TELEDYNE LECROY
Everywhereyoulook™

frontline BPA® 600

DUAL MODE *BLUETOOTH*® PROTOCOL ANALYZER

Hardware and Software User Manual

ProbeSync

ES™ Bluetooth® Protocol Expert System

ES™ Audio Expert System

Revision Date: 3/14/2017

FTS, Frontline, Frontline Test System, ComProbe Protocol Analysis System and ComProbe are registered trademarks of Teledyne LeCroy, Inc.

The following are trademarks of Teledyne LeCroy, Inc.

- BPA 600™
- Audio Expert System™
- Audio Rating Metric™
- ProbeSync™

The Bluetooth SIG, Inc. owns the Bluetooth® word mark and logos, and any use of such marks by Teledyne LeCroy, Inc. is under license.

All other trademarks and registered trademarks are property of their respective owners.

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/bpa600-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 BPA 600 Hardware

2.1.1 Attaching Antennas

When you remove the Frontline BPA 600 hardware from the box, the first step is to attach the antennas (Figure 2.1).

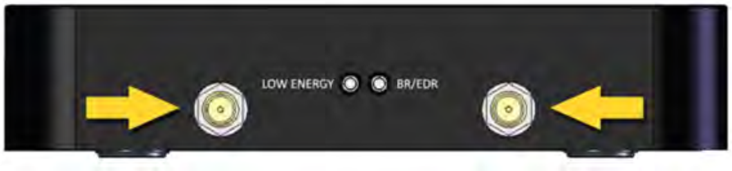


Figure 2.1 - BPA 600 Antenna Connectors

1. Attach antennas to the SMA connectors.

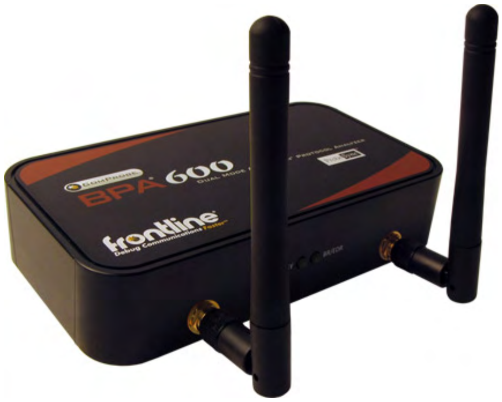


Figure 2.2 - Frontline BPA 600 with both antennas attached

2.1.1.1 Status LED

The Frontline BPA 600 has two Status LEDs on the RF panel. In the front panel center are the **LOW ENERGY** and **BR/EDR** LEDs.

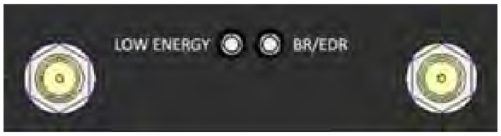


Figure 2.3 - BPA 600 Hardware LEDs

Table 2.1 - Frontline BPA 600 LED Status

LED Color	Frontline BPA 600 Activity
LED Off	Frontline BPA 600 device is idle.
Green	Frontline BPA 600 is actively sniffing waiting for configured devices to connect.
Blue	The configured devices have connected (Asynchronous Connectionless Link (ACL)).
Intermittent Blue	Configured devices are in "Sniff mode" (slave is listening at a reduced rate, conserving device power).

2.1.2 Connecting/Powering the Frontline BPA 600 Hardware

Once you have attached the antennas, the next step is to power up and connect the Frontline BPA 600 hardware to the computer.

1. Insert the USB cable into the USB port on the Frontline BPA 600 hardware. The Frontline BPA 600 analyzer requires no external power (Figure 2.4).

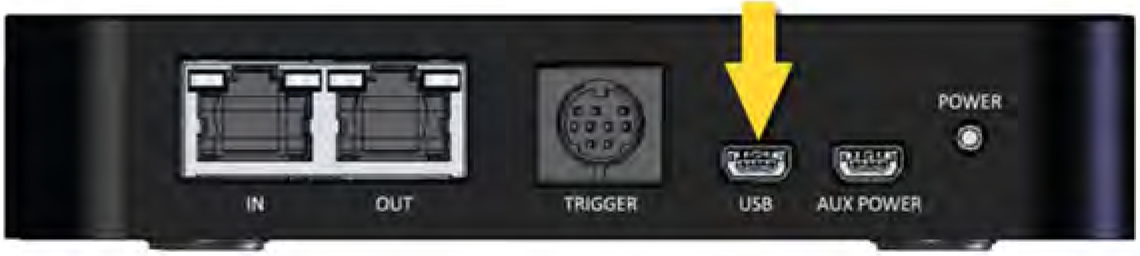


Figure 2.4 - BPA 600 USB Connector

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

The next thing to do is to turn on the devices that you will be testing.

2.1.3 BPA 600 ProbeSync

Any Frontline hardware with ProbeSync™ can be connected together to run off of a common clock, ensuring precise timestamp synchronization.

Simply plug the supplied Cat 5 cable into the **OUT** connector on the sniffer that will be supplying the clock and connect the other end to the **IN** connector on the sniffer receiving the clock. (Figure 2.5 -). If using a BPA 600 analyzer with a different Frontline analyzer, the BPA 600 analyzer must provide the clock. Combined cable length of all the ProbeSync cables connected at a given time should not exceed 1.5 meters (4.5 feet).

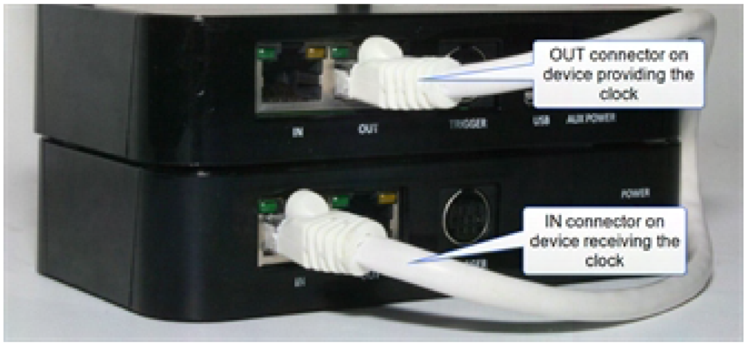

OUT connector on device providing the clock
IN connector on device receiving the clock
IN
OUT
TRIGGER
USB
AUX POWER
POWER

Figure 2.5 - BPA 600 Hardware ProbeSync connection

Connect the CAT 5 cable before connecting the USB cable to the BPA 600 hardware. If you must change the ProbeSync connections it may be necessary to cycle the power to the devices to ensure proper synchronization.

Should the CAT5 cable be connected incorrectly, that is **OUT** to **OUT** or **IN** to **IN**, an error message will appear when the BPA 600 software is run. Refer to on page 79

2.2 Data Capture Methods

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

2.2.1 Opening Data Capture Method

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

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

This opens a standard Windows file folder window.

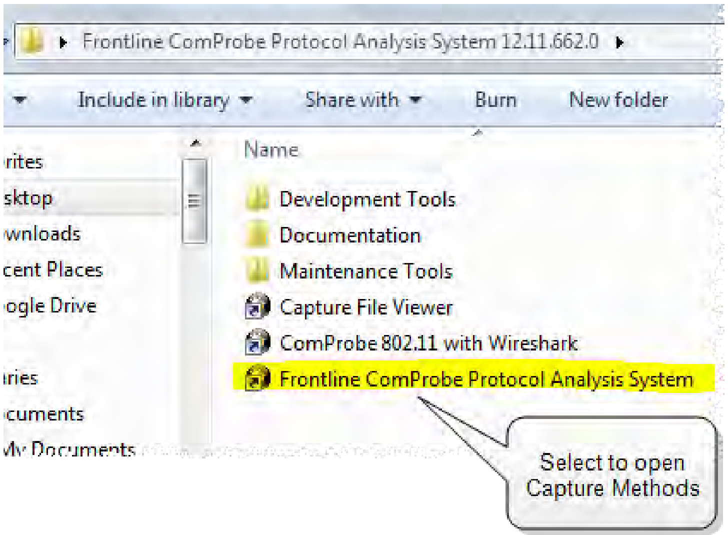
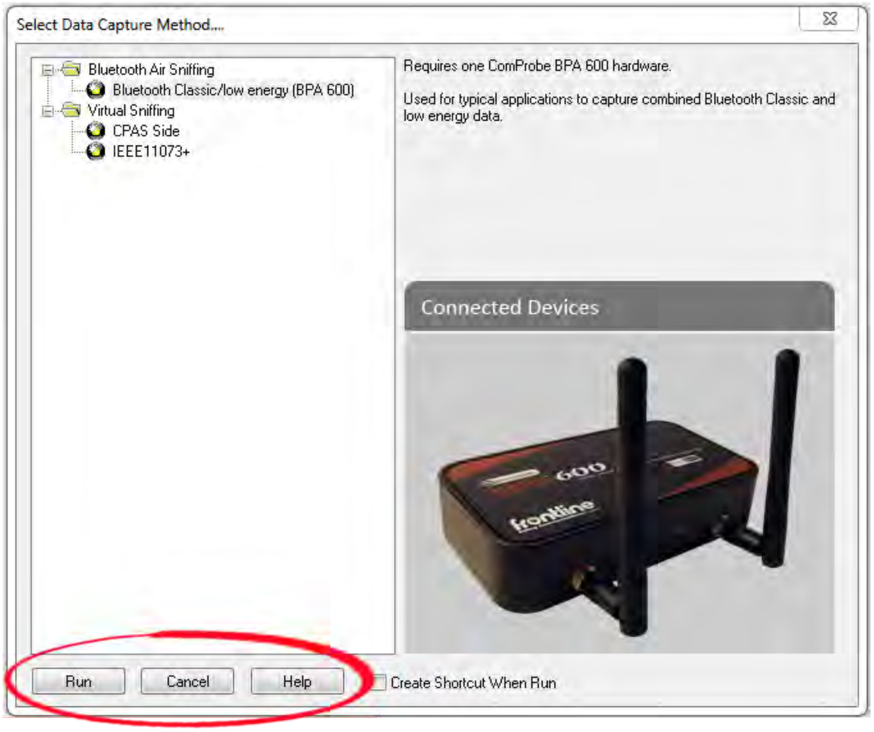


Figure 2.6 - Desktop Folder Link

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

> **Note:** You can also access this dialog by selecting Start > All Programs > Frontline (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 2.7 - Example: Select Data Capture Method..., BPA 600

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

Select Data Capture Method dialog buttons

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

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

4. Click on the Run button and the Frontline Control Window will open configured to the selected capture method.

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

Creating a Shortcut

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

Supporting Documentation

The Frontline <*version #*>directory contains supporting documentation for development (Automation, DecoderScript™, application notes), user documentation (Quick Start Guides and the Frontline User Manual), and maintenance tools.

2.2.2 Frontline BPA 600 Data Capture Methods

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

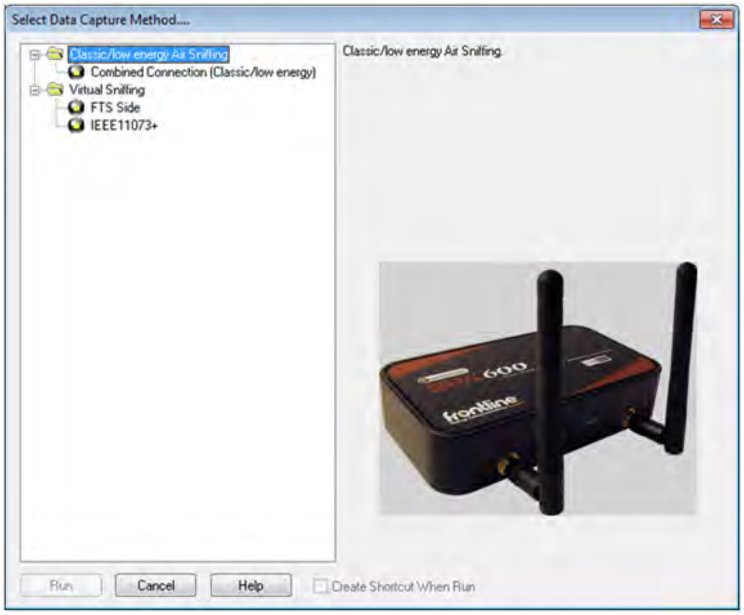

Select Data Capture Method....
Classic/low energy Air Sniffing
Combined Connection (Classic/low energy)
Virtual Sniffing
FTS Side
IEEE11073+
Classic/low energy Air Sniffing.
600
frontline
Run
Cancel
Help
□ Create Shortcut When Run

Figure 2.8 - BPA 600 Data Capture Dialog

- BR/EDR - low energy Air Sniffing
- This method requires one Frontline BPA 600 and is used to capture combined BR/EDR and Bluetooth® low energy data.
- Used for typical applications to capture Classic *Bluetooth* and *Bluetooth* low energy data.

- Modes include:
  - LE Only - *Bluetooth* low energy only
  - Classic Only Single Connection
  - Dual Mode - Classic *Bluetooth* and Bluetooth low energy.
  - Classic Only Multiple Connections
- Classic/low energy/802.11 Air Sniffing (optional)
- Two 802.11 and One BPA600
  - This method requires one Frontline BPA 600 and two Frontline 802.11 hardware.
  - An Frontline 802.11 hardware is included with the Wi-Fi Option.
  - Used for Bluetooth Classic/low energy/802.11 coexistence analysis.
  - Captures Bluetooth Classic, low energy, and 802.11 data and displays in the Frame Display and Coexistence View.
- 802.11/Classic/low energy Coexistence
  - This method requires one Frontline BPA 600 and one Frontline 802.11 hardware.
  - Captures Bluetooth Classic, low energy, and 802.11 data and displays in the Frame Display and Coexistence View.

2.2.3 Frontline ProbeSync™ for Coexistence and Multiple Frontline Device Capture

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

- Classic and low energy *Bluetooth* sniffing, and 802.11
- ProbeSync configurations include
  - ○ Two BPA 600 units
  - ○ One BPA 600 unit and one 802.11 unit.
  - ○ One BPA 600 unit and one HSU unit.
  - ○ One BPA 600 unit, one HSU unit, one 802.11 unit

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

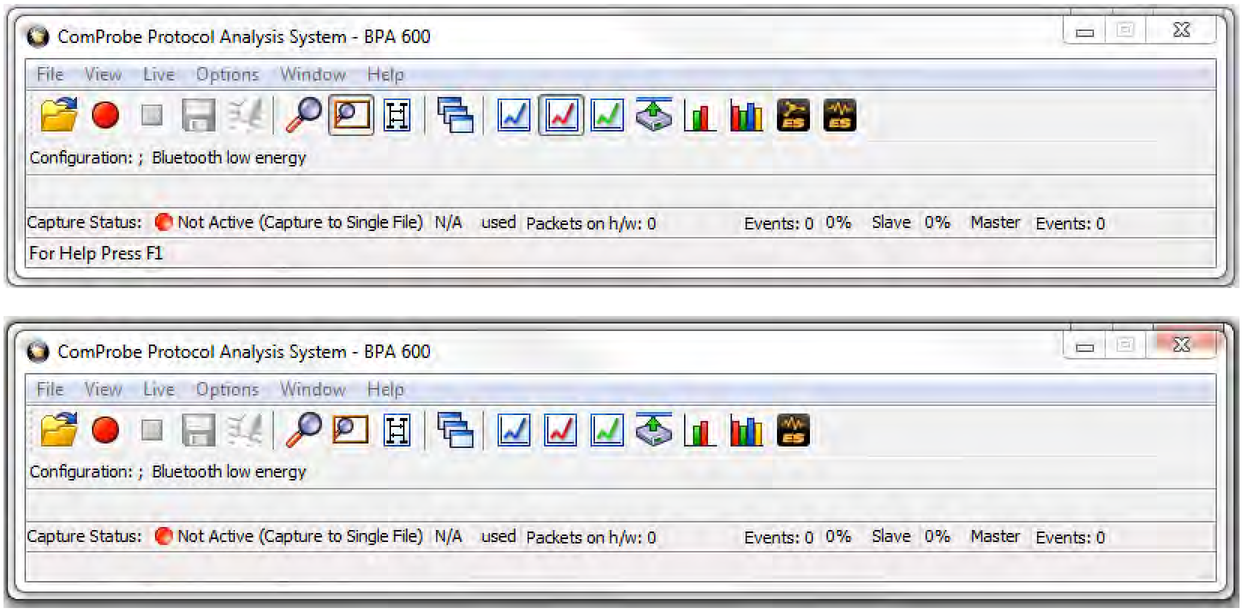
2.2.4 Virtual Sniffing

The Virtual Sniffer is a live import facility within Frontline® software that makes it possible to access any layer in a stack that the programmer has access to and feed this data into the Virtual Sniffer. Please refer to the “Show Live Import Information“ button on the Virtual Sniffer Datasource window in Frontline software. More information is available in the Live Import Developer's Kit located in the Development Tools folder in Frontline Protocol Analysis System desktop folder, and a white paper is available at Bluetooth Virtual Sniffing

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

2.3 Control Window

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


ComProbe Protocol Analysis System - BPA 600
File View Live Options Window Help

Configuration: ; Bluetooth low energy

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

For Help Press F1

ComProbe Protocol Analysis System - BPA 600
File View Live Options Window Help

Configuration: ; Bluetooth low energy

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

Figure 2.9 - 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 2.2 - Control Window Toolbar Icons

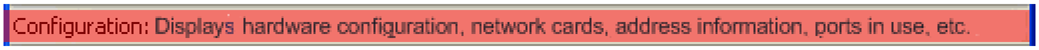
Icon	Description
📂	Open File - Opens a capture file.
⚙	I/O Settings - Opens settings
●	Start Capture - Begins data capture to disk
■	Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.
💾	Save - Saves the capture file.
🧹	Clear - Clears or saves the capture file.
🔍	Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.
🔍	Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.
🗒	Notes - Opens the Notes dialog.
🗗	Cascade - Arranges windows in a cascaded display.
📈	Bluetooth Packet Timeline - Opens the Packet Timeline dialog.
📈	Coexistence View - Opens the Coexistence View dialog.
📈	Low energy - Opens the low energy Timeline dialog.
⏏	Extract Data/Audio - Opens the Extract Data/Audio dialog.
H	MSC Chart - Opens the Message Sequence Chart

Table 2.2 - Control Window Toolbar Icons (continued)

Icon	Description
📊	Bluetooth low energy Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.
📊	Bluetooth Classic Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.
ES	Protocol Expert System - Opens *Bluetooth* Protocol Expert System window
ES	Audio Expert System - Opens Audio Expert System window

2.3.2 Configuration Information on the Control Window

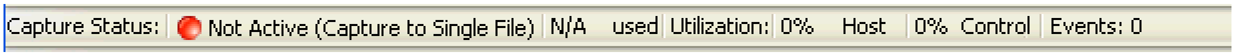
The Configuration bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc.



Configuration: Displays hardware configuration, network cards, address information, ports in use, etc.

2.3.3 Status Information on the Control Window

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



Capture Status: | Not Active (Capture to Single File) | N/A used | Utilization: 0% Host | 0% Control | Events: 0

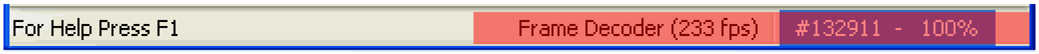
- Capture Status displays Not Active, Paused or Running and refers to the state of data capture.
  - Not Active means that the analyzer is not currently capturing data.
  - Paused means that data capture has been suspended.
  - Running means that the analyzer is actively capturing data.
- % Used

  The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 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 2.3 - 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 86
	Unframe		Removes start-of-frame and end-of-frame markers from your data. SeeUnframing on page 86
	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.

Table 2.3 - Control Window File Menu Selections (continued)

Mode	Selection	Hot Key	Description
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 2.4 - Control Window **View** Menu Selections

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

Table 2.5 - 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.

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

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

Mode	Selection	Hot-Key	Description
The following two rows apply to all Frontline products except Set in Target.			

Table 2.6 - Control Window Live Menu Selections (continued)

Mode	Selection	Hot-Key	Description
Live	**Start Capture**	Shift-F5	Begins data capture from the configured wireless devices.
	Stop Capture	F10	Stops data capture from the configured wireless devices.
The following rows apply to all Frontline products			
Live	Clear	Shift-F10	Clears or saves the capture file.

Table 2.6 - 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 2.6 - Control Window Live Menu Selections (continued)

Mode	Selection	Hot-Key	Description
	Enable/Disable Bluetooth Protocol Expert		When enabled, the Bluetooth Protocol Expert is active, otherwise it is not available. Only available when a Bluetooth Protocol Expert licensed device is connected.
	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 2.7 - 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 2.8 - 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

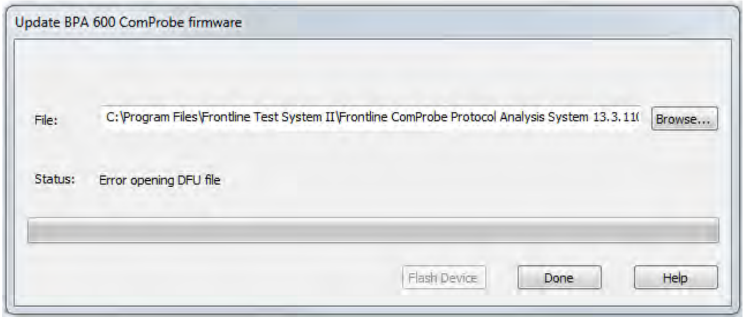
In this section the Frontline software is used to configure an analyzer for capturing data .

3.1 BPA 600 Configuration and I/O

3.1.1 BPA 600 - Update Firmware

When you select the **Update Firmware** on the BPA 600 Information, the **Update ComProbe BPA 600 firmware** dialog appears. You use this dialog to update your ComProbe hardware with the latest firmware.

It is very important that you update the firmware. If the firmware versions are not the same, you will not be able to start sniffing.


Update BPA 600 ComProbe firmware

File: C:\Program Files\Frontline Test System II\Frontline ComProbe Protocol Analysis System 13.3.11

Status: Error opening DFU file

Figure 3.1 - BPA 600 Update Firmware Dialog

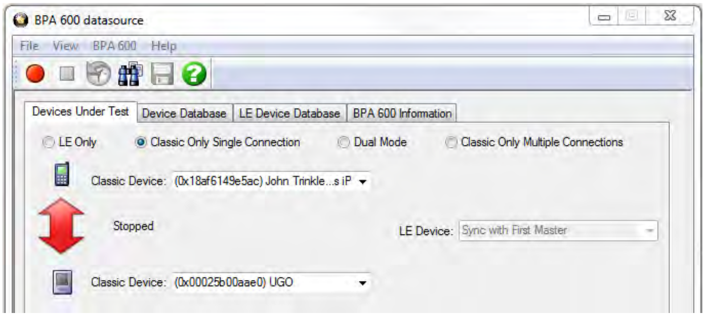
1. Make sure the cabling is attached to the ComProbe hardware.
2. Select Flash Device.

   The download begins, with the Status bar displaying the progress. When the download is complete, you can check the firmware version by checking the Status dialog.

3.1.2 BPA 600 IO Datasource Settings

3.1.2.1 Classic Bluetooth® Roleless Connection

When configuring the ComProbe BPA 600 devices for a Classic *Bluetooth* connection it is no longer necessary to assign a “Master” or “Slave” role to each of the devices. All Classic connection are “roleless”. For example, suppose you have a phone and a speaker as shown below:



○ LE Only ● Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Classic Device: (0x18af6149e5ac) John Trinkle...s iP

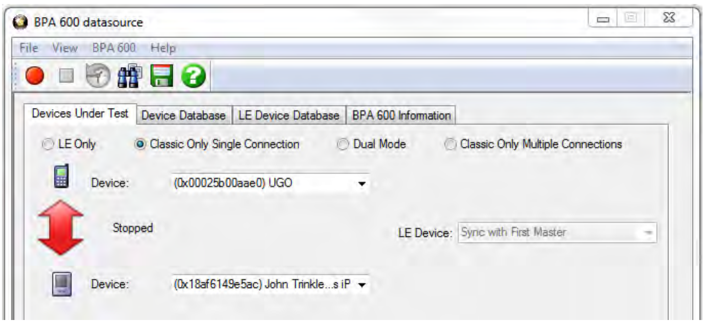
Stopped

LE Device: Sync with First Master

Classic Device: (0x00025b00aae0) UGO

Figure 3.2 - Example of BPA 600 "roleless" Connection

Alternatively, you can enter the devices as follows where **Classic Device** drop down controls have reversed the devices under test shown in the previous image.



○ LE Only ● Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Device: (0x00025b00aae0) UGO

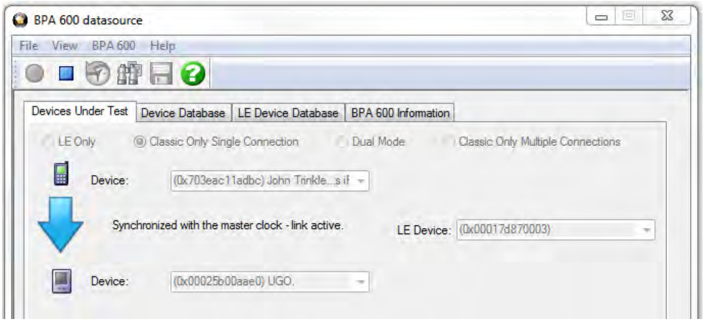
Stopped

LE Device: Sync with First Master

Device: (0x18af6149e5ac) John Trinkle...s iP

Figure 3.3 - Example BPA 600 "roleless" Connection - Switching DUT

It does not matter which position you enter the device. After you have started sniffing and a connection is made, the arrow will indicate the direction of the connection. In the following screen shot the phone has connected as the “Master” to the speaker as the “Slave”.



○ LE Only ● Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Device: (0x703eac11adbc) John Trinkle...s i

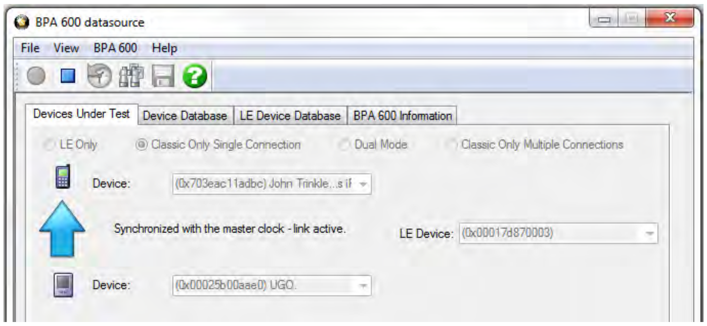
Synchronized with the master clock - link active.

LE Device: (0x00017d870003)

Device: (0x00025b00aae0) UGO.

Figure 3.4 - Arrow Shows master-slave Relationship

Should the roles change during the connection the arrow will change to show the new "Master/Slave" connection. In the following screen shot the speaker has connected as the “Master” to the phone as the “Slave”.



○ LE Only ● Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Device: (0x703eac11adbc) John Trinkle...s i

Synchronized with the master clock - link active.

LE Device: (0x00017d870003)

Device: (0x00025b00aae0) UGO.

Figure 3.5 - Arrow Showing Results of Role Switch

3.1.2.2 Datasource Toolbar/Menu

The Datasource dialog toolbar and menu options are listed below.

Table 3.1 - BPA 600 datasource Toolbar

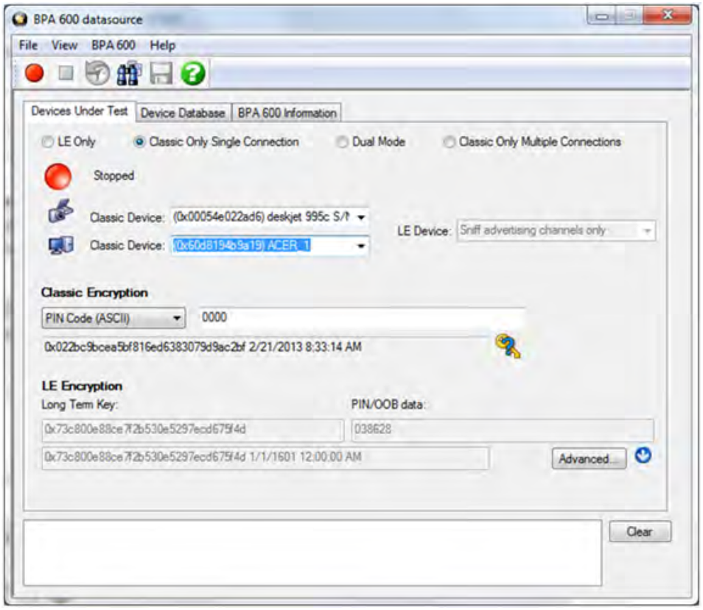
Icon	Description
●	Start Sniffing button to begin sniffing. All settings are saved automatically when you start sniffing. Selection of devices is disabled during sniffing. To select another device stop sniffing.
■	Pause button to stop sniffing
🔭	When you select the Discover Devices button, the software lists all the discoverable *Bluetooth* devices on the **Device Database** and **LE Device Database** tabs.
💾	Save button to save the configuration if you made changes but did not begin sniffing. All settings are saved automatically when you start sniffing.
?	Help button opens the help file.
Grayed-out icons are inactive and do not apply to ComProbe BPA 600	

Table 3.2 - BPA 600 datasource Menu

Menu Item	Description
File	Save and Exit options, self explanatory.
View	Hides or displays the toolbar.
BPA 600	Start Sniffing, Stop Sniffing, Discover Devices
Help	Opens ComProbe **Help**, and **About BPA 600**.

3.1.2.3 Selecting BPA 600 Devices Under Test

The **Devices Under Test** dialog has all the setup information the analyzer needs in order to synchronize with the piconet and capture data. The analyzer requires information on the clock synchronization method and the device address of the device to initially sync to. You must also choose what to sniff.



○ LE Only ● Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Stopped

Classic Device: (0x00054e022ad6) deskjet 995c S/N

Classic Device: (0x60d8194b9a19) ACER_1

LE Device: Sniff advertising channels only

Classic Encryption

PIN Code (ASCII) 0000

0x022bc9bcea5bf816ed6383079d9ac2bf 2/21/2013 8:33:14 AM

LE Encryption

Long Term Key: 0x73c800e88ce7f2b530e5297ecd675f4d

PIN/OOB data: 038628

0x73c800e88ce7f2b530e5297ecd675f4d 1/1/1601 12:00:00 AM

Figure 3.6 - BPA 600 Datasource Devices Under Test Dialog

You can choose to capture data using:

- low energy only
- Classic Only, Single Connection
- Dual Mode - Combination of Classic and low energy
- Classic Only, Multiple Connections

Select one of these links above for explanations on how to configure each option.

There are a couple of other functions on the dialog that you need to understand.

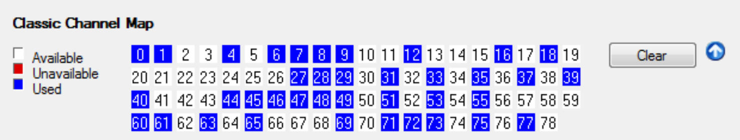
Advanced

Click here to see the BPA 600 Advanced Classic Settings.

Channel Map (Classic *Bluetooth*)

The **Channel Map** shows which channels are available for Adaptive Frequency Hopping.

- **Channel Map** Click this button to toggle on/off the display of the Channel Map.



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78

Figure 3.7 - Classic Bluetooth Channel Map

This display is used to determine which channels are available with

Table 3.3 - BPA 600 Channel Map Color Codes

Channel Color	Description
White	Channel is currently available for use.
Red	When Adaptive Frequency Hopping is in use, red indicates that the channel is marked as unavailable
Blue	Indicates that a packet was captured on the channel.

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

> **Note: Channel Map** is not available for **LE Only**.

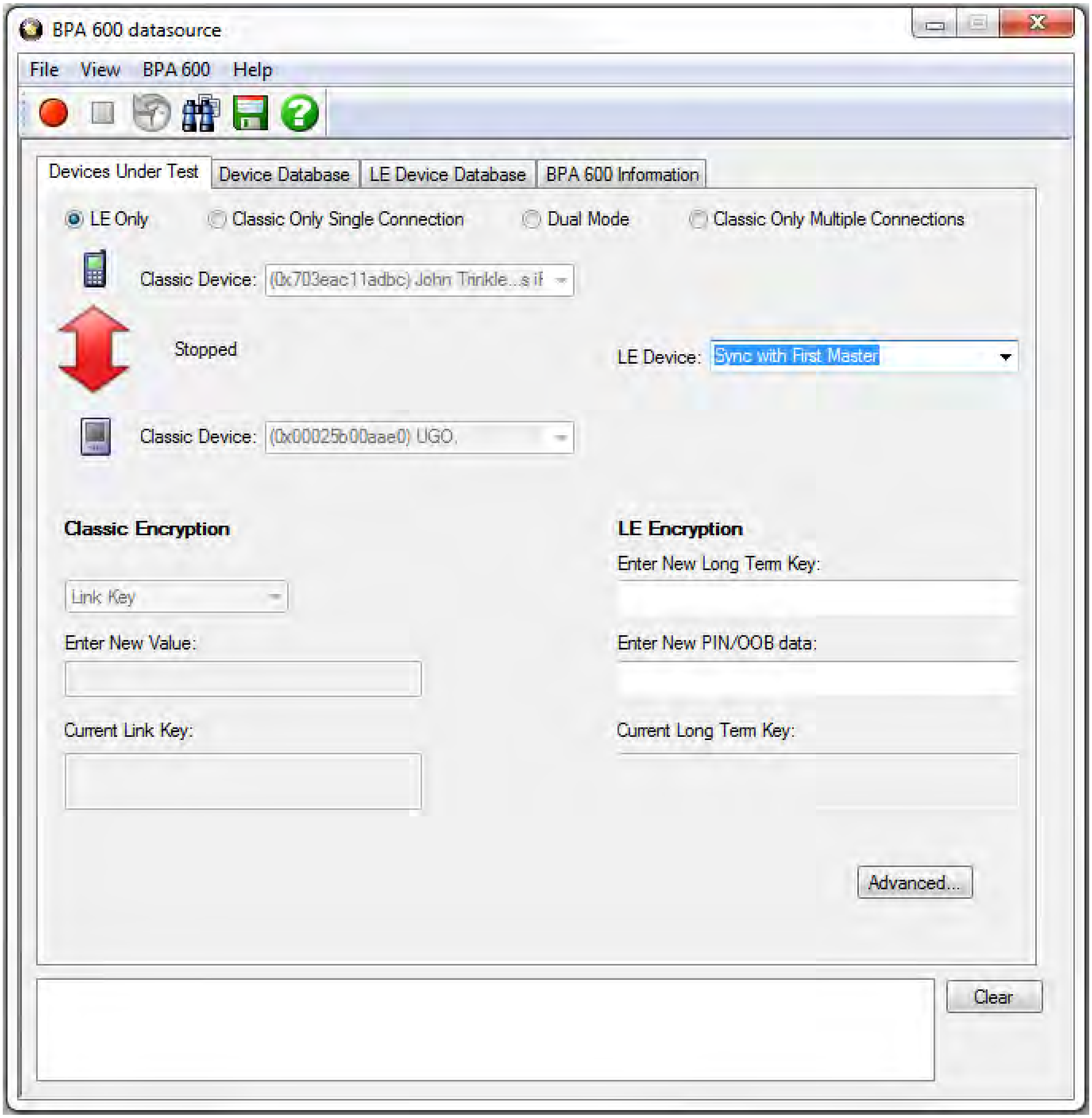
Status Window

A status window at the bottom of the dialog displays information about recent activity.

3.1.2.4 BPA 600 Devices Under Test

3.1.2.4.1 BPA 600 Devices Under Test - LE Only

By selecting the "LE Only" radio button under the "Devices Under Test" tab you can configure the BPA 600 protocol analyzer for sniffing Bluetooth low energy communications.



● 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:

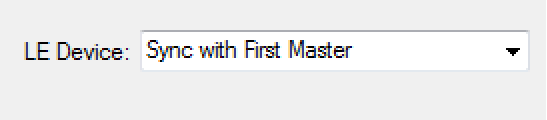
Current Long Term Key:

Figure 3.8 - BPA 600 Devices Under Test - low energy

The default value in the **LE Device** drop down is **Sync with First Master**. To begin sniffing *Bluetooth* low energy simply click the red button to start. The analyzer will capture packets from the first Master that makes a connection . To capture the advertising traffic and the connection(s), you must specify a device address.

Specifying the LE Device Address and Encryption

1. If you would like you may specify the LE device you are testing by typing in or choosing its address (BD_ ADDR). You can type it directly into the drop down, or choose it from the existing previous values list in the drop down.

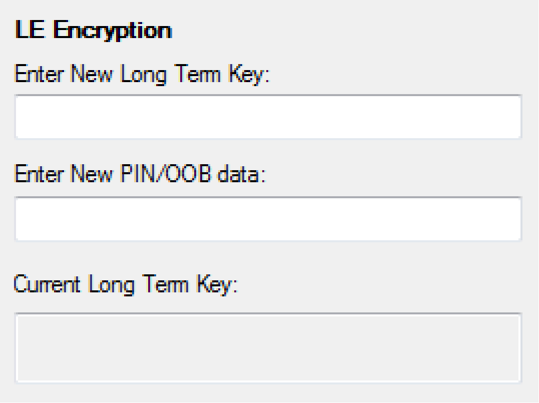


LE Device: Sync with First Master

   To enter the device manually type the address - 12 digit hex number (6 octets). The "0x" is automatically typed in the drop down control.

   Once you have the devices address identified, the next step is to identify the Encryption.

2. **Enter the Long Term Key** for the **LE Encryption**.



LE Encryption

Enter New Long Term Key:

Enter New PIN/OOB data:

Current Long Term Key:

The Long Term Key is similar to the Link key in Classic. 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.

Learn more about the Long Term Key.

The Long Term Key is similar to the Link key in Classic; 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.

There are a few differences though:

In Classic the Link key is derived from inputs from both devices and is calculated in the same way independently by both devices and then stored persistently. The link key itself is never transmitted over the air during pairing.

In LE, the long term key is generated solely on the slave device and then, during pairing, is distributed to a master device that wants to establish an encrypted connection to that slave in the future. Thus the long term key is transmitted over the air, albeit encrypted with a one-time key derived during the pairing process and discarded afterwards (the so called short term key).

Unlike the link key, this long term key is directional, i.e. it is only used to for connections from the master to the slave (referring to the roles of the devices during the pairing process). If the devices also want to connect the other way round in the future, the device in the master role (during the pairing process) also needs to send its own long term key to the device in the slave role during the pairing process (also encrypted with the short term key of course), so that the device which was in the slave during the pairing process can be a master in the future and connect to the device which was master during the pairing process (but then would be in a slave role).

Since most simple LE devices are only ever slave and never master at all, the second long term key exchange is optional during the pairing process.

> **Note:** If you use Copy/Paste to insert the Long Term Key , Frontline will auto correct (remove invalid white spaces) to correctly format the key.

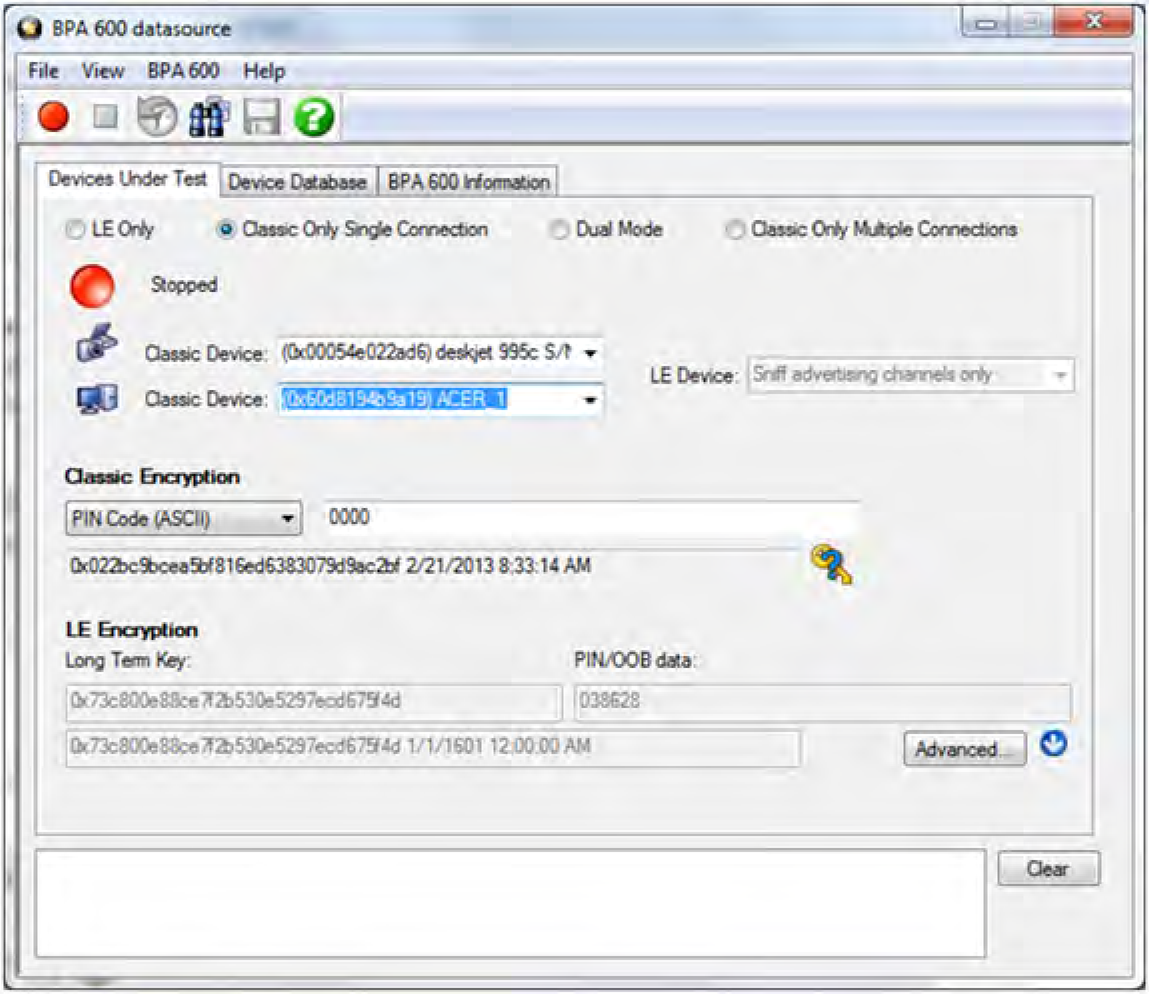
3. Enter a **PIN** or out-of-band (**OOB**) value for Pairing.

This optional information offers alternative pairing methods.

One of two pieces of data allow alternative pairing:

1. PIN is a six-digit (or less if leading zeros are omitted) decimal number.
2. Out-of-Band (OOB) data is a 16-digit hexadecimal code 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.

3.1.2.4.2 BPA 600 Devices Under Test - Classic Single Connection



○ LE Only ● Classic Only Single Connection ○ Dual Mode ○ Classic Only Multiple Connections

Stopped

Classic Device: (0x00054e022ad6) deskjet 995c S/N

Classic Device: (0x60d8194b9a19) ACER_1

LE Device: Sniff advertising channels only

Classic Encryption

PIN Code (ASCII) 0000

0x022bc9bcea5bf816ed6383079d9ac2bf 2/21/2013 8:33:14 AM

LE Encryption

Long Term Key: 0x73c800e88ce7f2b530e5297ecd675f4d

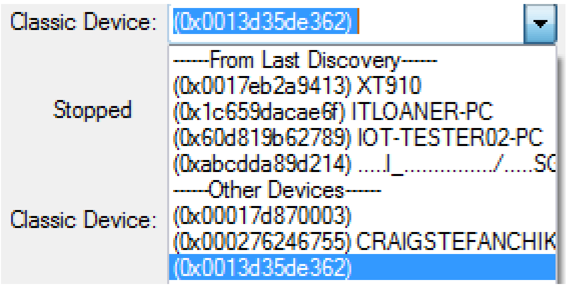
PIN/OOB data: 038628

0x73c800e88ce7f2b530e5297ecd675f4d 1/1/1601 12:00:00 AM

Figure 3.9 - BPA 600 Devices Under Test - Classic Only Single Connection

Specifying the Bluetooth Device Address (BD_ADDR)

Select the *Bluetooth* device address (BD_ADDR) form the **Classic Device:** drop down list or from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database


Classic Device: (0x0013d35de362)

Stopped
Classic Device:
------From Last Discovery------
(0x0017eb2a9413) XT910
(0x1c659dacae6f) ITLOANER-PC
(0x60d819b62789) IOT-TESTER02-PC
(0xabcdda89d214) .....l_............../.....SC
------Other Devices------
(0x00017d870003)
(0x000276246755) CRAIGSTEFANCHIK
(0x0013d35de362)

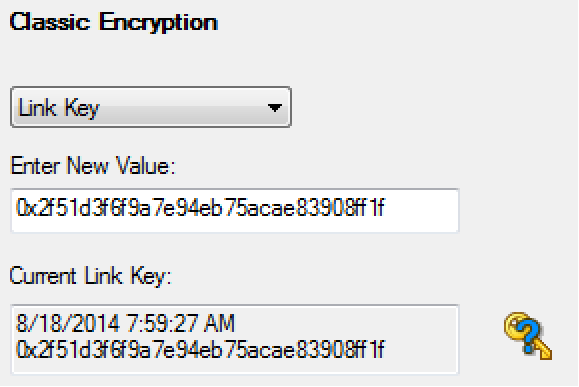
In single connection mode, the analyzer needs to know the Bluetooth® Device Address (BD_ADDR) for each device, but it does not need to know which is master or slave, ComProbe analyzercan figure that out for you through roleless connection. You can also manually specify the Bluetooth Device Address.

Classic Encryption

Once you have the devices address identified, the next step is to identify the Encryption.

1. Select an Encryption option.
2. Enter a value for the encryption.

The **Current Link Key** field displays the currently provided **Link Key** and the date and time the key was provided. The status of the **Link Key** is displayed with the following icons:


Classic Encryption

Link Key

Enter New Value:
0x2f51d3f6f9a7e94eb75acae83908ff1f

Current Link Key:
8/18/2014 7:59:27 AM
0x2f51d3f6f9a7e94eb75acae83908ff1f

Icon	Link Key Status
✓	Valid
?	Not Valid
✱	Connection Attempted But Failed

Bluetooth devices can have their data encrypted when they communicate. *Bluetooth* devices on an encrypted link share a common link key in order to exchange encrypted data. How that link key is created depends upon the pairing method used.

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

a. PIN Code (ASCII)

b. PIN Code (Hex)

c. Link Key

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

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

  Example:

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

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

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

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

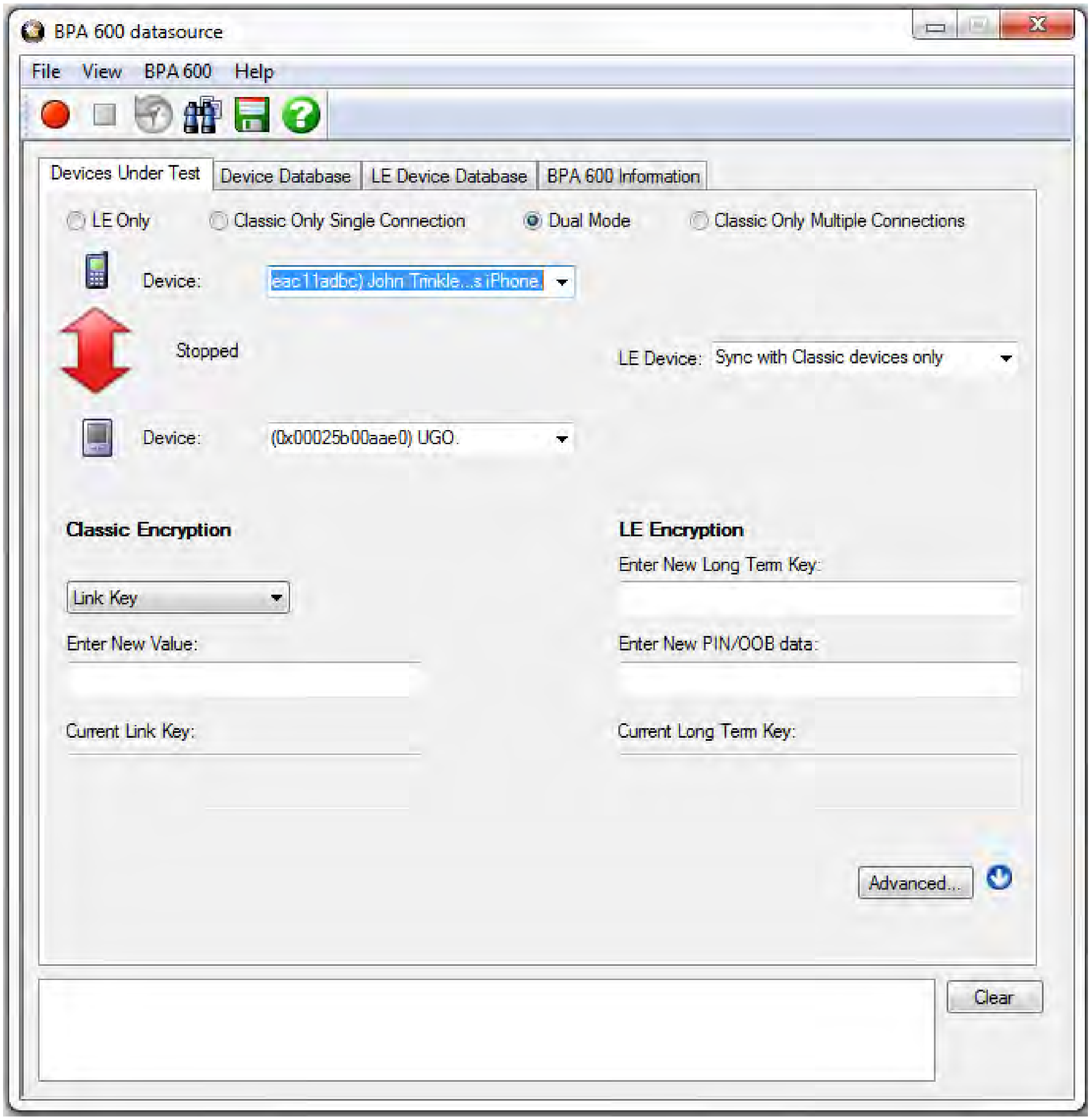
  Note: When the devices are in the Secure Simple Pairing (SSP) Debug Mode, SSP is automatically supported regardless of encryption configuration.

  - If any one of the *Bluetooth* devices is in SSP Debug Mode then the BPA 600 analyzer can automatically figure out the Link Key, and you do not have to do anything.

  - If the Bluetooth devices do not allow Debug Mode activation, enter the Link Key as described above or import the Link Key using the procedure in Programmatically Update Link Key from 3rd Party Software.

3.1.2.4.3 BPA 600 Devices Under Test- Dual Mode

Note: When selecting and using either "Dual Mode" or "Classic Only Multiple Connection" you must connect both antennas (LE and Classic) to the ComProbe BPA 600 hardware.



○ LE Only ○ Classic Only Single Connection ● Dual Mode ○ Classic Only Multiple Connections

Device: eac11adbc) John Trinkle...s iPhone

Stopped

LE Device: Sync with Classic devices only

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:

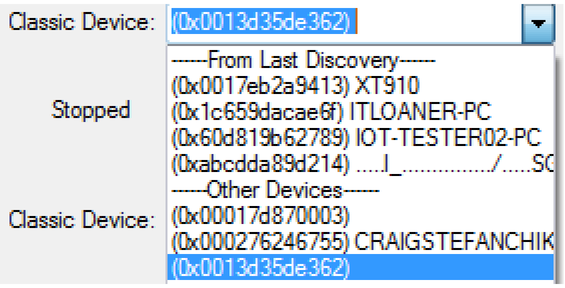
Current Long Term Key:

Figure 3.10 - BPA 600 Devices Under Test - Dual Mode

Specifying the *Bluetooth* Device Address (BD_ADDR)

In Dual Mode, the analyzer needs to know the *Bluetooth* Device Address (BD_ADDR) for each device, but it does not need to know which is master or slave for the Classic *Bluetooth* connection, ComProbe analyzser can figure that out for you through roleless connection.

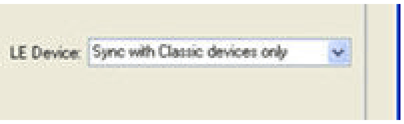
1. You can manually select Select the *Bluetooth* device address (BD_ADDR) form the **Classic Device:** drop down list or from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.



Classic Device: (0x0013d35de362)

Stopped
Classic Device:
------From Last Discovery------
(0x0017eb2a9413) XT910
(0x1c659dacae6f) ITLOANER-PC
(0x60d819b62789) IOT-TESTER02-PC
(0xabcdda89d214) .....I_............./.....SC
------Other Devices------
(0x00017d870003)
(0x000276246755) CRAIGSTEFANCHIK
(0x0013d35de362)

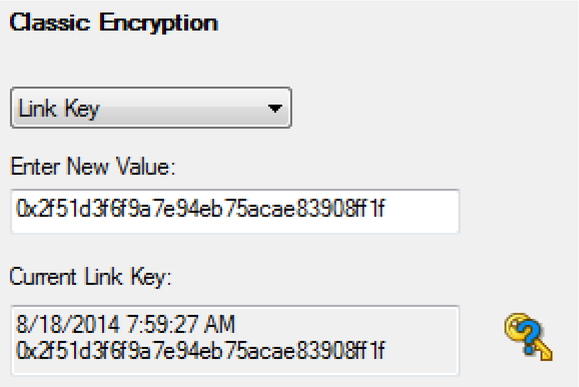
2. Specify the "BD_ADDR for the LE Device" by selecting "Sync with Classic Devices Only". By doing this, the low energy device will follow connections from or to the specified device, or from or to the first Classic device that connects over LE.



LE Device: Sync with Classic devices only

Classic Encryption

Bluetooth devices can have their data encrypted when they communicate. *Bluetooth* devices on an encrypted link share a common link key in order to exchange encrypted data. How that link key is created depends upon the pairing method used.



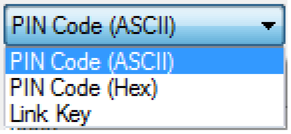
Classic Encryption

Link Key

Enter New Value: 0x2f51d3f6f9a7e94eb75acae83908ff1f

Current Link Key: 8/18/2014 7:59:27 AM 0x2f51d3f6f9a7e94eb75acae83908ff1f

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



a. PIN Code (ASCII)

b. PIN Code (Hex)

c. Link Key

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

  Example:

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

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

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

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

1. Select an Encryption option.

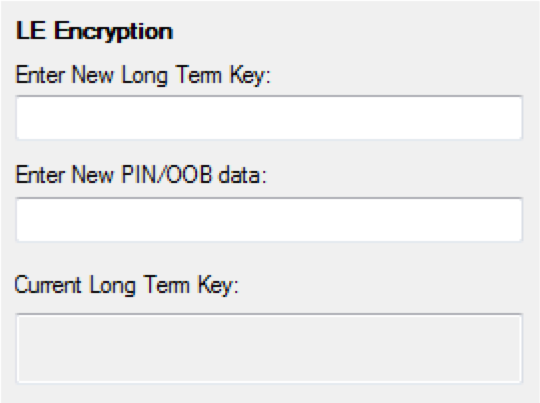
2. Enter a value for the encryption.

   The **Current Link Key** field displays the currently provided **Link Key** and the date and time the key was provided. The status of the **Link Key** is displayed with the following icons:

Icon	Link Key Status
✓	Valid
?	Not Valid
✱	Connection Attempted But Failed

LE Encryption

1. **Enter the New Long Term Key** for the **LE Encryption.**



LE Encryption

Enter New Long Term Key:

Enter New PIN/OOB data:

Current Long Term Key:

   The long term key is similar to the Link key in Classic. 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.

   Learn more about the Long Term Key.

   The Long Term Key is similar to the Link key in Classic; 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.

   There are a few differences though:

   In Classic the Link key is derived from inputs from both devices and is calculated in the same way independently by both devices and then stored persistently. The link key itself is never transmitted over the air during pairing.

   In LE, the long term key is generated solely on the slave device and then, during pairing, is distributed to a master device that wants to establish an encrypted connection to that slave in the future. Thus the long term key is transmitted over the air, albeit encrypted with a one-time key derived during the pairing process and discarded afterwards (the so called short term key).

Unlike the link key, this long term key is directional, i.e. it is only used to for connections from the master to the slave (referring to the roles of the devices during the pairing process). If the devices also want to connect the other way round in the future, the device in the master role (during the pairing process) also needs to send its own long term key to the device in the slave role during the pairing process (also encrypted with the short term key of course), so that the device which was in the slave during the pairing process can be a master in the future and connect to the device which was master during the pairing process (but then would be in a slave role).

Since most simple LE devices are only ever slave and never master at all, the second long term key exchange is optional during the pairing process.

> **Note:** If you use Copy/Paste to insert the Long Term Key , Frontline will auto correct (remove invalid white spaces) to correctly format the key.

2. Enter a **PIN** or out-of-band (**OOB**) value for Pairing.

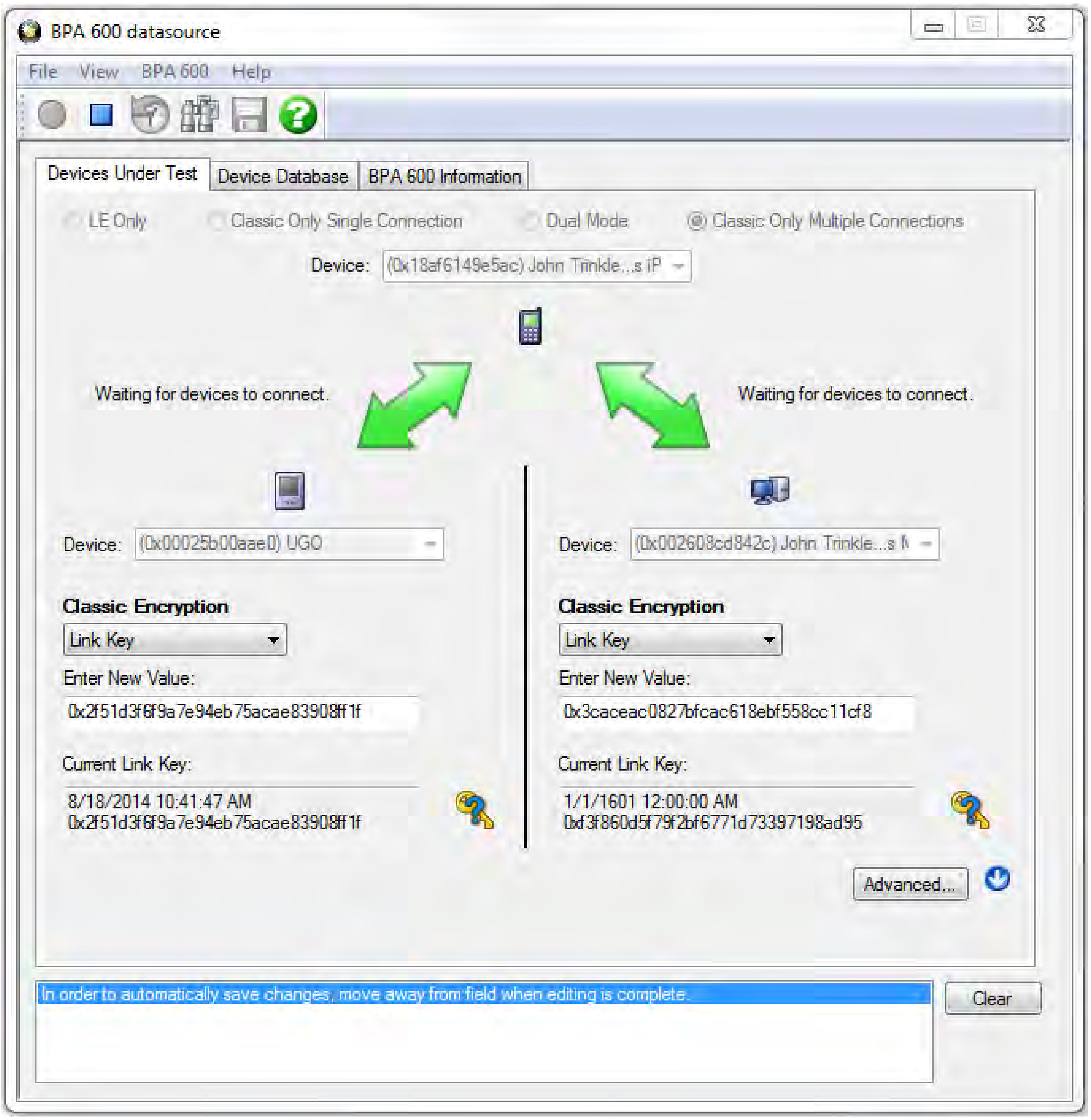
   This optional information offers alternative pairing methods.

One of two pieces of data allow alternative pairing:

1. PIN is a six-digit (or less if leading zeros are omitted) decimal number.
2. Out-of-Band (OOB) data is a 16-digit hexadecimal code 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.

3.1.2.4.4 BPA 600 Devices Under Test - Classic Only Multiple Connection

> **Note:** When selecting and using either **Dual Mode** or **Classic Only Multiple Connection** you must connect both antennas (**LE** and **Classic**) to the ComProbe BPA 600 hardware.



○ LE Only ○ Classic Only Single Connection ○ Dual Mode ● Classic Only Multiple Connections

Device: (0x18af6149e5ac) John Trinkle...s iP

Waiting for devices to connect.

Waiting for devices to connect.

Device: (0x00025b00aae0) UGO

Classic Encryption

Link Key

Enter New Value:

0x2f51d3f6f9a7e94eb75acae83908ff1f

Current Link Key:

8/18/2014 10:41:47 AM
0x2f51d3f6f9a7e94eb75acae83908ff1f

Device: (0x002608cd842c) John Trinkle...s M

Classic Encryption

Link Key

Enter New Value:

0x3caceac0827bfcac618ebf558cc11cf8

Current Link Key:

1/1/1601 12:00:00 AM
0xf3f860d5f79f2bf6771d73397198ad95

In order to automatically save changes, move away from field when editing is complete.

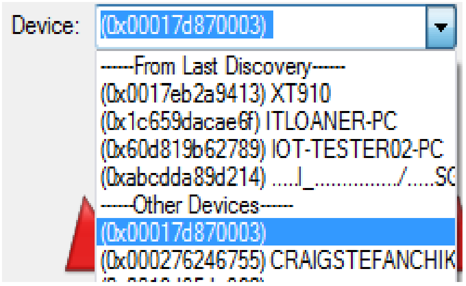
Figure 3.11 - BPA 600 Devices Under Test - Classic Only Multiple Connections

Specifying the *Bluetooth* Device Address (BD_ADDR)

Multiple connection refers to connecting one master with two slave *Bluetooth* devices. The analyzer needs to know the *Bluetooth* Device Address (BD_ADDR) for the Slaves and the Master. The analyzer needs to know the *Bluetooth* Device Address (BD_ADDR) for each device, but it does not need to know which is master or slave as the ComProbe analyzer can figure that out for you through roleless connection. You can also manually specify the Bluetooth Device Address.

Select the *Bluetooth* device address (BD_ADDR) form the **Classic Device:** drop down list or from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.

Using the **Device** drop down list, elect the *Bluetooth* Device Address (BD_ADDR) : from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.

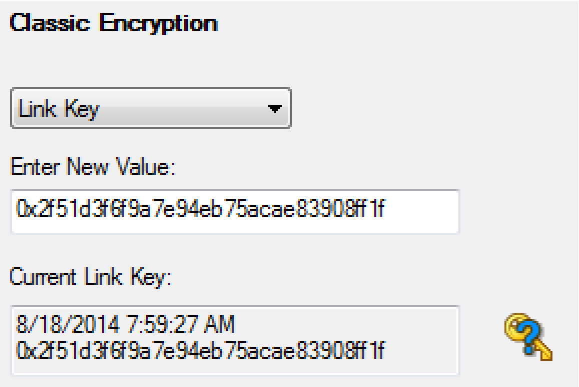


Device: (0x00017d870003)

------From Last Discovery------
(0x0017eb2a9413) XT910
(0x1c659dacae6f) ITLOANER-PC
(0x60d819b62789) IOT-TESTER02-PC
(0xabcdda89d214) .....l_............../.....SC
------Other Devices------
(0x00017d870003)
(0x000276246755) CRAIGSTEFANCHIK

Classic Encryption

Bluetooth devices can have their data encrypted when they communicate. *Bluetooth* devices on an encrypted link share a common link key in order to exchange encrypted data. How that link key is created depends upon the pairing method used.



Classic Encryption

Link Key

Enter New Value: 0x2f51d3f6f9a7e94eb75acae83908ff1f

Current Link Key: 8/18/2014 7:59:27 AM 0x2f51d3f6f9a7e94eb75acae83908ff1f

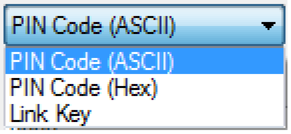
There are three encryption options in the I/O Settings dialog.

a. PIN Code (ASCII)

b. PIN Code (Hex)

c. Link Key

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



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

  Example:

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

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

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

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

> **Note:** When the devices are in the Secure Simple Pairing (SSP) Debug Mode, SSP is automatically supported regardless of encryption configuration.

  - If any one of the *Bluetooth* devices is in SSP Debug Mode then the BPA 600 analyzer can automatically figure out the Link Key, and you do not have to do anything.
  - If the Bluetooth devices do not allow Debug Mode activation, enter the Link Key as described above or import the Link Key using the procedure in Programmatically Update Link Key from 3rd Party Software.

1. Select an Encryption option.
2. Enter a value for the encryption.

   The **Current Link Key** field displays the currently provided **Link Key** and the date and time the key was provided. The status of the **Link Key** is displayed with the following icons:

Icon	Link Key Status
🔑✓	Valid
🔑?	Not Valid
🔑✸	Connection Attempted But Failed

3.1.2.4.5 SSP Debug Mode

Bluetooth Core Version 2.1 and later specifications require *Bluetooth* compliant chip manufactures to include Secure Simple Pairing (SSP) Debug Mode in the Host Controller. Debug Mode allows developers to debug and analyze data without exposing any information that is intended to be kept secret. SSP Debug Mode uses a different Link Key for encryption than is used during normal *Bluetooth* device operation. Debug Mode is activated in the Host Controller to allow for data analysis. Once the analysis is complete Debug Mode can be switched off.

While Bluetooth device 2.1 compliance applies to chip manufacturers, device manufacturers do not have the same obligation to support SSP Debug Mode therefore some devices may not have this feature enabled.

Debug Mode enables interoperability testing and analysis at all development stages, decreasing time to market.

3.1.2.4.6 Programmatically Update Link Key from 3rd Party Software

Now the BPA 600 protocol analyzer user can update the link keys for either of the classic links using a very common Windows message WM_COPYDATA. The mechanism is to send a WM_COPYDATA message to the BPA 600 datasource.

The best scenario for doing this is when the devices are doing SSP and they are NOT in debug mode. The following is a snippet of code that gives an example of programmatically sending link key to the ComProbe Protocol Analysis System software. In order to do this the user needs to know both addresses of the devices in the link for which they wish to update the link key. Also, the Datasource expects the master and slave addresses in LSB to MSB format.

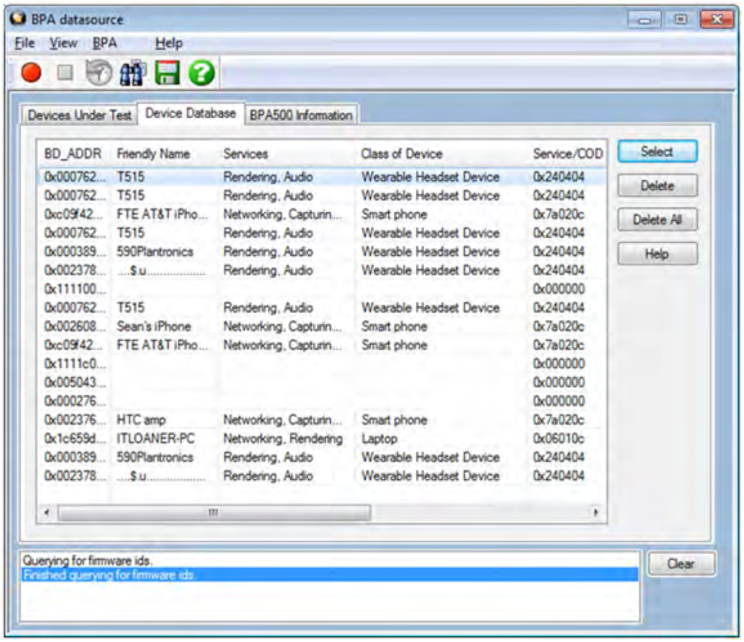
If the link key is sent to ComProbe software after encryption has been turned on over the air, ComProbe software will flag an error on the Start Encryption packet. Depending on when the link key has been sent down, ComProbe software may however still be able to sniff the link successfully. In order to guarantee that ComProbe software is able to sniff the link the link key should be sent to ComProbe software as soon as it is available and before encryption has been turned on over the air.

Use the following code for BPA 600:

```
#define HCI_LINK_KEY 1000

    HWND nHandle = ::FindWindow(NULL,"BPA 600 datasource");
    if(nHandle != 0)
    {

        COPYDATASTRUCT ds;
        enum
        {

            EncryptionKeySize = 16,
            sizeAddressDevice = 6

        };
        BYTE abytAddressDevice1[sizeAddressDevice] = { 0x12, 0x34, 0x56, 0x78, 0x9a, 0xbc }; //LSB-
            >MSB
        BYTE abytAddressDevice2[sizeAddressDevice] = { 0x21, 0x43, 0x65, 0x87, 0xa9, 0xcb };
        BYTE abytLinkKey[EncryptionKeySize] = { 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff,
            0xff, 0xff, 0xff, 0xff, 0xff, 0xff };
        ds.cbData = sizeAddressDevice + sizeAddressDevice + EncryptionKeySize;
        ds.dwData = HCI_LINK_KEY;
        BYTE bytData[sizeAddressDevice + sizeAddressDevice + EncryptionKeySize];
        memcpy(&bytData,&abytAddressDevice1,sizeAddressDevice);
        memcpy(&bytData[sizeAddressDevice],&abytAddressDevice2,sizeAddressDevice);
        memcpy(&bytData
            [sizeAddressDevice+sizeAddressDevice],&abytLinkKey,EncryptionKeySize);
        ds.lpData = &bytData;
        ::SendMessage(nHandle, WM_COPYDATA, (WPARAM)GetSafeHwnd(), (LPARAM)&ds);

    }
```

3.1.2.5 BPA 600 Device Database

The Device Database contains information about all the Classic Bluetooth® and *Bluetooth* low energy devices that have been discovered or entered by the user.



BD_ADDR	Friendly Name	Services	Class of Device	Service/COD
0x000762...	T515	Rendering, Audio	Wearable Headset Device	0x240404
0x000762...	T515	Rendering, Audio	Wearable Headset Device	0x240404
0xc09f42...	FTE AT&T iPho...	Networking, Capturin...	Smart phone	0x7a020c
0x000762...	T515	Rendering, Audio	Wearable Headset Device	0x240404
0x000389...	590Plantronics	Rendering, Audio	Wearable Headset Device	0x240404
0x002378...	....$.u..................	Rendering, Audio	Wearable Headset Device	0x240404
0x111100...				0x000000
0x000762...	T515	Rendering, Audio	Wearable Headset Device	0x240404
0x002608...	Sean's iPhone	Networking, Capturin...	Smart phone	0x7a020c
0xc09f42...	FTE AT&T iPho...	Networking, Capturin...	Smart phone	0x7a020c
0x1111c0...				0x000000
0x005043...				0x000000
0x000276...				0x000000
0x002376...	HTC amp	Networking, Capturin...	Smart phone	0x7a020c
0x1c659d...	ITLOANER-PC	Networking, Rendering	Laptop	0x06010c
0x000389...	590Plantronics	Rendering, Audio	Wearable Headset Device	0x240404
0x002378...	....$.u..................	Rendering, Audio	Wearable Headset Device	0x240404

```
Querying for firmware ids.
Finished querying for firmware ids.
```

BPA 600 Datasource Device Database Tab

The Device Database is automatically updated when you perform certain operation such as entering encryption information from the **Devices Under Test** dialog.

- When you select Discover Device on the toolbar, BPA 600 analyzer lists all the discoverable Bluetooth® devices.
- When you select a device from the list, then click **Select**, the information is transferred to the **Devices Under Test** dialog.
- You can delete records one at a time by selecting the record, then selecting **Delete**.
- You can also delete all the records by selecting **Delete All.**
- The **Help** opens this help topic.

In the Device Database table the following columns appear.

Table 3.4 - BPA 600 Datasource Device Database Fields

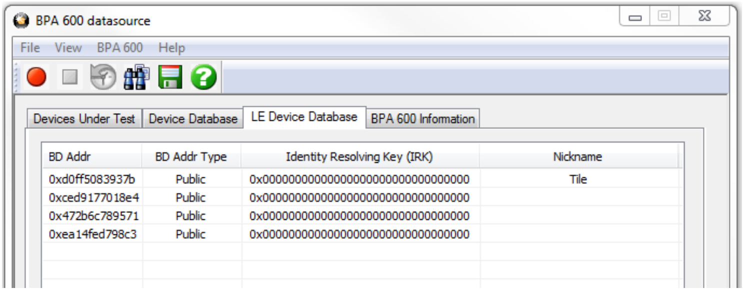
Column	Description
BD_ADDR	The address of the *Bluetooth* device
Friendly Name	If available the friendly name of the device
Services	An attribute of the Class of Device (COD) such as Networking, Rendering, Audio, etc. Data provided from devices supporting Extended Inquiry Response (EIR).during discovery. Service Class identifies a particular type of service/functionality provided by the device. Multiple services can occur. If the device does not support EIR the field will be empty.

Table 3.4 - BPA 600 Datasource Device Database Fields (continued)

Column	Description
Class of Device	A particular type of device such as phone, laptop, wearable, etc. Data provided from devices supporting Extended Inquiry Response (EIR).during discovery. COD is a value which identifies a particular type of functionality provided by the device. For example, there would be a Service Class to identify a printer, and another Service Class to identify a stereo headset. If the device does not support EIR the field will be empty.
Service/COD	Universally Unique Identifier (UUID) of the Services and COD. 128 bits, shown in hexadecimal format. If the device does not support EIR the field will be empty.
Paired BD_ADDR	The address of the *Bluetooth* device this device is paired with.
Paired Friendly Name	The friendly name of the device this device is paired with.
Link Key	The Link Key in Classic *Bluetooth* or the Long Term Key (LTK) in *Bluetooth* low energy used for encrypted data sent between paired devices.
Last Updated	The date the device was entered into the database.

3.1.2.6 BPA 600 low enegy Device Database

The **LE Device Database** contains information about Bluetooth® low energy devices that have been discovered or entered by the user. These devices are also listed in the **Device Database**, but this dataabase list contains additional information specific only to *Bluetooth* low energy technology.



BD Addr	BD Addr Type	Identity Resolving Key (IRK)	Nickname
0xd0ff5083937b	Public	0x00000000000000000000000000000000	Tile
0xced9177018e4	Public	0x00000000000000000000000000000000	
0x472b6c789571	Public	0x00000000000000000000000000000000	
0xea14fed798c3	Public	0x00000000000000000000000000000000	

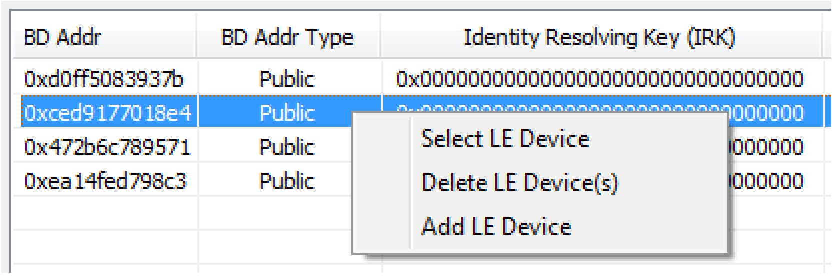
Figure 3.12 - BPA 600 Datasource LE Device Database Tab

The **LE Device Database** is automatically updated when you perform certain operation such as entering encryption information from the **Devices Under Test** dialog.

When you select Discover Device on the toolbar, BPA 600 analyzer adds to the lists any new discovered *Bluetooth* low energy devices. The list is cumulative and will contain all Bluetooth low energy devices previously add to the list.

Device Control Menu

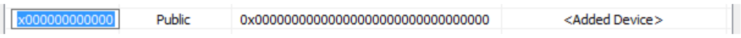
Right-clicking anywhere in the device list will display the device control menu that will Select, Delete, or Add a device.. Clicking on one of these menu items will perform the following actions.



BD Addr	BD Addr Type	Identity Resolving Key (IRK)
0xd0ff5083937b	Public	0x00000000000000000000000000000000
0xced9177018e4	Public	000000
0x472b6c789571	Public	000000
0xea14fed798c3	Public	000000

Table 3.5 - LE Device Database Control Menu

Menu Item	Action
Select	Will place this device into the **LE Device** field in the **LE Only** or **Dual Mode** options of the **Device Under Test** tab. The device must be selected/highlighted in the list prior to making this menu selection. If multiple devices have been selected/highlighted in the list, the first device in the list is placed in the Device Under Test.
Delete	Will deleted the selected/highlighted device from the database. Selecting/highlighting multiple devices in the list will delete all of those devices.
Add	Used for manual entry of a device into the database. A new device entry will append to the end of the device list. To enter data double click on the field and type in the data. For the BD_Addr Type field, double click and tab to select available types. See the following image.

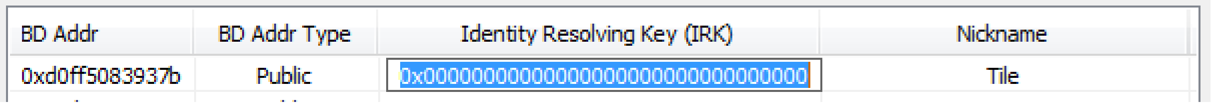


x000000000000	Public	0x00000000000000000000000000000000	<Added Device>

Figure 3.13 - Add Menu Option Fields Display

Editing a Device

Any device entry can be edited by double-clicking in the field. An edit box will open and new device information can be typed in.



BD Addr	BD Addr Type	Identity Resolving Key (IRK)	Nickname
0xd0ff5083937b	Public	0x00000000000000000000000000000000	Tile

Figure 3.14 - Editing IRK Field

When editing the **BD_Addr Type** field "<Tab to toggle>" appears. Press the keyboard Tab key until your selected device address type appears.

LE Device Database Fields

In the **LE Device Database** table the following columns appear.

Table 3.6 - BPA 600 Datasource LE Device Database Fields

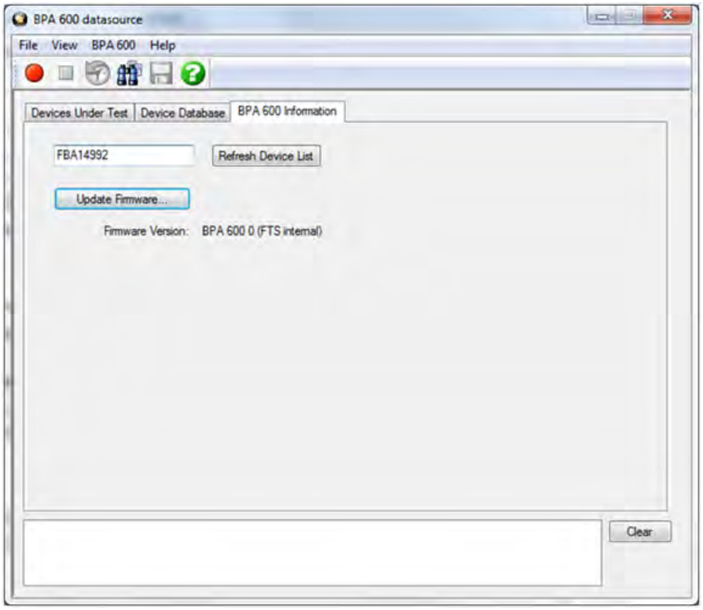
Column	Description
BD_Addr	The address of the *Bluetooth* low energy device

Table 3.6 - BPA 600 Datasource LE Device Database Fields (continued)

Column	Description
BD_Addr Type	May be either "Public" or "Random". "Public"addresses are set to BD_Addr. "Random" is either a 'static" or "private" address. "Static" address is a 48 bit randomly generated address. "Private" address is a 48 bit "non-resolvable" address or "resolvable' address. A "resolvable" address is generated using an IRK.
Identity Resolving Key (IRK)	Will appear when BD_Addr Type is Random, Private, and Resolvable. A host device with a list of IRKs can search the list to identify a peer device that has previously authenticated with the host. This field can be used to identify Bluetooth low energy devices that have previously authenticated.
Nickname	A user-added name for the device, often used to make device identification easier during the analysis. Can be any alpha-numeric string.

3.1.2.7 BPA 600 - Information

The BPA 600 Information dialog is one of the four tabs that appear when you first start ComProbe BPA 600 analyzer.



FBA14992

Firmware Version: BPA 600 0 (FTS internal)

Figure 3.15 - BPA 600 Information Tab

You can also access these tabs by selecting **I/O Settings** or **Hardware Settings** from the Options menu on the **Control** window toolbar.

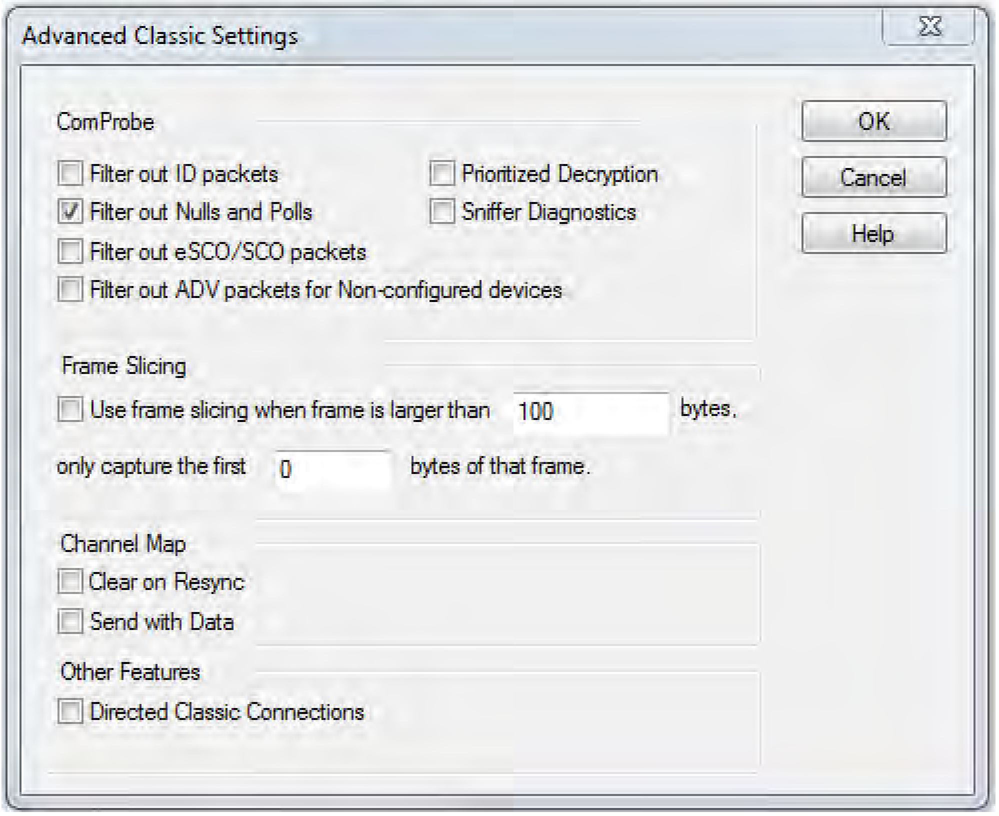
There are several pieces of information on this display:

- Displayed in the text window is the serial number of the connected BPA 600 devices. To update the device list click **Refresh Device List**.

- If you want to load the latest ComProbe BPA 600 hardware firmware, you select the **Update Firmware** button..
- The current firmware is displayed under **Firmware Version**.

3.1.2.8 BPA 600 Advanced Classic Settings

The Advanced Classic Settings dialog contains additional options for synchronizing the analyzer with the link to capture data.



Advanced Classic Settings

ComProbe

□ Filter out ID packets
☑ Filter out Nulls and Polls
□ Filter out eSCO/SCO packets
□ Filter out ADV packets for Non-configured devices
□ Prioritized Decryption
□ Sniffer Diagnostics

Frame Slicing

□ Use frame slicing when frame is larger than 100 bytes.

only capture the first 0 bytes of that frame.

Channel Map

□ Clear on Resync
□ Send with Data

Other Features

□ Directed Classic Connections

Figure 3.16 - BPA 600 Advanced Classic Settings

1. **ComProbe**

   Some packet types can be so numerous that they may make it more difficult to locate data packets in the Frame Display window. You have several options to exclude certain types of packets.

   - **Filter out ID packets** - When this is checked, all ID packets are filtered out.
   - **Filter out Nulls and Polls** - When this is checked, Nulls and Polls packets are filtered out.
   - **Filter out SCO/eSCO** - When this is checked, SCO/eSCO packets are filtered out.
   - **Prioritized Decryption** can be selected if you are having trouble establishing the correct decryption. This option adjusts the data capture to give priority to establishing the proper decryption over receiving

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

- **Sniffer Diagnostics** - When this is checked, some diagnostic data from the ComProbe are captured and stored in the .cfa file. This is useful when a .cfa file is sent to Frontline for analysis and diagnosis. Technical Support may ask you to check this option when you are experiencing issues with BPA 600.
- **Single Link Filtering** - When this is checked, only packets from the specific Master and Slave selected in Devices Under Test are displayed. Data from other devices that may be connected to the Master will be filtered out.

2. **Frame Slicing Settings**

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

3. **Channel Map**

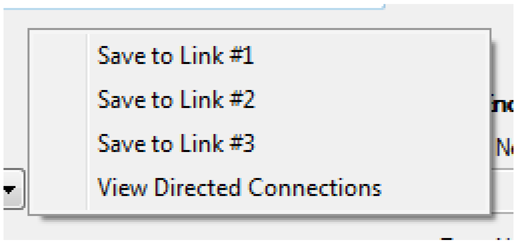
- **Clear on Resync** -used to clear the map each time a re-synchronization occurs
- **Send with Data** - allows you to send a map each time data is sent instead of just sending a map when changes occur.

4. **Other Features**

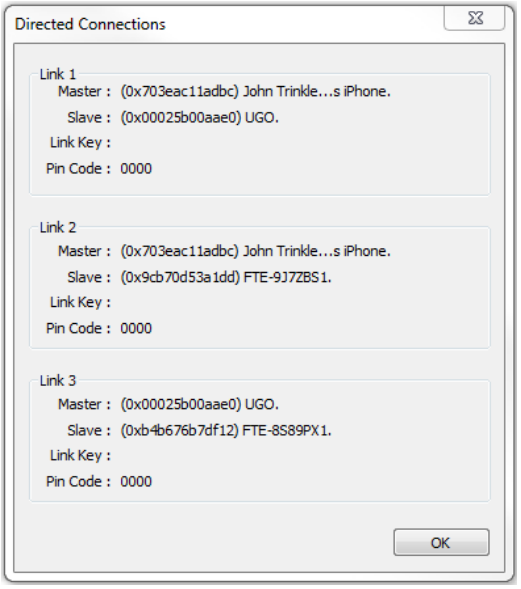
- **Directed Classic Connection** - Applies to **Classic Only Multiple Connections**

  The default configuration for **Classic Only Multiple Connections** is one master and two slaves. The **Directed Classic Connection** allows for simultaneous sniffing of up to three masters and three slaves in any combination. For example you can have one master with one slave along with a second master with two slaves, or three one-master one-slave connections.

  1. Click to place a check in the **Directed Classic Connection** check box.
  2. Click **OK**. The **Advance Classic Settings** dialog will close.
  3. In the **Devices Under Test** tab click on **Classic Only Single Connection**.
  4. In the **Classic Device** drop-down lists select the address of the devices to be in your first link. Then right-click anywhere in the dialog. A link selector pop-up will appear. Click on **Save to Link #1**. The pop-up will close.
  5. Repeat the link selection process for each additional link.



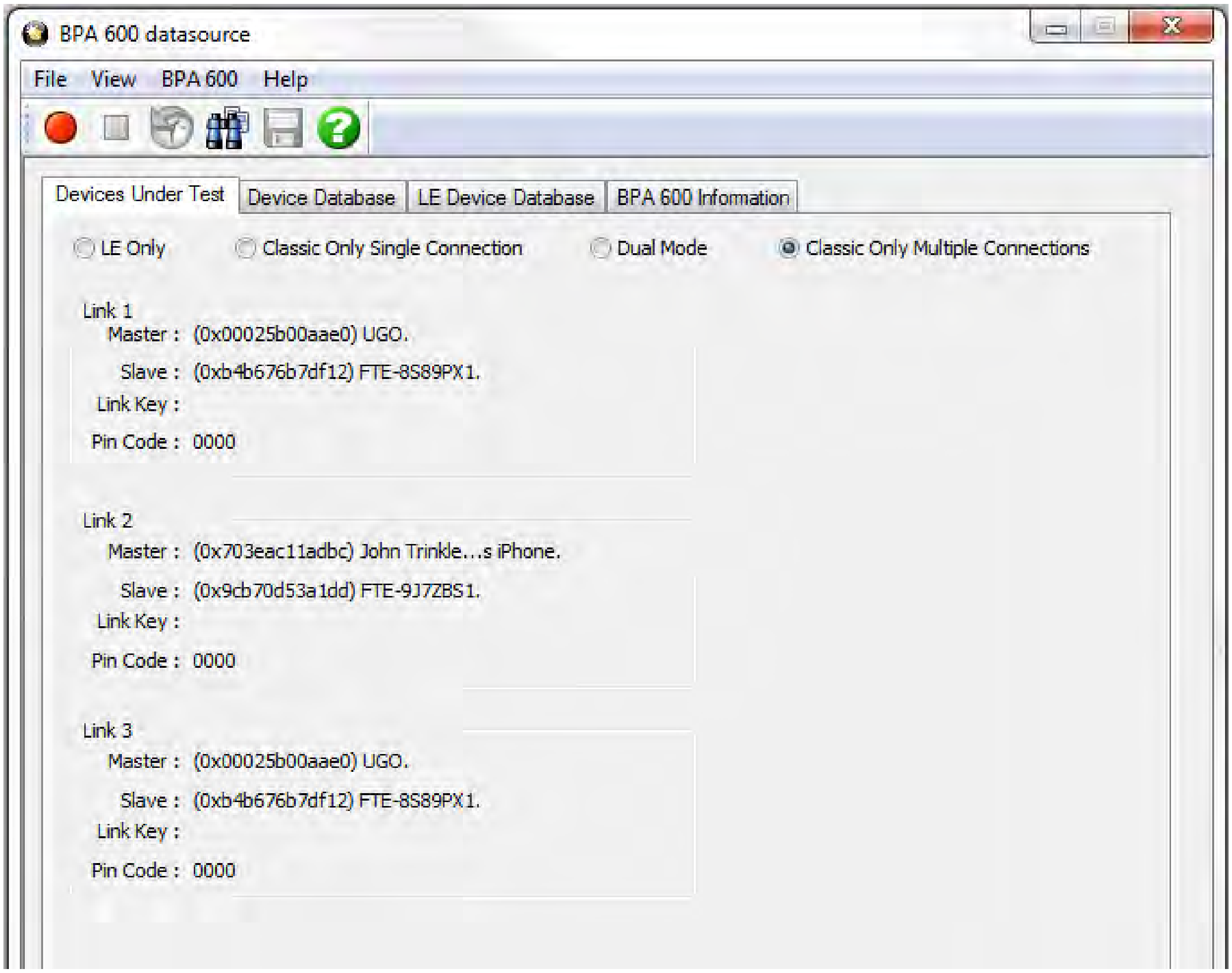
6. To review your saved links right-click and select **View Directed Connecctions**. All of your selections will appear in the **Directed Connections** pop-up window.
7. Click on **OK** to close the pop-up.
8. Selecting the **Classic Only Multiple Connections** will display the same information.
9. To reset the **Classic Only Multiple Connections** to its default mode, select any other datasource configuration radio button and click on the **Advanced** button. Click on **the Dircted Classic Connection** check box to remove the check. Click on **OK**. The **Classic Only Multiple Connections** dialog will return to its default one master two slave configuration.



Link 1
Master : (0x703eac11adbc) John Trinkle…s iPhone.
Slave : (0x00025b00aae0) UGO.
Link Key :
Pin Code : 0000

Link 2
Master : (0x703eac11adbc) John Trinkle…s iPhone.
Slave : (0x9cb70d53a1dd) FTE-9J7ZBS1.
Link Key :
Pin Code : 0000

Link 3
Master : (0x00025b00aae0) UGO.
Slave : (0xb4b676b7df12) FTE-8S89PX1.
Link Key :
Pin Code : 0000



○ LE Only ○ Classic Only Single Connection ○ Dual Mode ● Classic Only Multiple Connections

Link 1
Master : (0x00025b00aae0) UGO.
Slave : (0xb4b676b7df12) FTE-8S89PX1.
Link Key :
Pin Code : 0000

Link 2
Master : (0x703eac11adbc) John Trinkle...s iPhone.
Slave : (0x9cb70d53a1dd) FTE-9J7ZBS1.
Link Key :
Pin Code : 0000

Link 3
Master : (0x00025b00aae0) UGO.
Slave : (0xb4b676b7df12) FTE-8S89PX1.
Link Key :
Pin Code : 0000

Figure 3.17 - Classic Only Multiple Connections in Directed Classic Connections configuration

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.

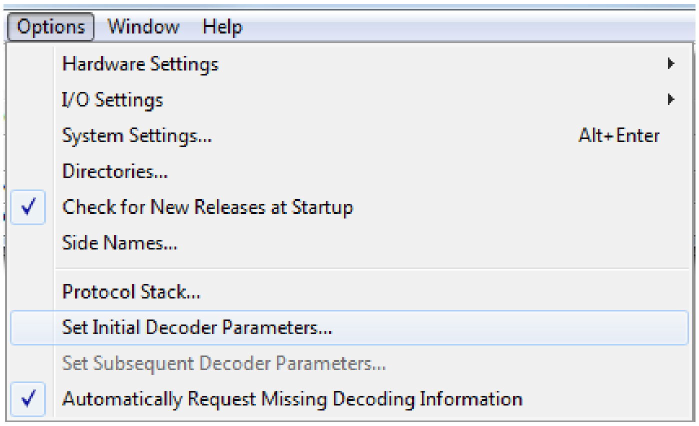

Options
Window
Help
Hardware Settings
I/O Settings
System Settings... Alt+Enter
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

Figure 3.18 - Select **Set Initial Decoder Parameters...** from **Control** window

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

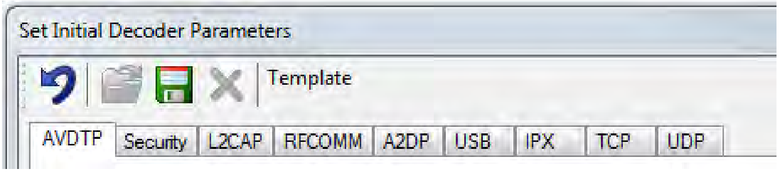


Figure 3.19 - Tabs for each decoder requiring parameters.

- 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.

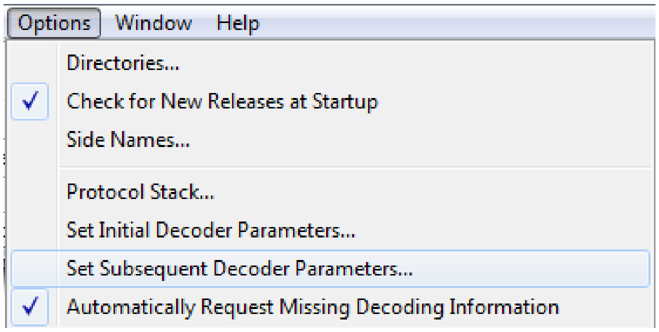
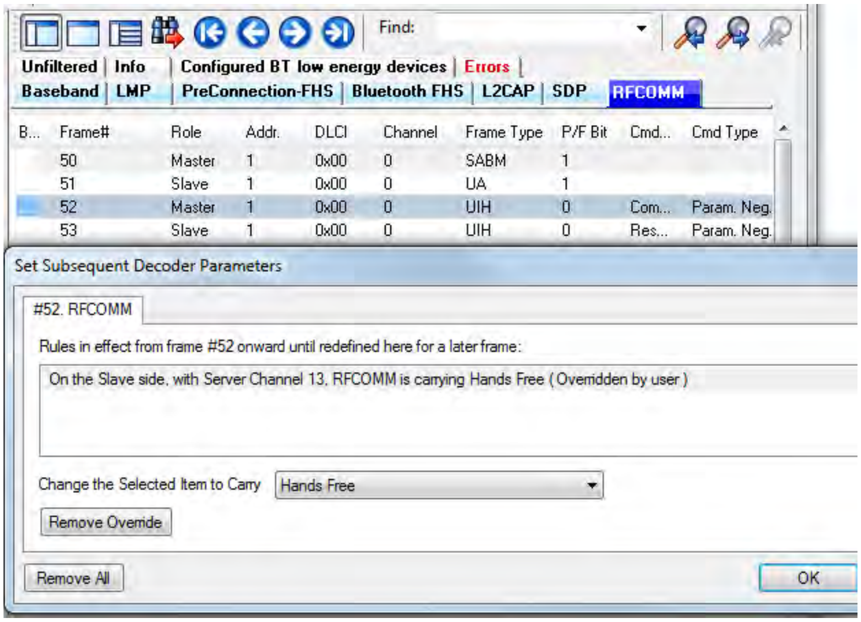

Options
Window
Help
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

Figure 3.20 - **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.

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

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

Change the Selected Item to Carry: Hands Free

Figure 3.21 - 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.

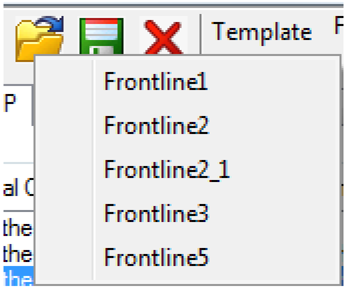
- The **Remove All** button will remove all decoder overrides.

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.



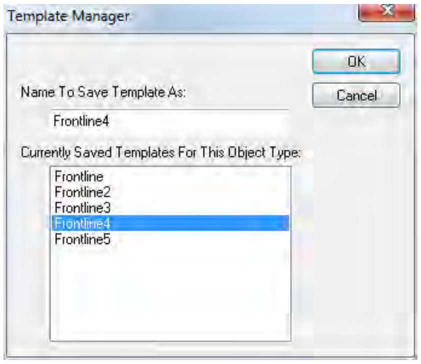
3.2.1.2 Adding a New or Saving an Existing Template

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

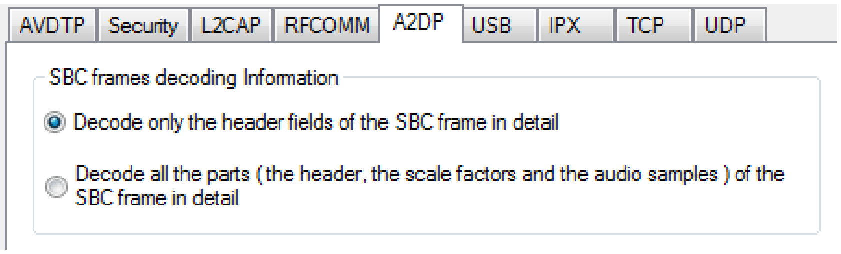
Decoding SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame. You can increase the decoding speed by decoding only the header fields and disregarding other parts. You can select the detail-level of decoding 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 3.22 - A2DP Decoder Settings

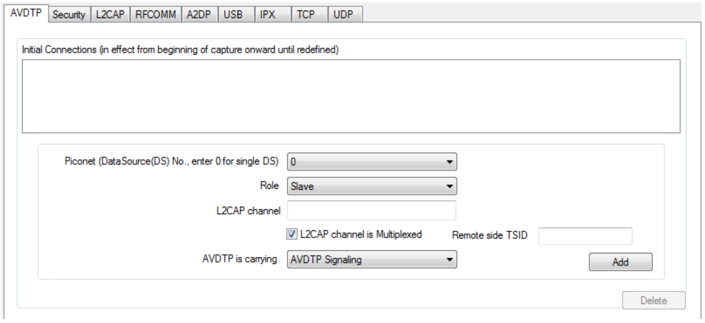
4. Follow steps to save the template changes or to save a new template.

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

3.2.3 AVDTP Decoder Parameters

3.2.3.1 About AVDTP Decoder Parameters

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



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

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

Role Slave

L2CAP channel

☑ L2CAP channel is Multiplexed

Remote side TSID

AVDTP is carrying AVDTP Signaling

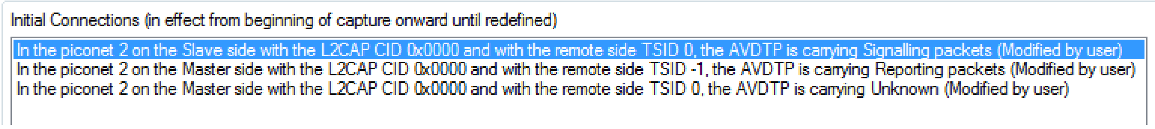
Figure 3.23 - AVDTP parameters tab

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

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

Adding, Deleting, and Saving AVDTP Parameters

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



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

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

Figure 3.24 - Parameters Added to Decoder

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

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

6. AVDTP parameters are saved when the template is saved as described in on page 1 on page 1

3.2.3.2 AVDTP Missing Decode Information

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

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

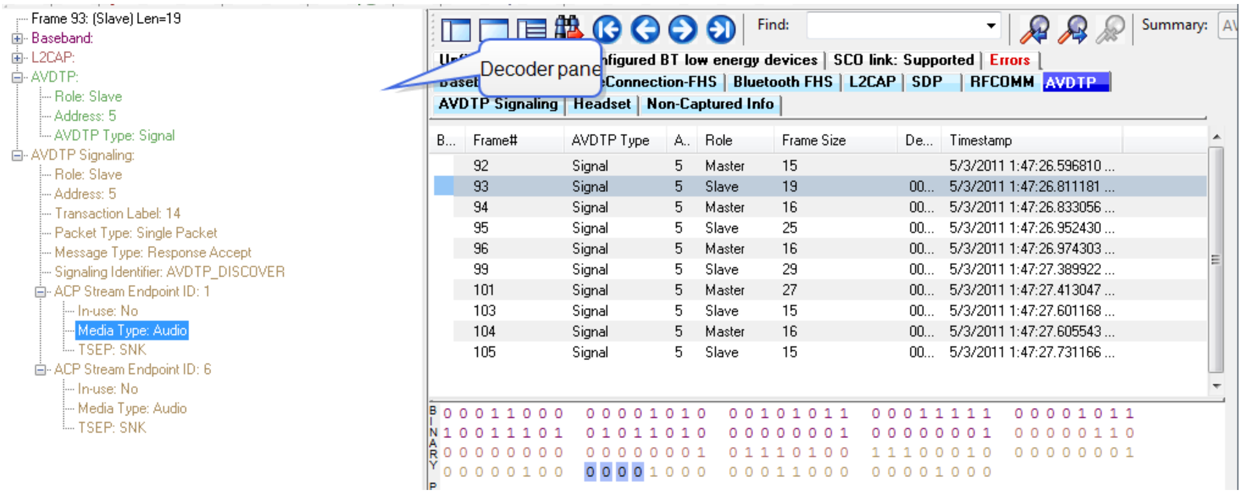
- The capture session started after transmission of the vital information.
- The analyzer incorrectly received a frame with the traversal information.
- The communication monitored takes place between two players with implicit information not included in the transmission.

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

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

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

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



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

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

```
0 0 0 1 1 0 0 0   0 0 0 0 1 0 1 0   0 0 1 0 1 0 1 1   0 0 0 1 1 1 1 1   0 0 0 0 1 0 1 1
1 0 0 1 1 1 0 1   0 1 0 1 1 0 1 0   0 0 0 0 0 0 0 1   0 0 0 0 0 0 0 1   0 0 0 0 0 1 1 0
0 0 0 0 0 0 0 0   0 0 0 0 0 0 0 1   0 1 1 1 0 1 0 0   1 1 1 0 0 0 1 0   0 0 0 0 0 0 0 1
0 0 0 0 0 1 0 0   0 0 0 0 1 0 0 0   0 0 0 1 1 0 0 0   0 0 0 0 1 0 0 0
```

Figure 3.25 - Look in Decoder pane for profile hints

3.2.3.3 AVDTP Override Decode Information

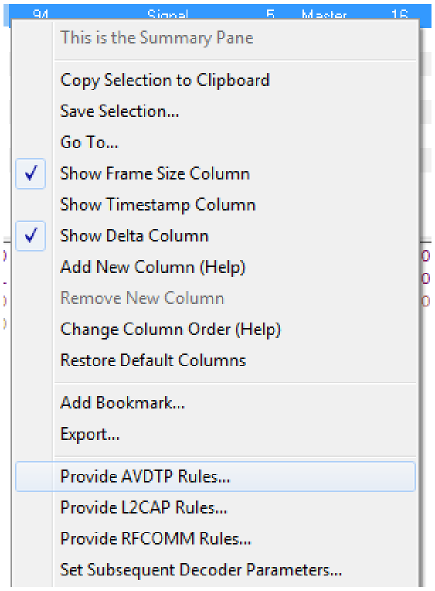
The Set **Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

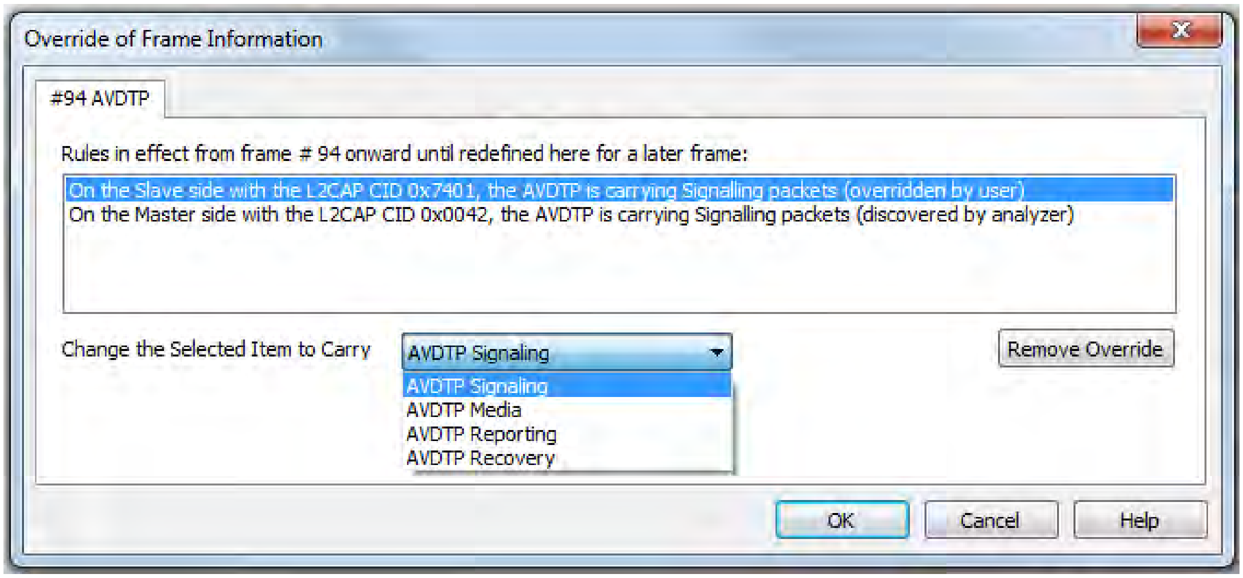
If you have a parameter in effect and wish to change that parameter:

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

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

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




Override of Frame Information

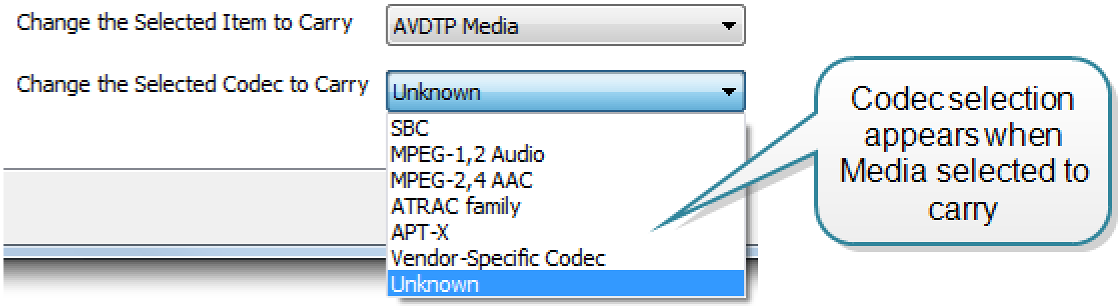
#94 AVDTP

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

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

Change the Selected Item to Carry: AVDTP Signaling

Figure 3.26 - AVDTP Override of Frame Information, Item to Carry

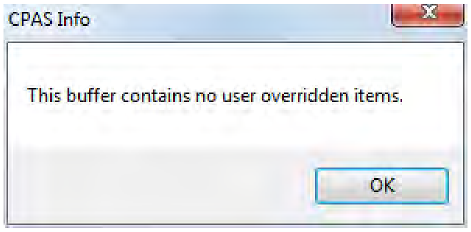

Change the Selected Item to Carry: AVDTP Media

Change the Selected Codec to Carry: Unknown

Codec selection appears when Media selected to carry

Figure 3.27 - AVDTP Override of Frame Information, Media Codec Selection

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


CPAS Info

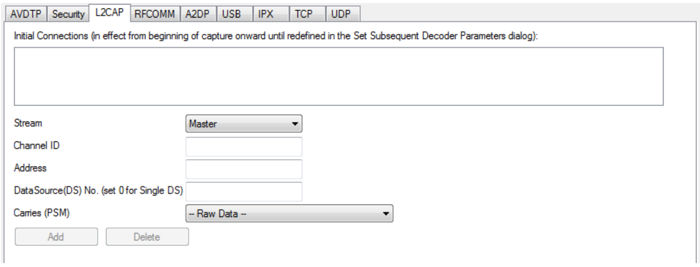
This buffer contains no user overridden items.

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

3.2.4 L2CAP Decoder Parameters

3.2.4.1 About L2CAP Decoder Parameters

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



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

Stream: Master

Channel ID

Address

DataSource(DS) No. (set 0 for Single DS)

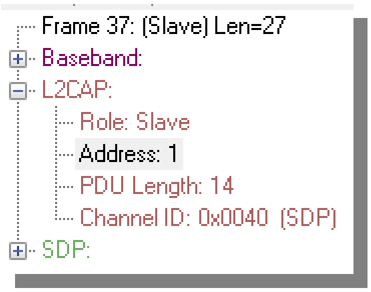
Carries (PSM): -- Raw Data --

Figure 3.28 - L2CAP Decoder parameters tab

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

- **Stream** - This identifies the role of the device initiating the frame (master or slave)
- **Channel ID** - The channel number 0 through 78
- **Address** - This is the physical connection values for the devices. Each link in the net will have an address. A piconet can have up to seven links. The **Frame Display** can provide address information.
- **Data Source (DS) No.** -When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source number.

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



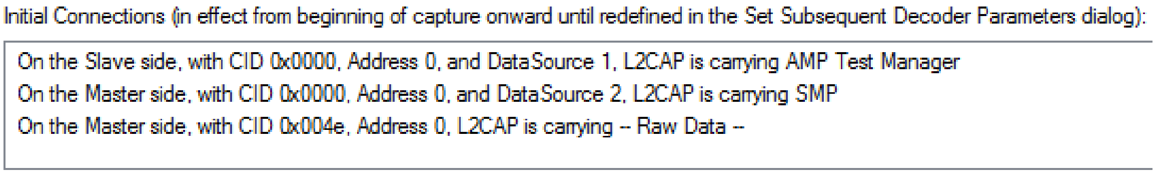
Frame 37: (Slave) Len=27
Baseband:
L2CAP:
Role: Slave
Address: 1
PDU Length: 14
Channel ID: 0x0040 (SDP)
SDP:

- 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 3.29 - Parameters Added to Decoder

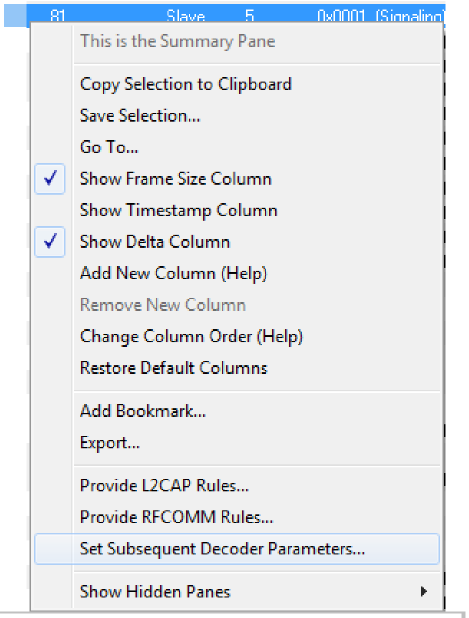
4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and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

3.2.4.2 L2CAP Override Decode Information

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

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

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



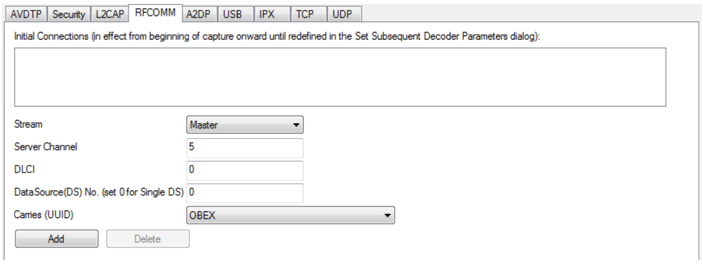
Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

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

3.2.5 RFCOMM Decoder Parameters

3.2.5.1 About RFCOMM Decoder Parameters

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



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

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

Figure 3.30 - RFCOMM parameters tab

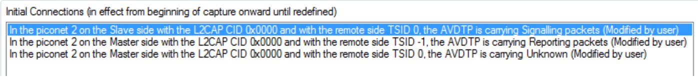
The **RFCOMM Set Initial Decoder Parameters** tab requires the following user inputs to complete a parameter:

- **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 3.31 - Parameters Added to Decoder

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

3.2.5.2 RFCOMM Missing Decode Information

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

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

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

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

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

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

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

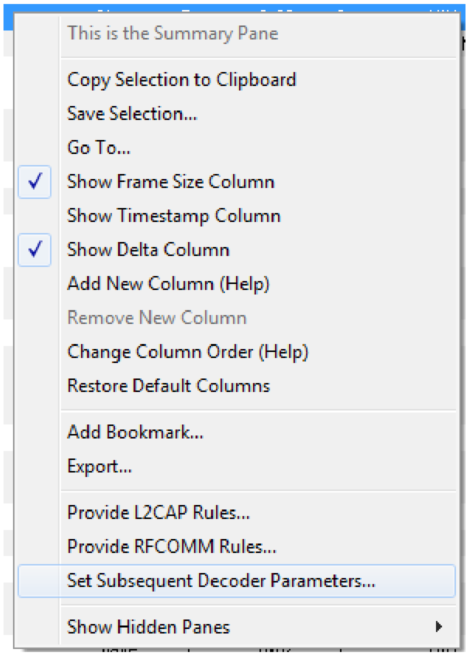
3.2.5.3 RFCOMM Override Decode Information

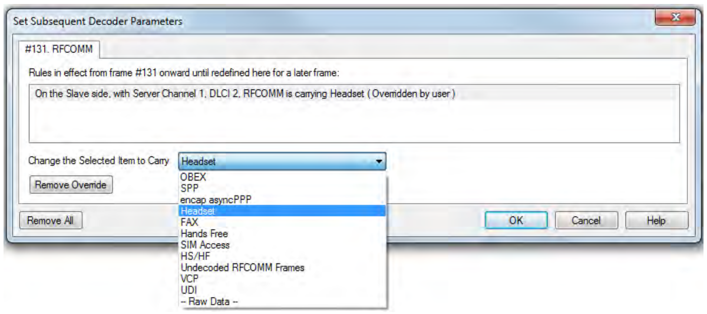
The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

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

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

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





Set Subsequent Decoder Parameters

#131. RFCOMM

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

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

Change the Selected Item to Carry: Headset

Figure 3.32 - 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 309 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 3.7 - *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,

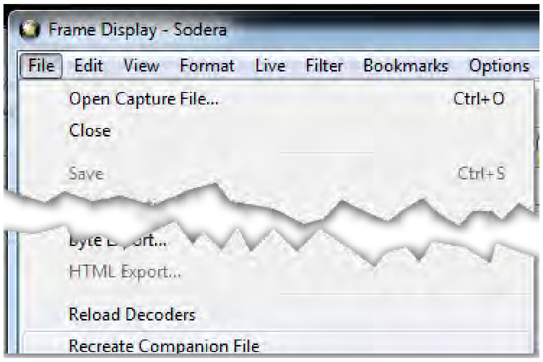
Table 3.8 - CSRmesh Passphrase Format

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 in BPA 600

BPA 600 will automatically capture any *Bluetooth* low energy Advertising packets. CSRmesh packets transmitted over random Non Resolvable Private Address will be captured and displayed in the **Frame Display**.

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 322.

Troubleshooting Tips

MeshOptions.ini Errors

Table 3.9 - Errors Associated with MeshOptions.ini

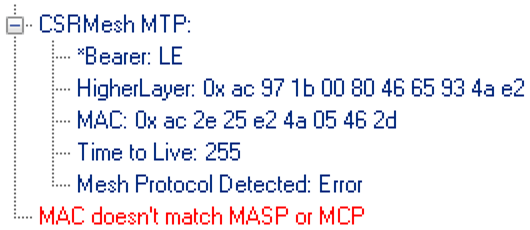
Error Displayed	Descripton
Error: IV Index should be 8 bytes	The IV Index read from MeshOptions.ini is not 8 bytes.
Error: App Key should be 16 bytes	The App Key read from MeshOptions.ini is not 16 bytes
Error: Net Key should be 16 bytes	The Net Key read from MeshOptions.ini is not 16 bytes
Error: Bad 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 3.33 - 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 3.10 - 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 Mesh Security Set in Target

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

Decryption of *Bluetooth* low energy using mesh networking requires a key or key sets. This information must be manually entered into the MeshOptions.ini file located in the system My Decoders folder. Refer to Changing Default File Locations on page 309 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 3.11 - *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 3.12 - CSRmesh Key Set Format

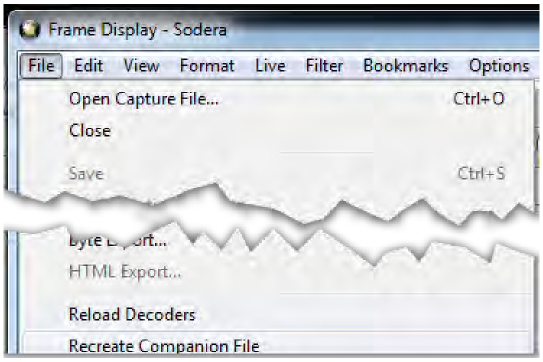
Name	Enter as	Description
Technology Identifier Tag	[CSRmesh]	Required to differentiate from [mesh]. Software will only look for keys after this tag, ignoring comments. Case insensitive within the brackets.
Key set	Name, passphrase	Comma separated: Name = the network name. passphrase = the network key.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

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

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

Loading keys or key sets

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



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

CSRmesh in BPA 600

BPA 600 will automatically capture any *Bluetooth* low energy Advertising packets. CSRmesh packets transmitted over random Non Resolvable Private Address will be captured and displayed in the **Frame Display**.

CSRmesh over GATT

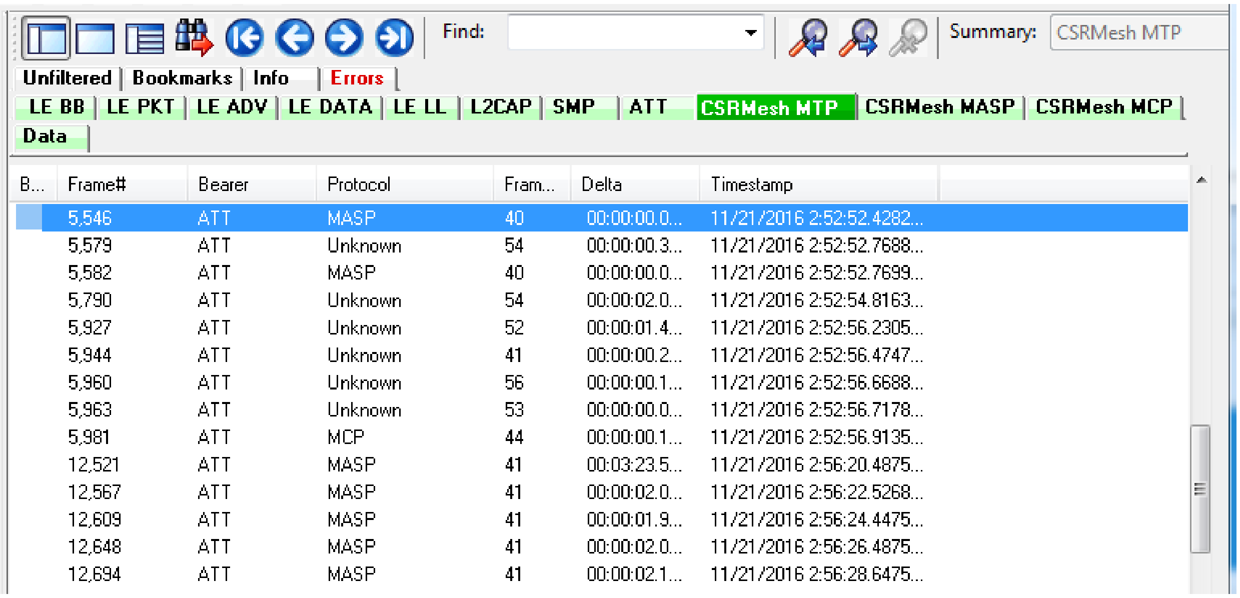
ATT maintains a database which maps handles & UUIDs. When there is a connection request the mappings will be loaded to the initiator and/or advertiser sides of the database.

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 322.

Mesh in the Frame Display

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



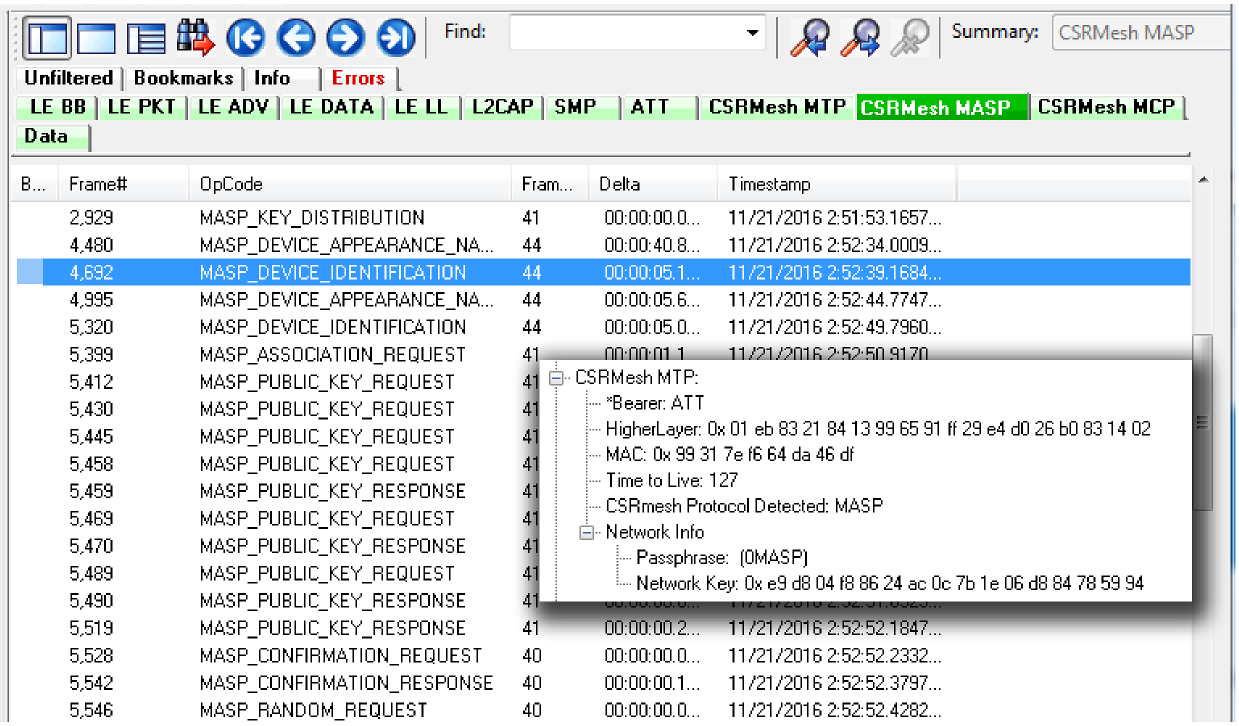
B...	Frame#	Bearer	Protocol	Fram...	Delta	Timestamp
	5,546	ATT	MASP	40	00:00:00.0...	11/21/2016 2:52:52.4282...
	5,579	ATT	Unknown	54	00:00:00.3...	11/21/2016 2:52:52.7688...
	5,582	ATT	MASP	40	00:00:00.0...	11/21/2016 2:52:52.7699...
	5,790	ATT	Unknown	54	00:00:02.0...	11/21/2016 2:52:54.8163...
	5,927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

Figure 3.34 - CSRMesh MTP tab Summay pane display

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

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

The CSRMesh MASP tab is shown in CSRMesh MSRP tab with Decoder pane inset on page 65 shows the Decoder pane (inset) with the "Network Info" passphrase and network key shown but there is no network name.

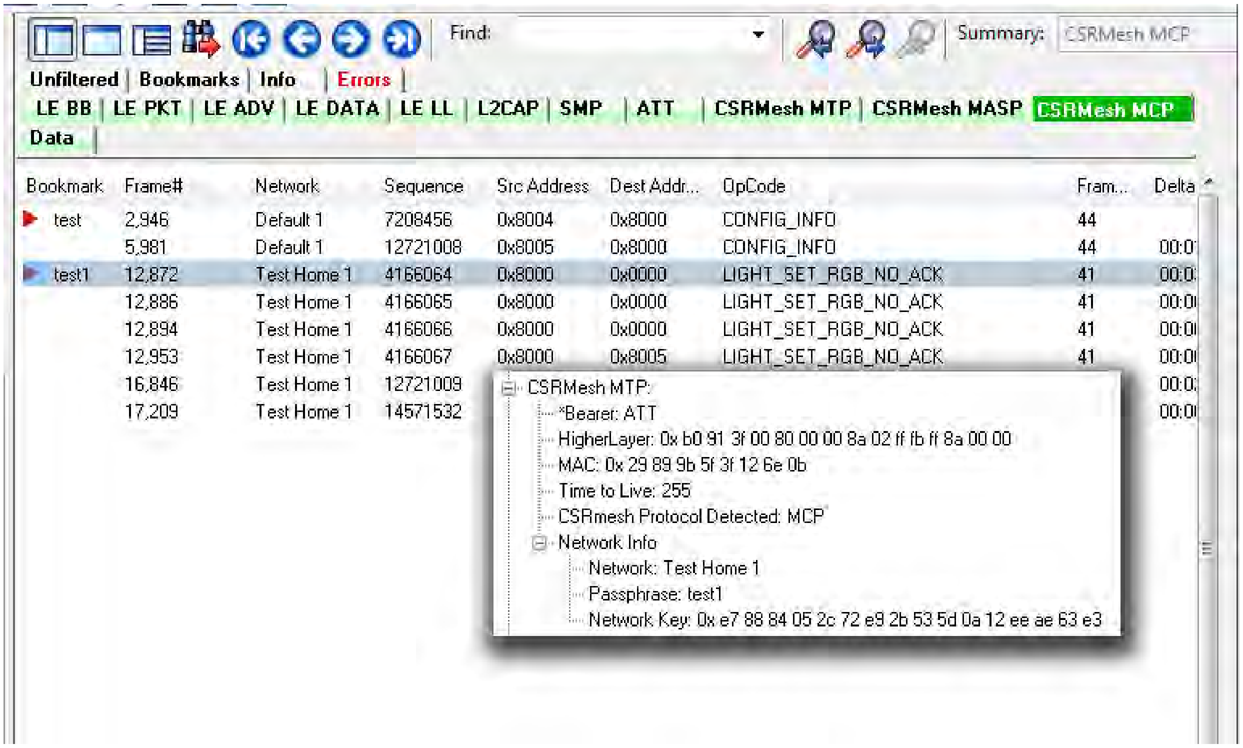

Find:
Summary: CSRMesh MASP
Unfiltered | Bookmarks | Info | Errors
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT | CSRMesh MTP | CSRMesh MASP | CSRMesh MCP | Data

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

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

Figure 3.35 - **CSRMesh MSRP** tab with Decoder pane inset

The CSRMesh MCP tab is shown in CSRMesh MCP tab with Decoder pane inset on page 66 shows the Decoder pane (inset) with the "Network Info" passphrase and network key and network name shown. The network name appears in the Network column of the Summary pane.


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

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

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

Figure 3.36 - **CSRMesh MCP** tab with Decoder pane inset

Troubleshooting Tips

MeshOptions.ini Errors

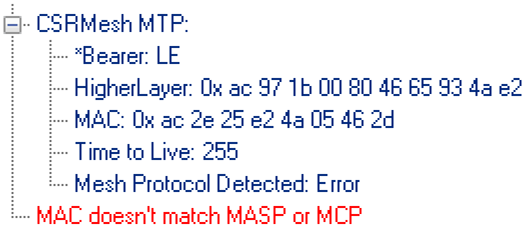
Table 3.13 - Errors Associated with MeshOptions.ini

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

CSRmesh Errors

a. Incorrect key set

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



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

Figure 3.37 - 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 3.14 - Errors: Bluetooth technology using mesh networking

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

Table 3.14 - Errors: Bluetooth technology using mesh networking (continued)

Error	Description
Possible error in app decryption	Possible error in app decryption

3.5 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.

3.5.1 Classic *Bluetooth* Transmitter Classes

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

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

Table 3.15 - 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.

3.5.2 *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 3.16 - *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.

3.5.3 BPA 600 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 test setups.

- Coaxial cable with adapter for connecting to DUT 1.
- Coaxial cable with adapter for connecting to DUT 2.
- 2 Coaxial T-connectors.
- 2 SMA adapters for connecting coaxial cable or attenuators to the BPA 600 antenna connectors.
- Attenuators depending on the *Bluetooth* Class being tested.
- Frontline BPA 600 Dual Mode *Bluetooth* Protocol Analyzer
- Personal computer for running Frontline software.

Test Set Up

BPA 600 Conductive Test Setup on page 70 shows the test setup.

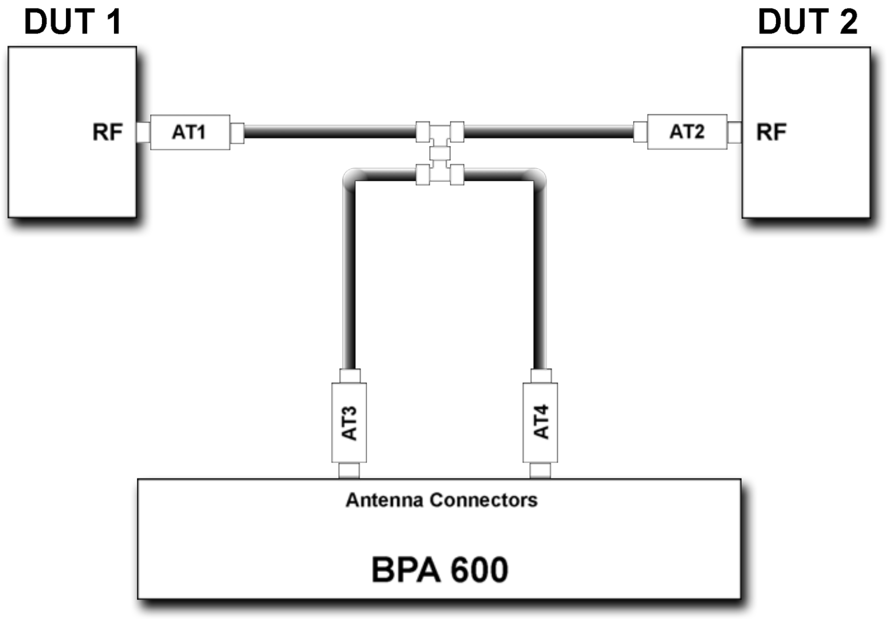


Figure 3.38 - BPA 600 Conductive Test Setup

Both ComProbe BPA 600 antennas must be connected as shown.

The AT1 through AT4 attenuator values will depend on the DUT1 and DUT2 transmitter Class. At higher power levels all four attenuators may be needed. In all cases, use good engineering practices to protect the devices under test and the ComProbe hardware from damage, and to ensure reliable operation.

Assuming that there is no attenuation in the test setup:

- At each T-connector the power will split in half. Therefore the power reaching the BPA 600 protocol analyzer will be one-fourth the transmitted power. For example if DUT 1 is a Class 1 device transmitting +20 dBm (100 mW), at the first T-connector it will split with +17 dBm (50 mW) going to DUT2 and +17dBm (50 mW) going to the ComProbe analyzer.
- The +17dBm (50 mW) going to the ComProbe analyzer splits again. Each coaxial cable going to a ComProbe analyzer antenna connector carries +14 dBm (25 mW).
- If DUT1 or DUT2 is a Class 2 device, +8 dBm (6.25 mW) will reach each ComProbe analyzer antenna connector. If they are Class 3 devices, -6 dBm (0.25 mW) will reach each antenna connector.
- Attenuation should be selected to limit the received power levels to prevent equipment damage, and to provide sufficient power to reliably operate the equipment. If using attenuation follow these recommendations:
- If the devices are of the same class, the attenuators AT1 and AT2 should be of equal value.
- Attenuators AT3 and AT4 should be of equal value.
- Determine the maximum power received at the ComProbe antenna jacks. Then select an appropriate attenuator value to limit the input power to -20 dBm (10 µW) maximum.

3.5.4 *Bluetooth* Conductive Test Process

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

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

Chapter 4 Capturing and Analyzing Data

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

4.1 Capture Data

4.1.1 Air Sniffing: Positioning Devices

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

Problems with indoor radio propagation

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

Estimating indoor propagation loss

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

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

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

Mitigating path loss and interference

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

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

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

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

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

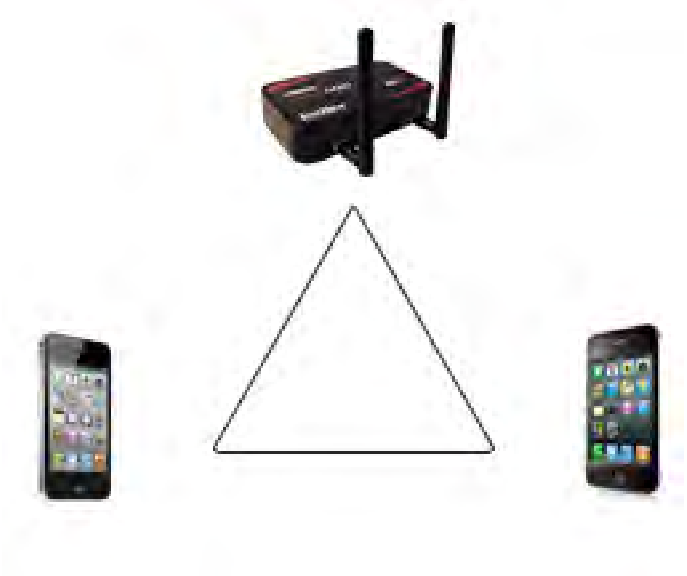


Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane

Finally, eliminate other RF sources.

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

Positioning for audio capture

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

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

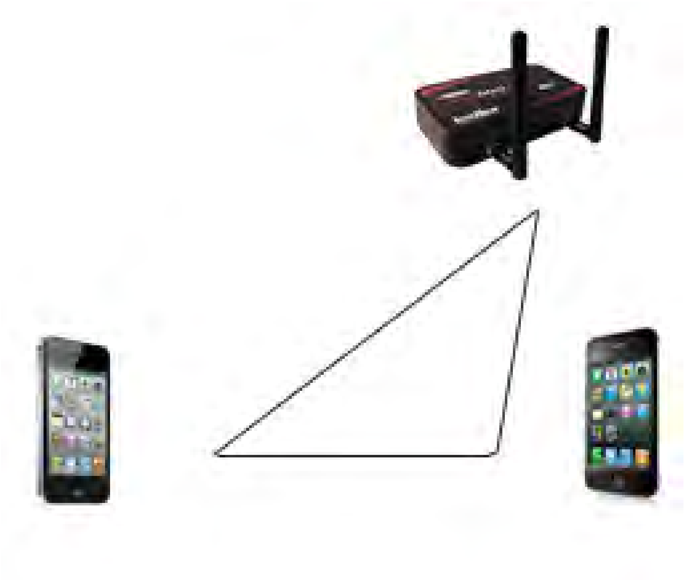


Figure 4.2 - For Audio A2DP, Position Closer to SINK DUT

Poor Placement

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

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

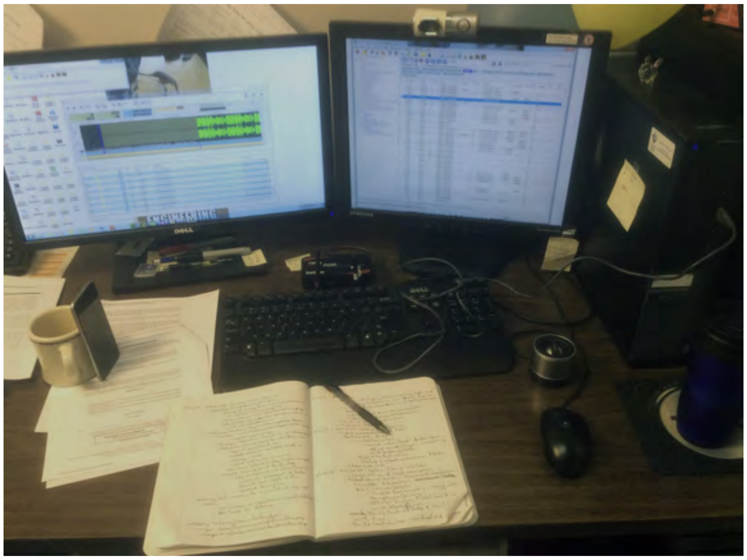


Figure 4.3 - Example: Poor Capture Environment

4.1.2 Capturing Data to Disk - General Procedure

> **Note:** Capture is not available in Viewer mode.

1. Click the **Start Capture** button ● to begin capturing to a file. This icon is located on the **Control** , **Event Display**, and **Frame Display** windows.
2. Files are placed in My Capture Files by default and have a .cfa extension. Choose **Directories** from the **Options** menu on the **Control** window to change the default file location.

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

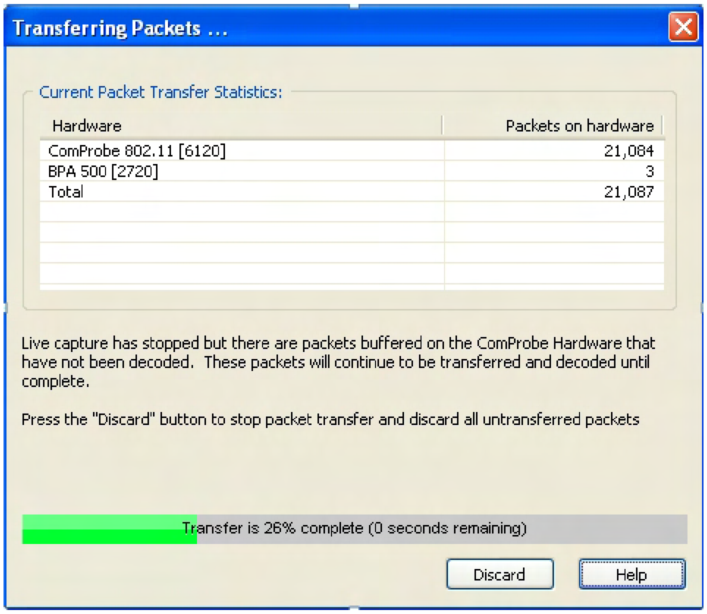
3. Watch the status bar on the **Control** window to monitor how full the file is. When the file is full, it begins to wrap, which means the oldest data will be overwritten by new data.
4. Click the **Stop Capture** icon ■ to temporarily stop data capture. Click the **Start Capture** icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured data remains in the file.
5. To clear captured data, click the **Clear** icon .
   - If you select **Clear** after selecting **Stop Capture**, a dialog appears asking whether you want to save the data.

  - You can click **Save File** and enter a file name when prompted .
  - If you choose **Do Not Save**, all data will be cleared.
  - If you choose **Cancel,** the dialog closes with no changes.
- If you select the **Clear** icon while a capture is occurring:
  - The capture stops.
  - A dialog appears asking if you want to save the capture
  - You can select **Yes** and save the capture or select **No** and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
  - If you choose **Cancel**, the dialog closes with no changes.

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

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

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



Transferring Packets ...

Current Packet Transfer Statistics:

Hardware	Packets on hardware
ComProbe 802.11 [6120]	21,084
BPA 500 [2720]	3
Total	21,087

Live capture has stopped but there are packets buffered on the ComProbe Hardware that have not been decoded. These packets will continue to be transferred and decoded until complete.

Press the "Discard" button to stop packet transfer and discard all untransferred packets

Transfer is 26% complete (0 seconds remaining)

Figure 4.4 - Packet Transfer Dialog

4.1.3 Capturing Data with BPA 600 Analyzer

So, now we have our ComProbe BPA 600 analyzer installed, devices under test turned on and identified in **BPA 600 datasource**; it is time to sniff the communication between the devices and capture data.

Once you have completed the **Devices Under Test** selection, you are ready to capture data.

1. Select **Start Sniffing** on the **Datasource** dialog from the toolbar (Figure 4.5) .

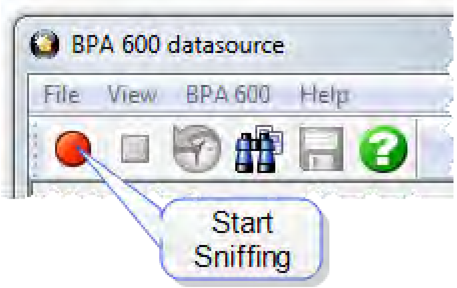


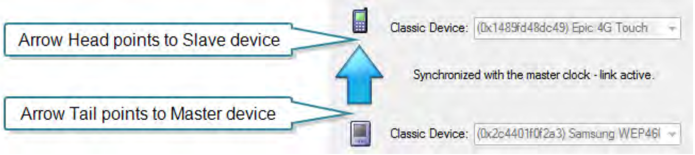
Figure 4.5 - Start Sniffing from Datasource Toolbar.

2. Begin the pairing process between the devices (Only if you are using Classic or Classic/low energy. Low energy by itself does not require that devices be paired.)

As data is being captured, the **Capture Status** message in the **Control** window indicates the synchronization status of the ComProbe BPA 600 analyzer as well as the Master-Slave relationship. The colored arrows change depending on the synchronization state and the direction of the arrow points from Master (arrow tail) to Slave (arrow head). There are five states:

Table 4.1 - BPA 600 Roleless Arrows

Arrow	Description
↑	Blue = synchronized with the Master clock - link active.
↕	Green = running and waiting for Master to connect to the Slave. A double headed arrow means that the master and slave have yet to be determined.
↕	Red = initializing or halted. A double headed arrow means that the master and slave have yet to be determined.
↕	Yellow = waiting for the Master to resume transmission.
↑	Gray = synchronized with the Master clock - link inactive.


Arrow Head points to Slave device
Arrow Tail points to Master device

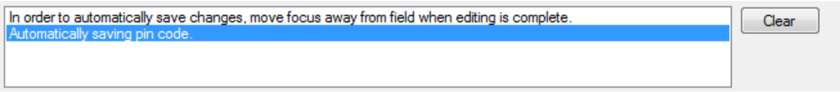
Classic Device: (0x1489fd48dc49) Epic 4G Touch

Synchronized with the master clock - link active.

Classic Device: (0x2c4401f0f2a3) Samsung WEP46l

When you are capturing data, there are several important concepts to consider.

- 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.
- 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.
- Click the **Stop** icon ■ to temporarily stop data capture. Click the **Start Capture** icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured date remains in the file.
- To clear captured data, click the **Clear** icon .
- If you select **Clear** after selecting **Stop**, a dialog appears asking whether you want to save the data.
  - You can click **Save File** and enter a file name when prompted .
  - If you choose **Do Not Save**, all data will be cleared.
  - If you choose **Cancel,** the dialog closes with no changes to the data.
- If you select the **Clear** icon while a capture is occurring:
  - The capture stops.
  - A dialog appears asking if you want to save the capture
  - You can select **Yes** and save the capture or select **No** and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
  - If you choose **Cancel**, the dialog closes with no changes to the data.
  - The link key/pin code can be changed while sniffing and the changes will be automatically saved in the configuration file.
    - While the device is sniffing click in the **Classic Encryption** link key/pin code field. This action places the focus on that window.
    - Change the link key/pin code.
    - The Status window at the bottom of the page will inform the user to move focus away from the link key/pin code window.
    - Click the mouse outside the link key/pin code field or press the Tab key. This action will remove the focus from the link key/pin code window.
    - The link key/pin code changes are automatically saved to the configuration file.



In order to automatically save changes, move focus away from field when editing is complete.
Automatically saving pin code.

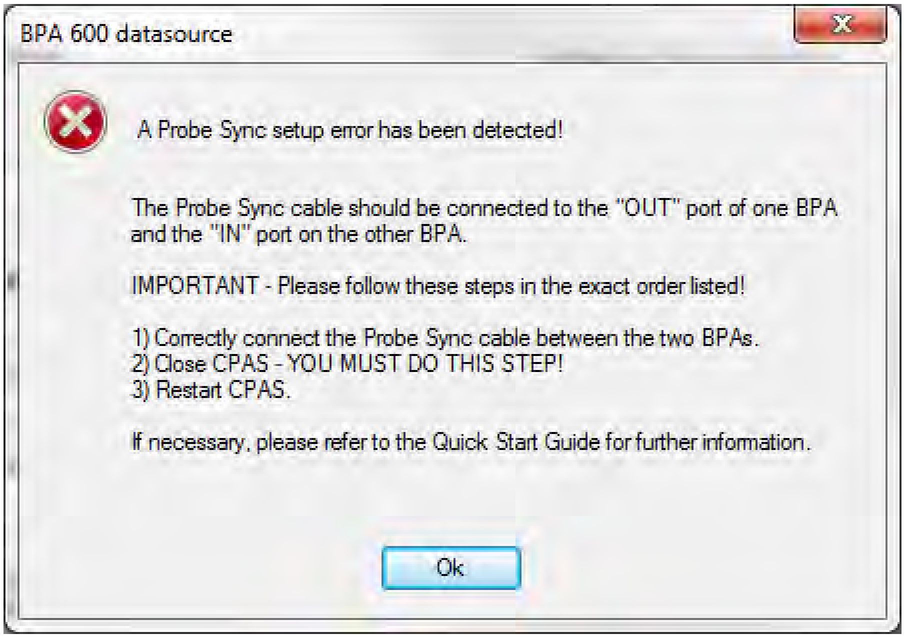
4.1.3.1 BPA 600 Capture with ProbeSync

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

If two ComProbe BPA 600 hardware are connected in a ProbeSync configuration, two to four links can be synchronized. Four links result when each BPA 600 analyzer is configured for Classic Only Multiple Connections with two links per BPA 600 device.

When configured for synchronization through ProbeSync one BPA 600 device provides the clock to the other device. The clock is provided by a CAT 5 cable between the master BPA 600 **OUT** connector—sending the synchronizing clock—to the BPA 600 hardware **IN** connector—receiving the clock.

When the BPA 600 software runs in ProbeSync one **Control** window opens with two **BPA 600 datasource** windows, one for each connected device. Each device datasource is setup individually to sniff their respective link. Should the hardware be connected incorrectly, that is **IN** to **IN** or **OUT** to **OUT**, an error message will appear. Follow the instructions in error message. To continue click on the **OK** button. The **BPA 600 datasource Status** window will also display a warning message suggesting information sources.



A Probe Sync setup error has been detected!

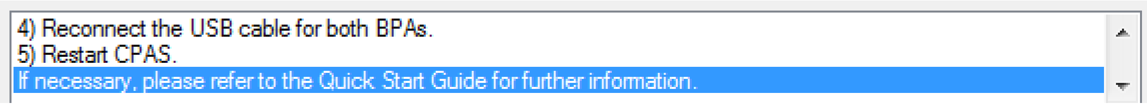
The Probe Sync cable should be connected to the "OUT" port of one BPA and the "IN" port on the other BPA.

IMPORTANT - Please follow these steps in the exact order listed!

1) Correctly connect the Probe Sync cable between the two BPAs.
2) Close CPAS - YOU MUST DO THIS STEP!
3) Restart CPAS.

If necessary, please refer to the Quick Start Guide for further information.

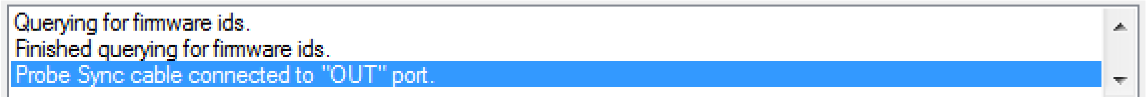
Figure 4.6 - Incorrect ProbeSync Hardware Connection Error



4) Reconnect the USB cable for both BPAs.
5) Restart CPAS.
If necessary, please refer to the Quick Start Guide for further information.

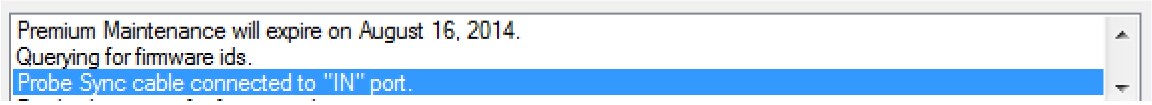
Figure 4.7 - Incorrect ProbeSync Hardware Connection Message In Datasource Status

In the device providing the clock, the **BPA 600 datasource** dialog the **Start Sniffing** ● button initiates the capture for both devices. On the device receiving the clock—cable connected to **IN**— the **BPA 600 datasource** dialog **Start Sniffing** button is disabled when using ProbeSync. In the both device's status window in the **BPA 600 Datasource** dialog will announce the synchronizing function of each.



Querying for firmware ids.
Finished querying for firmware ids.
Probe Sync cable connected to "OUT" port.

Figure 4.8 - BPA 600 ProbeSync Synchronizing Device Status Message



Premium Maintenance will expire on August 16, 2014.
Querying for firmware ids.
Probe Sync cable connected to "IN" port.

Figure 4.9 - BPA 600 ProbeSync Synchronized Device Status Message

Data captured in the synchronized device will appear in the **Frame Display**, **Event Display**, **Bluetooth Timeline**, **Bluetooth low energy Timeline**, and **Coexistence View**. Data saved as a capture file will include data captured on both devices.

BPA 600 hardware can also be connected via ProbeSync to ComProbe 802.11 hardware, but the BPA 600 device must be connected to provide the clock—the CAT5 cable connected to the BPA 600 **OUT** jack.

4.1.4 Combining BPA 600, 802.11, and HSU with ProbeSync

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

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

- ComProbe devices are connected serially in a daisy-chain fashion. The combined length of all cables in the chain cannot exceed 1.5 meters (4.5 ft.).
- The "master" ComProbe device provides the clock to the other devices. All other ComProbe devices are "slaves" and received the clock from the "master" device.
- On ComProbe devices with an **OUT** and **IN** connector, the function of these connectors is dependent on if they are a "master" or a "slave".
  - "master" device: **OUT** connector provides the clock to all "slave" devices. **IN** connector is not used.
  - "slave" device: **IN** connector receives the clock from the **OUT** connector of the prior device in the chain. The **OUT** connector is just a pass-through connector on a "slave" device.
- BPA 600 is always the "master" device and the first device in the chain, if being used.
- HSU is always the last "slave" device in the chain, if being used.
- HSU maximum capture data rate is 6 Mbit/sec.

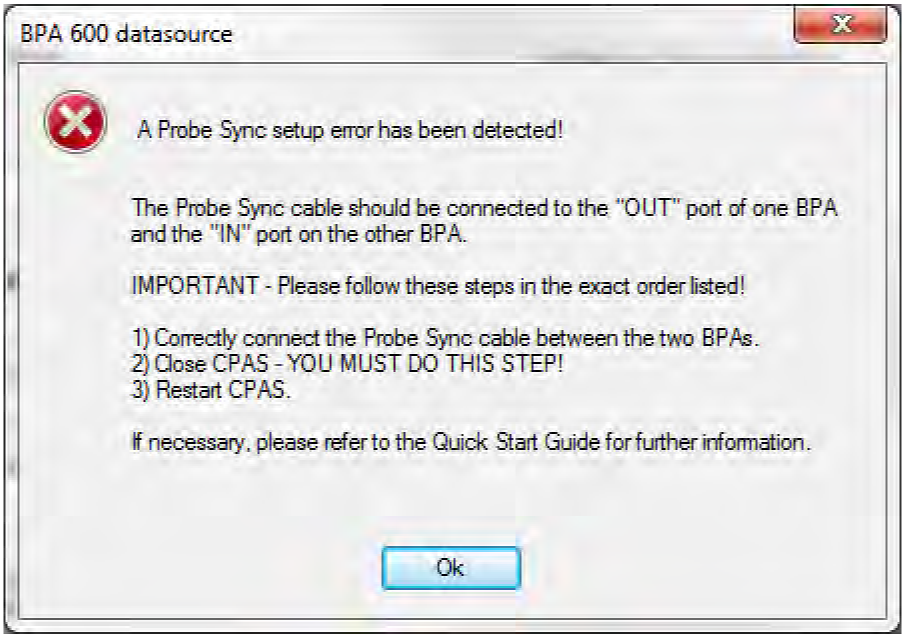
Connecting ComProbe BPA 600, ComProbe 802.11, and ComProbe HSU devices in ProbeSync takes place in the following steps.

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

Each device datasource is setup individually to sniff their respective link. That is, you will see a separate datasource window for the BPA 600 device, the 802.11 device, and the HSU device.

Data saved as a capture file will include data captured on each device.

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



BPA 600 datasource

A Probe Sync setup error has been detected!

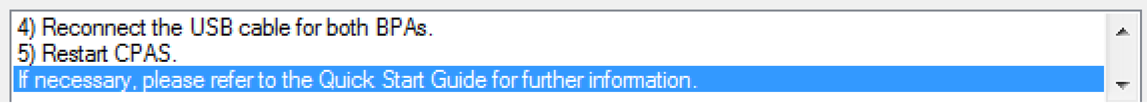
The Probe Sync cable should be connected to the "OUT" port of one BPA and the "IN" port on the other BPA.

IMPORTANT - Please follow these steps in the exact order listed!

1) Correctly connect the Probe Sync cable between the two BPAs.
2) Close CPAS - YOU MUST DO THIS STEP!
3) Restart CPAS.

If necessary, please refer to the Quick Start Guide for further information.

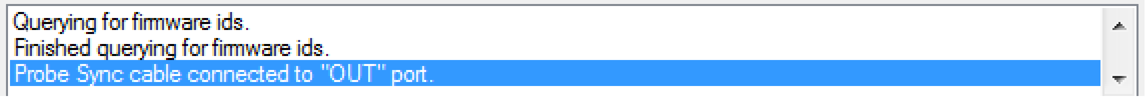
Figure 4.10 - Incorrect ProbeSync Hardware Connection Error



4) Reconnect the USB cable for both BPAs.
5) Restart CPAS.
If necessary, please refer to the Quick Start Guide for further information.

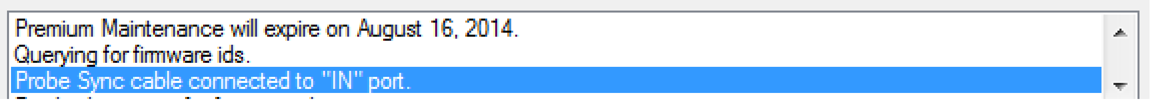
Figure 4.11 - Incorrect ProbeSync Hardware Connection Message In Datasource Status

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



Querying for firmware ids.
Finished querying for firmware ids.
Probe Sync cable connected to "OUT" port.

Figure 4.12 - ProbeSync Synchronizing Device Status Message



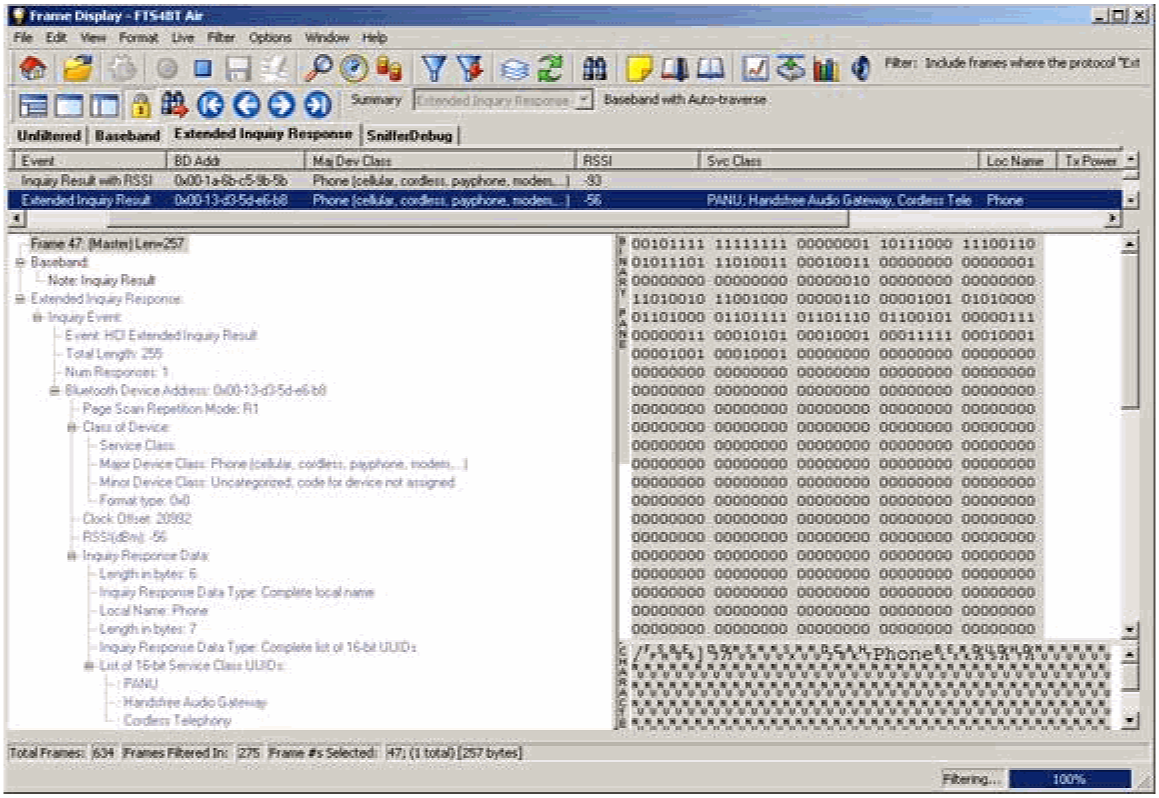
Premium Maintenance will expire on August 16, 2014.
Querying for firmware ids.
Probe Sync cable connected to "IN" port.

Figure 4.13 - ProbeSync Synchronized Device Status Message

Data captured in the synchronized device will appear in the **Frame Display**, **Event Display**, **Bluetooth Timeline**, **Bluetooth low energy Timeline**, and **Coexistence View**.

4.1.5 Extended Inquiry Response

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



Frame Display - FTS4BT Air
File Edit View Format Live Filter Options Window Help
Filter: Include frames where the protocol "Ext
Summary
Extended Inquiry Response
Baseband with Auto-traverse
Unfiltered
Baseband
Extended Inquiry Response
SnifferDebug
BINARY PANE
CHARACTER
Filtering...
100%

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

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

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

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

Figure 4.14 - Frame Display Extended Inquire Response

EIR displays extensive information about the Bluetooth® devices that are discovered as data is being captured. EIR provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode. Before the EIR tab was created, this type of information was not available until a connection was made to a device. Therefore, EIR can be used to determine whether a connection can/should be made to a device prior to making the connection.

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

4.2 Protocol Stacks

4.2.1 Protocol Stack Wizard

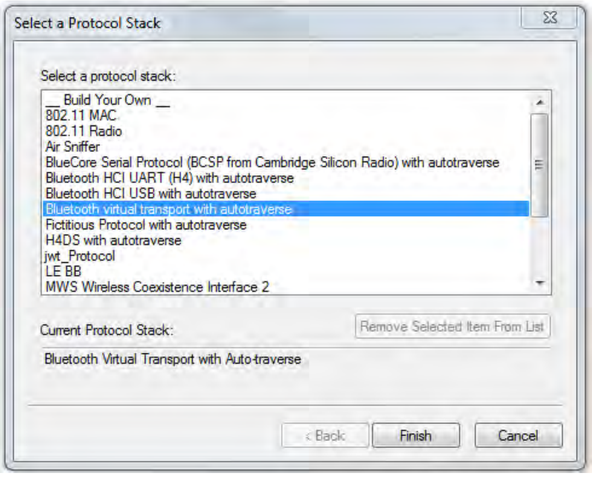
The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.

To start the wizard:

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

2. Select a protocol stack from the list, and click **Finish**.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating and Removing a Custom Stack on page 85.



Select a Protocol Stack

Select a protocol stack:

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

Current Protocol Stack:

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 86 for more information.

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

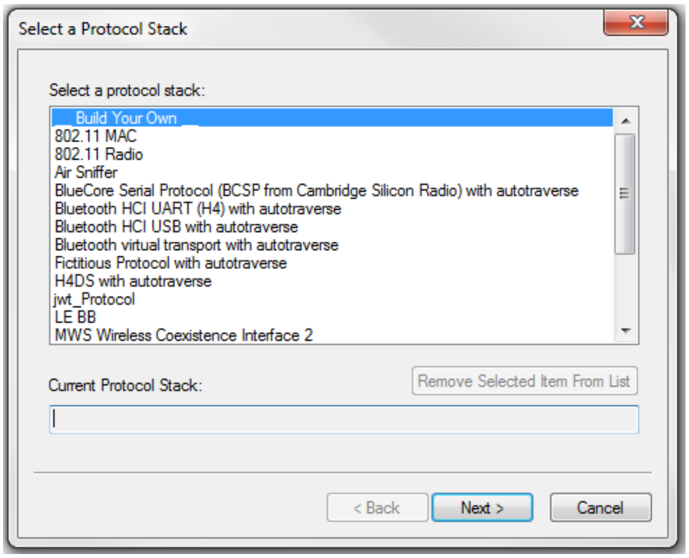
4.2.2 Creating and Removing a Custom Stack

To create a custom stack:

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

2. Select **Build Your Own** from the list and click **Next**.

3. The system displays an information screen that may help you decide if you need to define your own custom stack. Defining a custom stack means that the analyzer uses the stack for every frame. Frames that do not conform to the stack are decoded incorrectly. Click **Next** to continue.


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

Select Protocols

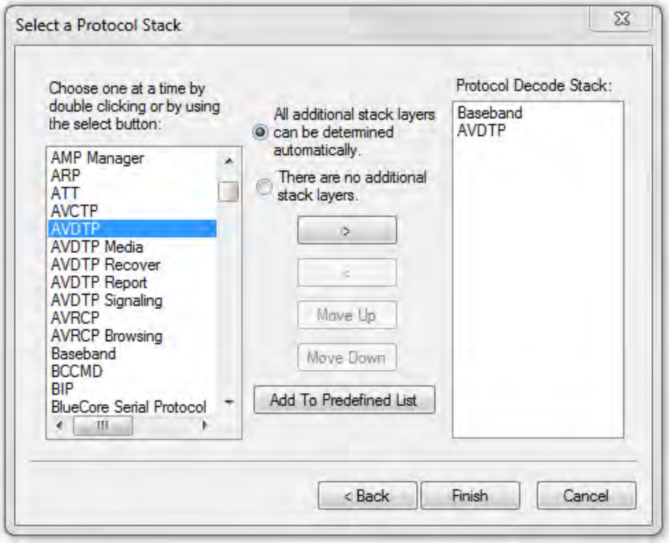
1. Select a protocol from the list on the left.

2. Click the right arrow button to move it to the **Protocol Decode Stack** box on the right, or double-click the protocol to move it to the right.

3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.

4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the **Move Up** and **Move Down** buttons until the protocol is in the correct position.

5. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.



Auto-traversal (Have the analyzer Determine Higher Layers)

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

1. Click the **All additional stack layers can be determined automatically** button.

2. If your protocol stack is complete and there are no additional layers, click the **There are no additional stack layers** button.

3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

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

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

Remove a Stack

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

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

4.2.3 Reframing

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

> **Note:** You cannot reframe from the Capture File Viewer .

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

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

1. Load your capture file by choosing **Open** from the **File** menu on the **Control** window, and select the file to load.
2. Select the protocol stack by choosing **Protocol Stack** from the **Options** menu on the **Control** window, select the desired stack and click **Finish**.
3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the **Protocol Stack Wizard** asks you if you want to reframe your data. Choose **Yes**.
4. The analyzer adds frame markers to your data, puts the framed data into a new file, and opens the new file. The original capture file is not altered.

See Unframing on page 86 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 86 for instructions on framing unframed data.

4.2.5 How the Analyzer Auto-traverses the Protocol Stack

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

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

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

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

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

4.2.6 Providing Context For Decoding When Frame Information Is Missing

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

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

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

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

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

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

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

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

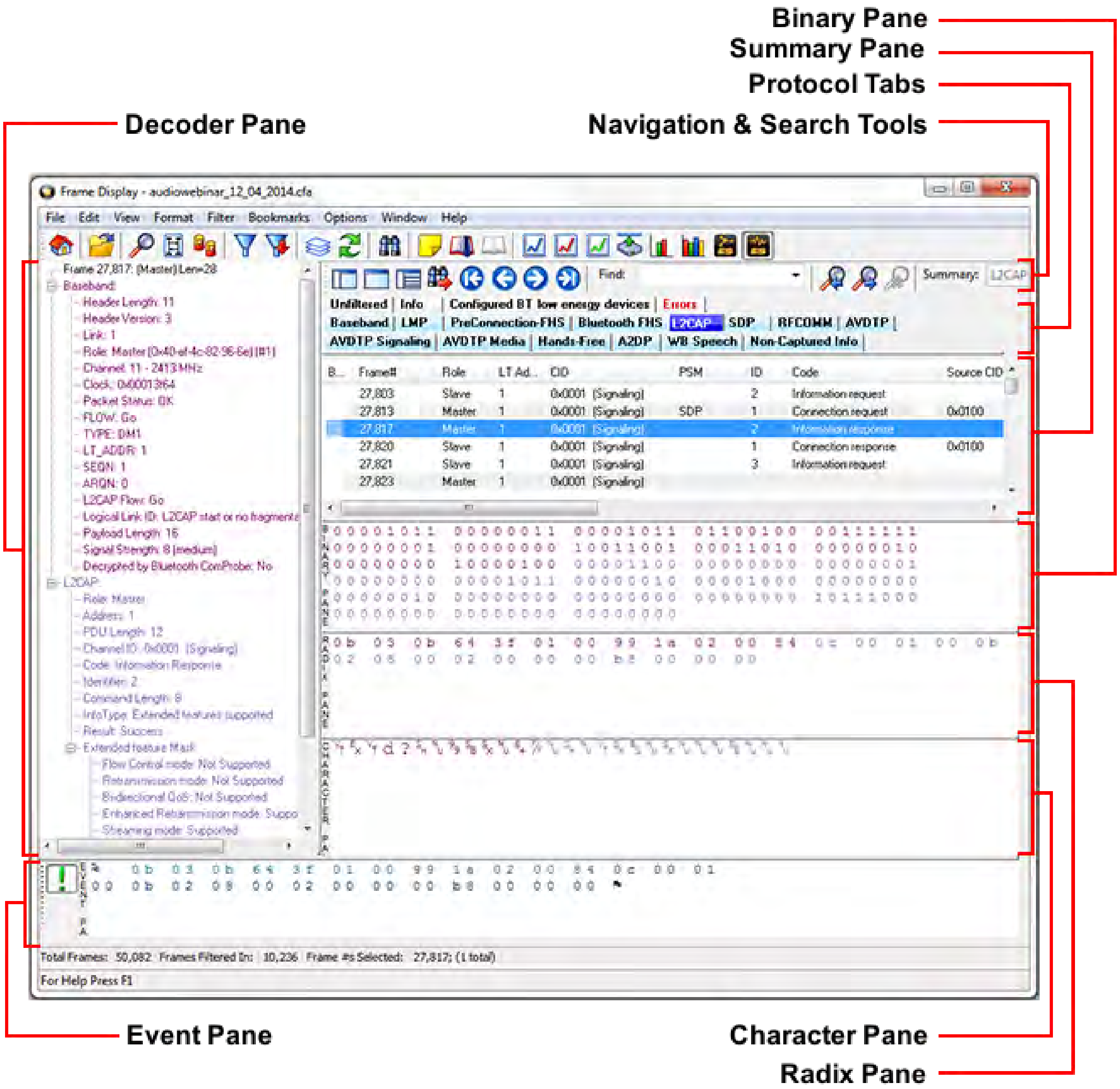
3. This option brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check **Automatically Request Missing Decoding Information.**
5. When unchecked, the analyzer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

4.3 Analyzing Protocol Decodes

4.3.1 The Frame Display

To open this window

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


Binary Pane
Summary Pane
Protocol Tabs
Decoder Pane
Navigation & Search Tools
Frame Display - audiowebinar_12_04_2014.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: L2CAP
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 | WB Speech | Non-Captured Info |
BINARY PANE
RADIX PANE
CHARACTER PA
EVENT PA
Event Pane
Character Pane
Radix Pane

```
Frame 27,817: (Master) Len=28
Baseband:
  Header Length: 11
  Header Version: 3
  Link: 1
  Role: Master [0x40-ef-4c-82-96-6e] (#1)
  Channel: 11 - 2413 MHz
  Clock: 0x00013f64
  Packet Status: OK
  FLOW: Go
  TYPE: DM1
  LT_ADDR: 1
  SEQN: 1
  ARQN: 0
  L2CAP Flow: Go
  Logical Link ID: L2CAP start or no fragmenta
  Payload Length: 16
  Signal Strength: 8 (medium)
  Decrypted by Bluetooth ComProbe: No
L2CAP:
  Role: Master
  Address: 1
  PDU Length: 12
  Channel ID: 0x0001 (Signaling)
  Code: Information Response
  Identifier: 2
  Command Length: 8
  InfoType: Extended features supported
  Result: Success
  Extended feature Mask
    Flow Control mode: Not Supported
    Retransmission mode: Not Supported
    Bi-directional QoS: Not Supported
    Enhanced Retransmission mode: Suppo
    Streaming mode: Supported
```

B...	Frame#	Role	LT Ad...	CID	PSM	ID	Code	Source CID
	27,803	Slave	1	0x0001 (Signaling)		2	Information request	
	27,813	Master	1	0x0001 (Signaling)	SDP	1	Connection request	0x0100
	27,817	Master	1	0x0001 (Signaling)		2	Information response	
	27,820	Slave	1	0x0001 (Signaling)		1	Connection response	0x0100
	27,821	Slave	1	0x0001 (Signaling)		3	Information request	
	27,823	Master	1	0x0001 (Signaling)				

```
00001011 00000011 00001011 01100100 00111111
00000001 00000000 10011001 00011010 00000010
00000000 10000100 00001100 00000000 00000001
00000000 00001011 00000010 00001000 00000000
00000010 00000000 00000000 00000000 10111000
00000000 00000000 00000000
```

```
0b 03 0b 64 3f 01 00 99 1a 02 00 84 0c 00 01 00 0b
02 08 00 02 00 00 00 b8 00 00 00
```

```
   0b 03 0b 64 3f 01 00 99 1a 02 00 84 0c 00 01
00 0b 02 08 00 02 00 00 00 b8 00 00 00
```

Total Frames: 50,082 Frames Filtered In: 10,236 Frame #s Selected: 27,817; (1 total)

For Help Press F1

Figure 4.15 - Frame Display with all panes active

Frame Display Panes

The **Frame Display** window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame.

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

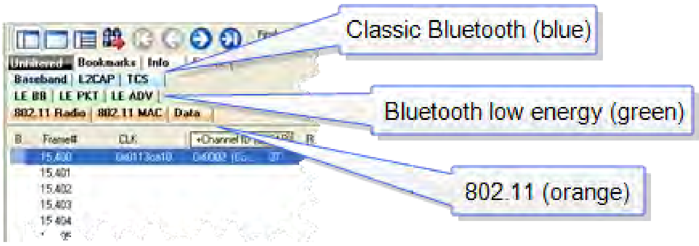
- Decode Pane - The **Decode Pane** displays a detailed decode of the highlighted frame. Fields selected in the **Decode Pane** have the appropriate bit(s) or byte(s) selected in the **Radix**, **Binary**, **Character** , and **Event** panes
- Radix Pane - The **Radix Pane** displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.
- Binary Pane - The **Binary Pane** displays a binary representation of the logical data bytes.
- Character Pane - The **Character Pane** displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.
- Event Pane - The Event Pane displays the physical data bytes in the frame, as received on the network.

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

Protocol Tabs

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

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



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

Select the **Unfiltered** tab to display all packets.

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

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

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

Comparing Frames

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

Frame Wrapping and Display

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

- All **Frame Display** panes except the Summary pane display "No frame selected" when the selected frame is in the buffer (i.e. not wrapped out) but not accessible in the **Summary** pane. This can happen when a tab is selected that doesn’t filter in the selected frame.
- When the selected frame wraps out (regardless of whether it was accessible in the Summary pane) all **Frame Display** panes except the **Summary** pane display "Frame wrapped out of buffer".
- When the selected frame is still being captured, all **Frame Display** panes except the Summary pane display "Frame incomplete".

4.3.1.1 Frame Display Toolbar

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

Table 4.2 - Frame Display Toolbar Icons

Icon	Description
🏠	Control – Brings the Control window to the front.
📂	Open File - Opens a capture file.
⚙	I/O Settings - Opens the I/O Settings dialog.
●	Start Capture - Begins data capture to a user designated file.
■	Stop Capture - Closes a capture file and stops data capture to disk.
💾	Save - Save the currently selected bytes or the entire buffer to file.
	Clear- Discards the temporary file and clears the display.
🔍	Event Display – Brings the Event Display window to the front.

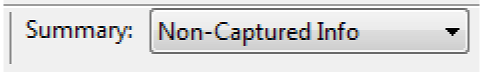
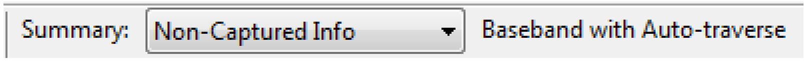
Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
H	Show Message Sequence Chart - Message Sequence Chart (MSC) displays information about the messages passed between protocol layers.
	Duplicate View - Creates a second Frame Display window identical to the first.
▽	Apply/Modify Display Filters - Opens the Display Filter dialog.
▽	Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.
≋	Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data
🔄	Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.
	Find - Search for errors, string patterns, special events and more.
📝	Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.
📕	Add/Modify Bookmark - Add a new or modify an existing bookmark.
📖	Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.
📈	*Bluetooth* Timeline - Opens the Bluetooth Timeline
📈	Coexistence View - Opens the Coexistence View
📈	low energy Timeline- Opens the low energy Timeline

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
⬆	Extract Data - Opens the Extract Data dialog.
📊	*Bluetooth* low energy Packet Error Rate Statistics Opens the Packet Error Rate Statistics display
📊	*Bluetooth* Classic Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.
ES	*Bluetooth* Expert System - Opens Bluetooth Expert System window
ES	Audio Expert System - Opens Audio Expert System Window
Reload Decoders - When **Reload Decoders** is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.	
Filter:	Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.
The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.	
▤	Show Default Panes - Returns the panes to their default settings.
▭	Show Only Summary Pane - Displays only the Summary pane.
◫	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.

Table 4.2 - Frame Display Toolbar Icons(continued)

Icon	Description
←	Previous Frame - Moves to the previous frame in the buffer.
→	Next Frame - Moves to the next frame in the buffer.
→|	Last Frame - Moves to the last frame in the buffer.
Find:	Find on Frame Display only searches the Decode Pane for a value you enter in the text box.
🔍←	Find Previous Occurrence - Moves to the previous occurrence of the value in the Frame Display Find.
🔍→	Find Next Occurrence - Moves to the next occurrence of the value in the Frame Display Find.
🔍✗	Cancel Current Search - Stops the current Frame Display Find.
Summary:	Summary Drop Down Box: Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to the analyzer, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol. When a low energy predefined Named Filter (like Nulls and Polls) is selected, the Summary drop-down is disabled.  Summary: Non-Captured Info
Text with Protocol Stack: To the right of the Summary Layer box is some text giving the protocol stack currently in use.  Summary: Non-Captured Info Baseband with Auto-traverse	

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

4.3.1.2 Frame Display Status Bar

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

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

4.3.1.3 Hiding and Revealing Protocol Layers in the Frame Display

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

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

There are two ways to hide a layer.

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

To reveal a hidden protocol layer:

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

4.3.1.4 Physical vs. Logical Byte Display

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

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

4.3.1.5 Sorting Frames

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

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

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

4.3.1.6 Frame Display - Find

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

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

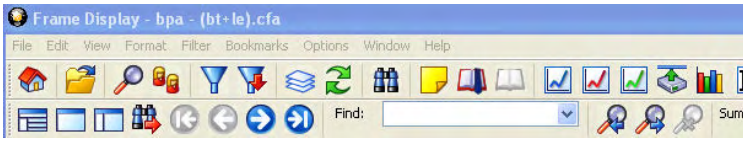
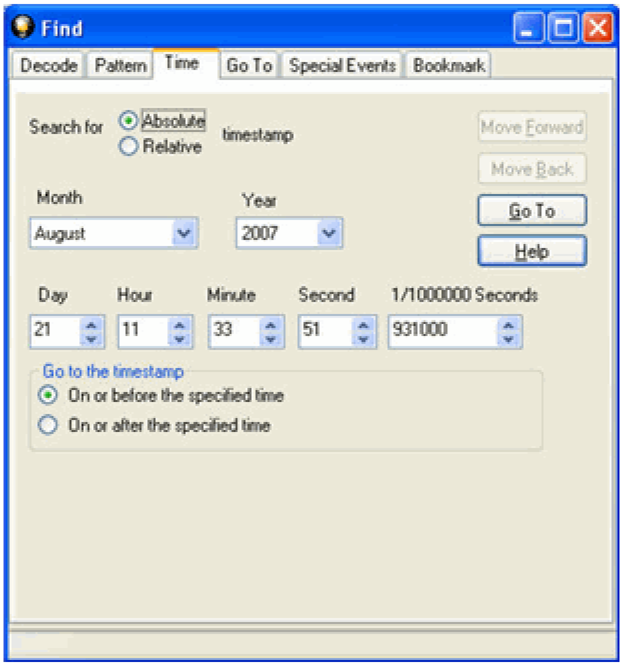

Frame Display - bpa - (bt+le).cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Sum

Figure 4.16 - Frame Display Find text entry field

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



Search for ● Absolute ○ Relative timestamp

Month: August

Year: 2007

Day	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

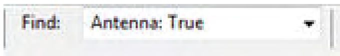
Figure 4.17 - Search/Find Dialog

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.

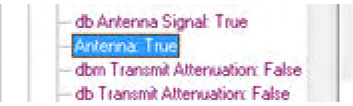
2. Enter a value in the **Find** text box.



Find: Antenna: True

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

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



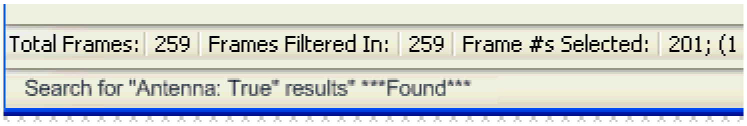
db Antenna Signal: True
Antenna: True
dbm Transmit Attenuation: False
db Transmit Attenuation: False

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

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

There are several important concepts to remember with Find.

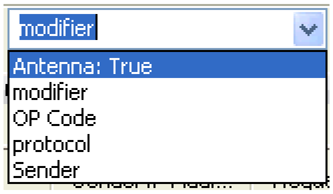
- When you enter a search string and select Enter, the search moves forward.
- If you select **Find Previous Occurrence**, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous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

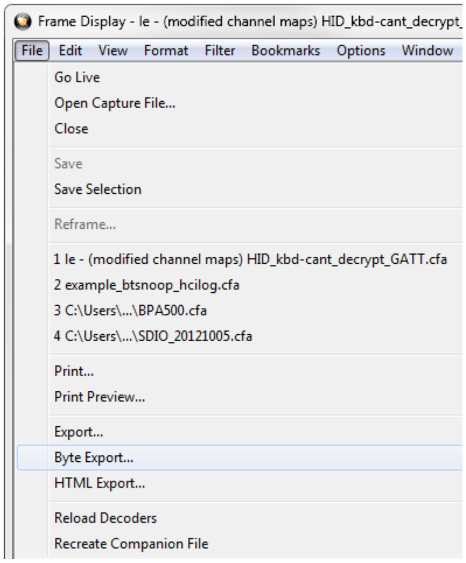
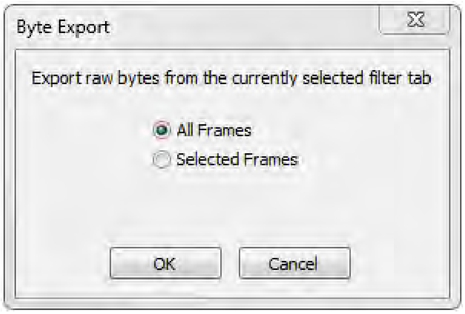

Frame Display - le - (modified channel maps) HID_kbd-cant_decrypt_
File
Edit
View
Format
Filter
Bookmarks
Options
Window
Go Live
Open Capture File...
Close
Save
Save Selection
Reframe...
1 le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa
2 example_btsnoop_hcilog.cfa
3 C:\Users\...\BPA500.cfa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

Figure 4.18 - 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

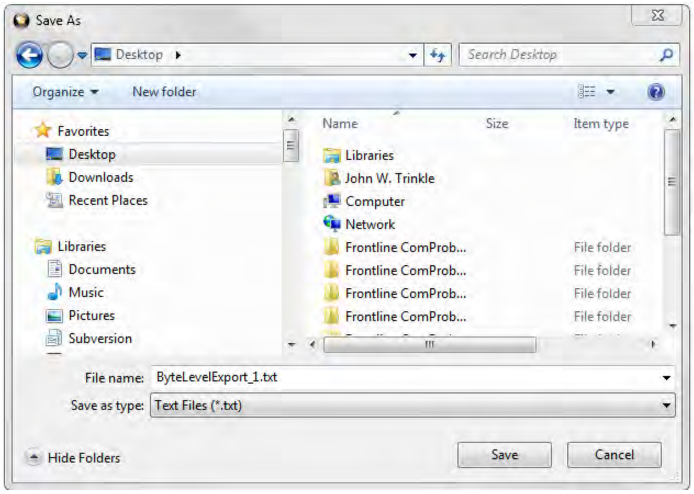
Export raw bytes from the currently selected filter tab

● All Frames
○ Selected Frames

Figure 4.19 - 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.

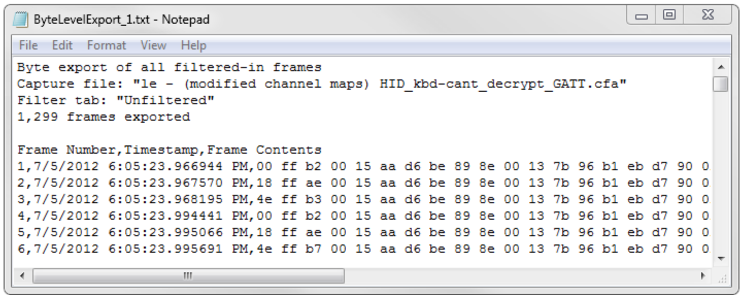

File name: ByteLevelExport_1.txt

Save as type: Text Files (*.txt)

Figure 4.20 - 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 4.21 - Sample Exported Frames Text File

4.3.1.11 Panes in the Frame Display

4.3.1.11.1 Summary Pane

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

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

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

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

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

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

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

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

Protocol Tabs

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

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

General group applies to all technologies. The other groups are technology-specific.

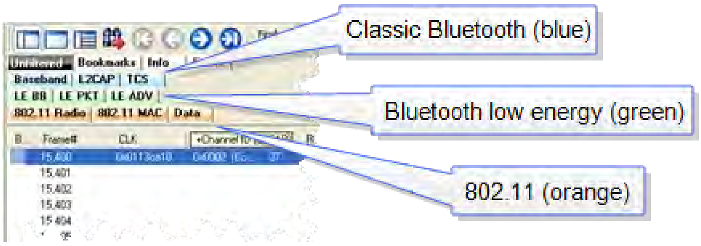

Unfiltered | Bookmarks | Info
Baseband | L2CAP | TCS
LE BB | LE PKT | LE ADV
802.11 Radio | 802.11 MAC | Data
Classic Bluetooth (blue)
Bluetooth low energy (green)
802.11 (orange)

Figure 4.22 - 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:

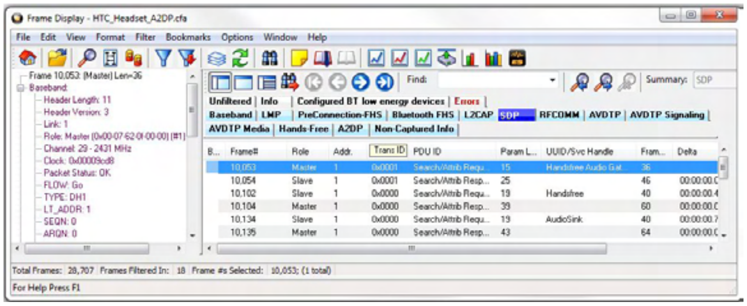
- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

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 |
Trans ID
For Help Press F1

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

B...	Frame#	Role	Addr.	Trans ID	PDU ID	Param L...	UUID/Svc Handle	Fram...	Delta
	10,053	Master	1	0x0001	Search/Attrib Requ...	15	Handsfree Audio Gat...	36	
	10,054	Slave	1	0x0001	Search/Attrib Resp...	25		46	00:00:00.0
	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)

Figure 4.23 - Summary pane (right) with Tooltip on Column 5 (Tran ID)

Sides in *Bluetooth* low energy

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

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

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

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

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

4.3.1.11.2 *Bluetooth* low energy Data Encryption/Master and Slave Assignment

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

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

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

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

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

4.3.1.11.3 *Bluetooth* low energy Decryption Status

Occasionally you may have a packet with an event status of “received without errors,” but a decryption status of “unable to decrypt.” There are three main causes for this, and in order of likelihood they are:

1. **Wrong Long-Term Key** – having the wrong long-term key will cause this error, so the first thing to check is that your long term key is entered correctly in the datasource settings.
2. **Dropped Packets** – Too much interference with a ComProbe device will cause dropped packets and may cause this error. As a rule of thumb, it is always a good idea to ensure the ComProbe device is positioned away from sources of interference, and is placed in between the two devices being sniffed.
3. **Faulty Device** – although the chances of this are low, it is possible that a device is not encrypting packets properly. This is likely to happen only if you are a firmware developer working on encryption.

4.3.1.11.4 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.

4.3.1.11.5 Frame Symbols in the Summary Pane

Table 4.3 - Frame Symbols

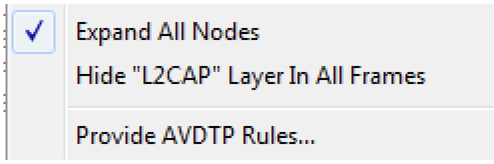
Symbol	Description
🟢	A green dot means the frame was decoded successfully, and the protocol listed in the **Summary Layer** drop-down box exists in the frame. No dot means the frame was decoded successfully, but the protocol listed in the **Summary Layer** drop-down box does not exist in the frame.

Table 4.3 - Frame Symbols (continued)

Symbol	Description
○	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.

4.3.1.11.6 Decode Pane

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



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

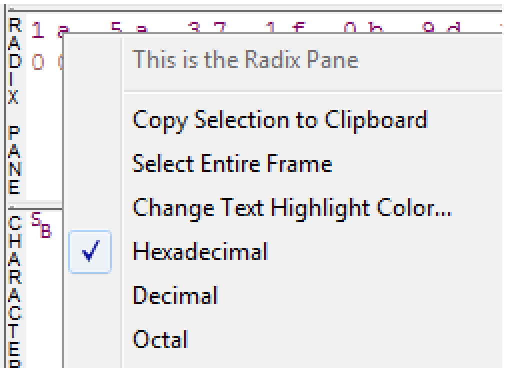
In a USB transaction, all messages that comprise the transaction are shown together in the detail pane. The color coding that is applied to layers when the detail pane displays a single message is applied to both layers and messages when the detail pane displays a transaction. To keep the distinction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

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

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

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

4.3.1.11.7 Radix or Hexadecimal Pane



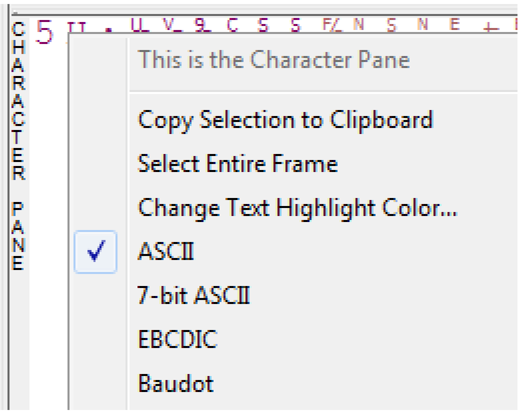
The **Radix** pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the **Format** menu, or by right-clicking on the pane and choosing **Hexadecimal**, **Decimal** or **Octal**.

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.

4.3.1.11.8 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.

4.3.1.11.9 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.

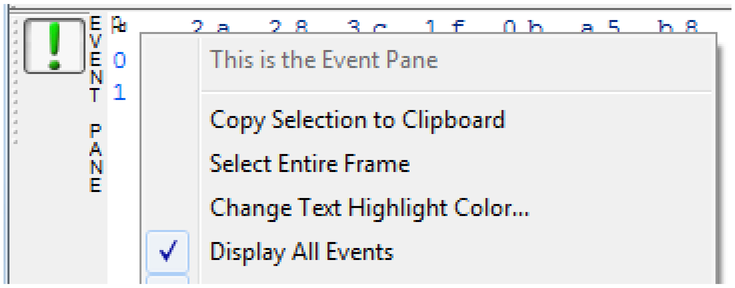
Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

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.

4.3.1.11.10 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.

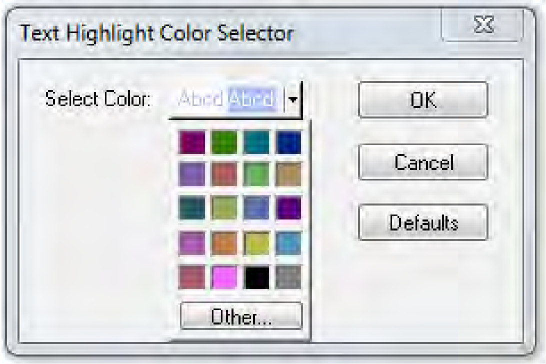
Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

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.

4.3.1.11.11 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.

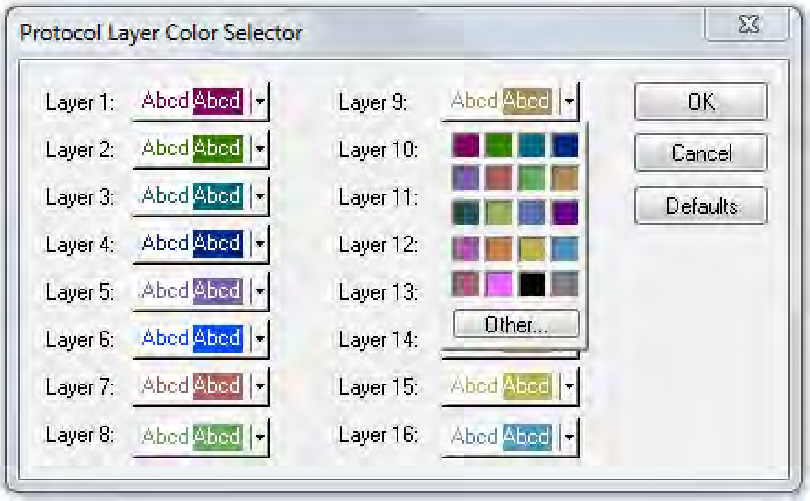


Figure 4.24 - Frame Display Protocol Layer Color Selector

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.

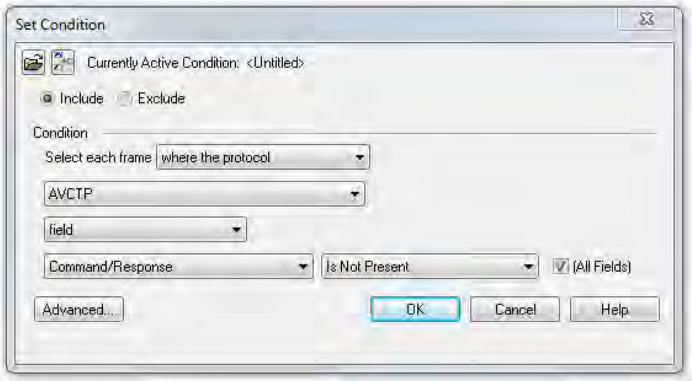
Quick Filters

- 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

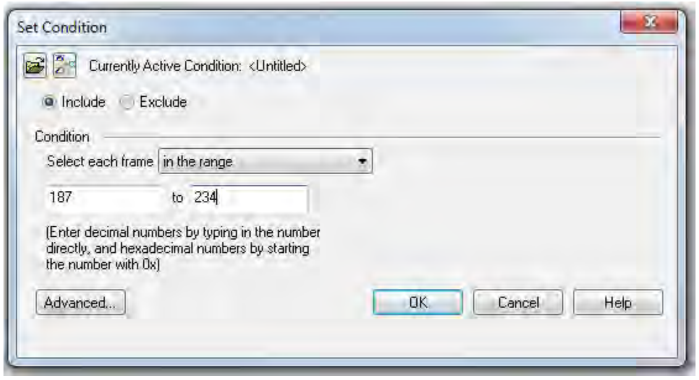
Select each frame: where the protocol

AVCTP

field

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

Figure 4.25 - 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 4.26 - 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.

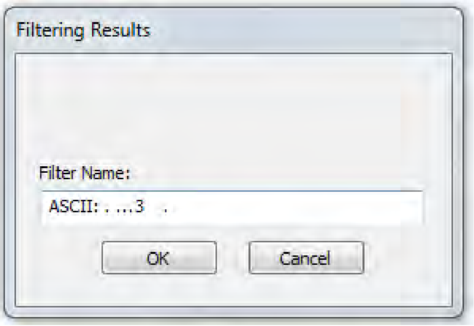
2. Right click in the one of the data columns in the **Summary** Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.

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.

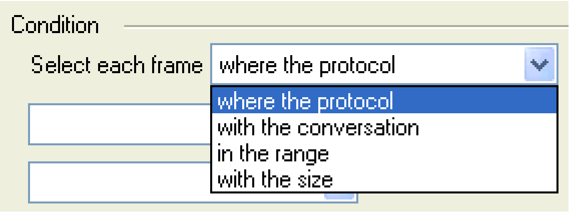
2. Click the **Advanced** button on the **Set Condition** dialog box.

3. Select **Include** or **Exclude** radio button.

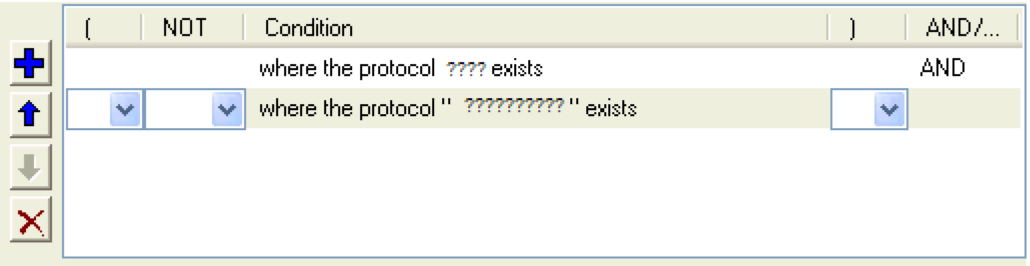
   Now you can set the conditions for the filter.

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

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.



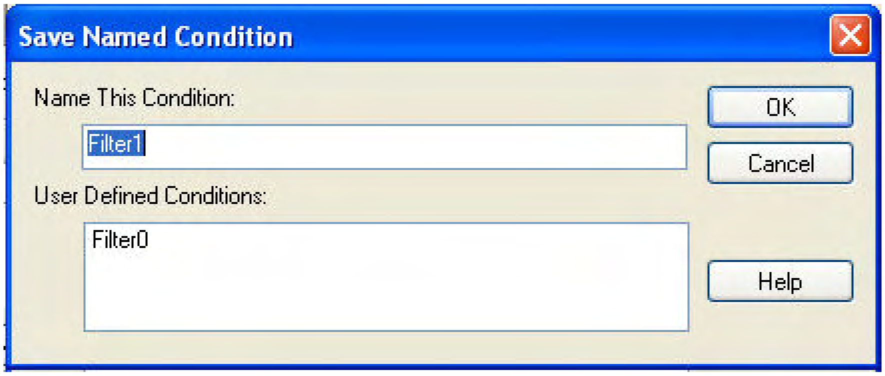
Select each frame: where the protocol



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

Figure 4.27 - 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**.



Name This Condition: Filter1

User Defined Conditions: Filter0

Figure 4.28 - 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.

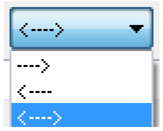
> **Note:** The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

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

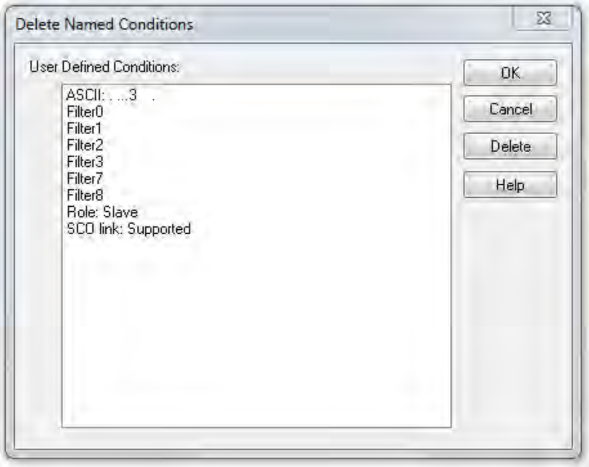
If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

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

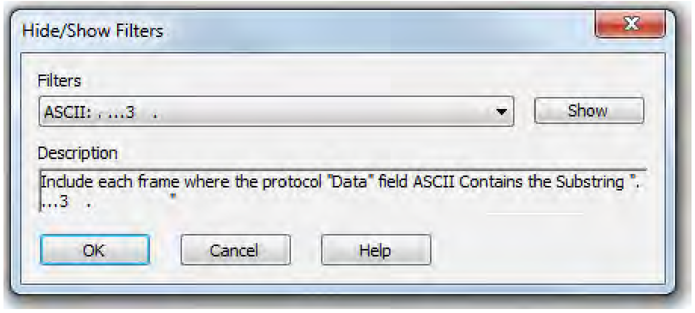
1. Select **Delete Display Filters** from the **Filter** menu in the **Frame Display** window to open the **Delete Named Condition** dialog. The system displays the **Delete Named Condition** dialog with a list of all user defined filters.
2. Select the filter to be deleted from the list.
3. Click the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



ASCII: . ...3 .

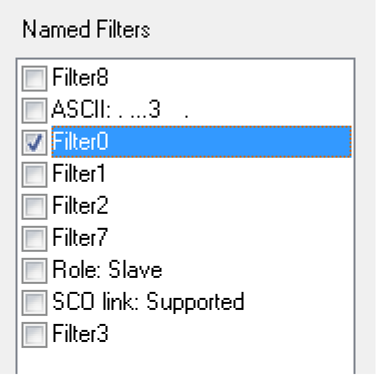
Include each frame where the protocol "Data" field ASCII Contains the Substring ". ...3 . ".

1. **Select Hide/Show Display Filters…** from the **Filter** menu on the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.
3. Click the **Hide** button. The **Hide** button is only showing if the selected filter is currently showing in the **Frame Display**.
4. Click **OK**. The **Hide/Show Filters** dialog box closes, and the system hides the filter and removes the filter tab from the Frame Display.

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

1. Select **Hide/Show Display Filters…** from the **Filter** menu in the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be revealed from the combo box.
3. Click the **Show** button.
4. Click **OK**. The **Hide/Show Filters** dialog box closes and the system reveals the filter in the **Frame Display**.

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



Named Filters

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

Figure 4.29 - Using Named Filters Section of Quick Filters to Show/Hide Filters

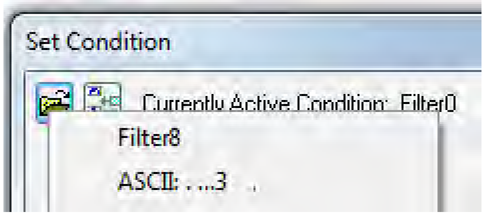
Note: When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Show dialog to display a filter created in one Frame Display in different Frame Display window.

4.3.1.13.1.7 Editing Filters

Modifying a Condition in a Filter

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.



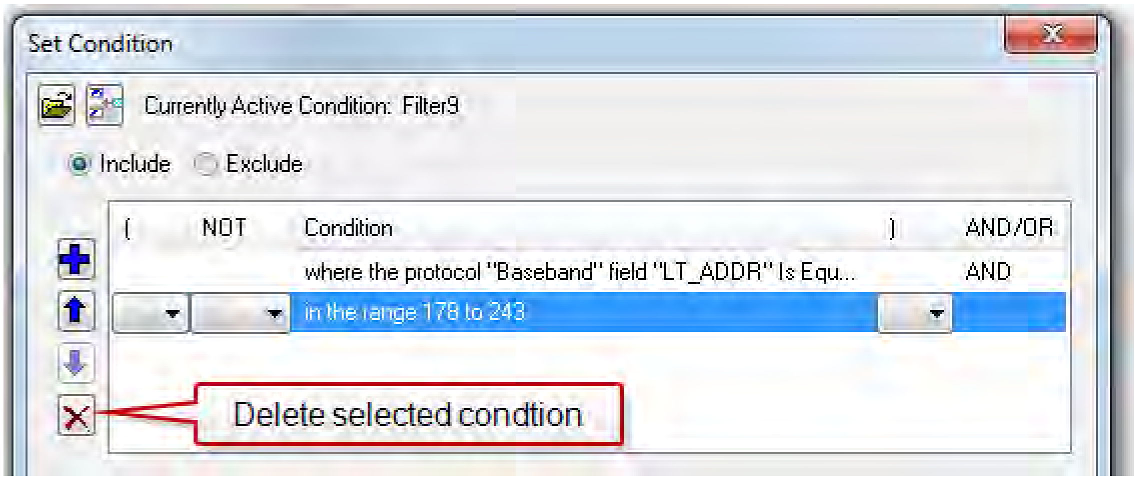
2. Edit the desired parameter of the condition: Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested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

Figure 4.30 - Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.

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

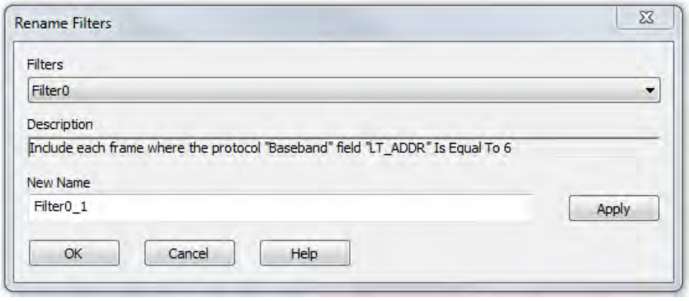
4. Edit the Boolean operators and parentheses as needed.

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

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

Renaming a Display Filter

1. Select **Rename Display Filters…** from the **Filter** menu in the **Frame Display** 🔍 window to open the **Rename Filter** dialog. The system displays the **Rename Filter** dialog with a list of all user defined filters in the **Filters** combo box.



Rename Filters

Filters: Filter0

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

New Name: Filter0_1

Figure 4.31 - 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

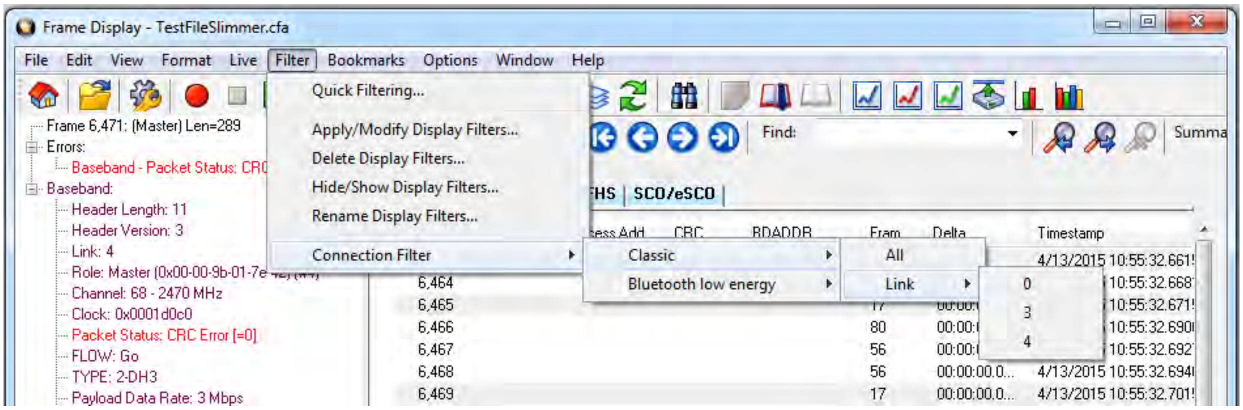
In the Frame Display there are four ways to create a connection filter.

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.


Frame Display - TestFileSlimmer.cfa
File Edit View Format Live Filter Bookmarks Options Window Help
Quick Filtering...
Apply/Modify Display Filters...
Delete Display Filters...
Hide/Show Display Filters...
Rename Display Filters...
Connection Filter
Classic
Bluetooth low energy
All
Link
0
3
4
Find:
Summa
FHS SCO/eSCO
Access Add CRC BDADDR Fram Delta Timestamp

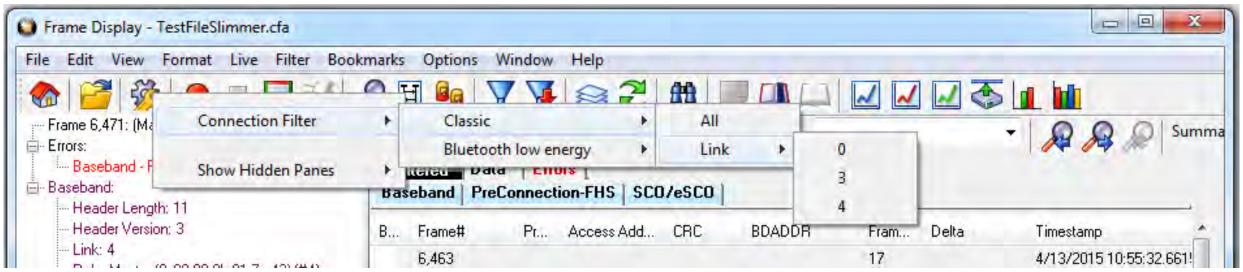
Frame 6,471: (Master) Len=289
Errors:
Baseband - Packet Status: CRC
Baseband:
Header Length: 11
Header Version: 3
Link: 4
Role: Master (0x00-00-9b-01-7e-42) (#4)
Channel: 68 - 2470 MHz
Clock: 0x0001d0c0
Packet Status: CRC Error [=0]
FLOW: Go
TYPE: 2-DH3
Payload Data Rate: 3 Mbps

Frame#	Fram...	Delta	Timestamp
6,464			4/13/2015 10:55:32.668
6,465	17	00:00:0	4/13/2015 10:55:32.671
6,466	80	00:00:0	4/13/2015 10:55:32.690
6,467	56	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

Figure 4.32 - 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
Filtered Data Errors
Baseband PreConnection-FHS SCO/eSCO
B... Frame# Pr... Access Add... CRC BDADDR Fram... Delta Timestamp

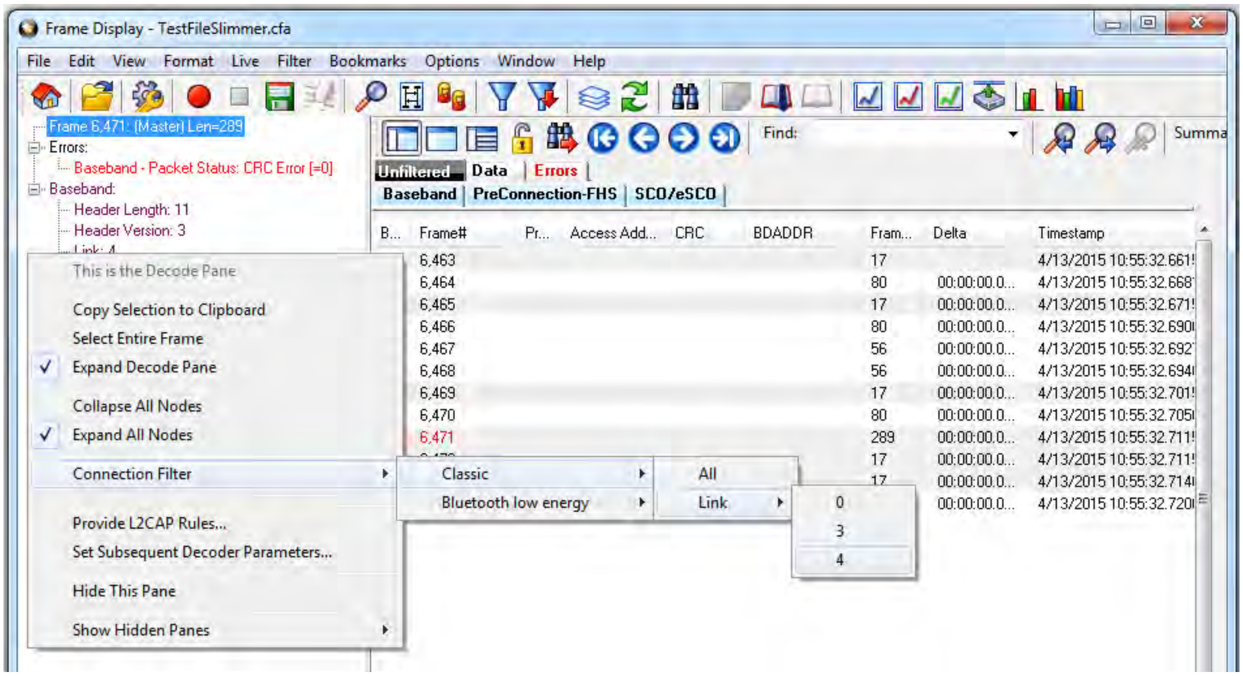
Frame 6,471: (Ma...
Errors:
Baseband - P...
Baseband:
Header Length: 11
Header Version: 3
Link: 4

Frame#	Fram...	Timestamp
6,463	17	4/13/2015 10:55:32.661

Figure 4.33 - Connection Filter from the Frame Display Toolbar right-click

From the Frame Display panes

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



B...	Frame#	Pr...	Access Add...	CRC	BDADDR	Fram...	Delta	Timestamp
	6,463					17		4/13/2015 10:55:32.661!
	6,464					80	00:00:00.0...	4/13/2015 10:55:32.668
	6,465					17	00:00:00.0...	4/13/2015 10:55:32.671!
	6,466					80	00:00:00.0...	4/13/2015 10:55:32.690
	6,467					56	00:00:00.0...	4/13/2015 10:55:32.692
	6,468					56	00:00:00.0...	4/13/2015 10:55:32.694
	6,469					17	00:00:00.0...	4/13/2015 10:55:32.701!
	6,470					80	00:00:00.0...	4/13/2015 10:55:32.705
	6,471					289	00:00:00.0...	4/13/2015 10:55:32.711!
						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 4.34 - 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.

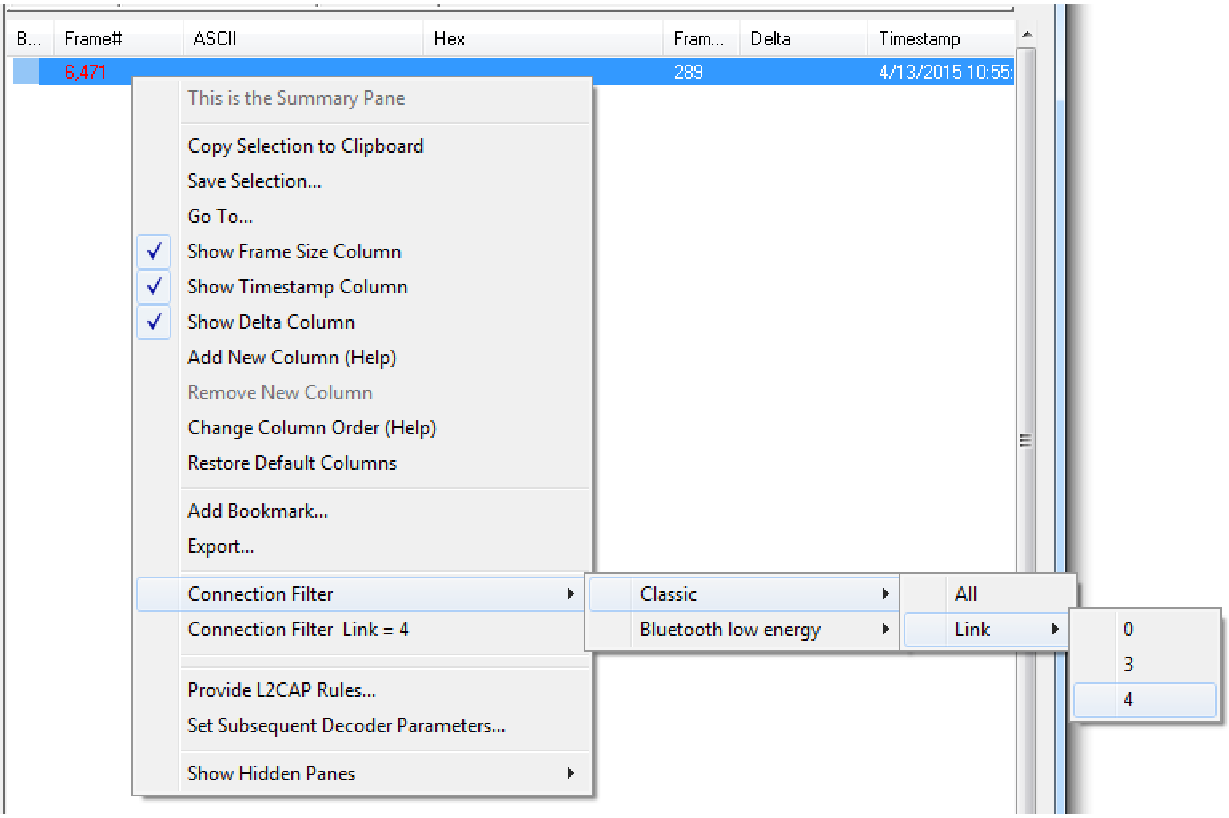


Figure 4.35 - Connection Filter from frame selection right-click

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.

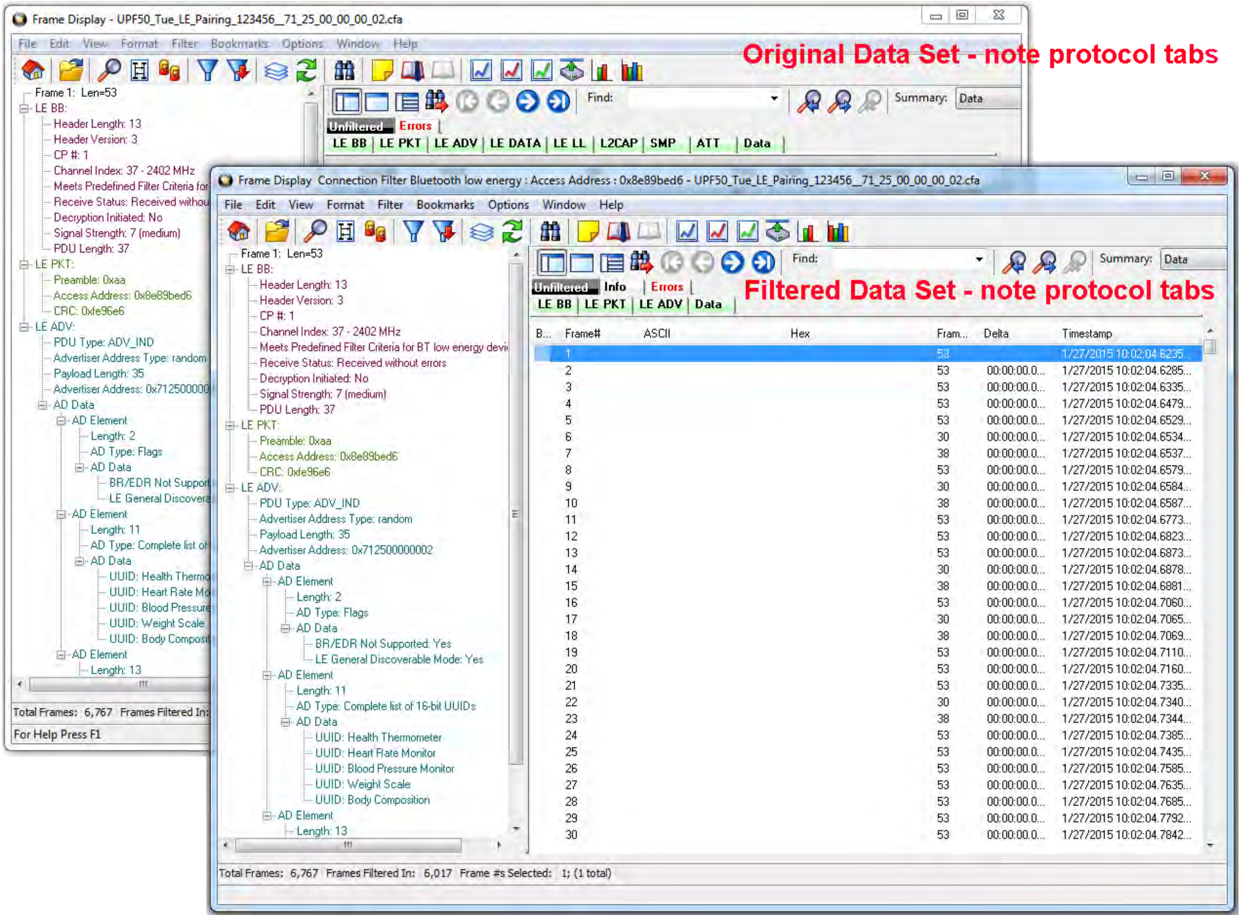
4.3.1.13.2.2 Connection Filter Display

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 98)

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



Original Data Set - note protocol tabs

Frame Display - UPF50_Tue_LE_Pairing_123456__71_25_00_00_00_02.cfa

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

Filtered Data Set - note protocol tabs

Frame Display Connection Filter Bluetooth low energy : Access Address : 0x8e89bed6 - UPF50_Tue_LE_Pairing_123456__71_25_00_00_00_02.cfa

LE BB | LE PKT | LE ADV | Data

```
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)

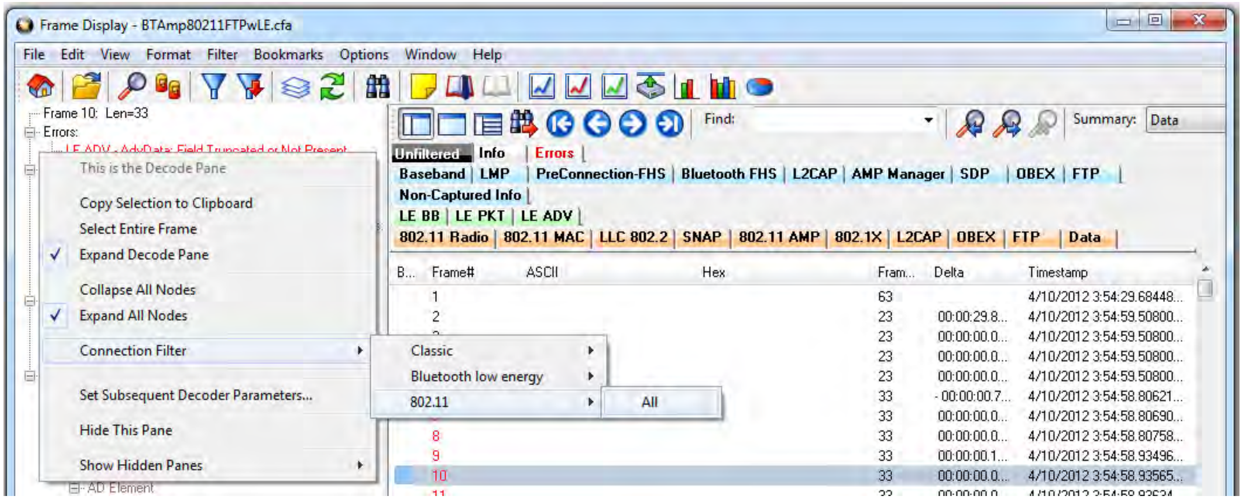
Figure 4.36 - Front Display: Filtered on Access Address 0x8e89bed6

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.

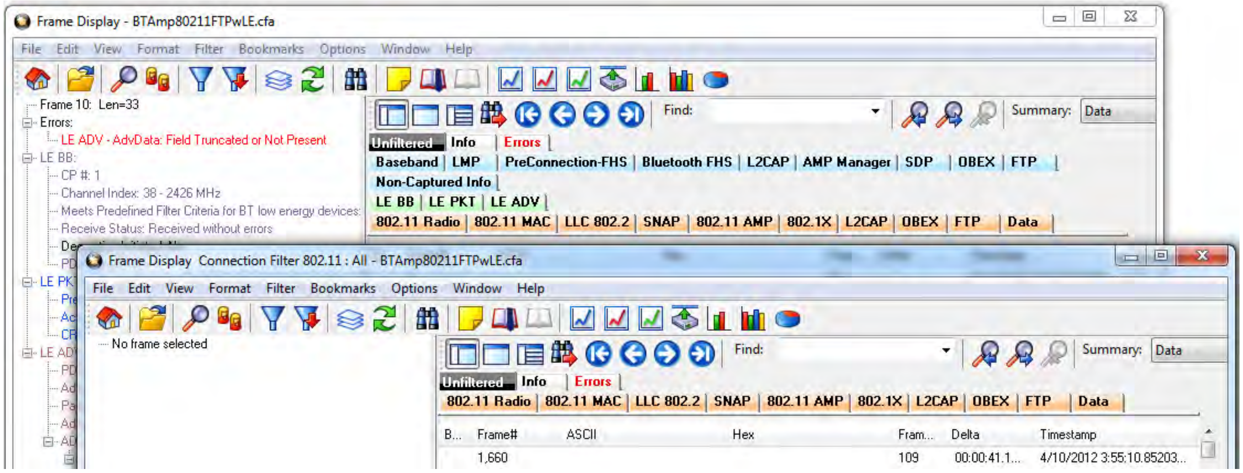

Frame Display - BTAmp80211FTPwLE.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: Data
Unfiltered | Info | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | AMP Manager | SDP | OBEX | FTP
Non-Captured Info
LE BB | LE PKT | LE ADV
802.11 Radio | 802.11 MAC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

Frame 10: Len=33
Errors:
LE ADV - AdvData: Field Truncated or Not Present
AD Element

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 4.37 - 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
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
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

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

No frame selected

B...	Frame#	ASCII	Hex	Fram...	Delta	Timestamp
	1,660			109	00:00:41.1...	4/10/2012 3:55:10.85203...

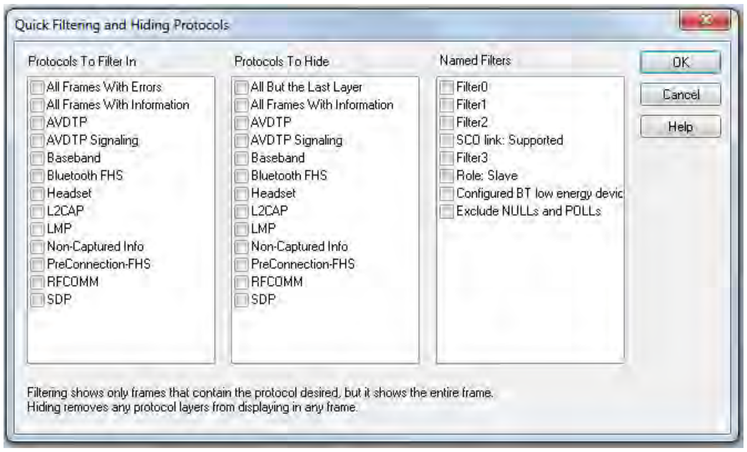
Figure 4.38 - Connection Filter selecting All 802.11 frames, front

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

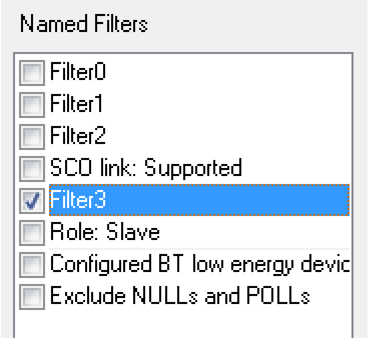
Filtering shows only frames that contain the protocol desired, but it shows the entire frame.
Hiding removes any protocol layers from displaying in any frame.

Figure 4.39 - Frame Display Quick Filtering and Hiding Protocols Dialog

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

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

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



Named Filters

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

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs. When you select the checkbox for the **Name Filters**, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With low energy, the Configured BT Low energy devices and Exclude NULLS and POLLs are default named filters.

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 BPA 600 Baseband Layer Signal Strength

The BPA 600 calculates the ‘Signal Strength’ value, a representation of the radio signal strength relative to the position of the sniffer, for every Bluetooth® packet that it captures. The Signal Strength is not the true RSSI observed at the *Bluetooth* devices in the network being sniffed.

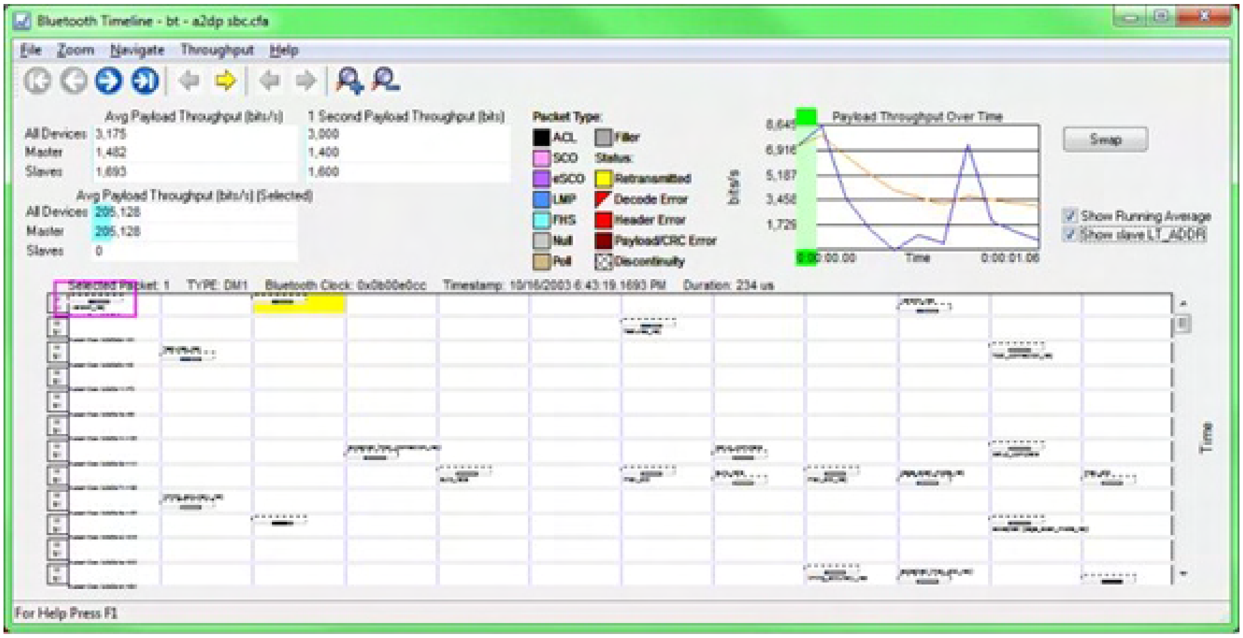
The Signal Strength is a value in the range from 1 through 14 with 1 being weakest and 14 being strongest . The BPA 600 firmware uses the built-in radio firmware features to calculate the Signal Strength value of the signal received at the ComProbe hardware. This calculated value is then mapped to the range of 1 to 14. This is an arbitrary range and does not have any units.

The Signal Strength value is shown as an additional decoded field in the Baseband layer. The field is called “Signal Strength at Sniffer” and will have a value in the range of 1 to 14 decimal. A value of 15 means that the signal strength was not reported. The field is also visible in the **Summary Pane** of the **Frame Display**.

4.3.2 *Bluetooth* Timeline

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

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



	Avg Payload Throughput (bits/s)	1 Second Payload Throughput (bits)
All Devices	3,175	3,000
Master	1,482	1,400
Slaves	1,693	1,600

	Avg Payload Throughput (bits/s) (Selected)
All Devices	205,128
Master	205,128
Slaves	0

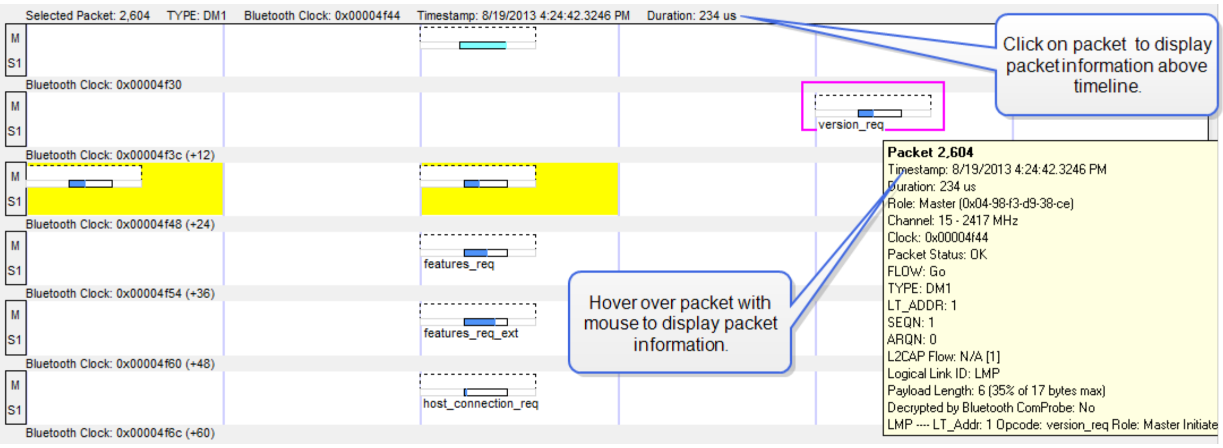
☑ Show Running Average
☑ Show slave LT_ADDR

Selected Packet: 1 TYPE: DM1 Bluetooth Clock: 0x0b00e0cc Timestamp: 10/16/2003 6:43:19.1693 PM Duration: 234 us

Figure 4.40 - Bluetooth Timeline window

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

4.3.2.1 *Bluetooth* Timeline Packet Depiction



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

Bluetooth Clock: 0x00004f30

Bluetooth Clock: 0x00004f3c (+12)

Bluetooth Clock: 0x00004f48 (+24)

Bluetooth Clock: 0x00004f54 (+36)

Bluetooth Clock: 0x00004f60 (+48)

Bluetooth Clock: 0x00004f6c (+60)

Click on packet to display packet information above timeline.

Hover over packet with mouse to display packet information.

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

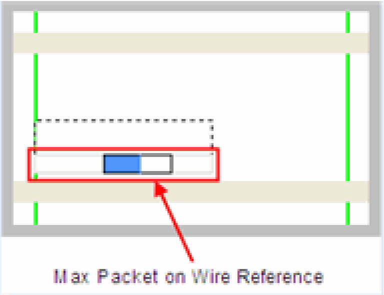
Figure 4.41 - Bluetooth Timeline Packet Depiction with Packet Information Shown

- The timeline shows *Bluetooth* packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.

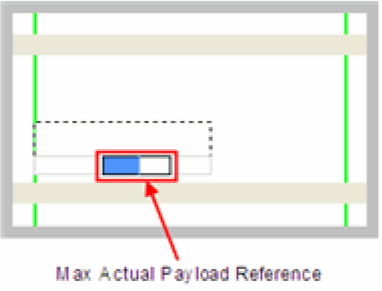
- Within each row are two divisions: **M** (master) and **S** (Slave). Packets are placed on **M** or **S** depending on the data's role.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet. You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

A packet is drawn using the following components:

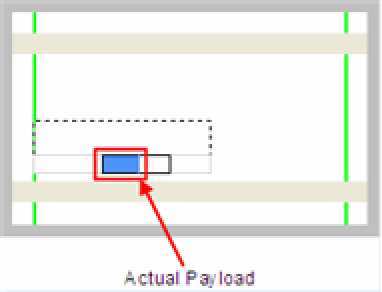
- A “max packet on wire reference” rectangle (light solid lines). This indicates the packet in the air with a max payload.



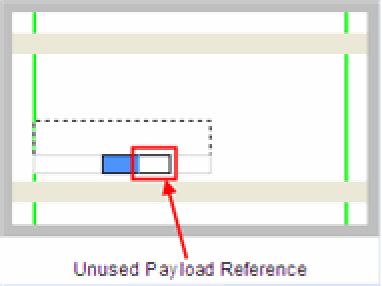
- A “max actual payload reference” rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload in the air contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates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



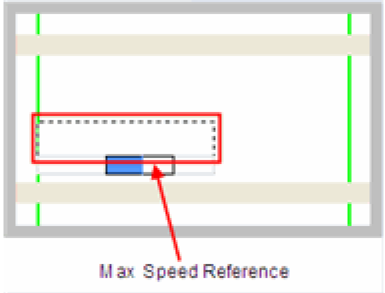
- An “actual payload” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference” rectangle. If the actual payload is of max size, the entire “max actual payload reference”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



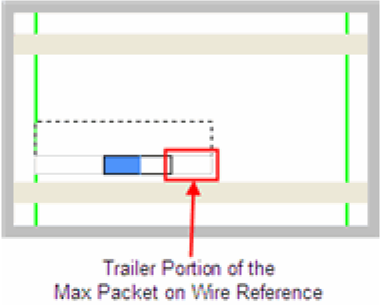
- An “unused payload reference” sub-rectangle (always white). This indicates the unused portion of a maximum payload. It is the remaining portion of the “max actual payload reference” rectangle. The packet in the air does not leave room for this. It is indicated for reference only.



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



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



This table shows how packets are colored:

Table 4.4 - Packet Type Colors

Packet Category	Packet Types	Color
ALC	DM1, DM3, DM5, DH1, 2-DH1, 3-DH1, DH3, 2-DH3, 3-DH3, DH5, 2-DH5, 3-DH5, AUX1	Black
SCO	HV1, HV2, HV3, DV	Pink
eSCO	EV3, 2-EV3, 3-EV3, EV4, EV5, 2-EV5, 3-EV5	Purple
LMP*	DM1, DV	Dark Blue
FHS	FHS	Light Blue
NULL	NULL	Light Gray
POLL	POLL	Light Brown
Filler	Filler provided by ComProbe software	Dark Gray
*LMP is a protocol layer that uses either DM1 or DV packets. If a packet has an LMP layer, the LMP color is used instead of the packet type color.		

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

Table 4.5 - Packet Information Presentation

Information	Text	Color	Graphic size	Position
Packet Type	X			
Packet Category		X		
Protocol	X	X		
Time of occurence	X			X

Table 4.5 - Packet Information Presentation (continued)

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

4.3.2.2 *Bluetooth* Timeline Packet Navigation and Selection

- Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous error packet, next or previous retransmitted packet (Bluetooth only), and the first or last packet.

- If there is no selected packet in the timeline, **First Packet** , **Next Packet** , and **Last Packet** are enabled, but **Previous Packet** is not.

- A single packet is selected either by clicking on it, navigating to it, or selecting it in the **Frame Display**. Selecting a packet activates **Previous Packet**.

- Selecting **Previous Packet** with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).

- Selecting **Next Packet** with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).

- Selecting **Previous Packet** or **Next Packet** for a packet that’s currently visible selects it without scrolling.

- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.

- When a single packet is selected in the timeline, it is also becomes selected in the **Frame Display**. When multiple packets are selected in the timeline, only one of them is selected in the **Frame Display.**

- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

4.3.2.3 *Bluetooth* Timeline Toolbar

The toolbarbar contains the following:

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

Unlock

First Packet

Previous Packet

Next Packet

Last Packet

Previous Retransmitted Packet

Next Retransmitted Packet

Previous Error Packet

Next Error Packet

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

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

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

4.3.2.4 *Bluetooth* Timeline Menu Bar

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

Table 4.6 - Bluetooth Timeline Menus

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

Table 4.6 - Bluetooth Timeline Menus (continued)

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

Table 4.6 - Bluetooth Timeline Menus (continued)

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

4.3.2.5 *Bluetooth* Timeline Visual Elements

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

- The timeline shows *Bluetooth* packets within a specific period of time.

- The timeline shows *Bluetooth* packets within a specific period of time.

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

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

  Selected packets are bounded by a magenta rectangle. See the Bluetooth Timeline Packet Navigation and Selection on page 131 .
- Floating Information Window (aka Tooltip): The information window displays when the mouse cursor hovers on a packet (not slot). It persists as long as the mouse cursor stays on the packet or tooltip. For Bluetooth, the tooltip shows the packet number (in bold), the Baseband layer decode from the decode pane of the Frame Display (with the percentage of the Payload Length max added).

  Discontinuities are indicated by cross-hatched slots. See the Bluetooth Timeline Discontinuities on page 141 section.

- Zoom Tools: **Zoom** tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See Bluetooth Timeline Zooming on page 136 .
- Packet Status: Packet status is indicated by color codes. A yellow slot indicates a re-transmitted packet, a dark red slot indicates a CRC error, and a small red triangle in the upper-left corner of the packet (not the slot) indicates a decode error.
- Right-Click Menu: The right-click menu provides zooming and tool selection. See the Bluetooth Timeline Discontinuities on page 141 .
- Graphical Packet Depiction: Each packet within the visible range is graphically depicted. See the Bluetooth Timeline Packet Depiction on page 127.
- Swap Button: The Swap button switches the position of the Timeline and the Throughput graph.
- Show Running Average: Selecting this check box shows a running average in the Throughput Over Time graph as an orange line.
- Show slave LT_ADDR: Selecting this checkbox displays the Slave LT_ADDR in the timeline row labels

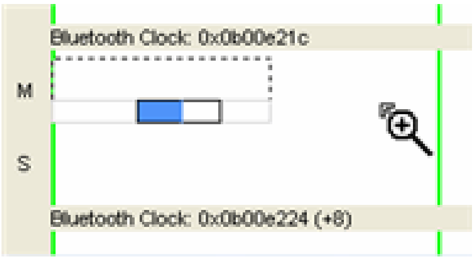
> **Note:** The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

4.3.2.6 *Bluetooth* Timeline Zooming

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

A couple of things to remember about Zooming.

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

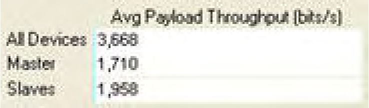


4.3.2.7 *Bluetooth* Timeline Throughput Displays

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

4.3.2.7.1 *Bluetooth* Timeline Average Payload Throughput

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

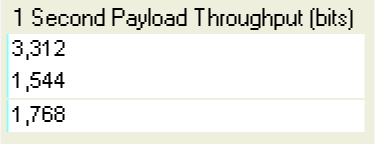


	Avg Payload Throughput (bits/s)
All Devices	3,668
Master	1,710
Slaves	1,958

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

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

4.3.2.7.2 *Bluetooth* Timeline 1 Second Throughput Indicators

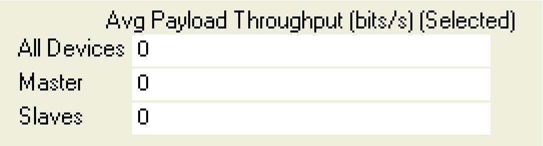


1 Second Payload Throughput (bits)
3,312
1,544
1,768

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

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

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



Avg Payload Throughput (bits/s) (Selected)

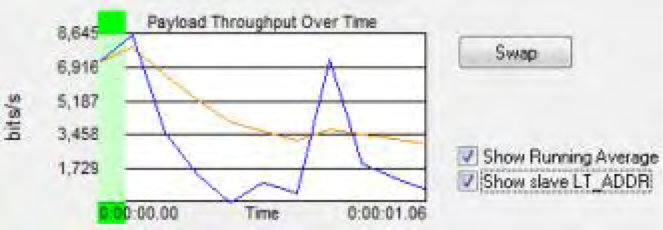
All Devices	0
Master	0
Slaves	0

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

- Duration for average throughput is beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- Average throughput can be nonzero when a single packet is selected.
- Average throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates relative percentage. Text displays the throughput value

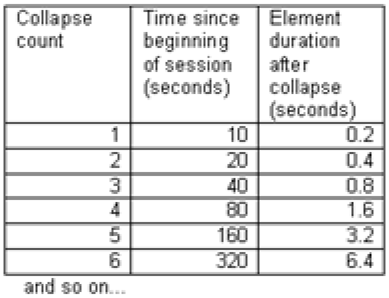
4.3.2.7.4 *Bluetooth* Payload Throughput Over Time Graph

The following figure depicts the Payload Throughput Over Time graph.



☑ Show Running Average
☑ Show slave LT_ADDR

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



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

and so on...

- The bottom of the graph shows a beginning time and an ending time. The beginning time is relative to the start of the session and initially 0. When packets start wrapping out it becomes the relative time offset of the first available packet. The ending time is always the total time of the session.
- Discontinuities are indicated by vertical dashed lines.
- A green view port indicates the time range corresponding to the visible slots in the timeline. The view port can be moved by clicking elsewhere in the graph or by dragging. Whenever it is moved, the timeline scrolls to match. When the slot range in the timeline changes, the view port moves and resizes as necessary to match.

- The **Swap** button - switches the position of the Timeline and the **Throughput** graph.
- **Show Running Average** - Selecting this check box shows a running average in the **Throughput Over Time** graph as an orange line.
- **Show slave LT_ADDR** - Selecting this checkbox displays the **Slave LT_ADDR** in the timeline row labels.

Comparison with the Coexistence View Throughput Graph

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

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

4.3.2.8 Export Payload Throughput Over Time

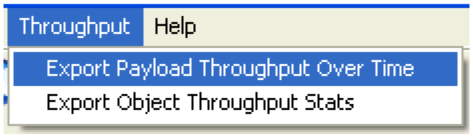
In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about the **Payload Throughput Over Time** graph. The file contains the following information:

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

To create the file:

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

   The **Save As** menu appears.


Throughput
Help
Export Payload Throughput Over Time
Export Object Throughput Stats

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

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

3. Enter a **File Name.**

4. Select **Save.**

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

4.3.2.9 Object Throughput Stats File

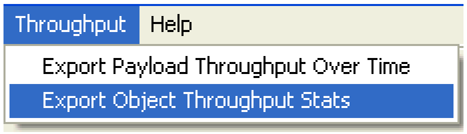
In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about objects in the timeline. The file contains the following information:

- Name
- Length (bytes)
- Connection Packet Number
- Begin Transfer Packet Number
- End Transfer Packet Number
- Disconnection Packet Number
- Connection Duration
- (Fractional Seconds)
- Transfer Duration
- (Fractional Seconds)
- Connection Throughput (bits/s)
- Transfer Throughput (bits/s)
- Transfer Duration Percentage of Connection Duration
- No Errors Packet Count (Includes Decode Errors) (While Connected)
- Retransmitted Packet Count (While Connected)
- Header Errors Packet Count (While Connected)
- Payload/CRC Errors Packet Count (While Connected)

To create the file:

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

   The **Save As** menu appears.


Throughput
Help
Export Payload Throughput Over Time
Export Object Throughput Stats

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

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

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

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

4.3.2.10 *Bluetooth* Timeline Discontinuities

The following figure depicts a discontinuity between two packets.

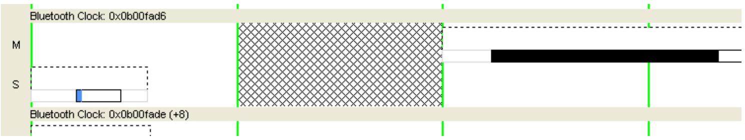
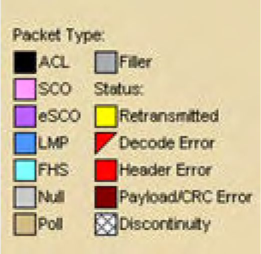


Figure 4.42 - *Bluetooth* Timeline Packet Discontinuity, cross-hatched area.

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

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

4.3.2.11 Legend



This legend identifies the color coding found in the timeline.

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

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

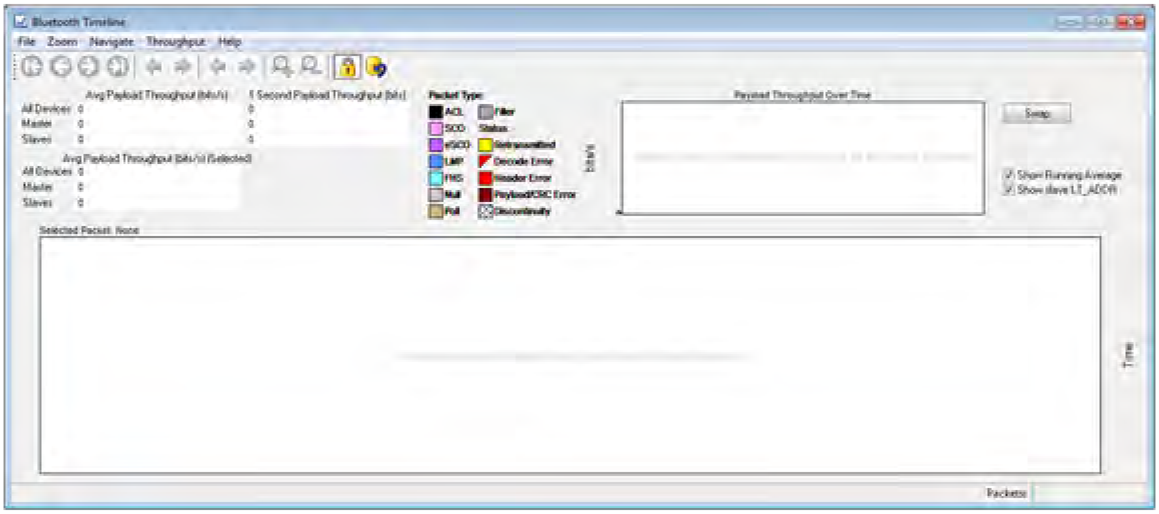
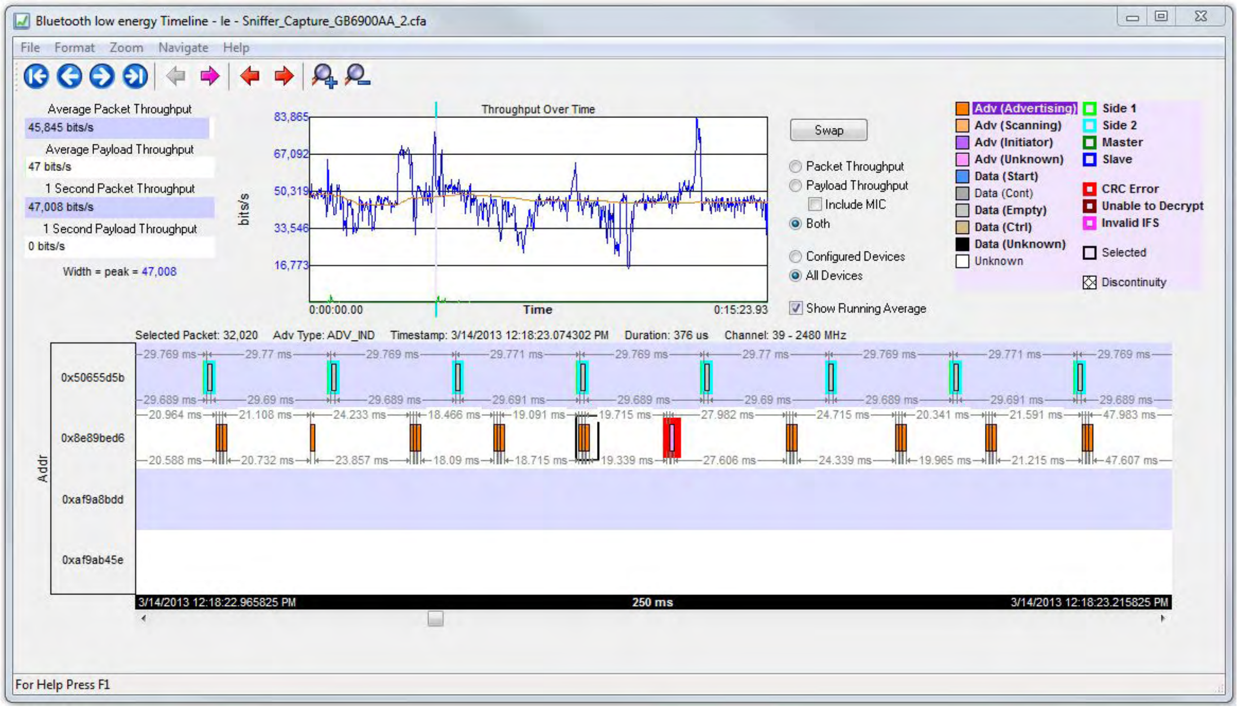


Figure 4.43 - Missing packets message in timeline pane.

4.3.3 low energy Timeline

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

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


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

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

Figure 4.44 - *Bluetooth* **low energy Timeline**

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

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

4.3.3.1 low energy Timeline Toolbar

The toolbar contains the following:

Table 4.7 - *Bluetooth* low energy Timeline Toolbar

Icon	Description
🔒	Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.
🔓	Unlock
⏮	First Packet
⬅	Previous Packet
➡	Next Packet
⏭	Last Packet
⇦	Previous Interframe Spacing (IFS) Error • Interframe Spacing is considered valid if it is within 150 µs + or – 2us • If the Interframe Spacing is less than 148 us or greater than 152 us but less than or equal to 300 µs, it is considered an IFS error.
⇨	Next Interframe Spacing (IFS) Error • Interframe Spacing is considered valid if it is within 150 µs + or – 2us • If the Interframe Spacing is less than 148 us or greater than 152 µs but less than or equal to 300 us, it is considered an IFS error.
⬅	Previous Error Packet
➡	Next Error Packet
🔍	Zoom In
🔍	Zoom Out

Table 4.7 - Bluetooth low energy Timeline Toolbar (continued)

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

4.3.3.2 low energy Timeline Menu Bar

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

Table 4.8 - Bluetooth low energy Timeline Menus

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

Table 4.8 - Bluetooth low energy Timeline Menus (continued)

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

Table 4.8 - Bluetooth low energy Timeline Menus (continued)

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

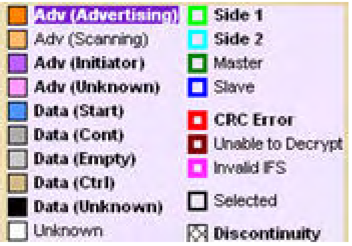
Table 4.8 - Bluetooth low energy Timeline Menus (continued)

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

4.3.3.3 low energy Timeline Legend

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)**
🟧 Adv (Scanning)
🟪 **Adv (Initiator)**
🟪 **Adv (Unknown)**
🟦 **Data (Start)**
⬜ **Data (Cont)**
⬜ **Data (Empty)**
🟫 **Data (Ctrl)**
⬛ **Data (Unknown)**
⬜ Unknown

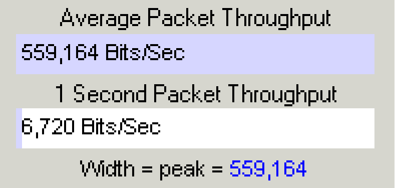
🟩 **Side 1**
□ **Side 2**
🟩 Master
🟦 Slave
🟥 **CRC Error**
🟥 Unable to Decrypt
🟪 Invalid IFS
□ Selected
☒ **Discontinuity**

4.3.3.4 Throughput Displays

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

4.3.3.5 Average and 1 Second Packet Throughput

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



Average Packet Throughput
559,164 Bits/Sec
1 Second Packet Throughput
6,720 Bits/Sec
Width = peak = 559,164

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

4.3.3.6 Average and 1 Second Payload Throughput

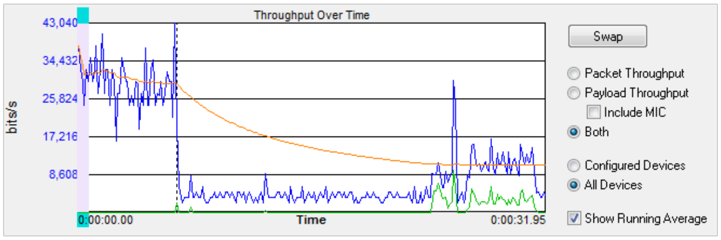
The figure depicts the **Average** and **One Second Payload** Throughput display. This display appears when you select the **Payload Throughput** radio button.

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

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

4.3.3.7 Throughput Graph

The following figure depicts the Throughput Graph.



Swap

○ Packet Throughput

○ Payload Throughput

☐ Include MIC

● Both

○ Configured Devices

● All Devices

☑ Show Running Average

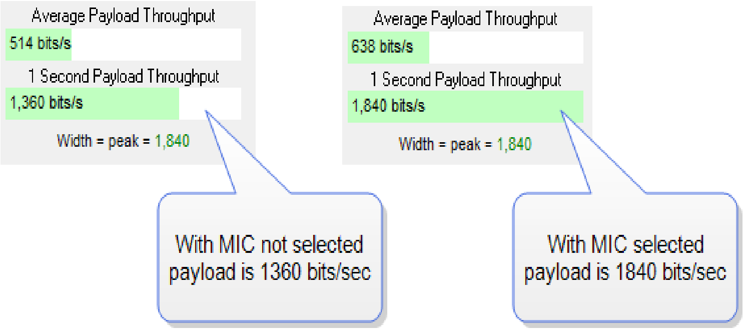
Figure 4.45 - *Bluetooth* low energy Timeline Throughput Graph

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

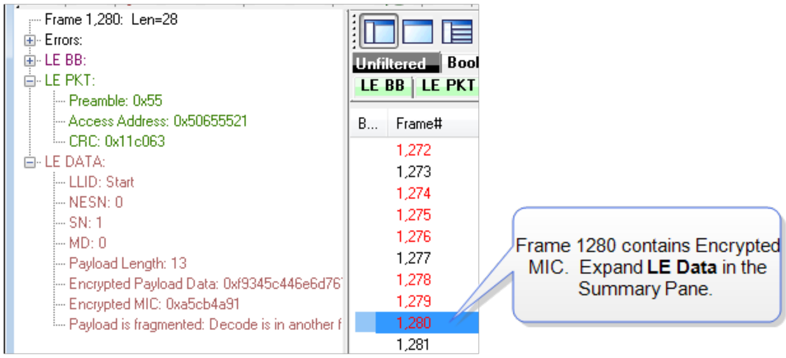
Average Payload Throughput
638 bits/s
1 Second Payload Throughput
1,840 bits/s
Width = peak = 1,840

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.

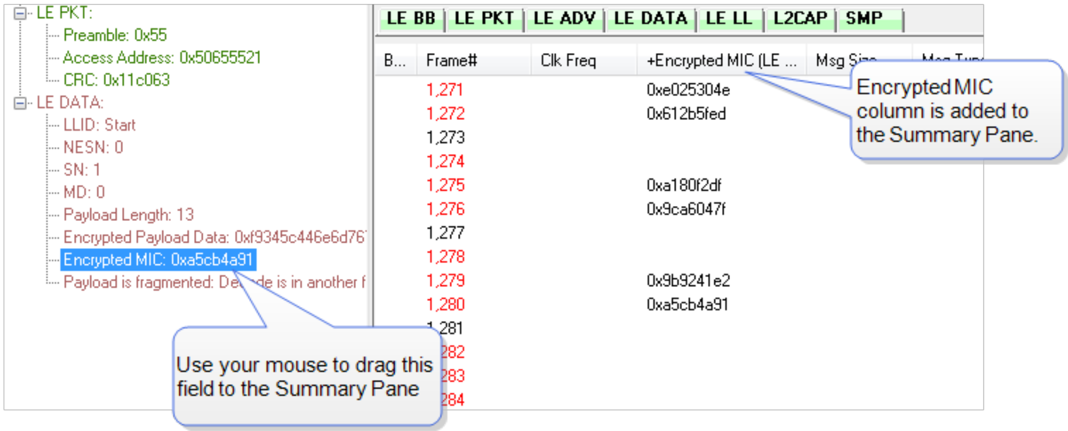


```
Frame 1,280:  Len=28
Errors:
LE BB:
LE PKT:
    Preamble: 0x55
    Access Address: 0x50655521
    CRC: 0x11c063
LE DATA:
    LLID: Start
    NESN: 0
    SN: 1
    MD: 0
    Payload Length: 13
    Encrypted Payload Data: 0xf9345c446e6d76
    Encrypted MIC: 0xa5cb4a91
    Payload is fragmented: Decode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

B...	Frame#	Clk Freq	+Encrypted MIC (LE ...	Msg Si	Msg Ty
	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				
	282				
	283				
	284				

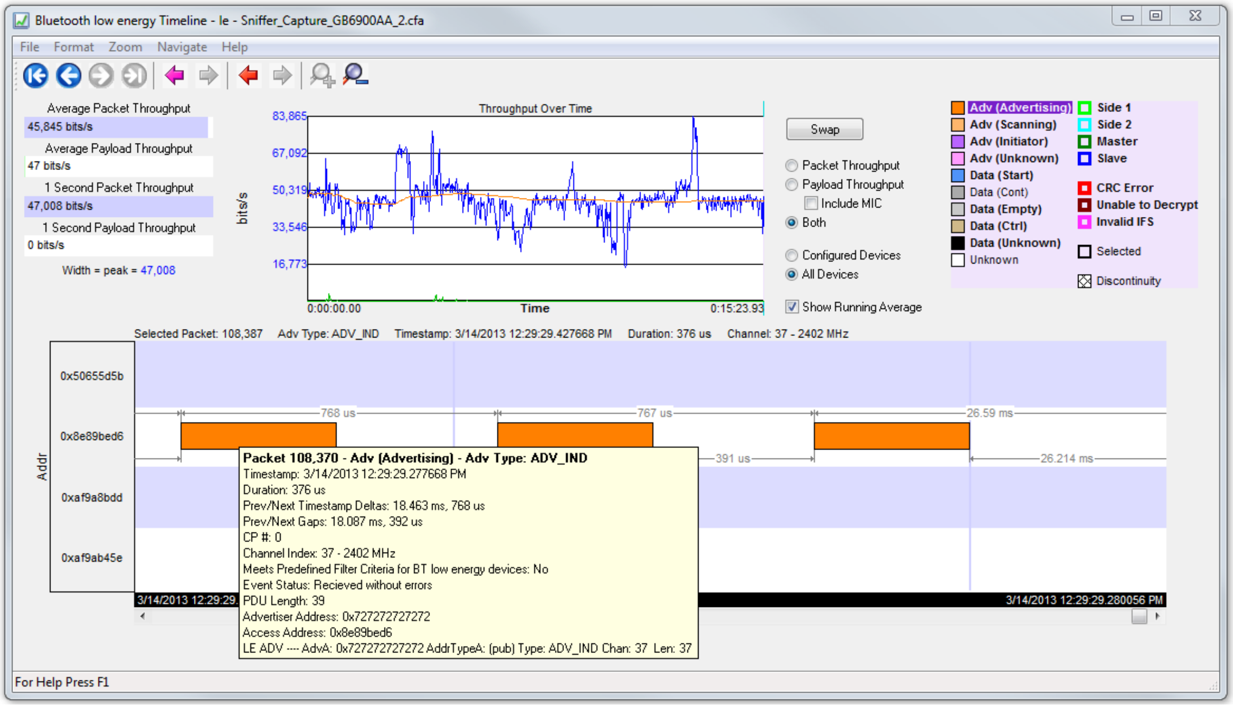
Encrypted MIC column is added to the Summary Pane.

Use your mouse to drag this field to the Summary Pane

Figure 4.46 - Creating Encrypted MIC in Frame Display Summary pane

4.3.3.8 The Timeline

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



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

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 4.47 - *Bluetooth***low energy Timeline**

4.3.3.9 How Packets Are Displayed

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

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

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

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

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

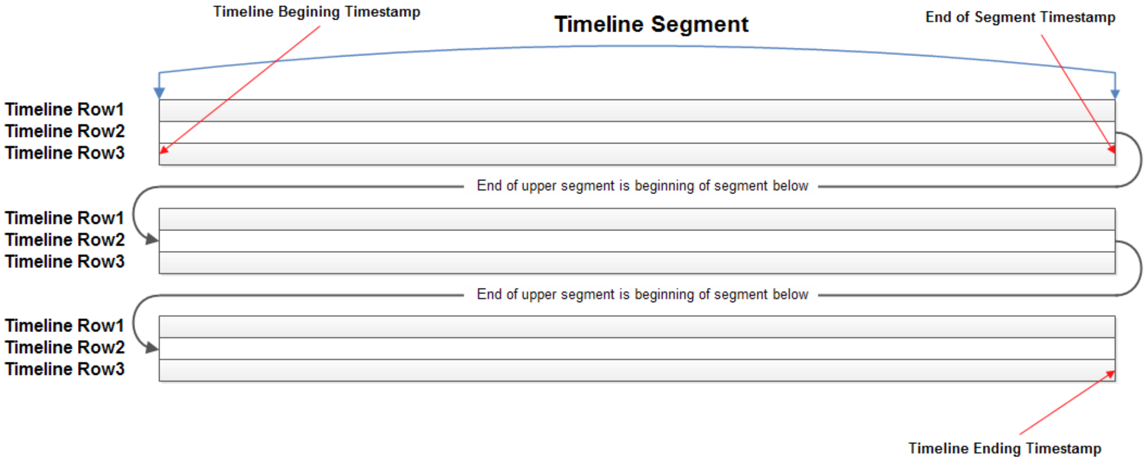
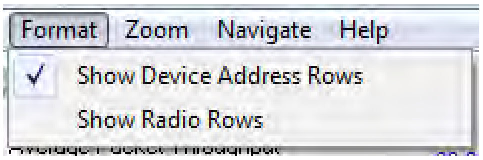


Figure 4.48 - Diagram of low energy Timeline Flow with Segment and Row Relationship

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

4.3.3.10 Format Menu



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

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

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

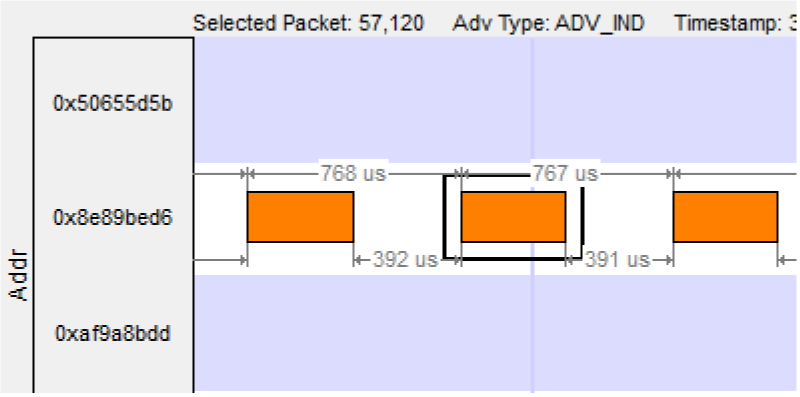


Figure 4.49 - Device Address Rows

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

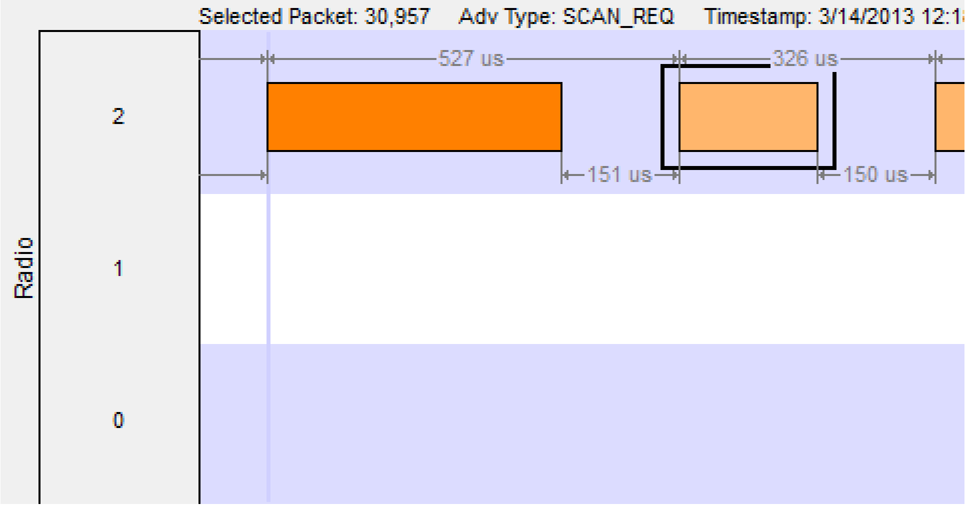
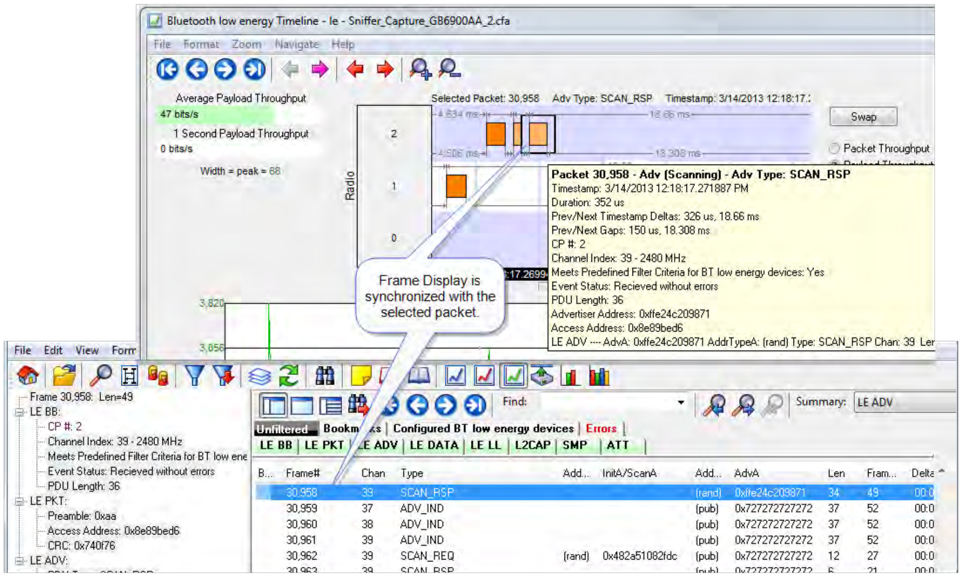


Figure 4.50 - Radio Rows

- 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

Average Payload Throughput: 47 bits/s

1 Second Payload Throughput: 0 bits/s

Width = peak = 68

Selected Packet: 30,958   Adv Type: SCAN_RSP   Timestamp: 3/14/2013 12:18:17.2

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 Display is synchronized with the selected packet.

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:

Find: Summary: LE ADV

Unfiltered | Bookmarks | Configured BT low energy devices | Errors |
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT |

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

Figure 4.51 - **low energy Timeline** and **Frame Display** Packet Synchronization

4.3.3.11 low energy Timeline Visual Elements

The low energy Timeline consists of the following visual elements:

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

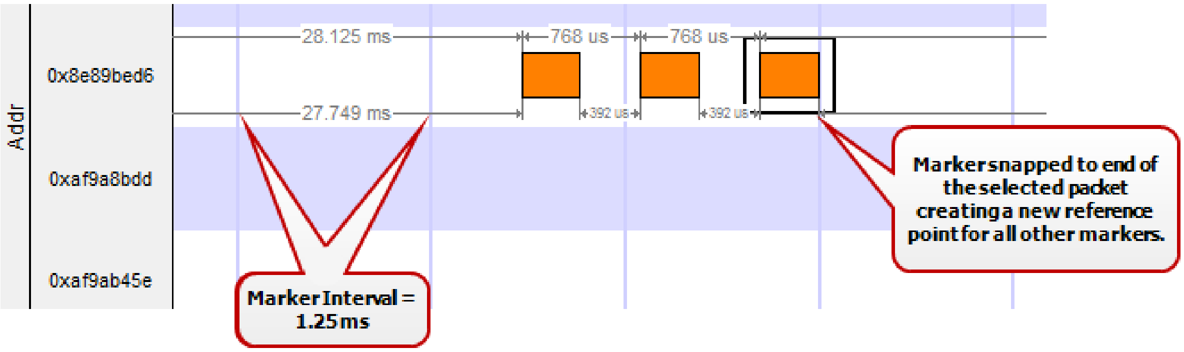


Figure 4.52 - Timeline Markers Shown Snapped to End of Packet

- 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.

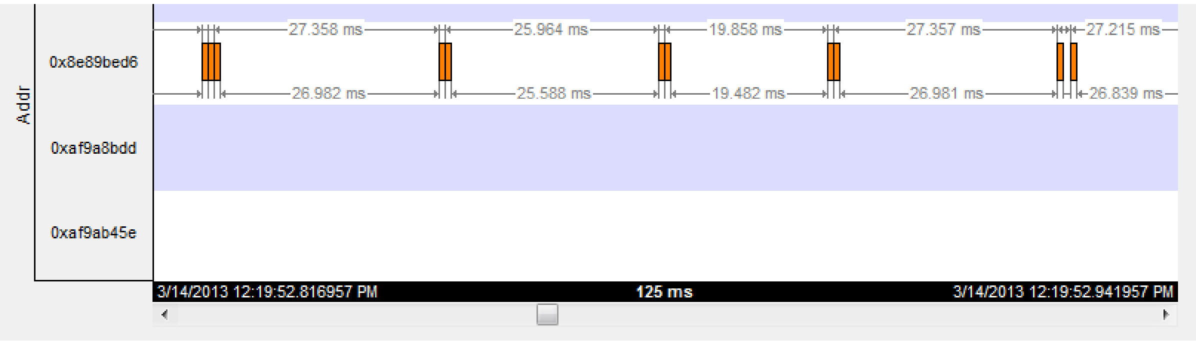
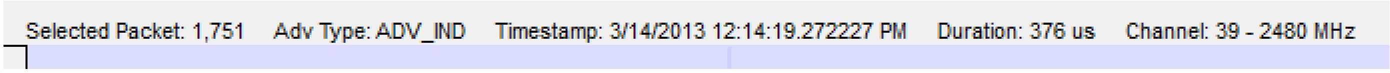


Figure 4.53 - Bluetooth le Timeline Segment Timestamp and Zoom Value

> **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 4.54 - 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

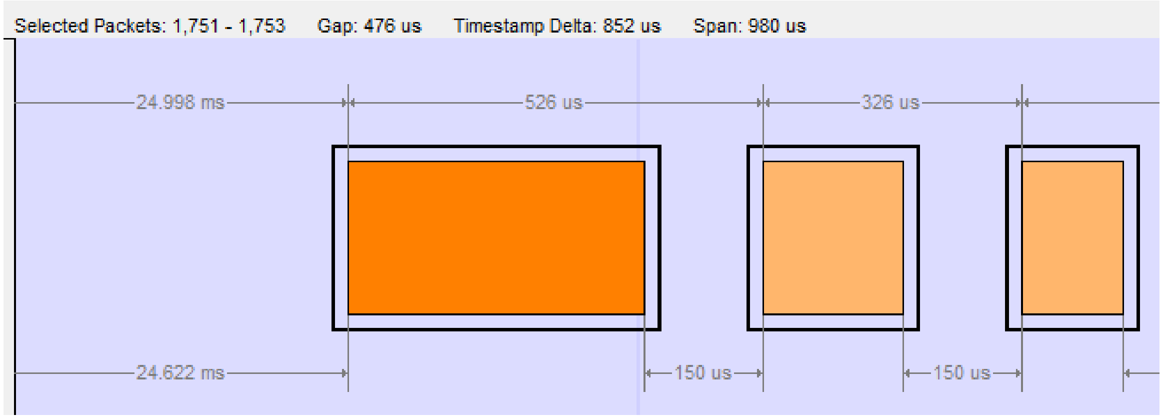
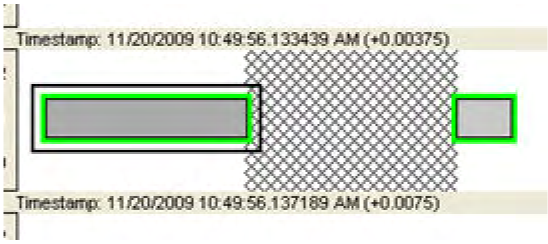

Selected Packets: 1,751 - 1,753 Gap: 476 us Timestamp Delta: 852 us Span: 980 us

Figure 4.55 - Bluetooth le Timeline Packet Info Line for Multiple Selected Packets

- Floating Information Window (aka Tooltip) - The information window displays when the mouse cursor hovers on a packet. It persists as long as the mouse cursor stays on the packet.
- Discontinuities - Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.
- Packet Status - Packet status is indicated by color codes. Refer to low energy Timeline Legends.
- Right-Click Menu. - The right-click menu provides zooming and time marker alignment.
- Graphical Packet Depiction - each packet within the visible range is graphically depicted. See the Packet Depiction section.
- Swap Button - The Swap button Swap switches the position of the Timeline and the Throughput graph.
- Show Running Average - -Selecting this check box shows a running average in the Throughput Over Time graph as an orange line ☑ Show Running Average .

4.3.3.12 low energy Packet Discontinuities

The following figure depicts a discontinuity between two packets.


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

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

Figure 4.56 - Bluetooth® low energy Packet Discontinuity

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

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

4.3.3.13 low energy Timeline Navigating and Selecting Data

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

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

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

          If the previous packet is not shown in the timeline display or a portion of the packet is displayed,the display will move the view port back in time and will display the selected packet in the top segment on the left edge. Each segment's timestamps will synchronously change as the view port scrolls backwards in time.
        - Selecting Next Packet will select the next packet moving forward in time (to the right)on the to the next packet regardless of which row or segment it is in.

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

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

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

4.3.3.14 low energy Timeline Zooming

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

A couple of things to remember about Zooming.

- Zooming using the toolbar buttons in a single segment display is relative to the center of the display. That is as you zoom out those packets on the left and right halves will move closer to the center. If you zoom in, those packets in the left and right halves will move towards the left and right edges respectively.
- Zooming using the toolbar buttons in a multiple segment display is relative to the number of segments. If you have a single display and zoom out they will become two segments, then three segments, then six, and so forth.
- Selecting a Zoom icon (+ or -) on the toolbar zooms in our out.
- The current Zoom setting is shown in the center of the timeline segment information bar at the bottom of each timeline segment.
- If you are in multiple segments the segment information bar will show the zoom level with the text "(Contiguous time segment *x/n*)" where "*x*" is 1,2, 3... segment and "*n*" is the total number of segments. For example: :"(Contiguous time segment 2/3)".

4.3.3.15 Zoom menu

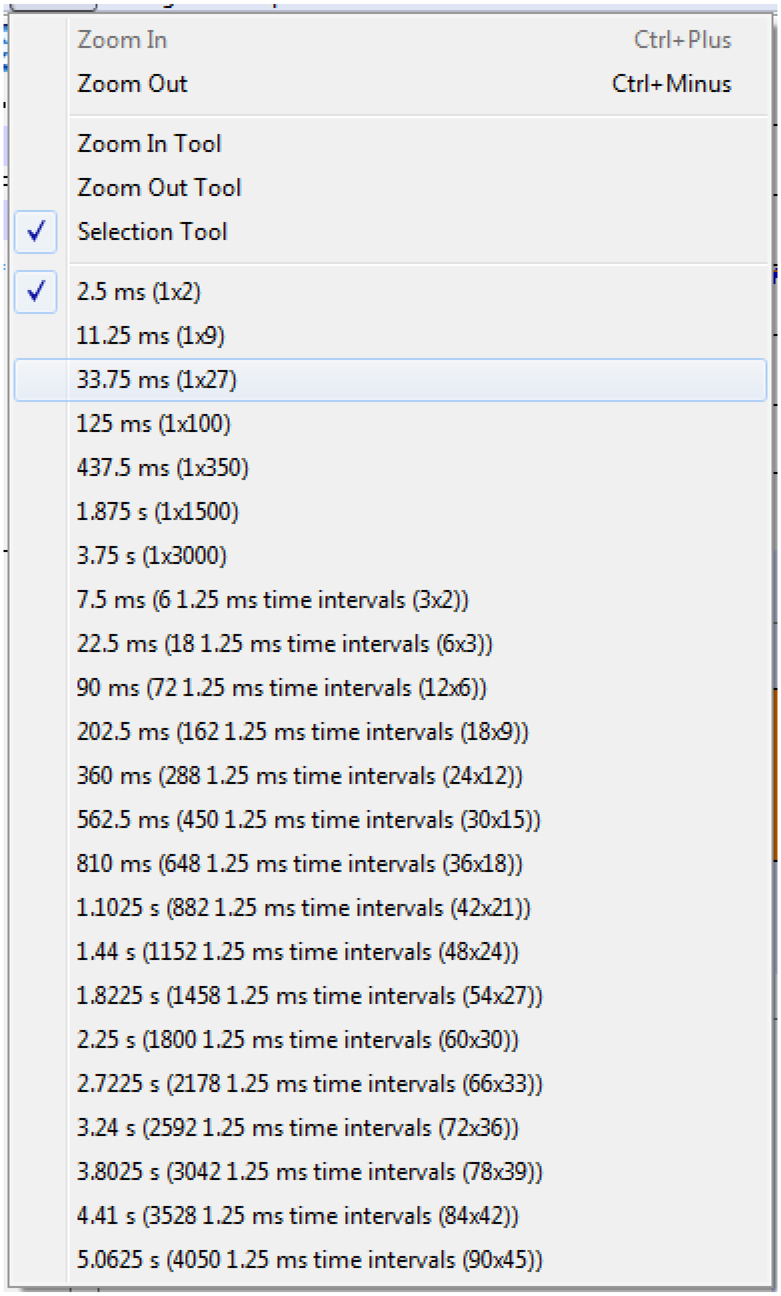
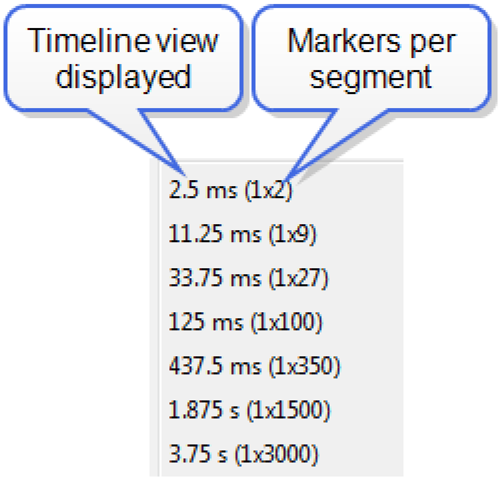

Zoom In Ctrl+Plus
Zoom Out Ctrl+Minus
Zoom In Tool
Zoom Out Tool
✓ Selection Tool
✓ 2.5 ms (1x2)
11.25 ms (1x9)
33.75 ms (1x27)
125 ms (1x100)
437.5 ms (1x350)
1.875 s (1x1500)
3.75 s (1x3000)
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals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

Figure 4.57 - low energy Timeline Zoom menu

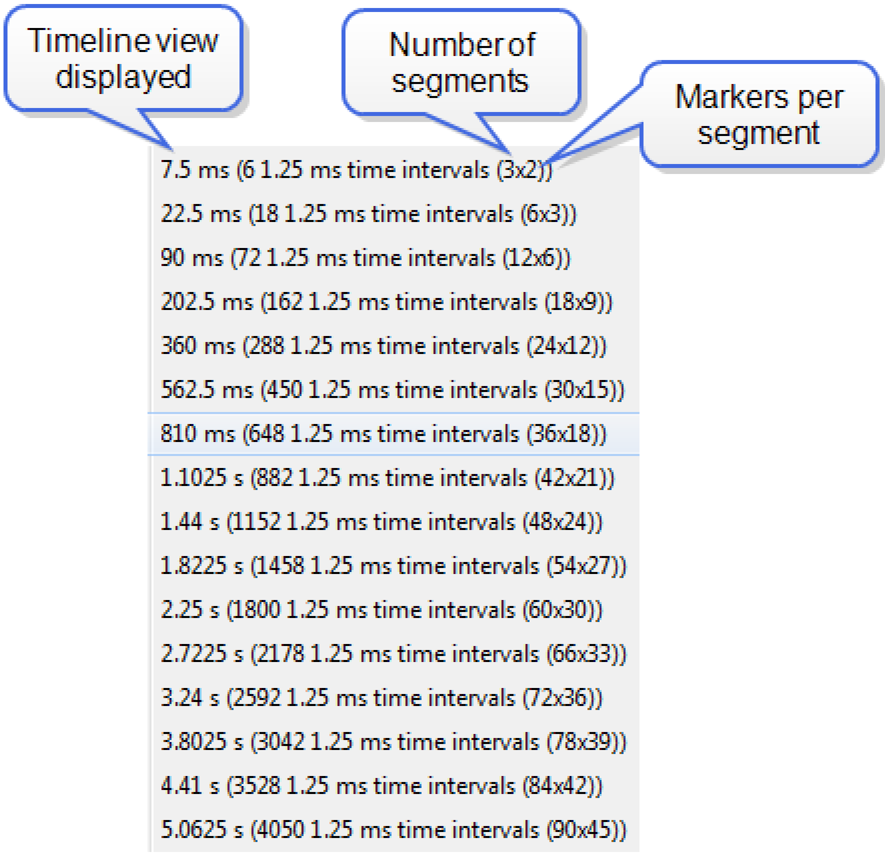
4.3.3.16 Single Segment Zoom



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

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

4.3.3.17 Multiple Segments


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

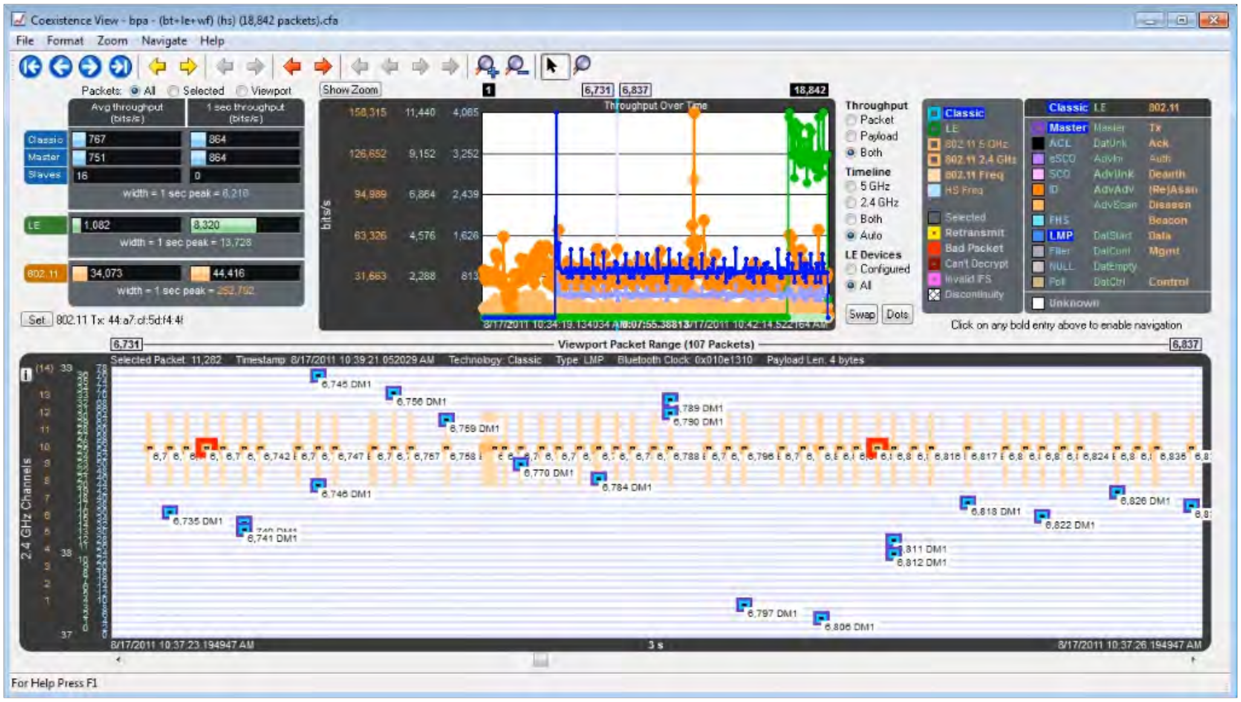
Zoom Menu Multiple Segment: Each selection defines the timeline view port, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "7.5 ms (6 1.25 ms time intervals (3x2))" will display "7.5 ms" of the total timeline in "3" segments of with "2" markers per segment for a total of "6" markers.

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

4.3.4 Coexistence View

(Click here to see an introduction video...)

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



Coexistence View - bpa - (bt+le+wf) (hs) (18,842 packets).cfa

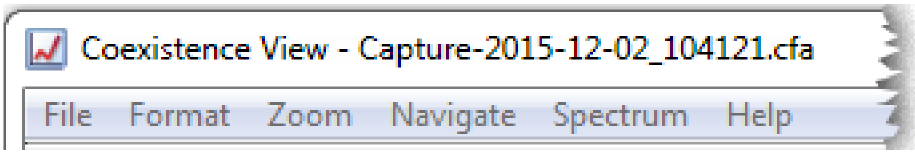
Selected Packet 11,282 Timestamp 8/17/2011 10:39:21.052029 AM Technology: Classic Type: LMP Bluetooth Clock: 0x010e1310 Payload Len: 4 bytes

Set 802.11 Tx: 44:a7:cf:5d:f4:4f

For Help Press F1

Figure 4.58 - Coexistence View Window

4.3.4.1 Coexistence View Menus



The following tables describe each of the Coexistence View Menus.

Table 4.9 - Coexistence View File Menu Selections

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

Table 4.10 - Coexistence View Format Menu Selections

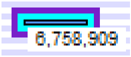
Selection	Description
Show Packet Number	When checked, the packet number shows below the packet in the Viewport. 
Show Packet Type	When checked, the packet type shows below the packet in the Viewport.
Show Packet Subtype	When checked, the packet subtype shows below the packet in the Viewport, if applicable.
Hide Packet Text	When checked, hides any text shown below the packet in the Viewport. Applies the text shown by the Show Packet Number, **Show Packet Type**, and **Show Packet Subtype** menu selections.
Auto Hide Packet Text When Duration > 31.25 ms.	When checked, automatically hides any text shown below the packet in the Viewport when the Viewport duration exceeds 31.25 ms. Applies the text shown by the Show Packet Number, **Show Packet Type**, and **Show Packet Subtype** menu selections. The Viewport duration is shown at the bottom of the Viewport. This selection reduces display clutter when viewing a larger timeline section.
Increase Auto Hide Packet Count from 4,000 to 20,000 (May Be Slow)	When not checked, the default, the packets in the viewport are hidden if the number of visible packets exceeds 4,000. When checked, the default count increased from 4,000 to 20,000 packets before the packets are hidden. Choosing this selection may slow down the displaying of the packets.
The following three selections are mutually exclusive.	
Use All Packets for Throughput Indicators	When checked, all captured packets are used for average throughput calculations and all packets in the last one second of the capture session are used for the 1 sec throughput. See on page 171 for more information. Performs the same function as the throughput indicator **All** radio button.
Use Selected Packets for Throughput Indicators	When checked, the packets selected in the Viewport are used for average throughput calculations, and selected packets in the one second before the last selected packet are used for the 1 sec throughput. See on page 171 for more information. Performs the same function as the throughput indicator **Selected** radio button.
Use Viewport Packets for Throughput Indicators	When checked, all packets appearing in the Viewport are used for average throughput calculations, and all packets in the one second before the last packet in the Viewport are used for the 1 sec throughput. See on page 171 for more information. Performs the same function as the throughput indicator **Viewport** radio button.

Table 4.10 - Coexistence View Format Menu Selections (continued)

Selection	Description
Set 802.11 Tx Address	When checked, this selection is used to specify the 802.11 source address, where any packet with that source address is considered a Tx packet and is shown with a purple border in the timelines. Performs the same function as the SET button. Refer to on page 180
The following three selections are mutually exclusive.	
Show Packet Throughput	When checked, the Throughput Graph and Throughput Indicator shows data based on packet throughput. Performs the same function as the **Throughput Packet** radio button.
Show Payload Throughput	When checked, the Throughput Graph and Throughput Indicator shows data based on payload throughput. Performs the same function as the **Throughput Payload** radio button.
Show Both Packet And Payload Throughput	When checked, the Throughput Graph will graph both the data based on packets throughput in darker colors and payloay throughput in lighter colors. The Throughput Indicator will show calculations based on packet throughput. Performs the same function as the **Throughput Both** radio button.
The following four selections are mutually exclusive.	
Show 5 GHz Timeline	When checked, the 5 GHz Timeline is visible and the 2.4 GHz Timeline is not visible. Only 802.11 5 GHz packets are shown. Performs the same function as the **Timeline 5 GHz** radio button.
Show 2.4 GHz Timeline	When checked, the 2.4 GHz Timeline is visible and the 5 GHz Timeline is not visible. The timeline will show Classic Bluetooth, Bluetooth Low Energy, and 802.11 2.4 GHz packets. Performs the same function as the **Timeline 2.4 GHz** radio button.
Show Both 2.4 GHz and 5 GHZ Timelines	When checked, the 2.4 GHz Timeline and the 5GHZ Timeline is visible. Performs the same function as the **Timeline Both** radio button.
Show Timelines Which Have or Had Packets (Auto Mode)	When check,shows only timelines which have had packets at some point during this session. If no packets are present, the 2.4 GHz Timeline is visible. Performs the same function as the **Timeline Auto** radio button.
The following two selections are mutually exclusive.	
Show Low Energy Packets From Configurated Devices Only	When checked, shows in the 2.4 GHz Timeline only packets from *Bluetooth* low enegry devices configured for this session, and uses these packets for throughput calculations. Performs the same function as the **LE Devices Configured** radio button.
Show All Low Energy Packets	When checked, shows in the 2.4 GHz Timeline all Bluetooth low energy packets captured in this session, and uses these packets for throughput calculations. Performs the same function as the **LE Devices All** radio button.

Table 4.10 - Coexistence View Format Menu Selections (continued)

Selection	Description
Large Throughput Graph	When checked, the Throughput Graph appears in the bottom half of the window, swapping position with the timeline. When not checked, the Throughput Graph appears in its default position at the top of the window. Performs the same function as clicking the **Swap** button. See on page 175.
Show Dots in Throughput Graph (Dots Reveal Overlapped Data Points)	When checked, displays dots on the Throughput Graph. Dots are different sizes for each technology so that they reveal overlapping data points which otherwise wouldn't be visible. A tooltip can be displayed for each dot. Performs the same function as the **Dots** button. See on page 176.
Show Zoomed Throughput Graph	When checked, dispalys a Zoomed Throughput Graph above the Throughput Graph. The Zoomed Throughput Graph shows the details of the throughput in the time range covered by the viewport in the Throughput Graph. Performs the same function as the **Show Zoom** button. When not checked, the Zoomed Throughput Graph is hidden. Performs the same function as the **Hide Zoom** button. See on page 177 .
Freeze Y Scales in Zoom Throughput Graph	Only active when the Zoomed Throughput Graph is visible. When checked, it freezes the y-axis scales and makes it possible to compare all time ranges and durations. Performs the same fuction as the **Freeze Y** button, which appears with the Zoomed Throughput Graph. When not checked, the y-axis scales are unfroozen. Performs the same function as the **Unfreeze Y** button, which appears with the Zoomed Throughput Graph. See on page 177
Show Tooltips in Upper-Left Corner of Screen	When checked, Timeline and Throughput Graph tooltips will appear in the upper-left corner of your computer sceen. You can relocate the tool tip for convenience or to see the timeline or throughput graph unobstructed while displaying packet information. See on page 185.

Table 4.11 - Coexistence View Zoom Menu Selections

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

Table 4.11 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
Zoom Out	When clicked, Viewport time duration increases	Ctrl+Minus
The following two selectioins are mutually exclusive.		
Scroll Tool (Mouse Wheel Scrolls - Ctrl Key Switches to Zoom Tool)	When checked, sets the mouse wheel to scroll the Viewport. Pressing the Ctrl key while scrolling switches to zooming the Viewport.	
Zoom Tool (Mouse Wheel Zooms- Ctrl Key Switches to Scroll Tool)	When checked, sets the mouse wheel to zoom the Viewport. Pressing the Ctrl key while zooming switches to scrolling the Viewport.	
Zoom To Time Range of Selected Packets	Active only when packets are selected. When clicked, the Viewport duration changes to the time range covered by the selected packets.	
Zoom To Throughput Graph Data Point	When clicked, the Viewport duration changes to the time range of the Throughput Graph selected data point.	
Custom Zoom (Set by Zoom To Time Range of Selected Packets, Zoom To Throughput Graph Data Point, or dragging Viewport Slide)	Automatically checked when taking any zoom action other than the fixed Viewport zoom durations listed below.	

Table 4.11 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
The following 21 selections are mutually exclusive.		
150 usec	Each of these Zoom selections sets the Viewport and the Timeline to a fixed time duration.	
300 usec		
625 usec (1 Bluetooth slot)		
1.25 msec (2 Bluetooth slots)		
1.875 msec (3 Bluetooth slots)		
2.5 msec (4 Bluetooth slots)		
3.125 msec (5 Bluetooth slots)		
6.25 msec (10 Bluetooth slots)		
15.625 msec (25 Bluetooth slots)		
31.25 msec (30 Bluetooth slots)		
62.5 msec (100 Bluetooth slots)		
156.255 msec (250 Bluetooth slots)		
31.25 msec (500 Bluetooth slots)		
625 msec (1,000 Bluetooth slots)		
1 sec (1,600 Bluetooth slots)		
2 sec (3,200 Bluetooth slots)		
3 sec (4,800 Bluetooth slots)		
4 sec (6,400 Bluetooth slots)		
5 sec (8,000 Bluetooth slots)		
10 sec (16,000 Bluetooth slots)		
20 sec (32,000 Bluetooth slots)		

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

Table 4.12 - Coexistence View Navigate Menu Selections

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

Table 4.12 - Coexistence View Navigate Menu Selections (continued)

Selection	Description	Hot key
Next Error Packet	When clicked, selects the next packet with an error from the current selection and displays it in the Timeline. Performs the same function as the ➡ Next Error Packet button.	Ctrl+Right Arrow
First Legend Packet	When clicked, selects the first legend packet in the session and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 182. Performs the same functions as the ⇤ First Legend Packet button.	
Previous Legend Packet	When clicked, selects the first prior legend packet in time from the current selection and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 182. Performs the same functions as the ⬅ Previous Legend Packet button.	
Next Legend Packet	When clicked, selects the next legend packet in time from the current selection and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 182. Performs the same functions as the ➡ Next Legend Packet button.	
Last Legend Packet	When clicked, selects the last legend packet in the session and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to on page 182. Performs the same functions as the ⇥ Last Legend Packet button.	
Toggle Display Lock	This selection is active during Live capture mode only. Checking this selection will lock the Throughput Graph and the Timeline in its current position, however the capture will continue. Not checking this selection will cause the Throughput Graph and the Timeline to scroll as data is collected.	

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

4.3.4.2 Coexistence View - Toolbar

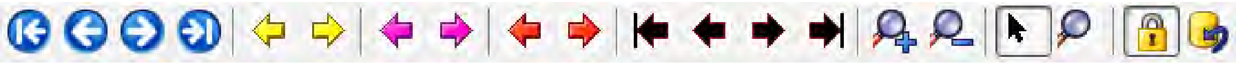


Figure 4.59 - Coexistence View Toolbar

The toolbar contains the following selections:

Table 4.13 - Coexistence View Toolbar icons

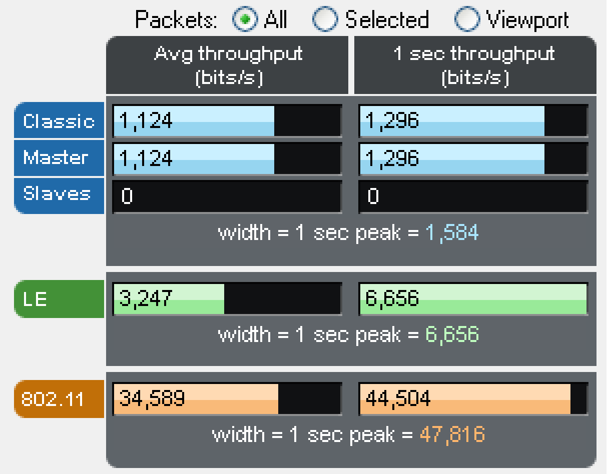
Icon	Description
⏮	Move to the first packet.
⬅	Move to the previous packet.
➡	Move to the next packet.
⏭	Move to the last packet.
⇦	Move to the previous retransmitted packet.
⇨	Move to the next retransmitted packet
⇦	Move to the previous invalid IFS for *Bluetooth* low energy.
⇨	Move to the next invalid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

Table 4.13 - Coexistence View Toolbar icons (continued)

Icon	Description
🔍	When selected the cursor changes from Scroll ↖ to a context-aware zooming cursor. Click on normal cursor to remove the zooming cursor.
🔍	Zooming cursor.
🔓	Scroll Lock/Unlock during live capture mode.
🔄	Reset during live capture mode. Clears the display.

4.3.4.3 Coexistence View - Throughput Indicators

(Click here to see a video on the Throughput Indicators...)
Throughput Indicators



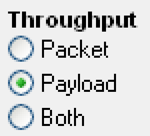
Packets: ● All ○ Selected ○ Viewport

	Avg throughput (bits/s)	1 sec throughput (bits/s)
Classic	1,124	1,296
Master	1,124	1,296
Slaves	0	0
	width = 1 sec peak = 1,584	
LE	3,247	6,656
	width = 1 sec peak = 6,656	
802.11	34,589	44,504
	width = 1 sec peak = 47,816	

Figure 4.60 - Coexistence View Throughput Indicators

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

4.3.4.4 Throughput

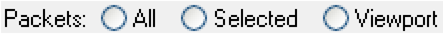


Throughput
○ Packet
● Payload
○ Both

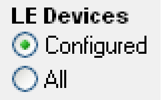
Throughput is total packet or payload size in bits of the included packets divided by the duration of the included packets, where:

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

4.3.4.5 Radio Buttons

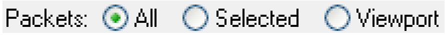

Packets: ○ All ○ Selected ○ Viewport

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


LE Devices
● Configured
○ All

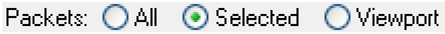
- *Bluetooth* low energy packets from non-configured devices are excluded if the **Configured** radio button in the LE Devices group is selected.
- **Frame Display** filtering has no effect here in that packets that are filtered-out in **Frame Display** are still used here as long as they otherwise meet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

4.3.4.6 All radio button


Packets: ● All ○ Selected ○ Viewport

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

4.3.4.7 Selected radio button


Packets: ○ All ● Selected ○ Viewport

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

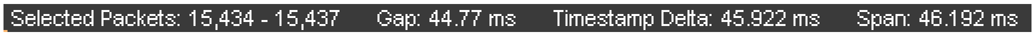
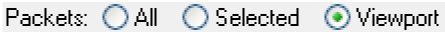

Selected Packets: 15,434 - 15,437 Gap: 44.77 ms Timestamp Delta: 45.922 ms Span: 46.192 ms

Figure 4.61 - Timeline Header Showing Selected Packets

4.3.4.8 Viewport radio button


Packets: ○ All ○ Selected ● Viewport

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

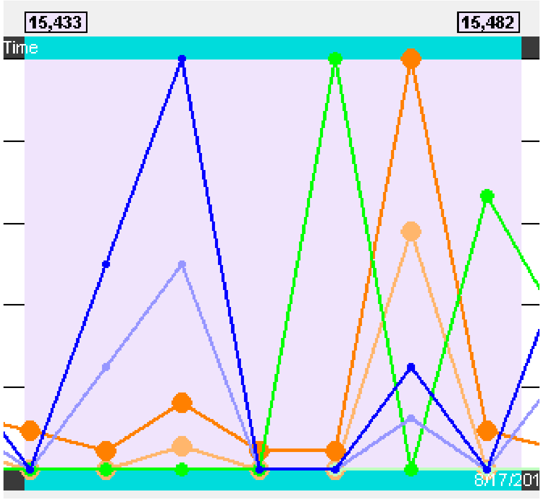
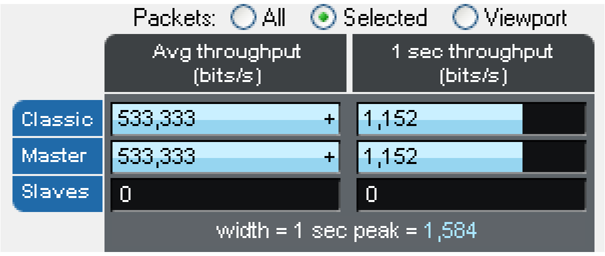


Figure 4.62 - **Throughput Graph** viewport.

4.3.4.9 Indicator width

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



Packets: ○ All ● Selected ○ Viewport

	Avg throughput (bits/s)	1 sec throughput (bits/s)
Classic	533,333 +	1,152
Master	533,333 +	1,152
Slaves	0	0

width = 1 sec peak = 1,584

Figure 4.63 - Average throughput indicators show a plus sign (+) when the indicator width is exceeded.

Figure 4.64 - A single selected packet

(Click here to see a video on how the Throughput is calculated...)

4.3.4.10 Coexistence View - Throughput Graph

(Click here to see aThroughput Graph video...)

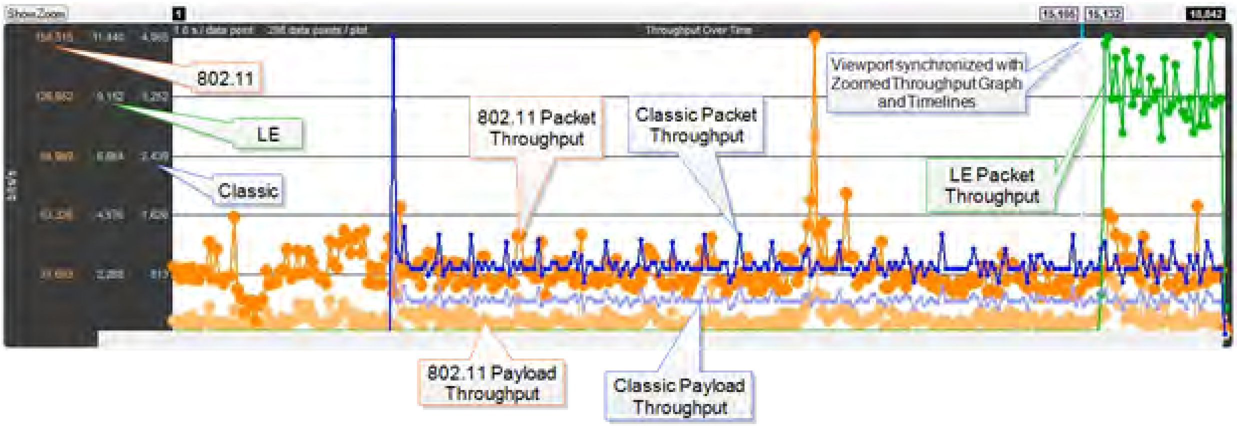


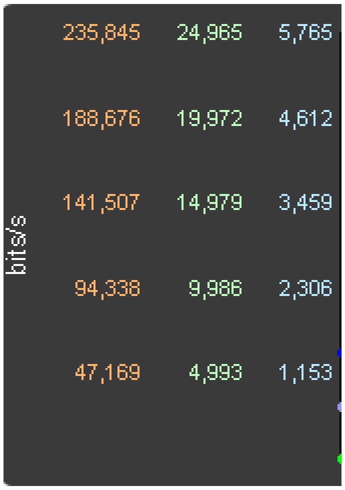
Figure 4.65 - Coexistence View Throughput Graph

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

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

4.3.4.11 Throughput Graph Y-axis labels

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



235,845	24,965	5,765
188,676	19,972	4,612
141,507	14,979	3,459
94,338	9,986	2,306
47,169	4,993	1,153

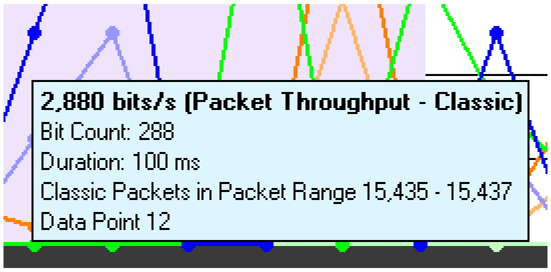
Figure 4.66 - **Throughput Graph** y-axis labels.

4.3.4.12 Excluded packets

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

4.3.4.13 Tooltips

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



2,880 bits/s (Packet Throughput - Classic)
Bit Count: 288
Duration: 100 ms
Classic Packets in Packet Range 15,435 - 15,437
Data Point 12

Figure 4.67 - Data point tooltip

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

4.3.4.14 Discontinuities

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

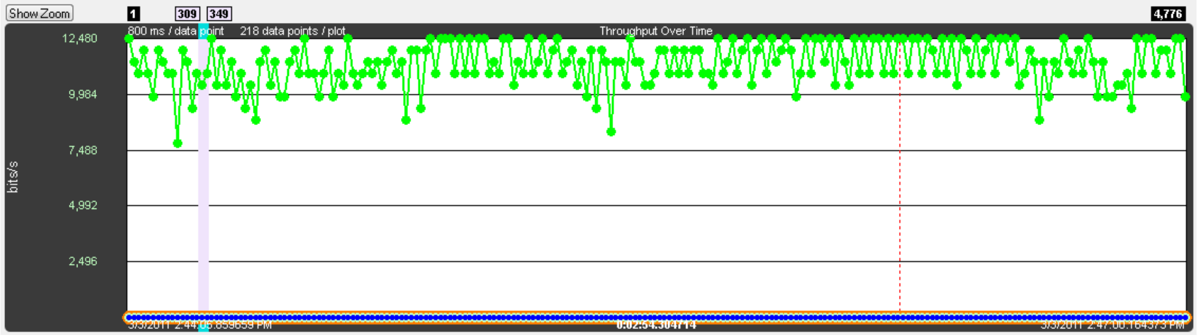


Figure 4.68 - A negative discontinuity.

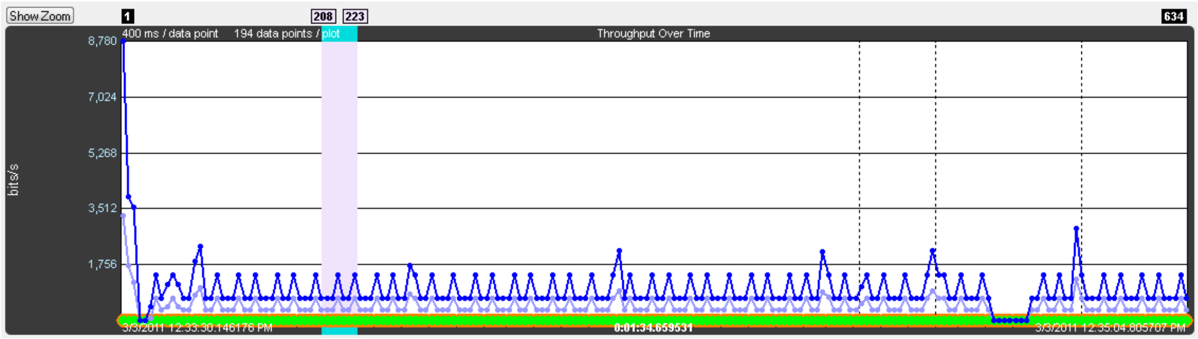


Figure 4.69 - Three positive discontinuities.

4.3.4.15 Viewport

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

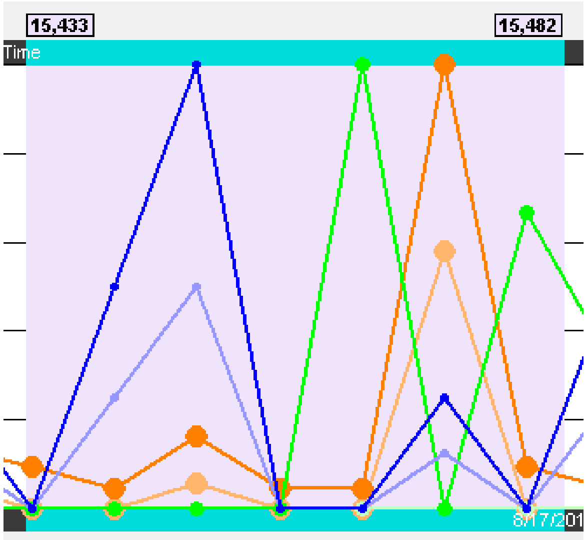


Figure 4.70 - **Throughput Graph** Viewport

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

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

4.3.4.16 Swap button

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

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

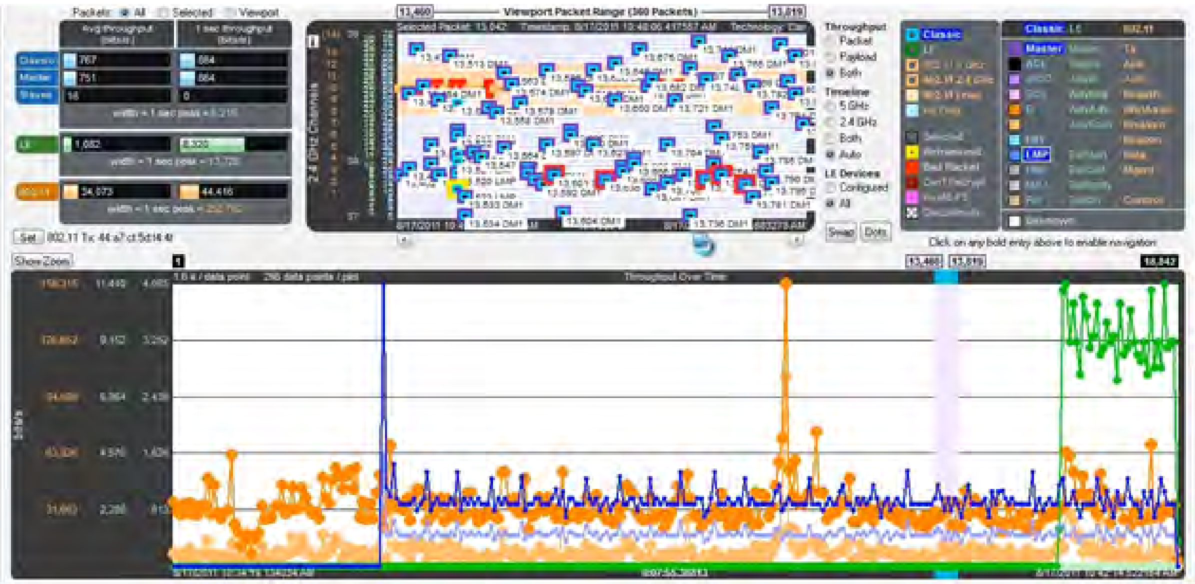


Figure 4.71 - Small Timeline and large Throughput Graph after pressing the Swap button.

4.3.4.17 Dots button

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

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

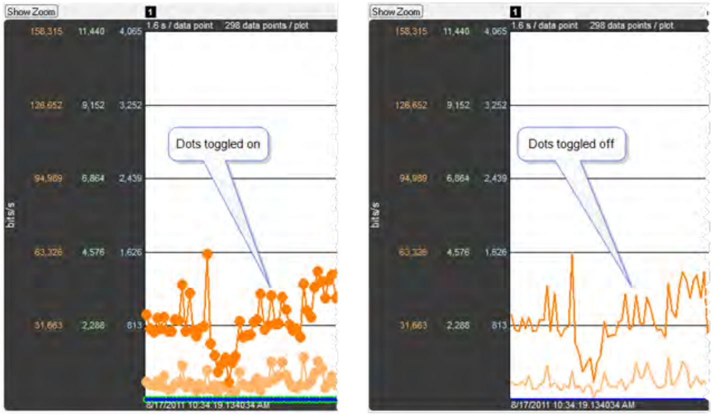
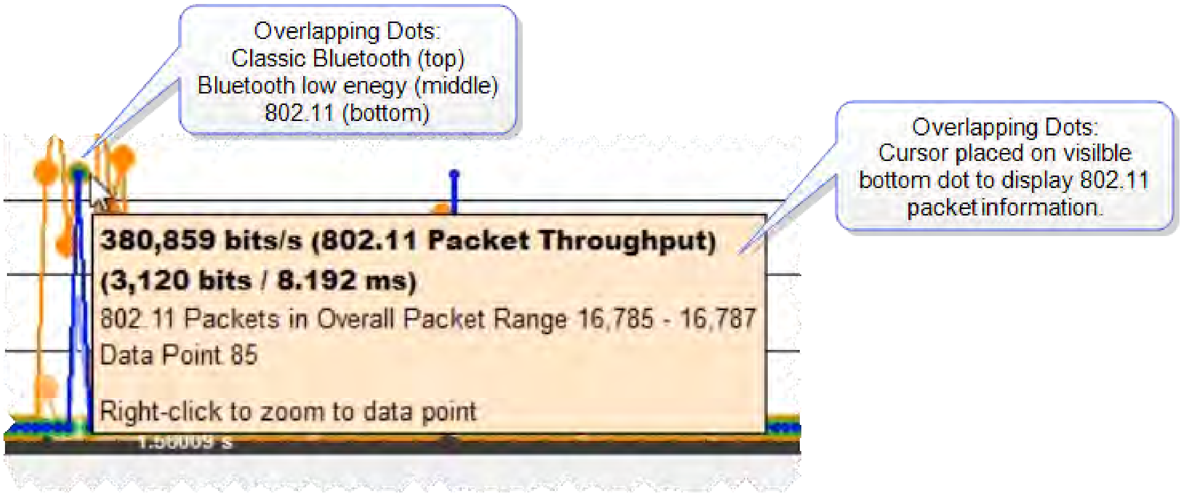


Figure 4.72 - Dots Toggled On and Off



Overlapping Dots:
Classic Bluetooth (top)
Bluetooth low enegy (middle)
802.11 (bottom)

Overlapping Dots:
Cursor placed on visilbe
bottom dot to display 802.11
packet information.

380,859 bits/s (802.11 Packet Throughput)
(3,120 bits / 8.192 ms)
802.11 Packets in Overall Packet Range 16,785 - 16,787
Data Point 85

Right-click to zoom to data point

Figure 4.73 - Overlapping **Dots** Information Display

4.3.4.18 Zoomed Throughput Graph

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

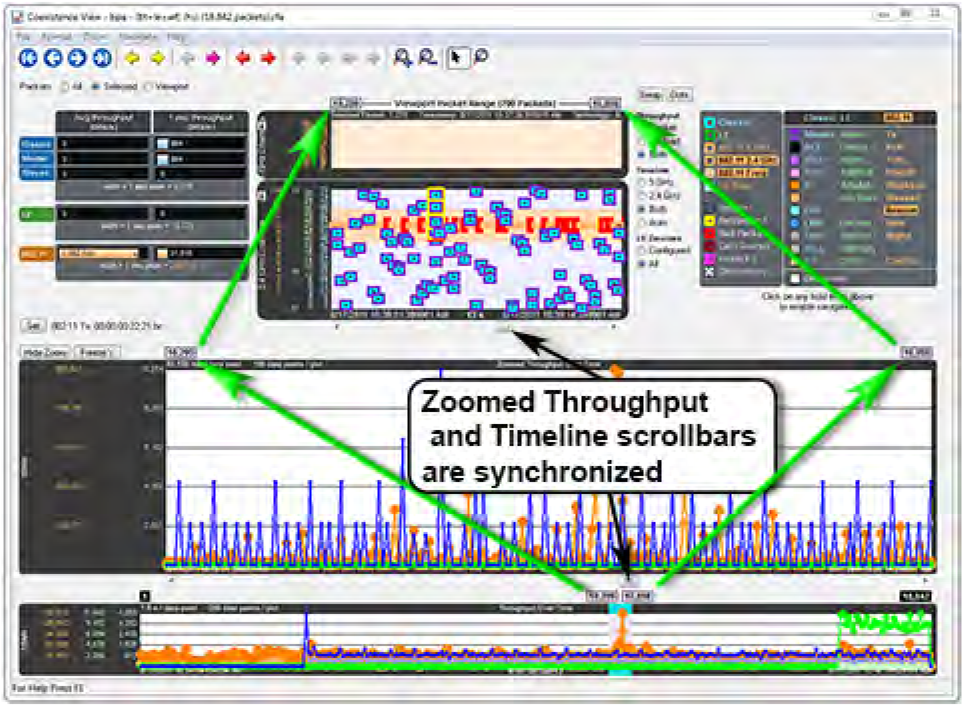

Zoomed Throughput and Timeline scrollbars are synchronized
Viewport Packet Range
Hide Zoom
Freeze Y
Zoomed Throughput Over Time
Throughput Over Time
For Help Press F1

Figure 4.74 - Synchronized Zoomed Throughput Graph and View Port

The largest value in each technology in the **Zoomed Throughput Graph** is snapped to the top of the graph. This makes the graph easier to read by using all of the available space, but because the y-axis scales can change it can make it difficult to compare different time ranges or durations. Clicking the **Freeze Y** Freeze Y button freezes the y-axis scales and makes it possible to compare all time ranges and durations (the name of the button changes to **Unfreeze Y** and a **Y Scales Frozen** indicator appears to the right of the title. Clicking the **Unfreeze Y** Unfreeze Y button unfreezes the y-axis scales.

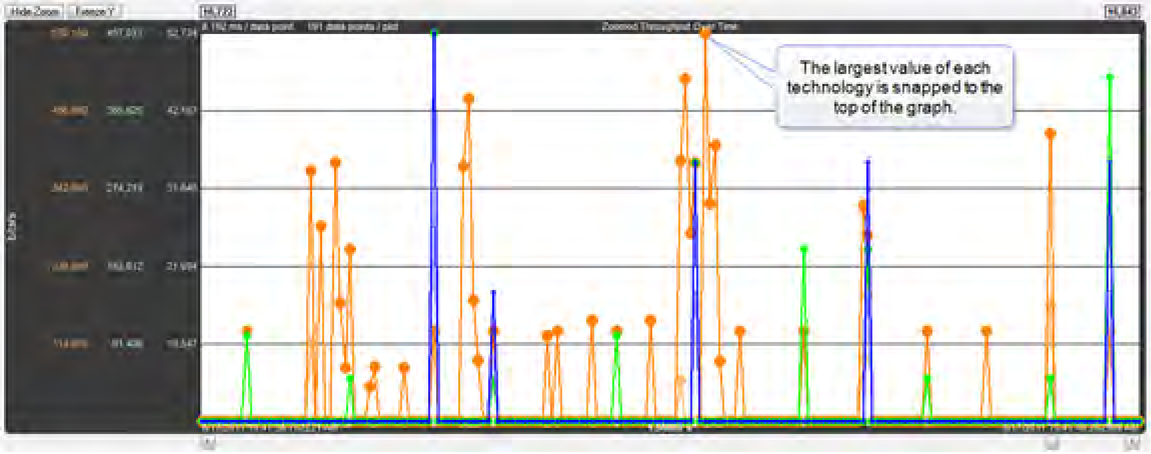

Hide Zoom
Freeze Y
Zoomed Throughput Over Time
The largest value of each technology is snapped to the top of the graph.
Bytes

Figure 4.75 - **Zoomed Throughput Graph**- Largest Value Snaps to Top

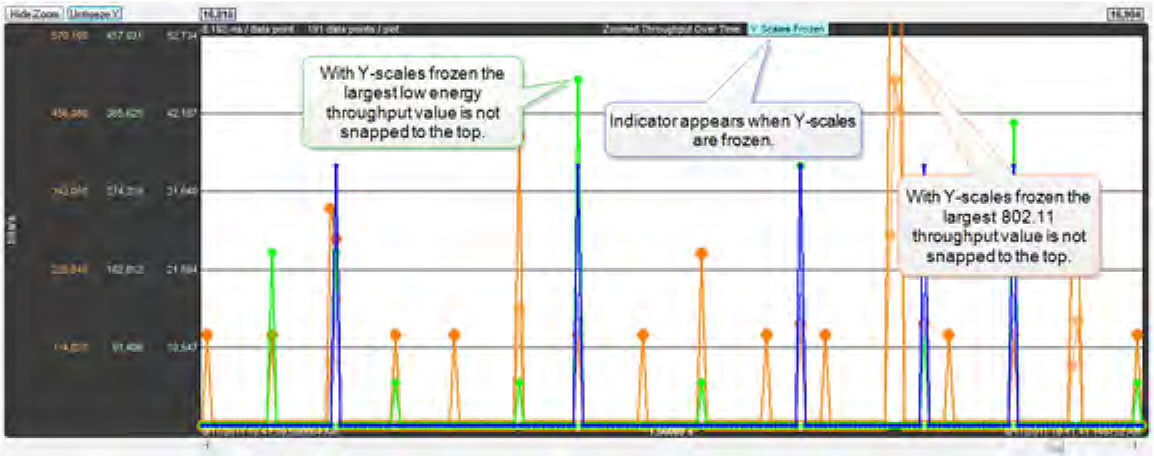
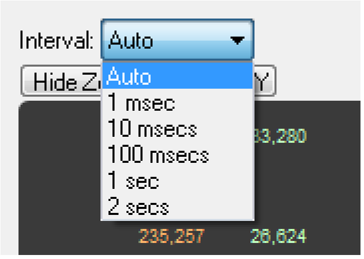

Hide Zoom
Unfreeze Y
Zoomed Throughput Over Time
Y Scales Frozen
With Y-scales frozen the largest low energy throughput value is not snapped to the top.
Indicator appears when Y-scales are frozen.
With Y-scales frozen the largest 802.11 throughput value is not snapped to the top.

Figure 4.76 - **Zoomed Throughput Graph** - **Freeze Y** keeps the y-axis constant

Interval Menu



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

4.3.4.19 Zoom Cursor

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

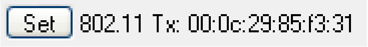
4.3.4.20 Comparison with the *Bluetooth* Timeline's Throughput Graph

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

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

4.3.4.21 Coexistence View - Set Button

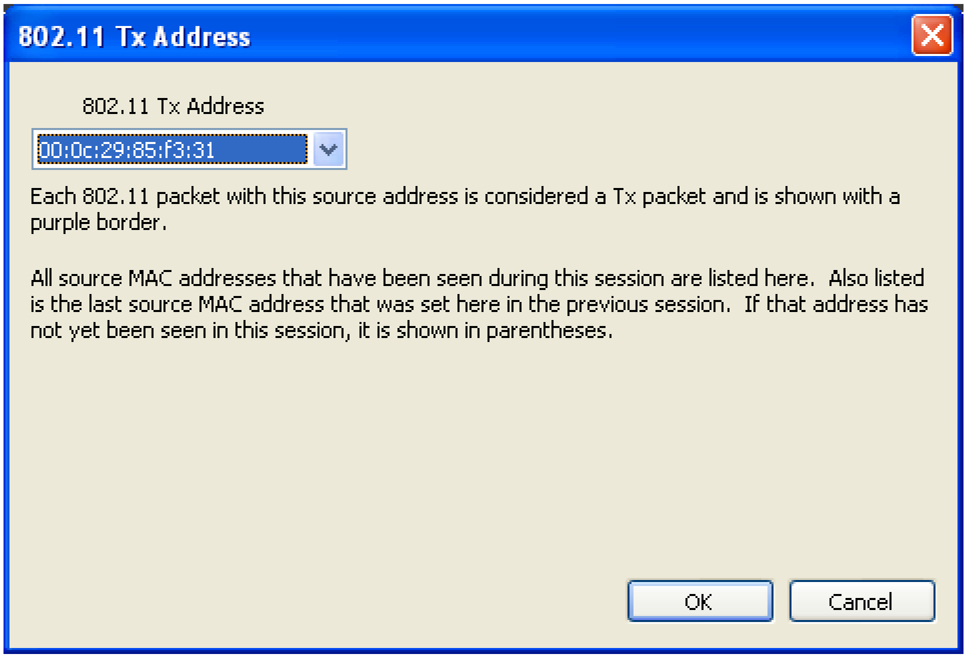
(Click here to see a video on the Wi-Fi Tx Address Set button...



802.11 Tx: 00:0c:29:85:f3:31

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

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


802.11 Tx Address

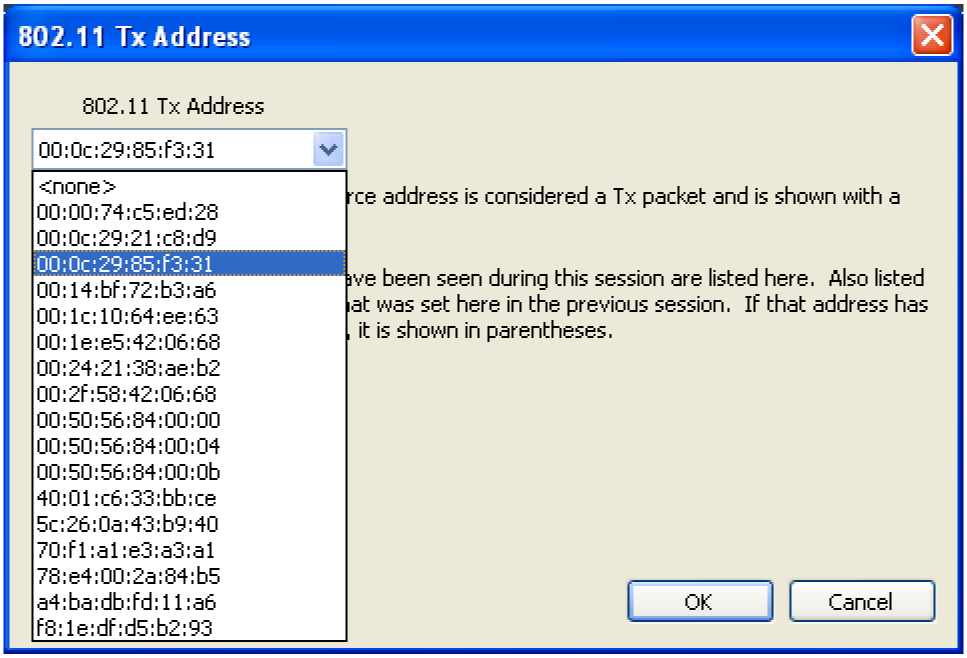
802.11 Tx Address

00:0c:29:85:f3:31

Each 802.11 packet with this source address is considered a Tx packet and is shown with a purple border.

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

Figure 4.77 - 802.11 Source Address Dialog



802.11 Tx Address

802.11 Tx Address

00:0c:29:85:f3:31

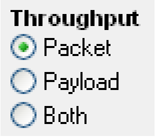
<none>
00:00:74:c5:ed:28
00:0c:29:21:c8:d9
00:0c:29:85:f3:31
00:14:bf:72:b3:a6
00:1c:10:64:ee:63
00:1e:e5:42:06:68
00:24:21:38:ae:b2
00:2f:58:42:06:68
00:50:56:84:00:00
00:50:56:84:00:04
00:50:56:84:00:0b
40:01:c6:33:bb:ce
5c:26:0a:43:b9:40
70:f1:a1:e3:a3:a1
78:e4:00:2a:84:b5
a4:ba:db:fd:11:a6
f8:1e:df:d5:b2:93

rce address is considered a Tx packet and is shown with a

ave been seen during this session are listed here. Also listed
at was set here in the previous session. If that address has
, it is shown in parentheses.

Figure 4.78 - 802.11 Source Address Drop Down Selector

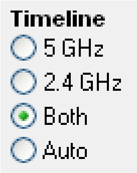
4.3.4.22 Coexistence View - Throughput Radio Buttons



Throughput
● Packet
○ Payload
○ Both

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

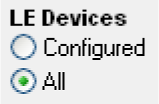
4.3.4.23 Coexistence View - Timeline Radio Buttons



Timeline
○ 5 GHz
○ 2.4 GHz
● Both
○ Auto

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

4.3.4.24 Coexistence View – low energy Devices Radio Buttons

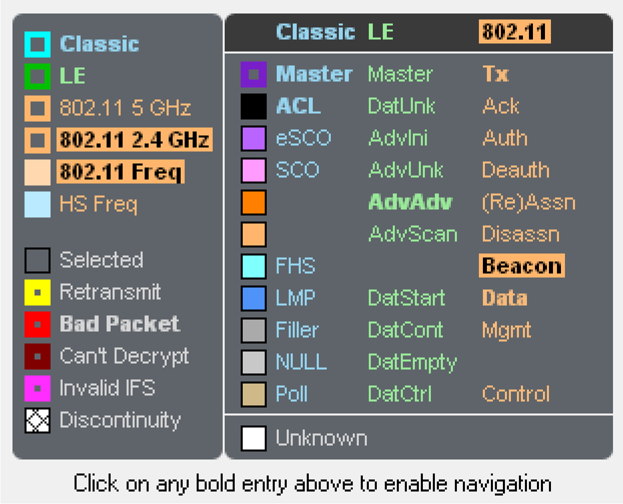


LE Devices
○ Configured
● All

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

4.3.4.25 Coexistence View – Legend

(This video provides more details on the Legend...)



- **Classic**
- **LE**
- 802.11 5 GHz
- **802.11 2.4 GHz**
- **802.11 Freq**
- HS Freq
- Selected
- Retransmit
- **Bad Packet**
- Can't Decrypt
- Invalid IFS
- Discontinuity

Classic	LE	**802.11**
Master	Master	**Tx**
ACL	DatUnk	Ack
eSCO	AdvIni	Auth
SCO	AdvUnk	Deauth
	AdvAdv	(Re)Assn
	AdvScan	Disassn
FHS		**Beacon**
LMP	DatStart	**Data**
Filler	DatCont	Mgmt
NULL	DatEmpty	
Poll	DatCtrl	Control
Unknown		

Click on any bold entry above to enable navigation

Figure 4.79 - Coexistence View Legend

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

4.3.4.26 Coexistence View – Timelines

(Click here to see a Coexistence View Timeline video...)

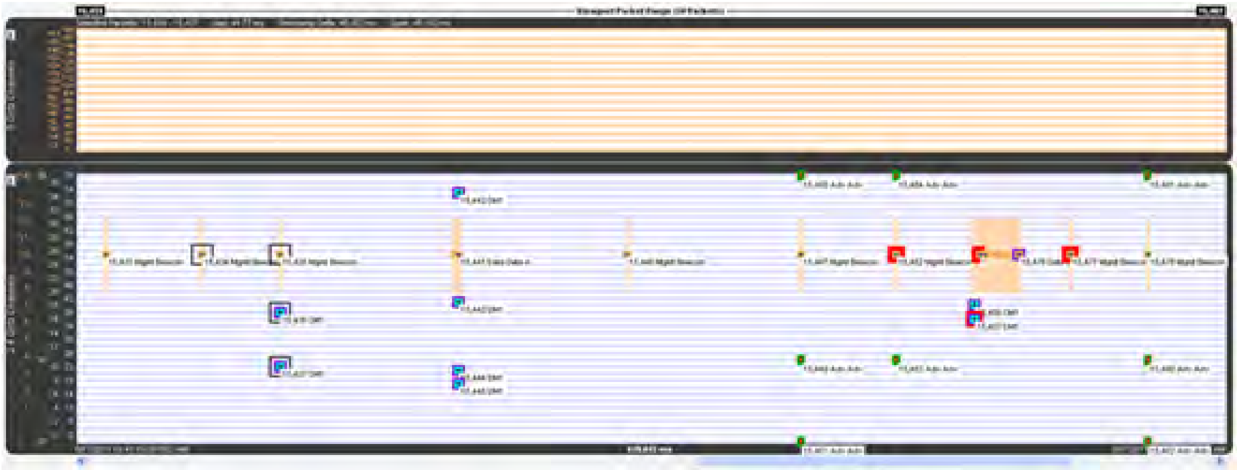


Figure 4.80 - Coexistence View Timelines

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

4.3.4.27 Packet information

Packet information is provided in various ways as described below.

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

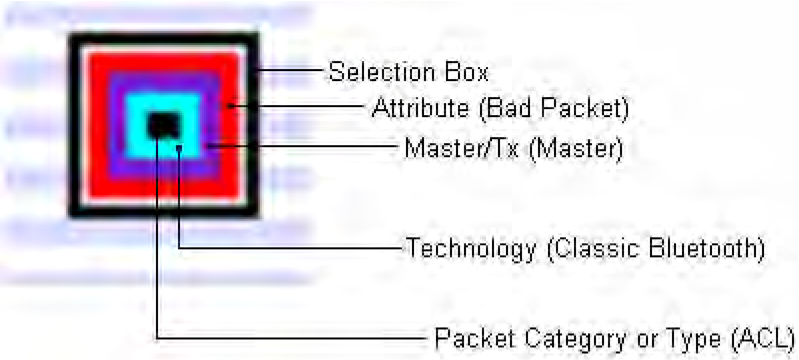
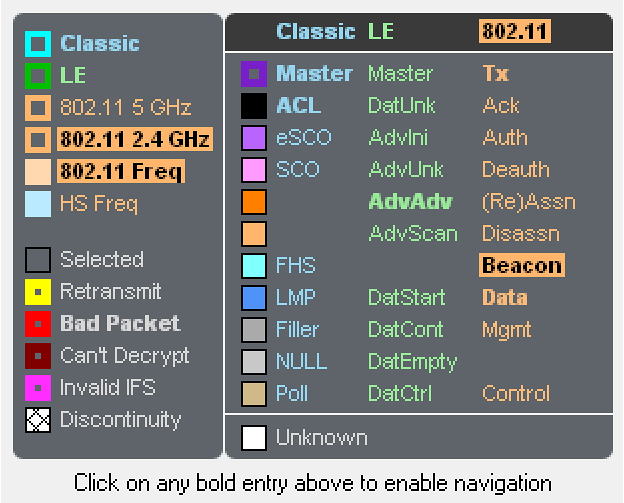


Figure 4.81 - Each packet is color-coded

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

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

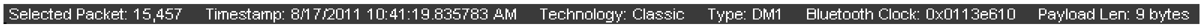
Selecting a packet by clicking on it draws a selection box around it (as shown above) and highlights the applicable entries in the legend.



Click on any bold entry above to enable navigation

Figure 4.82 - Highlighted entries in the legend for a selected packet.

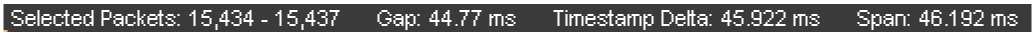
Summary information for a selected packet is displayed in the timeline header.



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

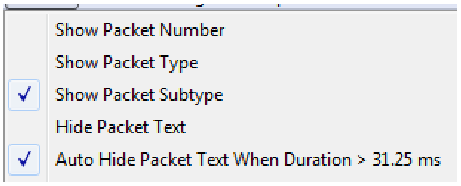
Figure 4.83 - **Timeline** header for a single selected packet.

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



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

Figure 4.84 - **Timeline** header for multiple selected packets



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

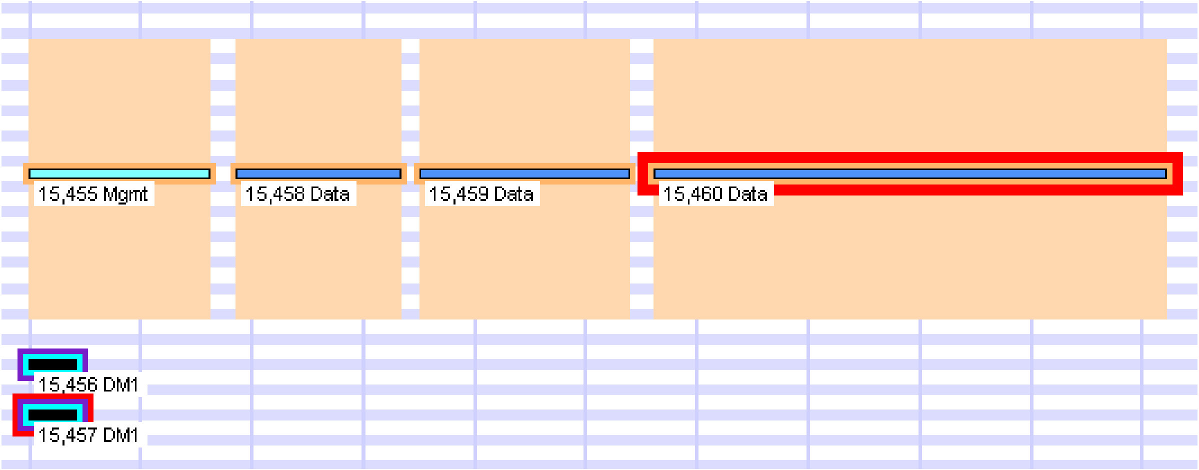
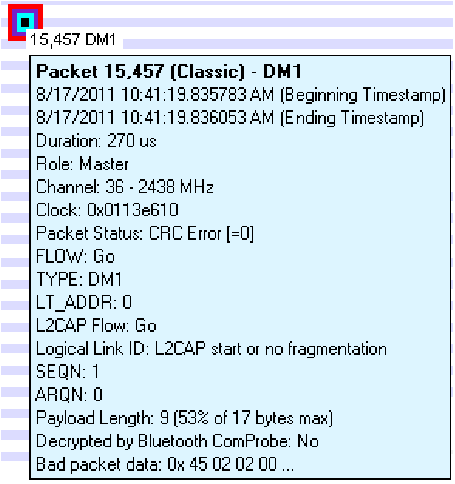


Figure 4.85 - Descriptive text on timeline packets.

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



Packet 15,457 (Classic) - DM1
8/17/2011 10:41:19.835783 AM (Beginning Timestamp)
8/17/2011 10:41:19.836053 AM (Ending Timestamp)
Duration: 270 us
Role: Master
Channel: 36 - 2438 MHz
Clock: 0x0113e610
Packet Status: CRC Error (=0)
FLOW: Go
TYPE: DM1
LT_ADDR: 0
L2CAP Flow: Go
Logical Link ID: L2CAP start or no fragmentation
SEQN: 1
ARQN: 0
Payload Length: 9 (53% of 17 bytes max)
Decrypted by Bluetooth ComProbe: No
Bad packet data: 0x 45 02 02 00 ...

Figure 4.86 - A tool tip for a Classic *Bluetooth* packet.

4.3.4.28 Relocating the tool tip

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