TELEDYNE LECROY
Everywhereyoulook™

frontline SODERA™ le

BLUETOOTH® LOW ENERGY PROTOCOL ANALYZER

frontline®

Hardware and Software User Manual

Revision Date: 12/14/2016

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/soderale-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 *low energy* Hardware Settings

2.1.1 Sodera LE Front Panel

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

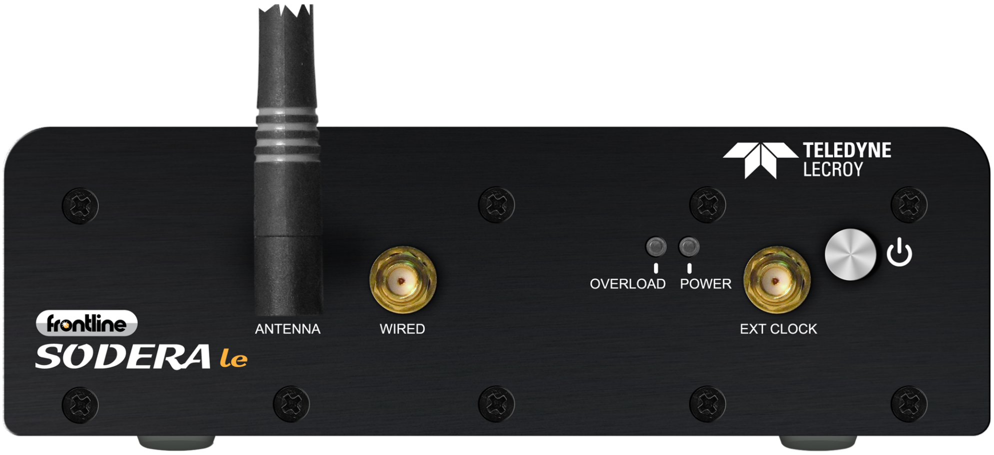


Figure 2.1 - Sodera LE Front Panel Controls and Indicators

Table 2.1 - Sodera LE Front Panel Controls

Control	Description
ANTENNA	Connect to the front panel antenna SMA connector. Used for wideband wireless capture of *Bluetooth* low energy transmissions. Maximum useable signal level: -10 dBm.

Table 2.1 - Sodera LE Front Panel Controls (continued)

Control	Description
WIRED	Low sensitivity RF input suitable for conductive testing that utilizes a wired connection from the devices under test (DUTs). Conductive testing allows for isolation of the DUTs from environmental interference. Maximum useable signal level: 27 dBm.
OVERLOAD	RF overload indicator. If the RF signal level on either the ANTENNA or WIRED connector is too high, then this LED will light red. RF overload occurs when the signal level is greater than 27 dBm. Should an RF overload occur with the ANTENNA in use, try switching to the less sensitive WIRED connecter to relieve the problem.
POWER	LED illuminates when the Sodera LE unit has been powered up using the power button. See Table 2.2 - Sodera LE Front Panel Power and Overload Indicators on page 4 for more information.
EXT CLOCK	Not used.
Power Button	Press and then release the button to power on or power off the system.

Table 2.2 - Sodera LE Front Panel Power and Overload Indicators

Indicator	Color	State	Status Indicated
Power	None	Off	Unit is powered off.
	Green	Constant	Unit is powered on.
	Amber	Constant	Unit is powering on.
	Red	Blinking	Unit has reached thermal overload. See Applying Power on page 5.
		Constant	Unit has reach thermal overload and has shut down. See Applying Power on page 5.
Overload	Red	Occassional	Illuminates each time RF power at the Antenna or Wired connectors has exceeded 27 dBm.

2.1.2 Sodera LE Rear Panel Connectors

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

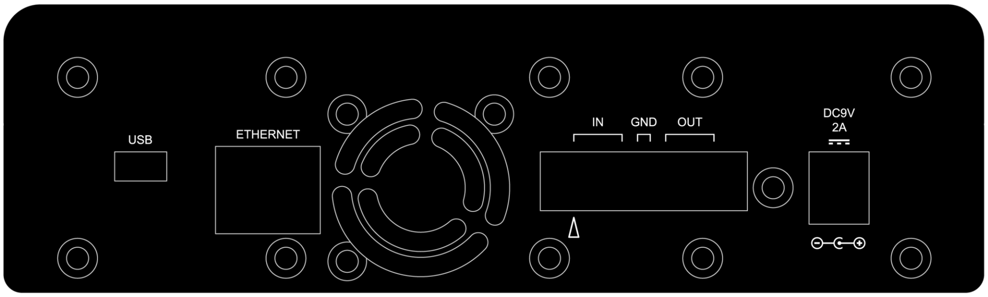


Figure 2.2 - Sodera LE Rear Panel Connectors

DC9V: 1.7 mm jack connector to the Frontline supplied AC-to-9 VDC power adapter.

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

Note: All other connectors are not used.

2.1.3 Attach Antenna

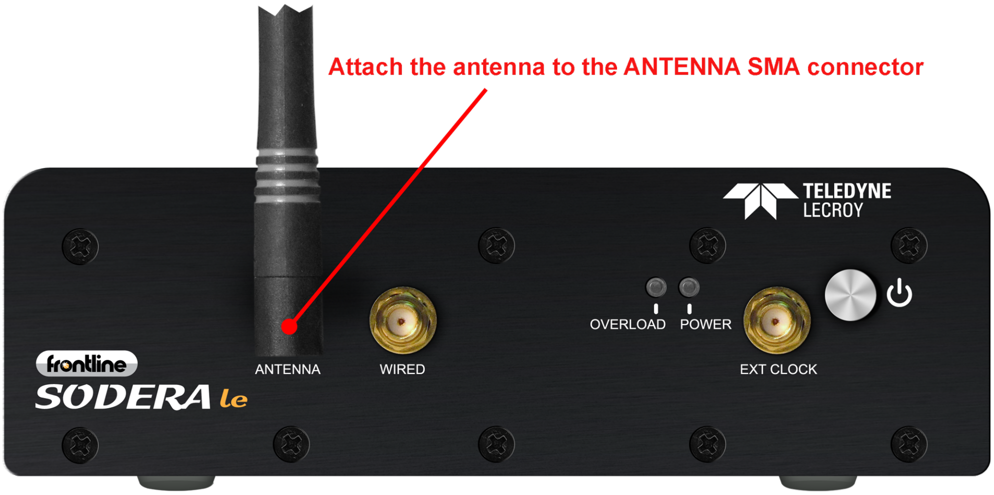

Attach the antenna to the ANTENNA SMA connector

Figure 2.3 - Antenna Attachment Point

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

2.1.4 Applying Power

The Sodera LE hardware is powered by an external 9 VDC power source using an AC-to-DC power adapter.

Note: Only use the Frontline supplied power. Do not substitute with another power adapter.

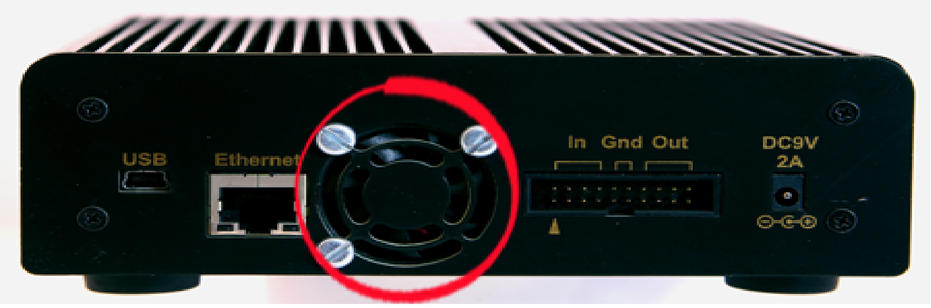
To apply power to the Sodera LE hardware, connect the provided AC-to-DC power adapter to the **DC9V** connector on the rear panel and then connect the adapter into an AC source.

To start the Sodera LE hardware, depress the Power button on the front panel and then release. This action will provide a clean start for the Sodera LE hardware.

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

Should the Sodera LE hardware reach thermal overload temperature between 50 °C and 60 °C (122 °F and 140 °F), it will shut down.

If the fan becomes blocked, the Sodera LE unit will power down. Should this happen check that nothing is blocking the airflow to the unit's air inlet, or that nothing is impeding the fan from spinning freely. Clear any obstructions and then apply power to the unit.



2.2 Data Capture Methods

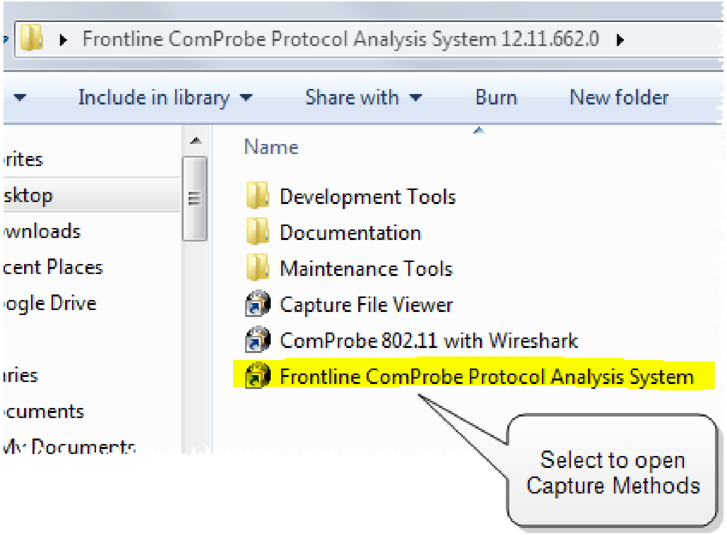
This section describes how to load TELEDYNE LECROY Frontline Protocol Analysis System software, and how to select the data capture method for your specific application.

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.

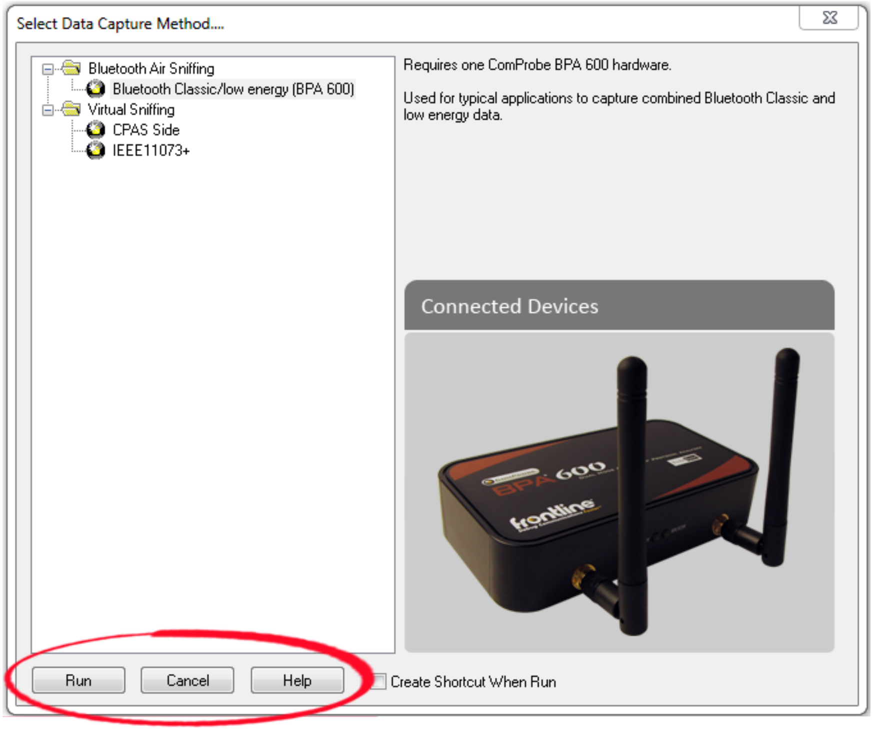


Select to open Capture Methods

Figure 2.4 - 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 2.5 - 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

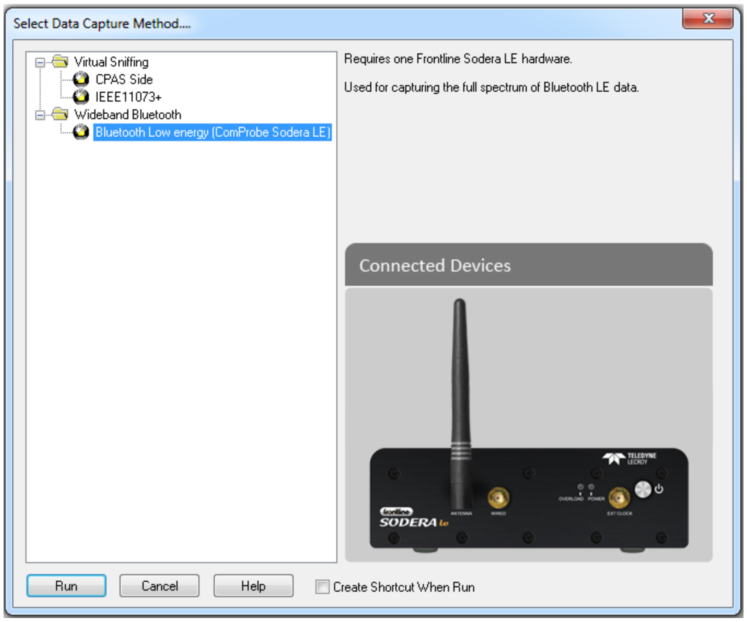
A checkbox labeled **Create Shortcut When Run** is located near the bottom of the dialog. This box is un-checked by default. Select this checkbox, and the system creates a shortcut for the selected method, and places it in the "Frontline ComProbe Protocol Analysis System <version#>" desktop folder and 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 LE Data Capture Method

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



Select Data Capture Method....

- Virtual Sniffing
  - CPAS Side
  - IEEE11073+
- Wideband Bluetooth
  - Bluetooth Low energy (ComProbe Sodera LE)

Requires one Frontline Sodera LE hardware.

Used for capturing the full spectrum of Bluetooth LE data.

Connected Devices

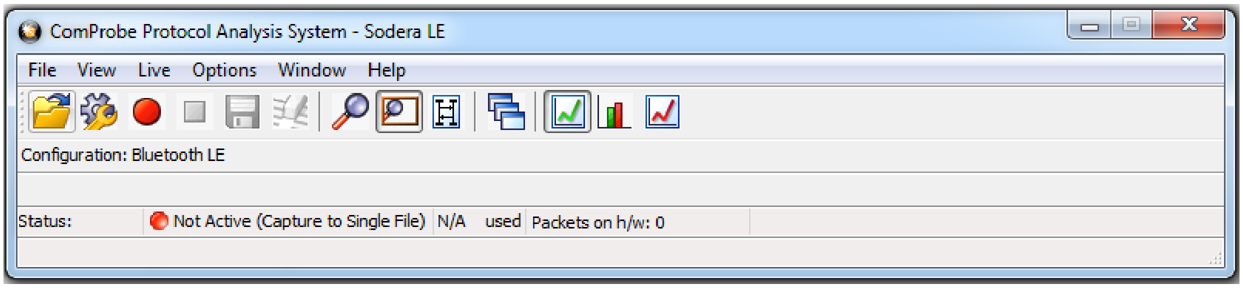
Figure 2.6 - Sodera LE Data Capture Method

Select **Wideband *Bluetooth*, Low energy (Sodera LE)**

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

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.



ComProbe Protocol Analysis System - Sodera LE

Configuration: Bluetooth LE

Status: Not Active (Capture to Single File) N/A used Packets on h/w: 0

Figure 2.7 - 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

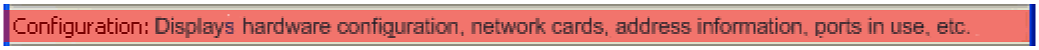
Toolbar icon displays vary according to operating mode and/or data displayed. Available icons appear in color, while unavailable icons are not visible. Grayed-out icons are available for the Frontline hardware and software configuration in use but are not active until certain operating conditions occur.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

Table 2.3 - Control Window Toolbar Icons

Icon	Description
📂	Open File - Opens a capture file.
⚙	I/O Settings - Opens settings
🔴	Start Analyze - data is being decoded from selected wireless devices. Performs the same function as setting the Sodera datasource **Capture Toolbar Analyze/Analyzing** button to **Analyzing**. Changing the **Analyze/Analyzing** button will change the state of this button.
🟦	Stop Analyze- stops decoding data from selected wireless devices. Performs the same function as setting the Sodera datasource **Capture Toolbar Analyze/Analyzing** button to **Analyze**. Changing the **Analyze/Analyzing** button will change the state of this button.
💾	Save - Saves the capture file.
	Clear - Clears or saves the capture file.
🔍	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.
📈	Low energy - Opens the low energy Timeline dialog.
📊	Bluetooth low energy Packet Error Rate Statistics - Opens the Packet Error Rate Statistics 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.

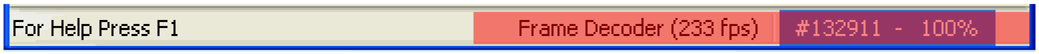
-
    - Not Active means that the analyzer is not currently capturing data.
    - Paused means that data capture has been suspended.
    - Running means that the analyzer is actively capturing data.
- % Used

  The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200 Kb capture file, the bar graph tells you how much of the capture file has been used. When the graph reaches 100%, capture either stops or the file begins to overwrite the oldest data, depending on the choices you made in the System Settings.
- Utilization/Events

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

2.3.4 Frame Information on the Control Window

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



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

2.3.5 Control Window Menus

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

Table 2.4 - 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 73
	Unframe		Removes start-of-frame and end-of-frame markers from your data. SeeUnframing on page 74
	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 2.5 - 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 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.

Table 2.6 - 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 2.7 - Control Window **Live** Menu Selections

Mode	Selection	Hot-Key	Description
The following two rows apply only to Sodera LE			
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 2.7 - 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 2.7 - 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 2.8 - 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 2.9 - 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

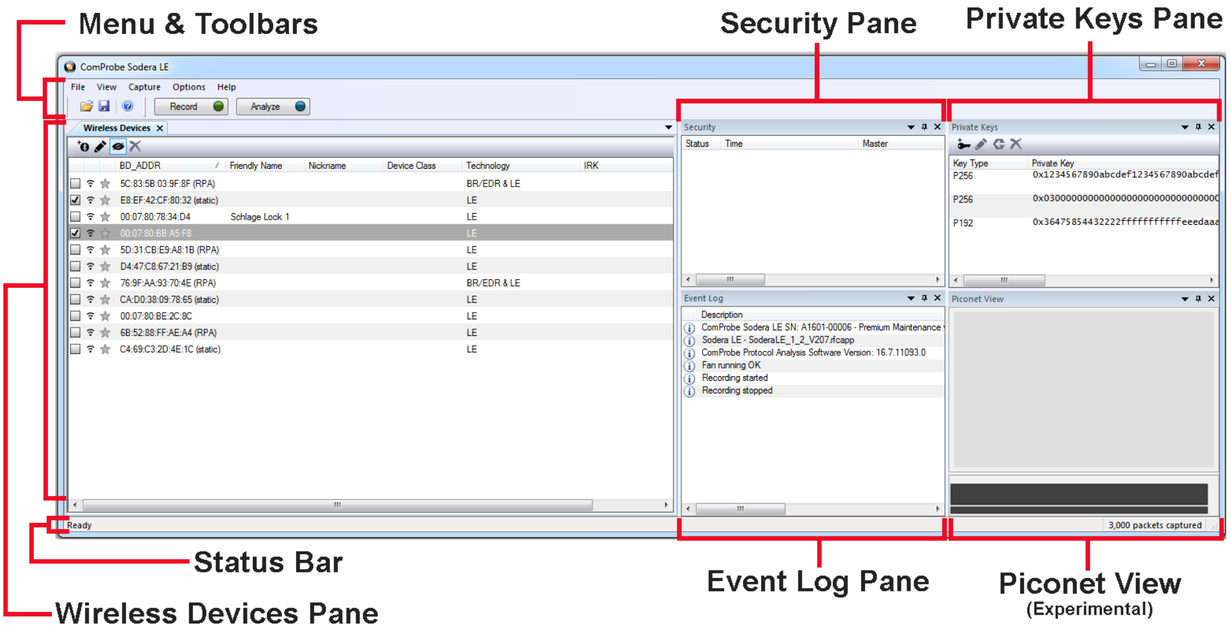
In this section the Frontline software is used to configure an analyzer for capturing data .

3.1 Sodera *low energy*

3.1.1 Sodera LE Datasource Window

When the Frontline software is loaded and started on the host computer the Frontline **Control** window and Sodera LE 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 *Bluetooth* low energy wireless devices, setup decryption , and log session events.



	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	

Status	Time	Master

Key Type	Private Key
P256	0x1234567890abcdef1234567890abcdef
P256	0x0300000000000000000000000000000
P192	0x36475854432222ffffffffffeeedaaa

```
Description
ComProbe Sodera LE SN: A1601-00006 - Premium Maintenance
Sodera LE - SoderaLE_1_2_V207.rfcapp
ComProbe Protocol Analysis Software Version: 16.7.11093.0
Fan running OK
Recording started
Recording stopped
```

Figure 3.1 - Sodera LE Window

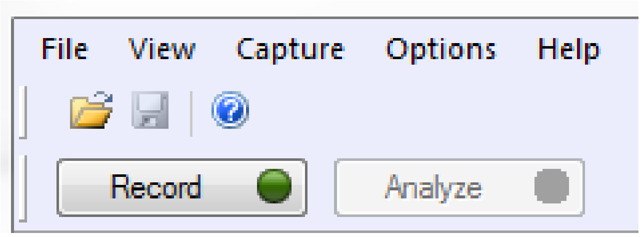
The Menus and Toolbars provide control of the window’s views, starts and stops recording and analysis, sets capture options, and provides file control.

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

The **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.

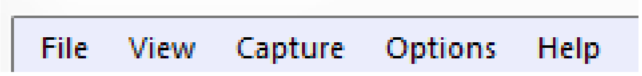
The **Security**, **Private Keys**, **Piconet View**, and **Event Log** Panes can be re-sized by hovering over the pane edge until a double headed arrow appears. Click and hold, dragging it to change the pane size.

3.1.1.1 Menu and Toolbars



At the top of the Sodera LE 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.

3.1.1.1.1 Sodera LE Menu Bar



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

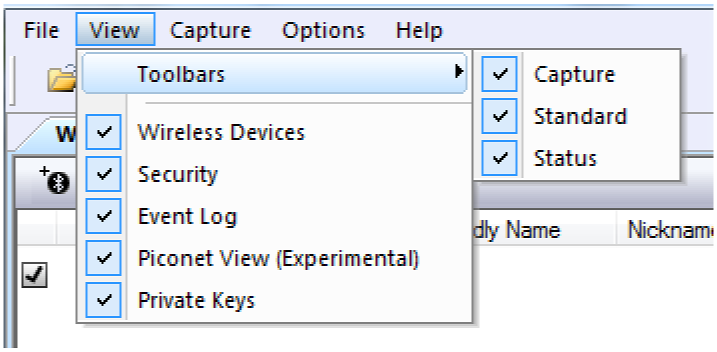
Table 3.1 - Menu Selections

Option	Selection	Description
File	**Open Capture File (Ctrl-O**	Opens a Windows Open dialog. Select the location, File name, and .cfa file to analyze. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.
	Save (Ctrl-S)	Opens a Windows Save dialog. Select a file location and name for a recorded and analyzed file. The file includes all data with all context, decryption, and work file information for both the recorded and analyzed packets.
	Exit	Closes Frontline software

Table 3.1 - Menu Selections(continued)

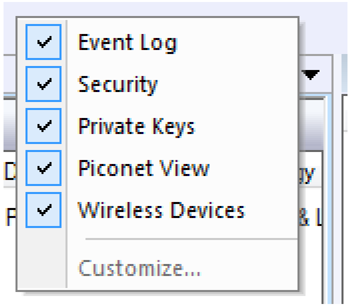
<table>
<tr><th>Option</th><th>Selection</th><th>Description</th></tr>
<tr><td>View</td><td>Toolbars</td><td><table><tr><th>Selection</th><th>Description</th></tr><tr><td>Capture</td><td>When checked the Capture Toolbar is visible. Checked is the default.</td></tr><tr><td>Standard</td><td>When checked the Standard Toolbar is visible. Checked is the default.</td></tr><tr><td>Status</td><td>When checked the Status Bar is visible. Checked is the default.</td></tr></table></td></tr>
<tr><td></td><td>Wireless Devices</td><td>When checked the **Wireless Devices** tab is visible in the Devices pane. Selecting the tab will display the Wireless Devices.</td></tr>
<tr><td></td><td>Security</td><td>When checked the **Security** pane is visible. Checked is the default.</td></tr>
<tr><td></td><td>Event Log</td><td>When checked the **Event Log** pane is visible. Checked is the default.</td></tr>
<tr><td></td><td>Piconet View (Experimental)</td><td>When checked, the **Piconet View** is visible. Not-checked is the default.
At this time the **Piconet View** is experimental and in development.</td></tr>
<tr><td></td><td>Private Keys</td><td>When checked, the **Private Keys** pane is visible. The Private Keys pane displays user entered Private/ Public key pairs for *Bluetooth* low energy legacy and secure connection pairing. By default, this pane is not displayed. When it is displayed it will be docked as a tab in the same area as the Security pane.
When Debug key is not used during pairing, the datasource will look for a matching Public key in the set of Private/Public key pairs. If a match is found, the datasource will use the corresponding Private Key to compute the Diffe-Hellman Key.</td></tr>
<tr><td>Capture</td><td>Record/Recording</td><td>Starts and stops the capture of data. Performs the same function as the Capture Toolbar **Record/Recording** button.</td></tr>
<tr><td></td><td>Analyze/Analyzing</td><td>Starts and stops the analysis of recorded data. Performs the same function as the Capture Toolbar **Analyze/Analyzing** button.</td></tr>
<tr><td>Options</td><td>Capture Options...</td><td>Opens the Capture Options dialog where the attached Sodera LE hardware can be configured for *Bluetooth* low energy tcapture mode. For additional information see Sodera LE Capture Options Dialog on page 22.</td></tr>
<tr><td></td><td>LE Test Mode Filters...</td><td>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 21.</td></tr>
<tr><td></td><td>Analyze LE Empty Packets</td><td>When checked will include *Bluetooth* low energy empty packets. Empty packets are normally ignored, so not-checked is the default.</td></tr>
<tr><td>Help</td><td>Help Topics</td><td>Opens Frontline help.</td></tr>
<tr><td></td><td>About Sodera...</td><td>Opens a pop-up window with version and configuration information.</td></tr>
</table>

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

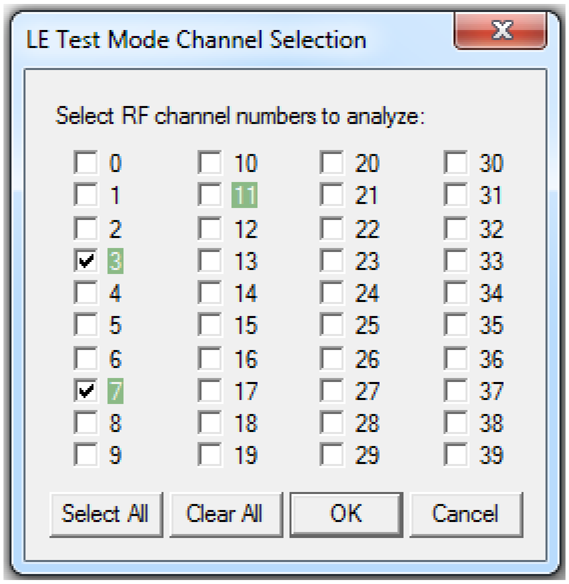


Right-clicking in the toolbar any of the following window/panes will display a pop-up View menu that performs the same as the main View menu:

- Sodera LE 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 LE 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.

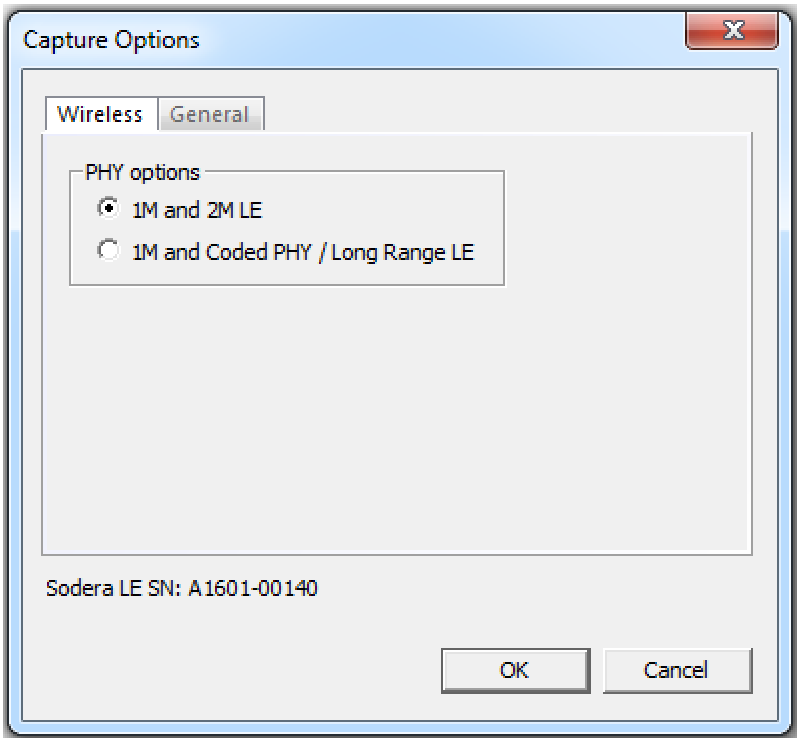
3.1.1.1.1.1 Sodera LE Capture Options Dialog

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

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

Clicking on **OK** will save the **Capture Options** settings on the connected Sodera LE unit. Any **Capture Options** parameter changes made will overwrite the previously saved **Capture Options**.

Wireless tab



● 1M and 2M LE
○ 1M and Coded PHY / Long Range LE

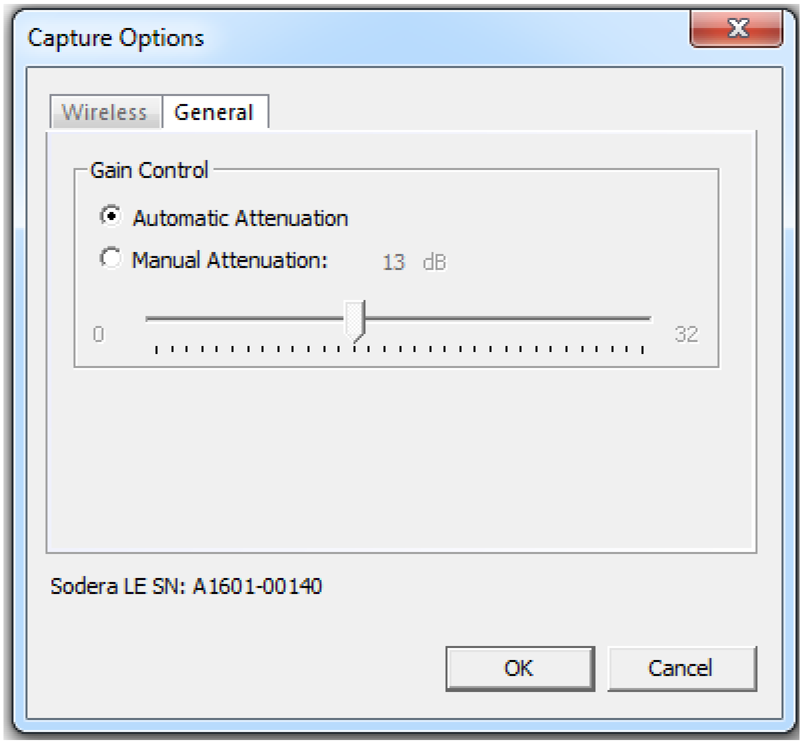
Sodera LE SN: A1601-00140

Figure 3.2 - Sodera LE Capture Options - Wireless tab.

Table 3.3 - Sodera LE Capture Options - Wireless Tab Selections

Section	Selection	Description
PHY Options	**1M and 2M LE**	Capture and record at 1 Mbps or 2 Mbps.
	1M and Coded PHY/Long Range LE	Allows for capture of Long Range *Bluetooth* low energy, also called Coded PHY. Long Range LE can only be captured at 1 Mbps.

General Tab



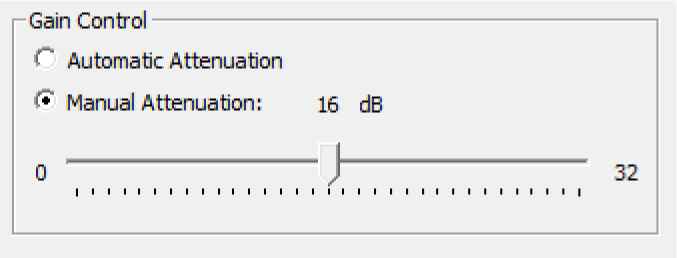
● Automatic Attenuation

○ Manual Attenuation: 13 dB

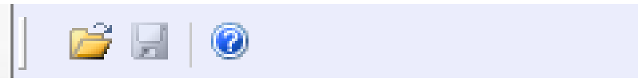
Sodera LE SN: A1601-00140

Figure 3.3 - Sodera LE Capture Options - General Tab

Table 3.4 - Sodera LE Capture Options - General Tab Selections

Section	Selection	Description
Gain Control	**Automatic Attenuation**	The Sodera LE unit will automatically adjust the gain of the received RF signal to estimated levels suitable for effective data capture..
	Manual Attenuation	Manual Selection of gain may be necessary if the capture does not provide reliable results. Gain can be adjusted from 0 to 32 dB in 1 dB steps. For example, in the presence of a strong Wi-Fi signal the user may have to increase the attenuation to achieve a reliable *Bluetooth* low energy data capture. The user should adjust the attenuation and then capture the data again. Repeat, if necessary, until a reliable data capture is acheived..  Gain Control ○ Automatic Attenuation ● Manual Attenuation: 16 dB 0 32

3.1.1.1.2 Sodera LE Standard Toolbar



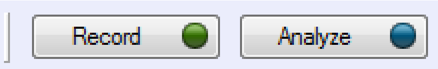
The Standard Toolbar provides quick one-click access to the same options that appear in menu **File** selection. This toolbar may be hidden by selecting from the menu View Toolbars selection and removing the check from Standard Toolbar selection.

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 3.5 - Sodera LE 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 LE Window topic.

3.1.1.1.3 Sodera LE Capture Toolbar



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

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 3.6 - Sodera LE Capture Toolbar Selections

Icon	Description
Record ● / Recording ●	In live mode or with a capture file, clicking on **Record** begins recording all data captured from active Bluetooth links that are within range. The button will change to **Recording** during the capture. Clicking on **Recording** will stop the capture and the button will change to **Record**. This button performs the same function as the **Capture** menu **Record/Recording** selections.
Analyze ● / Analyzing ●	Once data capture has begun in live mode or with a capture file and active devices are selected for analysis, clicking on the **Analyze** button begins protocol analysis in the ComProbe software. The button will change to **Analyzing** during the analysis process. Clicking on **Analyzing** will stop the analysis process and the button will change to **Analyze**. This button performs the same function as the **Capture** menu **Analyzing** selections. This button is linked to the **Control** window **Start Analysis** and **Stop Analysis** controls, these buttons and controls can be used interchangeably to start and stop protocol analysis.

3.1.1.2 Sodera LE Wireless Devices Pane

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

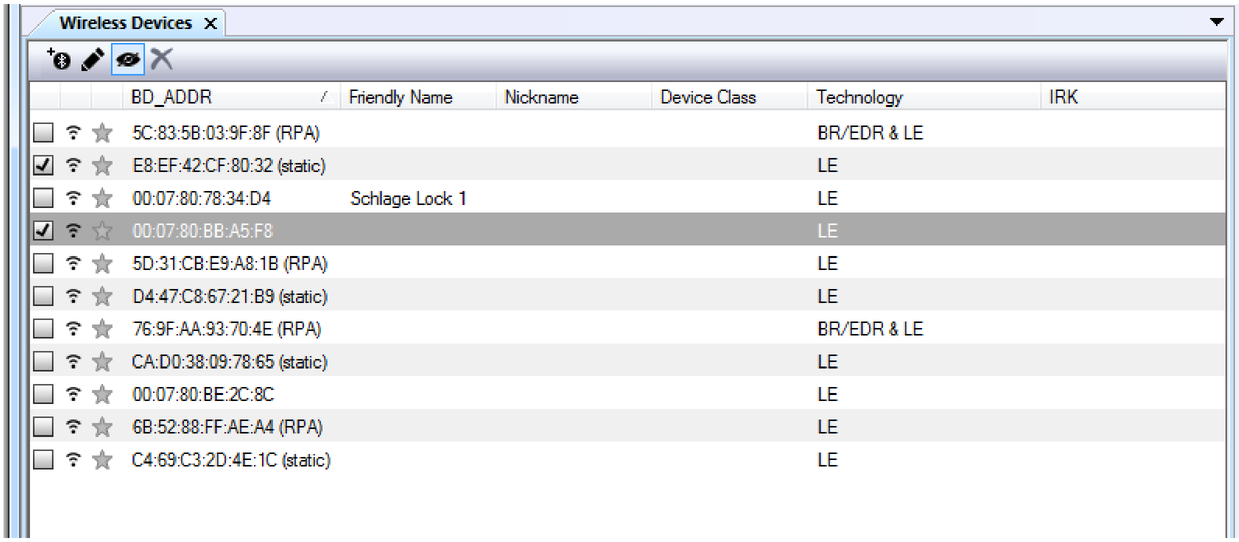
The **Wireless Devices** pane is a list populated by wireless devices that are:

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

For Bluetooth low energy, the full BD_ADDR is always displayed.

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

Table 3.7 - 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 LE 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 low energy wireless device. Bluetooth low energy Device Classes on page 27 list the classes by *Bluetooth* technology.
Technology	Device technology to include one of the following: • Smart(LE) • Smart Ready (LE & BR/EDR)
IRK	*Bluetooth* low energy 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 3.8 - *Bluetooth* low energy Device Classes

Class
Barcode Scanner
Barcode Scanner
Blood Pressure
Blood Pressure: Arm
Blood Pressure: Wrist
Card Reader
Clock
Computer
Cycling
Cycling: Cadence Sensor
Cycling: Cycling Computer
Cycling: Power Sensor
Cycling: Speed Cadence Sensor
Cycling: Speed Sensor
Digital Pen
Digitizer Tablet
Display
Eye-Glasses
Gamepad
Glucose Meter
Heart Rate Sensor
Heart Rate Sensor: Heart Rate Belt
Human Interface Device (HID)
Joystick
Keyboard
Keyring
Media Player
Mouse
Outdoor Sports Activity

Table 3.8 - Bluetooth low energy Device Classes (continued)

Class
Outdoor Sports: Location and Navigation Display
Outdoor Sports: Location and Navigation Pod
Outdoor Sports: Location Display
Outdoor Sports: Location Pod
Phone
Pulse Oximeter
Pulse Oximeter: Fingertip
Pulse Oximeter: Wrist
Remote Control
Running Walking Sensor
Running Walking Sensor : On Shoe
Running Walking Sensor: In Shoe
Running Walking Sensor: On Hip
Sports Watch
Tag
Generic Thermometer
Thermometer: Ear
Unknown
Watch
Weight Scale

Sorting Wireless Devices columns

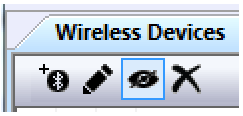
Any column in the **Wireless Devices** pane can be used to sort the entire table. Each column is sortable in ascending or descending order, but only one column at-a-time can be used to sort.

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.

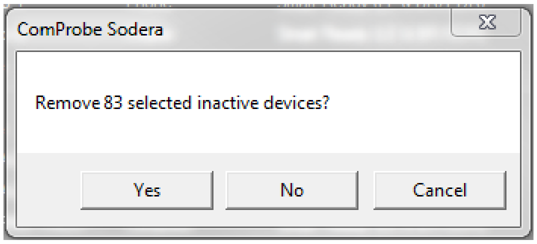
Favorite devices will always grouped together at the top of the Wireless Devices pane in sorted order. Non-favorite devices will appear immediately below the favorite devices in sorted order.

Device Management Tools

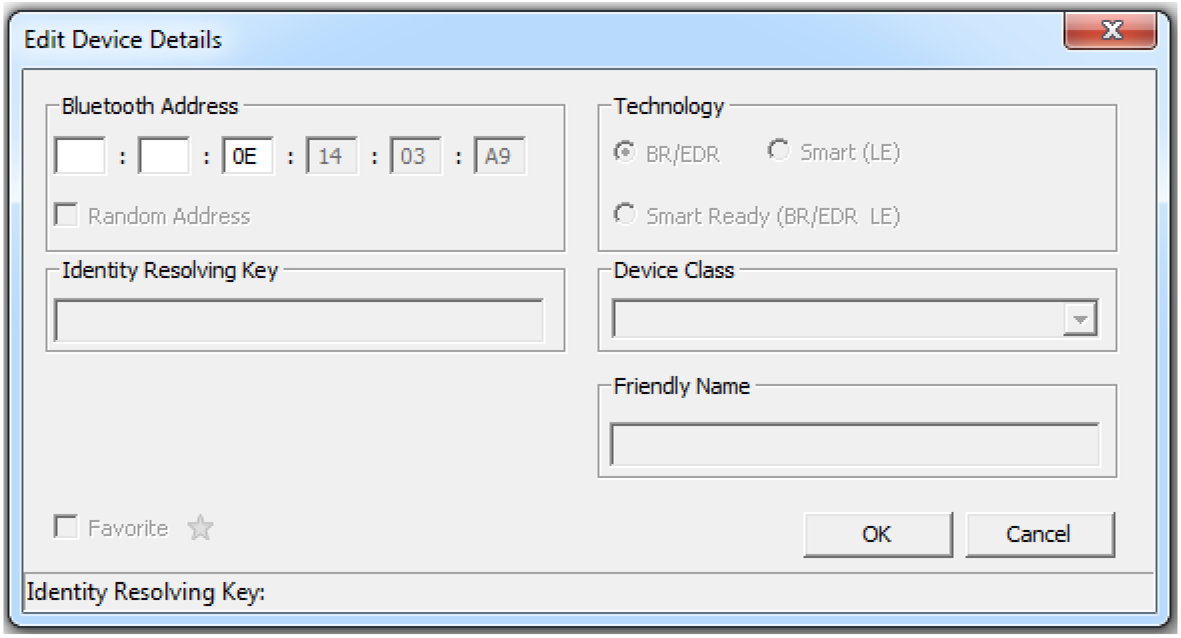


At the top of the Wireless Devices pane are three tools for managing the devices in the pane. You can add and edit devices, and delete inactive devices. During Analyzing this toolbar is not available for use.

Table 3.9 - Wireless Devices Management Tools

Tool	Icon	Description
Add New Device,	+ᛒ	Clicking this tool will open the **Edit Device Details** dialog. Enter the new device's *Bluetooth* address and other related data and press **OK**.
Edit Selected Device	✎	Allows the user to edit 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.  ComProbe Sodera 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



Bluetooth Address
: : 0E : 14 : 03 : A9
□ Random Address

Technology
● BR/EDR ○ Smart (LE)
○ Smart Ready (BR/EDR LE)

Identity Resolving Key

Device Class

Friendly Name

□ Favorite ☆

Identity Resolving Key:

Figure 3.5 - 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. Fields with invalid entries will display a red background and the **OK** button is disabled.

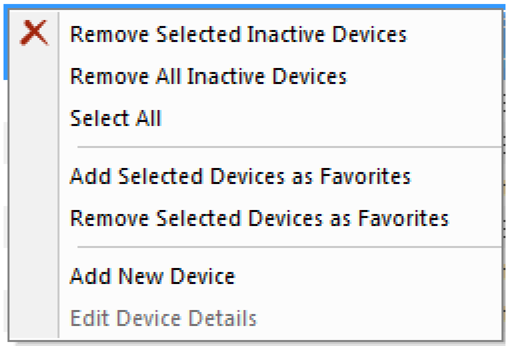
> **Note:** Editing of device details is not allowed during Analyzing.

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 only enabled for devices with a random resolving address. These devices are either Smart (LE) or Smart Ready (LE & BR/EDR) technology. The **Bluetooth Address Random Address** will be enabled and checked.
- This field is disabled for a valid IRK.
- Entered IRK values are validated against the BD_ADDR.
- 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.

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 3.10 - 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.

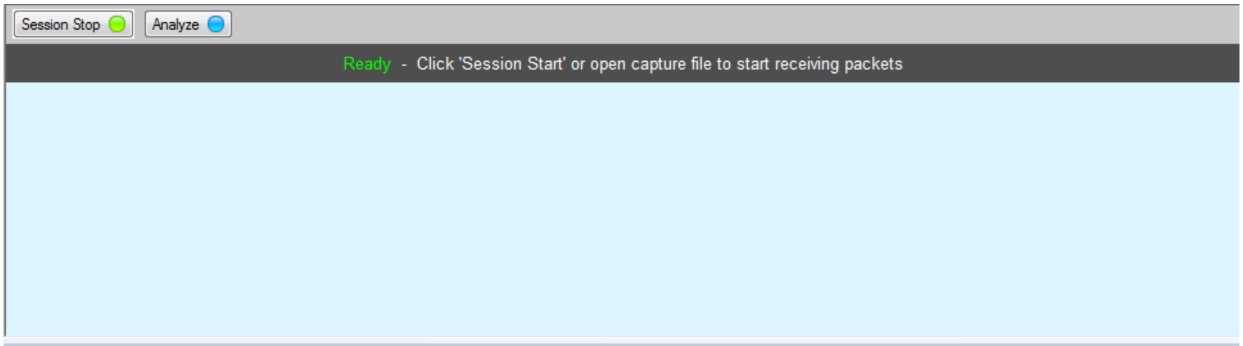
Table 3.10 - Right-Click Pop-Up Menu Selections (continued)

Selection	Description
Edit Device Details	Active when a single device has been selected. Allows the user to edit 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.

3.1.1.3 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.



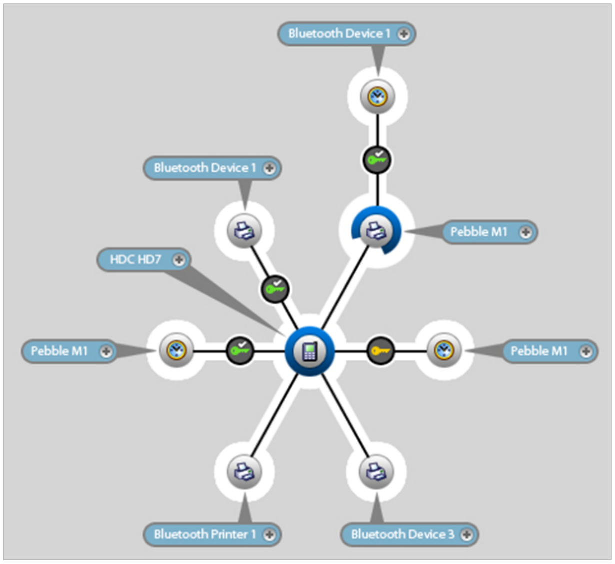
Ready - Click 'Session Start' or open capture file to start receiving packets

Figure 3.6 - **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

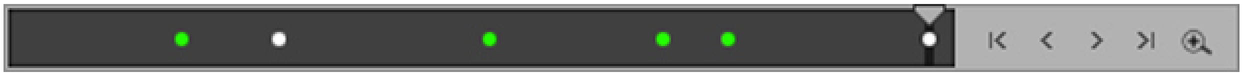


Figure 3.7 - **Piconet View** Timeline

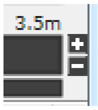
As device connections appear over time, the Timeline on the bottom of the **Piconet View** displays circles representing events over time where the piconet view has changed. Classic *Bluetooth* events appear as blue circles and *Bluetooth* low energy events appear as green circles. These events appear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

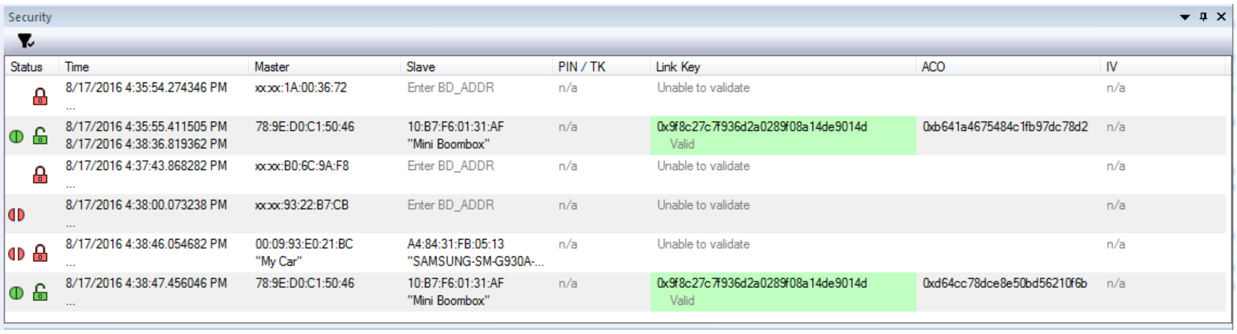
3.1.1.4 Sodera LE Datasource Security Pane

The Security pane is where the Frontline software identifies devices with captured traffic (ᯤ) 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 for a description of the critical packets. The Security pane will identify the type of key required for decryption.



Security

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 3.8 - Sodera LE Datasource Security Pane

The **Security** pane shows events in the current capture. When the (missing or bad snippet) 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.

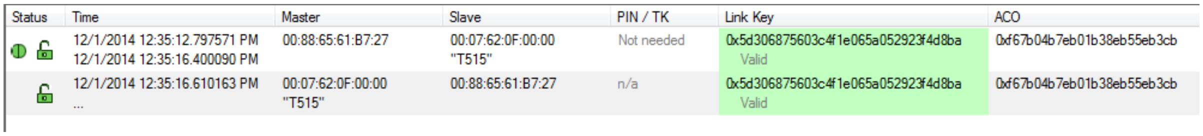
- **Status**: displays icons showing the pairing and encryption/decryption status.

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 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

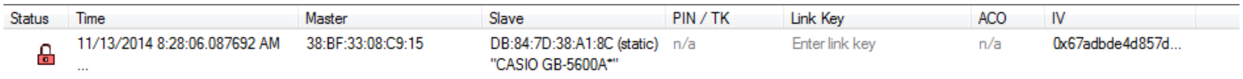
Figure 3.9 - Role Switch Example

- **PIN/TK**:
  - Bluetooth low energy
    - PIN: 6 digit numeric passkey (000000 - 999999)
    - Out-of-Band Temporary Key (OOB TK): 32 digit hexadecimal number
- **Link Key**
  - 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 LE 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**.
- **IV**: Initialization Vector is displayed for both *Bluetooth* low energy encryption . The slave will use the IV in starting the encrypted communications.

3.1.1.4.1 *Bluetooth* low energy Encryption/Decryption

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.

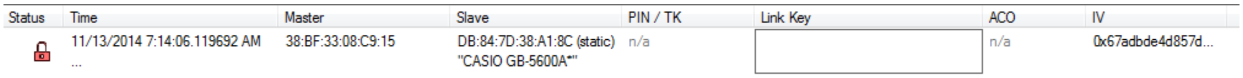


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔓	11/13/2014 8:28:06.087692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	Enter link key	n/a	0x67adbde4d857d...

Figure 3.10 - *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.

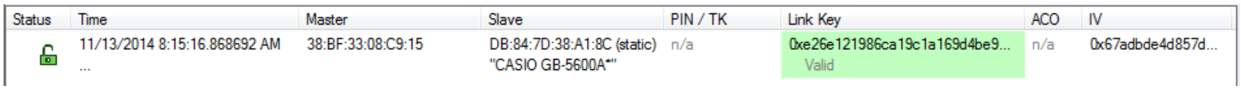


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔒	11/13/2014 7:14:06.119692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a		n/a	0x67adbde4d857d...

Figure 3.11 - *Bluetooth* low energy Enter Link Key

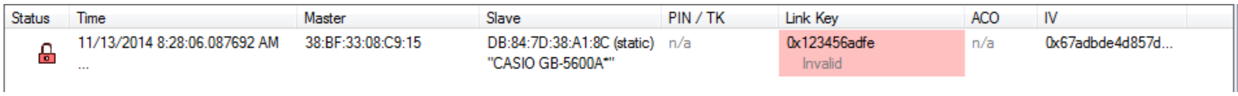
Press the Enter key or click outside the Link Key box. If the Link Key is valid the box will be green, beneath the Link Key will appear "Valid, and the Status will show an open, green lock indicating that decryption is enabled.

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 3.12 - *Bluetooth* low energy Valid Link Key

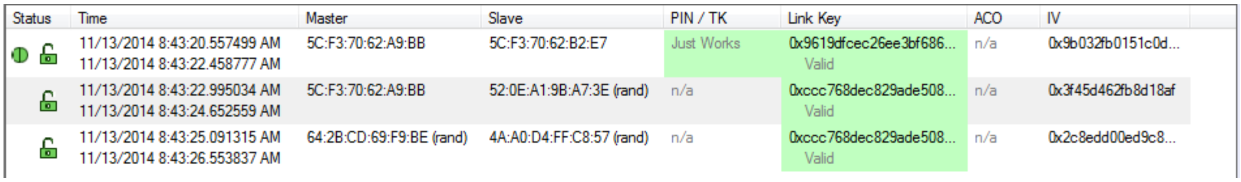


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
🔒	11/13/2014 8:28:06.087692 AM ...	38:BF:33:08:C9:15	DB:84:7D:38:A1:8C (static) "CASIO GB-5600A*"	n/a	0x123456adfe Invalid	n/a	0x67adbde4d857d...

Figure 3.13 - *Bluetooth* low energy Invalid Link Key

Legacy Just Works Pairing

In this example the devices under test use Legacy 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.

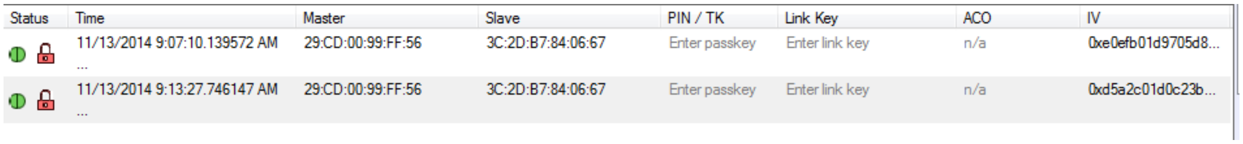


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
◐ 🔓	11/13/2014 8:43:20.557499 AM 11/13/2014 8:43:22.458777 AM	5C:F3:70:62:A9:BB	5C:F3:70:62:B2:E7	Just Works	0x9619dfcec26ee3bf686... Valid	n/a	0x9b032fb0151c0d...
🔓	11/13/2014 8:43:22.995034 AM 11/13/2014 8:43:24.652559 AM	5C:F3:70:62:A9:BB	52:0E:A1:9B:A7:3E (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 3.14 - *Bluetooth* low energy Piconet Public Key and Private Key Encryption

Legacy Passkey Pairing

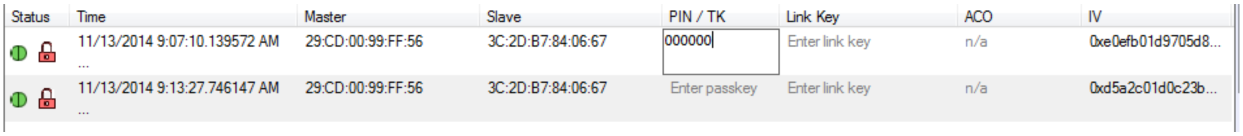
PIN is a six-digit decimal number. If a passkey is required by the device "Enter passkey" will appear in the device's **PIN/TK** field.



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 3.15 - *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.

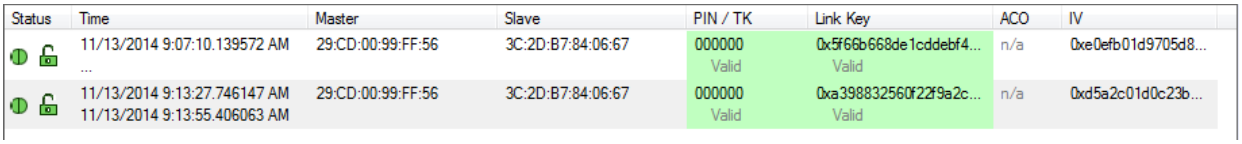


Status	Time	Master	Slave	PIN / TK	Link Key	ACO	IV
● 🔒	11/13/2014 9:07:10.139572 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	000000	Enter link key	n/a	0xe0efb01d9705d8...
● 🔒	11/13/2014 9:13:27.746147 AM ...	29:CD:00:99:FF:56	3C:2D:B7:84:06:67	Enter passkey	Enter link key	n/a	0xd5a2c01d0c23b...

Figure 3.16 - *Bluetooth* low energy Passkey Entry

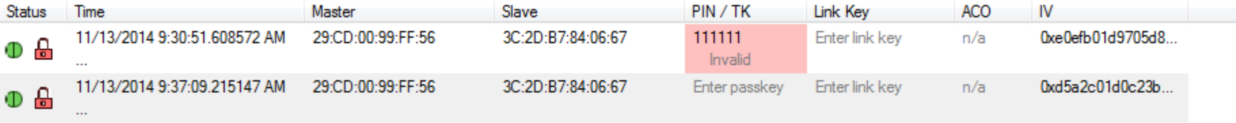
Press Enter or click outside the field. If the Passkey is correct it will appear in the **PIN/TK** field with "Valid" appearing below the passkey, **Link Key** field will automatically fill with the Link Key that will show "Valid" and appear green. The **Status** field will show an open, green lock to 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 3.17 - *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 3.18 - *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".

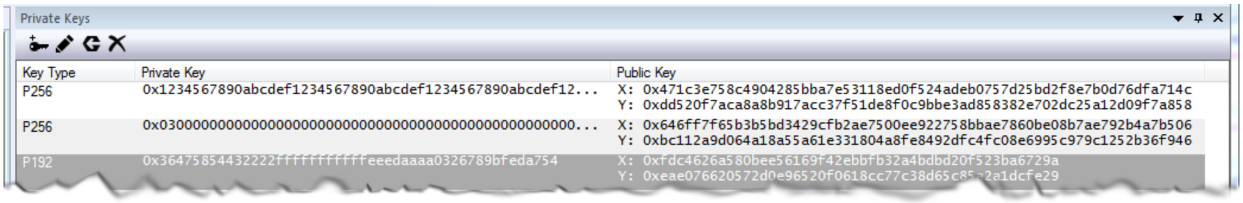
3.1.1.5 Sodera LE Private Keys Pane

For Sodera LE hardware 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

Sodera LE window is closed . When the window is opened while in live mode, saved Private Keys are loaded from persistent storage.



Private Keys

Key Type	Private Key	Public Key
P256	0x1234567890abcdef1234567890abcdef1234567890abcdef12...	X: 0x471c3e758c4904285bba7e53118ed0f524adeb0757d25bd2f8e7b0d76dfa714c Y: 0xdd520f7aca8a8b917acc37f51de8f0c9bbe3ad858382e702dc25a12d09f7a858
P256	0x030000000000000000000000000000000000000000000000...	X: 0x646ff7f65b3b5bd3429cfb2ae7500ee922758bbae7860be08b7ae792b4a7b506 Y: 0xbc112a9d064a18a55a61e331804a8fe8492dfc4fc08e6995c979c1252b36f946
P192	0x36475854432222ffffffffffffeeedaaaa0326789bfeda754	X: 0xfdc4626a580bee56169f42ebbfb32a4bdbd20f523ba6729a Y: 0xeae076620572d0e96520f0618cc77c38d65c85a2a1dcfe29

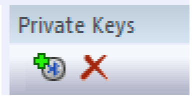
Figure 3.19 - Private Keys Pane

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

Table 3.11 - 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

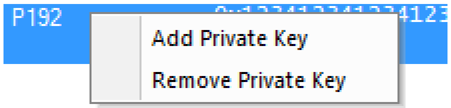
Private Key management tools



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

Table 3.12 - Private Keys Management Tools

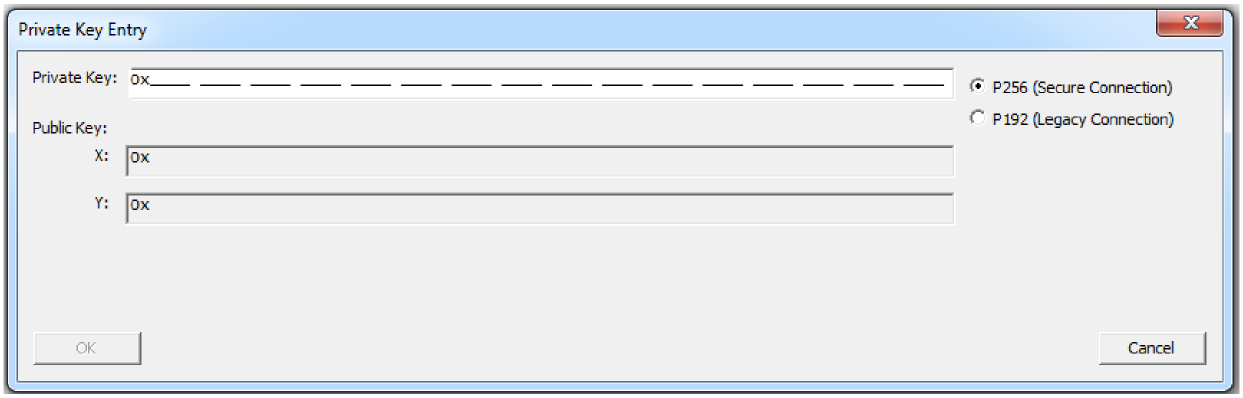
Tool	Icon	Descriptioin
Add Private Key	+🔑	Used to add a Private Key to the pane. When clicked, it opens the **Private Keys Entry** dialog. See Private Key Entry dialog on page 39
Edit Selected Private Key	✎	Enabled when a private key in the pane is selected. When clicked, it opens the **Private Keys Entry** dialog with the selected Private and Public Key filled in. See Private Key Entry dialog on page 39
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 3.20 - Private Key Entry Dialog

Table 3.13 - Private Key Entry Dialog Fields

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

To Add a Private Key:

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

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

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

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

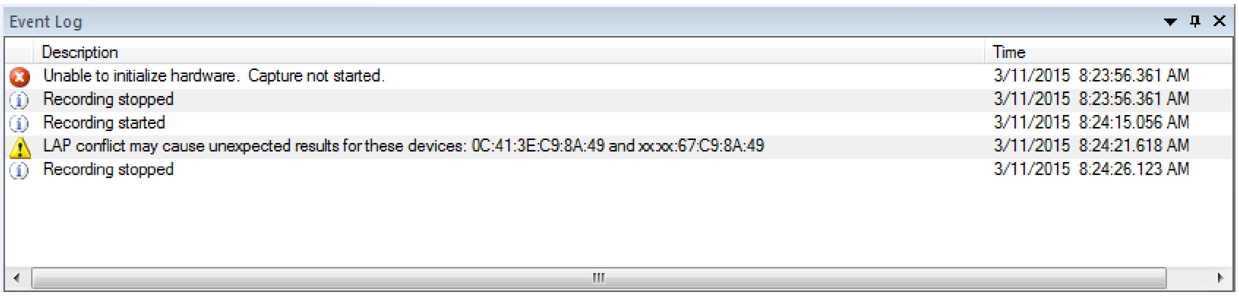
To Remove a Private Key:

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

3.1.1.6 Sodera LE Event Log Pane

The Event Log is a record of significant events that occurred at any time the Sodera LE datasource 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 3.21 - Sodera LE 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.

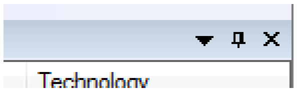
Table 3.14 - Event Log Columns

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

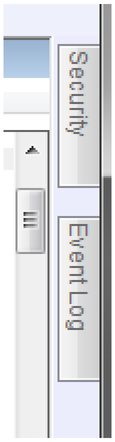
The Event log is automatically saved to "%appdata%\Frontline Test Equipment\Sodera\Logs\" as a .txt file. Logs are retained for each session.

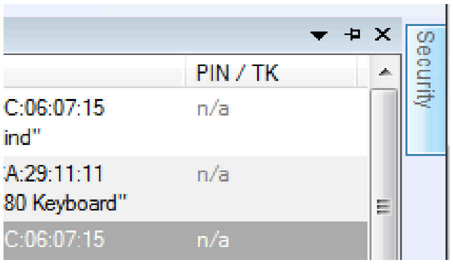
3.1.1.7 Pane Positioning and Control



Sodera LE window **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.

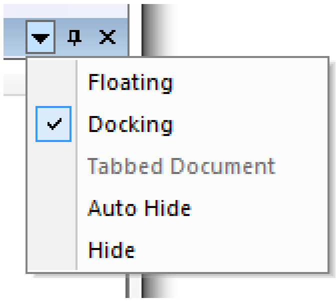




Hovering over the hidden pane title will expand the pane and the **Auto Hide** icon appears rotated 📌.

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

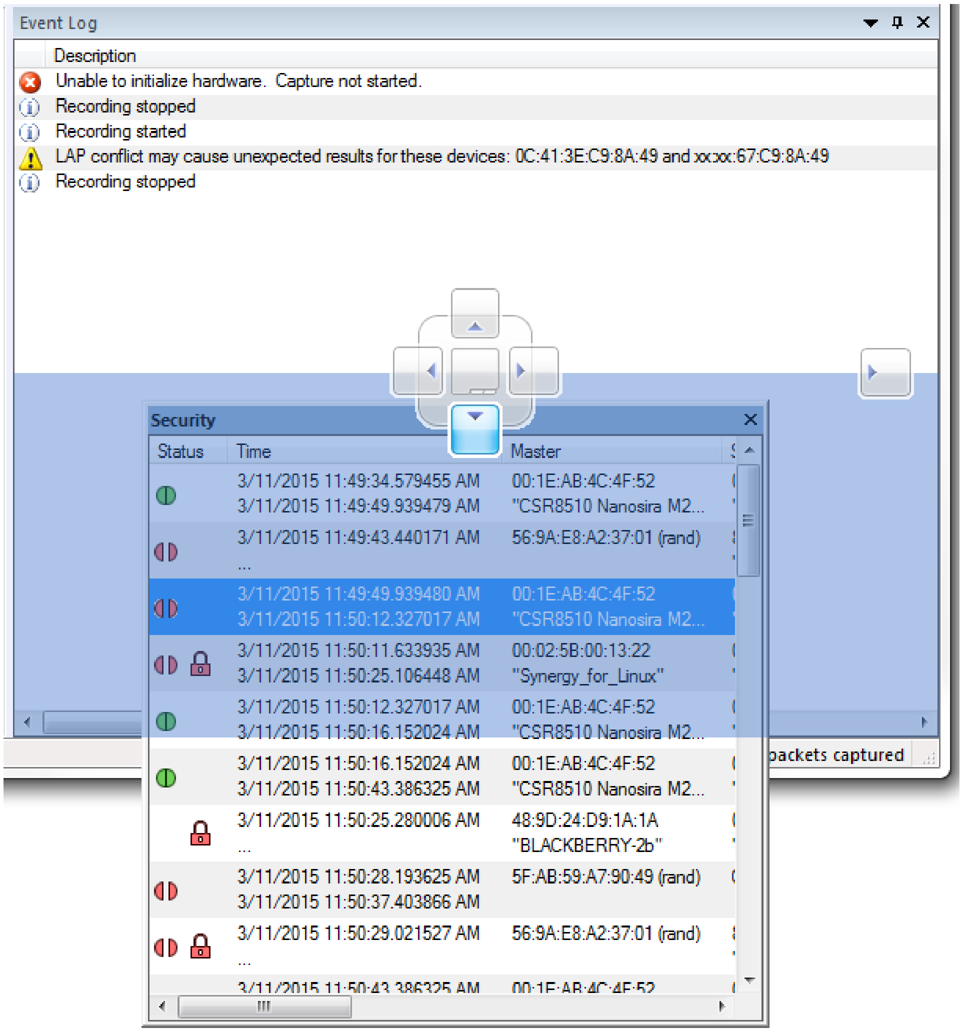
Positioning by Cursor

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

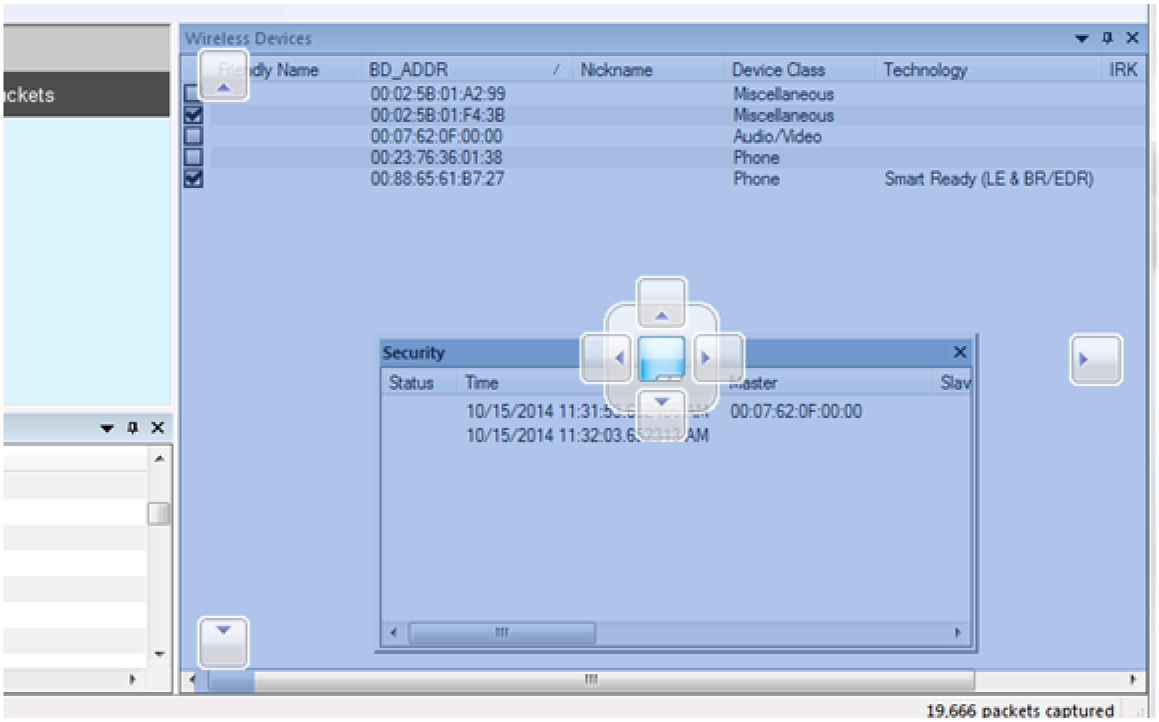
Status	Time	Master
🟢	3/11/2015 11:49:34.579455 AM 3/11/2015 11:49:49.939479 AM	00:1E:AB:4C:4F:52 "CSR8510 Nanosira M2...
🔴	3/11/2015 11:49:43.440171 AM ...	56:9A:E8:A2:37:01 (rand)
🔴	3/11/2015 11:49:49.939480 AM 3/11/2015 11:50:12.327017 AM	00:1E:AB:4C:4F:52 "CSR8510 Nanosira M2...
🔴 🔒	3/11/2015 11:50:11.633935 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 3.22 - 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

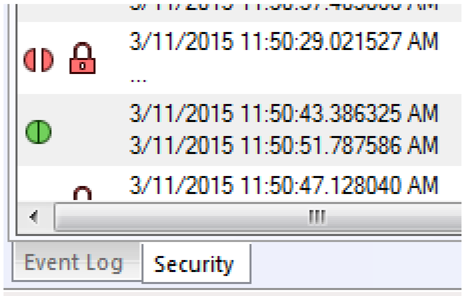
	Friendly Name	BD_ADDR	Nickname	Device Class	Technology	IRK
□		00:02:5B:01:A2:99		Miscellaneous		
☑		00:02:5B:01:F4:3B		Miscellaneous		
□		00:07:62:0F:00:00		Audio/Video		
□		00:23:76:36:01:38		Phone		
☑		00:88:65:61:B7:27		Phone	Smart Ready (LE & BR/EDR)	

Security

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

19,666 packets captured

Figure 3.23 - 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.

3.2 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.

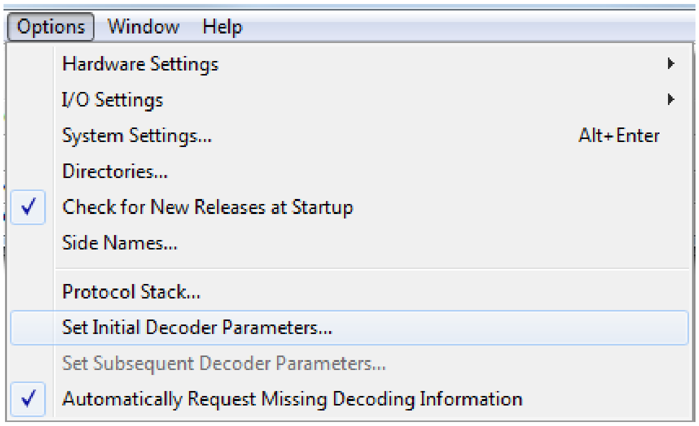

Options
Window
Help
Hardware Settings
I/O Settings
System Settings...
Alt+Enter
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

Figure 3.24 - Select **Set Initial Decoder Parameters...** from **Control** window

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

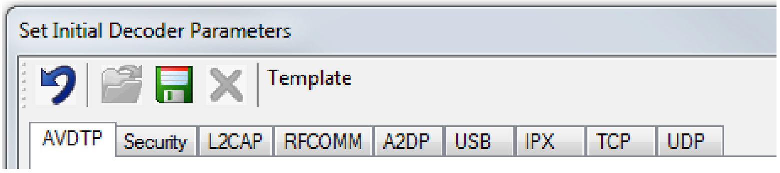


Figure 3.25 - Tabs for each decoder requiring parameters.

- 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.

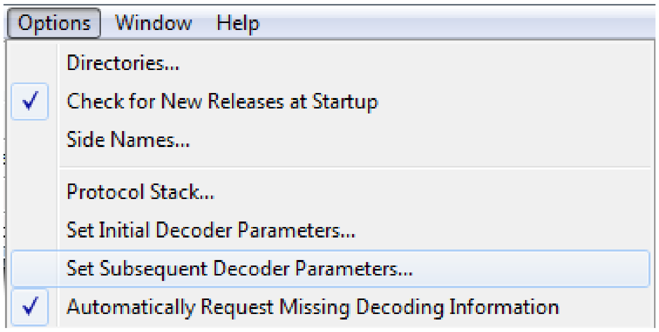
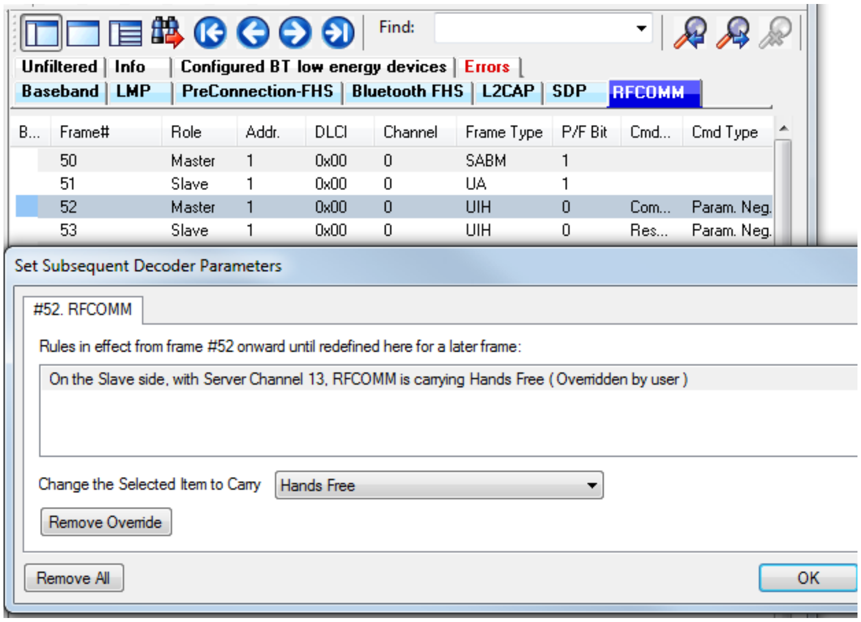

Options
Window
Help
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

Figure 3.26 - **Set Subsequent Decoder Parameters...** from **Control** window



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

Remove Override

Remove All

OK

Figure 3.27 - 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.

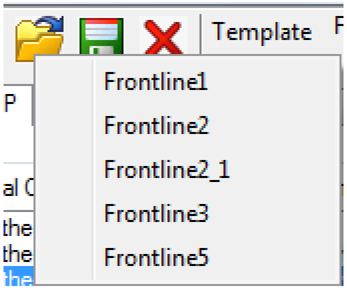
3.2.1 Decoder Parameter Templates

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

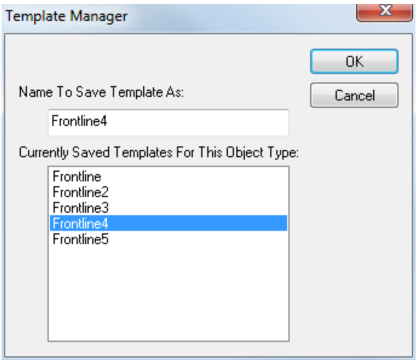
A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

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

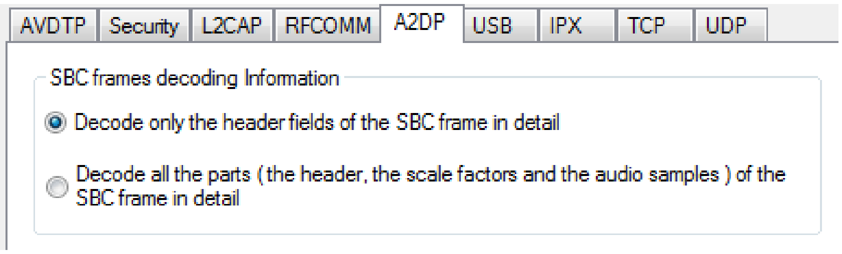
Decoding SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame. You can increase the decoding speed by decoding only the header fields and disregarding other parts. You can select the detail-level of decoding 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 3.28 - A2DP Decoder Settings

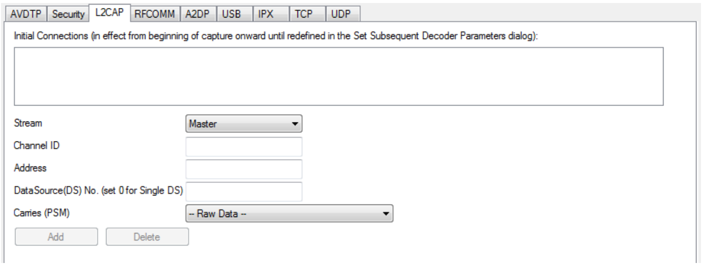
4. Follow steps to save the template changes or to save a new template.

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

3.2.3 L2CAP Decoder Parameters

3.2.3.1 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.



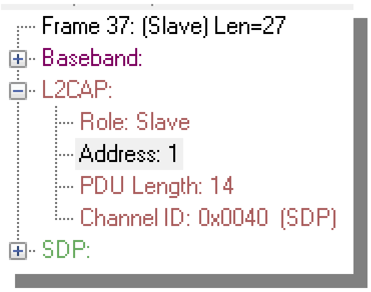
Initial Connections (in effect from beginning of capture onward until redefined in the Set Subsequent Decoder Parameters dialog):

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

Figure 3.29 - 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.



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

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

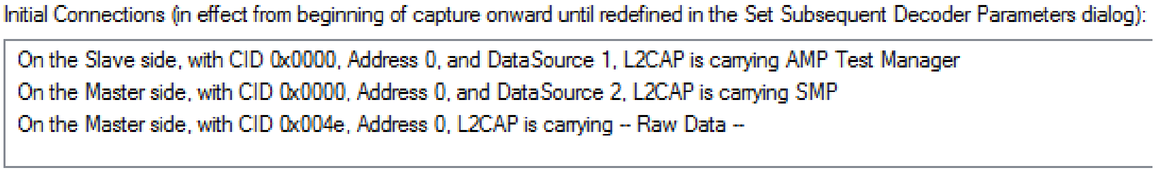
Carries (PSM) - Select the protocol that L2CAP traverses to from the following:

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

- IEEE P11073 20601
- -Raw Data-

Adding, Deleting, and Saving L2CAP Parameters

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



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

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

Figure 3.30 - Parameters Added to Decoder

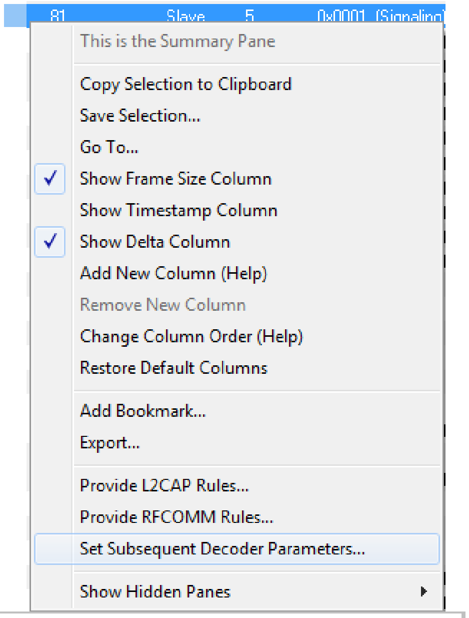
4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and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

3.2.3.2 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**.



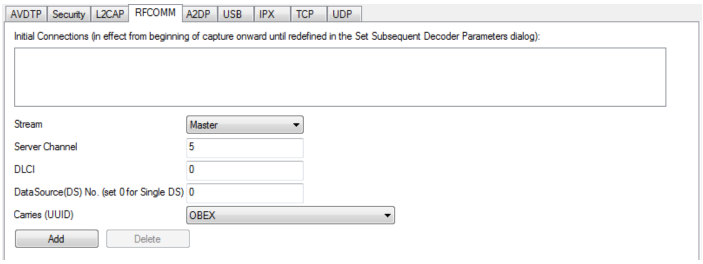
Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

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

3.2.4 RFCOMM Decoder Parameters

3.2.4.1 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 3.31 - RFCOMM parameters tab

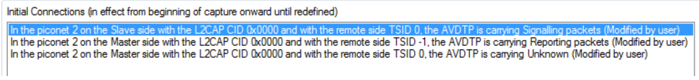
The **RFCOMM Set Initial Decoder Parameters** tab requires the following user inputs to complete a parameter:

- **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 3.32 - 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

3.2.4.2 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.

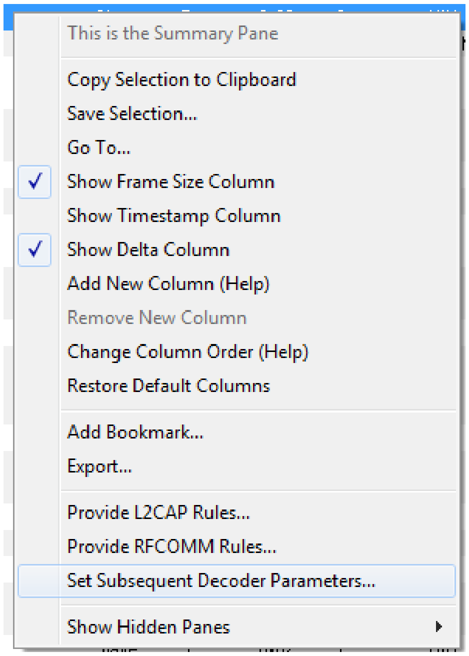
3.2.4.3 RFCOMM Override Decode Information

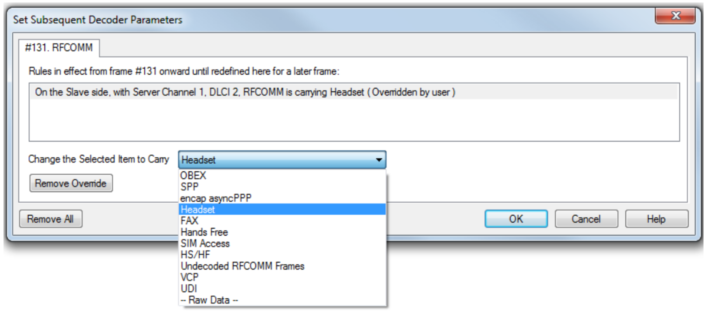
The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

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 3.33 - 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 passphrase. 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 191 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 3.15 - *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,

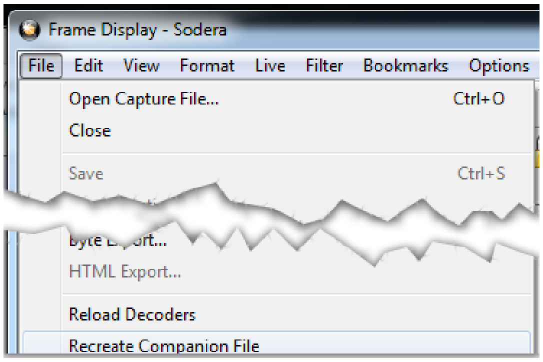
Table 3.16 - CSRmesh Passphrase Format

Name	Enter as	Description
Technology Identifier	[CSRMESH]	
Passphrase	PASSPHRASE	character string identical to the one used in CSRmesh Android/iOS App

The following code is an example of CSRmesh decryption passphrase entry.

```
[CSRMESH]
PASSPHRASE = test
```

Loading keys or passphrase



When the ComProbe software is initially loaded, keys or the passphrase will be automatically read from the MeshOptions.ini file. If the keys or the passphrase are modified while the ComProbe 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 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 201.

Troubleshooting Tips

MeshOptions.ini Errors

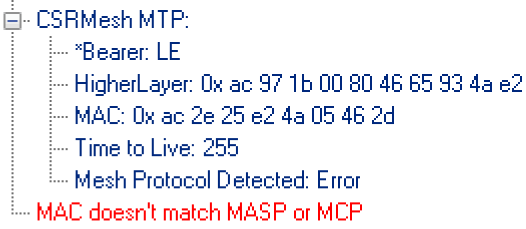
Table 3.17 - Errors Associated with MeshOptions.ini

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 Passphrase

- When the passphrase 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 3.34 - 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 3.18 - Errors: Bluetooth technology using mesh networking

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

3.4 Conductive Testing

Conductive testing could be used for many reasons, but the most common use is to isolate the 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 on the next page lists the maximum power and operating range for each Classic *Bluetooth* Class.

Table 3.19 - 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 3.20 - *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 LE Conductive Testing

Test Equipment

While exact conductive test setups are dependent on the specific circumstances surrounding the DUT RF interface, the following equipment is required for all 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 Sodera LE **Antenna** and **Wireded** connectors.
5. Attenuators, values depending on the *Bluetooth* technology or Class being tested.
6. Frontline Sodera LE Wideband *Bluetooth* low energy Protocol Analyzer.
7. Personal computer for running Frontline software.

Test Setup

The following figures show the conductive test setup. The values of AT1, AT2, and AT3 depend on the power transmitted by DTU1 and DTU2 and which setup is used.

> **Note:** Internal Sodera LE attenuation options are likely to preclude the use of external attenuators when using typical *Bluetooth* low energy power levels.

Wired Input Test Setup

Sodera LE Conductive Test Setup (a) below connects the test signal to the Sodera LE **Wired** input connector. This input provides internal 27 dB attenuation, so AT3 may not be necessary depending on the DUT1 and DUT2 transmitted power.

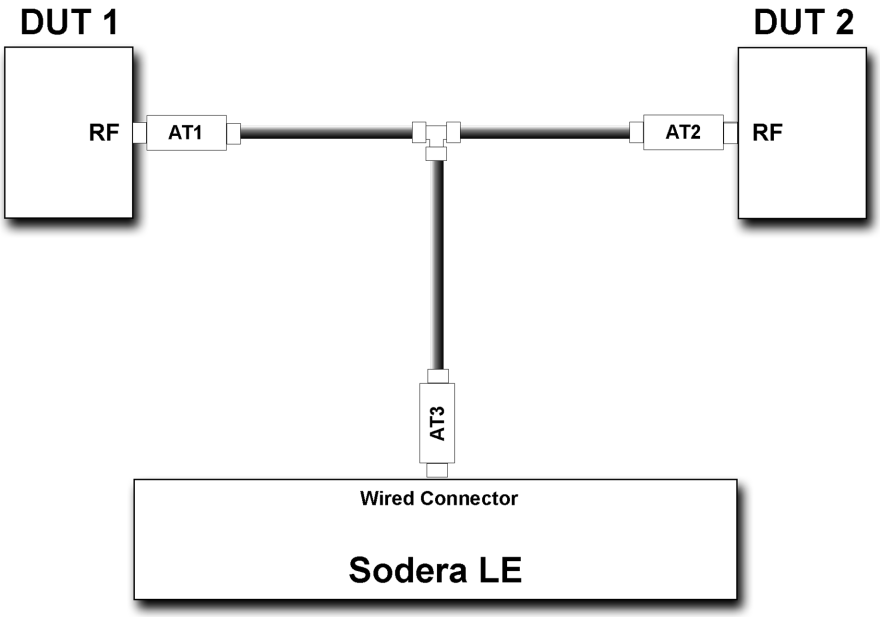


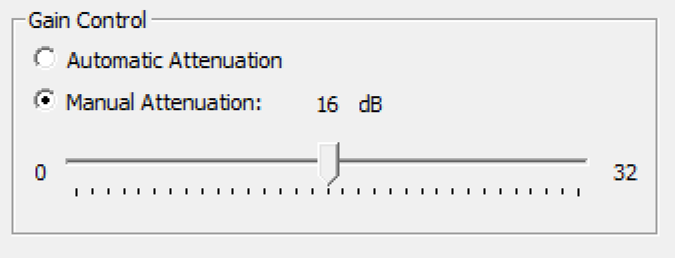
Figure 3.35 - Sodera LE Conductive Test Setup (a)

The AT1 through AT3 attenuator values will depend on the DUT 1 and DUT 2 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 (a): At the T-connector the power will split in half. For example, if DUT 1 is transmitting +20 dBm (100 mW), at the T-connector it will split with +17 dBm (50 mW) going to DUT 2 and +17 dBm (50 mW) going to the Sodera LE **Wired** connector. The Wired connector will provide an additional 27 dB attenuation after the connector reducing the 50 mW to -283 dBm (5x10^{-26} mW). This example points out that for conductive testing the **Wired** connector is best for larger RF signals.

Antenna Input Test Setup

Sodera LE Conductive Test Setup (b) on page 61 shows an alternate test setup that connects the devices under test to the Sodera LE **Antenna** connector. This setup provides a wider range of control over the internal attenuation. To use the variable attenuator on the **Antenna** input, the Sodear LE unit must be configured by selecting **Capture Options** from the **Options** menu. Select the **Manual Attenuation** in the **Gain Control** section. With this control you can select Sodera LE internal attenuation between 0 and 32 dB in 1 dB steps. Refer to Sodera LE Sodera LE Menu Bar on page 19 for additional information about this control.



Gain Control

○ Automatic Attenuation

● Manual Attenuation: 16 dB

Figure 3.36 - Sodera LE Capture Options Gain Controls

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.

Using the signal levels as in the example above for the **Wired** input setup, 2.5 mW will appear at the Sodera LE Antenna connector, again assuming that no attenuators AT1 through AT3 are being used. You can adjust the Manual Attenuation to adjust achieve reliable packet Recording and Analysis. As an alternative, you can also try using the **Gain Control Automatic Attenuation** option that will adjust the received signal level for estimated best reliable analysis results.

Note: Each Sodera LE **Manual Attenuation** setting must be configured prior to Recording.

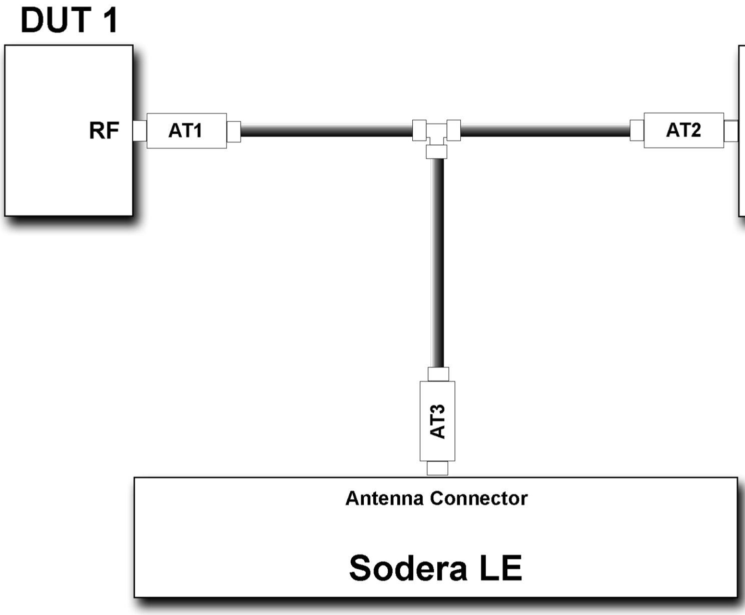


Figure 3.37 - Sodera LE Conductive Test Setup (b)

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.

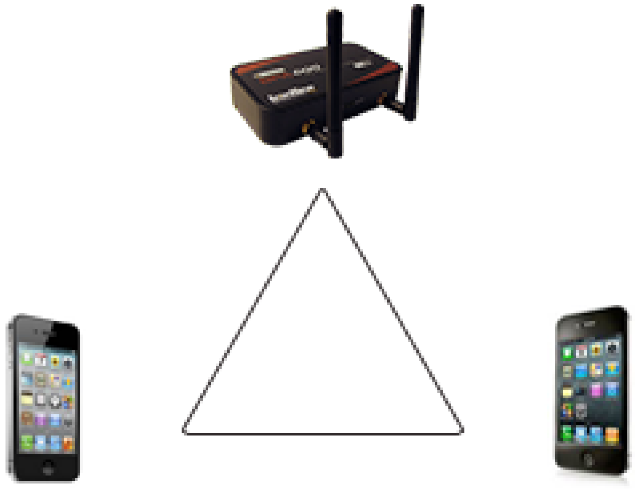


Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane

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.

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.

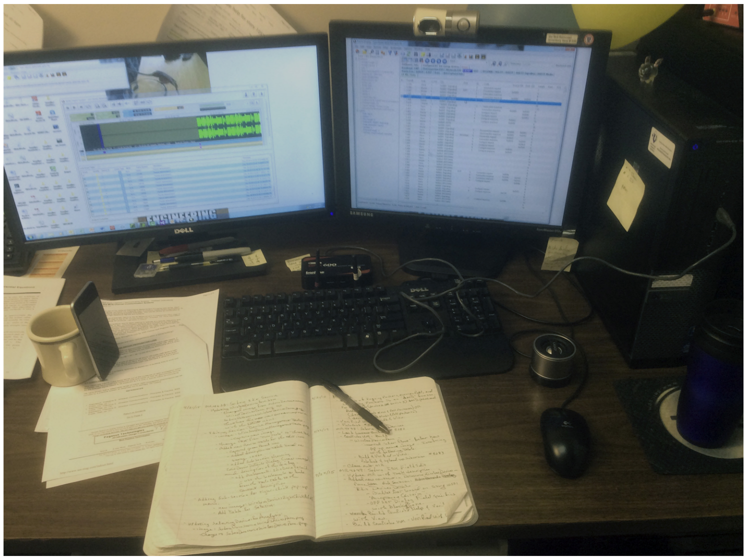


Figure 4.2 - Example: Poor Capture Environment

4.1.2 Sodera LE Capturing Data: Introduction

Data capture using Sodera LE 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 LE: Record—Begin Capture

When starting a capture session

- the active status of all devices is cleared in the **Wireless 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 LE 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** 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.

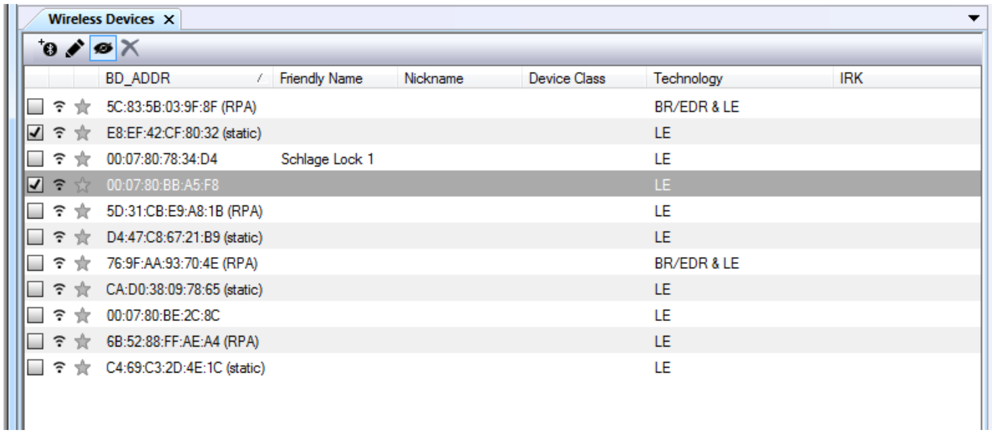
The **Event Log** pane will begin to populate with information, warnings, and error messages.

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 LE hardware and the Frontline software. If it has not been saved, then a pop-up warning message will appear.

4.1.2.2 Sodera LE: Selecting Devices for Analysis

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

Figure 4.3 - Sodera LE Wireless Devices Pane

In the **Wireless Devices** pane, place a check in the row of each active device ᯤ 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).

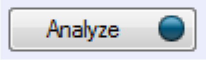
The following table lists some common data capture and device selection scenarios.

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

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

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

- Status Bar (see Sodera LE Datasource Window on page 17) - Displays "SIGNAL TOO STRONG".
- The Sodera LE Overload LED on the front panel will illuminate red.

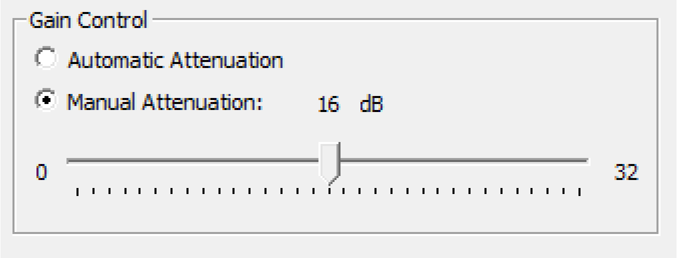
Note: These warnings will occur only in live capture mode. No visual indications will occur in capture file playback or in excursion mode playback.

Conditions for "too strong" RF signal

For the Sodera LE hardware, the Frontline software will determine that a received signal is *too strong* if it exceeds

27 dBM.

Suggested Corrective Action



Gain Control

○ Automatic Attenuation

● Manual Attenuation: 16 dB

0 32

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

Move the antenna from the **Antenna** connector to the **Wired** connector. Try capturing again.

With a persistent Signal too Strong indication with the antenna on the **Antenna** connector, try checking the **Gain Control Manual Attenuation)** from the **Capture Options...** selection of the **Options** menu. Use the slider control to adjust the attenuation and then try capturing again. Repeat until successful capture is achieved.

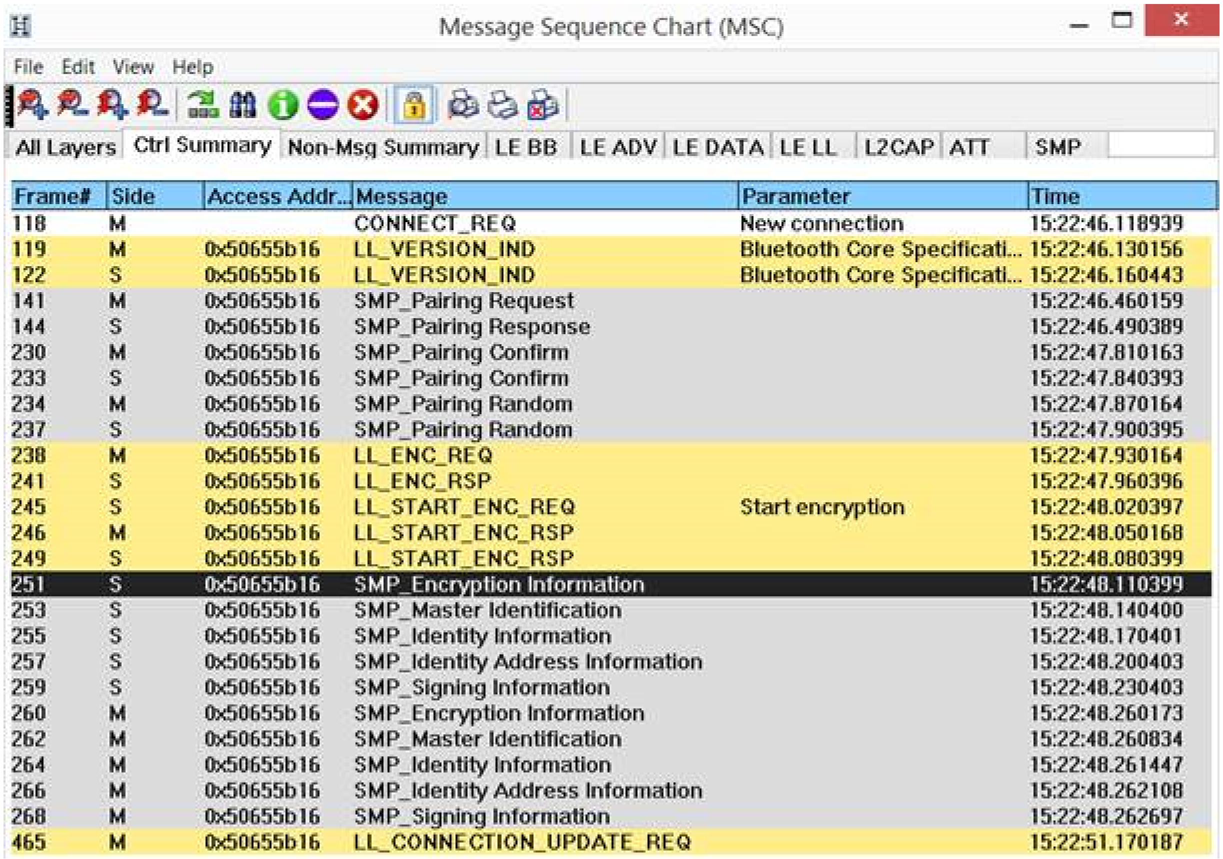
4.1.2.5 Sodera LE: Critical Packets and Information for Decryption

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

Bluetooth low energy Encryption (AES)

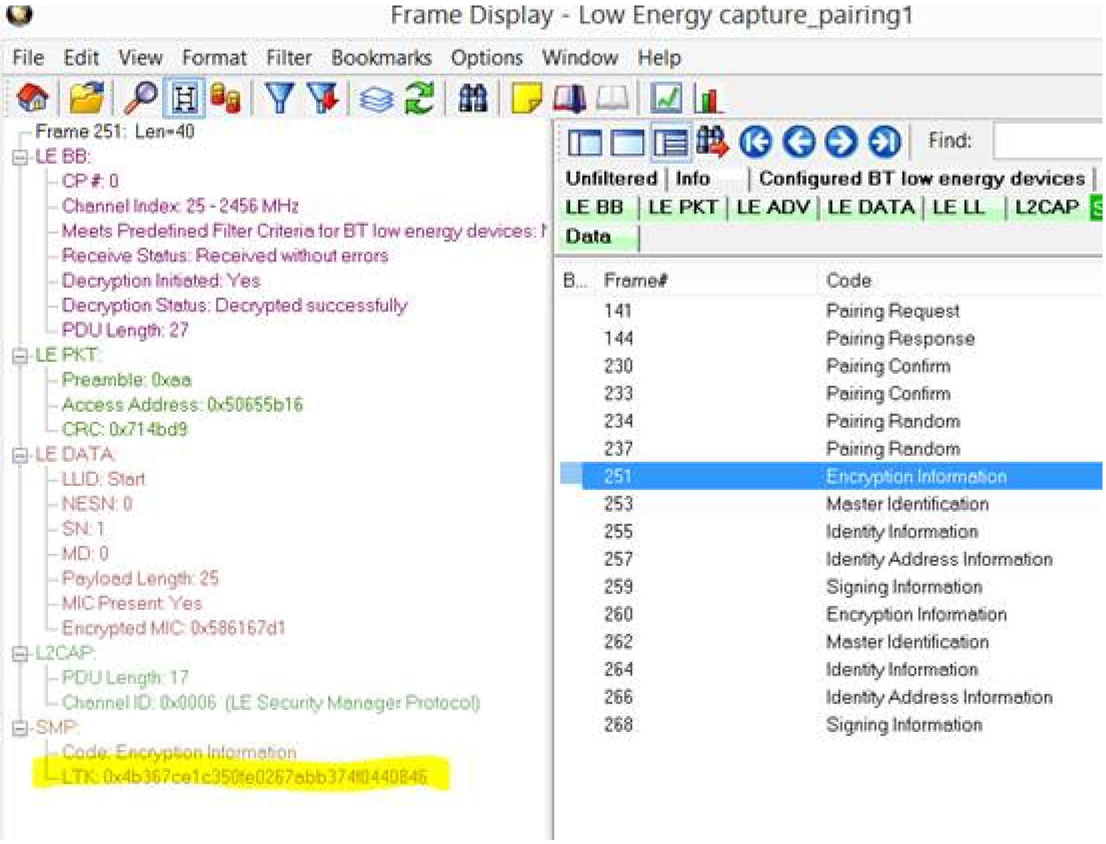
The following information and packets are needed to follow decryption:

- 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 4.4 - 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: N
   -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: 0x4b367ce1c350fe0267abb374f0440846
```

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 4.5 - Bluetooth low energy Critical Decryption Packets, Frame Display

4.1.2.6 Capturing Sodera LE 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 LE will begin capturing data from all wireless devices within range .
2. In the **Wireless 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.

4.2 Protocol Stacks

4.2.1 Protocol Stack Wizard

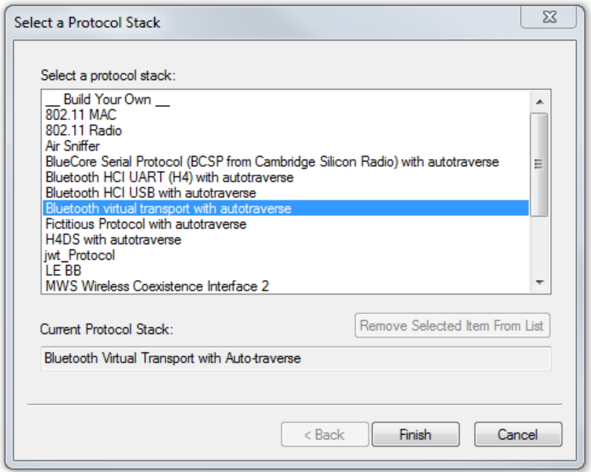
The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.

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 72.



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.

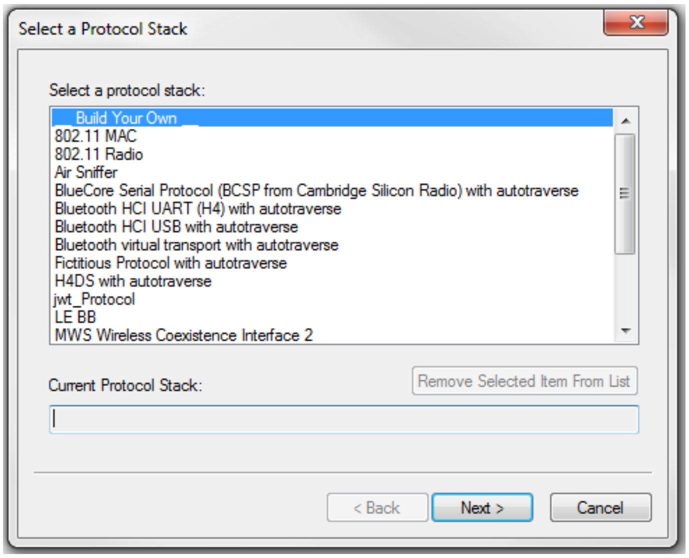
If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing on page 73 for more information.

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

4.2.2 Creating and Removing a Custom Stack

To create a custom stack:

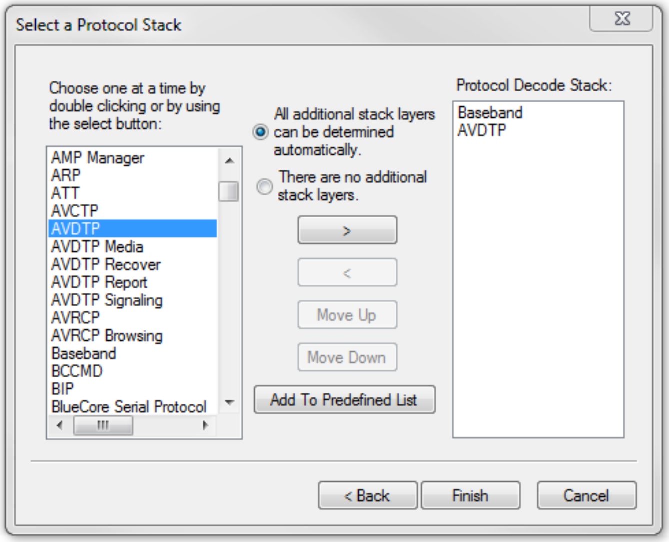
1. Choose **Protocol Stack** from the **Options** menu on the **Control** window or click the Protocol Stack icon on the **Frame Display** toolbar.
2. Select **Build Your Own** from the list and click **Next**.
3. The system displays an information screen that may help you decide if you need to define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



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

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.



Choose one at a time by double clicking or by using the select button:

AMP Manager
ARP
ATT
AVCTP
AVDTP
AVDTP Media
AVDTP Recover
AVDTP Report
AVDTP Signaling
AVRCP
AVRCP Browsing
Baseband
BCCMD
BIP
BlueCore Serial Protocol

● All additional stack layers can be determined automatically.
○ There are no additional stack layers.

Protocol Decode Stack:
Baseband
AVDTP

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 74 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 73 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.

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.

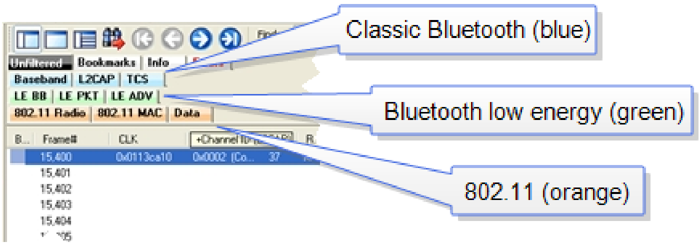
- Summary Pane - The **Summary Pane** displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.
- Decode Pane - The **Decode Pane** displays a detailed decode of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

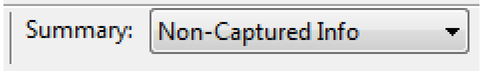
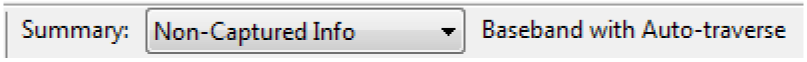
Table 4.2 - Frame Display Toolbar Icons(continued)

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.
Reload Decoders - When **Reload Decoders** is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.	
Filter:	Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.
The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.	
	Show Default Panes - Returns the panes to their default settings.

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
▭	Show Only Summary Pane - Displays only the Summary pane.
◫	Shall All Panes Except Event Pane - Makes the Decode pane taller and the Summary pane narrower.
🔒	Toggle Display Lock - Prevents the display from updating.
	Go To Frame
⏮	First Frame - Moves to the first frame in the buffer.
←	Previous Frame - Moves to the previous frame in the buffer.
→	Next Frame - Moves to the next frame in the buffer.
⏭	Last Frame - Moves to the last frame in the buffer.
Find:	Find on Frame Display only searches the Decode Pane for a value you enter in the text box.
🔍	Find Previous Occurrence - Moves to the previous occurrence of the value in the Frame Display Find.
🔍	Find Next Occurrence - Moves to the next occurrence of the value in the Frame Display Find.
🔍	Cancel Current Search - Stops the current Frame Display Find.

Table 4.2 - Frame Display Toolbar Icons(continued)

<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td> Summary:</td><td>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</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

> **Note:** If the frames are sorted in other than ascending frame number order, the order of the frames in the buffer is the sorted order. Therefore the last frame in the buffer may not have the last frame number.

4.3.1.2 Frame Display Status Bar

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

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

4.3.1.3 Hiding and Revealing Protocol Layers in the Frame Display

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

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

There are two ways to hide a layer.

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

To reveal a hidden protocol layer:

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

4.3.1.4 Physical vs. Logical Byte Display

The **Event Display** window and **Event Pane** in the **Frame Display** window show the physical bytes. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the logical data, or the resulting byte values after escape codes or other character altering codes have been applied (a process called transformation).

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

4.3.1.5 Sorting Frames

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

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

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

4.3.1.6 Frame Display - Find

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

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

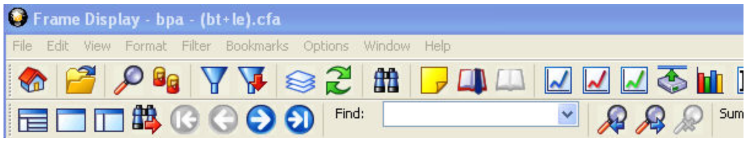
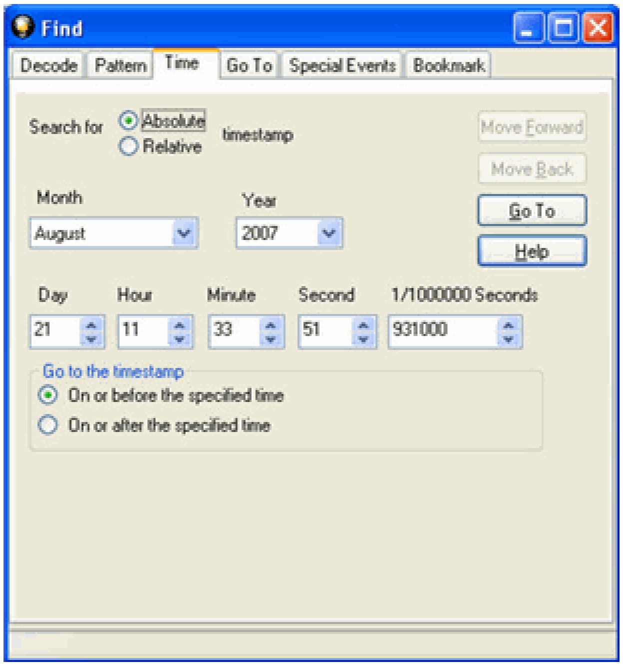


Figure 4.6 - Frame Display Find text entry field

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	Year
August	2007

Day	Hour	Minute	Second	1/1000000 Seconds
21	11	33	51	931000

Go to the timestamp

● On or before the specified time

○ On or after the specified time

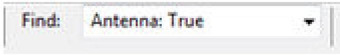
Figure 4.7 - Search/Find Dialog

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.

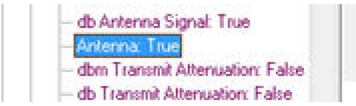
2. Enter a value in the **Find** text box.



Find: Antenna: True

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

Select **Find Previous Occurren3e** 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.



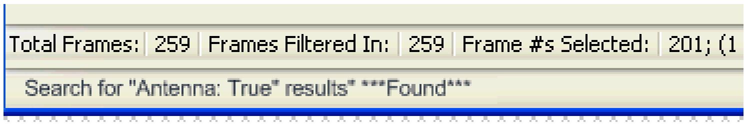
db Antenna Signal: True
Antenna: True
dbm Transmit Attenuation: False
db Transmit Attenuation: False

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.

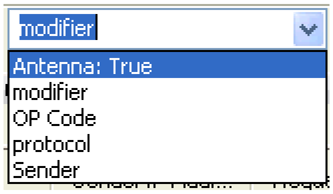
- When you enter a search string and select Enter, the search moves forward.
- If you select **Find Previous Occurrence**, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous 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.
- The search occurs only on the protocol layer selected.
- To search across all the protocols on the Frame Display, select the Unfiltered tab.



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

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

- A drop-down list displays the search values entered during the current session of Frame Display.
- The search is cancelled when you select a different protocol tab during a search.
- You can cancel the search at any time by selecting the **Cancel Current Search** button.



modifier

Antenna: True
modifier
OP Code
protocol
Sender

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...**.

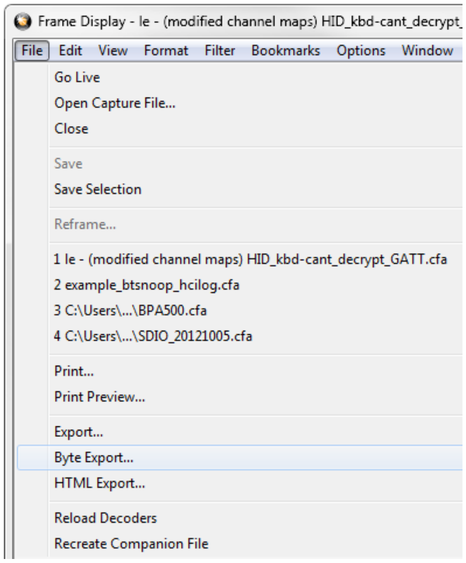
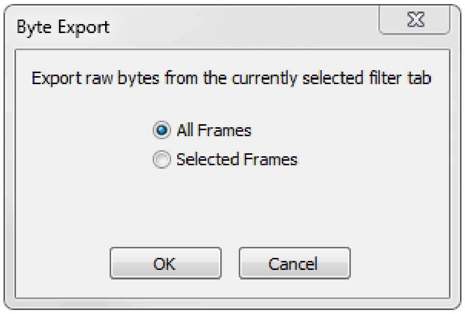

Frame Display - le - (modified channel maps) HID_kbd-cant_decrypt_
File
Edit
View
Format
Filter
Bookmarks
Options
Window
Go Live
Open Capture File...
Close
Save
Save Selection
Reframe...
1 le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa
2 example_btsnoop_hcilog.cfa
3 C:\Users\...\BPA500.cfa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

Figure 4.8 - 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

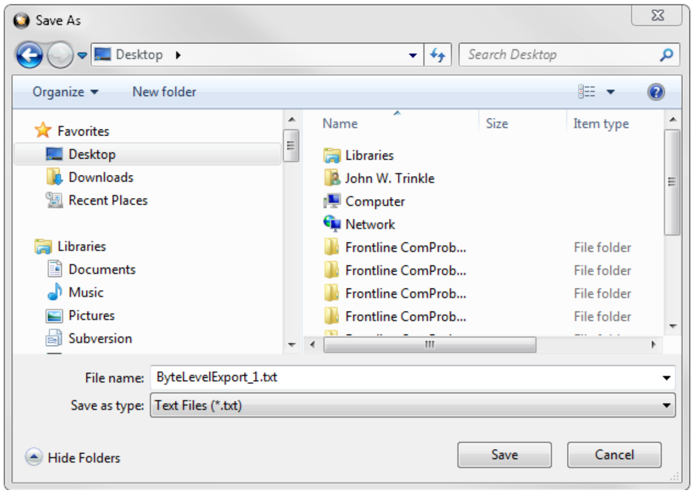
Export raw bytes from the currently selected filter tab

● All Frames
○ Selected Frames

Figure 4.9 - 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.



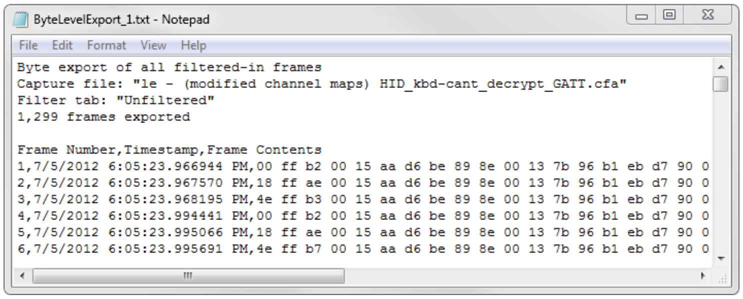
File name: ByteLevelExport_1.txt

Save as type: Text Files (*.txt)

Figure 4.10 - 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 4.11 - 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.

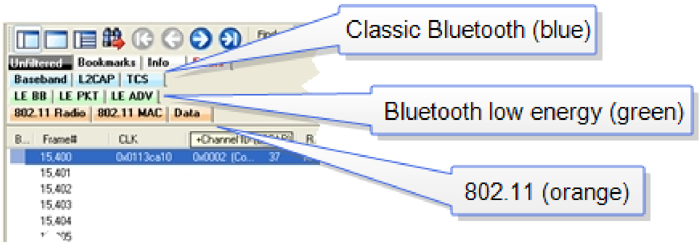


Figure 4.12 - Example Protocol Tags

- 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:

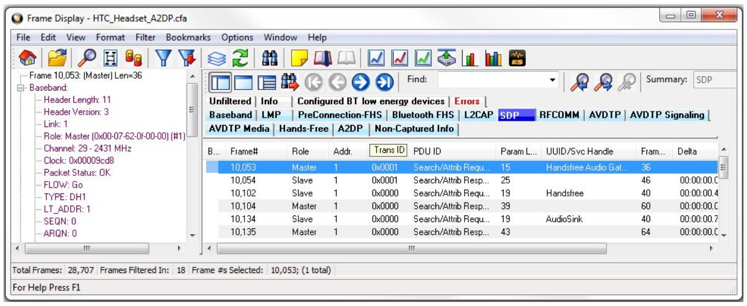
- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

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 (0x00-07-62-0f-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	00:00:00.0
	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	00:00:00.0
	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	00:00:00.0

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

For Help Press F1

Figure 4.13 - 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.

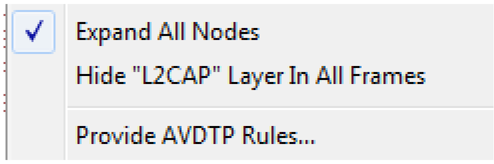
4.3.1.11.3 Frame Symbols in the Summary Pane

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.



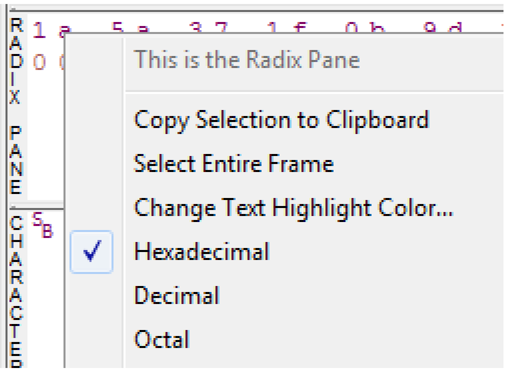
Protocol layers can be hidden, preventing them from being displayed on the **Decode** pane. Right-click on any protocol layer and choose **Hide** [protocol name] from the right-click menu.

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



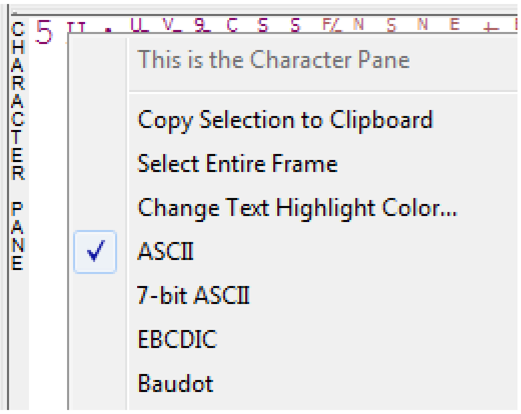
The **Radix** pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the **Format** menu, or by right-clicking on the pane and choosing **Hexadecimal**, **Decimal** or **Octal**.

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.

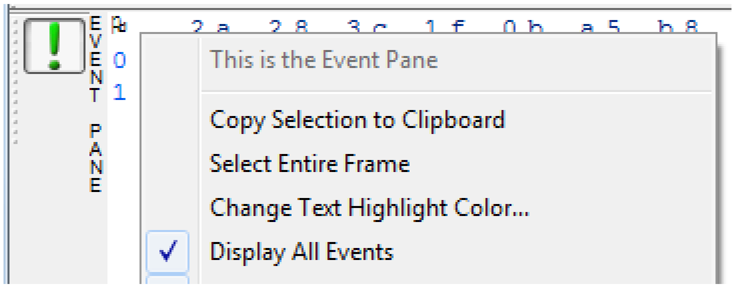
Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

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.



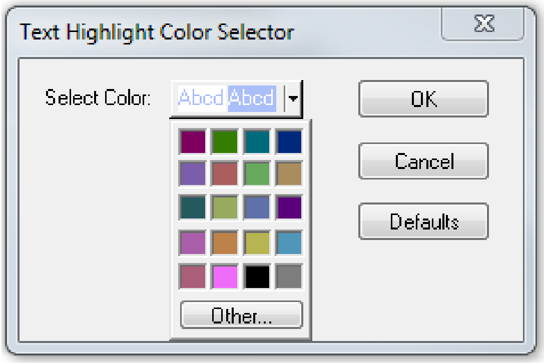
The status lines at the bottom of the pane give the same information as the status lines in the **Event Display** window. This includes physical data errors, control signal changes (if appropriate), and timestamps.

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 Protocol Layer Colors

4.3.1.12.1 Data Byte Color Notation

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

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

4.3.1.12.2 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.

4.3.1.12.3 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.

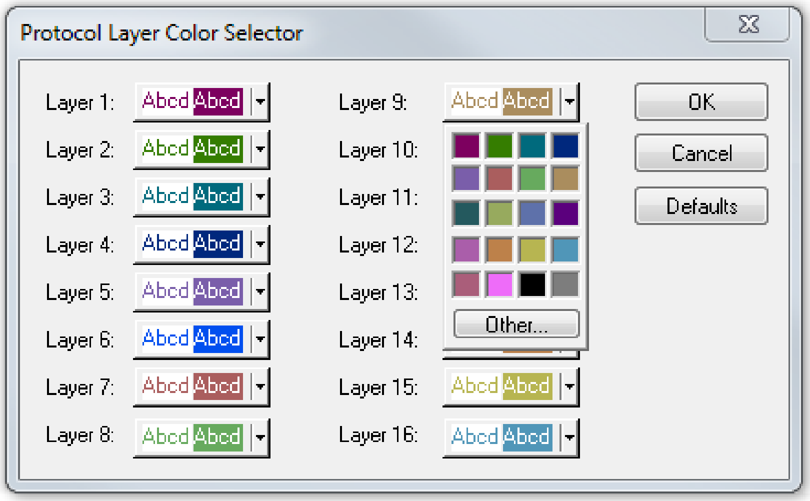


Figure 4.14 - Frame Display Protocol Layer Color Selector

4.3.1.13 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.

4.3.1.13.1 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.

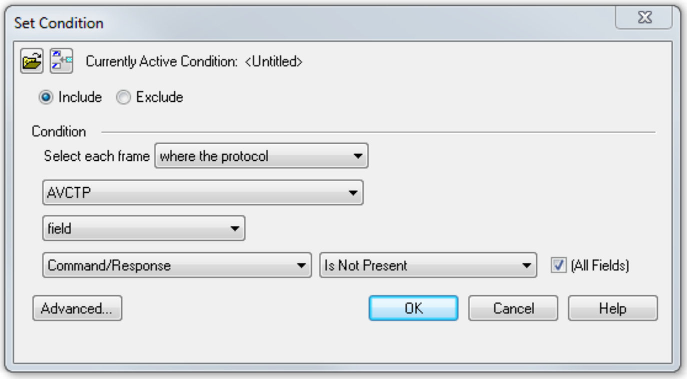
Quick Filters

- 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.

4.3.1.13.1.1 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

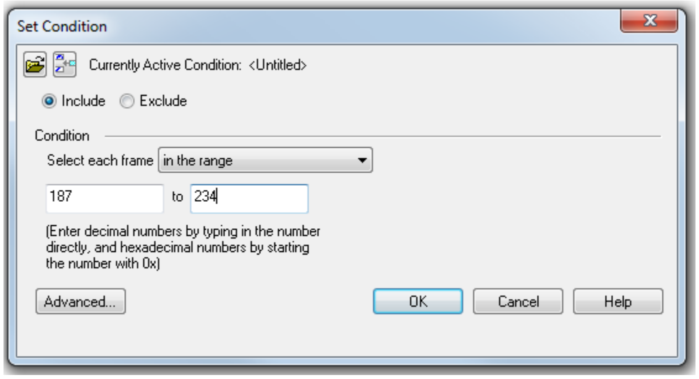
Select each frame: where the protocol

AVCTP

field

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

Figure 4.15 - 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 4.16 - 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.

4.3.1.13.1.2 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.

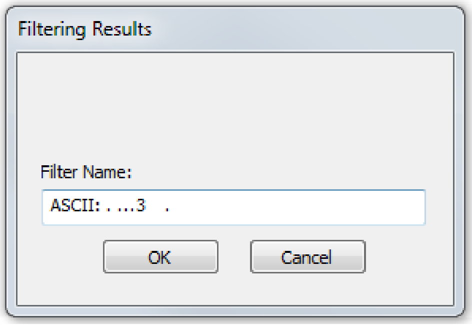
Exclude: A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

4.3.1.13.1.3 Named Display Filters

You can create a unique display filter by selecting a data type on the **Frame Display** and using a right click menu. When you create a **Name Filter**, it appears in the Quick Filtering dialog, where you can use it do customize the data you see in the **Frame Display** panes.

1. Select a frame in the **Frame Display Summary** Pane.
2. Right click in the one of the data columns in the **Summary** Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.
3. Select **Filter in *(data type)* =** . The **Filtering Results** dialog appears.
4. Enter a name for the filter
5. Select **OK**.

The filter you just created appears in the **Named Filters** section of the Quick Filtering dialog.



Filter Name: ASCII: . ...3 .

4.3.1.13.1.4 Using Compound Display Filters

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

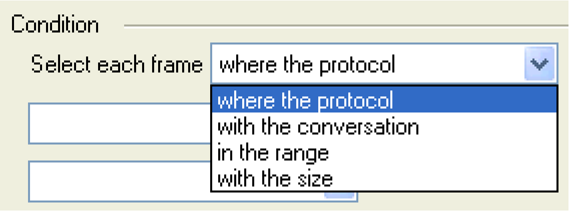
The **AND** operator narrows the filter, the **OR** operator broadens the filter, and the **NOT** operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

There are two steps to using a compound filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the filter menu to open the **Set Condition** dialog box.
2. Click the **Advanced** button on the **Set Condition** dialog box.
3. Select **Include** or **Exclude** radio button.

Now you can set the conditions for the filter.

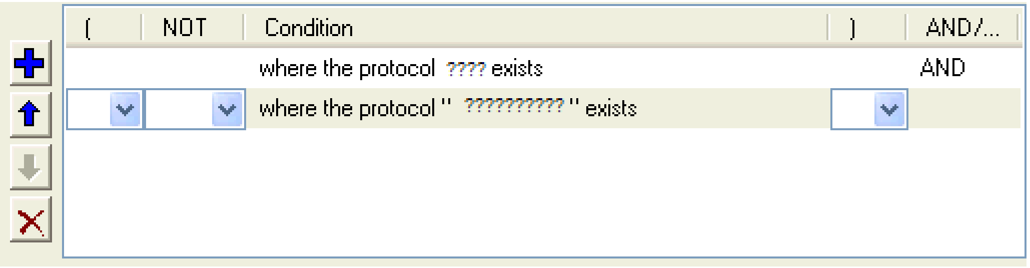
4. Select the initial condition for the filter from the combo box at the bottom of the dialog for **Select each frame.**



Condition

Select each frame: where the protocol

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 4.17 - 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.

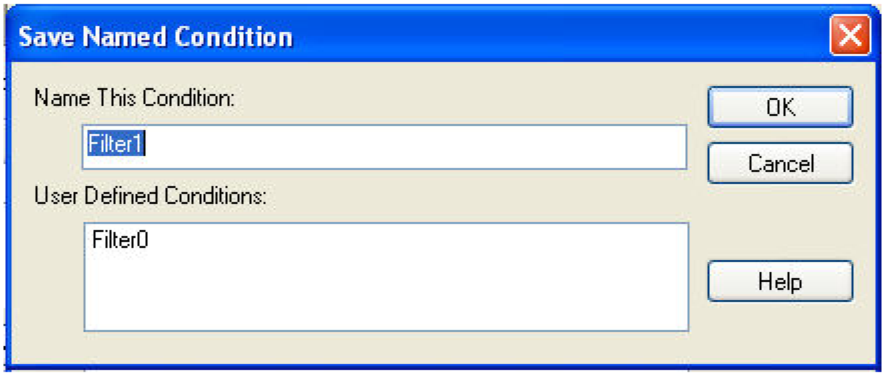
   Use the up ⬆ and down ⬇ arrow icons on the left side of the dialog box to order your conditions, and the delete button ✕ to delete conditions from your filter.

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**.



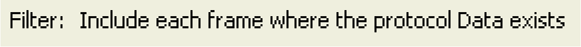
Save Named Condition

Name This Condition: Filter1

User Defined Conditions: Filter0

Figure 4.18 - 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

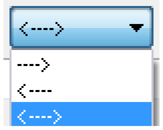
When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

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

4.3.1.13.1.5 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.

4.3.1.13.1.6 The Difference Between Deleting and Hiding Display Filters

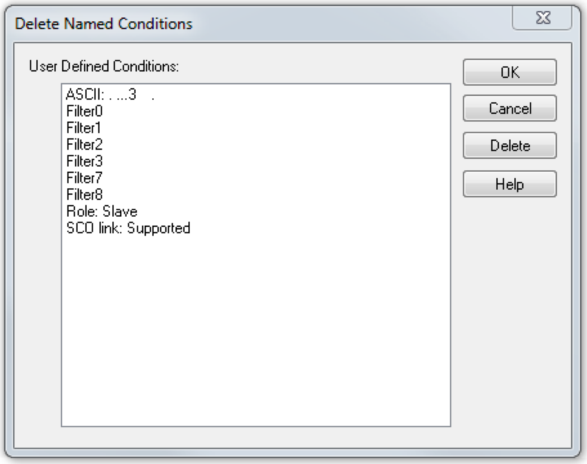
If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

Deleting a saved filter removes the filter from the current session and all subsequent sessions. In order to retrieve a deleted filter, the user must recreate it using the **Set Conditions** dialog.

Hiding a filter merely removes the filter from the display. A hidden filter can be reapplied using the Show/Hide procedure.

Deleting Saved Display Filters

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

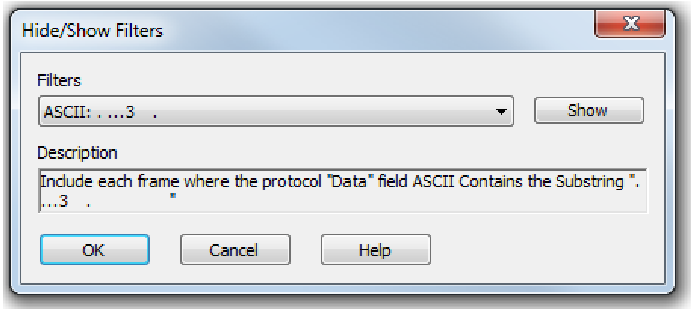


ASCII: . ...3 .
Filter0
Filter1
Filter2
Filter3
Filter7
Filter8
Role: Slave
SCO link: Supported

Hiding and Revealing Display Filters

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

1. **Select Hide/Show Display Filters…** from the **Filter** menu on the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.



Filters: ASCII: . ...3 .

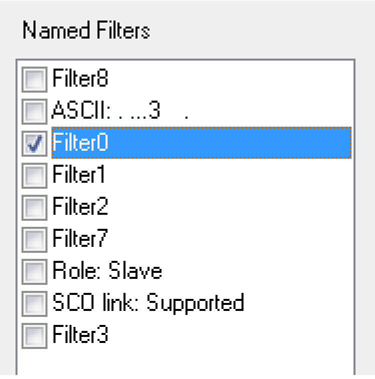
Description: Include each frame where the protocol "Data" field ASCII Contains the Substring ". ...3 . "

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

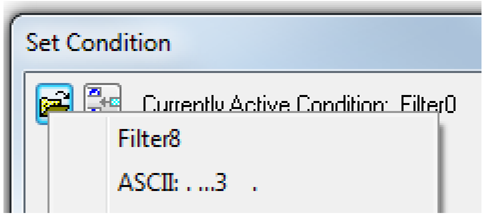
- □ Filter8
- □ ASCII: . ...3 .
- ☑ Filter0
- □ Filter1
- □ Filter2
- □ Filter7
- □ Role: Slave
- □ SCO link: Supported
- □ Filter3

Figure 4.19 - 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.

4.3.1.13.1.7 Editing Filters

Modifying a Condition in a Filter



Set Condition

Currently Active Condition: Filter0

Filter8

ASCII: . ...3 .

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the **Filter** menu to open the **Set Condition** dialog box. The **Set Condition** dialog box displays the current filter definition at the top of the dialog.

   To display another filter, click the **Open** icon, and select the filter from the pop-up list of all the saved filters.

2. Edit the desired parameter of the condition: Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.

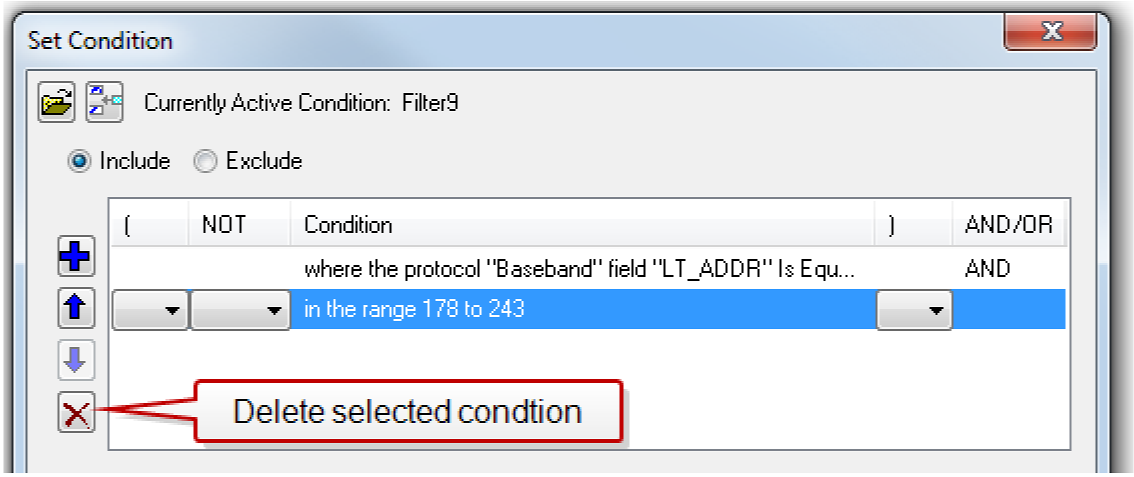
3. Click **OK**. The system displays the **Save Named Condition** dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click **OK**. If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided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

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

Deleting a Condition in a Filter

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

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



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		

Delete selected condtion

Figure 4.20 - Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.

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

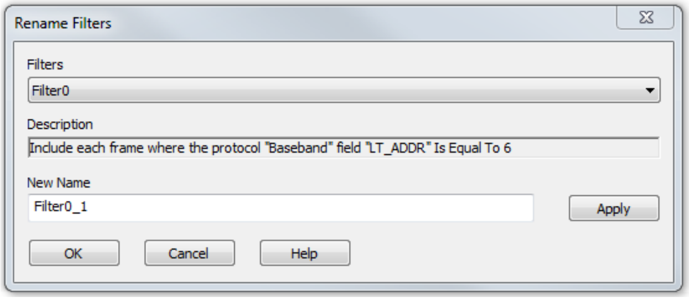
4. Edit the Boolean operators and parentheses as needed.

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.



Filters: Filter0

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

New Name: Filter0_1

Figure 4.21 - 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.

4.3.1.13.2 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.

4.3.1.13.2.1 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.

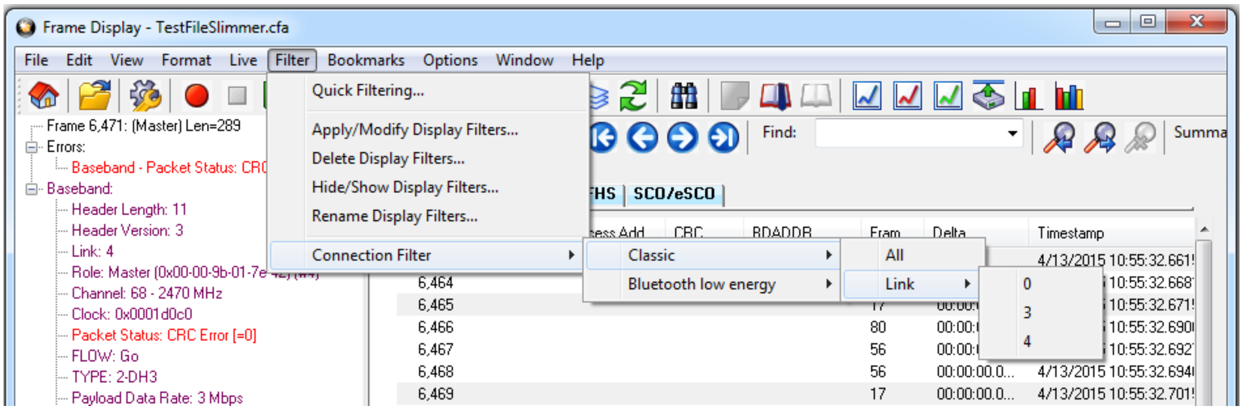


Figure 4.22 - Connection Filter from the Frame Display Menu

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.

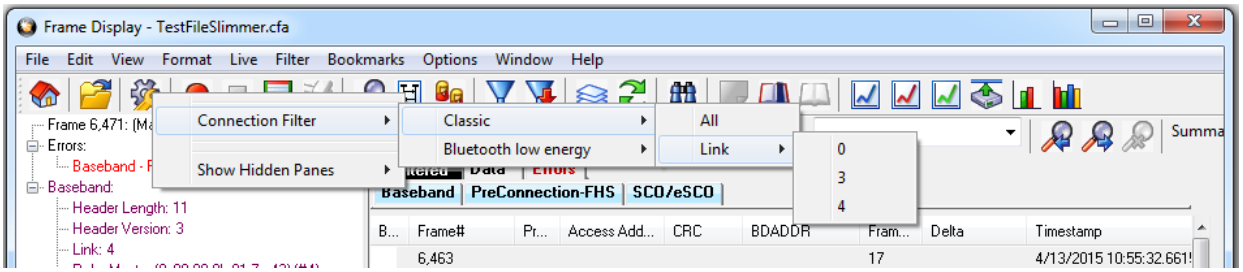
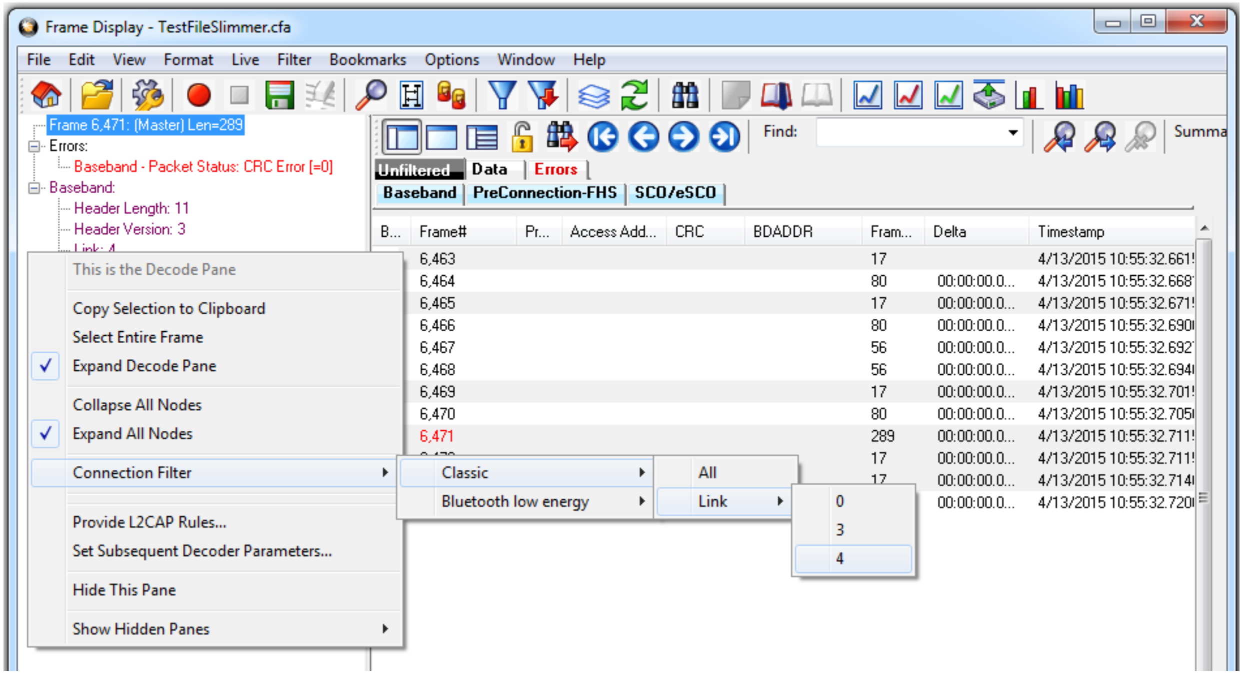

Frame Display - TestFileSlimmer.cfa
File Edit View Format Live Filter Bookmarks Options Window Help
Connection Filter
Show Hidden Panes
Classic
Bluetooth low energy
All
Link
0
3
4
Summa
Frame 6,471: (Ma
Errors:
Baseband - F
Baseband:
Header Length: 11
Header Version: 3
Link: 4
Baseband PreConnection-FHS SCO/eSCO
B... Frame# Pr... Access Add... CRC BDADDR Fram... Delta Timestamp
6,463 17 4/13/2015 10:55:32.661

Figure 4.23 - 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.



Frame 6,471: (Master) Len=289
Errors:
Baseband - Packet Status: CRC Error [=0]
Baseband:
Header Length: 11
Header Version: 3
Link: 4

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
						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 4.24 - 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.

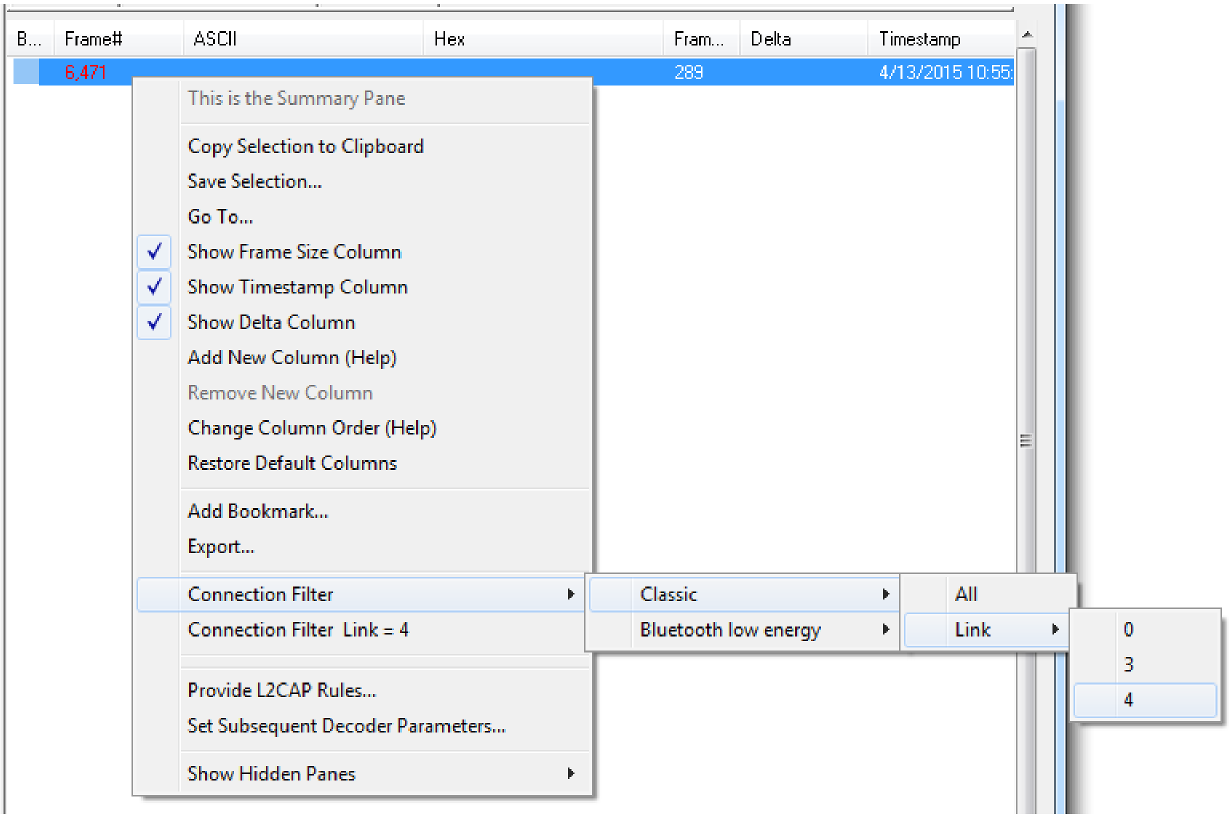


Figure 4.25 - Connection Filter from frame selection right-click

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.

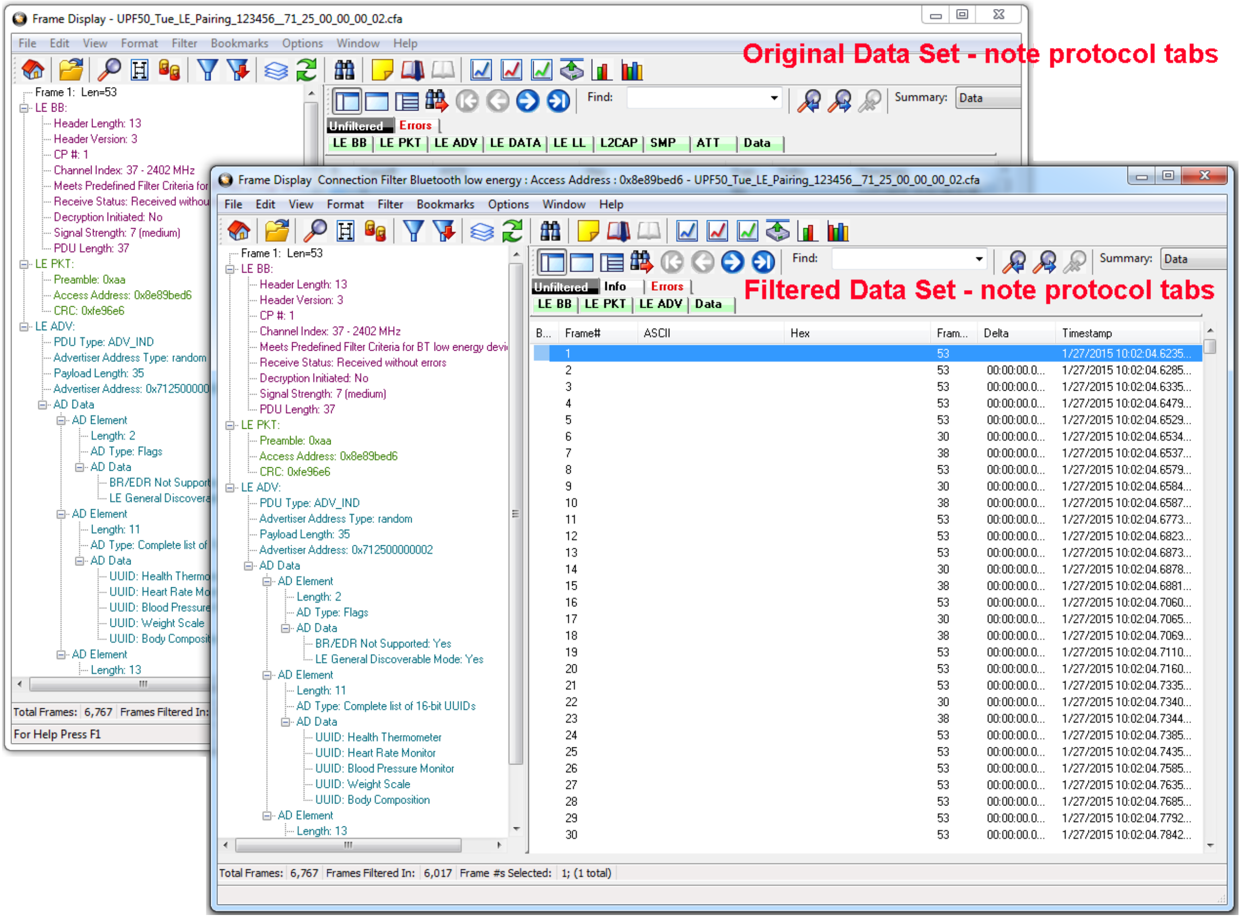
4.3.1.13.2.2 Connection Filter Display

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 84)

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
Original Data Set - note protocol tabs
Find:
Summary: Data
Unfiltered Errors
LE BB LE PKT LE ADV LE DATA LE LL L2CAP SMP ATT Data
Total Frames: 6,767 Frames Filtered In:
For Help Press F1
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
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)

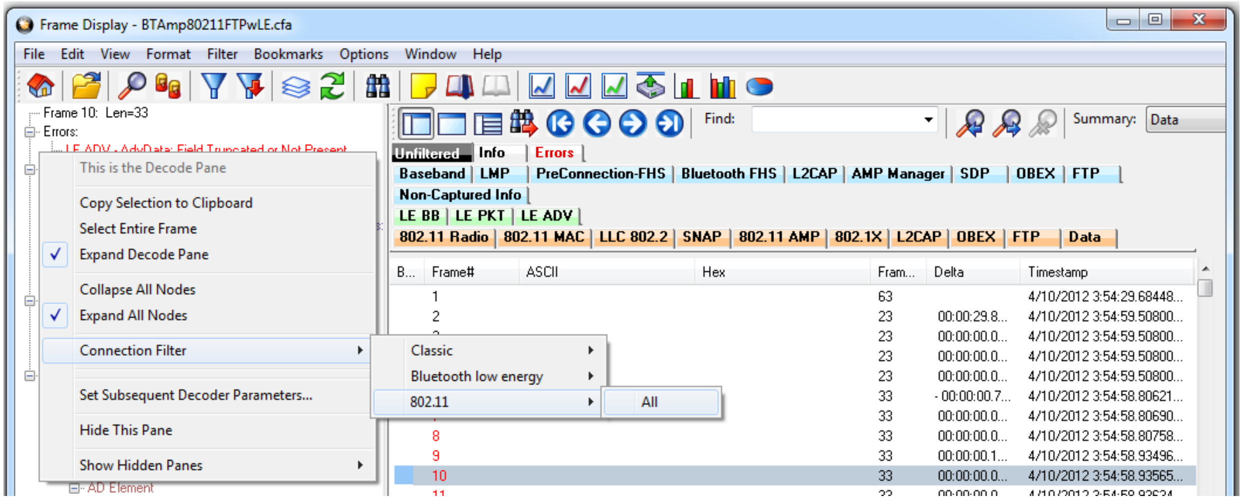
Figure 4.26 - Front Display: Filtered on Access Address 0x8e89bed6

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

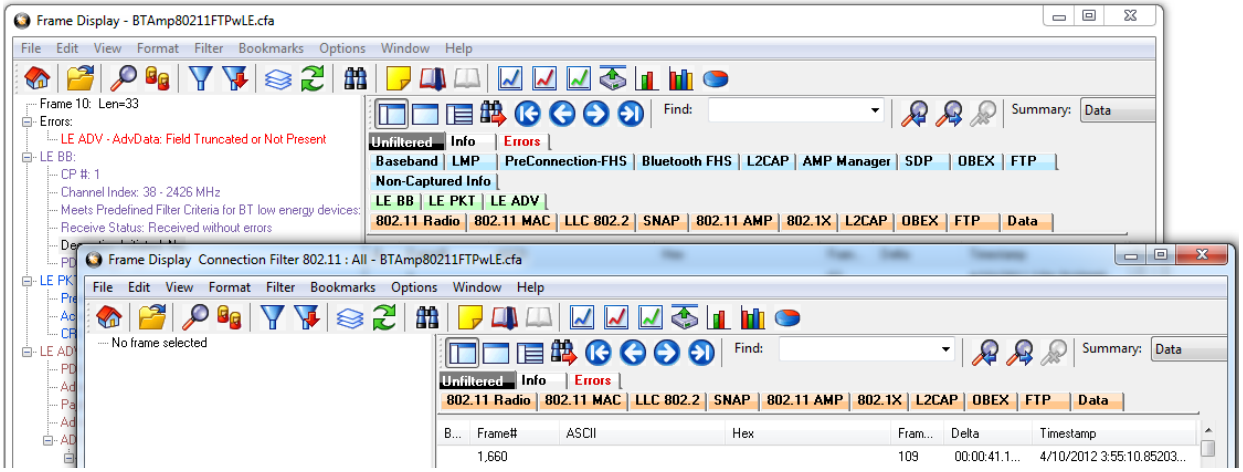
In this example, there is a capture file with Classic *Bluetooth*, *Bluetooth* low energy, and 802.11. To view just the 802.11 data set, 802.11 = All is selected from the right-click pop up menu.


Frame Display - BTAmp80211FTPwLE.cfa
File Edit View Format Filter Bookmarks Options Window Help
Frame 10: Len=33
Errors:
LE ADV - AdvData: Field Truncated or Not Present
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
AD Element
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
	1			63		4/10/2012 3:54:29.68448...
	2			23	00:00:29.8...	4/10/2012 3:54:59.50800...
				23	00:00:00.0...	4/10/2012 3:54:59.50800...
				23	00:00:00.0...	4/10/2012 3:54:59.50800...
				23	00:00:00.0...	4/10/2012 3:54:59.50800...
				33	- 00:00:00.7...	4/10/2012 3:54:58.80621...
				33	00:00:00.0...	4/10/2012 3:54:58.80690...
	8			33	00:00:00.0...	4/10/2012 3:54:58.80758...
	9			33	00:00:00.1...	4/10/2012 3:54:58.93496...
	10			33	00:00:00.0...	4/10/2012 3:54:58.93565...

Figure 4.27 - 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
File Edit View Format Filter Bookmarks Options Window Help
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
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
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...

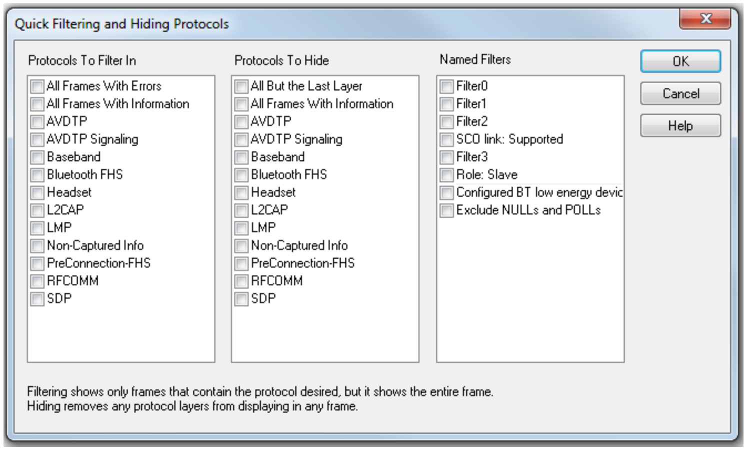
Figure 4.28 - Connection Filter selecting All 802.11 frames, front

4.3.1.13.3 Protocol Filtering from the Frame Display

4.3.1.13.3.1 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.

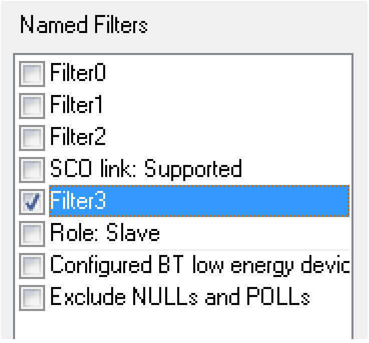
Figure 4.29 - Frame Display Quick Filtering and Hiding Protocols Dialog

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.

Quick Filter

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.

Filter3

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**

4.3.1.13.3.2 Easy Protocol Filtering

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

Filtering on the Summary Layer Protocol

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

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

Filtering on all Frames with Errors

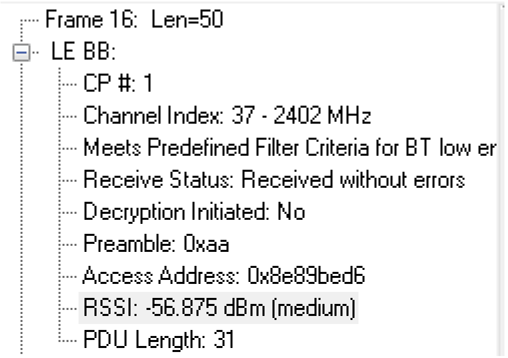
To filter on all frames with errors:

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

Errors

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

4.3.1.14 Sodera LE 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
```

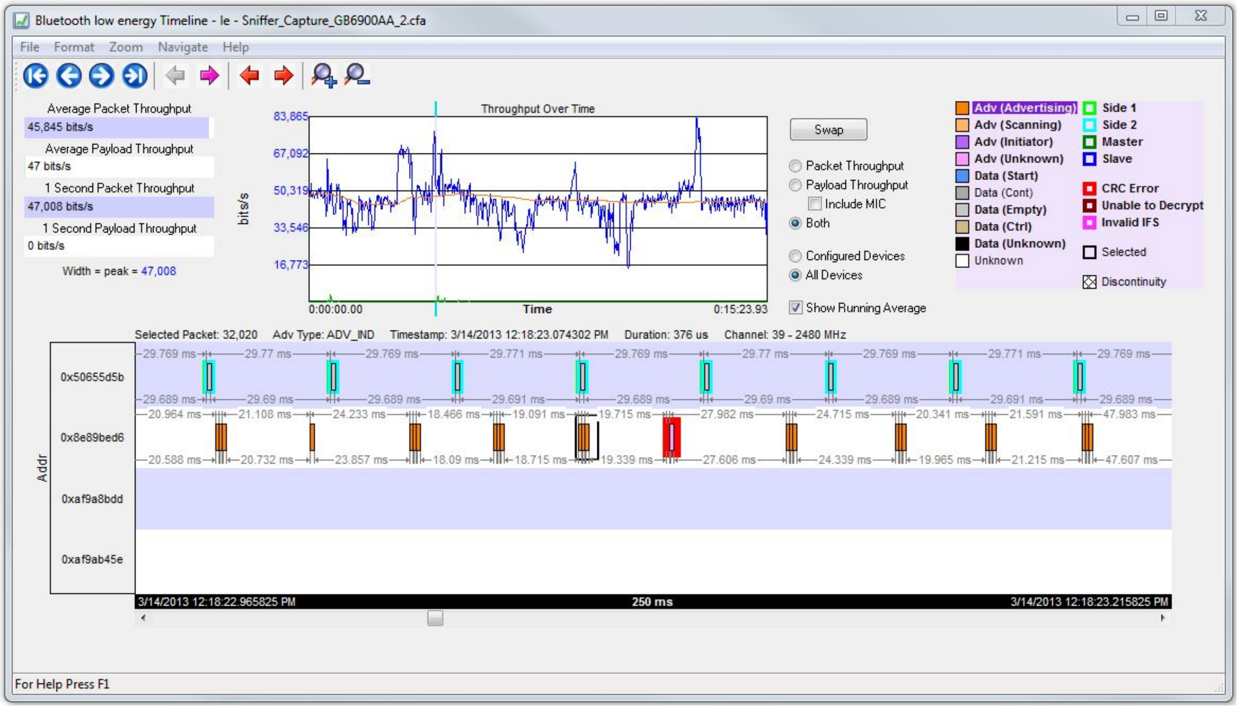
The Sodera LE calculates the RSSI (Receiver Signal Strength Indicator) value, a representation of the radio signal strength at the Sodera LE receiver, for every *Bluetooth* packet that it captures. RSSI is shown in dBm with a relative signal strength in parentheses. The RSSI value is shown as a decoded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

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

4.3.2 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.



Bluetooth low energy Timeline - le - Sniffer_Capture_GB6900AA_2.cfa

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

For Help Press F1

Figure 4.30 - *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.

4.3.2.1 low energy Timeline Toolbar

The toolbar contains the following:

Table 4.4 - *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

Table 4.4 - Bluetooth low energy Timeline Toolbar (continued)

Icon	Description
⇥	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
↺	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.

4.3.2.2 low energy Timeline Menu Bar

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

Table 4.5 - 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 4.5 - 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 4.5 - 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

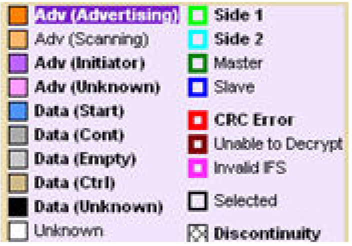
Table 4.5 - Bluetooth low energy Timeline Menus (continued)

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.

4.3.2.3 low energy Timeline Legend

This legend identifies the color coding found in the timeline.

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



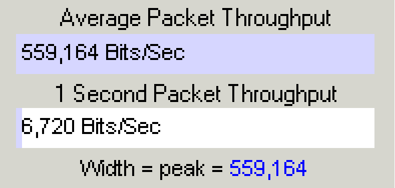
🟧 **Adv (Advertising)**	🟩 **Side 1**
🟧 Adv (Scanning)	🟦 **Side 2**
🟪 **Adv (Initiator)**	🟩 **Master**
🟪 **Adv (Unknown)**	🟦 Slave
🟦 **Data (Start)**	🟥 **CRC Error**
⬜ **Data (Cont)**	🟥 Unable to Decrypt
⬜ **Data (Empty)**	🟪 Invalid IFS
🟫 **Data (Ctrl)**	⬜ Selected
⬛ **Data (Unknown)**	▨ **Discontinuity**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

4.3.2.4 Throughput Displays

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

4.3.2.5 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.

4.3.2.6 Average and 1 Second Payload Throughput

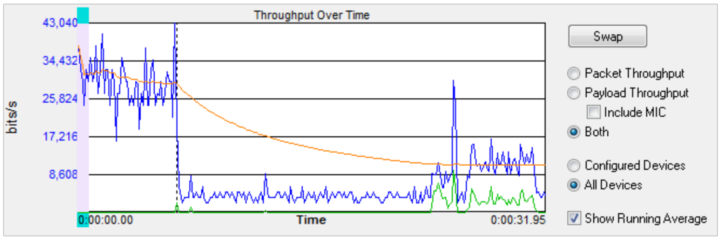
The figure depicts the **Average** and **One Second Payload** Throughput display. This display appears when you select the **Payload Throughput** radio button.

- **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.

4.3.2.7 Throughput Graph

The following figure depicts the Throughput Graph.



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

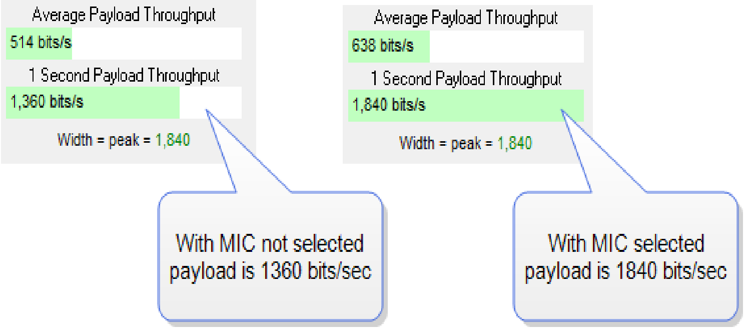
Figure 4.31 - *Bluetooth* low energy Timeline Throughput Graph

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

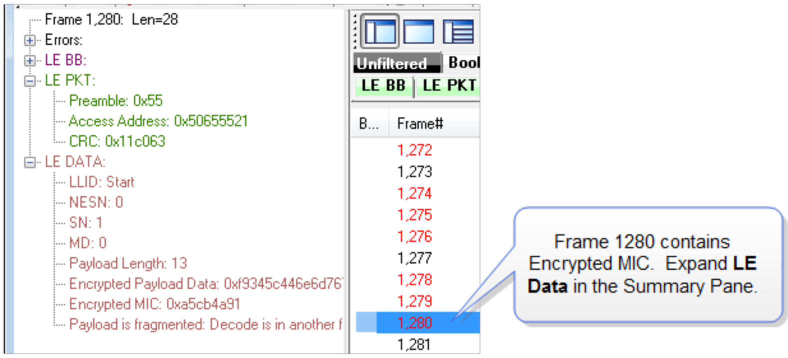
With MIC selected payload is 1840 bits/sec

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.

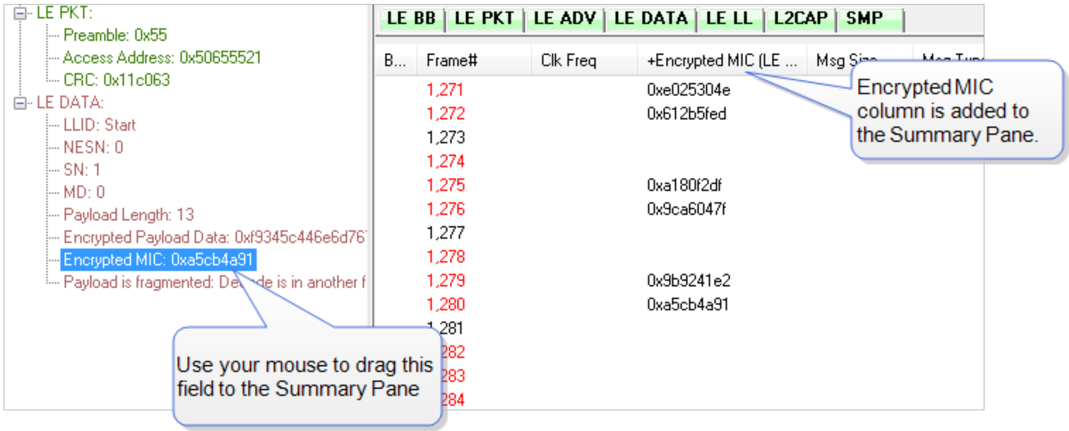


```
Frame 1,280:  Len=28
Errors:
LE BB:
LE PKT:
   Preamble: 0x55
   Access Address: 0x50655521
   CRC: 0x11c063
LE DATA:
   LLID: Start
   NESN: 0
   SN: 1
   MD: 0
   Payload Length: 13
   Encrypted Payload Data: 0xf9345c446e6d76
   Encrypted MIC: 0xa5cb4a91
   Payload is fragmented: Decode is in another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

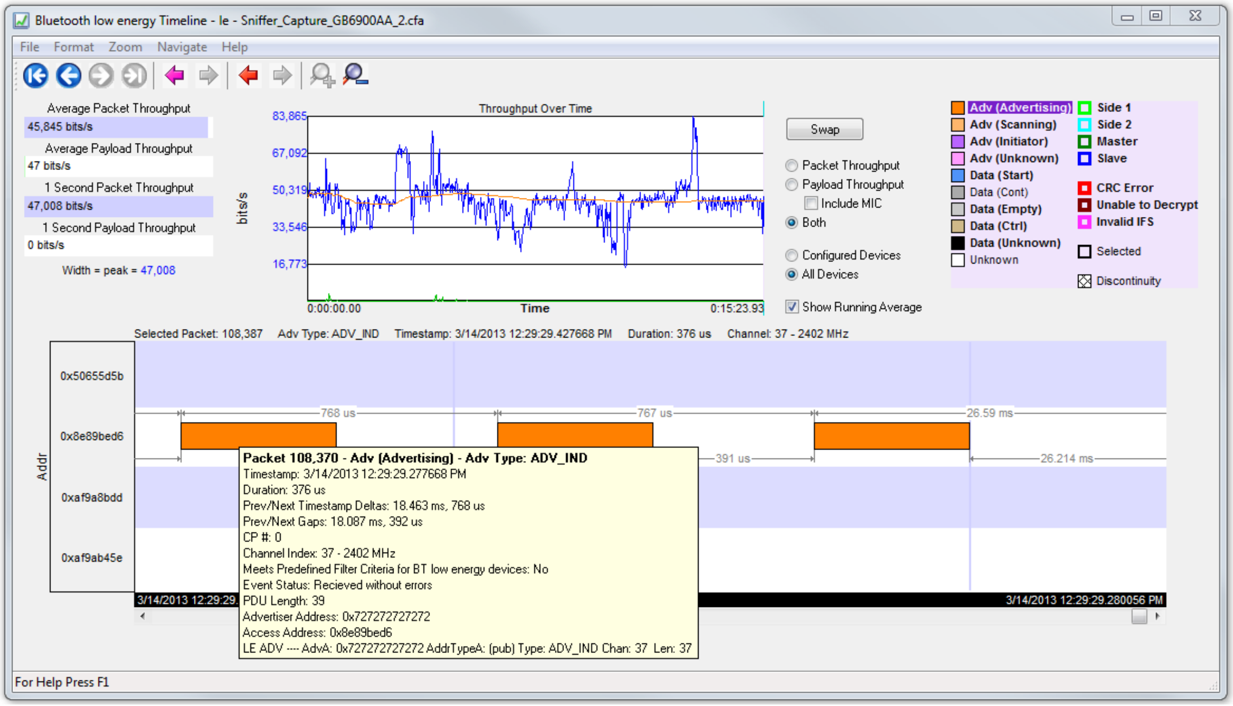
Encrypted MIC column is added to the Summary Pane.

Use your mouse to drag this field to the Summary Pane

Figure 4.32 - Creating Encrypted MIC in Frame Display Summary pane

4.3.2.8 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

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 4.33 - *Bluetooth***low energy Timeline**

4.3.2.9 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.

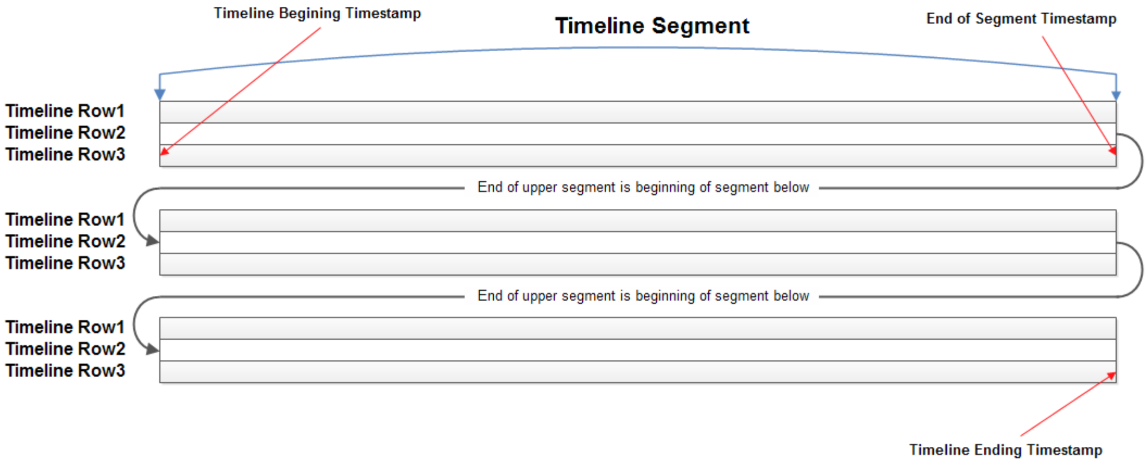
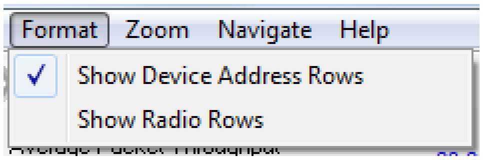


Figure 4.34 - Diagram of low energy Timeline Flow with Segment and Row Relationship

- 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.

4.3.2.10 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.

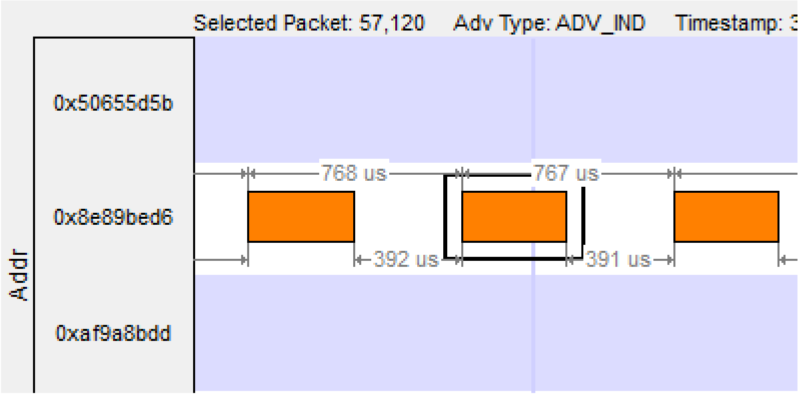


Figure 4.35 - Device Address Rows

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

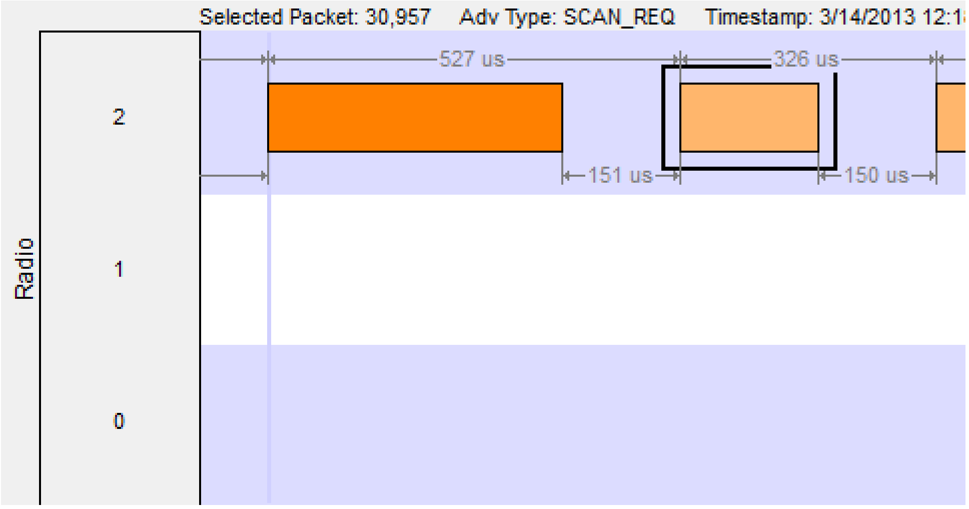

Selected Packet: 30,957 Adv Type: SCAN_REQ Timestamp: 3/14/2013 12:1
Radio
2
1
0
527 us
326 us
151 us
150 us

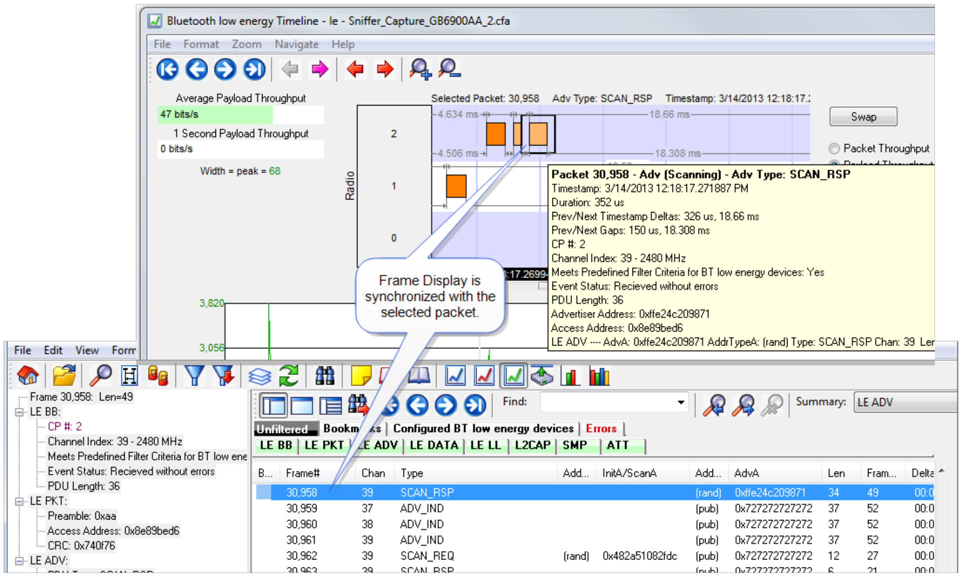
Figure 4.36 - Radio Rows

- 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
Radio
2
1
0
Selected Packet: 30,958 Adv Type: SCAN_RSP Timestamp: 3/14/2013 12:18:17.
4.634 ms
18.66 ms
4.506 ms
18.308 ms
Swap
Packet Throughput
3,820
3,056
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

Frame Display is synchronized with the selected packet.

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
	30,963	39	SCAN_RSP			(pub)	0x727272727272	6	21	00:0

Figure 4.37 - **low energy Timeline** and **Frame Display** Packet Synchronization

4.3.2.11 low energy Timeline Visual Elements

The low energy Timeline consists of the following visual elements:

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

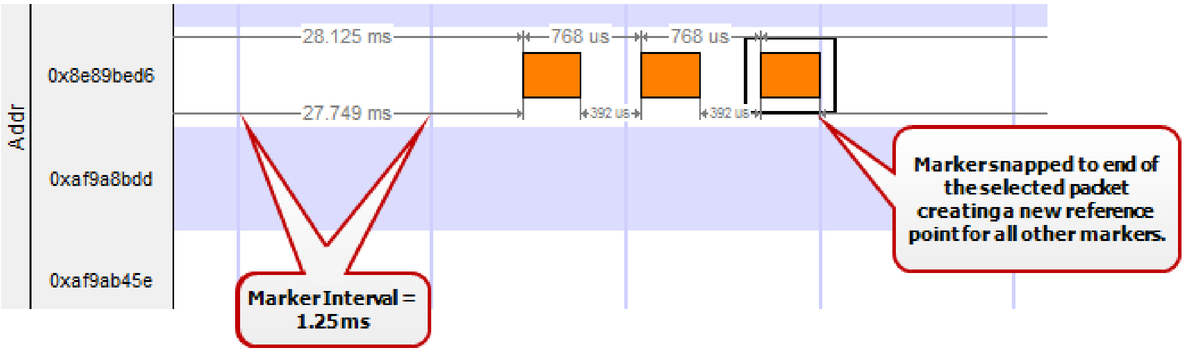


Figure 4.38 - Timeline Markers Shown Snapped to End of Packet

- 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.

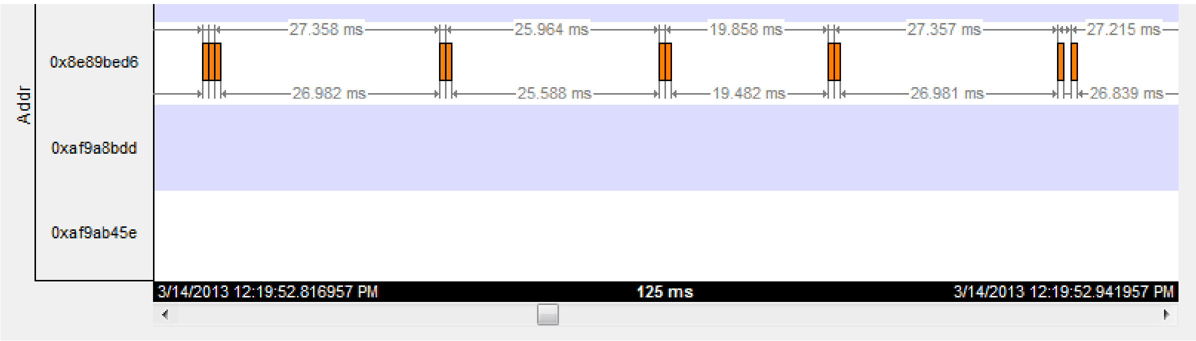
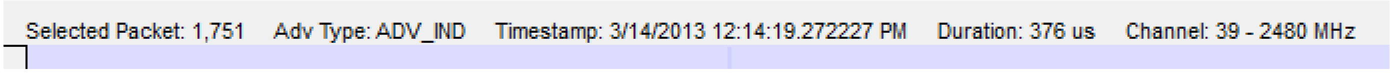


Figure 4.39 - Bluetooth le Timeline Segment Timestamp and Zoom Value

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

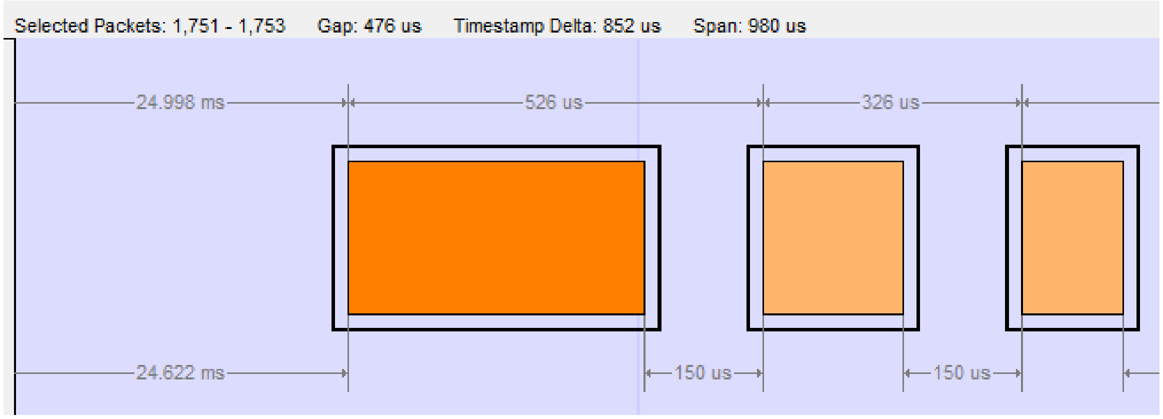
- Packet Info Line - The packet info line appears just above the timeline and displays information for the currently selected packet.



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 4.40 - 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



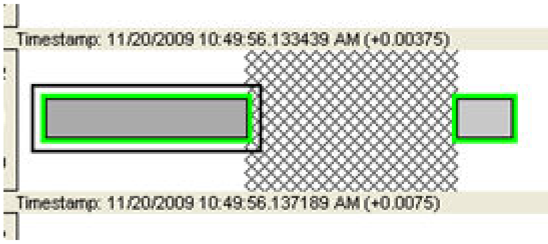
Selected Packets: 1,751 - 1,753 Gap: 476 us Timestamp Delta: 852 us Span: 980 us

Figure 4.41 - 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 .

4.3.2.12 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 4.42 - 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.

4.3.2.13 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.

4.3.2.14 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)".

4.3.2.15 Zoom menu

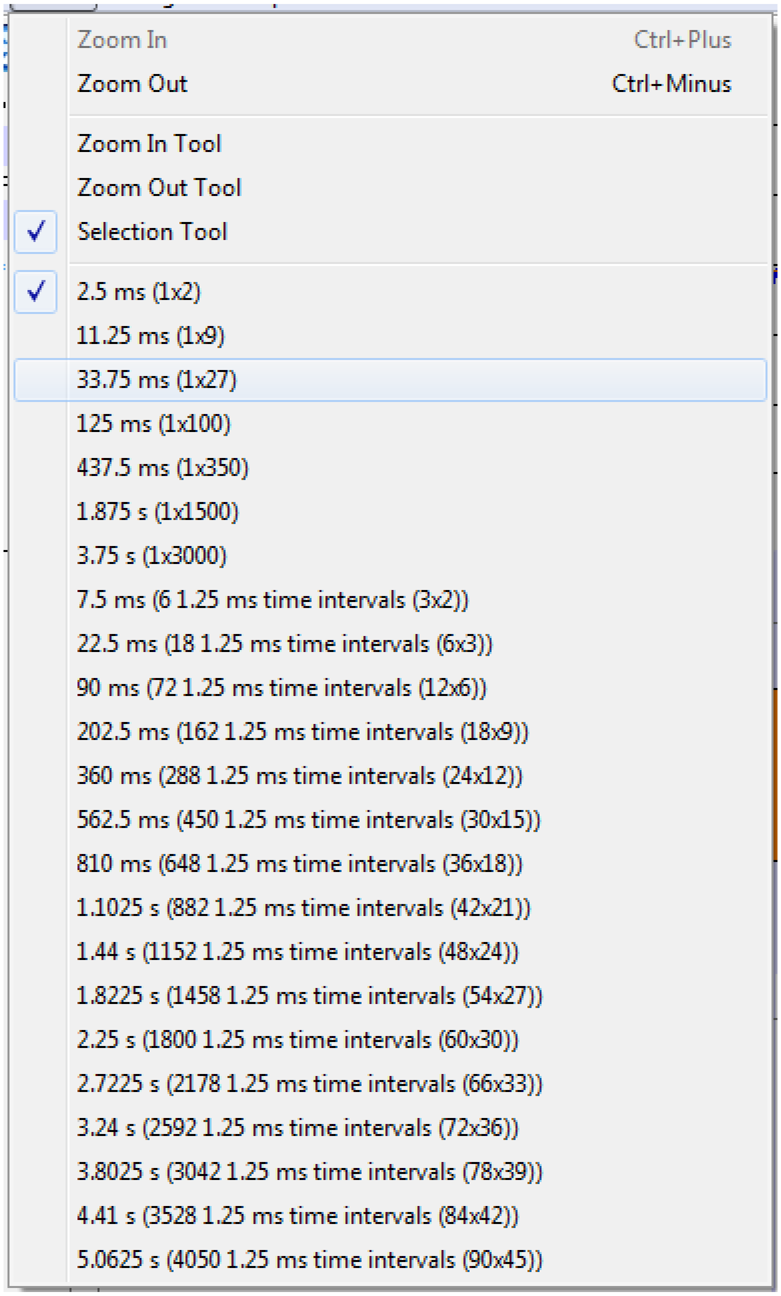
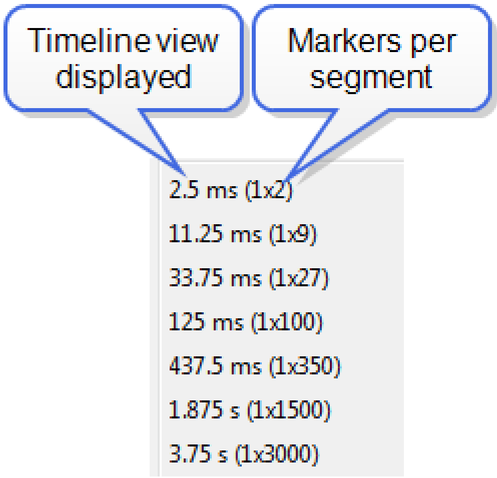

Zoom In Ctrl+Plus
Zoom Out Ctrl+Minus
Zoom In Tool
Zoom Out Tool
✓ Selection Tool
✓ 2.5 ms (1x2)
11.25 ms (1x9)
33.75 ms (1x27)
125 ms (1x100)
437.5 ms (1x350)
1.875 s (1x1500)
3.75 s (1x3000)
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (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 4.43 - low energy Timeline Zoom menu

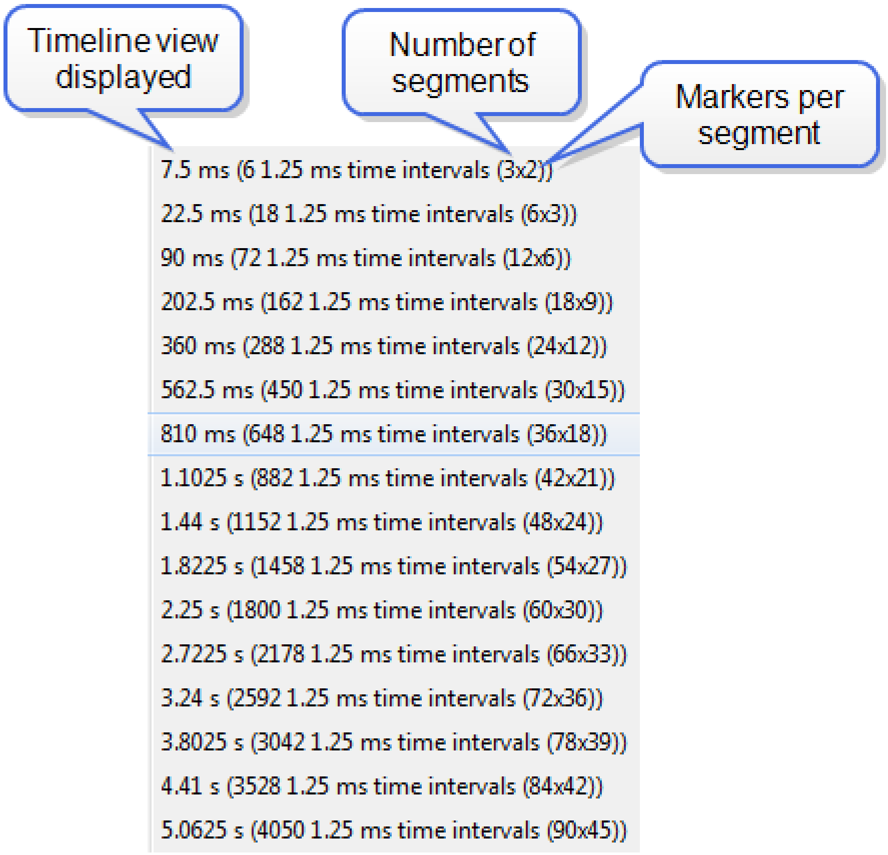
4.3.2.16 Single Segment Zoom



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.

4.3.2.17 Multiple Segments

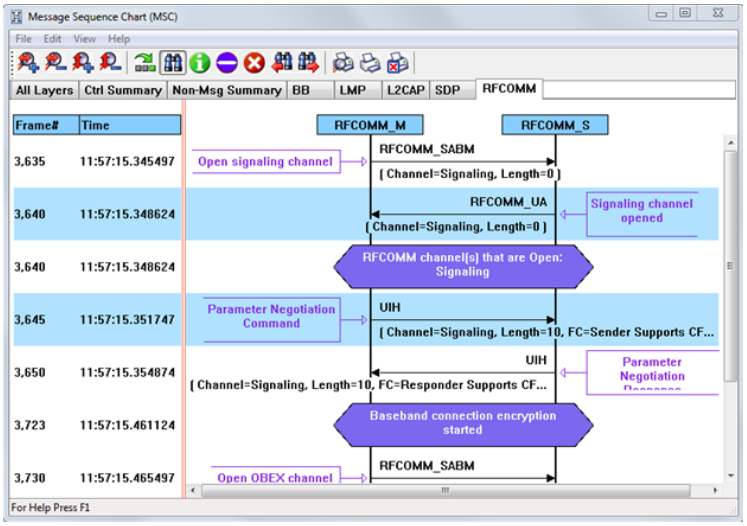

Timeline view displayed
Number of segments
Markers per segment
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (12x6))
202.5 ms (162 1.25 ms time intervals (18x9))
360 ms (288 1.25 ms time intervals (24x12))
562.5 ms (450 1.25 ms time 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.

4.3.3 Message Sequence Chart (MSC)

The **Message Sequence Chart** (MSC) displays information about the messages passed between protocol layers. MSC displays a concise overview of a *Blutetooth* connection, highlighting the essential elements fo the connection. At a glance, you can see the flow of the data including role switches, connection requests, and errors. You can look at all the packets int he capture, or filter by protocol or profile. the MSC is color coded for a clear and easy view of your data.



3,635 11:57:15.345497 Open signaling channel RFCOMM_SABM (Channel=Signaling, Length=0)

3,640 11:57:15.348624 RFCOMM_UA (Channel=Signaling, Length=0) Signaling channel opened

3,640 11:57:15.348624 RFCOMM channel(s) that are Open: Signaling

3,645 11:57:15.351747 Parameter Negotiation Command UIH (Channel=Signaling, Length=10, FC=Sender Supports CF...

3,650 11:57:15.354874 UIH (Channel=Signaling, Length=10, FC=Responder Supports CF... Parameter Negotiation

3,723 11:57:15.461124 Baseband connection encryption started

3,730 11:57:15.465497 Open OBEX channel RFCOMM_SABM

Figure 4.44 - Message Sequence Chart Window

How do I access the chart?

You access the **Message Sequence Chart** by selecting the icon or **MSC Chart** from the **View** menu from the **Control** window or **Frame Display**.

What do I see on the dialog?

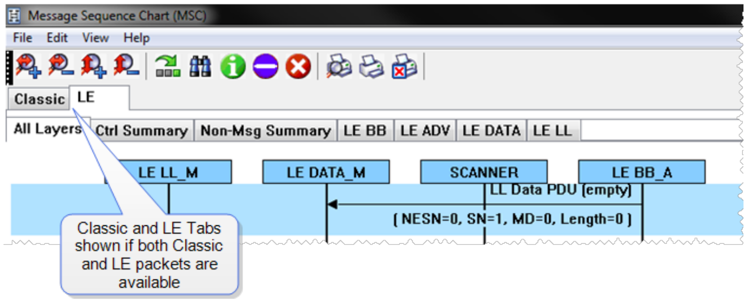
At the top of the dialog you see four icons that you use to zoom in and out of the display vertically and horizontally. The same controls are available under the **View** menu.

There are three navigation icons also on the toolbar.

ℹ	This takes you to the first Information Frame.

⊖	This takes you to first Protocol State Message.
⊗	This takes you to the first Error Frame. Click here to learn more about this option.

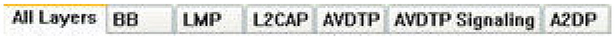
If there is both Classic and low energy packets, there will be a **Classic** and **LE** tab at the top of the dialog.



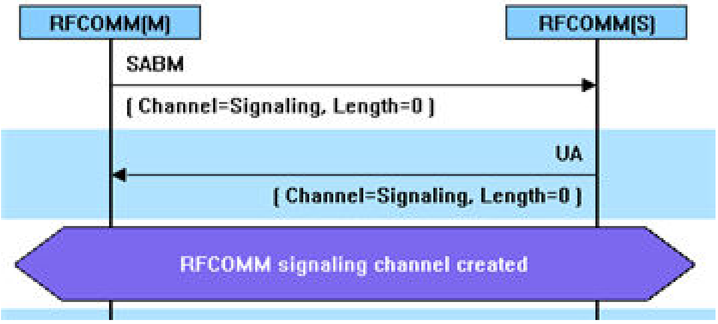
Classic and LE Tabs shown if both Classic and LE packets are available

Figure 4.45 - Classic and LE tabs

If the **Classic** tab is selected, you will see Classic protocols. If you select the **LE** tab, you will see LE Protocols. If there is only Classic or only LE, the Classic and LE tabs will not appear.



Also along the top of the dialog are a series of protocol tabs. The tabs will vary depending on the captured protocols.


RFCOMM[M]
RFCOMM[S]
SABM
(Channel=Signaling, Length=0)
UA
(Channel=Signaling, Length=0)
RFCOMM signaling channel created

Clicking on a tab displays the messaging between the master and slave for that protocol. For example, if you select **RFCOMM**, you will see the messaging between the **RFCOMM{M}** Master, and the **RFCOMM{S}** Slave.

The Non-Message Summary tab displays all the non-message items in the data.

The **Ctrl Summary** tab displays the signaling packets for all layers in one window in the order in which they are received.

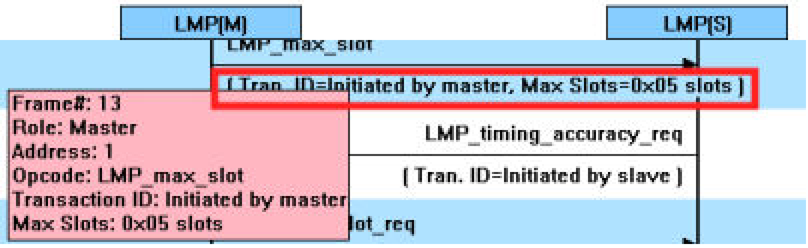
The information in the colored boxes displays general information about the messaging. The same is true for each one of the protocols.

If you want to see the all the messaging in one dialog, you select the **All Layers** tab.

When you move the mouse over the message description you see an expanded tool tip.

If you position the cursor outside of the message box, the tool tip will only display for a few seconds.

If, however, you position the cursor within the tool tip box, the message will remain until you move the cursor out of the box.

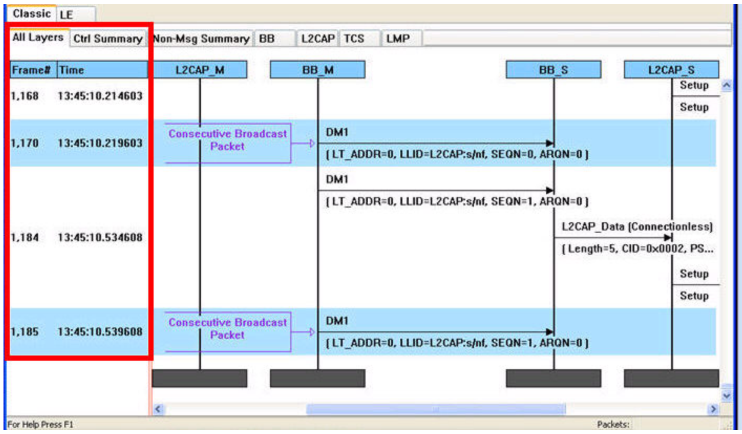

LMP[M]
LMP[S]
LMP_max_slot
[Tran. ID=Initiated by master, Max Slots=0x05 slots]
LMP_timing_accuracy_req
[Tran. ID=Initiated by slave]
lot_req

Frame#: 13
Role: Master
Address: 1
Opcode: LMP_max_slot
Transaction ID: Initiated by master
Max Slots: 0x05 slots

Additionally, If you right click on a message description, you will see the select Show all Layers button.

When you select **Show all Layers**, the chart will display all the messaging layers.

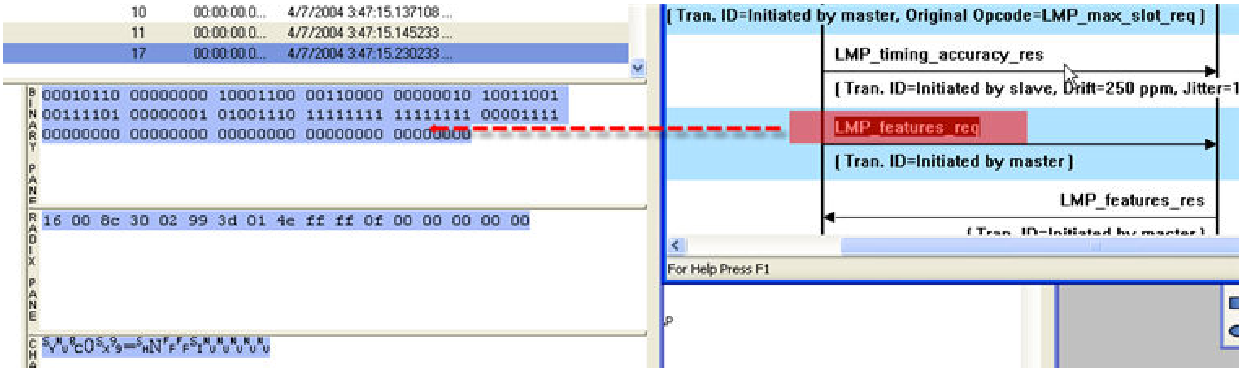
The **Frame#** and **Time** of the packets are displayed on the left side of the chart.


Classic
LE
All Layers
Ctrl Summary
Non-Msg Summary
BB
L2CAP
TCS
LMP
L2CAP_M
BB_M
BB_S
L2CAP_S
Setup
Consecutive Broadcast Packet
DM1
[LT_ADDR=0, LLID=L2CAP:s/nl, SEQN=0, ARQN=0]
[LT_ADDR=0, LLID=L2CAP:s/nl, SEQN=1, ARQN=0]
L2CAP_Data [Connectionless]
[Length=5, CID=0x0002, PS...
For Help Press F1
Packets:

Frame#	Time
1,168	13:45:10.214603
1,170	13:45:10.219603
1,184	13:45:10.534608
1,185	13:45:10.539608

Figure 4.46 - Frame# and Time Display, inside red box.

If you click on the description of the message interaction, the corresponding information is highlighted in Frame Display.


[Tran. ID=Initiated by master, Original Opcode=LMP_max_slot_req]
LMP_timing_accuracy_res
[Tran. ID=Initiated by slave, Drift=250 ppm, Jitter=1
LMP_features_req
[Tran. ID=Initiated by master]
LMP_features_res
[Tran. ID=Initiated by master]
BINARY PANE
RADIX PANE
CHA
For Help Press F1

```
10   00:00:00.0...   4/7/2004 3:47:15.137108 ...
11   00:00:00.0...   4/7/2004 3:47:15.145233 ...
17   00:00:00.0...   4/7/2004 3:47:15.230233 ...

00010110 00000000 10001100 00110000 00000010 10011001
00111101 00000001 01001110 11111111 11111111 00001111
00000000 00000000 00000000 00000000 00000000

16 00 8c 30 02 99 3d 01 4e ff ff 0f 00 00 00 00 00
```

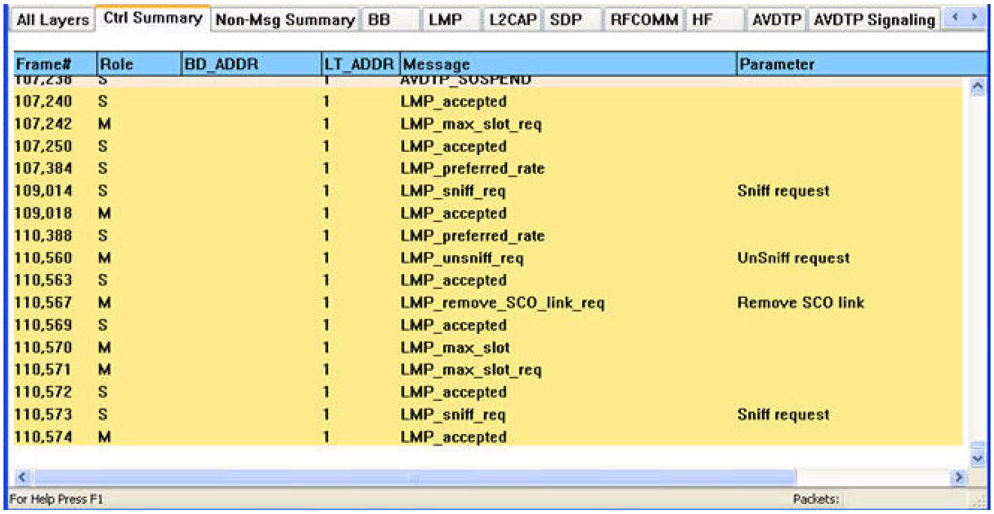
Figure 4.47 - MSC Synchronization with Frame Display

How do I navigate in the dialog?

You can use the navigation arrows at the bottom and the right side of the dialog to move vertically and horizontally. You can also click and hold while moving the pointer within dialog that brings up a directional arrow that you can use to move left/right and up/down.

Ctrl Summary tab

When you select the **Ctrl Summary tab** you will see a summary of the control and signaling frames in the order that they are received/transmitted from and to devices.

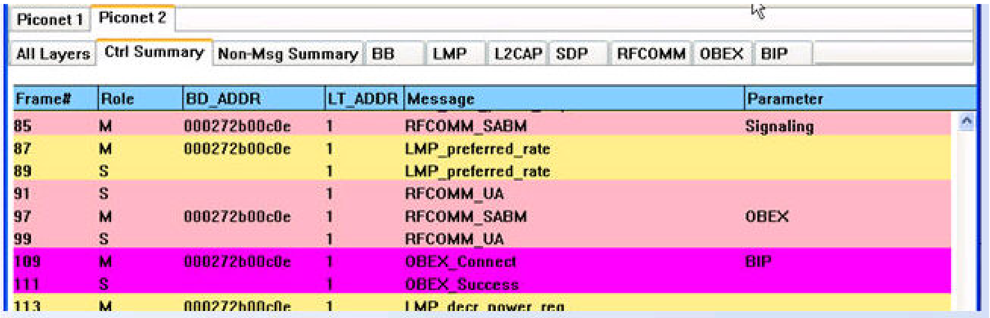


Frame#	Role	BD_ADDR	LT_ADDR	Message	Parameter
107,238	S		1	AVDTP_SUSPEND	
107,240	S		1	LMP_accepted	
107,242	M		1	LMP_max_slot_req	
107,250	S		1	LMP_accepted	
107,384	S		1	LMP_preferred_rate	
109,014	S		1	LMP_sniff_req	Sniff request
109,018	M		1	LMP_accepted	
110,388	S		1	LMP_preferred_rate	
110,560	M		1	LMP_unsniff_req	UnSniff request
110,563	S		1	LMP_accepted	
110,567	M		1	LMP_remove_SCO_link_req	Remove SCO link
110,569	S		1	LMP_accepted	
110,570	M		1	LMP_max_slot	
110,571	M		1	LMP_max_slot_req	
110,572	S		1	LMP_accepted	
110,573	S		1	LMP_sniff_req	Sniff request
110,574	M		1	LMP_accepted	

Figure 4.48 - Control and Signaling Frames Summay

The frame numbered is shown, whether the message comes from the Master or Slave, the message Address, the message itself, and the timestamp.

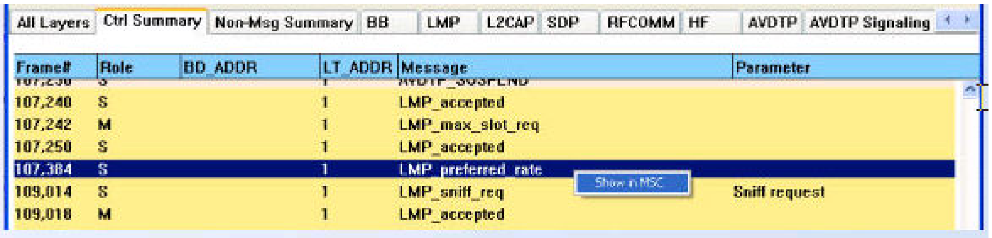
Additionally, the control/signaling packets for each layer are shown in a different background color.



Frame#	Role	BD_ADDR	LT_ADDR	Message	Parameter
85	M	000272b00c0e	1	RFCOMM_SABM	Signaling
87	M	000272b00c0e	1	LMP_preferred_rate	
89	S		1	LMP_preferred_rate	
91	S		1	RFCOMM_UA	
97	M	000272b00c0e	1	RFCOMM_SABM	OBEX
99	S		1	RFCOMM_UA	
109	M	000272b00c0e	1	OBEX_Connect	BIP
111	S		1	OBEX_Success	
113	M	000272b00c0e	1	LMP_decr_power_req	

Figure 4.49 - Packet Layers Shown in Different Colors

If you right click within the **Ctrl Summary**, you can select **Show in MSC**.



Frame#	Role	BD_ADDR	LT_ADDR	Message	Parameter
107,240	S		1	LMP_accepted	
107,242	M		1	LMP_max_slot_req	
107,250	S		1	LMP_accepted	
107,384	S		1	LMP_preferred_rate	
109,014	S		1	LMP_sniff_req	Sniff request
109,018	M		1	LMP_accepted	

Figure 4.50 - Right-Click in Ctrl Summary to Display Show in MSC

The window then displays the same information, but in the normal MSC view.

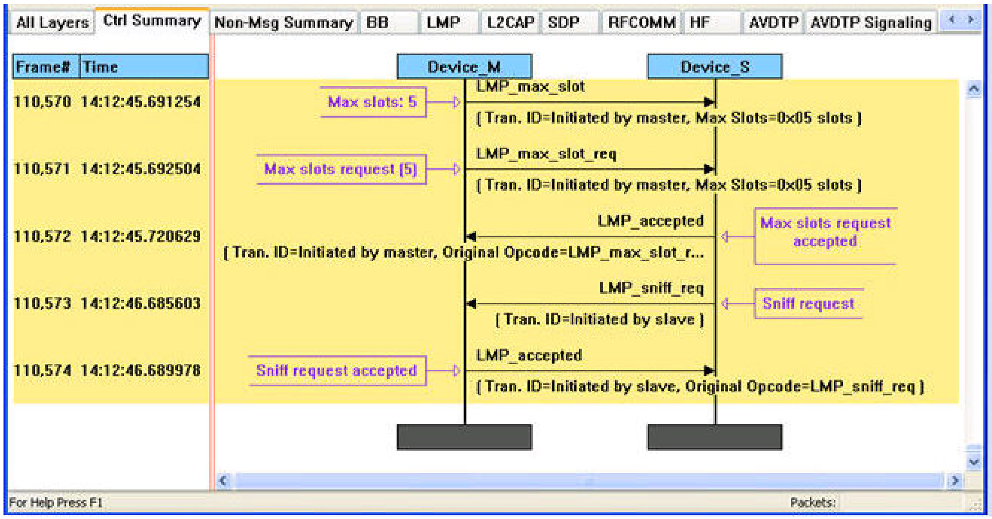


Figure 4.51 - MSC View of Selected Packet from Ctrl Summary

You can return to the text version by using a right click and selecting **Show in Text.**

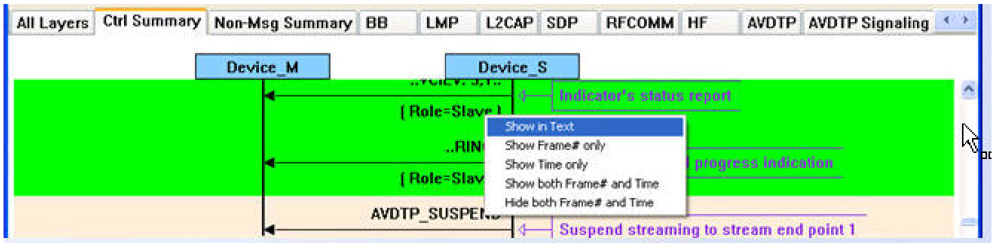


Figure 4.52 - Return to Text View Using Right-Click Menu

You can also choose to show:

- Frame # only
- Time only
- Show both Frame# and Time
- Hide both Frame# and Time

4.3.3.1 Message Sequence Chart Toolbar

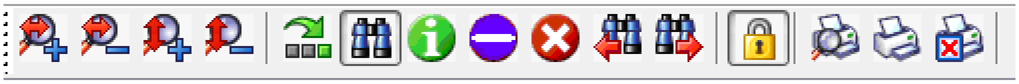


Figure 4.53 - Message Sequence Chart Toolbar

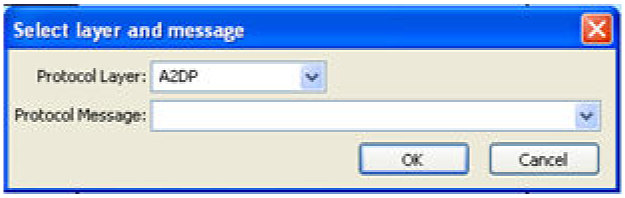
Table 4.6 - Message Sequence Chart Tools

Tool	Keyboard	Description
	Ctrl + H	Zoom in horizontal - expands the chart horizontal view
	Shift + H	Zoom out horizontal - compresses the chart horizontal view
	Ctrl + V	Zoom in vertical - expands the chart vertical view
	Shift + V	Zoom out vertical - compresses the chart vertical view
	Shift + F	Go to frame
	F3	Search
	F2	Search for prior Search criteria.
	F4	search for Next criteria.
	Ctrl + I	Go to first information message
	Ctrl +S	Go to first protocol state message
	Ctrl +E	Go to first error frame
🔒 / 🔓	Shift + L	Lock / unlock the chart display. Clicking on the active icon or typing the keyboard command will toggle to the other state.
	Ctrl + W	Print display preview
	Ctrl + P	Print the display
	Ctrl + C	Cancel an in-process print

4.3.3.2 Message Sequence Chart - Search

The Message Sequence Chart has a Search function that makes it easy to find a specific type message within the layers.

When you select the 1) **Search** icon or 2) use **F3** key, the **Select layer and message** dialog appears.

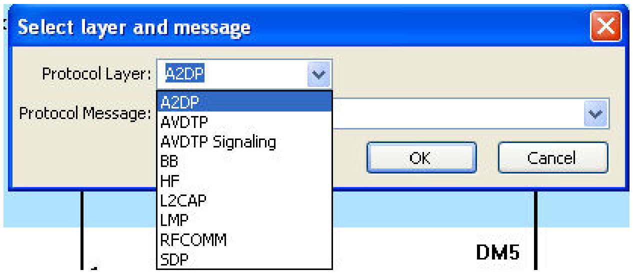


From this dialog you can search for specific protocol messages or search for the first error frame.

1. On the MSC dialog select one of the protocol tabs at the top.

> **Note:** If you select **All Layers** in Step 1, the Protocol Layers drop-down list is active. If you select any of the other single protocols, the Protocol Layers drop-down is grayed out.

2. Or Open the Search dialog using the Search icon or the **F3** key.
3. Select a specific Protocol Message from the drop-down list.
4. Once you select the Protocol Message, click **OK**



The Search dialog disappears and the first search result is highlight in the Message Sequence Chart.

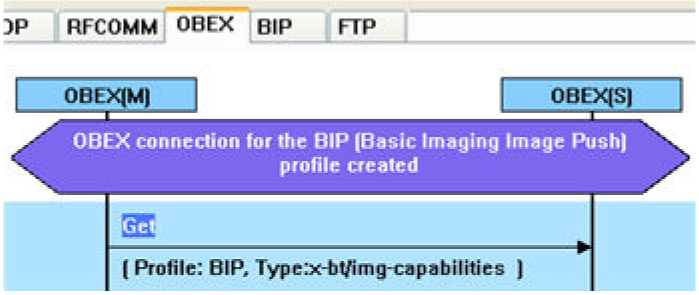
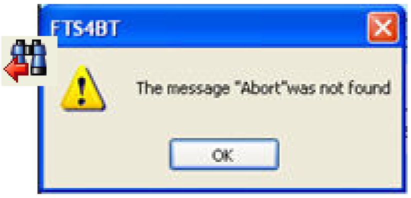

)P
RFCOMM
OBEX
BIP
FTP
OBEX(M)
OBEX(S)
OBEX connection for the BIP (Basic Imaging Image Push) profile created
Get
(Profile: BIP, Type:x-bt/img-capabilities)

Figure 4.54 - Highlighted First Search Result

If there is no instance of the search value, you see this following dialog.



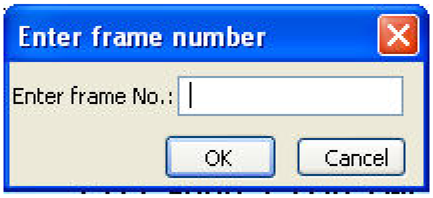
Once you have set the search value, you can 1) use the **Search Previous** and **Search Next** buttons or 2) **F2** and **F4** to move to the next or previous frame in the chart.

4.3.3.3 Message Sequence Chart - Go To Frame

The **Message Sequence Chart** has a **Go To Frame** function that makes it easy to find a specific frame within the layers.

In addition to Search, you can also locate specific frames by clicking on the **Go To Frame** toolbar icon.

1. Click **Go To Frame** in the toolbar.
2. Enter a frame number in the **Enter frame No.:** text box.
3. Click **OK**.

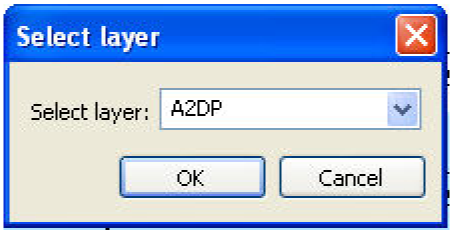


The Go To Frame dialog disappears and the selected frame is highlighted in the chart.

Once you have identified the frame in Go To, you can 1) use the Search Previous and Search Next buttons or 2) **F2** and **F4** keys to move to the next or previous frame in the chart.

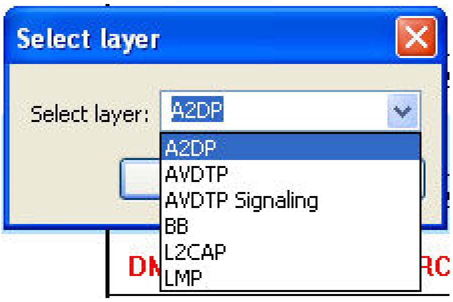
4.3.3.4 Message Sequence Chart - First Error Frame

When you select **Go to first error frame** from the toolbar , the **Select layer** dialog appears.



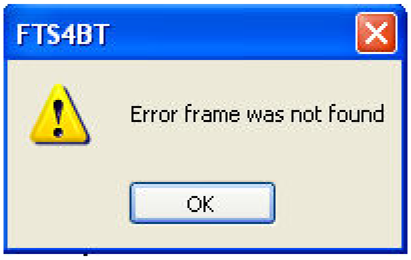
Select layer: A2DP

You have to select a layer from the drop down list to choose what layer you want to search for the error.



Once you select a layer, then **OK**, the first error for that layer will be displayed.

If no error is found, a dialog will announce that event.



FTS4BT

Error frame was not found

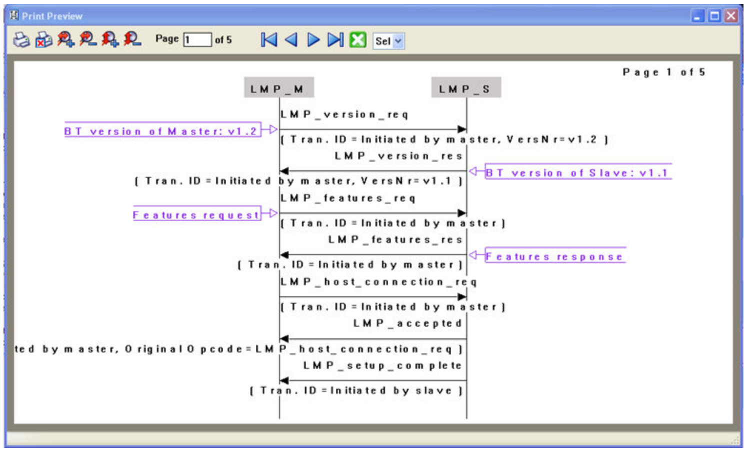
4.3.3.5 Message Sequence Chart - Printing

There are three standard MSC print buttons. **Print Preview**, **Print**, and **Cancel Printing**.

Print Preview

1. When you select **Print Preview**, the **Print Setup** dialog appears.
2. You next need to select your printer from the drop-down list, set printer properties, and format the print output..
3. Then you select **OK**.

After you select **OK**, the **Message Sequence Chart Print Preview** dialog appears.



Print Preview
Page 1 of 5
Sel
Page 1 of 5
LMP_M
LMP_S
LMP_version_req
BT version of Master: v1.2
[Tran. ID = Initiated by master, VersNr=v1.2]
LMP_version_res
BT version of Slave: v1.1
[Tran. ID = Initiated by master, VersNr=v1.1]
LMP_features_req
Features request
[Tran. ID = Initiated by master]
LMP_features_res
Features response
[Tran. ID = Initiated by master]
LMP_host_connection_req
[Tran. ID = Initiated by master]
LMP_accepted
ted by master, OriginalOpcode=LMP_host_connection_req]
LMP_setup_complete
[Tran. ID = Initiated by slave]

Figure 4.55 - Message Sequence Chart Print Preview

The information in the dialog will vary depending on the layer that is selected in the Message Sequence Chart, the properties of the printer you select, and the amount of data in the layer (which will correspond to the number of pages displayed).

You control what you see and when to print using the toolbar at the top of the dialog.

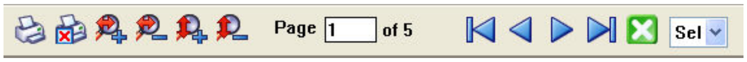


Figure 4.56 - Print Preview Toolbar

Table 4.7 - Print Preview Icons

Icon	Name	Description
🖨	Print	Prints all the pages to the printer you select in Print Setup dialog. When you select Print, you will output the data that is currently being displayed.
🖨 ☒	Cancel Printing	Cancels the current printing.
🔍+ 🔍− 🔍+ 🔍−	Zoom In Horizontally	Expands the data horizontally so it can be easier to read.
	Zoom Out Horizontally	Squeezes the data together so that more fits on one page.
	Zoom In Vertically	Expands the data vertically so it can be easier to read.
	Zoom Out Vertically	Squeezes the data so that more fits on one page.
Page 1 of 5	Current Page	The current page text box displays the page number this is currently shown in the dialog. You can enter a number in the text box, then press Enter, and the dialog will display the data for that page.
⏮ ◀ ▶ ⏭	Page navigation	If the data requires multiple pages, the navigation buttons will take you to: • The first page • The previous page • The next page • The last page
☒	Close Print Preview	Closes the dialog and returns to the Message Sequence Chart
Sel ▾	Select Font Size	Allows selection of the print font size from the drop-down control.

4.4 Packet Error Rate Statistics

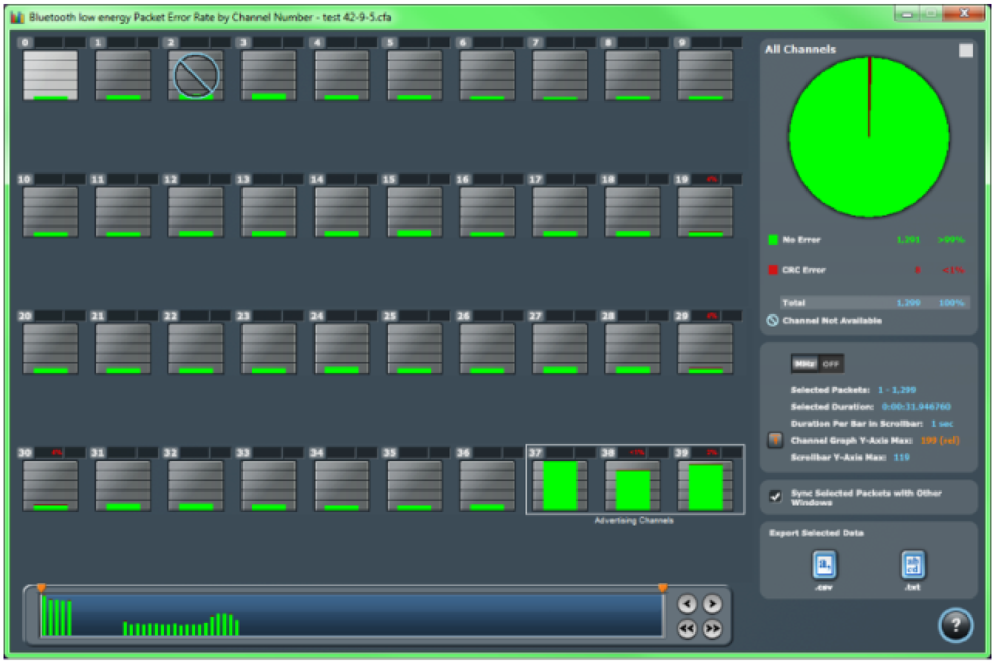
The **Packet Error Rate** (PER) Stats view provides a dynamic graphical representation of the Packet Error Rate for each channel. The dialog displays a graph for each *Bluetooth* low energy channel numbered 0 through 39.

Packet Error Rate Stats assist in detecting bad communication connections. When a high percentage of re-transmits, and/or header/payload errors occur, careful analysis of the statistics indicate whether the two devices under test are experiencing trouble communicating, or the packet sniffer is having difficulty listening.

Generally, if the statistics display either a large number of re-transmits with few errors or an equal number of errors and re-transmits, then the two devices are not communicating clearly. However, if the statistics display a large number of errors and a small number of re-transmits, then the packet sniffer is not receiving the transmissions clearly.

You can access this window in *Bluetooth* low energy by selecting the ***Bluetooth* low energy Packet Error Rates Statistics** icon from the **Control** window or **Frame Display**. You can also open the window from the View menu on the same windows.

Bluetooth low energy Packet Error Rate



🟩 No Error	1,291	>99%
🟥 CRC Error	8	<1%
Total	1,299	100%

Channel Not Available

Selected Packets: 1 - 1,299
Selected Duration: 0:00:11.946760
Duration Per Bar in Scrollbar: 1 sec
Channel Graph Y-Axis Max: 199 (rel)
Scrollbar Y-Axis Max: 119

☑ Sync Selected Packets with Other Windows

Figure 4.57 - *Bluetooth* low energy PER Stats Window

4.4.1 Packet Error Rate - Channels

The main portion of the PER Stats dialog displays the 40 individual channels, 0-39, for *Bluetooth* low energy.

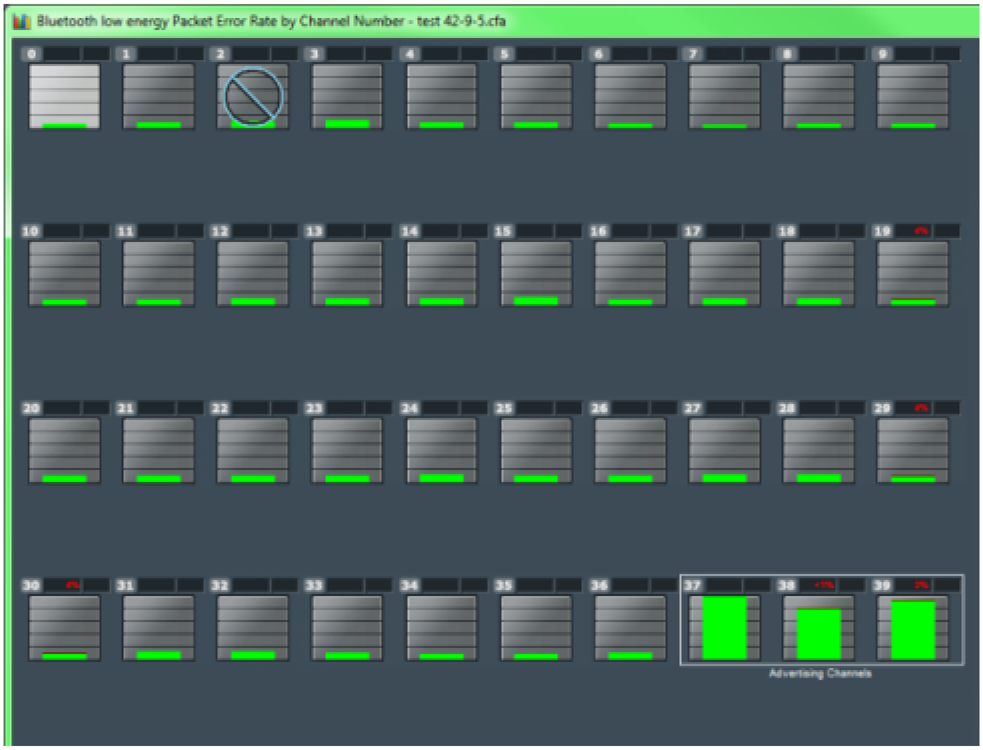
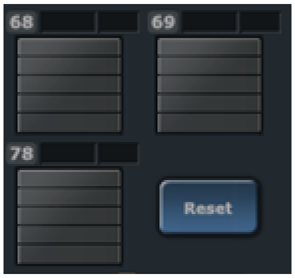


Figure 4.58 - *Bluetooth* low energy Packet Error Rate Channels

- The red number at the top of the channel shows the percentage of Header Error and Payload/CRC Errors in relationship to the total number of packets in the channel.
- The light blue number at the top of each channel shows the megahertz (MHz) for the channel if the option is chosen in the Additional Statistics section.
- When you select a channel, detailed information for that channel is displayed in the expanded chart on the upper right.
- The channels change dynamically as the Viewport is moved or new data appears within the Viewport.
- The **Channel Not Available** symbol is displayed if the channel is not available in the most recent channel map that is in or before the last selected packet, even if that channel map comes before the first selected packet. *Bluetooth* Adaptive Frequency Hopping processes will block channels determined to be unreliable. These channels are not available because the Bluetooth devices have decided not to use them.

- "s" changes the size of the entire dialog.
- "c" changes the contrast of the dialog

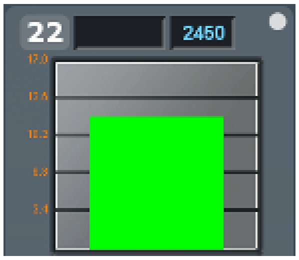
- The **Reset** button is only available in live mode. The button will appear in the lower right-hand corner of the Channels section. Clicking on the **Reset** button will clear all prior data from PER Stats.



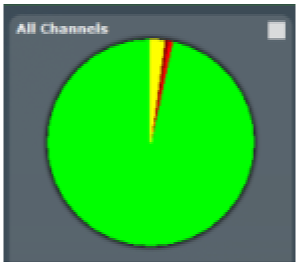
4.4.2 Packet Error Rate - Pie Chart and Expanded Chart

The **Expanded PER Stats Chart** (in the upper right) displays detailed information about the channel selected from the main channel dialog.

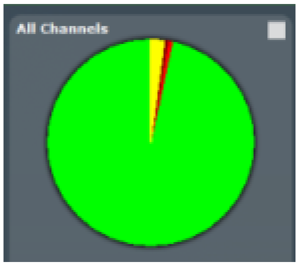
Expanded Chart



Pie Chart



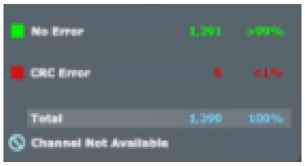
- When PER Stats is first opened, Channel 0 is displayed in the expanded chart.
- The top orange number on the Y-Axis displays the maximum number of packets in Snap Mode. If Snap Mode is turned off, the number will display in light blue. For information about Snap Mode, seePacket Error Rate - Additional Statistics on the facing page
- The number of the selected channel is displayed in the upper-left corner of the expanded chart.
- The combined value of Header and Payload/CRC errors for the channel is displayed in red as a percentage to the right of the channel number.
- The megahertz (MHz) value is displayed in light blue text if the MHz option is selected in the Additional Statistics section.
- The number of packets with no errors is displayed in light green in the bar chart.
- All the values, except MHz, change dynamically when multiple time periods are selected in the Packet Error Rate - Scroll Bar on page 143.
- When you select the ● in the upper-right corner, the bar chart is replaced by a pie chart. The pie chart applies to all channels, not a selected channel. To return to the bar chart, click on the channel again or click on the □ in the upper right hand corner.



4.4.3 Packet Error Rate - Legend

The **Legend** displays color coded information about the channel selected.

Bluetooth low energy



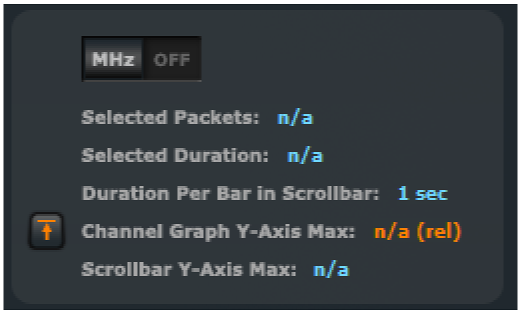
🟩	No Error	1,291	>99%
🟥	CRC Error	8	<1%
	Total	1,299	100%
⃠	Channel Not Available		

For *Bluetooth* low energy:

- The number of Packets with **No Errors** and percentage of packets with **No Errors** in relationship to total packets for the channel is displayed in green.
- The number of Packets with **CRC Errors** and percentage of packets with **CRC Errors** in relationship to total packets for the channel is displayed in dark red.
- **Total** packets and **Total** percentage is displayed in light blue.

For a description of the **Channel Not Available** symbol, see PER Stats Channel.

4.4.4 Packet Error Rate - Additional Statistics



MHz OFF

Selected Packets: n/a

Selected Duration: n/a

Duration Per Bar in Scrollbar: 1 sec

Channel Graph Y-Axis Max: n/a (rel)

Scrollbar Y-Axis Max: n/a

This Additional Statistics section of PER Stats displays information about selected packets, duration, and Y-Axis max, and it also has two controls.

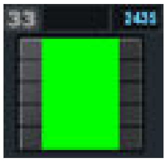
- Selecting **MHz On** ON MHz displays the megahertz value for each channel in the main channels chart and also in the expanded chart.
- Selecting **MHz Off** MHz OFF removes the megahertz value.
- **Selected Packets** displays the packet range selected in the Scroll Bar. This includes inapplicable packets.

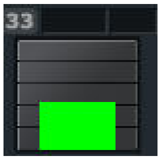
Inapplicable packets include Wi-Fi packets, Sniffer Debug packets, any packets that are not relevant to PER Stats. Inapplicable packets do not appear as part of the Additional Statistics. packets.

- **Selected Duration** identifies the total amount of time in the selected packet range displayed in the Scroll Bar.
- **Duration Per Bar in Scrollbar:** identifies the amount of time represented by each bar in the Scroll Bar.
- The **Channel Graph Y-Axis Max** can display two different values. When the **Snap Arrow** is orange , the values for channels in the main chart are shown in relative terms in **Snap Mode**. This means that one channel (or channels) with the greatest value is "snapped" to the top of the chart. In the graphic below left,

Channel 33 is snapped to the top of the chart.

The channel(s) with the greatest value become a full-scale reference display for the other channels that have been relatively scaled. Channel comparisons become easier. With Snap On you can select multiple time values in the Scroll Bar. When the **Snap Arrow** is white (Snap Mode turned off), the values for channels in the main chart are shown in absolute values where the max value of each channel graph is the same regardless of the position of the Viewport. Channel 33, which is snapped to the top of the chart in Snap Mode (shown above left), appears like the right image when Snap Mode is turned off.





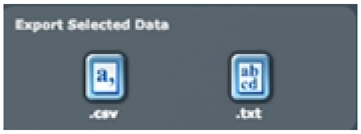
- **Scrollbar Y-Axis Max** displays the maximum Y-Axis value in the Scroll Bar.

4.4.5 Packet Error Rate - Sync Selected Packets With Other Windows

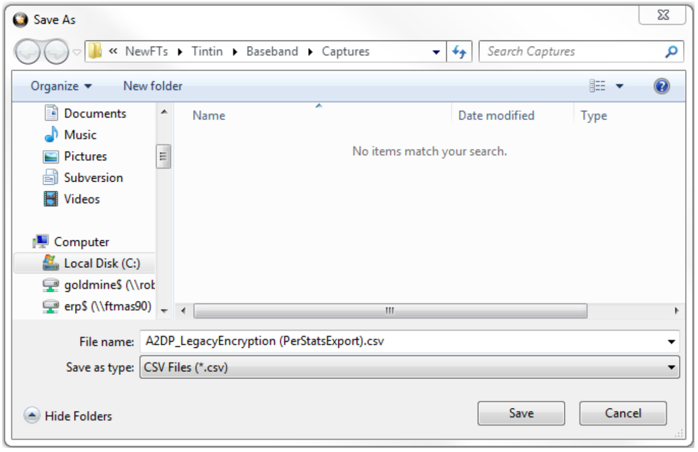
By default, and unlike other windows, PER Stats is not synchronized with other windows such as Frame Display in that selecting a frame range in one does not highlight the same frame range in the other. This ensures that **Frame Display** isn’t constantly re-synchronizing during live capture while the view-port is maximized in PER Stats. If PER Stats synchronization is desired, it can be enabled by checking the **Sync Selected Packets with Other Windows** check box.

4.4.6 Packet Error Rate - Export

The Export section of PER Stats allows you to export data to a .csv or .txt file.



1. To use the Export, select a range of data using the Viewport.
2. Select .csv or .txt from **Export Selected Data**, depending on what type of data file you want. The **Save As** dialog appears.



File name: A2DP_LegacyEncryption (PerStatsExport).csv

Save as type: CSV Files (*.csv)

Figure 4.59 - Save As dialog in PER Stats Export

3. Select a location where you want to save the file in "Save in:".

4. Enter a file name in "File name:".

5. Select "Save".

The file will be saved to that location.

4.4.7 Packet Error Rate - Scroll Bar

The PER Stats **Scroll Bar** displays stats for all packets, divided into equal time intervals.

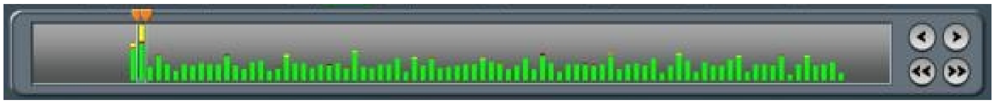
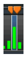
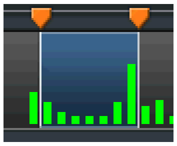
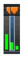
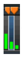


Figure 4.60 - PER Stats Scroll Bar

- Captured data begins to appear on the left and fills the width of the bar, left to right.
- The vertical bars in the **Scroll Bar** each indicate a fixed duration. When data first appears in the **Scroll Bar** as it is being captured, each bar equals one second. When the data fills the bar, reaching the right side limit, the last bar moves back to the center of the **Scroll Bar**. The bars stay the same size, but doubles in duration (for example, the first time the **Scroll Bar** fills, the bars return to the middle, but now each bar represent two seconds of time instead of one). Each time the bars cycle to the middle, the time they represent doubles. When the bars move and the **Viewport** (see below) is not maximized, the **Viewport** moves with the bars so that the same packet range is indicated. When the **Viewport** is maximized it stays maximized regardless of what the bars do. This ensures that the display can be made to reflect all packets at all times by maximizing the .
- The **Viewport** is used to select single  or multiple vertical bars  .
- You can drag the sides of the **Viewport** or the slider buttons to select multiple bars, representing a greater time range.
- You can click and drag the **Viewport** within the **Scroll Bar**.
- When you select a packet range in **Frame Display** that includes only some of the frames in PER Stats, the **Viewport** snaps up against the side of the bar with the unselected frames .
- When you select a packet range in Frame Display that includes all of the frames in PER Stats, the Viewport displays a space between the Viewport sides and the bar .
- Double clicking anywhere inside the **Scroll Bar** selects the entire **Scroll Bar**. Double clicking again toggles back to the previous size of the **Viewport**.
- Selecting Ctrl+A is the same as double-clicking.
- Clicking on a vertical bar left justifies the **Viewport** to that bar.
- Shift-clicking on a bar extends the nearest **Viewport** side to include that bar.

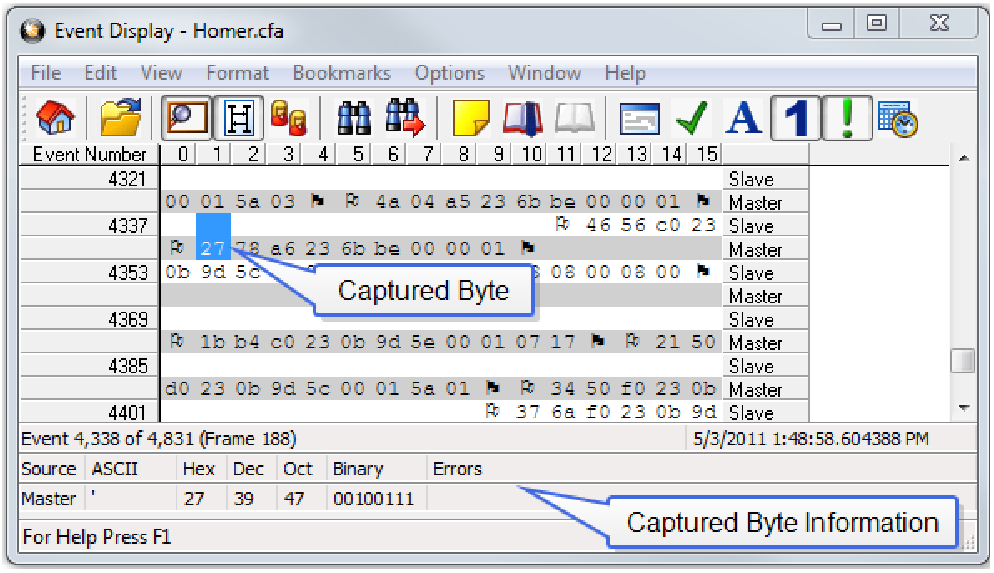
- The Home key moves the **Viewport** to the left edge.
- The End key moves the **Viewport** to the right edge.
- Pressing the left arrow button ◀, the left arrow key, or the up arrow key moves the **Viewport** to the left, one vertical bar at a time.
- Pressing the right arrow button ▶. the right arrow key, or the down arrow key moves the **Viewport** to the right, one vertical bar at a time.
- Pressing the double left arrow button ⏪ or the PgUp key moves the **Viewport** to the left by the current width of the **Viewport**. Holding down the Shift key will prevent the **Viewport** from moving if there is not enough room to move by its full width.
- Pressing the double right arrow button ⏩ or the PgDn key moves the **Viewport** to the right by the current width of the **Viewport**. Holding down the Shift key will prevent the **Viewport** from moving if there is not enough room to move by its full width.
- Holding the Shift key down and the right or left arrows moves the right side of the **Viewport**.
- Holding the Ctrl key down and the right or left arrows moves the left side of the **Viewport**.
- The Scroll bar includes inapplicable packets (sniffer debug, WiFi, etc) so that the packet range selected in Frame Display can be shown. Inapplicable packets are not, however, included in the statistics reports.
- If the **Viewport** is adjusted within PER Stats, as opposed to selecting a packet range in Frame Display, it uses only whole bars on both sides.
- Statistics are retained for all packets regardless of whether any of those packets have wrapped out. You can select the **Reset** button Reset, which is located above the right portion of the **Scroll Bar**, to discard all stats for packets received up to that point.
- The **Reset** button is only available when you are capturing data.

4.5 Analyzing Byte Level Data

4.5.1 Event Display

To open this window click the **Event Display** icon 🔍 on the **Control** window toolbar.

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


Event Display - Homer.cfa
File Edit View Format Bookmarks Options Window Help
Captured Byte
Captured Byte Information

```
Event Number   0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
4321                                                            Slave
              00 01 5a 03 ⚑  ⚐ 4a 04 a5 23 6b be 00 00 01 ⚑    Master
4337                                         ⚐ 46 56 c0 23     Slave
              ⚐ 27 78 a6 23 6b be 00 00 01 ⚑                   Master
4353          0b 9d 5c                  08 00 08 00 ⚑          Slave
                                                                Master
4369                                                            Slave
              ⚐ 1b b4 c0 23 0b 9d 5e 00 01 07 17 ⚑  ⚐ 21 50    Master
4385                                                            Slave
              d0 23 0b 9d 5c 00 01 5a 01 ⚑  ⚐ 34 50 f0 23 0b   Master
4401                                    ⚐ 37 6a f0 23 0b 9d    Slave
Event 4,338 of 4,831 (Frame 188)                5/3/2011 1:48:58.604388 PM
```

Source	ASCII	Hex	Dec	Oct	Binary	Errors
Master	'	27	39	47	00100111	

For Help Press F1

Figure 4.61 - Event Display

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

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

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

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

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

4.5.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Open a capture file

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

Clear- Discards the temporary file and clears the display.

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

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

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

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

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

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

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

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

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

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

Mixed Sides - (Serial data only) By default, the analyzer shows data with the DTE side above the DCE side. This is called DTE over DCE format. DTE data has a white background and DCE data has a gray background. The analyzer can also display data in mixed side format. In this format, the analyzer does not separate DTE data from DCE data but shows all data on the same line as it comes in. DTE data is still shown with a white background and DCE data with a gray background so that you can distinguish between the two. The benefit of using this format is that more data fits onto one screen.

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

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

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

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

4.5.3 Opening Multiple Event Display Windows

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

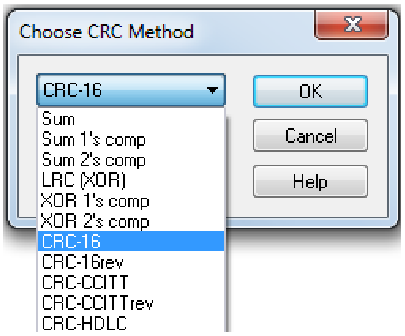
You can open as many **Event Display** windows as you like. Each **Event Display** is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

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

4.5.4 Calculating CRCs or FCSs

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

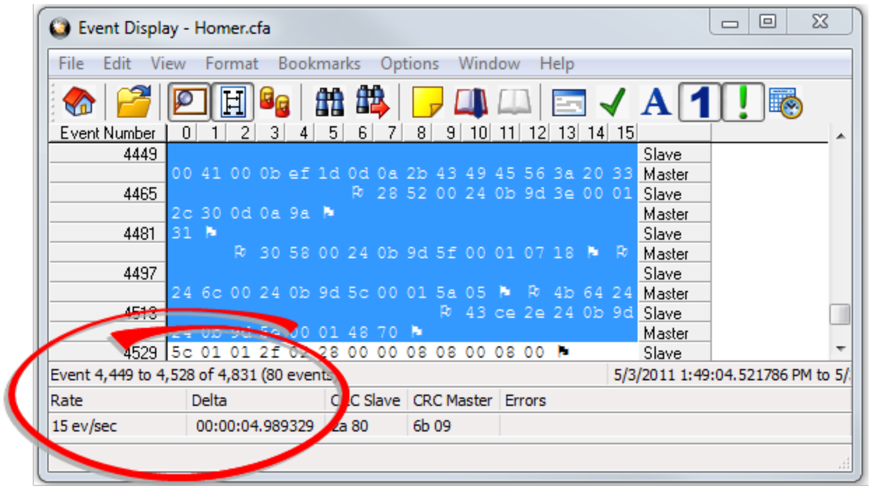
1. Open the **Event Display** 🔍 window.
2. Click and drag to select the data for which you want to generate a CRC.
3. Click on the **CRC** icon ✓.
4. In the **CRC** dialog box, click on the down arrow to show the list of choices for CRC algorithms..
5. Enter a **Seed** value in hexadecimal if desired.
6. Click **OK** to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC is calculated automatically.



Calculating CRC for interwoven data

4.5.5 Calculating Delta Times and Data Rates

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



```
Event Number | 0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
        4449 |                                                  Slave
             | 00 41 00 0b ef 1d 0d 0a 2b 43 49 45 56 3a 20 33 Master
        4465 |                      ⚑ 28 52 00 24 0b 9d 3e 00 01 Slave
             | 2c 30 0d 0a 9a ⚑                                  Master
        4481 | 31 ⚑                                              Slave
             |      ⚑ 30 58 00 24 0b 9d 5f 00 01 07 18 ⚑  ⚑     Master
        4497 |                                                  Slave
             | 24 6c 00 24 0b 9d 5c 00 01 5a 05 ⚑  ⚑ 4b 64 24   Master
        4513 |                            ⚑ 43 ce 2e 24 0b 9d   Slave
             | 24 0b 9d 5c 00 01 48 70 ⚑                         Master
        4529 | 5c 01 01 2f 02 28 00 00 08 08 00 08 00 ⚑          Slave
Event 4,449 to 4,528 of 4,831 (80 events)   5/3/2011 1:49:04.521786 PM to 5/
```

Rate	Delta	CRC Slave	CRC Master	Errors
15 ev/sec	00:00:04.989329	2a 80	6b 09	

Figure 4.62 - Delta fields

4.5.6 Switching Between Live Update and Review Mode

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

1. Make sure the **Lock** icon 🔒 is active so the display is locked and unable to scroll.

2. Click the **Unlock** 🔓 icon again to resume live update.

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

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

4.5.7 Data Formats and Symbols

4.5.7.1 Switching Between Viewing All Events and Viewing Data Events

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

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

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

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

See on page 151 for a list of all the special events shown in the analyzer and what they mean.

4.5.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the **radix**[1] used to display data.

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

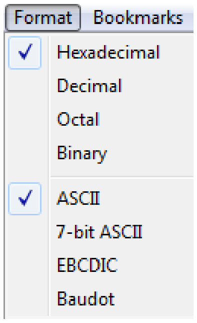


Figure 4.63 - Format Menu

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

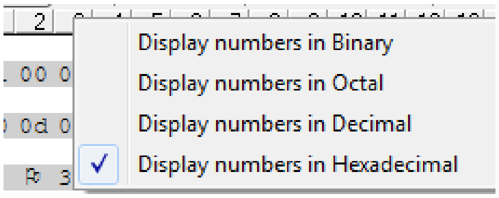

Display numbers in Binary
Display numbers in Octal
Display numbers in Decimal
✓ Display numbers in Hexadecimal

Figure 4.64 - Header labels, right click

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

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

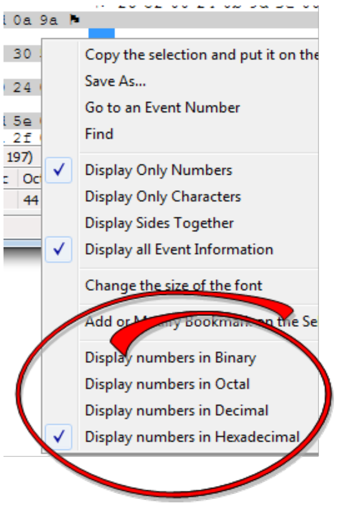

Copy the selection and put it on the
Save As...
Go to an Event Number
Find
✓ Display Only Numbers
Display Only Characters
Display Sides Together
✓ Display all Event Information
Change the size of the font
Add or Modify Bookmark on the Se
Display numbers in Binary
Display numbers in Octal
Display numbers in Decimal
✓ Display numbers in Hexadecimal

Figure 4.65 - Data display right click menu

If you want to see only the numerical values, click on the **Numbers Only** icon 1 on the **Event Display** toolbar.

4.5.7.3 Switching Between ASCII, EBCDIC, and Baudot

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

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

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

4.5.7.4 Selecting Mixed Channel/Sides

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

1. Click once on the **Mixed Sides** icon to put the display in mixed sides mode.
2. Click again to return to side over side mode.
3. You can right click in the center of the data display window to change between mixed and side over side modes by selecting **Display Sides Together**. A check mark is displayed. Click on **Display Sides Together** to remove the check mark and return to side-by-side display.
4. Right click in the sides panel on the right of the data display and select **Display Sides Together**. A check mark is displayed. Click on **Display Sides Together** to remove the check mark and return to side-by-side display.

4.5.7.5 List of all Event Symbols

By default, the **Event Display** shows all **events**[1], which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button ! . Click again to display all events.

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

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

Table 4.8 - Event Symbols

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

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

Table 4.8 - Event Symbols (continued)

Symbol	Event
ϟ	Low Power - The battery in the ComProbe® is low.
≀	Short Break
☼	SPY Event (SPY Mode only) - SPY events are commands sent by the application being spied on to the UART.
⚐	Start of Frame - Marks the start of a frame.
⊘	Begin Sync Character Strip
⊡	End Sync Character Strip
⇩	Sync Dropped
⦿	Sync Found
⧖	Sync Hunt Entered
⊗	Sync Lost
⊞	Test Device Stopped Responding - The analyzer lost contact with the ComProbe for some reason, often because there is no power to the ComProbe.
✚	Test Device Began Responding - The analyzer regained contact with the ComProbe.
⌀	Timestamping Disabled - Timestamping was turned off. Events following this event are not timestamped.
◷	Timestamping Enabled - Timestamping was turned on. Events following this event have timestamps.
⚑	Truncated Frame- A frame that is not the same size as indicated within its protocol.
⊖	Underrun Error
◇	Unknown Event

4.5.7.6 Font Size

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

To change the font size:

1. Click on **Event Display** menu **Options,** and select **Change the Font Size**.

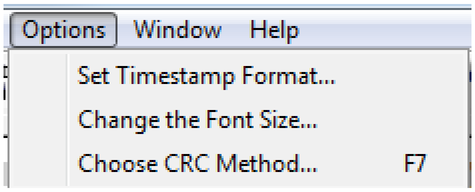


Figure 4.66 - Event Display Options menu

2. Choose a font size from the list.

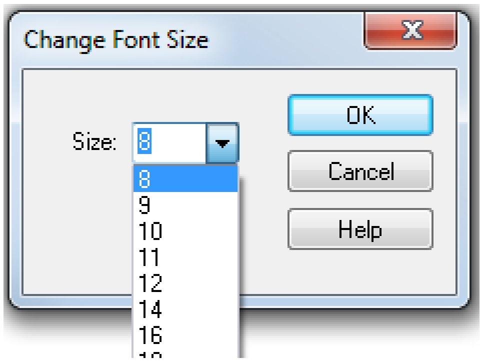


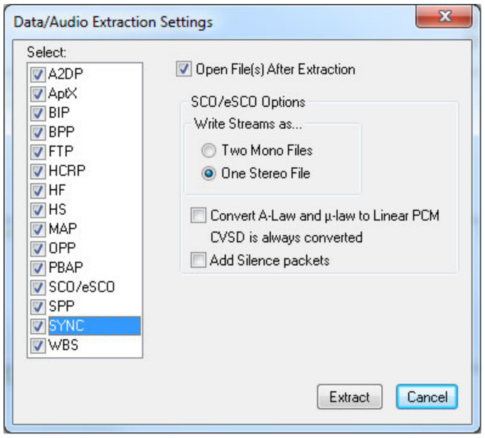
Figure 4.67 - Event Display Font Size Selection

3. Click **OK**.

4.6 Data/Audio Extraction

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

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



Data/Audio Extraction Settings

Select:

☑ A2DP
☑ AptX
☑ BIP
☑ BPP
☑ FTP
☑ HCRP
☑ HF
☑ HS
☑ MAP
☑ OPP
☑ PBAP
☑ SCO/eSCO
☑ SPP
☑ SYNC
☑ WBS

☑ Open File(s) After Extraction

SCO/eSCO Options

Write Streams as...

○ Two Mono Files
● One Stereo File

□ Convert A-Law and µ-law to Linear PCM
CVSD is always converted
□ Add Silence packets

Figure 4.68 - Data/Audio Extraction Settings dialog

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

   It's important to note that if there is no data for the profile(s) you select, no extracted file is created.

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

   Note: This does not work for SCO/eSCO.

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

   Note: This option is for SCO/eSCO only.

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

   Note: This option is for SCO/eSCO only.

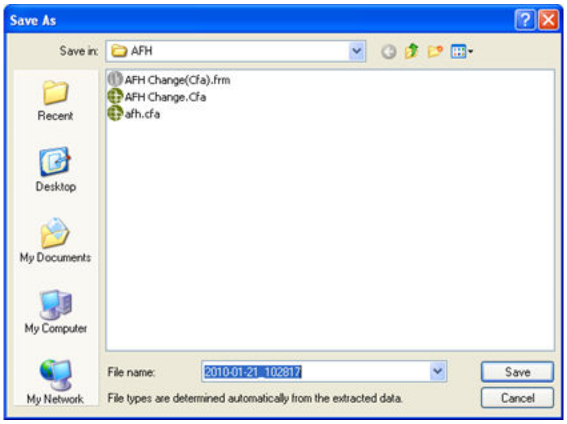
6. Select the **Add Silence packets** to insert the silence packets (dummy packets) for the reserved empty slots into the extracted file. If this option is not selected, the audio packets are extracted without inserting the silence packets for the reserved empty slots.

   Note: This option is for SCO/eSCO only.

7. Select **Extract.**

   A **Save As** dialog appears.

   The application will assign a file name and file type for each profile you select in Step 1 above. The file type varies depending on the original profile. A separate file for each profile will be created, but only for those profiles with available data.



Save in: AFH

AFH Change(Cfa).frm
AFH Change.Cfa
afh.cfa

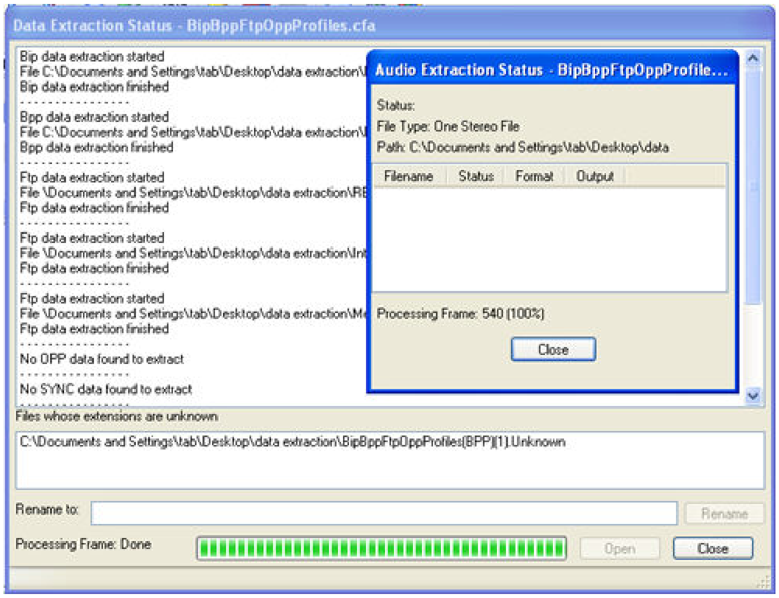
File name: 2010-01-21_102817

File types are determined automatically from the extracted data.

8. Select a location for the file.

9. Click **Save**.

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


Data Extraction Status - BipBppFtpOppProfiles.cfa
Audio Extraction Status - BipBppFtpOppProfile...
Filename
Status
Format
Output
Close
Rename
Open
Close

```
Bip data extraction started
File C:\Documents and Settings\tab\Desktop\data extraction\
Bip data extraction finished
- - - - - - - - - - - - - - -
Bpp data extraction started
File C:\Documents and Settings\tab\Desktop\data extraction\
Bpp data extraction finished
- - - - - - - - - - - - - - -
Ftp data extraction started
File \Documents and Settings\tab\Desktop\data extraction\RE
Ftp data extraction finished
- - - - - - - - - - - - - - -
Ftp data extraction started
File \Documents and Settings\tab\Desktop\data extraction\Int
Ftp data extraction finished
- - - - - - - - - - - - - - -
Ftp data extraction started
File \Documents and Settings\tab\Desktop\data extraction\Me
Ftp data extraction finished
- - - - - - - - - - - - - - -
No OPP data found to extract
- - - - - - - - - - - - - - -
No SYNC data found to extract
```

Status:
File Type: One Stereo File
Path: C:\Documents and Settings\tab\Desktop\data

Processing Frame: 540 (100%)

Files whose extensions are unknown

C:\Documents and Settings\tab\Desktop\data extraction\BipBppFtpOppProfiles(BPP)(1).Unknown

Rename to:

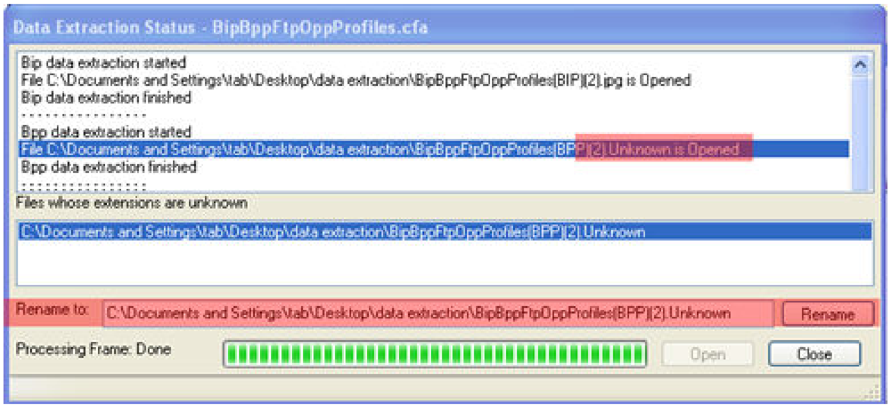
Processing Frame: Done

Figure 4.69 - Data and Audio Extraction Status

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

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

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



```
Bip data extraction started
File C:\Documents and Settings\tab\Desktop\data extraction\BipBppFtpOppProfiles[BIP][2].jpg is Opened
Bip data extraction finished
. . . . . . . . . . . . . . . .
Bpp data extraction started
File C:\Documents and Settings\tab\Desktop\data extraction\BipBppFtpOppProfiles[BPP][2].Unknown is Opened
Bpp data extraction finished
: : : : : : : : : : : : : : : :
```

Files whose extensions are unknown

C:\Documents and Settings\tab\Desktop\data extraction\BipBppFtpOppProfiles[BPP][2].Unknown

Rename to: C:\Documents and Settings\tab\Desktop\data extraction\BipBppFtpOppProfiles[BPP][2].Unknown

Processing Frame: Done

Figure 4.70 - Rename To in the bottom section of Data Extraction Status

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

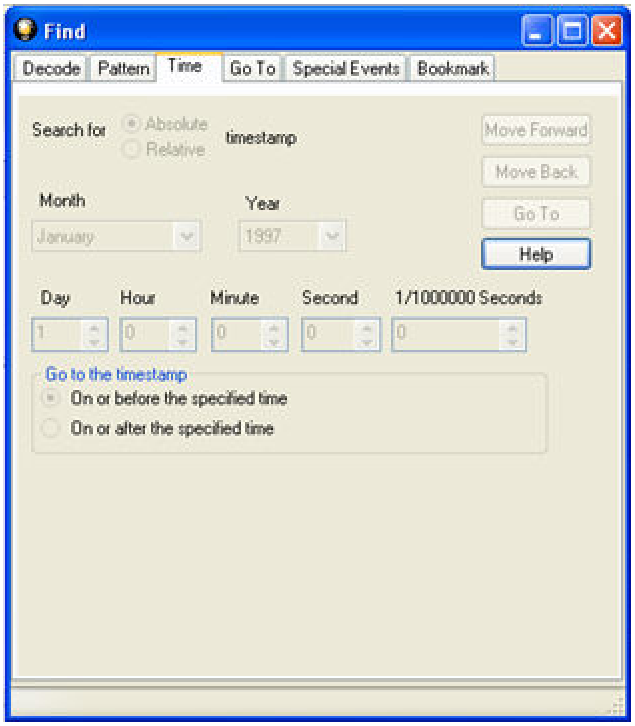
When you are finished, select **Close** to close the dialogs.

Chapter 5 Navigating and Searching the Data

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

5.1 Find

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



Search for ● Absolute ○ Relative timestamp

Month: January

Year: 1997

Day: 1

Hour: 0

Minute: 0

Second: 0

1/1000000 Seconds: 0

Go to the timestamp
● On or before the specified time
○ On or after the specified time

Figure 5.1 - Find Dialog

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

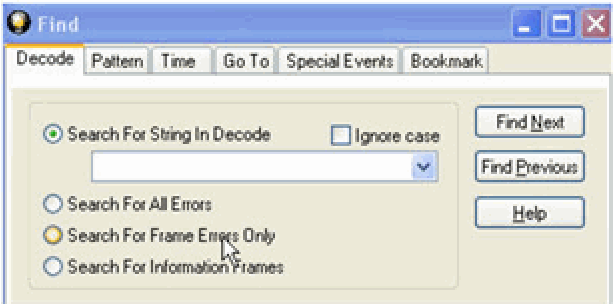
5.1.1 Searching within Decodes

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

To access the search within decodes function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Decode** tab of the **Find** dialog.

> **Note:** The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



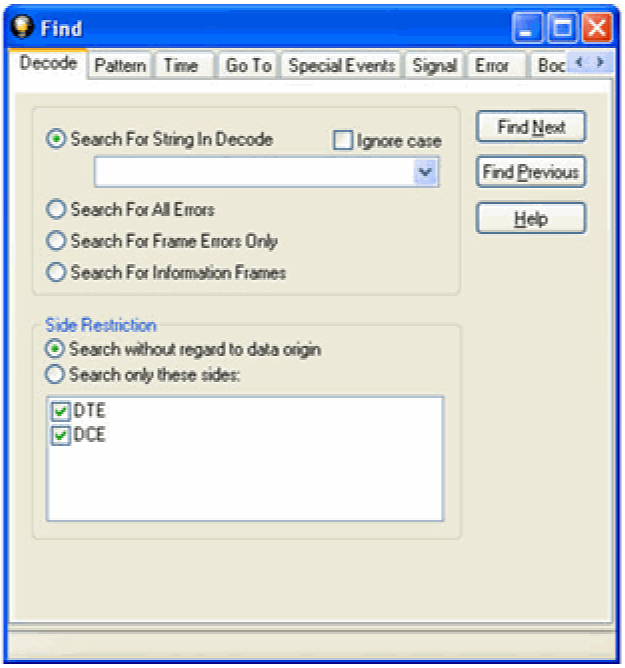
● Search For String In Decode □ Ignore case

○ Search For All Errors

○ Search For Frame Errors Only

○ Search For Information Frames

Figure 5.2 - Find Decode Tab Search for String



● Search For String In Decode □ Ignore case

○ Search For All Errors

○ Search For Frame Errors Only

○ Search For Information Frames

● Search without regard to data origin

○ Search only these sides:

☑ DTE

☑ DCE

Figure 5.3 - Find Decode Tab Side Restriction

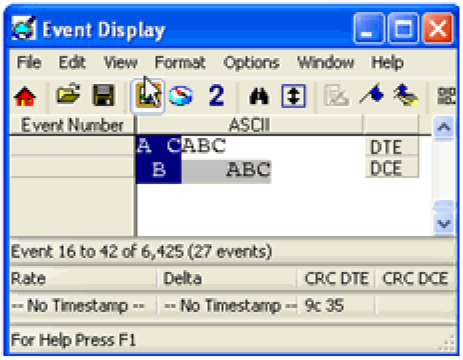
There are several options for error searching on the **Decoder** tab.

- **Search For String in Decoder** allows you to enter a string in the text box. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the analyzer saves the search. The next time you open **Find**, the drop-down list will contain your search parameters.
- **Search for All Errors** finds frame errors as well as frames with byte-level errors (such as parity or CRC errors).
- **Search for Frame Errors Only** finds frame specific errors, such as frame check errors.
- **Search for Information Frame** only searches information frames.

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

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

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



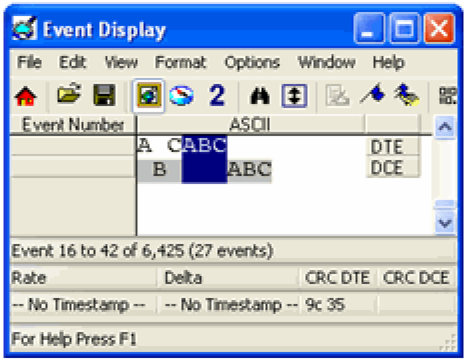
Event Number	ASCII	
	A CABC	DTE
	B ABC	DCE

Event 16 to 42 of 6,425 (27 events)

Rate	Delta	CRC DTE	CRC DCE
-- No Timestamp --	-- No Timestamp --	9c 35	

For Help Press F1

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



Event Number	ASCII	
	A CABC	DTE
	B ABC	DCE

Event 16 to 42 of 6,425 (27 events)

Rate	Delta	CRC DTE	CRC DCE
-- No Timestamp --	-- No Timestamp --	9c 35	

For Help Press F1

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

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

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

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

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

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

5.1.2 Searching by Pattern

Search by Pattern lets you perform a traditional string search. You can combine any of the formats when entering your string, and your search can include wildcards.

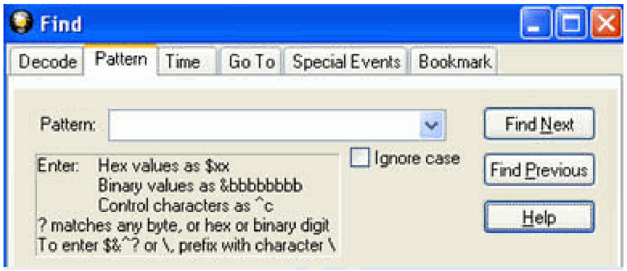
To access the search by pattern function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.

3. Click on the **Find** icon or choose **Find** from the **Edit** menu.

4. Click on the **Pattern** tab of the **Find** dialog.

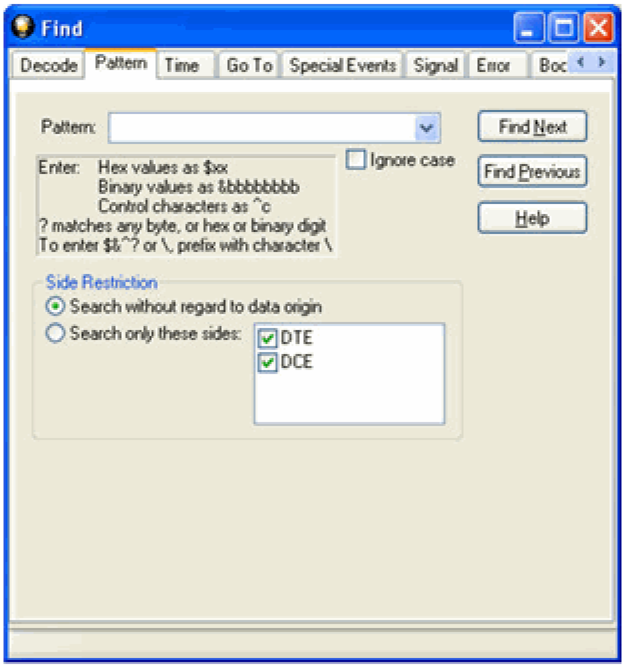
> **Note:** The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



☐ Ignore case

Enter: Hex values as $xx
Binary values as &bbbbbbbb
Control characters as ^c
? matches any byte, or hex or binary digit
To enter $&^? or \, prefix with character \

Figure 5.4 - Find Pattern Tab



☐ Ignore case

Enter: Hex values as $xx
Binary values as &bbbbbbbb
Control characters as ^c
? matches any byte, or hex or binary digit
To enter $&^? or \, prefix with character \

● Search without regard to data origin
○ Search only these sides: ☑ DTE ☑ DCE

Figure 5.5 - Find Pattern Tab Side Restrictions

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

1. Enter the search pattern.

2. Check **Ignore Case** to do a case-insensitive search.

3. When you have specified the pattern you want to use, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

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

Refer to Searching by Decode on page 158 for information on **Side Restrictions**

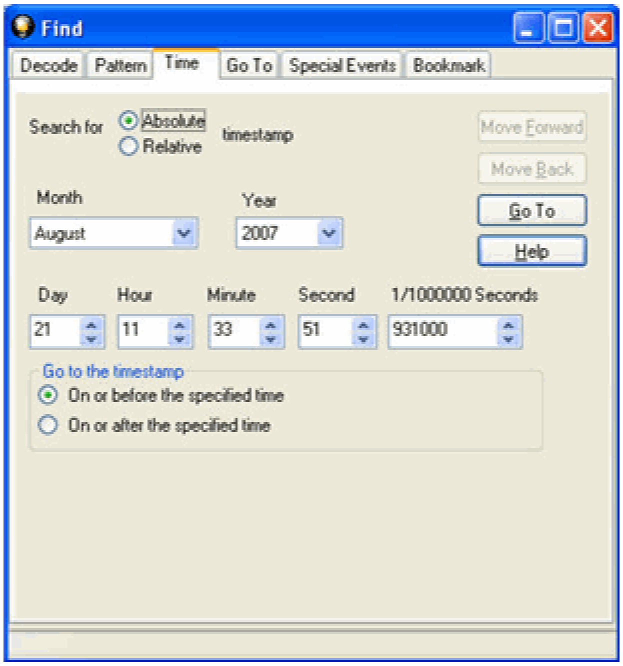
5.1.3 Searching by Time

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

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Time** tab of the **Find** dialog.

> **Note:** The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



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 5.6 - Find by Time tab

The analyzer can search by time in several different ways.

Search for Absolute/Relative timestamp.

- Absolute - An absolute timestamp search means that the analyzer searches for an event at the exact date and time specified. If no event is found at that time, the analyzer goes to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.
- Relative - A relative search means that the analyzer begins searching from whatever event you are currently on, and search for the next event a specific amount of time away.

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

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

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

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

Go to the timestamp: On or before/ On or after

The analyzer searches for an event that matches the time specified. If no event is found at the time specified, the analyzer goes to the nearest event either before or after the specified time. Choose whether to have the analyzer go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the **Go to the timestamp** box.

If you are searching forward in the buffer, you usually want to choose the **On or After** option. If you choose the **On or Before** option, it may be that the analyzer finishes the search and not move from the current byte, if that byte happens to be the closest match.

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

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

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

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

- The analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.

- Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.
- The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

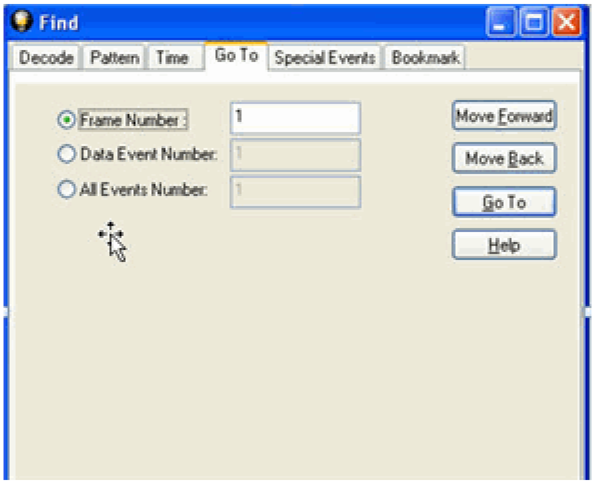
5.1.4 Using Go To

Searching with Go To allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To access the Go To function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Go To** tab of the **Find** dialog.
5. The system displays the **Find** dialog with the **Go To** tab selected.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



● Frame Number : 1
○ Data Event Number: 1
○ All Events Number: 1

Figure 5.7 - Find Go To tab

To go to a particular frame :

1. Select the **Frame Number** radio button
2. Type the frame number in the box.
3. Click the **Go To** button.

4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the **Move Forward** or **Move Back** button.

To go to a particular event :

1. Select the **Data Event Number** or **All Events Number** radio button.
2. Type the number of the event in the box.
3. Click the **Go To** button.
4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the **Move Forward** or **Move Backward** button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on **Move Forward**. Each time you click on **Move Forward,** Frontline moves forward 10 events.

See Event Numbering for why the **Data Event Number** and **All Events Number** may be different. As a general rule, if you have the **Show All Events** icon ! depressed on the **Event Display** window or **Frame Display Event** pane, choose **All Events Number**. If the **Show All Events** button is up, choose **Data Event Number**.

5.1.5 Searching for Special Events

Frontline inserts or marks events other than data bytes in the data stream. For example, the analyzer inserts start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, the analyzer shows this using a special event marker. You can use Find to locate single or multiple special events.

To access the search for special events function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Special Events** tab of the Find dialog.

> **Note:** The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

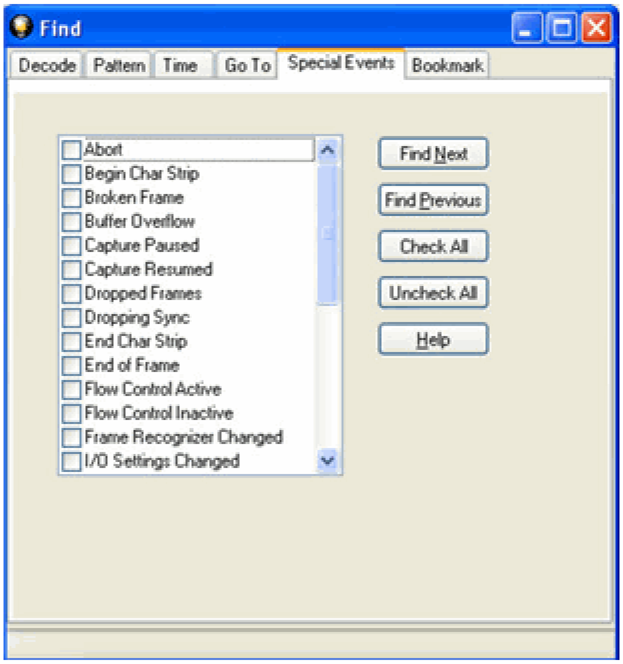


Figure 5.8 - Find Special Events tab

5. Check the event or events you want to look for in the list of special events. Use **Check All** or **Uncheck All** buttons to make your selections more efficient.

6. Click Find Next and Find Previous to move to the next instance of the event.

Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

For a list of all special events and their meanings, see List of all Event Symbols on page 151.

5.1.6 Searching by Signal

Searching with Signal allows you to search for changes in control signal states for one or more control signals. You can also search for a specific state involving one or more control signals, with the option to ignore those control signals whose states you don't care about.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where control signals changed.

To access the search by time function:

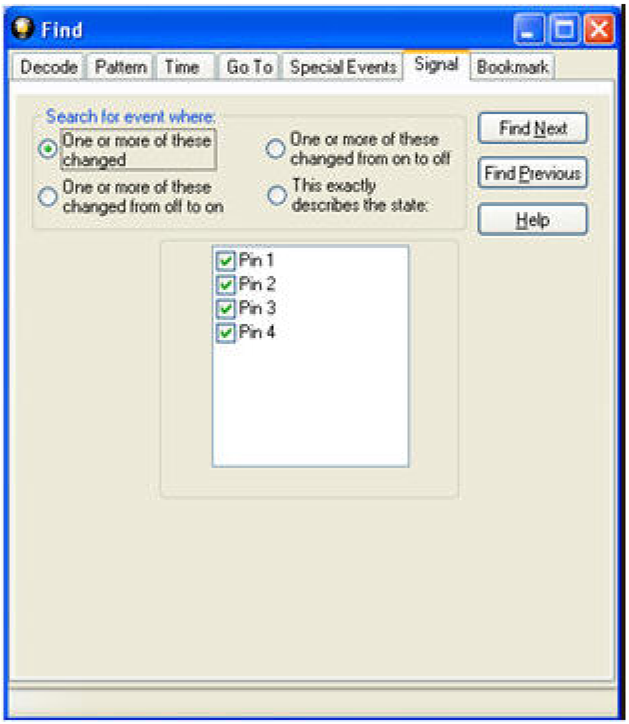
1. Open a capture file to search.

2. Open the **Event Display** or **Frame Display** window.

3. Click on the **Find** icon or choose **Find** from the **Edit** menu.

4. Click on the **Signal** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



Search for event where:

● One or more of these changed

○ One or more of these changed from off to on

○ One or more of these changed from on to off

○ This exactly describes the state:

☑ Pin 1
☑ Pin 2
☑ Pin 3
☑ Pin 4

Figure 5.9 - Find Signal tab.

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

Control Signals

The section with the check boxes allows you to specify which control signals the analyzer should pay attention to when doing the search. The analyzer pays attention to any control signal with a check mark.

- Click on a box to place a check mark next to a control signal
- Click again to uncheck the box
- By default, the analyzer searches all control signals, which means all boxes start out checked.

For example, if you are only interested in finding changes in **RTS** and **CTS**, you would check those two boxes and uncheck all the other boxes. This tells the analyzer to look only at the **RTS** and **CTS** lines when running the search. The other signals are ignored.

The control signals types include:

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

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

Searching for event where:

- The first three options are all fairly similar, and are described together. These options are searching for an event where:
    - One or more control signals changed
    - One or more control signals changed from off to on
    - One or more control signals changed from on to off
- Searching for an event where one or more signals changed means that the analyzer looks at every control signal that you checked, and see if any one of those signals changed state at any time.
    - If you want to look at just one control signal:
        - Check the box for the signal.
        - Uncheck all the other boxes.
        - Choose to search for an event where one or more signals changed.
        - The analyzer notes the state of the selected signal at the point in the buffer where the cursor is, search the buffer, and stop when it finds an event where RTS changed state.
        - If the end of the buffer is reached before an event is found, the analyzer tells you that no matches were found.
- Searching for events where control signals changed state from off to on, or vice versa, is most useful if the signals are usually in one state, and you want to search for occasions where they changed state.

  For example:

    - If DTR is supposed to be on all the time but you suspect that DTR is being dropped
    - Tell the analyzer to look only at DTR by checking the DTR box and unchecking the others
    - Do a search for where one or more control signals changed from on to off.
    - The analyzer would search the DTR signal and stop at the first event where DTR dropped from on to off.
- Searching for an Exact State

  To search for an exact state means that the analyzer finds events that match exactly the state of the control signals that you specify.

    - First, choose to search for an event where your choices exactly describe the state.
    - This changes the normal check boxes to a series of radio buttons labeled On, Off and Don’t Care for each control signal.
    - Choose which state you want each control signal to be in.
    - Choose Don’t Care to have the analyzer ignore the state of a control signal.
    - When you click Find Next, the analyzer searches for an event that exactly matches the conditions selected, beginning from the currently selected event.

- If the end of the buffer is reached before a match is found, the analyzer asks you if you want to continue searching from the beginning.
- If you want to be sure to search the entire buffer, place your cursor on the first event in the buffer.
- Select one of the four radio buttons to choose the condition that must be met in the search
- Select one or more of the checkboxes for Pin 1, 2, 3, or 4.
- Click **Find Next** to locate the next occurrence of the search criteria or **Find Previous** to locate an earlier occurrence of the search criteria.

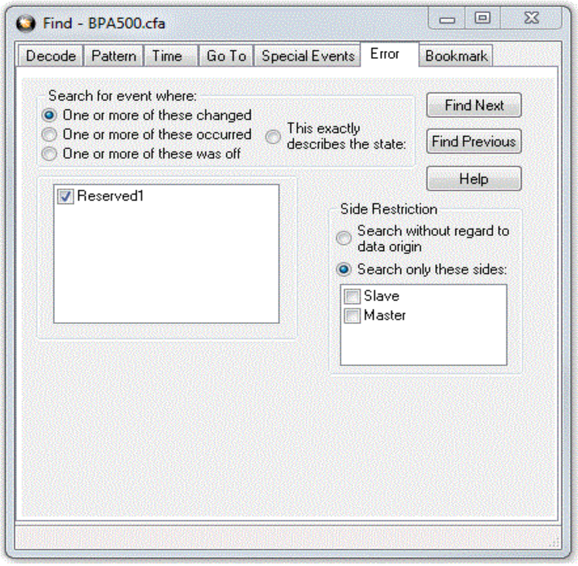
5.1.7 Searching for Data Errors

The analyzer can search for several types of data errors. Searching for data error sallows you to choose which errors you want to search for and whether to search the DTE or DCE data or both. Bytes with errors are shown in red in the **Event Display** window, making it easy to find errors visually when looking through the data.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Errors** tab of the **Find** dialog.

> **Note:** The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



Find - BPA500.cfa

Search for event where:
● One or more of these changed
○ One or more of these occurred
○ One or more of these was off
○ This exactly describes the state:

☑ Reserved1

Side Restriction
○ Search without regard to data origin
● Search only these sides:
□ Slave
□ Master

Figure 5.10 - Find Error tab.

Searching for event where

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- one or more error conditions changed
- one or more error conditions occurred
- one or more error conditions were off (i.e. no errors occurred)

Selecting Which Errors to Search

The section with the check boxes allows you to choose which errors the analyzer should look for. Click on a box to check or un-check it.

If you want to search only for overrun errors

- check the box if shown
- un-check the other boxes.

To search for all types of errors

- check all boxes

The most common search is looking for a few scattered errors in otherwise clean data.

To do this type of search:

- choose to **Search for an event where** one or more error conditions occurred
- choose which errors to look for
- By default, the analyzer looks for all types of errors.

In contrast, searching for an event where one or more error conditions were off means that the analyzer looks for an event where the errors were not present.

For example, if you have data that is full of framing errors, and you know that somewhere in your 20 megabyte capture file the framing got straightened out, you could choose to search for an event where one or more error conditions were off, and choose to search only for framing. The analyzer searches the file, and finds the point at which framing errors stopped occurring.

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

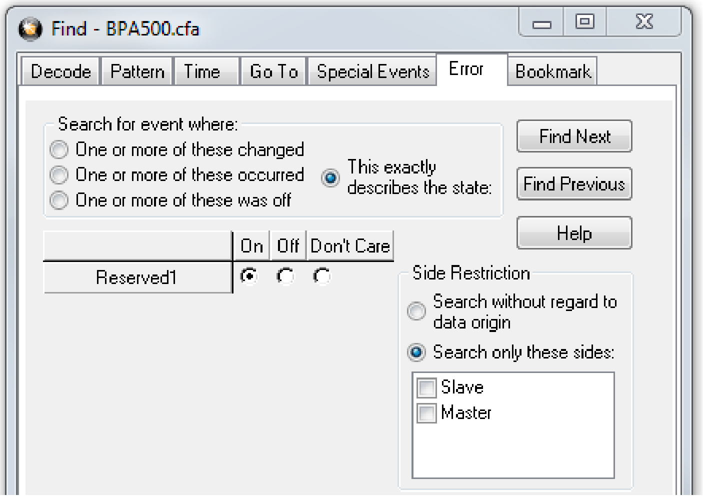
For example, if you have data where sometimes the framing is wrong and sometimes right, you would choose to search framing errors where the error condition changed. This first takes you to the point where the framing errors stopped occurring. When you click **Find Next,** the analyzer stops at the point when the errors began occurring again. Clicking **Find Previous** will search backwards from the current postion.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where error conditions changed. The analyzer searches until it finds an event where error conditions changed or it reaches the end of the buffer, at which point the analyzer tells you that there are no more events found in the buffer. If you are searching for an exact match, the analyzer asks you if you want to continue searching from the beginning of the buffer.

Searching for Exact Error Conditions

To search for an exact state means that the analyzer finds events that exactly match the error conditions that you specify.

- Select the **This exactly describes the state** radio button.
- This changes the normal check boxes to a series of radio buttons labeled **On**, **Off** and **Don't Care** for each error.
    - **On** means that the error occurred
    - **Off** means that the error did not occur
    - **Don't Care** means that the analyzer ignores that error condition.



Find - BPA500.cfa

Search for event where:

○ One or more of these changed
○ One or more of these occurred
○ One or more of these was off
● This exactly describes the state:

	On	Off	Don't Care
Reserved1	●	○	○

Side Restriction

○ Search without regard to data origin
● Search only these sides:

□ Slave
□ Master

- Select the appropriate state for each type of error.

Example:

If you need to find an event where just an overrun error occurred, but not any other type of error, you would choose overrun error to be On, and set all other errors to Off. This causes the analyzer to look for an event where only an overrun error occurred.

If you want to look for events where overrun errors occurred, and other errors may have also occurred but it really doesn't matter if they did or not, choose overrun to be On, and set the others to Don't Care. The analyzer ignores any other type of error, and find events where overrun errors occurred.

To find the next error, click the Find Next button. To find an error that occurred earlier in the buffer to where you are, click the Find Previous button.

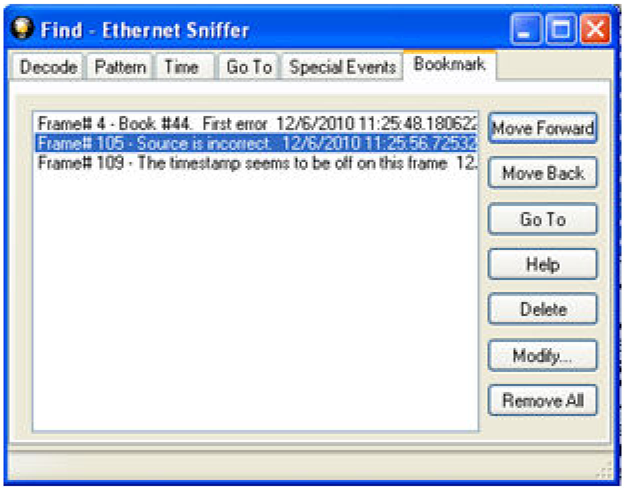
5.1.8 Find - Bookmarks

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

To access the search for bookmarks

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Bookmarks** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.



Frame# 4 - Book #44. First error 12/6/2010 11:25:48.180622
Frame# 105 - Source is incorrect. 12/6/2010 11:25:56.72532
Frame# 109 - The timestamp seems to be off on this frame 12.

Figure 5.11 - Find Bookmark tab.

There are several ways to locate bookmarks.

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

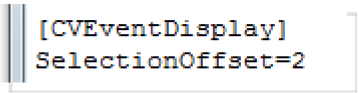
There are three ways to modify bookmarks.

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

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

5.1.9 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the **Event Display**. The first selected byte appears on the third line of the display.



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

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

1. Open fts.ini (located in the C:\User\Public\Public Documents\Frontline Test Equipment\)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

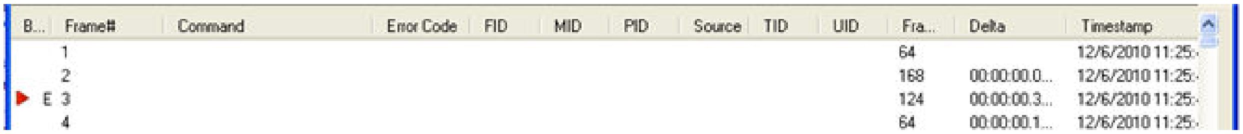
5.1.10 Subtleties of Timestamp Searching

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.

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

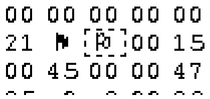
5.2 Bookmarks

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



B...	Frame#	Command	Error Code	FID	MID	PID	Source	TID	UID	Fra...	Delta	Timestamp
	1									64		12/6/2010 11:25:·
	2									168	00:00:00.0...	12/6/2010 11:25:·
▶ E	3									124	00:00:00.3...	12/6/2010 11:25:·
	4									64	00:00:00.1...	12/6/2010 11:25:·

Figure 5.12 - Bookmarked Frame (3) in the Frame Display



```
00 00 00 00 00
21           00 15
00 45 00 00 47
```

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

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

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

5.2.1 Adding, Modifying or Deleting a Bookmark

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

Add:

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

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

Modify

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

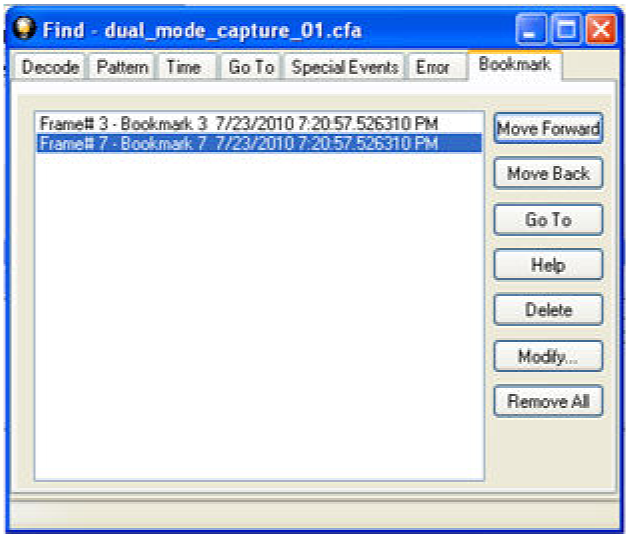
Delete

1. Select the frame or event with the bookmark to be deleted.
2. There are three ways to access the **Add/Modfy Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**,
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Modify Bookmark…** on the selection.
3. Click on the **Delete** button. The bookmark will be deleted.
4. You can also select **Display All Bookmarks** from the **Frame Display** and **Event Display** toolbar or the **Bookmarks** menu. the **Find** window will open on the **Bookmark** tab. Select the bookmark you want to delete and click the **Delete** button.

5.2.2 Displaying All and Moving Between Bookmarks

There are three ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.
2. Select Go to Next Bookmark from the Bookmarks menu.
3. Click the Display All Bookmarks icon . Select the bookmark you want to move to and click the Go To button, or simply double-click on the bookmark. Click the Move Forward and Move Back buttons to cycle through the bookmarks.



Frame# 3 - Bookmark 3 7/23/2010 7:20:57.526310 PM
Frame# 7 - Bookmark 7 7/23/2010 7:20:57.526310 PM

Figure 5.13 - Find Window Bookmark tab Used to Move Around With Bookmarks

To delete a bookmark, select it and click the **Delete** button.

To modify a bookmark, select it and click the **Modify** button.

Click **Remove All** to delete all the bookmarks.

Chapter 6 Saving and Importing Data

6.1 Adding Comments to a Capture File

The **Notes** feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the **Notes** window :

1. Click the **Show Notes** icon . This icon is present on the toolbars of the **Frame Display** , as well as the **Event Display** . **Notes** can be selected from the **Edit** menu on one of these windows.
2. Type your comments in the large edit box on the **Notes** window. The **Cut**, **Copy**, **Paste** features are supported from **Edit** menu and the toolbar when text is selected. Undo and Redo features are all supported from **Edit** menu and the toolbar at the current cursor location.
3. Click the thumbtack icon to keep the **Notes** window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

6.2 Confirm Capture File (CFA) Changes

This dialog appears when you close a capture file after changing the Notes, the protocol stack, or bookmarks. The dialog lists information that was added or changed and allows you to select which information to save, and whether to save it to the current file or to a new one.

Changes made to the file appear in a list in the left pane. You can click on each item to see details in the right pane about what was changed for each item. You simply check the boxes next to the changes you want to keep. Once you decide what changes to keep, select one of the following:

- **Save To This File** – Saves the changes you have made to the current capture file.
- **Save As** – Saves the changes to a new file.
- **Cancel the Close Operation** – Closes the file and returns you back to the display. No changes are saved.
- **Discard Changes** – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

6.3 Loading and Importing a Capture File

6.3.1 Loading a Capture File

From the Control Window:

1. Go to the **File** menu.
2. Choose a file from the recently used file list.
3. If the file is not in the **File** menu list, select **Open Capture File** from the **File** menu or simply click on the **Open** icon on the toolbar.
4. Capture files have a .cfa extension. Browse if necessary to find your capture file.
5. Click on your file, and then click **Open**.

6.3.2 Importing Capture Files

1. From the **Control** window , go to the **File** menu and select Open Capture File or click on the Open icon on the toolbar.
2. Left of the **File name** text box, select from the drop-down list **Supported File Types** box to **All Importable File Types** or **All Supported File Types (*.cfa, *.log, *.txt, *.csv, *.cap)**. Select the file and click **Open**.

The analyzer automatically converts the file to the analyzer's format while keeping the original file in its original format. You can save the file in the analyzer's format, close the file without saving it in the analyzer's format, or have the analyzer automatically save the file in the analyzer's format (see the System Settings to set this option). All of these options keep your original file untouched.

When you first open the file, the analyzer brings up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for the analyzer to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

6.4 Printing

6.4.1 Printing from the Frame Display/HTML Export

The **Frame Display Print** dialog and the **Frame Display HTML Export** are very similar. This topic discusses both dialogs.

Frame Display Print

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

When **Print Preview** is selected, the output displays in a browser print preview window, where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images.

Print Background Colors Using Internet Explorer

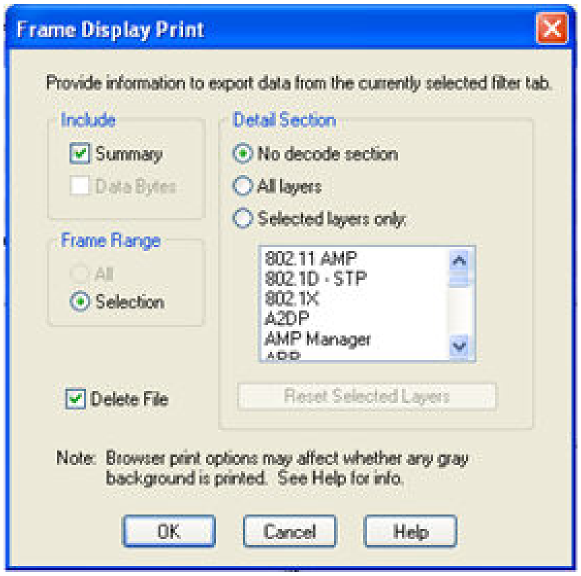
1. Open the Tools menu on the browser menu bar
2. Select “Internet Options…” menu entry.
3. Click Advanced tab.
4. Check “Print background colors and images” under the Printing section
5. Click the Apply button, then click OK

Configure the Print File Range in the Frame Display Print Dialog

Selecting more than one frame in the Frame Display window defaults the radio button in the Frame Display Print dialog to Selection and allows the user to choose the All radio button. When only one frame is selected, the All radio button in the Frame Display Print dialog is selected.

How to Print Frame Display Data

1. Select **Print** or **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print** dialog. Select **Print** if you just want to print your data to your default printer. Select **Print Preview** if you want access to printer options.
2. Choose to include the **Summary** pane (check the box) in the print output. The **Summary** pane appears at the beginning of the printed output in tabular format. If you select **All layers** in the **Detail Section**, the **Data Bytes** option becomes available.
3. In the **Detail Section**, choose to exclude—**No decode section**—the decode from the **Detail** pane in the **Frame Display**, or include **All Layers** or **Selected Layers Only.** If you choose to include selected layers, then select (click on and highlight) the layers from the list box.
4. Click on selected layers in the list to de-select, or click the **Reset Selected Layers** button to de-select all selected layers.



Frame Display Print

Provide information to export data from the currently selected filter tab.

Include
- ☑ Summary
- □ Data Bytes

Frame Range
- ○ All
- ● Selection

☑ Delete File

Detail Section
- ● No decode section
- ○ All layers
- ○ Selected layers only:

802.11 AMP
802.1D - STP
802.1X
A2DP
AMP Manager
ARP

Note: Browser print options may affect whether any gray background is printed. See Help for info.

Figure 6.1 - Frame Display Print Dialog

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

   Choosing **All** prints up to 1000 frames from the buffer.

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

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

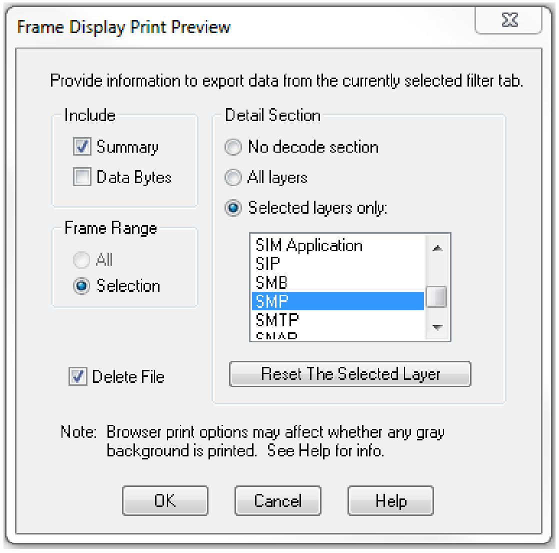
7. Click the **OK** button.

Frame Display Print Preview

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

If you chose **Print Preview**, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

1. Select **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print Preview**.



Frame Display Print Preview

Provide information to export data from the currently selected filter tab.

Include

☑ Summary

□ Data Bytes

Frame Range

○ All

● Selection

☑ Delete File

Detail Section

○ No decode section

○ All layers

● Selected layers only:

SIM Application
SIP
SMB
SMP
SMTP
SNAP

Note: Browser print options may affect whether any gray background is printed. See Help for info.

Figure 6.2 - Frame Display Print Preview Dialog

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

3. Click the **OK** button, and after a brief wait a browser window will appear.

6.4.2 Printing from the Event Display

The Event Display Print feature provides the user with the option to print either the entire capture buffer or the current selection. When Print Preview is selected, the output displays in a browser print preview window where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar

2. Select “Internet Options...” menu entry.

3. Click Advanced tab.

4. Check “Print background colors and images” under the Printing section

5. Click the Apply button, then click OK

The **Event Display Print** feature uses the current format of the **Event Display** as specified by the user.

See About Event Display for an explanation on formatting the **Event Display** prior to initiating the print feature.

Configure the Print File Range in the Event Display Print dialog

Selecting more than one event in the **Event Display** window defaults the radio button in the **Event Display Print** dialog to **Selection** and allows the user to choose the **All** radio button. When only one event is selected , the **All** radio button in the **Event Display Print** dialog is selected.

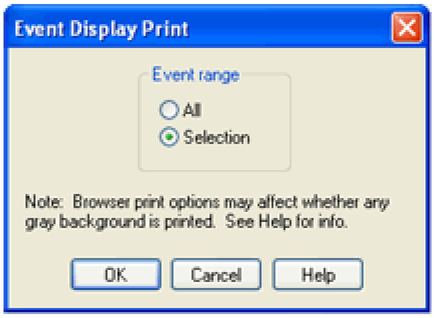
How to Print Event Display Data to a Browser

1. Select **Print** or **Print Preview** from the **File** menu on the **Event Display** window to display the **Event Display Print** dialog. Select **Print** if you just want to print your data to your default printer. Select **Print Preview** if you want preview the print in your browser.

2. Select the range of events to include from either **All** or **Selection** in the **Event Range** section . Choosing **All** prints all of the events in the capture file or buffer. Choosing **Selection** prints only the selected events in the Event Display window.

   Note: In order to prevent a Print crash, you cannot select **All** if there are more than 100,000 events in the capture buffer.

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



○ All
● Selection

Note: Browser print options may affect whether any gray background is printed. See Help for info.

Figure 6.3 - Event Display Print Dialog

3. Click the OK button.

If you chose **Print Preview**, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

6.5 Exporting

6.5.1 Frame Display Export

You can dump the contents of the **Summary** pane on the **Frame Display** into a Comma Separated File (.csv).

To access this feature:

1. Right click on the **Summary** pane or open the **Frame Display File** menu.

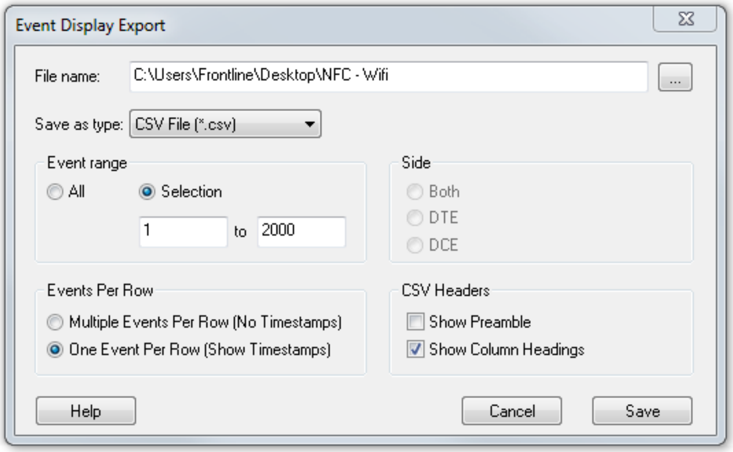
2. Select the **Export…** menu item.

3. Select a storage location and enter a **File name**.

4. Select **Save**.

6.5.2 Exporting a File with Event Display Export

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



Event Display Export

File name: C:\Users\Frontline\Desktop\NFC - Wifi

Save as type: CSV File (*.csv)

Event range
○ All ● Selection
1 to 2000

Side
○ Both
○ DTE
○ DCE

Events Per Row
○ Multiple Events Per Row (No Timestamps)
● One Event Per Row (Show Timestamps)

CSV Headers
□ Show Preamble
☑ Show Column Headings

Figure 6.4 - Event Display Export Example: .csv file.

How to Export Event Display Data to a File

1. Select **Export Events** from the **File** menu on the **Event Display** window to display the **Event Display Export** dialog.

2. Enter a file path and name, or click the browser button to display the Windows **Save As** dialog and navigate to the desired storage location.

3. Select a file type from the **Save as type:** drop-down List Menu on the Event Display Export dialog. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

   Binary File (*.bin)

4. Select the range of events to include in the file from either **All** or **Selection** in the **Event Range** section of the **Event Display Export** dialog.

   - Selecting more than one event in the Event Display window defaults the radio button in the Event Display Export dialog to Selection and allows the user to choose the All radio button.

   - When only one event is selected (something must be selected), the All radio button in the Event Display Export dialog is selected by default.

5. Next you need to select the Side variable for serial communications.

   - is used to determine whether you want to export data from , or both.

   - Choose or Both to determine how you want to export the data.

5. Choose or Both to determine how you want to export the data.

6. Choose whether you want to display multiple events or single events per row.

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

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

   .

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

   Timestamp

   Delta

   Event Number

   Byte Number

   Frame Number

   Type

   Hex

   Dec

   Oct

   Bin

   Side

   ASCII | 7-bit ASCII | EBCDIC | Baudot

   RTS

   CTS

   DSR

   DTR

   CD

   RI

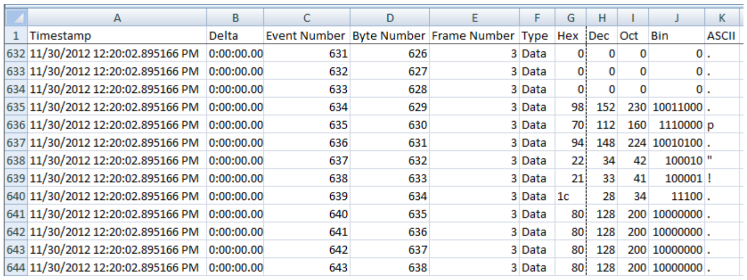
   UART Overrun

   Parity Error

   Framing Error

7. If you select .csv as the file type, choose whether you want to hide/display **Preambles** or **Column Headings** in the exported file

8. Click **Save**. The Event Display Export file is saved to the locations you specified in **File name**.



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

Figure 6.5 - Example: .csv Event Display Export, Excel spreadsheet

6.5.2.1 Export Filter Out

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the **Filter Out** box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Non-printable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the non-printable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between $20 and $7e.

6.5.2.2 Exporting Baudot

When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field shows letters and vice versa.

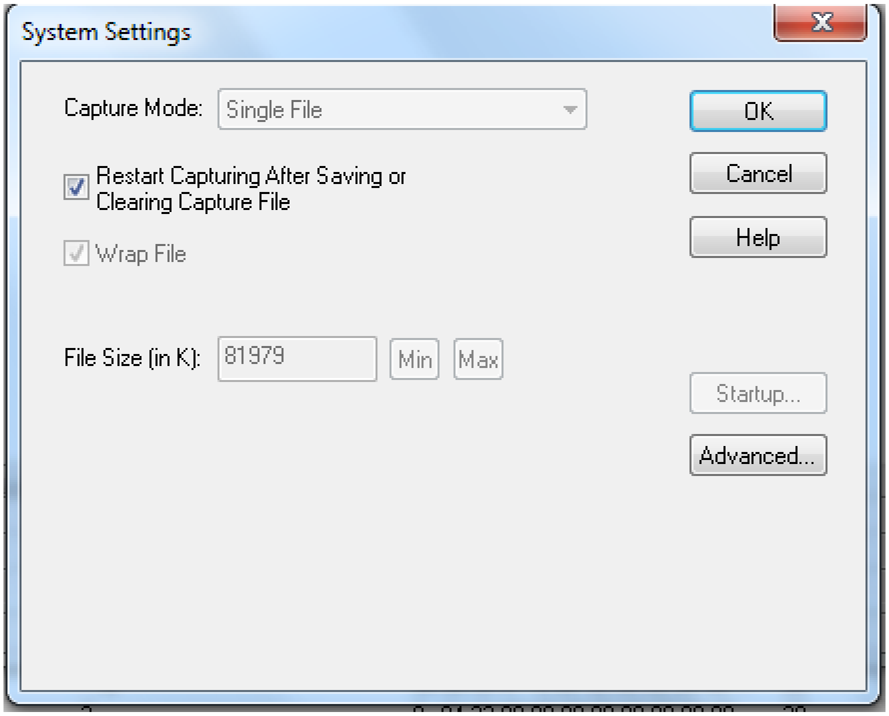
Chapter 7 General Information

7.1 System Settings and Progam Options

7.1.1 System Settings

Open the **System Settings** window by choosing **System Settings** from the **Options** menu on the **Control** window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.

Single File



System Settings

Capture Mode: Single File

☑ Restart Capturing After Saving or Clearing Capture File

☑ Wrap File

File Size (in K): 81979

Figure 7.1 - System Settings Single File Mode

This option allows the analyzer to capture data to a file. Each time you capture the file you must provide a file name. The size of each file cannot larger than the number given in File Size (in K). The name of each file is the name you give it in the Name box followed by the date and time. The date and time are when the series was opened.

- **Restart Capturing After Saving or Clearing Capture File**

  If the Automatically Restart feature is enabled, the analyzer restarts capture to the file immediately after the file is closed.

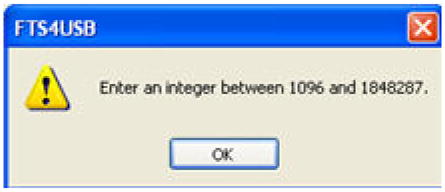
- **Wrap File**

  When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.

- **File Size**: The size of the file will depend of the available hard disk space.

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

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



Enter an integer between 1096 and 1848287.

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

- **Start up**

  Opens the Program Start up Options window. **Start up** options let you choose whether to start data capture immediately on opening the analyzer.

- **Advanced**

  Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

7.1.1.1 System Settings - Disabled/Enabled Options

Some of the **System Settings** options are disabled depending upon the status of the data capture session.

- As the default, all the options on the **System Settings** dialog are enabled.
- Once the user begins to capture data by selecting the Start Capture button, some of the options on the System Settings dialog are disabled until the user stops data capture and either saves or erases the captured data.
- The user can go into the **Startup** options and **Advanced** system options on the **System Settings** dialog and make changes to the settings at any time.

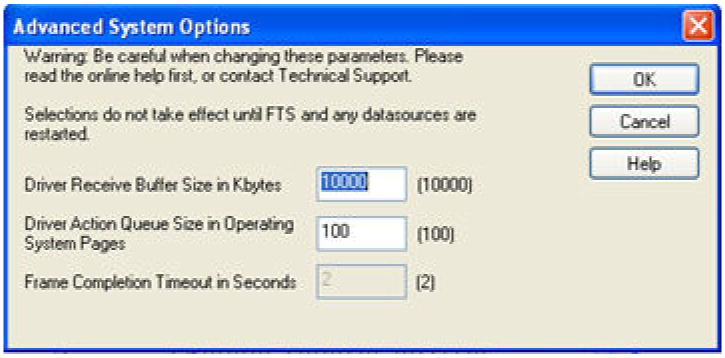
7.1.1.2 Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box.

Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of the analyzer, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options:

1. Go to the Control 🏠 window.
2. Choose **System Settings** from the **Options** menu.
3. On the **System Settings** window, click the **Advanced** button.



Advanced System Options

Warning: Be careful when changing these parameters. Please read the online help first, or contact Technical Support.

Selections do not take effect until FTS and any datasources are restarted.

Driver Receive Buffer Size in Kbytes: 10000 (10000)

Driver Action Queue Size in Operating System Pages: 100 (100)

Frame Completion Timeout in Seconds: 2 (2)

Figure 7.2 - Advanced System Options dialog

- **Driver Receive Buffer Size in Kbytes** - This is the size of the buffer used by the driver to store incoming data. This value is expressed in Kbytes.
- **Driver Action Queue Size In Operating System Pages** - This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages.
- **Frame Completion Timeout in Seconds** - This is the number of seconds that the analyzer waits to receive data on a side while in the midst of receiving a frame on that side.

  If no data comes in on that side for longer than the specified number of seconds, an "aborted frame" event is added to the Event Display and the analyzer resumes decoding incoming data. This can occur when capturing interwoven data (DTE and DCE) and one side stops transmitting in the middle of a frame.

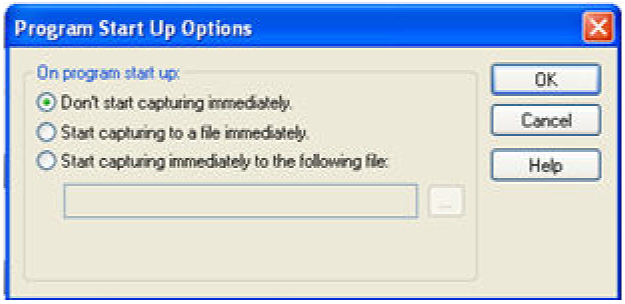
  The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

  Note: This option is currently disabled.

7.1.1.3 Selecting Start Up Options

To open this window:

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



Program Start Up Options

On program start up:

● Don't start capturing immediately.

○ Start capturing to a file immediately.

○ Start capturing immediately to the following file:

Figure 7.3 - Start Up Options dialog

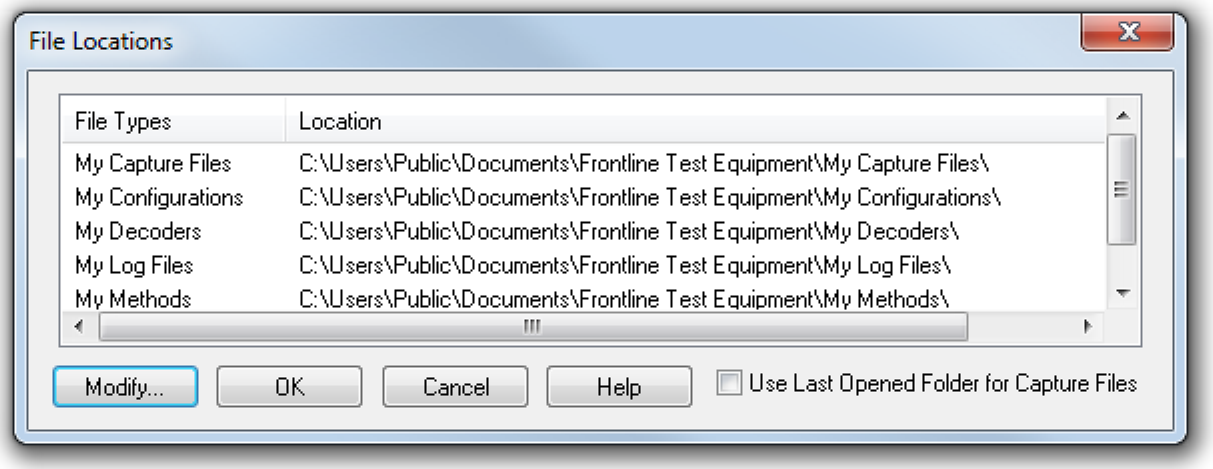
- **Don't start capturing immediately** - This is the default setting. The analyzer begins monitoring data but does not begin capturing data until clicking the **Start Capture** ● icon on the **Control**, **Event Display** or **Frame Display** windows.
- **Start capturing to a file immediately** - When the analyzer starts up, it immediately opens a capture file and begins data capture to it. This is the equivalent of clicking the**Start Capture** ● icon. The file is given a name based on the settings for capturing to a file or series of files in the **System Settings** window.
- **Start capturing immediately to the following file:** - Enter a file name in the box below this option. When the analyzer starts up, it immediately begins data capture to that file. If the file already exists, the data in it is overwritten.

7.1.2 Changing Default File Locations

The analyzer saves user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. These locations are set at installation.

Follow the steps below to change the default locations.

1. Choose **Directories** from the **Options** menu on the **Control** window to open the **File Locations** window.

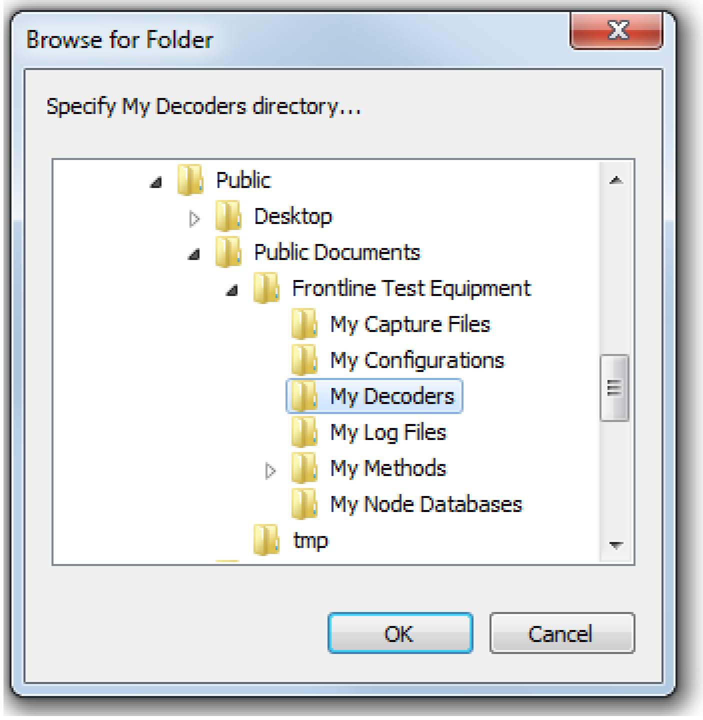


File Types	Location
My Capture Files	C:\Users\Public\Documents\Frontline Test Equipment\My Capture Files\
My Configurations	C:\Users\Public\Documents\Frontline Test Equipment\My Configurations\
My Decoders	C:\Users\Public\Documents\Frontline Test Equipment\My Decoders\
My Log Files	C:\Users\Public\Documents\Frontline Test Equipment\My Log Files\
My Methods	C:\Users\Public\Documents\Frontline Test Equipment\My Methods\

☐ Use Last Opened Folder for Capture Files

Figure 7.4 - File Locations dialog

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



Specify My Decoders directory...

Figure 7.5 - File Locations Browse dialog

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

If a user sets the My Decoders directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch Frontline. For example, if an Frontline product is installed at C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\ then "My Decoders" cannot be set to any of the following:

- C:\ My Decoders\
- C:\Users\ My Decoders\
- C:\Users\\Public\My Decoders\
- C:\Users\Public\Public Documents\My Decoders\
- or to any directory that already exists in the path C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\

Default Capture File Folder Checkbox

If the **Use Last Opened Folder for Capture Files** checkbox is checked, then the system automatically changes the default location for saving capture files each time you open a file from or save a file to a new location. For example, let's say the default location for saving capture files is Drive A > Folder A. Now you select the **Use Last Opened Folder for Capture Files** checkbox. The next time, however, you open a capture file from a different location, Folder B > Removable Flash Drive for example. Now when you save the capture file, it will be saved to Folder B > Removable Flash Drive. Also, all subsequent files will be saved to that location. This remains true until you open a file from or save a file to a different location.

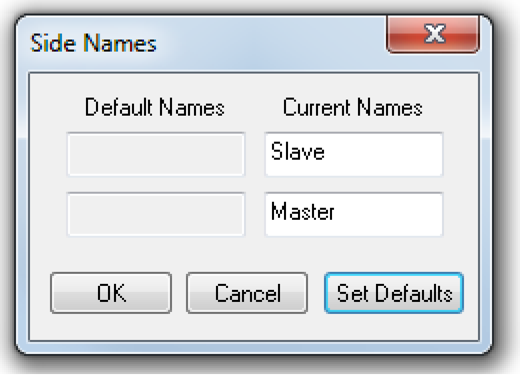
There is one caveat to this scenario, however. Let's say you have selected **Use Last Opened Folder for Capture Files** and opened a file from a location other than the default directory. All subsequent capture files will be saved to that location. Suppose, however, the next time you want to save a capture file, the new file location is not available because the directory structure has changed: a folder has been moved, a drive has been reassigned, a flash drive has been disconnected, etc. In the case of a "lost" directory structure, subsequent capture files will be saved to the default location. **ComProbe software will always try to save a file to the folder where the last file was opened from or saved to, if Use Last Opened Folder for Capture Files is checked.** If, however, the location is not accessible, files are saved to the default directory that is set at installation.

If the checkbox is unchecked, then the system always defaults to the directory listed in the File Locations dialog.

7.1.3 Side Names

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

Changes to the Names are used throughout the program.



Slave

Master

Figure 7.6 - Example: Side Names Where "Slave" and "Master" are current

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

7.1.4 Timestamping

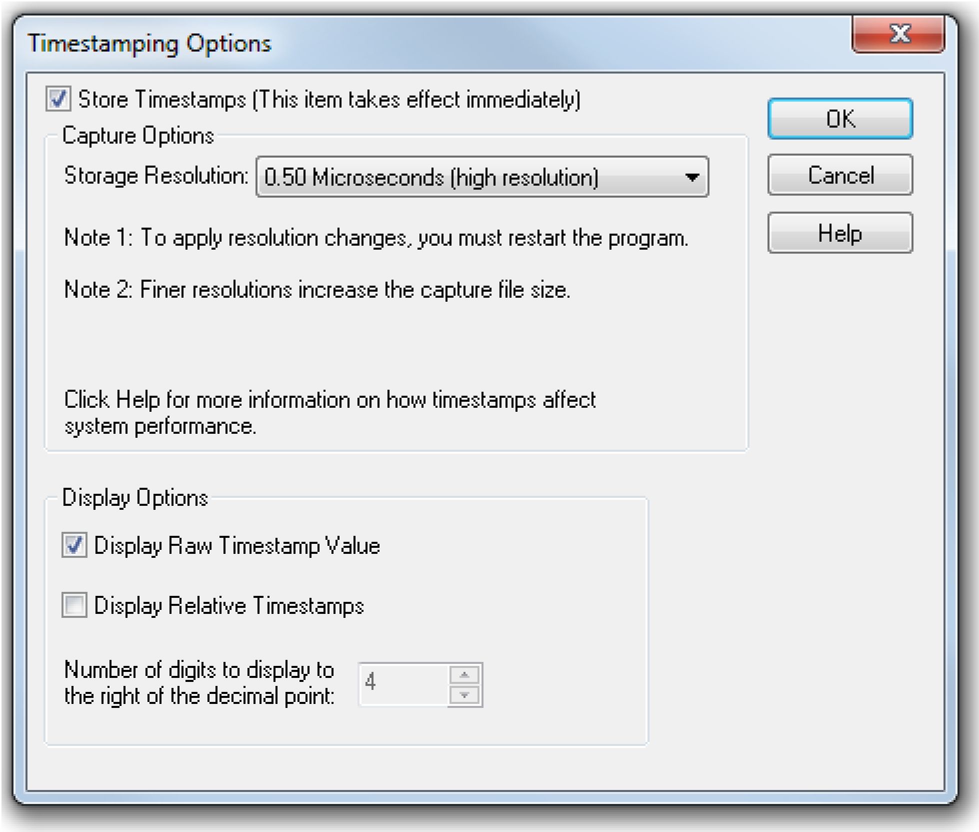
Timestamping is the process of precise recording in time of packet arrival. Timestamps is an optional parameter in the Frame Display and Event Display that can assist in troubleshooting a network link.

7.1.4.1 Timestamping Options

The Timestamping Options window allows you to enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.

To open this window:

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



☑ Store Timestamps (This item takes effect immediately)

Capture Options

Storage Resolution: 0.50 Microseconds (high resolution)

Note 1: To apply resolution changes, you must restart the program.

Note 2: Finer resolutions increase the capture file size.

Click Help for more information on how timestamps affect system performance.

Display Options

☑ Display Raw Timestamp Value

☐ Display Relative Timestamps

Number of digits to display to the right of the decimal point: 4

Figure 7.7 - Timestamping Options dialog

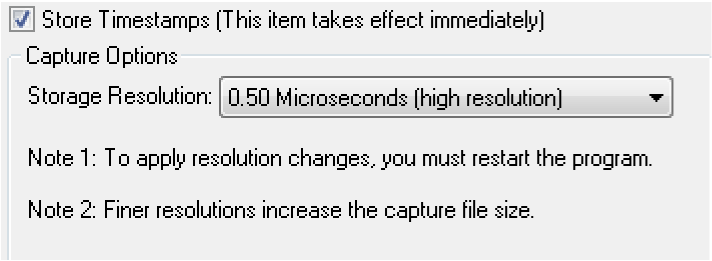
Enabling/Disabling Timestamp

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

Changing the Timestamp Resolution

This option affects the resolution of the timestamp stored in the capture file. The default timestamp is 10 milliseconds. This value is determined by the operating system and is the smallest "normal" resolutions possible.

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



☑ Store Timestamps (This item takes effect immediately)

Capture Options

Storage Resolution: 0.50 Microseconds (high resolution)

Note 1: To apply resolution changes, you must restart the program.

Note 2: Finer resolutions increase the capture file size.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked by an asterisk as high resolution in the drop down list. To change timestamping resolutions:

1. Go to the **Capture Options** section of the window.

2. Change the resolution listed in the

Storage Resolution box.

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

Performance Issues with High Resolution Timestamp

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions. The second issue is that using high resolution timestamping may affect performance on slower machines

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file has more data events in it, because less room is used to store timestamps.

You can increase the size of your capture file in the System Settings.

Switching Between Relative and Absolute Time

With Timestamping you can choose to employ Relative Time or Absolute time.

1. Choose **System Settings** from the **Options** menu on the **Control** window, and click the **Timestamping Options** button, or click the click the **Timestamping Options** icon from the **Event Display** window.
2. Go to the **Display Options** section at the bottom of the window and find the **Display Relative Timestamps** checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

> **Note:** The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

- **Display Raw Timestamp Value** shows the timestamp as the total time in hundred nanoseconds from a specific point in time.
- **Display Relative Timestamps** shows the timestamp as the amount of time that has passed since the first byte was captured. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.
- Selecting both values displays the total time in nanoseconds from the start of the capture as opposed to a specific point in time.
- Selecting neither value displays the actual chronological time.

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

Displaying Fractions of a Second

1. Choose **System Settings** from the **Options** menu on the **Control** window, and click the **Timestamping Options** button, or click the click the **Timestamping Options** icon from the **Event Display** window.
2. Go to the **Display Options** section at the bottom of the window, and find the **Number of Digits to Display** box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

7.2 Technical Information

7.2.1 Performance Notes

As a software-based product, the speed of your computer's processor affects the analyzer's performance. Buffer overflow errors are an indicator that the analyzer is unable to keep up with the data. The information below describes what happens to the data as it arrives, what the error means, and how various aspects of the analyzer affect performance. Also included are suggestions on how to improve performance.

The analyzer's driver takes data from the driver and counts each byte as they are put into the driver's buffer. The analyzer's driver tells the user interface that data is ready to be processed. The analyzer takes the data from the driver's buffer and puts the data into the capture buffer.

Driver Buffer Overflows occur when the user interface does not retrieve frames from the driver quickly enough. Buffer overflows are indicated in the **Event Display** window by a plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost.

There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by the analyzer. (Ethernet Only)
- Close all other programs that are doing work while the analyzer is running. Refrain from doing searches in the **Event Display** window or other processor intensive activities while the analyzer is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the file. Try turning off timestamping from the Timestamping Options window.
- For **Driver Buffer Overflows**, change the size of the driver buffer. This value is changed from the **Advanced System Settings**. Go to the **Control** window and choose **System Settings** from the **Options** menu. Click on the **Advanced** button. Find the value D**river Receive Buffer Size in Operating System Pages**. Take the number listed there and double it.
- The analyzer's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause the analyzer to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the **Event Display** and

Frame Display windows. The analyzer can capture data with no windows other than the **Control** window open.

- If you are still experiencing buffer overflows after trying all of the above options, then you need to use a faster PC.

7.2.2 Progress Bars

The analyzer uses progress bars to indicate the progress of a number of different processes. Some progress bars (such as the filtering progress bar) remain visible, while others are hidden.

The title on the progress bar indicates the process underway.

7.2.3 Event Numbering

This section provides information about how events are numbered when they are first captured and how this affects the display windows in the analyzer. The information in this section applies to frame numbering as well.

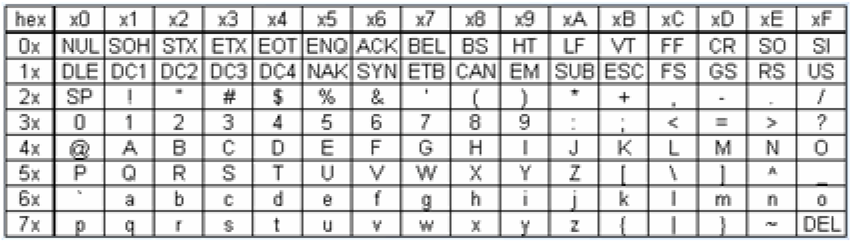
When the analyzer captures an event, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are wrapped out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague’s file use the same event numbers that your file does.

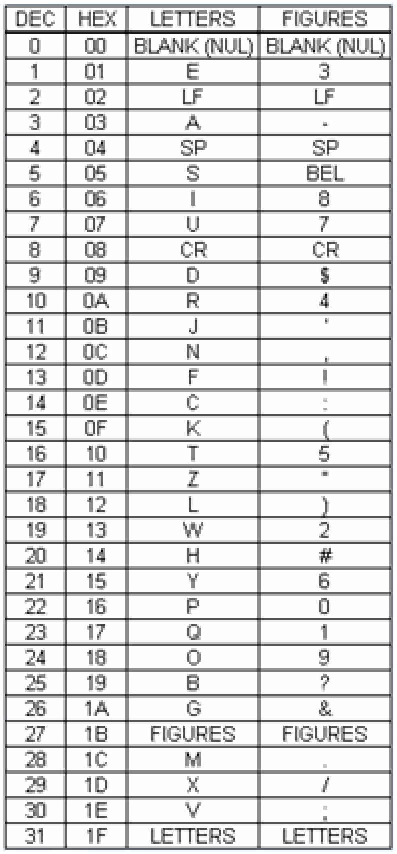
7.2.4 Useful Character Tables

7.2.4.1 ASCII Codes



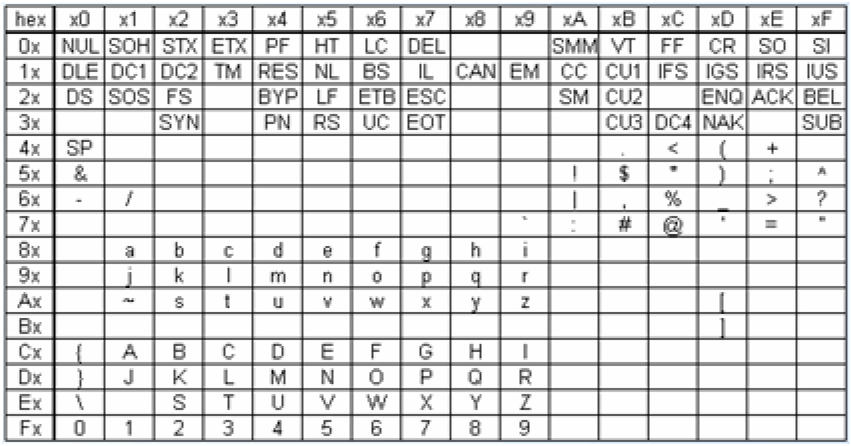
hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

7.2.4.2 Baudot Codes



DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L	)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

7.2.4.3 EBCDIC Codes



hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(	+	
5x	&										!	$	*	)	;	^
6x	-	/									|	,	%	_	>	?
7x										`	:	#	@	'	=	"
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[		
Bx														]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

7.2.4.4 Communication Control Characters

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and two-character system abbreviation for each one. Some abbreviations have forward slash characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Table 7.1 - Communications Control Characters

Abbreviation	Control Character	Text
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of Medium
EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed
FS	FS	File Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle

Table 7.1 - Communications Control Characters(continued)

Abbreviation	Control Character	Text
US	US	Unit Separator
VT	VT	Vertical Tabulation

7.2.5 *Bluetooth* low energy ATT Decoder Handle Mapping

Low energy device attributes contain a 16-bit address called the attribute handle. Each handle is associated with an attribute Universally Unique Identifier (UUID) that is 128-bits long. In the attribute database, the handle is unique while the UUID is not unique.

The ComProbe software detects and stores the relationships (mappings) between handle and UUID during the GATT discovery process. But sometimes, there is no GATT discovery process because

- The discovery has previously taken place and both devices stored the mappings and the discovery will not repeat at every subsequent connection.
- The developer owns both devices in the conversation and chose to ignore discovery because the mappings are known.
- The devices are in development and the code to perform the mappings has not been written yet.

The solution to this problem is to

1. define the mappings in a file and
2. then pre-loading the mapping using the ComProbe software.

Creating handle-UUID mapping file

Create a file named "ATT_Handle_UUID_Preload.ini' in the root directory of "C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\", but the file can be located anywhere.

Assume that you want to create a GATT service starting at handle 1.

Create a section in the ini file called

```
[Service Base Handles]
A=1
```

"A" will be your first service. Make the base handle equal to the handle of your service. You can use all upper and lower case letters so you can have up to 52 service handles.

Next add the following section.

```
[Advertiser Handles]
; Generic Access Profile (GAP)
A0 = 1800
A1 = 2803
A2 = 2a00
A3 = 2803
A4 = 2a01
A5 = 2803
A6 = 2a04
```

A few things of note:

- In the code above, lines begging with a semi-colon are comments.
- If you want to change the base handle of the GAP service, change the "1" to some other number.
- If you want to comment out the entire service, comment out the base handle. If no "A" is defined, the software will ignore "A1", "A2" and so on.

Contacting Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

On the Web: http://fte.com/support/supportrequest.aspx

Email: tech_support@fte.com

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

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Instructional Videos

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

Appendicies

Appendix A: Sodera LE Technical Specifications/Service Information

- Dimensions: 160 mm wide X 56 mm tall X 167 mm deep (6.3” X 2.2" X 6.6")
- Weight: 1.4 kg (3.1 lb)
- Humidity: Operating: 0% - 90% (0 °C – 35 °C), non-condensing
- Temperature: 0 °C to +40 °C (32 °F to +104 °F)
- Power Input: 9 VDC (tip positive)
- Max Power: 12 W

Service Notes

The Sodera LE hardware does not contain any user serviceable items. Any repairs and maintenance must be performed by a service technician that has been trained and approved by Frontline.

Before any service is performed on the Sodera LE hardware, all power sources must be removed. This includes disconnecting any power sources from the **DC9V** input power connector on the rear panel.

Appendix B: Application Notes

B.1 Decrypting Encrypted Bluetooth® low energy

B.1.1 How Encryption Works in *Bluetooth* low energy

Data encryption is used to prevent passive and active—man-in-the-middle (MITM) — eavesdropping attacks on a *Bluetooth* low energy link. Encryption is the means to make the data unintelligible to all but the *Bluetooth* master and slave devices forming a link. Eavesdropping attacks are directed on the over-the-air transmissions between the *Bluetooth* low energy devices, so data encryption is accomplished prior to transmission using a shared, secret key.

B.1.2 Pairing

A *Bluetooth* low energy device that wants to share secure data with another device must first pair with that device. The Security Manager Protocol (SMP) carries out the pairing in three phases.

1. The two connected *Bluetooth* low energy devices announce their input and output capabilities and from that information determine a suitable method for phase 2.
2. The purpose of this phase is to generate the Short Term Key (STK) used in the third phase to secure key distribution. The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.
3. In this phase each device may distribute to the other device up to three keys:
    a. the Long Term Key (LTK) used for Link Layer encryption and authentication,
    b. the Connection Signature Resolving Key (CSRK) used for data signing at the ATT layer, and
    c. the Identity Resolving Key (IRK) used to generate a private address.

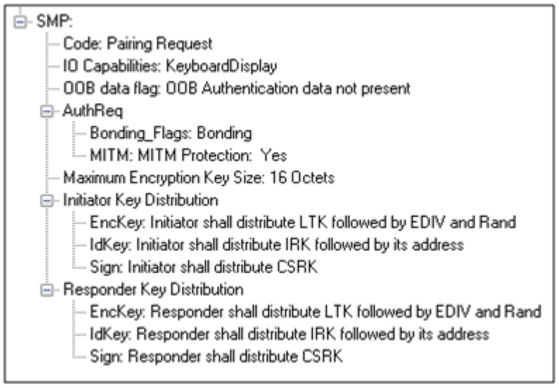
    Of primary interest in this paper is the LTK. CSRK and IRK are covered briefly at the end.

Bluetooth low energy uses the same pairing process as Classic *Bluetooth*: Secure Simple Pairing (SSP). During SSP initially each device determines its capability for input and output (IO). The input can be None, Yes/No, or Keyboard with Keyboard having the ability to input a number. The output can be either None or Display with Display having the ability to display a 6-digit number. For each device in a paring link the IO capability determines their ability to create encryption shared secret keys.

The Pairing Request message is transmitted from the initiator containing the IO capabilities, authentication data availability, authentication requirements, key size requirements, and other data. A Pairing Response message is transmitted from the responder and contains much of the same information as the initiators Pairing Request message thus confirming that a pairing is successfully negotiated.

In the sample SMP decode, in the figure at the right, note the "keys" identified. Creating a shared, secret key is an evolutionary process that involves several intermediary keys. The resulting keys include,

1. IRK: 128-bit key used to generate and resolve random address.
2. CSRK: 128-bit key used to sign data and verify signatures on the receiving device.
3. LTK: 128-bit key used to generate the session key for an encrypted connection.
4. Encrypted Diversifier (EDIV): 16-bit stored value used to identify the LTK. A new EDIV is generated each time a new LTK is distributed.
5. Random Number (RAND): 64-bit stored value used to identify the LTK. A new RAND is generated each time a unique LTK is distributed.



```
SMP:
  Code: Pairing Request
  IO Capabilities: KeyboardDisplay
  OOB data flag: OOB Authentication data not present
  AuthReq
    Bonding_Flags: Bonding
    MITM: MITM Protection:  Yes
  Maximum Encryption Key Size: 16 Octets
  Initiator Key Distribution
    EncKey: Initiator shall distribute LTK followed by EDIV and Rand
    IdKey: Initiator shall distribute IRK followed by its address
    Sign: Initiator shall distribute CSRK
  Responder Key Distribution
    EncKey: Responder shall distribute LTK followed by EDIV and Rand
    IdKey: Responder shall distribute IRK followed by its address
    Sign: Responder shall distribute CSRK
```

Figure 1 - Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

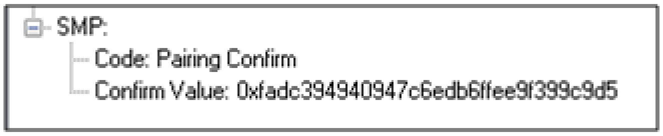
Of particular importance to decrypting the encrypted data on a *Bluetooth* low energy link is LTK, EDIV, and RAND.

B.1.3 Pairing Methods

The two devices in the link use the IO capabilities from Pairing Request and Pairing Response packet data to determine which of two pairing methods to use for generation of the Temporary Key (TK). The two methods are **Just Works** and **Passkey Entry**[1]. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

In **Just Works** the TK = 0. In the **Passkey Entry** method,

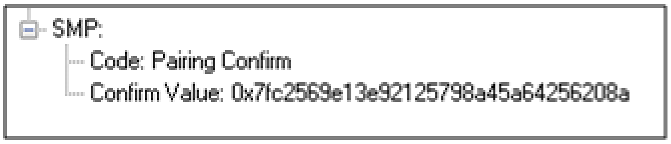
$$TK = \begin{cases} \textbf{6 numeric digits, Input} = \textbf{Keyboard} \\ \textbf{6 random digits, Input} = \textbf{Display} \end{cases}$$



```
SMP:
  Code: Pairing Confirm
  Confirm Value: 0xfadc394940947c6edb6ffee9f399c9d5
```

Figure 2 - Initiator Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

[1] A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link such as NFC.



```
SMP:
  Code: Pairing Confirm
  Confirm Value: 0x7fc2569e13e92125798a45a64256208a
```

Figure 3 - Responder Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

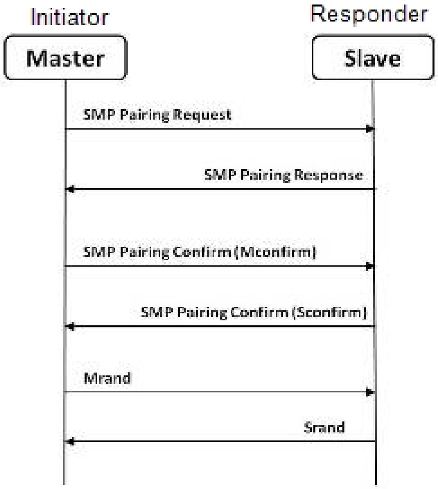


Figure 4 - Message Sequence Chart: SMP Pairing

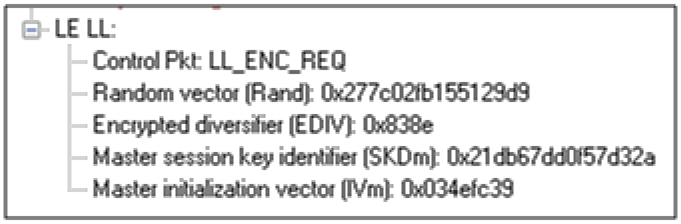
The initiating device will generate a 128-bit random number that is combined with TK, the Pairing Request command, the Pairing Response command, the initiating device address and address type, and the responding device address and address type. The resulting value is a random number **Mconfirm** that is sent to the responding device by the Pairing Confirm command. The responding device will validate the responding device data in the Pairing Confirm command and if it is correct will generate a **Sconfirm** value using the same methods as used to generate **Mconfirm** only with different 128-bit random number and TK. The responding device will send a Pairing Confirm command to the initiator and if accepted the authentication process is complete. The random number in the **Mconfirm** and **Sconfirm** data is **Mrand** and **Srand** respectively. **Mrand** and **Srand** have a key role in setting encrypting the link.

Finally the master and slave devices exchange **Mrand** and **Srand** so that the slave can calculate and verify Mconfirm and the master can likewise calculate and verify Sconfirm.

B.1.4 Encrypting the Link

The Short Term Key (STK) is used for encrypting the link the first time the two devices pair. STK remains in each device on the link and is not transmitted between devices. STK is formed by combining **Mrand** and **Srand** which were formed using device information and TKs exchanged with Pairing Confirmation (**Pairing Confirm**).

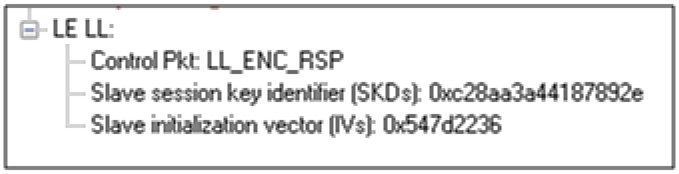
B.1.5 Encryption Key Generation and Distribution



```
LE LL:
  Control Pkt: LL_ENC_REQ
  Random vector (Rand): 0x277c02fb155129d9
  Encrypted diversifier (EDIV): 0x838e
  Master session key identifier (SKDm): 0x21db67dd0f57d32a
  Master initialization vector (IVm): 0x034efc39
```

Figure 5 - Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

To distribute the LTK, EDIV, and Rand values an encrypted session needs to be set up. The initiator will use STK to enable encryption on the link. Once an encrypted link is set up, the LTK is distributed. LTK is a 128-bit random number that the slave device will generate along with EDIV and Rand. Both the master and slave devices can distribute these numbers, but *Bluetooth* low energy is designed to conserve energy, so the slave device is often resource constrained and does not have the database storage resources for holding LTKs. Therefore the slave will distribute LTK, EDIV, and Rand to the master device for storage. When a slave begins a new encrypted session with a previously linked master device, it will request distribution of EDIV and Rand and will regenerate LTK.



LE LL:
Control Pkt: LL_ENC_RSP
Slave session key identifier (SKDs): 0xc28aa3a44187892e
Slave initialization vector (IVs): 0x547d2236

Figure 6 - Encryption Response from Slave, Example (ComProbe Frame Display, BPA 600 low energy capture)

B.1.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the master device to send Link Layer encryption request message (LL_ ENC_REQ) that contains the SKD_{master}. The SKD_{master} is generated using the LTK. The slave receives SKD_{master}, generates SKD_{slave}, and generates SK by concatenating parts of SKD_{master} and SKD_{slave}. The slave device responds with an encryption response message (LL_ENC_RSP) that contains SKD_{slave}; the master will create the same SK.

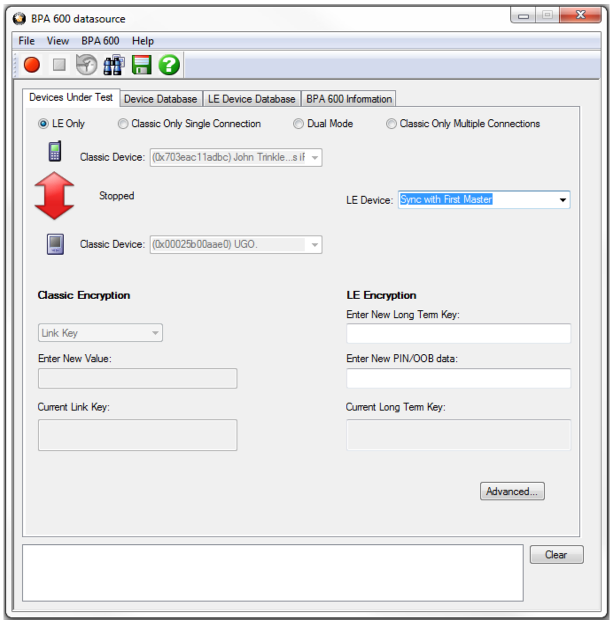
Now that a SK has been calculated, the master and slave devices will now begin a handshake process. The slave will transmit unencrypted LL_START_ENC_REQ, but sets the slave to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_ENC_RSP that uses the same SK just calculated and setting the master to receive encrypted data. Once the slave receives the master’s encrypted LL_START_ENC_RSP message and responds with an encrypted LL_START_ENC_RSP message the *Bluetooth* low energy devices can now begin transmitting and receiving encrypted data.

B.1.7 Decrypting Encrypted Data Using Frontline® BPA 600 low energy Capture

Note: The following discussion uses the ComProbe BPA 600 in low energy capture mode to illustrate how to identify the encryption process and to view decrypted data. However any of the ComProbe devices (BPA 500, BPA low energy) that are low energy capable will accomplish the same objectives, although the datasource setup will be slightly different for each device.

B.1.7.1 Setting up the BPA 600

1. Run the ComProbe Protocol Analysis Software and select **Bluetooth Classic/low energy (BPA 600)**. This will bring up the **BPA 600 datasource** window. This is where the parameters are set for sniffing, including the devices to be sniffed and how the link is to be decrypted.
2. Select **Devices Under Test** tab on the Datasource window.
3. Click/select **LE Only**.
4. To decrypt encrypted data transmissions between the *Bluetooth* low energy devices the ComProbe analyzer needs to know the LTK because this is the shared secret used to encrypt the session. There are two ways to provide this information and which to select will depend on the pairing method: **Just Works** or **Passkey Entry**.



● LE Only ○ Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Classic Device: (0x703eac11adbc) John Trinkle...s iF

Stopped

LE Device: Sync with First Master

Classic Device: (0x00025b00aae0) UGO.

Classic Encryption

Link Key

Enter New Value:

Current Link Key:

LE Encryption

Enter New Long Term Key:

Enter New PIN/OOB data:

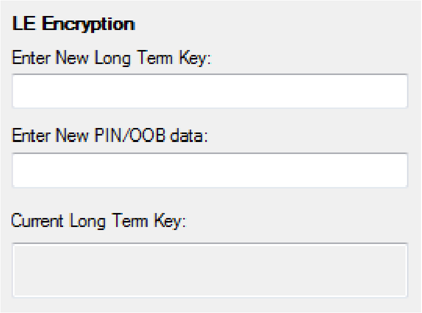
Current Long Term Key:

Figure 7 - ComProbe BPA 600 low energy only datasource settings

a. **Passkey Entry** is easiest if you have the code that was displayed or entered during device pairing. The code is what is used to generate the LTK. Under **LE Encryption** enter the code in the **Enter New PIN/OOB** data text box.

b. **Just Works** is more of a challenge because you must know the LTK that is created at the time of pairing and identification of an encrypted link.

- If your device was previously used in an encrypted capture session, the device information including LTK can be found in the **Device Database** tab.
- In a design and development environment the LTK is often known beforehand.



LE Encryption

Enter New Long Term Key:

Enter New PIN/OOB data:

Current Long Term Key:

Figure 8 - BPA 600 datasource Encryption Key Entry

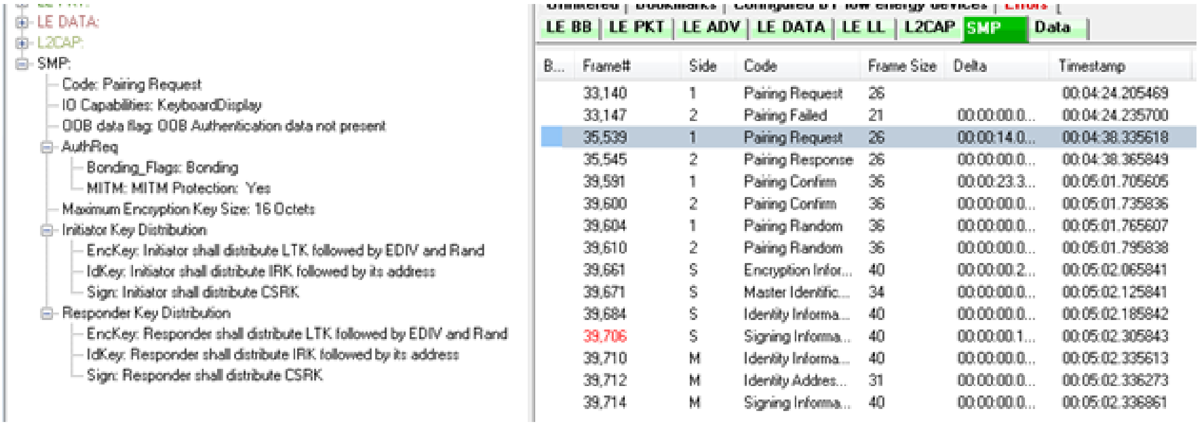
- Capture of Host Controller Interface (HCI) events using ComProbe HSU can reveal the LTK, which is contained in the HCI_Link_Key_Request_Reply command. HCI capture is through direct connection to the device host controller. The information obtained in a direct connection can later be used in a wireless encrypted capture session that requires prior knowledge of encryption keys.

5. To start capture click on the Start Sniffing button ● on the **BPA 600 datasource** toolbar.

B.1.7.2 Use Frame Display to View Encryption/Decryption Process

B.1.7.2.1 Security Manager Protocol

The Security Manager Protocol (SMP) controls the process for pairing and key distribution. The results of a pairing and key distribution can be observed in the ComProbe software **Frame Display**. Activate the **Frame Display** by clicking on the icon on the **Control** window toolbar. On the **Frame Display** low energy protocols are shown in light green tabs. Click on the **SMP** protocol tab that will show only the SMP commands from the full data set.



```
SMP:
    Code: Pairing Request
    IO Capabilities: KeyboardDisplay
    OOB data flag: OOB Authentication data not present
    AuthReq
        Bonding_Flags: Bonding
        MITM: MITM Protection:  Yes
    Maximum Encryption Key Size: 16 Octets
    Initiator Key Distribution
        EncKey: Initiator shall distribute LTK followed by EDIV and Rand
        IdKey: Initiator shall distribute IRK followed by its address
        Sign: Initiator shall distribute CSRK
    Responder Key Distribution
        EncKey: Responder shall distribute LTK followed by EDIV and Rand
        IdKey: Responder shall distribute IRK followed by its address
        Sign: Responder shall distribute CSRK
```

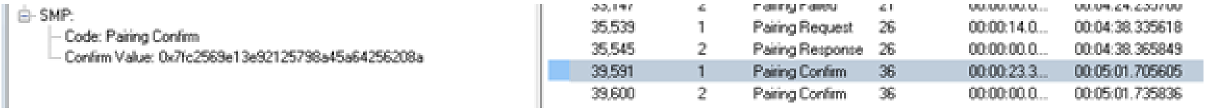
B...	Frame#	Side	Code	Frame Size	Delta	Timestamp
	33,140	1	Pairing Request	26		00:04:24.205469
	33,147	2	Pairing Failed	21	00:00:00.0...	00:04:24.235700
	35,539	1	Pairing Request	26	00:00:14.0...	00:04:38.335618
	35,545	2	Pairing Response	26	00:00:00.0...	00:04:38.365849
	39,591	1	Pairing Confirm	36	00:00:23.3...	00:05:01.705605
	39,600	2	Pairing Confirm	36	00:00:00.0...	00:05:01.735836
	39,604	1	Pairing Random	36	00:00:00.0...	00:05:01.765607
	39,610	2	Pairing Random	36	00:00:00.0...	00:05:01.795838
	39,661	S	Encryption Infor...	40	00:00:00.2...	00:05:02.065841
	39,671	S	Master Identific...	34	00:00:00.0...	00:05:02.125841
	39,684	S	Identity Informa...	40	00:00:00.0...	00:05:02.185842
	39,706	S	Signing Informa...	40	00:00:00.1...	00:05:02.305843
	39,710	M	Identity Informa...	40	00:00:00.0...	00:05:02.335613
	39,712	M	Identity Addres...	31	00:00:00.0...	00:05:02.336273
	39,714	M	Signing Informa...	40	00:00:00.0...	00:05:02.336861

Figure 9 - SMP Pairing Request (Frame# 35,539) from Initiator (Side 1)

On the left side of the figure above is the **Frame Display Decoder** pane that shows the decoded information supplied in the selected frame in the Summary pane, Frame# 35,539. Shown is the SMP data associated with and encrypted link (MITM Protection = Yes). The requested keys are also shown. Selecting Frame# 35,545 would provide the response from the responder (Side 2) and would contain similar information.

Selecting Frame# 39,591 will display the Pairing Confirm from the initiator (Side 1) in the **Decoder** pane. The Confirm Value shown is the Mconfirm 128-bit random number that contains TK, Pairing Request command, Pairing Response command, initiating device address, and the responding device address. Selecting Frame# 39,600 would provide the Sconfirm random number from the responder (Side 2) with similar information from that device but the random number would be different than Mconfirm.

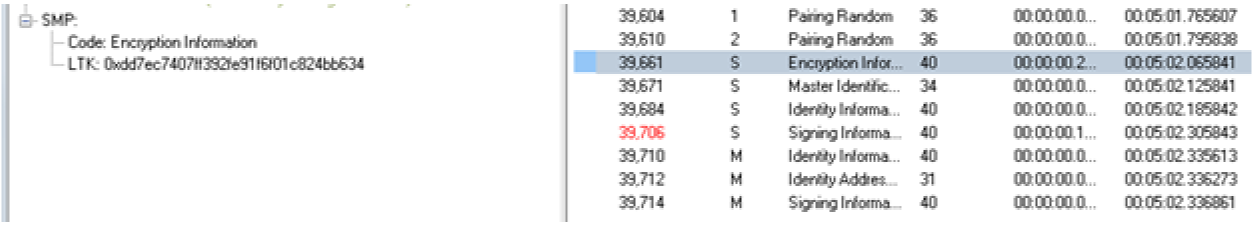
Once pairing is complete and an encrypted session established, the keys are distributed by the master and slave now identified by Side = M and Side = S respectively in the **Summary** pane. In Frame# 39,661 the slave has distributed LTK to the master to allow exchange of encrypted data. Frame# 39,661 through 39,714 in the Summary pane SMP tab are the key distribution frames.



```
SMP:
    Code: Pairing Confirm
    Confirm Value: 0x7fc2569e13e92125798a45a64256208a
```

33,147	2	Pairing Failed	21	00:00:00.0...	00:04:24.235700
35,539	1	Pairing Request	26	00:00:14.0...	00:04:38.335618
35,545	2	Pairing Response	26	00:00:00.0...	00:04:38.365849
39,591	1	Pairing Confirm	36	00:00:23.3...	00:05:01.705605
39,600	2	Pairing Confirm	36	00:00:00.0...	00:05:01.735836

Figure 10 - SMP Pairing Confirm (Frame# 39,591) from Initiator (Side 1)



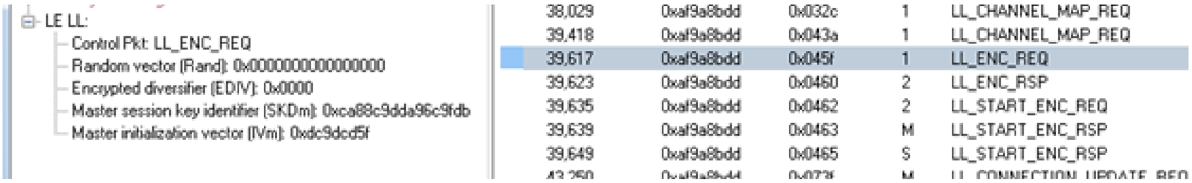
SMP:
- Code: Encryption Information
- LTK: 0xdd7ec7407ff392fe91f6f01c824bb634

39,604	1	Pairing Random	36	00:00:00.0...	00:05:01.765607
39,610	2	Pairing Random	36	00:00:00.0...	00:05:01.795838
39,661	S	Encryption Infor...	40	00:00:00.2...	00:05:02.065841
39,671	S	Master Identific...	34	00:00:00.0...	00:05:02.125841
39,684	S	Identity Informa...	40	00:00:00.0...	00:05:02.185842
39,706	S	Signing Informa...	40	00:00:00.1...	00:05:02.305843
39,710	M	Identity Informa...	40	00:00:00.0...	00:05:02.335613
39,712	M	Identity Addres...	31	00:00:00.0...	00:05:02.336273
39,714	M	Signing Informa...	40	00:00:00.0...	00:05:02.336861

Figure 11 - SMP Key Distribution Frames

B.1.7.2.2 Link Layer

The Link Layer (LL) protocol manages the *Bluetooth* low energy radio transmissions and is involved in starting link encryption. To observe the decoded LL commands, click on the **Frame Display LE LL** tab, search for and select ControlPkt “LL_ENC_REQ”. This command should originate with Side 1, the initiator of the encryption link. In Figure 11 Frame# 39,617 is selected in the Summary pane and we see the decoded LE LL frame is display in the **Decoder** pane. Shown in this frame packet is the SKDm that is the Master Session Key Diversifier (SKDmaster). In Frame# 39,623 you will find SKDslave that is combined with SKDmaster to create the Session Key (SK). Both SDKs were created using the LTK. Frame# 39,635 through 39,649 in the **LE LL** tab completes starting of the encryption process. After the slave sends LL_START_ENC_RSP (Frame# 36,649) the *Bluetooth* devices can exchange encrypted data, and the ComProbe sniffing device can also receive and decrypt the encrypted data because the appropriate “key” is provided in the **BPA 600 Datasource** window.

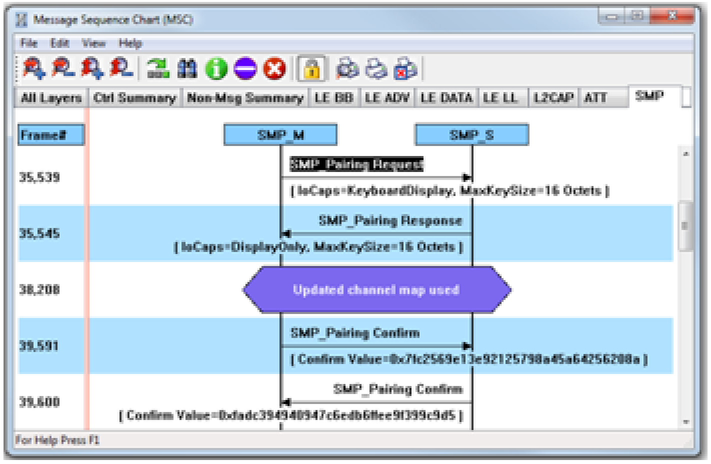


LE LL:
- Control Pkt: LL_ENC_REQ
- Random vector (Rand): 0x0000000000000000
- Encrypted diversifier (EDIV): 0x0000
- Master session key identifier (SKDm): 0xca88c9dda96c9fdb
- Master initialization vector (IVm): 0xdc9dcd5f

38,029	0xaf9a8bdd	0x032c	1	LL_CHANNEL_MAP_REQ
39,418	0xaf9a8bdd	0x043a	1	LL_CHANNEL_MAP_REQ
39,617	0xaf9a8bdd	0x045f	1	LL_ENC_REQ
39,623	0xaf9a8bdd	0x0460	2	LL_ENC_RSP
39,635	0xaf9a8bdd	0x0462	2	LL_START_ENC_REQ
39,639	0xaf9a8bdd	0x0463	M	LL_START_ENC_RSP
39,649	0xaf9a8bdd	0x0465	S	LL_START_ENC_RSP
43,250	0xaf9a8bdd	0x073f	M	LL_CONNECTION_UPDATE_REQ

Figure 12 - LE LL Tab Encryption Request (Frame# 39,617) from Initiator (Side 1)

B.1.7.3 Viewing Encryption in the Message Sequence Chart



35,539 SMP_Pairing Request [IoCaps=KeyboardDisplay, MaxKeySize=16 Octets]

35,545 SMP_Pairing Response [IoCaps=DisplayOnly, MaxKeySize=16 Octets]

38,208 Updated channel map used

39,591 SMP_Pairing Confirm [Confirm Value=0x7fc2569e13e92125798a45a64256208a]

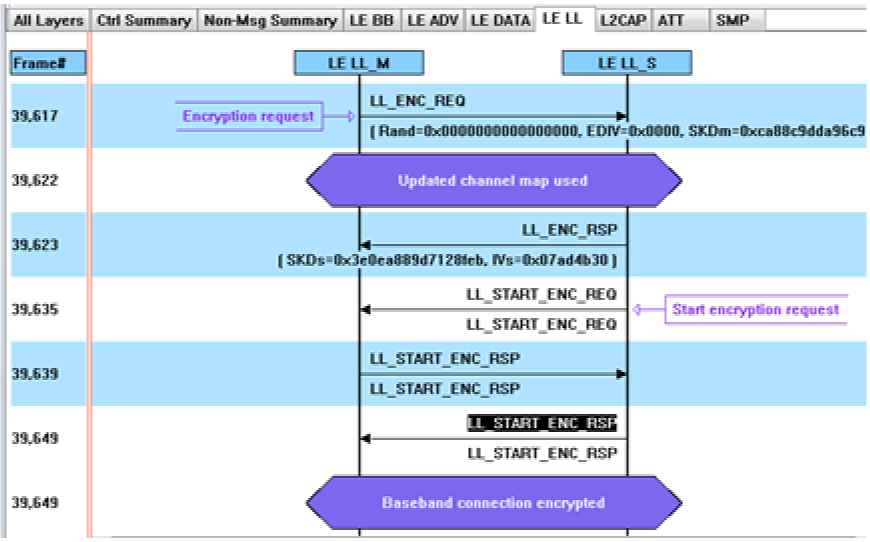
39,600 SMP_Pairing Confirm [Confirm Value=0xdadc394940947c6edb6ffee9f399c9d5]

Figure 13 - MSC SMP Paring (BPA 600 low energy capture)

The ComProbe software **Message Sequence Chart** (**MSC**) links directly to frames being viewed in the Frame Display. Similarly MSC will display the same information as the **Frame Display Decoder** pane. Frames are synchronized between the **Frame Display Summary** pane and the **MSC**, so clicking on a frame in either window will select that same frame in the other window. Also the protocol tabs are the same in each window. To see the pairing process, click on the SMP tab.

In the image above we see Frame# 35,539 initiating the pairing from the master device. The response, SMP_Pairing Response, is sent from the slave in Frame# 35,545. SMP_Pairing Confirm occurs between the master and the slave devices at Frame# 39,591 and 39,600 respectively.

Clicking on the **MSC** LE LL tab will show the process of encrypting a session link. Clicking on Frame# 39,617 displays the LL_ENC_REQ command from the master to the slave. In the **MSC** below this command you will see the data transferred that includes SKD$_{master}$ used to generate the LTK. At Frame# 39,623 the slave responds with LL_ENC_RSP sending SKD$_{slave}$ to generate LTK at the master. Up to this point all transmissions are unencrypted. For this example the slave sends the request to start encryption, LL_START_ENC_REQ, at Frame#39,635. The master responds with LL_START_ENC_RSP at Frame# 39,639, and finally the slave responds with LL_START_ENC_RSP at Frame# 36,649. At this point the session link is encrypted.



39,617 LL_ENC_REQ
(Rand=0x0000000000000000, EDIV=0x0000, SKDm=0xca88c9dda96c9

39,622 Updated channel map used

39,623 LL_ENC_RSP
(SKDs=0x3e0ea889d7128feb, IVs=0x07ad4b30)

39,635 LL_START_ENC_REQ
LL_START_ENC_REQ

39,639 LL_START_ENC_RSP
LL_START_ENC_RSP

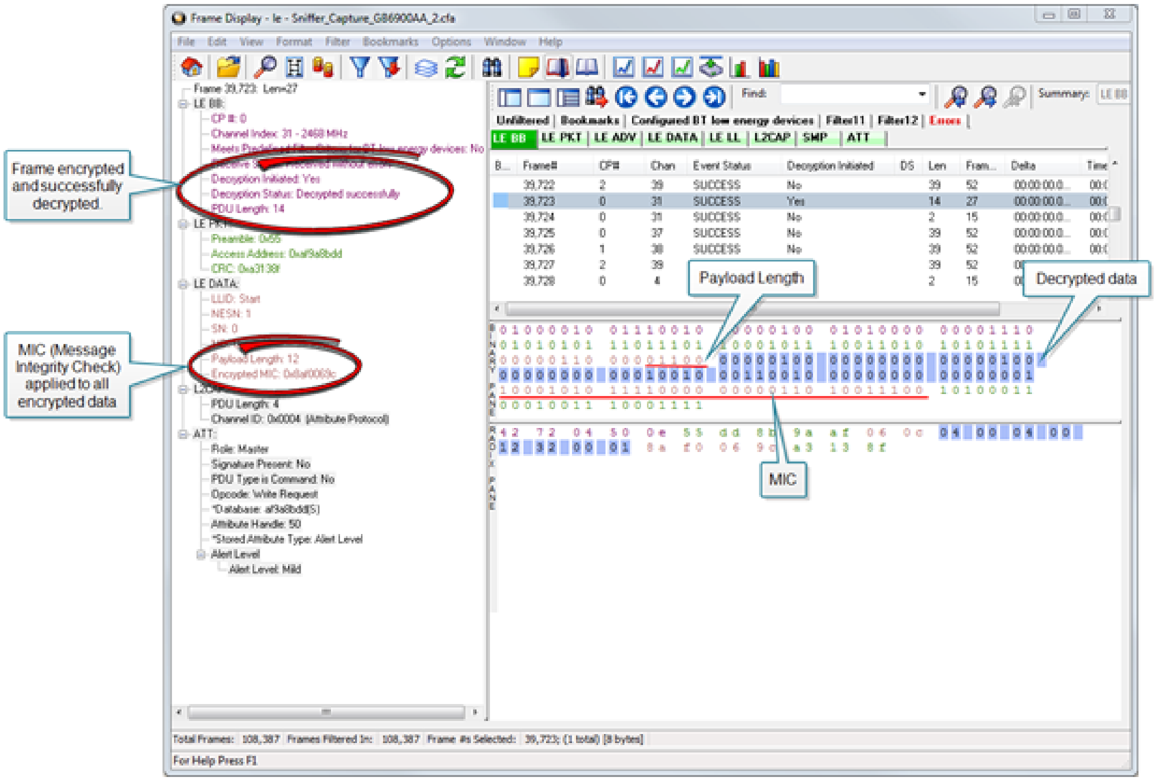
39,649 LL_START_ENC_RSP
LL_START_ENC_RSP

39,649 Baseband connection encrypted

Figure 14 - MSC link Layer Encryption (BPA 600 low energy capture)

B.1.7.4 Viewing Decrypted Data

In the ComProbe software **Frame Display** click on the **LE BB** tab. Search in the **Summary** pane for Decryption Initiated = Yes frames. In the example depicted in the following figure, Frame# 39723 is selected. In the **Decoder** pane LE BB shows that the decryption was initiated and decryption was successful. In LE Data we see the Encrypted MIC value. The MIC value is used to authenticate the sender of the data packet to ensure that the data was sent by a peer device in the link and not by a third party attacker. The actual decrypted data appears between the Payload Length and the MIC in the packet. This is shown in the **Binary** pane below the **Summary** pane.


Frame Display - le - Sniffer_Capture_GB6900AA_2.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: LE BB
Unfiltered | Bookmarks | Configured BT low energy devices | Filter11 | Filter12 | Errors
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT
BINARY PANE
RADIX PANE

Frame encrypted and successfully decrypted.

MIC (Message Integrity Check) applied to all encrypted data

Payload Length

Decrypted data

MIC

```
Frame 39,723: Len=27
LE BB:
   CP #: 0
   Channel Index: 31 - 2468 MHz
   Meets Predefined Filter Criteria for BT low energy devices: No
   Receive Status: Received without error
   Decryption Initiated: Yes
   Decryption Status: Decrypted successfully
   PDU Length: 14
LE PKT:
   Preamble: 0x55
   Access Address: 0xaf9a8bdd
   CRC: 0xa3138f
LE DATA:
   LLID: Start
   NESN: 1
   SN: 0
   MD: 0
   Payload Length: 12
   Encrypted MIC: 0x8af0069c
L2CAP:
   PDU Length: 4
   Channel ID: 0x0004  (Attribute Protocol)
ATT:
   Role: Master
   Signature Present: No
   PDU Type is Command: No
   Opcode: Write Request
   *Database: af9a8bdd[S]
   Attribute Handle: 50
   *Stored Attribute Type: Alert Level
   Alert Level
      Alert Level: Mild
```

B...	Frame#	CP#	Chan	Event Status	Decryption Initiated	DS	Len	Fram...	Delta	Time
	39,722	2	39	SUCCESS	No		39	52	00:00:00.0...	00:(
	39,723	0	31	SUCCESS	Yes		14	27	00:00:00.0...	00:(
	39,724	0	31	SUCCESS	No		2	15	00:00:00.0...	00:(
	39,725	0	37	SUCCESS	No		39	52	00:00:00.0...	00:(
	39,726	1	38	SUCCESS	No		39	52	00:00:00.0...	00:(
	39,727	2	39				39	52	0(	
	39,728	0	4				2	15	0(	

```
0 1 0 0 0 0 1 0   0 1 1 1 0 0 1 0   0 0 0 0 0 1 0 0   0 1 0 1 0 0 0 0   0 0 0 0 1 1 1 0
0 1 0 1 0 1 0 1   1 1 0 1 1 1 0 1   1 0 0 0 1 0 1 1   1 0 0 1 1 0 1 0   1 0 1 0 1 1 1 1
0 0 0 0 0 1 1 0   0 0 0 0 1 1 0 0   0 0 0 0 0 1 0 0   0 0 0 0 0 0 0 0   0 0 0 0 0 1 0 0
0 0 0 0 0 0 0 0   0 0 0 1 0 0 1 0   0 0 1 1 0 0 1 0   0 0 0 0 0 0 0 0   0 0 0 0 0 0 0 1
1 0 0 0 1 0 1 0   1 1 1 1 0 0 0 0   0 0 0 0 0 1 1 0   1 0 0 1 1 1 0 0   1 0 1 0 0 0 1 1
0 0 0 1 0 0 1 1   1 0 0 0 1 1 1 1
```

```
4 2  7 2  0 4  5 0  0 e  5 5  d d  8 b  9 a  a f  0 6  0 c  0 4  0 0  0 4  0 0
1 2  3 2  0 0  0 1  8 a  f 0  0 6  9 c  a 3  1 3  8 f
```

Total Frames: 108,387 Frames Filtered In: 108,387 Frame #s Selected: 39,723; (1 total) [8 bytes]

For Help Press F1

Figure 15 - Decrypted Data Example (Frame# 39,723)

Author: John Trinkle

Publish Date: 9 April 2014

Revised: 23 May 2014

B.2 Bluetooth® low energy Security

"Paris is quiet and the good citizens are content." Upon seizing power in 1799 Napoleon sent this message on Claude Chappe’s optical telegraph. Chappe had invented a means of sending messages line-of-sight . The stations were placed approximately six miles apart and each station had a signaling device made of paddles on the ends of a rotating “regulator” arm whose positions represented code numbers. Each station was also outfitted with two telescopes for viewing the other stations in the link, and clocks were used to synchronize the stations. By 1803 a communications network extended from Paris across the countryside and into Belgium and Italy.

Figure 16 - Chappe's Optical Telegraph

Chappe developed several coding schemes through the next few years. The station operators only knew the codes, not what characters they represented. Not only was Chappe’s telegraph system the first working network with protocols, synchronization of serial transmissions but it also used data encryption. Although cryptography has been around for millenniums—dating back to 2000 B.C. — Chappe, was the first to use it in a wide area network in the modern sense.

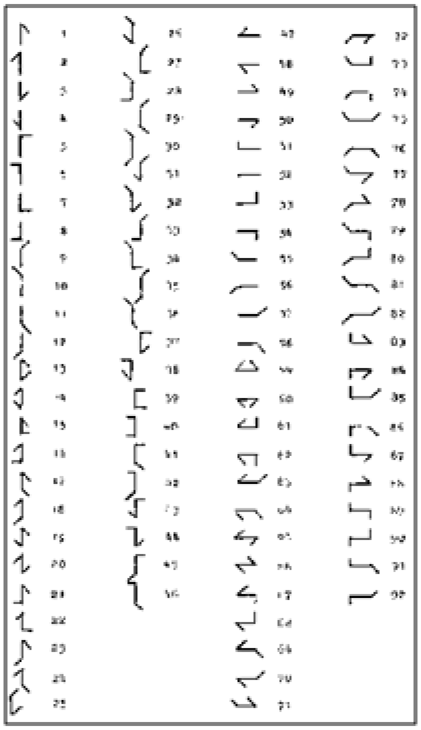


Figure 17 - Chappe's Telegraph Code

Of course anyone positioned between the telegraph stations that had Chappe's telegraph code in hand could decode the transmission. So securing the code was of paramount importance in Chappe's protocol.

Modern wireless networks such as *Bluetooth* low energy employ security measures to prevent similar potentially man-in-the-middle attacks that may have malicious intent.

Bluetooth low energy devices connected in a link can pass sensitive data by setting up a secure encrypted link. The process is similar to but not identical to *Bluetooth* BR/EDR Secure Simple Pairing. One difference is that in *Bluetooth* low energy the confidential payload includes a Message Identification Code (MIC) that is encrypted with the data. In *Bluetooth* BR/EDR only the data is encrypted. Also in Bluetooth low energy the secure link is more vulnerable to passive eavesdropping, however because of the short transmission periods this vulnerability is considered a low risk. The similarity to BR/EDR occurs with "shared secret key", a fundamental building block of modern wireless network security.

This paper describes the process of establishing a *Bluetooth* low energy secure link.

B.2.1 How Encryption Works in *Bluetooth* low energy

Data encryption is used to prevent passive and active—man-in-the-middle (MITM) — eavesdropping attacks on a *Bluetooth* low energy link. Encryption is the means to make the data unintelligible to all but the *Bluetooth* master and slave devices forming a link. Eavesdropping attacks are directed on the over-the-air transmissions between the *Bluetooth* low energy devices, so data encryption is accomplished prior to transmission using a shared, secret key.

B.2.2 Pairing

A *Bluetooth* low energy device that wants to share secure data with another device must first pair with that device. The Security Manager Protocol (SMP) carries out the pairing in three phases.

1. The two connected *Bluetooth* low energy devices announce their input and output capabilities and from that information determine a suitable method for phase 2.

2. The purpose of this phase is to generate the Short Term Key (STK) used in the third phase to secure key distribution. The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.

3. In this phase each device may distribute to the other device up to three keys:

    a. the Long Term Key (LTK) used for Link Layer encryption and authentication,

    b. the Connection Signature Resolving Key (CSRK) used for data signing at the ATT layer, and

c. the Identity Resolving Key (IRK) used to generate a private address.

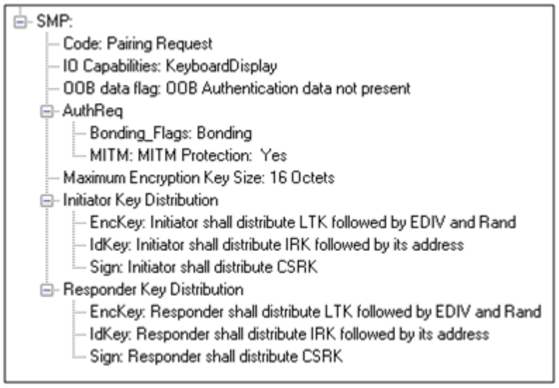
Of primary interest in this paper is the LTK. CSRK and IRK are covered briefly at the end.

Bluetooth low energy uses the same pairing process as Classic *Bluetooth*: Secure Simple Pairing (SSP). During SSP initially each device determines its capability for input and output (IO). The input can be None, Yes/No, or Keyboard with Keyboard having the ability to input a number. The output can be either None or Display with Display having the ability to display a 6-digit number. For each device in a paring link the IO capability determines their ability to create encryption shared secret keys.

The Pairing Request message is transmitted from the initiator containing the IO capabilities, authentication data availability, authentication requirements, key size requirements, and other data. A Pairing Response message is transmitted from the responder and contains much of the same information as the initiators Pairing Request message thus confirming that a pairing is successfully negotiated.

In the sample SMP decode, in the figure at the right, note the "keys" identified. Creating a shared, secret key is an evolutionary process that involves several intermediary keys. The resulting keys include,

1. IRK: 128-bit key used to generate and resolve random address.
2. CSRK: 128-bit key used to sign data and verify signatures on the receiving device.
3. LTK: 128-bit key used to generate the session key for an encrypted connection.
4. Encrypted Diversifier (EDIV): 16-bit stored value used to identify the LTK. A new EDIV is generated each time a new LTK is distributed.
5. Random Number (RAND): 64-bit stored value used to identify the LTK. A new RAND is generated each time a unique LTK is distributed.



```
⊟ SMP:
  ├ Code: Pairing Request
  ├ IO Capabilities: KeyboardDisplay
  ├ OOB data flag: OOB Authentication data not present
  ⊟ AuthReq
  │  ├ Bonding_Flags: Bonding
  │  └ MITM: MITM Protection:  Yes
  ├ Maximum Encryption Key Size: 16 Octets
  ⊟ Initiator Key Distribution
  │  ├ EncKey: Initiator shall distribute LTK followed by EDIV and Rand
  │  ├ IdKey: Initiator shall distribute IRK followed by its address
  │  └ Sign: Initiator shall distribute CSRK
  ⊟ Responder Key Distribution
     ├ EncKey: Responder shall distribute LTK followed by EDIV and Rand
     ├ IdKey: Responder shall distribute IRK followed by its address
     └ Sign: Responder shall distribute CSRK
```

Figure 18 - Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

Of particular importance to decrypting the encrypted data on a *Bluetooth* low energy link is LTK, EDIV, and RAND.

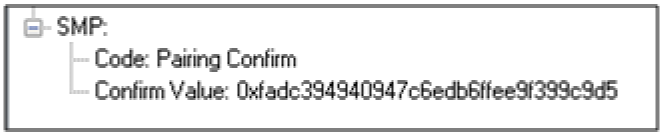
B.2.3 Pairing Methods

The two devices in the link use the IO capabilities from Pairing Request and Pairing Response packet data to determine which of two pairing methods to use for generation of the Temporary Key (TK). The two methods are **Just Works** and **Passkey Entry**[1]. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

In **Just Works** the TK = 0. In the **Passkey Entry** method,

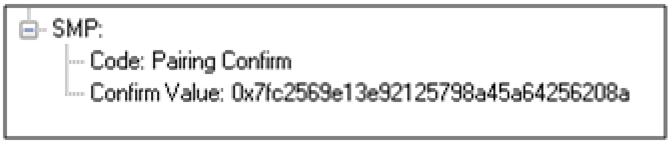
$$TK = \begin{cases} \textbf{6 numeric digits, Input} = \textbf{Keyboard} \\ \textbf{6 random digits, Input} = \textbf{Display} \end{cases}$$

[1] A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link such as NFC.



```
SMP:
    Code: Pairing Confirm
    Confirm Value: 0xfadc394940947c6edb6ffee9f399c9d5
```

Figure 19 - Initiator Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)



```
SMP:
    Code: Pairing Confirm
    Confirm Value: 0x7fc2569e13e92125798a45a64256208a
```

Figure 20 - Responder Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

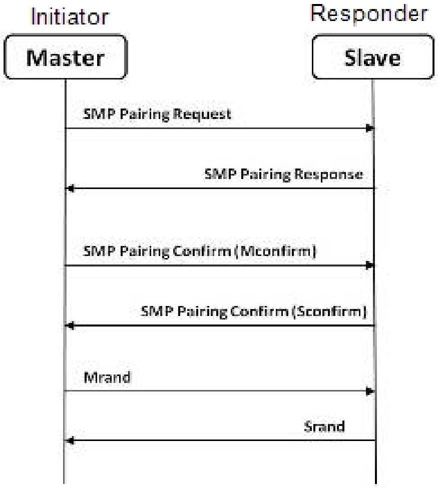


Figure 21 - Message Sequence Chart: SMP Pairing

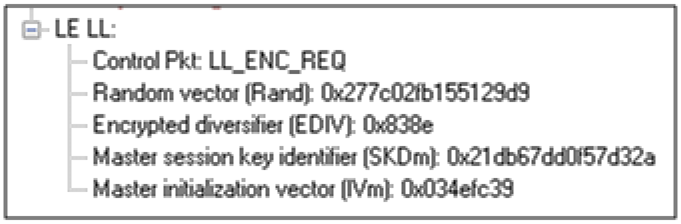
The initiating device will generate a 128-bit random number that is combined with TK, the Pairing Request command, the Pairing Response command, the initiating device address and address type, and the responding device address and address type. The resulting value is a random number **Mconfirm** that is sent to the responding device by the Pairing Confirm command. The responding device will validate the responding device data in the Pairing Confirm command and if it is correct will generate a **Sconfirm** value using the same methods as used to generate **Mconfirm** only with different 128-bit random number and TK. The responding device will send a Pairing Confirm command to the initiator and if accepted the authentication process is complete. The random number in the **Mconfirm** and **Sconfirm** data is **Mrand** and **Srand** respectively. **Mrand** and **Srand** have a key role in setting encrypting the link.

Finally the master and slave devices exchange **Mrand** and **Srand** so that the slave can calculate and verify Mconfirm and the master can likewise calculate and verify Sconfirm.

B.2.4 Encrypting the Link

The Short Term Key (STK) is used for encrypting the link the first time the two devices pair. STK remains in each device on the link and is not transmitted between devices. STK is formed by combining **Mrand** and **Srand** which were formed using device information and TKs exchanged with Pairing Confirmation (**Pairing Confirm**).

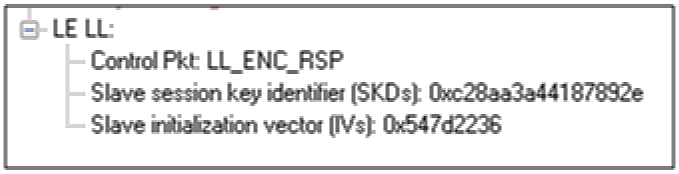
B.2.5 Encryption Key Generation and Distribution



```
LE LL:
    Control Pkt: LL_ENC_REQ
    Random vector (Rand): 0x277c02fb155129d9
    Encrypted diversifier (EDIV): 0x838e
    Master session key identifier (SKDm): 0x21db67dd0f57d32a
    Master initialization vector (IVm): 0x034efc39
```

Figure 22 - Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

To distribute the LTK, EDIV, and Rand values an encrypted session needs to be set up. The initiator will use STK to enable encryption on the link. Once an encrypted link is set up, the LTK is distributed. LTK is a 128-bit random number that the slave device will generate along with EDIV and Rand. Both the master and slave devices can distribute these numbers, but *Bluetooth* low energy is designed to conserve energy, so the slave device is often resource constrained and does not have the database storage resources for holding LTKs. Therefore the slave will distribute LTK, EDIV, and Rand to the master device for storage. When a slave begins a new encrypted session with a previously linked master device, it will request distribution of EDIV and Rand and will regenerate LTK.



```
LE LL:
  Control Pkt: LL_ENC_RSP
  Slave session key identifier (SKDs): 0xc28aa3a44187892e
  Slave initialization vector (IVs): 0x547d2236
```

Figure 23 - Encryption Response from Slave, Example
(ComProbe Frame Display, BPA 600 low energy capture)

B.2.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the master device to send Link Layer encryption request message (LL_ ENC_REQ) that contains the SKD$_{master}$. The SKD$_{master}$ is generated using the LTK. The slave receives SKD$_{master}$, generates SKD$_{slave}$, and generates SK by concatenating parts of SKD$_{master}$ and SKD$_{slave}$. The slave device responds with an encryption response message (LL_ENC_RSP) that contains SKD$_{slave}$; the master will create the same SK.

Now that a SK has been calculated, the master and slave devices will now begin a handshake process. The slave will transmit unencrypted LL_START_ENC_REQ, but sets the slave to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_ENC_RSP that uses the same SK just calculated and setting the master to receive encrypted data. Once the slave receives the master’s encrypted LL_START_ENC_RSP message and responds with an encrypted LL_START_ENC_RSP message the *Bluetooth* low energy devices can now begin transmitting and receiving encrypted data.

B.2.7 IRK and CSRK Revisited

Earlier in this paper it was stated that LTK would be the focus, however the IRK and CSRK were mentioned. We revisit these keys because they are used in situations that require a lesser level of security. First let us note that IRK and CSRK are passed in an encrypted link along with LTK and EDIV.

Use of the IRK and CSRK attempt to place an identity on devices operating in a piconet. The probability that two devices will have the same IRK and generate the same random number is low, but not absolute.

IRK and *Bluetooth* low energy Privacy Feature

Bluetooth low energy has a feature that reduces the ability of an attacker to track a device over a long period buy frequently and randomly changing an advertising device's address. This is the privacy feature. This feature is not used in the discovery mode and procedures but is used in the connection mode and procedures.

If the advertising device was previously discovered and has returned to an advertising state, the device must be identifiable by trusted devices in future connections without going through discovery procedure again. The IRK stored in the trusted device will overcome the problem of maintaining privacy while saving discovery computational load and connection time. The advertising devices IRK was passed to the master device during initial bonding. The a master device will use the IRK to identify the advertiser as a trusted device.

CSRK and Signing for Authentication

Bluetooth low energy supports the ability to authenticate data sent over an unencrypted ATT bearer between two devices in a trust relationship. If authenticated pairing has occurred and encryption is not required (security mode 2) data signing is used if CSRK has been exchanged. The sending device attaches a digital signature after the data in the packet that includes a counter and a message authentication code (MAC). The key used to generate MAC is CSRK. Each peer device in a piconet will have a unique CSRK.

The receiving device will authenticate the message from the trusted sending device using the CSRK exchanged from the sending device. The counter is initialized to zero when the CSRK is generated and is incremented with each message signed with a given CSRK. The combination of the CSRK and counter mitigates replay attacks.

B.2.8 Table of Acronyms

CSRK	Connection Signature Resolving Key
EDIV	Encrypted Diversifier
IO	Input and output
IRK	Identity Resolving Key
LTK	Long Term Key
Mconfirm	128-bit confirm value from initiator
MIC	Message Integrity Check
MITM	Man-in-the-middle
Mrand	128-bit random number used to generate Mconfirm
OOB	Out of Band
RAND	Random Number
Sconfirm	128-bit confirmation value from the responder
SK	Session key
SMP	Security Manager Protocol
Srand	128-bit random number used to generate Sconfirm
SSP	Secure Simple Pairing
STK	Short Term Key
TK	Temporary Key

Author: John Trinkle

Publish Date:21 May 2014

B.3 Bluetooth Virtual Sniffing

B.3.1 Introduction

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

This white paper discusses:

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

B.3.2 Why HCI Sniffing and Virtual Sniffing are Useful

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

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

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

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

B.3.3 *Bluetooth* Sniffing History

Frontline has a strong appreciation for the importance of HCI sniffing because of the way we got involved with *Bluetooth*. Because of our company history, we are uniquely qualified to offer a multi-mode analyzer that provides many ways to sniff and supports a wide variety of protocols. This brief *Bluetooth* sniffing history should help you understand our approach to *Bluetooth* protocol analysis.

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

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

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

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

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

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

B.3.4 Virtual Sniffing—What is it?

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

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

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

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

B.3.5 The Convenience and Reliability of Virtual Sniffing

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

This means:

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

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

B.3.6 How Virtual Sniffing Works

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

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

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

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

B.3.7 Virtual Sniffing and *Bluetooth* Stack Vendors

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

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

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

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

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

B.3.8 Case Studies: Virtual Sniffing and *Bluetooth* Mobile Phone Makers

Case Study # 1

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

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

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

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

Case Study # 2

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

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

B.3.9 Virtual Sniffing and You

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

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

Author: Eric Kaplan

Publish Date: May 2003

Revised: December 2013