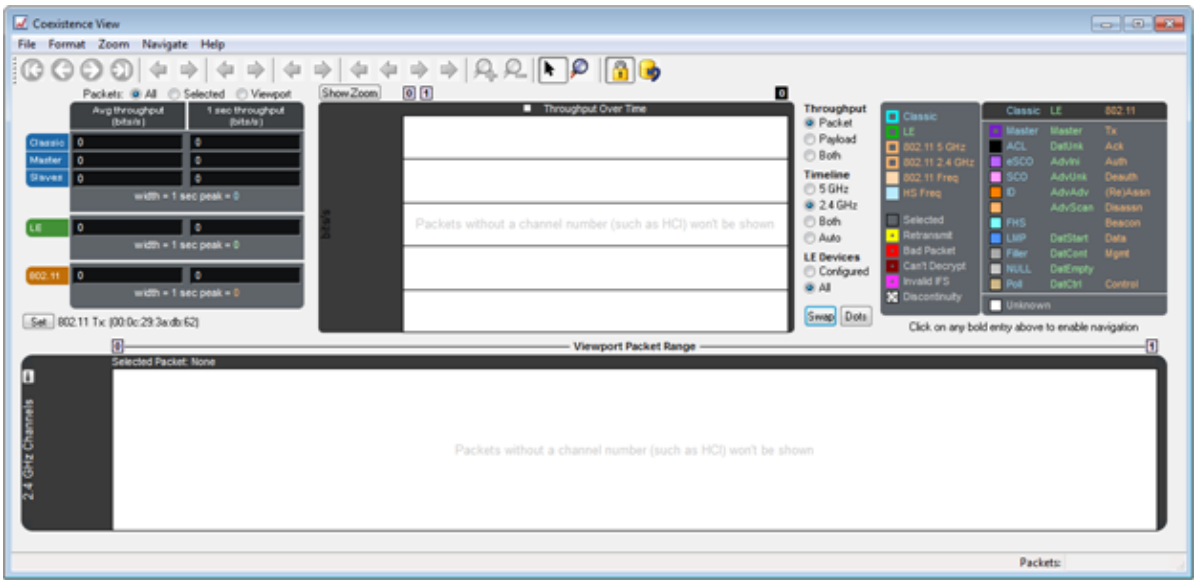


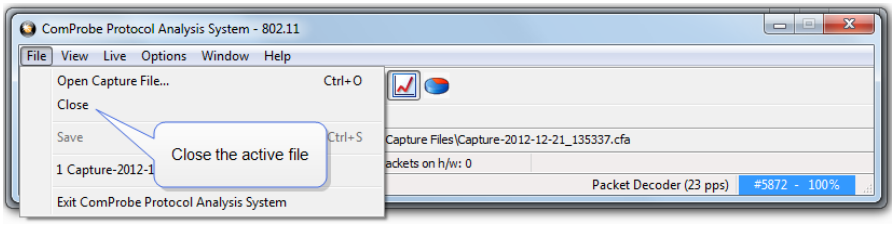
Figure 4.96 - Missing Channel Numbers Message in Timelines

4.3.4.35 High Speed Live View

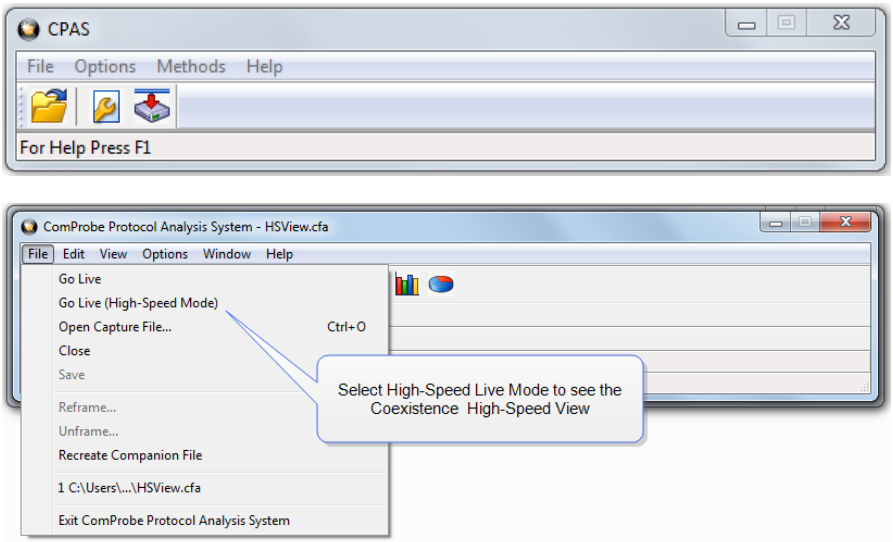
When using the Frontline® 802.11 in conjunction with other ComProbe devices, or in a stand-alone configuration, a smaller version of the standard **Coexistence View** is available. This **High Speed Live View** is essentially the **Viewport** from the standard **Coexistence View**.

When viewing **High Speed Live**, only 802.11 traffic is visible. Because *Bluetooth* packets are slow they are not visible in High Speed mode.

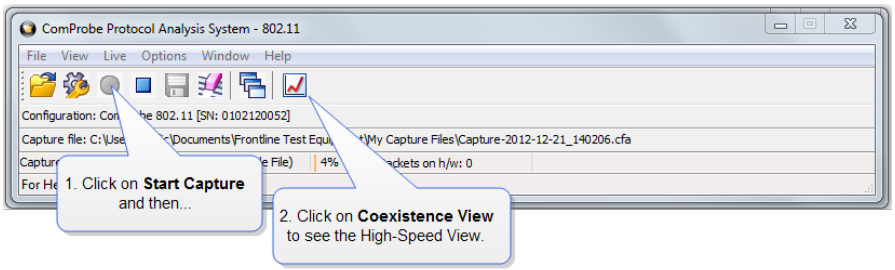
1. Click on the **Control** window **File** menu and select **Close**.



2. The **Control** window will open again. Click on the Control Window **File** menu and select **Go Live (High-Speed Mode)**



3. Click on the **Control** window **Start Capture** button to begin capturing data. Click on the **Coexistence View** button and the **High-Speed View** will appear.



The Coexistence View (High Speed Live Mode) window will appear.

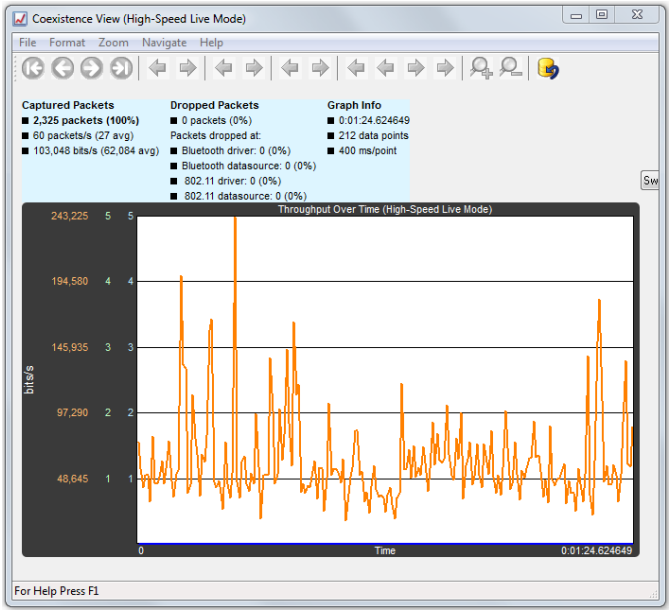


Figure 4.97 - High-Speed Live Window

4.3.4.36 Coexistence View - Spectrum

Sodera has the option to sample the 2.4 GHz RF spectrum at the Sodera unit antenna connector. The spectrum data represents the Received Signal Strength Indicator (RSSI). The spectrum data is synchronized in time to the captured *Bluetooth* packets and is displayed in the **Coexistence View** 2.4 GHz Timeline. The spectrum power level is shown as a "heat map" behind the timeline packets. The "heat map" appears in shades of blue with darker blues representing higher power levels and lighter blues representing lower power levels (white represents the lowest power level). The darkest shade of blue represents -15dBm and above, while white represents -100 dBm and below.

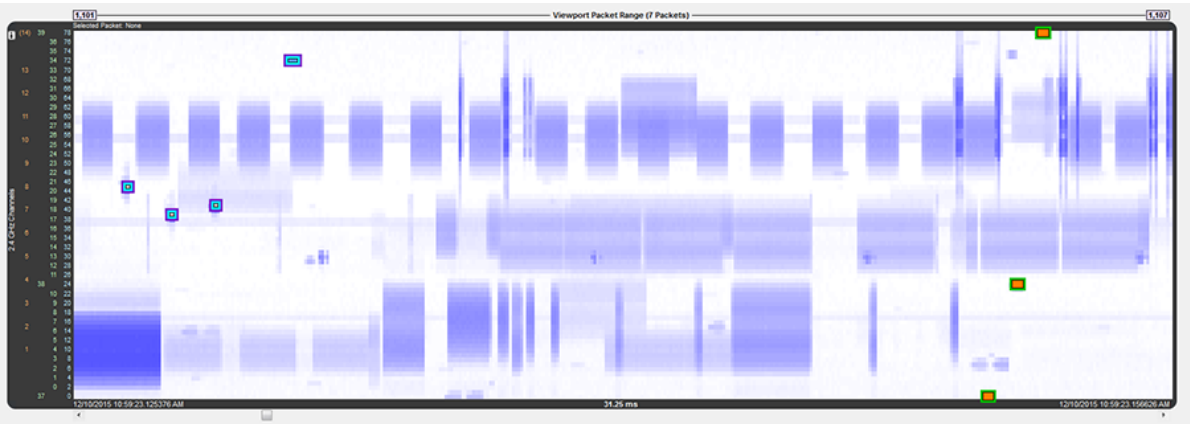


Figure 4.98 - Coexistence View Timeline with Packets and Spectrum Heat Map

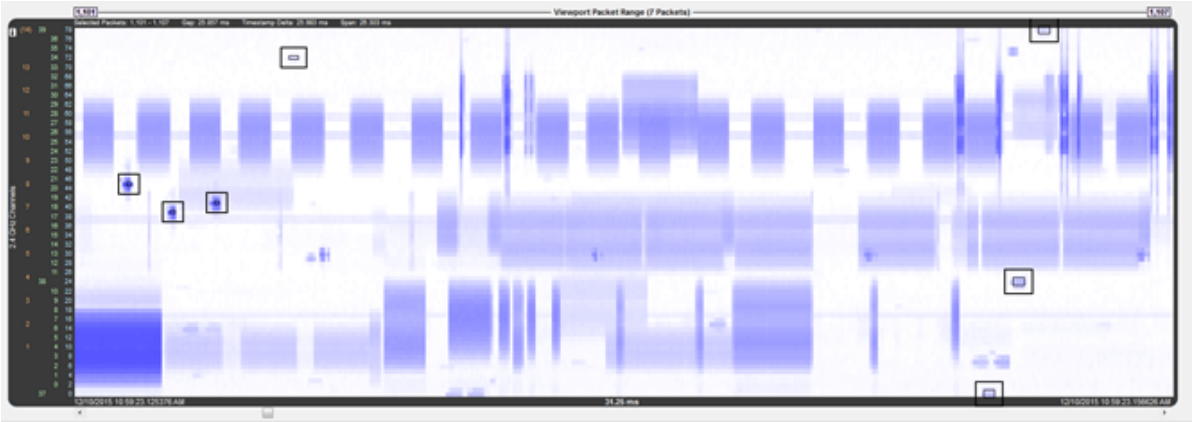
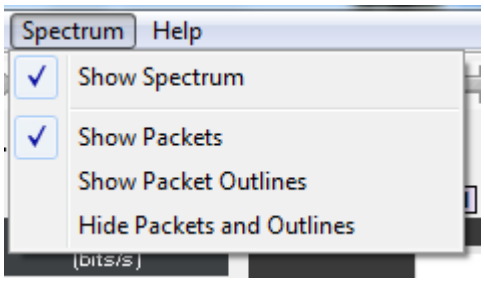


Figure 4.99 - Coexistence View Timeline with Packet Outlines, Packet Selection Boxes, and Spectrum Heat Map



The Spectrum heat map view is controlled from the **Spectrum** menu. If spectrum data is available, the spectrum heat map is shown with the packets by default. To hide the spectrum data heat map, uncheck the **Show Spectrum** option.

When displaying the heat map, the user can control how the packets are displayed. The following table describes the options for packet display. These options are mutually exclusive and they are available only when **Show Spectrum** is checked.

Table 4.14 - Spectrum Menu Packet Display Options

Option	Description
Show Packets	Displays each packet. Tooltips, packet text, and selection boxes are available as usual.
Show Packet Outlines	Displays an outline of each packet. In this mode the spectrum data comprising each packet is clearly visible and indicated. Tooltips, packet text, and selection boxes are available as usual.
Hide Packets and Outlines	Packets and packet outlines are not displayed. Tooltips, packet text, and selection boxes are available as usual.

4.3.5 Message Sequence Chart (MSC)

The **Message Sequence Chart** (MSC) displays information about the messages passed between protocol layers. MSC displays a concise overview of a *Blutetooth* connection, highlighting the essential elements fo the connection. At a glance, you can see the flow of the data including role switches, connection requests, and errors. You can look at all the packets int he capture, or filter by protocol or profile. the MSC is color coded for a clear and easy view of your data.

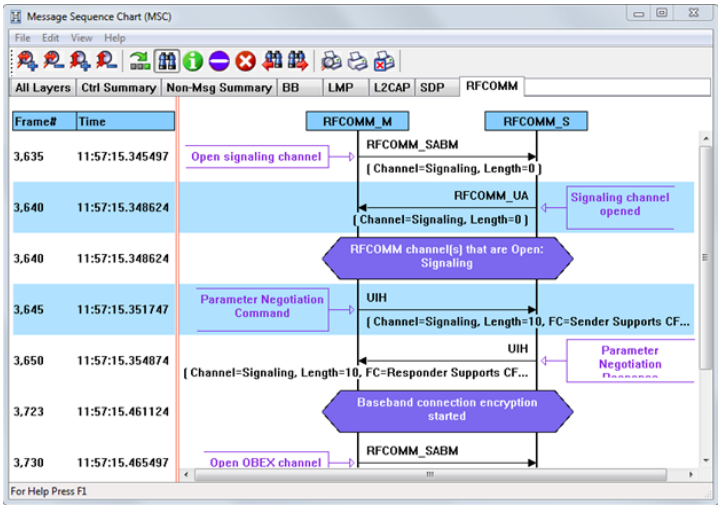


Figure 4.100 - Message Sequence Chart Window

How do I access the chart?

You access the **Message Sequence Chart** by selecting the icon or **MSC Chart** from the **View** menu from the **Control** window or **Frame Display**.

What do I see on the dialog?

At the top of the dialog you see four icons that you use to zoom in and out of the display vertically and horizontally. The same controls are available under the **View** menu.

There are three navigation icons also on the toolbar.

	This takes you to the first Information Frame.
	This takes you to first Protocol State Message.
	This takes you to the first Error Frame. Click here to learn more about this option.

If there is both Classic and low energy packets, there will be a **Classic** and **LE** tab at the top of the dialog.

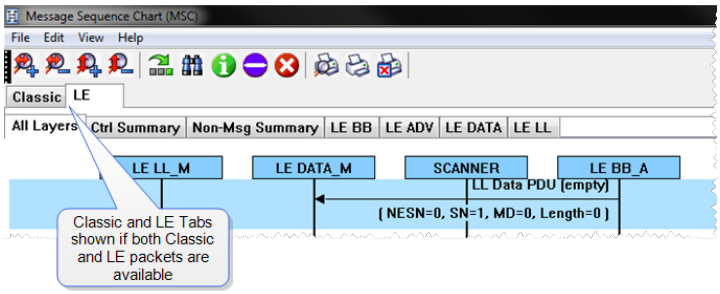
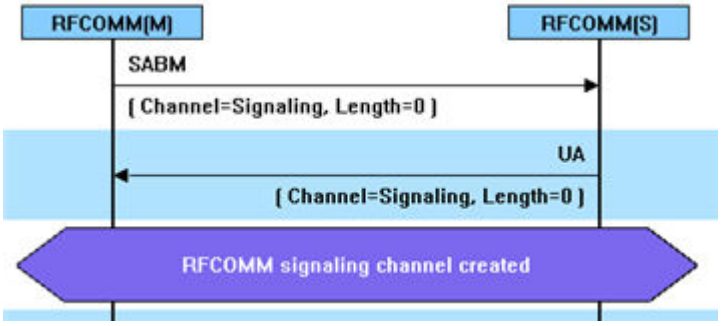


Figure 4.101 - Classic and LE tabs

If the **Classic** tab is selected, you will see Classic protocols. If you select the **LE** tab, you will see LE Protocols. If there is only Classic or only LE, the Classic and LE tabs will not appear.

Also along the top of the dialog are a series of protocol tabs. The tabs will vary depending on the captured protocols.

Clicking on a tab displays the messaging between the master and slave for that protocol. For example, if you select **RFCOMM**, you will see the messaging between the **RFCOMM{M}** Master, and the **RFCOMM{S}** Slave.



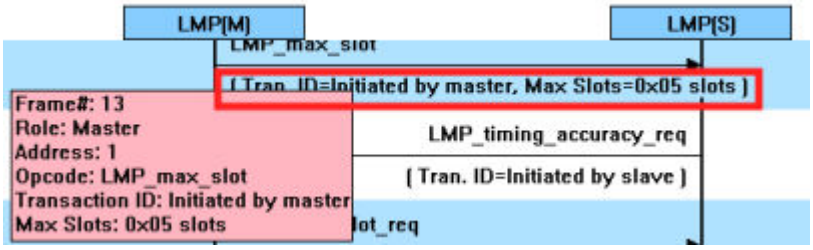
The Non-Message Summary tab displays all the non-message items in the data.

The **Ctrl Summary** tab displays the signaling packets for all layers in one window in the order in which they are received.

The information in the colored boxes displays general information about the messaging. The same is true for each one of the protocols.

If you want to see the all the messaging in one dialog, you select the **All Layers** tab.

When you move the mouse over the message description you see an expanded tool tip.



If you position the cursor outside of the message box, the tool tip will only display for a few seconds.

If, however, you position the cursor within the tool tip box, the message will remain until you move the cursor out of the box.

Additionally, If you right click on a message description, you will see the select Show all Layers button.

When you select **Show all Layers**, the chart will display all the messaging layers.

The **Frame#** and **Time** of the packets are displayed on the left side of the chart.

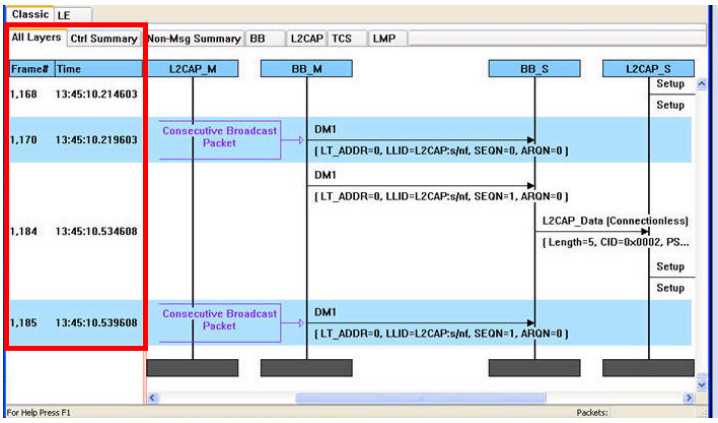


Figure 4.102 - Frame# and Time Display, inside red box.

If you click on the description of the message interaction, the corresponding information is highlighted in Frame Display.

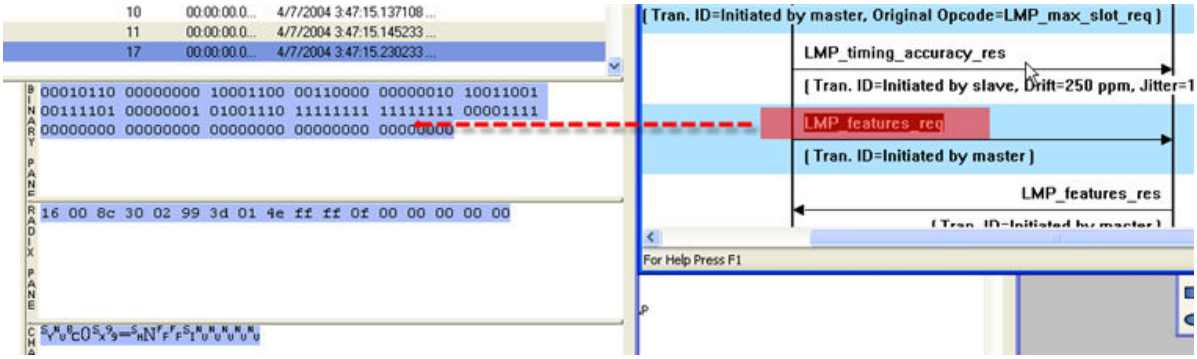


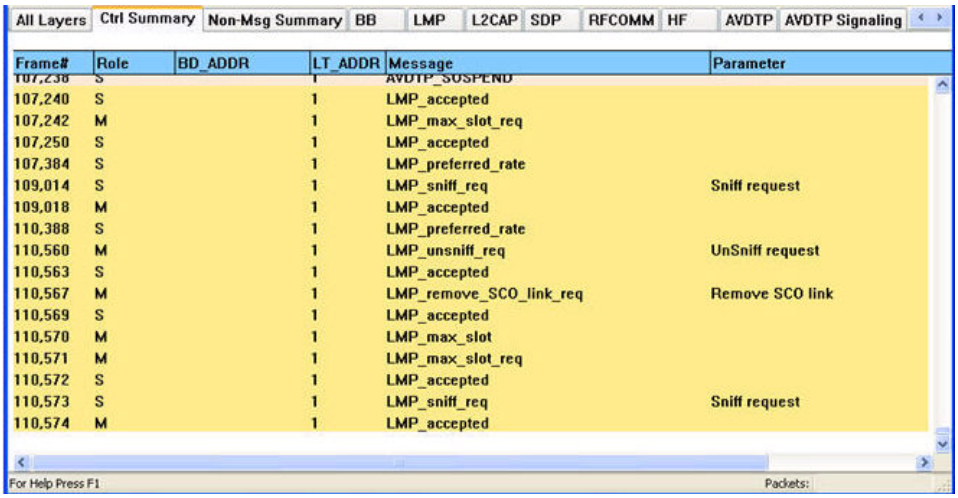
Figure 4.103 - MSC Synchronization with Frame Display

How do I navigate in the dialog?

You can use the navigation arrows at the bottom and the right side of the dialog to move vertically and horizontally. You can also click and hold while moving the pointer within dialog that brings up a directional arrow that you can use to move left/right and up/down.

Ctrl Summary tab

When you select the **Ctrl Summary tab** you will see a summary of the control and signaling frames in the order that they are received/transmitted from and to devices.



Frame#	Role	BD_ADDR	LT_ADDR	Message	Parameter
107,238	S		1	AVDTP_SUSPEND	
107,240	S		1	LMP_accepted	
107,242	M		1	LMP_max_slot_req	
107,250	S		1	LMP_accepted	
107,384	S		1	LMP_preferred_rate	
109,014	S		1	LMP_sniff_req	Sniff request
109,018	M		1	LMP_accepted	
110,388	S		1	LMP_preferred_rate	
110,560	M		1	LMP_unsniff_req	UnSniff request
110,563	S		1	LMP_accepted	
110,567	M		1	LMP_remove_SCO_link_req	Remove SCO link
110,569	S		1	LMP_accepted	
110,570	M		1	LMP_max_slot	
110,571	M		1	LMP_max_slot_req	
110,572	S		1	LMP_accepted	
110,573	S		1	LMP_sniff_req	Sniff request
110,574	M		1	LMP_accepted	

Figure 4.104 - Control and Signaling Frames Summay

The frame numbered is shown, whether the message comes from the Master or Slave, the message Address, the message itself, and the timestamp.

Additionally, the control/signaling packets for each layer are shown in a different background color.

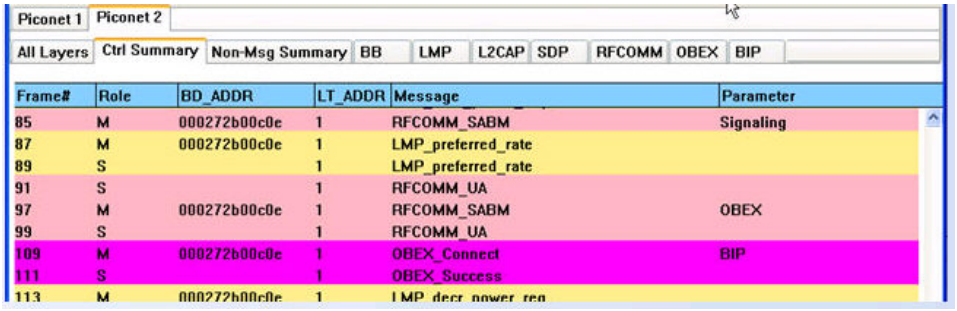


Figure 4.105 - Packet Layers Shown in Different Colors

If you right click within the **Ctrl Summary**, you can select **Show in MSC**.

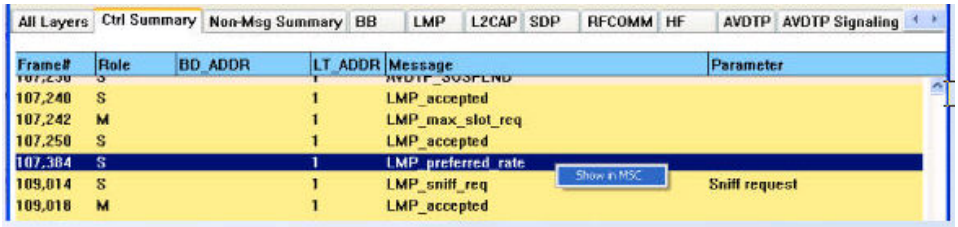


Figure 4.106 - Right-Click in Ctrl Summary to Display Show in MSC

The window then displays the same information, but in the normal MSC view.

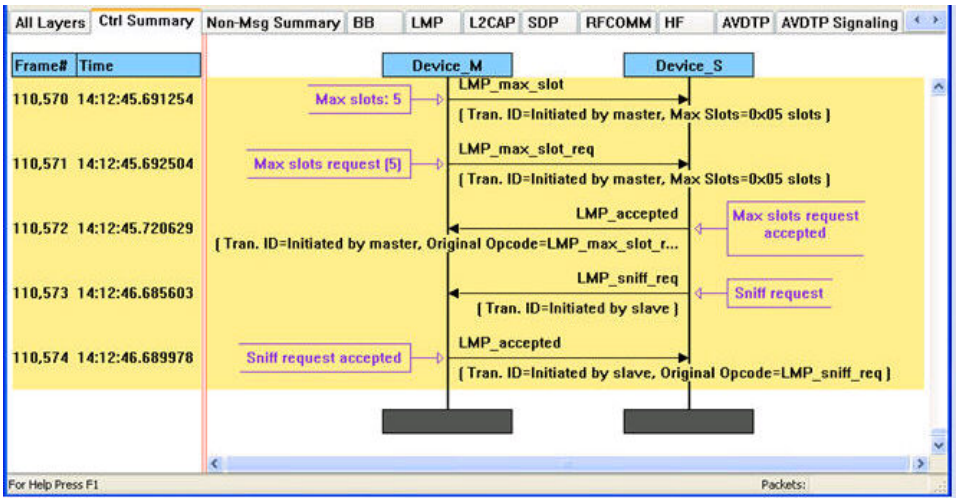


Figure 4.107 - MSC View of Selected Packet from Ctrl Summary

You can return to the text version by using a right click and selecting **Show in Text.**

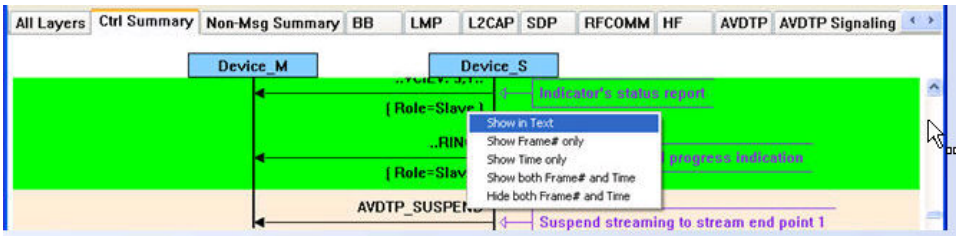


Figure 4.108 - Return to Text View Using Right-Click Menu

You can also choose to show:

- Frame # only
- Time only
- Show both Frame# and Time
- Hide both Frame# and Time

4.3.5.1 Message Sequence Chart Toolbar

Figure 4.109 - Message Sequence Chart Toolbar

Table 4.15 - Message Sequence Chart Tools

Tool	Keyboard	Description
	Ctrl + H	Zoom in horizontal - expands the chart horizontal view
	Shift + H	Zoom out horizontal - compresses the chart horizontal view
	Ctrl + V	Zoom in vertical - expands the chart vertical view
	Shift + V	Zoom out vertical - compresses the chart vertical view
	Shift + F	Go to frame
	F3	Search
	F2	Search for prior Search criteria.
	F4	search for Next criteria.
	Ctrl + I	Go to first information message
	Ctrl +S	Go to first protocol state message
	Ctrl +E	Go to first error frame
/	Shift + L	Lock / unlock the chart display. Clicking on the active icon or typing the keyboard command will toggle to the other state.
	Ctrl + W	Print display preview
	Ctrl + P	Print the display

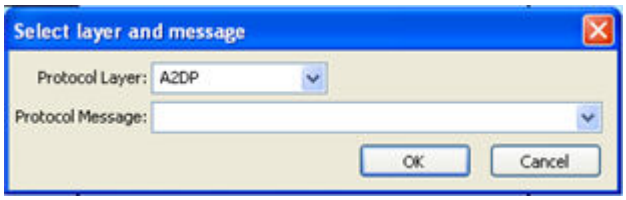
Table 4.15 - Message Sequence Chart Tools (continued)

Tool	Keyboard	Description
	Ctrl + C	Cancel an in-process print

4.3.5.2 Message Sequence Chart - Search

The Message Sequence Chart has a Search function that makes it easy to find a specific type message within the layers.

When you select the 1) **Search** icon or 2) use **F3** key, the **Select layer and message** dialog appears.



From this dialog you can search for specific protocol messages or search for the first error frame.

1. On the MSC dialog select one of the protocol tabs at the top.

> **Note:** If you select **All Layers** in Step 1, the Protocol Layers drop-down list is active. If you select any of the other single protocols, the Protocol Layers drop-down is grayed out.

2. Or Open the Search dialog using the Search icon or the **F3** key.
3. Select a specific Protocol Message from the drop-down list.
4. Once you select the Protocol Message, click **OK**

The Search dialog disappears and the first search result is highlight in the Message Sequence Chart.

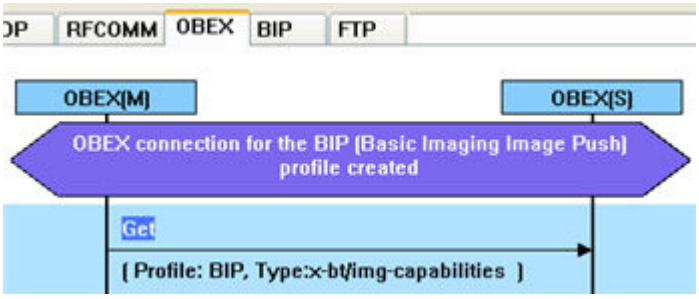
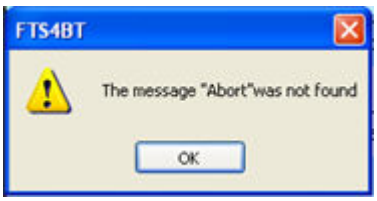


Figure 4.110 - Highlighted First Search Result

If there is no instance of the search value, you see this following dialog.



Once you have set the search value, you can 1) use the **Search Previous** and **Search Next** buttons or 2) **F2** and **F4** to move to the next or previous frame in the chart.

4.3.5.3 Message Sequence Chart - Go To Frame

The **Message Sequence Chart** has a **Go To Frame** function that makes it easy to find a specific frame within the layers.

In addition to Search, you can also locate specific frames by clicking on the **Go To Frame** toolbar icon.

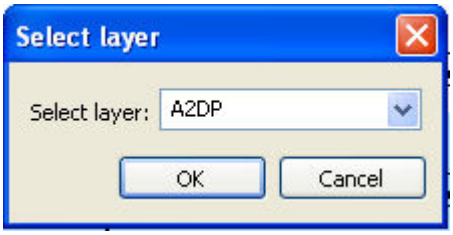
1. Click **Go To Frame** in the toolbar.
2. Enter a frame number in the **Enter frame No.:** text box.
3. Click **OK**.

The Go To Frame dialog disappears and the selected frame is highlighted in the chart.

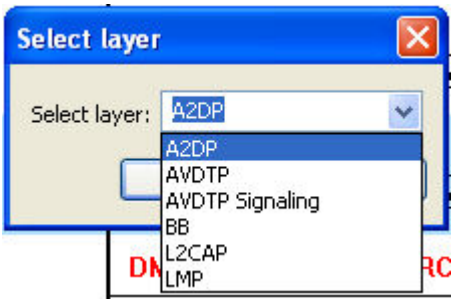
Once you have identified the frame in Go To, you can 1) use the Search Previous and Search Next buttons or 2) **F2** and **F4** keys to move to the next or previous frame in the chart.

4.3.5.4 Message Sequence Chart - First Error Frame

When you select **Go to first error frame** from the toolbar, the **Select layer** dialog appears.



You have to select a layer from the drop down list to choose what layer you want to search for the error.



Once you select a layer, then **OK**, the first error for that layer will be displayed.

If no error is found, a dialog will announce that event.

4.3.5.5 Message Sequence Chart - Printing

There are three standard MSC print buttons. **Print Preview**, **Print**, and **Cancel Printing**.

Print Preview

1. When you select **Print Preview**  , the **Print Setup** dialog appears.
2. You next need to select your printer from the drop-down list, set printer properties, and format the print output..
3. Then you select **OK**.

After you select **OK**, the **Message Sequence Chart Print Preview** dialog appears.

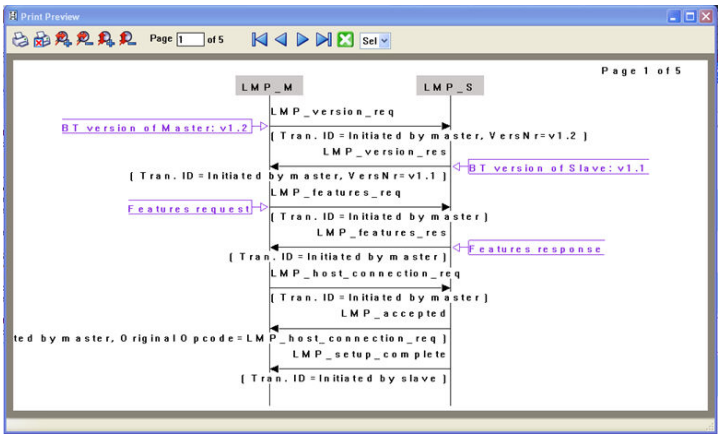


Figure 4.111 - Message Sequence Chart Print Preview

The information in the dialog will vary depending on the layer that is selected in the Message Sequence Chart, the properties of the printer you select, and the amount of data in the layer (which will correspond to the number of pages displayed).

You control what you see and when to print using the toolbar at the top of the dialog.

Figure 4.112 - Print Preview Toolbar

Table 4.16 - Print Preview Icons

Icon	Name	Description
	Print	Prints all the pages to the printer you select in Print Setup dialog. When you select Print, you will output the data that is currently being displayed.
	Cancel Printing	Cancels the current printing.
	Zoom In Horizontally	Expands the data horizontally so it can be easier to read.
	Zoom Out Horizontally	Squeezes the data together so that more fits on one page.
	Zoom In Vertically	Expands the data vertically so it can be easier to read.
	Zoom Out Vertically	Squeezes the data so that more fits on one page.
Page 1 of 5	Current Page	The current page text box displays the page number this is currently shown in the dialog. You can enter a number in the text box, then press Enter, and the dialog will display the data for that page.
	Page navigation	If the data requires multiple pages, the navigation buttons will take you to: • The first page • The previous page • The next page • The last page
	Close Print Preview	Closes the dialog and returns to the Message Sequence Chart
Sel	Select Font Size	Allows selection of the print font size from the drop-down control.

4.3.6 Logic Analyzer

The **Logic Analyzer** provides a display and measurement tool for logic signals captured using the Sodera HCI pods and HCI UART and USB data. In addition, the display can include graphical display of Classic *Bluetooth*, and *Bluetooth* low energy packets. The packets are displayed simultaneously and time synchronized with captured logic signals.

The **Logic Analyzer** displays signals/protocols available to the **Frame Display**. This means you will see only the recorded data for devices in the Sodera **Wireless** and **Wired** panes selected for analysis and for *Bluetooth* technologies selected in the **Capture Options Wireless** and **Wired** tabs. If the data filter changes due to changes in device selection and/or technology selection, the **Logic Analyzer** display will refresh with the next analysis.

> **Note:** Filters applied in the **Frame Display** do not apply to the signals/protocols displayed in the **Logic Analyzer**.

See Connecting for HCI/WCI-2 & Logic Capture on page 14,andCapture Options Dialog on page 38 procedures for configuring the Sodera HCI pod hardware and the Frontline software. See Sodera Logic Event Capture and Analysis on page 1 for information on logic capture, recording, and analysis procedures. See UART Capture Configuration on page 17 for information on capturing UART. See Connecting for USB Capture on page 17 for information on capturing USB.

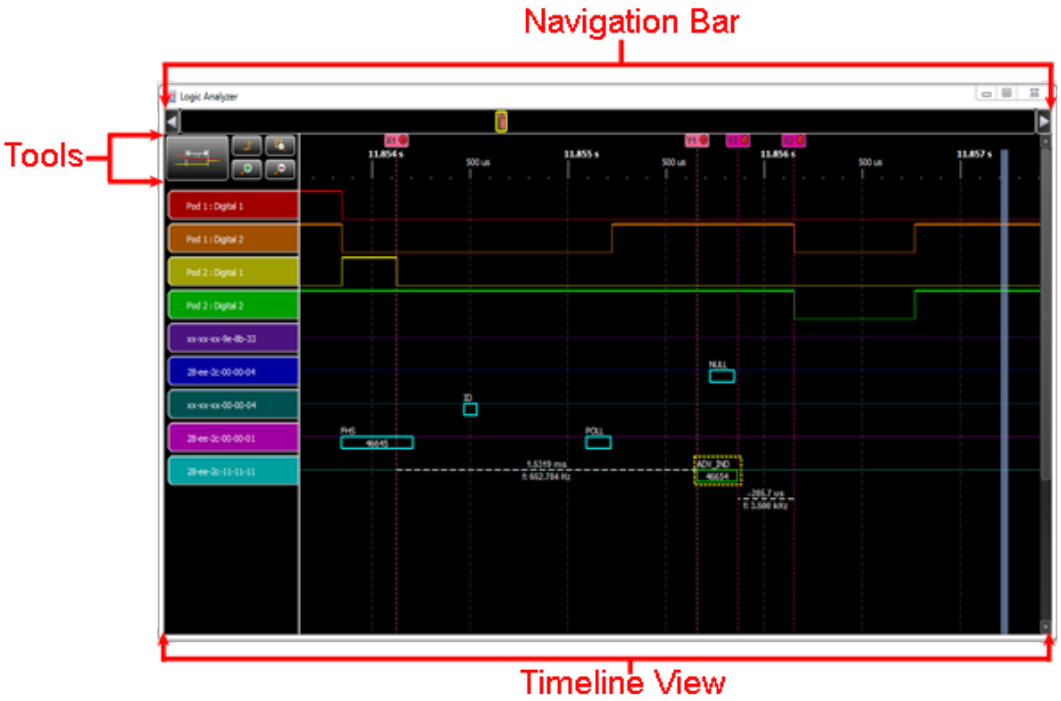


Figure 4.113 - **Logic Analyzer**Window

The **Logic Analyzer** window has three major areas:

- Tools - provides tools for positioning, displaying, and measuring elements in the Timeline View.
- Timeline View- Displays the logic signal waveform, the packets, and measurements.
- Navigation Bar - Contains a viewport that represents the range of the Timeline View. Drag-and-drop control provides horizontal zooming and positioning of the viewport. Timing cursor timeline locations are represented in the Navigation Bar.

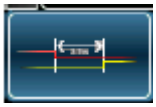
Acknowledgment: The Frontline Logic Analyzer contains features utilizing the Qt open source library, licensed under LGPL. To obtain the utilized Qt library source code , please contact Teledyne LeCroy Technical Support.

4.3.6.1 Logic Analyzer Tools

The tools control the display of the Timeline View. Detailed information on how to use the tools is contained in Logic Analyzer Timeline View on page 223.

Figure 4.114 - Logic Analyzer Tools

Table 4.17 - Tools pane Selections

Icon	Selection	Description
	Timing	Places cursor in the timeline. A pair of cursors—left (X) and right (Y)—will display the time between them. Multiple pairs of cursors can be placed on the timeline. See Timing Cursors & Measuring in Timeline View on page 229.
	Overlay	This button toggles between enabling and disabling the overlay signals mode. The overlay signals mode allows placing of a timeline row on top of another row, which makes it easier to compare data on those rows. See Overlay Signals Mode in Timeline View on page 231.
	Zoom Box	This button toggles between enabling and disabling the zoom box mode. The zoom box allows you to zoom in or out by dragging your mouse around an area of the Timeline View . See Zooming in Timeline View on page 228.
	Zoom In	Clicking on these buttons will zoom the Timeline Viewin or out. The buttons will turn gray when the timeline display is zoomed to at either its maximum or minimum. See Zooming in Timeline View on page 228.
	Zoom Out	

4.3.6.2 Logic Analyzer Navigation Bar

The Navigation Bar spans the entire duration of the capture session from the beginning of the first packet or logic signal to the end of the last packet or logic signal. Within the Navigation Bar viewport appears that represents the visible Timeline View . The viewport is a moveable and resizeable slider.

Figure 4.115 - Logic Analyzer Navigation Bar

Within the Navigation Bar you will see

- the viewport, which is discussed in detail below.
- Timing cursor markers placed in the timeline using the Timing button in the Tools . See Logic Analyzer Tools on the previous page. When a measurement is set the Navigation Bar will display  at each location of a timing cursor.
- Scrolling buttons at each end of the Navigation Bar. These buttons will scroll the viewport across the Navigation Bar.

Moving the viewport

By moving the viewport along the Navigation Bar you horizontally scroll the Timeline View. There are three methods for moving the viewport.

- Click on the Scroll left or right buttons to move the viewport. The viewport will jump left or right respectively.
- Position the cursor inside the viewport ; the cursor changes to a cross (+). Hold down the left mouse button and drag the viewport along the Navigation Bar.
- Left click the mouse with the cursor outside the viewport but inside the Navigation Bar. The viewport left edge will jump to the cursor location.

Expanding or Collapsing the viewport

Expanding or collapsing the viewport has the effect of zooming the Timeline View out or in, respectively.

- Position the mouse cursor over either the viewport's left or right edge; the cursor changes to a double-headed arrow (↔). Hold down the left mouse button and drag the viewport edge to collapse or expand the viewport thereby zooming the Timeline View in or out respectively.

You can anchor the viewport to the beginning or end of the timeline.

- Position the mouse cursor inside the viewport; the cursor changes to a cross (+). Holding down the left mouse button, drag the viewport along the Navigation Bar to the left edge, which is time zero. Position the cursor on the viewport right edge and drag to expand or collapse the viewport.
- Position the mouse cursor inside the viewport; the cursor changes to a cross (+). Holding down the left mouse button, drag the viewport along the Navigation Bar to the right edge, which is the maximum time. Position the cursor on the viewport left edge and drag to expand or collapse the viewport.

Dragging the viewport edges has the same effect as using the Logic Analyzer zooming tools. When you use the zooming tools the viewport will expand when zooming out or collapse when zooming in. See Logic Analyzer Tools on the previous page

4.3.6.3 Logic Analyzer Timeline View

Timeline View displays captured logic signals, Classic *Bluetooth*, and *Bluetooth* low energy, and HCI packets. The signals and packets are synchronized and displayed on a horizontal time axis. The amount of time displayed in the view is controlled by the Navigation Bar viewport. As the viewport expands, more of the timeline is displayed and the signals and packets will compress. Conversely, as the viewport collapses—gets smaller—less of the timeline displays and the logic signals and packets will expand.

Each signal or packet set displayed in the Timeline View appears on a single row. All logic signals, *Bluetooth*, and HCI UART/USB packets available in the **Frame Display Unfiltered** tab will appear in the Timeline View from both live capture and a capture file.

> **Note:** Filters applied in the **Frame Display** do not apply to the signals/protocols displayed in the**Logic Analyzer**.

Each Timeline View protocol row contains the packets from a single source device selected for analysis from the **Wireless Devices** or **Wired Devices** panes. If a *Bluetooth* device cannot be determined, packets will be placed in an appropriate aggregate row— "BR/EDR Other" or "LE Other". Bluetooth packets have the following characteristics and information:

- Wireless packet width indicates the in-air duration. HCI packet width is computed assuming a bus rate of 12 Mbps that is 100% utilized (utilization is always less than 100%, but exact utilization is unknowable, so this method provides a reasonable approximation).
- Packet type.
- Frame number.

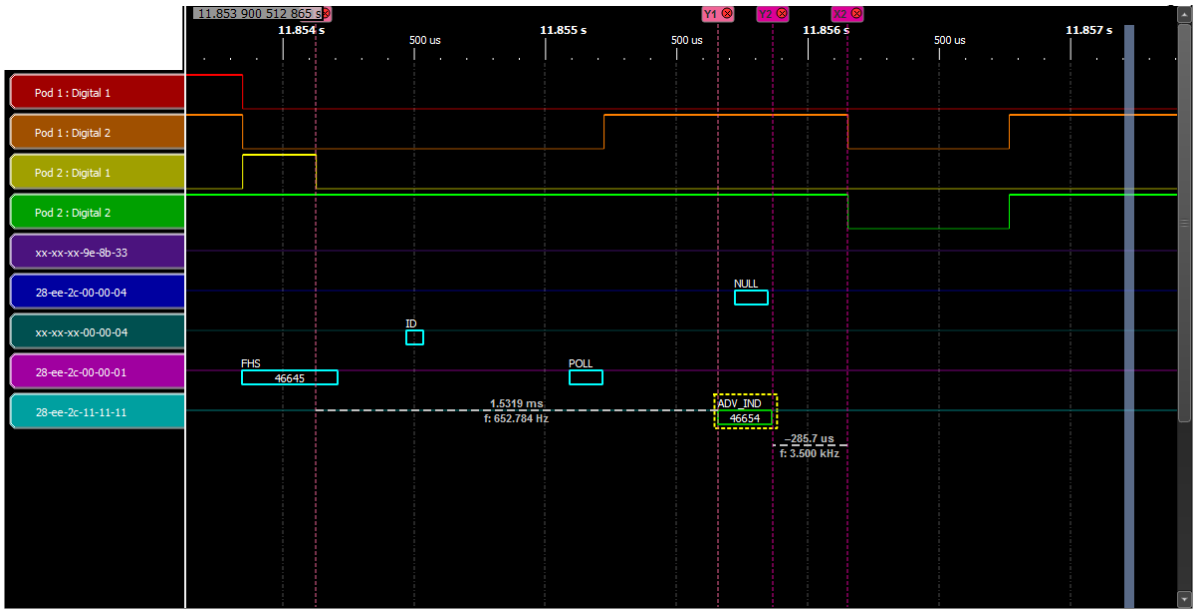
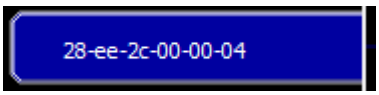


Figure 4.116 - Logic Analyzer Timeline View

At the top of the Timeline View is a time scale. its time range is the time span of the viewport.

Row Label



On the left of each row is a row label. There are two label categories: (1) Sodera Wired capture (either logic, UART, or USB), and (2) Wireless. The row labels are color coded for easy identification and the color carries through in the signal/packet timeline. Logic Analyzer Timeline Row Labels on page 225 provides details of the label format.

Table 4.18 - Logic Analyzer Timeline Row Labels

Category	Type	Label	Source Connector
Wired	Logic	<*HCI Pod #*> = Pod 1 or Pod 2	Pod 1 or Pod 2 Digital 1
			Pod 1 or Pod 2 Digital 2
	UART	HCI POD 1 (Host)	Pod 1
		HCI POD 1 (Ctlr)	
		HCI POD 2 (Host)	Pod 2
		HCI POD 2 (Ctlr)	
	USB	HCI USB 1 (Host)	USB 1
		HCI USB 1 (Ctlr)	
		HCI USB 2 (Host)	USB 2
		HCI USB 2 (Ctlr)	
Wireless	Bluetooth	If an address cannot be determined an aggregate label is used. For example, "BR/EDR Other" or "LE Other"	Antenna

Timeline

In the Timeline appears a representation of the captured logic signal or HCI UART/USB and *Bluetooth* packets. Synchronization of these timelines provides for a means of accurate timing analysis. The viewport and the zoom tools controls the amount of signals and packets displayed in the Timeline View. The larger the viewport—zooming out—the more of the captured range that is displayed, and the smaller the signals and packets will appear. As the resolution decreases, logic signals will become smaller and smaller until they become a gray-hash bar.

Decreasing the viewport size by zooming in will decrease the time duration covered by the timeline, and the signals will appear with greater resolution. Should a logic signal or signal be not differentiable from adjacent signals or packets they are displayed as a hash-bar. This ensures that all signals and packets are visible when the timeline displays the complete capture session. Figure 4.117 on the next page and Figure 4.118 on the next page show examples of the same display in hash-bars and zoomed in to show the actual logic signals and packets in the same time frame.

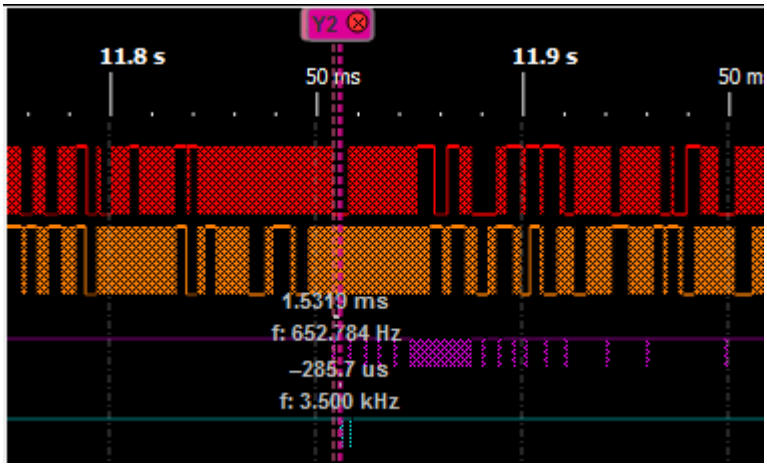


Figure 4.117 - Example: Timeline View Hash-Bar at Low Resolution

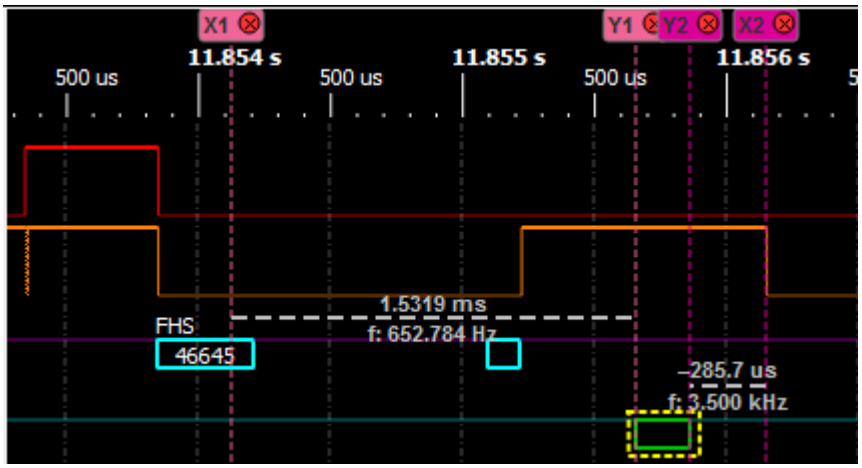


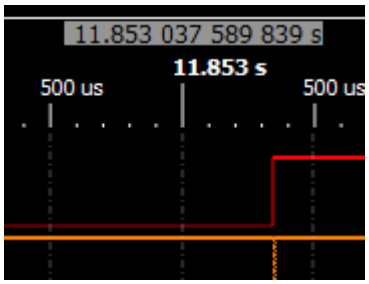
Figure 4.118 - Example: Timeline View at Higher Resolution, Zoomed In to same area.

Repositioning the Timeline

The Navigation Bar viewport can be used to reposition the timeline, however this is best used for large changes to the view. For small changes to the view port, disable the Tools Zoom Box and click the mouse pointer anywhere in the timeline view. The cursor will change to a grabbing hand, ✋. While holding the mouse left key down, move the timeline view.

At the top of the Timeline View is a time scale. The visible time range of the Timeline View corresponds to the time covered by the viewport.

When moving the cursor over the Timeline, a gray box appears just above the time scale. The time shown in this box is the time corresponding to the cursor position within the timeline.



To the right of the timeline is vertical scroll bar that is useful when displaying a large number of devices.

Keyboard and Mouse Controls

Table 4.19 - Timeline View Keyboard Controls

Keys	Action
Left/Right Arrow	Moves timeline left/right. Equivalent to moving the viewport.
Up/Down Arrow	Scrolls timeline rows up/down. Equivalent to using the Timeline View scroll bar.
Up/Down Arrow + Ctrl	Zooms timeline in/out. Equivalent to using the Tools Zoom In/Out buttons, or collapsing/expanding the viewport.
Page Up/Down	Pages the timeline left/right. Paging Up moves the timeline left side over to the right side, that is jumping to the left. Paging Down moves the timeline right side over to the left side, that is jumping to the right.
Ctrl + Home	Moves the timeline and viewport to the beginning of the capture.
Ctrl + End	Moves the timeline and viewport to the end of the capture.

Table 4.20 - Timeline View Mouse Controls

Keys	Action
Double Left Click	Sets a wide cursor at the timeline point where clicked and then centers the cursor and in the timeline view. The viewport size does not change.
Scroll Wheel	Moves rows up and down.Equivalent to using the Timeline View scroll bar.
Scroll Wheel + Ctrl	Zooms timeline in/out. Equivalent to using the Tools Zoom In/Out buttons, or collapsing/expanding the viewport.
Scroll Wheel + Shift	Moves timeline left/right. Equivalent to moving the viewport.

4.3.6.3.1 Logic Signals in Timeline View

A logic signal timeline is shown as a high/low representation of the captured signal. A high level appears beginning at the time when the captured signal transitioned from a low state up through the logic-high threshold voltage. The high state is shown at the row label top edge. The logic low state occurs when the captured logic signal transitions from a high state down through the logic-high threshold voltage. A logic low state is shown at the row label bottom edge. State transition is displayed as instantaneous.

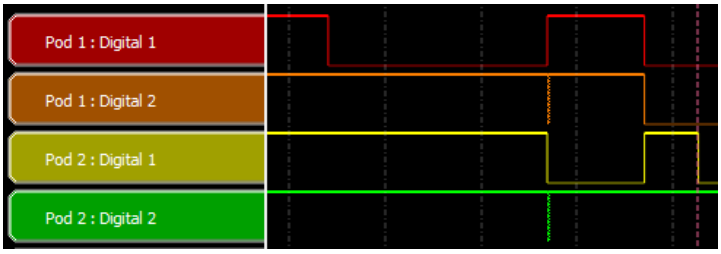


Figure 4.119 - Example: Logic State Transition

The high level threshold is determined by the HCI POD **LIO LVL** voltage. The minimum threshold voltage is 1.65 Vdc. Refer to Connecting for HCI/WCI-2 & Logic Capture on page 14 for more information about the threshold level.

4.3.6.3.2 *Bluetooth* & HCI Signals in Timeline View

A protocol row in the Timeline View shows the packets associated with a single source device. The devices appearing in the row labels were selected for analysis in the Sodera **Wireless Devices** and **Wired Devices** panes. The packets for each device appear as color-coded rectangles on the timeline.

Table 4.21 - Timeline Packet Color Codes

Category	Color	Description
Bluetooth	Blue	Classic *Bluetooth*
	Green	Bluetooth low energy
HCI	Purple	UART
		USB
Error	Red	Surrounding dashed line. Status errors, e.g. CRC or link errors.
Selected	Yellow	Surrounding dashed line. Selected packet. Can result from selection in **Frame Display** or one of the **Timeline** views.

Packet information appearing on the rectangle is

- Packet type - Above the packet rectangle top border. HCI will show packet type and, for HCI ALC and SCO data, the source.
- Frame number - In the rectangle center.
- Frame selection - If a dashed yellow line appears surrounding the packet, that packet has been selected in either the **Frame Display**, **Coexistence View**, **Bluetooth Timeline**, or **Bluetooth Low Energy Timeline**.

The length of the rectangle represents the *Bluetooth* packet in-the-air duration or the HCI packet duration.

Figure 4.120 - Example: Timeline View Protocol Rows

4.3.6.3.3 Zooming in Timeline View

Zooming the timeline display in or out is accomplished using four methods:

1. Drag the edges of the viewport. The Timeline will expand or decrease with the size of the viewport. See Logic Analyzer Navigation Bar on page 222.
2. Enable the Tools Zoom Box  , and then drag a zoom area with the mouse cursor.

   Zoom In: After enabling the Zoom Box, click and hold anywhere in the Timeline. When the cursor changes to a "+", drag to the right and down and a box will appear along with text showing the start

and end times of the box. Release the mouse key and the timeline will zoom in to the time range covered by the box.

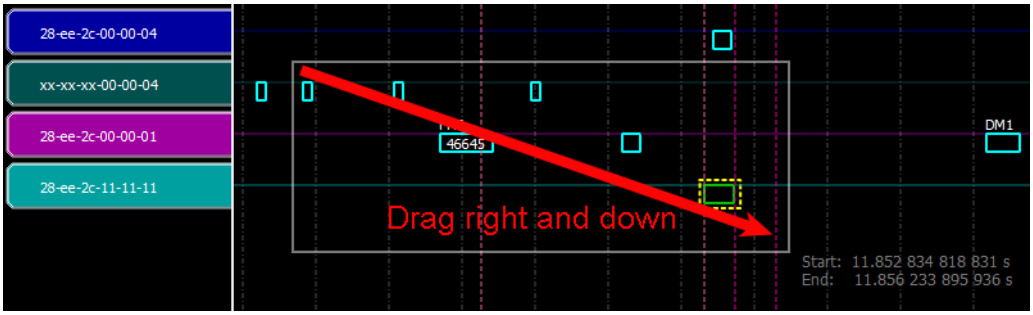


Figure 4.121 - Zoom Box Tool - Zoom In

Zoom Out: After enabling the Zoom Box, click the mouse and hold anywhere in the Timeline. When the cursor changes to a "+", drag to the left and up and a box will appear with the start and times of the box. Release the mouse key and the timeline will zoom out.

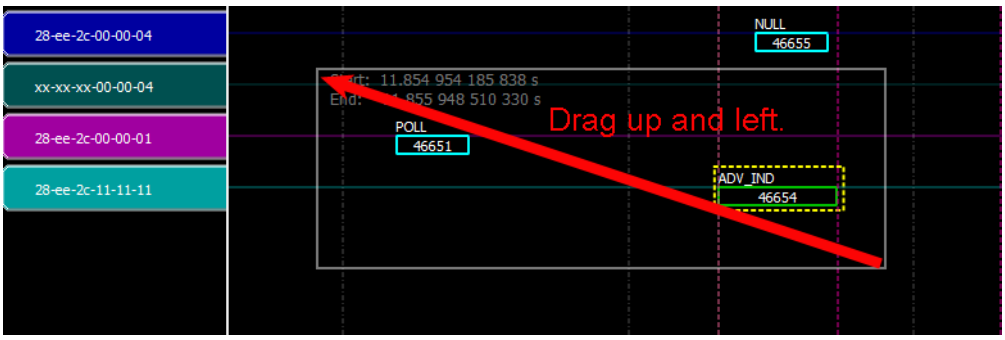


Figure 4.122 - Zoom Box Tool - Zoom Out

3. Clicking on the Tools Zoom In and Zoom Out buttons.

   Zoom In: Click on the Zoom In tool  and the displayed timeline's duration incrementally decreases.

   Zoom Out: Clink on the Zoom Out tool  and the displayed timeline's duration incrementally increases.

4. Hold down the keyboard Ctrl key and use the mouse scroll wheel to zoom in and out.

> **Note:** The timeline view can be zoomed in to nanosecond resolution.

4.3.6.3.4 Timing Cursors & Measuring in Timeline View

Using the Tools Timing button (see Logic Analyzer Tools on page 222) you can place a set of left and right timing cursors on the timeline. The timing cursors provide a means to measure relative time differences between logic signals, packets, or both, or arbitrary positions on the timeline.

1. Enable the Timing button  .

2. With the mouse cursor In the Timeline, click the left mouse button to place the left ("X") timing cursor.

3. Then, anywhere in the Timeline, click the right mouse button to place the right ("Y") timing cursor. The time between the X/Y pair is displayed on a connecting line.

When the + cursor is near a logic signal transition or a packet right or left edge, a down-pointing triangle appears on the transition. Releasing the mouse when the triangle appears, results in the timing cursor snapping to the transition. If there is no snapping triangle, the timing cursor is placed at the location of the + cursor.

You can place multiple timing cursor pairs on the timeline. The timing cursor pairs are identified with subscript notation: X1/Y1, X2/Y2…Xn/Yn. The timing cursor pairs are locked to the timeline and will expand or collapse with the timeline display.

Timing cursor X/Y pair tags appear at the top of the time scale and are color coded. Vertical lines extend from the tag through the timeline and the lines are color matched to their tags. Between the tag lines is a white dashed connecting line with the time span of the tag pair above the line, and the frequency of the time span (reciprocal of the time) below the line. If the Y-cursor is placed to the left of the X-cursor the time value will be negative, however, the frequency is the absolute time span reciprocal.

Timing cursors can be moved by positioning the mouse cursor over the timing cursor tag, holding and dragging the tag to a new position. When a cursor pair is selected the cursor tag color changes to white.

To remove the timing cursors, click on the red circle "x" in the cursor tag 

at the top of the timeline.

Clicking in either the X or the Y tag will remove the X/Y cursor pair.

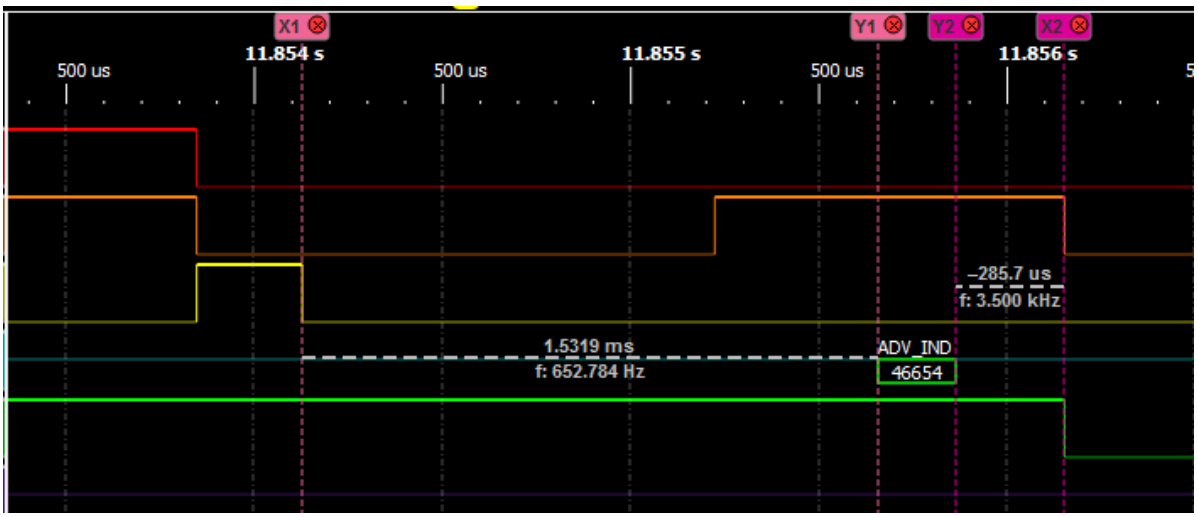


Figure 4.123 - Example: Logic Analyzer Cursor Pairs

If you click on the cursor connecting time line a navigation bar appears. This bar is especially useful when both cursor are not visible within the Timeline View, such as when you have zoomed in; or for when there are multiple cursor pairs within the same view. Clicking on one of the navigation buttons moves a cursor into the Timeline View. The following table provides a description of the navigation actions.

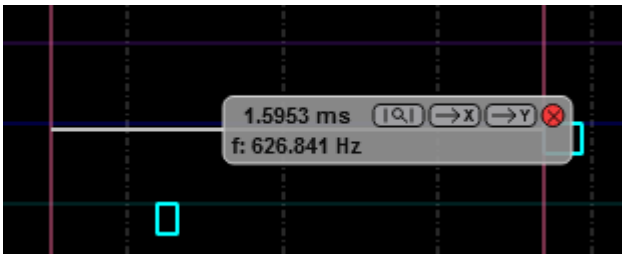


Table 4.22 - Cursor Timeline Navigation Bar Buttons

Button	Description/Action
	Search for Cursor Pair: Adjusts the Timeline View to display both the X- and Y-cursor. The cursors are centered around the middle of the Timeline View.
	Search for X-Cursor: scrolls the X-cursor to the middle of the Timeline View without changing the current range of the Timeline view.
	Search for Y-Cursor: scrolls the Y-cursor to the middle of the Timeline View without changing the current range of the Timeline View.
	Delete the Cursor Pair: Deletes the cursor pair without changing the current range of the Timeline View.

When a X/Y cursor pair is created, a marker appears in the Navigation Bar. The marker has the same color code as the cursor pair tags. This feature aids in quickly navigating to important parts of the capture time range.

Figure 4.124 - Navigation Bar Time Measurement Cursor Markers

4.3.6.3.5 Overlay Signals Mode in Timeline View

Click on the Overlay Signals Mode button  to enable the Overlay Signals Mode. The Overlay Signals Mode allows you to take a row and superimpose it on top of another. Any number of rows can be overlaid. Data in all overlaid rows remains visible.

1. Click on the Overlay Signals Mode button to activate it.
2. Click and hold on the row label of the row to be moved.
3. Drag the row over the row to be overlaid.

To undo the overlays, click on the Overlay Signals Mode button to disable overlay mode. The rows return to their original position.

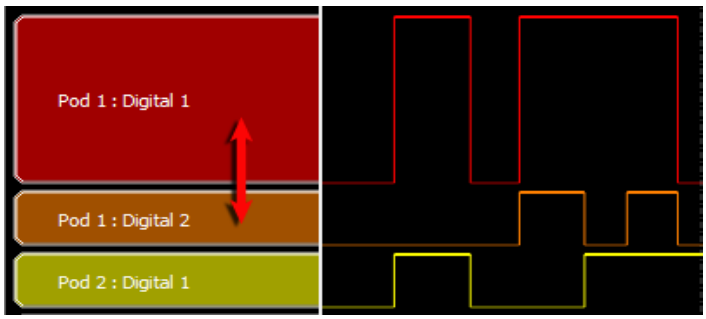
Figure 4.125 - Logic Analyzer Overlay Signal Example

4.3.6.3.6 Arranging Rows in Timeline View

Note: Rows cannot be rearranged when in Overlay Signals Mode.

Resizing

The Timeline View can be scrolled vertically by using the scroll bar on the right side of the view. Additionally the rows can be rearranged to aid in analysis and measurement. Click and hold the mouse cursor on a row label and drag it to a new position. A white horizontal bar will appear between row labels to indicate where the row you are moving will be dropped when the mouse key is released.



Rows can be resized by dragging the bottom of the row label. The row data also resizes with the row label.

Positioning

Rows can be moved up or down to change the order. Click and hold anywhere in a row label. Drag the mouse cursor up or down the rows over the labels. A line with the same color as the row label that you clicked on will appear. Position the line where you want to move the row and release the mouse key. The row will snap to the new location.

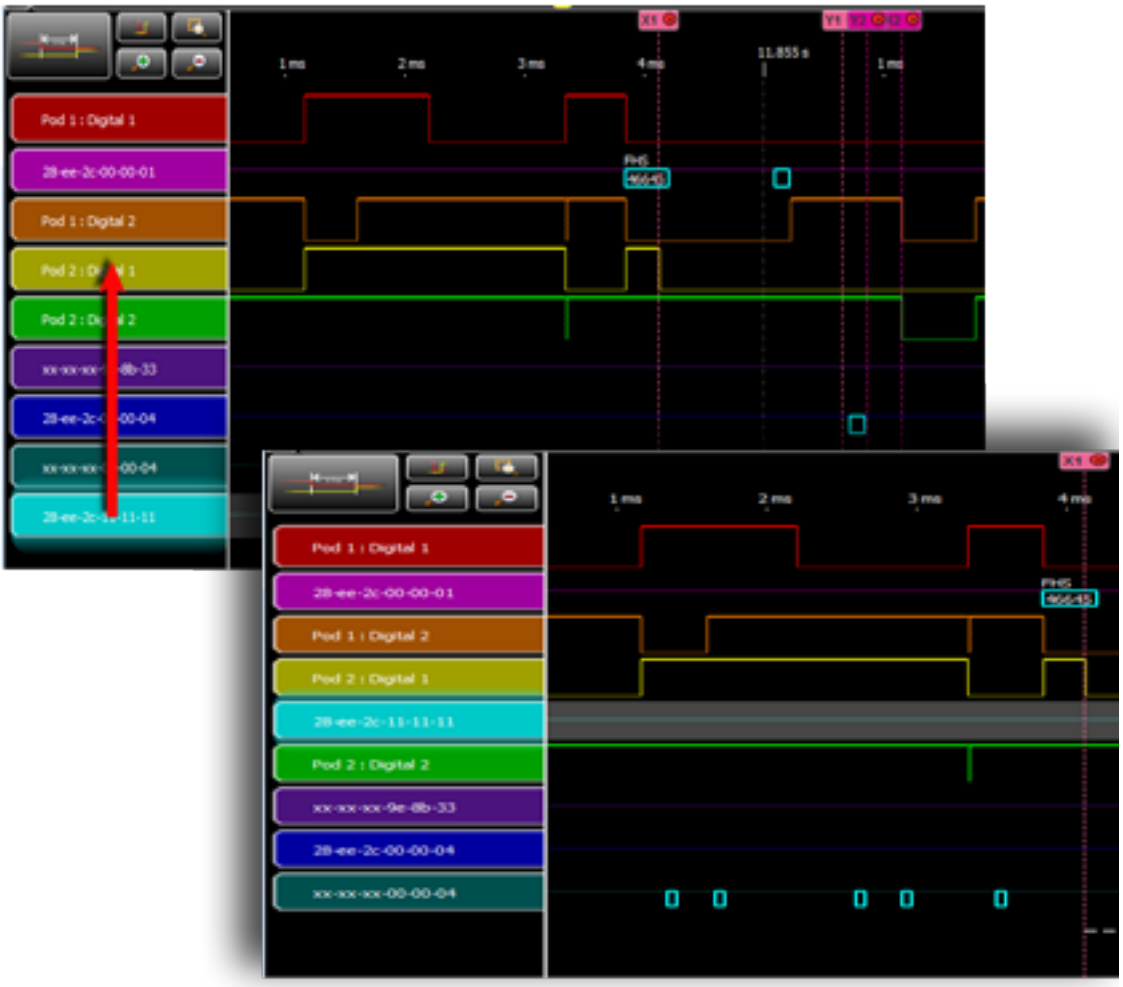


Figure 4.126 - Positioning Rows in the Timeline View

4.4 Packet Error Rate Statistics

The **Packet Error Rate** (PER) Stats view provides a dynamic graphical representation of the Packet Error Rate for each channel. The dialog displays a graph for each Classic *Bluetooth* channel numbered 0 through 78 and for each *Bluetooth* low energy channel numbered 0 through 39.

Packet Error Rate Stats assist in detecting bad communication connections. When a high percentage of re-transmits, and/or header/payload errors occur, careful analysis of the statistics indicate whether the two devices under test are experiencing trouble communicating, or the packet sniffer is having difficulty listening.

Generally, if the statistics display either a large number of re-transmits with few errors or an equal number of errors and re-transmits, then the two devices are not communicating clearly. However, if the statistics display a large number of errors and a small number of re-transmits, then the packet sniffer is not receiving the transmissions clearly.

You can access this window in *Bluetooth* low energy by selecting the ***Bluetooth* low energy Packet Error Rates Statistics** icon from the **Control** window or **Frame Display**. You can also open the window from the View menu on the same windows.

Classic *Bluetooth* Packet Error Rate

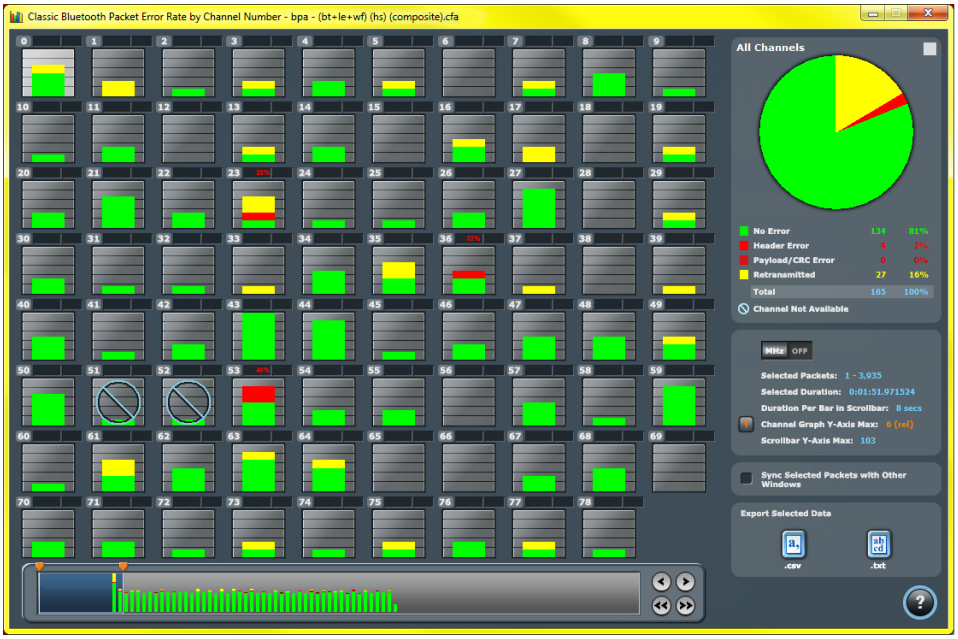


Figure 4.127 - Classic *Bluetooth* PER Stats Window

Bluetooth low energy Packet Error Rate

Figure 4.128 - *Bluetooth* low energy PER Stats Window

4.4.1 Packet Error Rate - Channels

The main portion of the PER Stats dialog displays the 79 individual channels, 0-78, for Classic Bluetooth® 40 individual channels, 0-39, for *Bluetooth* low energy.

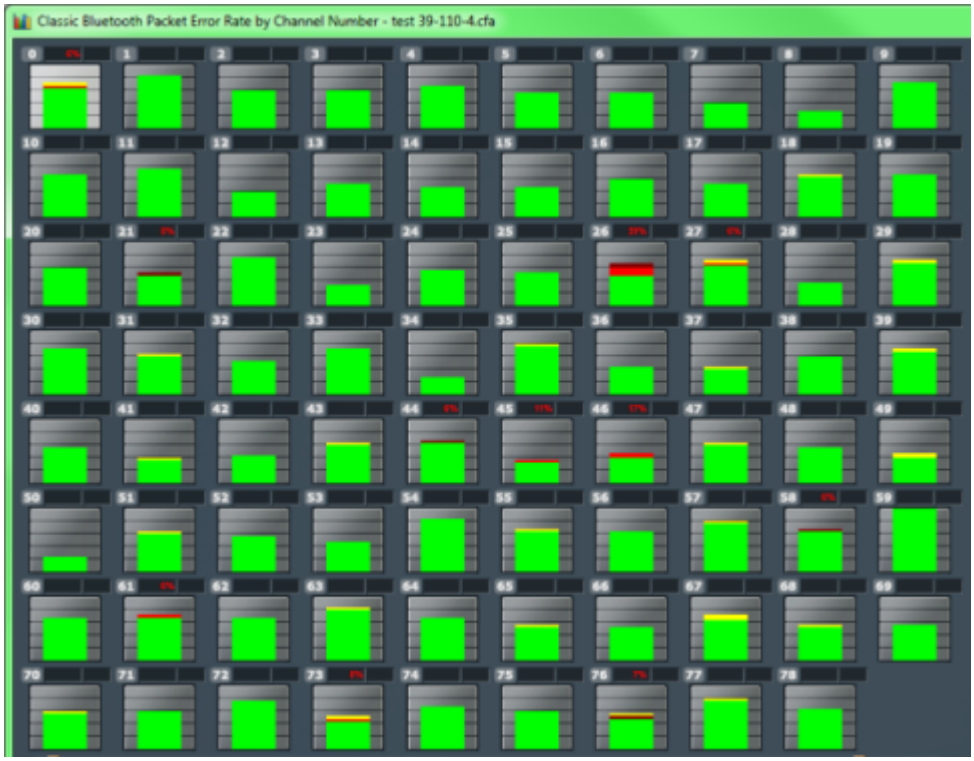


Figure 4.129 - Classic *Bluetooth* Packet Error Rate Channels

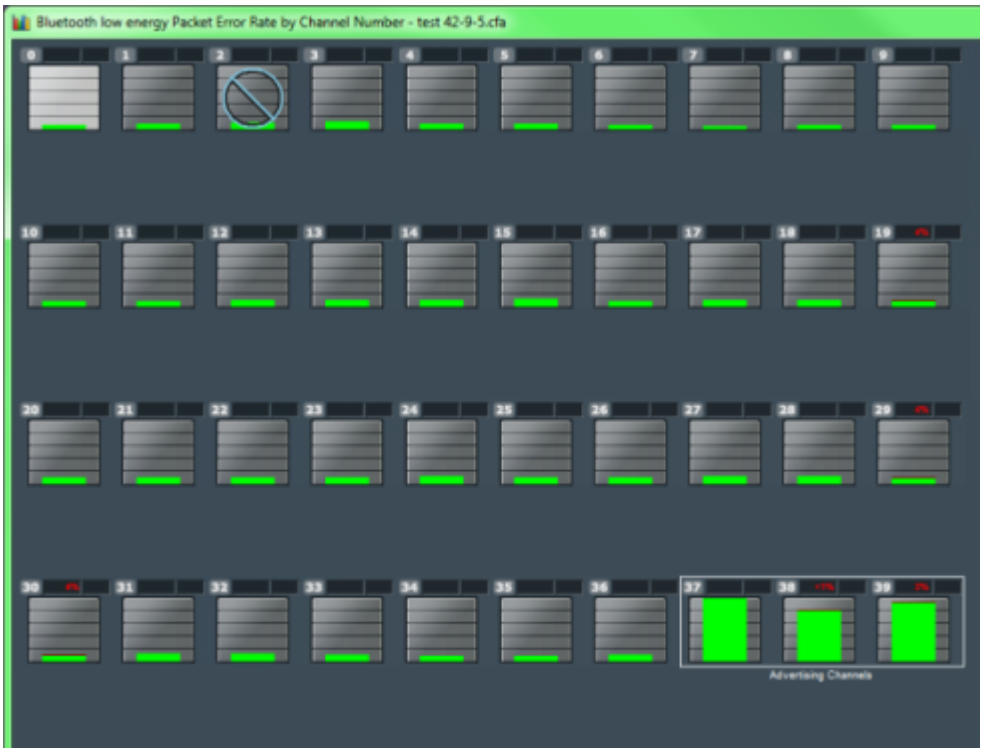


Figure 4.130 - *Bluetooth* low energy Packet Error Rate Channels

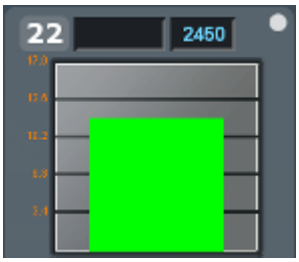
- **For Classic *Bluetooth:*** Each channel contains a bar that displays the number of packets with no errors in green, packets with Header Errors in red, packets with Payload or CRC errors in dark red, and Retransmitted packets in yellow.
- **For *Bluetooth* low energy**: Each channel contains a bar that displays the number of packets with no errors in green, packets with CRC errors in dark red..
- The red number at the top of the channel shows the percentage of Header Error and Payload/CRC Errors in relationship to the total number of packets in the channel.
- The light blue number at the top of each channel shows the megahertz (MHz) for the channel if the option is chosen in the Additional Statistics section.
- When you select a channel, detailed information for that channel is displayed in the expanded chart on the upper right.
- The channels change dynamically as the Viewport is moved or new data appears within the Viewport.
- The **Channel Not Available** symbol is displayed if the channel is not available in the most recent channel map that is in or before the last selected packet, even if that channel map comes before the first selected packet. *Bluetooth* Adaptive Frequency Hopping processes will block channels determined to be unreliable. These channels are not available because the Bluetooth devices have decided not to use them.

- "s" changes the size of the entire dialog.
- "c" changes the contrast of the dialog
- The **Reset** button is only available in live mode. The button will appear in the lower right-hand corner of the Channels section. Clicking on the **Reset** button will clear all prior data from PER Stats.

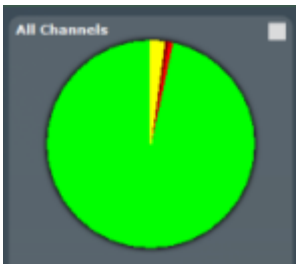
4.4.2 Packet Error Rate - Pie Chart and Expanded Chart

The **Expanded PER Stats Chart** (in the upper right) displays detailed information about the channel selected from the main channel dialog.

Expanded Chart

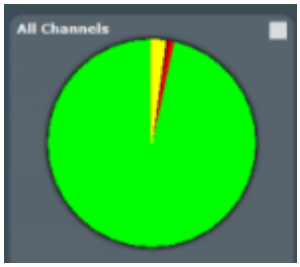


Pie Chart



- When PER Stats is first opened, Channel 0 is displayed in the expanded chart.

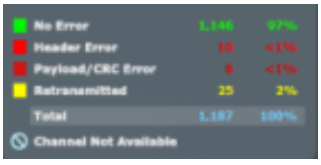
- The top orange number on the Y-Axis displays the maximum number of packets in Snap Mode. If Snap Mode is turned off, the number will display in light blue. For information about Snap Mode, seePacket Error Rate - Additional Statistics on the next page
- The number of the selected channel is displayed in the upper-left corner of the expanded chart.
- The combined value of Header and Payload/CRC errors for the channel is displayed in red as a percentage to the right of the channel number.
- The megahertz (MHz) value is displayed in light blue text if the MHz option is selected in the Additional Statistics section.
- The number of packets with no errors is displayed in light green in the bar chart.
- **For Classic Bluetooth®** : The number of packets that have header errors is displayed in red in the bar chart.
- **For Classic *Bluetooth***: The number of payload errors is displayed in dark red in the bar chart.
- **For Classic *Bluetooth***: The number of re-transmits is displayed in yellow in the bar chart.
- All the values, except MHz, change dynamically when multiple time periods are selected in the Packet Error Rate - Scroll Bar on page 239.
- When you select the in the upper-right corner, the bar chart is replaced by a pie chart. The pie chart applies to all channels, not a selected channel. To return to the bar chart, click on the channel again or click on the in the upper right hand corner.



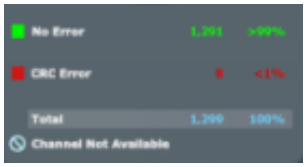
4.4.3 Packet Error Rate - Legend

The **Legend** displays color coded information about the channel selected.

Classic *Bluetooth*



Bluetooth low energy



For Classic *Bluetooth*

- The number of Packets with **No Errors** and percentage of packets with **No Errors** in relationship to total packets for the channel is displayed in green.
- The number of Packets with **Header Errors** and percentage of packets with **Header Errors** in relationship to total packets for the channel is displayed in red.
- The number of Packets with **Payload/CRC Errors** and percentage of packets with **Payload/CRC Errors** in relationship to total packets for the channel is displayed in dark red.
- The number of **Retransmitted** Packets and percentage of **Retransmitted** packets in relationship to

total packets for the channel is displayed in yellow.

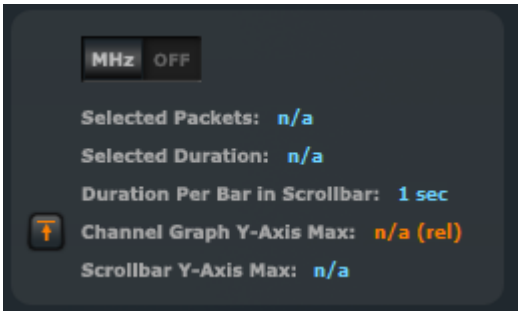
- **Total** packets and **Total** percentage is displayed in light blue.

For *Bluetooth* low energy:

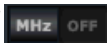
- The number of Packets with **No Errors** and percentage of packets with **No Errors** in relationship to total packets for the channel is displayed in green.
- The number of Packets with **CRC Errors** and percentage of packets with **CRC Errors** in relationship to total packets for the channel is displayed in dark red.
- **Total** packets and **Total** percentage is displayed in light blue.

For a description of the **Channel Not Available** symbol, see PER Stats Channel.

4.4.4 Packet Error Rate - Additional Statistics



This Additional Statistics section of PER Stats displays information about selected packets, duration, and Y-Axis max, and it also has two controls.

- Selecting **MHz On**  displays the megahertz value for each channel in the main channels chart and also in the expanded chart.
- Selecting **MHz Off**  removes the megahertz value.
- **Selected Packets** displays the packet range selected in the Scroll Bar. This includes inapplicable packets.
  Inapplicable packets include Wi-Fi packets, Sniffer Debug packets, any packets that are not relevant to PER Stats. Inapplicable packets do not appear as part of the Additional Statistics. packets.
- **Selected Duration** identifies the total amount of time in the selected packet range displayed in the Scroll Bar.
- **Duration Per Bar in Scrollbar:** identifies the amount of time represented by each bar in the Scroll Bar.
- The **Channel Graph Y-Axis Max** can display two different values. When the **Snap Arrow** is orange  , the values for channels in the main chart are shown in relative terms in **Snap Mode**. This means that one channel (or channels) with the greatest value is "snapped" to the top of the chart. In the graphic below left, Channel 33 is snapped to the top of the chart.
  The channel(s) with the greatest value become a full-scale reference display for the other channels that have been relatively scaled. Channel comparisons become easier. With Snap On you can select multiple time values in the Scroll Bar. When the **Snap Arrow** is white  (Snap Mode turned off), the values for channels in the main chart are shown in absolute values where the max value of each channel graph is the same regardless of the position of the Viewport. Channel 33, which is snapped to the top of the chart in Snap Mode (shown above left), appears like the right image when Snap Mode is turned off.

- **Scrollbar Y-Axis Max** displays the maximum Y-Axis value in the Scroll Bar.

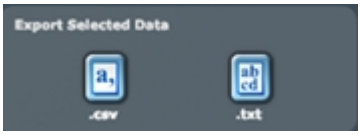
4.4.5 Packet Error Rate - Sync Selected Packets With Other Windows

By default, and unlike other windows, PER Stats is not synchronized with other windows such as Frame Display in that selecting a frame range in one does not highlight the same frame range in the other. This ensures that **Frame Display** isn't constantly re-synchronizing during live capture while the view-port is maximized in PER Stats. If PER Stats synchronization is desired, it can be enabled by checking the **Sync Selected Packets with Other Windows** check box.

4.4.6 Packet Error Rate - Export

The Export section of PER Stats allows you to export data to a .csv or .txt file.

1. To use the Export, select a range of data using the Viewport.
2. Select .csv or .txt from **Export Selected Data**, depending on what type of data file you want. The **Save As** dialog appears.



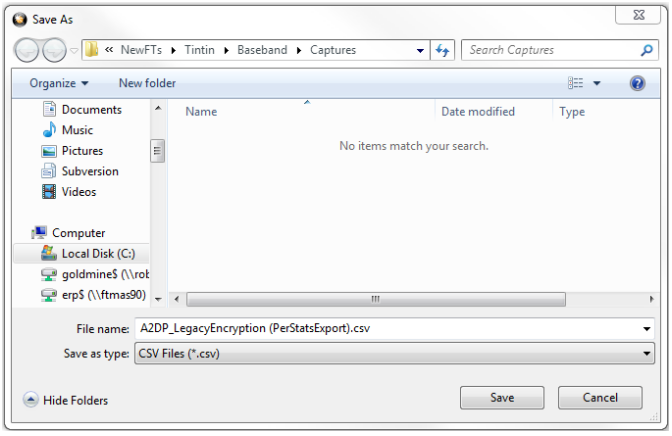


Figure 4.131 - Save As dialog in PER Stats Export

3. Select a location where you want to save the file in "Save in:".
4. Enter a file name in "File name:".
5. Select "Save".

The file will be saved to that location.

4.4.7 Packet Error Rate - Scroll Bar

The PER Stats **Scroll Bar** displays stats for all packets, divided into equal time intervals.

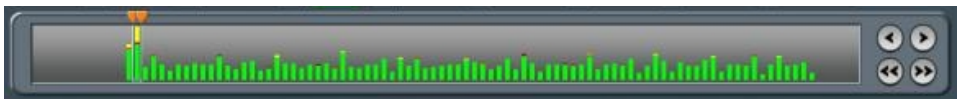
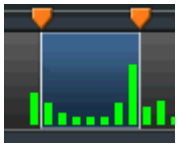


Figure 4.132 - PER Stats Scroll Bar

- Captured data begins to appear on the left and fills the width of the bar, left to right.
- The vertical bars in the **Scroll Bar** each indicate a fixed duration. When data first appears in the **Scroll Bar** as it is being captured, each bar equals one second. When the data fills the bar, reaching the right side limit, the last bar moves back to the center of the **Scroll Bar**. The bars stay the same size, but doubles in duration (for example, the first time the **Scroll Bar** fills, the bars return to the middle, but now each bar represent two seconds of time instead of one). Each time the bars cycle to the middle, the time they represent doubles. When the bars move and the **Viewport** (see below) is not maximized, the **Viewport** moves with the bars so that the same packet range is indicated. When the **Viewport** is maximized it stays maximized regardless of what the bars do. This ensures that the display can be made to reflect all packets at all times by maximizing the .
- The **Viewport** is used to select single  or multiple vertical bars  .
- You can drag the sides of the **Viewport** or the slider buttons to select multiple bars, representing a greater time range.
- You can click and drag the **Viewport** within the **Scroll Bar**.
- When you select a packet range in **Frame Display** that includes only some of the frames in PER Stats, the **Viewport** snaps up against the side of the bar with the unselected frames  .
- When you select a packet range in Frame Display that includes all of the frames in PER Stats, the Viewport displays a space between the Viewport sides and the bar  .
- Double clicking anywhere inside the **Scroll Bar** selects the entire **Scroll Bar**. Double clicking again toggles back to the previous size of the **Viewport**.
- Selecting Ctrl+A is the same as double-clicking.
- Clicking on a vertical bar left justifies the **Viewport** to that bar.
- Shift-clicking on a bar extends the nearest **Viewport** side to include that bar.
- The Home key moves the **Viewport** to the left edge.
- The End key moves the **Viewport** to the right edge.
- Pressing the left arrow button  , the left arrow key, or the up arrow key moves the **Viewport** to the left, one vertical bar at a time.
- Pressing the right arrow button  . the right arrow key, or the down arrow key moves the **Viewport** to the right, one vertical bar at a time.
- Pressing the double left arrow button  or the PgUp key moves the **Viewport** to the left by the current width of the **Viewport**. Holding down the Shift key will prevent the **Viewport** from moving if there is not enough room to move by its full width.
- Pressing the double right arrow button  or the PgDn key moves the **Viewport** to the right by the current width of the **Viewport**. Holding down the Shift key will prevent the **Viewport** from moving if there is not enough room to move by its full width.

- Holding the Shift key down and the right or left arrows moves the right side of the **Viewport**.
- Holding the Ctrl key down and the right or left arrows moves the left side of the **Viewport**.
- The Scroll bar includes inapplicable packets (sniffer debug, WiFi, etc) so that the packet range selected in Frame Display can be shown. Inapplicable packets are not, however, included in the statistics reports.
- If the **Viewport** is adjusted within PER Stats, as opposed to selecting a packet range in Frame Display, it uses only whole bars on both sides.
- Statistics are retained for all packets regardless of whether any of those packets have wrapped out. You can select the **Reset** button  , which is located above the right portion of the **Scroll Bar**, to discard all stats for packets received up to that point.
- The **Reset** button is only available when you are capturing data.

4.4.8 Packet Error Rate - Excluded Packets

ID packets and packets that are missing channel numbers (such as HCI and BTSnoop) will not display data. ID packets are excluded because they can not have errors or indicate retransmission and therefore dilute the percentages for other packet types. Packets without channel numbers are excluded because the graphs are channel-specific. Before packets are captured, the Scroll Bar in Classic *Bluetooth* PER Stats contains the message "ID packets and packets without a channel number (such as HCI) are excluded", and the Scroll Bar in *Bluetooth* low energy PER Stats contains the message "Packets without a channel number (such as HCI) are excluded".

Figure 4.133 - Example: Excluded Packets Message in Scroll Bar (Classic *Bluetooth*)

4.5 *Bluetooth* Audio Expert System™

The *Bluetooth* Audio Expert System™ monitors and analyzes *Bluetooth* audio streams with the purpose of detecting and reporting audio impairments. The primary goal of the Audio Expert System™ is to expedite the detection and resolution of *Bluetooth* protocol related audio impairments. To achieve this, the system automatically identifies audio impairments and reports them to a user as "events". It also correlates the audio events with any detected codec or *Bluetooth* protocol anomalies (events). The system allows a user to view the audio waveform, audio events, codec events, and *Bluetooth* protocol events on a time-aligned display.

An Audio Expert System™ event identifies to the user information, warnings, and errors. Event categories are shown in the following table.

Table 4.23 - Audio Expert System™ General Events

Event Category	General Events Reported
Bluetooth Protocol	Protocol violations
	Best practice violations
Codec	Configuration changes
	errors
Audio	impairments (errors)
	information data

When the Frontline software captures data, if there is audio content that must be debugged this data must be systematically examined when looking for the problem source. The effort to identify and correlate the audio related data can be daunting because the problem source may be caused by protocol, codec, or the audio itself. Using the Audio Expert System™ identifies events that are likely candidates for audio root cause analysis. The expert system examines all captured frames—in live capture or in capture file viewer—and selects audio-related protocol, codec, and audio events. The events are time correlated to the audio stream and identified with specific frames. In general, a cluster of events suggests an area for investigation, and in the presence of multiple event clusters the cluster with the most events suggests the best starting point.

The expert system works in conjunction with Frontline software that is operating in live capture mode or in capture file viewer mode. Selecting an event in the Audio Expert System™ will simultaneously highlight related packets in the Frontline software **Frame Display**, **Coexistence View**, **Message Sequence Chart**, **Bluetooth Timeline**, and **Packet Error Rate Statistics** (**PER Stats**) windows.

Audio Expert System™ further provides methods for isolating testing to specific audio events by using two operating modes: non-referenced and referenced.

Table 4.24 - Audio Expert System Operating Modes

Mode	Description
Non-referenced	Processing audio of completely unknown program content (e.g. arbitrary music or speech content). Since the system does not have any prior knowledge of the audio being analyzed, the types of audio analysis that can be performed is limited.

Table 4.24 - Audio Expert System Operating Modes (continued)

Mode	Description
Referenced	A “pseudo closed loop” test scenario where the user plays specific Reference Audio files (pre-recorded audio test files provided by Frontline) on the Source DUT (Device Under test). The analysis of the received audio results in a series of “Audio Events” being reported by comparing changes in the received audio to expected changes of the Reference Audio, and reporting deviation events when they occur.

Reference mode detects a larger number of events because the reference audio has specific frequency, amplitude, and duration occurring at known points in time allowing for precise comparison.

4.5.1 Supported Codec Parameters

Supported Parameters for SBC Codec

- Sampling Frequencies: 16 KHz*, 32 KHz*, 44.1 KHz, 48 KHz
- Channel Modes: Mono, Dual Channel, Stereo, Joint Stereo
- Block Length: 4, 8, 12, 16
- Number of subbands: 4, 8
- Allocation Method: SNR, Loudness
- Minimum Bitpool Value: 2
- Maximum Bitpool Value: 53

Supported Parameters for MPEG-2, 4 AAC

- Object Types; MPEG-4 AAC LC
- Sampling Frequencies: 44.1 KHz, 48 KHz, 8 KHz*, 11.025 KHz*, 12 KHz*, 16 KHz*, 22.050 KHz*, 24 KHz*, 32 KHz*, 64 KHz*, 88.2 KHz*, 96 KHz*
- Channels: 1 and 2
- Variable Bit Rate and Specified Bit rate

* Audio Analysis not supported . Although, user will be able to play back the audio live.

Supported Parameters for aptX

- Object Types; aptX-classic, aptX-LL (both content protected and non-content protected)
- Audio Format: 16-bit, 44.1kHz
- Data Rates: 352 kbps

Supported Parameters for CVSD

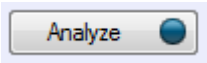
- Channel Mode: Mono
- Sampling Rate: 64 kHz

Supported Parameters for mSBC codec

- Channel Mode: Mono
- Sampling Rate: 16 kHz
- Allocation method: Loudness
- Subbands: 8
- Block Length: 15
- Bitpool: 26

4.5.2 Using Audio Expert System™ with Sodera

When analyzing audio data using the Sodera Wideband *Bluetooth* Protocol Analyzer, the Audio Expert System™ supports from 1 to 4 slave devices. All the slave devices must be in the same piconet, that is, they all have the same master device. The slave devices are selected in the Wireless Devices pane.



After selecting the devices, and, if necessary, providing the key in the **Security** pane, click on the Sodera **Analyze** button. When an audio stream is detected the Audio Expert System™ window will automatically open and display the steam information.

4.5.3 Starting the AudioExpert System

To use the Audio Expert System™, the user must have

- Current Premium Maintenance purchased from Frontline
- Frontline hardware, with Audio Expert System™ license installed, connected to the PC. This is a requirement for both live capture and when viewing a saved capture file.

For live capture, set up the Frontline Sodera datasource and begin capturing data.

> **Note:** Proper positioning of the Frontline hardware relative to the devices under test (DUT1-source, DUT2-sink) will contribute to effective data capture. Air Sniffing: Positioning Devices on page 93.

For viewing a capture file, load the saved file from the **Control** window **File** menu.

When an audio stream is available the open the **Audio Expert System™ Window** by clicking on the **Control** window Audio Expert System™ button  . If the Frontline hardware is not licensed for Audio Expert System™, the button will not be present.

4.5.4 Operating Modes

The *Bluetooth* audio analysis can be accomplished in two modes: 1) unreferenced mode, and 2) referenced mode.

4.5.4.1 Non-Referenced Mode

In Non-Referenced Mode, the system is typically processing audio of completely unknown program content (e.g. arbitrary music or speech content). Since the system does not have any prior knowledge of the audio being analyzed, the types of audio analysis that can be performed is limited.

The following events are reported whenever the system is operating in Non-Reference mode. These are the meaningful audio analysis that the system can perform without reporting too many false positive results.

- Volume Level (Low Volume or High Volume): Reported if the average volume level is not in a range conducive to performing meaningful audio analysis.
- Clipping: Amplitude distortion due to a signal amplitude exceeding the maximum value that can be represented by the digital system
- Dropout: Abrupt and very short duration intervals of silence
- Glitch: Extremely large sample-to-sample audio amplitude transitions that have little probability of occurring within natural speech or music

4.5.4.2 Referenced Mode

In Referenced Mode, the system operates in a “pseudo closed loop” test scenario where the user plays a specific Reference Audio file on the Source DUT. The Source DUT negotiates with the Sink DUT to determine the appropriate codec and audio parameters to use and will then process the Reference Audio file accordingly before transmitting the resulting audio via *Bluetooth*. The Reference Audio is a pre-recorded audio test file provided in the Frontline software installer.

The Sink DUT receives the encoded audio, decodes it, and processes it for playback. In parallel, the Frontline analyzer unit snoops the over-the-air signal between the Source DUT and Sink DUT and emulates the RF reception and decoding done inside the Sink DUT. The Audio Expert System™ automatically detects that a Reference Audio file is being received and then analyzes the resulting audio for deviations from expected parameters.

Referenced Audio files are protocol specific.

The following events are reported whenever the system is operating in the Referenced mode.

- Test ID Found
- Test Script Not Found
- Invalid Test Script
- Synchronization Lost
- Unexpected Frequency
- Unexpected Level
- Unexpected Duration
- Amplitude Fluctuation
- Unexpected Phase Change
- Clipping
- Excess Noise
- CVSD HF Level Too High
- End of Test

Reference Audio Test Files

The Reference Audio files are specific audio files that exercise the system so that audio impairments can more efficiently and accurately be identified and reported. The Reference Audio files are composed of a series of back-to-back and relatively short duration tones of changing amplitude, frequency, and duration.

The test files are stored on the users computer In the directory "\Frontline <*version #*>\Development Tools\Audio Expert Test Files\". For example,

Test_1.03_48kHz_16Bit_3Loops_2Ch.wav

> **Note:** Reference test files are periodically updated. Shown here is an example. Files delivered with your latest Frontline software version may have changed. Contact Frontline Technical Support for information on the latest reference file versions.

The test files have a set of tones forming a unique Test ID that lets the ComProbe analyzer know that it is capturing a test file instead of an arbitrary audio stream. There is no need for special configuration of the ComProbe analyzer. The Test ID will have the identifier notation N.vv, where N = the file number and vv = a two digit version, for example 1.02.

Using the Test Files

The analysis of the received audio results in a series of Audio Events being reported by comparing changes in the received audio to expected changes of the Reference Audio, and reporting deviation events when they occur.

The system starts up in Non-Referenced mode, and is continuously looking for a valid Reference Audio file by measuring frequency and amplitude of the received over-the-air audio. Transitioning to Referenced mode requires the successful detection of a Test ID tone sequence of proper frequency, duration, and value.

Once the Referenced Mode state is achieved, the expectation is that all tones encountered will conform to the script identified by the Collected Digits (the “Test ID”). The system remains in the Referenced Mode state until either the end of test is reached, or a loss of synchronization occurs.

The synchronization of the received audio (from the Reference Audio files) versus the internal Test Script is achieved based on changes in frequency of the tones in the Reference Audio file. Frequency changes are used because this parameter is relatively immune to the configuration of the network.

For a comparison of reference mode detectable problems to unreferenced detectable problems see the table in the audio event type table.

The Test Script

The Reference Audio used for Referenced Mode testing is generated from scripts that define a series of audio segments. Each segment provides an audio tone parameters including frequency, amplitude, duration, fade in and fade out durations, and start time. The script is an XML file delivered with the Frontline software. This file is used during Referenced mode testing for comparison to the "sniffed" Reference Audio parameters of frequency, amplitude, duration, etc.

Below is a sample script table and the resulting sample Reference Audio .wav file. The generated .wav file begins with a Test ID that is used to identify the "sniffed" audio as a Reference Audio file, and the Audio Expert System™ automatically switches from Non-Referenced mode to Referenced mode.


```
  <?xml version="1.0" encoding="UTF-8"?>
- <SegmentArray>
  - <Segment>
      <SegID>0</SegID>
      <Opcode>F</Opcode>
      <Frequency>100</Frequency>
      <Level>-95</Level>
      <Cycles>10</Cycles>
      <Duration>0.1</Duration>
      <FadeIn>0</FadeIn>
      <FadeOut>0</FadeOut>
      <StartTime>0</StartTime>
    </Segment>
  - <Segment>
      <SegID>1</SegID>
      <Opcode>F</Opcode>
      <Frequency>210</Frequency>
      <Level>-3</Level>
      <Cycles>21</Cycles>
      <Duration>0.1</Duration>
      <FadeIn>0</FadeIn>
      <FadeOut>0</FadeOut>
      <StartTime>0.1</StartTime>
    </Segment>
  - <Segment>
      <SegID>2</SegID>
      <Opcode>F</Opcode>
```


Table 4.25 - Sample Test Script Table

Segment	OpCode	Frequency	Level	Cycles	Duration	Fade in	Fade Out	Start Time
1	F	200	0	5	0.025	0	0	0.000
2	F	1000	0	25	0.025	0	0	0.025
3	F	300	-12	15	0.050	0	0	0.050
4	F	600	0	30	0.050	0	0	0.100
5	F+	880	-6	44	0.050	0	0	0.150
6	F+	240	-6	12	0.050	0	0	0.150
7	F	600	-95	30	0.050	0	0	0.200
8	F	600	0	30	0.050	0	10	0.200

4.5.4.3 Referenced Mode Testing Processes

In the Referenced mode, the devices under test use a specific audio file (called reference file or test file) provided by Frontline whose contents are already known to the Frontline software. The software compares the parameters of the received audio data against its parameters and presents analysis for the user. Commonly, in Bluetooth technology the music sent via A2DP and speech sent via HFP. There are a few ways users can conduct referenced mode testing depending upon what profile they are using. The figure 17 shows the source of the audio and the medium through which it can be accessed by Source device to send to sink device via Bluetooth.

Table 4.26 - Referenced Mode Testing Process Between Two DUTs

Audio Source	Process to Send Using A2DP	Process to Send Using HFP
A file stored on the device's local memory	Play the locally stored file on the audio source device	Play using the third party App that transmits music data on HFP.
Streaming audio over a cellular network	Play the test in a browser on the audio source device https://youtu.be/rmirDbikrtM	Make a call to 434-964-1407 or 434-964-1304 through a cellular network. The phone number receiving the call playbacks recorded test signal.
Streaming audio over a Wi-Fi network	Play the test in a browser on the audio source device https://youtu.be/rmirDbikrtM	Make a call to 434-964-1407 or 434-964-1304 through a VoIP provider such as Skype. The phone number receiving the call playbacks recorded test signal. **Potential problem**: The VoIP provider might use custom codecs and cause undesirable behavior.

A2DP

Playing the test file locally

The simplest way to perform music data testing is to directly play the reference file from DUT1 to DUT2. To do that, save the reference file provided with the Frontline software on the Source device. Then connect the Bluetooth enabled devices and play the music file from one device to the other. The software will automatically detect the mode and present analysis for the user.

Playing the test file via Internet

If the user is testing a scenario where they need to analyze audio played through the internet (either using Wi-Fi or cellular data plan), they may access the reference file on YouTube provided by Frontline - https://youtu.be/rmirDbikrtM. Note that the software is only analyzing the Bluetooth link between the two DUTs. Any abnormalities at the Wi-Fi and cellular network level will affect the audio quality that may not be Bluetooth protocol related and the software will not be able to detect that.

HFP

Playing the test file by calling a phone number

Frontline provides the following phone numbers - 434-964-1407 and 434-964-1304 that users can call, to conduct speech audio data analysis over Bluetooth. The calls can be made using the cellular network (most common method) or VoIP. Again, the VoIP provider might use custom codecs and cause undesirable behavior which cannot be detected by Audio Expert System™ software.

Playing the test file using Third party Apps

Bluetooth Audio Expert System™ Reference mode testing can be accomplished using third party apps on Android, iOS, and Windows phones. The following apps are available from their respective App stores:

- BTmono, Android
- Blue2Car, IOS
- Windows Headset player lite

> **Note:** When selecting and using these apps, thoroughly review all the vendor documentation. While Teledyne LeCroy has conducted testing of these apps, Teledyne LeCroy has not completed full interoperability testing with our library of *Bluetooth* devices and does not warrant the use of these apps with every device when using the following procedures. Teledyne LeCroy does not provide support or maintenance for third party apps. Any issues or questions should be directed to the app developer.

1. In the following steps Device Under Test 1 (DUT1) is the device sending the reference test file to DUT2.
2. Download the third party app to DUT1 and follow the app vendor's instructions for installation and use.
3. Load the Audio Expert System reference test file

   "Test_1.02_64.1kHz_16Bit.wav"

   on DUT1.The test file is stored on the users computer In the directory "\Frontline <version #>\Development Tools\Audio Expert Test Files\".

   > **Note:** Reference test files are periodically updated. Shown here is an example. Files delivered with your latest Frontline software version may have changed. Contact Teledyne LeCroy Technical Support for information on the latest reference file versions.

4. With the Sodera connected to the computer, configure the datasource, and follow procedures to capture data.
5. Launch Audio Expert System by clicking on the **Control** window .
6. Turn on Bluetooth on your DUTs, DUT1 and DUT2. Turn on the third party *Bluetooth* app for routing the reference file over A2DP or HFP by following the vendor's directions.
7. Send the reference test file from DUT1 to DUT2 via the third party app.
8. Observe the events in the Audio Expert System™ **Events Table**. Look for an event **Description**:

   “TestIDFound : REF: Test ID 1.02, Channel Gain = -11.8 dB TermFreq=400.0”.

   > **Note:** This is an example. The display may vary with the reference file version.

   The Frontline analyzer has successfully detected the reference test signal and the system is locked into reference mode.

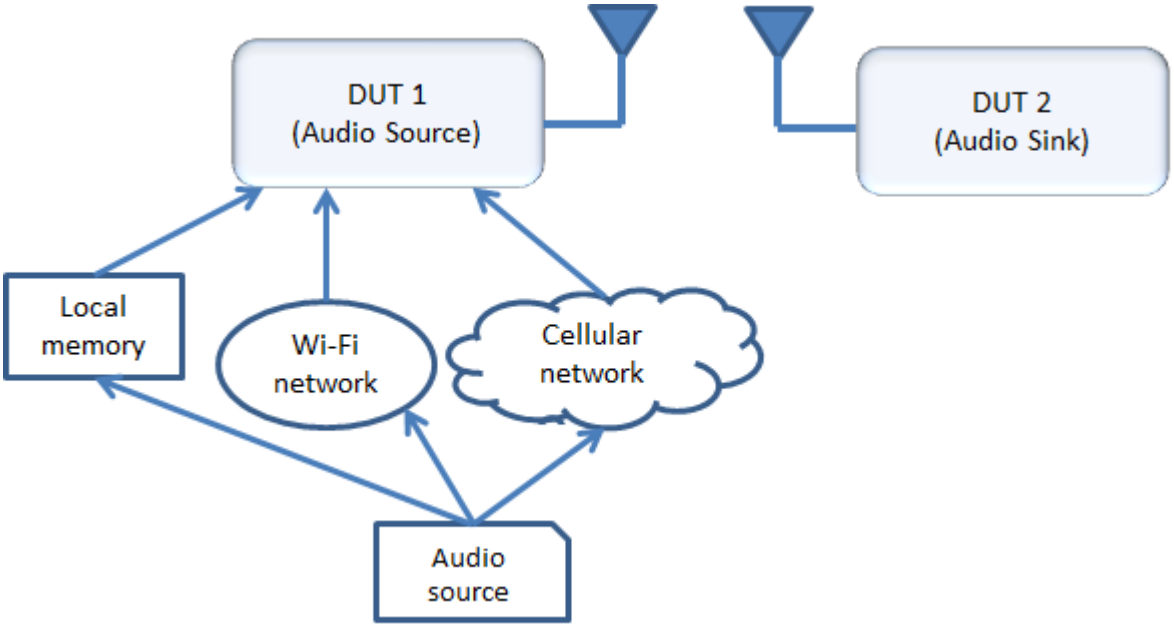


Figure 4.134 - Test Cases for Referenced Mode Testing

4.5.4.3.1 System Calibration for Referenced Mode

The objective is to achieve settings at the *Bluetooth* source device (DUT1) that bring the PCM sample levels of tones in the Reference Audio files sent over-the-air as close as possible to the levels at which they were created, without exceeding them. Test ID tones, and the tones in test file sequences for Referenced Mode are generally recorded with a maximum tone segment level of -3 dBFS, although there are a few exceptions where signal levels may be as high as -1 dBFS.

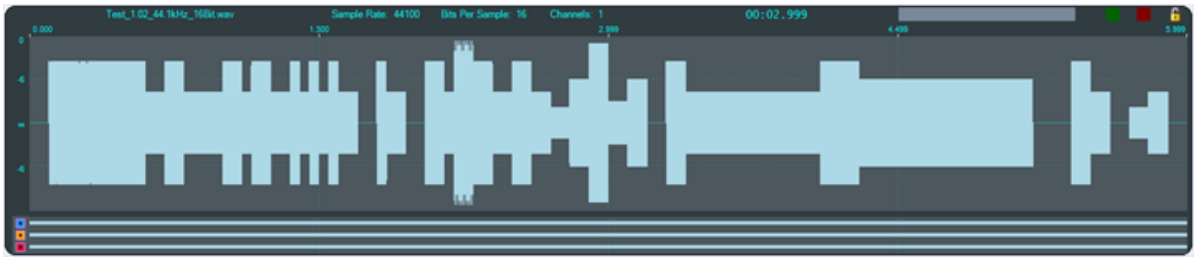


Figure 4.135 - Test_1.02_44.1kHz_16Bit.wav Waveform

Show in the image above, is a graphic of the overall envelope of the Reference Audio test file “Test_1.02_ 44.1kHz_16Bit.wav. Test 1.02 is a test file that enables a wide range of tests that includes a number amplitude changes, frequency changes, intentional silence, and multi-frequency tone segments. Its goal is to flush out the audio chain’s general ability to convey amplitude, frequency, silence, and duration.

The ideal calibration for this file is one where the waveform visualization on Frontline’s Expert System User Interface (UI) looks identical to the one shown below with respect to maximum levels. In particular, there are three segments in this test whose peaks are at exactly -6 dBFS. That is, there is zero loss or gain through the chain.

Table 4.27 - Test 1.02 -6 dBFS Segments

SegmentID	Frequency, Hz	Start Time, sec.	Duration, sec.
32	800	2.800	0.100
35	1120	3.100	0.100
40	400	4.300	0.900

These -6 dBFS segments are described in the Test 1.02 -6dBFS Segments table . These segments serve as a convenient and quick visual indicator that levels are appropriate, especially the longer 3rd case which is evident at the 4.999 second reference time of the above image(a little over 2/3 of the way through the test).

The first 0.500 seconds of Test 1.02, which contains the Test ID value “1.02” is shown below. The three digits ‘1’, ‘0’, and ‘2’ are represented by the low frequencies 210Hz, 200Hz, and 220Hz, respectively, which are 100 milliseconds in duration, and are separated by 1 kHz digit delimiters of 50 milliseconds duration. The final tone is a 100 millisecond segment at 400 Hz, defined as a “Test ID Terminator”. Note that since the levels of all of these tones are at exactly -3 dBFS, the peak levels should be exactly halfway between any available -6 dBFS (50%) gridline.

Figure 4.136 - Test 1.02 Test ID Segment

The three digits ‘1’, ‘0’, and ‘2’ are represented by the low frequencies 210 Hz, 200 Hz, and 220 Hz, respectively, which are 100 ms in duration, and are separated by 1 kHz digit delimiters of 50 ms duration. The final tone is a 100 ms segment at 400 Hz, defined as a “Test ID Terminator”. Note that since the levels of all of these tones are at exactly -3 dBFS, the peak levels -3 dBFS.

The value in the Info1 parameter of the “Test ID Found” event is optimally the value 23196 and may be converted to dBFS by the relationship

$$\mathrm{dBFS} = 20\log_{10}\left(\frac{\mathrm{info1}}{32767.0}\right).$$

Optionally the value can be interpreted as “Channel Gain” via the relationship

$$\mathrm{dB} = 20\log_{10}\left(\frac{\mathrm{info1}}{23196.0}\right).$$

Table 4.28 - "Test ID Found" Event "info1" Maximum and Minimum Values

Format	Application	Maximum	Minimum
Integer	Speech	23196	5826
	Music	23196	3297
Level	Speech	-3 dBFS	-15 dBFS
	Music	-3 dBFS	-20 dBFS
Chanel Gain	Speech	0 dB	-12 dB
	Music	0 dB	-17 dB

This table indicates the maximum and minimum acceptable levels for the “Test ID Found” Info1 parameter in integer form, decibel level in dBFS, and Channel Gain in dB.

Example 1: For the case where the Info1 parameter is converted to “Channel Gain”, if the audio is speech (i.e. transported via a SCO channel), then a value of -11.9 dB is acceptable, and a value of -12.1 dB is not.

Example 2: For the case where the Info1 parameter is converted to “Channel Gain”, if the audio is music (i.e. transported via an A2DP connection), then a

value of -16.9 dB is acceptable, and a value of -17.1 dB is not.

For both cases, at the high volume end, a value of -0.1 dB is acceptable, a value of 0.1 dB is not.

The dynamic range of the audio path is important to understand because it has a direct impact on measurement accuracy. Only levels at or above the minimum and at or below the maximum are examined for expected level and frequency.

4.5.4.3.2 Adjusting for Optimal Volume Levels

The exact steps that need to be taken depend on the exact devices being used, and their device specific setup requirements, and the speech or audio configuration under test. For the simplest case where, for example, a “music” audio file is to be played by a smartphone to a set of *Bluetooth* speakers, the typical steps would include the following.

1. Choose an audio reference file to be played at DUT1 appropriate for the configuration to be tested.

   The test files are stored on the users computer In the directory "\Frontline <*version #*>\Development Tools\Audio Expert Test Files\". For example,

   Test_1.03_48kHz_16Bit_3Loops_2Ch.wav

   > **Note:** Reference test files are periodically updated. Shown here is an example. Files delivered with your latest Frontline software version may have changed. Contact Frontline Technical Support for information on the latest reference file versions.

2. Before establishing the *Bluetooth* connection, play the file while listening to it on the DUT1 device itself, and become familiar with the overall sound quality, generally ignoring exact volume.
3. Set the playback volume at DUT1 to maximum.
4. Set the playback volume at DUT2 to minimum.
5. Establish the *Bluetooth* connection and begin playback of the file on DUT1, if possible in “Loop” or “Repeat” mode to avoid having to continuously restart.
6. Slowly increase the volume on DUT2 until it is at a comfortable level.
7. If the audio sounds distorted, reduce the playback volume at DUT1, and repeat Step 6.
8. When the clarity of the audio is comparable to that heard when listening to the DUT1 device, proceed with using the Frontline software enabled to capture and analyze the Bluetooth data.
9. Visually observe the waveform in the Audio Expert System **Wave Panel** comparing it to the image above, Figure 1.1. If the level of the -6 dB, 0.9 sec duration, 400 Hz tone (a little over 2/3 of the way through the test) is grossly above or below the –6 dB (50% volume) grid line, adjust the DUT1 volume accordingly and repeat this step. Optimally it would be on or just below the -6 dB gridline, but not above. The peak should never hit the maximum positive or negative limits of the display.
10. Find the “Test ID Found” event in the **Event Table** to verify that the system has transitioned to Referenced Mode, and verify that the value for “Channel Gain” (or “Level” as implemented in the UI) is within the range of values specified in Table 1-2.

If the observed (captured) waveforms do not reasonably conform to the above graphic for Test_1.02, or the “Test ID Found” event is not reported, there is a problem along the audio chain. This could be as simple as a configuration setting, or more subtle such as an encoder/decoder incompatibility.

4.5.5 Audio Expert System™ Event Type

The following tables list the Audio Expert System™ *Bluetooth*, Codec, and audio events with description. Included in the tables is the event severity that can have three values: Information, Warning, and Error. The event severity will appear as icons and text in the Audio Event System once an audio streams has been captured. Refer to 4.5.6.3 Event Table, Event Table Columns on page 271 for an explanation of the severity types.

4.5.5.1 Event Type: *Bluetooth* Protocol

Table 4.29 - Event Type: *Bluetooth* Protocol

Protocol	Severity	Description
A2DP	Warning	AVDTP signal response received for unknown command.
A2DP	Warning	Unrecognized capability type
A2DP	Error	eSCO parameters requested.
A2DP	Error	Profile TX PDUs larger than available bandwidth for active A2DP Streaming interval.
A2DP	Error	Bitpool value does not match configured bitpool range.
A2DP	Error	Attempt to suspend inactive stream.
A2DP	Error	Configuration attempt using unsupported CODEC.
A2DP	Error	Incorrect AVTDP command length.
A2DP	Error	Unknown command Stream End Point Identifier (SEID).
A2DP	Error	A2DP stream configuration attempt using invalid CODEC parameters.
A2DP	Error	A2DP stream configuration request sent during active stream.
A2DP	Error	Audio data length does not match length header.
A2DP	Error	Incorrect A2DP SBC frame fragmentation.
A2DP	Error	A2DP SBC frame header contents does not match stream configuration.
A2DP	Error	Attempt to configure A2DP stream with unsupported configuration.
A2DP	Error	Reported A2DP stream capabilities do not contain mandatory features.
A2DP	Error	A2DP streaming L2CAP channel not disconnected after ABORT operation.
A2DP	Error	Fragmented AVDTP packet not terminated before sending next packet.
A2DP	Error	Invalid AVDTP transaction ID.
A2DP	Error	Missing AVDTP command response.
A2DP	Error	Unrecognized A2DP content protection type.
A2DP	Error	Attempt to configure delay reporting during incorrect stream state.
A2DP	Error	Attempt to open A2DP stream that has not been configured.
A2DP	Error	Attempt to close A2DP stream that is not active.
A2DP	Error	A2DP streaming channel created before configuration completed.
A2DP	Error	Configuration command contains invalid length parameter.
A2DP	Error	Configuration command contains invalid media transport format.

Table 4.29 - Event Type: Bluetooth Protocol(continued)

Protocol	Severity	Description
A2DP	Error	SBC CRC Error.
A2DP	Error	SBC invalid channel mode.
A2DP	Error	SBC invalid header.
A2DP	Error	Invalid AVDTP configuration parameter.
A2DP	Error	Invalid AVDTP stream state

4.5.5.2 Event Type: Codec

Table 4.30 - Event Type: Codec

Codec	Severity	Event	Description
SBC	Information	Codec Initialization	Codec session started
SBC	Information	Codec tear-down	Codec session ended
SBC	Information	Stream Re-configuration	Stream Re-configuration
SBC	Error	Incorrect Configuration Detected	SBC Codec detected a change in audio parameters
SBC	Error	Lost Sync	SBC Codec expected to find synch word: 0x9C instead found: 0x: typically due to corrupted data
SBC	Error	Bad Header	SBC Codec detected corrupted header: typically due to corrupted data
SBC	Error	CRC Failure	SBC Codec detected bad CRC: typically due to corrupted data
SBC	Error	No output	SBC Codec generated no output due to corrupted data
mSBC	Information	Codec tear-down	Codec Session Ended
mSBC	Information	Stream Re-configuration	Stream Re-configuration
mSBC	Warning	Packet Loss Concealment	mSBC Codec detected a bad frame and generated substitute data to compensate for it
mSBC	Error	Incorrect Configuration Detected	mSBC Codec detected a change in audio parameters
mSBC	Error	Lost Sync	mSBC Codec expected to find synch word: 0xAD instead found: 0x: typically due to corrupted data
mSBC	Error	Bad Header	mSBC Codec detected corrupted header: typically due to corrupted data
mSBC	Error	CRC Failure	mSBC Codec detected bad CRC: typically due to corrupted data
mSBC	Error	No output	mSBC Codec generated no output due to corrupted data when PLC not configured

Table 4.30 - Event Type: Codec(continued)

Codec	Severity	Event	Description
AAC	Information	Codec initialization	Codec session started
AAC	Information	Codec tear-down	Codec session ended
AAC	Information	Bitstream type set	The bitstream type has been set. For Blueooth, it should be LATM.
AAC	Warning	Single frame error, concealment triggered.	During decoding, a single frame error was detected which triggered built in concealment processing.
AAC	Error	Codec setting change	The codec has been re-initialized due to a setting change.
AAC	Error	Unframed stream error	A frame error was detected for an unframed stream. The codec is being reset in order to continue processing.
AAC	Error	Transport not initialized	The codec cannot be initialized for the given transport.
AAC	Error	Transport not supported	The selected transport is not supported. This could occur when an out of band LATM is selected opposed to in band.
AAC	Error	Transport failure	General failure in the transport.
AAC	Error	Transport error	This typically occurs when there isn't any configuration information available.
AptX	Information	Codec initialization	Codec session started
AptX	Information	Codec tear-down	Codec session ended
AptX	Error	Bad Data	Non-stereo data has been detected for incoming data stream.

4.5.5.3 Event Type: Audio

Table 4.31 - Event Type: Audio

Test Mode	Severity	Event	Description
Non-Referenced	Warning	Low Volume Alarm	Warn the user that the volume level of the detected audio is below the best range for performing meaningful audio analysis. Alarm is initialized when volume level above the "**Measurement Threshold**[1]" level is detected. Alarm is activated when the detected volume drops below the "Measurement Threshold" level for 10 consecutive 0.5 sec measurement intervals.

[1]The volume threshold above which useful audio analysis is possible.

Table 4.31 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Non-Referenced	Warning	Clipping	Reports the detection of suspected distortion that occurs when the amplitude of a signal exceeds a digital systems ability to represent it accurately. Clipping is a type of amplitude distortion. The system reports a Clipping event when consecutive samples at the maximum value that can be represented by the digital system have been detected. Note that the maximum value that can be represented is different depending on the number of bits per sample (i.e. bits of resolution) of the audio stream. The system limits the number of reported Clipping events to typically 10 to 20 per sec.
Non-Referenced	Warning	High Volume Alarm	Warn the user that the volume level of the detected audio is above the best range for performing meaningful audio analysis (i.e. above a level where the audio will likely become distorted). Alarm is activated when the detected audio volume is continuously above the **high volume threshold**[1] (see Figure 2) for 10 consecutive 0.5 sec measurement intervals (i.e. 5 sec total). The event will not be repeated again until the detected volume level drops below the high volume threshold for 10 more consecutive 0.5 sec measurement connections.
Non-Referenced	Warning	Dropout	Reports the detection of an unusual brief silence period where the brief silence is preceded and followed by “normal” audio levels. A typical definition of Dropout is the short dramatic loss of volume typically caused by lost digital information. Root causes include transmission system errors resulting in lost data packets, transmission channel reconfigurations, bad sections of memory, processor overloads that temporarily interrupt the flow of information, and so on.
Non-Referenced	Warning	Glitch	Extremely large **sample-to-sample audio amplitude transitions**[2] that have little probability of occurring within natural speech or music. Such dramatic changes would typically happen only in situations of dropped samples.

[1]High Volume Threshold for speech: - 6dBFS High Volume Threshold for music: -12 dBFS

[2]Glitch sample-to-sample audio amplitude transitons: Speech: greater than 40 dB change Music: greater than 90 dB change

Table 4.31 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Info	TestID Found	Occurs when a valid **Test ID**[1] has been recognized. A valid Test ID must meet the level, frequency, duration, and delimiter requirements. If any of these parameters do not match, the process is terminated and is reset to the initial conditions. Until a Test ID is successfully recognized, the system will continue to operate in Non Referenced Mode; therefore, no events related to false starts are reported. This is because for arbitrary audio there is no expectation of any Test ID.
Referenced	Warning	Test Script Not Found	Occurs if a valid Test ID was found , but the script for that Test ID was not found. The system reverts to Non-Referenced Mode if this happens. This event should not occur if using a valid Reference Audio file provided by Frontline.
Referenced	Error	Invalid Test Script	This event is generated when an error occurs while accessing information in a script. This event should not occur if using a valid reference audio file provided by Frontline.
Referenced	Error	Synchronization Lost	Generated when after a successful TestID recognition the system encounters unexpected frequencies or durations of audio segments while analyzing a received Reference Audio file. If this situation occurs, the internal segment tracking logic attempts to look forward and/or backward in the test script to determine if the currently measured characteristics are consistent with the previous or next segment of the script. If there is a match, the internal segment pointer is advanced or retarded appropriately, the Synchronization Lost event is not generated, and the audio analysis continues. However, if a match cannot be found, the system declares itself out of sync and generates the Synchronization Lost Event, terminates any active test script, and reverts to Non-Referenced Mode.
Referenced	Error	Unexpected Frequency	Reported when a measured frequency deviates from an expected frequency by a specific percentage (determined by the negotiated parameters of the over-the-air audio stream). The system knows the Reference Audio file that is being played on the Source DUT; therefore, the system knows which frequencies (tones) to expect at a given time.

[1]A “Test ID” is three digits minimum in length, representing a dot notation “N.vv” Test Identifier. The Value ‘N’ may be any length >= 1 indicating a specific test number, and “vv” represents a two digit version. Each digit is represented by a tone between 200 and 290 Hz, and is followed either by a 1 kHz delimiter tone or a 400 Hz Test ID terminator. The digit ‘0’ is represented by 200 Hz, the digit ‘1’ by 210 Hz, and so on, up to the digit ‘9’ represented by 290 Hz.

Table 4.31 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Error	Unexpected Level	Reported when the measured level at the start of a tone segment is not within tolerance. The tolerance is dependent on sample rate and bits per sample, but it generally is +/- 3 dB for speech and +/11 dB for music. The system knows the Reference Audio file that is being played on the Source DUT; therefore, the system knows which amplitude level to expect at a given time.
Referenced	Error	Unexpected Duration	Reported when a tone segment of the Reference Audio file is **shorter or longer than expected**[1]. The system knows the Reference Audio file that is being played on the Source DUT and therefore knows how long a specific tone segment should last. If either a change of amplitude or frequency arrives either before or after that programmed duration, then the change is by definition unexpected. This type of audio impairment can be caused by lost or corrupted data, repeated data, faulty packet loss concealment algorithms, etc.
Referenced	Error	Amplitude Fluctuations	Reported if the system detects unexpected amplitude changes over a given interval. The test tones in Frontline's Reference Audio files have a fixed amplitude level over their duration. Therefore, if the corresponding audio levels received over the air by the system **fluctuates**[2] more than a specified level (this level is based on the received audio stream parameters), then the system generates an Amplitude Fluctuations event.

[1]The amount that a measured duration must deviate from the programmed duration of a tone segment before the system declares this event varies, depending on the negotiated over-the-air audio stream specific parameters, but it is generally in the range of 5% to 10%. Note that this event will result in an attempt to resynchronize if the measured duration is greater than expected.

[2]The system calculates amplitude fluctuations as: (Max Level – Min Level) / (Max Level + Min Level) * 100

Table 4.31 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Error	Unexpected Phase Change	Provides a fine-grained indication of lost or repeated energy. The system knows when a specific tone should be expected. During this interval, the system checks that the measured average frequency is the same as the expected frequency. If this is correct, the system will continue to monitor the instantaneous frequency. If the instantaneous frequency deviates sufficiently from the current average frequency, the frequency measurement state machine will reset and begin re-measuring. Typically, the outcome is the discovery of the next scripted (expected) frequency. However, another outcome can be that the same frequency as the previous average frequency is rediscovered, and this is reported as an Unexpected Phase Change event. Such phase changes are an indicator of losses of signal that do not result in amplitude dropouts, or signal substitution (repetition) of previous audio energy due to things such as “packet loss concealment” tactics.
Referenced	Error	Excess Noise	The Excess Noise event is reported when energy sufficiently above the “Silence Threshold” is detected during programmed segments of silence. Excess noise can indicate a poor analog audio chain with an inherently poor noise floor, glitches occurring during silence intervals, or codecs that do not transition to silence instantaneously.
Referenced	Error	Clipping	Reports the detection of suspected distortion that occurs when the amplitude of a signal exceeds a digital systems ability to represent it accurately. Clipping is a type of amplitude distortion. The system reports a Clipping event when consecutive samples at the maximum value that can be represented by the digital system have been detected. Note that the maximum value that can be represented is different depending on the number of bits per sample (i.e. bits of resolution) of the audio stream. The system limits the number of reported Clipping events to typically 10 to 20 per sec.
Referenced	Error	CVSD HF Level Too High	Reported when a CVSD encoded audio stream is detected and there is high frequency energy above 4 kHz that is greater than -20 dBFS.

Table 4.31 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Info	End of Test Event	Reported to indicate that the system has completed processing a test script for a Reference Audio file, and that the system has exited Reference Mode. This event is generated when the elapsed time from the start of test is equal to or greater than the scripted duration of a test. It is reached when the number of samples processed equals the number of samples associated with the test duration.

Clipping

The number of consecutive samples needed to qualify as a clipping event depends on both sample rate and number of bits per sample. Table 1 specifies the number of consecutive samples at the maximum value level that will generate a Clipping event.

Table 4.32 - Clipping Event Thresholds

Consecutive Samples	Sample Rate, Samples/sec	Resolution, bits
3	8000	16
5	16000	16
11	41000	16
2	64000	16
12	48000	16
24	96000	16

Table 4.33 - Clipping Event Thresholds

Consecutive Samples	Sample Rate, Samples/sec	Resolution, bits
3	8000	16
5	16000	16
11	41000	16
2	64000	16
12	48000	16
24	96000	16

Dropout

Dropout events are reported when the average audio level (RMS) is initially above the Measurement Threshold, then falls below the Silence Threshold, and then quickly rises above the Measurement Threshold again). This approach largely disqualifies the natural inter-syllable silence and pauses that occur in natural speech, but will detect gaps caused by dropped data. Note that the system does not report dropouts that begin at very low energy levels.

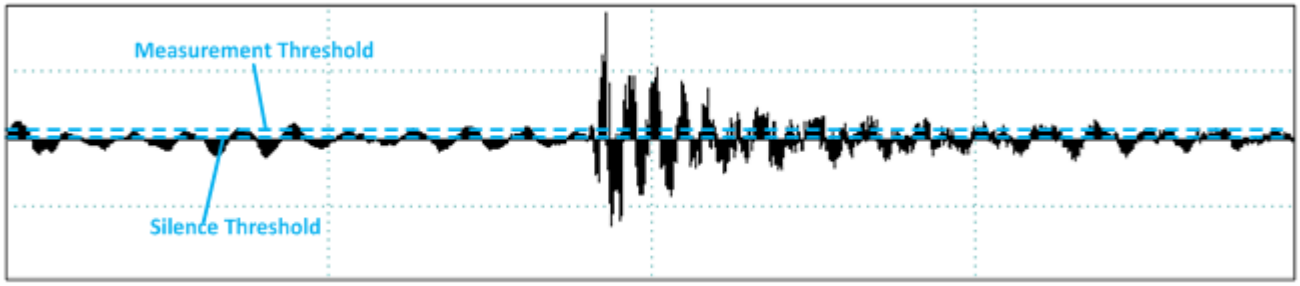


Figure 4.137 - Dropout: Measurement and Silence Threshold

Glitch

The Glitch event is reported whenever an extremely large sample to sample amplitude transition occurs that has little or no probability of occurring within natural speech or music. As illustration, back to back +N, -N, …, +N, -N values (where N is any non-zero number), represents energy at the Nyquist frequency, or ½ the sample rate. Neither speech nor music contain average energy levels at this frequency more the 20 dB below nominal. However, moderately large sample to sample changes in amplitude do occur, and these naturally limit how sensitive this measure can be configured.

The system uses back to back transition levels of 90 dB for music and 40 dB for speech as the threshold for reporting the Glitch event.

Such dramatic changes would typically happen only in the face of dropped samples, and serve as an additional means of detecting gross abnormalities

4.5.6 Audio Expert System™ Window

This window is the working space for the Audio Expert System™. Upon opening Audio Expert System™ the window shown below will open with four main areas displayed :

- Global Toolbar - Provides play cursor controls, waveform viewing controls, and volume controls that affect all Wave Panels.
- Wave Panel - Displays the waveforms for each captured audio stream. There is a separate Wave Panel for each stream. Each panel contains local information, controls, and an event timeline specific to the displayed audio stream being shown. Other Wave Panels that may be off scream may be viewed using the vertical scroll control or by collapsing other Wave Panels.
- Event Timeline - The Event Timeline shows *Bluetooth* events, Codec events, and Audio events synchronized to the displayed waveform. There is an Event Timeline in each Wave Panel.
- Event Table – A tabular listing of *Bluetooth*, codec, and audio events with information on event severity, related *Bluetooth* frame, timestamp, and event information.

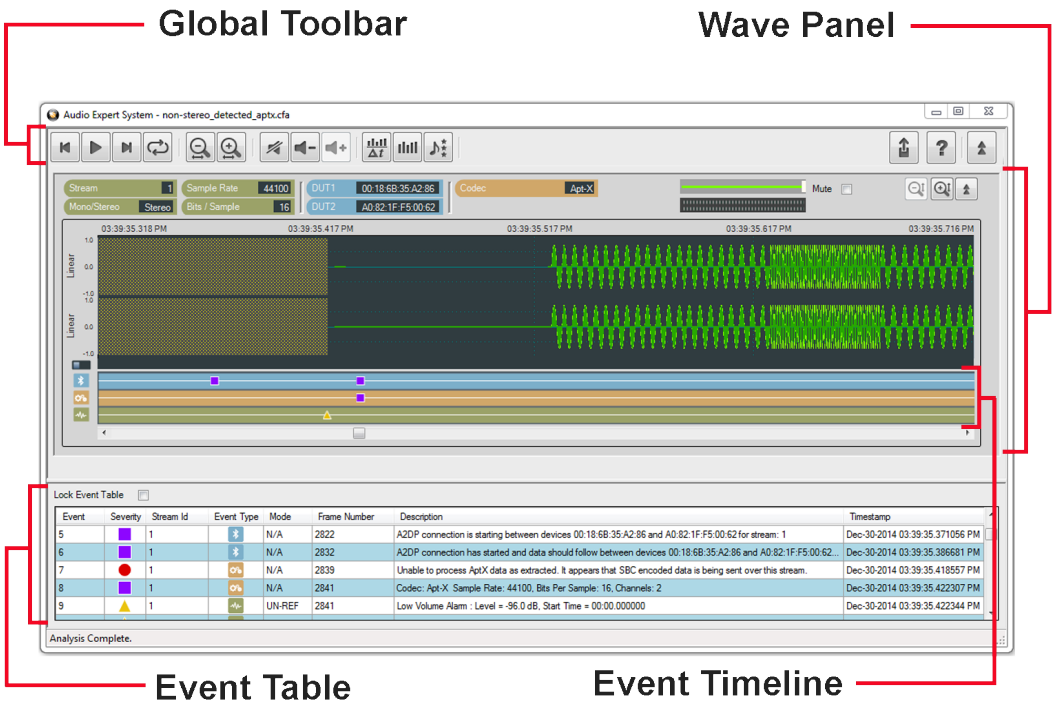


Figure 4.138 - Audio Expert System™ Window

Color Codes and Icons

The Audio Expert System™ uses standard color codes and icons to assist the user in focusing on specific issues.

Table 4.34 - Audio Expert System™ Color Codes and Icons

Category	Sub-Category	Color Code	Icon
Technology	Bluetooth	blue	
	Codec	orange	
	Audio	green	
Event Severity	Information	purple	
	Warning	yellow	
	Error	red	

Note: If an Event Severity icon is surrounded by a dark line, the event is a global event and not applying to a particular captured waveform. The event is assigned to "Stream 0" in the Event Table.

The following topics describe the Global Toolbar, Wave Panel, Event Timeline and Event Table in more detail.

4.5.6.1 Global Toolbar

The global toolbar provides audio play controls, audio play cursor positioning controls, waveform viewing controls, and volume controls. Global toolbar controls apply simultaneously to all waveform panels.

Table 4.35 - Global Toolbar Controls

Icon	Description
	Home: Moves play cursor to beginning of the waveform
	Play : Start playing the audio from the current play cursor position. Toggles to Pause when clicked. Pause: Stops audio play back at its current position, toggles to Play when clicked.
	End: Moves the play cursor to the end of the waveform
	Loop: Loops waveform playback continuously. If the Play button is visible it will toggle to the Pause. Clicking the Pause button will stop Loop playback. Clicking on the Loop button will stop the loop and the playback. If there is a selection on the waveform, only the selection will loop.
	Horizontal Zoom Out: Increases the amount of data that is visible on the screen; however, less detail is discernible.
	Horizontal Zoom In: Decreases the amount of data that is visible on the screen; however, more detail is discernible
	Lock/Unlock (Operational in live mode only): Selecting Lock will freeze the waveform display; however, the Audio Expert System™ will still continue to analysis new audio data.. Selecting Unlock will jump to the waveform end and then resume following the waveform.
	Mute: Mute will mute / unmute audio playback for all Wave Panels. Individual Wave Panel Mute control will override the Global Toolbar Mute for that panel only.
	Volume Down: Decreases the audio playback volume of all Wave Panels based on the current volume level setting for each individual Wave Panel.
	Volume Down: Decreases the audio playback volume of all Wave Panels based on the current volume level setting for each individual Wave Panel.

Table 4.35 - Global Toolbar Controls (continued)

Icon	Description
	Average Bit Rate Overlay: Displays an overlay graph of the average bit rate for the audio stream in each Wave Panel. The average is based on a 0.10 second moving window. When active, will deactivate Actual Bit Rate Overlay .
	Actual Bit Rate Overlay: Displays an overlay graph of the instantaneous bit rate for the audio stream in each Wave Panel. When active, will deactivate Average Bit Rate Overlay
	Export Data: Exports audio data in .raw and/or .wav format for selected Wave Panels or all the Wave Panels. This button also lets user export Event Table data in .csv format. Refer to Waveform Export Audio Data for more details .
	Help - Opens Frontline software help.
/	Collapse/Expand: Toggles between collapsing and expanding all Wave Panels. Note that the Wave Panel Local Controls Collapse/Expand control will locally override the Global Toolbar Collapse/Expand control.

4.5.6.2 Wave Panel

The Stream Panel is where the details of the captured audio stream are presented. The Stream Panel displays the captured audio waveform along with an event timeline that displays discrete *Bluetooth*, Codec, and Audio events synchronized to the captured waveform. .

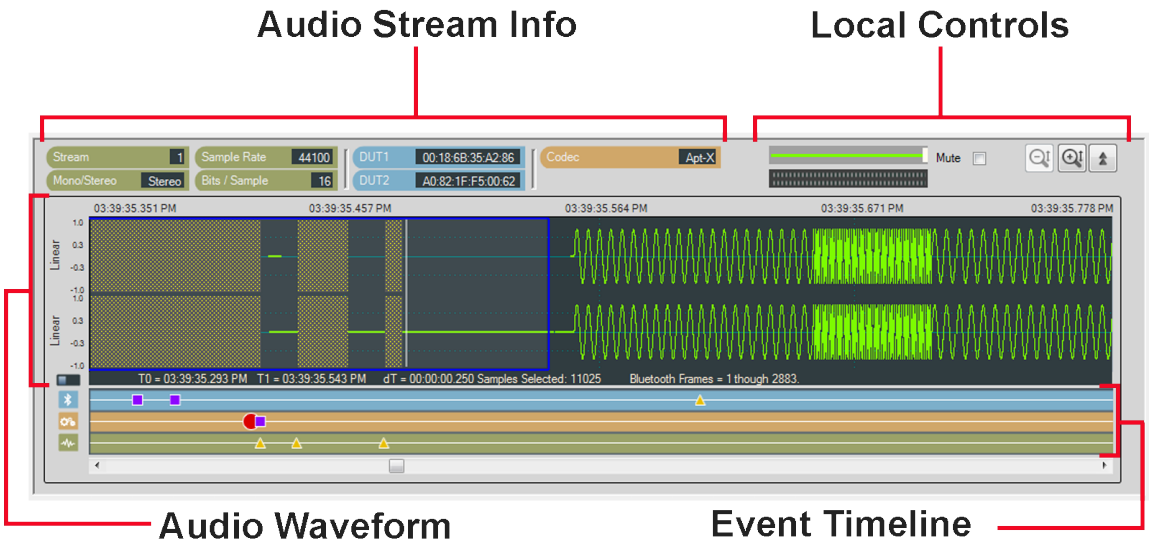


Figure 4.139 - Wave Panel

The Wave Panel contains four sections.

1. Audio Stream Info that provides users with information, such as sample rate, bit/sample, codec and DUT (Device Under Test) addresses.
2. Local Controls include audio volume controls and Indicators, “Mute”, “Vertical Zoom” and “Collapse/Expand”
3. An Audio Waveform which is plotted as amplitude (linear or dB) versus time and an interactive play cursor. The play cursor appears as a white vertical line across the waveform.
4. Event Timeline that shows color coded *Bluetooth* , Codec , and Audio events. Details of these events are listed in the Audio Expert System™ Event Table.

4.5.6.2.1 Audio Stream Info

The Audio Stream Info displays Audio, *Bluetooth*, and Codec information (left to right in the image below) about the audio waveform displayed in the panel. This information is discovered during AVDTP signaling when the devices under test (DUT) negotiate audio streaming parameters.

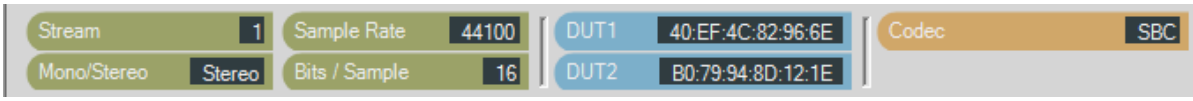


Figure 4.140 - Audio Stream Info in the Wave Panel

Table 4.36 - Audio Stream Info Tags

Category	Name	Description
Audio	**Steam**	A system assigned index number that represents an audio waveform between a pair of Bluetooth devices. This number appears in the Event Table for easy cross-referencing.
	Sample Rate	Displays the sampling frequency used to digitize the original audio.
	Mono/Stereo	Indicates if the audio data is monaural or stereophonic.
	Bits/Sample	Displays the number of bits per sample of the audio data.
Bluetooth	**DUT1**	*Bluetooth* address of one device in the connection. Can be either sending or receiving the audio data.
	DUT2	*Bluetooth* address of the other device in the connection. Can be either sending or receiving the audio data.
Codec	**Codec**	Displays the Codec type used by the captured audio stream. The supported codecs include SBC, AAC, aptX, mSBC, and CVSD.

SBC Codec Information Pop-up

When you hover over the **Codec** tag and the Codec = SBC a pop up will appear that shows additional information about which SBC parameters can be used. The pop-up is visible as long as the cursor hovers over the **Codec** tag.

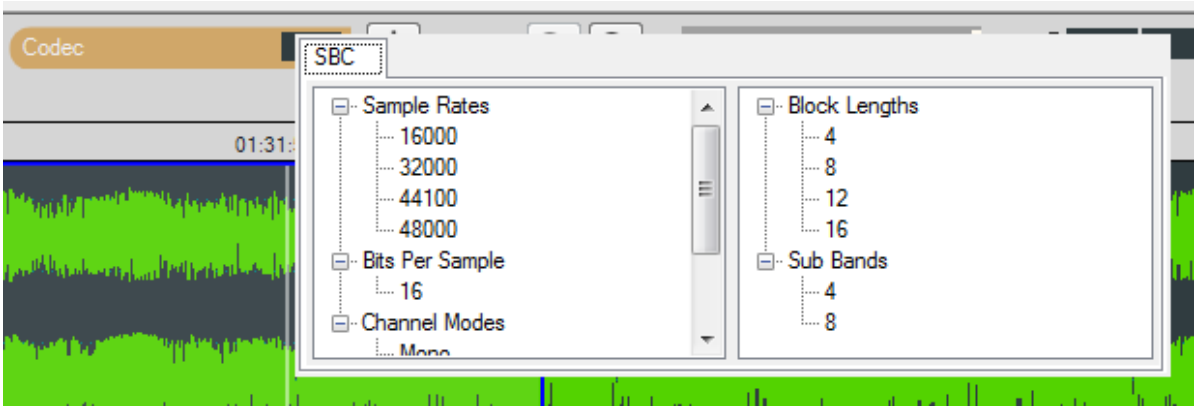


Figure 4.141 - SBC Codec Information Pop-Up on Cursor Hover Over

4.5.6.2.2 Local Controls

The Local Controls in each Wave Panel provide the user with indicators and controls for waveform display and audio play back.

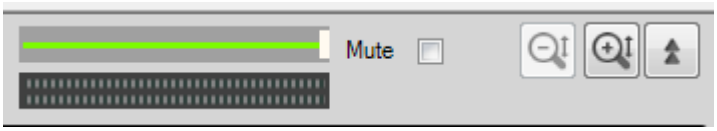


Figure 4.142 - Wave Panel Local Controls

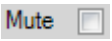
Waveform Play Back Volume

The volume slider controls the playback volume for the audio in each Wave Panel.

Audio Volume Indicator

The volume indicator shows the relative audio volume at the waveform display play cursor. When the green bars completely fill the indicator the audio volume is at its highest level. As the volume decreases, the bars will move to the right linearly, with no visible green bar indicating no audio. The volume indicator will continue to operate if the audio stream has been muted.

Mute



Checking the **Mute** check box will silence the Wave Panel's audio output. The volume indicator will respond to the audio volume but nothing will be heard. All panels can be simultaneously muted using the Audio Expert System™ Global Toolbar. The Wave Panel mute is a local control only. However, the Global Toolbar mute control will set the Stream Panel's Local Controls mute.

Vertical Zoom

Each Wave Panel contains local Vertical Zoom controls that expands or reduces the waveform display vertically. The waveform amplitude is always visible, and the Vertical Zoom controls increases or decreases the entire vertical size of the display. The vertical zoom buttons will turn gray and become inactive when the maximum and minimum values are reached.

Collapse/Expand Control

Collapse/Expand button toggles between two views. The top image indicates that the Wave Panel is expanded. When the bottom image is visible it indicates that the Wave Panel is collapsed.

When the top image is visible, clicking on it will collapse the Wave Panel to the minimum size that shows only the Stream Info and the Local Controls. When the bottom image is visible, clicking on it expands the Wave Panel to full size.

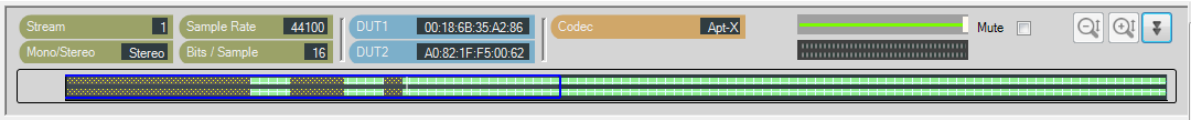


Figure 4.143 - Collapsed Wave Panel

4.5.6.2.3 Audio Waveform Panel

The Audio Waveform Panel displays the captured audio waveform. If the waveform is stereo, both channels are visible in the Wave Panel. The user can view the entire waveform or can zoom to view a portion of the waveform in more detail.

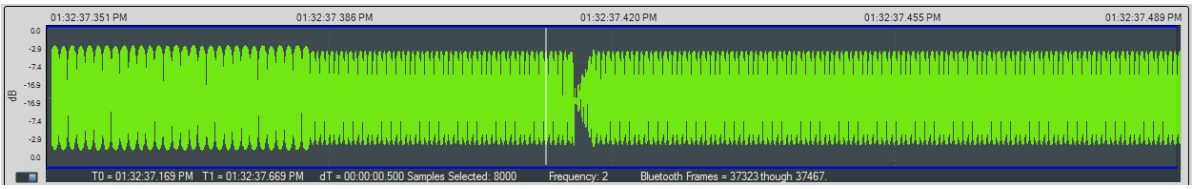
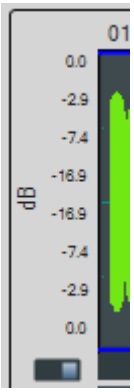


Figure 4.144 - Audio Waveform Panel in the Wave Panel

Table 4.37 - Global Toolbar Waveform Horizontal Zoom Controls

Control	Description
	Horizontal Zoom: Increases the amount of data that is visible on the screen; however, less detail is discernible.
	Horizontal Zoom: Decreases the amount of data that is visible on the screen; however, more detail is discernible.

Waveform



The audio waveform is plotted as amplitude versus time on the Wave Panel. The amplitude scale is located on the left edge of the Wave Panel. The waveform's amplitude can be linear or in decibels. The linear range is -1.0 to +1.0. The range for the dB scale is 0 dB for the maximum positive and maximum negative values, and silence is negative infinity. A toggle switch at the bottom of the amplitude scale will switch between **Linear** scale and **dB** scale. Moving the switch to the left will display the **Linear** scale and moving it to the right will display the **dB** scale.

Play Cursor

The Play Cursor is identified by a white vertical line on the Wave Panel. The Play Cursor appears when user clicks on any point in the waveform, or, if the cursor is already present it can be dragged to another position. To drag the Play Cursor, hover the mouse cursor over the Play Cursor until the mouse cursor changes to a pointing hand; click and drag the cursor to a new position.

Waveform Segment Selection

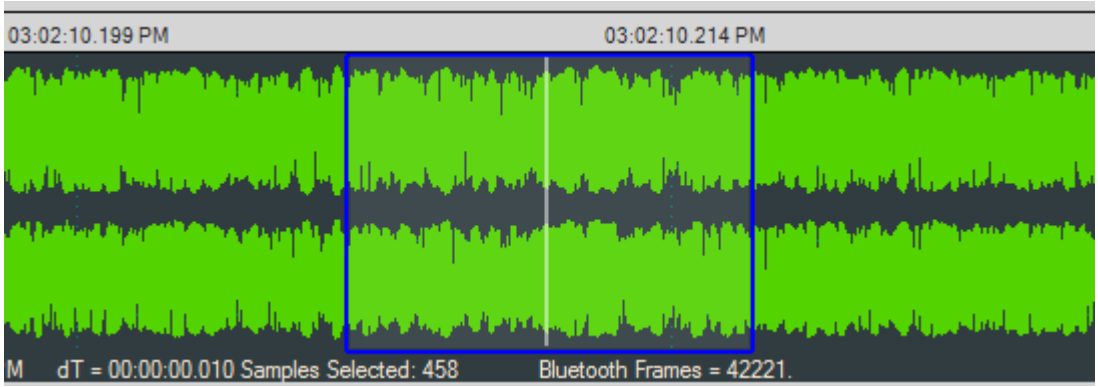


Figure 4.145 - Selection in the Audio Waveform

A waveform segment selection is identified by a blue border surrounding the selection. Procedures for selecting a segment depend on the desired actions.

Table 4.38 - Segment Selection Procedures

Desired Action	Procedure
Loop play back	1. Zoom in to the waveform segment of interest. 2. Click in the approximate center of the proposed selection. This will place the Play Cursor in the area to be selected. 3. Move the mouse cursor to the right or left of the Play Cursor, click and hold, then drag over the waveform segment of interest. Release the mouse key. The selection is surrounded by a blue border.
View waveform details	1. Zoom in to the segment of interest. 2. Move the mouse cursor to the right or left limit of the waveform segment of interest; click and hold, then drag over the waveform segment of interest. Release the mouse key. The selection is surrounded by a blue border.

For either of the procedures described in the table above, once the selection is made details of the segment appear below and to the left of the waveform. These details include selection start and stop range ("T0" and "T1"), the time difference ("dT"), samples selected, frequency, and "*Bluetooth* Frames" selected.

Right-clicking in the Waveform panel will open a pop up menu (see Wave Panel & Event Table Pop-up Menu on page 272. Selecting **Zoom to Selection** will expand the selection to the full width of the Wave Panel. Other selection option in the pop up are **Select Area**, **Clear Selection**, and **Copy Selection**.

Actual Bitrate Overlay Display

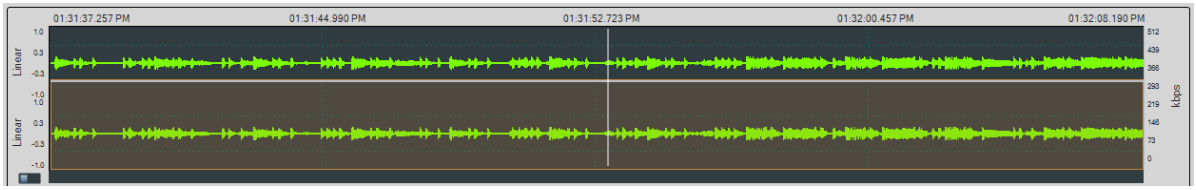


Figure 4.146 - Actual Bitrate Overlay

The Average and Actual audio stream bitrate graphs can be displayed over the audio waveform using the Global Toolbar Average Bitrate Overlay and Actual Bitrate Overlay buttons respectively. These are presented as overlays onto the main Wave Panel so the user can correlate audio issues with bitrate changes and the like. The scale is in kbps (kilo bits per second). Hovering over the bitrate scale will display a pop-up showing the bitrate at the play cursor position.

Actual Bitrate is based on the throughput at the Codec level.

The Average Bitrate is the moving average over 0.1 sliding-second window.

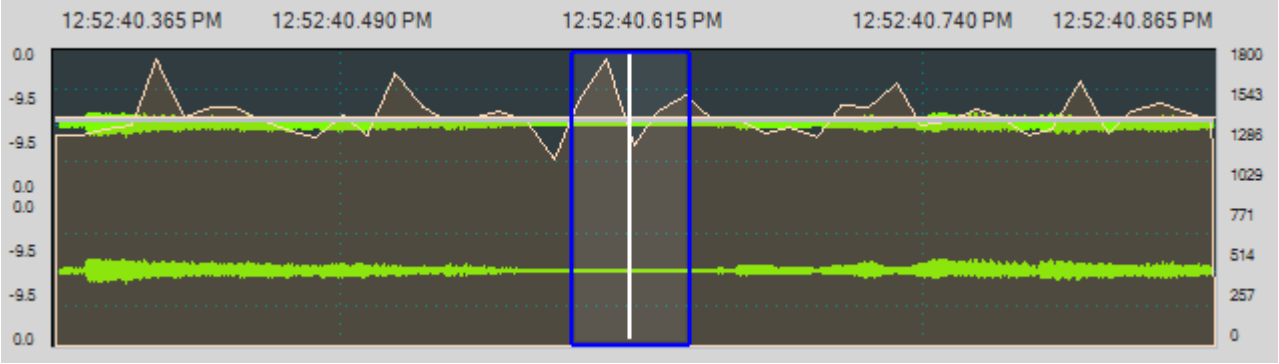


Figure 4.147 - Average Bitrate Overlay

All of the information for calculating the Acutal and Average Bitrate is in the codec data frame header.

4.5.6.2.4 Event Timeline

The Event Timeline in the Wave Panel shows the *Bluetooth* , Codec , and Audio events related to the waveform being viewed. The events are synchronized in time to the waveform displayed in the Wave Panel. The event severity is displayed as Information , Warning , and Error .

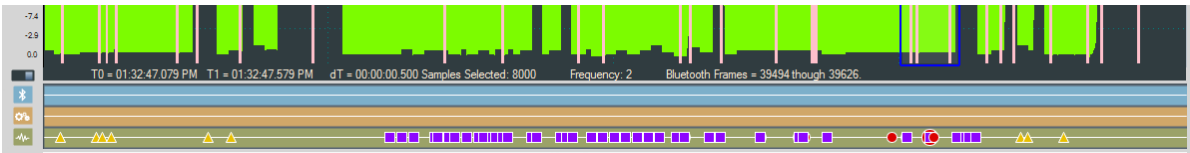


Figure 4.148 - Event Timeline Shown with Wave Panel

Clicking on an event in the Event Timeline shows a relevant selection in the Audio Waveform Panel. The size of the selection depends on the number of frames associated with the selected event. This selection will appear in all Wave Panels; however, the event severity icon will only appear in the Wave Panel associated with the event.

To assist the user with viewing events in detail, the Event Timeline will zoom in and out in sync with the Wave Panel.

Event Timeline Example

This example shows that event 159 was selected in the Event Table resulting in the severity icon being enlarged in the Event Timeline. The system automatically selected the surrounding area—the blue outline.

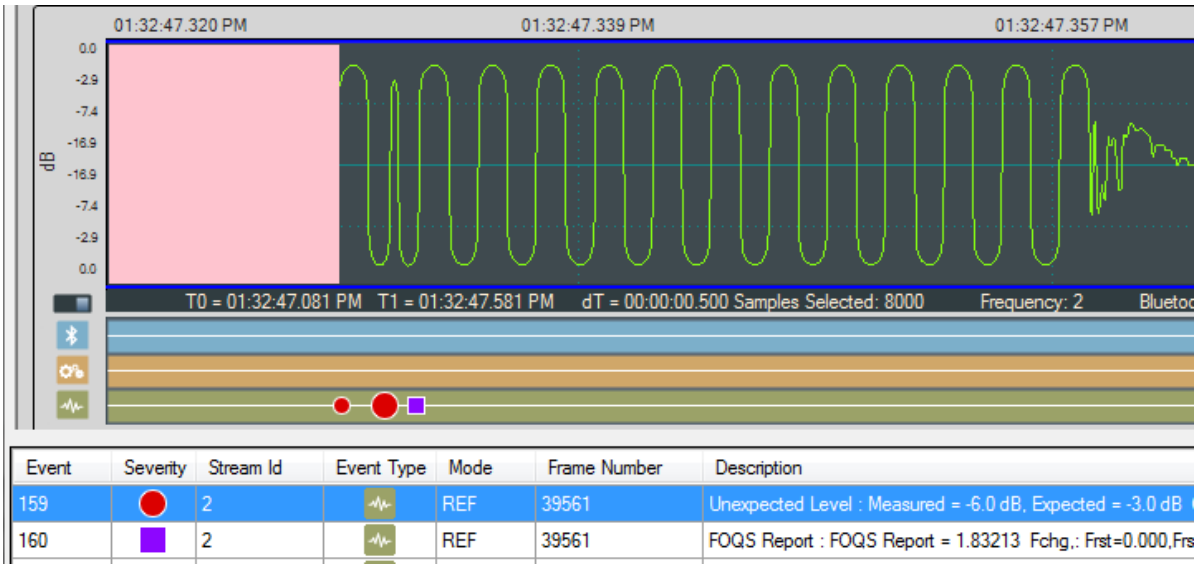


Figure 4.149 - Example: Event Table Selection Shown in Event Timeline

Event Pop Up

When the cursor hovers over a selected event severity icon in the Event Timeline, a pop-up will display the event class, severity, and associated *Bluetooth* frame.

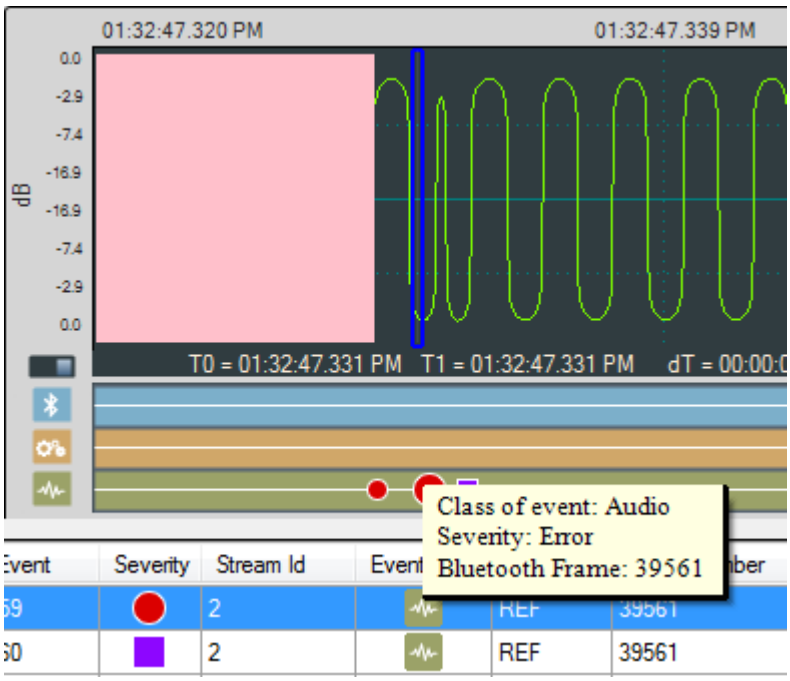


Figure 4.150 - Event Timeline Selected Event Pop Up

4.5.6.3 Event Table

The Event Table lists all audio stream events . Clicking on an event will select that event in the Event Timeline in the Wave Panel. If the selected event is outside the visible area of the waveform, the waveform will move and bring the selected event to the center of the display. The event icon in the Event Timeline is also centered and the selected icon will be larger than the non-selected event icons. Selecting one or more events in the table will highlight the associated frames in the standard Frontkline software windows, such as **Frame Display**, **Coexistence View**, **Bluetooth Timeline**, etc. .

Lock Event Table

Event	Severity	Stream Id	Event Type	Mode	Frame Number	Description	Timestamp
17	▲	1		N/A	3039	Packet retransmission.	Mar-31-2014 12:52:38.080991 PM
18	■	1		N/A	4094	A2DP paused between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:52:45.553569 PM
19	■	1		N/A	4095	A2DP paused between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:52:45.617944 PM
20	▲	0		N/A	4101	SCO connection request.	Mar-31-2014 12:52:46.151071 PM
21	■	2		N/A	4105	SCO connection established between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 2 using cod...	Mar-31-2014 12:52:46.504191 PM
22	■	3		N/A	4105	SCO connection established between devices 00:07:62:0F:00:00 and 98:0D:2E:23:B6:2E for stream: 3 using cod...	Mar-31-2014 12:52:46.504191 PM
23	■	2		N/A	4108	Codec: CVSD Frequency: 64000, Bits Per Sample: 16, Channels: 1	Mar-31-2014 12:52:46.806067 PM
24	■	3		N/A	4256	Codec: CVSD Frequency: 64000, Bits Per Sample: 16, Channels: 1	Mar-31-2014 12:52:47.357946 PM
25	■	2		N/A	13222	SCO disconnected between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 2 using codec: CVSD	Mar-31-2014 12:53:04.151789 PM
26	■	3		N/A	13222	SCO disconnected between devices 00:07:62:0F:00:00 and 98:0D:2E:23:B6:2E for stream: 3 using codec: CVSD	Mar-31-2014 12:53:04.151789 PM
27	■	1		N/A	13253	A2DP resumed between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:53:05.446738 PM
28	■	1		N/A	13254	A2DP resumed between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:53:05.474864 PM
29	▲	0		N/A	13479	Packet retransmission for unknown CID.	Mar-31-2014 12:53:07.712976 PM
30	▲	1		N/A	14187	AVDTP packet loss detected based on missing packet sequence number.	Mar-31-2014 12:53:13.742943 PM
31	▲	1		N/A	14351	AVDTP packet loss detected based on missing packet sequence number.	Mar-31-2014 12:53:15.385434 PM

Figure 4.151 - Event Table

Several events can be selected by clicking and dragging over the events, or by holding down the Shift key and clicking on events. To select events that are not adjacent hold down the Ctrl key and click on the events.

When selecting multiple events, the Wave Panels will not scroll to the selected events.

The Event Table contains eight columns.

Table 4.39 - Event Table Columns

Name	Value	Description
Event	integer	System generated sequential numbering of events.
Severity	■	**Information** - provides information of interest but does not indicate a problem event.
	▲	**Warning** -identifies a potential problem where further investigation may be appropriate
	●	**Error** - identifies a definite problem.
Stream Id	integer	A system generated ID that is assigned in the order that the audio streams are detected. The ID is not maintained between captures for the same device with the same audio. It identifies the Wave Panel where the event can be viewed. The ID appears in the Audio Stream Info of the Wave Panel.
Event Type		*Bluetooth* -Events generated by analyzing Bluetooth protocol activities.
		Codec -Events generated from analyzing the audio coding/decoding activities.
		Audio -Events generated by analyzing the audio data.

Table 4.39 - Event Table Columns (continued)

Name	Value	Description
Mode	N/A	Mode does not apply to this event.
	REF	Referenced Mode. Refer to 4.5.4.2 Referenced Mode on page 245 .
	UN-REF	Non-Referenced Mode. Refer to 4.5.4.1 Non-Referenced Mode on page 244 .
Frame Number	integer	The system generated identification for a specific frame.
Description		Details and explanation about this event.
Timestamp	clock date and time	A system generated time stamp for each frame.

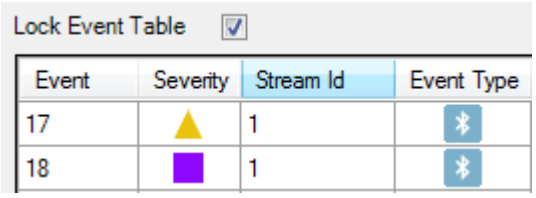
Sorting

Event table entries are sortable by column. Left-click on the column heading to sort.

Event Table Pop-Up Menu

Right-clicking with the cursor over the Event Table will open a menu of additional options. For more on this option see Wave Panel & Event Table Pop-up Menu on page 272.

Lock Event Table

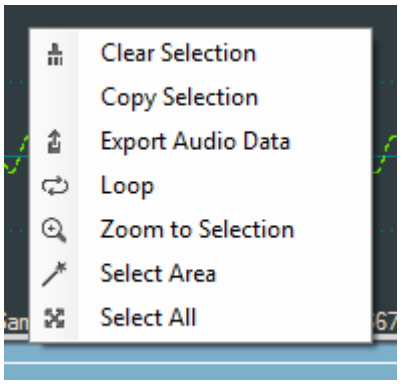


The **Lock Event Table** checkbox is available in live mode only. Clicking to check the box will prevent the Event Table from scrolling during live capture. Un-checking the box will resume scrolling of events as they are detected. When analyzing a capture file the checkbox has no effect.

4.5.6.4 Wave Panel & Event Table Pop-up Menu

Additional Wave Panel and Event Table options are available by right clicking the mouse with the cursor anywhere in the Wave Panel or in the Event Table.

Wave Panel Pop-up Menu Actions

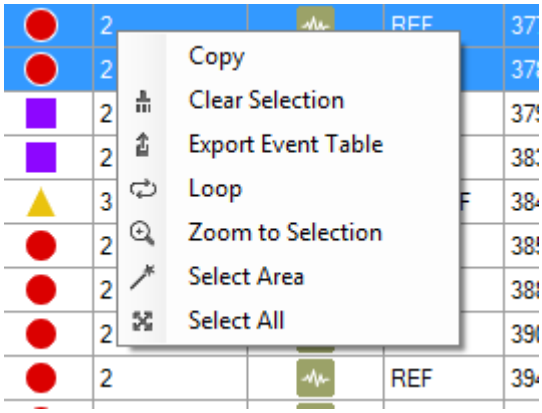


Right-clicking anywhere in the Wave Panel will provide you with a selection of the following actions.

Table 4.40 - Wave Panel Pop-up Menu Selections

Option	Description
Clear Selection	Clears the current selection in the viewer
Copy Selection	Saves a copy of the selection to the computer clipboard. The clipboard can be pasted into a Word document, an e-mail, or other Windows clipboard-compatible application.
Export Audio Data	Opens the Export pop-up menu with options to export the waveform as a .raw, .wav, or Event Data. For additional details on exporting refer to Waveform Display Export.
Loop	Loops through the audio selected on the Wave Panel.
Zoom to Selection	Expands or compresses the selection to fill the Wave Panel view.
Select Area	When the mouse cursor is positioned over data (not fill, pause, or gaps) in the Wave Panel and selecting this option will select all the data between and fills, pauses, or gaps.
Select All	Selects the entire waveform

Event Table Pop-up Menu Actions



Right-clicking in the Event Table will provide you with a selection of the following actions.

Table 4.41 - Event Table Pop-up Menu Selectioin

Options	Description
Copy	Copies the selected events to Windows clipboard as text.
Clear Selection	Clears the current event selection in the table
Export Event Table	Copies the current event selection and saves it as a .csv file. For additional details on exporting refer to Event Table Export.
Loop	Loops through the audio selected on the Wave Panel.

Table 4.41 - Event Table Pop-up Menu Selectioin(continued)

Options	Description
Zoom to Selection	Expands the Event Table selection to fill the Wave Panel view.
Select Area	Expands the selection.
Select All	Selects all events.

4.5.6.5 Export Audio Data

There are two ways to export audio data:

1. Clicking the Audio Expert System™ window **Global Toolbar** Export button .
2. Right-click in a Stream Panel Wave Panel and a pop-up menu will appear. Select **Export** .

Two windows will appear:

1. The standard Windows Save As.
2. The **Export Audio Data** dialog.

In the Windows Save As window enter a **File name** and directory location. Click on **Save**.

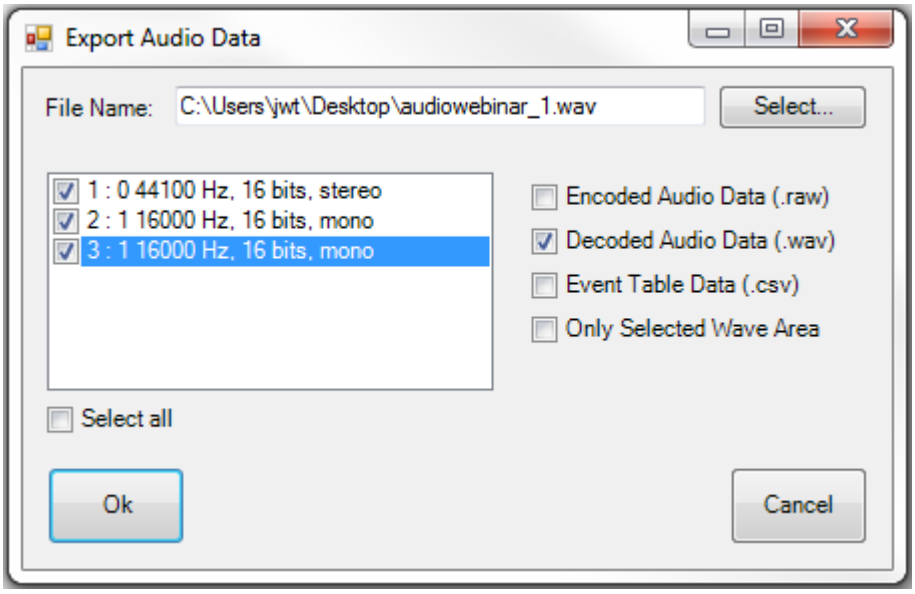


Figure 4.152 - Export Audio Data dialog

The Save As window will close, and the file name will appear in the **File Name** field in the **Export Audio Data** window. Should the file name need to be changed, click on the **Select** button and the Windows Save As dialog will open. By default the .wav file extension is used in the file name.

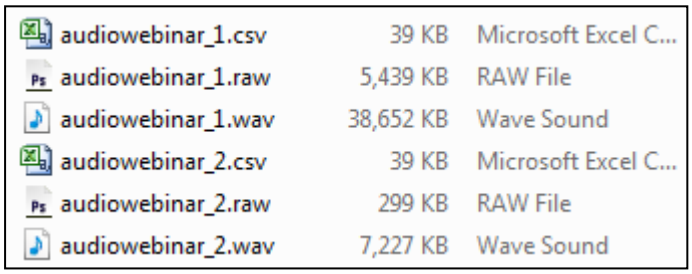
In the window below **File Name** will appear a list of **Stream Id**s with a description from the Audio Stream Info . If opening from the Audio Expert System™ **Global Toolbar** all **Stream ID**s are checked by default. If opening from a Wave Panel, the **Stream ID** where the export dialog was opened is automatically checked. You can check each stream that is to be exported. For convenience checking **Select all** below the stream list window will place checks in all streams.

Export Options

After selecting the streams to export, select the desired formats to export.

Table 4.42 - Export Audio Data Format Options

Option	Description
Encoded Audio Data	Exports the selected files as .raw format. The audio data is in an encrypted format and user will need a codec to decode it.
Decoded Audio Data	Exports the selected files as .wav format that can be played on a wide variety of media players.
Event Table Data	Exports a text .csv file of all the detected events
Only Selected Wave Area	Exports the Encoded, Decoded, or Event Data for the selected waveform. This option is only active if a selection has been made in one of the Wave Panels



Click on **OK** to save the waveform. The dialog will close and a series of progress bars will appear. Each progress bar is associated with a file for each export option. The exported files will have the following syntax: *<filename>_n.<filetype>*, where *<filename>* = the name entered into the File Name field, *n* = the stream id number (1, 2, 3, ...), and *<filetype>* = "raw", "wav", and "csv'. The image shows an example where the user exported **Stream Id**'s 1 and 2 in Encoded Audio , Decoded Audio , and Event Table data to filename "audiowebinar".

Click on **Cancel** to close the window without exporting.

4.5.6.6 Export Event Table

Right-clicking in the Event table will open a pop-up menu with the option to **Export Event Table**. This option will export selected events in the in comma separated variable (.csv) format for used in Microsoft Excel or any other Windows .csv compatible application.

First select the events to export. Multiple events are selectable by selecting an event then holding the Shift key while clicking on another event. This will select all events between the two selections. If the selections are not adjacent you can hold the Ctrl (control) key while clicking events.

Next right-click anywhere int he Event Table to open the pop-up menu and click on the **Export Event Table** option. A Windows **Save As** dialog will open. Enter a file name and select a file location and click on **Save**. A confirmation dialog will open. Click **OK** to close the confirmation dialog.

If you have not selected an event in the table before exporting, a warning to "Please select an event row first." appears.

4.5.7 Frame, Packet, and Protocol Analysis Synchronization

The Audio Expert System™ module integrates seamlessly with Frontline software with common timestamping of *Bluetooth* protocol data, audio events, audio waveform display, and codec events. The audio expert data and results are synchronized and coordinated with the existing Frontline software data views, such as **Frame**

Display, **Bluetooth Timeline**, etc. to expedite the root-cause analysis of *Bluetooth* protocol related audio issues. When a frame is selected in any Frontline software data views, the corresponding audio data associated with those frames is also selected in the Wave Panel, Event Timeline and Event Table and vice-verse.

Protocol analysis tools synchronized to the Audio Expert System™ include:

- **Frame Display**
- **Coexistence View**
- **Bluetooth Timeline**
- **Message Sequence Chart**
- **Packet Error Rate Statistics**

When a portion of the waveform is selected in the Wave Panel, all frames within the selection will be highlighted in the **Frame Display**, **Coexistence View**, and **Bluetooth Timeline**.

> **Note:** If the **Frame Display** is filtered to show non-audio events then the frames associated with selected audio events may not show.

4.6 Bluetooth Protocol Expert System

The *Bluetooth* Protocol Expert System is used to debug protocol-related events for *Bluetooth* protocols. The expert system provides the ability to interactively select protocol events from a table of events in live capture mode or in analyzing a previously captured file. Selecting an event will dynamically link the related packet selection to the ComProbe software **Frame Display**, **Coexistence View**, **Message Sequence Chart**, **Bluetooth Timeline**, and **Packet Error Rate Statistics** (**PER Stats**).

Protocol error events appearing in the **Protocol Events** pane identify the related *Bluetooth* specification reference that is likely to point to a solution to the error. The expert system references *Bluetooth* specification 5.0 and the following protocols for both Classic *Bluetooth* and *Bluetooth* low energy.

- L2CAP
- A2DP
- SDP
- SMP
- ATT

4.6.1 Starting the *Bluetooth* Protocol Expert System

To use the *Bluetooth* Protocol Expert System the user must have

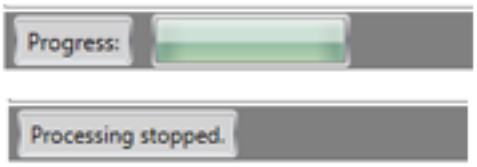
- Current Premium Maintenance
- Set in Target hardware with *Bluetooth* Protocol Expert System license installed and connected to the PC. This is a requirement for both live capture and when viewing a saved capture file.

For live capture, set up the Set in Target device datasource and begin capturing data.

For viewing a capture file, load the saved file from the **Control** window **File** menu.

> **Note:** To use the *Bluetooth* Protocol Expert System with a capture file, Set in Target hardware with *Bluetooth* Protocol Expert System license installed must be connected to the PC.

Bluetooth Protocol Expert System Window is opened by clicking on on the **Control** window toolbar. If the Set in Target hardware is not licensed for *Bluetooth* Protocol Expert System, a tooltip will appear with "Bluetooth Protocol Expert System is not licensed. Please contact sales@fte.com." Click on the or select **Bluetooth Protocol Expert** from the **View** menu. The *Bluetooth* Protocol Expert System window will open.



When the protocol analyzer begins analysis of the captured data, the **Bluetooth Protocol Expert System** window status bar (bottom of the window) will show **Progress** with a progress bar. The expert system will search and evaluate for protocol events for warnings and errors. When the expert system has completed, the status bar will show **Processing stopped**. If no protocol warnings or errors are detected, the window will remain empty of data.

For instructions on using the expert system Toolbox with the Frontline Sodera, see Bluetooth Protocol Expert System on page 1.

4.6.2 *Bluetooth* Protocol Expert System Window

This window is the working space for the *Bluetooth* Protocol Expert System. Upon opening *Bluetooth* Protocol Expert System by clicking on the **Control** window button, the window shown below will open with four main areas displayed described in the table below. Detailed explanations of each window section follow.

Table 4.43 - *Bluetooth* Protocol Expert System Window Panes

Section	Description
Connections	Displays the *Bluetooth* master and slave device connections with associated link layer logic transport type.
Statistics	Displays the protocol statistics associated with the warning or error selected in the **Protocol Events** pane, or associated with the selected *Bluetooth* address and protocols selected in **Connections** pane. Tabbed sections contain the statistics for the protocols associated with the analyzed data. Statistics will vary depending on the protocol.
Protocol Events	Displays the *Bluetooth* protocol warnings and errors. Clicking on an event will select the associated protocol tab in the Statistics pane.
Test Tools	Used for testing audio when using the *Bluetooth* USB adapter on the HCI USB ports. See Bluetooth Protocol Expert System on page 1.

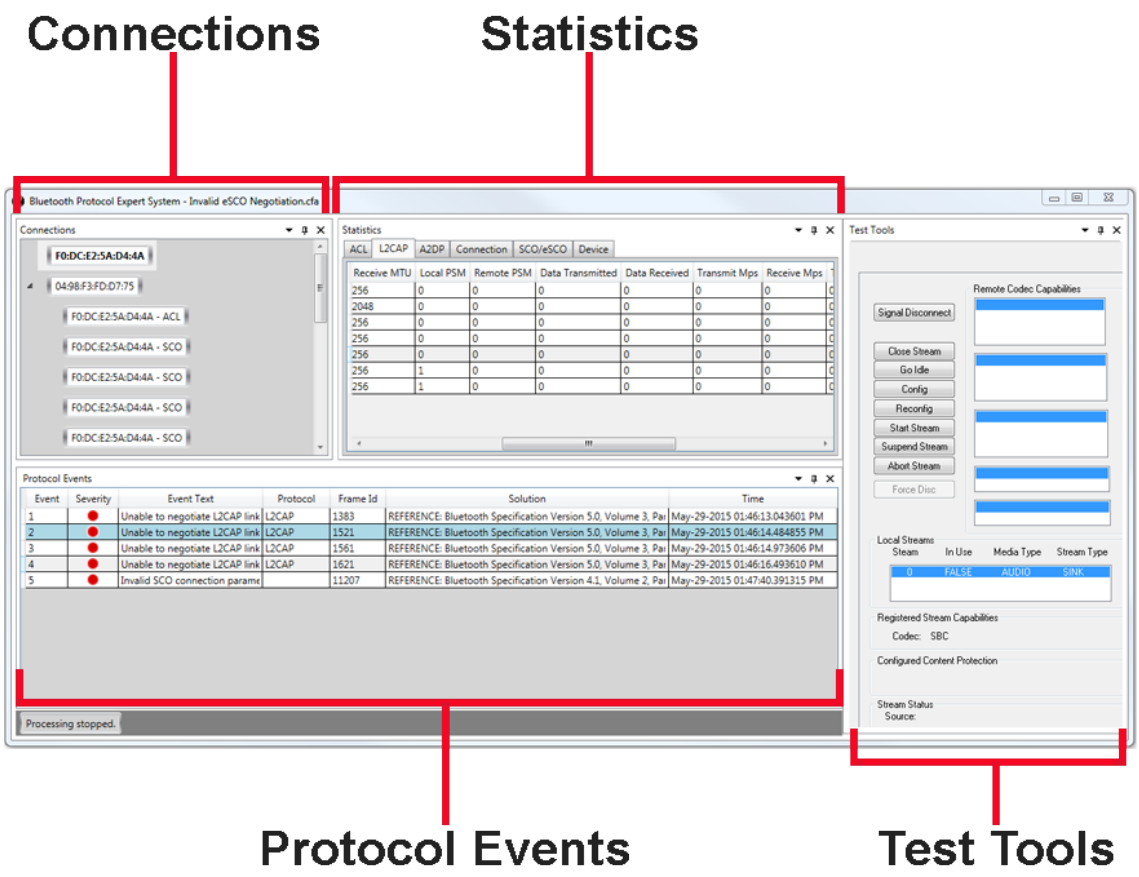


Figure 4.153 - *Bluetooth* Protocol Expert System Window

4.6.2.1 Expert System Connections Pane

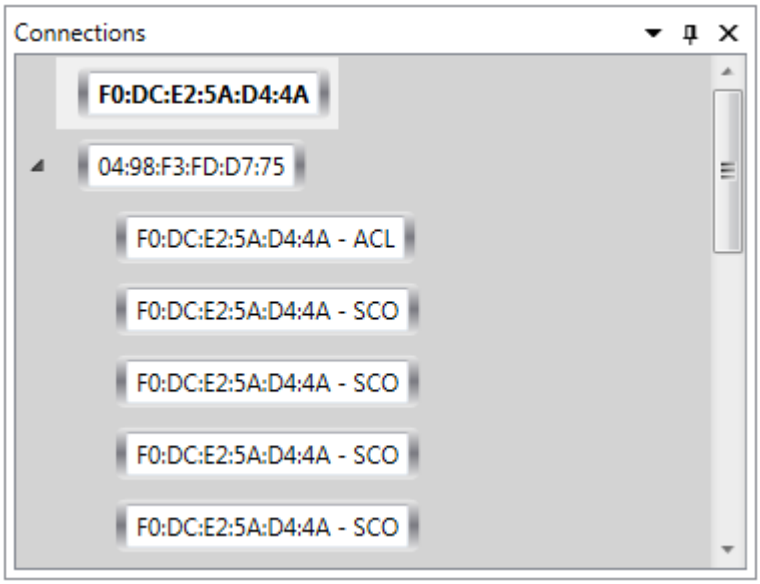


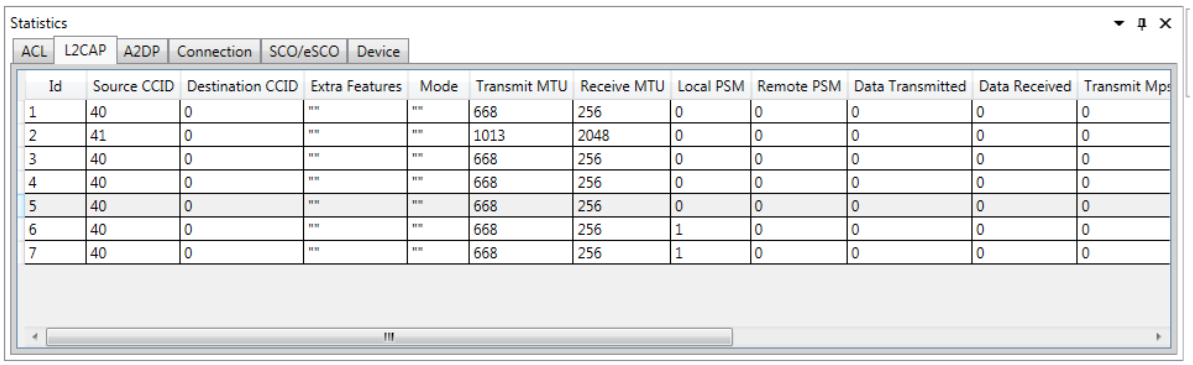
Figure 4.154 - Bluetooth Protocol Expert System **Connections** Pane

The **Connections** pane provides a chart of all the connected devices from the current live recording session or from a loaded capture file that have a protocol error or warning appearing in the **Protocol Events** pane.

Devices are identified by their BD_ADDR. A device address with an arrow symbol will expand to show the connected device and the link layer logical transport type.

4.6.2.2 Expert System Statistics Pane

The Statistics pane contains detailed information about the links, protocols, and connections associated with frames or range of frames and devices of detected events. The tabs across the top list the links, protocols, or connections. Details are contained with the



Id	Source CCID	Destination CCID	Extra Features	Mode	Transmit MTU	Receive MTU	Local PSM	Remote PSM	Data Transmitted	Data Received	Transmit Mps
1	40	0	""	""	668	256	0	0	0	0	0
2	41	0	""	""	1013	2048	0	0	0	0	0
3	40	0	""	""	668	256	0	0	0	0	0
4	40	0	""	""	668	256	0	0	0	0	0
5	40	0	""	""	668	256	0	0	0	0	0
6	40	0	""	""	668	256	1	0	0	0	0
7	40	0	""	""	668	256	1	0	0	0	0

Figure 4.155 - Bluetooth Protocol Expert System **Statistics** Pane

Table 4.44 - Bluetooth Protocol Expert System Statistics Pane

Tab	Tab Description	Column	Column Description
ACL	An asynchronous (packet switched) connection between devices created on LMP level.	**ID**	System assigned identifier for ACL connections.
		Device A	Contains the BD_Addr of a device in the connection.
		Device B	Contains the BD_Addr of a device in the connection.
		AddrType	BR_EDR or LE
		Handle	
		Active	
		Errors	

Table 4.44 - Bluetooth Protocol Expert System Statistics Pane (Continued)

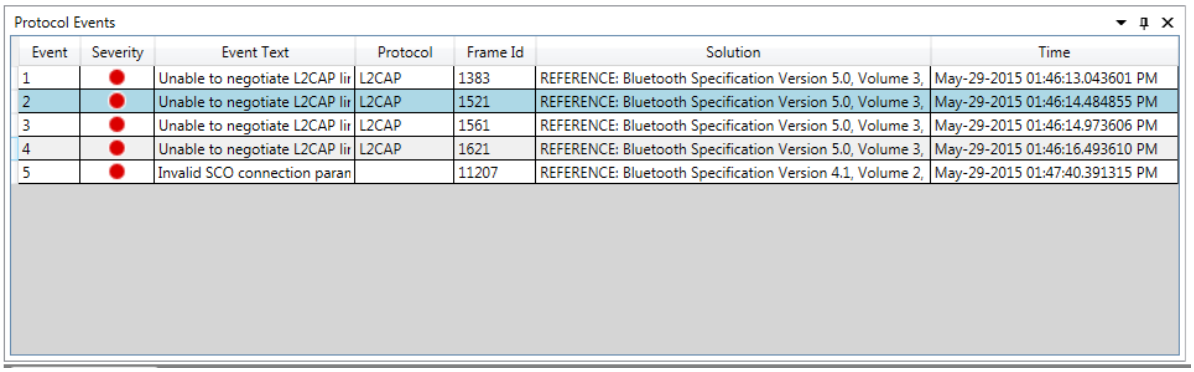
Tab	Tab Description	Column	Column Description
L2CAP	L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions.	**ID**	System assigned identifier for ACL connections
		Source CID	Channel Identifier for the source device.
		Destination CID	Channel Identifier for the destination device.
		Extra Features	
		Mode	
		Transmit MTU	Maximum Transmission Unit in bytes during transmission.
		Receive MTU	Maximum Transmission Unit in bytes during receive.
		Local PSM	Local device Protocol and Service Multiplexer.
		Remote PSM	Remote device Protocol and Service Multiplexer.
		Data Transmitted	
		Data Received	
		Transmit Mps	
		Receive Mps	
		Transmit Window	
		Receive Window	
		Number of Retransmissions	
		Active	
		Error Count	Number of errors associated with this **L2CAP Id**.
A2DP			
Connection	Provides a cross-reference among the **Statistics** tab **Id**, the **Frame Display** frame range, and the **Connection Type**.	**Id**	System assigned identification
		Connection Type	The protocol type
		Parent Id	????????
		Statistics Id	The system assigned Id that appears in the **Statistics Connection Type** tab.

Table 4.44 - Bluetooth Protocol Expert System Statistics Pane (Continued)

Tab	Tab Description	Column	Column Description
SCO/eSCO	Synchronous Connection-oriented (SCO)/extended SCO.	**Id**	System assigned identification.
		Type	SCO or eSCO
		Air Mode	Part of the *voice_settings* parameter in the air mode negotiations designed to improve or optimize audio quality during transmissions. SCO: CVSD, A-law, µ-law. eSCO: CVSD, A-law, µ-law, transparent.
		Handle	
		Active	
		Error Count	
Device	This tab serves the purpose of assigning a unique expert system identification to the devices listed in the **Connections** pane.	**Id**	System assigned identification.
		Address	BD_ADDR of a device found in the **Connections** pane.

Any column in the Protocol Events list can be sorted in ascending or descending order. Refer to Expert System Table Sorting on page 283 for sorting instructions.

4.6.2.3 Expert System Protocol Events Pane



Bluetooth protocol events that generate a warning or an error in the expert system are listed in the **Protocol Events** pane. Events are listed in the order that they occur.

Table 4.45 - Protocol Events Pane Fields

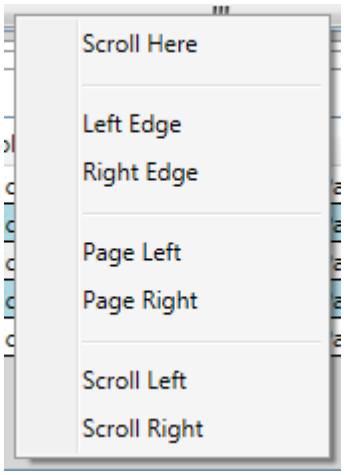
Row Field	Description
Event	System assigned event number. Events are numbered in the order that they appear.
Severity	▲ = Warning. The event has not created a failure, but should receive some attention and further investigation.. ● = Error. The event has identified a situation that does not conform to the *Bluetooth* specification. Corrective action is required.

Table 4.45 - Protocol Events Pane Fields (Continued)

Row Field	Description
Event Text	Event description.
Protocol	Protocol in which the event occurred.
Frame Id	Frame where the event occurred. Clicking in the event row will select the related **Statistics** pane protocol tab and protocol **Id**. The corresponding frame is selected in the **Frame Display**, **Event Display**, **Message Sequence Chart**, **Coexistence View**, and ***Bluetooth* Timeline** or ***Bluetooth* low energy Timeline**.
Solution	A solution to the event is provided by reference to the Bluetooth specification that applies to the Event Text content.
Time	Event timestamp.

Any column in the Protocol Events list can be sorted in ascending or descending order. Refer to Expert System Table Sorting on page 283 for sorting instructions.

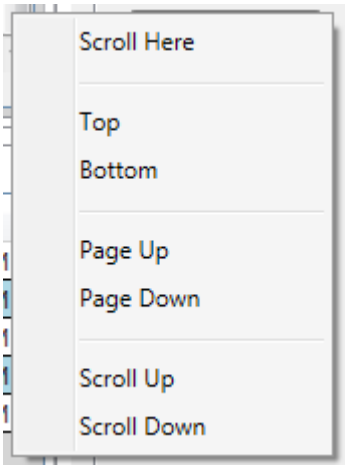
4.6.2.4 Expert System Window Scroll Bar Navigation



Some tabs in the Statistics pane display a horizontal scroll bar that can be clicked and dragged to view the tab columns. An alternative scroll navigation is to right-click the mouse cursor on the scroll bar. A navigation menu will appear, and you click on the direction and amount of scrolling to move the horizontal scroll bar in discrete steps.

Table 4.46 - Horizontal Scroll Bar Navigation Sections

Selection	Description
Scroll Here	Scrolls to the point on the scroll pane where the mouse was last positioned.
Left/Right Edge	Scrolls the table to the beginning (left edge) or to the end (right edge)
Page Left/Right	Left: Moves the current right edge to the left edge of the current view range. Right: Moves the current left edge to the right edge of the current view range.
Scroll Left/Right	Moves the table is small increment to the left or right. Same action as the left/right scroll arrows at the ends of the scroll bar.



Some tabs in the Statistics pane display a vertical scroll bar that can be clicked and dragged to view the tab columns. An alternative scroll navigation is to right-click the mouse cursor on the vertical scroll bar. A navigation menu will appear, and you click on the direction and amount of scrolling to move the scroll bar vertically in discrete steps.

Table 4.47 - Vertical Scroll Bar Navigation Sections

Selection	Description
Scroll Here	Scrolls to the point on the scroll pane where the mouse was last positioned.
Top/Botton	Scrolls the table to thefirst row (top) or to the last row (bottom)
Page Up/Down	Up: moves the current view bottom row to the top row of the current view range. Down: Moves the current view top row to the bottom row of the current view range.
Scroll Up/Down	Moves the table one row up or down.

4.6.2.5 Expert System Table Sorting

Tables in the Bluetooth Protocol Expert System can be sorted in ascending or descending order. This process includes tables in the **Statistics** pane and the **Protocol Events** pane.

1. In any table click in the header for the column you want to sort. The column header will turn blue and an arrow head will appear.
2. If the arrow head is pointing up, the column is sorted in ascending order. If the arrow head is pointing down the column is sorted in descending order.
3. To change the direction of the sort, click in the column header to change the arrow head direction accordingly.

All other columns in the table are sorted relative to the selected column sort. Refer to the following Statistics pane images for an example.

Statistics

ACL | L2CAP | A2DP | Connection | SCO/eSCO | Device

Id	Type	Air Mode	Handle	Active	Error Count
1	eSCO	Transparent	1	False	0
2	SCO	CVSD	1	False	0
3	eSCO	Transparent	1	False	0
4	SCO	CVSD	1	False	0

Figure 4.156 - Sorting **Id** Ascending

Statistics

ACL | L2CAP | A2DP | Connection | SCO/eSCO | Device

Id	Type	Air Mode	Handle	Active	Error Count
4	SCO	CVSD	1	False	0
2	SCO	CVSD	1	False	0
1	eSCO	Transparent	1	False	0
3	eSCO	Transparent	1	False	0

Figure 4.157 - Sorting **Air Mode** Ascending; Note **Id** Sort

Statistics

ACL | L2CAP | A2DP | Connection | SCO/eSCO | Device

Id	Type	Air Mode	Handle	Active	Error Count
3	eSCO	Transparent	1	False	0
1	eSCO	Transparent	1	False	0
4	SCO	CVSD	1	False	0
2	SCO	CVSD	1	False	0

Figure 4.158 - Sorting **Air Mode** Descending; Note how other columns follow.

4.7 Analyzing Byte Level Data

4.7.1 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.

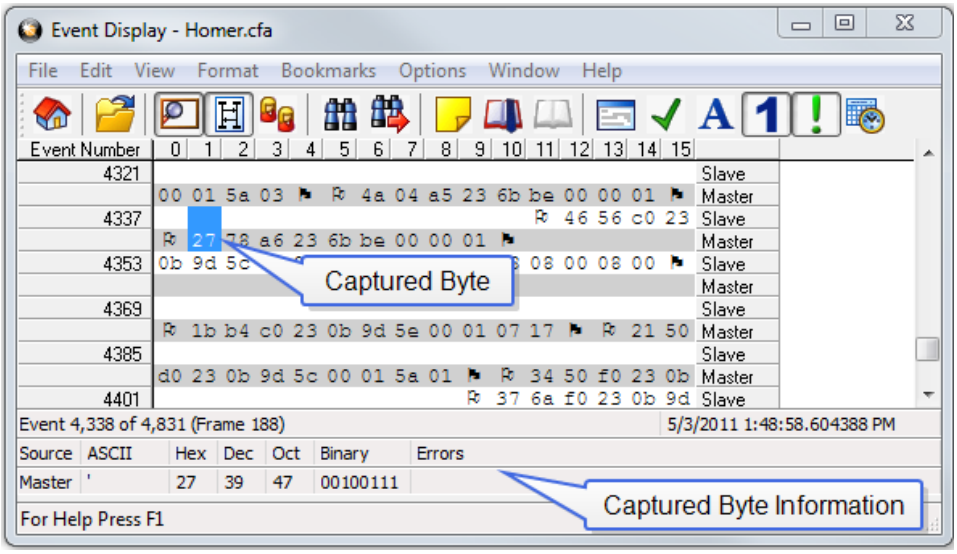


Figure 4.159 - Event Display

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**.

4.7.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Open a capture file

Start Analyze- Begins data analysis..

Stop Analyze- Stops the analysis and clears the data from the ComProbe analyzer.


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.

4.7.3 Opening Multiple Event Display Windows

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

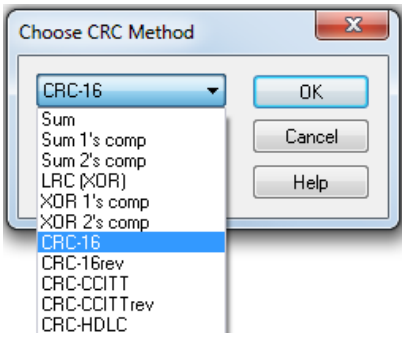
You can open as many **Event Display** windows as you like. Each **Event Display** is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

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.

4.7.4 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..
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 is calculated automatically.



Calculating CRC for interwoven data

4.7.5 Calculating Delta Times and Data Rates

1. Click on the E**vent 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.

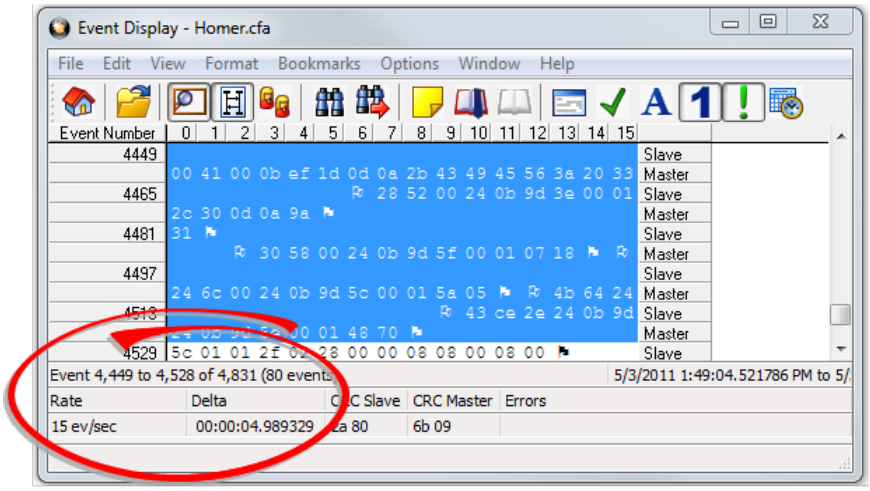


Figure 4.160 - Delta fields

4.7.6 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.

4.7.7 Data Formats and Symbols

4.7.7.1 Switching Between Viewing All Events and Viewing Data Events

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

- 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 on page 290 for a list of all the special events shown in the analyzer and what they mean.

[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.

4.7.7.2 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.

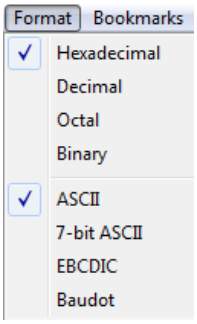


Figure 4.161 - Format Menu

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

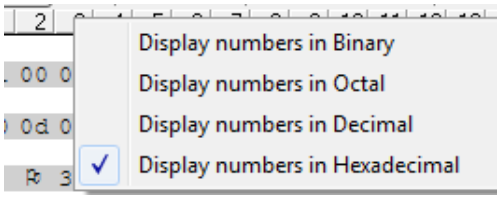


Figure 4.162 - Header labels, right click

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

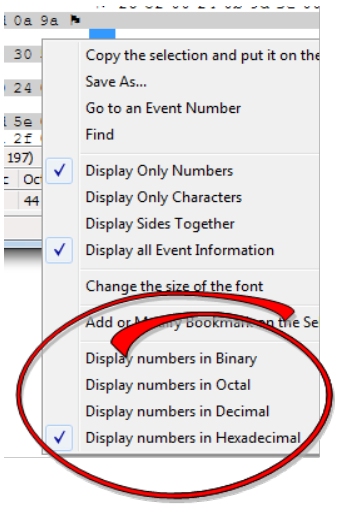


Figure 4.163 - Data display right click menu

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

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

4.7.7.3 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.

4.7.7.4 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.

4.7.7.5 List of all Event Symbols

By default, the **Event Display** shows all events**events**[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):

Table 4.48 - Event Symbols

Symbol	Event
⊗	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.

[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.

Table 4.48 - Event Symbols (continued)

Symbol	Event
	Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.
	Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.
	Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
	Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
	Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.
	End of Frame - Marks the end of a frame.
	Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.
	Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
	Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.
	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.

Table 4.48 - Event Symbols (continued)

Symbol	Event
✚	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

4.7.7.6 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**.

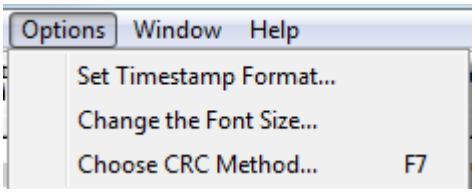


Figure 4.164 - Event Display Options menu

2. Choose a font size from the list.

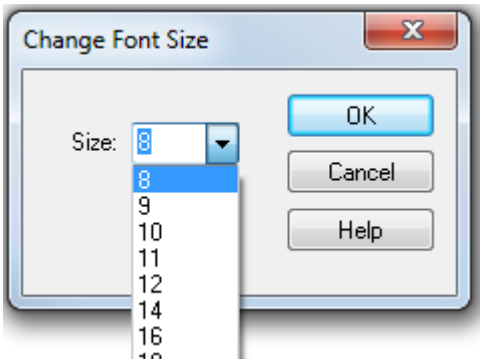


Figure 4.165 - Event Display Font Size Selection

3. Click **OK**.

4.8 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  .

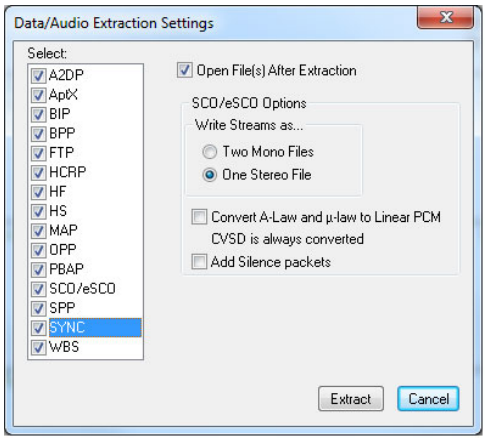


Figure 4.166 - Data/Audio Extraction Settings dialog

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.

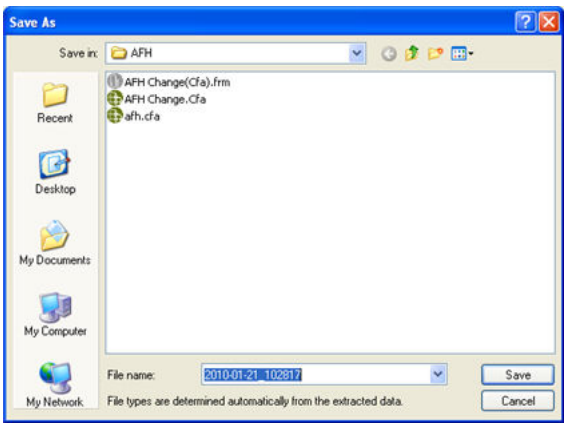
6. Select the **Add Silence packets** to insert the silence packets (dummy packets) for the reserved empty slots into the extracted file. If this option is not selected, the audio packets are extracted without inserting the silence packets for the reserved empty slots.

   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.

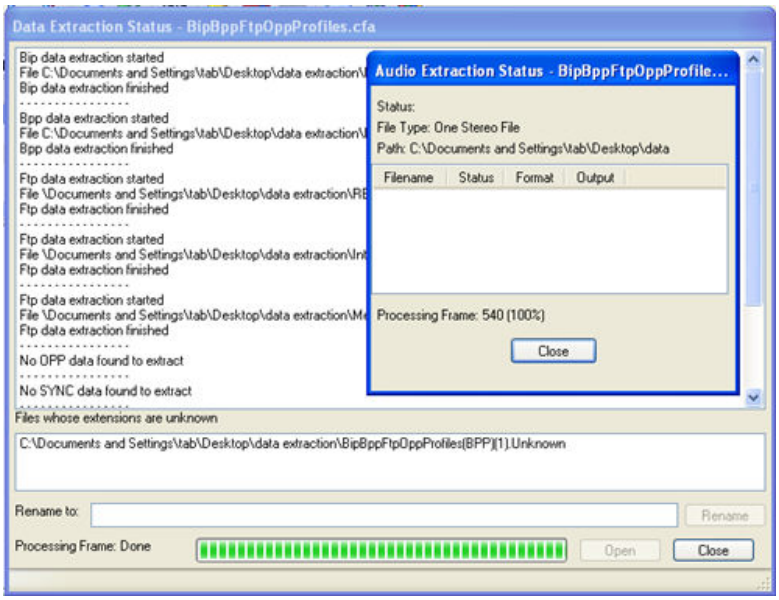


Figure 4.167 - Data and Audio Extraction Status

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.

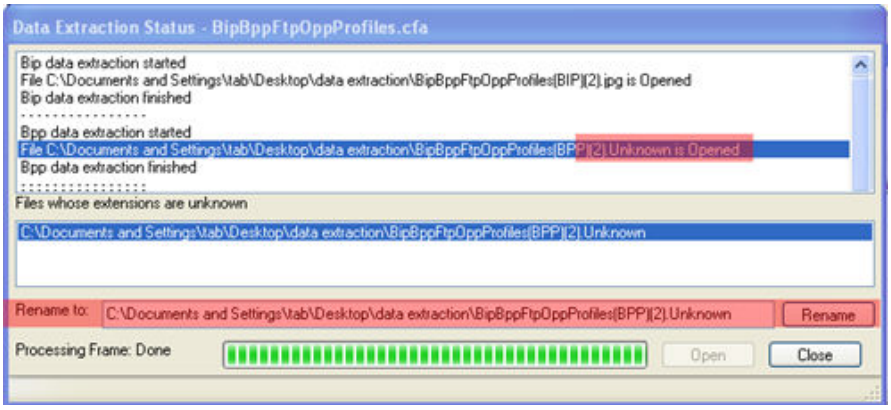


Figure 4.168 - Rename To in the bottom section of Data Extraction Status

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.

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**.

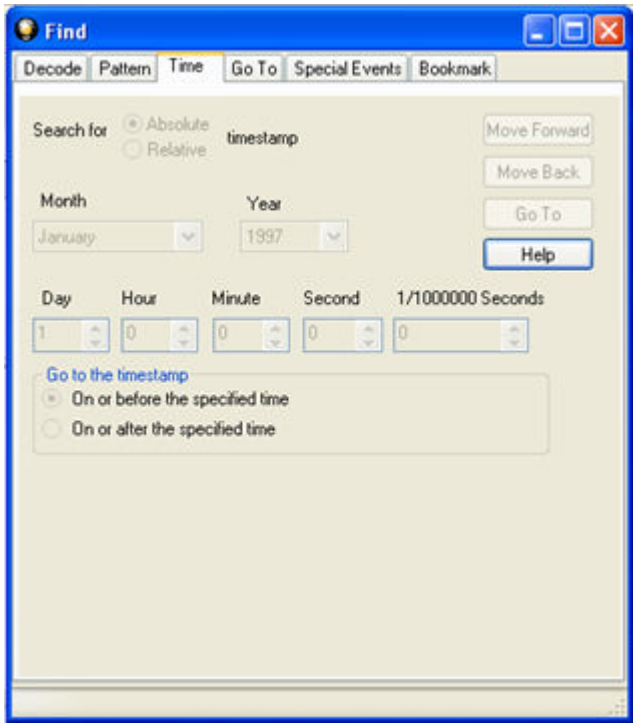


Figure 5.1 - Find Dialog

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.

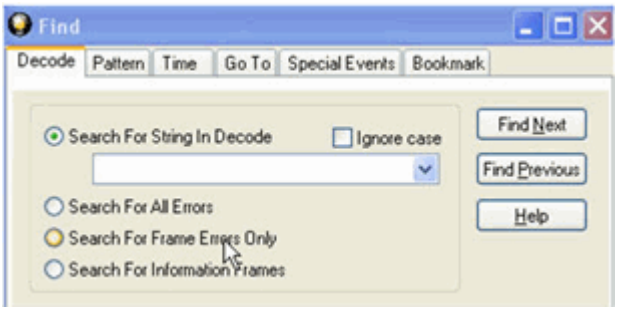


Figure 5.2 - Find Decode Tab Search for String

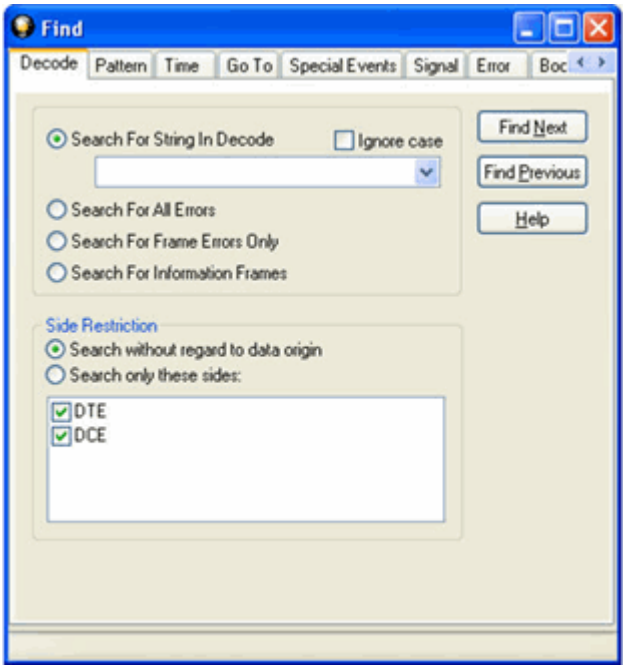


Figure 5.3 - Find Decode Tab Side Restriction

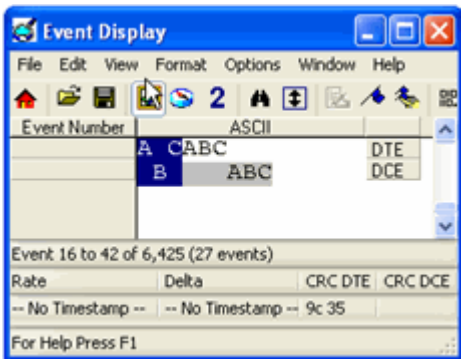
There are several options for error searching on the **Decoder** tab.

- **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.

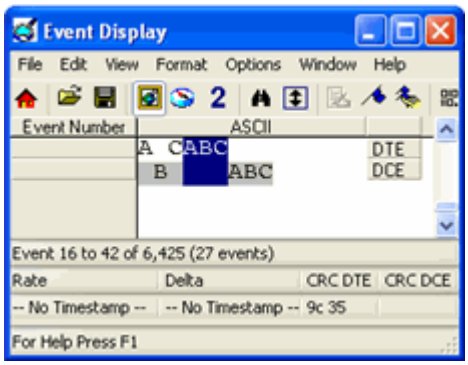
The result of the search is displayed in the **Decode** pane in **Frame Display.**

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.

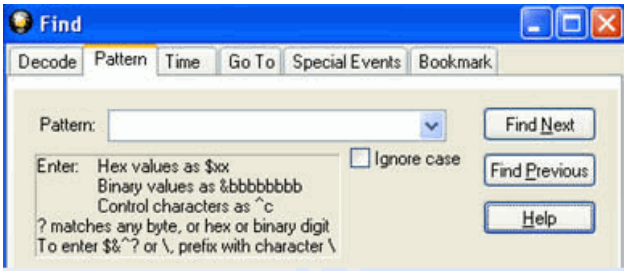


Figure 5.4 - Find Pattern Tab

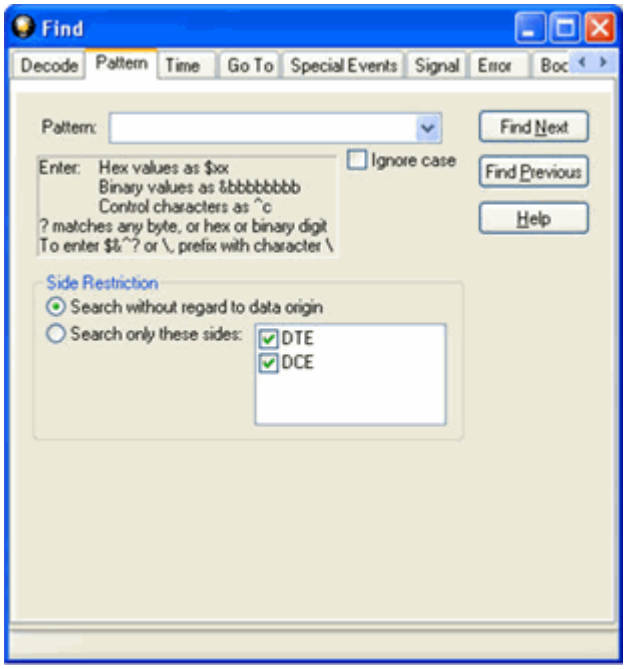


Figure 5.5 - Find Pattern Tab Side Restrictions

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 298 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.

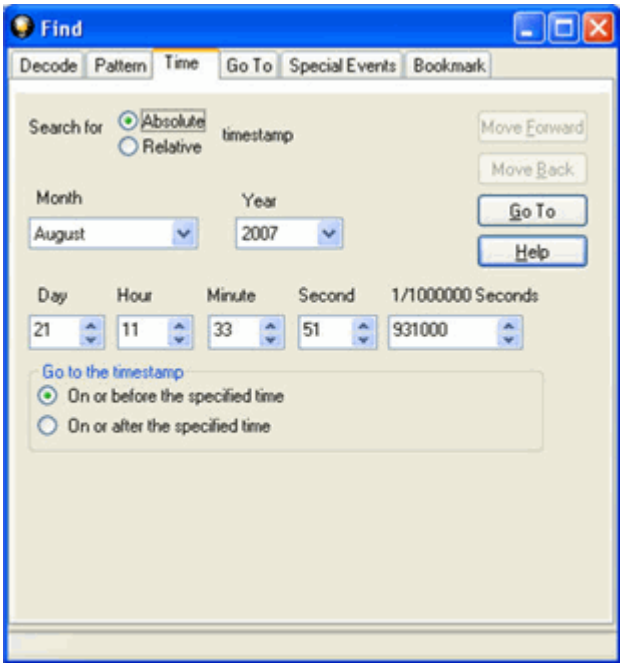


Figure 5.6 - Find by Time tab

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 Backward**is 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 Backward**is 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.

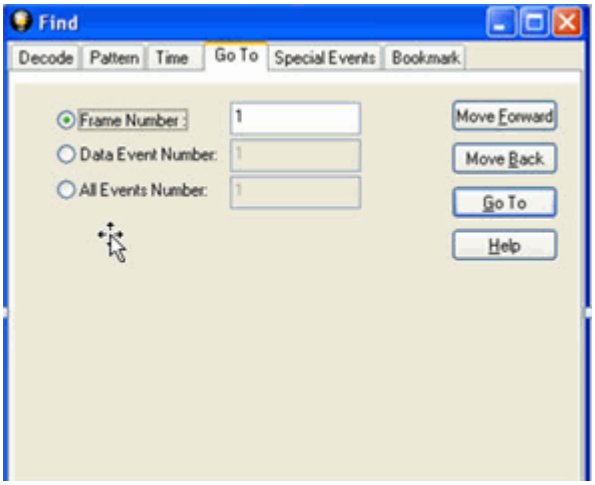


Figure 5.7 - Find Go To tab

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.

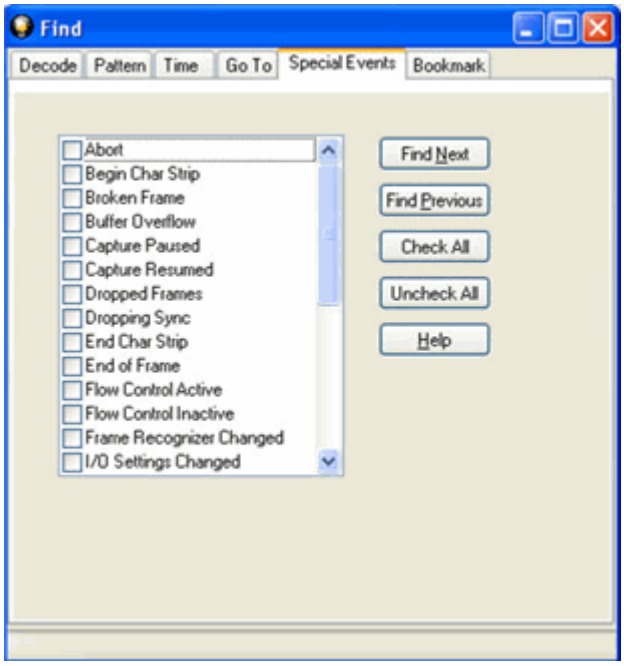


Figure 5.8 - Find Special Events tab

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 290.

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.

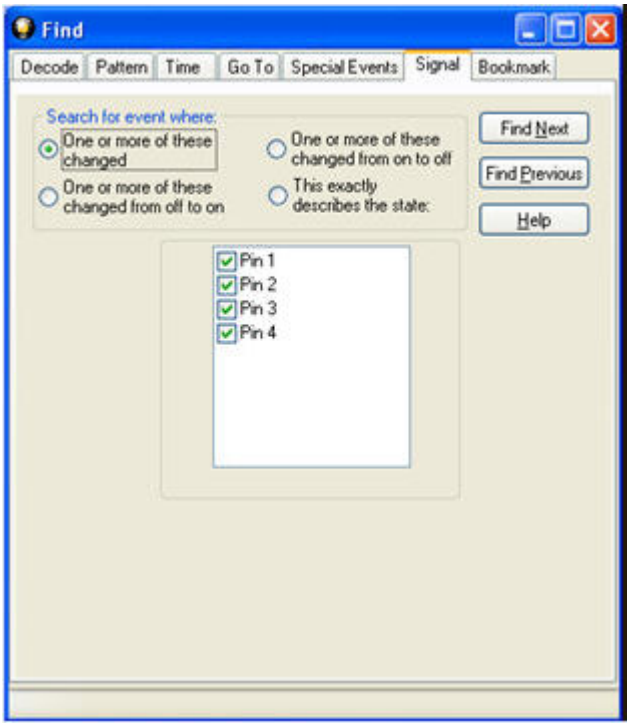


Figure 5.9 - Find Signal tab.

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

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.
  - 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.

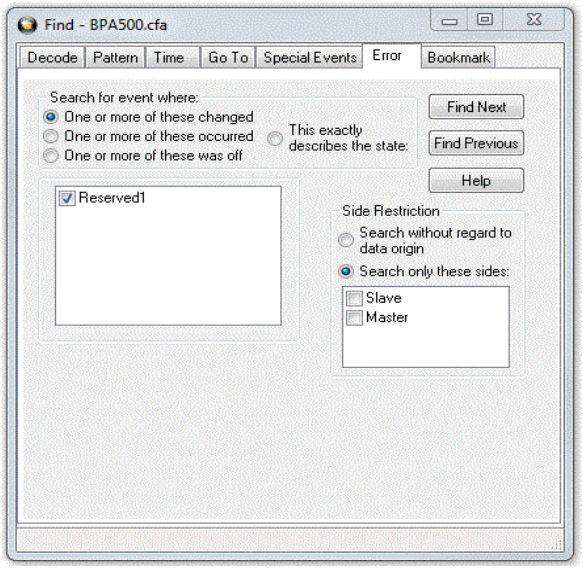


Figure 5.10 - Find Error tab.

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.

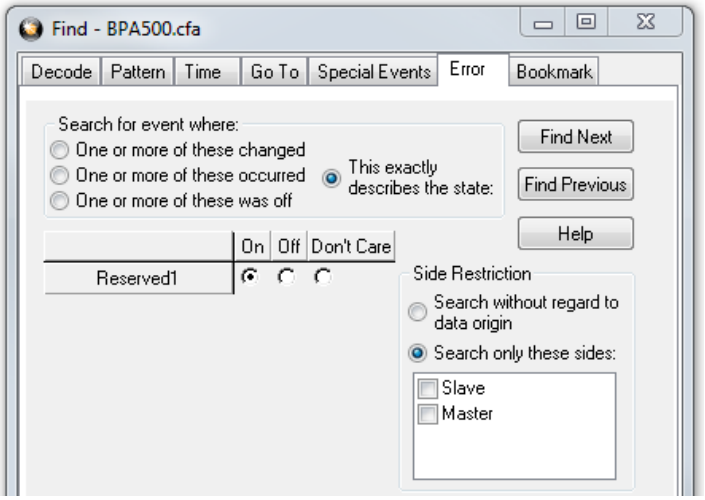
For example, if you have data that is full of framing errors, and you know that somewhere in your 20 megabyte capture file the framing got straightened out, you could choose to search for an event where one or more error conditions were off, and choose to search only for framing. The analyzer searches 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.

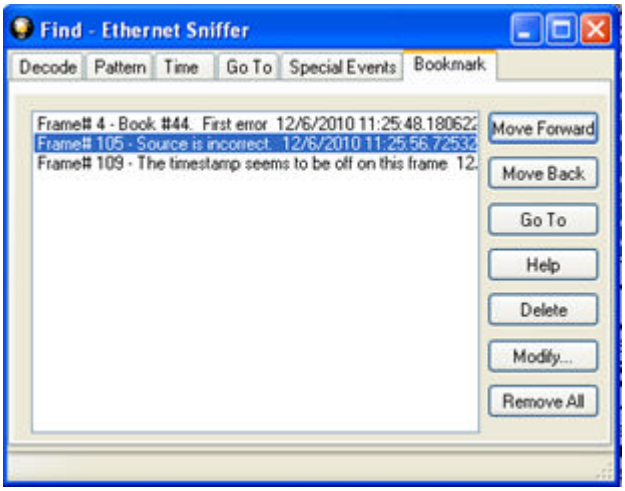


Figure 5.11 - Find Bookmark tab.

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.

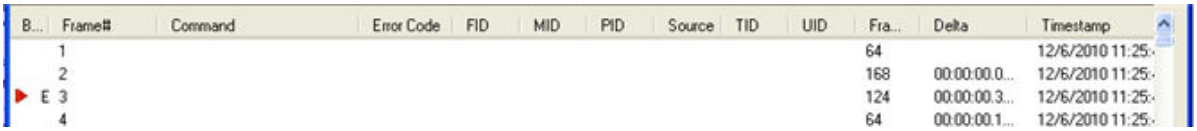
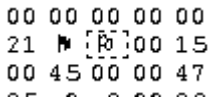


Figure 5.12 - Bookmarked Frame (3) in the Frame Display



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**

   toolbar or the **Bookmarks** menu. the **Find** window will open on the **Bookmark** tab. Select the bookmark 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.

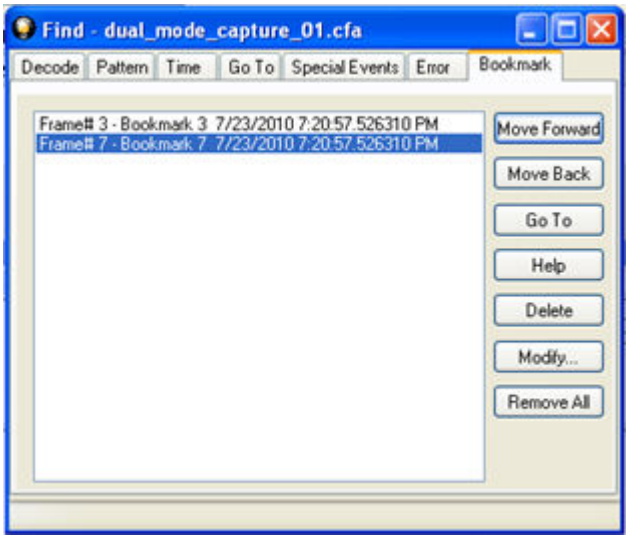


Figure 5.13 - Find Window Bookmark tab Used to Move Around With Bookmarks

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.

Chapter 6 Saving and Importing Data

6.1 Saving Your Sodera 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** window toolbar you can set up to capture a single file. Click here to see those settings.

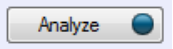
There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data to disk..

6.1.1 Saving the Capture File

Once your Sodera capture and analysis is completed, you can save the captured file for future analysis. All data captured from start session (**Recording**) to stop session (**Record**) is saved.

Before saving the following conditions must be met:

1. **Sodera** window Capture Toolbar shows 

.
2. **Sodera** window Capture Toolbar shows 

.

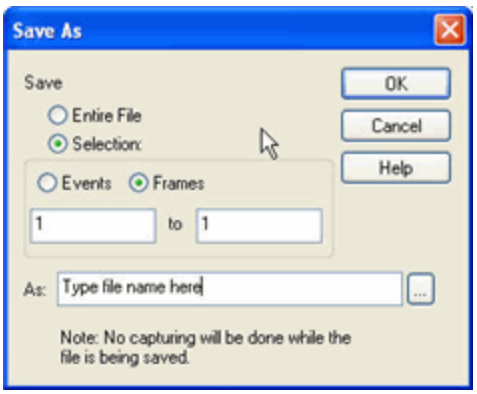
To save the captured data use one of the following methods:

- on the **Sodera** window **File** menu select **Save**,
- on the **Sodera** window Standard Toolbar click on the Save button  ,
- on the Sodera **Control** window **File** menu select **Save** or click on the Save  tool.
- On either the **Frame Display** or the **Event Display** window **File** menu select **Save** or click on the Save  tool.

A **Save As** window will open. Select a location and enter a file name. Click on the **Save** button.

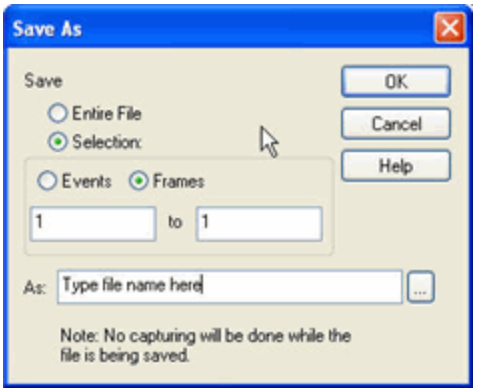
6.1.2 Saving the Entire Capture File with Save Selection

1. Open the **Event Display** or **Frame Display** window.
2. Right click in the data
3. 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 Save a Portion of Capture File with Save Selection

1. Open the **Event Display** or **Frame Display** window, depending on whether you want to specify a range in bytes or in frames.
2. 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.
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 **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.
6. Select either **Events** or **Frames** to indicate whether the numbers are event or frame numbers.
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. Click **OK** when you are finished.



6.2 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.

6.3 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.

6.4 Loading and Importing a Capture File

6.4.1 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**.

6.4.2 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.

6.5 Printing

6.5.1 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.

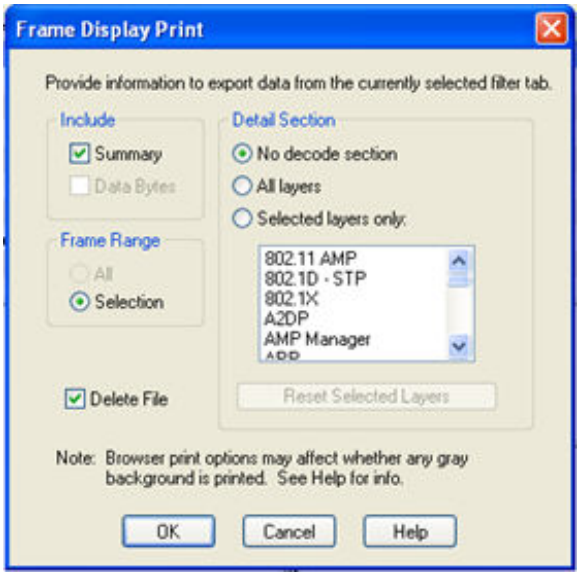


Figure 6.1 - Frame Display Print Dialog

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.

Frame Display Print Preview

The **Frame Display Print Preview** 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.

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.

1. Select **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print Preview**.

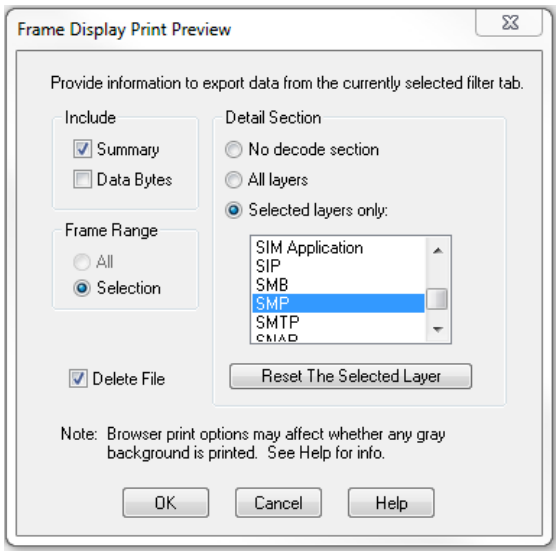


Figure 6.2 - Frame Display Print Preview Dialog

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, and after a brief wait a browser window will appear.

6.5.2 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 preview the print in your browser.

2. Select the range of events to include from either **All** or **Selection** in the **Event Range** section . Choosing **All** prints all of the events in the capture file or buffer. Choosing **Selection** prints only the selected events in the Event Display window.

> **Note:** In order to prevent a Print crash, you cannot select **All** if there are more than 100,000 events in the capture buffer.

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

Figure 6.3 - 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.

6.6 Exporting

6.6.1 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**.

6.6.2 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.

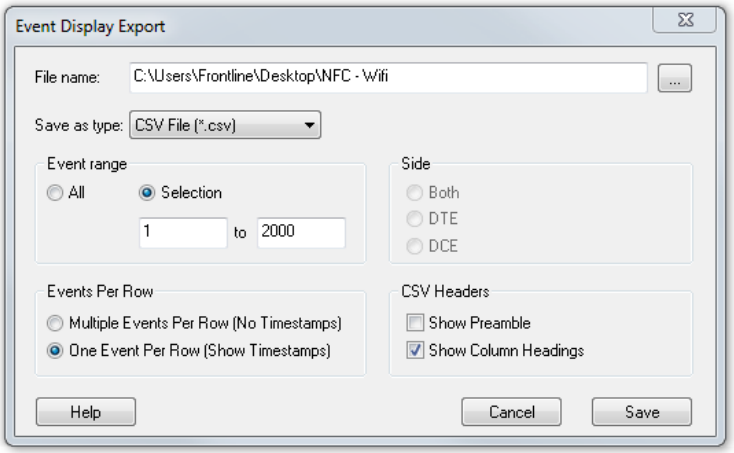


Figure 6.4 - Event Display Export Example: .csv file.

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 or Both to determine how you want to export the data.

5. Choose 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 6.5 - Example: .csv Event Display Export, Excel spreadsheet

6.6.2.1 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.

6.6.2.2 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.

Single File

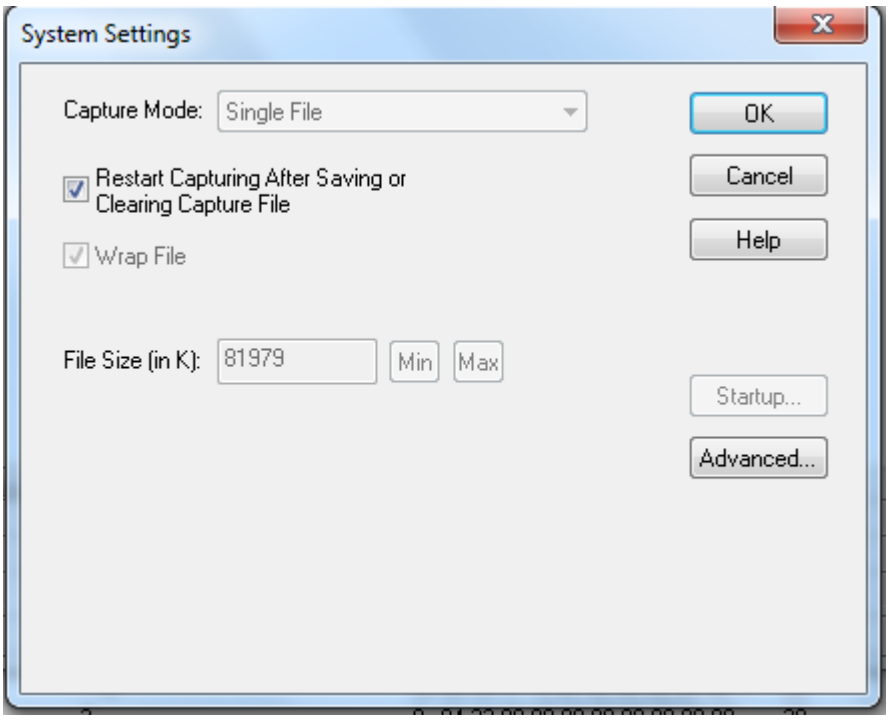


Figure 7.1 - System Settings Single File Mode

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.

- **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.

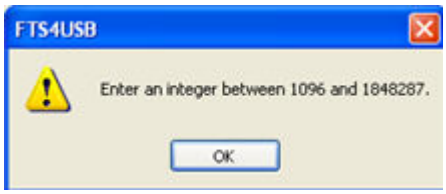
- **Wrap File**

  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.

7.1.1.1 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.

7.1.1.2 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.

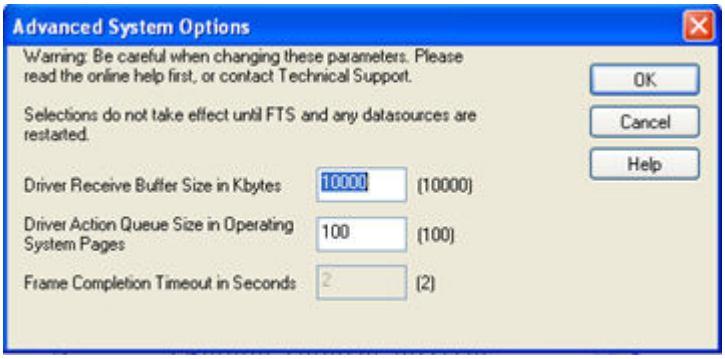


Figure 7.2 - Advanced System Options dialog

- **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.

7.1.1.3 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.

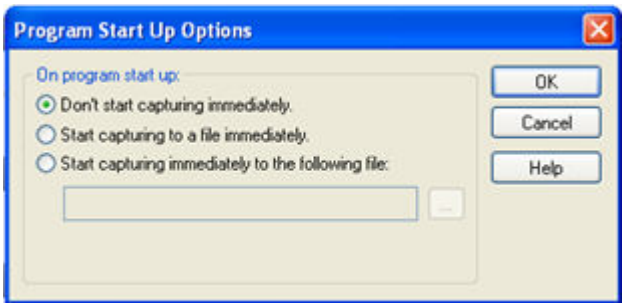


Figure 7.3 - Start Up Options dialog

- **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.

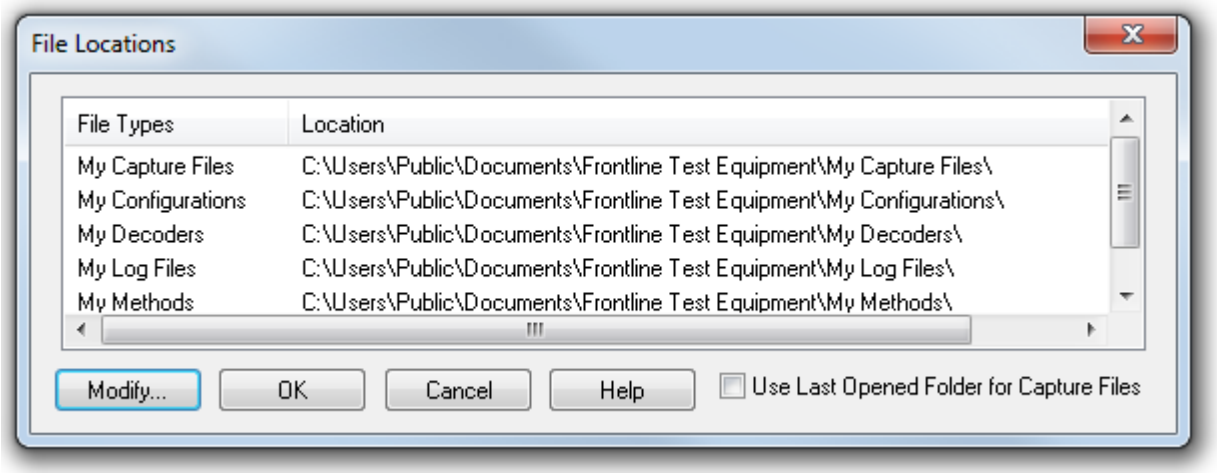


Figure 7.4 - File Locations dialog

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

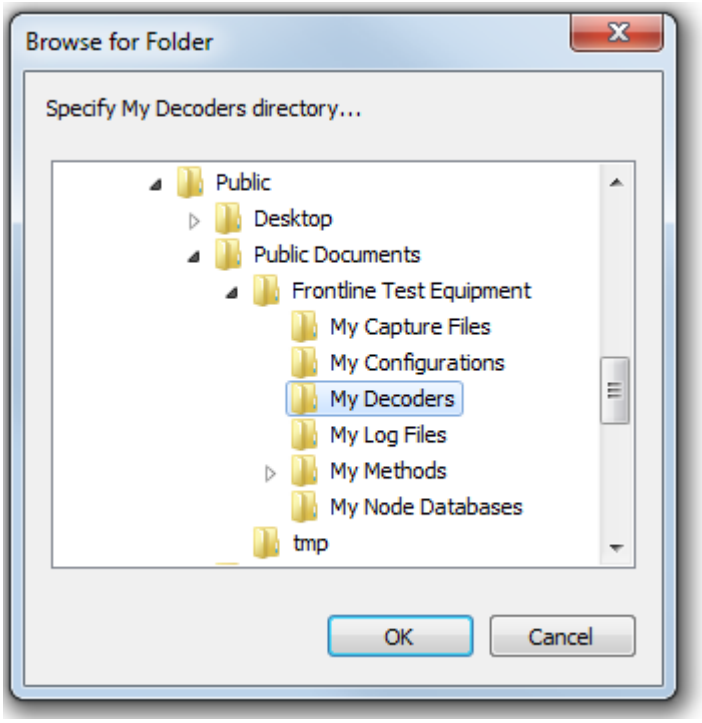


Figure 7.5 - File Locations Browse dialog

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.

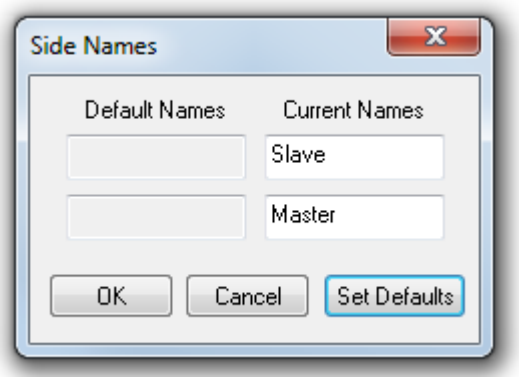


Figure 7.6 - Example: Side Names Where "Slave" and "Master" are current

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.

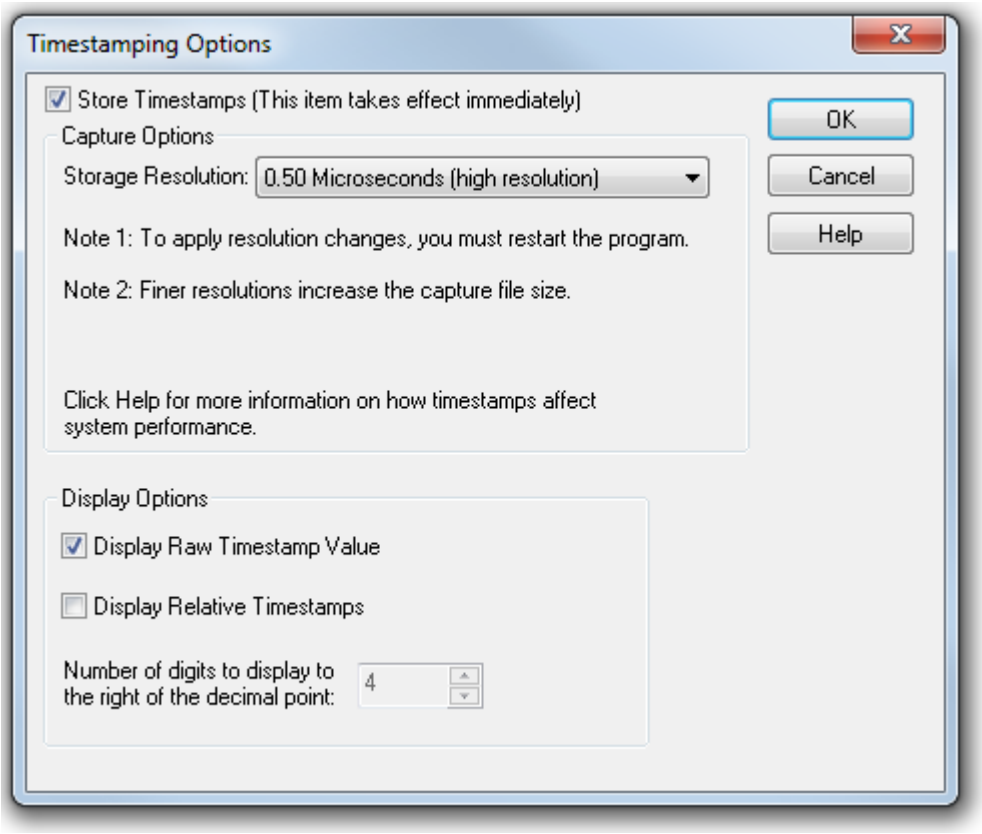


Figure 7.7 - Timestamping Options dialog

Enabling/Disabling Timestamp

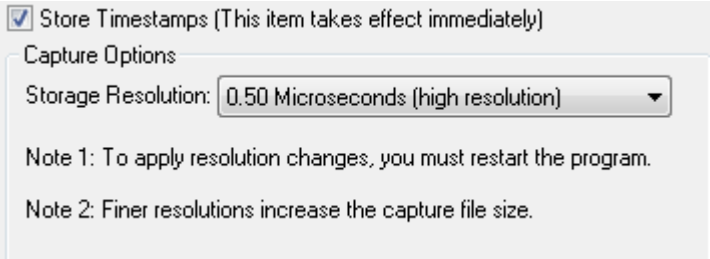
To enable timestamping click to make a check appear in the check box **Store Timestamps (This time takes effect immediately)**. Removing the check will disable timestamping.

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.

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.

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.

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 D**river 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.

Table 7.1 - 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

Table 7.1 - Communications Control Characters(continued)

Abbreviation	Control Character	Text
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit Separator
VT	VT	Vertical Tabulation

7.2.6 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.

7.2.7 *Bluetooth* low energy ATT Decoder Handle Mapping

Low energy device attributes contain a 16-bit address called the attribute handle. Each handle is associated with an attribute Universally Unique Identifier (UUID) that is 128-bits long. In the attribute database, the handle is unique while the UUID is not unique.

The ComProbe software detects and stores the relationships (mappings) between handle and UUID during the GATT discovery process. But sometimes, there is no GATT discovery process because

- The discovery has previously taken place and both devices stored the mappings and the discovery will not repeat at every subsequent connection.
- The developer owns both devices in the conversation and chose to ignore discovery because the mappings are known.
- The devices are in development and the code to perform the mappings has not been written yet.

The solution to this problem is to

1. define the mappings in a file and
2. then pre-loading the mapping using the ComProbe software.

Creating handle-UUID mapping file

Create a file named "ATT_Handle_UUID_Preload.ini' in the root directory of "C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\", but the file can be located anywhere.

Assume that you want to create a GATT service starting at handle 1.

Create a section in the ini file called

```
[Service Base Handles]
A=1
```

"A" will be your first service. Make the base handle equal to the handle of your service. You can use all upper and lower case letters so you can have up to 52 service handles.

Next add the following section.

```
[Advertiser Handles]
; Generic Access Profile (GAP)
A0 = 1800
A1 = 2803
A2 = 2a00
A3 = 2803
A4 = 2a01
A5 = 2803
A6 = 2a04
```

A few things of note:

- In the code above, lines begging with a semi-colon are comments.
- If you want to change the base handle of the GAP service, change the "1" to some other number.
- If you want to comment out the entire service, comment out the base handle. If no "A" is defined, the software will ignore "A1", "A2" and so on.

Contacting Frontline 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 Sodera product, support is available between 9 am and 5 pm, U.S. Eastern Time zone, and between 9 am and 5 pm, Pacific Time zone, on Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Instructional Videos

Teledyne LeCroy 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.

Appendicies

Appendix A: Sodera Technical Specifications/Service Information

- Dimensions: 159 mm wide X 57 mm tall” X 165 mm deep” (6.3” X 2.3 " 6.5" X mm)
- Weight: 1.0 kg (2.2 lb)
- Humidity: Operating: 0% - 90% (0 °C – 35 °C)
- Temperature: -10 °C to +40 °C (14 °F to +104 °F)
- Power Input: 12 VDC (tip positive)
- Max Power: 25 W
- Battery: NB2037FQ31

Caution: There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of old batteries according to your local regulations.

Service Notes

The Sodera hardware does not contain any user serviceable items. Any repairs and maintenance must be performed by a service technician that has been trained and approved by Frontline.

Before any service is performed on Sodera, all power sources must be removed. This includes removing the battery and disconnecting any power sources from the 12 VDC input power connector on Sodera. Typical power sources include external AC/DC power supplies or auxiliary power sources from a vehicle.

Internal Fuse Information

- Manufacturer: Littlefuse
- Type: OmniBlok
- Current rating: 5A
- Speed rating: Very Fast Acting
- Voltage rating: 125V ac/dc

Appendix B: Application Notes

B.1 Audio Expert System: aptX 'hiccup' Detected

This paper presents a case study in Bluetooth® audio debugging that highlights the importance of Frontline's Audio Expert System (AES) in the process. The actual case involves transmission of a high quality, stereo audio using the aptX codec from a smartphone to a *Bluetooth* headset. The transmission contained SBC encoded packets despite a successful negotiation of aptX encoding and decoding mechanism between the source and the sink devices. Frontline's AES software discovered this transmission error which most likely would not have been easily discovered by using traditional *Bluetooth* protocol and event analysis. Without the Audio Expert System a product may have been shipped that was not performing as expected by the manufacturer.

B.1.1 Background

In *Bluetooth* technology, Audio/Video Distribution Transport Protocol (AVDTP) uses Advanced Audio Distribution Profile (A2DP) for streaming audio in stereo. The A2DP encompasses compression techniques to reduce the amount of radio frequency bandwidth required to transmit audio. In addition to A2DP, Audio/Video Remote Control Profile (AVRCP) controls certain functions of the sending device such as pause, play, next track, etc.

All *Bluetooth* products using A2DP are required to implement audio encoding and decoding using low complexity Sub Band Coding (SBC) that supports up to 345 kb per second bit rate for stereo audio. The SBC codec has some issues though. SBC coding and decoding produces some undesirable artifacts in the audio signal. In addition, the SBC encoding and decoding cycle introduces a time lag in the audio. To improve on SBC's artifacts and time lag issues, a CSR proprietary codec that is called aptX® is implemented on some Bluetooth products.

During the negotiation phase, both Bluetooth devices handshake and they automatically discover the best codec and the highest bit rate to use for audio. If both devices support aptX, it is used rather than the default SBC.

The AES software helps identify audio issues in *Bluetooth* protocol by highlighting information, warnings, and errors related to audio data, codec used, and *Bluetooth* protocol implementation. They are collectively called “events” in AES.The AES window shows audio data plotted as PCM samples versus time in the Wave Panel. The audio data, codec, and protocol events are also graphically displayed in the Wave Panel, and with a single click on an event, engineers and testers are brought directly to the exact packets or frames related to the event in the *Bluetooth* protocol trace in the Frame Display. This helps users find issues quickly and easily. The events are shown time aligned with both the actual audio waveform and bit rate variances graph in the Wave Panel. The bit rate variance graph shows the average or actual amount of Bluetooth audio data sent over a period of time.

AES can operate in two modes: 1) referenced mode, and 2) non-referenced mode. In referenced mode a Frontline provided audio test file is streamed between the Devices Under Test (DUTs). The test file content and parameters are known to the AES software that performs a comparison for deviations. This process helps the software accurately detect anomalies created by the streaming process. In non-referenced mode DUTs stream audio of unknown content, limiting the types of detectable events. The software automatically determines the operation mode with no user input required.

B.1.2 Test Setup

The following DUTs below were used in our test setup:

- DUT1 = smartphone with *Bluetooth* and aptX capability. The smartphone operating system was Android.
- DUT2 = Earphones with *Bluetooth* and aptX capability.

The protocol analyzer: ComProbe BPA 600 Dual Mode *Bluetooth* Protocol Analyzer with *Bluetooth* Audio Expert System activated. The BPA 600 is connected to a personal computer (PC) that is running ComProbe Protocol Analysis System software.

DUT1 was used as a source device. DUT1 was streaming an AES Reference file.

DUT2 was used as a sink device. After establishing a valid *Bluetooth* link, DUT2 played the AES Reference file.

The audio test file was played from the Bluetooth smart phone to the Bluetooth headphone. The data captured by the ComProbe BPA 600 hardware was sent to the analysis computer running ComProbe software with AES. As the data was captured, it was analyzed by the AES module and displayed live in the AES window. The AES software automatically detected the test ID tones in the captured audio and operated in the referenced mode. The figure 1 below shows the test setup.

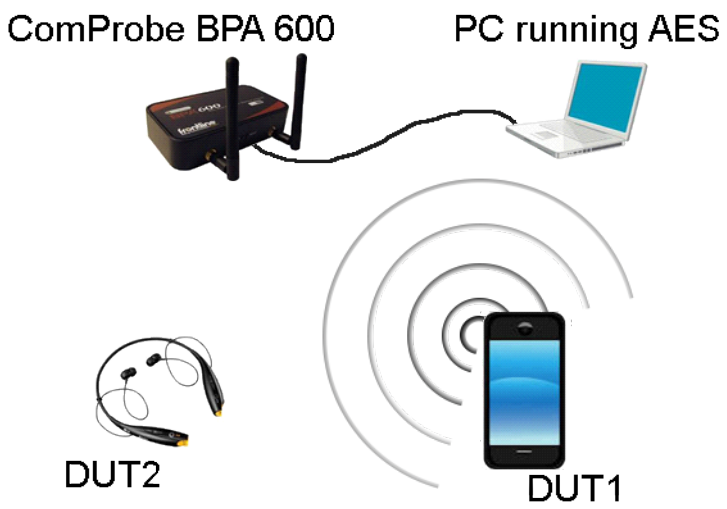


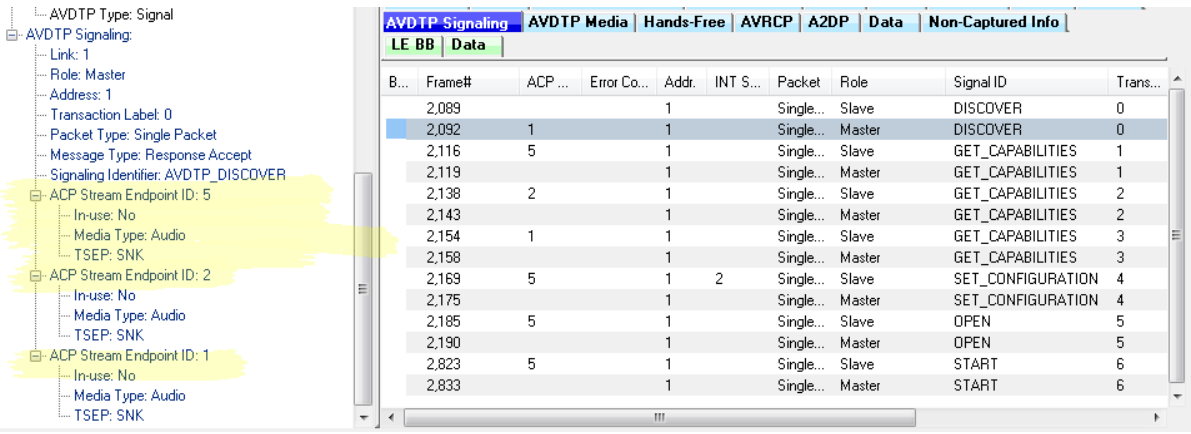
Figure 1 - The Test Setup.

B.1.3 Discussion

The test began without any issue. DUT1 and DUT2 negotiated a Bluetooth connection suitable for transmitting the audio. When the Reference Audio was played there were no obvious audio distortions or anomalies heard by the tester.

The tester used a ComProbe BPA 600 configured for capturing Classic Bluetooth over a single connection.

In Frame Display AVDTP Signaling tab we see the start of the negotiation between DUT1 and DUT2 to establish an audio connection, see Figure 2. At frames 2089 and 2092 the initiating or local device sends an AVDTP_ DDISCOVER command. The remote device responds by identifying the ACP Stream Endpoint IDs. In this case the remote device identifies three audio media-type devices that are SNK (sink) devices currently not in use: SEPID (Stream Endpoint Identification) 5, 2, and 1.



B...	Frame#	ACP ...	Error Co...	Addr.	INT S...	Packet	Role	Signal ID	Trans...
	2,089			1		Single...	Slave	DISCOVER	0
	2,092	1		1		Single...	Master	DISCOVER	0
	2,116	5		1		Single...	Slave	GET_CAPABILITIES	1
	2,119			1		Single...	Master	GET_CAPABILITIES	1
	2,138	2		1		Single...	Slave	GET_CAPABILITIES	2
	2,143			1		Single...	Master	GET_CAPABILITIES	2
	2,154	1		1		Single...	Slave	GET_CAPABILITIES	3
	2,158			1		Single...	Master	GET_CAPABILITIES	3
	2,169	5		1	2	Single...	Slave	SET_CONFIGURATION	4
	2,175			1		Single...	Master	SET_CONFIGURATION	4
	2,185	5		1		Single...	Slave	OPEN	5
	2,190			1		Single...	Master	OPEN	5
	2,823	5		1		Single...	Slave	START	6
	2,833			1		Single...	Master	START	6

Figure 2 - Frame Display for AVDTP Signaling Frame 2089 & 2092

> **Note:** "ACP" is AVDTP terminology for the remote device.

The next step in the negotiation is to get the audio capabilities of each SEPID. For each SEPID there is an exchange of GET_CAPABILITIES AVDTP signals.

Examination of the Frame Display AVDTP Signaling protocol tab shows at frame 2116 the slave device request SEP (Stream End Point) characteristics. for SEPID (SEP Identifier) 5. Details of the GET_CAPABILITIES command are shown in the Figure 3.

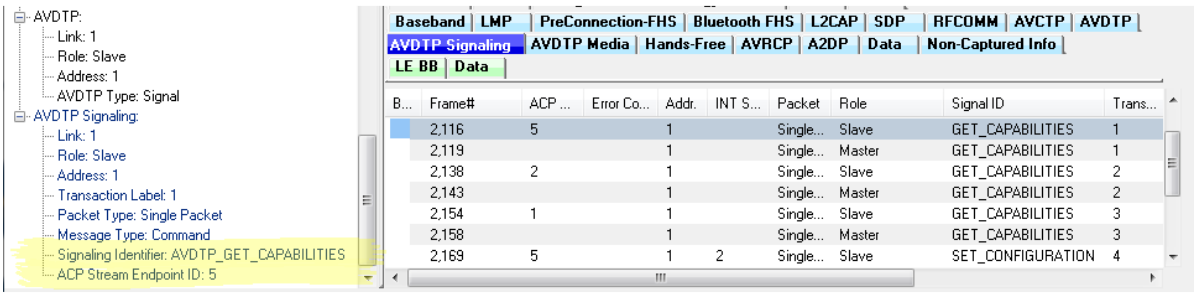


Figure 3 - Frame Display for AVDTP Signaling Frame 2116

At frame 2119 the remote device responds to the GET_CAPABILITIES for SEPID 5 reporting that this SEP codec is aptX with a Channel Mode Stereo.

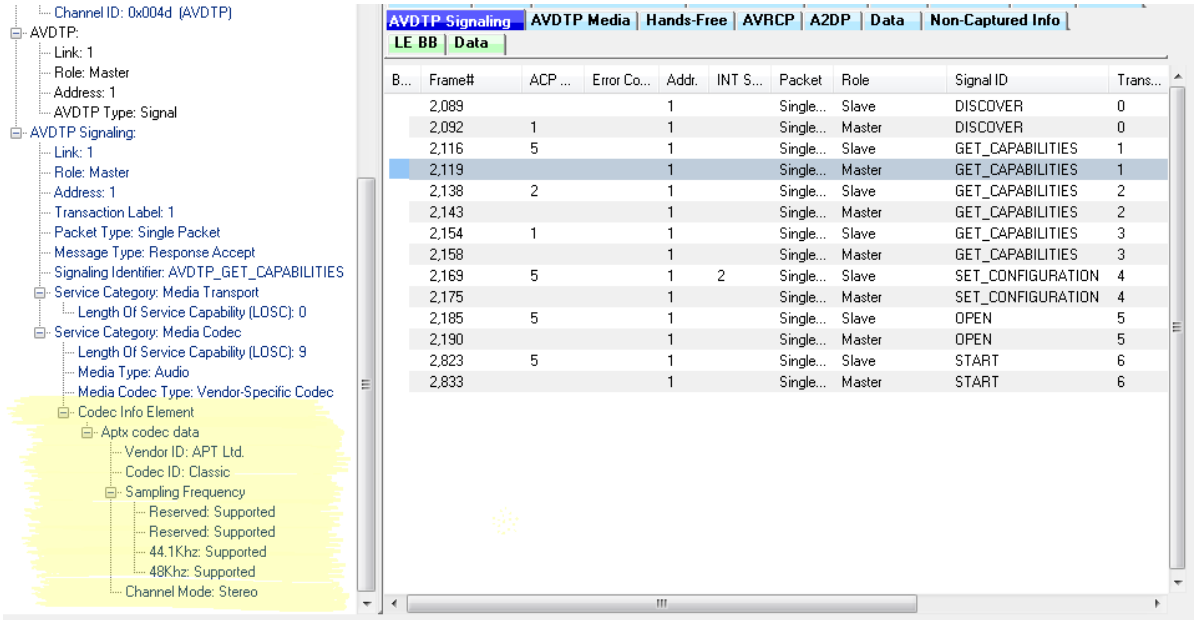


Figure 4 - Frame Display for AVDTP Signaling Frame 2119

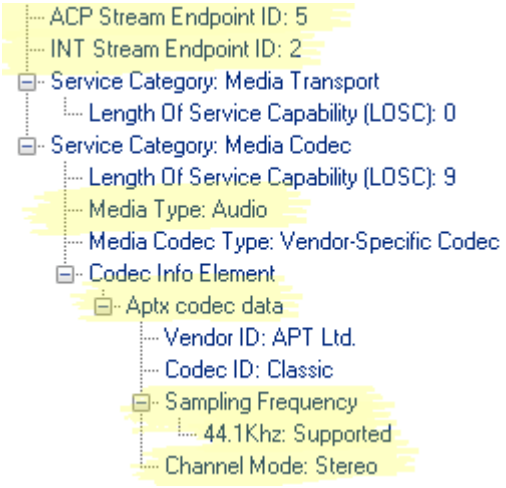
In Figure 4, frames 2138 through 2158 perform the GET_CAPABILITIES negotiation between the local and remote device for SEPIDs 2 and 1. SEPID 2 is an MPEG SEP, and SEPID 1 is the SBC SEP.

Frames 2169 and 2175 sets the specific details of the connection with the SET_CONFIGURATION signal. The local device sets the remote endpoint to the aptX device (ACP Stream Endpoint ID: 5), and sets the local endpoint to SEPID 1 (INT Stream Endpoint ID: 2). The Codec, Sampling Frequency, and Channel Mode are also configured. See Figure 5.

At frame 2175 the remote device sends the message "Response Accept" completing the audio stream setup.

Frames 2185 and 2190 are the local request and the remote response to OPEN the audio stream.

Frames 2823 and 2833 START the audio stream with the local request and the remote response respectively.



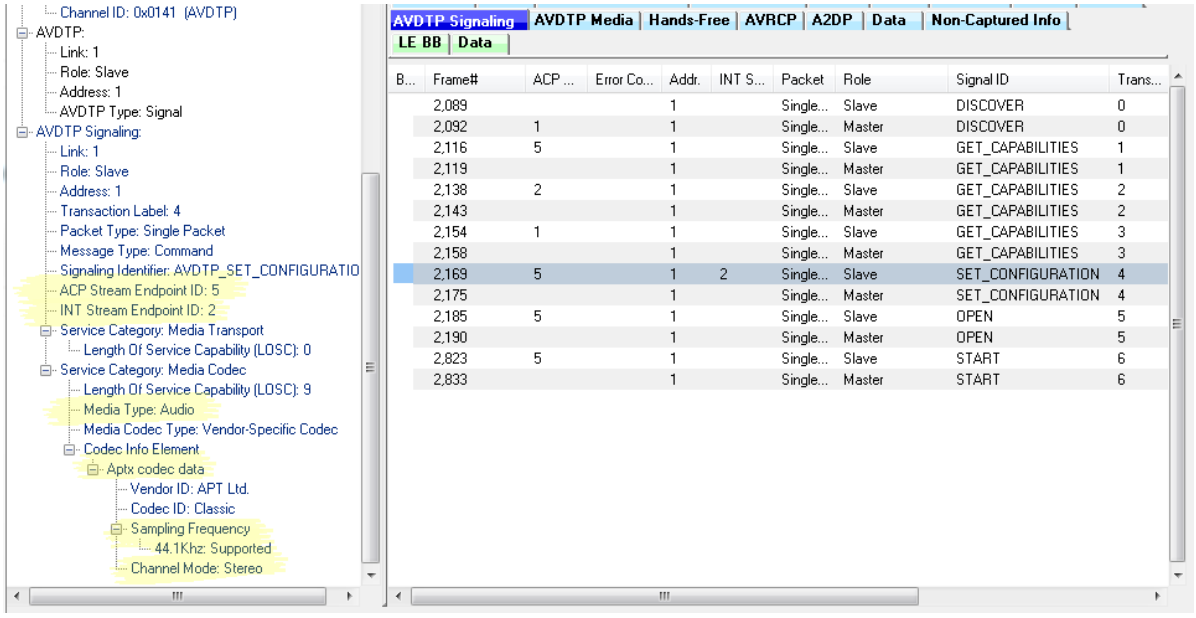


Figure 5 - Frame Display for AVDTP Signaling Frame 2169, SET_CONFIGURATION

So far the process of setting up an aptX audio connection between DUT1 and DUT2 appears normal, correct and error free. We now move from he AVDTP protocol to the A2DP protocol to observe the audio.

Problem Discovery

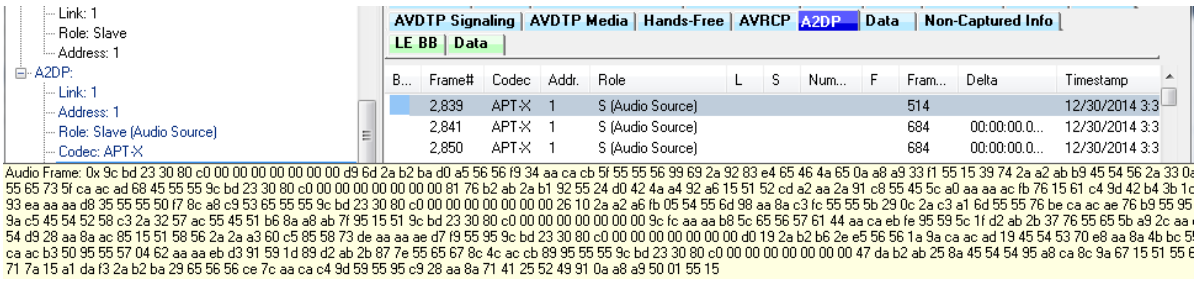


Figure 6 - Frame Display for A2DP Streaming at Frame 2839 with Audio Expanded

In the ComProbe software, the audio data is shown in the A2DP tab in the Frame Display, see Figure 6. The frame 2839, which is the first audio frame, is identified as being aptX encoded because of the successful codec negotiation. At this frame, the conventional audio data analysis methods do not show any issues. Assuming the data is aptX encoded, the AES software passes it to the AES aptX decoder. However, the data was not decoded.correctly and is marked as a bad aptX frame.On further analysis, the AES software discovers that the frame is not aptX encoded but is actually SBC encoded. Frame 2839 begins with “0x9C”, and all SBC audio frames begin with sync word “0x9c” as shown in Figure 6. The AES cannot solely rely on the sync word to determine if it is a SBC frame. To confirm the suspicion, the AES passed the data through its SBC decoder, and the data came out cleanly decoded.

The AES software not only showed that there is a problem in the audio data but also made it clear where the problem is.

The Error that is identified by Event 4, the Severity red circle , is a codec event at Frame 2839 states "Unable to process AptX data as extracted. It appears that SBC encoded data is being sent over this stream."

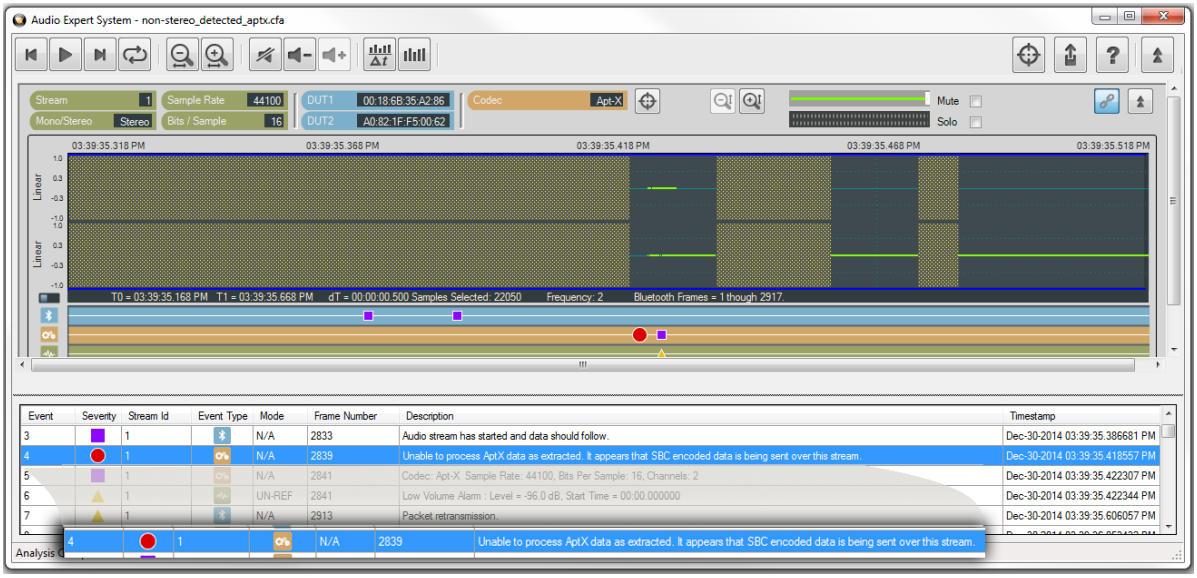


Figure 7 - Audio Expert System Error on Frame 2839: Data not aptX.

B.1.4 Conclusions

This case shows the value of Frontline's Audio Expert System. An error in the transmission of an audio stream compressed using aptX was not easily detected in the protocol analysis using frames. While, in this situation with audio streaming between a smartphone and a *Bluetooth* headset, there was not a significant disruption of the audio, but in playback using other devices there may have been a more significant interruption of the audio streaming.

The smartphone manufacturer may wish to find out why aptX compressed audio contained SBC compressed data in the stream. We can speculate that there may be an underlying problem with clearing stacks or memory between streaming events. This investigation is beyond the scope of this paper.

If there is interest in the Audio Expert System as an expansion of your ComProbe Bluetooth analyzer contact the Frontline sales at sales@fte.com or visit our web site at fte.com.

Author: John Trinkle & Priyanka Gupta

Publish Date:27 February 2015

B.2 Getting the Android Link Key for Classic Decryption

Bluetooth devices on an encrypted link share a common “link key” used to exchange encrypted data. For a *Bluetooth* sniffer, such as the ComProbe BPA 600, to be able to decrypt the encrypted data, it must also have this shared link key. For obvious security reasons, the link key is never sent over the air, so either the user must get the key out of one of the devices being sniffed and supply the key to the sniffer or the sniffer must create the key itself.

Bluetooth devices using the Android operating system have a "developer" option that will provide the link key for Classic *Bluetooth* decryption. This procedure will use the developer options to obtain the Android HCI (Host Controller Interface) log that contains the link keys for all active links..

B.2.1 What You Need to Get the Android Link Key

The process applies to the Android 4.4 or later operating system.

- Android device with Bluetooth enabled and paired with another *Bluetooth* device.
- ComProbe Protocol Analysis System installed on your computer
- Android Debug Bridge (optional)

> **Note:** Each Android device model can vary in screen organization, layout and format. The directions in this paper are based on known typical Android device. Refer to the manufacturer's manual,on-line help, or technical support for detailed information about your particular device.

B.2.2 Activating Developer options

The Android HCI log will contain the link key for an active *Bluetooth* link.

1. On the Android device go to **Settings**,
2. Select **About**.
3. In the About screen tap on **Build number** eight times. At some point you will see a notice similar to

"You are now a developer!".

> **Note:** On some devices the build information may be under one or more sub-screens below the About screen. Also the number of taps may vary; in most cases the screen will provide status of your tap count.

4. Return to the **Settings** screen and you will see **Developer options**

B.2.3 Retrieving the HCI Log

Now that **Developer options** have been activated on the Android device, you can retrieve the HCI log.

1. On the Android device go to **Settings**.
2. Select **Developer options**.
3. Click to enable **Bluetooth HCI snoop logging.**
4. Return to the **Settings** screen and select **Developer options**.
5. In the **Developer options** screen select **Enable Bluetooth HCI snoop log**. The log file is now enabled.

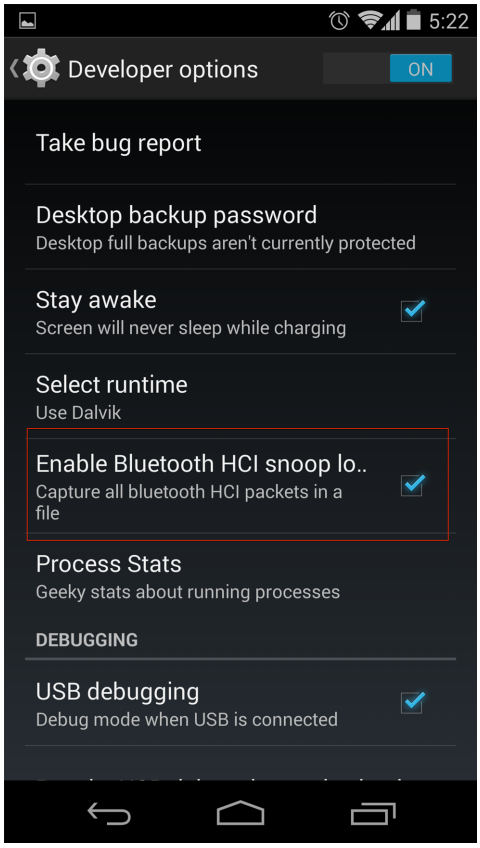


Figure 8 - Typical Android Developer options screen

6. On the Android device turn off *Bluetooth*.
7. Turn on *Bluetooth*.
8. Reboot the Android device.

The HCI log file is now being generated and is saved to */sdcard/btsnoop_hci.log*.

> **Note:** Samsung devices have a slightly different location for the btsnoop file.

There are two options for retrieving the HCI log from the Android device.

a. Attach the Android device to your computer. The file */sdcard/btsnoop_hci.log* is in the root of one of the mountable drives. Copy the file to directory *C:/Users/Public/Public Documents/Frontline Test Equipement/My Capture File/*.

b. The second option is to use the Android Debug Bridge (ADB)using the following steps. The debug bridge is included with Android Software Developer Kit.

(1). On the Androd device **Development** screen, select **Android debugging** or **USB debugging**.

(2). Connect your computer and Android device with a USB cable.

(3). Open a terminal on your computer and run the following command.

```
adb devices.
```

(4). Your Android device should show up in this list confirming that ADB is working.

```
List of devices attached
XXXXXXXXXXX device
```

(5). In the terminal enter the following command to copy the HCI Log to your computer.

```
adb pull /sdcard/btsnoop_hci.log
```

B.2.4 Using the ComProbe Software to Get the Link Key

You will load the HCI Log file *btsnoop_HCI.log* into the ComProbe Protocol Analysis System on your computer as a capture file. Then you can use the **Frame Display** to locate the link key.

1. Activate the ComProbe Protocol Analysis System. (Refer to the ComProbe BPA 600 User Manual on fte.com).
2. From the Control window menu select **File**, **Open Capture File...**.
3. When the **Open** window appears, set the file type to **BTSnoop Files (*.log)**. If not already selected navigate to the *My Capture Files* directory and select *btsnoop_hci.log*.

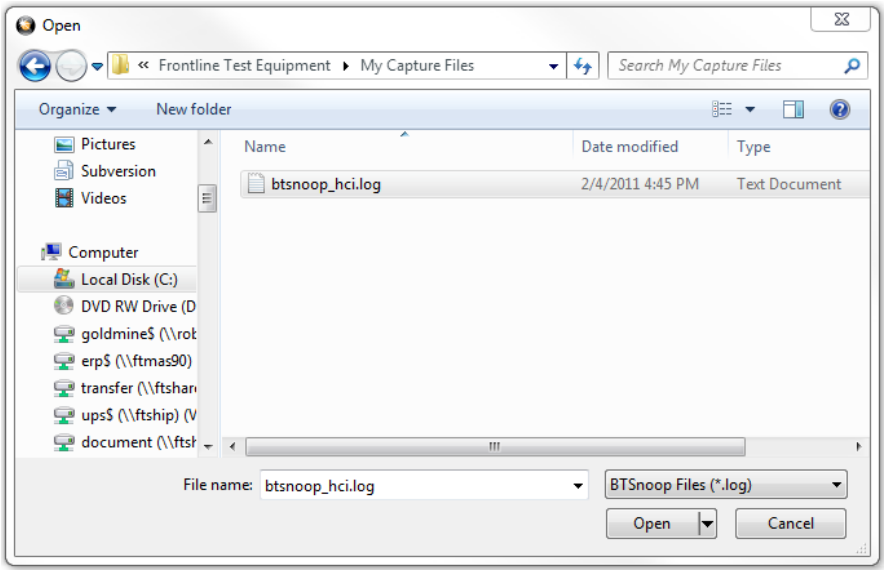


Figure 9 - Select Capture File

4. Open the **Frame Display** 

5. In the **Frame Display** protocol tabs select **HCI**. (See image below)

6. Select Find  , click on the **Decode** tab, and enter "link key" in the Search for String in Decode.

   Check the **Ignore Case** option. Click on **Find Next** until the Event column shows Link Key Notification.

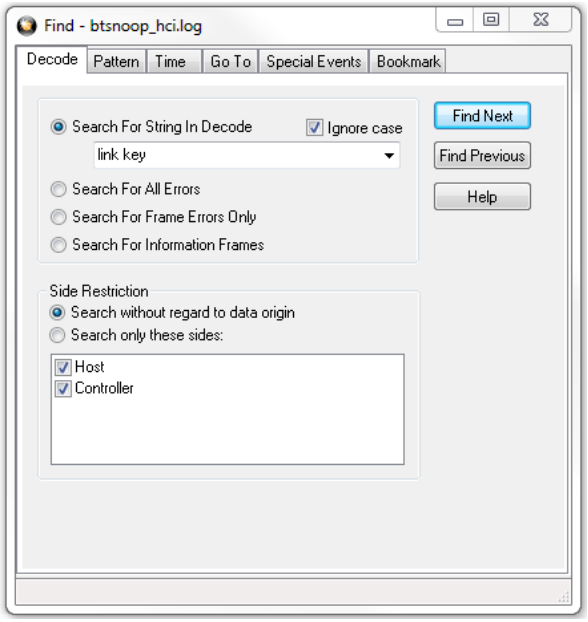


Figure 10 - Find Dialog

In the **Frame Display** Detail pane, expand HCI and HCI Event where the Link Key is shown. Copy and paste the Link Key into the appropriate BPA 600 datasource dialog. (See the example below)

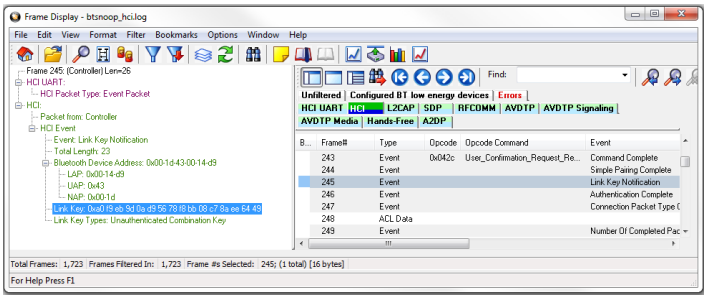


Figure 11 - Frame Display Showing Link Key Notification Event with the Link Key

---

Author: John Trinkle with Joe Skupniewitz

Publish Date: 30 September 2014

B.3 Decrypting Encrypted Bluetooth® low energy

B.3.1 How Encryption Works in *Bluetooth* low energy

Data encryption is used to prevent passive and active—man-in-the-middle (MITM) — eavesdropping attacks on a *Bluetooth* low energy link. Encryption is the means to make the data unintelligible to all but the *Bluetooth* master and slave devices forming a link. Eavesdropping attacks are directed on the over-the-air transmissions between the *Bluetooth* low energy devices, so data encryption is accomplished prior to transmission using a shared, secret key.

B.3.2 Pairing

A *Bluetooth* low energy device that wants to share secure data with another device must first pair with that device. The Security Manager Protocol (SMP) carries out the pairing in three phases.

1. The two connected *Bluetooth* low energy devices announce their input and output capabilities and from that information determine a suitable method for phase 2.
2. The purpose of this phase is to generate the Short Term Key (STK) used in the third phase to secure key distribution. The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.
3. In this phase each device may distribute to the other device up to three keys:
    a. the Long Term Key (LTK) used for Link Layer encryption and authentication,
    b. the Connection Signature Resolving Key (CSRK) used for data signing at the ATT layer, and
    c. the Identity Resolving Key (IRK) used to generate a private address.

    Of primary interest in this paper is the LTK. CSRK and IRK are covered briefly at the end.

Bluetooth low energy uses the same pairing process as Classic *Bluetooth*: Secure Simple Pairing (SSP). During SSP initially each device determines its capability for input and output (IO). The input can be None, Yes/No, or Keyboard with Keyboard having the ability to input a number. The output can be either None or Display with Display having the ability to display a 6-digit number. For each device in a paring link the IO capability determines their ability to create encryption shared secret keys.

The Pairing Request message is transmitted from the initiator containing the IO capabilities, authentication data availability, authentication requirements, key size requirements, and other data. A Pairing Response message is transmitted from the responder and contains much of the same information as the initiators Pairing Request message thus confirming that a pairing is successfully negotiated.

In the sample SMP decode, in the figure at the right, note the “keys” identified. Creating a shared, secret key is an evolutionary process that involves several intermediary keys. The resulting keys include,

1. IRK: 128-bit key used to generate and resolve random address.
2. CSRK: 128-bit key used to sign data and verify signatures on the receiving device.
3. LTK: 128-bit key used to generate the session key for an encrypted connection.
4. Encrypted Diversifier (EDIV): 16-bit stored value used to identify the LTK. A new EDIV is generated each time a new LTK is distributed.
5. Random Number (RAND): 64-bit stored value used to identify the LTK. A new RAND is generated each time a unique LTK is distributed.

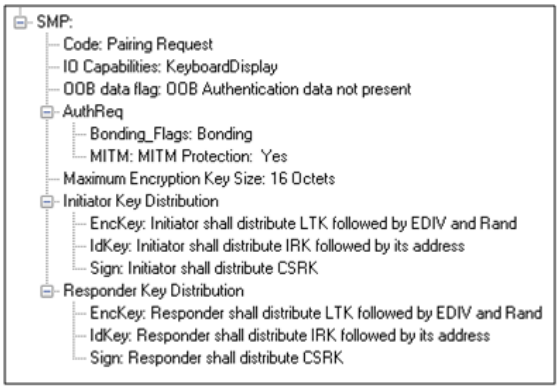


Figure 12 - Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

Of particular importance to decrypting the encrypted data on a *Bluetooth* low energy link is LTK, EDIV, and RAND.

B.3.3 Pairing Methods

The two devices in the link use the IO capabilities from Pairing Request and Pairing Response packet data to determine which of two pairing methods to use for generation of the Temporary Key (TK). The two methods are **Just Works** and **Passkey Entry**[1]. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

In **Just Works** the TK = 0. In the **Passkey Entry** method,

$$TK = \begin{cases} \text{6 numeric digits, Input} = \text{Keyboard} \\ \text{6 random digits, Input} = \text{Display} \end{cases}$$

Figure 13 - Initiator Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

[1]A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link such as NFC.

```
SMP:
    Code: Pairing Confirm
    Confirm Value: 0x7fc2569e13e92125798a45a64256208a
```

Figure 14 - Responder Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

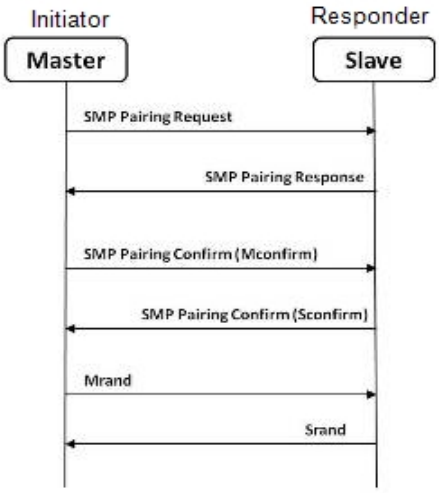


Figure 15 - Message Sequence Chart: SMP Pairing

The initiating device will generate a 128-bit random number that is combined with TK, the Pairing Request command, the Pairing Response command, the initiating device address and address type, and the responding device address and address type. The resulting value is a random number **Mconfirm** that is sent to the responding device by the Pairing Confirm command. The responding device will validate the responding device data in the Pairing Confirm command and if it is correct will generate a **Sconfirm** value using the same methods as used to generate **Mconfirm** only with different 128-bit random number and TK. The responding device will send a Pairing Confirm command to the initiator and if accepted the authentication process is complete. The random number in the **Mconfirm** and **Sconfirm** data is **Mrand** and **Srand** respectively. **Mrand** and **Srand** have a key role in setting encrypting the link.

Finally the master and slave devices exchange **Mrand** and **Srand** so that the slave can calculate and verify Mconfirm and the master can likewise calculate and verify Sconfirm.

B.3.4 Encrypting the Link

The Short Term Key (STK) is used for encrypting the link the first time the two devices pair. STK remains in each device on the link and is not transmitted between devices. STK is formed by combining **Mrand** and **Srand** which were formed using device information and TKs exchanged with Pairing Confirmation (**Pairing Confirm**).

B.3.5 Encryption Key Generation and Distribution

```
LE LL:
    Control Pkt: LL_ENC_REQ
    Random vector (Rand): 0x277c02fb155129d9
    Encrypted diversifier (EDIV): 0x838e
    Master session key identifier (SKDm): 0x21db67dd0f57d32a
    Master initialization vector (IVm): 0x034efc39
```

Figure 16 - Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

To distribute the LTK, EDIV, and Rand values an encrypted session needs to be set up. The initiator will use STK to enable encryption on the link. Once an encrypted link is set up, the LTK is distributed. LTK is a 128-bit random number that the slave device will generate along with EDIV and Rand. Both the master and slave devices can distribute these numbers, but *Bluetooth* low energy is designed to conserve energy, so the slave device is often resource constrained and does not have the database storage resources for holding LTKs. Therefore the slave will distribute LTK, EDIV, and Rand to the master device for storage. When a slave begins a new encrypted session with a previously linked master device, it will request distribution of EDIV and Rand and will regenerate LTK.

Figure 17 - Encryption Response from Slave, Example
(ComProbe Frame Display, BPA 600 low energy capture)

B.3.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the master device to send Link Layer encryption request message (LL_ENC_REQ) that contains the SKD_{master}. The SKD_{master} is generated using the LTK. The slave receives SKD_{master}, generates SKD_{slave}, and generates SK by concatenating parts of SKD_{master} and SKD_{slave}. The slave device responds with an encryption response message (LL_ENC_RSP) that contains SKD_{slave}; the master will create the same SK.

Now that a SK has been calculated, the master and slave devices will now begin a handshake process. The slave will transmit unencrypted LL_START_ENC_REQ, but sets the slave to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_ENC_RSP that uses the same SK just calculated and setting the master to receive encrypted data. Once the slave receives the master's encrypted LL_START_ENC_RSP message and responds with an encrypted LL_START_ENC_RSP message the *Bluetooth* low energy devices can now begin transmitting and receiving encrypted data.

B.3.7 Decrypting Encrypted Data Using Frontline® BPA 600 low energy Capture

Note: The following discussion uses the ComProbe BPA 600 in low energy capture mode to illustrate how to identify the encryption process and to view decrypted data. However any of the ComProbe devices (BPA 500, BPA low energy) that are low energy capable will accomplish the same objectives, although the datasource setup will be slightly different for each device.

B.3.7.1 Setting up the BPA 600

1. Run the ComProbe Protocol Analysis Software and select **Bluetooth Classic/low energy (BPA 600)**. This will bring up the **BPA 600 datasource** window. This is where the parameters are set for sniffing, including the devices to be sniffed and how the link is to be decrypted.

2. Select **Devices Under Test** tab on the Datasource window.

3. Click/select **LE Only**.

4. To decrypt encrypted data transmissions between the *Bluetooth* low energy devices the ComProbe analyzer needs to know the LTK because this is the shared secret used to encrypt the session. There are two ways to provide this information and which to select will depend on the pairing method: **Just Works** or **Passkey Entry**.

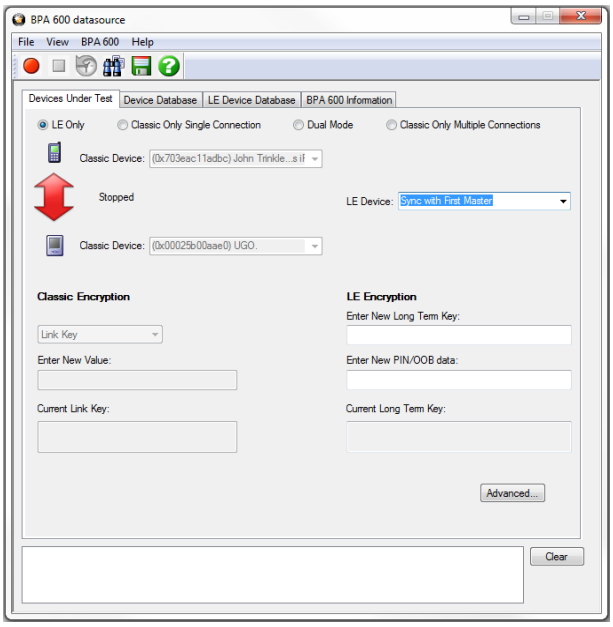


Figure 18 - ComProbe BPA 600 low energy only datasource settings

   a. **Passkey Entry** is easiest if you have the code that was displayed or entered during device pairing. The code is what is used to generate the LTK. Under **LE Encryption** enter the code in the **Enter New PIN/OOB** data text box.

   b. **Just Works** is more of a challenge because you must know the LTK that is created at the time of pairing and identification of an encrypted link.

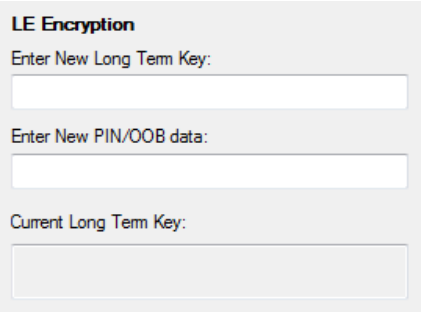


Figure 19 - BPA 600 datasource Encryption Key Entry

   - If your device was previously used in an encrypted capture session, the device information including LTK can be found in the **Device Database** tab.

   - In a design and development environment the LTK is often known beforehand.

   - Capture of Host Controller Interface (HCI) events using ComProbe HSU can reveal the LTK, which is contained in the HCI_Link_Key_Request_Reply command. HCI capture is through direct connection to the device host controller. The information obtained in a direct connection can later be used in a wireless encrypted capture session that requires prior knowledge of encryption keys.

5. To start capture click on the Start Sniffing button on the **BPA 600 datasource** toolbar.

B.3.7.2 Use Frame Display to View Encryption/Decryption Process

B.3.7.2.1 Security Manager Protocol

The Security Manager Protocol (SMP) controls the process for pairing and key distribution. The results of a pairing and key distribution can be observed in the ComProbe software **Frame Display**. Activate the **Frame Display** by clicking on the icon on the **Control** window toolbar. On the **Frame Display** low energy protocols are shown in light green tabs. Click on the **SMP** protocol tab that will show only the SMP commands from the full data set.

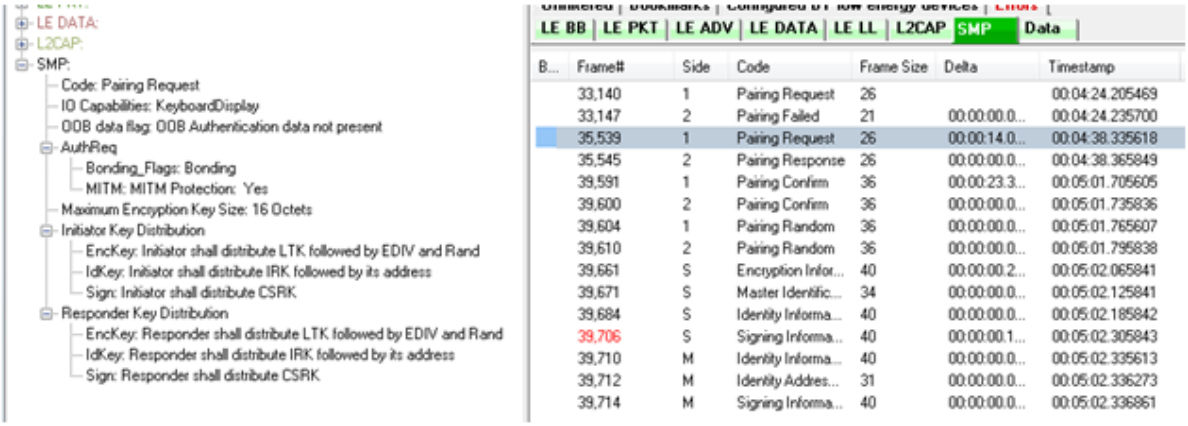


Figure 20 - SMP Pairing Request (Frame# 35,539) from Initiator (Side 1)

On the left side of the figure above is the **Frame Display Decode**r pane that shows the decoded information supplied in the selected frame in the Summary pane, Frame# 35,539. Shown is the SMP data associated with and encrypted link (MITM Protection = Yes). The requested keys are also shown. Selecting Frame# 35,545 would provide the response from the responder (Side 2) and would contain similar information.

Selecting Frame# 39,591 will display the Pairing Confirm from the initiator (Side 1) in the **Decoder** pane. The Confirm Value shown is the Mconfirm 128-bit random number that contains TK, Pairing Request command, Pairing Response command, initiating device address, and the responding device address. Selecting Frame# 39,600 would provide the Sconfirm random number from the responder (Side 2) with similar information from that device but the random number would be different than Mconfirm.

Once pairing is complete and an encrypted session established, the keys are distributed by the master and slave now identified by Side = M and Side = S respectively in the **Summary** pane. In Frame# 39,661 the slave has distributed LTK to the master to allow exchange of encrypted data. Frame# 39,661 through 39,714 in the Summary pane SMP tab are the key distribution frames.

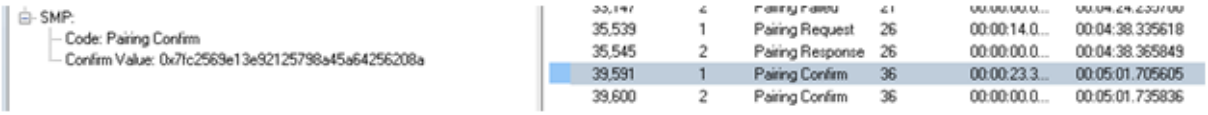


Figure 21 - SMP Pairing Confirm (Frame# 39,591) from Initiator (Side 1)

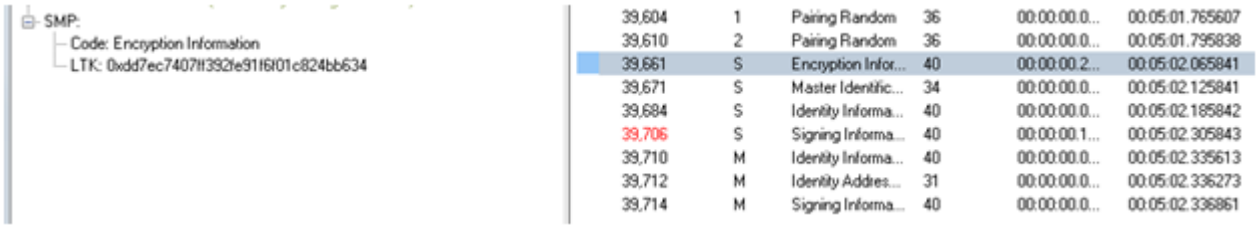


Figure 22 - SMP Key Distribution Frames

B.3.7.2.2 Link Layer

The Link Layer (LL) protocol manages the *Bluetooth* low energy radio transmissions and is involved in starting link encryption. To observe the decoded LL commands, click on the **Frame Display LE LL** tab, search for and select ControlPkt "LL_ENC_REQ". This command should originate with Side 1, the initiator of the encryption link. In Figure 11 Frame# 39,617 is selected in the Summary pane and we see the decoded LE LL frame is display in the **Decoder** pane. Shown in this frame packet is the SKDm that is the Master Session Key Diversifier (SKDmaster). In Frame# 39,623 you will find SKDslave that is combined with SKDmaster to create the Session Key (SK). Both SDKs were created using the LTK. Frame# 39,635 through 39,649 in the **LE LL** tab completes starting of the encryption process. After the slave sends LL_START_ENC_RSP (Frame# 36,649) the *Bluetooth* devices can exchange encrypted data, and the ComProbe sniffing device can also receive and decrypt the encrypted data because the appropriate "key" is provided in the **BPA 600 Datasource** window.

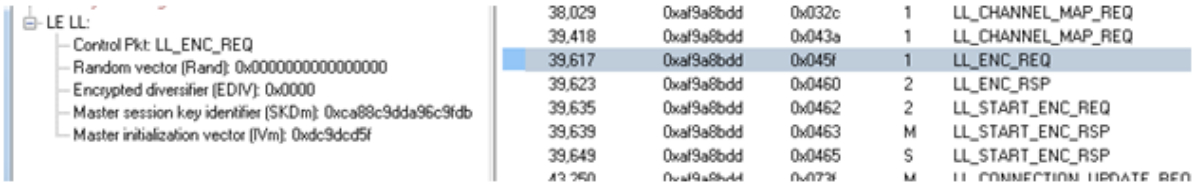


Figure 23 - LE LL Tab Encryption Request (Frame# 39,617) from Initiator (Side 1)

B.3.7.3 Viewing Encryption in the Message Sequence Chart

The ComProbe software **Message Sequence Chart** (**MSC**) links directly to frames being viewed in the Frame Display. Similarly MSC will display the same information as the **Frame Display Decoder** pane. Frames are synchronized between the **Frame Display Summary** pane and the **MSC**, so clicking on a frame in either window will select that same frame in the other window. Also the protocol tabs are the same in each window. To see the pairing process, click on the SMP tab.

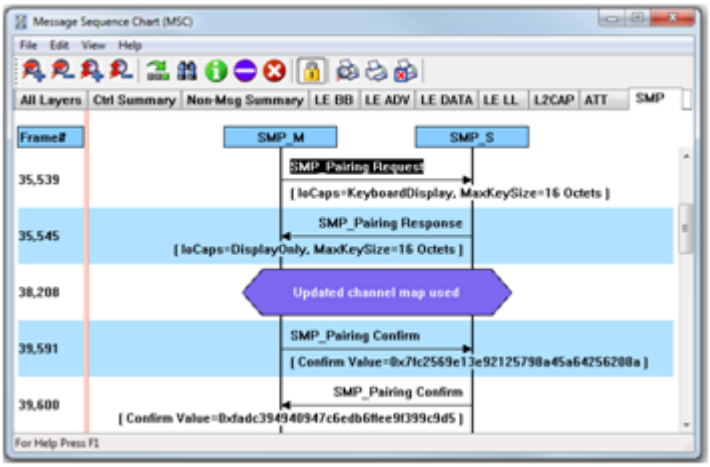


Figure 24 - MSC SMP Paring (BPA 600 low energy capture)

In the image above we see Frame# 35,539 initiating the pairing from the master device. The response, SMP_ Pairing Response, is sent from the slave in Frame# 35,545. SMP_Pairing Confirm occurs between the master and the slave devices at Frame# 39,591 and 39,600 respectively.

Clicking on the **MSC** LE LL tab will show the process of encrypting a session link. Clicking on Frame# 39,617 displays the LL_ENC_REQ command from the master to the slave. In the **MSC** below this command you will see the data transferred that includes SKD_{master} used to generate the LTK. At Frame# 39,623 the slave responds with LL_ENC_RSP sending SKD_{slave} to generate LTK at the master. Up to this point all transmissions are unencrypted. For this example the slave sends the request to start encryption, LL_START_ENC_REQ, at Frame#39,635. The master responds with LL_START_ENC_RSP at Frame# 39,639, and finally the slave responds with LL_START_ENC_RSP at Frame# 36,649. At this point the session link is encrypted.

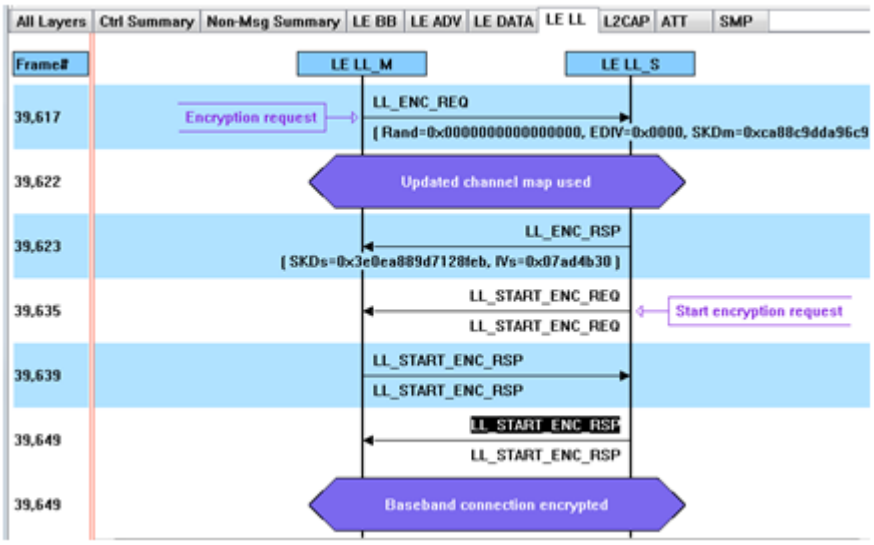


Figure 25 - MSC link Layer Encryption (BPA 600 low energy capture)

B.3.7.4 Viewing Decrypted Data

In the ComProbe software **Frame Display** click on the **LE BB** tab. Search in the **Summary** pane for Decryption Initiated = Yes frames. In the example depicted in the following figure, Frame# 39723 is selected. In the **Decoder** pane LE BB shows that the decryption was initiated and decryption was successful. In LE Data we see the Encrypted MIC value. The MIC value is used to authenticate the sender of the data packet to ensure that the data was sent by a peer device in the link and not by a third party attacker. The actual decrypted data appears between the Payload Length and the MIC in the packet. This is shown in the **Binary** pane below the **Summary** pane.

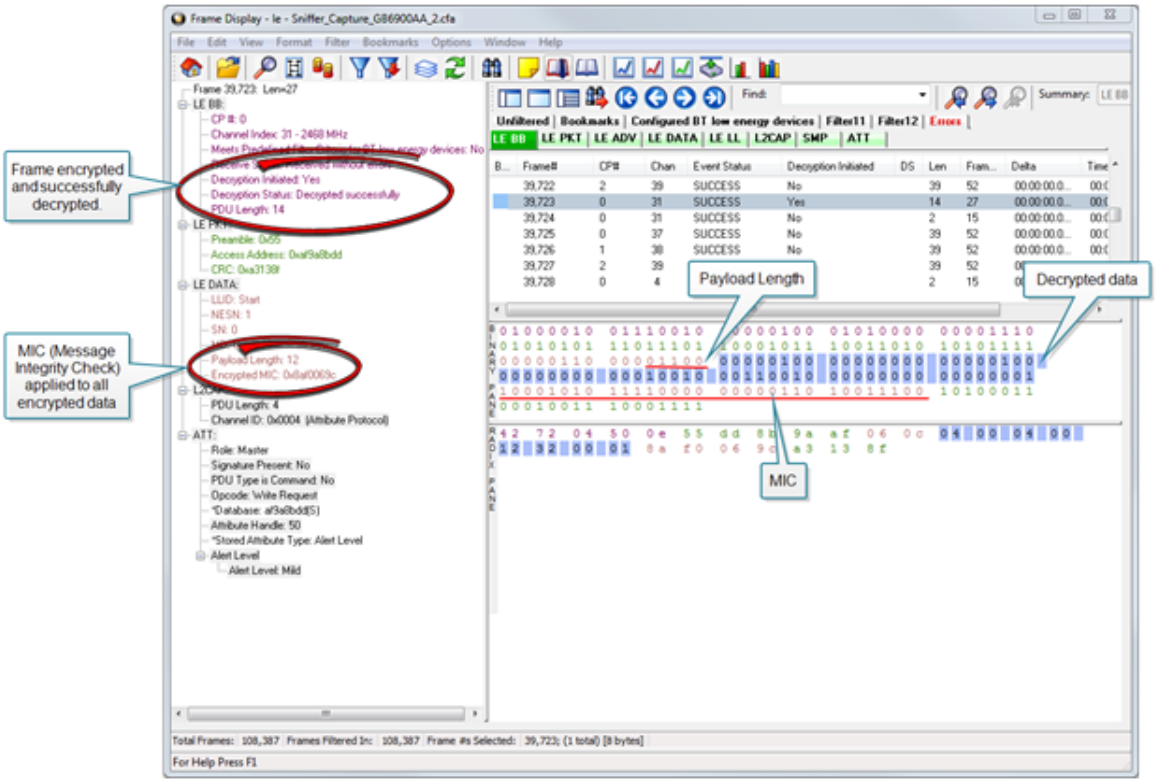


Figure 26 - Decrypted Data Example (Frame# 39,723)

Author: John Trinkle

Publish Date: 9 April 2014

Revised: 23 May 2014

B.4 Bluetooth® low energy Security

"Paris is quiet and the good citizens are content." Upon seizing power in 1799 Napoleon sent this message on Claude Chappe's optical telegraph. Chappe had invented a means of sending messages line-of-sight . The stations were placed approximately six miles apart and each station had a signaling device made of paddles on the ends of a rotating "regulator" arm whose positions represented code numbers. Each station was also outfitted with two telescopes for viewing the other stations in the link, and clocks were used to synchronize the stations. By 1803 a communications network extended from Paris across the countryside and into Belgium and Italy.

Figure 27 - Chappe's Optical Telegraph

Chappe developed several coding schemes through the next few years. The station operators only knew the codes, not what characters they represented. Not only was Chappe's telegraph system the first working network with protocols, synchronization of serial transmissions but it also used data encryption. Although cryptography has been around for millenniums—dating back to 2000 B.C. — Chappe, was the first to use it in a wide area network in the modern sense.

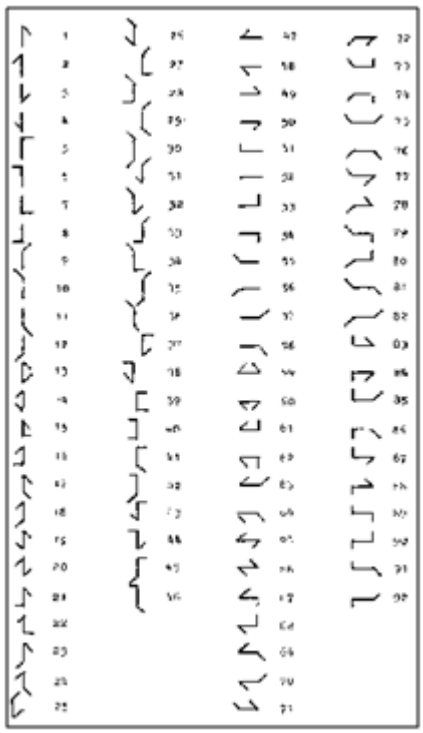


Figure 28 - Chappe's Telegraph Code

Of course anyone positioned between the telegraph stations that had Chappe's telegraph code in hand could decode the transmission. So securing the code was of paramount importance in Chappe's protocol.

Modern wireless networks such as *Bluetooth* low energy employ security measures to prevent similar potentially man-in-the-middle attacks that may have malicious intent.

Bluetooth low energy devices connected in a link can pass sensitive data by setting up a secure encrypted link. The process is similar to but not identical to *Bluetooth* BR/EDR Secure Simple Pairing. One difference is that in *Bluetooth* low energy the confidential payload includes a Message Identification Code (MIC) that is encrypted with the data. In *Bluetooth* BR/EDR only the data is encrypted. Also in Bluetooth low energy the secure link is more vulnerable to passive eavesdropping, however because of the short transmission periods this vulnerability is considered a low risk. The similarity to BR/EDR occurs with "shared secret key", a fundamental building block of modern wireless network security.

This paper describes the process of establishing a *Bluetooth* low energy secure link.

B.4.1 How Encryption Works in *Bluetooth* low energy

Data encryption is used to prevent passive and active—man-in-the-middle (MITM) — eavesdropping attacks on a *Bluetooth* low energy link. Encryption is the means to make the data unintelligible to all but the *Bluetooth* master and slave devices forming a link. Eavesdropping attacks are directed on the over-the-air transmissions between the *Bluetooth* low energy devices, so data encryption is accomplished prior to transmission using a shared, secret key.

B.4.2 Pairing

A *Bluetooth* low energy device that wants to share secure data with another device must first pair with that device. The Security Manager Protocol (SMP) carries out the pairing in three phases.

1. The two connected *Bluetooth* low energy devices announce their input and output capabilities and from that information determine a suitable method for phase 2.
2. The purpose of this phase is to generate the Short Term Key (STK) used in the third phase to secure key distribution. The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.
3. In this phase each device may distribute to the other device up to three keys:
    a. the Long Term Key (LTK) used for Link Layer encryption and authentication,
    b. the Connection Signature Resolving Key (CSRK) used for data signing at the ATT layer, and
    c. the Identity Resolving Key (IRK) used to generate a private address.

    Of primary interest in this paper is the LTK. CSRK and IRK are covered briefly at the end.

Bluetooth low energy uses the same pairing process as Classic *Bluetooth*: Secure Simple Pairing (SSP). During SSP initially each device determines its capability for input and output (IO). The input can be None, Yes/No, or

Keyboard with Keyboard having the ability to input a number. The output can be either None or Display with Display having the ability to display a 6-digit number. For each device in a paring link the IO capability determines their ability to create encryption shared secret keys.

The Pairing Request message is transmitted from the initiator containing the IO capabilities, authentication data availability, authentication requirements, key size requirements, and other data. A Pairing Response message is transmitted from the responder and contains much of the same information as the initiators Pairing Request message thus confirming that a pairing is successfully negotiated.

In the sample SMP decode, in the figure at the right, note the "keys" identified. Creating a shared, secret key is an evolutionary process that involves several intermediary keys. The resulting keys include,

1. IRK: 128-bit key used to generate and resolve random address.
2. CSRK: 128-bit key used to sign data and verify signatures on the receiving device.
3. LTK: 128-bit key used to generate the session key for an encrypted connection.
4. Encrypted Diversifier (EDIV): 16-bit stored value used to identify the LTK. A new EDIV is generated each time a new LTK is distributed.
5. Random Number (RAND): 64-bit stored value used to identify the LTK. A new RAND is generated each time a unique LTK is distributed.

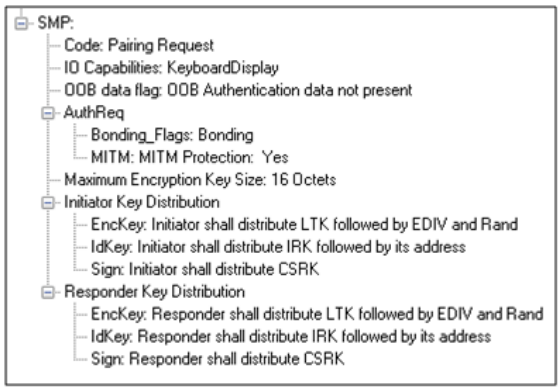


Figure 29 - Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

Of particular importance to decrypting the encrypted data on a *Bluetooth* low energy link is LTK, EDIV, and RAND.

B.4.3 Pairing Methods

The two devices in the link use the IO capabilities from Pairing Request and Pairing Response packet data to determine which of two pairing methods to use for generation of the Temporary Key (TK). The two methods are **Just Works** and **Passkey Entry**[1]. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

In **Just Works** the TK = 0. In the **Passkey Entry** method,

$$TK = \begin{cases} \text{6 numeric digits, Input} = \text{Keyboard} \\ \text{6 random digits, Input} = \text{Display} \end{cases}$$

Figure 30 - Initiator Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

[1]A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link such as NFC.

```
SMP:
  Code: Pairing Confirm
  Confirm Value: 0x7fc2569e13e92125798a45a64256208a
```

Figure 31 - Responder Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

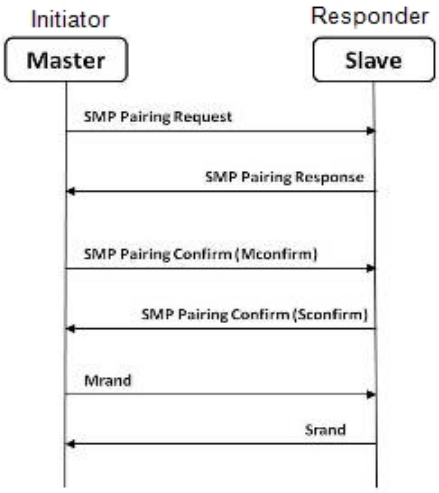


Figure 32 - Message Sequence Chart: SMP Pairing

The initiating device will generate a 128-bit random number that is combined with TK, the Pairing Request command, the Pairing Response command, the initiating device address and address type, and the responding device address and address type. The resulting value is a random number **Mconfirm** that is sent to the responding device by the Pairing Confirm command. The responding device will validate the responding device data in the Pairing Confirm command and if it is correct will generate a **Sconfirm** value using the same methods as used to generate **Mconfirm** only with different 128-bit random number and TK. The responding device will send a Pairing Confirm command to the initiator and if accepted the authentication process is complete. The random number in the **Mconfirm** and **Sconfirm** data is **Mrand** and **Srand** respectively. **Mrand** and **Srand** have a key role in setting encrypting the link.

Finally the master and slave devices exchange **Mrand** and **Srand** so that the slave can calculate and verify Mconfirm and the master can likewise calculate and verify Sconfirm.

B.4.4 Encrypting the Link

The Short Term Key (STK) is used for encrypting the link the first time the two devices pair. STK remains in each device on the link and is not transmitted between devices. STK is formed by combining **Mrand** and **Srand** which were formed using device information and TKs exchanged with Pairing Confirmation (**Pairing Confirm**).

B.4.5 Encryption Key Generation and Distribution

```
LE LL:
  Control Pkt: LL_ENC_REQ
  Random vector (Rand): 0x277c02fb155129d9
  Encrypted diversifier (EDIV): 0x838e
  Master session key identifier (SKDm): 0x21db67dd0f57d32a
  Master initialization vector (IVm): 0x034efc39
```

Figure 33 - Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

To distribute the LTK, EDIV, and Rand values an encrypted session needs to be set up. The initiator will use STK to enable encryption on the link. Once an encrypted link is set up, the LTK is distributed. LTK is a 128-bit random number that the slave device will generate along with EDIV and Rand. Both the master and slave devices can distribute these numbers, but *Bluetooth* low energy is designed to conserve energy, so the slave device is often resource constrained and does not have the database storage resources for holding LTKs. Therefore the slave will distribute LTK, EDIV, and Rand to the master device for storage. When a slave begins a new encrypted session with a previously linked master device, it will request distribution of EDIV and Rand and will regenerate LTK.

Figure 34 - Encryption Response from Slave, Example
(ComProbe Frame Display, BPA 600 low energy capture)

B.4.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the master device to send Link Layer encryption request message (LL_ENC_REQ) that contains the SKD_{master}. The SKD_{master} is generated using the LTK. The slave receives SKD_{master}, generates SKD_{slave}, and generates SK by concatenating parts of SKD_{master} and SKD_{slave}. The slave device responds with an encryption response message (LL_ENC_RSP) that contains SKD_{slave}; the master will create the same SK.

Now that a SK has been calculated, the master and slave devices will now begin a handshake process. The slave will transmit unencrypted LL_START_ENC_REQ, but sets the slave to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_ENC_RSP that uses the same SK just calculated and setting the master to receive encrypted data. Once the slave receives the master's encrypted LL_START_ENC_RSP message and responds with an encrypted LL_START_ENC_RSP message the *Bluetooth* low energy devices can now begin transmitting and receiving encrypted data.

B.4.7 IRK and CSRK Revisited

Earlier in this paper it was stated that LTK would be the focus, however the IRK and CSRK were mentioned. We revisit these keys because they are used in situations that require a lesser level of security. First let us note that IRK and CSRK are passed in an encrypted link along with LTK and EDIV.

Use of the IRK and CSRK attempt to place an identity on devices operating in a piconet. The probability that two devices will have the same IRK and generate the same random number is low, but not absolute.

IRK and *Bluetooth* low energy Privacy Feature

Bluetooth low energy has a feature that reduces the ability of an attacker to track a device over a long period buy frequently and randomly changing an advertising device's address. This is the privacy feature. This feature is not used in the discovery mode and procedures but is used in the connection mode and procedures.

If the advertising device was previously discovered and has returned to an advertising state, the device must be identifiable by trusted devices in future connections without going through discovery procedure again. The IRK stored in the trusted device will overcome the problem of maintaining privacy while saving discovery computational load and connection time. The advertising devices IRK was passed to the master device during initial bonding. The a master device will use the IRK to identify the advertiser as a trusted device.

CSRK and Signing for Authentication

Bluetooth low energy supports the ability to authenticate data sent over an unencrypted ATT bearer between two devices in a trust relationship. If authenticated pairing has occurred and encryption is not required (security mode 2) data signing is used if CSRK has been exchanged. The sending device attaches a digital signature after the data in the packet that includes a counter and a message authentication code (MAC). The key used to generate MAC is CSRK. Each peer device in a piconet will have a unique CSRK.

The receiving device will authenticate the message from the trusted sending device using the CSRK exchanged from the sending device. The counter is initialized to zero when the CSRK is generated and is incremented with each message signed with a given CSRK. The combination of the CSRK and counter mitigates replay attacks.

B.4.8 Table of Acronyms

CSRK	Connection Signature Resolving Key
EDIV	Encrypted Diversifier
IO	Input and output
IRK	Identity Resolving Key
LTK	Long Term Key
Mconfirm	128-bit confirm value from initiator
MIC	Message Integrity Check
MITM	Man-in-the-middle
Mrand	128-bit random number used to generate Mconfirm
OOB	Out of Band
RAND	Random Number
Sconfirm	128-bit confirmation value from the responder
SK	Session key
SMP	Security Manager Protocol
Srand	128-bit random number used to generate Sconfirm
SSP	Secure Simple Pairing
STK	Short Term Key
TK	Temporary Key

Author: John Trinkle

Publish Date:21 May 2014

B.5 Bluetooth Virtual Sniffing

B.5.1 Introduction

The ComProbe software Virtual sniffing function simplifiesBluetooth® 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.

B.5.2 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.

B.5.3 *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.

B.5.4 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.

B.5.5 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.

B.5.6 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.

B.5.7 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.

B.5.8 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.

B.5.9 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.

Author: Eric Kaplan

Publish Date: May 2003

Revised: December 2013

Index

F

G

H

I