TELEDYNE LECROY
Everywhereyoulook™

frontline SODERA™

WIDEBAND *BLUETOOTH*® PROTOCOL ANALYZER

Hardware and Software User Manual

ProbeSync

ES™
Audio Expert System

Revision Date: 3/16/2017

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.

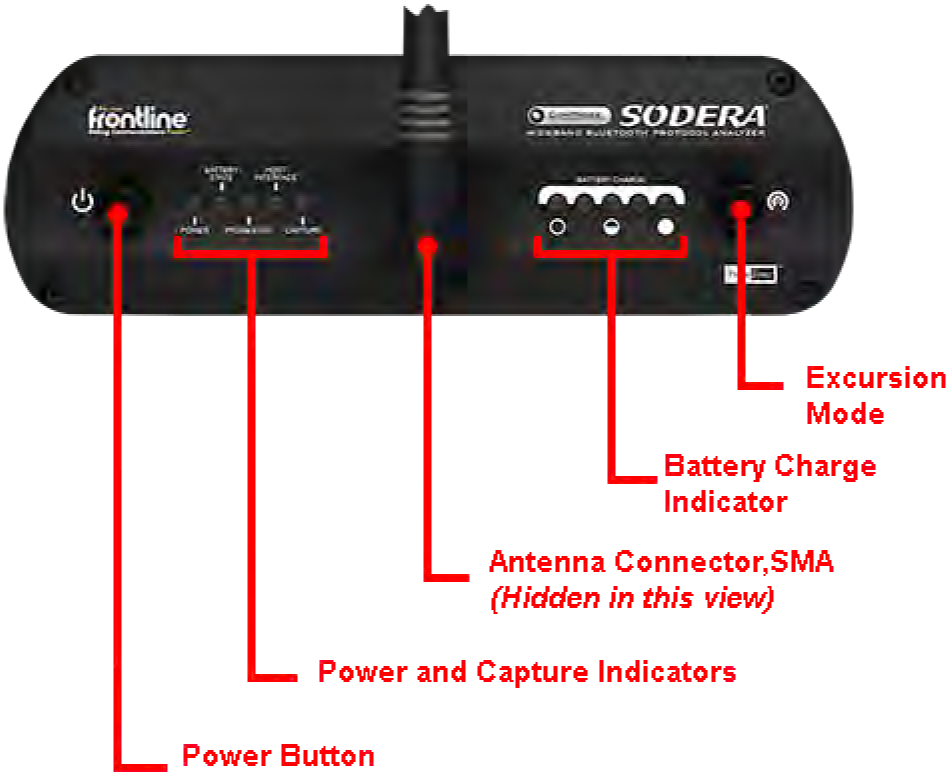


Figure 2.1 - Sodera Front Panel Controls and Indicators

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.

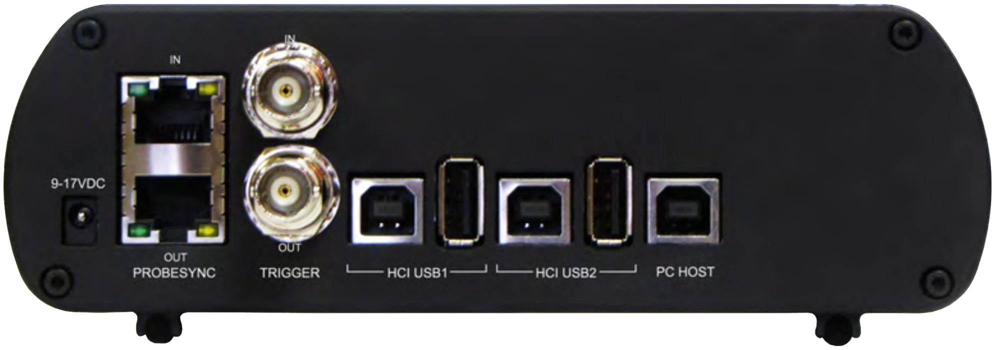


Figure 2.2 - Sodera Rear Panel Connectors

+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

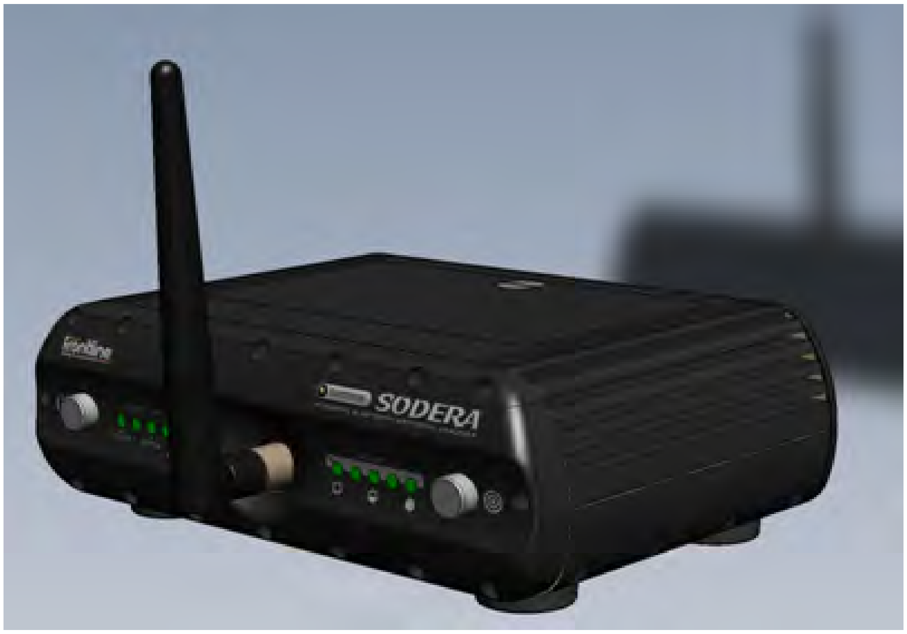


Figure 2.3 - Antenna Attachment Point

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.

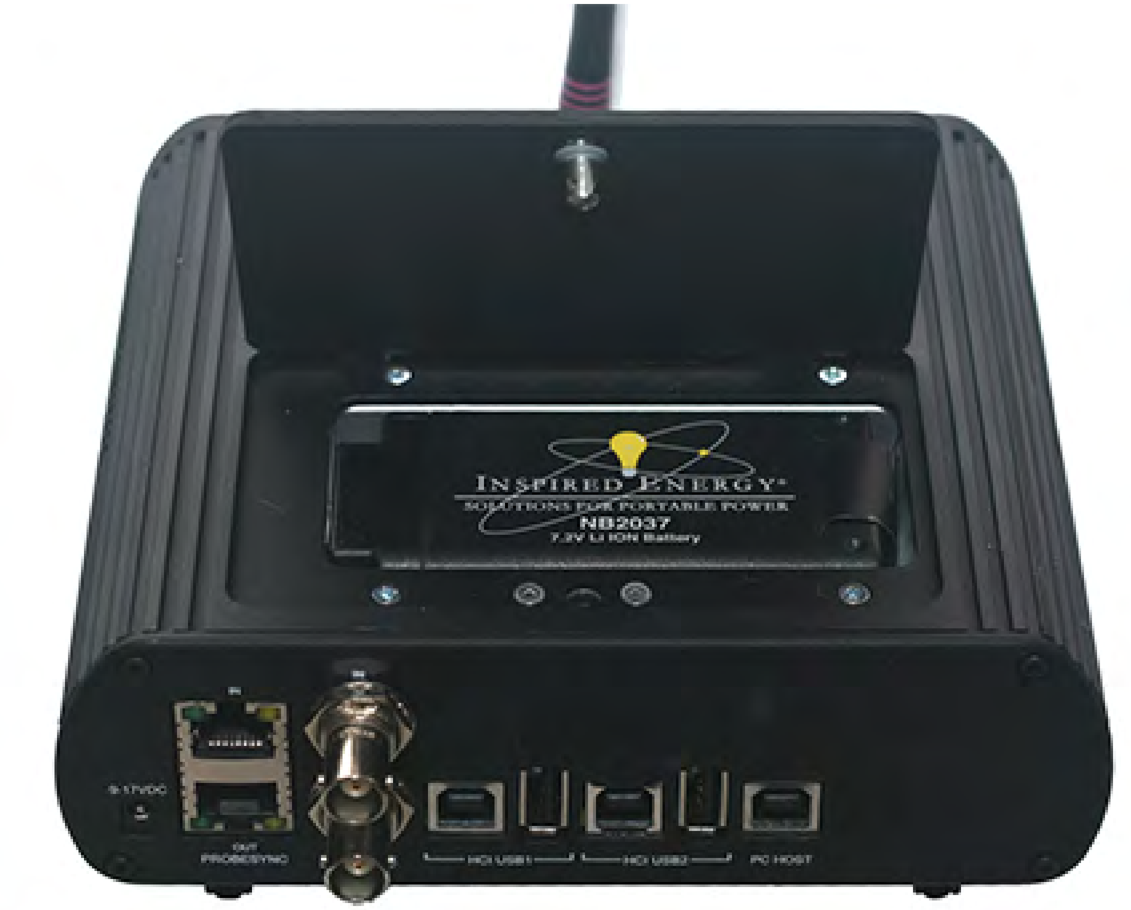


Figure 2.4 - Sodera Battery Compartment with Cover Opened

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.

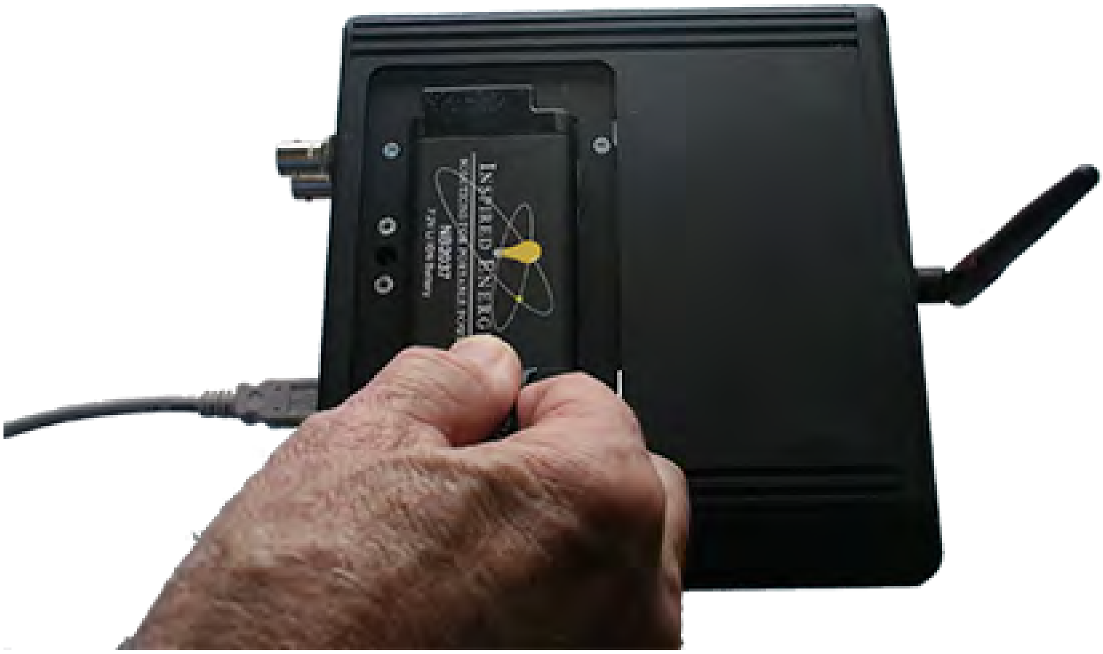


Figure 2.5 - Sodera Battery Removal Using the Tab

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.

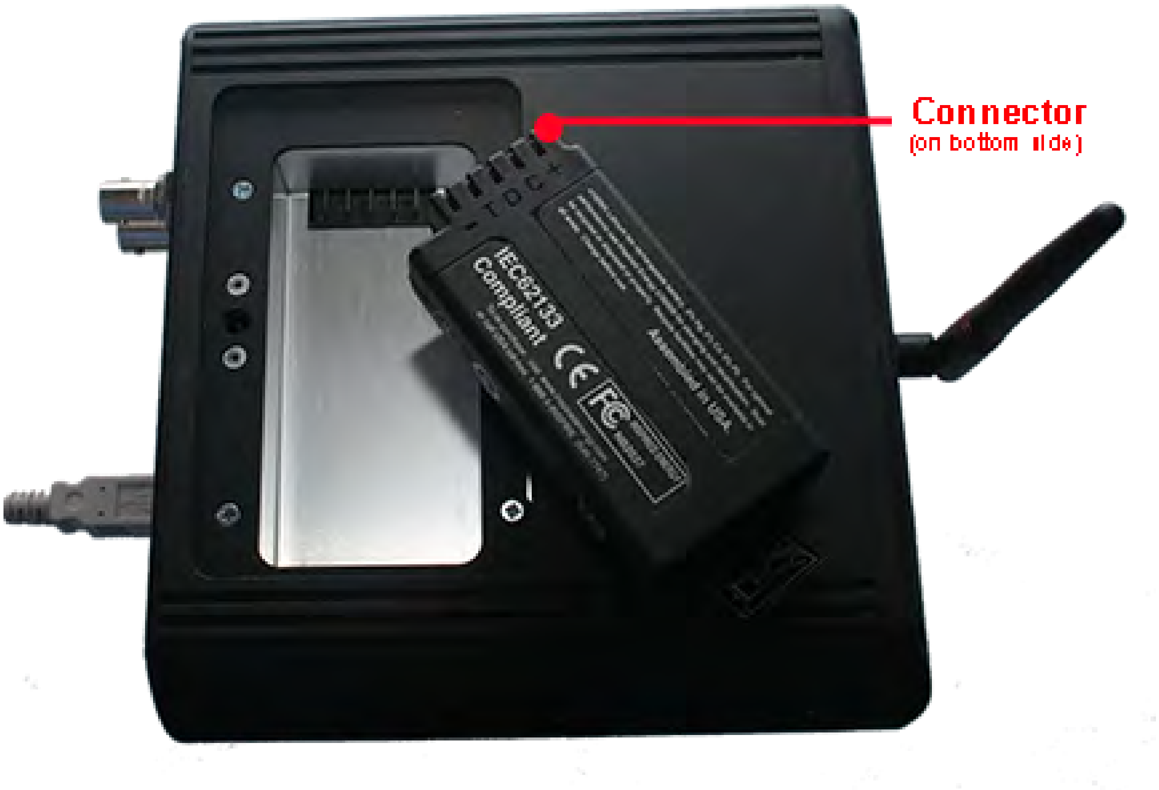


Figure 2.6 - Sodera Battery Connectors, bottom side shown.

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.

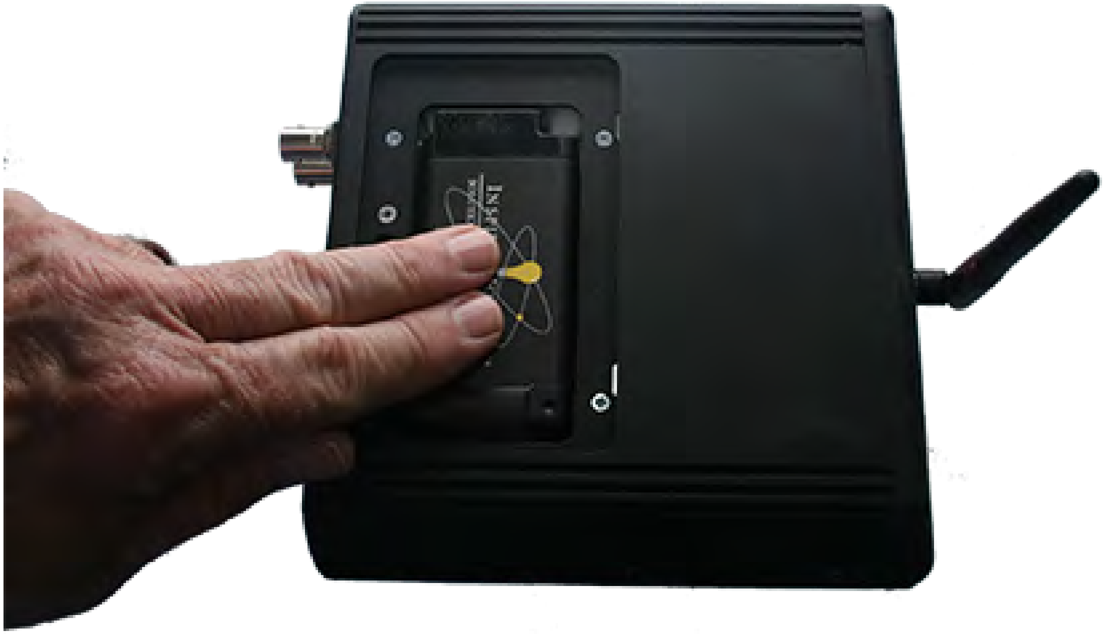


Figure 2.7 - Sodera Battery: Press to Make Contact

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.

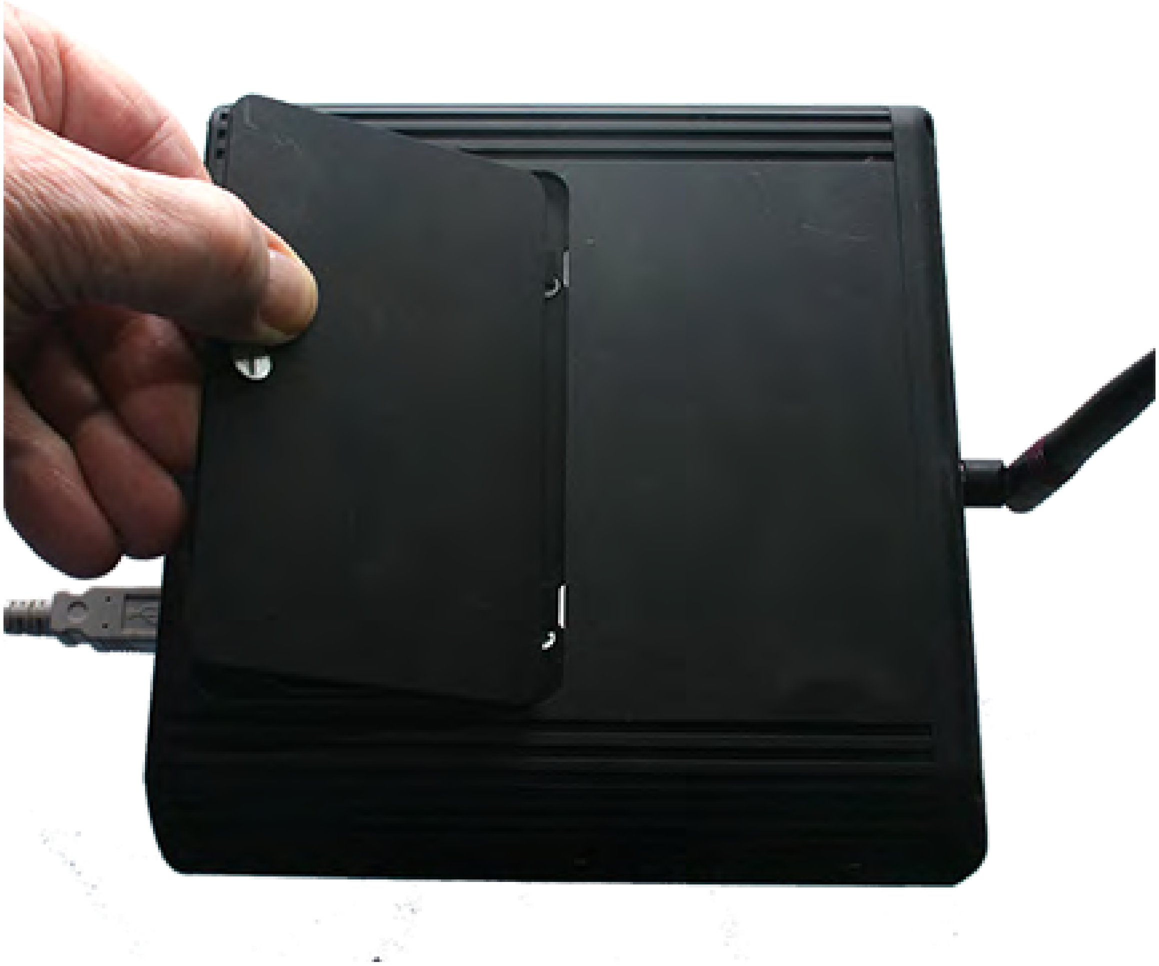
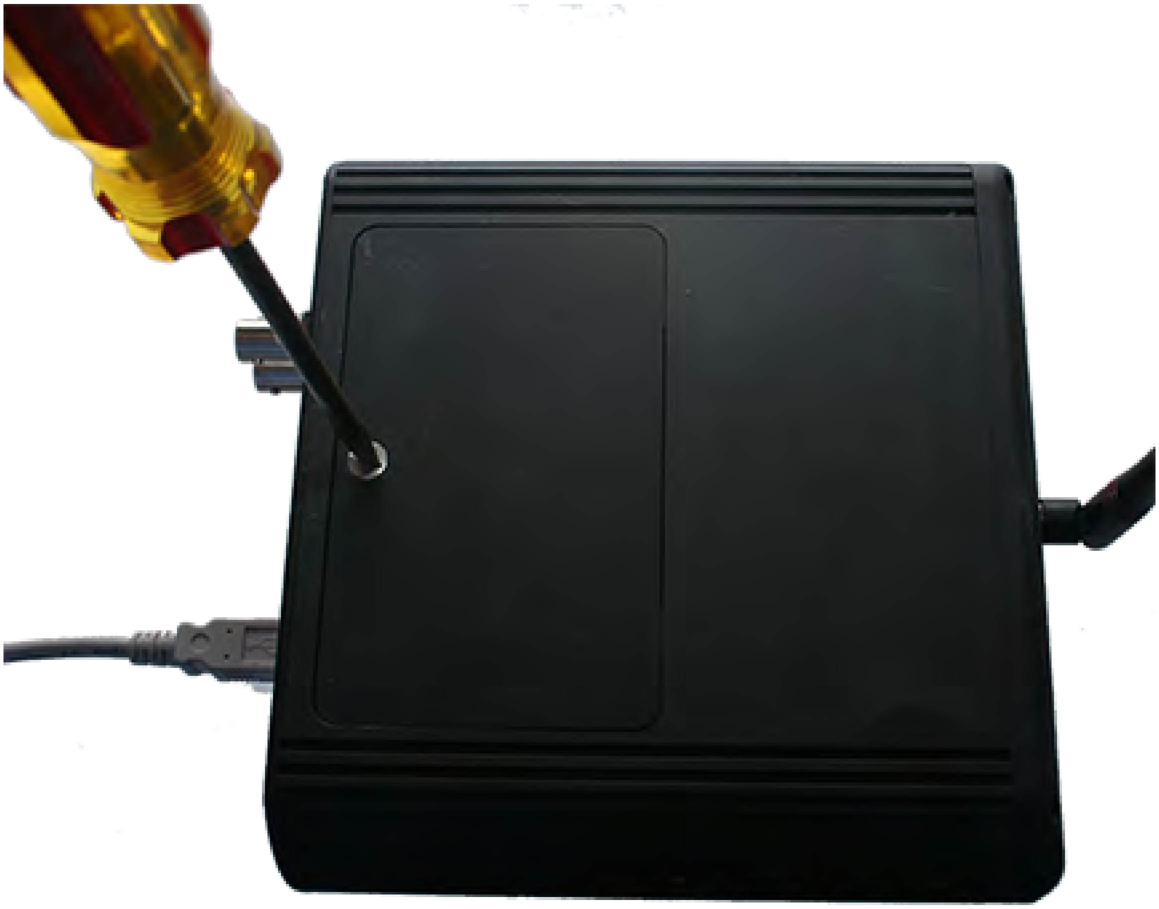


Figure 2.8 - Sodera Battery Cover: Insert Tabs



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.

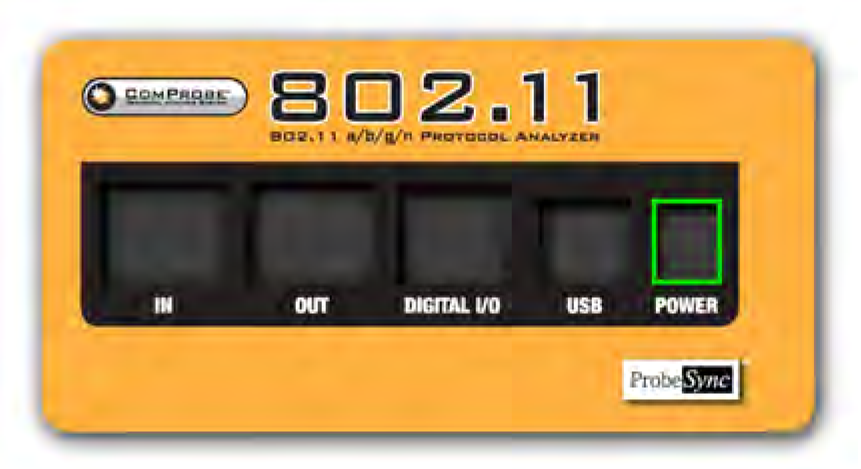


Figure 2.9 - ComProbe 802.11 Back Panel

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**.

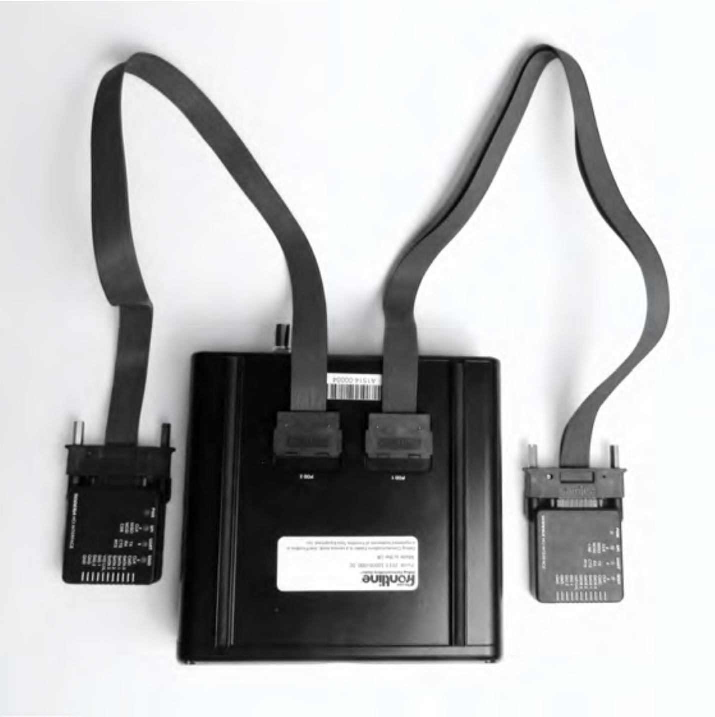


Figure 2.10 - HCI Pods Installed on Sodera

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

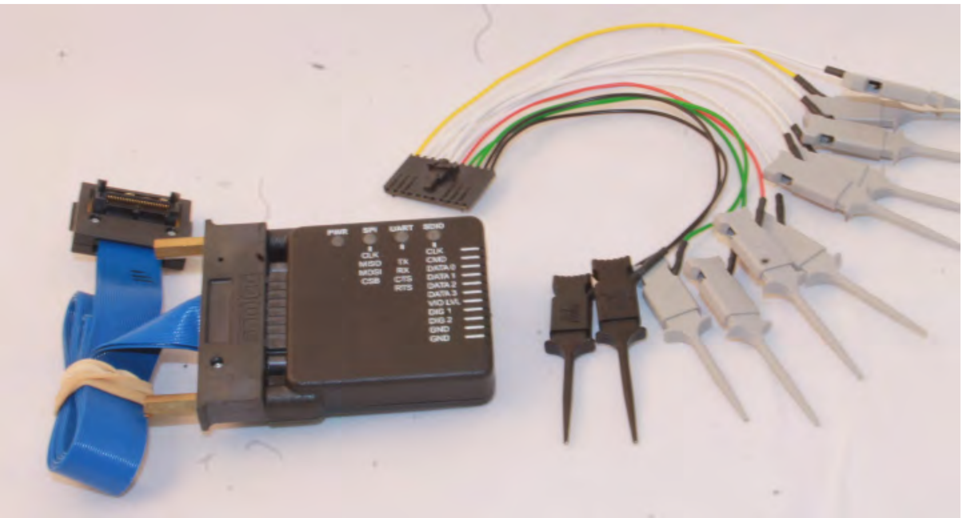


Figure 2.11 - HCI Pod with Flying Lead Assembly

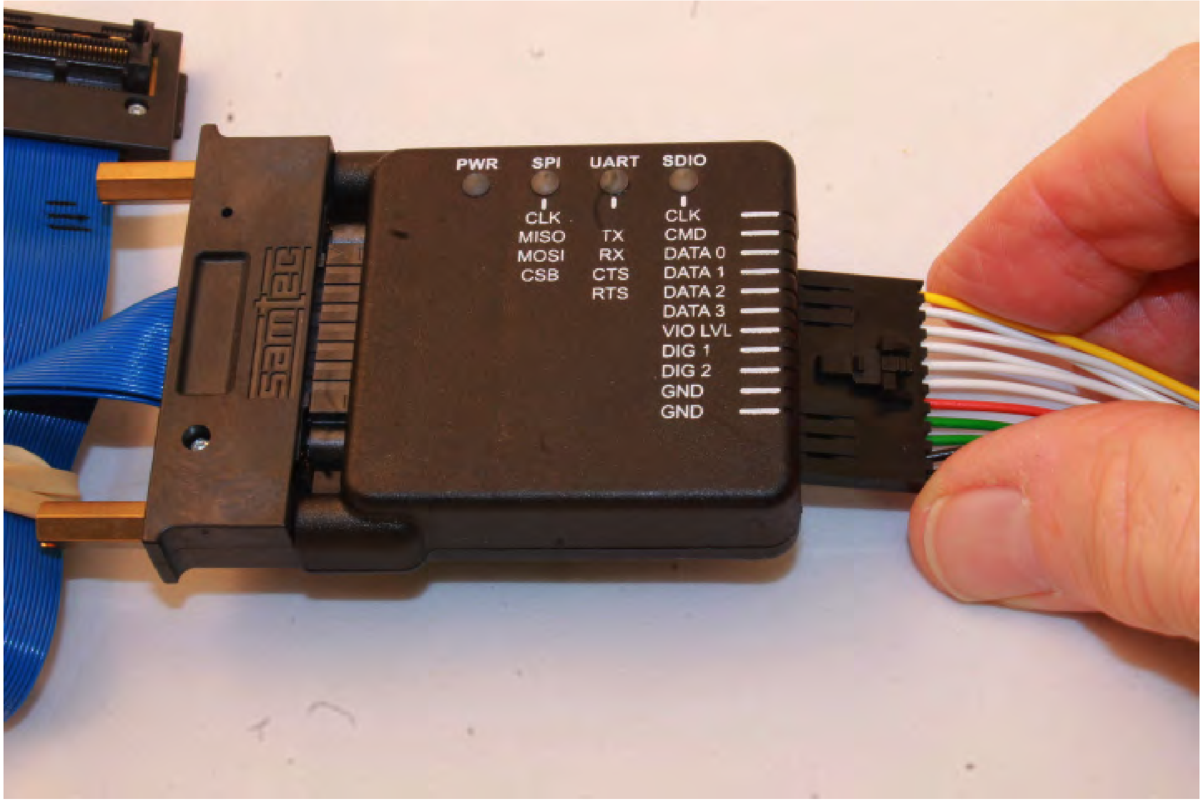


Figure 2.12 - Installing the Flying Lead Assembly on the HCI Pod

- 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.

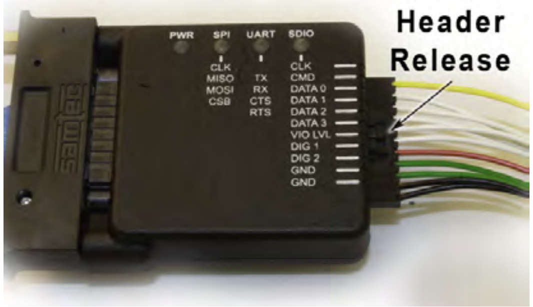


Figure 2.13 - Flying Lead Assembly Header Release

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.

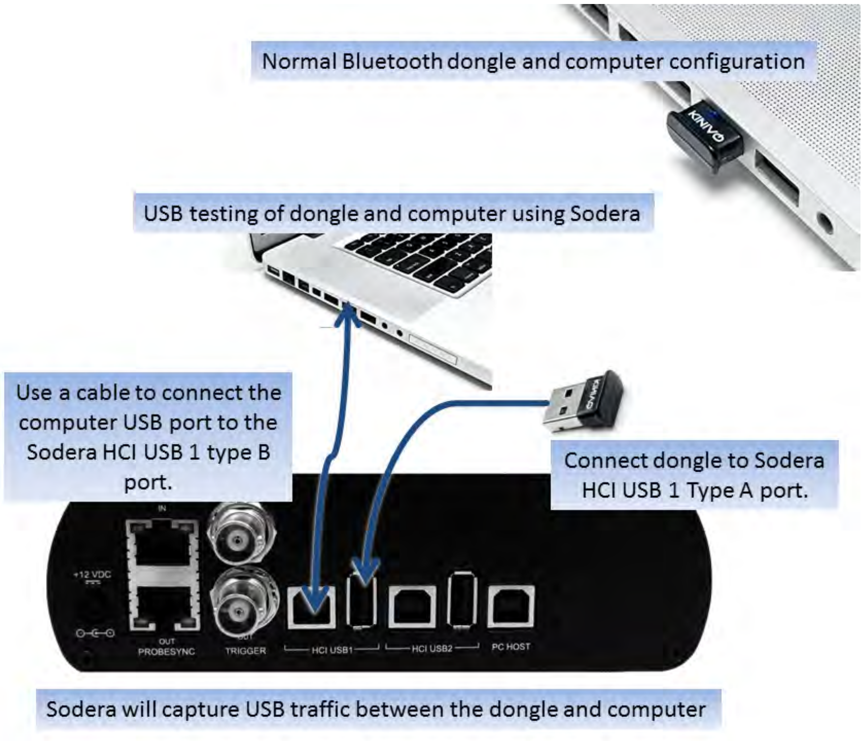

Normal Bluetooth dongle and computer configuration
USB testing of dongle and computer using Sodera
Use a cable to connect the computer USB port to the Sodera HCI USB 1 type B port.
Connect dongle to Sodera HCI USB 1 Type A port.
IN
+12 VDC
OUT
PROBESYNC
TRIGGER
HCI USB1
HCI USB2
PC HOST
Sodera will capture USB traffic between the dongle and computer

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

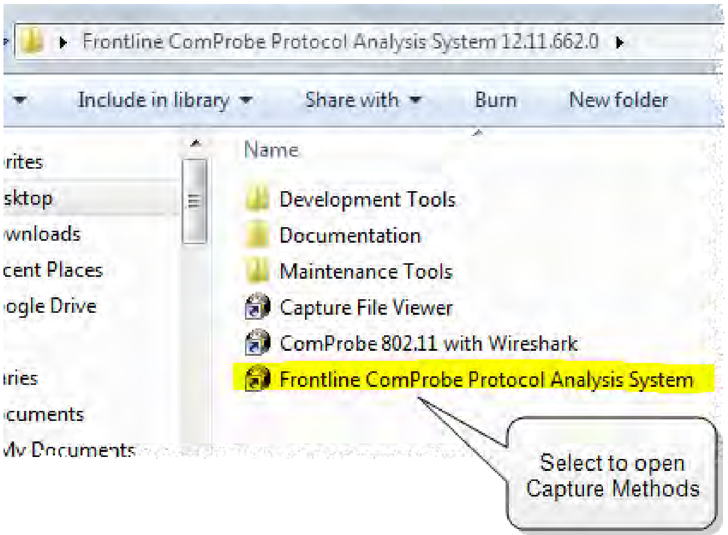
This section describes how to load TELEDYNE LECROY Frontline Protocol Analysis System software, and how to select the data capture method for your specific application.

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.

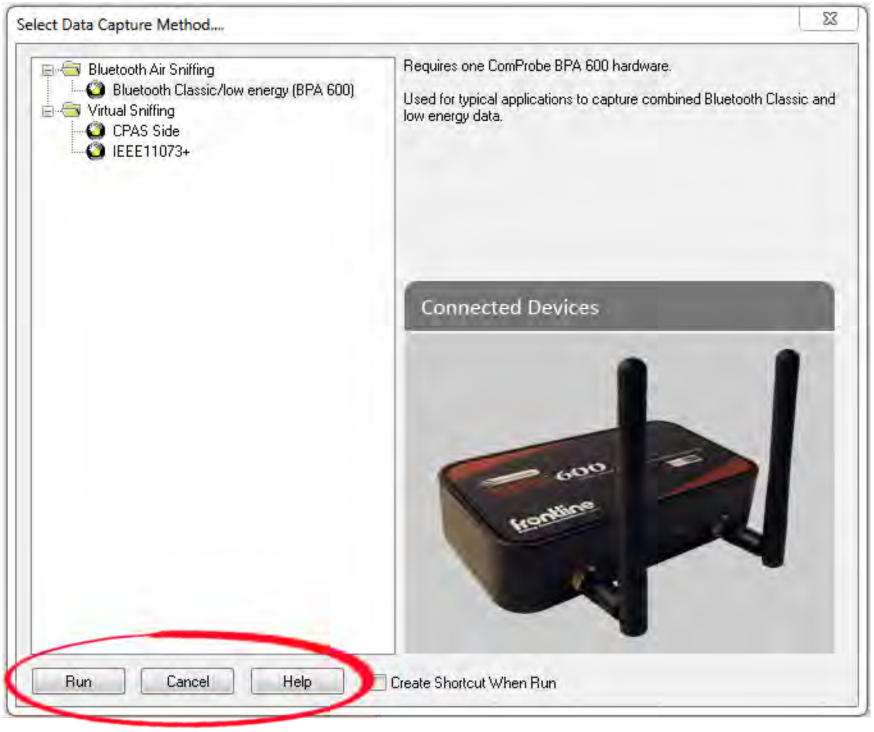


Select to open Capture Methods

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



Requires one ComProbe BPA 600 hardware.

Used for typical applications to capture combined Bluetooth Classic and low energy data.

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
	Becomes active when a capture method is selected. Starts the selected capture method.
	Closes the dialog and exits the user back to the computer desktop.
	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.

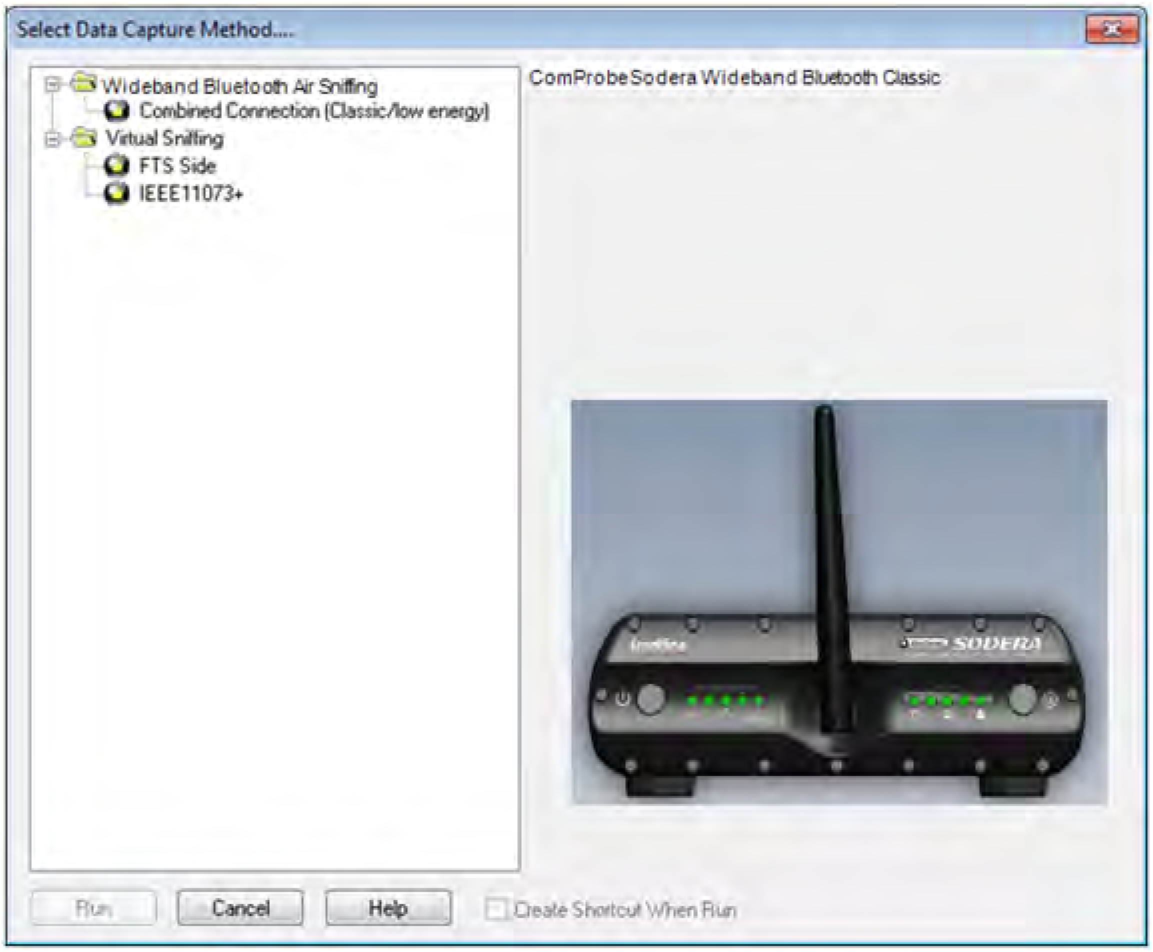

Select Data Capture Method....
Wideband Bluetooth Air Sniffing
Combined Connection (Classic/low energy)
Virtual Sniffing
FTS Side
IEEE11073+
ComProbe Sodera Wideband Bluetooth Classic
SODERA
Run
Cancel
Help
□ Create Shortcut When Run

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

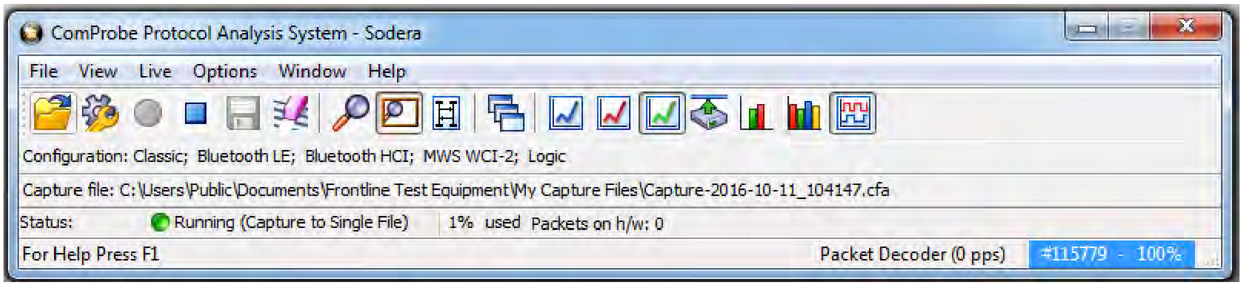
ProbeSync™ allows multiple Frontline analyzers to work seamlessly together and to share a common clock. Clock sharing allows the analyzers to precisely synchronize communications streams and to display resulting packets in a single shared or coexistent view.

- 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.



Configuration: Classic; Bluetooth LE; Bluetooth HCI; MWS WCI-2; Logic

Capture file: C:\Users\Public\Documents\Frontline Test Equipment\My Capture Files\Capture-2016-10-11_104147.cfa

Status: Running (Capture to Single File) 1% used Packets on h/w: 0

For Help Press F1 Packet Decoder (0 pps) #115779 - 100%

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.

Table 2.6 - Control Window Toolbar Icons (continued)

Icon	Description
■	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.
🔍	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.
ES	Audio Expert System - Opens Audio Expert System window

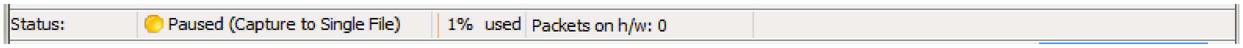
2.3.2 Configuration Information on the Control Window

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.

Configuration: Displays hardware configuration, network cards, 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: Paused (Capture to Single File) 1% used Packets on h/w: 0

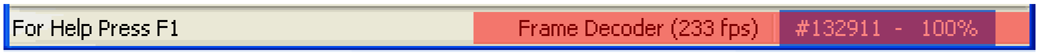
- Status displays Not Active, Paused or Running and refers to the state of data analysis.
  - Not Active means that the analyzer is not currently capturing data.
  - Paused means that data capture has been suspended.
  - Running means that the analyzer is actively capturing data.
- % Used

  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.


For Help Press F1 Frame Decoder (233 fps) #132911 - 100%

- 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.
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 115
	Unframe		Removes start-of-frame and end-of-frame markers from your data. SeeUnframing on page 115
	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.
	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.

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

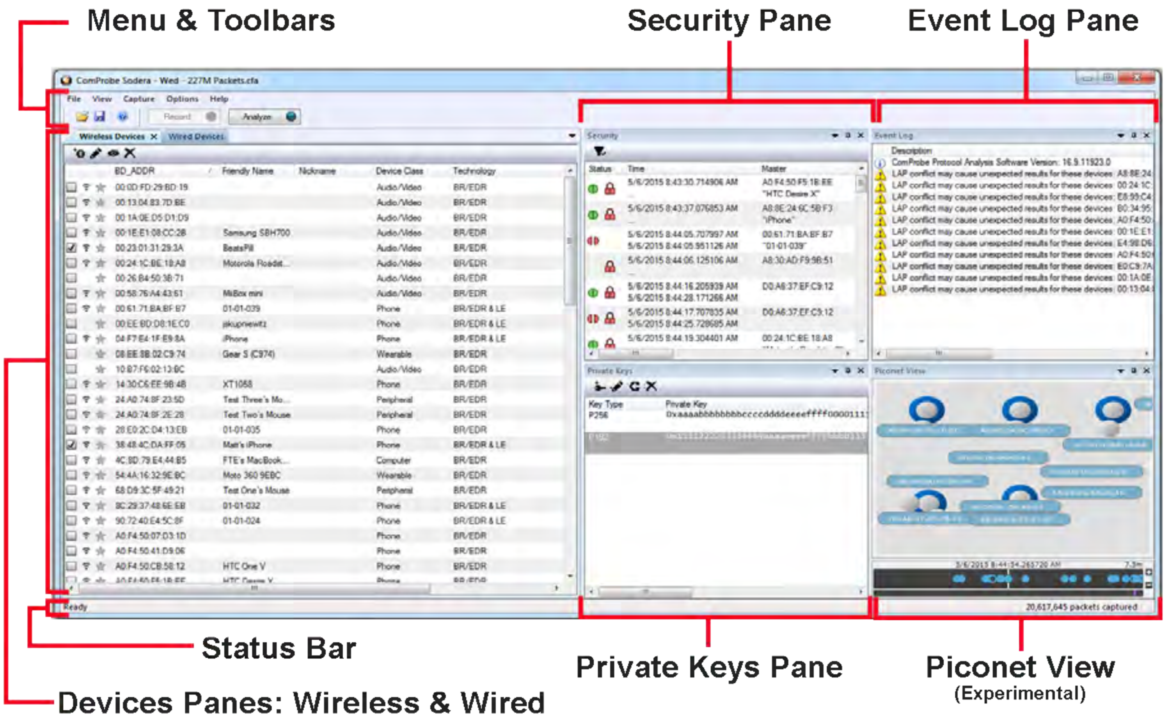
Coexistence capture scenario is an extension of the standard capture scenario with the addition of a Frontline 802.11 Wi-Fi analyzer through the use of ProbeSync™ technology. Frontline Sodera operates in conjunction with Frontline 802.11 to capture transmissions from their respective technologies. ProbeSync™ 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.



	BD_ADDR	Friendly Name	Nickname	Device Class	Technology
□	00:0D:FD:29:BD:19			Audio/Video	BR/EDR
□	00:13:04:83:7D:BE			Audio/Video	BR/EDR
□	00:1A:0E:D5:D1:D9			Audio/Video	BR/EDR
□	00:1E:E1:08:CC:28	Samsung SBH700		Audio/Video	BR/EDR
☑	00:23:01:31:29:3A	BeatsPill		Audio/Video	BR/EDR
□	00:24:1C:BE:18:A8	Motorola Roadst...		Audio/Video	BR/EDR
□	00:26:B4:50:3B:71			Audio/Video	BR/EDR
□	00:58:76:A4:43:61	MiBox mini		Audio/Video	BR/EDR
□	00:61:71:BA:BF:B7	01-01-039		Phone	BR/EDR & LE
□	00:EE:BD:D8:1E:C0	jskupniewitz		Phone	BR/EDR & LE
□	04:F7:E4:1F:E9:8A	iPhone		Phone	BR/EDR & LE
□	08:EE:8B:02:C9:74	Gear S (C974)		Wearable	BR/EDR
□	10:B7:F6:02:13:BC			Audio/Video	BR/EDR
□	14:30:C6:EE:9B:4B	XT1058		Phone	BR/EDR
□	24:A0:74:8F:23:5D	Test Three's Mo...		Peripheral	BR/EDR
□	24:A0:74:8F:2E:28	Test Two's Mouse		Peripheral	BR/EDR
□	28:E0:2C:D4:13:EB	01-01-035		Phone	BR/EDR
☑	38:48:4C:DA:FF:05	Matt's iPhone		Phone	BR/EDR & LE
□	4C:8D:79:E4:44:B5	FTE's MacBook...		Computer	BR/EDR
□	54:4A:16:32:9E:BC	Moto 360 9EBC		Wearable	BR/EDR
□	68:D9:3C:5F:49:21	Test One's Mouse		Peripheral	BR/EDR
□	8C:29:37:48:6E:EB	01-01-032		Phone	BR/EDR & LE
□	90:72:40:E4:5C:8F	01-01-024		Phone	BR/EDR & LE
□	A0:F4:50:07:D3:1D			Phone	BR/EDR
□	A0:F4:50:41:D9:06			Phone	BR/EDR
□	A0:F4:50:CB:58:12	HTC One V		Phone	BR/EDR

Ready

Status	Time	Master
	5/6/2015 8:43:30.714906 AM	A0:F4:50:F5:1B:EE "HTC Desire X"
	5/6/2015 8:43:37.076853 AM	A8:8E:24:6C:5B:F3 "iPhone"
	5/6/2015 8:44:05.707997 AM 5/6/2015 8:44:05.951126 AM	00:61:71:BA:BF:B7 "01-01-039"
	5/6/2015 8:44:06.125106 AM	A8:30:AD:F9:9B:51
	5/6/2015 8:44:16.205939 AM 5/6/2015 8:44:28.171266 AM	D0:A6:37:EF:C9:12
	5/6/2015 8:44:17.707835 AM 5/6/2015 8:44:25.728685 AM	D0:A6:37:EF:C9:12
	5/6/2015 8:44:19.304401 AM	00:24:1C:BE:18:A8

Description
ComProbe Protocol Analysis Software Version: 16.9.11923.0
LAP conflict may cause unexpected results for these devices: A8:8E:24
LAP conflict may cause unexpected results for these devices: 00:24:1C:
LAP conflict may cause unexpected results for these devices: E8:99:C4
LAP conflict may cause unexpected results for these devices: B0:34:95:
LAP conflict may cause unexpected results for these devices: A0:F4:50:
LAP conflict may cause unexpected results for these devices: 00:1E:E1:
LAP conflict may cause unexpected results for these devices: E4:98:D6
LAP conflict may cause unexpected results for these devices: A0:F4:50
LAP conflict may cause unexpected results for these devices: E0:C9:7A
LAP conflict may cause unexpected results for these devices: 00:1A:0E:
LAP conflict may cause unexpected results for these devices: 00:13:04:

Key Type	Private Key
P256	0xaaaabbbbbbbbccccddddeeeeffff00001111

20,617,645 packets captured

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.

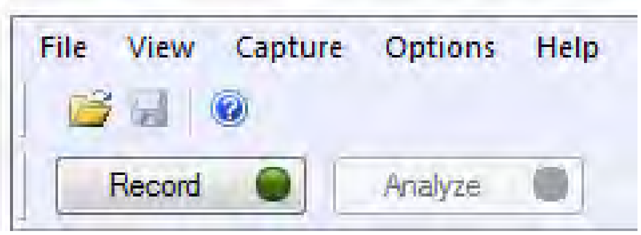
The Devices Pane is always visible and cannot be docked, however if the other panes are docked or not visible the Devices Pane can be expanded to fill the window pane area.

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.

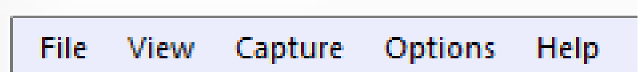
The **Wired Devices**, **Security**, **Private Keys**, **Piconet View**, and **Event Log** Panes can be re-sized by hovering over the pane edge until a double headed arrow appears. Click and hold, dragging it to change the pane size.

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

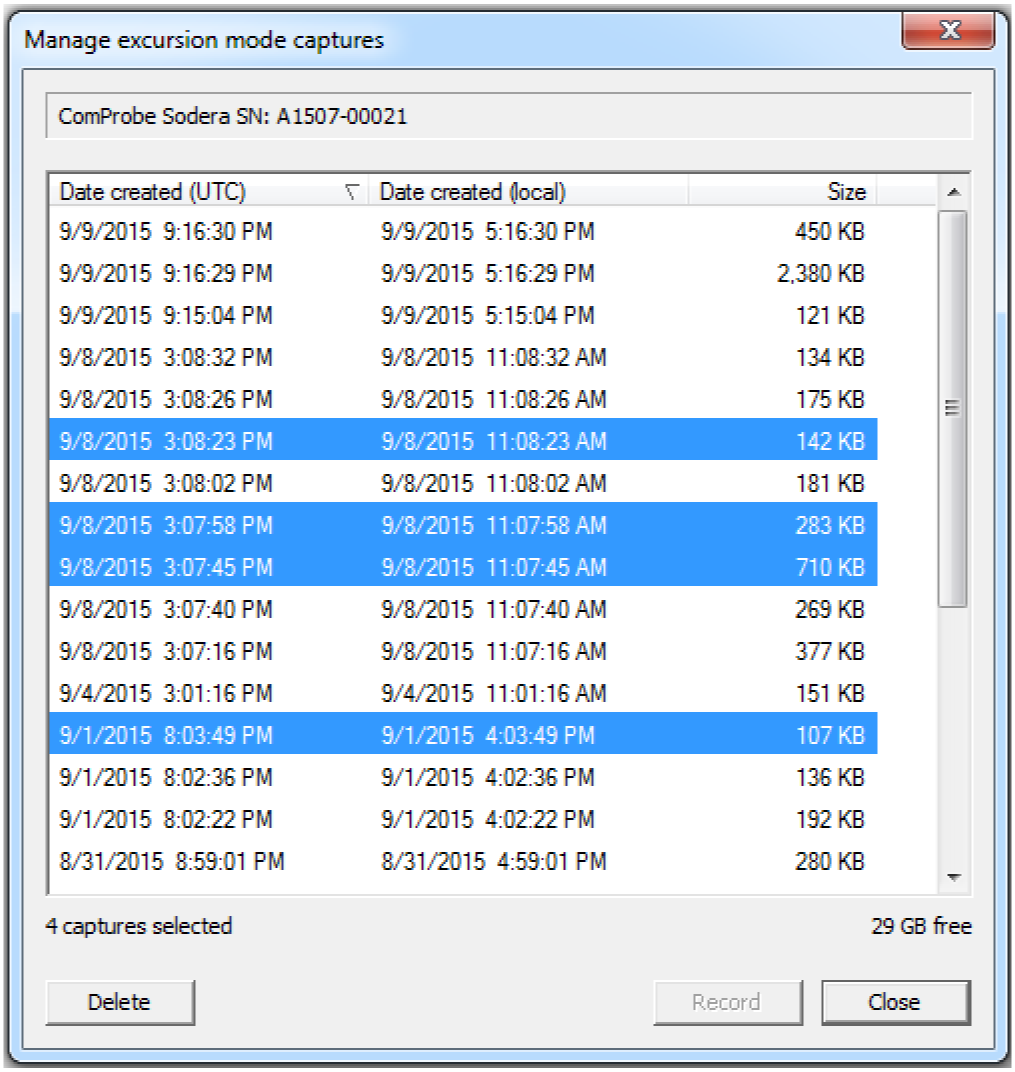
<table>
<tr><th>Option</th><th>Selection</th><th>Description</th></tr>
<tr><td rowspan="4"><b>File</b></td><td><b>Open Capture File (Ctrl-O)</b></td><td>Opens a Windows Open dialog. Select the location, File name, and .cfa file to analyze. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.</td></tr>
<tr><td><b>Save (Ctrl-S)</b></td><td>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.</td></tr>
<tr><td><b>Manage excursion mode captures...</b></td><td>Record or delete captures from the Sodera hardware that were created using excursion mode. Opens the <b>Manage excursion mode captures</b> dialog.
This selection is disabled during live capture.</td></tr>
<tr><td><b>Exit</b></td><td>Closes Frontline software</td></tr>
<tr><td rowspan="8"><b>View</b></td><td><b>Toolbars</b></td><td><table>
<tr><th>Selection</th><th>Description</th></tr>
<tr><td><b>Capture</b></td><td>When checked the Capture Toolbar is visible. Checked is the default.</td></tr>
<tr><td><b>Standard</b></td><td>When checked the Standard Toolbar is visible. Checked is the default.</td></tr>
<tr><td><b>Status</b></td><td>When checked the Status Bar is visible. Checked is the default.</td></tr>
</table></td></tr>
<tr><td><b>Wireless Devices</b></td><td>When checked the <b>Wireless Devices</b> tab is visible in the Devices pane. Selecting the tab will display the Wireless Devices.</td></tr>
<tr><td><b>Wired Devices</b></td><td>When checked the <b>Wired Devices</b> tab is visible in the Devices pane. Selecting the tab will display the Wired Devices connected to <b>POD 1</b> and <b>POD 2</b>.</td></tr>
<tr><td><b>Security</b></td><td>When checked the <b>Security</b> pane is visible. Checked is the default.</td></tr>
<tr><td><b>Event Log</b></td><td>When checked the <b>Event Log</b> pane is visible. Checked is the default.</td></tr>
<tr><td><b>Piconet View (Experimental)</b></td><td>When checked, the <b>Piconet View</b> is visible. Not-checked is the default.
At this time the <b>Piconet View</b> is experimental and in development.</td></tr>
<tr><td><b>Private Keys</b></td><td>When checked, the <b>Private Keys</b> pane is visible. The Private Keys pane displays user entered Private/ Public key pairs for <i>Bluetooth</i> 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>
</table>

Table 3.1 - Menu Selections(continued)

Option	Selection	Description
Capture	**Record/Recording**	Starts and stops the capture of data. Performs the same function as the Capture Toolbar **Record/Recording** button.
	Analyze/Analyzing	Starts and stops the analysis of recorded data. Performs the same function as the Capture Toolbar **Analyze/Analyzing** button.
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.



Manage excursion mode captures

ComProbe Sodera SN: A1507-00021

Date created (UTC)	Date created (local)	Size
9/9/2015 9:16:30 PM	9/9/2015 5:16:30 PM	450 KB
9/9/2015 9:16:29 PM	9/9/2015 5:16:29 PM	2,380 KB
9/9/2015 9:15:04 PM	9/9/2015 5:15:04 PM	121 KB
9/8/2015 3:08:32 PM	9/8/2015 11:08:32 AM	134 KB
9/8/2015 3:08:26 PM	9/8/2015 11:08:26 AM	175 KB
9/8/2015 3:08:23 PM	9/8/2015 11:08:23 AM	142 KB
9/8/2015 3:08:02 PM	9/8/2015 11:08:02 AM	181 KB
9/8/2015 3:07:58 PM	9/8/2015 11:07:58 AM	283 KB
9/8/2015 3:07:45 PM	9/8/2015 11:07:45 AM	710 KB
9/8/2015 3:07:40 PM	9/8/2015 11:07:40 AM	269 KB
9/8/2015 3:07:16 PM	9/8/2015 11:07:16 AM	377 KB
9/4/2015 3:01:16 PM	9/4/2015 11:01:16 AM	151 KB
9/1/2015 8:03:49 PM	9/1/2015 4:03:49 PM	107 KB
9/1/2015 8:02:36 PM	9/1/2015 4:02:36 PM	136 KB
9/1/2015 8:02:22 PM	9/1/2015 4:02:22 PM	192 KB
8/31/2015 8:59:01 PM	8/31/2015 4:59:01 PM	280 KB

4 captures selected

29 GB free

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

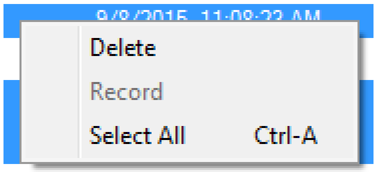
- Pressing the Delete key, or
- Right-clicking and selecting **Delete** from the context menu, or
- Clicking the dialog **Delete** button.

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.

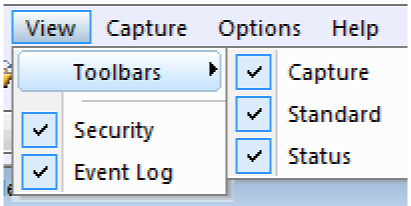
Record - Selecting a single file will enable the **Record** button and the **Record** right-click pop-up menu item. Clicking the **Record** button or menu item will close the dialog and start recording the selected excursion mode capture to the user's computer.

Right-click pop-up menu

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

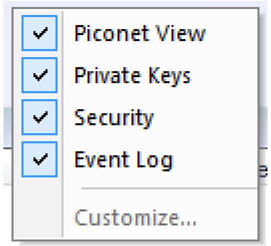


View Menu



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

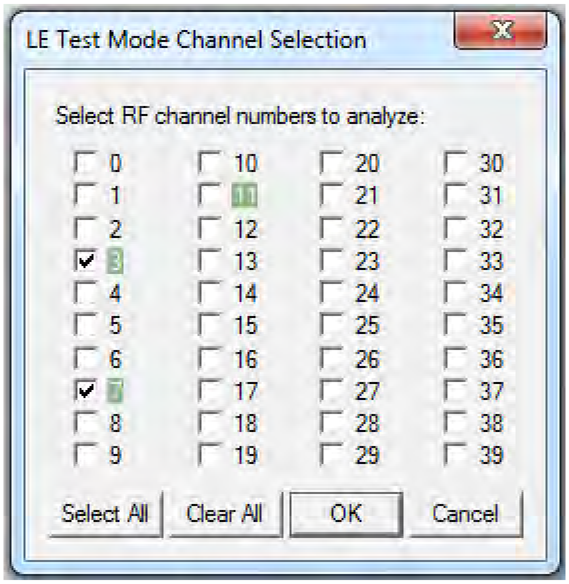


Right-clicking in the toolbar any of the following window/panes will display a pop-up View menu that performs the same as the main View menu:

- 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


LE Test Mode Channel Selection

Select RF channel numbers to analyze:

□ 0 □ 10 □ 20 □ 30
□ 1 □ 11 □ 21 □ 31
□ 2 □ 12 □ 22 □ 32
☑ 3 □ 13 □ 23 □ 33
□ 4 □ 14 □ 24 □ 34
□ 5 □ 15 □ 25 □ 35
□ 6 □ 16 □ 26 □ 36
☑ 7 □ 17 □ 27 □ 37
□ 8 □ 18 □ 28 □ 38
□ 9 □ 19 □ 29 □ 39

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

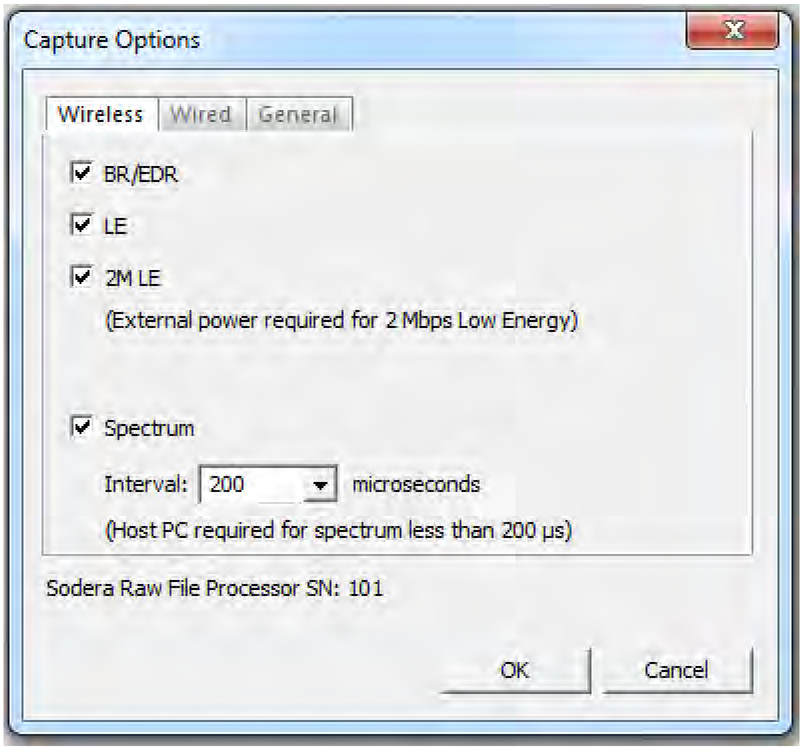
Button	Description
Select All	Selects all 40 low energy channels
Clear All	Deselects all 40 low energy channels
OK	Active once a channels selection is made. When clicked the selected channels are saved for analysis, and the dialog closes.
Cancel	Closes the dialog without saving any changes.

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



☑ BR/EDR

☑ LE

☑ 2M LE

(External power required for 2 Mbps Low Energy)

☑ Spectrum

Interval: 200 microseconds

(Host PC required for spectrum less than 200 µs)

Sodera Raw File Processor SN: 101

Figure 3.3 - Sodera Capture Options - Wireless tab.

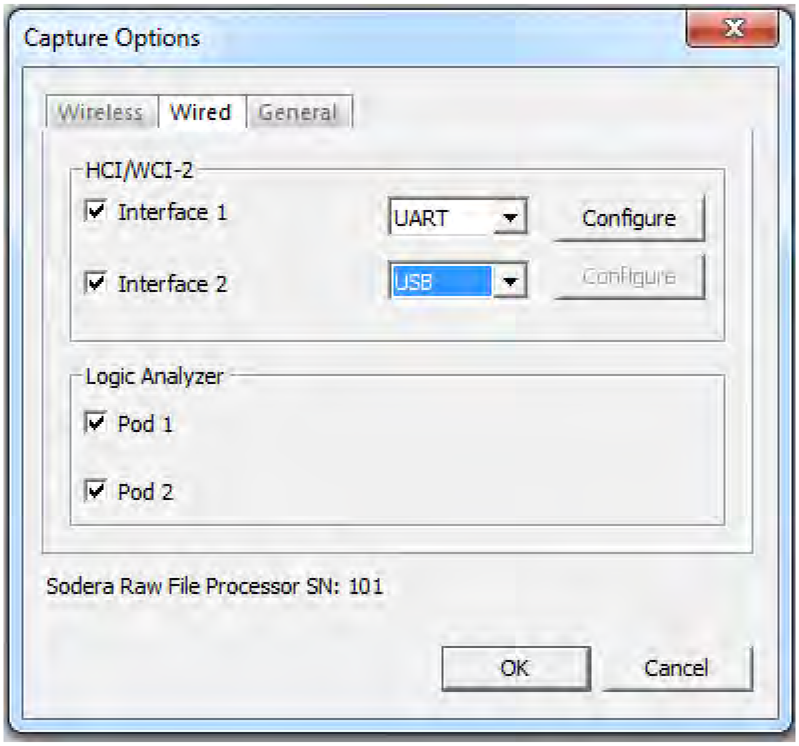
Table 3.3 - Capture Options Wireless Tab Selections

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.

Table 3.3 - Capture Options Wireless Tab Selections (continued)

Selection	Description
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 108 and Coexistence View - Spectrum (Sodera Only) on page 222 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



Capture Options

Wireless | Wired | General

HCI/WCI-2

☑ Interface 1 — UART

☑ Interface 2 — USB

Logic Analyzer

☑ Pod 1

☑ Pod 2

Sodera Raw File Processor SN: 101

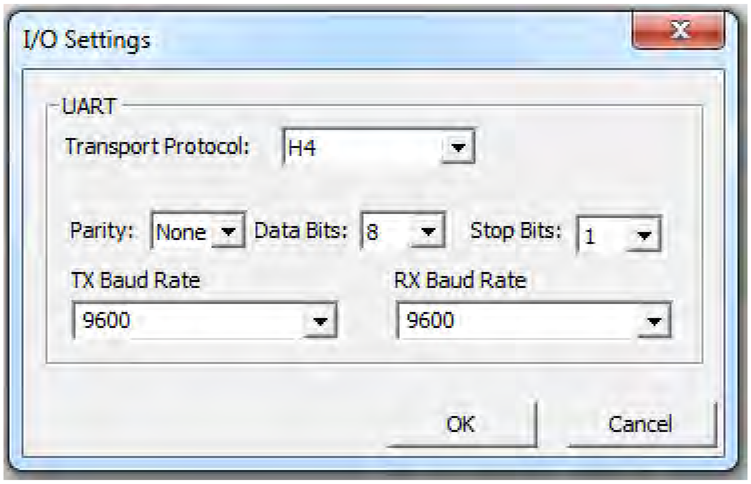
Figure 3.4 - Sodera Capture Options - Wired tab.

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 below. • 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 below. • 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.


I/O Settings

UART

Transport Protocol: H4

Parity: None Data Bits: 8 Stop Bits: 1

TX Baud Rate 9600

RX Baud Rate 9600

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.

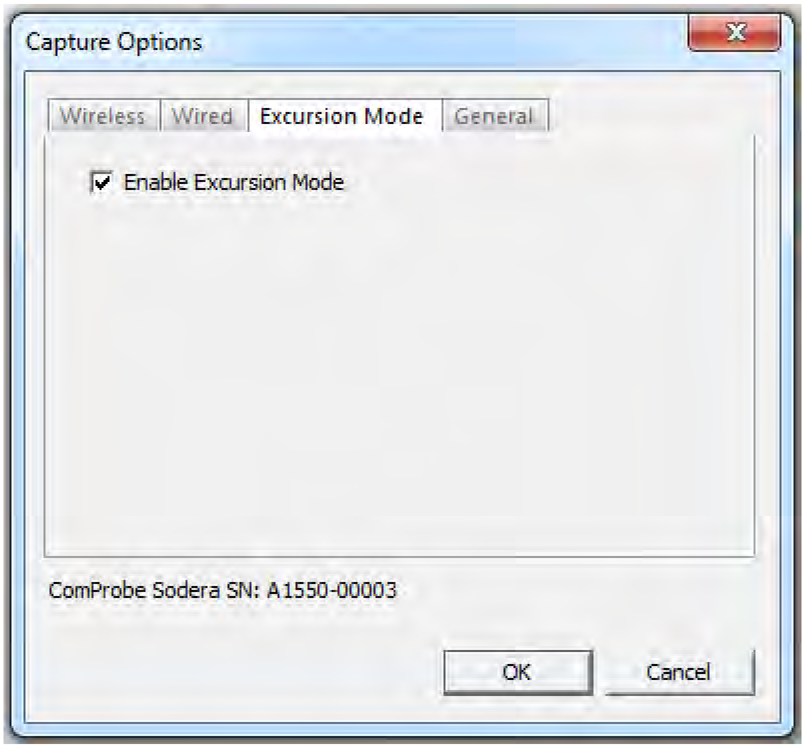
Table 3.5 - HCI I/O Settings for UART (continued)

Setting	Value	Description
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



☑ Enable Excursion Mode

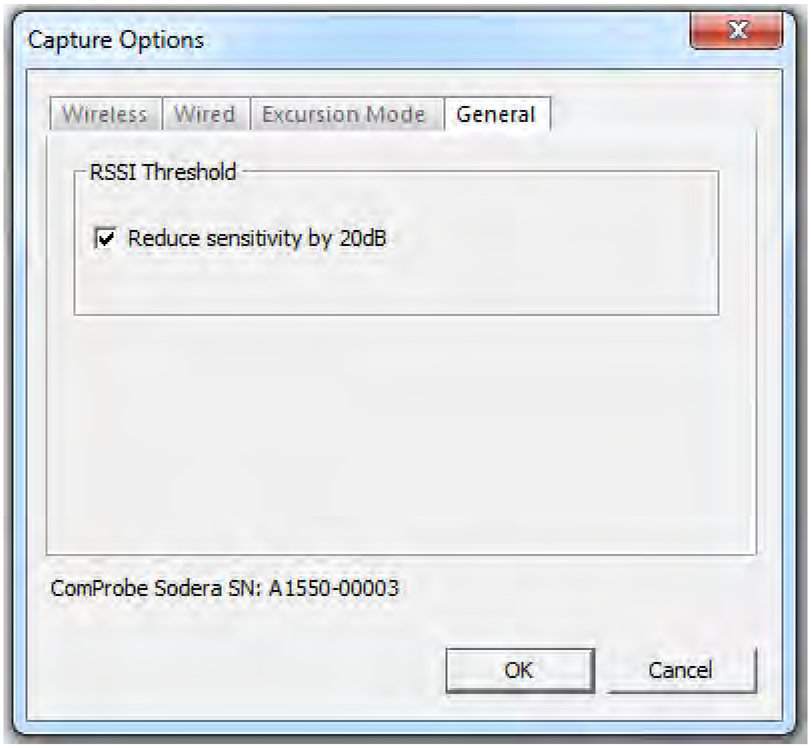
ComProbe Sodera SN: A1550-00003

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 74 for more information about the Excursion Mode.

General Tab


Capture Options

RSSI Threshold

☑ Reduce sensitivity by 20dB

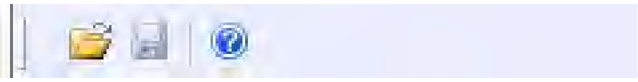
ComProbe Sodera SN: A1550-00003

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 153. When unchecked, normal gain is enabled on the Sodera hardware.

3.1.2.1.2 Standard Toolbar



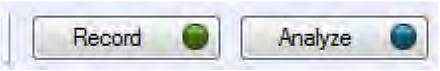
The Standard Toolbar provides quick one-click access to the same options that appear in menu **File** selection. This toolbar may be hidden by selecting from the menu View Toolbars selection and removing the check from Standard Toolbar selection.

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.
💾	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

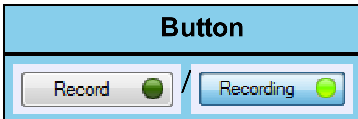
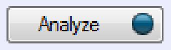
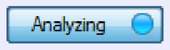
Button	View	Description
	**Record**	When this button view is active Sodera is not capturing data. Clicking this button view will begin data capture from wireless devices within range and wired devices connected to the Sodera unit and the view will change to **Recording**. The default capture is both 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**	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.

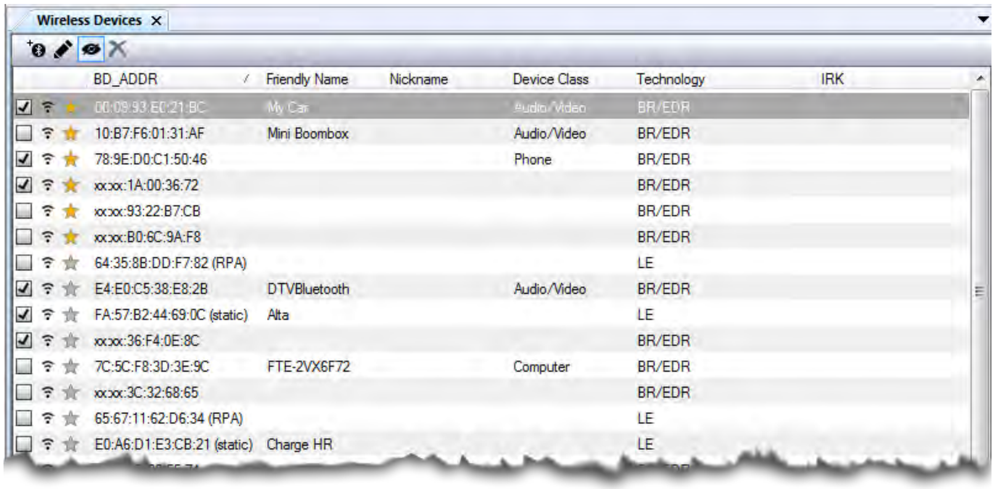
A new device/BD_ADDR is automatically added to the Device Pane when:

- 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.

[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.

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. 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.



	BD_ADDR	Friendly Name	Nickname	Device Class	Technology	IRK
☑ 📶 ★	00:09:93:E0:21:BC	My Car		Audio/Video	BR/EDR	
☐ 📶 ★	10:B7:F6:01:31:AF	Mini Boombox		Audio/Video	BR/EDR	
☑ 📶 ★	78:9E:D0:C1:50:46			Phone	BR/EDR	
☑ 📶 ★	xx:xx:1A:00:36:72				BR/EDR	
☐ 📶 ★	xx:xx:93:22:B7:CB				BR/EDR	
☐ 📶 ★	xx:xx:B0:6C:9A:F8				BR/EDR	
☐ 📶 ☆	64:35:8B:DD:F7:82 (RPA)				LE	
☑ 📶 ☆	E4:E0:C5:38:E8:2B	DTVBluetooth		Audio/Video	BR/EDR	
☑ 📶 ☆	FA:57:B2:44:69:0C (static)	Alta			LE	
☑ 📶 ☆	xx:xx:36:F4:0E:8C				BR/EDR	
☐ 📶 ☆	7C:5C:F8:3D:3E:9C	FTE-2VX6F72		Computer	BR/EDR	
☐ 📶 ☆	xx:xx:3C:32:68:65				BR/EDR	
☐ 📶 ☆	65:67:11:62:D6:34 (RPA)				LE	
☐ 📶 ☆	E0:A6:D1:E3:CB:21 (static)	Charge HR			LE	

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

Table 3.11 - Device Classes (continued)

Class	BR/EDR	low energy
Health	X	
Heart Rate Sensor		X
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

Table 3.11 - Device Classes (continued)

Class	BR/EDR	low energy
Tag		X
Generic Thermometer		X
Thermometer: Ear		X
Toy	X	
Uncategorized	X	
Unknown		X
Watch		X
Wearable	X	
Weight Scale		X

Sorting Wireless Devices columns

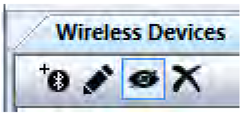
Any column in the **Wireless Devices** pane can be used to sort the entire table. Each column is sortable in ascending or descending order, but only one column at-a-time can be used to sort.

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

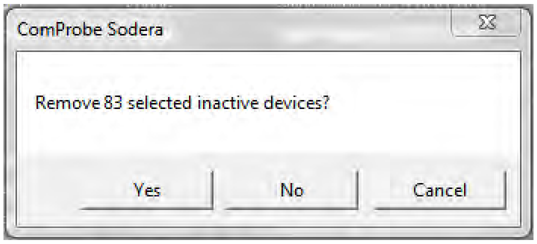


At the top of the Wireless Devices pane are three tools for managing the devices in the pane. You can add and edit devices, and delete inactive devices. During Analyzing this toolbar is not available for use.

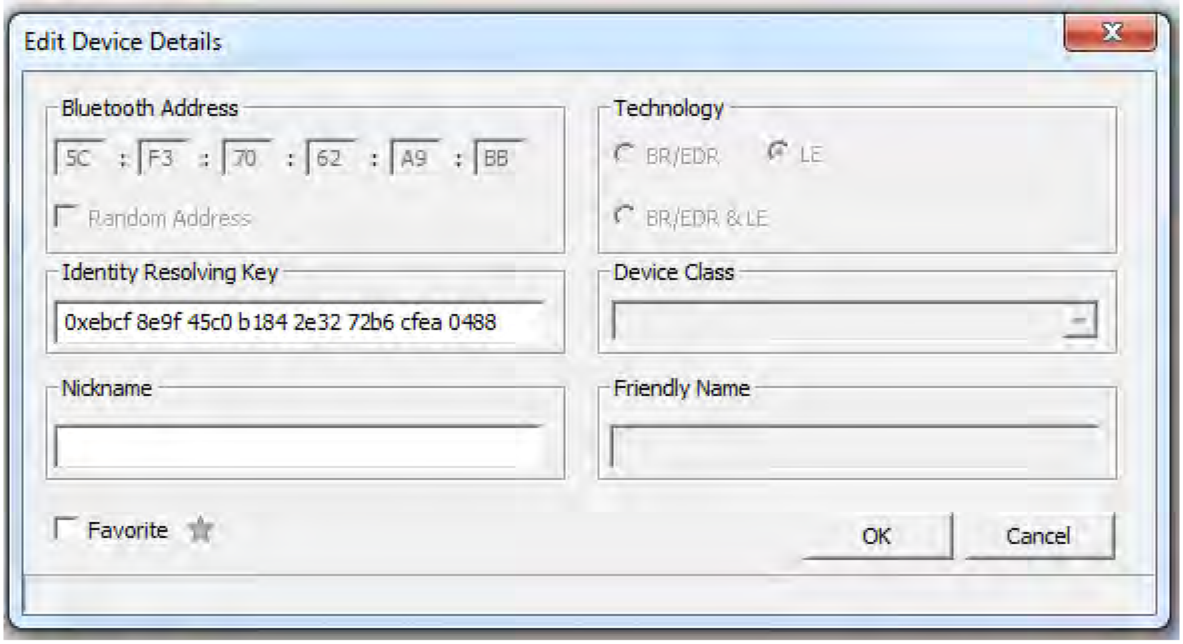
Table 3.12 - Wireless Devices Management Tools

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**.

Table 3.12 - Wireless Devices Management Tools (continued)

Tool	Icon	Description
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.
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.  Remove 83 selected inactive devices? 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



Edit Device Details

Bluetooth Address

5C : F3 : 70 : 62 : A9 : BB

□ Random Address

Technology

○ BR/EDR ● LE

○ BR/EDR & LE

Identity Resolving Key

0xebcf 8e9f 45c0 b184 2e32 72b6 cfea 0488

Device Class

Nickname

Friendly Name

□ Favorite ☆

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.

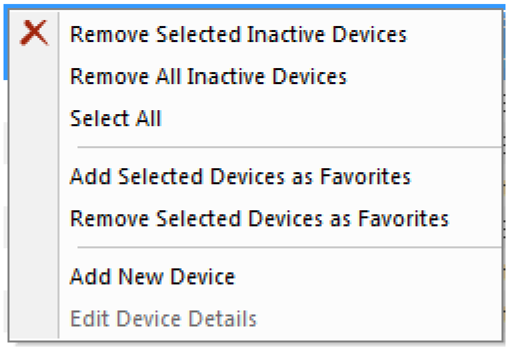
The **Favorite** designation can be changed in this dialog in addition to directly clicking on the star in the table or by using the right-click pop-up menu.

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 55 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


Remove Selected Inactive Devices
Remove All Inactive Devices
Select All
Add Selected Devices as Favorites
Remove Selected Devices as Favorites
Add New Device
Edit Device Details

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.
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.

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

Selection	Description
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.

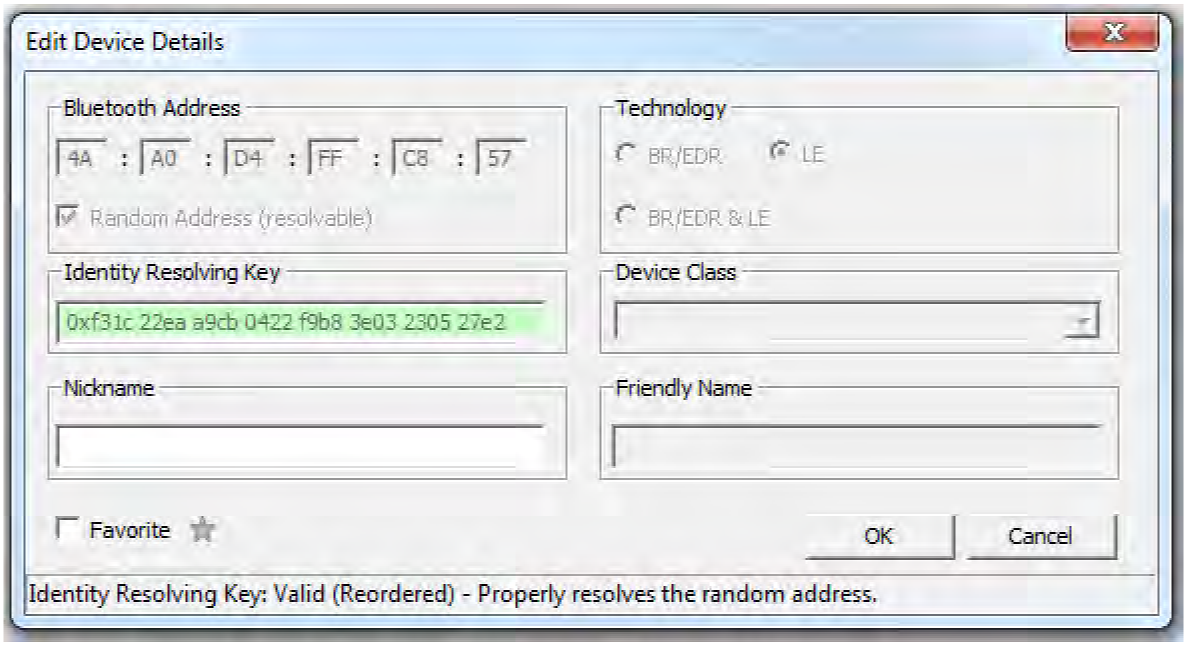
A reversed IRK is defined as the original IRK value with its endianness reversed. For example, the IRK *0xf31c 22ea a9cb 0422 f9b8 3e03 2305 27e2* in reverse order is *0xe227 0523 033e b8f9 2204 cba9 ea22 1cf3*.

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.



Edit Device Details

Bluetooth Address

4A : A0 : D4 : FF : C8 : 57

☑ Random Address (resolvable)

Technology

○ BR/EDR ● LE

○ BR/EDR & LE

Identity Resolving Key

0xf31c 22ea a9cb 0422 f9b8 3e03 2305 27e2

Device Class

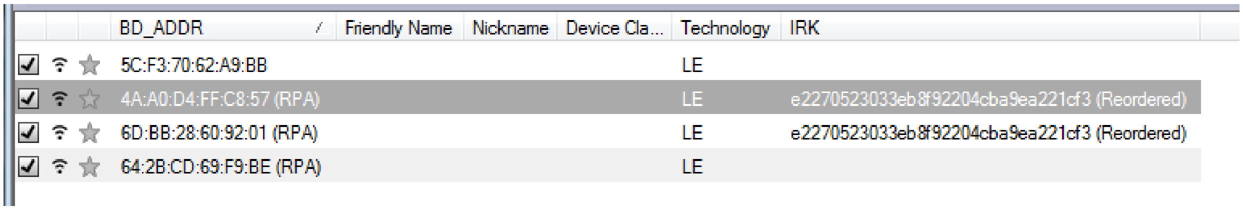
Nickname

Friendly Name

□ Favorite

Identity Resolving Key: Valid (Reordered) - Properly resolves the random address.

Figure 3.8 - RPA Device IRK Valid and Reordered



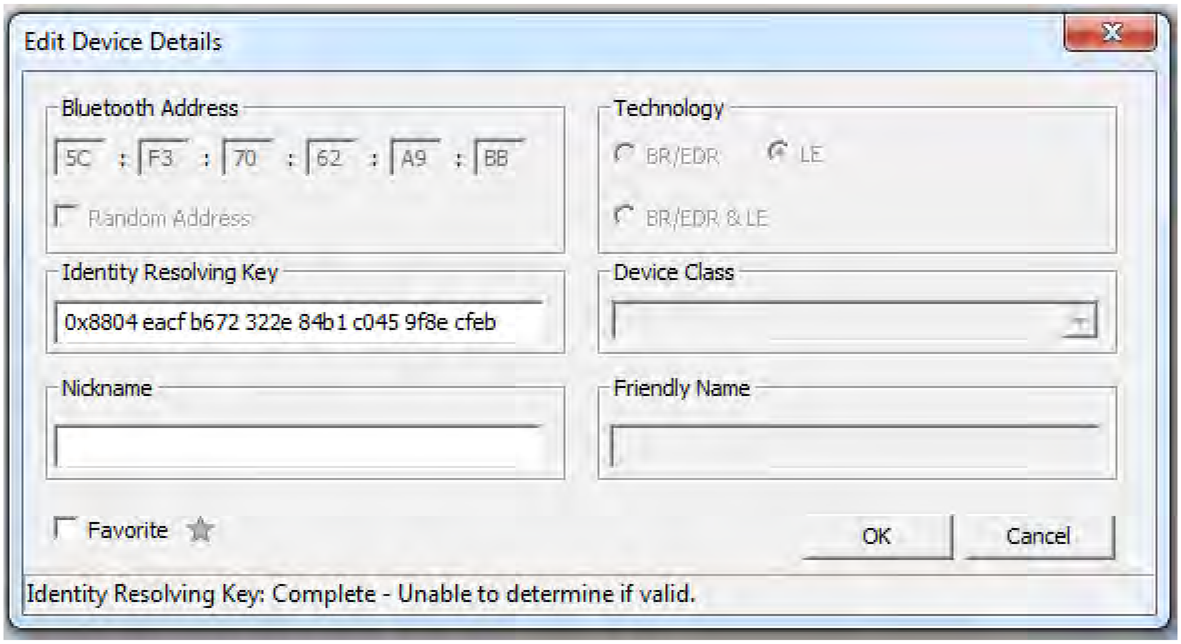
			BD_ADDR	Friendly Name	Nickname	Device Cla...	Technology	IRK
☑	ᯤ	☆	5C:F3:70:62:A9:BB				LE	
☑	ᯤ	☆	4A:A0:D4:FF:C8:57 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3 (Reordered)
☑	ᯤ	☆	6D:BB:28:60:92:01 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3 (Reordered)
☑	ᯤ	☆	64:2B:CD:69:F9:BE (RPA)				LE	

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.



Bluetooth Address

5C : F3 : 70 : 62 : A9 : BB

□ Random Address

Technology

○ BR/EDR ● LE

○ BR/EDR & LE

Identity Resolving Key

0x8804 eacf b672 322e 84b1 c045 9f8e cfeb

Device Class

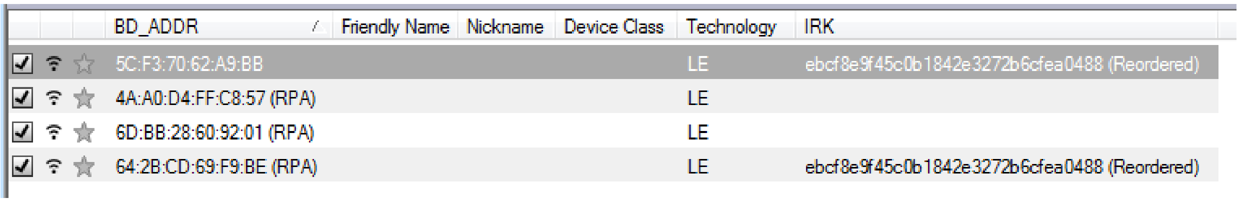
Nickname

Friendly Name

□ Favorite ☆

Identity Resolving Key: Complete - Unable to determine if valid.

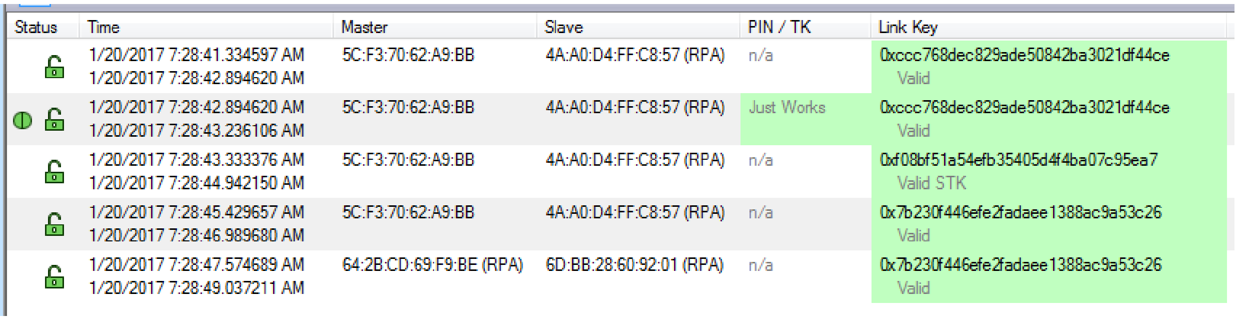
Figure 3.10 - Public Address Device IRK: Unable to Determine if Valid



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

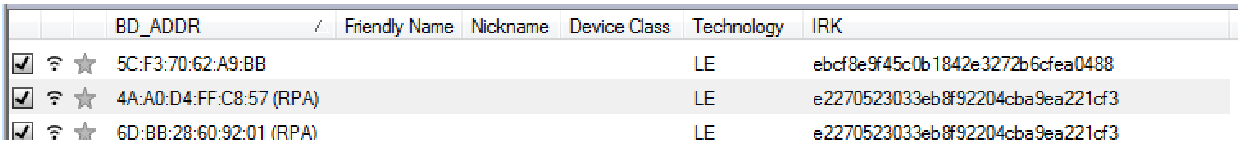
Public Address Device IRK Reordered

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

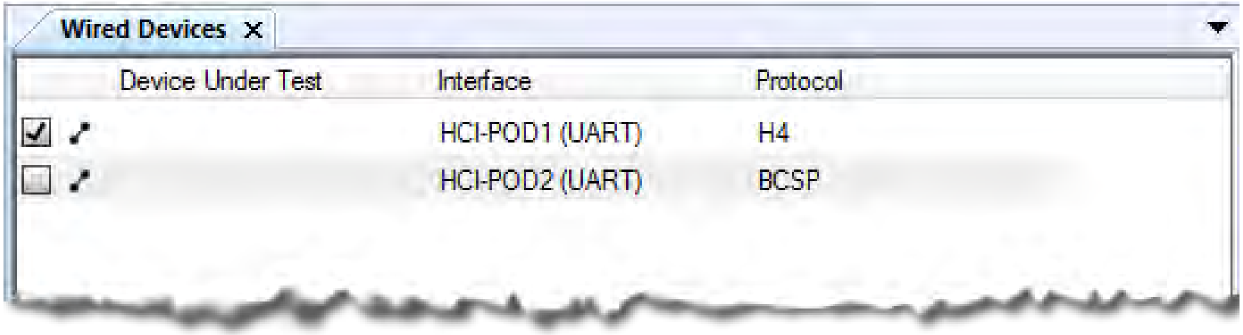
Figure 3.11 - Public Address Device: LTK Entered in Security pane to Validate IRK



	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



Wired Devices ✕

	Device Under Test	Interface	Protocol
☑ ⤢		HCI-POD1 (UART)	H4
□ ⤢		HCI-POD2 (UART)	BCSP

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).

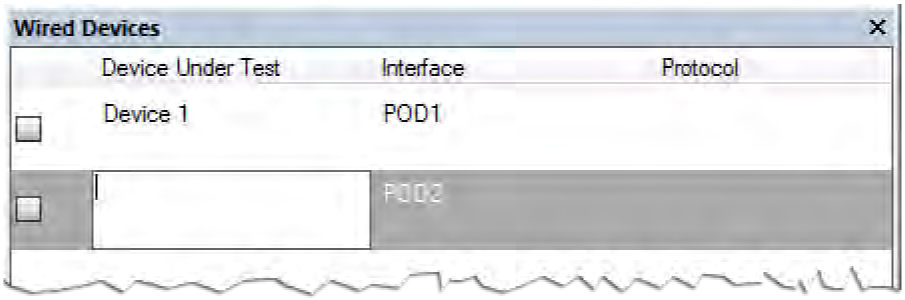
The Wired Devices pane contains five columns. Their functions are listed below.

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.



Wired Devices

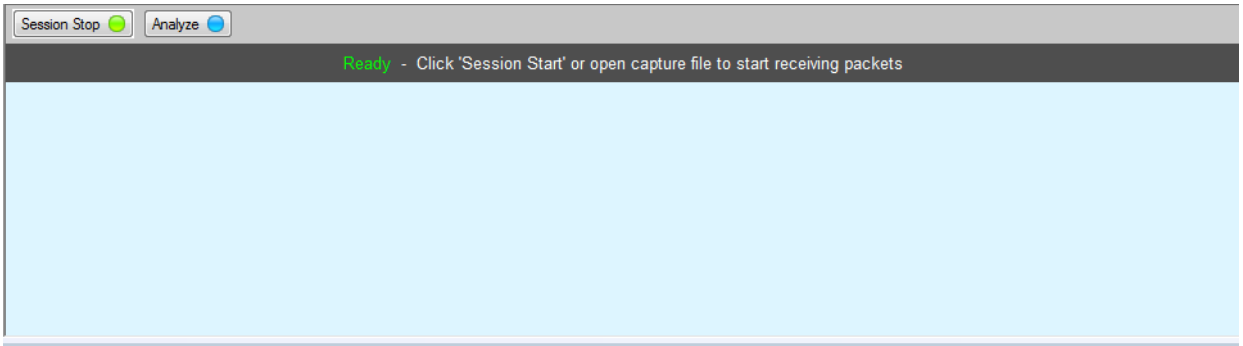
	Device Under Test	Interface	Protocol
□	Device 1	POD1	
□		POD2	

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.



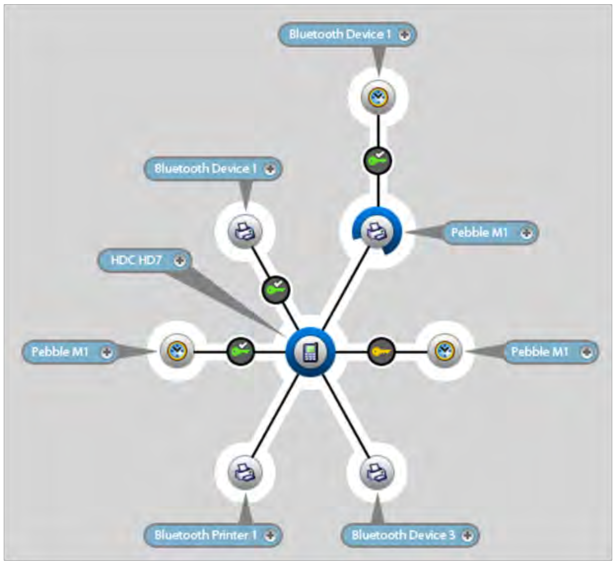
Ready - Click 'Session Start' or open capture file to start receiving packets

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

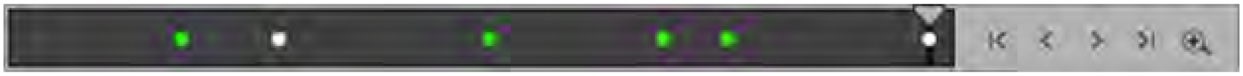


Figure 3.15 - **Piconet View** Timeline

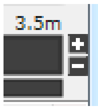
As device connections appear over time, the Timeline on the bottom of the **Piconet View** displays circles representing events over time where the piconet view has changed. Classic *Bluetooth* events appear as blue circles and *Bluetooth* low energy events appear as green circles. These events appear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

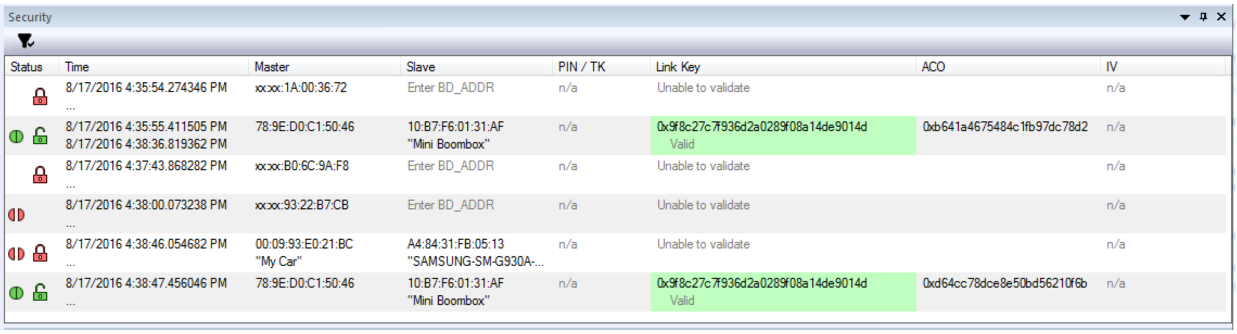
3.1.2.5 Security Pane

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 109 for a description of the critical packets. The Security pane will identify the type of key required for decryption.



Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔒	8/17/2016 4:35:54.274346 PM ...	xx:xx:1A:00:36:72	Enter BD_ADDR	n/a	Unable to validate		n/a
⦶ 🔓	8/17/2016 4:35:55.411505 PM 8/17/2016 4:38:36.819362 PM	78:9E:D0:C1:50:46	10:B7:F6:01:31:AF "Mini Boombox"	n/a	0x9f8c27c7f936d2a0289f08a14de9014d Valid	0xb641a4675484c1fb97dc78d2	n/a
🔒	8/17/2016 4:37:43.868282 PM ...	xx:xx:B0:6C:9A:F8	Enter BD_ADDR	n/a	Unable to validate		n/a
◐	8/17/2016 4:38:00.073238 PM ...	xx:xx:93:22:B7:CB	Enter BD_ADDR	n/a	Unable to validate		n/a
◐ 🔒	8/17/2016 4:38:46.054682 PM ...	00:09:93:E0:21:BC "My Car"	A4:84:31:FB:05:13 "SAMSUNG-SM-G930A-...	n/a	Unable to validate		n/a
⦶ 🔓	8/17/2016 4:38:47.456046 PM ...	78:9E:D0:C1:50:46	10:B7:F6:01:31:AF "Mini Boombox"	n/a	0x9f8c27c7f936d2a0289f08a14de9014d Valid	0xd64cc78dce8e50bd56210f6b	n/a

Figure 3.16 - Sodera Datasource Security Pane

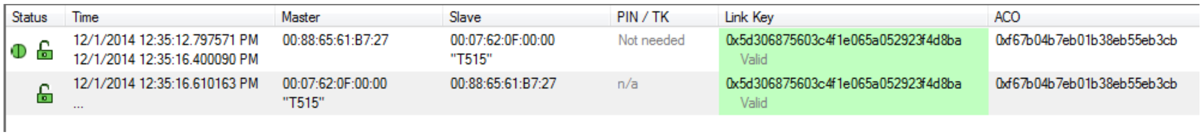
The **Security** pane shows events in the current capture. When the **Record** button is clicked, all devices with active traffic that require decryption are shown. Security events appear in starting time order with the most recent event at the bottom.

- **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 109 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

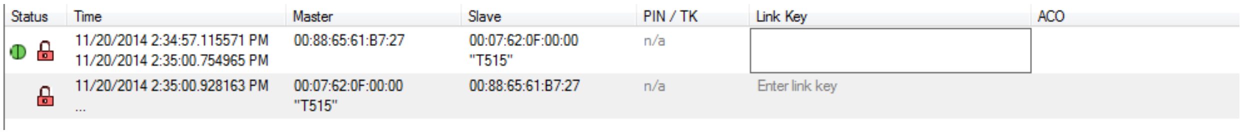
The first option uses a PIN to generate the Link Key. If the analyzer is given the PIN and has observed complete pairing it can determine the Link Key. Since the analyzer also needs other information exchanged between the two devices, the analyzer must catch the entire Pairing Process or else it cannot 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

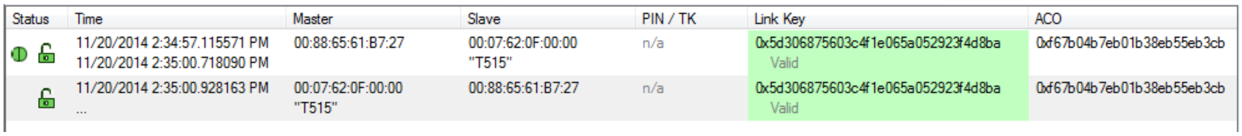
If you know the Link Key in advance you may enter it directly. To enter the Link Key click on the device row **Link Key** field and enter the Link Key in hex followed by the keyboard Enter key. If the link key has previously been entered it is automatically entered in the edit box after the Master and 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	

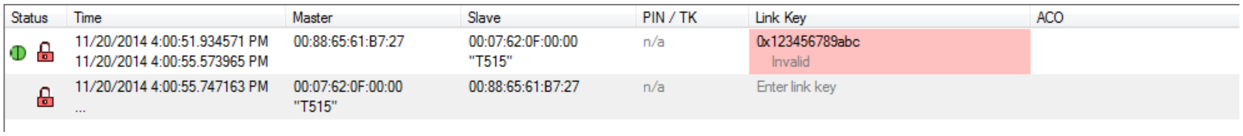
Figure 3.18 - Classic Bluetooth Link Key Entry



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..

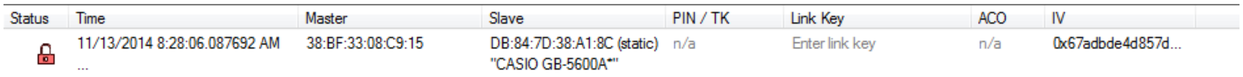
Note: Only one device in the link must be in SSP Debug Mode.

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.

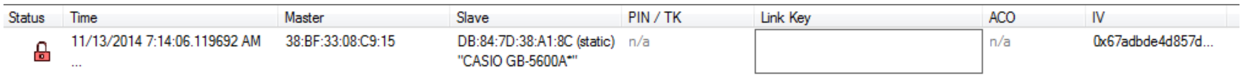


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔒	11/13/2014 8:28:06.087692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	Enter link key	n/a	0x67adbde4d857d...

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.

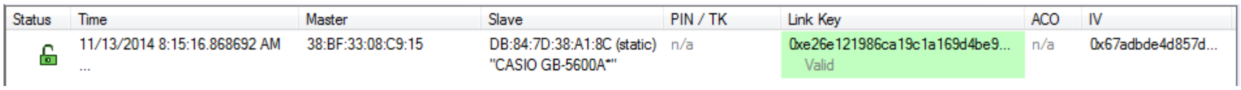


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔒	11/13/2014 7:14:06.119692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a		n/a	0x67adbde4d857d...

Figure 3.22 - Bluetooth low energy Enter Link Key

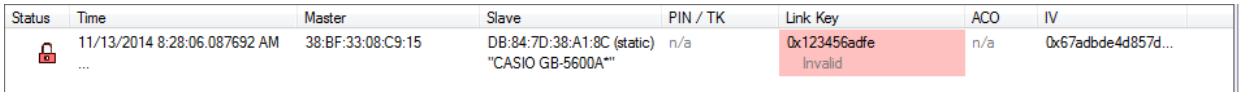
Press the Enter key or click outside the Link Key box. If the Link Key is valid the box will be green, beneath the Link Key will appear "Valid, and the Status will show an open, green lock indicating that decryption is enabled.

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

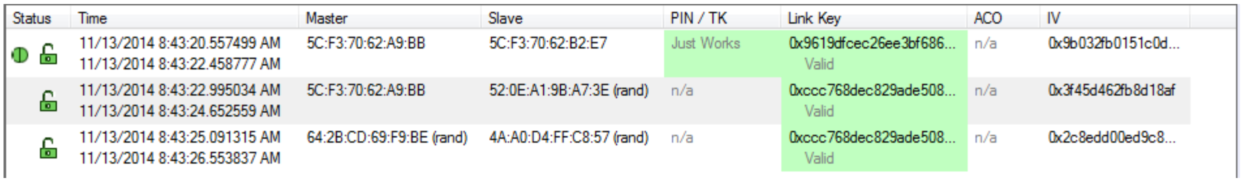


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔒	11/13/2014 8:28:06.087692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	0x123456adfe Invalid	n/a	0x67adbde4d857d...

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.

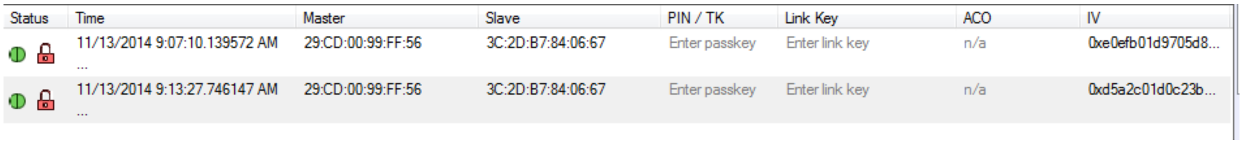


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
● 🔓	11/13/2014 8:43:20.557499 AM 11/13/2014 8:43:22.458777 AM	5C:F3:70:62:A9:BB	5C:F3:70:62:B2:E7	Just Works	0x9619dfcec26ee3bf686... Valid	n/a	0x9b032fb0151c0d...
🔓	11/13/2014 8:43:22.995034 AM 11/13/2014 8:43:24.652559 AM	5C:F3:70:62:A9:BB	52:0E:A1:9B:A7:3E (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

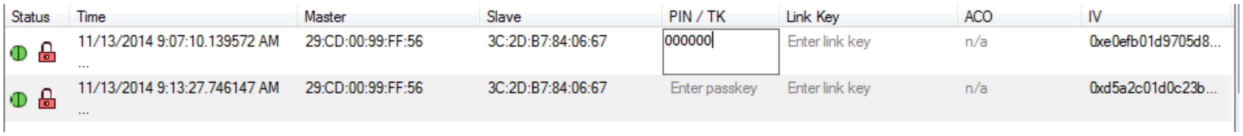
PIN is a six-digit decimal number. If a passkey is required by the device "Enter passkey" will appear in the device's **PIN/TK** field.



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.

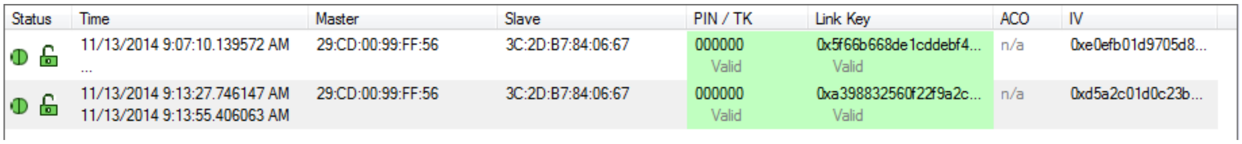


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
◑ 🔒	11/13/2014 9:07:10.139572 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	000000	Enter link key	n/a	0xe0efb01d9705d8...
◑ 🔒	11/13/2014 9:13:27.746147 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	Enter passkey	Enter link key	n/a	0xd5a2c01d0c23b...

Figure 3.27 - Bluetooth low energy Passkey Entry

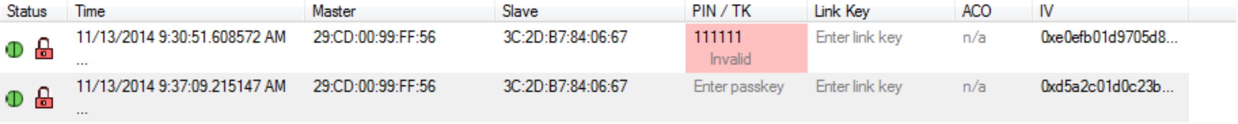
Press Enter or click outside the field. If the Passkey is correct it will appear in the **PIN/TK** field with "Valid" appearing below the passkey, **Link Key** field will automatically fill with the Link Key that will show "Valid" and appear green. The **Status** field will show an open, green lock to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

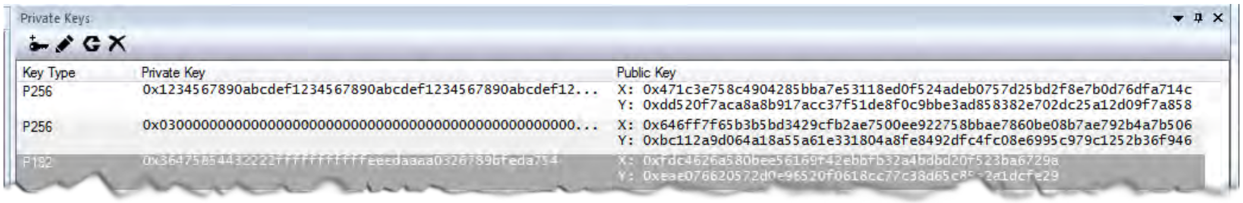
If a device requires OOB data the device Link Key field will show "Enter OOB TK".

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.



Key Type	Private Key	Public Key
P256	0x1234567890abcdef1234567890abcdef1234567890abcdef12...	X: 0x471c3e758c4904285bba7e53118ed0f524adeb0757d25bd2f8e7b0d76dfa714c Y: 0xdd520f7aca8a8b917acc37f51de8f0c9bbe3ad858382e702dc25a12d09f7a858
P256	0x0300000000000000000000000000000000000000000000000...	X: 0x646ff7f65b3b5bd3429cfb2ae7500ee922758bbae7860be08b7ae792b4a7b506 Y: 0xbc112a9d064a18a55a61e331804a8fe8492dfc4fc08e6995c979c1252b36f946
P192	0x364758544432222ffffffffffeeedaaaa0326789bfeda754	X: 0xfdc4626a580bee56169f42ebbfb32a4bdbd20f523ba6729a Y: 0xeae076620572d0e96520f0618cc77c38d65c8[illegible]2a1dcfe29

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

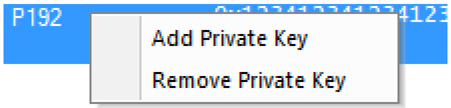
In the header of the **Private Keys** pane is a toolbar for adding or deleting keys.

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 68

Table 3.16 - Private Keys Management Tools (continued)

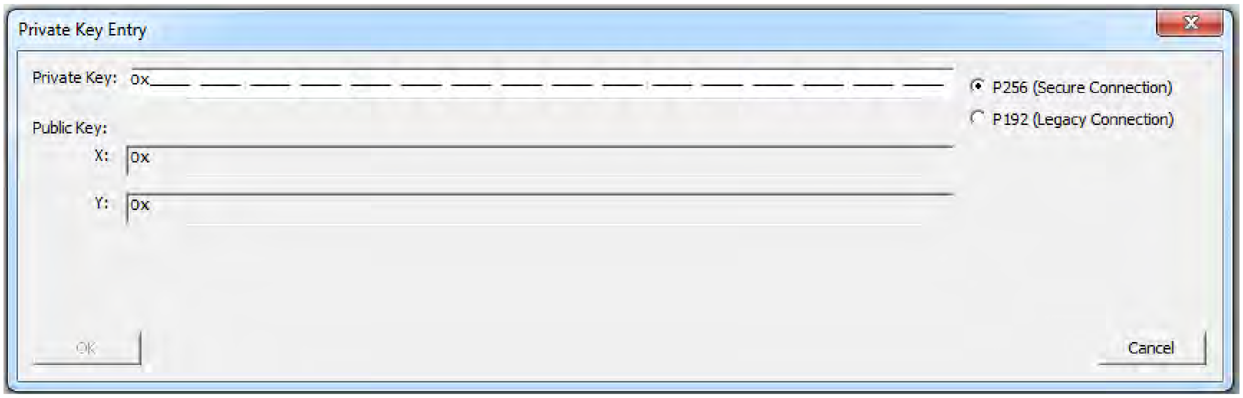
Tool	Icon	Descriptioin
Edit Selected Private Key	✎	Enabled when a private key in the pane is selected. When clicked, it opens the **Private Keys Entry** dialog with the selected Private and Public Key filled in. See Private Key Entry dialog on page 68
Reverse Private Key	↻	Enabled with a private key 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.
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.



Private Key: 0x

Public Key:

X: 0x

Y: 0x

● P256 (Secure Connection)

○ P192 (Legacy Connection)

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.

Table 3.17 - Private Key Entry Dialog Fields (continued)

Section	Field	Description
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:

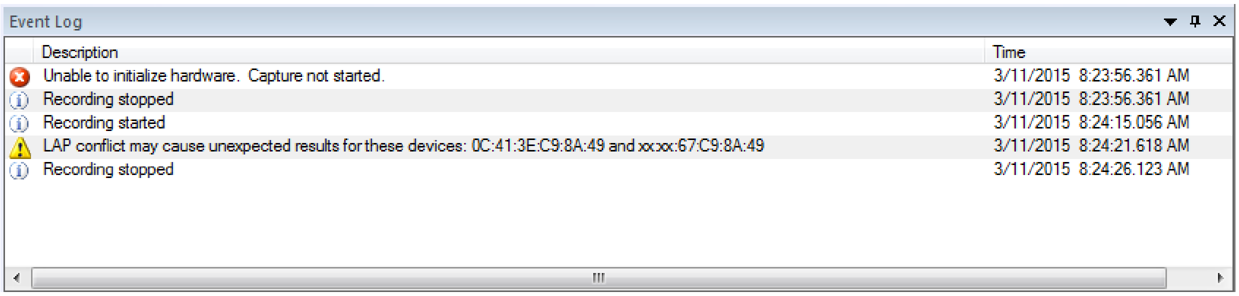
    a. Click on the **Remove Private Key** ✕ tool in the Private Key Management toolbar. The key is removed from the list.

    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.



Event Log

	Description	Time
⊗	Unable to initialize hardware. Capture not started.	3/11/2015 8:23:56.361 AM
ⓘ	Recording stopped	3/11/2015 8:23:56.361 AM
ⓘ	Recording started	3/11/2015 8:24:15.056 AM
⚠	LAP conflict may cause unexpected results for these devices: 0C:41:3E:C9:8A:49 and xx:xx:67:C9:8A:49	3/11/2015 8:24:21.618 AM
ⓘ	Recording stopped	3/11/2015 8:24:26.123 AM

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.

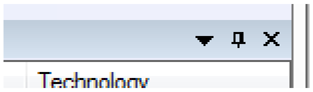
Table 3.18 - Event Log Columns

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

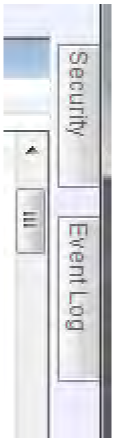
The Event log is automatically saved to "%appdata%\Frontline Test Equipment\Sodera\Logs\" as a .txt file. Logs are retained for each session.

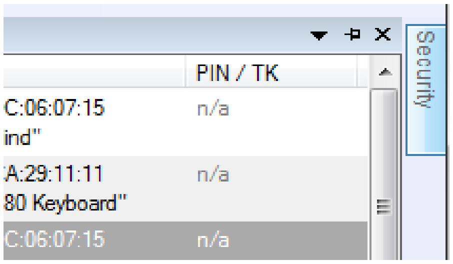
3.1.2.8 Pane Positioning and Control



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.

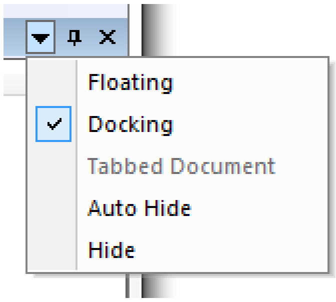




Hovering over the hidden pane title will expand the pane and the **Auto Hide** icon appears rotated 📌.

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

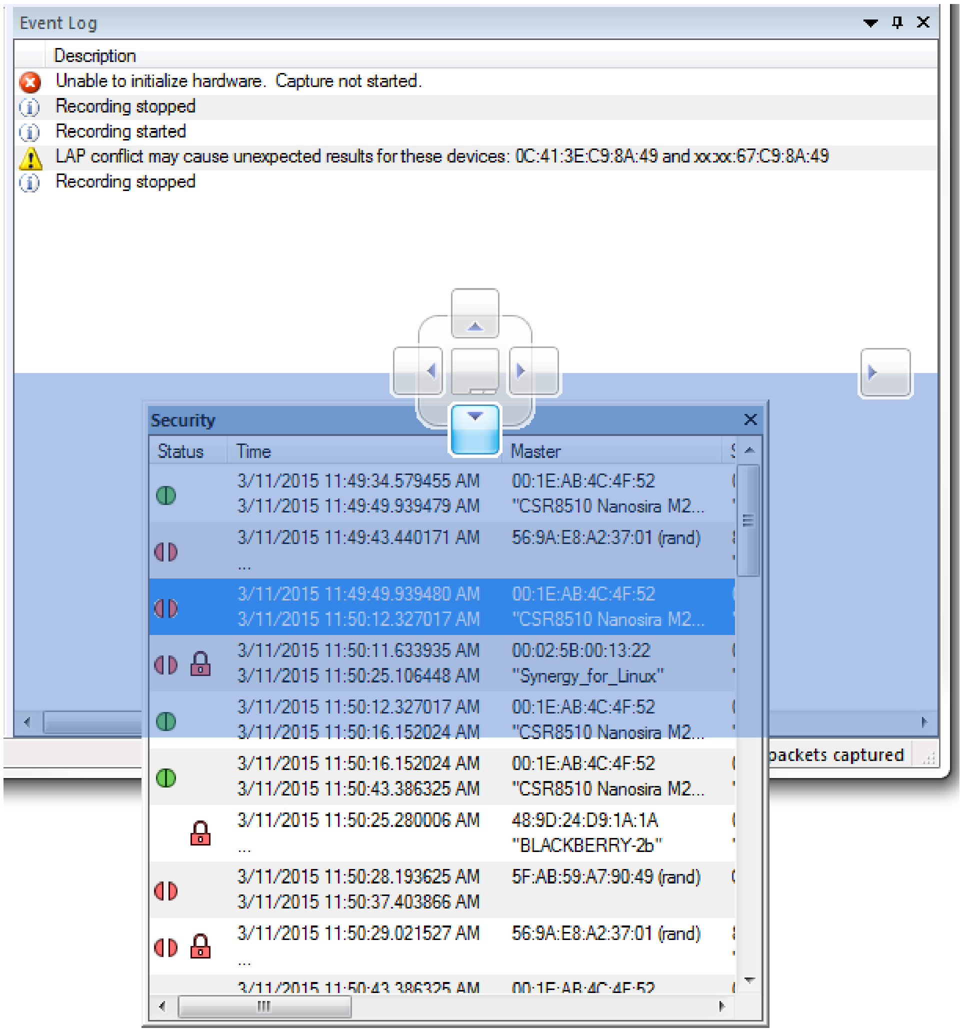
Positioning by Cursor

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



Description
Unable to initialize hardware. Capture not started.
Recording stopped
Recording started
LAP conflict may cause unexpected results for these devices: 0C:41:3E:C9:8A:49 and xx:xx:67:C9:8A:49
Recording stopped

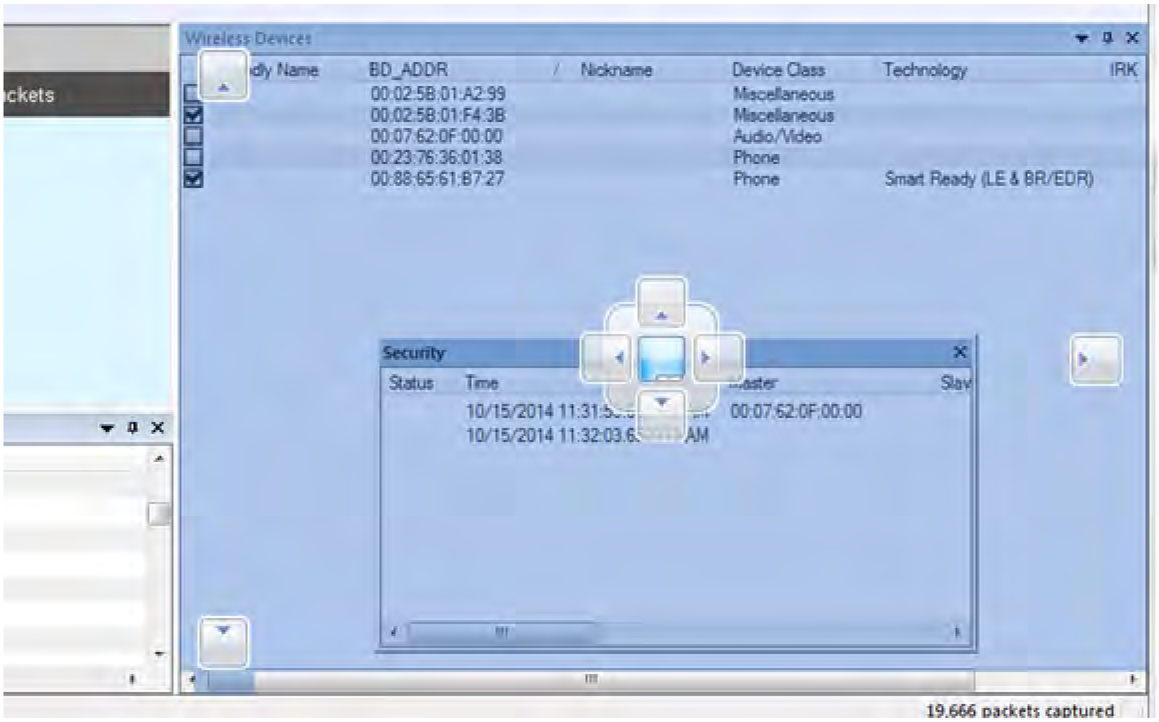
Status	Time	Master
●	3/11/2015 11:49:34.579455 AM 3/11/2015 11:49:49.939479 AM	00:1E:AB:4C:4F:52 "CSR8510 Nanosira M2...
●	3/11/2015 11:49:43.440171 AM ...	56:9A:E8:A2:37:01 (rand)
●	3/11/2015 11:49:49.939480 AM 3/11/2015 11:50:12.327017 AM	00:1E:AB:4C:4F:52 "CSR8510 Nanosira M2...
● 🔒	3/11/2015 11:50:11.633935 AM 3/11/2015 11:50:25.106448 AM	00:02:5B:00:13:22 "Synergy_for_Linux"
●	3/11/2015 11:50:12.327017 AM 3/11/2015 11:50:16.152024 AM	00:1E:AB:4C:4F:52 "CSR8510 Nanosira M2...
●	3/11/2015 11:50:16.152024 AM 3/11/2015 11:50:43.386325 AM	00:1E:AB:4C:4F:52 "CSR8510 Nanosira M2...
🔒	3/11/2015 11:50:25.280006 AM ...	48:9D:24:D9:1A:1A "BLACKBERRY-2b"
●	3/11/2015 11:50:28.193625 AM 3/11/2015 11:50:37.403866 AM	5F:AB:59:A7:90:49 (rand)
● 🔒	3/11/2015 11:50:29.021527 AM ...	56:9A:E8:A2:37:01 (rand)
	3/11/2015 11:50:43.386325 AM	00:1E:AB:4C:4F:52

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



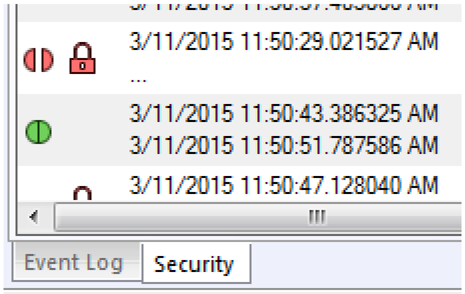
Wireless Devices

	...dly Name	BD_ADDR	Nickname	Device Class	Technology	IRK
□		00:02:5B:01:A2:99		Miscellaneous		
☑		00:02:5B:01:F4:3B		Miscellaneous		
□		00:07:62:0F:00:00		Audio/Video		
□		00:23:76:36:01:38		Phone		
☑		00:88:65:61:B7:27		Phone	Smart Ready (LE & BR/EDR)	

Security

Status	Time	...aster	Slav...
	10/15/2014 11:31:5...	00:07:62:0F:00:00	
	10/15/2014 11:32:03.6... AM		

Figure 3.34 - Position Control for Setting Tabbed Security Pane



```
3/11/2015 11:50:29.021527 AM
...
3/11/2015 11:50:43.386325 AM
3/11/2015 11:50:51.787586 AM
3/11/2015 11:50:47.128040 AM
```

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.

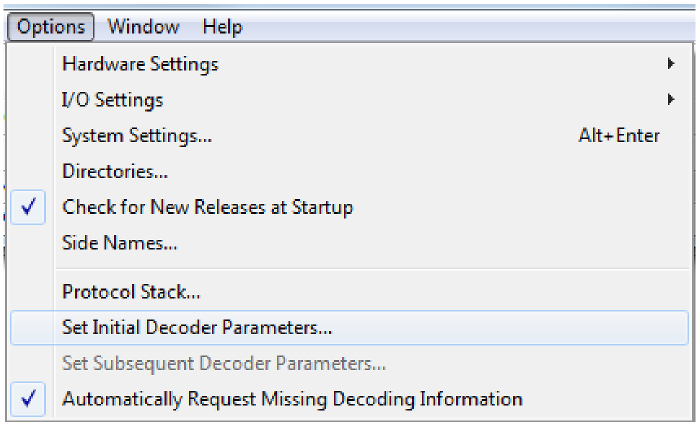

Options
Window
Help
Hardware Settings
I/O Settings
System Settings... Alt+Enter
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

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.

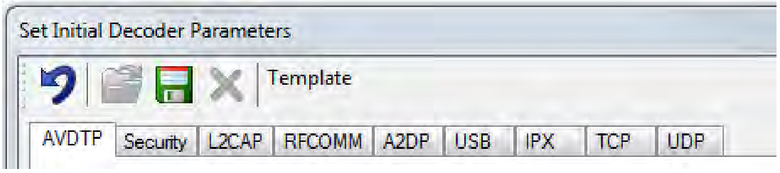


Figure 3.36 - Tabs for each decoder requiring parameters.

- 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.

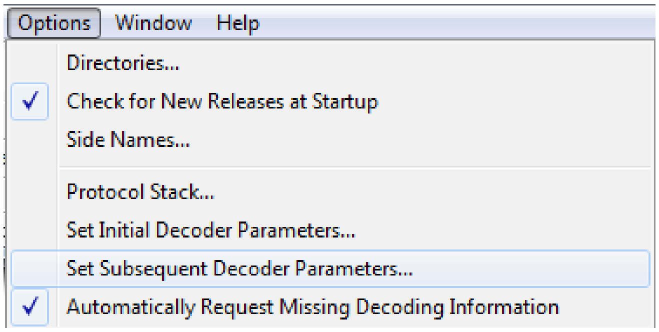
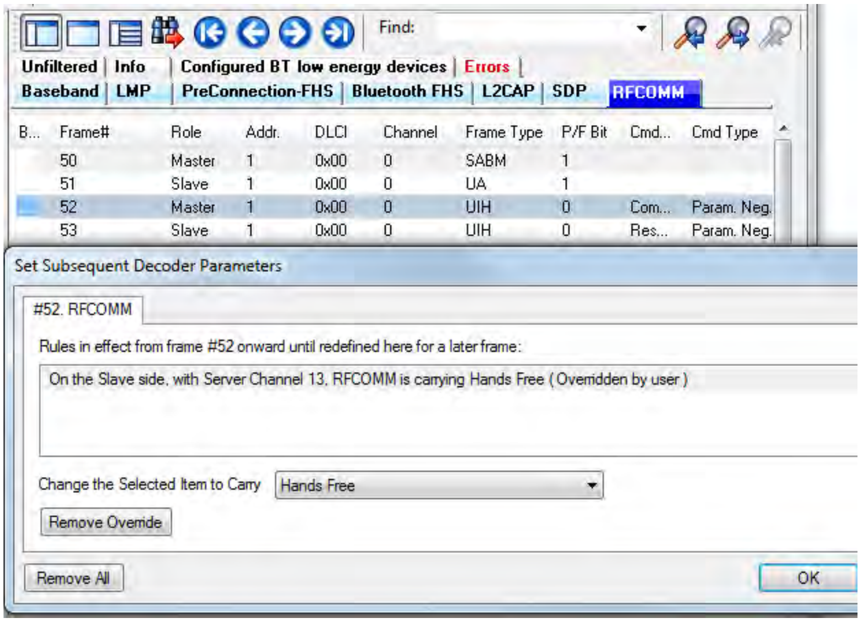

Options
Window
Help
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

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


Find:
Unfiltered | Info | Configured BT low energy devices | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM

B...	Frame#	Role	Addr.	DLCI	Channel	Frame Type	P/F Bit	Cmd...	Cmd Type
	50	Master	1	0x00	0	SABM	1		
	51	Slave	1	0x00	0	UA	1		
	52	Master	1	0x00	0	UIH	0	Com...	Param. Neg.
	53	Slave	1	0x00	0	UIH	0	Res...	Param. Neg.

Set Subsequent Decoder Parameters

#52. RFCOMM

Rules in effect from frame #52 onward until redefined here for a later frame:

On the Slave side, with Server Channel 13, RFCOMM is carrying Hands Free (Overridden by user)

Change the Selected Item to Carry: Hands Free

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.

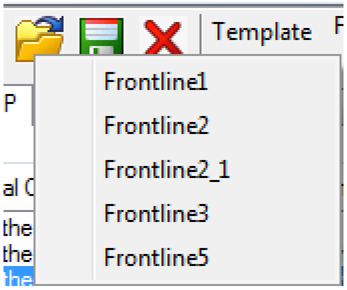
If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

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

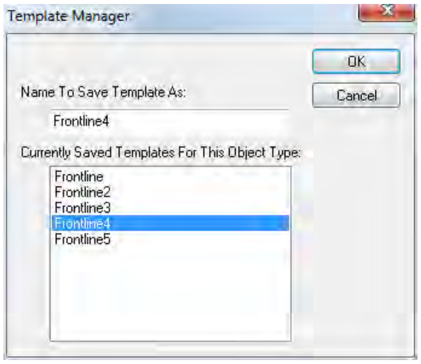
A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

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.



Name To Save Template As:

Frontline4

Currently Saved Templates For This Object Type:

Frontline
Frontline2
Frontline3
Frontline4
Frontline5

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

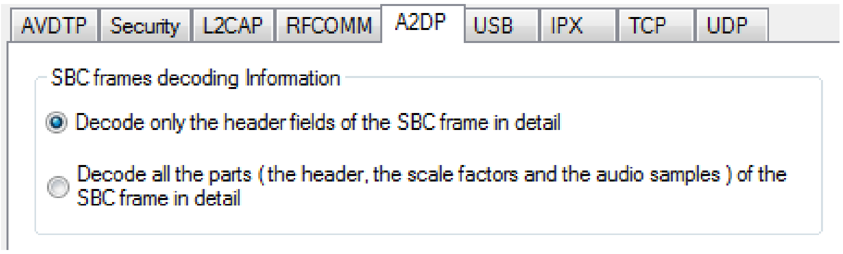
Decoding SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame. You can increase the decoding speed by decoding only the header fields and disregarding other parts. You can select the detail-level of decoding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



SBC frames decoding Information

● Decode only the header fields of the SBC frame in detail

○ Decode all the parts (the header, the scale factors and the audio samples) of the SBC frame in detail

Figure 3.39 - A2DP Decoder Settings

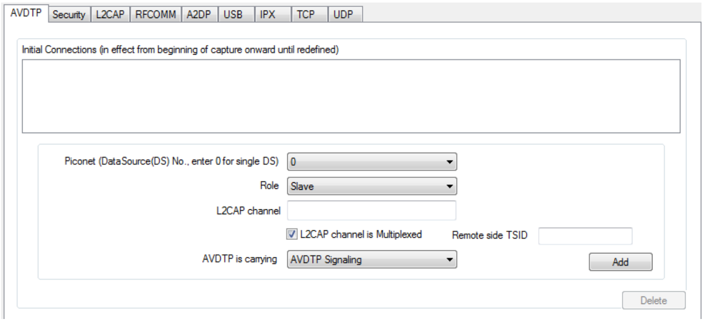
4. Follow steps to save the template changes or to save a new template.

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.



Initial Connections (in effect from beginning of capture onward until redefined)

Piconet (DataSource(DS) No., enter 0 for single DS) 0

Role Slave

L2CAP channel

☑ L2CAP channel is Multiplexed Remote side TSID

AVDTP is carrying AVDTP Signaling

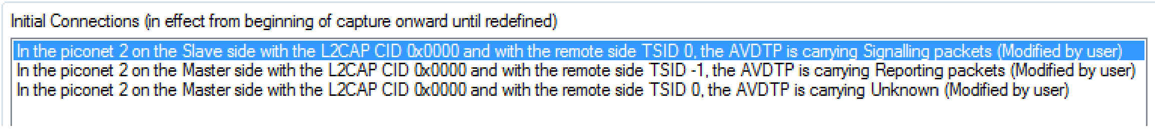
Figure 3.40 - AVDTP parameters tab

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.



Initial Connections (in effect from beginning of capture onward until redefined)

In the piconet 2 on the Slave side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Signalling packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID -1, the AVDTP is carrying Reporting packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Unknown (Modified by user)

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:

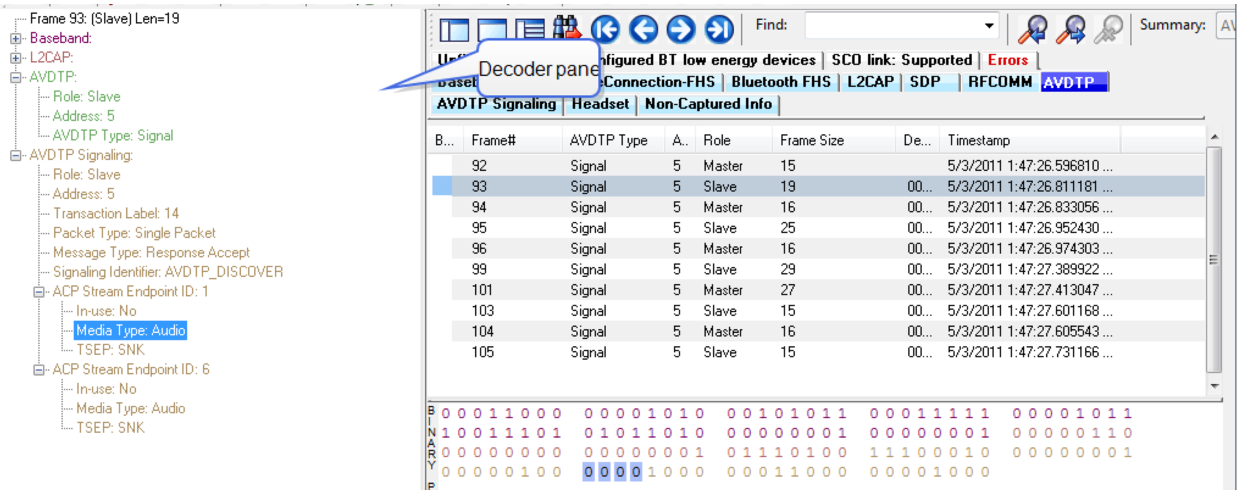
- The capture session started after transmission of the vital information.
- The analyzer incorrectly received a frame with the traversal information.
- The communication monitored takes place between two players with implicit information not included in the transmission.

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.



```
Frame 93: (Slave) Len=19
+ Baseband:
+ L2CAP:
- AVDTP:
    Role: Slave
    Address: 5
    AVDTP Type: Signal
- AVDTP Signaling:
    Role: Slave
    Address: 5
    Transaction Label: 14
    Packet Type: Single Packet
    Message Type: Response Accept
    Signaling Identifier: AVDTP_DISCOVER
  - ACP Stream Endpoint ID: 1
      In-use: No
      Media Type: Audio
      TSEP: SNK
  - ACP Stream Endpoint ID: 6
      In-use: No
      Media Type: Audio
      TSEP: SNK
```

B...	Frame#	AVDTP Type	A..	Role	Frame Size	De...	Timestamp
	92	Signal	5	Master	15		5/3/2011 1:47:26.596810 ...
	93	Signal	5	Slave	19	00...	5/3/2011 1:47:26.811181 ...
	94	Signal	5	Master	16	00...	5/3/2011 1:47:26.833056 ...
	95	Signal	5	Slave	25	00...	5/3/2011 1:47:26.952430 ...
	96	Signal	5	Master	16	00...	5/3/2011 1:47:26.974303 ...
	99	Signal	5	Slave	29	00...	5/3/2011 1:47:27.389922 ...
	101	Signal	5	Master	27	00...	5/3/2011 1:47:27.413047 ...
	103	Signal	5	Slave	15	00...	5/3/2011 1:47:27.601168 ...
	104	Signal	5	Master	16	00...	5/3/2011 1:47:27.605543 ...
	105	Signal	5	Slave	15	00...	5/3/2011 1:47:27.731166 ...

```
BINARY
0 0 0 1 1 0 0 0   0 0 0 0 1 0 1 0   0 0 1 0 1 0 1 1   0 0 0 1 1 1 1 1   0 0 0 0 1 0 1 1
1 0 0 1 1 1 0 1   0 1 0 1 1 0 1 0   0 0 0 0 0 0 0 1   0 0 0 0 0 0 0 1   0 0 0 0 0 1 1 0
0 0 0 0 0 0 0 0   0 0 0 0 0 0 0 1   0 1 1 1 0 1 0 0   1 1 1 0 0 0 1 0   0 0 0 0 0 0 0 1
0 0 0 0 0 1 0 0   0 0 0 0 1 0 0 0   0 0 0 1 1 0 0 0   0 0 0 0 1 0 0 0
```

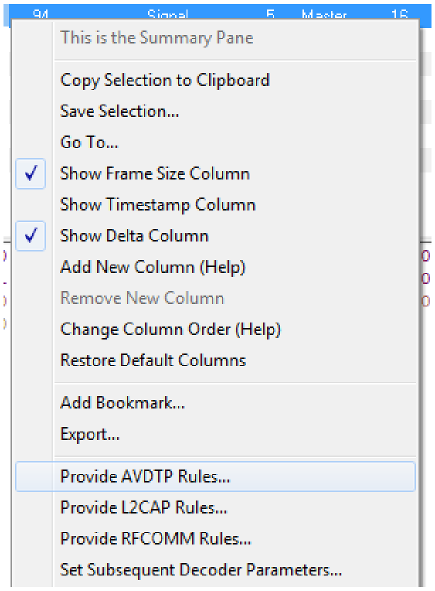
Figure 3.42 - Look in Decoder pane for profile hints

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.

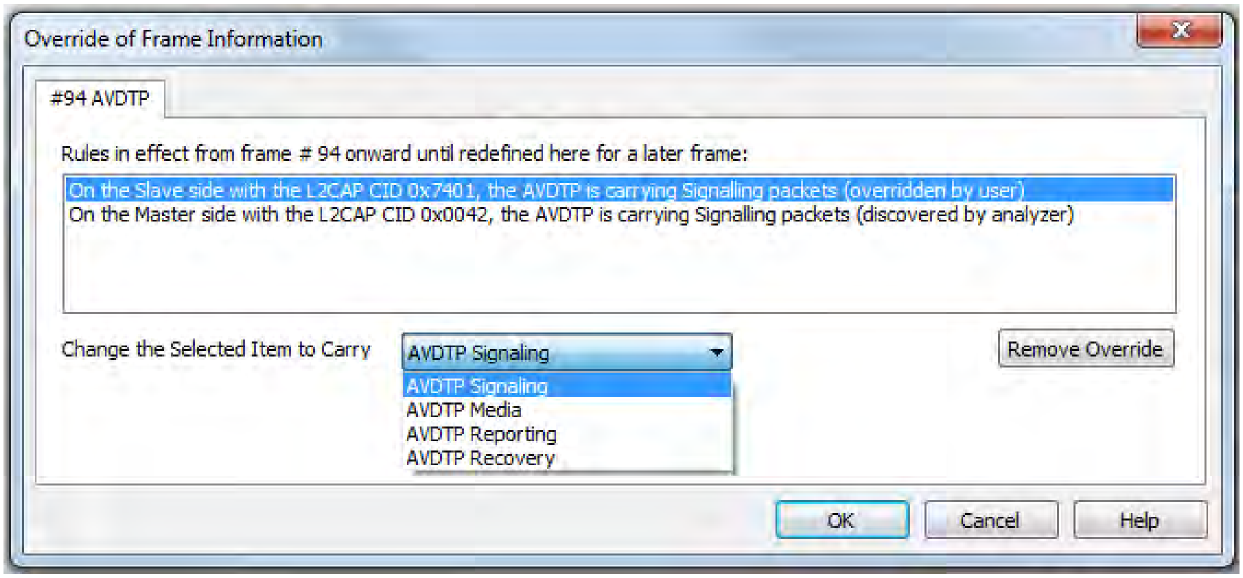
If you have a parameter in effect and wish to change that parameter:

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.



Override of Frame Information

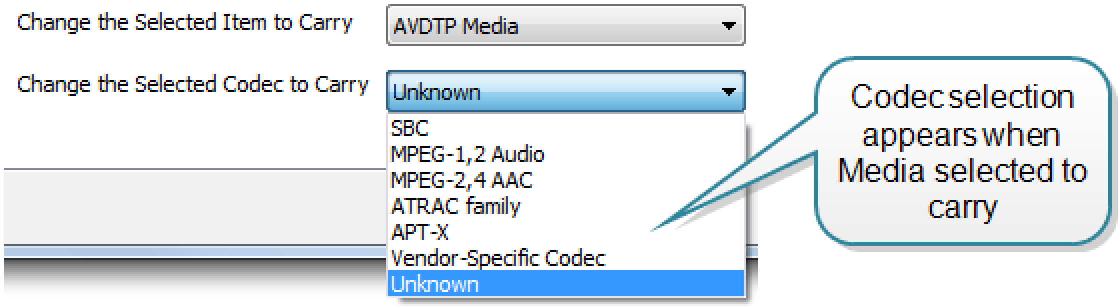
#94 AVDTP

Rules in effect from frame # 94 onward until redefined here for a later frame:

On the Slave side with the L2CAP CID 0x7401, the AVDTP is carrying Signalling packets (overridden by user)
On the Master side with the L2CAP CID 0x0042, the AVDTP is carrying Signalling packets (discovered by analyzer)

Change the Selected Item to Carry: AVDTP Signaling

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



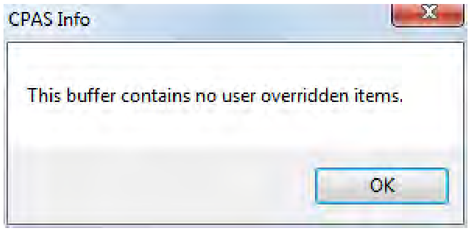
Change the Selected Item to Carry: AVDTP Media

Change the Selected Codec to Carry: Unknown

Codec selection appears when Media selected 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.



CPAS Info

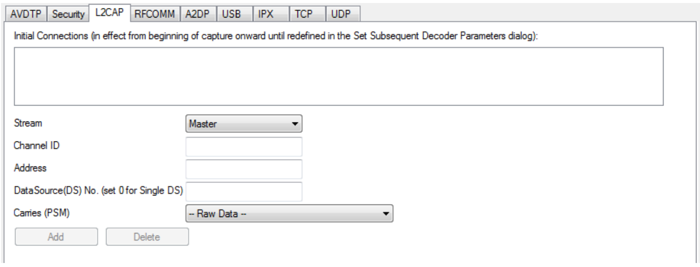
This buffer contains no user overridden items.

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.



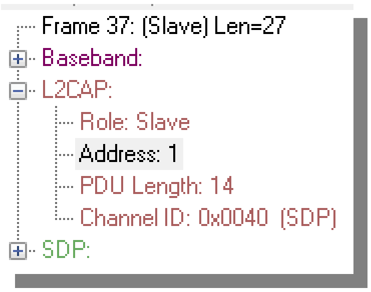
Initial Connections (in effect from beginning of capture onward until redefined in the Set Subsequent Decoder Parameters dialog):

Stream: Master
Channel ID:
Address:
DataSource(DS) No. (set 0 for Single DS):
Carries (PSM): -- Raw Data --

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.



Frame 37: (Slave) Len=27
Baseband:
L2CAP:
Role: Slave
Address: 1
PDU Length: 14
Channel ID: 0x0040 (SDP)
SDP:

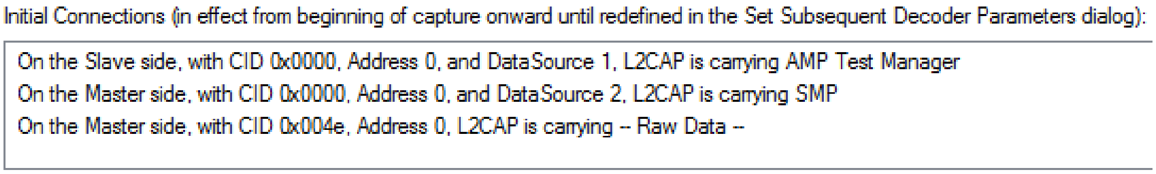
Carries (PSM) - Select the protocol that L2CAP traverses to from the following:

- 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

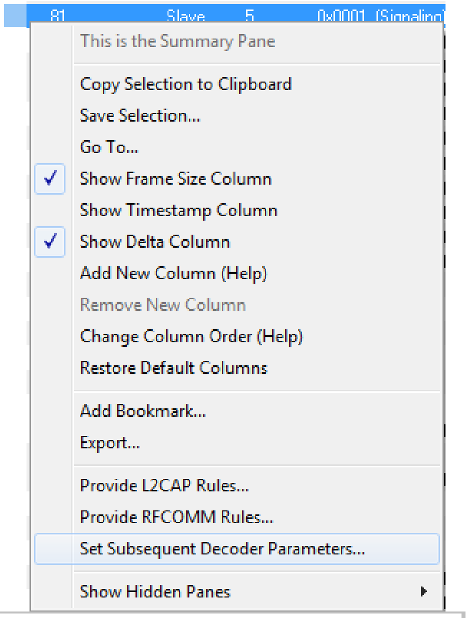
4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and 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**.



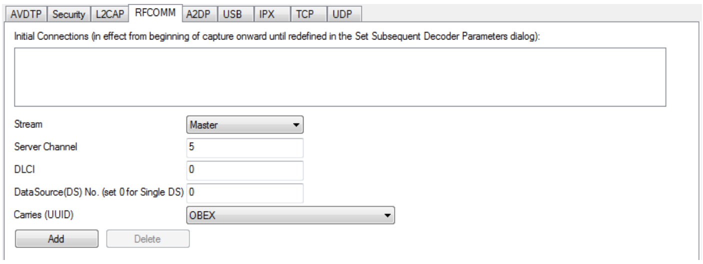
Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

> **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.



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

Stream	Master
Server Channel	5
DLCI	0
DataSource(DS) No. (set 0 for Single DS)	0
Carries (UUID)	OBEX

Figure 3.47 - RFCOMM parameters tab

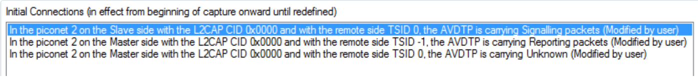
The **RFCOMM Set Initial Decoder Parameters** tab requires the following user inputs to complete a parameter:

- **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.



Initial Connections (in effect from beginning of capture onward until redefined)

In the piconet 2 on the Slave side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Signalling packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID -1, the AVDTP is carrying Reporting packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Unknown (Modified by user)

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.

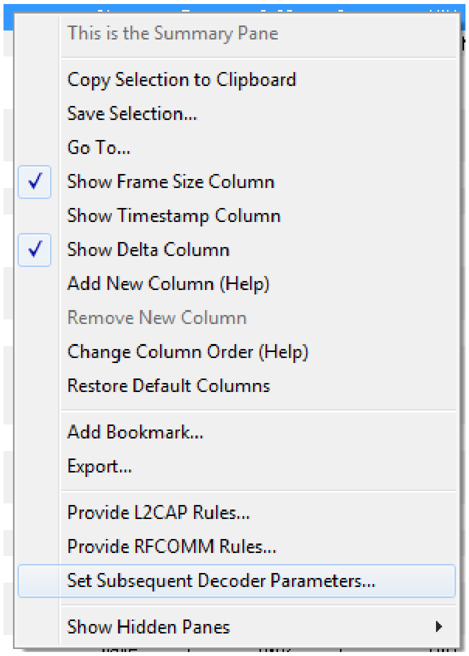
If you are not sure of the payload carried by the subject frame, look at the raw data shown under **data** in the **Decode** pane in the **Frame Display**. You may notice something that hints as to the profile in use.

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

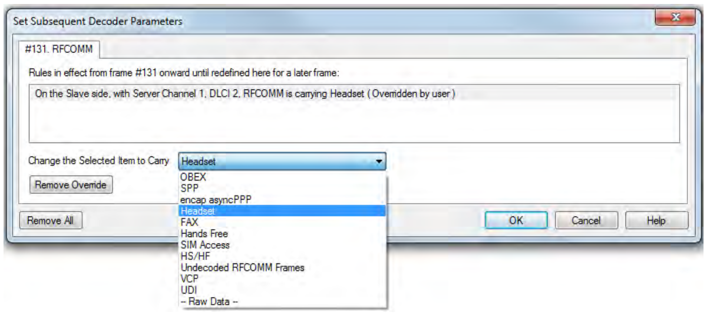
The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

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.



Set Subsequent Decoder Parameters

#131. RFCOMM

Rules in effect from frame #131 onward until redefined here for a later frame:

On the Slave side, with Server Channel 1, DLCI 2, RFCOMM is carrying Headset (Overridden by user)

Change the Selected Item to Carry: Headset

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 345 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,

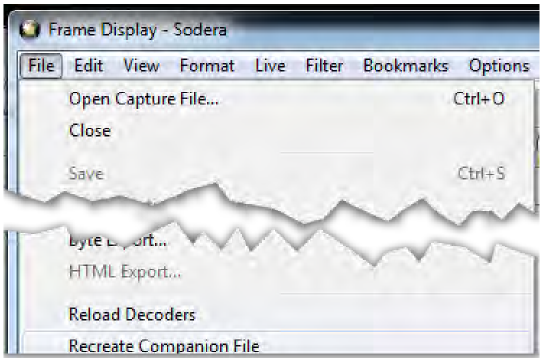
Table 3.20 - CSRmesh Key Set Format

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
```

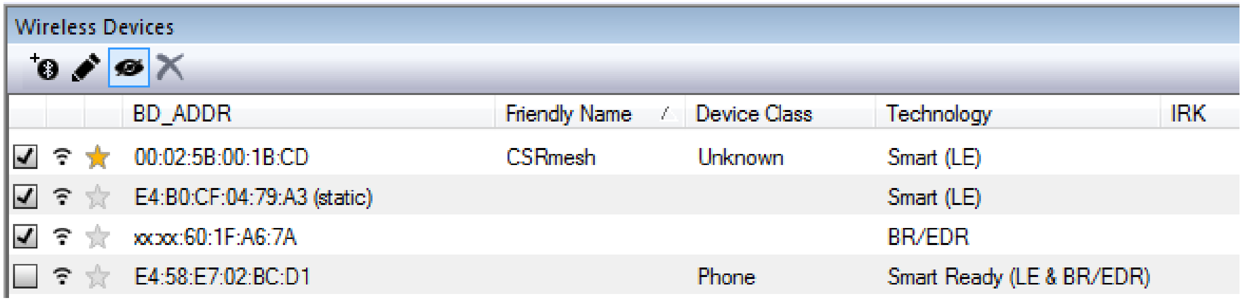
Loading keys or key sets



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



Wireless Devices

			BD_ADDR	Friendly Name	Device Class	Technology	IRK
☑		★	00:02:5B:00:1B:CD	CSRmesh	Unknown	Smart (LE)	
☑		☆	E4:B0:CF:04:79:A3 (static)			Smart (LE)	
☑		☆	xx:xx:60:1F:A6:7A			BR/EDR	
□		☆	E4:58:E7:02:BC:D1		Phone	Smart Ready (LE & BR/EDR)	

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 Analyze .

CSRmesh over GATT

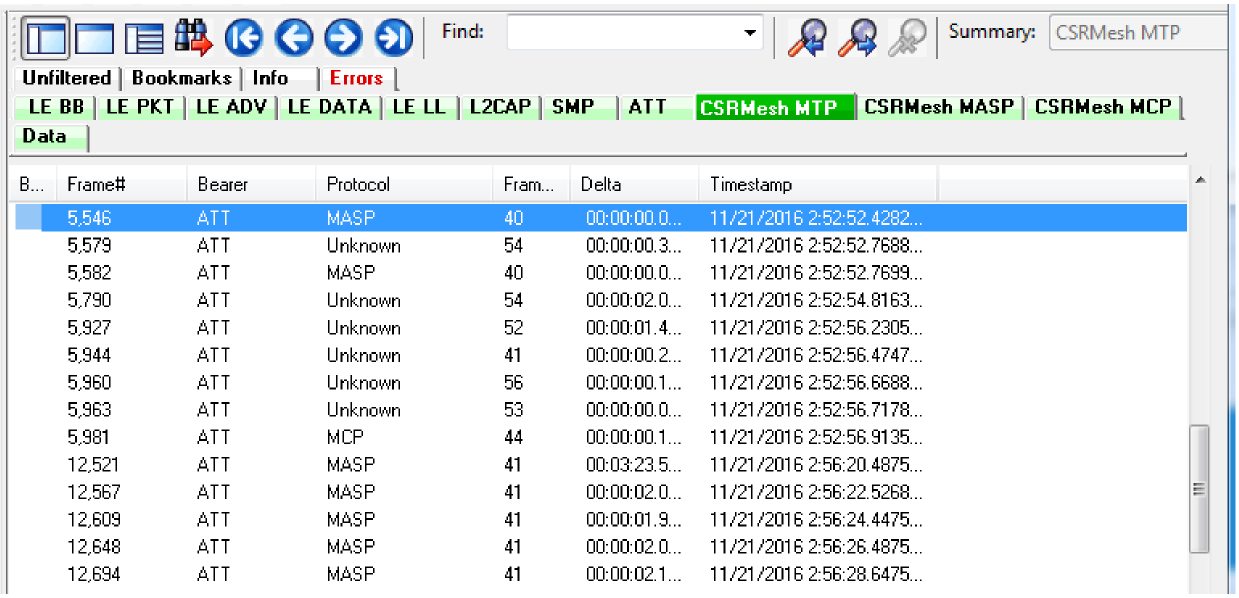
ATT maintains a database which maps handles & UUIDs. When there is a connection request the mappings will be loaded to the initiator and/or advertiser sides of the database.

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 354.

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.



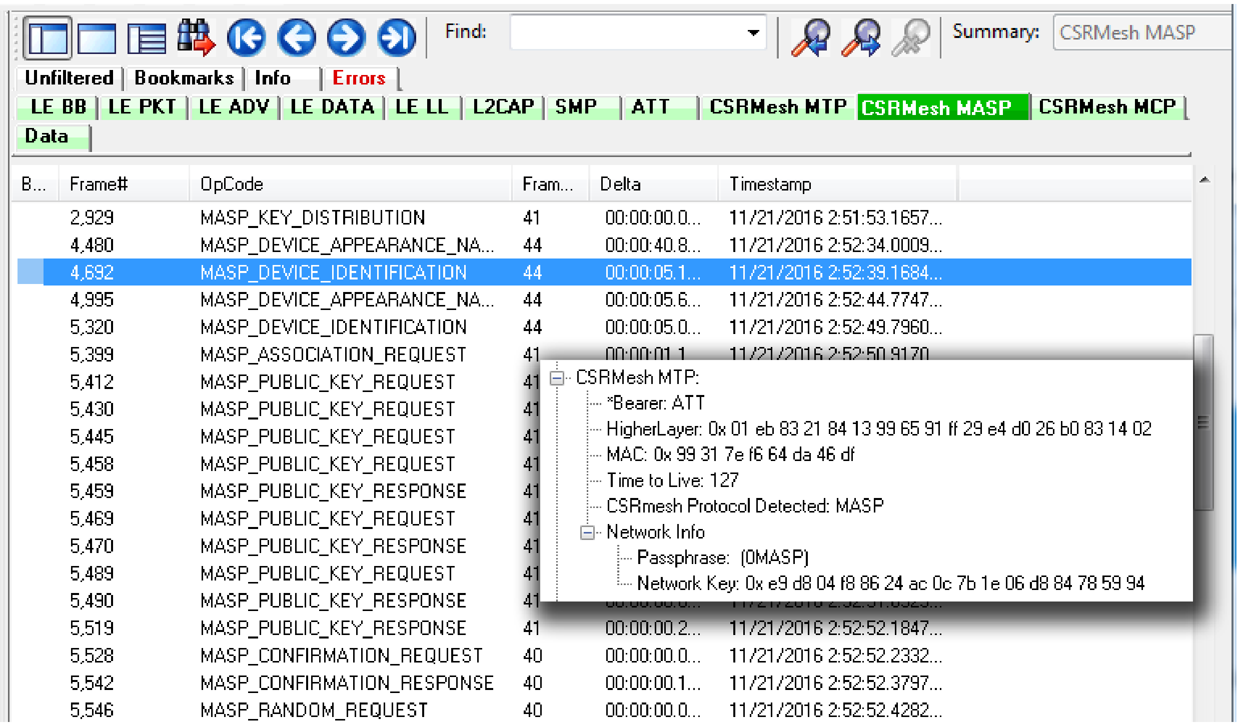
B...	Frame#	Bearer	Protocol	Fram...	Delta	Timestamp
	5,546	ATT	MASP	40	00:00:00.0...	11/21/2016 2:52:52.4282...
	5,579	ATT	Unknown	54	00:00:00.3...	11/21/2016 2:52:52.7688...
	5,582	ATT	MASP	40	00:00:00.0...	11/21/2016 2:52:52.7699...
	5,790	ATT	Unknown	54	00:00:02.0...	11/21/2016 2:52:54.8163...
	5,927	ATT	Unknown	52	00:00:01.4...	11/21/2016 2:52:56.2305...
	5,944	ATT	Unknown	41	00:00:00.2...	11/21/2016 2:52:56.4747...
	5,960	ATT	Unknown	56	00:00:00.1...	11/21/2016 2:52:56.6688...
	5,963	ATT	Unknown	53	00:00:00.0...	11/21/2016 2:52:56.7178...
	5,981	ATT	MCP	44	00:00:00.1...	11/21/2016 2:52:56.9135...
	12,521	ATT	MASP	41	00:03:23.5...	11/21/2016 2:56:20.4875...
	12,567	ATT	MASP	41	00:00:02.0...	11/21/2016 2:56:22.5268...
	12,609	ATT	MASP	41	00:00:01.9...	11/21/2016 2:56:24.4475...
	12,648	ATT	MASP	41	00:00:02.0...	11/21/2016 2:56:26.4875...
	12,694	ATT	MASP	41	00:00:02.1...	11/21/2016 2:56:28.6475...

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 92 shows the Decoder pane (inset) with the "Network Info" passphrase and network key shown but there is no network name.

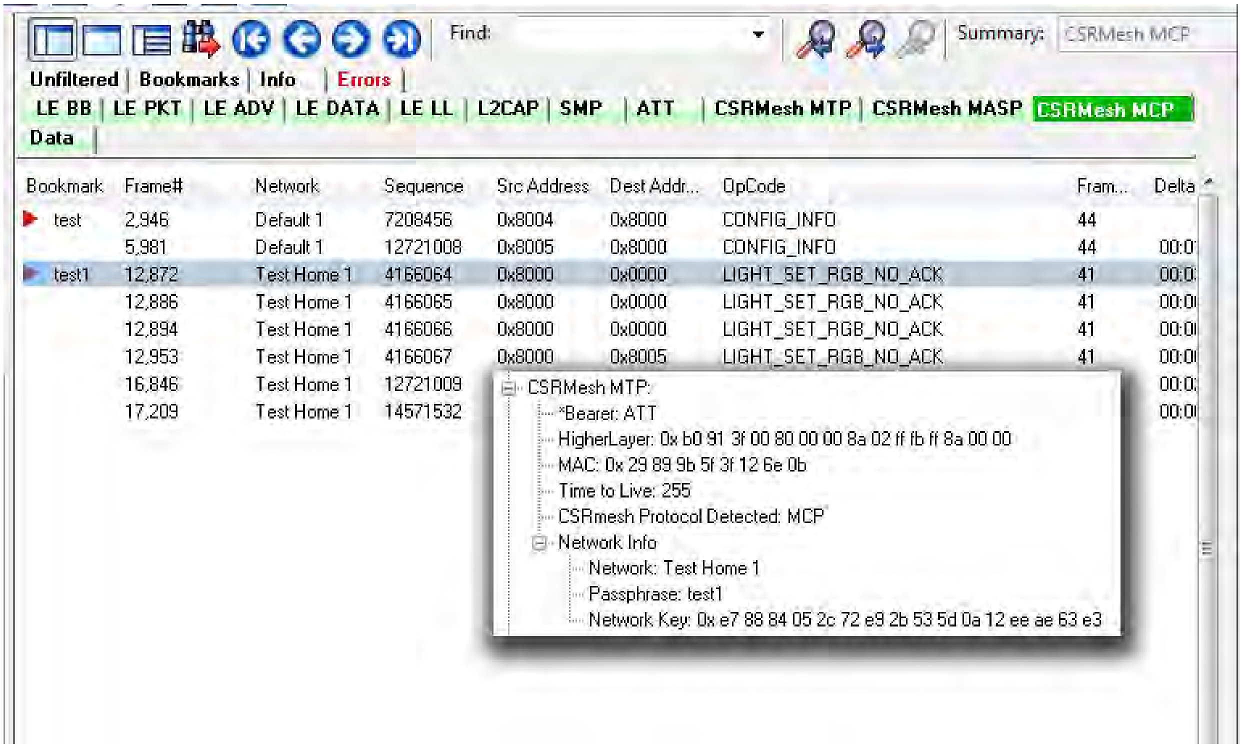

Find:
Summary: CSRMesh MASP
Unfiltered | Bookmarks | Info | Errors
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT | CSRMesh MTP | CSRMesh MASP | CSRMesh MCP | Data

B...	Frame#	OpCode	Fram...	Delta	Timestamp
	2,929	MASP_KEY_DISTRIBUTION	41	00:00:00.0...	11/21/2016 2:51:53.1657...
	4,480	MASP_DEVICE_APPEARANCE_NA...	44	00:00:40.8...	11/21/2016 2:52:34.0009...
	4,692	MASP_DEVICE_IDENTIFICATION	44	00:00:05.1...	11/21/2016 2:52:39.1684...
	4,995	MASP_DEVICE_APPEARANCE_NA...	44	00:00:05.6...	11/21/2016 2:52:44.7747...
	5,320	MASP_DEVICE_IDENTIFICATION	44	00:00:05.0...	11/21/2016 2:52:49.7960...
	5,399	MASP_ASSOCIATION_REQUEST	41	00:00:01.1	11/21/2016 2:52:50.9170
	5,412	MASP_PUBLIC_KEY_REQUEST	41		
	5,430	MASP_PUBLIC_KEY_REQUEST	41		
	5,445	MASP_PUBLIC_KEY_REQUEST	41		
	5,458	MASP_PUBLIC_KEY_REQUEST	41		
	5,459	MASP_PUBLIC_KEY_RESPONSE	41		
	5,469	MASP_PUBLIC_KEY_REQUEST	41		
	5,470	MASP_PUBLIC_KEY_RESPONSE	41		
	5,489	MASP_PUBLIC_KEY_REQUEST	41		
	5,490	MASP_PUBLIC_KEY_RESPONSE	41		
	5,519	MASP_PUBLIC_KEY_RESPONSE	41	00:00:00.2...	11/21/2016 2:52:52.1847...
	5,528	MASP_CONFIRMATION_REQUEST	40	00:00:00.0...	11/21/2016 2:52:52.2332...
	5,542	MASP_CONFIRMATION_RESPONSE	40	00:00:00.1...	11/21/2016 2:52:52.3797...
	5,546	MASP_RANDOM_REQUEST	40	00:00:00.0...	11/21/2016 2:52:52.4282...

```
CSRMesh MTP:
    *Bearer: ATT
    HigherLayer: 0x 01 eb 83 21 84 13 99 65 91 ff 29 e4 d0 26 b0 83 14 02
    MAC: 0x 99 31 7e f6 64 da 46 df
    Time to Live: 127
    CSRmesh Protocol Detected: MASP
    Network Info
        Passphrase:  (0MASP)
        Network Key: 0x e9 d8 04 f8 86 24 ac 0c 7b 1e 06 d8 84 78 59 94
```

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 93 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.



Bookmark	Frame#	Network	Sequence	Src Address	Dest Addr...	OpCode	Fram...	Delta
test	2,946	Default 1	7208456	0x8004	0x8000	CONFIG_INFO	44	
	5,981	Default 1	12721008	0x8005	0x8000	CONFIG_INFO	44	00:0
test1	12,872	Test Home 1	4166064	0x8000	0x0000	LIGHT_SET_RGB_NO_ACK	41	00:0
	12,886	Test Home 1	4166065	0x8000	0x0000	LIGHT_SET_RGB_NO_ACK	41	00:0
	12,894	Test Home 1	4166066	0x8000	0x0000	LIGHT_SET_RGB_NO_ACK	41	00:0
	12,953	Test Home 1	4166067	0x8000	0x8005	LIGHT_SET_RGB_NO_ACK	41	00:0
	16,846	Test Home 1	12721009					00:0
	17,209	Test Home 1	14571532					00:0

```
CSRMesh MTP:
    *Bearer: ATT
    HigherLayer: 0x b0 91 3f 00 80 00 00 8a 02 ff fb ff 8a 00 00
    MAC: 0x 29 89 9b 5f 3f 12 6e 0b
    Time to Live: 255
    CSRmesh Protocol Detected: MCP
    Network Info
        Network: Test Home 1
        Passphrase: test1
        Network Key: 0x e7 88 84 05 2c 72 e9 2b 53 5d 0a 12 ee ae 63 e3
```

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

Troubleshooting Tips

MeshOptions.ini Errors

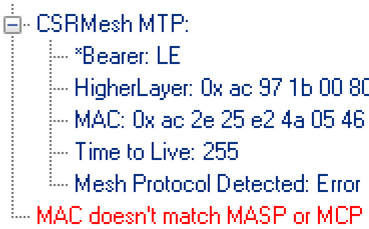
Table 3.21 - Errors Associated with MeshOptions.ini

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.



```
CSRMesh MTP:
    *Bearer: LE
    HigherLayer: 0x ac 97 1b 00 80 46 65 93 4a e2
    MAC: 0x ac 2e 25 e2 4a 05 46 2d
    Time to Live: 255
    Mesh Protocol Detected: Error
MAC doesn't match MASP or MCP
```

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

Table 3.22 - Errors: Bluetooth technology using mesh networking (continued)

Error	Description
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 Bluetooth 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 Bluetooth.

“Conductive” in this context means that you are not “air sniffing”, that is, capturing Bluetooth 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

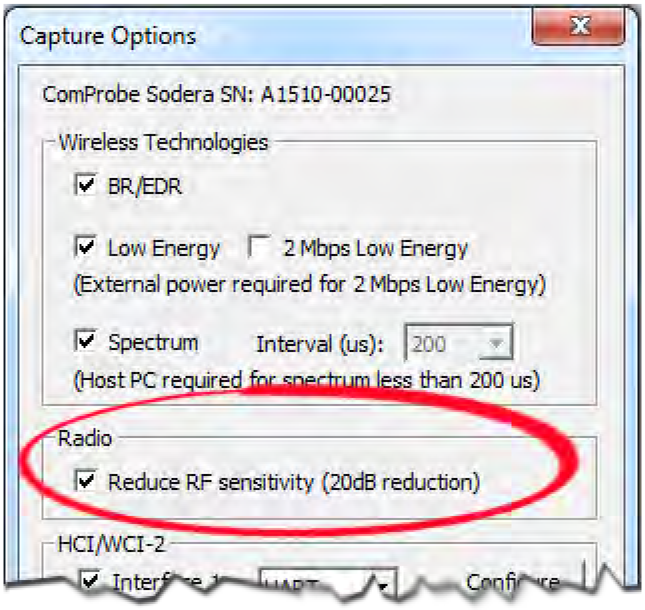
While exact conductive test setups are dependent on the specific circumstances surrounding the DUT (Device Under Test) RF interface, the following equipment is required for most testing situations.

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.



Capture Options

ComProbe Sodera SN: A1510-00025

Wireless Technologies

☑ BR/EDR

☑ Low Energy □ 2 Mbps Low Energy

(External power required for 2 Mbps Low Energy)

☑ Spectrum Interval (us): 200

(Host PC required for spectrum less than 200 us)

Radio

☑ Reduce RF sensitivity (20dB reduction)

HCI/WCI-2

☑ Interf

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 below 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.

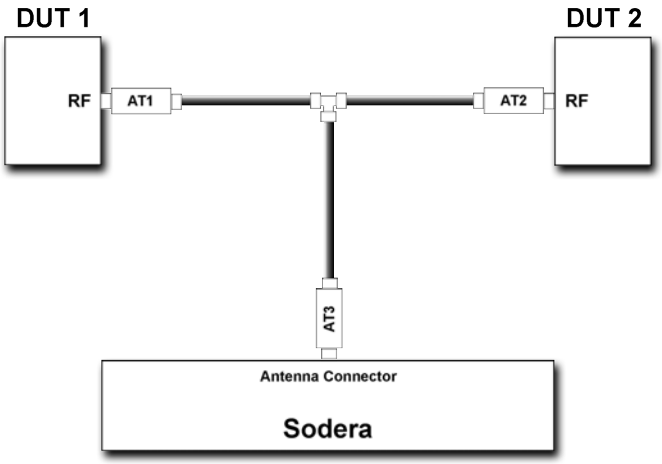


Figure 3.56 - Sodera Conductive Test Setup

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.

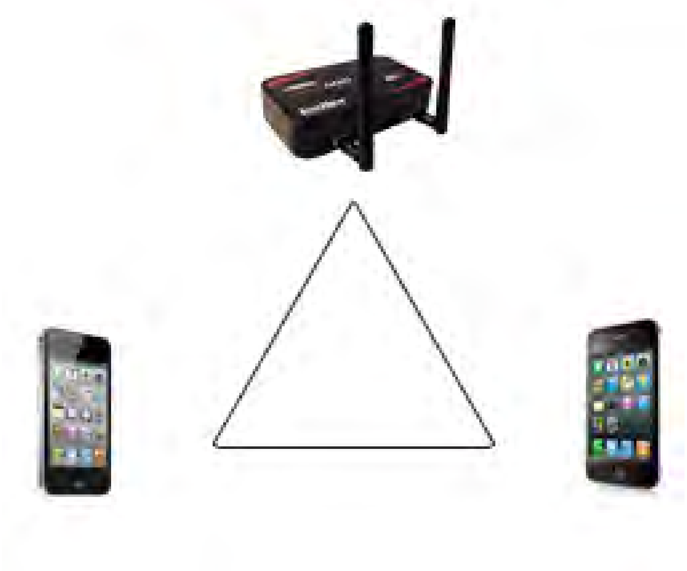


Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane

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.

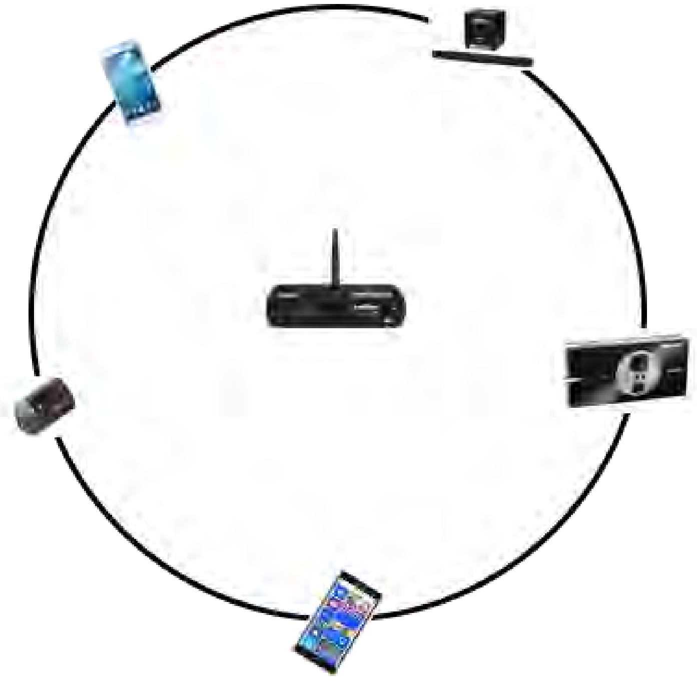


Figure 4.2 - Wideband Capture: Devices Equally Spaced in the Same Horizontal Plane

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.

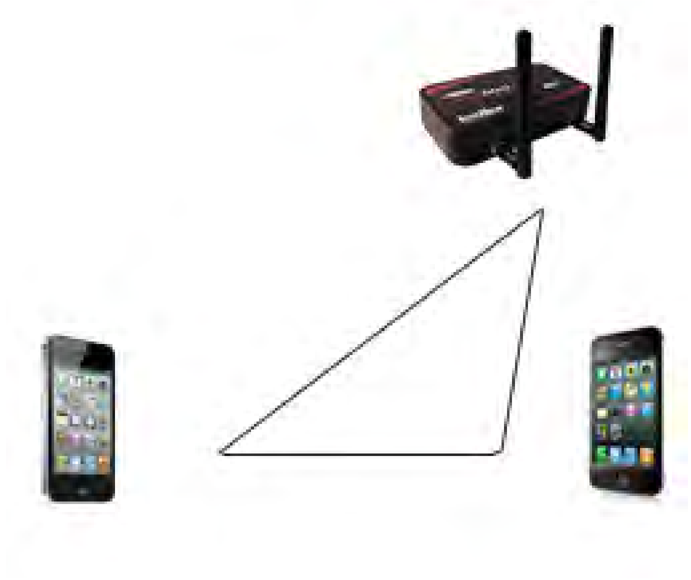


Figure 4.3 - For Audio A2DP, Position Closer to SINK DUT

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.

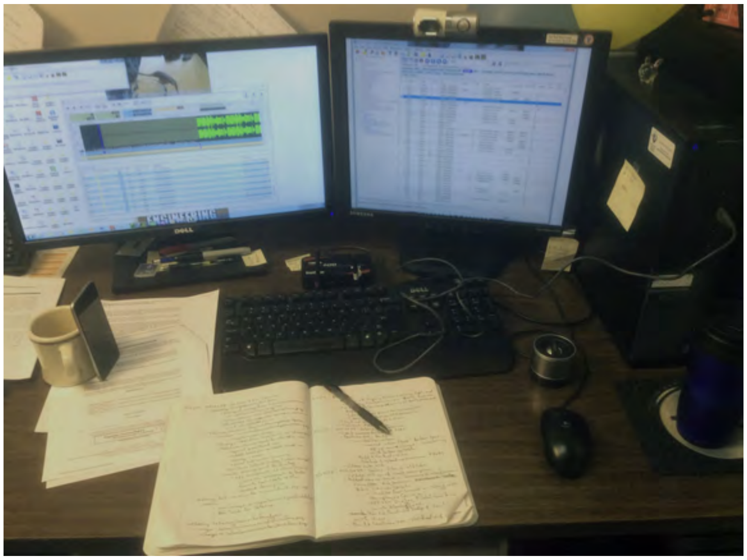


Figure 4.4 - Example: Poor Capture Environment

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.

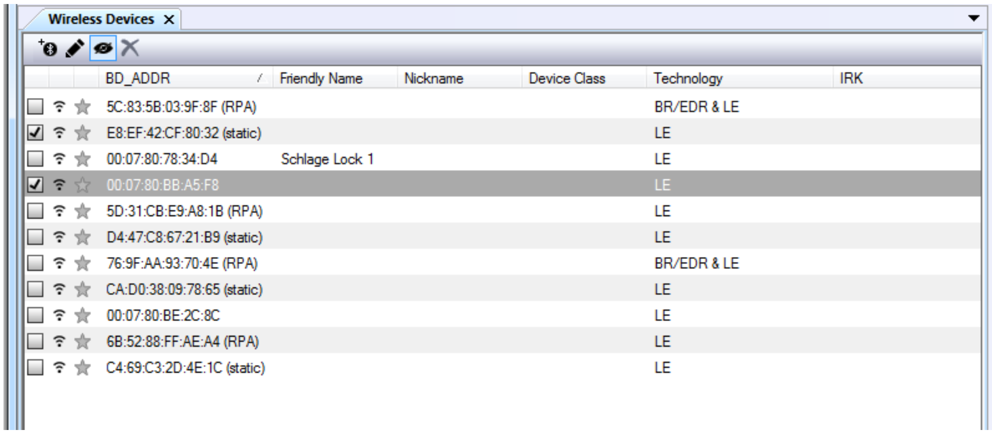
The **Event Log** pane will begin to populate with information, warnings, and error messages.

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.



	BD_ADDR	Friendly Name	Nickname	Device Class	Technology	IRK
□	5C:83:5B:03:9F:8F (RPA)				BR/EDR & LE	
☑	E8:EF:42:CF:80:32 (static)				LE	
□	00:07:80:78:34:D4	Schlage Lock 1			LE	
☑	00:07:80:BB:A5:F8				LE	
□	5D:31:CB:E9:A8:1B (RPA)				LE	
□	D4:47:C8:67:21:B9 (static)				LE	
□	76:9F:AA:93:70:4E (RPA)				BR/EDR & LE	
□	CA:D0:38:09:78:65 (static)				LE	
□	00:07:80:BE:2C:8C				LE	
□	6B:52:88:FF:AE:A4 (RPA)				LE	
□	C4:69:C3:2D:4E:1C (static)				LE	

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).

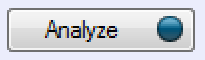
The following table lists some common data capture and device selection scenarios.

Table 4.1 - Common Data Capture and Device Selection Scenarios

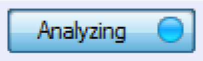
Scenario	Wireless Devices Pane Selection
Analyzing traffic between a slave Device Under Test (DUT) and its master.	Select only the slave DUT for analysis
Analyzing all traffic on a piconet	Select the Master for analysis
Analyzing all traffic involved in Inquiries	In the **Sodera** Options menu select **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 70 - 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 70 - Displays "Received Signal Strength OK" with an Information icon ℹ . 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.

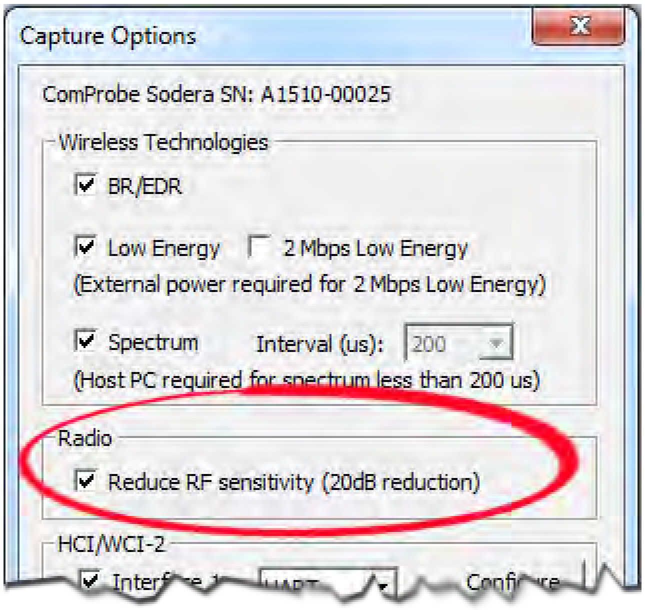
- Normal Gain **Capture Options** setting (see Menu on page 33)- No packets with RSSI greater than -24 dBm within the last 5 seconds.

- 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.



Capture Options

ComProbe Sodera SN: A1510-00025

Wireless Technologies

☑ BR/EDR

☑ Low Energy ☐ 2 Mbps Low Energy

(External power required for 2 Mbps Low Energy)

☑ Spectrum Interval (us): 200

(Host PC required for spectrum less than 200 us)

Radio

☑ Reduce RF sensitivity (20dB reduction)

HCI/WCI-2

☑ Interface 1 UART Configure

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.

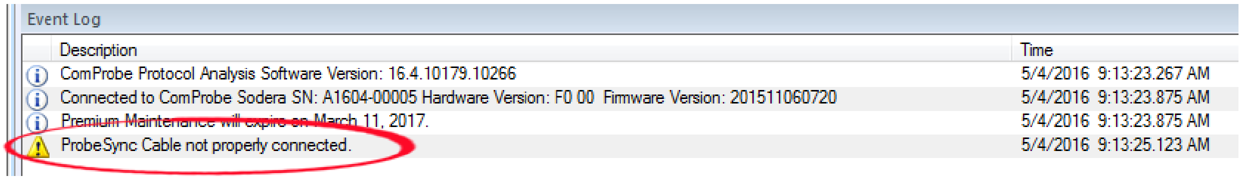
1. Connect the Sodera hardware that contains the excursion mode capture to be analyzed, to a computer.
2. Apply power to the Sodera hardware.
3. Open the ComProbe Protocol Analysis System.
4. When the **ComProbe Sodera** window opens, select **Manage excursion mode captures...** from the **File** menu.
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 103.
7. Follow the procedures in Sodera: Record—Begin Capture on page 103.

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.



Event Log

Description	Time
ComProbe Protocol Analysis Software Version: 16.4.10179.10266	5/4/2016 9:13:23.267 AM
Connected to ComProbe Sodera SN: A1604-00005 Hardware Version: F0 00 Firmware Version: 201511060720	5/4/2016 9:13:23.875 AM
Premium Maintenance will expire on March 11, 2017.	5/4/2016 9:13:23.875 AM
ProbeSync Cable not properly connected.	5/4/2016 9:13:25.123 AM

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 105 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 345 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)

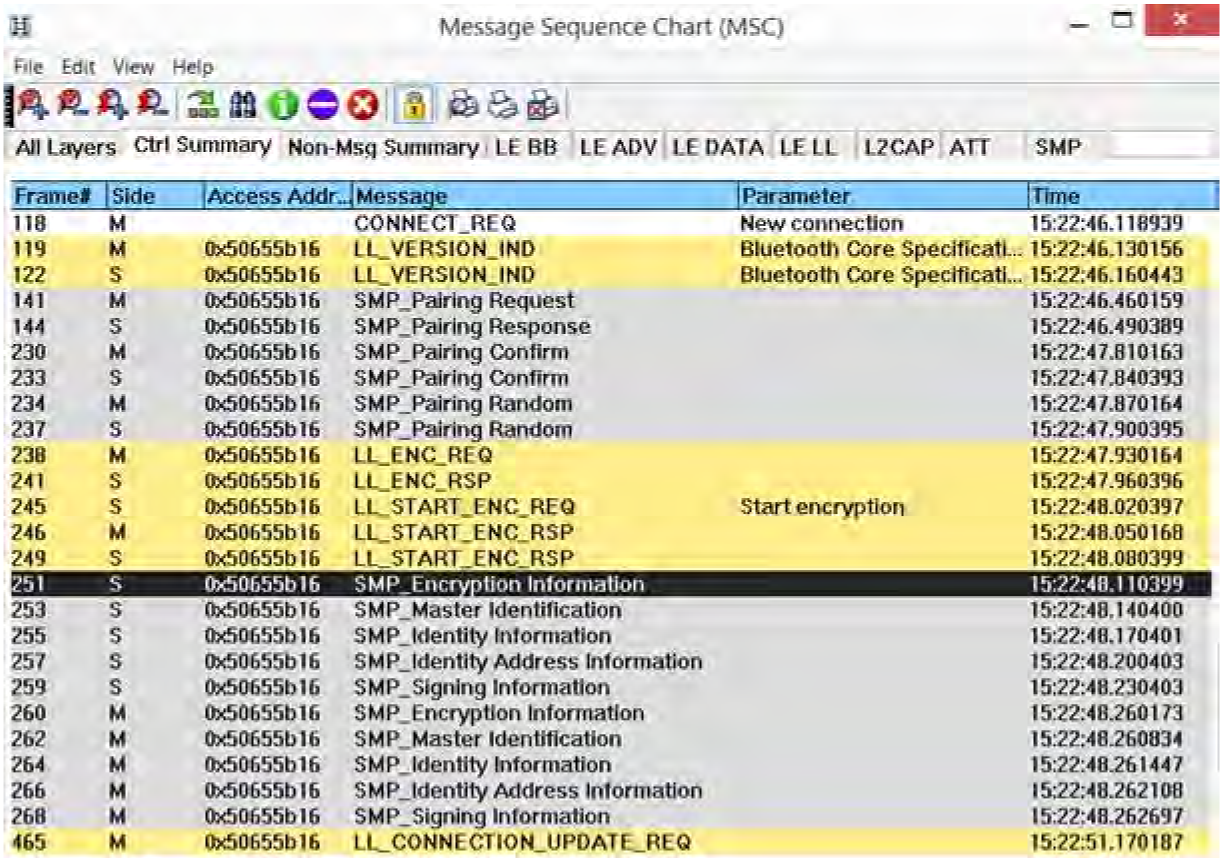
The following information and packets are needed to follow decryption:

- 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)

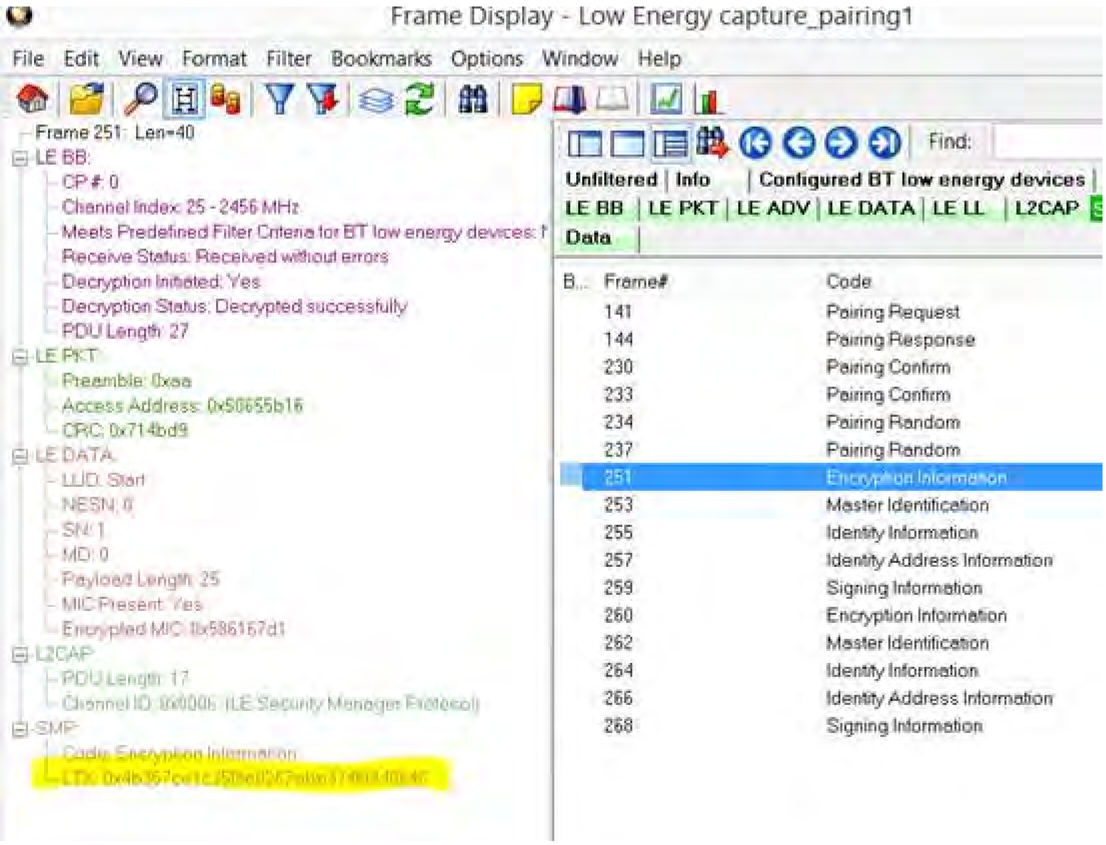
The following information and packets are needed to follow decryption:

- 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


Frame Display - Low Energy capture_pairing1
File Edit View Format Filter Bookmarks Options Window Help
Find:
Unfiltered | Info | Configured BT low energy devices
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP
Data

```
Frame 251: Len=40
⊟ LE BB:
    CP #: 0
    Channel Index: 25 - 2456 MHz
    Meets Predefined Filter Criteria for BT low energy devices: !
    Receive Status: Received without errors
    Decryption Initiated: Yes
    Decryption Status: Decrypted successfully
    PDU Length: 27
⊟ LE PKT:
    Preamble: 0xaa
    Access Address: 0x50655b16
    CRC: 0x714bd9
⊟ LE DATA:
    LLID: Start
    NESN: 0
    SN: 1
    MD: 0
    Payload Length: 25
    MIC Present: Yes
    Encrypted MIC: 0x586167d1
⊟ L2CAP:
    PDU Length: 17
    Channel ID: 0x0006 (LE Security Manager Protocol)
⊟ SMP:
    Code: Encryption Information
    LTK: [illegible]
```

B...	Frame#	Code
	141	Pairing Request
	144	Pairing Response
	230	Pairing Confirm
	233	Pairing Confirm
	234	Pairing Random
	237	Pairing Random
	251	Encryption Information
	253	Master Identification
	255	Identity Information
	257	Identity Address Information
	259	Signing Information
	260	Encryption Information
	262	Master Identification
	264	Identity Information
	266	Identity Address Information
	268	Signing Information

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.

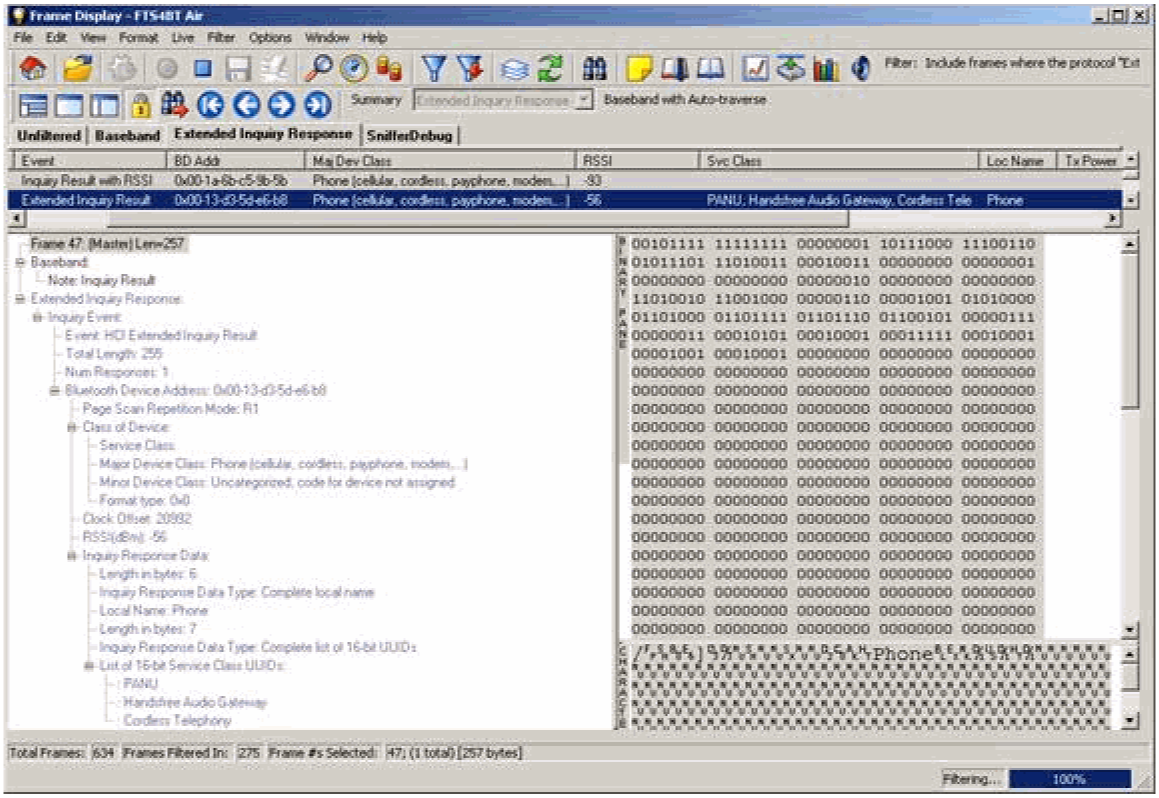
1. Click the **Record** [Record ●] button on the Standard Toolbar. Sodera will begin capturing data from all wireless devices within range and from all connected wired devices.
2. In the **Wireless Devices** and **Wired Devices** pane select the active devices for analysis
3. Click on **Analyze** [Analyze ●] 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.



Filter: Include frames where the protocol "Ext

Event	BD Addr	Maj Dev Class	RSSI	Svc Class	Loc Name	Tx Power
Inquiry Result with RSSI	0x00-1a-6b-c5-9b-5b	Phone (cellular, cordless, payphone, modem,...)	-93			
Extended Inquiry Result	0x00-13-d3-5d-e6-b8	Phone (cellular, cordless, payphone, modem,...)	-56	PANU; Handsfree Audio Gateway, Cordless Tele	Phone	

```
Frame 47: (Master) Len=257
Baseband
    Note: Inquiry Result
Extended Inquiry Response
    Inquiry Event
        Event: HCI Extended Inquiry Result
        Total Length: 255
        Num Responses: 1
        Bluetooth Device Address: 0x00-13-d3-5d-e6-b8
            Page Scan Repetition Mode: R1
            Class of Device
                Service Class
                Major Device Class: Phone (cellular, cordless, payphone, modem,...)
                Minor Device Class: Uncategorized, code for device not assigned
                Format type: 0x0
            Clock Offset: 20892
            RSSI(dBm): -56
            Inquiry Response Data
                Length in bytes: 6
                Inquiry Response Data Type: Complete local name
                Local Name: Phone
                Length in bytes: 7
                Inquiry Response Data Type: Complete list of 16-bit UUIDs
                List of 16-bit Service Class UUIDs
                    PANU
                    Handsfree Audio Gateway
                    Cordless Telephony
```

```
00101111 11111111 00000001 10111000 11100110
01011101 11010011 00010011 00000000 00000001
00000000 00000000 00000010 00000000 00000000
11010010 11001000 00000110 00001001 01010000
01101000 01101111 01101110 01100101 00000111
00000011 00010101 00010001 00011111 00010001
00001001 00010001 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000
```

Total Frames: 634 Frames Filtered In: 275 Frame #s Selected: 47; (1 total) [257 bytes]

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

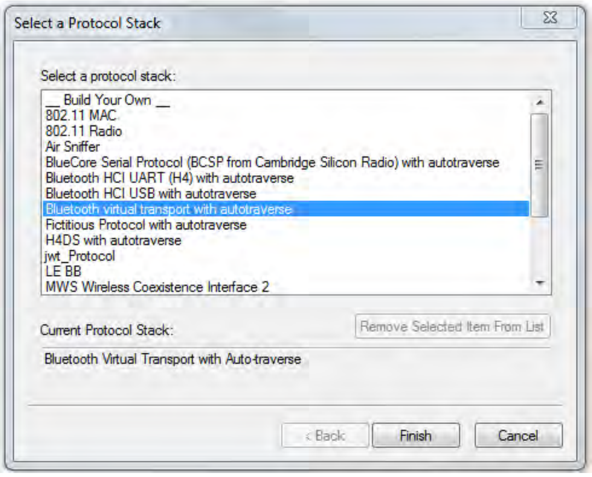
4.2.1 Protocol Stack Wizard

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 114.



Select a protocol stack:

__ Build Your Own __
802.11 MAC
802.11 Radio
Air Sniffer
BlueCore Serial Protocol (BCSP from Cambridge Silicon Radio) with autotraverse
Bluetooth HCI UART (H4) with autotraverse
Bluetooth HCI USB with autotraverse
Bluetooth virtual transport with autotraverse
Fictitious Protocol with autotraverse
H4DS with autotraverse
jwt_Protocol
LE BB
MWS Wireless Coexistence Interface 2

Current Protocol Stack: Bluetooth Virtual Transport with Auto-traverse

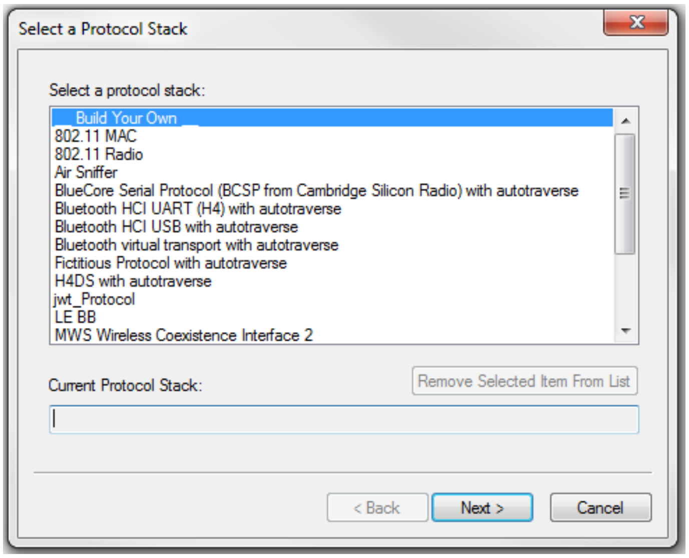
1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the **Remove Selected Item From List** button becomes active.
2. Click the **Remove Selected Item From List**button to remove the stack from the list. You cannot remove stacks provided with the analyzer. 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 115 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

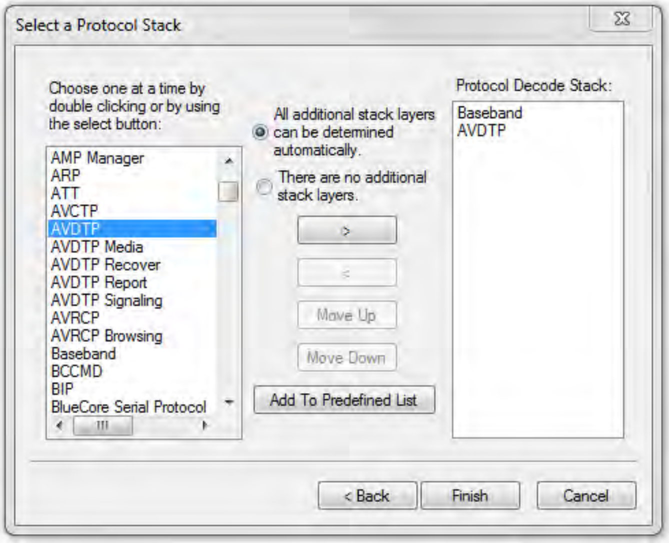
To create a custom stack:


Select a Protocol Stack
Select a protocol stack:
Build Your Own
802.11 MAC
802.11 Radio
Air Sniffer
BlueCore Serial Protocol (BCSP from Cambridge Silicon Radio) with autotraverse
Bluetooth HCI UART (H4) with autotraverse
Bluetooth HCI USB with autotraverse
Bluetooth virtual transport with autotraverse
Fictitious Protocol with autotraverse
H4DS with autotraverse
jwt_Protocol
LE BB
MWS Wireless Coexistence Interface 2
Current Protocol Stack:
Remove Selected Item From List
< Back
Next >
Cancel

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 115 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 115 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.

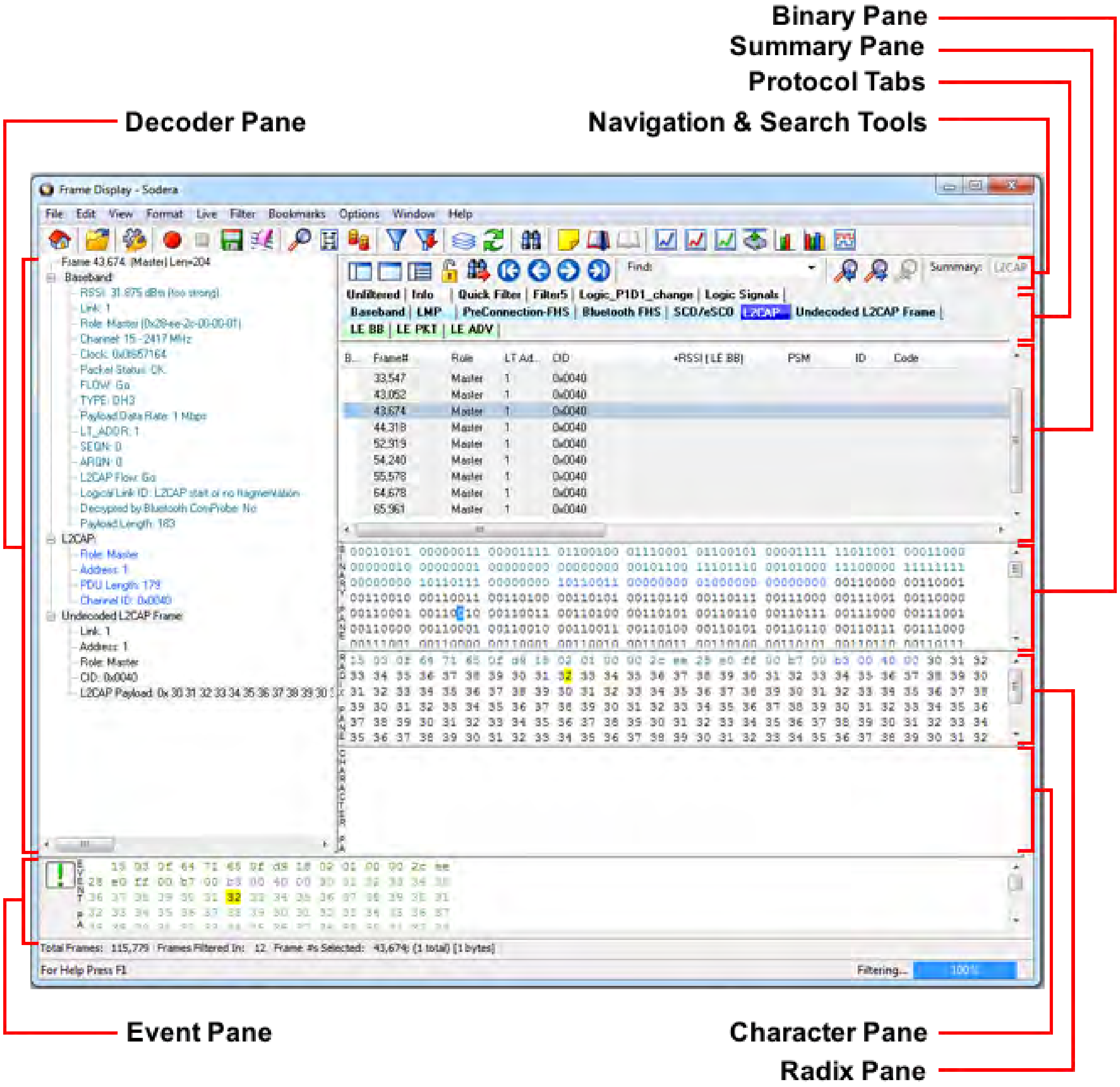
3. This option brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check **Automatically Request Missing Decoding Information.**
5. When unchecked, the analyzer 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.


Binary Pane
Summary Pane
Protocol Tabs
Decoder Pane
Navigation & Search Tools
Frame Display - Sodera
File Edit View Format Live Filter Bookmarks Options Window Help
Find:
Summary: L2CAP
Unfiltered | Info | Quick Filter | Filter5 | Logic_P1D1_change | Logic Signals |
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | SCO/eSCO | L2CAP | Undecoded L2CAP Frame |
LE BB | LE PKT | LE ADV |
BINARY PANE
RADIX PANE
CHARACTER PANE
EVENT PANE
Event Pane
Character Pane
Radix Pane

```
Frame 43,674 (Master) Len=204
⊟ Baseband
   RSSI: 31.875 dBm (too strong)
   Link: 1
   Role: Master (0x28-ee-2c-00-00-01)
   Channel: 15 - 2417 MHz
   Clock: 0x08657164
   Packet Status: OK
   FLOW: Go
   TYPE: DH3
   Payload Data Rate: 1 Mbps
   LT_ADDR: 1
   SEQN: 0
   ARQN: 0
   L2CAP Flow: Go
   Logical Link ID: L2CAP start or no fragmentation
   Decrypted by Bluetooth ComProbe: No
   Payload Length: 183
⊟ L2CAP:
   Role: Master
   Address: 1
   PDU Length: 179
   Channel ID: 0x0040
⊟ Undecoded L2CAP Frame
   Link: 1
   Address: 1
   Role: Master
   CID: 0x0040
   L2CAP Payload: 0x 30 31 32 33 34 35 36 37 38 39 30 3
```

B...	Frame#	Role	LT Ad...	CID	•RSSI (LE BB)	PSM	ID	Code
	33,547	Master	1	0x0040				
	43,052	Master	1	0x0040				
	43,674	Master	1	0x0040				
	44,318	Master	1	0x0040				
	52,919	Master	1	0x0040				
	54,240	Master	1	0x0040				
	55,578	Master	1	0x0040				
	64,678	Master	1	0x0040				
	65,961	Master	1	0x0040				

```
00010101 00000011 00001111 01100100 01110001 01100101 00001111 11011001 00011000
00000010 00000001 00000000 00000000 00101100 11101110 00101000 11100000 11111111
00000000 10110111 00000000 10110011 00000000 01000000 00000000 00110000 00110001
00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001 00110000
00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001
00110000 00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000
00111001 00110000 00110001 00110010 00110011 00110100 00110101 00110110 00110111
```

```
15 03 0f 64 71 65 0f d9 18 02 01 00 00 2c ee 28 e0 ff 00 b7 00 b3 00 40 00 30 31 32
33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30
31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38
39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36
37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34
35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32
```

Total Frames: 115,779 Frames Filtered In: 12 Frame #s Selected: 43,674 (1 total) [1 bytes]

For Help Press F1 Filtering... 100%

Figure 4.10 - 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.

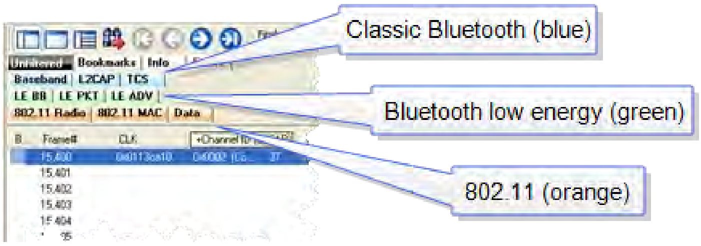
- Decode Pane - The **Decode Pane** displays a detailed decode of the highlighted frame. Fields selected in the **Decode Pane** have the appropriate bit(s) or byte(s) selected in the **Radix**, **Binary**, **Character** , and **Event** panes
- Radix Pane - The **Radix Pane** displays the logical data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

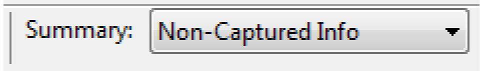
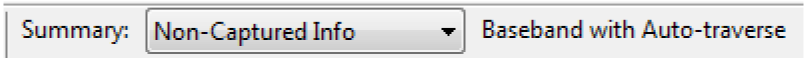
Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
	Apply/Modify Display Filters - Opens the Display Filter dialog.
	Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.
	Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data
	Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.
	Find - Search for errors, string patterns, special events and more.
	Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.
	Add/Modify Bookmark - Add a new or modify an existing bookmark.
	Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.
ES	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.	

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
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.
◫	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.

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
🔍	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.  Summary: Non-Captured Info
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.

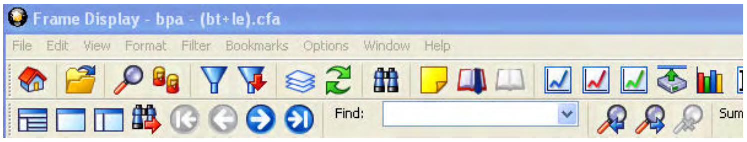
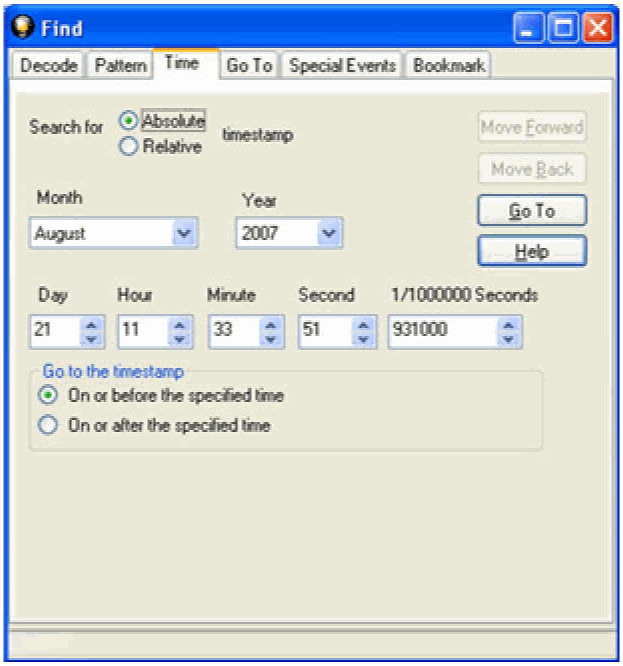

Frame Display - bpa - (bt+le).cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Sum

Figure 4.11 - 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.,



Search for ● Absolute ○ Relative timestamp

Month: August

Year: 2007

Day: 21

Hour: 11

Minute: 33

Second: 51

1/1000000 Seconds: 931000

Go to the timestamp

● On or before the specified time

○ On or after the specified time

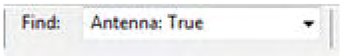
Figure 4.12 - Search/Find Dialog

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.



Find: Antenna: True

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

3. 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.

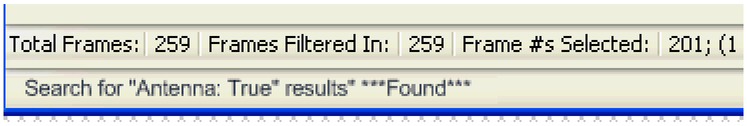
db Antenna Signal: True
Antenna: True
dbm Transmit Attenuation: False
db Transmit Attenuation: False

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.

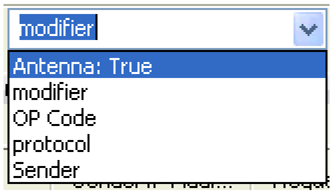
- When you enter a search string and select Enter, the search moves forward.
- If you select **Find Previous Occurrence**, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous 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.



Total Frames: 259 Frames Filtered In: 259 Frame #s Selected: 201; (1

Search for "Antenna: True" results" ***Found***

- 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.



modifier

Antenna: True
modifier
OP Code
protocol
Sender

- 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...**.

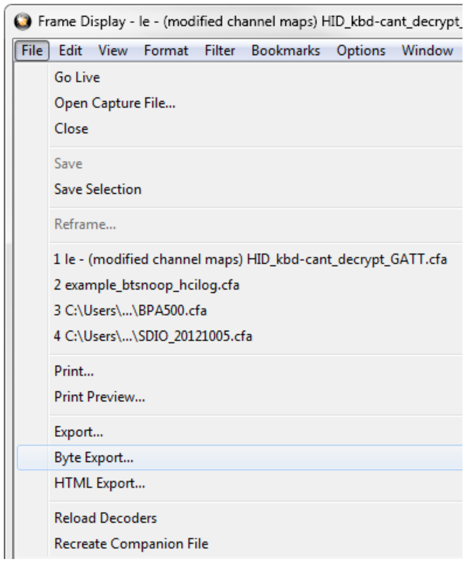
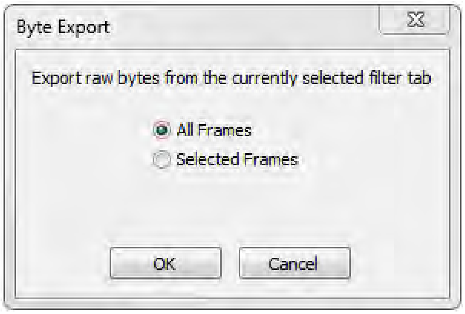

Frame Display - le - (modified channel maps) HID_kbd-cant_decrypt_
File
Edit
View
Format
Filter
Bookmarks
Options
Window
Go Live
Open Capture File...
Close
Save
Save Selection
Reframe...
1 le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa
2 example_btsnoop_hcilog.cfa
3 C:\Users\...\BPA500.cfa
4 C:\Users\...\SDIO_20121005.cfa
Print...
Print Preview...
Export...
Byte Export...
HTML Export...
Reload Decoders
Recreate Companion File

Figure 4.13 - 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.


Byte Export

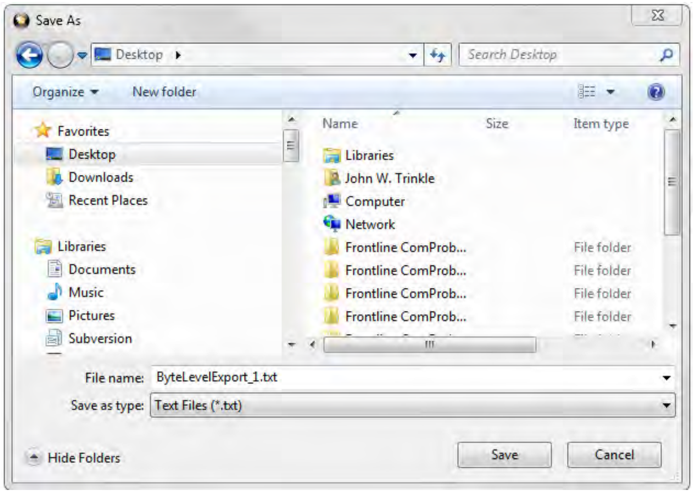
Export raw bytes from the currently selected filter tab

● All Frames
○ Selected Frames

Figure 4.14 - 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.



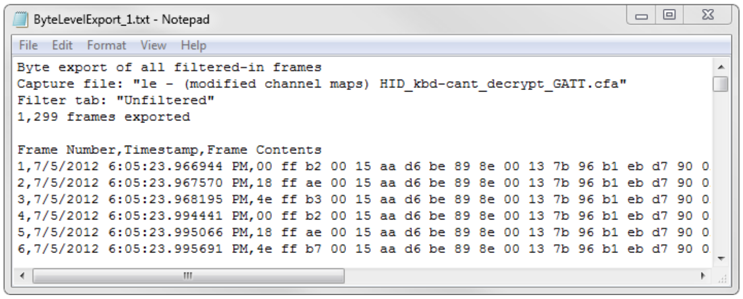
File name: ByteLevelExport_1.txt

Save as type: Text Files (*.txt)

Figure 4.15 - 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.



```
Byte export of all filtered-in frames
Capture file: "le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa"
Filter tab: "Unfiltered"
1,299 frames exported

Frame Number,Timestamp,Frame Contents
1,7/5/2012 6:05:23.966944 PM,00 ff b2 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
2,7/5/2012 6:05:23.967570 PM,18 ff ae 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
3,7/5/2012 6:05:23.968195 PM,4e ff b3 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
4,7/5/2012 6:05:23.994441 PM,00 ff b2 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
5,7/5/2012 6:05:23.995066 PM,18 ff ae 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
6,7/5/2012 6:05:23.995691 PM,4e ff b7 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
```

Figure 4.16 - 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.

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.

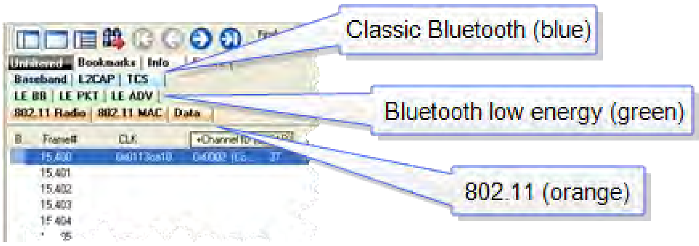


Figure 4.17 - Example Protocol Tags

- 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:

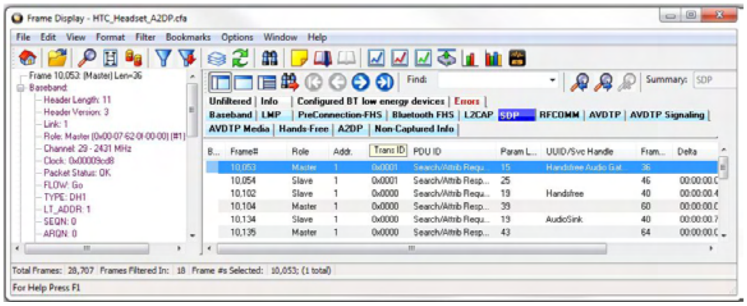
- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

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.


Frame Display - HTC_Headset_A2DP.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: SDP
Unfiltered | Info | Configured BT low energy devices | Errors |
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVDTP | AVDTP Signaling |
AVDTP Media | Hands-Free | A2DP | Non-Captured Info |

- Frame 10,053: (Master) Len=36
- Baseband:
  - Header Length: 11
  - Header Version: 3
  - Link: 1
  - Role: Master (0x00-07-62-01-00-00) (#1)
  - Channel: 29 - 2431 MHz
  - Clock: 0x00009cd8
  - Packet Status: OK
  - FLOW: Go
  - TYPE: DH1
  - LT_ADDR: 1
  - SEQN: 0
  - ARQN: 0

B...	Frame#	Role	Addr.	Trans ID	PDU ID	Param L...	UUID/Svc Handle	Fram...	Delta
	10,053	Master	1	0x0001	Search/Attrib Requ...	15	Handsfree Audio Gat...	36	
	10,054	Slave	1	0x0001	Search/Attrib Resp...	25		46	00:00:00.C
	10,102	Slave	1	0x0000	Search/Attrib Requ...	19	Handsfree	40	00:00:00.4
	10,104	Master	1	0x0000	Search/Attrib Resp...	39		60	00:00:00.C
	10,134	Slave	1	0x0000	Search/Attrib Requ...	19	AudioSink	40	00:00:00.7
	10,135	Master	1	0x0000	Search/Attrib Resp...	43		64	00:00:00.C

Total Frames: 28,707 Frames Filtered In: 18 Frame #s Selected: 10,053; (1 total)

For Help Press F1

Figure 4.18 - Summary pane (right) with Tooltip on Column 5 (Tran ID)

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.

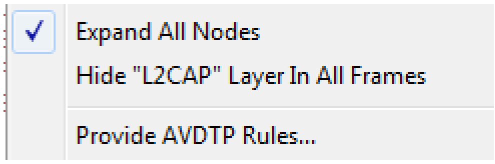
4.3.1.11.3 Frame Symbols in the Summary Pane

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.



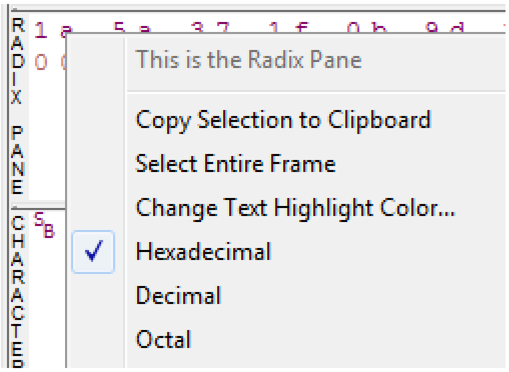
Protocol layers can be hidden, preventing them from being displayed on the **Decode** pane. Right-click on any protocol layer and choose **Hide** [protocol name] from the right-click menu.

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



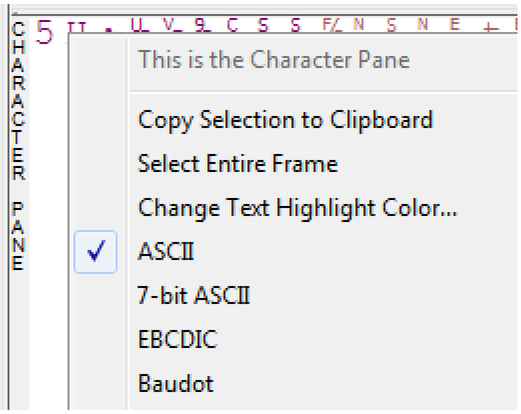
The **Radix** pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the **Format** menu, or by right-clicking on the pane and choosing **Hexadecimal**, **Decimal** or **Octal**.

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


CHARACTER PANE
This is the Character Pane
Copy Selection to Clipboard
Select Entire Frame
Change Text Highlight Color...
✓ ASCII
7-bit ASCII
EBCDIC
Baudot

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.

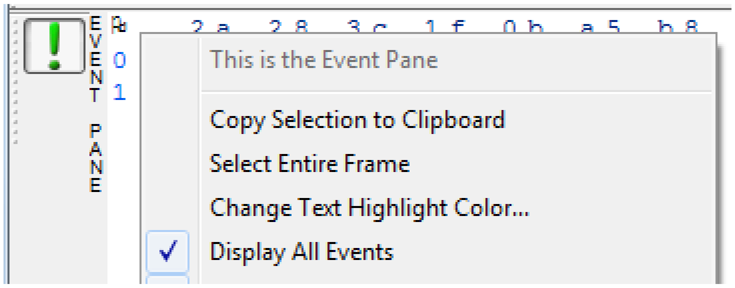
Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

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.

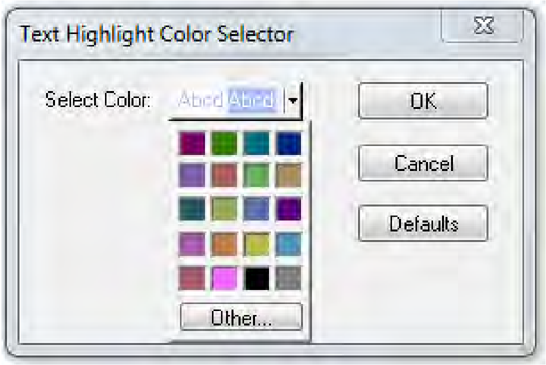
Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

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.

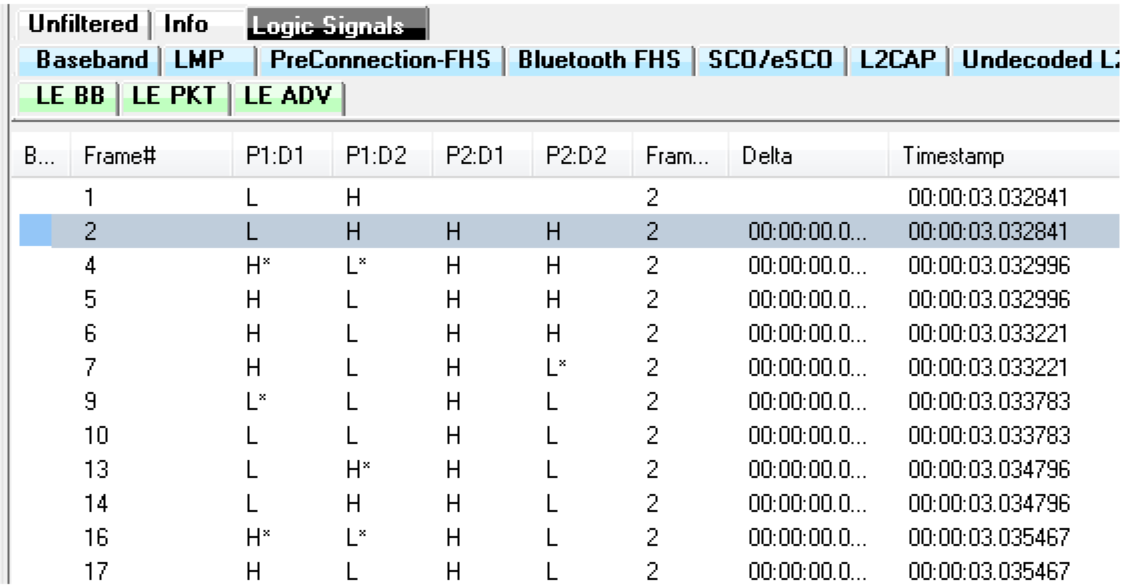
Select **Cancel** to discard any selection. Select **Defaults** to return the highlight color to blue.

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.

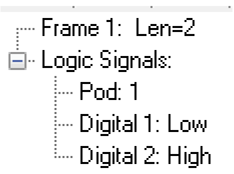
In Figure 4.19 below, Frame# 1 shows logic levels for P1:D1 and P1:D2 but P2:D1 and P2:D2 contain no data. This first frame contains a packet with logic data for POD1. In the next frame—Frame# 2—note that P1:D1 and P1:D2 contain the same logic as in Frame#1, and this data is a copy of the preceding Logic 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.



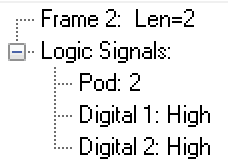
B...	Frame#	P1:D1	P1:D2	P2:D1	P2:D2	Fram...	Delta	Timestamp
	1	L	H			2		00:00:03.032841
	2	L	H	H	H	2	00:00:00.0...	00:00:03.032841
	4	H*	L*	H	H	2	00:00:00.0...	00:00:03.032996
	5	H	L	H	H	2	00:00:00.0...	00:00:03.032996
	6	H	L	H	H	2	00:00:00.0...	00:00:03.033221
	7	H	L	H	L*	2	00:00:00.0...	00:00:03.033221
	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 4.19 - Example: Logic Signals Starting Sequence



Frame 1: Len=2
Logic Signals:
Pod: 1
Digital 1: Low
Digital 2: High

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



Frame 2: Len=2
Logic Signals:
Pod: 2
Digital 1: High
Digital 2: High

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.

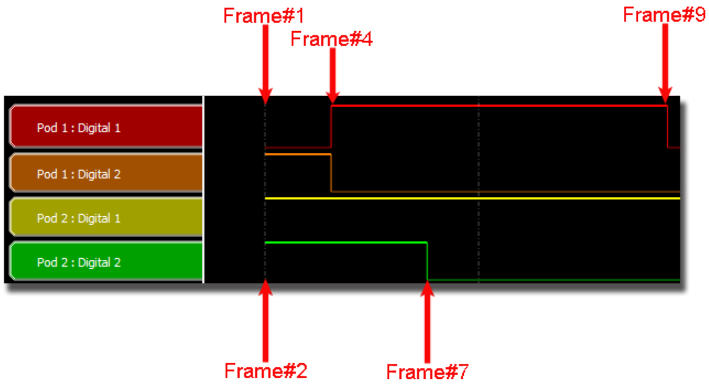


Figure 4.20 - Example: Logic Signals from Frame Display Frame#1 to Frame#9

In Figure 4.20 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.

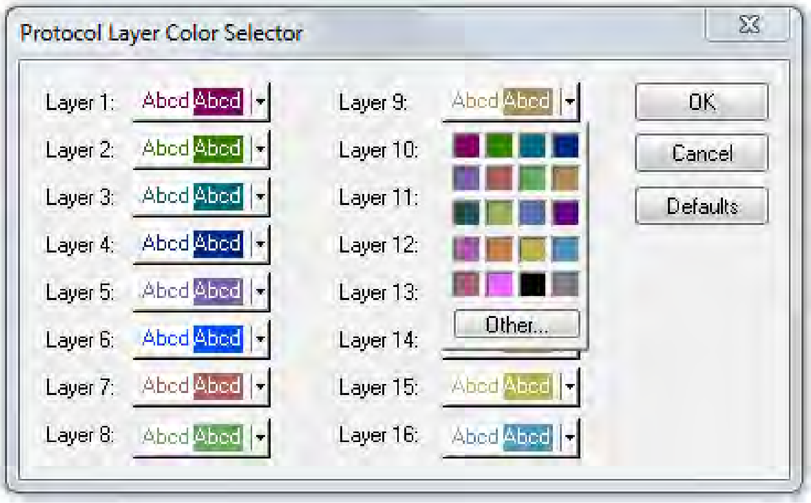


Figure 4.21 - Frame Display Protocol Layer Color Selector

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.

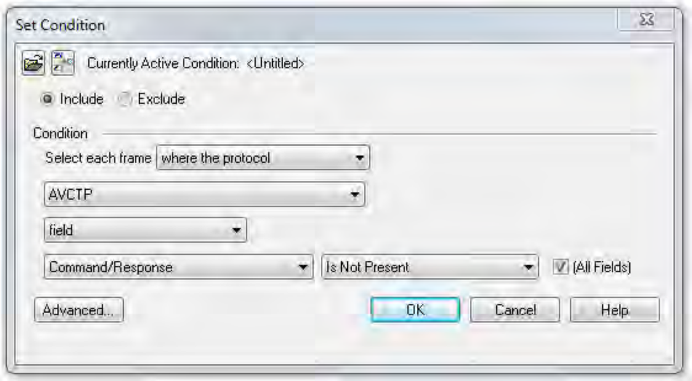
Quick Filters

- 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.



Set Condition

Currently Active Condition: <Untitled>

● Include ○ Exclude

Condition

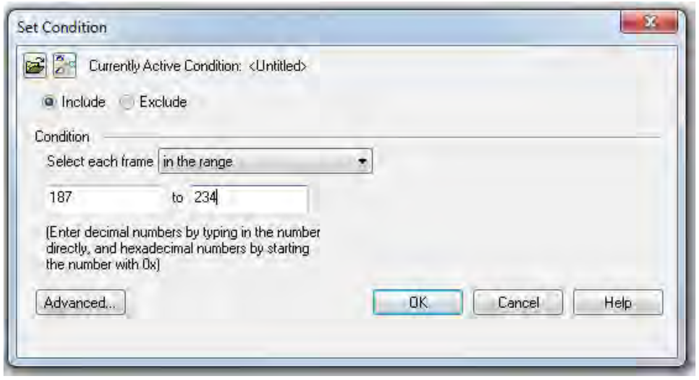
Select each frame: where the protocol

AVCTP

field

Command/Response — Is Not Present — ☑ (All Fields)

Figure 4.22 - Example: Set Conditions Self Configuring Based on Protocol Selection



Set Condition

Currently Active Condition: <Untitled>

● Include ○ Exclude

Condition

Select each frame: in the range

187 to 234

(Enter decimal numbers by typing in the number directly, and hexadecimal numbers by starting the number with 0x)

Figure 4.23 - 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.

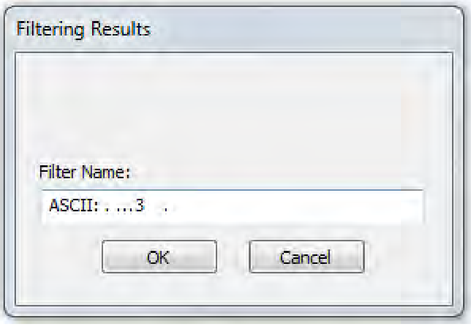
Include: A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

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**.



Filtering Results

Filter Name:

ASCII: . ...3 .

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

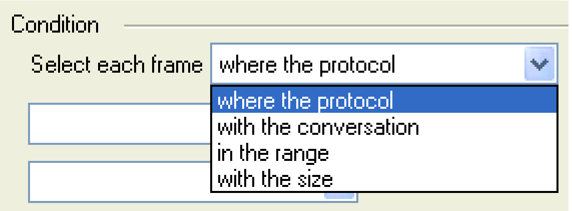
Compound filters use boolean logic to create complex and precise filters. There are three primary Boolean logic operators: **AND**, **OR**, and **NOT**.

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.

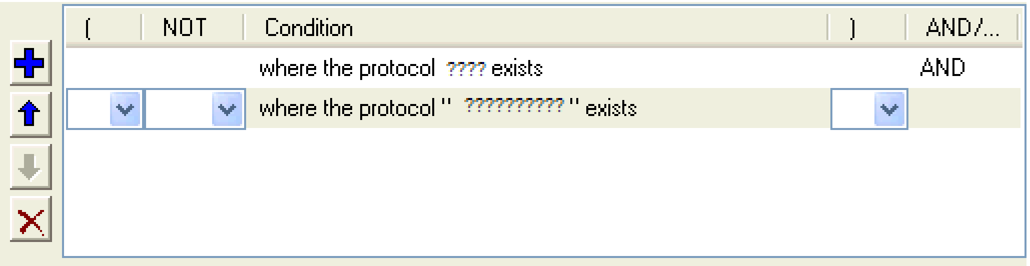


Condition

Select each frame: where the protocol

- where the protocol
- with the conversation
- in the range
- with the size

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.

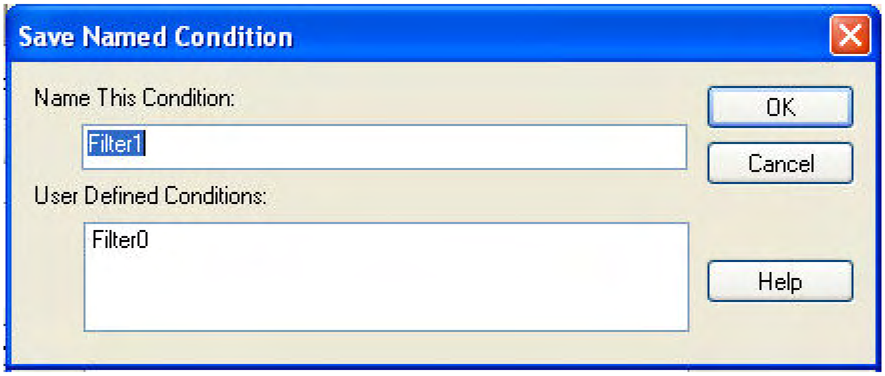


(	NOT	Condition	)	AND/...
		where the protocol ???? exists		AND
		where the protocol " ?????????? " exists		

Figure 4.24 - 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**.



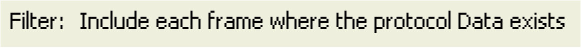
Save Named Condition

Name This Condition: Filter1

User Defined Conditions: Filter0

Figure 4.25 - 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

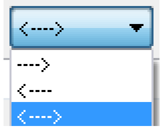
When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

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

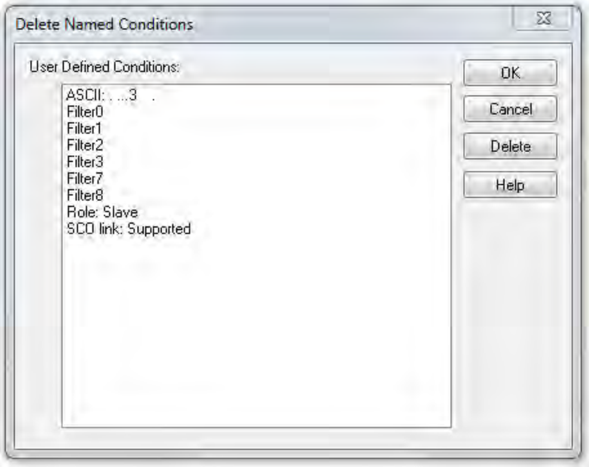
If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

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.



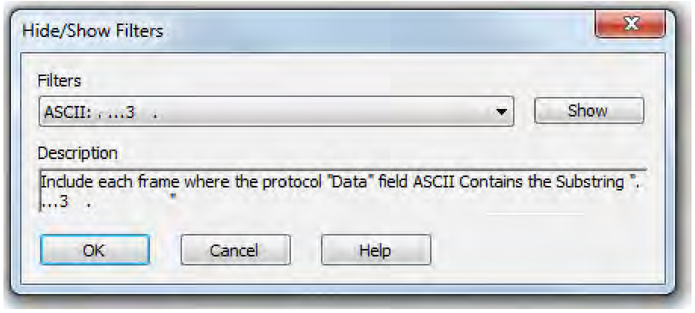
ASCII: . ...3 .
Filter0
Filter1
Filter2
Filter3
Filter7
Filter8
Role: Slave
SCO link: Supported

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.



ASCII: . ...3 .

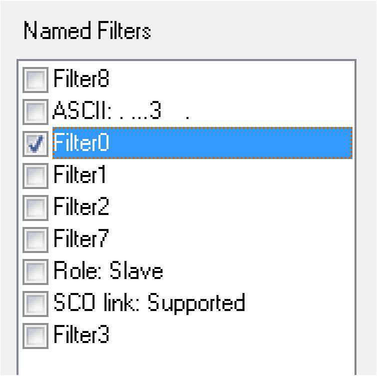
Include each frame where the protocol "Data" field ASCII Contains the Substring ". ...3 . "

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.



Named Filters

□ Filter8
□ ASCII: . ...3 .
☑ Filter0
□ Filter1
□ Filter2
□ Filter7
□ Role: Slave
□ SCO link: Supported
□ Filter3

Figure 4.26 - Using Named Filters Section of Quick Filters to Show/Hide Filters

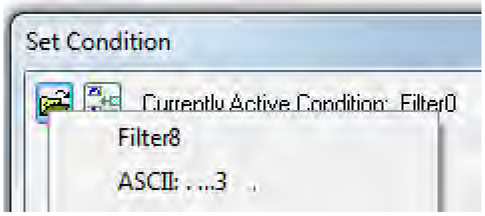
> **Note:** When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Show dialog to display a filter created in one Frame Display in different Frame Display window.

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.



Set Condition

Currently Active Condition: Filter0

Filter8

ASCII: . ...3 .

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.

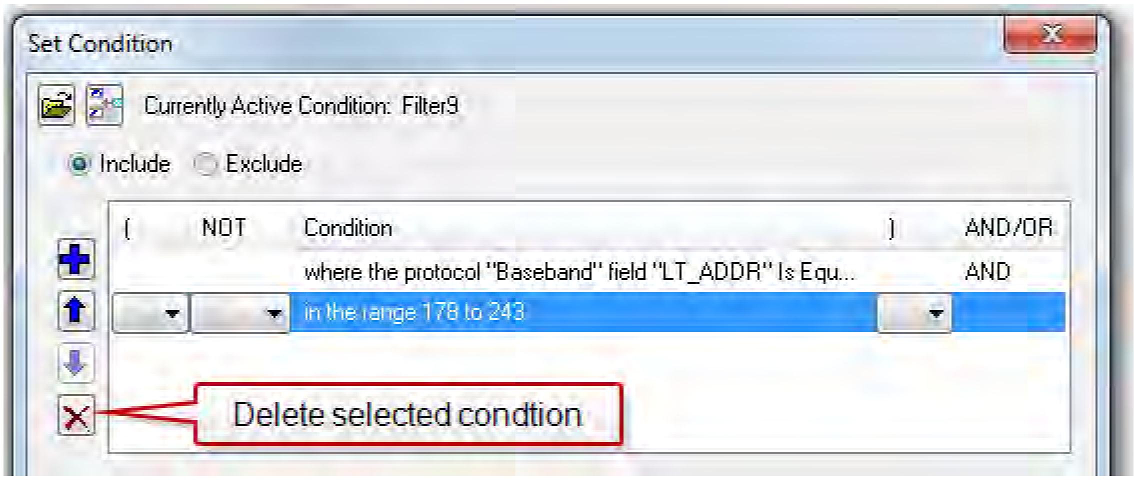
3. Click **OK**. The system displays the **Save Named Condition** dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click **OK**. If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided 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.


Set Condition

Currently Active Condition: Filter9

● Include ○ Exclude

(	NOT	Condition	)	AND/OR
		where the protocol "Baseband" field "LT_ADDR" Is Equ...		AND
		in the range 178 to 243		

Figure 4.27 - Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.

3. Click the **Delete Selected Line** icon.

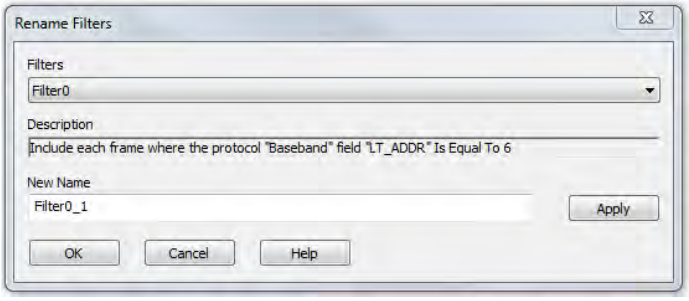
4. Edit the Boolean operators and parentheses as needed.

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.



Rename Filters

Filters: Filter0

Description: Include each frame where the protocol "Baseband" field "LT_ADDR" Is Equal To 6

New Name: Filter0_1

Figure 4.28 - 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.

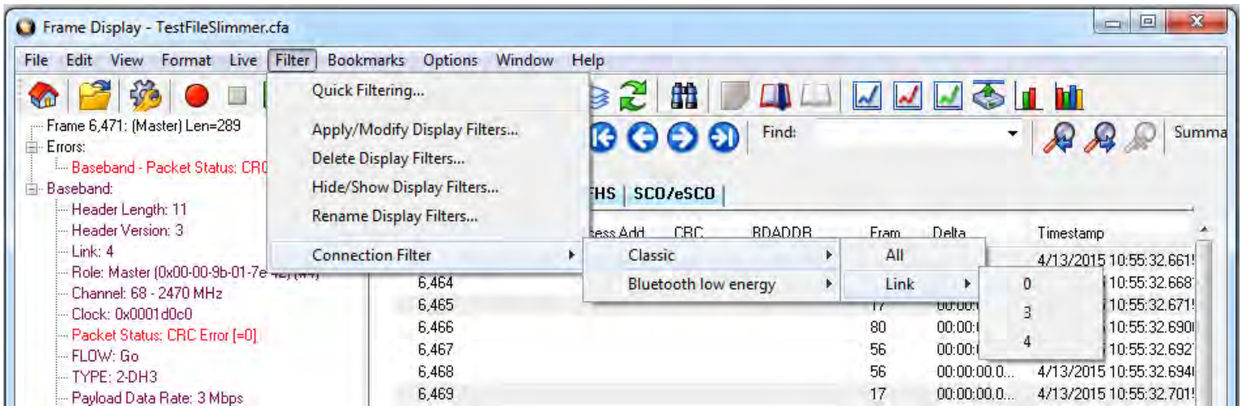


Figure 4.29 - Connection Filter from the Frame Display Menu

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.

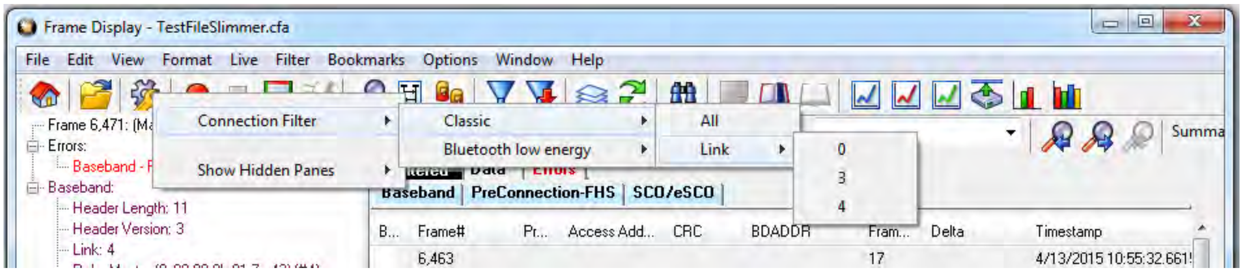
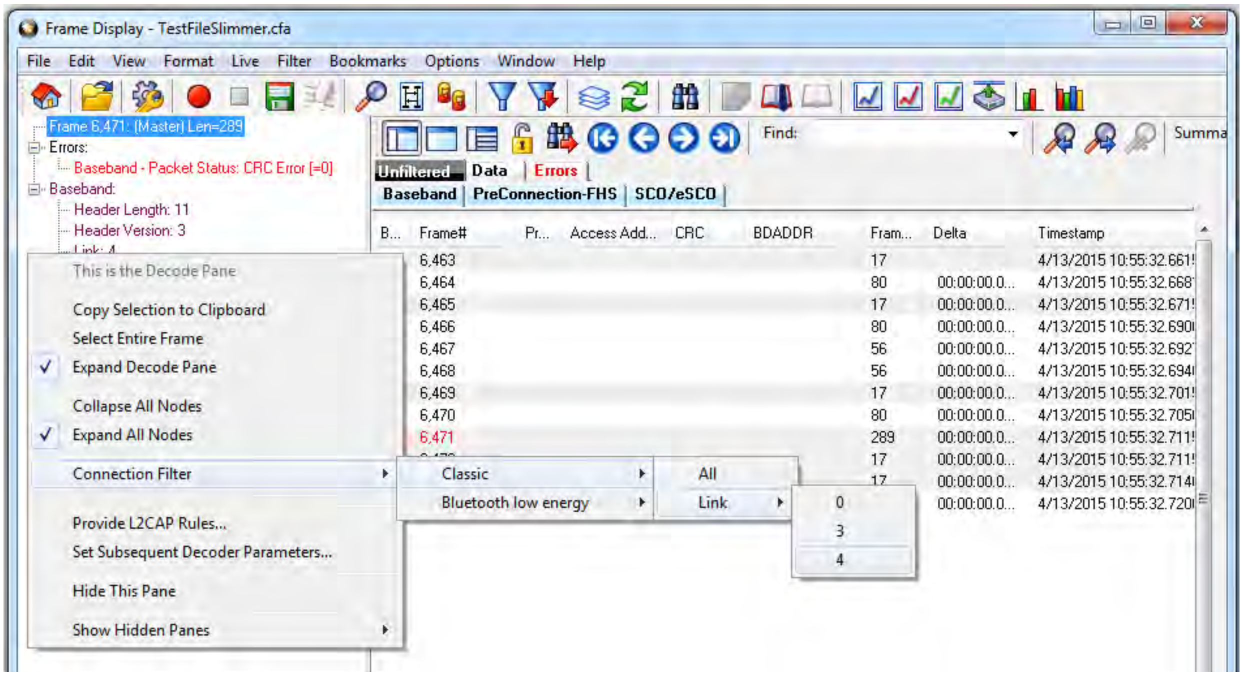


Figure 4.30 - Connection Filter from the Frame Display Toolbar right-click

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.



B...	Frame#	Pr...	Access Add...	CRC	BDADDR	Fram...	Delta	Timestamp
	6,463					17		4/13/2015 10:55:32.661!
	6,464					80	00:00:00.0...	4/13/2015 10:55:32.668'
	6,465					17	00:00:00.0...	4/13/2015 10:55:32.671!
	6,466					80	00:00:00.0...	4/13/2015 10:55:32.690(
	6,467					56	00:00:00.0...	4/13/2015 10:55:32.692'
	6,468					56	00:00:00.0...	4/13/2015 10:55:32.694(
	6,469					17	00:00:00.0...	4/13/2015 10:55:32.701!
	6,470					80	00:00:00.0...	4/13/2015 10:55:32.705(
	6,471					289	00:00:00.0...	4/13/2015 10:55:32.711!
	6,472					17	00:00:00.0...	4/13/2015 10:55:32.711!
						17	00:00:00.0...	4/13/2015 10:55:32.714(
							00:00:00.0...	4/13/2015 10:55:32.720(

Figure 4.31 - 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.

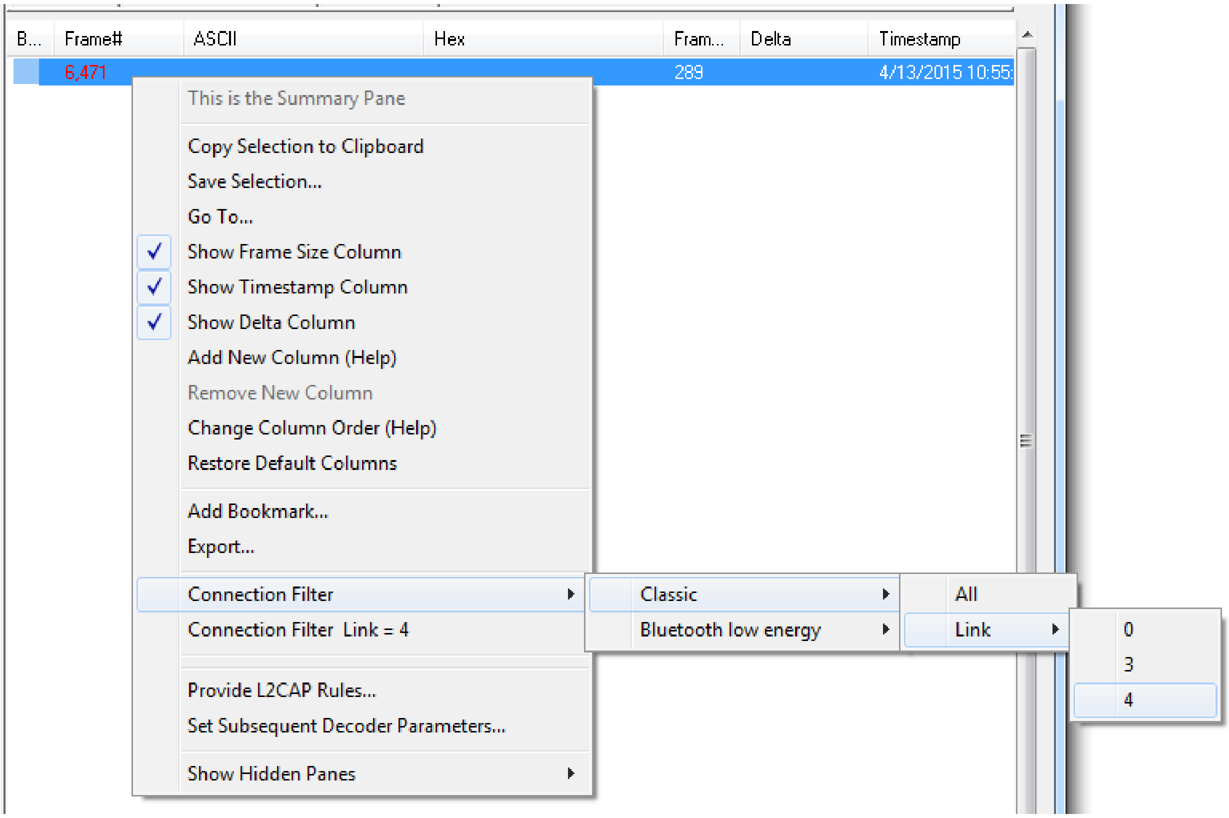


Figure 4.32 - Connection Filter from frame selection right-click

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.

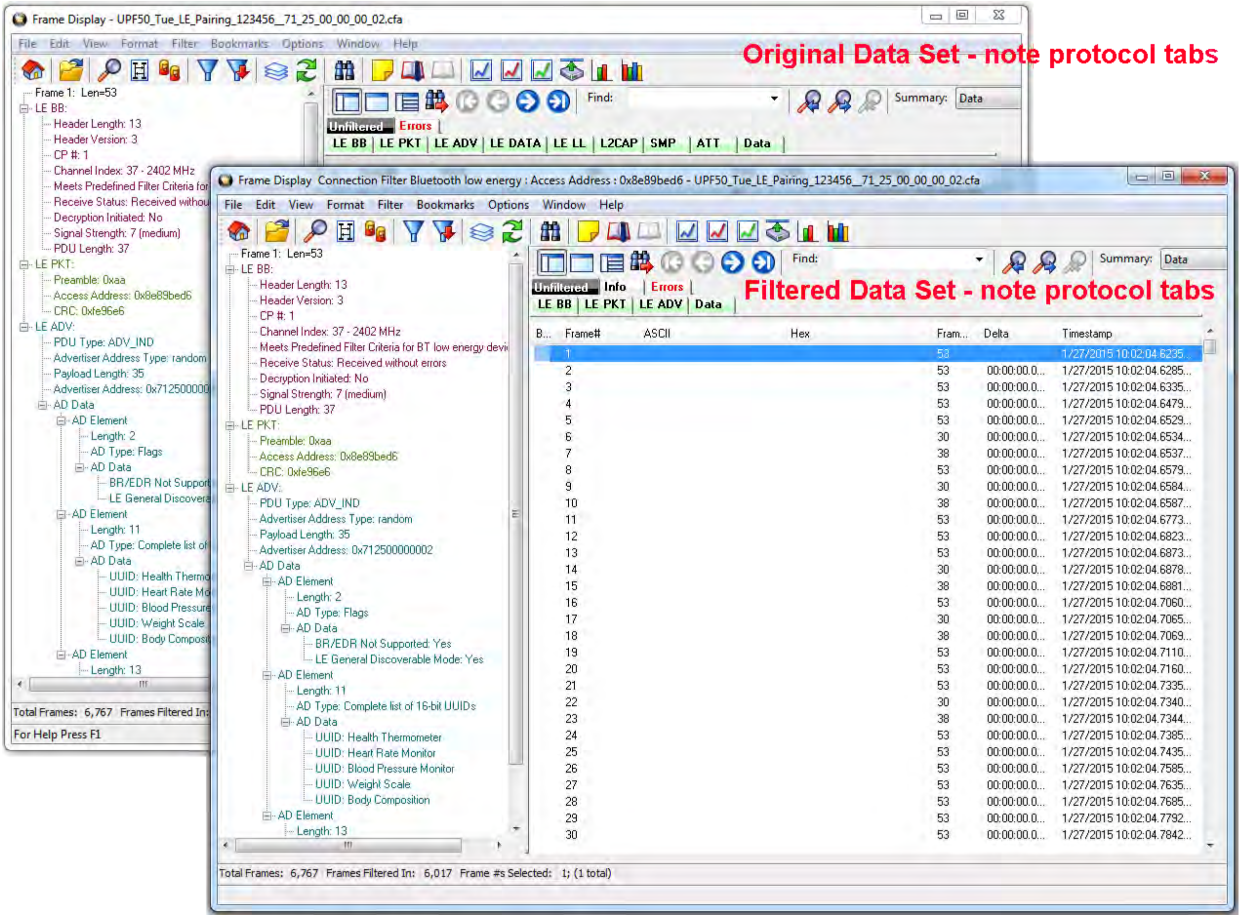
4.3.1.14.2.2 Connection Filter Display

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 127)

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


Frame Display - UPF50_Tue_LE_Pairing_123456__71_25_00_00_00_02.cfa
File Edit View Format Filter Bookmarks Options Window Help
Unfiltered Errors
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT | Data
Frame Display Connection Filter Bluetooth low energy : Access Address : 0x8e89bed6 - UPF50_Tue_LE_Pairing_123456__71_25_00_00_00_02.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: Data
Unfiltered Info Errors
LE BB | LE PKT | LE ADV | Data

Original Data Set - note protocol tabs

Filtered Data Set - note protocol tabs

```
Frame 1:  Len=53
LE BB:
    Header Length: 13
    Header Version: 3
    CP #: 1
    Channel Index: 37 - 2402 MHz
    Meets Predefined Filter Criteria for BT low energy devi
    Receive Status: Received without errors
    Decryption Initiated: No
    Signal Strength: 7 (medium)
    PDU Length: 37
LE PKT:
    Preamble: 0xaa
    Access Address: 0x8e89bed6
    CRC: 0xfe96e6
LE ADV:
    PDU Type: ADV_IND
    Advertiser Address Type: random
    Payload Length: 35
    Advertiser Address: 0x712500000002
    AD Data
        AD Element
            Length: 2
            AD Type: Flags
            AD Data
                BR/EDR Not Supported: Yes
                LE General Discoverable Mode: Yes
        AD Element
            Length: 11
            AD Type: Complete list of 16-bit UUIDs
            AD Data
                UUID: Health Thermometer
                UUID: Heart Rate Monitor
                UUID: Blood Pressure Monitor
                UUID: Weight Scale
                UUID: Body Composition
        AD Element
            Length: 13
```

B...	Frame#	ASCII	Hex	Fram...	Delta	Timestamp
	1			53		1/27/2015 10:02:04.6235...
	2			53	00:00:00.0...	1/27/2015 10:02:04.6285...
	3			53	00:00:00.0...	1/27/2015 10:02:04.6335...
	4			53	00:00:00.0...	1/27/2015 10:02:04.6479...
	5			53	00:00:00.0...	1/27/2015 10:02:04.6529...
	6			30	00:00:00.0...	1/27/2015 10:02:04.6534...
	7			38	00:00:00.0...	1/27/2015 10:02:04.6537...
	8			53	00:00:00.0...	1/27/2015 10:02:04.6579...
	9			30	00:00:00.0...	1/27/2015 10:02:04.6584...
	10			38	00:00:00.0...	1/27/2015 10:02:04.6587...
	11			53	00:00:00.0...	1/27/2015 10:02:04.6773...
	12			53	00:00:00.0...	1/27/2015 10:02:04.6823...
	13			53	00:00:00.0...	1/27/2015 10:02:04.6873...
	14			30	00:00:00.0...	1/27/2015 10:02:04.6878...
	15			38	00:00:00.0...	1/27/2015 10:02:04.6881...
	16			53	00:00:00.0...	1/27/2015 10:02:04.7060...
	17			30	00:00:00.0...	1/27/2015 10:02:04.7065...
	18			38	00:00:00.0...	1/27/2015 10:02:04.7069...
	19			53	00:00:00.0...	1/27/2015 10:02:04.7110...
	20			53	00:00:00.0...	1/27/2015 10:02:04.7160...
	21			53	00:00:00.0...	1/27/2015 10:02:04.7335...
	22			30	00:00:00.0...	1/27/2015 10:02:04.7340...
	23			38	00:00:00.0...	1/27/2015 10:02:04.7344...
	24			53	00:00:00.0...	1/27/2015 10:02:04.7385...
	25			53	00:00:00.0...	1/27/2015 10:02:04.7435...
	26			53	00:00:00.0...	1/27/2015 10:02:04.7585...
	27			53	00:00:00.0...	1/27/2015 10:02:04.7635...
	28			53	00:00:00.0...	1/27/2015 10:02:04.7685...
	29			53	00:00:00.0...	1/27/2015 10:02:04.7792...
	30			53	00:00:00.0...	1/27/2015 10:02:04.7842...

Total Frames: 6,767 Frames Filtered In: 6,017 Frame #s Selected: 1; (1 total)

Figure 4.33 - 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.

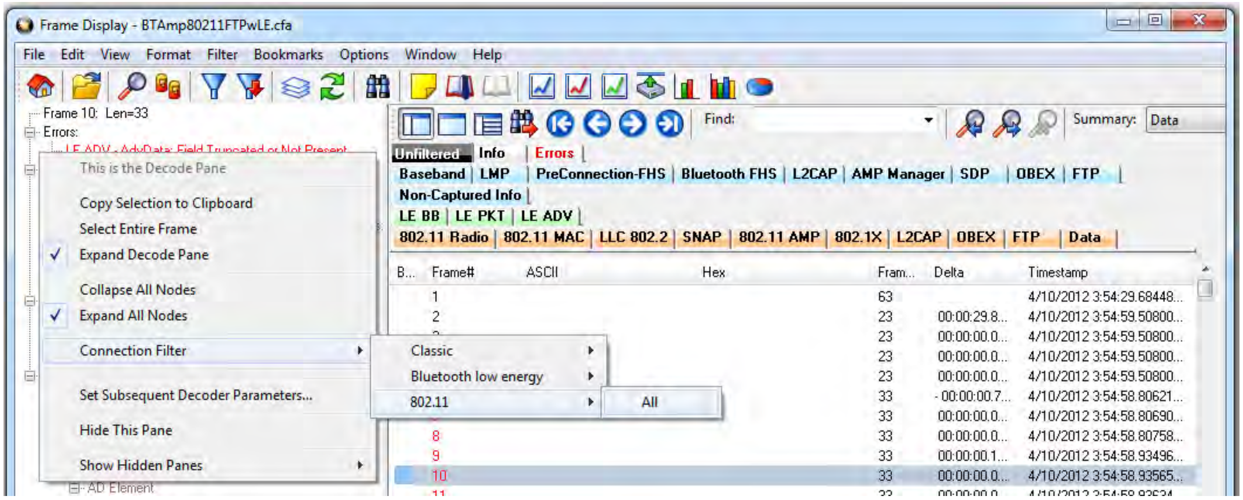

Frame Display - BTAmp80211FTPwLE.cfa
File Edit View Format Filter Bookmarks Options Window Help
Frame 10: Len=33
Errors:
This is the Decode Pane
Copy Selection to Clipboard
Select Entire Frame
Expand Decode Pane
Collapse All Nodes
Expand All Nodes
Connection Filter
Set Subsequent Decoder Parameters...
Hide This Pane
Show Hidden Panes
Classic
Bluetooth low energy
802.11
All
Find:
Summary: Data
Unfiltered Info Errors
Baseband LMP PreConnection-FHS Bluetooth FHS L2CAP AMP Manager SDP OBEX FTP
Non-Captured Info
LE BB LE PKT LE ADV
802.11 Radio 802.11 MAC LLC 802.2 SNAP 802.11 AMP 802.1X L2CAP OBEX FTP Data
B... Frame# ASCII Hex Fram... Delta Timestamp

Figure 4.34 - 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.

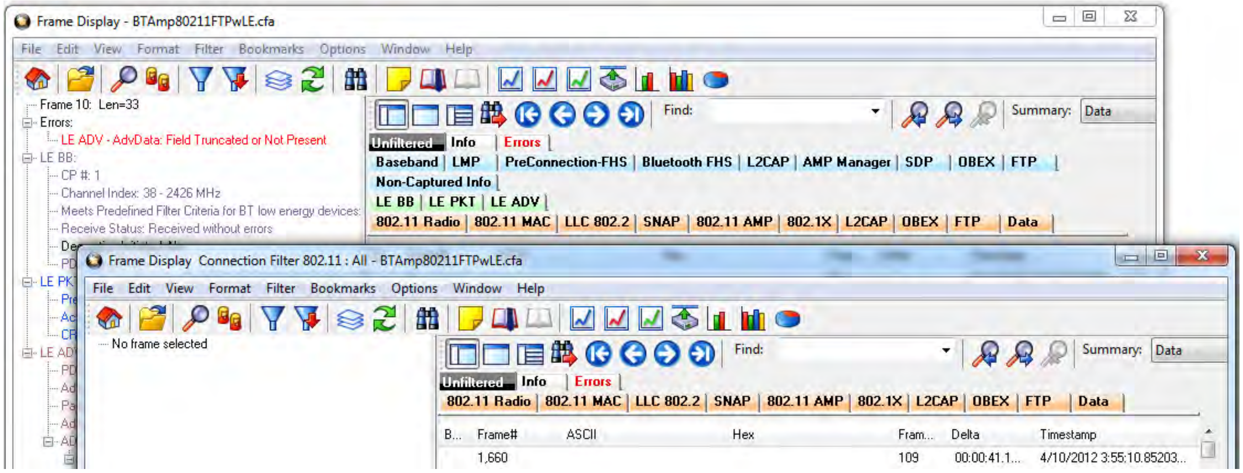

Frame Display - BTAmp80211FTPwLE.cfa
Frame 10: Len=33
Errors:
LE ADV - AdvData: Field Truncated or Not Present
LE BB:
CP #: 1
Channel Index: 38 - 2426 MHz
Meets Predefined Filter Criteria for BT low energy devices
Receive Status: Received without errors
Frame Display Connection Filter 802.11 : All - BTAmp80211FTPwLE.cfa
File Edit View Format Filter Bookmarks Options Window Help
No frame selected
Find:
Summary: Data
Unfiltered Info Errors
802.11 Radio 802.11 MAC LLC 802.2 SNAP 802.11 AMP 802.1X L2CAP OBEX FTP Data
B... Frame# ASCII Hex Fram... Delta Timestamp
1,660 109 00:00:41.1... 4/10/2012 3:55:10.85203...

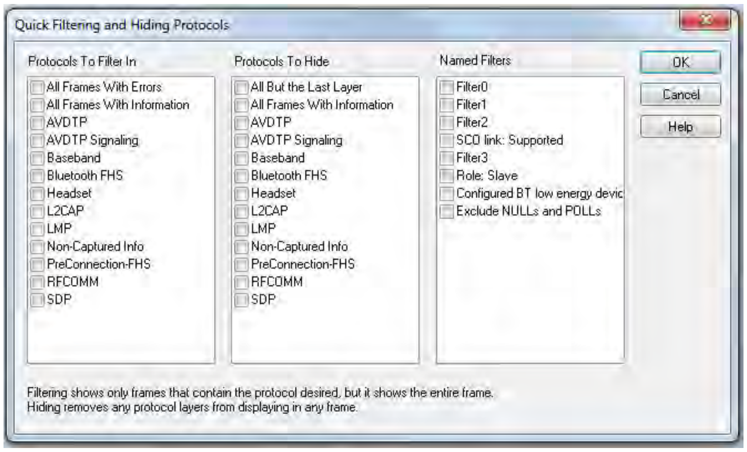
Figure 4.35 - Connection Filter selecting All 802.11 frames, front

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.


Quick Filtering and Hiding Protocols

Protocols To Filter In
□ All Frames With Errors
□ All Frames With Information
□ AVDTP
□ AVDTP Signaling
□ Baseband
□ Bluetooth FHS
□ Headset
□ L2CAP
□ LMP
□ Non-Captured Info
□ PreConnection-FHS
□ RFCOMM
□ SDP

Protocols To Hide
□ All But the Last Layer
□ All Frames With Information
□ AVDTP
□ AVDTP Signaling
□ Baseband
□ Bluetooth FHS
□ Headset
□ L2CAP
□ LMP
□ Non-Captured Info
□ PreConnection-FHS
□ RFCOMM
□ SDP

Named Filters
□ Filter0
□ Filter1
□ Filter2
□ SCO link: Supported
□ Filter3
□ Role: Slave
□ Configured BT low energy devic
□ Exclude NULLs and POLLs

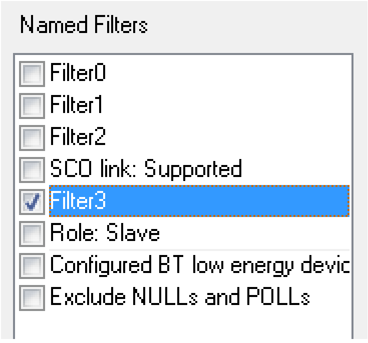
Filtering shows only frames that contain the protocol desired, but it shows the entire frame.
Hiding removes any protocol layers from displaying in any frame.

Figure 4.36 - 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.


Named Filters
□ Filter0
□ Filter1
□ Filter2
□ SCO link: Supported
☑ Filter3
□ Role: Slave
□ Configured BT low energy devic
□ Exclude NULLs and POLLs

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.

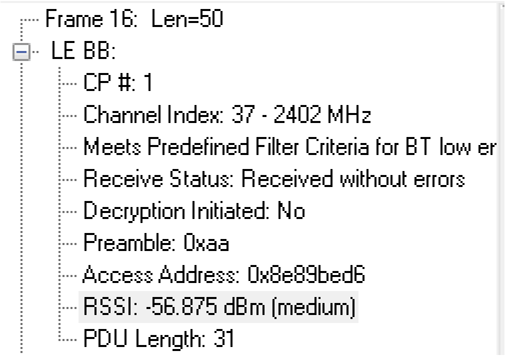
Filtering on all Frames with Errors

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.

> **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



```
Frame 16:  Len=50
LE BB:
    CP #: 1
    Channel Index: 37 - 2402 MHz
    Meets Predefined Filter Criteria for BT low er
    Receive Status: Received without errors
    Decryption Initiated: No
    Preamble: 0xaa
    Access Address: 0x8e89bed6
    RSSI: -56.875 dBm (medium)
    PDU Length: 31
```

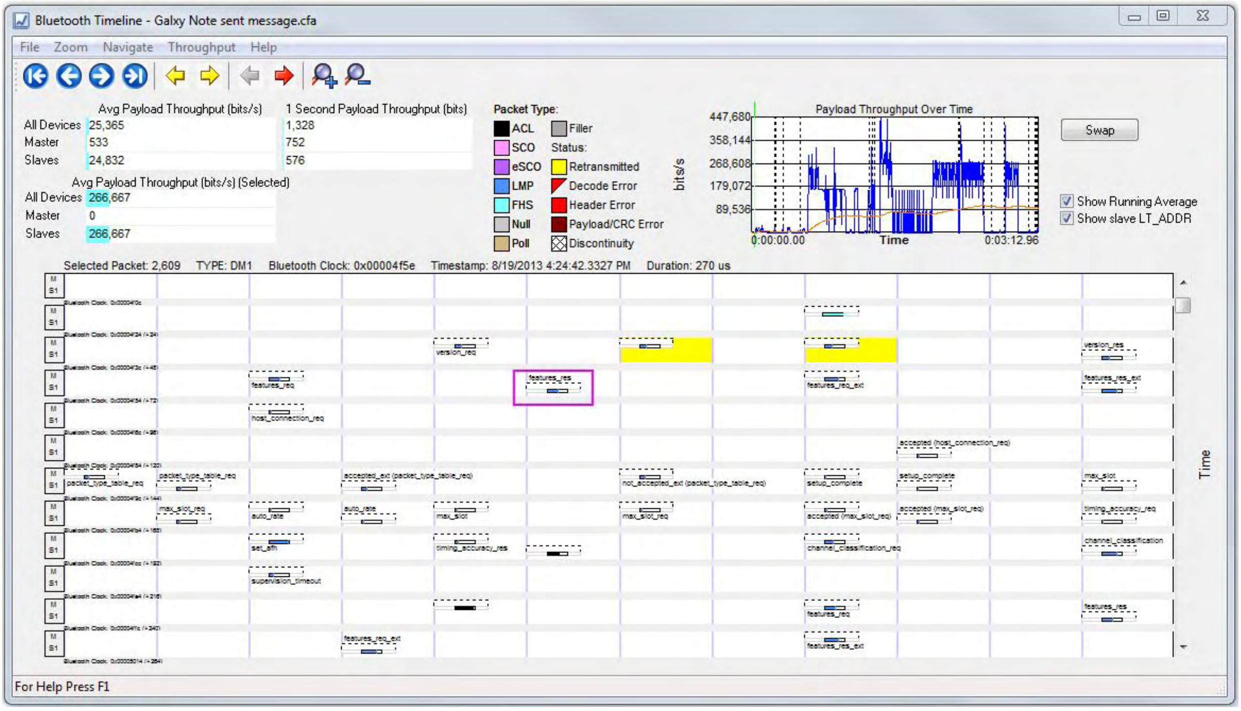
The Sodera calculates the RSSI (Receiver Signal Strength Indicator) value, a representation of the radio signal strength at the Sodera receiver, for every *Bluetooth* packet that it captures. RSSI is shown in dBm with a relative signal strength in parentheses. The RSSI value is shown as a decoded field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



Bluetooth Timeline - Galxy Note sent message.cfa

	Avg Payload Throughput (bits/s)	1 Second Payload Throughput (bits)
All Devices	25,365	1,328
Master	533	752
Slaves	24,832	576

	Avg Payload Throughput (bits/s) (Selected)
All Devices	266,667
Master	0
Slaves	266,667

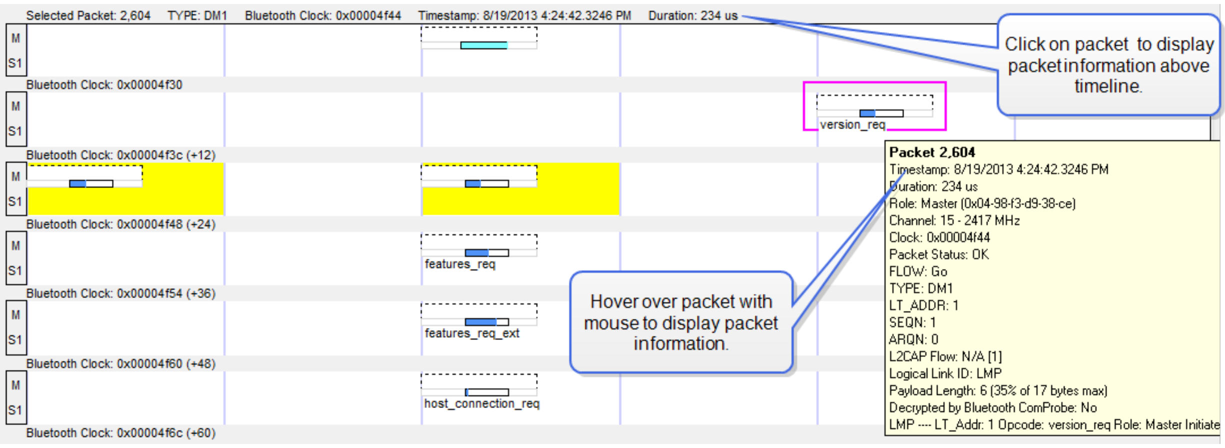
Selected Packet: 2,609 TYPE: DM1 Bluetooth Clock: 0x00004f5e Timestamp: 8/19/2013 4:24:42.3327 PM Duration: 270 us

For Help Press F1

Figure 4.37 - 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



Selected Packet: 2,604 TYPE: DM1 Bluetooth Clock: 0x00004f44 Timestamp: 8/19/2013 4:24:42.3246 PM Duration: 234 us

Click on packet to display packet information above timeline.

Hover over packet with mouse to display packet information.

Packet 2,604
Timestamp: 8/19/2013 4:24:42.3246 PM
Duration: 234 us
Role: Master (0x04-98-f3-d9-38-ce)
Channel: 15 - 2417 MHz
Clock: 0x00004f44
Packet Status: OK
FLOW: Go
TYPE: DM1
LT_ADDR: 1
SEQN: 1
ARQN: 0
L2CAP Flow: N/A [1]
Logical Link ID: LMP
Payload Length: 6 (35% of 17 bytes max)
Decrypted by Bluetooth ComProbe: No
LMP ---- LT_Addr: 1 Opcode: version_req Role: Master Initiate

M
S1
Bluetooth Clock: 0x00004f30
Bluetooth Clock: 0x00004f3c (+12)
Bluetooth Clock: 0x00004f48 (+24)
Bluetooth Clock: 0x00004f54 (+36)
Bluetooth Clock: 0x00004f60 (+48)
Bluetooth Clock: 0x00004f6c (+60)
version_req
features_req
features_req_ext
host_connection_req

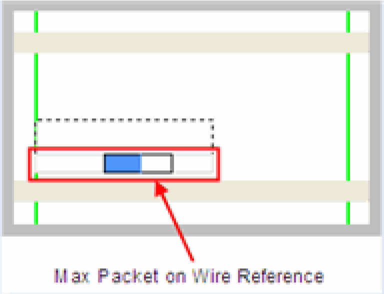
Figure 4.38 - Bluetooth Timeline Packet Depiction with Packet Information Shown

- 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.

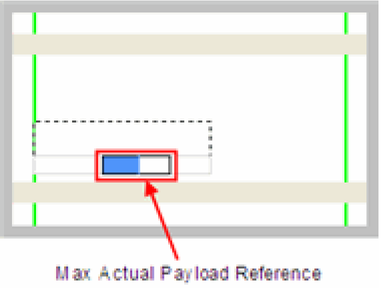
- Within each row are two divisions: **M** (master) and **S** (Slave). Packets are placed on **M** or **S** depending on the data's role.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about 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:

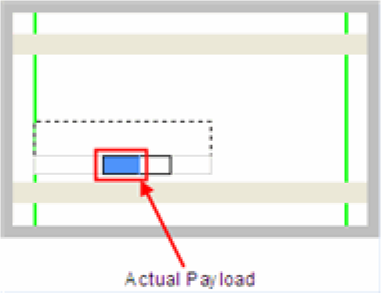
- A “max packet on wire reference” rectangle (light solid lines). This indicates the packet in the air with a max payload.



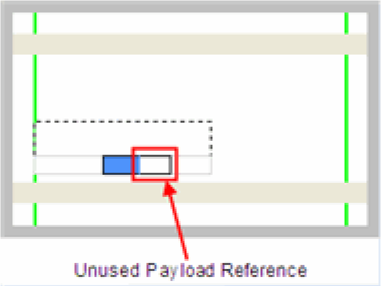
- A “max actual payload reference” rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload in the air contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates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



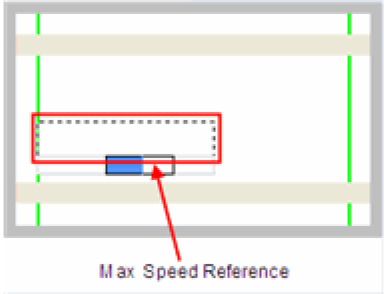
- An “actual payload” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference” rectangle. If the actual payload is of max size, the entire “max actual payload reference”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



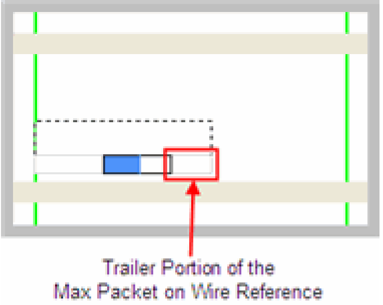
- An “unused payload reference” sub-rectangle (always white). This indicates the unused portion of a maximum payload. It is the remaining portion of the “max actual payload reference” rectangle. The packet in the air does not leave room for this. It is indicated for reference only.



- 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
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

Table 4.5 - Packet Information Presentation (continued)

Information	Text	Color	Graphic size	Position
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 158 .
- 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 168 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 163 .
- 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 168 .
- Graphical Packet Depiction: Each packet within the visible range is graphically depicted. See the Bluetooth Timeline Packet Depiction on page 154.
- 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

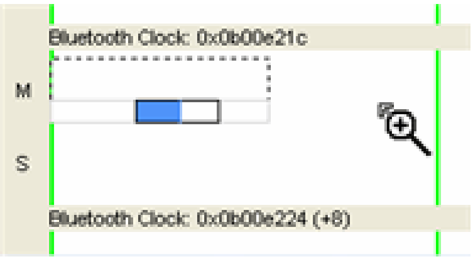
> **Note:** The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

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.

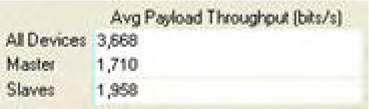


4.3.2.7 *Bluetooth* Timeline Throughput Displays

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.

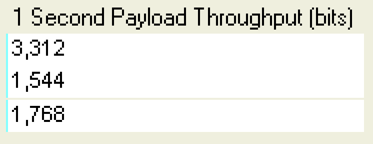


	Avg Payload Throughput (bits/s)
All Devices	3,668
Master	1,710
Slaves	1,958

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

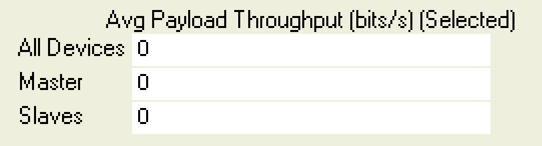


1 Second Payload Throughput (bits)
3,312
1,544
1,768

- 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)

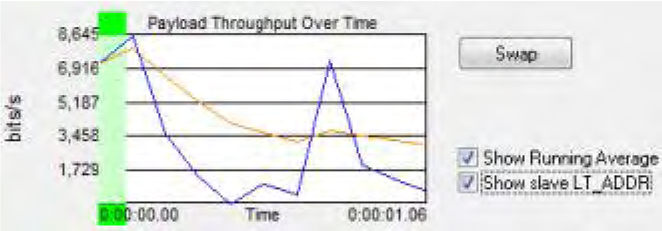
All Devices	0
Master	0
Slaves	0

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.

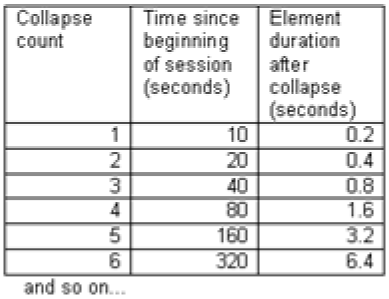
- Duration for average throughput is beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- Average throughput can be nonzero when a single packet is selected.
- Average throughput is shown for all devices, master devices, and slave devices.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

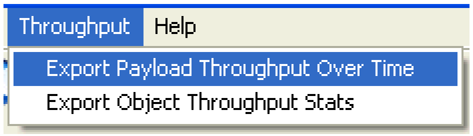
In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about the **Payload Throughput Over Time** graph. The file contains the following information:

- 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.


Throughput
Help
Export Payload Throughput Over Time
Export Object Throughput Stats

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

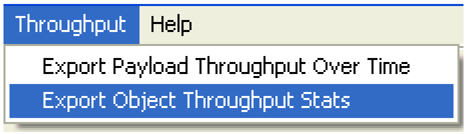
In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about objects in the timeline. The file contains the following information:

- 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.


Throughput
Help
Export Payload Throughput Over Time
Export Object Throughput Stats

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.

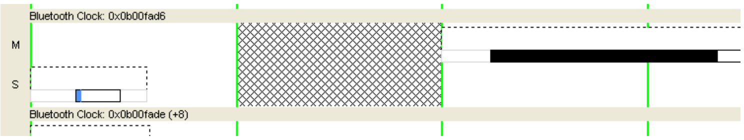
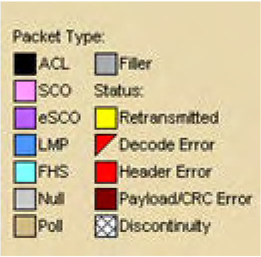


Figure 4.39 - *Bluetooth* Timeline Packet Discontinuity, cross-hatched area.

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."

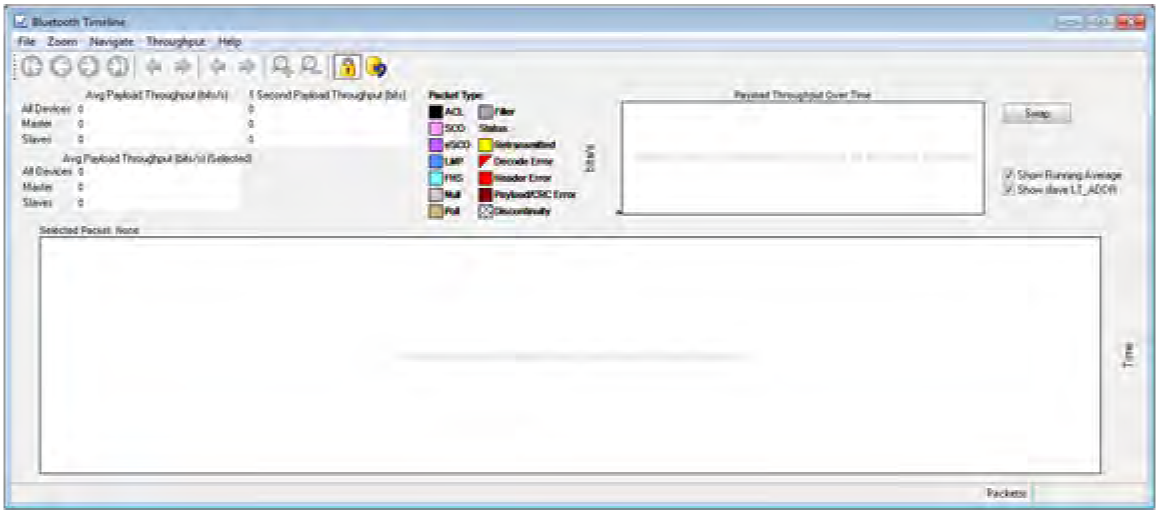
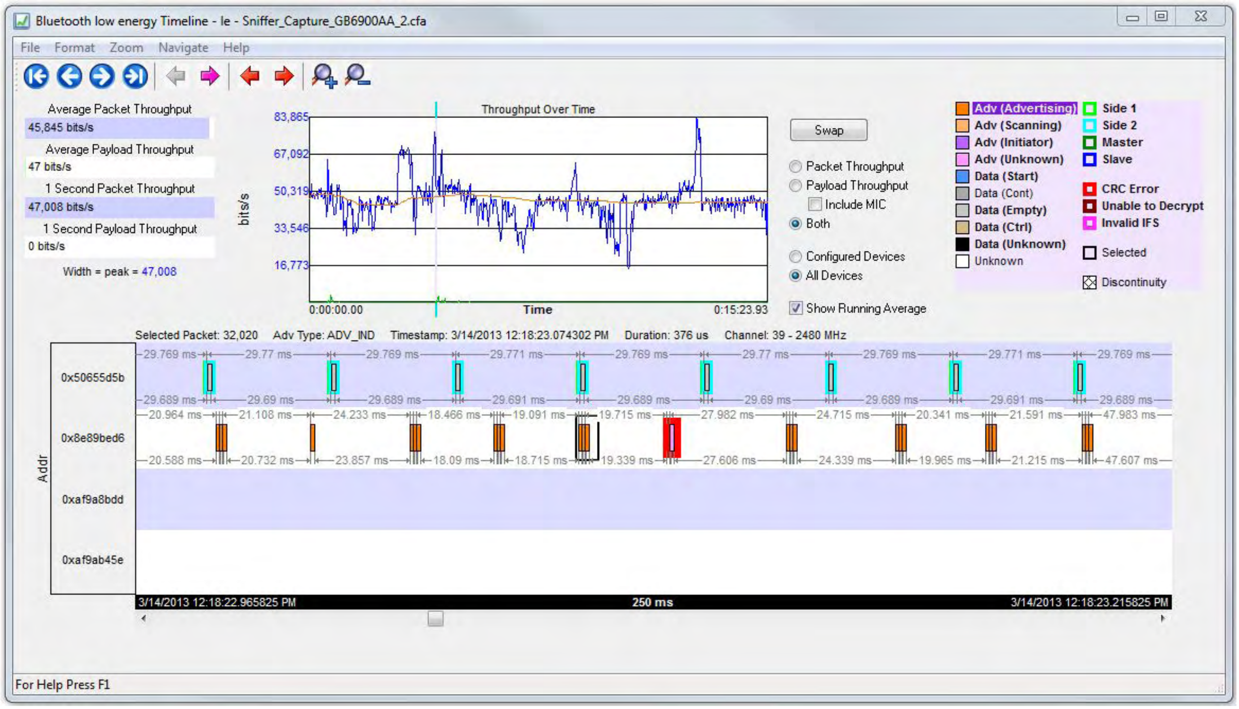


Figure 4.40 - Missing packets message in timeline pane.

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.


Average Packet Throughput
45,845 bits/s
Average Payload Throughput
47 bits/s
1 Second Packet Throughput
47,008 bits/s
1 Second Payload Throughput
0 bits/s
Width = peak = 47,008

Selected Packet: 32,020 Adv Type: ADV_IND Timestamp: 3/14/2013 12:18:23.074302 PM Duration: 376 us Channel: 39 - 2480 MHz

Figure 4.41 - *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
⇦	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

Table 4.7 - Bluetooth low energy Timeline Toolbar (continued)

Icon	Description
↻	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

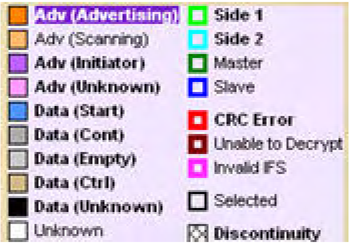
Table 4.8 - Bluetooth low energy Timeline Menus (continued)

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



🟧 **Adv (Advertising)**	🟩 **Side 1**
🟧 Adv (Scanning)	🟦 **Side 2**
🟪 **Adv (Initiator)**	🟩 Master
🟪 **Adv (Unknown)**	🟦 Slave
🟦 **Data (Start)**	🟥 **CRC Error**
⬜ **Data (Cont)**	🟥 Unable to Decrypt
⬜ **Data (Empty)**	🟪 Invalid IFS
🟫 **Data (Ctrl)**	□ Selected
⬛ **Data (Unknown)**	☒ **Discontinuity**
□ Unknown	

This legend identifies the color coding found in the timeline.

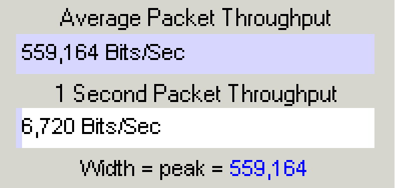
- When you select a packet in the timeline, items in the legend that relate to the packet are highlighted.
- Bold text indicates that the type of packet has been seen in the timeline.

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

559,164 Bits/Sec

1 Second Packet Throughput

6,720 Bits/Sec

Width = peak = 559,164

- **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

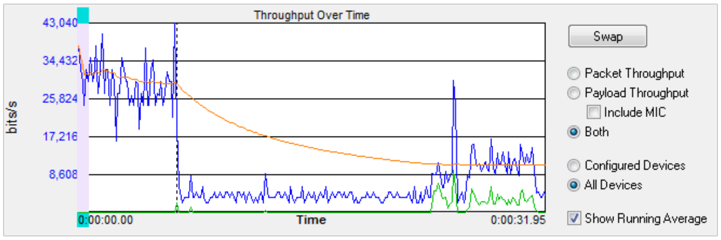
The figure depicts the **Average** and **One Second Payload** Throughput display. This display appears when you select the **Payload Throughput** radio button.

- **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.



○ Packet Throughput
○ Payload Throughput
□ Include MIC
● Both
○ Configured Devices
● All Devices
☑ Show Running Average

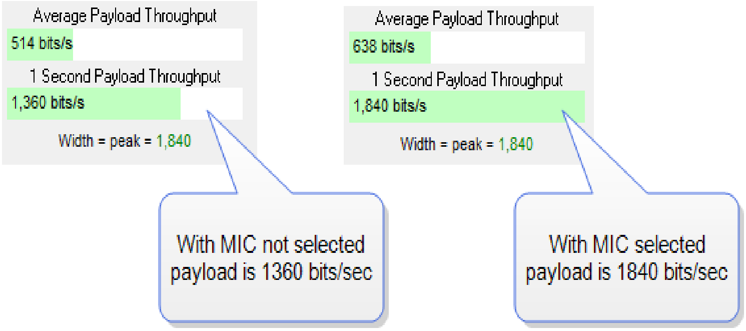
Figure 4.42 - *Bluetooth* low energy Timeline Throughput Graph

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.



Average Payload Throughput
514 bits/s
1 Second Payload Throughput
1,360 bits/s
Width = peak = 1,840

With MIC not selected payload is 1360 bits/sec

Average Payload Throughput
638 bits/s
1 Second Payload Throughput
1,840 bits/s
Width = peak = 1,840

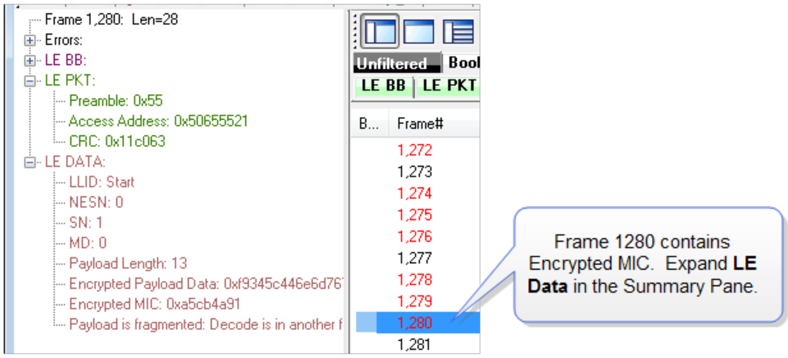
With MIC selected payload is 1840 bits/sec

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.

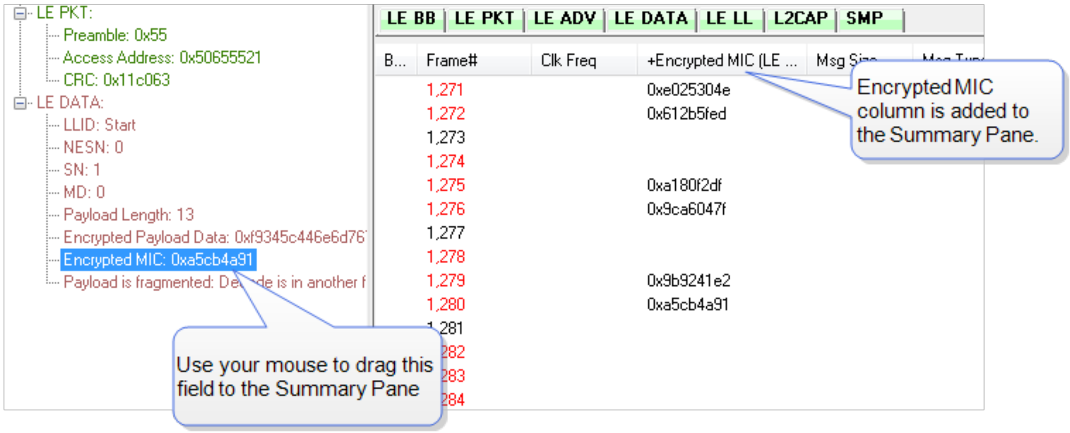


```
Frame 1,280:  Len=28
Errors:
LE BB:
LE PKT:
    Preamble: 0x55
    Access Address: 0x50655521
    CRC: 0x11c063
LE DATA:
    LLID: Start
    NESN: 0
    SN: 1
    MD: 0
    Payload Length: 13
    Encrypted Payload Data: 0xf9345c446e6d76
    Encrypted MIC: 0xa5cb4a91
    Payload is fragmented: Decode is in another f
```

B...	Frame#
	1,272
	1,273
	1,274
	1,275
	1,276
	1,277
	1,278
	1,279
	1,280
	1,281

Frame 1280 contains Encrypted MIC. Expand **LE Data** in the Summary Pane.

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



```
LE PKT:
    Preamble: 0x55
    Access Address: 0x50655521
    CRC: 0x11c063
LE DATA:
    LLID: Start
    NESN: 0
    SN: 1
    MD: 0
    Payload Length: 13
    Encrypted Payload Data: 0xf9345c446e6d76
    Encrypted MIC: 0xa5cb4a91
    Payload is fragmented: Decode is in another f
```

B...	Frame#	Clk Freq	+Encrypted MIC (LE ...	Msg Size	Msg Type
	1,271		0xe025304e		
	1,272		0x612b5fed		
	1,273				
	1,274				
	1,275		0xa180f2df		
	1,276		0x9ca6047f		
	1,277				
	1,278				
	1,279		0x9b9241e2		
	1,280		0xa5cb4a91		
	1,281				
	1,282				
	1,283				
	1,284				

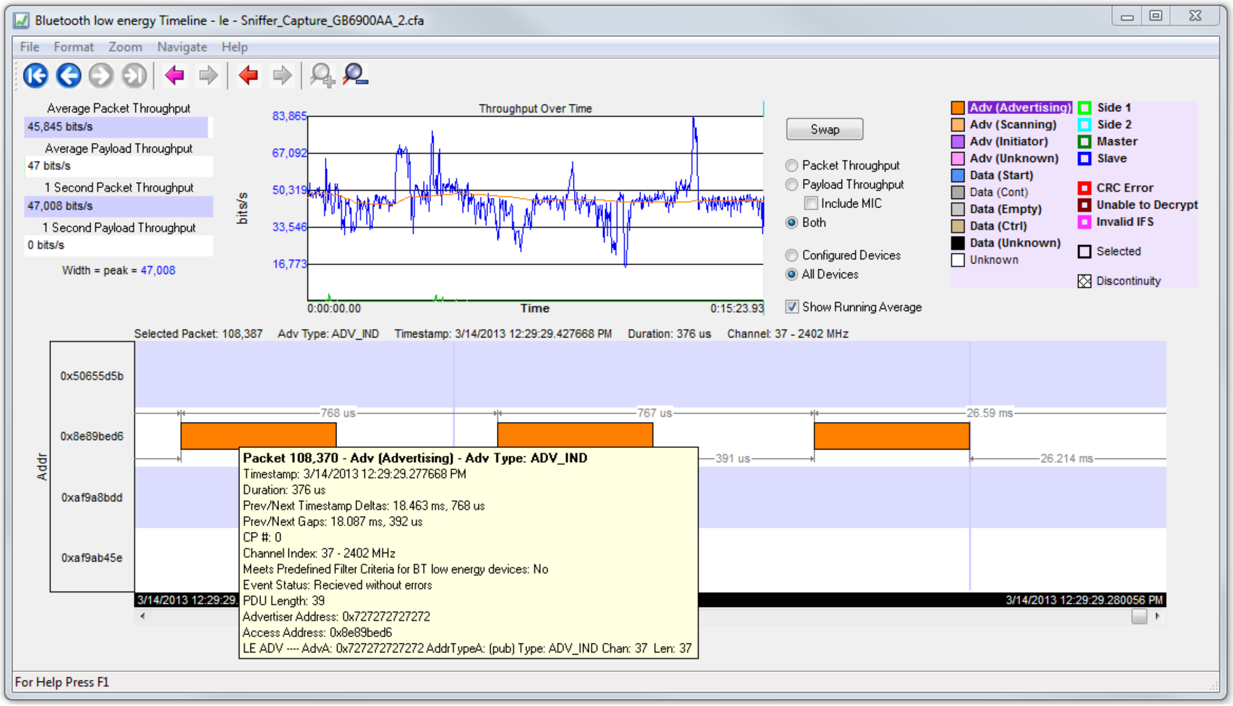
Encrypted MIC column is added to the Summary Pane.

Use your mouse to drag this field to the Summary Pane

Figure 4.43 - 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.



Average Packet Throughput: 45,845 bits/s

Average Payload Throughput: 47 bits/s

1 Second Packet Throughput: 47,008 bits/s

1 Second Payload Throughput: 0 bits/s

Width = peak = 47,008

○ Packet Throughput
○ Payload Throughput
□ Include MIC
● Both

○ Configured Devices
● All Devices

☑ Show Running Average

Selected Packet: 108,387 Adv Type: ADV_IND Timestamp: 3/14/2013 12:29:29.427668 PM Duration: 376 us Channel: 37 - 2402 MHz

Packet 108,370 - Adv (Advertising) - Adv Type: ADV_IND
Timestamp: 3/14/2013 12:29:29.277668 PM
Duration: 376 us
Prev/Next Timestamp Deltas: 18.463 ms, 768 us
Prev/Next Gaps: 18.087 ms, 392 us
CP #: 0
Channel Index: 37 - 2402 MHz
Meets Predefined Filter Criteria for BT low energy devices: No
Event Status: Recieved without errors
PDU Length: 39
Advertiser Address: 0x727272727272
Access Address: 0x8e89bed6
LE ADV ---- AdvA: 0x727272727272 AddrTypeA: (pub) Type: ADV_IND Chan: 37 Len: 37

Figure 4.44 - *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.

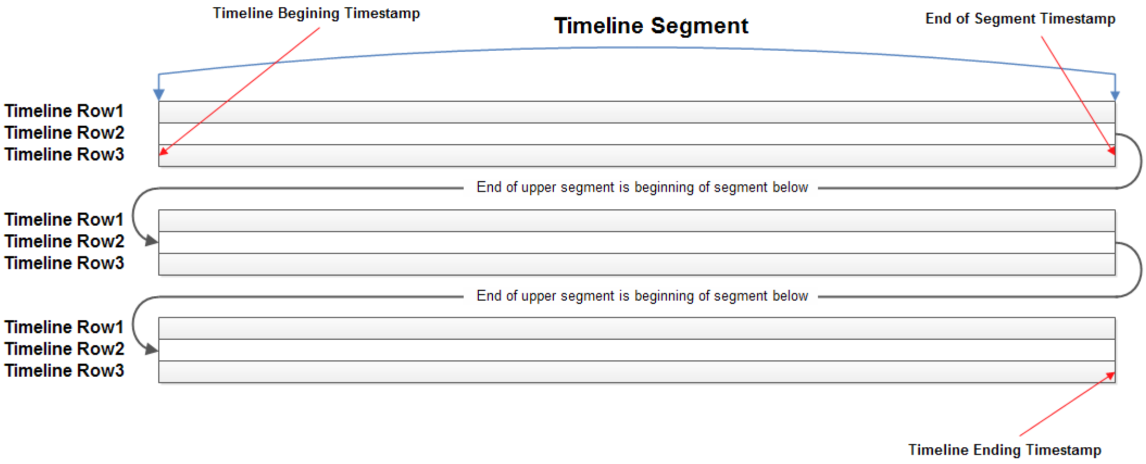
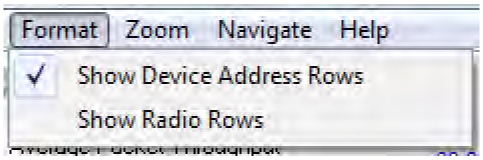


Figure 4.45 - Diagram of low energy Timeline Flow with Segment and Row Relationship

- 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.

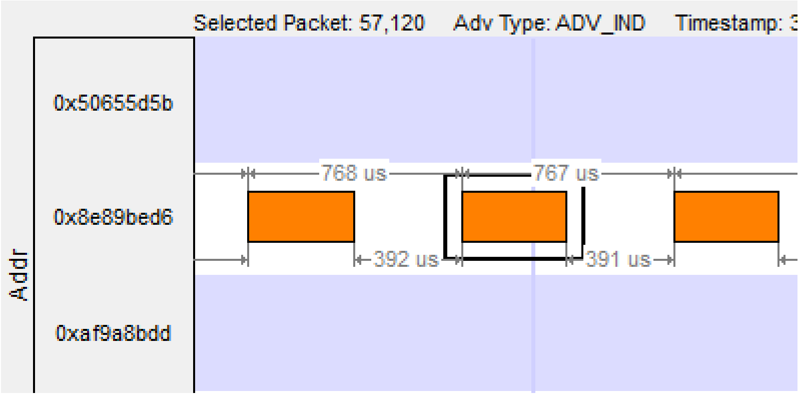


Figure 4.46 - Device Address Rows

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

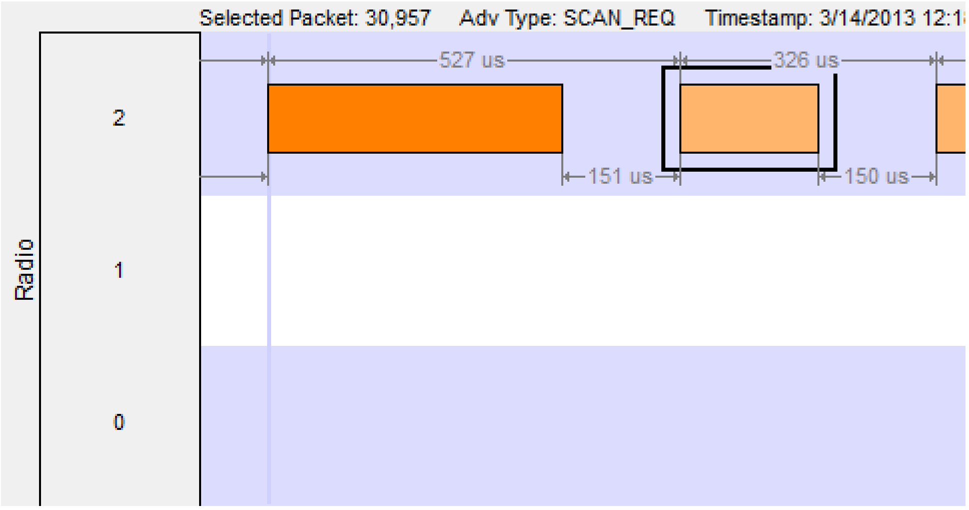
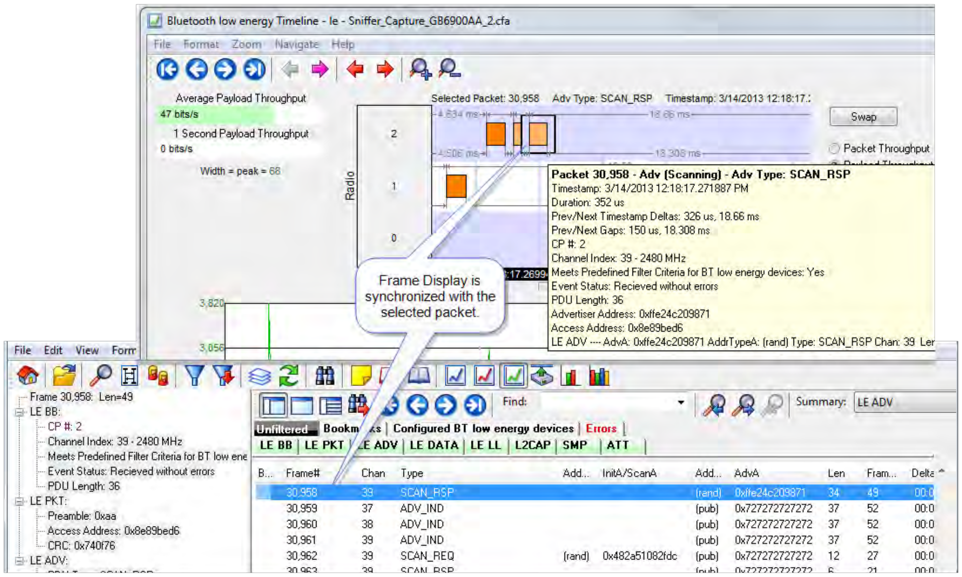


Figure 4.47 - Radio Rows

- 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.


Bluetooth low energy Timeline - le - Sniffer_Capture_GB6900AA_2.cfa
File Format Zoom Navigate Help
Average Payload Throughput
47 bits/s
1 Second Payload Throughput
0 bits/s
Width = peak = 68
Selected Packet: 30,958 Adv Type: SCAN_RSP Timestamp: 3/14/2013 12:18:17.:
Swap
Packet Throughput
Radio
2
1
0
4.834 ms
18.66 ms
4.506 ms
18.308 ms
3,820
3,056
:17.2699
Frame Display is synchronized with the selected packet.
File Edit View Form
Find:
Summary: LE ADV
Unfiltered Bookm ks | Configured BT low energy devices | Errors |
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT

Packet 30,958 - Adv (Scanning) - Adv Type: SCAN_RSP
Timestamp: 3/14/2013 12:18:17.271887 PM
Duration: 352 us
Prev/Next Timestamp Deltas: 326 us, 18.66 ms
Prev/Next Gaps: 150 us, 18.308 ms
CP #: 2
Channel Index: 39 - 2480 MHz
Meets Predefined Filter Criteria for BT low energy devices: Yes
Event Status: Recieved without errors
PDU Length: 36
Advertiser Address: 0xffe24c209871
Access Address: 0x8e89bed6
LE ADV ---- AdvA: 0xffe24c209871 AddrTypeA: (rand) Type: SCAN_RSP Chan: 39 Ler

```
Frame 30,958:  Len=49
LE BB:
    CP #: 2
    Channel Index: 39 - 2480 MHz
    Meets Predefined Filter Criteria for BT low ene
    Event Status: Recieved without errors
    PDU Length: 36
LE PKT:
    Preamble: 0xaa
    Access Address: 0x8e89bed6
    CRC: 0x740f76
LE ADV:
```

B...	Frame#	Chan	Type	Add...	InitA/ScanA	Add...	AdvA	Len	Fram...	Delta
	30,958	39	SCAN_RSP			(rand)	0xffe24c209871	34	49	00:0
	30,959	37	ADV_IND			(pub)	0x727272727272	37	52	00:0
	30,960	38	ADV_IND			(pub)	0x727272727272	37	52	00:0
	30,961	39	ADV_IND			(pub)	0x727272727272	37	52	00:0
	30,962	39	SCAN_REQ	(rand)	0x482a51082fdc	(pub)	0x727272727272	12	27	00:0

Figure 4.48 - **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.

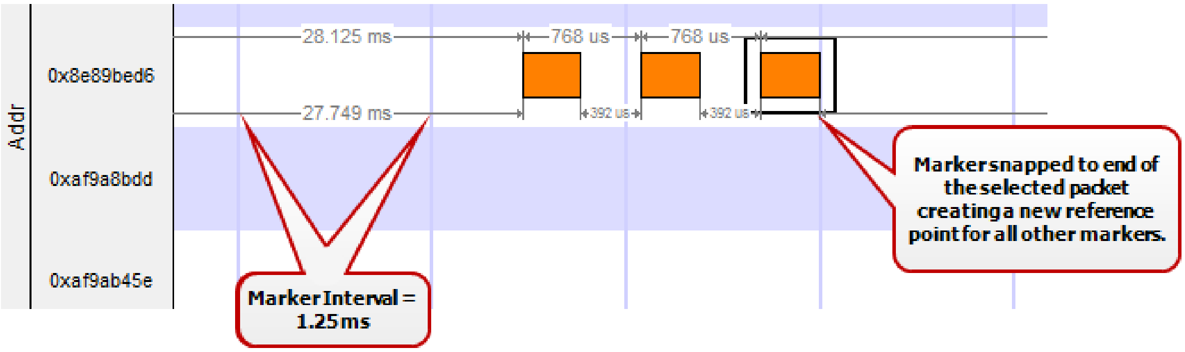

Addr
0x8e89bed6
0xaf9a8bdd
0xaf9ab45e
28.125 ms
768 us
768 us
27.749 ms
392 us
392 us
Marker Interval = 1.25 ms
Marker snapped to end of the selected packet creating a new reference point for all other markers.

Figure 4.49 - 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.

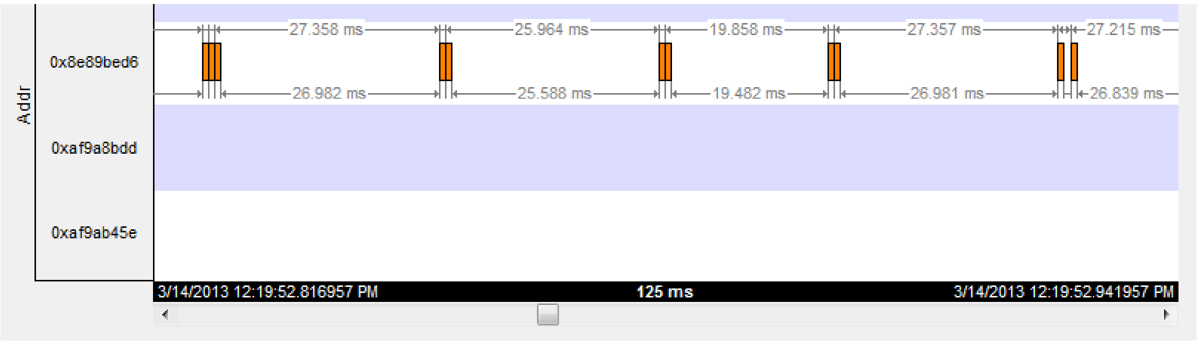
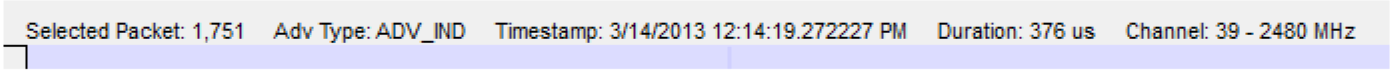


Figure 4.50 - Bluetooth le Timeline Segment Timestamp and Zoom Value

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

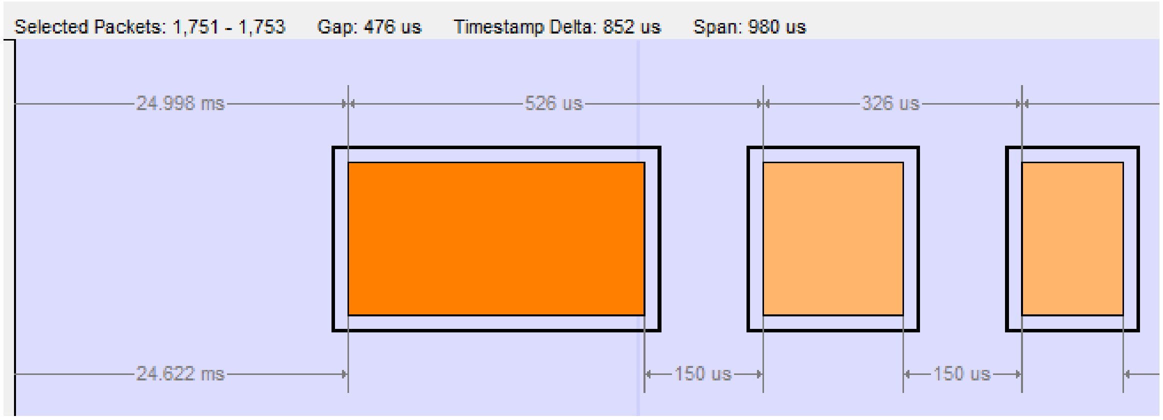
- Packet Info Line - The packet info line appears just above the timeline and displays information for the currently selected packet.



Selected Packet: 1,751 Adv Type: ADV_IND Timestamp: 3/14/2013 12:14:19.272227 PM Duration: 376 us Channel: 39 - 2480 MHz

Figure 4.51 - 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



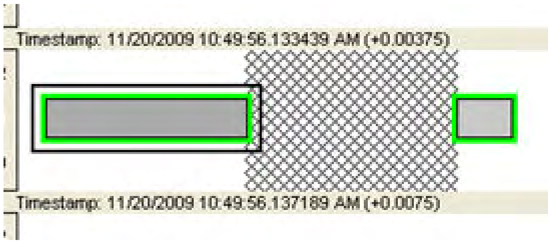
Selected Packets: 1,751 - 1,753 Gap: 476 us Timestamp Delta: 852 us Span: 980 us

Figure 4.52 - 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.



Timestamp: 11/20/2009 10:49:56.133439 AM (+0.00375)

Timestamp: 11/20/2009 10:49:56.137189 AM (+0.0075)

Figure 4.53 - 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

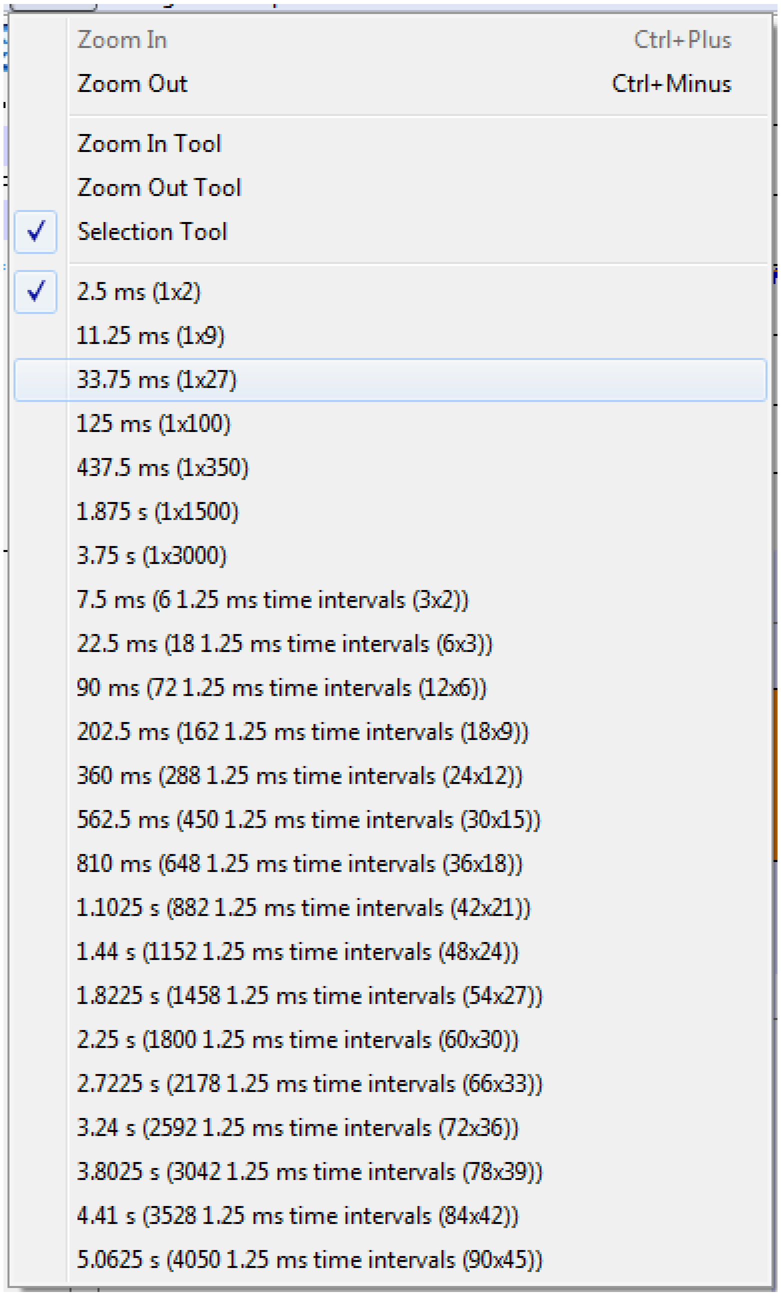
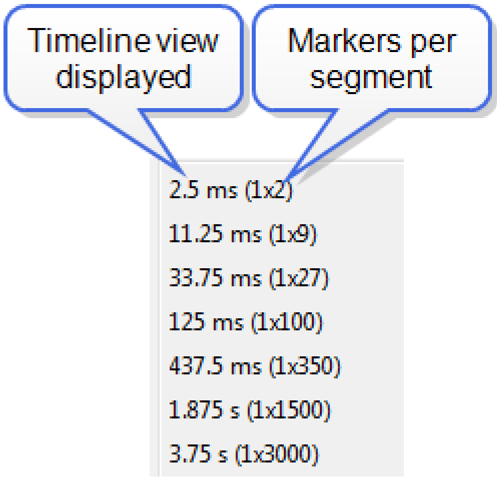

Zoom In Ctrl+Plus
Zoom Out Ctrl+Minus
Zoom In Tool
Zoom Out Tool
✓ Selection Tool
✓ 2.5 ms (1x2)
11.25 ms (1x9)
33.75 ms (1x27)
125 ms (1x100)
437.5 ms (1x350)
1.875 s (1x1500)
3.75 s (1x3000)
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (12x6))
202.5 ms (162 1.25 ms time intervals (18x9))
360 ms (288 1.25 ms time intervals (24x12))
562.5 ms (450 1.25 ms time intervals (30x15))
810 ms (648 1.25 ms time intervals (36x18))
1.1025 s (882 1.25 ms time intervals (42x21))
1.44 s (1152 1.25 ms time intervals (48x24))
1.8225 s (1458 1.25 ms time intervals (54x27))
2.25 s (1800 1.25 ms time intervals (60x30))
2.7225 s (2178 1.25 ms time intervals (66x33))
3.24 s (2592 1.25 ms time intervals (72x36))
3.8025 s (3042 1.25 ms time intervals (78x39))
4.41 s (3528 1.25 ms time intervals (84x42))
5.0625 s (4050 1.25 ms time intervals (90x45))

Figure 4.54 - low energy Timeline Zoom menu

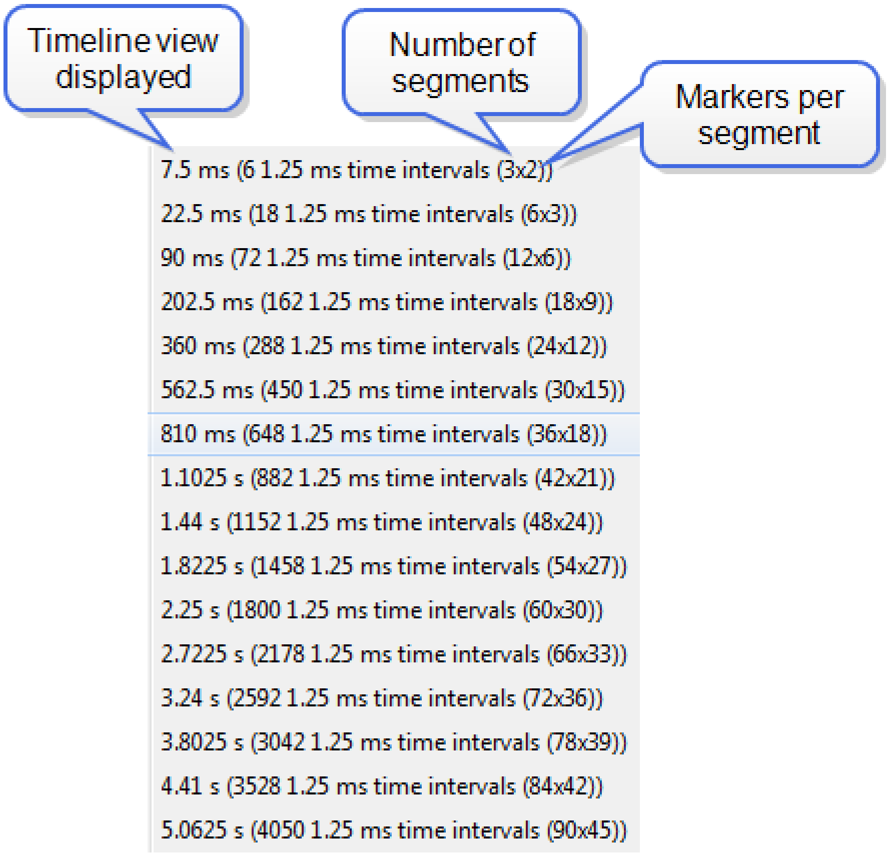
4.3.3.16 Single Segment Zoom



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


Timeline view displayed
Number of segments
Markers per segment
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (12x6))
202.5 ms (162 1.25 ms time intervals (18x9))
360 ms (288 1.25 ms time intervals (24x12))
562.5 ms (450 1.25 ms time intervals (30x15))
810 ms (648 1.25 ms time intervals (36x18))
1.1025 s (882 1.25 ms time intervals (42x21))
1.44 s (1152 1.25 ms time intervals (48x24))
1.8225 s (1458 1.25 ms time intervals (54x27))
2.25 s (1800 1.25 ms time intervals (60x30))
2.7225 s (2178 1.25 ms time intervals (66x33))
3.24 s (2592 1.25 ms time intervals (72x36))
3.8025 s (3042 1.25 ms time intervals (78x39))
4.41 s (3528 1.25 ms time intervals (84x42))
5.0625 s (4050 1.25 ms time intervals (90x45))

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.

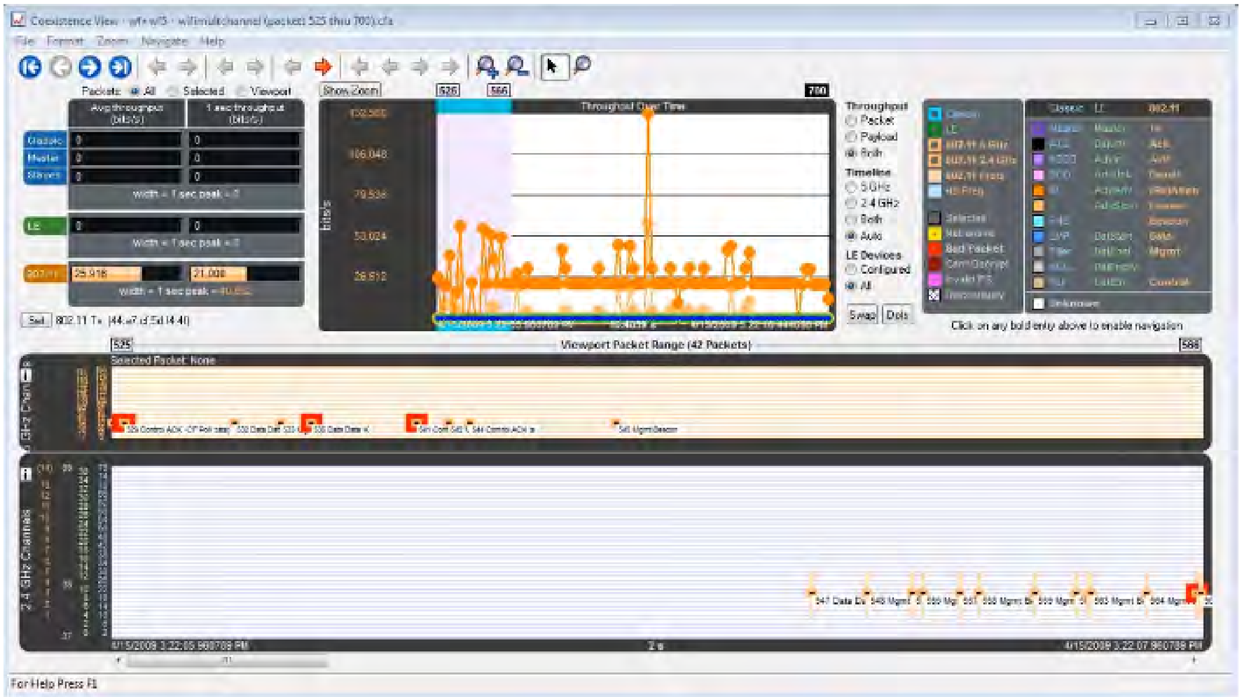
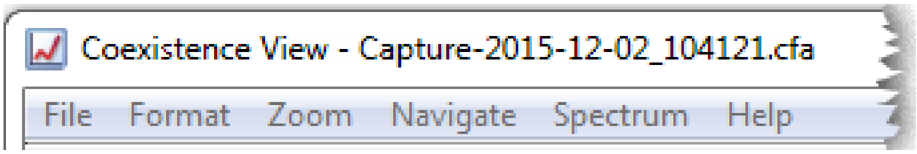

Coexistence View - wfi+wf5 - wifimultichannel (packets 525 thru 700).cfa
File Format Zoom Navigate Help
Packets: All Selected Viewport
Avg throughput (bits/s)
1 sec throughput (bits/s)
Classic
Master
Slaves
LE
802.11
Show Zoom
526
566
700
Throughput Over Time
bits/s
132,560
106,048
79,536
53,024
26,512
Throughput
Packet
Payload
Both
Timeline
5 GHz
2.4 GHz
Both
Auto
LE Devices
Configured
All
Swap
Dots
Classic LE 802.11
Click on any bold entry above to enable navigation
525
Viewport Packet Range (42 Packets)
566
Selected Packet: None
2.4 GHz Channels
4/15/2009 3:22:05.960789 PM
2 s
4/15/2009 3:22:07.960789 PM
For Help Press F1

Figure 4.55 - 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

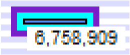
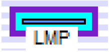
Selection	Description
Show Packet Number	When checked, the packet number shows below the packet in the Viewport. 
Show Packet Type	When checked, the packet type shows below the packet in the Viewport. 
Show Packet Subtype	When checked, the packet subtype shows below the packet in the Viewport, if applicable.
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 198 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 198 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 198 for more information. Performs the same function as the throughput indicator **Viewport** radio button.

Table 4.10 - Coexistence View Format Menu Selections (continued)

Selection	Description
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 208
The following three selections are mutually exclusive.	
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.

Table 4.10 - Coexistence View Format Menu Selections (continued)

Selection	Description
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 203.
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 204.
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 205 .
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 205
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 213.

Table 4.11 - Coexistence View Zoom Menu Selections

Selection	Description	Hot Key
Zoom In	When clicked, Viewport time duration decreased.	Ctrl+Plus

Table 4.11 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
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.	
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.	

Table 4.11 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
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 210. 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 210. 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 210. 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 210. 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

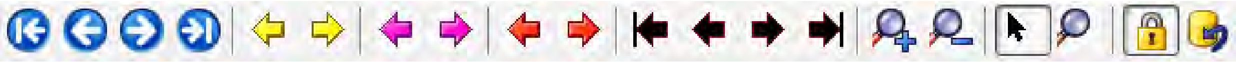


Figure 4.56 - Coexistence View Toolbar

The toolbar contains the following selections:

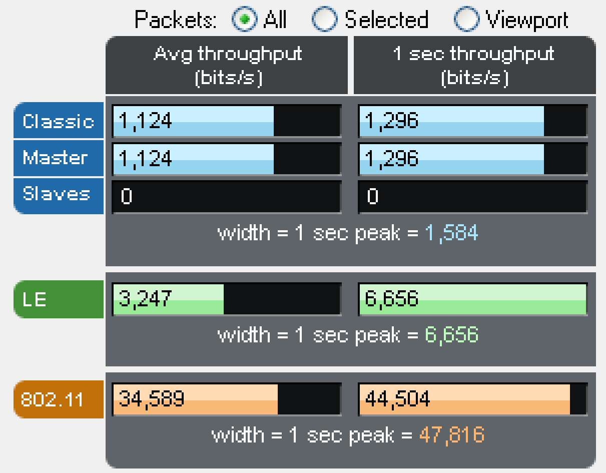
Table 4.13 - Coexistence View Toolbar icons

Icon	Description
⇤	Move to the first packet.
←	Move to the previous packet.
→	Move to the next packet.
⇥	Move to the last packet.
⇦	Move to the previous retransmitted packet.
⇨	Move to the next retransmitted packet
⇦	Move to the previous invalid IFS for *Bluetooth* low energy.
⇨	Move to the next invalid IFS for *Bluetooth* low energy.
⇦	Move to the previous bad packet.
⇨	Move to the next bad packet.
⇤	Move to the first packet of the type selected in the legend.
⬅	Move to the previous packet of the type selected in the legend
➡	Move to the next packet of the type selected in the legend.
⇥	Move to the last packet of the type selected in the legend.
🔍+	Zoom in.
🔍−	Zoom out.
↖	Scroll cursor.

Table 4.13 - Coexistence View Toolbar icons (continued)

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

4.3.4.3 Coexistence View - Throughput Indicators



Packets: ● All ○ Selected ○ Viewport

	Avg throughput (bits/s)	1 sec throughput (bits/s)
Classic	1,124	1,296
Master	1,124	1,296
Slaves	0	0

width = 1 sec peak = 1,584

LE	3,247	6,656

width = 1 sec peak = 6,656

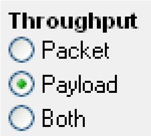
802.11	34,589	44,504

width = 1 sec peak = 47,816

Figure 4.57 - 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
○ Packet
● Payload
○ Both

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.