fte.com frontline®
Debug Communications Faster℠

ComProbe®
Protocol Analysis System

BPA® low energy

Bluetooth® Protocol Analyzer

ComProbe® User Manual

Revision Date: 4/10/2014

Contents

List of Figures

Chapter 1: ComProbe Hardware & Software

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

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

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

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

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

1.1 What is in this manual

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

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

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

1.2 Minimum System Requirements

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

1.3 Software Installation

1.3.1 From CD:

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

1.3.2 From Download:

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

Chapter 2: Getting Started

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

2.1 BPA low energy Hardware

The following sections describe the ComProbe BPA low energy hardware connectors and hardware setup.

2.1.1 Connecting/Powering

1. Insert the USB cable mini-connector into the USB port on the ComProbe BPA low energy hardware.
2. Insert the other end of the USB cable into the PC.

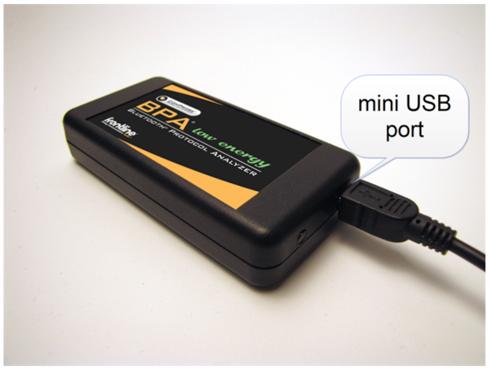


Figure 1. BPA low energy Hardware USB PortComProbe 802 11 QSG frontline

2.2 Data Capture Methods

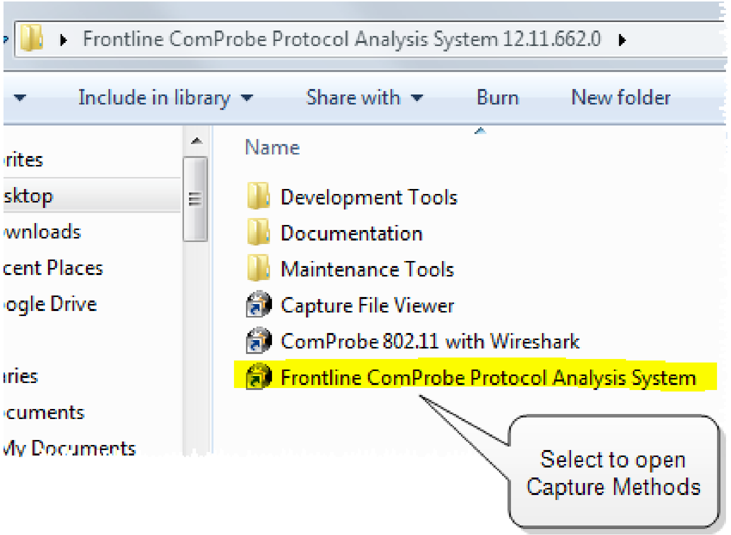
This section describes how to load Frontline Test Equipment, Inc ComProbe Protocol Analysis System software, and how to select the data capture method for your specific application.

2.2.1 Opening ComProbe® Data Capture Method

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

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

This opens a standard Windows file folder window.



Frontline ComProbe Protocol Analysis System 12.11.662.0

Include in library ▾ Share with ▾ Burn New folder

rites
sktop
wnloads
cent Places
ogle Drive

ries
cuments
My Documents

Name

Development Tools
Documentation
Maintenance Tools
Capture File Viewer
ComProbe 802.11 with Wireshark
Frontline ComProbe Protocol Analysis System

Select to open Capture Methods

Figure 2. Desktop Folder Link

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

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

This dialog lists all the methods ComProbe supports in a tree control. See Protocol List

Three buttons appear at the bottom of the dialog; Run, Cancel, and Help. When the dialog first opens, Cancel and Help are active, and the Run button is inactive (grayed out).

Run starts the selected protocol stack.

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

Help takes the user to this help file as does pressing the F1 key.

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

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

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

Creating a Shortcut

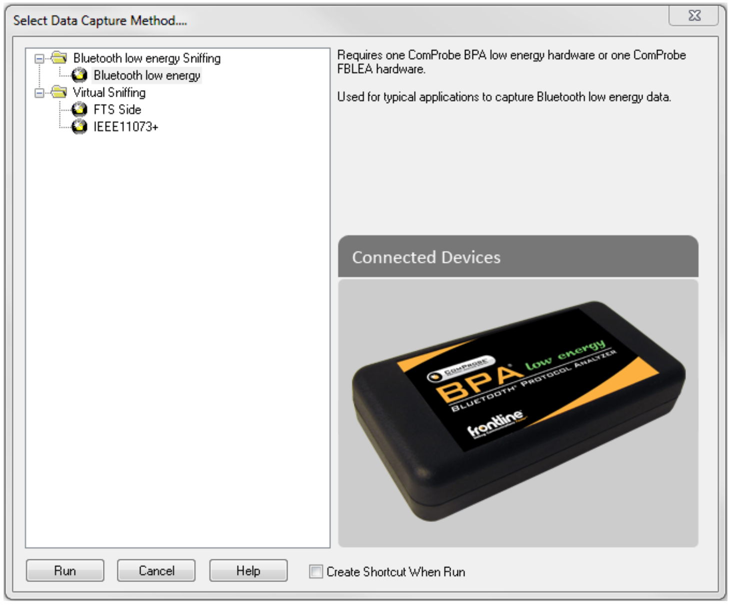
A checkbox labeled Create Shortcut When Run is located near the bottom of the dialog. This box is unchecked by default. Select this checkbox, and the system creates a shortcut for the selected method, and places it in the "Frontline ComProbe Protocol Analysis System <version#>" desktop folder and in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

Supporting Documentation

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

2.2.2 ComProbe® BPA low energy Data Capture Methods

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



Select Data Capture Method....

Requires one ComProbe BPA low energy hardware or one ComProbe FBLEA hardware.

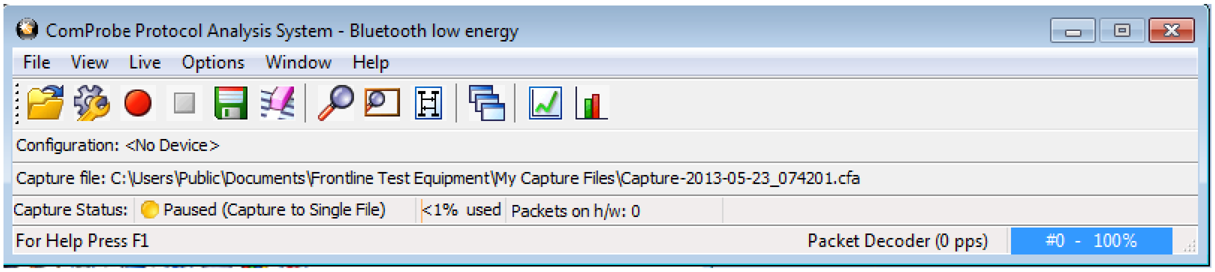
Used for typical applications to capture Bluetooth low energy data.

Bluetooth low energy Sniffing
Bluetooth low energy
Virtual Sniffing
FTS Side
IEEE11073+
Connected Devices
ComProbe BPA low energy Bluetooth® Protocol Analyzer
frontline
Run
Cancel
Help
□ Create Shortcut When Run

- **Bluetooth® low energy**
  - This method requires one ComProbe BPA low energy hardware or one ComProbe FBLEA hardware.
  - Used for typical applications to capture *Bluetooth* low energy data.

2.3 Control Window

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



Configuration: <No Device>

Capture file: C:\Users\Public\Documents\Frontline Test Equipment\My Capture Files\Capture-2013-05-23_074201.cfa

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

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

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

2.3.1 Control Window Toolbar

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

Open File - Opens a capture file.

I/O Settings - Opens settings

Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.

Save - Saves the file the capture file.

Clear - Clears or saves the capture file.

Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.

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

Cascade - Arranges windows in a cascaded display.

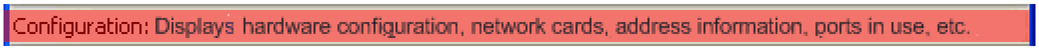
Low energy - Opens the low energy Timeline dialog.

MSC Chart - Opens the Message Sequence Chart

Bluetooth low energy Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.

2.3.2 Configuration Information on the Control Window

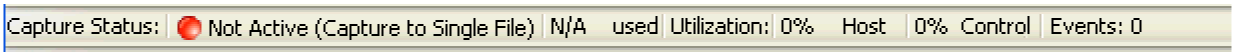
The Configuration bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc.



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

2.3.3 Status Information on the Control Window

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



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

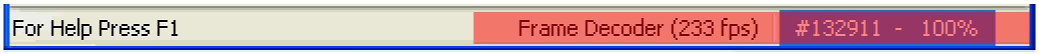
- Capture Status displays Not Active, Paused or Running and refers to the state of data capture. It will also display whether you are capturing to a series of files or capturing to a single file.
  - Not Active means that the analyzer is not currently capturing data.
  - Paused means that data capture has been suspended.
  - Running means that the analyzer is actively capturing data.
- % Used

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

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

2.3.4 Frame Information on the Control Window

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



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

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

- #132911 displays the total frames decoded.

- 100% displays the percentage of buffer space used.

2.3.5 Drop-Down Menus

The menus that you see on the Control Window and dialogs like Frame Display and Event Display vary depending on whether the data is being captured live or whether you are looking at a .cfa file. You will see File, Edit, View, Filter, Bookmarks, Live, Options, Window, and Help. Most of the options are self explanatory.

- Many of the File/Edit menu items are standard Windows type commands: Open, Close, Save, Recent Files, etc. There are, however, several of these menu items that have unique functionality:
- Recreate Companion File: This option is available when you are working with decoders. If you change a decoder while working with data, you can use Recreate Companion File to recreate the ".frm file", the companion file to the ".cfa file". Recreating the ".frm file" helps ensure that the decoders will work properly.
- Reload Decoders: When clicked, the plug-ins are reset and received frames are decoded again.
- Under the View menu you can choose which Frontline windows are available to open.
- Live contains commands that are used in capturing data.
- Under Options you have opportunities to set/modify various system settings. These include:
    - Hardware Settings
    - I/O Settings
    - System Settings
    - Check for New Releases at Startup: When this is enabled, the application automatically checks for the latest Frontline releases. If a new version is detected, a dialog appears similar to the sample below . The system and version will vary dependent upon the ComProbe® hardware being used.
- The Window menu displays the open Frontline dialogs and standard options like Cascade, Minimize, Tile, etc.
- Within the Help menu you can open the electronic Help file, About <hardware.where <hardware> if the specific ComProbe capture method, e.g. "About BPA 600".

2.3.6 Minimizing Windows

Windows can be minimized individually or as a group when the Control window is minimized. To minimize windows as a group:

1. Go to the Window menu on the Control 🏠 window
2. Select Minimize Control Minimizes All. The analyzer puts a check next to the menu item, indicating that when the Control window is minimized, all windows are minimized.
3. Select the menu item again to deactivate this feature.
4. The windows minimize to the top of the operating system Task Bar.

Chapter 3: Configuration Settings

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

3.1 BPA low energy Configuration

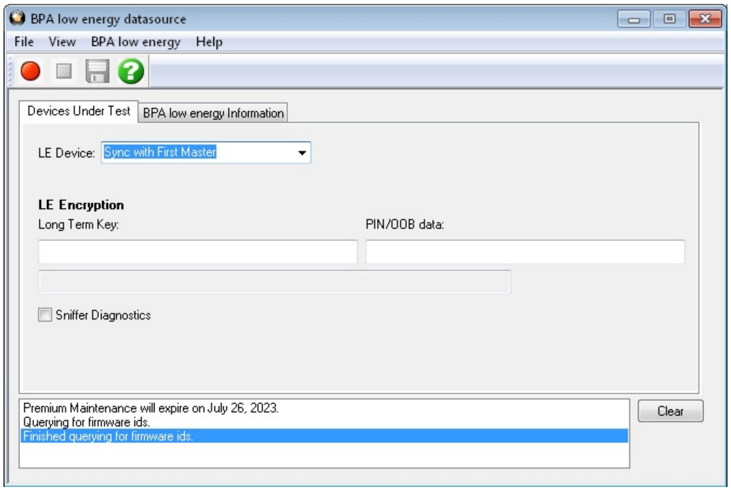
3.1.1 BPA low energy I/O Settings

Click on the topics listed below for information about ComProbe BPA low energy I/O settings.

1. Datasource
2. Information
3. Update Firmware

3.1.1.1 Datasource

You can select the ComProbe BPA low energy analyzer for sniffing Bluetooth low energy communications on available devices.



LE Device: Sync with First Master

Long Term Key:

PIN/OOB data:

□ Sniffer Diagnostics

Premium Maintenance will expire on July 26, 2023.
Querying for firmware ids.
Finished querying for firmware ids.

Figure 3. BPA low enegy Datasource Devices Under Test Tab

The default value in the LE Device drop down is Sync with First Master. To begin sniffing *Bluetooth* low energy simply click the red Start button on the datasource toolbar.

3.1.1.1.1 Specifying the LE Device Address

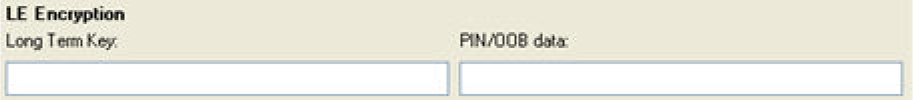
You may specify the LE device you are testing by typing in or choosing its address (BD_ADDR). You can type it directly into the drop down, or choose it from the existing previous values list in the drop down.

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

To refresh or discover devices click on the [BPA low energy Information] tab.

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

3.1.1.1.2 LE Encryption



LE Encryption

Long Term Key:

PIN/OOB data:

Figure 4. BPA low energy Devices Under Test LE Encryption

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

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.

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 afterward (the so called short term key).

The 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: f you use Copy/Paste to insert the Long Term Key , ComProbe software 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:

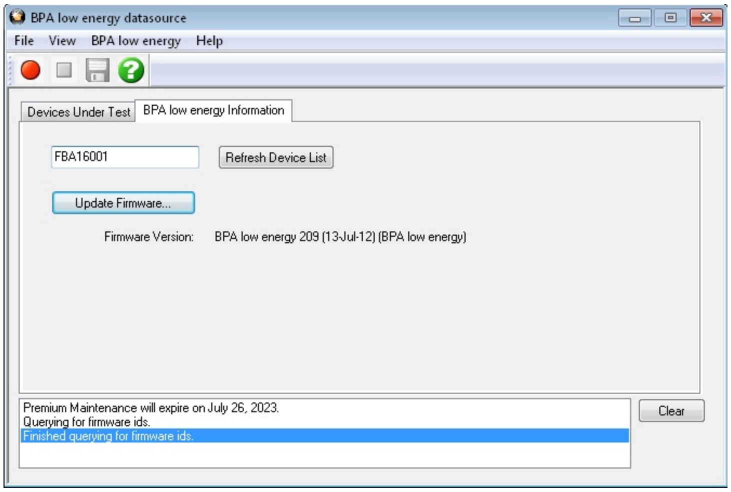
1. PIN is a six-digit (or less if leading zeros are omitted) decimal number.
2. Out-of-Band (OOB) data is a 16-digit hexadecimal code which the devices exchange via a channel that is different than the le transmission itself. This channel is called OOB.

   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.

Click here to see how to capture data after completing the configuration.

3.1.1.2 Information

The ComProbe BPA low energy Information tab is one of the two tabs that appear when you first start the low energy analyzer.



FBA16001

Firmware Version: BPA low energy 209 (13-Jul-12) (BPA low energy)

Premium Maintenance will expire on July 26, 2023.
Querying for firmware ids.
Finished querying for firmware ids.

Figure 5. BPA low energy Information Tab

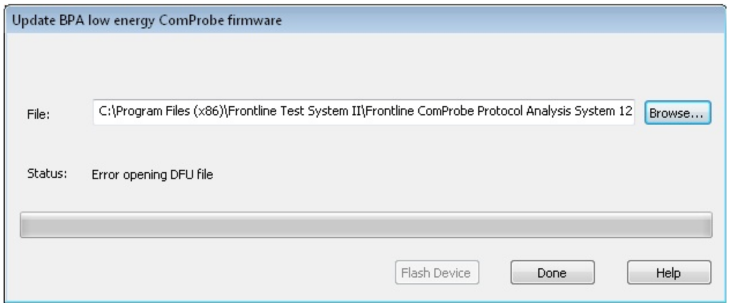
There are several pieces of information on this display:

- The current ComProbe BPA low energy hardware firmware is displayed under Firmware Version.
- If you want to make sure the most up-to-date list of devices is shown, select Refresh Device .
- If you want to load the latest firmware, you select the Update Firmware button.
- A message box at the bottom of the dialog displays status for devices that are connected.

3.1.1.3 Update Firmware

When you select the Update Firmware on the Information tab, the Update BPA low energy ComProbe firmware dialog appears. You use this dialog to update your low energy analyzer 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.



File: C:\Program Files (x86)\Frontline Test System II\Frontline ComProbe Protocol Analysis System 12

Status: Error opening DFU file

Figure 6. BPA low enerby Information Tab Update Firmware Dialog

1. Make sure the ComProbe BPA low energy analyzer.is attached.
2. Select the location of the firmware file.
3. 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.
4. Select Done when the update is finished.

3.1.1.4 Datasource Toolbar/Menu

The Datasource dialog toolbar and menu options are listed below.

Toolbar	
●	Start Sniffing button to begin sniffing. All settings are saved automatically when you start 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 dialog.
💾	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.
Menu	
File	Save and Exit options, self explanatory.
View	Hides or displays the toolbar.
BPA 500	Start Sniffing, Stop Sniffing, Resync Now, Discover Devices
Help	Opens ComProbe Help, and About BPA 500.

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.

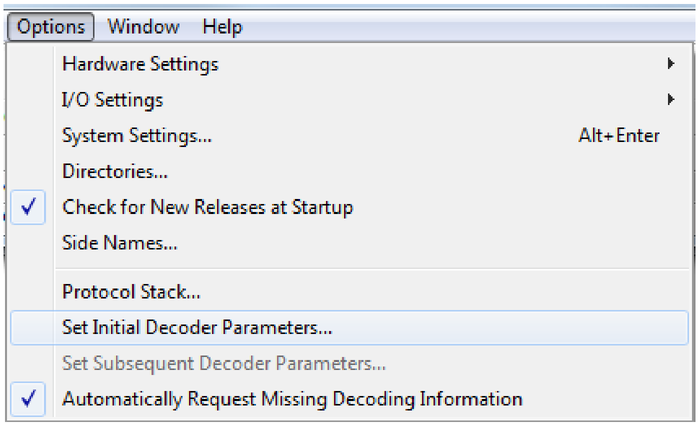

Options
Window
Help
Hardware Settings
I/O Settings
System Settings... Alt+Enter
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

Figure 7. Select Set Initial Decoder Parameters... from Control window

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

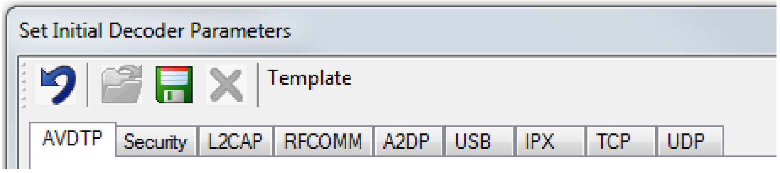


Figure 8. Tabs for each decoder requiring parameters.

- 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.

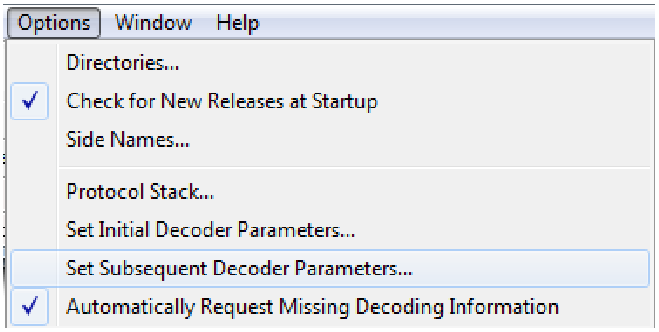
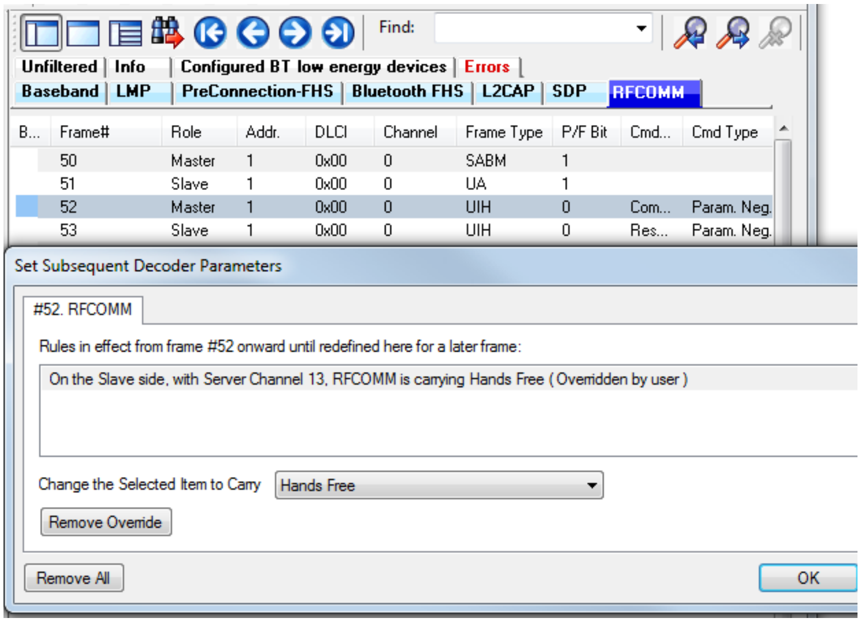

Options
Window
Help
Directories...
✓ Check for New Releases at Startup
Side Names...
Protocol Stack...
Set Initial Decoder Parameters...
Set Subsequent Decoder Parameters...
✓ Automatically Request Missing Decoding Information

Figure 9. Set Subsequent Decoder Parameters… from Control window



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

Set Subsequent Decoder Parameters

#52. RFCOMM

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

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

Change the Selected Item to Carry: Hands Free

Figure 10. 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.

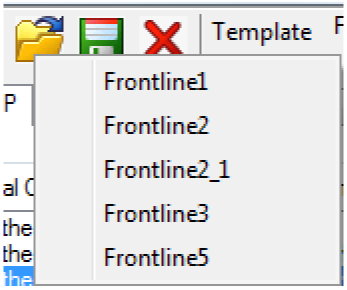
3.2.1 Decoder Parameter Templates

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

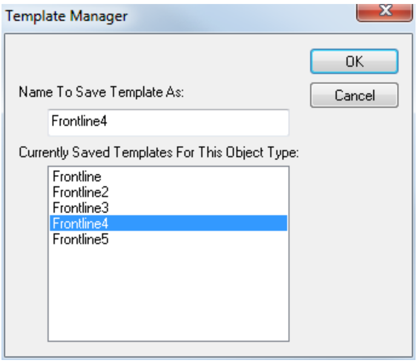
A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

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 tool-bar.

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

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

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

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

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

3.2.2 Selecting A2DP Decoder Parameters

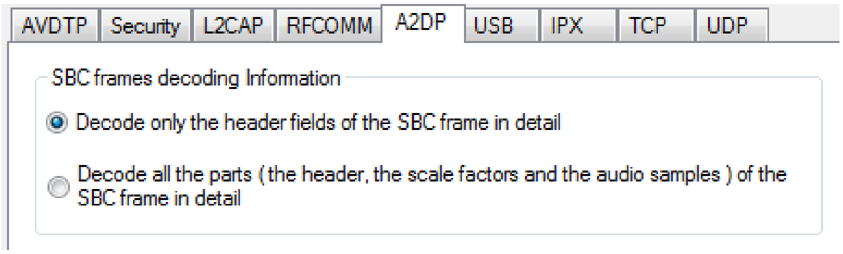
Decoding SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame. You can increase the decoding speed by decoding only the header fields and disregarding other parts. You can select the detail-level of decoding 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 11. A2DP Decoder Settings

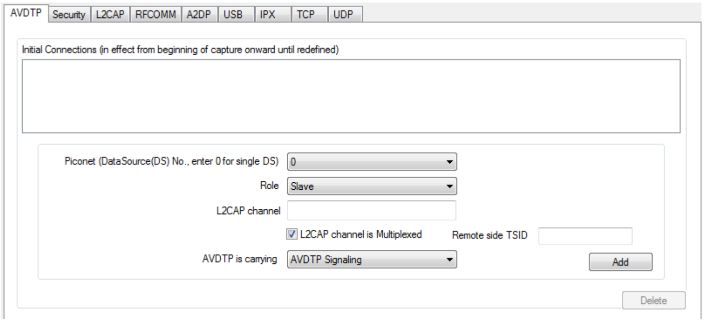
4. Follow steps to save the template changes or to save a new template.

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 12. AVDTP parameters tab

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

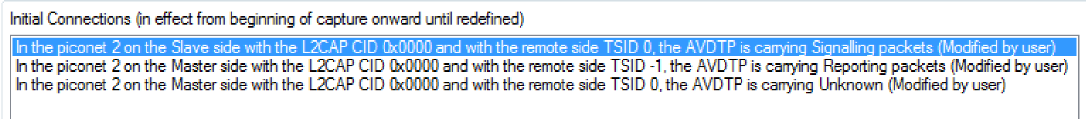
- Piconet (Data Source (DS) No.) - When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired number of data sources.
- Role - This identifies the role of the device initiating the frame (Master or Slave)
- L2CAP Channel - The channel number 0 through 78.
  - 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)

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 Adding a New or Saving an Existing Template on page 16Adding a New or Saving an Existing Template on page 16

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:

1. The capture session started after transmission of the vital information.

2. The analyzer incorrectly received a frame with the traversal information.

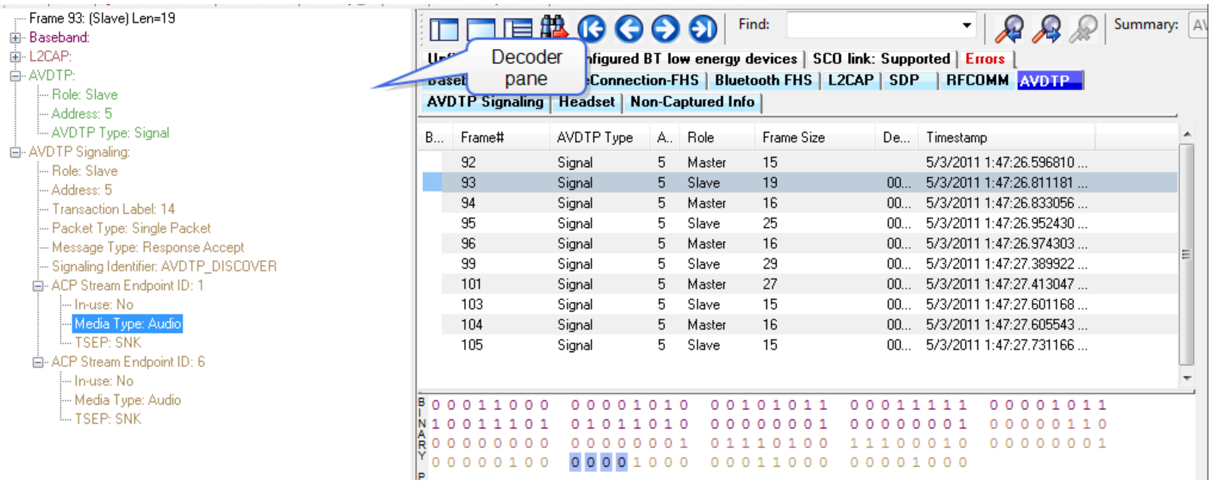
3. The communication monitored takes place between two players with implicit information not included in the transmission.

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 ...

```
B 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
N 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
R 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
Y 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
```

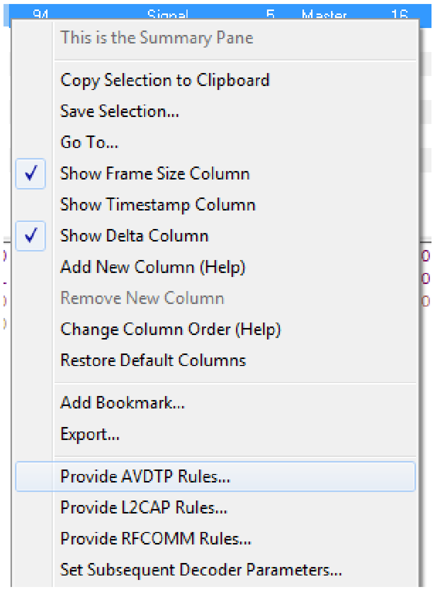
Figure 13. Look in Decoder pane for profile hints

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.

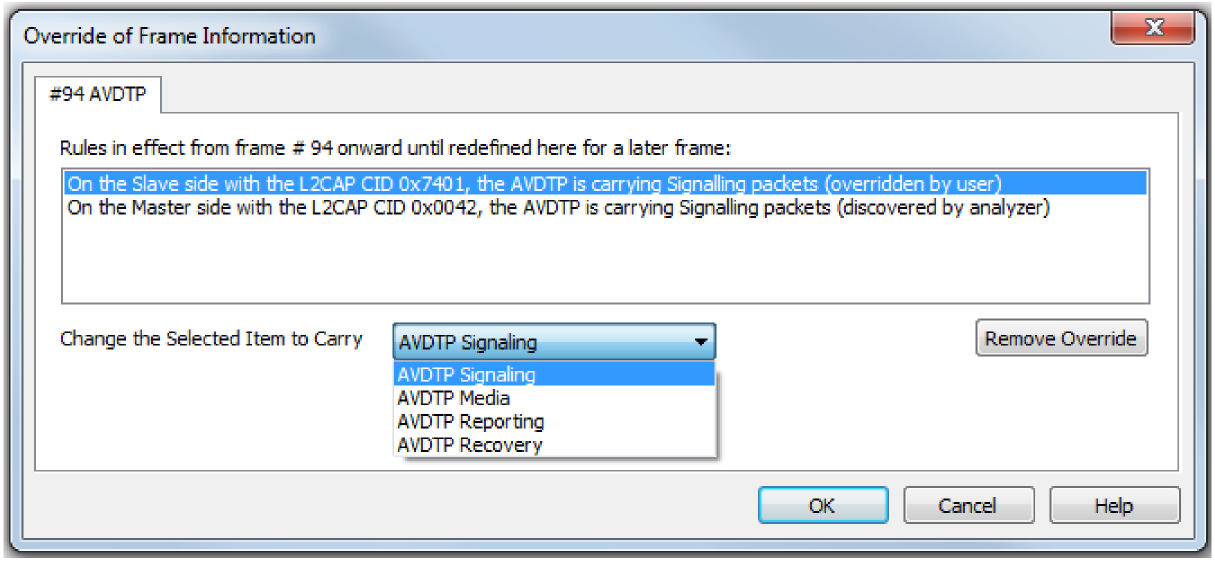
If you have a parameter in effect and wish to change that parameter:

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 over-riding AVDTP parameters.



Override of Frame Information

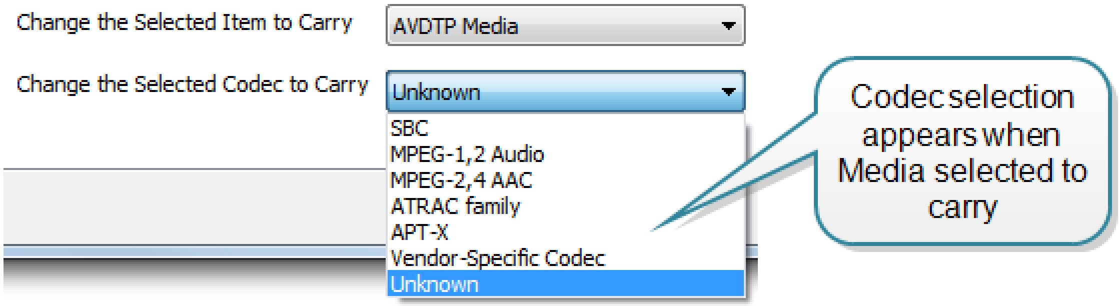
#94 AVDTP

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 14. AVDTP Override of Frame Information, Item to Carry



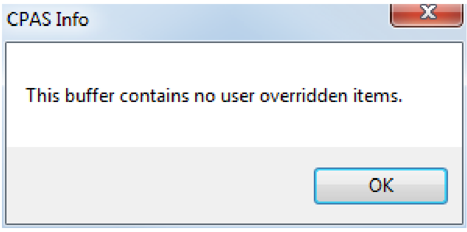
Change the Selected Item to Carry: AVDTP Media

Change the Selected Codec to Carry: Unknown

Codec selection appears when Media selected to carry

Figure 15. 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

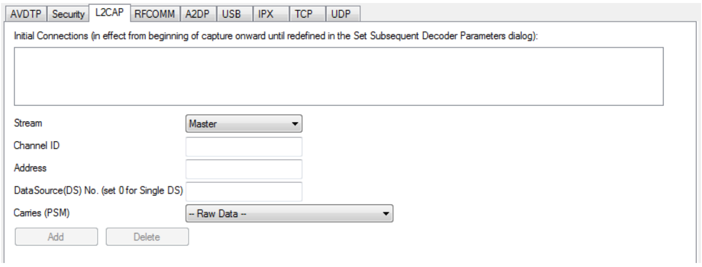
This buffer contains no user overridden items.

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

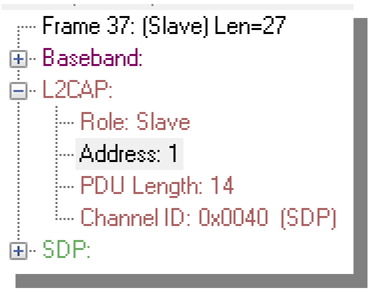
DataSource(DS) No. (set 0 for Single DS)

Carries (PSM): -- Raw Data --

Figure 16. L2CAP Decoder parameters tab

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

- Stream - This identifies the role of the device initiating the frame (master or slave)
- Channel ID - The channel number 0 through 78
- Address - This is the physical connection values for the devices. Each link in the net will have an address. A piconet can have up to seven links. The Frame Display can provide address information.



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

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

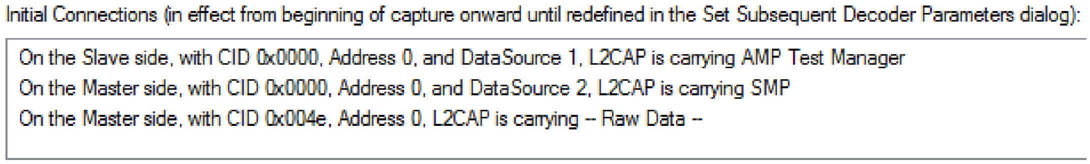
Carries (PSM) - Select the protocol that L2CAP traverses to from the following:

- AMP Manager
- AMP Test Manager
- SDP
- RFCOMM
- TCS
- LPMP
- BNEP
- HCRP Control
- HCRP Data

- HID
- AVCTP
- AVDTP
- CMTP
- MCAP Control
- IEEE P11073 20601
- -Raw Data-

Adding, Deleting, and Saving L2CAP Parameters

1. From the Set Initial Decoder Parameters window, click on the L2CAP tab.
2. Set or select the L2CAP decoder parameters.
3. Click ont he ADD button. The Intial 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 --

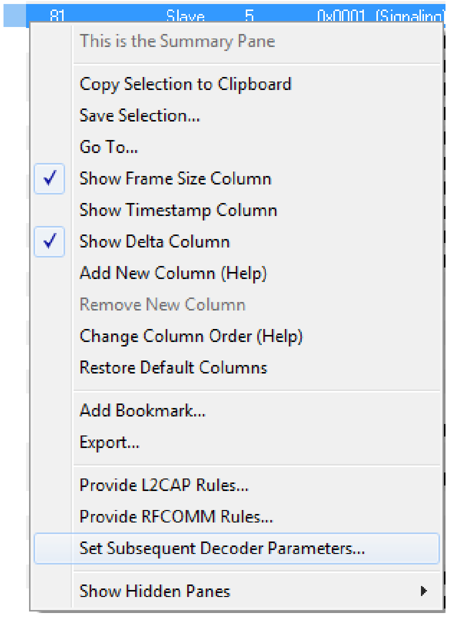
Figure 17. Parameters Added to Decoder

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 as described in Adding a New or Saving an Existing Template on page 16Adding a New or Saving an Existing Template on page 16

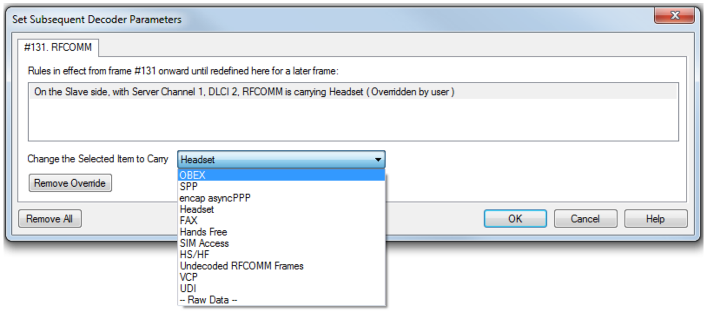
3.2.4.2 L2CAP Override Decode Information

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 Change the Selected Item to Carry drop down list.
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.


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 18. Change the Selected Items to Carry selection list

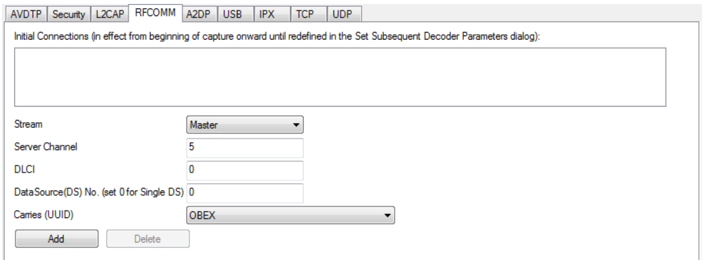
Each entry in the Set Subsequent Decoder Parameters dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

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

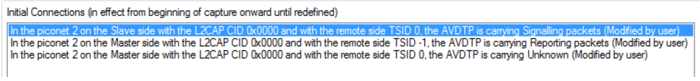
Figure 19. RFCOMM parameters tab

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 Bluetoothchannel 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 RFCOMMParameters

1. From the Set Initial Decoder Parameters window, click on the RFCOMMtab.
2. Set or select the RFCOMMdecoder parameters.
3. Click ont he 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)

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 Adding a New or Saving an Existing Template on page 16

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.

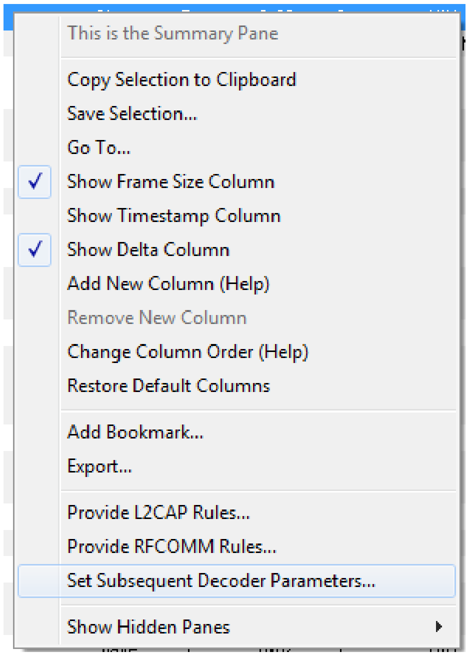
If you are not sure of the payload carried by the subject frame, look at the raw data shown under data in the Decode pane in the Frame Display. You may notice something that hints as to the profile in use.

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

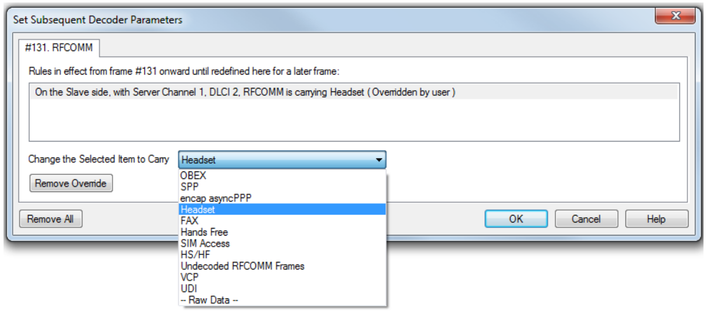
The Set Subsequent Decoder Parameters dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

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.



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 (Overidden by user)

Figure 20. 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.

Chapter 4: Capturing and Analyzing Data

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

4.1 Capture Data

4.1.1 Capturing Data to Disk

Note: Capture is not available in Viewer mode.

1. Click the Start Capture icon ● to begin capturing to a file. This icon is located on the Control, Event Display, and Frame Display windows.

   Files are placed in My Capture Files by default and have a .cfa extension. Choose Directories from the Options menu on the Control window to change the default file location.

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

2. Watch the status bar on the Control window to monitor how full the file is. When the file is full, it begins to **wrap**, which means the oldest data will be overwritten by new data.

3. Click the Stop icon ■ to temporarily stop data capture. Click the Start Capture icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured date remains in the file.

4. To clear captured data, click the Clear icon .

   - If you select Clear after selecting Stop, a dialog appears asking whether you want to save the data.
     - You can click Save File and enter a file name when prompted .
     - If you choose Do Not Save, all data will be cleared.
     - If you choose Cancel, the dialog closes with no changes.
   - If you select the Clear icon while a capture is occurring:
     - The capture stops.
     - A dialog appears asking if you want to save the capture

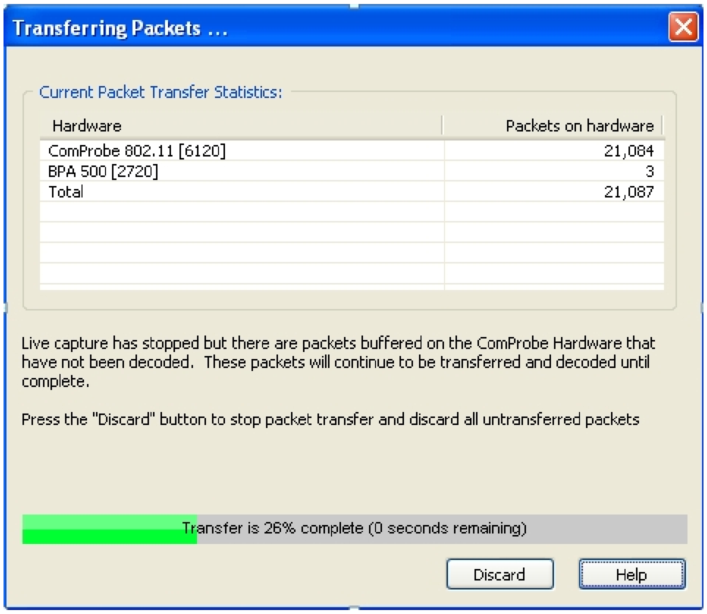
- You can select Yes and save the capture or select No and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
- If you choose Cancel, the dialog closes with no changes.

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

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.

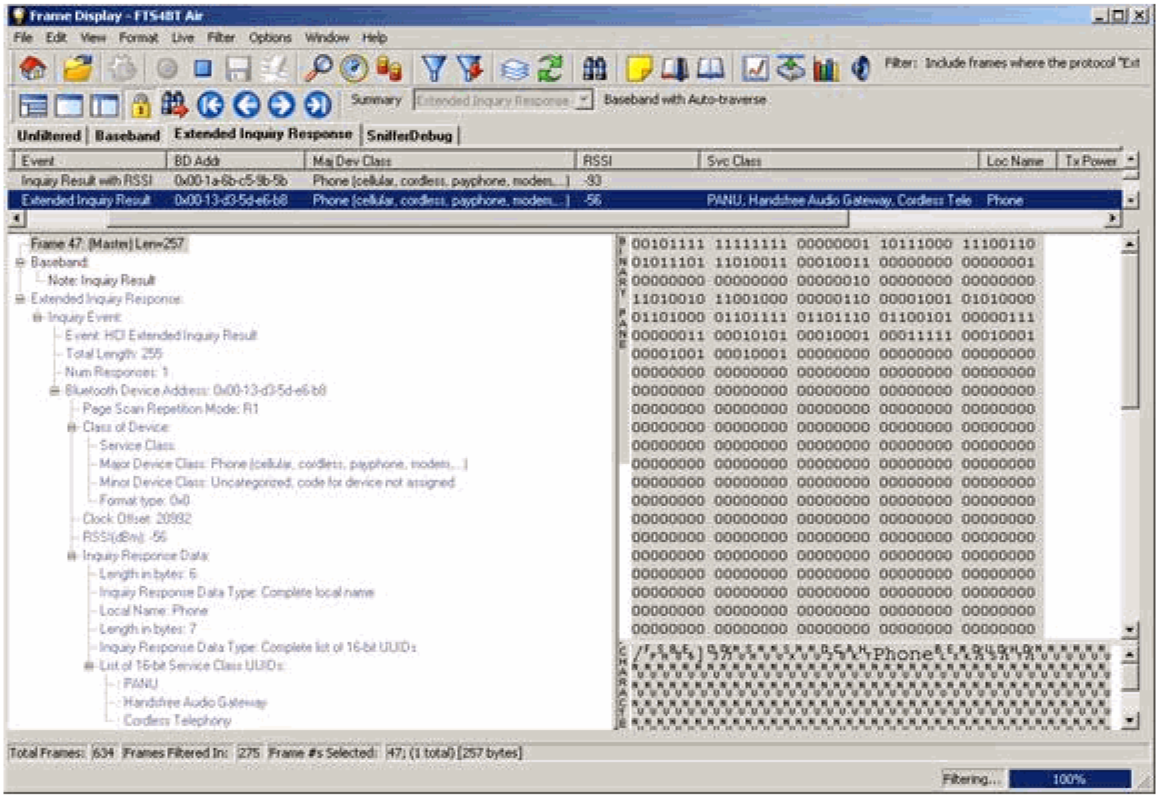
Press the "Discard" button to stop packet transfer and discard all untransferred packets

Transfer is 26% complete (0 seconds remaining)

Figure 21. Packet Transfer Dialog

4.1.2 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
Summary
Extended Inquiry Response
Unfiltered
Baseband
Extended Inquiry Response
SnifferDebug
Filtering...
100%

Filter: Include frames where the protocol "Ext

Baseband with Auto-traverse

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: 20992
      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 22. Frame Display Extended Inquire Response

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

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

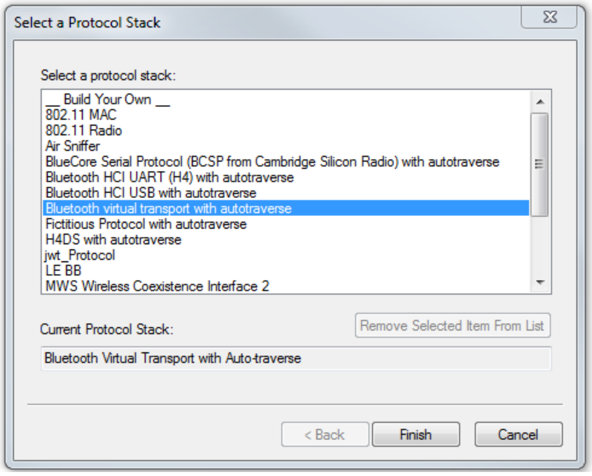
4.2 Protocol Stacks

4.2.1 Protocol Stack Wizard

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

To start the wizard:

1. Choose Protocol Stack from the Options menu on the Control window or click the Protocol Stack icon on the Frame Display.
2. Select a protocol stack from the list, and click Finish.



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

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 32.

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

If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing on page 33 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.

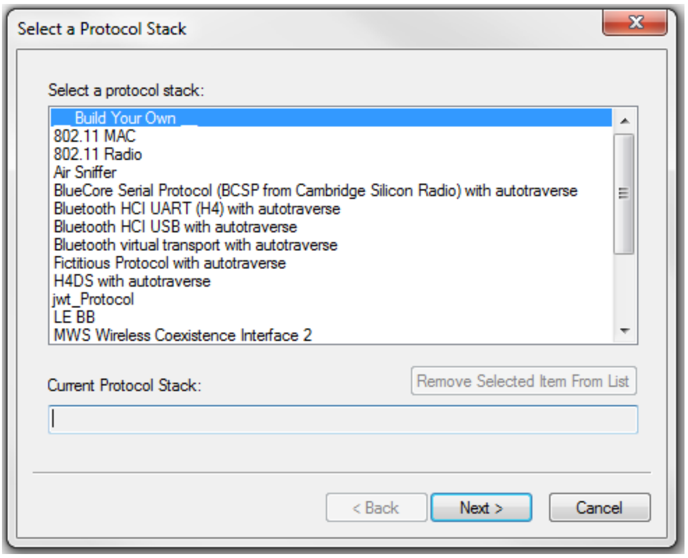
4.2.2 Creating and Removing a Custom Stack

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:

Select Protocols

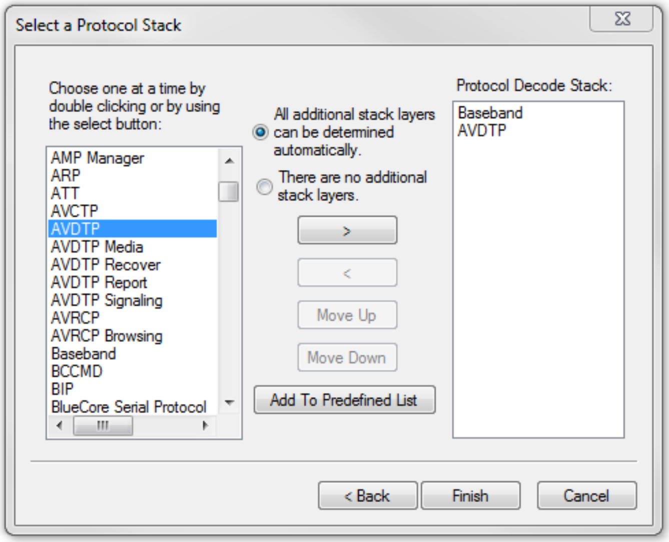
1. Select a protocol from the list on the left.

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.


Select a Protocol Stack

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

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

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

Protocol Decode Stack:

Baseband
AVDTP

Auto-traversal (Have the analyzer Determine Higher Layers)

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

1. Click the All additional stack layers can be determined automatically button.
2. If your protocol stack is complete and there are no additional layers, click the There are no additional stack layers button.
3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

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

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

Remove a Stack

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

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

4.2.3 Reframing

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

Note: You cannot reframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

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

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

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

See Unframing on page 34 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 33 for instructions on framing unframed data.

4.2.5 How the Analyzer Auto-traverses the Protocol Stack

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

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

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

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

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

4.2.6 Providing Context For Decoding When Frame Information Is Missing

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

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

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

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

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

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

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

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

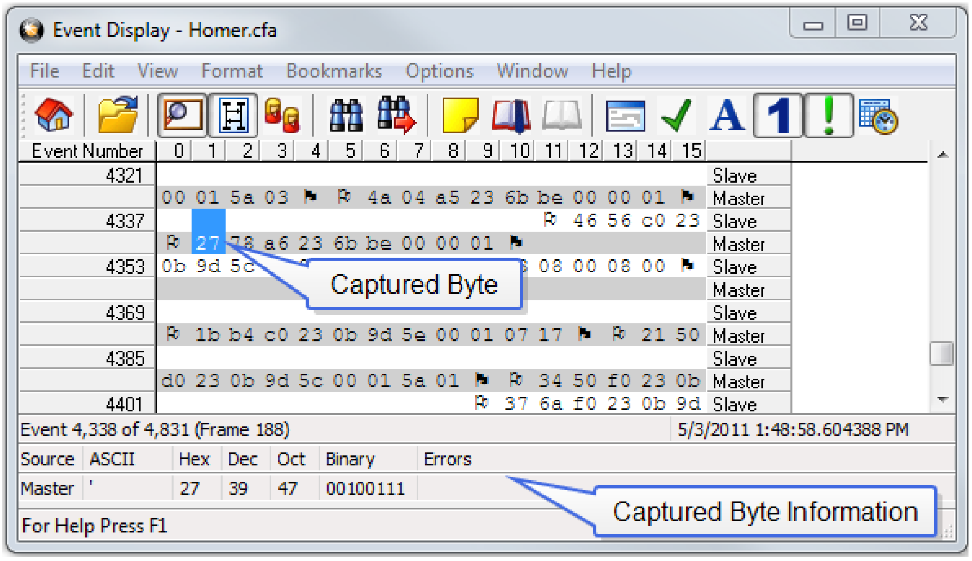
3. This option brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check Automatically Request Missing Decoding Information.
5. When unchecked, the analyzer doesn't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

4.3 Analyzing Byte Level Data

4.3.1 Event Display

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

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


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

```
Event Number | 0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 |
        4321 |                                                | Slave
             | 00 01 5a 03 ⚑  ⚐  4a 04 a5 23 6b be 00 00 01 ⚑ | Master
        4337 |                               ⚐  46 56 c0 23 | Slave
             | ⚐  27 78 a6 23 6b be 00 00 01 ⚑                | Master
        4353 | 0b 9d 5c                   3 08 00 08 00 ⚑    | Slave
             |                                                | Master
        4369 |                                                | Slave
             | ⚐  1b b4 c0 23 0b 9d 5e 00 01 07 17 ⚑  ⚐  21 50 | Master
        4385 |                                                | Slave
             | d0 23 0b 9d 5c 00 01 5a 01 ⚑  ⚐  34 50 f0 23 0b | Master
        4401 |                         ⚐  37 6a f0 23 0b 9d   | Slave
Event 4,338 of 4,831 (Frame 188)                5/3/2011 1:48:58.604388 PM
Source  ASCII   Hex  Dec  Oct  Binary    Errors
Master  '       27   39   47   00100111
For Help Press F1
```

Figure 23. Event Display

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

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

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

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

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

4.3.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Home – Brings the Control window to the front.

Start Capture - Begins data capture to disk.

Stop Capture - Closes a capture file and stops data capture to disk.

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

Clear- Discards the temporary file and clears the display.

MSC Chart - Opens the Message Sequence Chart

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3.3 Opening Multiple Event Display Windows

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

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

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

4.3.4 Calculating CRCs or FCSs

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

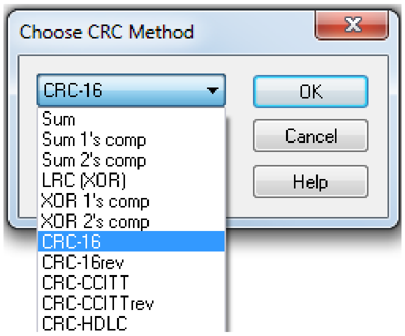
1. Open the Event Display window.
2. Click and drag to select the data for which you want to generate a CRC.

3. Click on the CRC icon ✓.

4. In the CRC dialog box, click on the down arrow to show the list of choices for CRC algorithms. Choose an algorithm to use. Choose CRC 32 (Ethernet). Choose CRC 32 (Ethernet) for Ethernet data or the appropriate CRC type for serial data.

5. Enter a Seed value in hexadecimal if desired.

6. Click OK to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC using the algorithm you selected is calculated automatically.



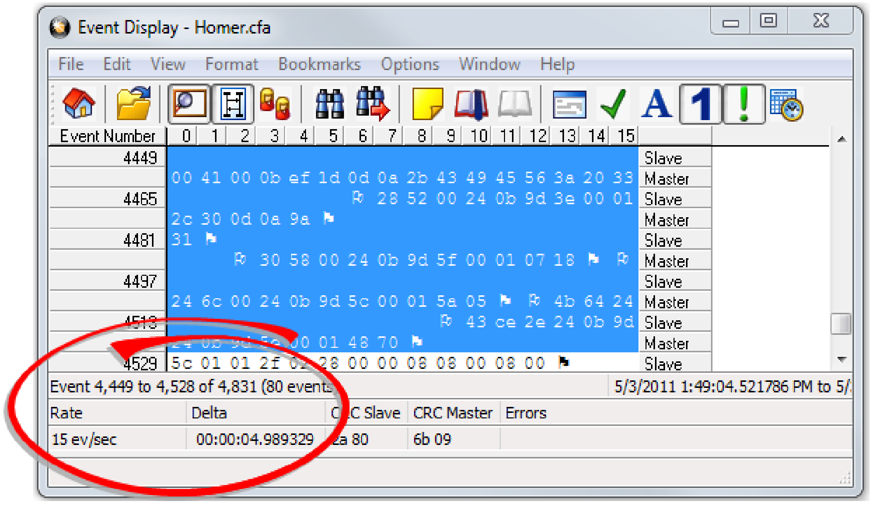
Calculating CRC for interwoven data

4.3.5 Calculating Delta Times and Data Rates

1. Click on the Event Display icon on the Control window to open the Event Display window.

2. Use the mouse to select the data you want to calculate a delta time and rate for.

3. The Event Display window displays the delta time and the data rate in the status lines at the bottom of the window.



```
Event Number  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
        4449                                                  Slave
              00 41 00 0b ef 1d 0d 0a 2b 43 49 45 56 3a 20 33 Master
        4465                    28 52 00 24 0b 9d 3e 00 01    Slave
              2c 30 0d 0a 9a                                  Master
        4481  31                                              Slave
                    30 58 00 24 0b 9d 5f 00 01 07 18          Master
        4497                                                  Slave
              24 6c 00 24 0b 9d 5c 00 01 5a 05       4b 64 24 Master
        4513                           43 ce 2e 24 0b 9d      Slave
              24 0b 9d 5e 00 01 48 70                         Master
        4529  5c 01 01 2f 02 28 00 00 08 08 00 08 00          Slave
Event 4,449 to 4,528 of 4,831 (80 events          5/3/2011 1:49:04.521786 PM to 5/
Rate          Delta              CRC Slave   CRC Master   Errors
15 ev/sec     00:00:04.989329    2a 80       6b 09
```

Figure 24. Delta fields

4.3.6 Switching Between Live Update and Review Mode

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

1. Make sure the Lock icon 🔒 is active so the display is locked and unable to scroll.
2. Click the Unlock 🔓 icon again to resume live update.

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

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

4.3.7 Data Formats and Symbols

4.3.7.1 Switching Between Viewing All Events and Viewing Data Events

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

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

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

See List of all Event Symbols on page 42 for a list of all the special events shown in the analyzer and what they mean.

4.3.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the **radix**[2] used to display data.

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

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

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

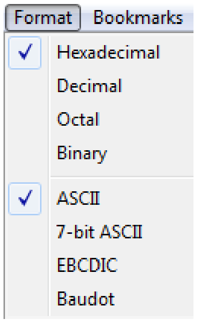


Figure 25. Format Menu

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

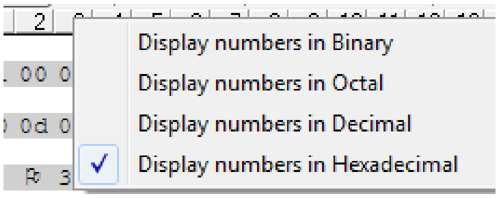

Display numbers in Binary
Display numbers in Octal
Display numbers in Decimal
✓ Display numbers in Hexadecimal

Figure 26. Header labels, right click

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

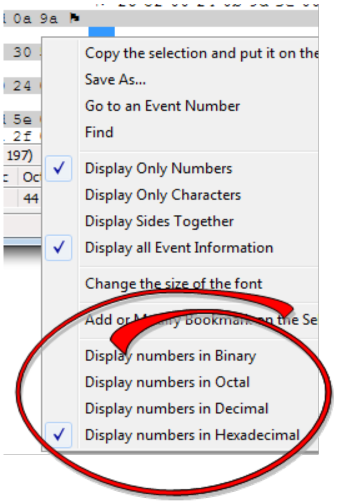

Copy the selection and put it on the
Save As...
Go to an Event Number
Find
✓ Display Only Numbers
Display Only Characters
Display Sides Together
✓ Display all Event Information
Change the size of the font
Add or Modify Bookmark on the Se
Display numbers in Binary
Display numbers in Octal
Display numbers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

Figure 27. Data display right click menu

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

4.3.7.3 Switching Between ASCII, EBCDIC, and Baudot

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

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

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

4.3.7.4 Selecting Mixed Channel/Sides

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

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

4.3.7.5 List of all Event Symbols

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

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

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

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

⊗ Abort

☒ Broken Frame - The frame did not end when the analyzer expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.

⊕ Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.

↕ Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.

☺ Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.

» Data Capture Resumed - The Pause icon was clicked again, resuming data capture.

⓪ Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.

⚑ End of Frame - Marks the end of a frame.

⏭ Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.

▶ Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.

⍓ Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.

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

≋ Long Break

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

≀ Short Break

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

Start of Frame - Marks the start of a frame.

Begin Sync Character Strip

End Sync Character Strip

Sync Dropped

Sync Found

Sync Hunt Entered

Sync Lost

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

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

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

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

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

Underrun Error

Unknown Event

4.3.7.6 Font Size

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

To change the font size:

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

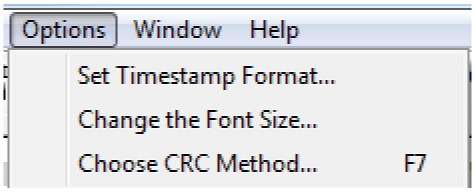


Figure 28. Event Display Options menu

2. Choose a font size from the list.

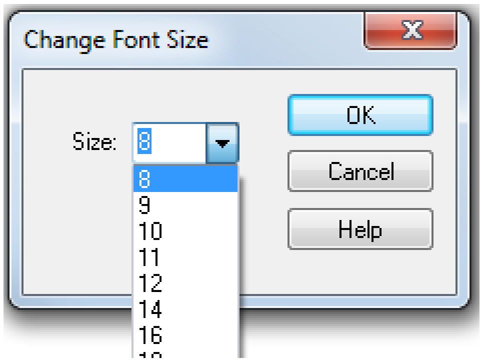


Figure 29. Event Display Font Size Selection

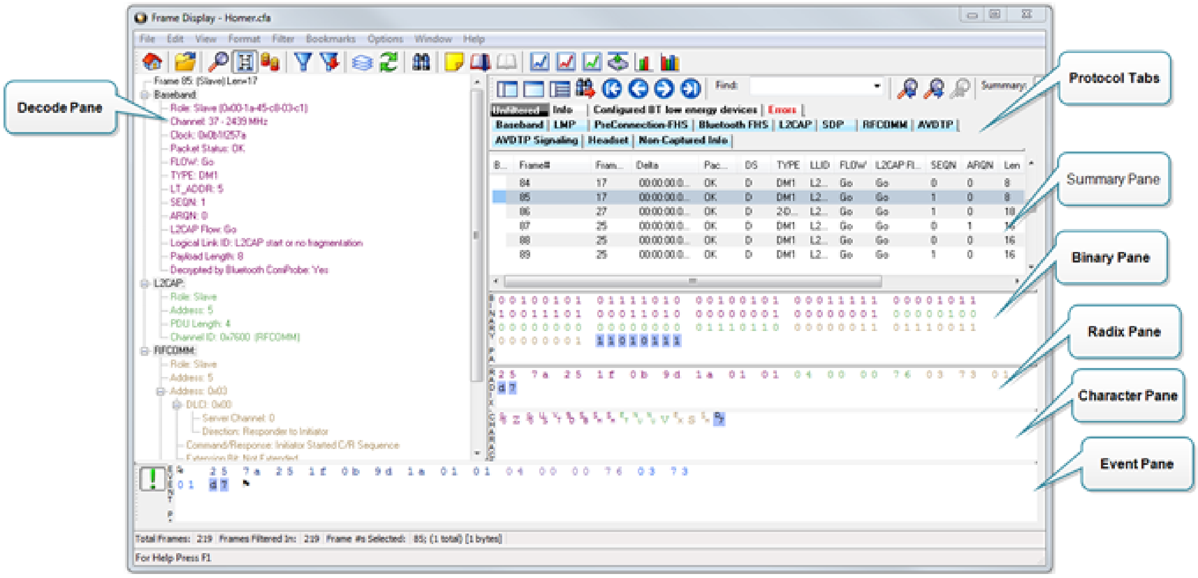
3. Click OK.

4.4 Analyzing Protocol Decodes

4.4.1 Frame Display Window

To open this window

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



Frame 85: (Slave) Len=17
- Baseband:
  - Role: Slave (0x00-1a-45-c8-03-c1)
  - Channel: 37 - 2439 MHz
  - Clock: 0x0b1f257a
  - Packet Status: OK
  - FLOW: Go
  - TYPE: DM1
  - LT_ADDR: 5
  - SEQN: 1
  - ARQN: 0
  - L2CAP Flow: Go
  - Logical Link ID: L2CAP start or no fragmentation
  - Payload Length: 8
  - Decrypted by Bluetooth ComProbe: Yes
- L2CAP:
  - Role: Slave
  - Address: 5
  - PDU Length: 4
  - Channel ID: 0x7600 (RFCOMM)
- RFCOMM:
  - Role: Slave
  - Address: 5
  - Address: 0x03
    - DLCI: 0x00
      - Server Channel: 0
      - Direction: Responder to Initiator
    - Command/Response: Initiator Started C/R Sequence
    - Extension Bit: Not Extended

Unfiltered | Info | Configured BT low energy devices | Errors |
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVDTP |
AVDTP Signaling | Headset | Non-Captured Info |

B...	Frame#	Fram...	Delta	Pac...	DS	TYPE	LLID	FLOW	L2CAP Fl...	SEQN	ARQN	Len
	84	17	00:00:00.0...	OK	D	DM1	L2...	Go	Go	0	0	8
	85	17	00:00:00.0...	OK	D	DM1	L2...	Go	Go	1	0	8
	86	27	00:00:00.0...	OK	D	2-D...	L2...	Go	Go	1	0	18
	87	25	00:00:00.0...	OK	D	DM1	L2...	Go	Go	0	1	16
	88	25	00:00:00.0...	OK	D	DM1	L2...	Go	Go	0	0	16
	89	25	00:00:00.0...	OK	D	DM1	L2...	Go	Go	1	0	16

```
00100101 01111010 00100101 00011111 00001011
10011101 00011010 00000001 00000001 00000100
00000000 00000000 01110110 00000011 01110011
00000001 11010111
```

```
25 7a 25 1f 0b 9d 1a 01 01 04 00 00 76 03 73 01
d7
```

```
25 7a 25 1f 0b 9d 1a 01 01 04 00 00 76 03 73
01 d7
```

Total Frames: 219 Frames Filtered In: 219 Frame #s Selected: 85; (1 total) [1 bytes]

For Help Press F1

Figure 30. Frame Display with all panes active

Frame Display Panes

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

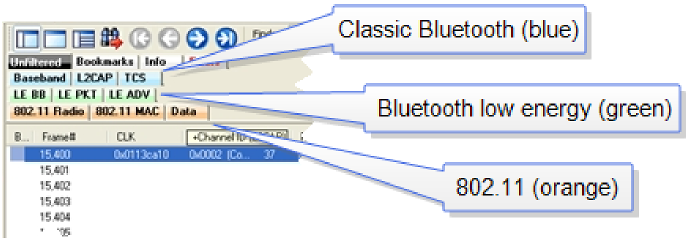
- Summary Pane - The Summary Pane displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.
- Decode Pane - The Decode Pane displays a detailed decode of the highlighted frame. Fields selected in the Decode Pane have the appropriate bit(s) or byte(s) selected in the Radix, Binary, Character , and Event panes
- Radix Pane - The Radix Pane displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.
- Binary Pane - The Binary Pane displays a binary representation of the logical data bytes.
- Character Pane - The Character Pane displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.
- Event Pane - The Event Pane displays the physical data bytes in the frame, as received on the network.

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

Protocol Tabs

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

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



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

- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.

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

Select the Unfiltered tab to display all packets.

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

- Bookmarks appear when a bookmark is first seen.

- Errors appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.

- Info appears when a frame containing an Information field is first seen.

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

Comparing Frames

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

Frame Wrapping and Display

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

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

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

- When the selected frame is still being captured, all Frame Display panes except the Summary pane display "Frame incomplete".

4.4.1.1 Frame Display Toolbar

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

Control – Brings the Control window to the front.

Open File - Opens a capture file.

I/O Settings - Opens the I/O Settings dialog.

Start Capture - Begins data capture to a user designated file.

Stop Capture - Closes a capture file and stops data capture to disk.

Save - Save the currently selected bytes or the entire buffer to file.

Clear- Discards the temporary file and clears the display.

Event Display – Brings the Event Display window to the front.

Show 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.

low energy Timeline- Opens the low energy Timeline

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.

Network View - Opens the Network View Window.

Dashboard - Opens the Dashboard Dialog

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.

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.

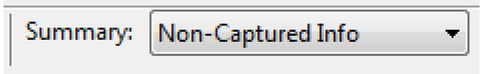
Find Previous Occurrence - Moves to the previous occurrence of the value in the Frame Display Find.

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

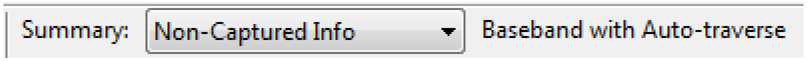
Cancel Current Search - Stops the current Frame Display Find.

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


Summary: Non-Captured Info Baseband with Auto-traverse

currently in use.

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

4.4.1.2 Frame Display Status Bar

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

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

4.4.1.3 Hiding and Revealing Protocol Layers in the Frame Display

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

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

There are two ways to hide a layer.

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

To reveal a hidden protocol layer:

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

4.4.1.4 Physical vs. Logical Byte Display

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

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

4.4.1.5 Sorting Frames

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

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

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

4.4.1.6 Frame Display - Find

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

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

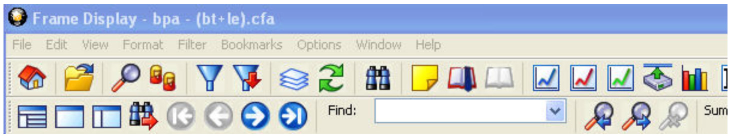
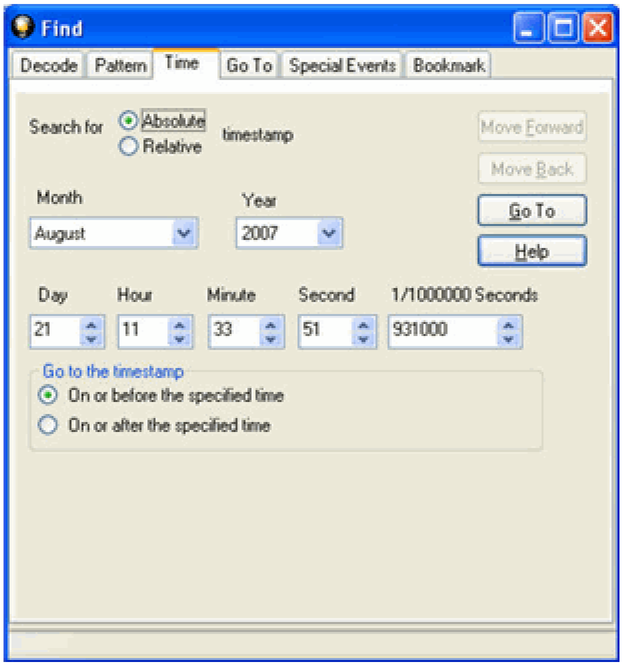

Frame Display - bpa - (bt+le).cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Sum

Figure 31. 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.,



Find

Decode | Pattern | Time | Go To | Special Events | Bookmark

Search for ● Absolute ○ Relative timestamp

Month: August

Year: 2007

Day: 21

Hour: 11

Minute: 33

Second: 51

1/1000000 Seconds: 931000

Go to the timestamp

● On or before the specified time

○ On or after the specified time

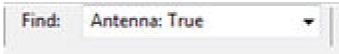
Figure 32. Searh/Find Dialog

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.

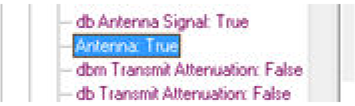
2. Enter a value in the Find text box.



Find: Antenna: True

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

Select Find Previous Occurrence3 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.



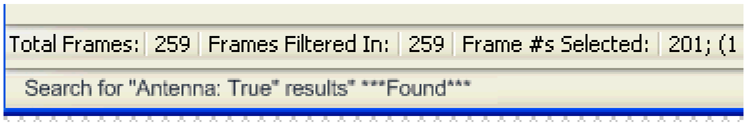
db Antenna Signal: True
Antenna: True
dbm Transmit Attenuation: False
db Transmit Attenuation: False

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.

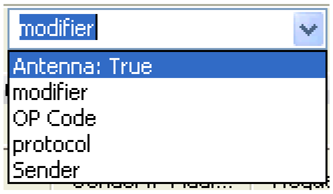
- When you enter a search string and select Enter, the search moves forward.
- If you select Find Previous Occurrence, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous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

4.4.1.7 Synchronizing the Event and Frame Displays

The Frame Display is synchronized with the Event Display. Click on a frame in the Frame Display and the corresponding bytes is highlighted in the Event Display. Each Frame Display has its own Event Display.

As an example, here's what happens if the following sequence of events occurs.

1. Click on the Frame Display icon in Control window toolbar to open the Frame Display.
2. Click on the Duplicate View icon to create Frame Display #2.
3. Click on Event Display icon in Frame Display #2. Event Display #2 opens. This Event Display is labeled #2, even though there is no original Event Display, to indicate that it is synchronized with Frame Display #2.

4. Click on a frame in Frame Display #2. The corresponding bytes are highlighted in Event Display #2.

5. Click on a frame in the original Frame Display. Event Display #2 does not change.

4.4.1.8 Working with Multiple Frame Displays

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset or two filtered subsets against each other.

- To create a second Frame Display, click the Duplicate View icon on the Frame Display toolbar.

  This creates another Frame Display window. You can have as many Frame Displays open as you wish. Each Frame Display is given a number in the title bar to distinguish it from the others.

- To navigate between multiple Frame Displays, click on the Frame Display icon in the Control window toolbar.

  A drop-down list appears, listing all the currently open Frame Displays.

- Select the one you want from the list and it comes to the front.

Note: When you create a filter in one Frame Display, that filter does not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

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

4.4.1.9 Working with Panes on Frame Display

When the Frame Display first opens, all panes are displayed except the Event pane (To view all the panes, select Show All Panes from the View menu).

- The Toggle Expand Decode Pane icon makes the decode pane longer to view lengthy decodes better.

- The Show Default Panes icon returns the Frame Display to its default settings.

- The Show only Summary Pane icon displays on the Summary Pane.

To close a pane, right-click on the pane and select Hide This Pane from the pop-up menu, or de-select Show [Pane Name] from the View menu.

To open a pane, right-click on the any pane and select Show Hidden Panes from the pop-up menu and select the pane from the fly-out menu, or select Show [Pane Name] from the View menu.

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

4.4.1.10 Frame Display - Byte Export

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

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

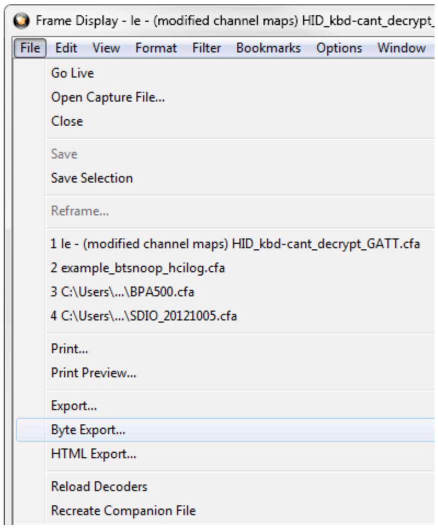
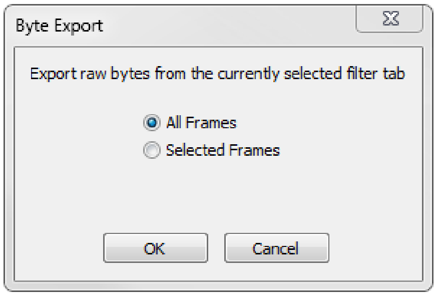

Frame Display - le - (modified channel maps) HID_kbd-cant_decrypt_
File
Edit
View
Format
Filter
Bookmarks
Options
Window
Go Live
Open Capture File...
Close
Save
Save Selection
Reframe...
1 le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa
2 example_btsnoop_hcilog.cfa
3 C:\Users\...\BPA500.cfa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

Figure 33. 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

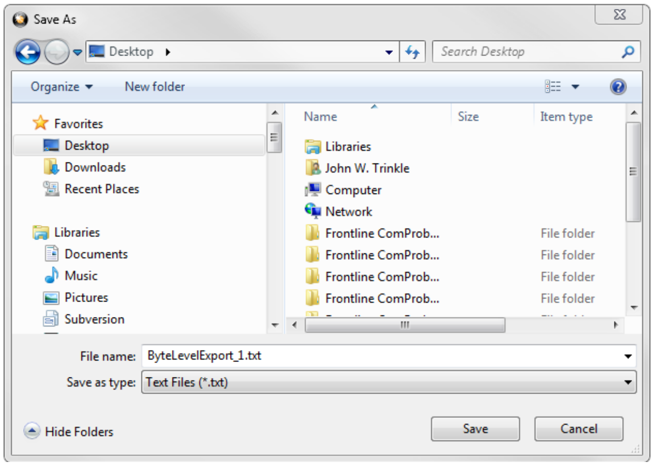
Export raw bytes from the currently selected filter tab

● All Frames
○ Selected Frames

Figure 34. 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.



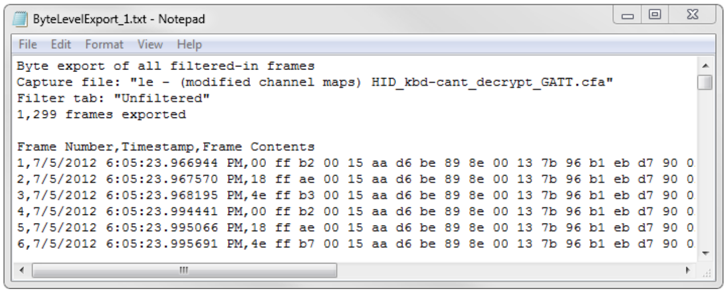
File name: ByteLevelExport_1.txt

Save as type: Text Files (*.txt)

Figure 35. Save As dialog

Click on the Save button.

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



```
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 36. Sample Exported Frames Text File

4.4.1.11 Panes in the Frame Display

4.4.1.11.1 Summary Pane

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

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

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

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

Protocol Tabs

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

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

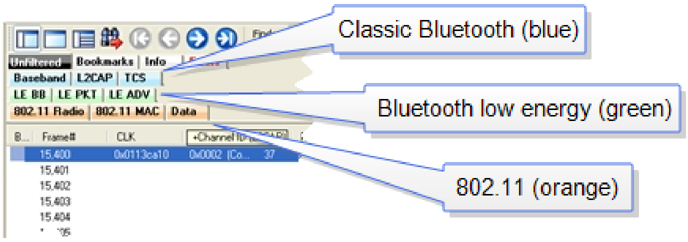


Figure 37. Example Protocol Tags

- 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:

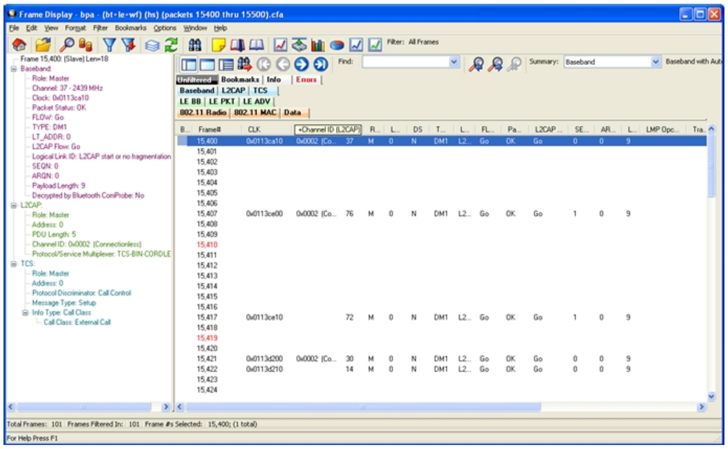
- Bookmarks appear when a bookmark is first seen.
- Errors appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- Info appears when a frame containing an Information field is first seen.

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 - bpa - (bt+le+wf) (hs) (packets 15400 thru 15500).cfa
File Edit View Format Filter Bookmarks Options Window Help
Filter: All Frames
Find:
Summary: Baseband
Baseband with Aut
Unfiltered Bookmarks Info Errors
Baseband L2CAP TCS
LE BB LE PKT LE ADV
802.11 Radio 802.11 MAC Data

```
Frame 15,400: (Slave) Len=18
⊟ Baseband:
    Role: Master
    Channel: 37 - 2439 MHz
    Clock: 0x0113ca10
    Packet Status: OK
    FLOW: Go
    TYPE: DM1
    LT_ADDR: 0
    L2CAP Flow: Go
    Logical Link ID: L2CAP start or no fragmentation
    SEQN: 0
    ARQN: 0
    Payload Length: 9
    Decrypted by Bluetooth ComProbe: No
⊟ L2CAP:
    Role: Master
    Address: 0
    PDU Length: 5
    Channel ID: 0x0002 (Connectionless)
    Protocol/Service Multiplexer: TCS-BIN-CORDLE
⊟ TCS:
    Role: Master
    Address: 0
    Protocol Discriminator: Call Control
    Message Type: Setup
  ⊟ Info Type: Call Class
      Call Class: External Call
```

B...	Frame#	CLK	+Channel ID (L2CAP)		R...	L...	DS	T...	L...	FL...	Pa...	L2CAP ...	SE...	AR...	L...	LMP Opc...	Tra...
	15,400	0x0113ca10	0x0002 (Co...	37	M	0	N	DM1	L2...	Go	OK	Go	0	0	9		
	15,401																
	15,402																
	15,403																
	15,404																
	15,405																
	15,406																
	15,407	0x0113ce00	0x0002 (Co...	76	M	0	N	DM1	L2...	Go	OK	Go	1	0	9		
	15,408																
	15,409																
	15,410																
	15,411																
	15,412																
	15,413																
	15,414																
	15,415																
	15,416																
	15,417	0x0113ce10		72	M	0	N	DM1	L2...	Go	OK	Go	1	0	9		
	15,418																
	15,419																
	15,420																
	15,421	0x0113d200	0x0002 (Co...	30	M	0	N	DM1	L2...	Go	OK	Go	0	0	9		
	15,422	0x0113d210		14	M	0	N	DM1	L2...	Go	OK	Go	0	0	9		
	15,423																
	15,424																

Total Frames: 101 Frames Filtered In: 101 Frame #s Selected: 15,400; (1 total)

For Help Press F1

Figure 38. Summay pane (right) with Decoder pane (left)

Sides in *Bluetooth* low energy

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

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

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

If no packets in the connection event are missed by the sniffer, the device labeled ‘1’ is the master and the device labeled ‘2’ is the slave. However, if we do not capture the very first packet in a connection event (i.e.

the packet sent by the master) but do capture the packet sent by the slave, we label the slave as side ‘1’ since it is the first device we heard in the connection event. Because there is potential clock drift since the last connection event, we cannot use the absolute timing to correct this error; there would still be cases where we get it wrong. Therefore we always assign ‘1’ to the first packet in a connection event. So even though it is rare, there are connection events where packets sent by the slave device are labeled ‘1’ and packets sent by the master are labeled ‘2’.

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

4.4.1.11.2 Customizing Fields in the Summary Pane

You can modify the Summary Pane in Frame Display.

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

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

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

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

Changing Column Widths

To change the width of a column:

1. Place the cursor over the right column divider until the cursor changes to a solid double arrow.
2. Click and drag the divider to the desired width.
3. To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column:

1. Drag the right divider of the column all the way to the left.
2. The cursor changes to a split double arrow when a hidden column is present.
3. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.
4. The Frame Size, Timestamp, and Delta columns can be hidden by right-clicking on the header and selecting Show Frame Size Column, Show Timestamp Column, or Show Delta Column. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column :

1. Click and hold on the column header
2. Drag the mouse over the header row.
3. A small white triangle indicates where the column is moved to.
4. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations, their default widths, and show any hidden columns

1. Right-click on any column header and choose Restore Default Column Widths, or select Restore Default Column Widths from the Format menu.

4.4.1.11.3 Frame Symbols in the Summary Pane

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

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

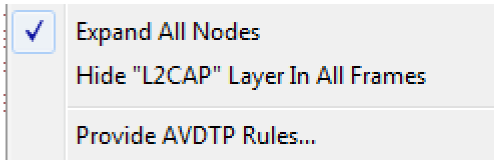
- One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for the analyzer to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If the analyzer is busy capturing data, frame compilation may fall behind. When the analyzer catches up, the green circle changes to either a green dot or no dot.

- Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has changed. If the analyzer does not capture the first frame with the complete header, it cannot decode subsequent frames with partial header information.

▶ A magenta triangle indicates that a bookmark is associated with this frame. Any comments associated with the bookmark appear in the column next to the bookmark symbol.

4.4.1.11.4 Decode Pane

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



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

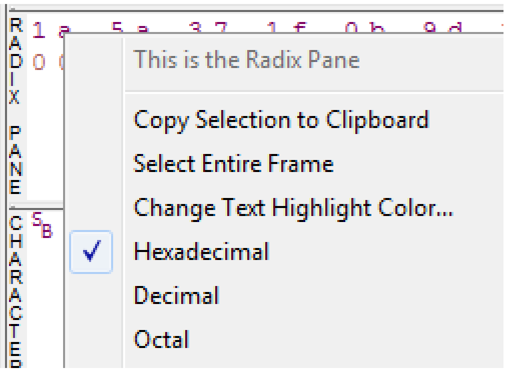
Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the Event, Radix, Binary and Character panes. The colors are not assigned to a protocol, but are assigned to the layer.

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

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

4.4.1.11.5 Radix or Hexadecimal Pane

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



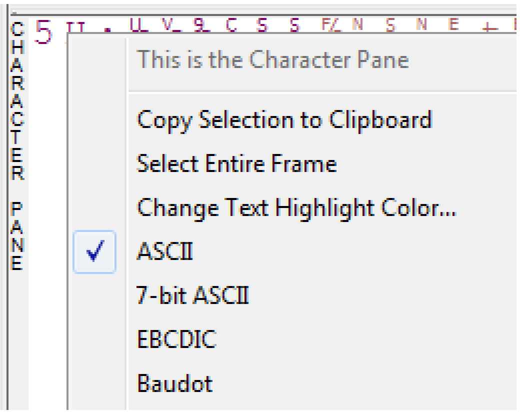
Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

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

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

4.4.1.11.6 Character Pane

The Character pane represents the logical bytes in the frame in ASCII, EBCDIC or Baudot. The character set can be changed from the Format menu, or by right-clicking on the pane and choosing the appropriate character set.


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

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

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

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

4.4.1.11.7 Binary Pane

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

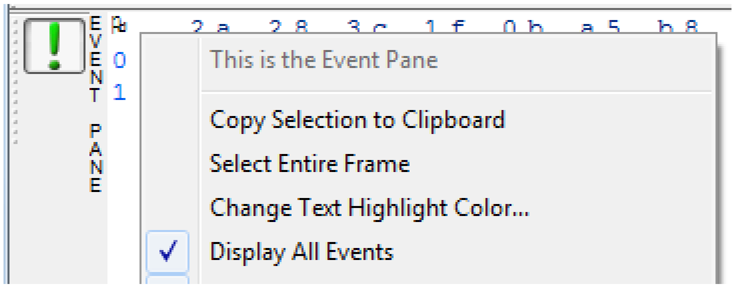
Because the Binary pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

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

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

4.4.1.11.8 Event Pane

The Event pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the All Events icon !.



Displaying all events means that special events, such as Start of Frame, End of Frame and any signal change events, are displayed as special symbols within the data.

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

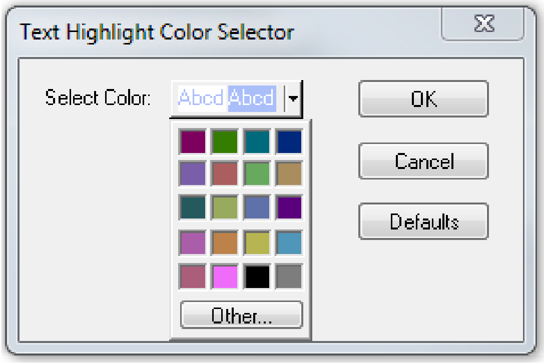
Because the Event pane displays the physical bytes rather than the logical bytes, the data in the Event pane may be different from that in the Radix, Binary and Character panes. See Physical vs. Logical Byte Display for more information.

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

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

4.4.1.11.9 Change Text Highlight Color

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



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

The highlight color for the text is changed.

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

4.4.1.12 Protocol Layer Colors

4.4.1.12.1 Data Byte Color Notation

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

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

4.4.1.12.2 Changing Protocol Layer Colors

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

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

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

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

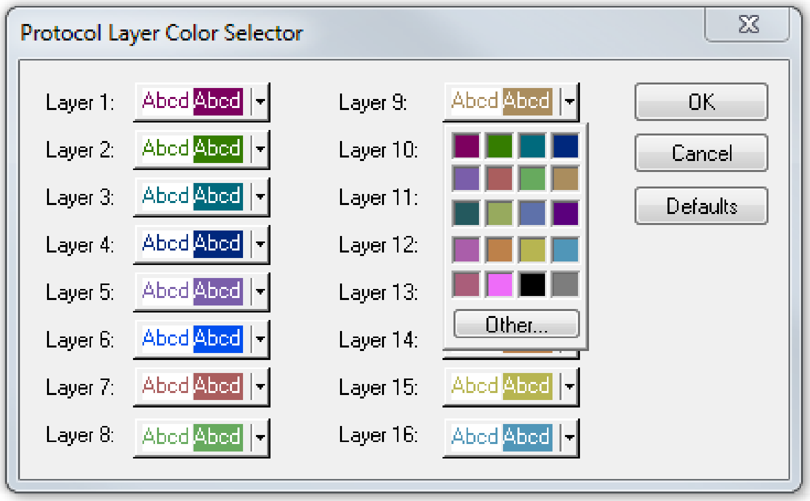
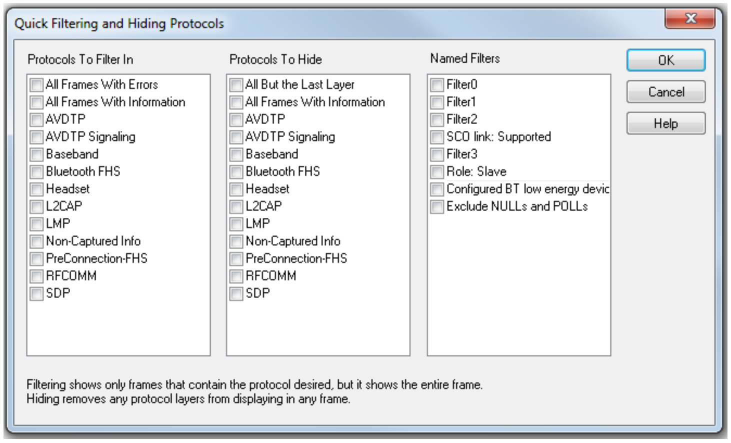


Figure 39. Frame Display Protocol Layer Color Selector

4.4.1.13 Protocol Filtering From the Frame Display

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.



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

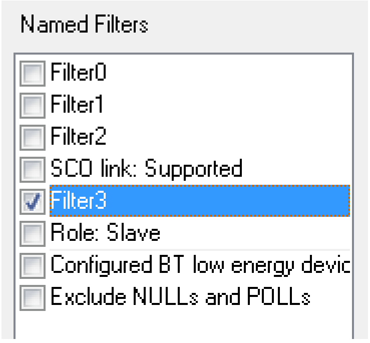
Filtering shows only frames that contain the protocol desired, but it shows the entire frame.
Hiding removes any protocol layers from displaying in any frame.

Figure 40. 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

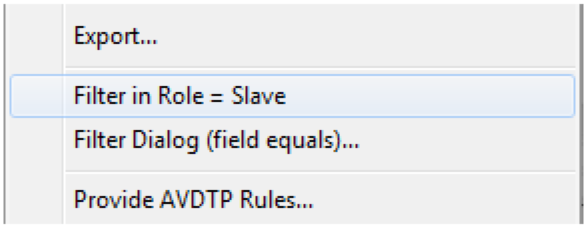
4.4.1.13.1 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary pane using the Filtering Results dialog.

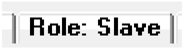
Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:



1. Right-click on a value in the Summary pane. For example, the "S" for Slave under Role
2. On the drop-down list select Filter in name = value, where name is the column name and value is the column-value to filter. For our example "Filter in Role = Slave" appears in the menu.

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



A new protocol tab with the "Filter Name" you just created appears in the Summary pane. The new tab displays data specific to the layer you selected.

4.4.1.13.1.1 Filtering On the Summary Layer Protocol

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

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

4.4.1.13.1.2 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

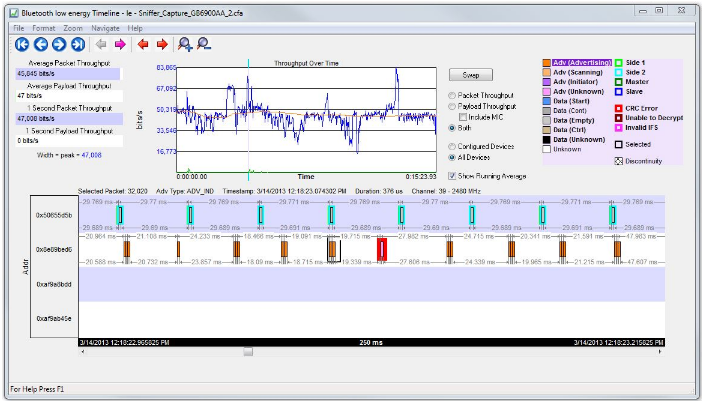
1. Open the Frame Display window.
2. Click the starred Quick Filter icon or select Quick Filtering from the Filter menu
3. Check the box for All Frames With Errors in the Protocols To Filter In pane, and click OK.
4. The system creates a tab on the Frame Display labeled "Errors" that displays the results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

4.4.2 low energy Timeline

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

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



Bluetooth low energy Timeline - le - Sniffer_Capture_GB6900AA_2.cfa

File Format Zoom Navigate Help

Average Packet Throughput: 45,845 bits/s

Average Payload Throughput: 47 bits/s

1 Second Packet Throughput: 47,008 bits/s

1 Second Payload Throughput: 0 bits/s

Width = peak = 47,008

○ Packet Throughput
○ Payload Throughput
□ Include MIC
● Both

○ Configured Devices
● All Devices

☑ Show Running Average

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

3/14/2013 12:18:22.965825 PM 250 ms 3/14/2013 12:18:23.215825 PM

For Help Press F1

Figure 41. *Bluetooth* low energy Timeline

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

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

4.4.2.1 low energy Timeline Toolbar

The toolbar 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 Interframe Spacing (IFS) Error

- Interframe Spacing is considered valid if it is within 150 µs + or – 2us
- If the Interframe Spacing is less than 148 us or greater than 152 us but less than or equal to 300 µs, it is considered an IFS error.

Next Interframe Spacing (IFS) Error

- Interframe Spacing is considered valid if it is within 150 µs + or – 2us
- If the Interframe Spacing is less than 148 us or greater than 152 µs but less than or equal to 300 us, it is considered an IFS error.

Previous Error Packet

Next Error Packet

Zoom In

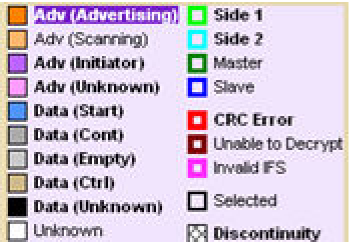
Zoom Out

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

4.4.2.2 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.



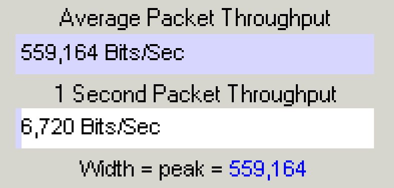
🟧 **Adv (Advertising)**
🟧 Adv (Scanning)
🟪 **Adv (Initiator)**
🟪 **Adv (Unknown)**
🟦 **Data (Start)**
■ **Data (Cont)**
■ **Data (Empty)**
■ **Data (Ctrl)**
■ **Data (Unknown)**
□ Unknown

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

4.4.2.3 Throughput Displays

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

4.4.2.3.1 Average and 1 Second Packet Throughput



Average Packet Throughput

559,164 Bits/Sec

1 Second Packet Throughput

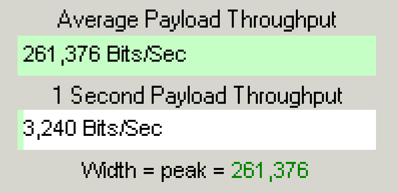
6,720 Bits/Sec

Width = peak = 559,164

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

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

4.4.2.3.2 Average and 1 Second Payload Throughput



Average Payload Throughput

261,376 Bits/Sec

1 Second Payload Throughput

3,240 Bits/Sec

Width = peak = 261,376

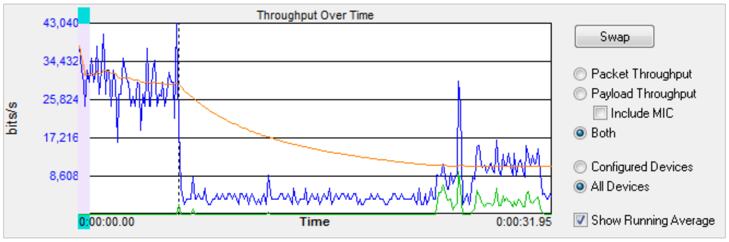
The figure depicts the Average and One Second Payload Throughput display. This display appears when you select the Payload Throughput radio button.

- Average Payload Throughput is the total payload over the entire session divided by the total time.
- 1-second Payload Throughputis 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.

4.4.2.3.3 Throughput Graph

The following figure depicts the Throughput Graph.



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

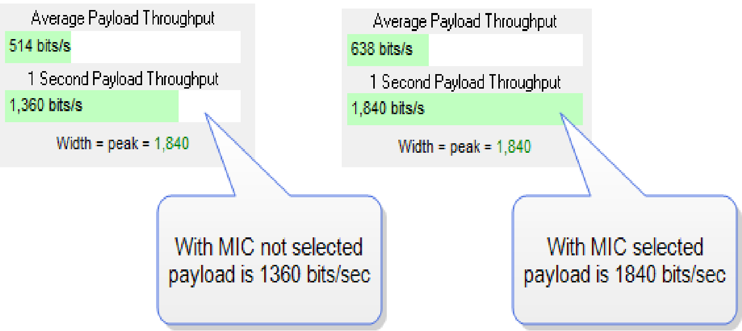
Figure 42. Bluetooth low energy Timeline Throughput Graph

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

Selecting Throughput Display

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

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



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

With MIC not selected payload is 1360 bits/sec

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

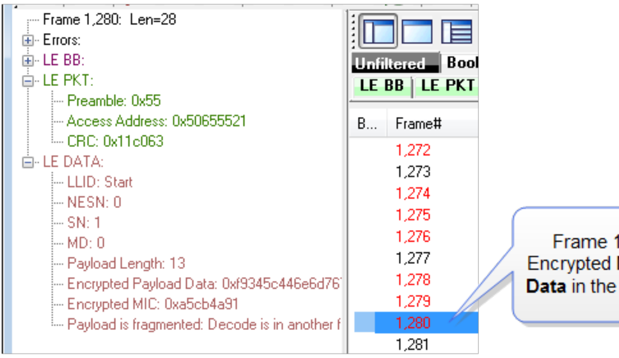
With MIC selected payload is 1840 bits/sec

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

T-

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

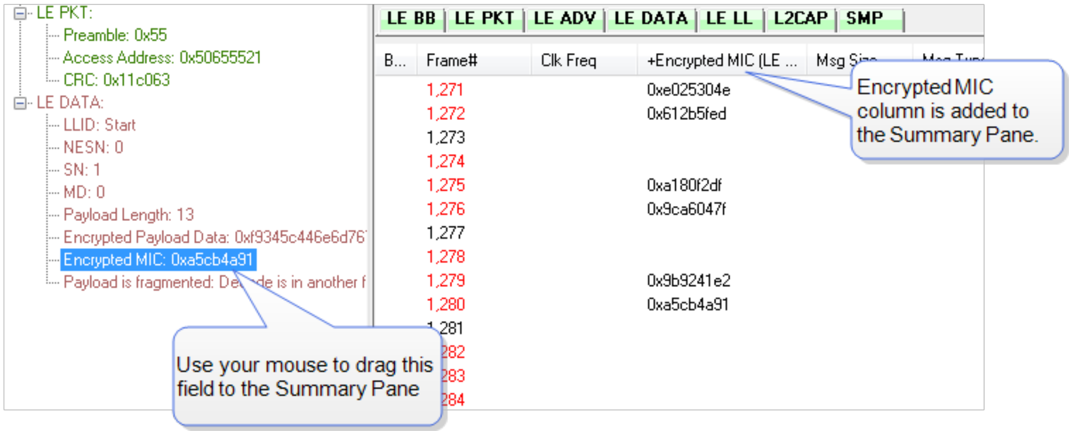
1. Using the Decoder pane scroll through the frames until LE Data shows "Encrypted MIC".
2. Place the cursor on the Encrypted MIC data and while holding the left mouse button drag the field to the Summary pane.
3. An Encrypted MIC column is added to the Summary pane.



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 1
Encrypted
Data in the



- 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 Typ
	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 43. Creating Encrypted MIC in Frame Display Summary pane

- Selecting Both displays both Packet and Payload Throughput. The y-axis numbers appear in blue. In the Throughput Graph packets appears as:
- Packet Throughput = Blue
- Payload Throughput = Green
- Selecting Configured Devices: Dispalays data from configured devices.The low energy Timeline considers a packet to be from a configured device if:
  1. The packet has an LE ADV layer and field "Meets Predefined Filter Criteria for BT low energy devices" == "Yes" in the LE BB layer,
  2. or the packet has anLE DATA layer.
- Selecting All Devices displays data from all available devices.

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 is 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.

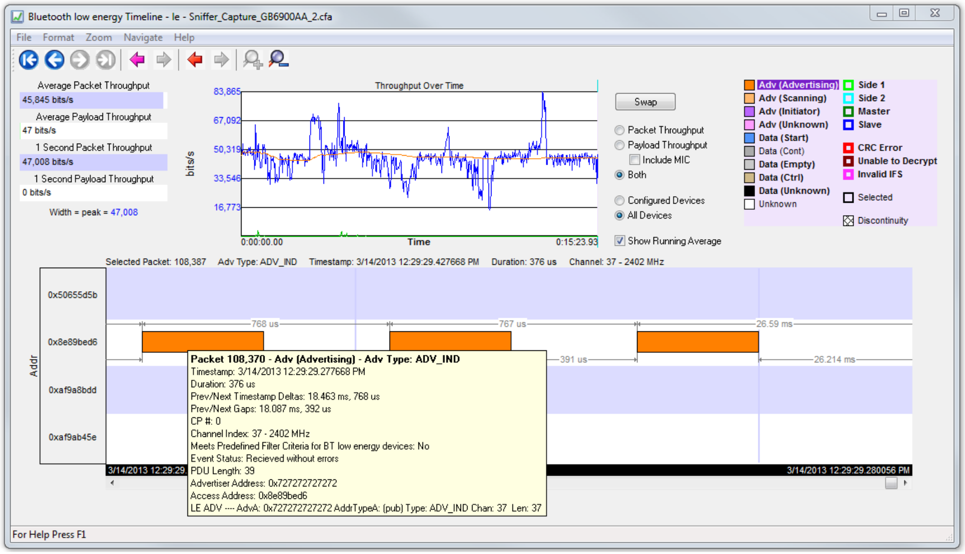
Discontinuities are indicated by vertical dashed lines.

A purple viewport indicates the time range corresponding to the visible timeline. The viewport can be moved by clicking elsewhere in the graph or by dragging it. Whenever it is moved, the timeline scrolls to match. When the timestamp range in the timeline changes, the viewport moves and resizes as necessary to match.

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

4.4.2.4 The Timeline

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



Average Packet Throughput
45,845 bits/s

Average Payload Throughput
47 bits/s

1 Second Packet Throughput
47,008 bits/s

1 Second Payload Throughput
0 bits/s

Width = peak = 47,008

○ Packet Throughput
○ Payload Throughput
□ Include MIC
● Both

○ Configured Devices
● All Devices

☑ Show Running Average

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

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

Figure 44. *Bluetooth*low energy Timeline

4.4.2.4.1 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.

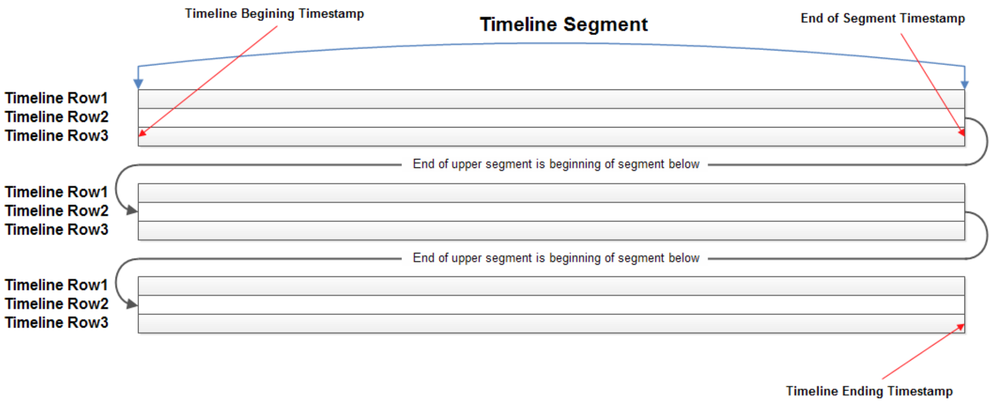
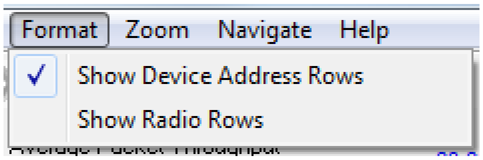


Figure 45. Diagram of low energy Timeline Flow with Segment and Row Relationship

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

4.4.2.4.2 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.

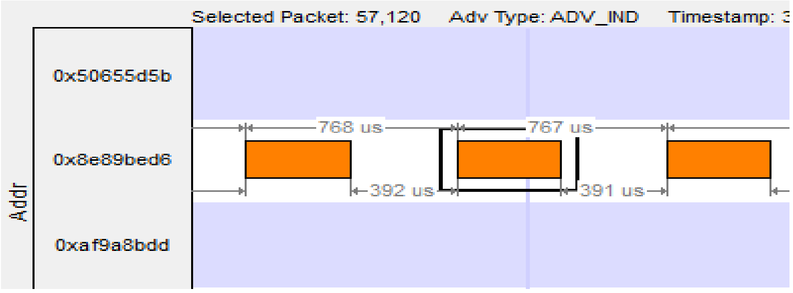


Figure 46. Device Address Rows

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

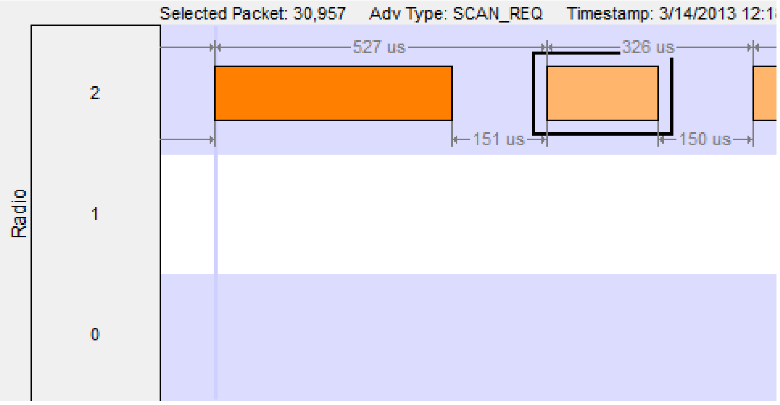
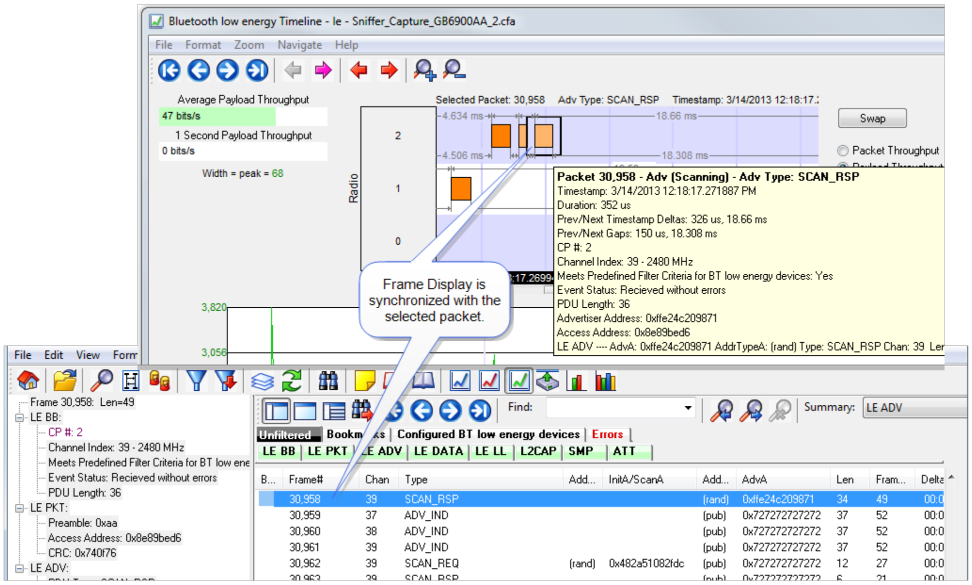

Selected Packet: 30,957 Adv Type: SCAN_REQ Timestamp: 3/14/2013 12:1
527 us
326 us
151 us
150 us
Radio
2
1
0

Figure 47. Radio Rows

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


Bluetooth low energy Timeline - le - Sniffer_Capture_GB6900AA_2.cfa
File Format Zoom Navigate Help
Average Payload Throughput
47 bits/s
1 Second Payload Throughput
0 bits/s
Width = peak = 68
Selected Packet: 30,958 Adv Type: SCAN_RSP Timestamp: 3/14/2013 12:18:17.
4.634 ms
18.66 ms
4.506 ms
18.308 ms
Radio
2
1
0
Swap
○ Packet Throughput
3,820
3,056
:17.2699
Frame Display is synchronized with the selected packet.
File Edit View Form
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

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

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

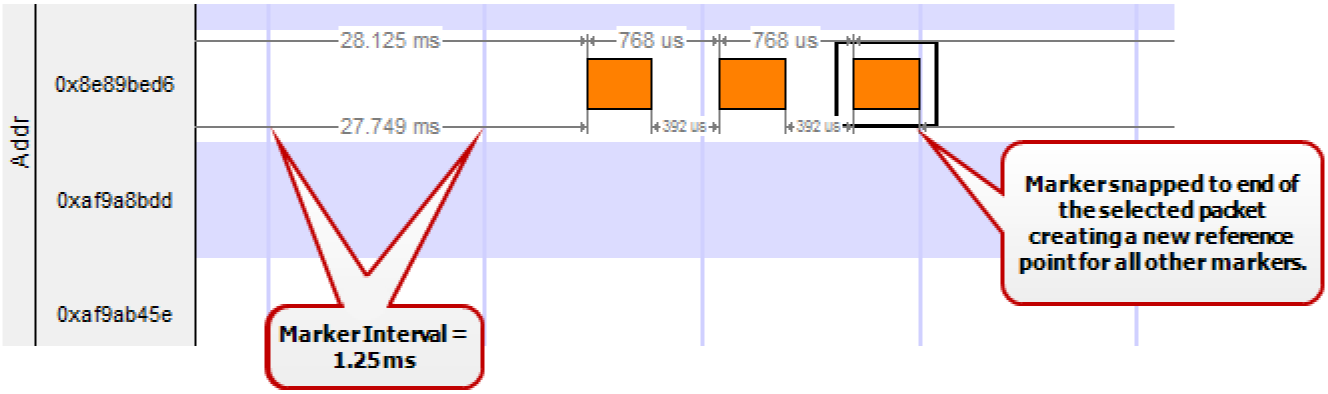
B...	Frame#	Chan	Type	Add...	InitA/ScanA	Add...	AdvA	Len	Fram...	Delta
	30,958	39	SCAN_RSP			(rand)	0xffe24c209871	34	49	00:0
	30,959	37	ADV_IND			(pub)	0x727272727272	37	52	00:0
	30,960	38	ADV_IND			(pub)	0x727272727272	37	52	00:0
	30,961	39	ADV_IND			(pub)	0x727272727272	37	52	00:0
	30,962	39	SCAN_REQ	(rand)	0x482a51082fdc	(pub)	0x727272727272	12	27	00:0
	30,963	39	SCAN_RSP			(pub)	0x727272727272	6	21	00:0

Figure 48. low energy Timeline and Frame Display Packet Synchronization

4.4.2.5 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.



Marker Interval = 1.25ms

Marker snapped to end of the selected packet creating a new reference point for all other markers.

Figure 49. Timeline Markers Shown Snapped to End of Packet

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

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

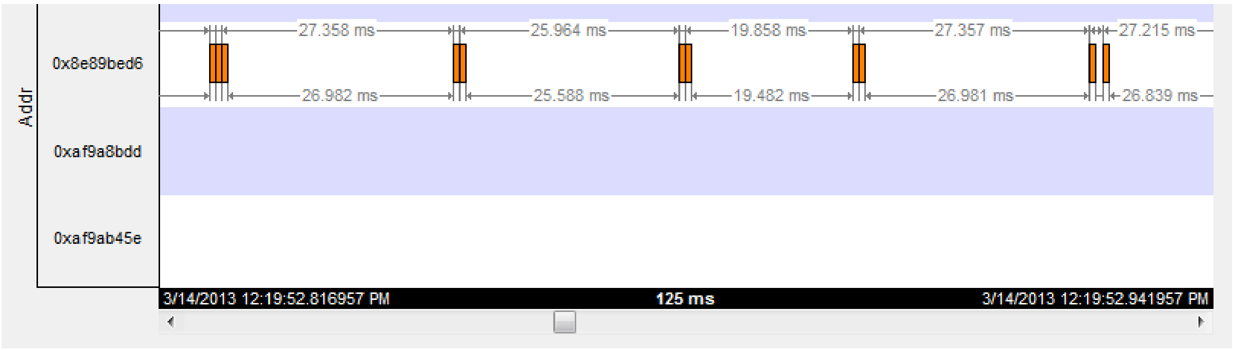
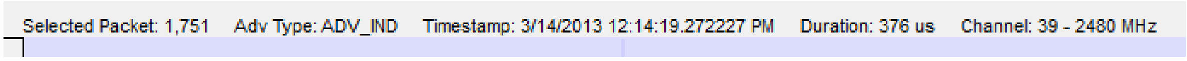


Figure 50. Bluetooth le Timeline Segment Timestamp and Zoom Value

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

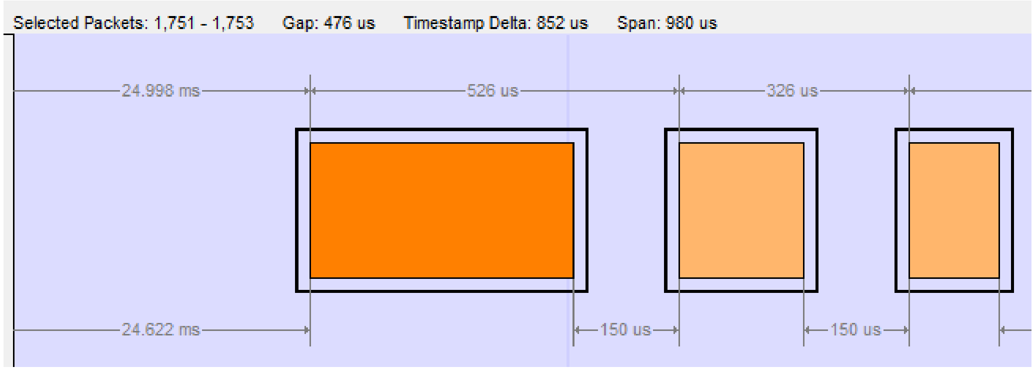
- Packet Info Line - The packet info line appears just above the timeline and displays information for the currently selected packet.



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

Figure 51. Bluetooth le Timeline Packet Info Line

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



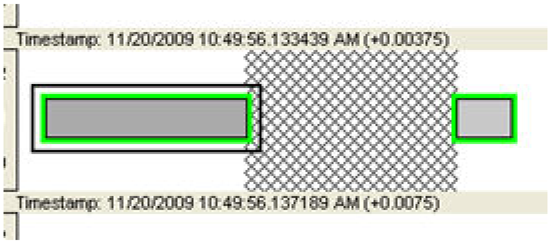
Selected Packets: 1,751 - 1,753 Gap: 476 us Timestamp Delta: 852 us Span: 980 us

Figure 52. Bluetooth le Timeline Packet Info Line for Multiple Selected Packets

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

4.4.2.6 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 53. Bluetooth low energy Packet Discontinuity

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

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

4.4.2.7 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.

4.4.2.8 le Timeline Zooming

Zoom features can be accessed from the Bluetooth low energy Timeline Zoom menuor 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 inthe 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 numbr of segments. For example: :"(Contiguous time segment 2/3)".

4.4.2.8.1 Zoom menu

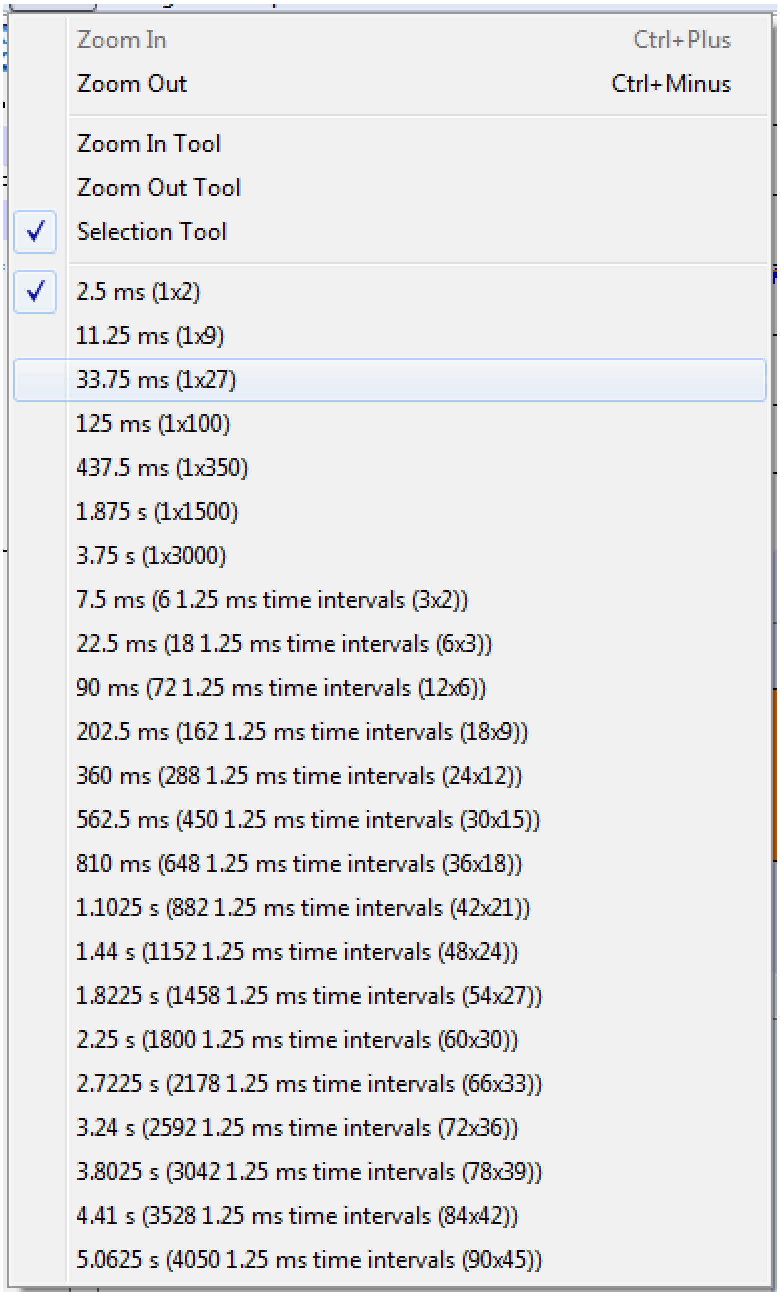
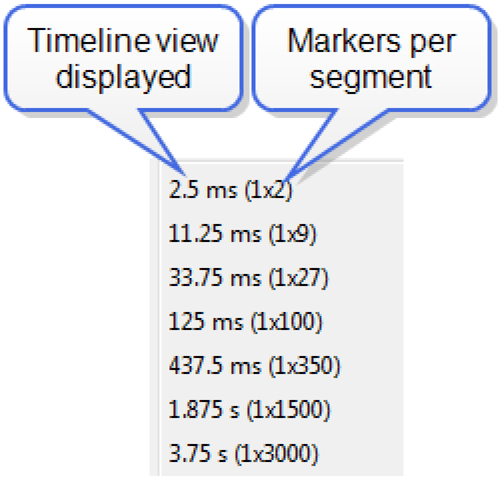

Zoom In Ctrl+Plus
Zoom Out Ctrl+Minus
Zoom In Tool
Zoom Out Tool
✓ Selection Tool
✓ 2.5 ms (1x2)
11.25 ms (1x9)
33.75 ms (1x27)
125 ms (1x100)
437.5 ms (1x350)
1.875 s (1x1500)
3.75 s (1x3000)
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (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 54. low energy Timeline Zoom menu

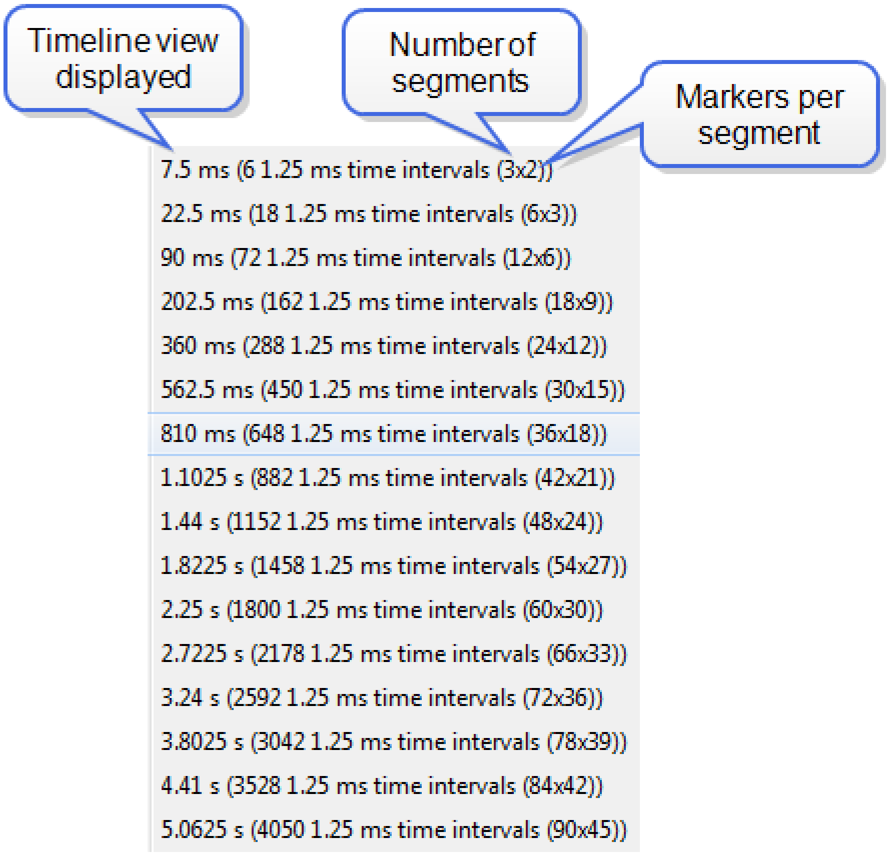
4.4.2.8.1.1 Single Segment Zoom



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.

4.4.2.8.1.2 Multiple Segments

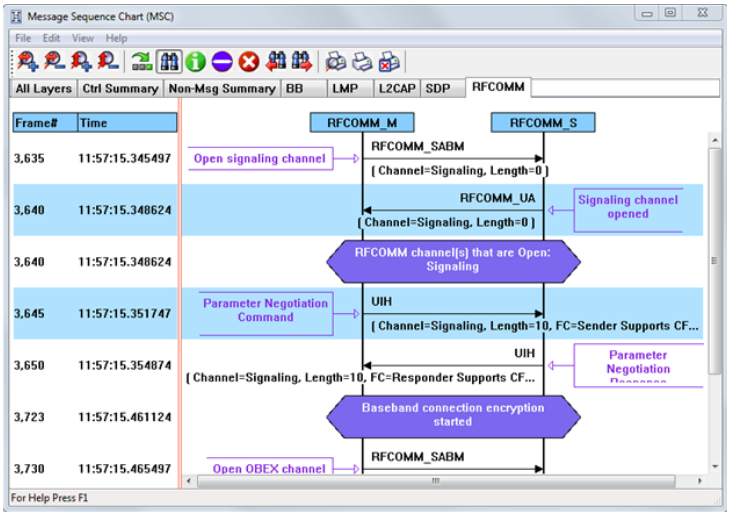

Timeline view displayed
Number of segments
Markers per segment
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (12x6))
202.5 ms (162 1.25 ms time intervals (18x9))
360 ms (288 1.25 ms time intervals (24x12))
562.5 ms (450 1.25 ms time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

4.4.3 Message Sequence Chart

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



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

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

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

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

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

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

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

Figure 55. Message Sequence Chart Window

How do I access the chart?

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

What do I see on the dialog?

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

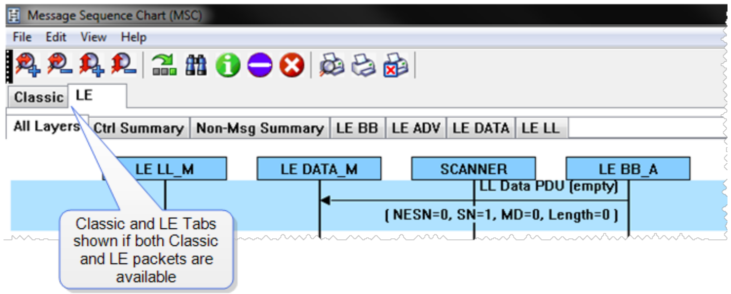
There are three navigation icons also on the toolbar.

This takes you to the first Information Frame.

This takes you to first Protocol State Message.

This takes you to the first Error Frame. Click here to learn more about this option.

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



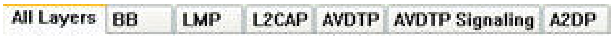
LL Data PDU (empty)

(NESN=0, SN=1, MD=0, Length=0)

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

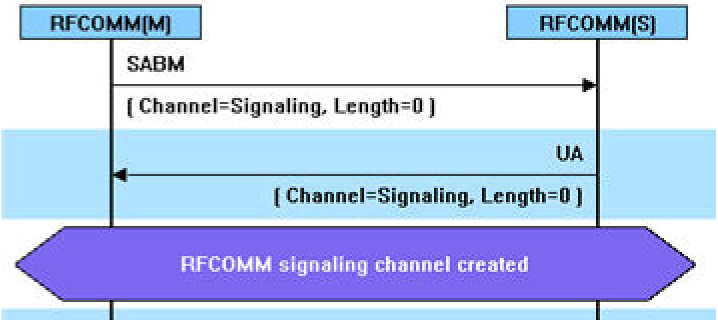
Figure 56. Classic and LE tabs

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



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

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



SABM

(Channel=Signaling, Length=0)

UA

(Channel=Signaling, Length=0)

RFCOMM signaling channel created

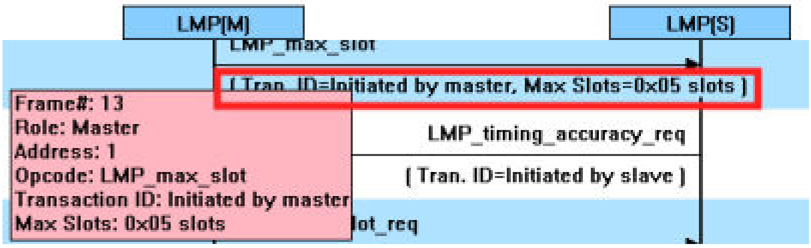
The Non-Message Summary tab displays all the non-message items in the data.

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

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

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

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



LMP_max_slot

(Tran. ID=Initiated by master, Max Slots=0x05 slots)

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

LMP_timing_accuracy_req

(Tran. ID=Initiated by slave)

lot_req

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

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

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

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

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

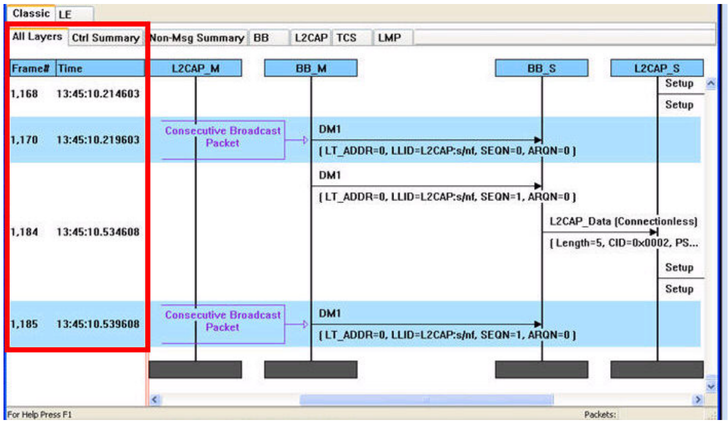

Classic
LE
All Layers
Ctrl Summary
Non-Msg Summary
BB
L2CAP
TCS
LMP
Frame#
Time
L2CAP_M
BB_M
BB_S
L2CAP_S
1,168
13:45:10.214603
Setup
Setup
1,170
13:45:10.219603
Consecutive Broadcast Packet
DM1
[LT_ADDR=0, LLID=L2CAP:s/nf, SEQN=0, ARQN=0]
DM1
[LT_ADDR=0, LLID=L2CAP:s/nf, SEQN=1, ARQN=0]
1,184
13:45:10.534608
L2CAP_Data (Connectionless)
[Length=5, CID=0x0002, PS...
Setup
Setup
1,185
13:45:10.539608
Consecutive Broadcast Packet
DM1
[LT_ADDR=0, LLID=L2CAP:s/nf, SEQN=1, ARQN=0]
For Help Press F1
Packets:

Figure 57. Frame# and Time Display, inside red box.

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

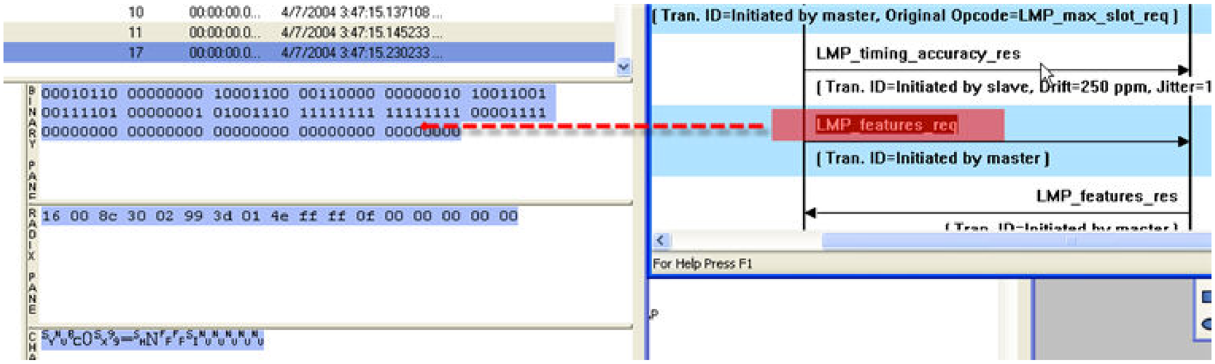


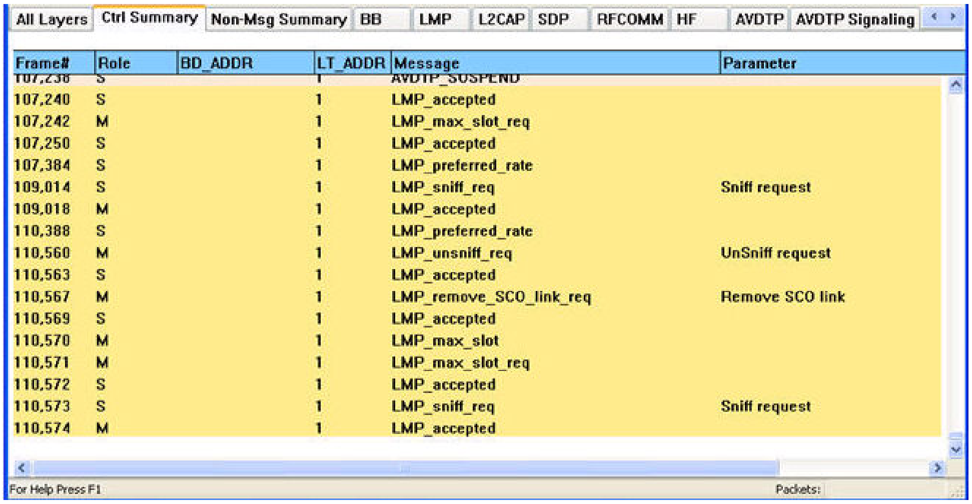
Figure 58. MSC Synchronization with Frame Display

How do I navigate in the dialog?

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

Ctrl Summary tab

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

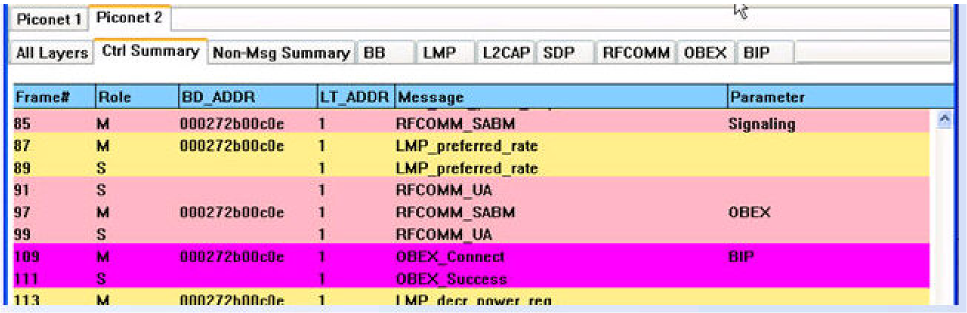


Frame#	Role	BD_ADDR	LT_ADDR	Message	Parameter
107,238	S		1	AVDTP_SUSPEND	
107,240	S		1	LMP_accepted	
107,242	M		1	LMP_max_slot_req	
107,250	S		1	LMP_accepted	
107,384	S		1	LMP_preferred_rate	
109,014	S		1	LMP_sniff_req	Sniff request
109,018	M		1	LMP_accepted	
110,388	S		1	LMP_preferred_rate	
110,560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

Figure 59. Control and Signaling Frames Summay

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

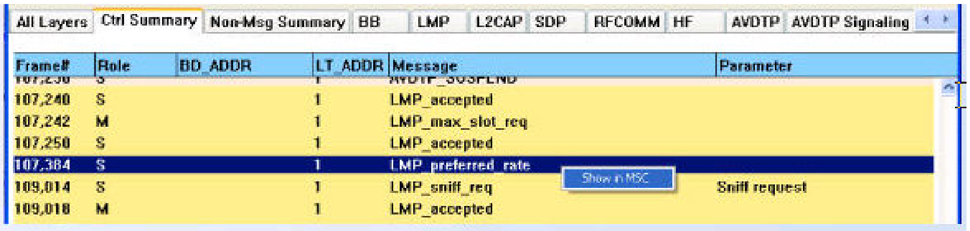
Additionally, the control/signaling packets for each layer are shown in a different background color.



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

Figure 60. Packet Layers Shown in Different Colors

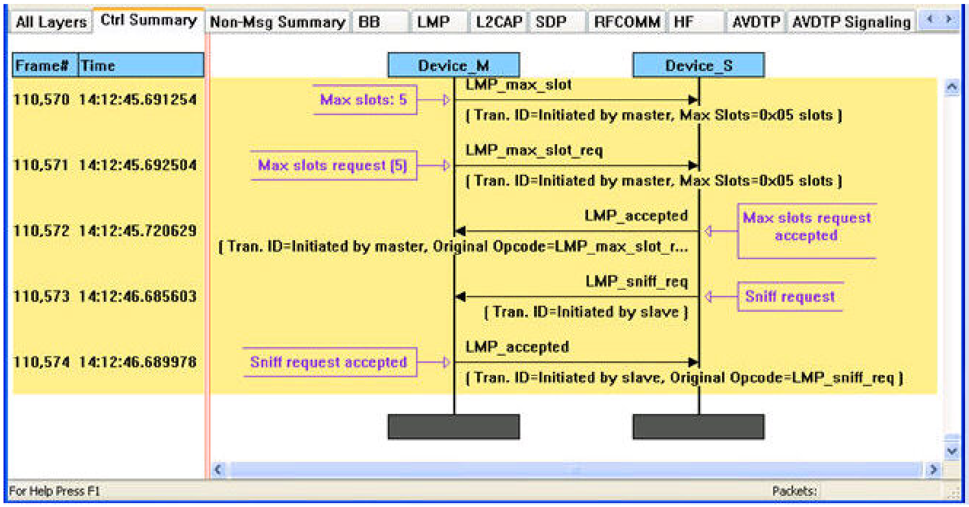
If you right click within the Ctrl Summary, you can select Show in MSC.



Frame#	Role	BD_ADDR	LT_ADDR	Message	Parameter
107,238	S		1	AVDTP_SUSPEND	
107,240	S		1	LMP_accepted	
107,242	M		1	LMP_max_slot_req	
107,250	S		1	LMP_accepted	
107,384	S		1	LMP_preferred_rate	
109,014	S		1	LMP_sniff_req	Sniff request
109,018	M		1	LMP_accepted	

Figure 61. Right-Click in Ctrl Summary to Display Show in MSC

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


All Layers
Ctrl Summary
Non-Msg Summary
BB
LMP
L2CAP
SDP
RFCOMM
HF
AVDTP
AVDTP Signaling
Device_M
Device_S
Max slots: 5
LMP_max_slot
[Tran. ID=Initiated by master, Max Slots=0x05 slots]
Max slots request [5]
LMP_max_slot_req
[Tran. ID=Initiated by master, Max Slots=0x05 slots]
LMP_accepted
Max slots request accepted
[Tran. ID=Initiated by master, Original Opcode=LMP_max_slot_r...
LMP_sniff_req
Sniff request
[Tran. ID=Initiated by slave]
Sniff request accepted
LMP_accepted
[Tran. ID=Initiated by slave, Original Opcode=LMP_sniff_req]
For Help Press F1
Packets:

Frame#	Time
110,570	14:12:45.691254
110,571	14:12:45.692504
110,572	14:12:45.720629
110,573	14:12:46.685603
110,574	14:12:46.689978

Figure 62. MSC View of Selected Packet from Ctrl Summary

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

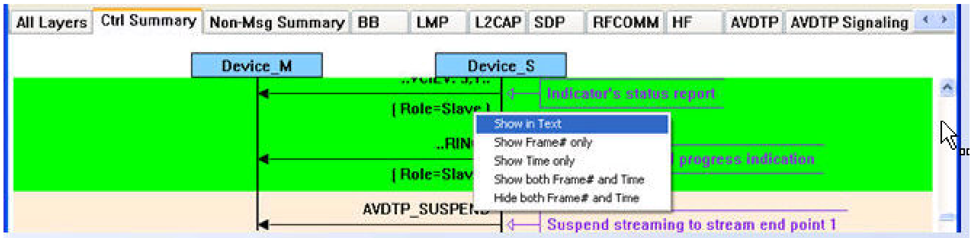


Figure 63. Return to Text View Using Right-Click Menu

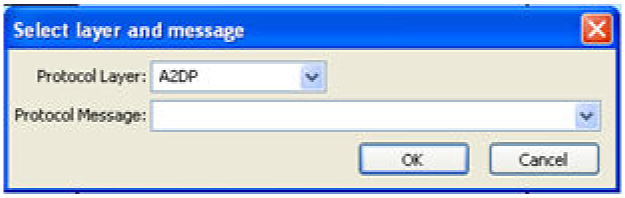
You can also choose to show:

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

4.4.3.1 Message Sequence Chart - Search

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

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


Select layer and message

Protocol Layer: A2DP

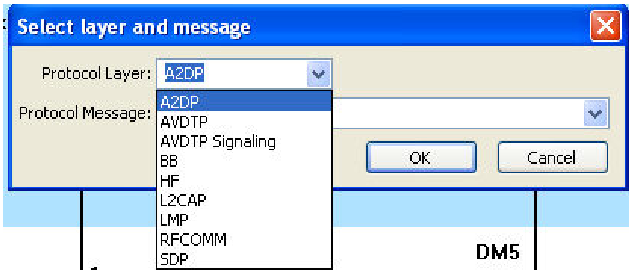
Protocol Message:

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

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

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

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


Select layer and message

Protocol Layer: A2DP

Protocol Message:

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

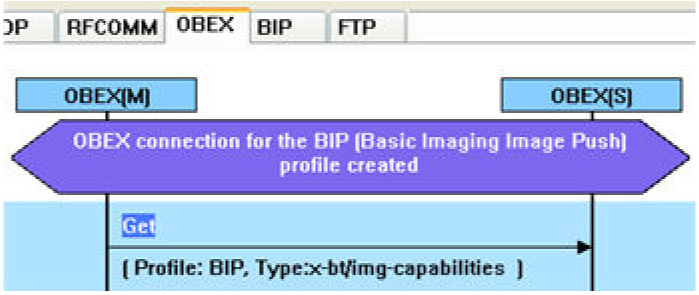
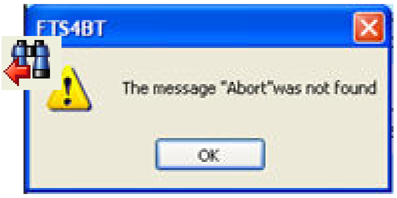

DP
RFCOMM
OBEX
BIP
FTP
OBEX(M)
OBEX(S)
OBEX connection for the BIP (Basic Imaging Image Push) profile created
Get
(Profile: BIP, Type:x-bt/img-capabilities)

Figure 64. Highlighted First Search Result

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


FTS4BT

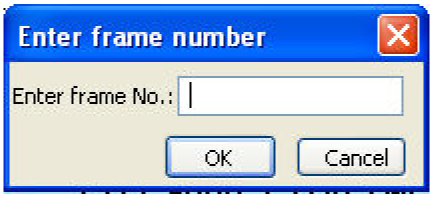
The message "Abort"was not found

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

4.4.3.2 Message Sequence Chart - Go To Frame

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

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



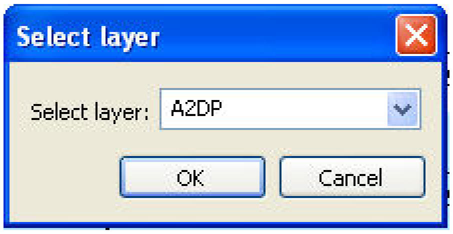
1. Click Go To Frame in the toolbar.
2. Enter a frame number in the Enter frame No.: text box.
3. Click OK.

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

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

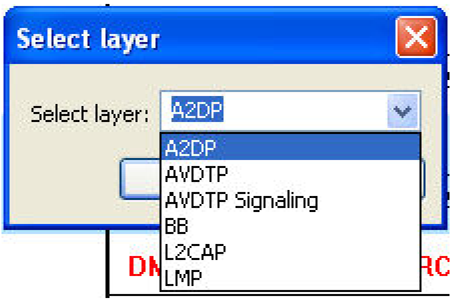
4.4.3.3 Message Sequence Chart - First Error Frame

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



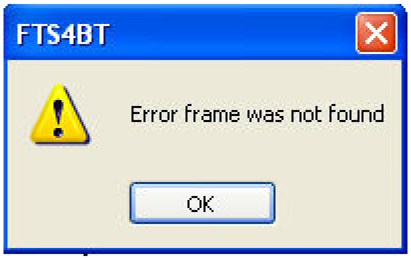
Select layer: A2DP

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



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

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



Error frame was not found

4.4.3.4 Message Sequence Chart - Printing

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

Print Preview

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

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

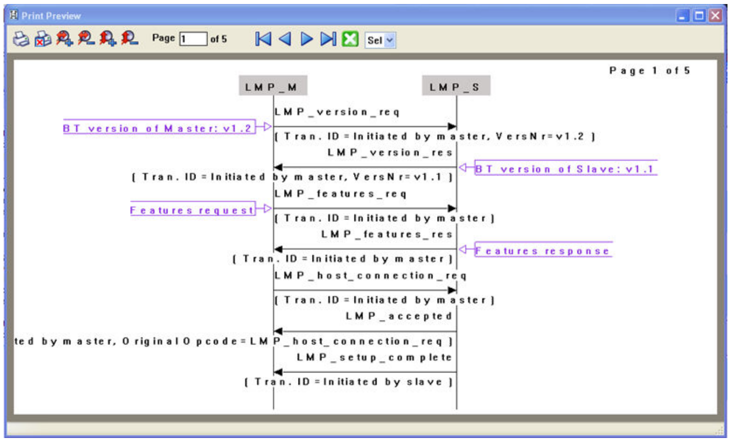

Print Preview
Page 1 of 5
Sel
Page 1 of 5
LMP_M
LMP_S
LMP_version_req
BT version of Master: v1.2
[Tran. ID = Initiated by master, VersNr=v1.2]
LMP_version_res
BT version of Slave: v1.1
[Tran. ID = Initiated by master, VersNr=v1.1]
LMP_features_req
Features request
[Tran. ID = Initiated by master]
LMP_features_res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

Figure 65. Message Sequence Chart Print Preview

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

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

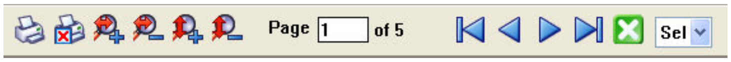


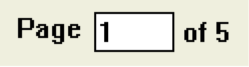
Figure 66. Print Preview Toolbar

Print: Prints all the pages to the printer you select in Print Setup dialog.

Cancel Printing: Cancels the current printing.

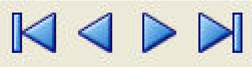
Zoom In Horizontally, Zoom Out Horizontally, Zoom In Vertically, and Zoom Out Vertically allow you to change the look of the printed page.

- Zoom In Horizontally expands the data horizontally so it can be easier to read.
- Zoom Out Horizontally squeezes the data together so that more fits on one page.
- Zoom in Vertically expands the data vertically so it can be easier to read.
- Zoom Out Vertically squeezes the data so that more fits on one page.



The current page text box displays the page number that is currently being shown on the dialog.

You can enter a number in the text box, then press Enter, and the dialog will display the data for that page.



If the data requires multiple pages, the navigation buttons will take you to the:

- First page
- Previous Page
- Next Page
- Last Page

☒ Close Print Preview closes the dialog and returns to the Message Sequence Chart.

The Select font size drop-down allows you to select the text font size for the printed data. Simply select a font size from the drop-down list.

When you select Print, you will output the data that is currently being displayed.

4.4.4 Packet Error Rate Statistics

The Packet Error Rate (PER) Stats view provides a dynamic graphical representation of the Packet Error Rate for each channel. The dialog displays a graph for each channel numbered 0 through 78.

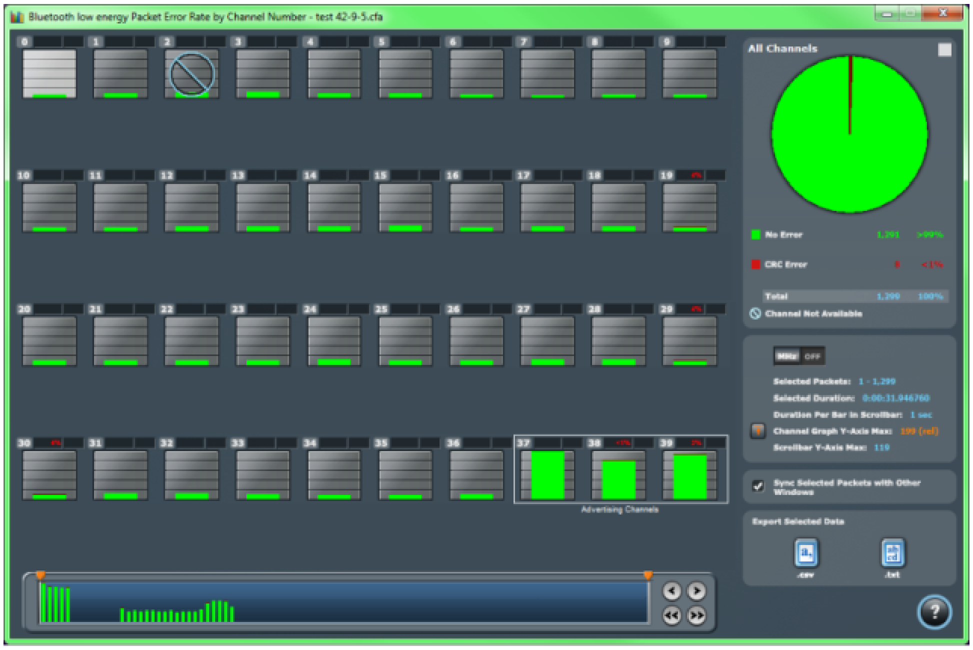
Data Analysis

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

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

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

4.4.4.1 *Bluetooth* low energy Packet Error Rate



Bluetooth low energy Packet Error Rate by Channel Number - test 42-9-5.cfa

All Channels

🟩 No Error 1,291 >99%

🟥 CRC Error 8 <1%

Total 1,299 100%

Channel Not Available

MHz OFF

Selected Packets: 1 - 1,299

Selected Duration: 0:00:31.946760

Duration Per Bar in Scrollbar: 1 sec

Channel Graph Y-Axis Max: 199 (ref)

Scrollbar Y-Axis Max: 119

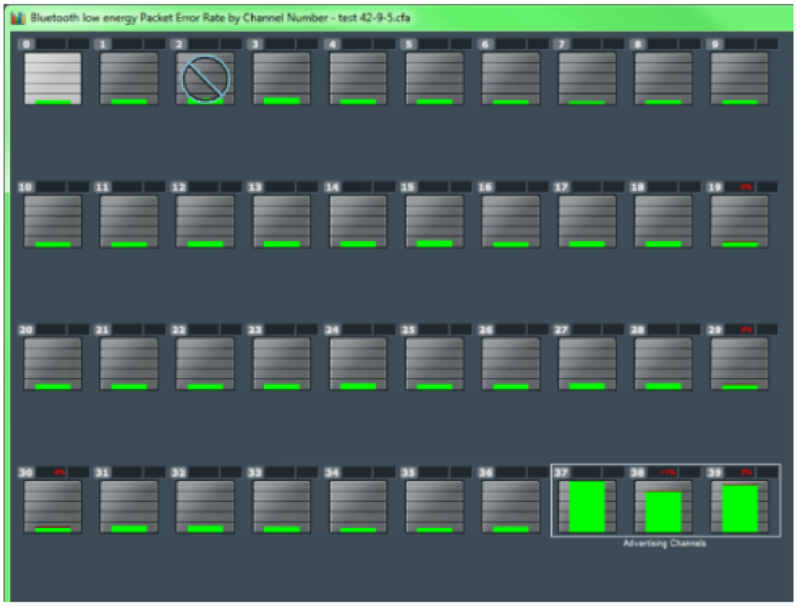
☑ Sync Selected Packets with Other Windows

Export Selected Data

Figure 67. *Bluetooth* low energy PER Stats Window

4.4.4.2 Packet Error Rate - Channels

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

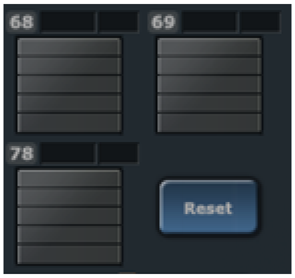


Bluetooth low energy Packet Error Rate by Channel Number - test 42-9-5.cfa

Figure 68. *Bluetooth* low energy Packet Error Rate Channels

- **For *Bluetooth* low energy**: Each channel contains a bar that displays the number of packets with no errors in green, packets with CRC errors in dark red..
- The red number at the top of the channel shows the percentage of Header Error and Payload/CRC Errors in relationship to the total number of packets in the channel.
- The light blue number at the top of each channel shows the megahertz (MHz) for the channel if the option is chosen in the Additional Statistics section.
- When you select a channel, detailed information for that channel is displayed in the expanded chart on the upper right.
- The channels change dynamically as the Viewport is moved or new data appears within the Viewport.
- The Channel Not Available symbol is displayed if the channel is not available in the most recent channel map that is in or before the last selected packet, even if that channel map comes before the first selected packet. *Bluetooth* Adaptive Frequency Hopping processes will block channels determined to be unreliable. These channels are not available because the Bluetooth devices have decided not to use them.

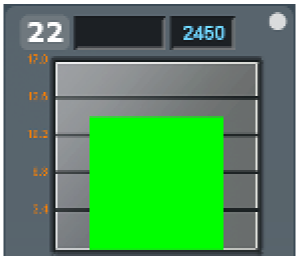
- "s" changes the size of the entire dialog.
- "c" changes the contrast of the dialog
- The Reset button is only available in live mode. The button will appear in the lower right-hand corner of the Channels section. Clicking on the Reset button will clear all prior data from PER Stats.



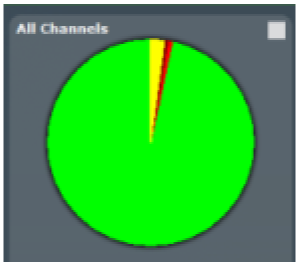
4.4.4.3 Packet Error Rate - Pie Chart and Expanded Chart

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

Expanded Chart

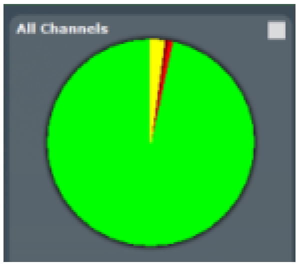


Pie Chart



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

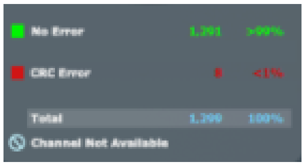
  To return to the bar chart, click on the channel again or click on the □ in the upper right hand corner.



4.4.4.4 Packet Error Rate - Legend

The Legend displays color coded information about the channel selected.

Bluetooth low energy



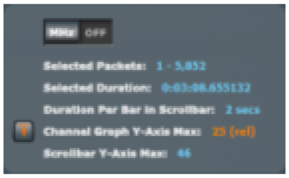
🟩 No Error	1,391	>99%
🟥 CRC Error	8	<1%
Total	1,399	100%
⃠ Channel Not Available		

For *Bluetooth* low energy:

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

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

4.4.4.5 Packet Error Rate - Additional Statistics



MHz OFF

Selected Packets: 1 - 5,852

Selected Duration: 0:03:08.655132

Duration Per Bar in Scrollbar: 2 secs

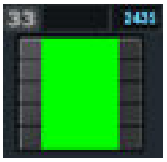
Channel Graph Y-Axis Max: 25 (rel)

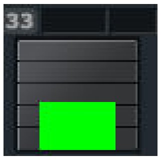
Scrollbar Y-Axis Max: 46

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

- Selecting MHz On displays the megahertz value for each channel in the main channels chart and also in the expanded chart.
- Selecting MHz Off removes the megahertz value.

- Selected Packets displays the packet range selected in the Scroll Bar. This includes inapplicable Inapplicable packets include Wi-Fi packets, Sniffer Debug packets, any packets that are not relevant to PER Stats. Inapplicable packets do not appear as part of the Additional Statistics. packets.
- Selected Duration identifies the total amount of time in the selected packet range displayed in the Scroll Bar.
- Duration Per Bar in Scrollbar: identifies the amount of time represented by each bar in the Scroll Bar.
- The Channel Graph Y-Axis Max can display two different values. When the Snap Arrow is orange , the values for channels in the main chart are shown in relative terms in Snap Mode. This means that one channel (or channels) with the greatest value is "snapped" to the top of the chart. In the graphic below left, Channel 33 is snapped to the top of the chart.
  The channel(s) with the greatest value become a full-scale reference display for the other channels that have been relatively scaled. Channel comparisons become easier. With Snap On you can select multiple time values in the Scroll Bar.

  When the Snap Arrow is white (Snap Mode turned off), the values for channels in the main chart are shown in absolute values where the max value of each channel graph is the same regardless of the position of the Viewport. Channel 33, which is snapped to the top of the chart in Snap Mode (shown above left), appears like the right image when Snap Mode is turned off.
- Scrollbar Y-Axis Max displays the maximum Y-Axis value in the Scroll Bar.

4.4.4.6 Packet Error Rate - Sync Selected Packets With Other Windows

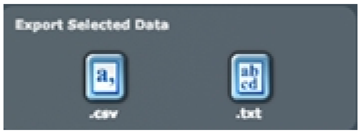
□ Sync Selected Packets with Other Windows

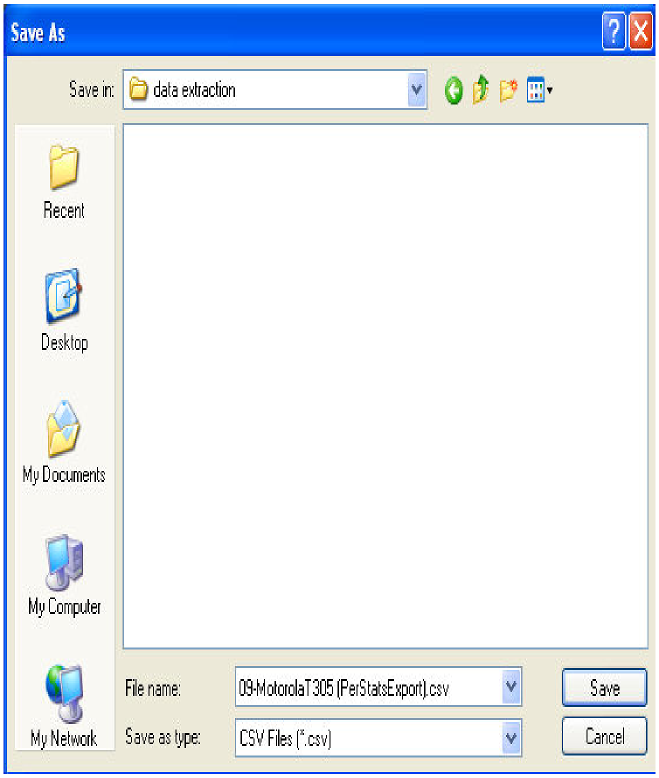
By default, and unlike other windows, PER Stats is not synchronized with other windows such as Frame Display in that selecting a frame range in one does not highlight the same frame range in the other. This ensures that Frame Display isn't constantly re-synchronizing during live capture while the view-port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

4.4.4.7 Packet Error Rate - Export

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

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





Save in: data extraction

File name: 09-MotorolaT305 (PerStatsExport).csv

Save as type: CSV Files (*.csv)

3. Select a location where you want to save the file in "Save in:".
4. Enter a file name in "File name:".
5. Select "Save".

The file will be saved to that location.

4.4.4.8 Packet Error Rate - Scroll Bar

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

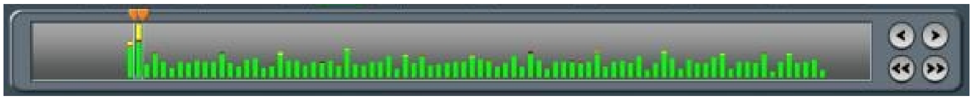
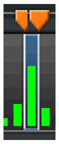
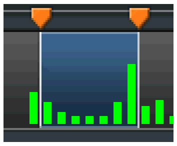
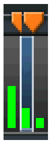
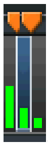


Figure 69. PER Stats Scroll Bar

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

- Pressing the left arrow button ◀, the left arrow key, or the up arrow key moves the Viewport to the left, one vertical bar at a time.

- Pressing the right arrow button ▶. the right arrow key, or the down arrow key moves the Viewport to the right, one vertical bar at a time.

- Pressing the double left arrow button ⏪ or the PgUp key moves the Viewport to the left by the current width of the Viewport. Holding down the Shift key will prevent the Viewport from moving if there is not enough room to move by its full width.

- Pressing the double right arrow button ⏩ or the PgDn key moves the Viewport to the right by the current width of the Viewport. Holding down the Shift key will prevent the Viewport from moving if there is not enough room to move by its full width.

- Holding the Shift key down and the right or left arrows moves the right side of the Viewport.

- Holding the Ctrl key down and the right or left arrows moves the left side of the Viewport.

- The Scroll bar includes inapplicable packets (sniffer debug, WiFi, etc) so that the packet range selected in Frame Display can be shown. Inapplicable packets are not, however, included in the statistics reports.

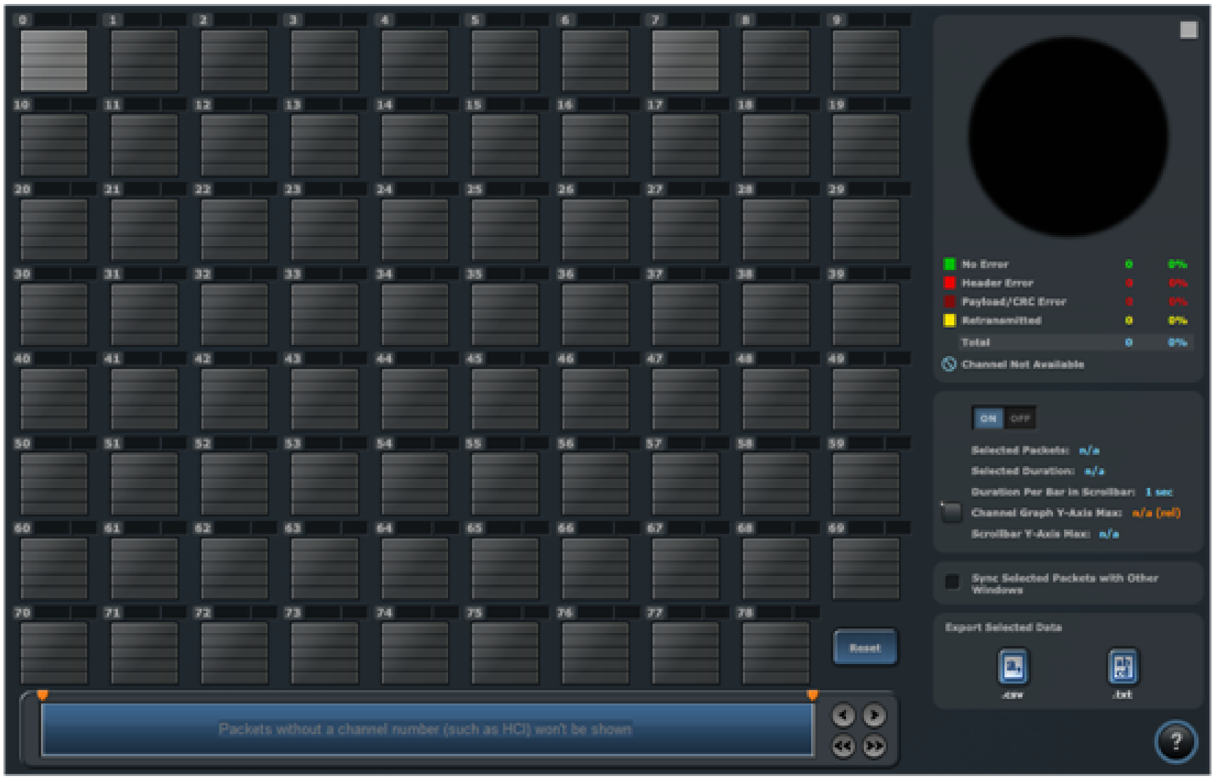
- If the Viewport is adjusted within PER Stats, as opposed to selecting a packet range in Frame Display, it uses only whole bars on both sides.

- Statistics are retained for all packets regardless of whether any of those packets have wrapped out. You can select the Reset button Reset, which is located above the right portion of the Scroll Bar, to discard all stats for packets received up to that point.

- The Reset button is only available when you are capturing data.

4.4.4.9 Packet Error Rate - Excluded Packets

ID packets and packets that are missing channel numbers (such as HCI and BTSnoop) will not display data. ID packets are excluded because they can not have errors or indicate retransmission and therefore dilute the percentages for other packet types. Packets without channel numbers are excluded because the graphs are channel-specific. Before packets are captured, the Scroll Bar in Classic *Bluetooth* PER Stats contains the message "ID packets and packets without a channel number (such as HCI) are excluded", and the Scroll Bar in *Bluetooth* low energy PER Stats contains the message "Packets without a channel number (such as HCI) are excluded".



Packets without a channel number (such as HCI) won't be shown

🟩	No Error	0	0%
🟥	Header Error	0	0%
🟥	Payload/CRC Error	0	0%
🟨	Retransmitted	0	0%
	Total	0	0%

Channel Not Available

ON OFF

Selected Packets: n/a

Selected Duration: n/a

Duration Per Bar in Scrollbar: 1 sec

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

Scrollbar Y-Axis Max: n/a

□ Sync Selected Packets with Other Windows

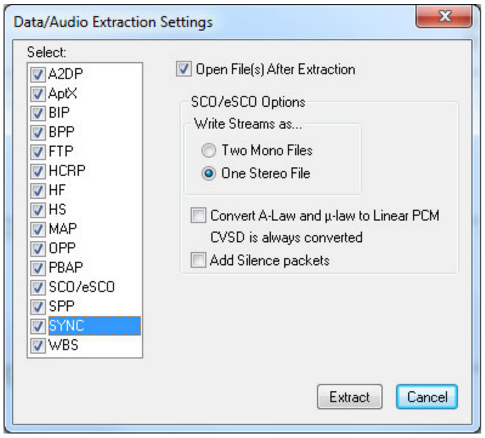
Export Selected Data

Figure 70. Example: Excluded Packets Message in Scroll Bar (Classic *Bluetooth*)

4.5 Data/Audio Extraction

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

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



Data/Audio Extraction Settings

Select:

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

☑ Open File(s) After Extraction

SCO/eSCO Options

Write Streams as...

○ Two Mono Files

● One Stereo File

□ Convert A-Law and µ-law to Linear PCM

CVSD is always converted

□ Add Silence packets

Figure 71. Data/Audio Extraction Settings dialog

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

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

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

   Note: This does not work for SCO/eSCO.

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

   Note: This option is for SCO/eSCO only.

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

   Note: This option is for SCO/eSCO only.

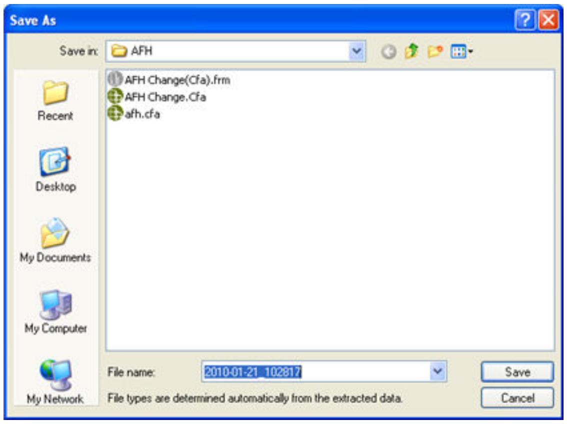
6. Select the Add Silence packets to insert the silence packets (dummy packets) for the reserved empty slots into the extracted file. If this option is not selected, the audio packets are extracted without inserting the silence packets for the reserved empty slots.

   Note: This option is for SCO/eSCO only.

7. Select Extract.

   A Save As dialog appears.

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



Save in: AFH

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

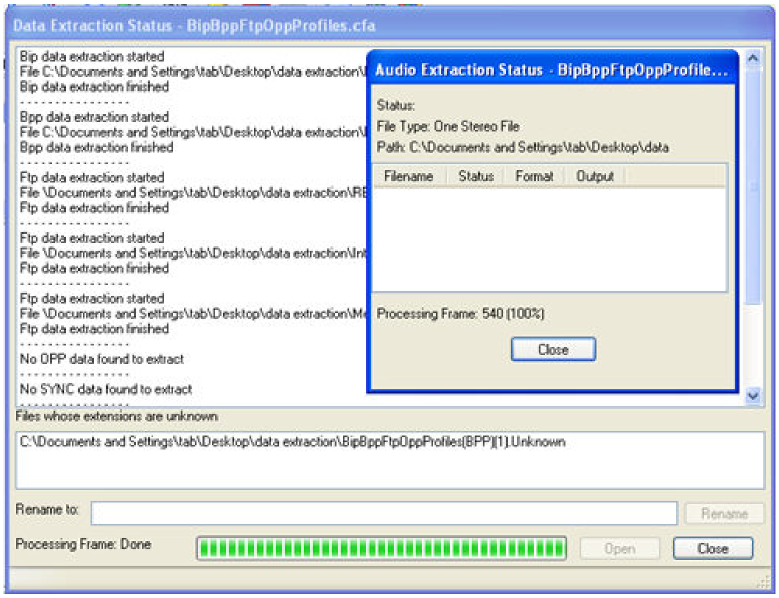
File name: 2010-01-21 102817

File types are determined automatically from the extracted data.

8. Select a location for the file.

9. Click Save.

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



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

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

Status:

File Type: One Stereo File

Path: C:\Documents and Settings\tab\Desktop\data

Processing Frame: 540 (100%)

Files whose extensions are unknown

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

Rename to:

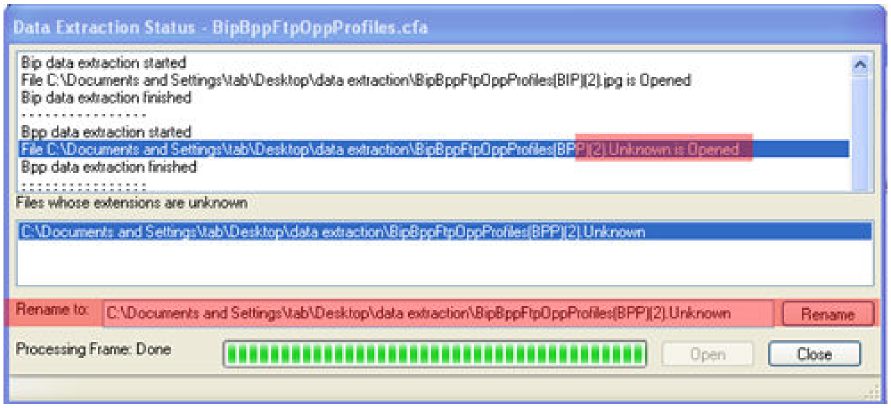
Processing Frame: Done

Figure 72. Data and Audio Extraction Status

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

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

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



Data Extraction Status - BipBppFtpOppProfiles.cfa

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

Files whose extensions are unknown

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

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

Processing Frame: Done

Figure 73. Rename To in the bottom section of Data Extraction Status

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

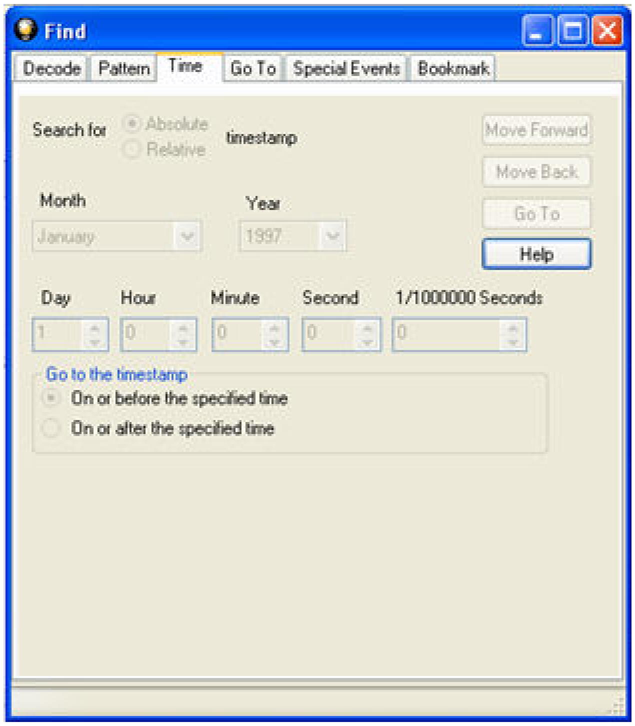
When you are finished, select Close to close the dialogs.

Chapter 5: Navigating and Searching the Data

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

5.1 Find

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



Search for ● Absolute ○ Relative timestamp

Month: January

Year: 1997

Day: 1 Hour: 0 Minute: 0 Second: 0 1/1000000 Seconds: 0

Go to the timestamp

● On or before the specified time

○ On or after the specified time

Figure 74. Find Diaglog

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

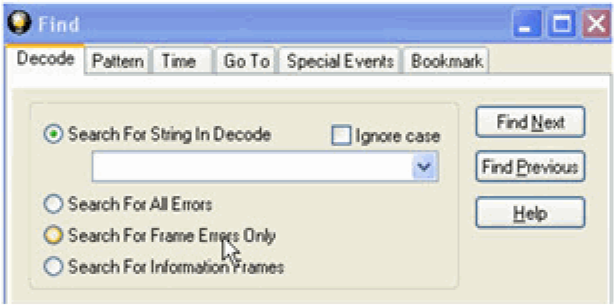
5.1.1 Searching within Decodes

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

To access the search within decodes function:

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

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



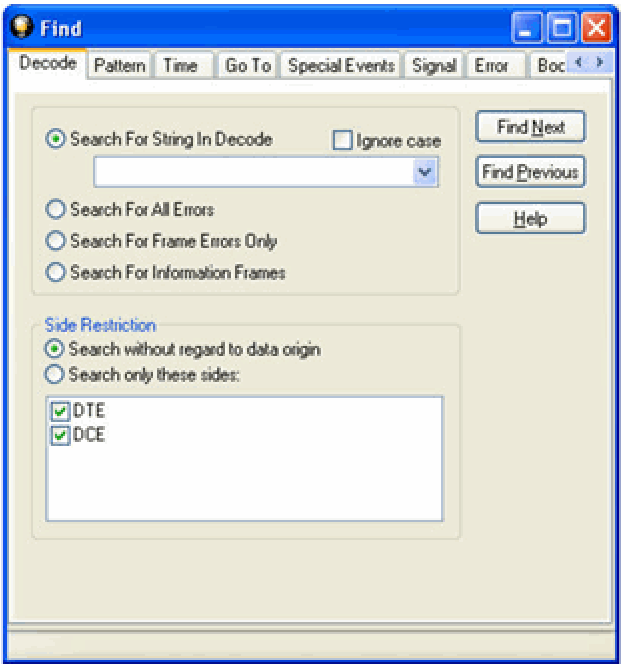
● Search For String In Decode □ Ignore case

○ Search For All Errors

○ Search For Frame Errors Only

○ Search For Information Frames

Figure 75. Find Decode Tab Search for String



● Search For String In Decode □ Ignore case

○ Search For All Errors

○ Search For Frame Errors Only

○ Search For Information Frames

Side Restriction

● Search without regard to data origin

○ Search only these sides:

☑ DTE

☑ DCE

Figure 76. Find Decode Tab Side Restriction

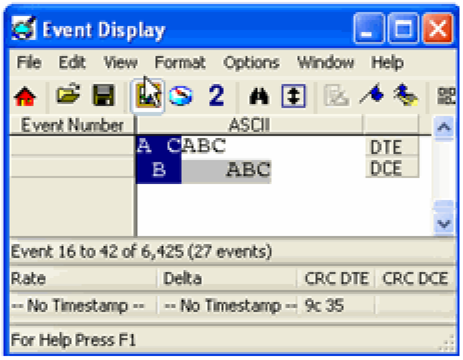
There are several options for error searching on the Decoder tab.

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

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

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

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

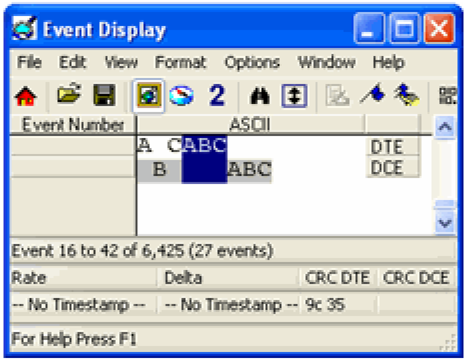


Event 16 to 42 of 6,425 (27 events)

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

For Help Press F1

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



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

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

For Help Press F1

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

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

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

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

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

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

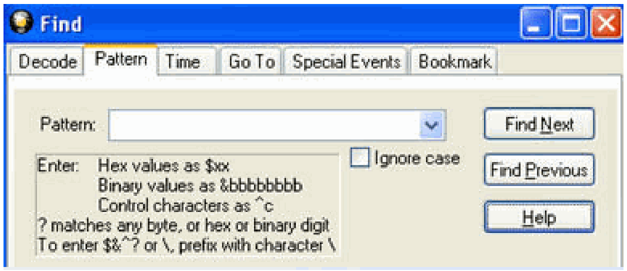
5.1.2 Searching by Pattern

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

To access the search by pattern function:

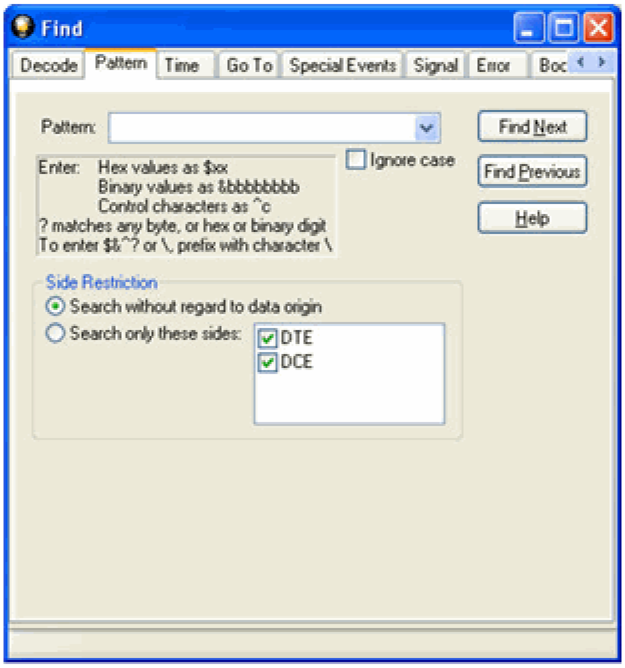
1. Open a capture file to search.
2. Open the Event Display or Frame Display window.
3. Click on the Find icon or choose Find from the Edit menu.
4. Click on the Pattern tab of the Find dialog.

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



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

Figure 77. Find Pattern Tab



Pattern:

□ Ignore case

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

Side Restriction

● Search without regard to data origin

○ Search only these sides: ☑ DTE ☑ DCE

Figure 78. Find Pattern Tab Side Restrictions

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

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

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

Refer to Searching by Decode on page 103 for information on Side Restrictions

5.1.3 Searching by Time

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

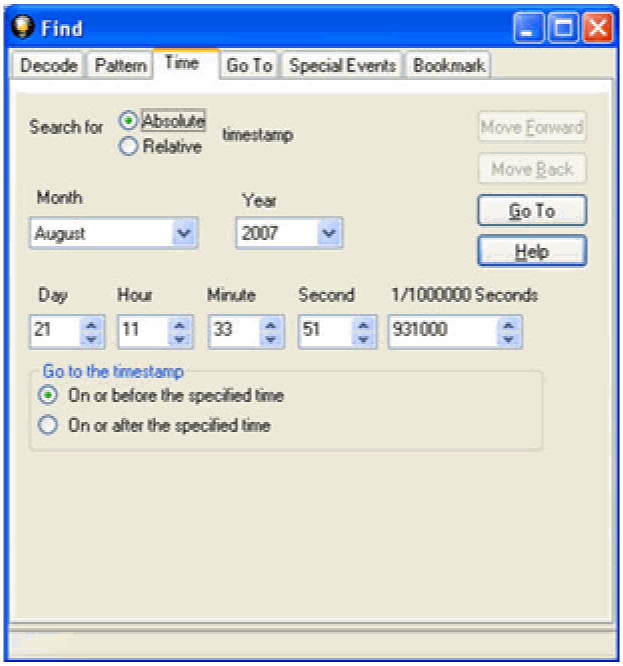
To access the search by time function:

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

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

4. Click on the Time tab of the Find dialog.

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



Search for ● Absolute ○ Relative timestamp

Month: August

Year: 2007

Day: 21

Hour: 11

Minute: 33

Second: 51

1/1000000 Seconds: 931000

Go to the timestamp

● On or before the specified time

○ On or after the specified time

Figure 79. Find by Time tab

The analyzer can search by time in several different ways.

Search for Absolute/Relative timestamp.

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

1. Select Absolute or Relative

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

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

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

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

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

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

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

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

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

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

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

- The analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.
- Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.
- The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

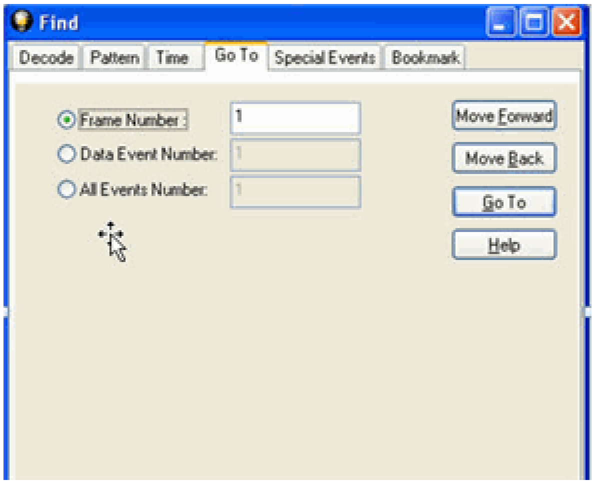
5.1.4 Using Go To

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

To access the Go To function:

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

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



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

Figure 80. Find Go To tab

To go to a particular frame :

1. Select the Frame Number radio button
2. Type the frame number in the box.
3. Click the Go To button.
4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the Move Forward or Move Back button.

To go to a particular event :

1. Select the Data Event Number or All Events Number radio button.
2. Type the number of the event in the box.
3. Click the Go To button.

4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the Move Forward or Move Backward button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on Move Forward. Each time you click on Move Forward, Frontline moves forward 10 events.

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

5.1.5 Searching for Special Events

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

To access the search for special events function:

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

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

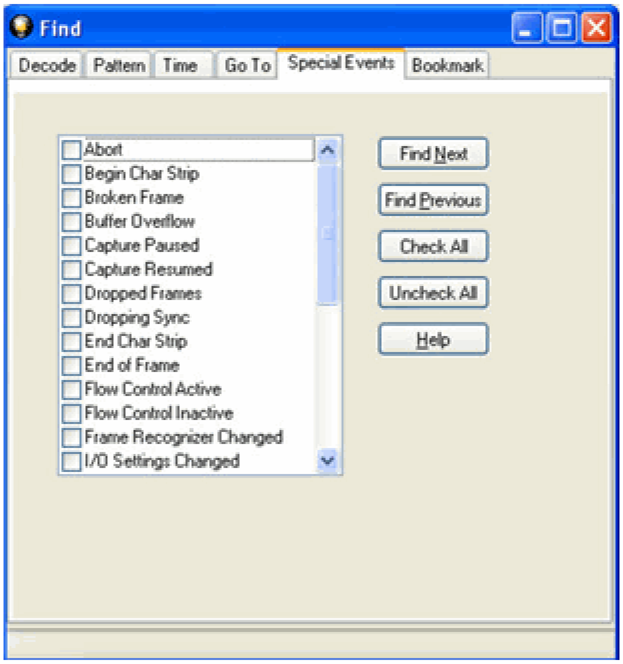


Figure 81. Find Special Events tab

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

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

For a list of all special events and their meanings, see List of All Event Symbols on page 42.

5.1.6 Searching by Signal

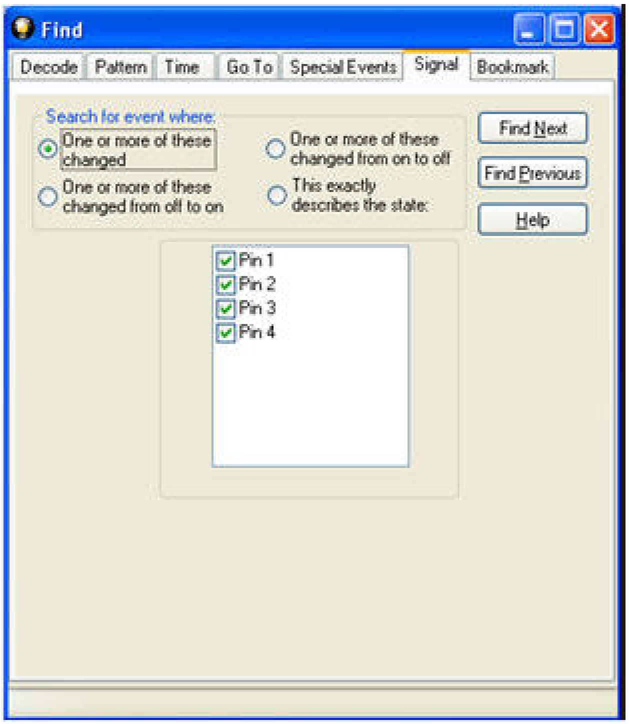
Searching with Signal allows you to search for changes in control signal states for one or more control signals. You can also search for a specific state involving one or more control signals, with the option to ignore those control signals whose states you don't care about.

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

To access the search by time function:

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

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



Search for event where:

● One or more of these changed

○ One or more of these changed from off to on

○ One or more of these changed from on to off

○ This exactly describes the state:

☑ Pin 1

☑ Pin 2

☑ Pin 3

☑ Pin 4

Figure 82. Find Signal tab.

Figure 83. Find Signal Tab

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

Control Signals

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

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

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

The control signals types include:

- USB - Pin 1
- USB - Pin 2

- USB - Pin 3
- USB - Pin 4

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

Searching for event where:

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

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

  To search for an exact state means that the analyzer finds events that match exactly the state of the control signals that you specify.
  - First, choose to search for an event where your choices exactly describe the state.
  - This changes the normal check boxes to a series of radio buttons labeled On, Off and Don’t Care for each control signal.
  - Choose which state you want each control signal to be in.

- Choose Don’t Care to have the analyzer ignore the state of a control signal.
- When you click Find Next, the analyzer searches for an event that exactly matches the conditions selected, beginning from the currently selected event.
- If the end of the buffer is reached before a match is found, the analyzer asks you if you want to continue searching from the beginning.
- If you want to be sure to search the entire buffer, place your cursor on the first event in the buffer.
- Select one of the four radio buttons to choose the condition that must be met in the search
- Select one or more of the checkboxes for Pin 1, 2, 3, or 4.
- Click Find Next to locate the next occurrence of the search criteria or Find Previous to locate an earlier occurrence of the search criteria.

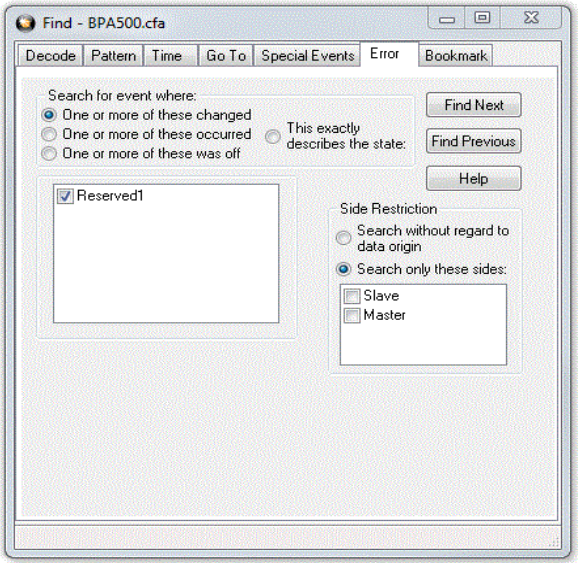
5.1.7 Searching for Data Errors

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

To access the search by time function:

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

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



Search for event where:

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

☑ Reserved1

Side Restriction

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

□ Slave
□ Master

Figure 84. Find Error tab.

Searching for event where

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

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

Selecting Which Errors to Search

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

If you want to search only for overrun errors

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

To search for all types of errors

- check all boxes

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

To do this type of search:

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

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

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

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

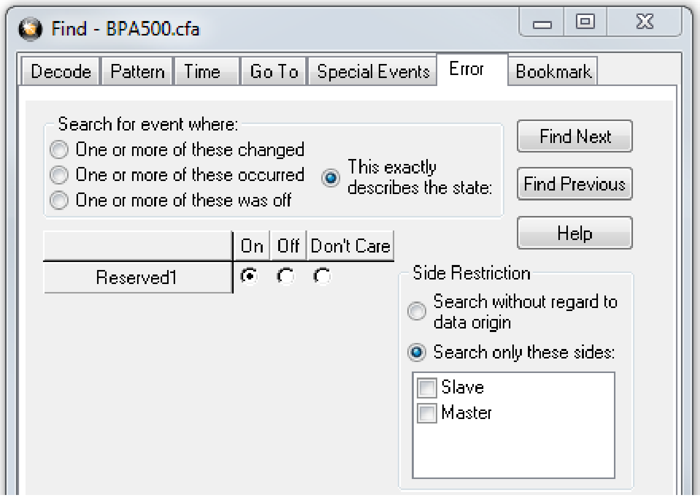
For example, if you have data where sometimes the framing is wrong and sometimes right, you would choose to search framing errors where the error condition changed. This first takes you to the point where the framing errors stopped occurring. When you click Find Next, the analyzer stops at the point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

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

Searching for Exact Error Conditions

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

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



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

	On	Off	Don't Care
Reserved1	●	○	○

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

Example:

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

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

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

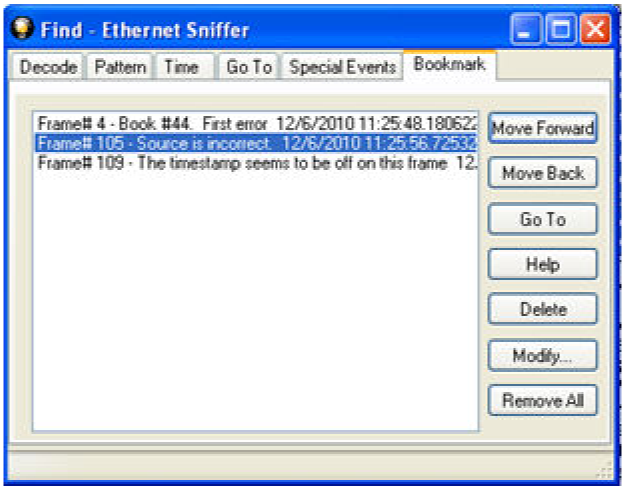
5.1.8 Find - Bookmarks

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

To access the search for bookmarks

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

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



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

Figure 85. Find Bookmark tab.

There are several ways to locate bookmarks.

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

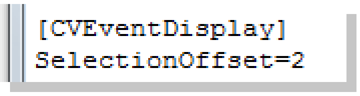
There are three ways to modify bookmarks:

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

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

5.1.9 Changing Where the Search Lands

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



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

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

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

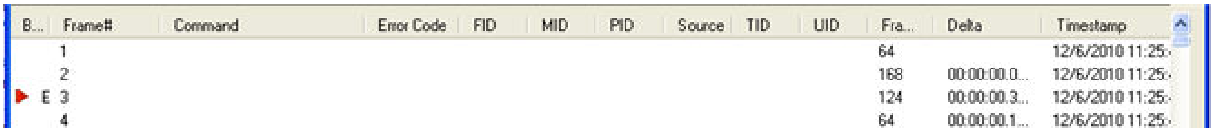
5.1.10 Subtleties of Timestamp Searching

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

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

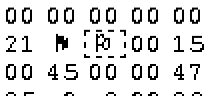
5.2 Bookmarks

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



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

Figure 86. Bookmarked Frame (3) in the Frame Display



```
00 00 00 00 00
21 ⚑ [illegible] 00 15
00 45 00 00 47
```

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

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

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

5.2.1 Adding, Modifying or Deleting a Bookmark

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

Add:

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

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

Modify

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

Delete

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

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

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

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

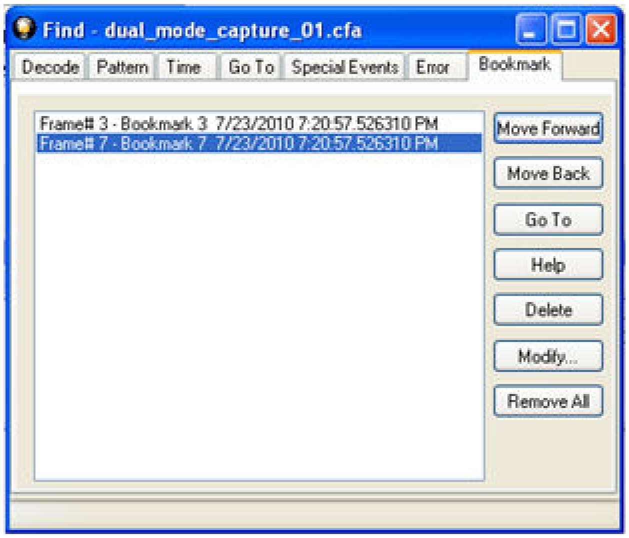
3. Click on the Delete button. The bookmark will be deleted.

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

5.2.2 Displaying All and Moving Between Bookmarks

There are three ways to move between bookmarks.

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



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

Figure 87. Find Window Bookmark tab Used to Move Around With Bookmarks

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

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

Click Remove All to delete all the bookmarks.

5.3 Filtering

5.3.1 About Display Filters

A display filter looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Display filters allow a user to look at a subset of captured data without affecting the capture content. There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filter

Protocol Filters

Protocol filters test for the existence of a specific single layer. The system creates a protocol filter for each decoder that is loaded if that layer is encountered in a capture session.

There are also three special purpose filters that are treated as protocol filters:

- All Frames with Errors
- All Frames with Bookmarks
- All Special Information Nodes

Named Filters

- Named filters test for anything other than simple single layer existence. Named filters can be constructed that test for the existence of multiple layers, field values in layers, frame sizes, etc., as well as combinations of those things. Named filters are persistent across sessions.
- Named filters are user-defined. User-defined filters persist in a template file. User defined filters can be deleted.

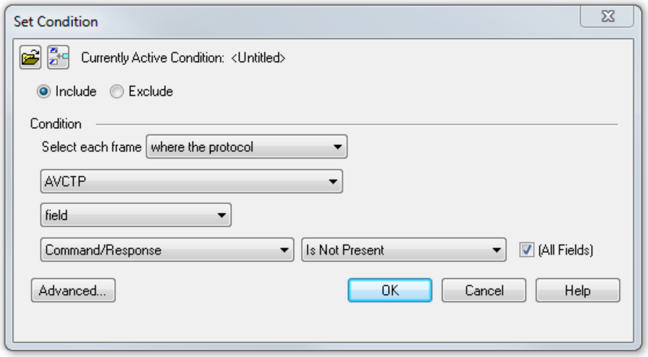
Quick Filters

- Quick Filters are combinations of Protocol Filters and/or Named Filters that are displayed on the Quick Filter tab.
- Quick Filters cannot be saved and do not persist across sessions.
- Quick Filters are created on the Quick Filter Dialog.

5.3.1.1 Creating a Display Filter

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

1. Click the Display Filters icon on the Frame Display window or select Apply/Modify Display Filters from the Filter menu to open the Set Condition dialog box. The Set Condition dialog is self configuring which means that when you Select each frame under Conditions the following displayed fields depend on your selection. With each subsequent selection the dialog fields will change depending on you selection in that field.



Set Condition

Currently Active Condition: <Untitled>

● Include ○ Exclude

Condition

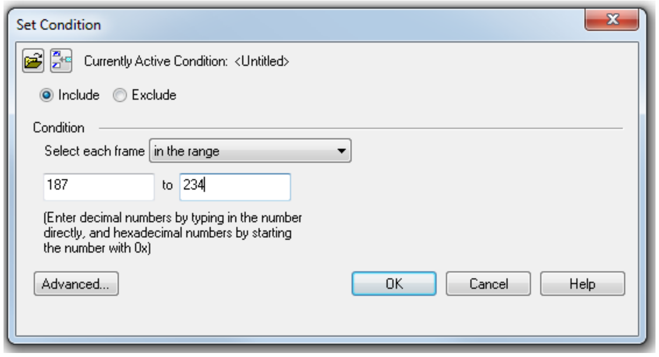
Select each frame: where the protocol

AVCTP

field

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

Figure 88. 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 89. Example: Set Conditions Self Configuring Based on Frame Range

2. Select Include or Exclude to add filtered data or keep out filtered data respectively.

3. Select the initial condition for the filter from the drop-down list.

4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the condition statement is complete.

5. Click OK. The system displays the Save Named Condition dialog. Provide a name for the filter condition or accept the default name provided by the system and click OK. Prohibited characters are left bracket '[', right bracket ']' and equal sign '='. The Set Condition dialog box closes, creates a tab on the Frame Display with the filter name, and applies the filter.

The filter also appears in the Quick Filtering and Hiding Protocols dialog.

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

Notes:

- The system requires naming and saving of all filters created by the user.
- The OK button on the Set Condition dialog box is unavailable (grayed out) until the condition selections are complete.
- When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

5.3.1.2 Including and Excluding Radio Buttons

All filter dialog boxes contain an Include and an Exclude radio button. These buttons are mutually exclusive. The Include/Exclude selection becomes part of the filter definition, and appears as part of the filter description displayed to the right of the Toolbar.

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

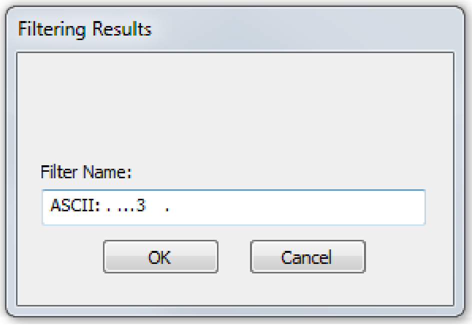
Exclude: A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

5.3.1.3 Named Display Filters

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

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

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


Filtering Results

Filter Name:

ASCII: 3   .

5.3.1.4 Using Compound Display Filters

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

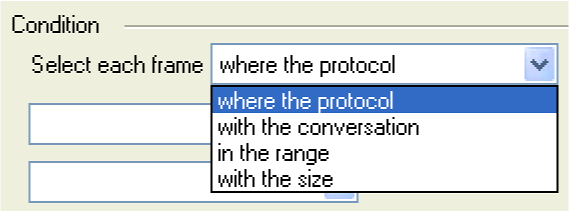
The AND operator narrows the filter, the OR operator broadens the filter, and the NOT operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

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

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

   Now you can set the conditions for the filter.

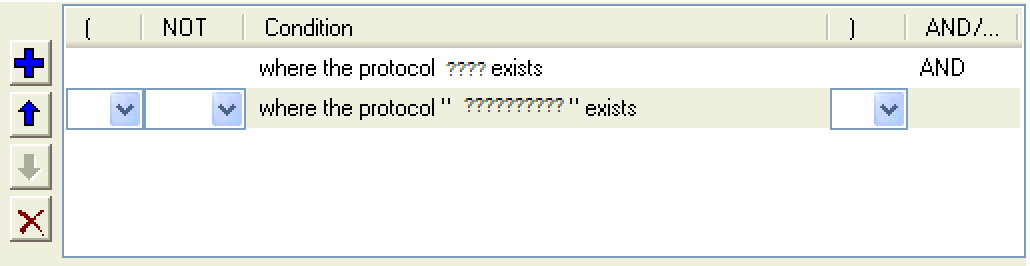
4. Select the initial condition for the filter from the combo box at the bottom of the dialog for Select each frame.



Condition

Select each frame: where the protocol

5. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.



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

Figure 90. Two Filter Conditions Added with an AND Operator

6. Click the plus icon ✚ on the left side of the dialog box and repeat steps 4 and 5 for the next condition. Use the up ↑ and down ↓ arrow icons on the left side of the dialog box to order your conditions, and the delete button ✕ to delete conditions from your filter.
7. Continue adding conditions until your filter is complete.
8. Include parentheses as needed and set the boolean operators.
9. Click OK.
10. The system displays the Save Named Condition dialog. Provide a name for the filter condition or accept the default name provided by the system and click OK.

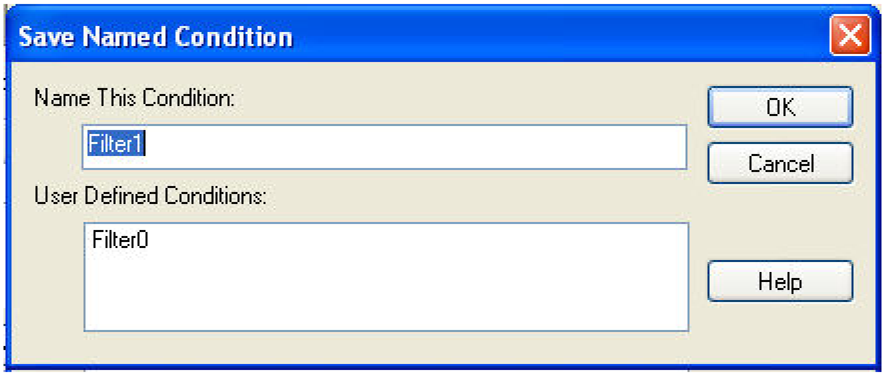
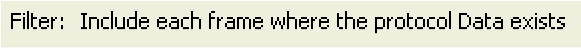


Figure 91. Save Named Filter Condition Dialog

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



Filter: Include each frame where the protocol Data exists

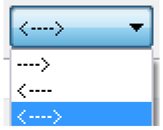
When a display filter is applied, a description of the filter appears to the right of the toolbar in the Frame Display windows.

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

5.3.1.5 Defining Node and Conversation Filters

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

1. Click the Display Filters icon on the Frame Display window or select Apply/Modify Display Filters… from the filter menu to open the Set Condition dialog box.
2. From the Select each frame combo box choose frames with the conversation as the initial condition.
3. Select an address type—IP, MAC, TCP/UDB—from the Typecombo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first Address combo box.
5. Choose a direction arrow from the direction box . The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.



6. If you want to filter on just one node address, skip step 7 and continue with step 8.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select a

node address from the second Address combo box..

8. Click OK. The Set Condition dialog box closes and the analyzer applies the filter.

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

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

5.3.1.6 The Difference Between Deleting and Hiding Display Filters

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

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

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

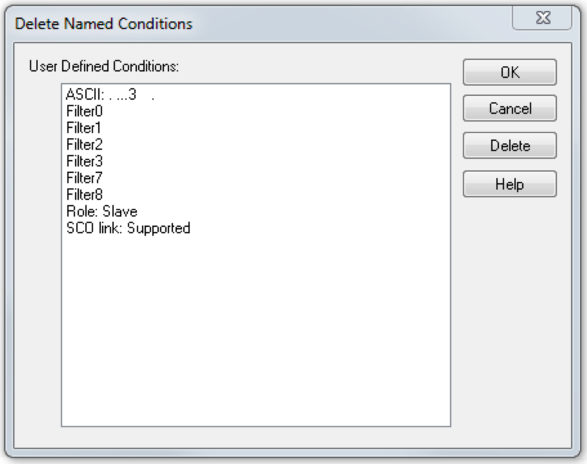
5.3.1.6.1 Deleting Saved Display Filters

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

2. Select the filter to be deleted from the list.

3. Click the Delete button.

4. Click OK. The Delete Named Condition dialog box closes and the system deletes the filter.



Delete Named Conditions

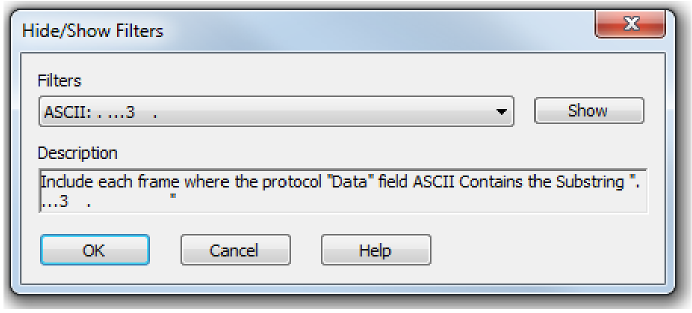
User Defined Conditions:

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

5.3.1.6.2 Hiding/Showing a Display Filter

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

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



Filters: ASCII: . ...3 .

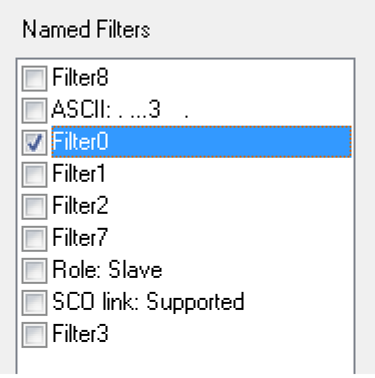
Description: Include each frame where the protocol "Data" field ASCII Contains the Substring ". ...3 . "

2. Select the filter to be hidden from the combo box.
3. Click the Hide button. The Hide button is only showing if the selected filter is currently showing in the Frame Display.
4. Click OK. The Hide/Show Filters dialog box closes, and the system hides the filter and removes the filter tab from the Frame Display.

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

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

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



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

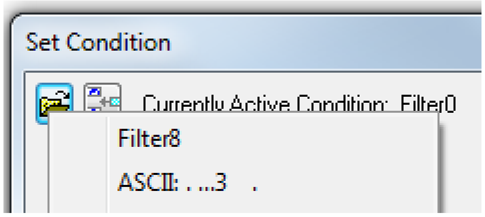
Figure 92. Using Named Filters Section of Quick Filters to Show/Hide Filters

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

5.3.1.7 Editing Filters

5.3.1.7.1 Modifying a Condition in a Filter

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



2. Edit the desired parameter of the condition: Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.
3. Click OK. The system displays the Save Named Condition dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click OK. If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click OK.) The Set Condition dialog box closes, and the system applies the modified filter.

5.3.1.7.2 Deleting a Condition in a Filter

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

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

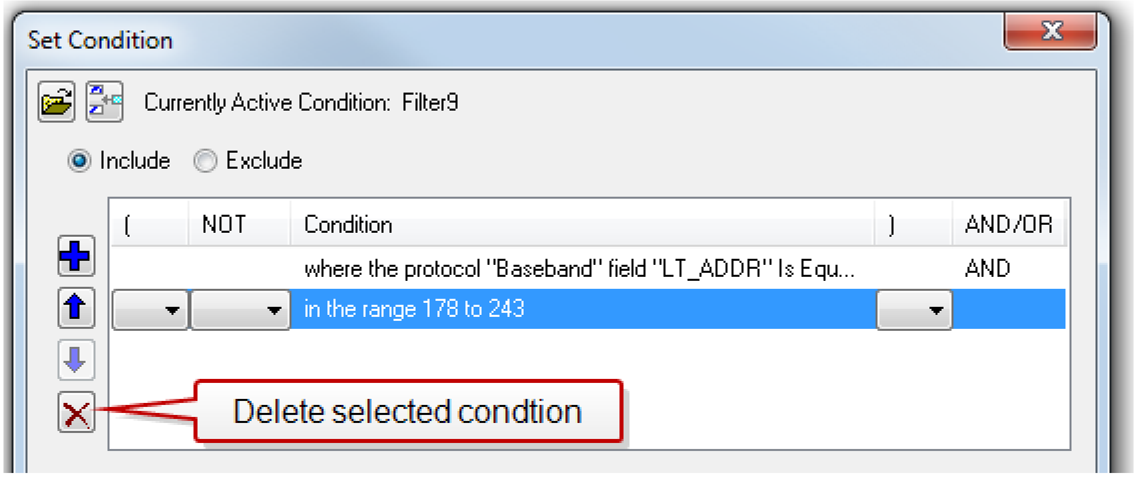


Figure 93. Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.

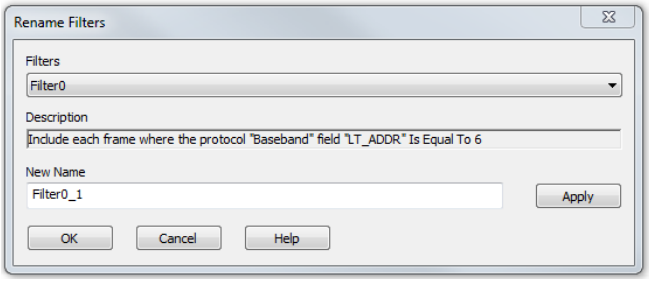
3. Click the Delete Selected Line ☒ icon.

4. Edit the Boolean operators and parentheses as needed.

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

5.3.1.7.3 Renaming a Display Filter

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


Rename Filters

Filters: Filter0

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

New Name: Filter0_1

Figure 94. Rename Filters Dialog

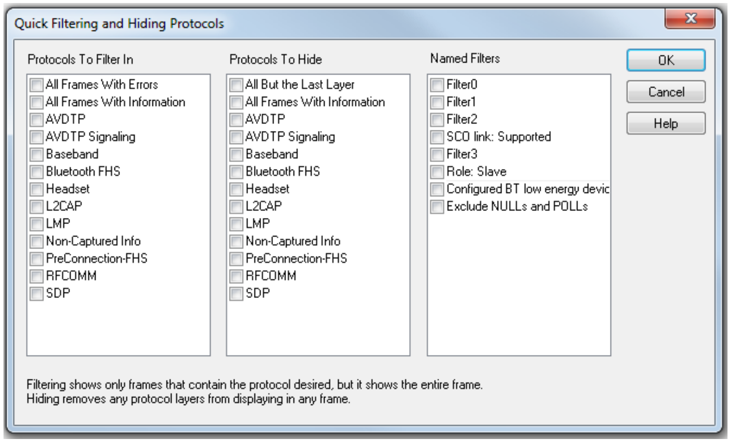
2. Select the filter to be renamed from the combo box.

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

5.3.2 Protocol Filtering From the Frame Display

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

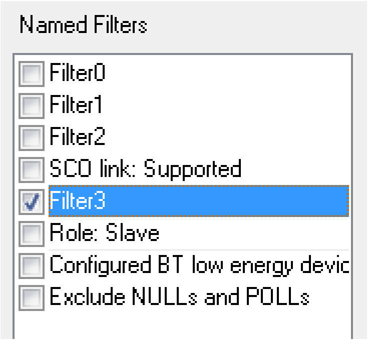
Filtering shows only frames that contain the protocol desired, but it shows the entire frame.
Hiding removes any protocol layers from displaying in any frame.

Figure 95. 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.

Filter3

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

5.3.2.1 Filtering On the Summary Layer Protocol

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

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

5.3.2.2 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

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

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.

Chapter 6: Saving and Importing Data

6.1 Saving Your Data

You can save all or part of the data that you have captured. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.

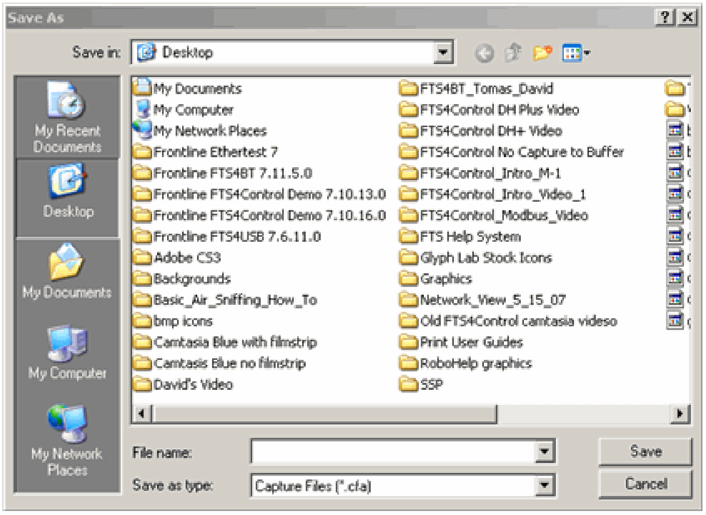
On the Control toolbar you can set up to capture a single file or series of files. Click here to see those settings.

There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data.

6.1.1 Saving the Entire Capture File using File Save or the Save icon

This option is only available when you select Single File from the Capture Mode on System Settings. Click here to learn more about selecting Save options from System Settings.

1. If you are capturing data, click on the Stop icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the Event Display or Frame Display window.
3. Click the Save icon, or select Save from the File menu.



Save in: Desktop

File name:

Save as type: Capture Files (*.cfa)

Figure 96. Windows Save dialog

4. Type a file name in the File name box at the bottom of the screen.

5. Browse to select a specific directory. Otherwise your file is saved in the default capture file directory.

6. When you are finished, click OK.

6.1.2 Saving the Entire Capture File with Save Selection

1. If you are capturing data, click on the Stop icon to stop data capture. You cannot save data to file while it is being captured.

2. Open the Event Display or Frame Display window.

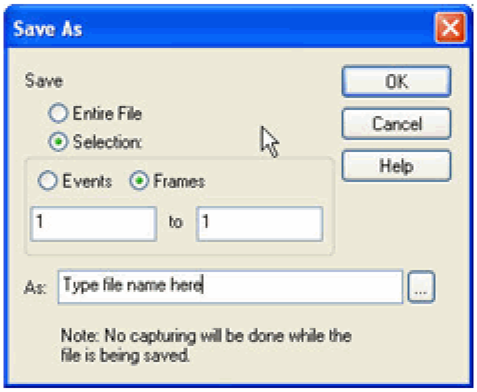
3. Right click in the data

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

5. Click on the radio button labeled Entire File.

6. Choose to save Events or Frames . Choosing to save Events saves the entire contents of the capture file. Choosing to save Frames does not save all events in the capture file.

7. Type a file name in the As box at the bottom of the screen. Click the Browse icon to browse to a specific directory. Otherwise your file is saved in the



Save
○ Entire File
● Selection:
○ Events ● Frames
1 to 1

As: Type file name here

Note: No capturing will be done while the file is being saved.

default capture file directory.

8. When you are finished, click OK.

6.1.3 Saving a Portion of a Capture File

1. If you are capturing data, click on the Stop icon to pause data capture. You cannot save data to a file while it is being captured.

2. Open the Event Display or Frame Display window, depending on whether you want to specify a range in bytes or in frames.

3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range, or use the Shift key with the keyboard arrows or the navigation icons in the Frame Display toolbar. If the range you want to save is too large to select, note the numbers of the first and last item in the range.

4. Right click in the data

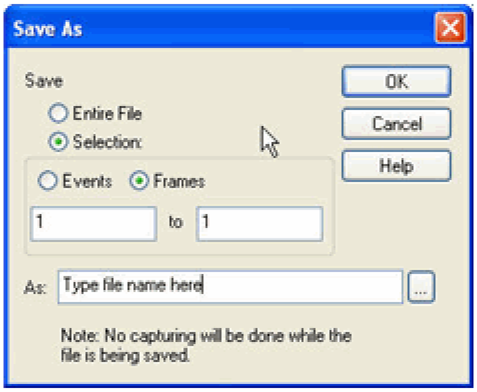
5. Select Save Selection or Save As from the right click menu

6. Click on the radio button labeled Selection. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes.

7. Select either Events or Frames to indicate whether the numbers are event or frame numbers.

8. Type a file name in the As box at the bottom of the screen. Click the Browse icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.

9. Click OK when you are finished.


Save As

Save
○ Entire File
● Selection:
○ Events ● Frames
1 to 1
As: Type file name here
Note: No capturing will be done while the file is being saved.

6.1.4 Confirm Capture File (CFA) Changes

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

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

- Save To This File – Saves the changes you have made to the current capture file.
- Save As – Saves the changes to a new file.

- Cancel the Close Operation – Closes the file and returns you back to the display. No changes are saved.
- Discard Changes – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

6.1.5 Adding Comments to a Capture File

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

To open the Notes window :

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

6.2 Loading and Importing a Capture File

6.2.1 Loading a Capture File

From the Control Window:

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

6.2.2 Importing Capture Files

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

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

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

At present, the analyzer supports the following file types:

- Frontline Serialtest* Async and Serialtest ComProbe® for DOS – requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- Greenleaf ViewComm* 3.0 for DOS - requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- Frontline Ethertest* for DOS – requires 3 files: filename.cap, filename.ca0 and filename.ca1.
- Sniffer Type 1 – supports files with the .enc extension. Does not support Sniffer files with a .cap extension.
- Snoop or Sun Snoop – files with a .cap extension based on RFC 1761. For file format, see http://www.-faqs.org/rfcs/rfc1761.html.
- Shomiti Surveyor files in Snoop format – files with a .cap extension. For file format, contact Technical Support.
- CATC Merlin - files with a .csv extension. Files must be exported with a specific format. See File Format for Merlin Files for information.
- CATC Chief - files with a .txt extension.

6.3 Printing

6.3.1 Printing from the Frame Display/HTML Export

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

Frame Display Print

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

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

Print Background Colors Using Internet Explorer

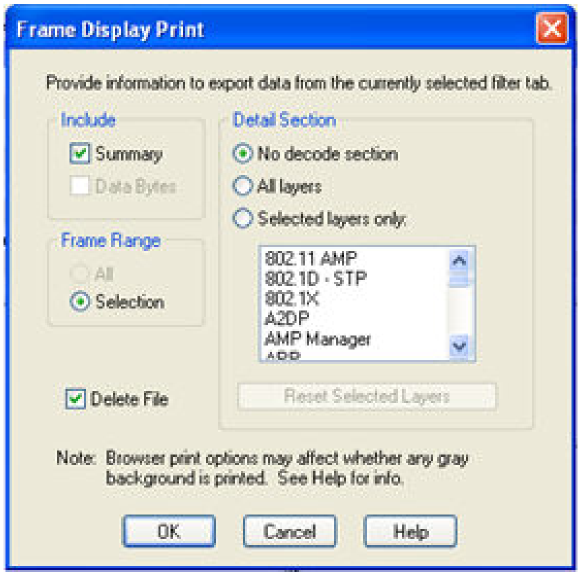
1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

Configure the Print File Range in the Frame Display Print Dialog

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

How to Print Frame Display Data

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



Frame Display Print

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

Include

☑ Summary

☐ Data Bytes

Frame Range

○ All

● Selection

☑ Delete File

Detail Section

● No decode section

○ All layers

○ Selected layers only:

802.11 AMP
802.1D - STP
802.1X
A2DP
AMP Manager

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

Figure 97. Frame Display Print Dialog

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

   Choosing All prints up to 1000 frames from the buffer.

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

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

7. Click the OK button.

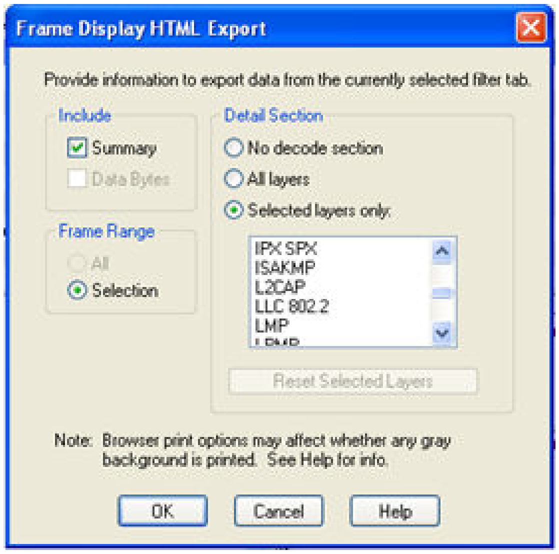
If you chose Print Preview, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file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

Frame Display HTML Export

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

How to export display data to an .html file

1. Select HTML Export from the File menu on the Frame Display window to display the Frame Display HTML Export.



Frame Display HTML Export

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

Include
☑ Summary
□ Data Bytes

Frame Range
○ All
● Selection

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

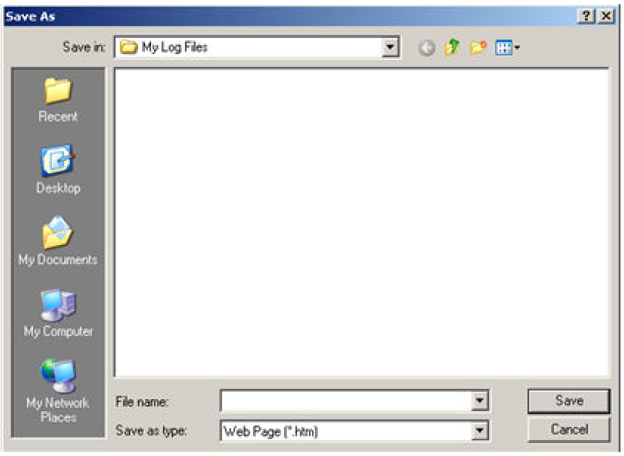
Note: Browser print options may affect whether any gray background is printed. See Help for info.

Figure 98. Frame Display HTML Export Dialog

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

3. Click the OK button.

   The Save As dialog appears



Save As

Save in: My Log Files

File name:

Save as type: Web Page (*.htm)

Figure 99. Save As Dialog

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

5. Select Save

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

6.3.2 Printing from the Event Display

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

Print Background Colors Using Internet Explorer

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

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

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

Configure the Print File Range in the Event Display Print dialog

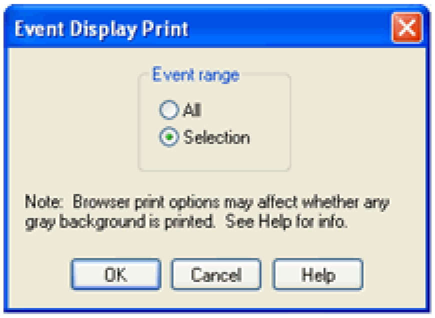
Selecting more than one event in the Event Display window defaults the radio button in the Event Display Print dialog to Selection and allows the user to choose the All radio button. When only one event is selected , the All radio button in the Event Display Print dialog is selected.

How to Print Event Display Data to a Browser

1. Select Print or Print Preview from the File menu on the Event Display window to display the Event Display Print dialog. Select Print if you just want to print your data to your default printer. Select Print Preview if you want access to printer options.
2. Select the range of events to include from either All or Selection in the Event Range section of the Event Display Print dialog. Choosing All prints all of the events in the capture file or buffer. Choosing Selection prints only the selected events in the Event Display window.

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

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



Event Display Print

Event range

○ All
● Selection

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

Figure 100. Event Display Print Dialog

3. Click the OK button.

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

6.4 Exporting

6.4.1 Frame Display Export

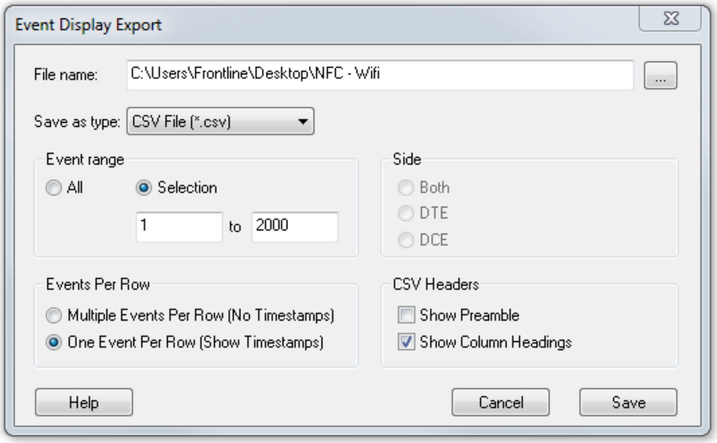
You can dump the contents of the Summary pane on the Frame Display into a Comma Separated File (.csv).

To access this feature:

1. Right click on the Summary pane or open the Frame Display File menu.
2. Select the Export… menu item.
3. Select a storage location and enter a File name.
4. Select Save.

6.4.2 Exporting a File with Event Display Export

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



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

Save as type: CSV File (*.csv)

Event range: ○ All ● Selection 1 to 2000

Side: ○ Both ○ DTE ○ DCE

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

CSV Headers: □ Show Preamble ☑ Show Column Headings

Figure 101. Event Display Export Example: .csv file.

How to Export Event Display Data to a File

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

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

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

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

   Binary File (*.bin)

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

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

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

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

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

   - Choose Host, Function\Control or Both to determine how you want to export the data.

5. Choose Host, Function\Control or Both to determine how you want to export the data.

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

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

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

.

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

Timestamp

Delta

Event Number

Byte Number

Frame Number

Type

Hex

Dec

Oct

Bin

Side

ASCII | 7-bit ASCII | EBCDIC | Baudot

RTS

CTS

DSR

DTR

CD

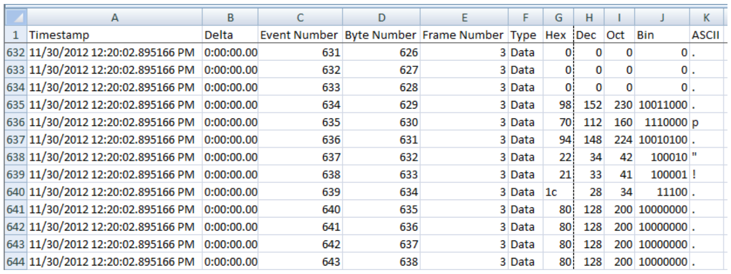
RI

UART Overrun

Parity Error

Framing Error

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



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

Figure 102. Example: .csv Event Display Export, Excel spreadsheet

6.4.2.1 Export Filter Out

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

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

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

6.4.2.2 Exporting Baudot

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

Chapter 7: General Information

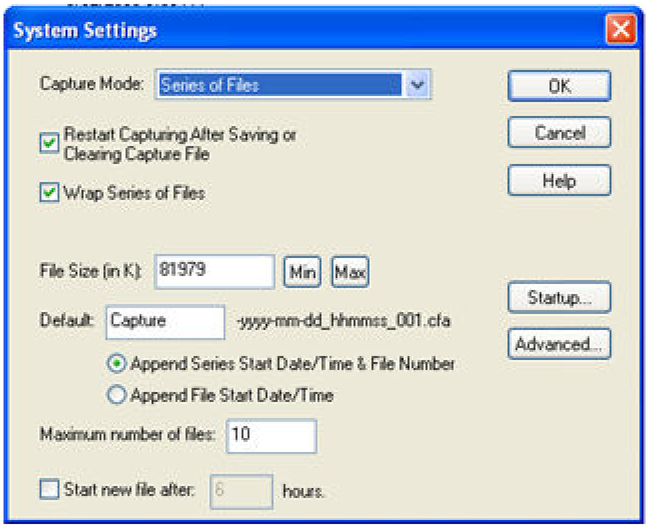
7.1 System Settings and Progam Options

7.1.1 System Settings

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

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

7.1.1.1 Series of files



Capture Mode: Series of Files

☑ Restart Capturing After Saving or Clearing Capture File

☑ Wrap Series of Files

File Size (in K): 81979

Default: Capture -yyyy-mm-dd_hhmmss_001.cfa

● Append Series Start Date/Time & File Number

○ Append File Start Date/Time

Maximum number of files: 10

□ Start new file after: 6 hours.

Figure 103. System Settings for defining how to capture data

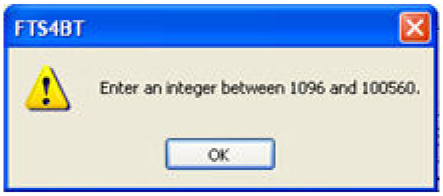
This option lets you capture to more than one file, based on file size or time.

- Restart Capturing After Saving or Clearing Capture File: the analyzer restarts capture to the file immediately after the file is closed.
- Wrap Series of Files: When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.
- File Size:

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

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

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



Enter an integer between 1096 and 100560.

- Default:

  Enter a name for the capture file in the Default text box. Each saved file will begin with this name. The name of each file is the name you give it in the Name box followed by the date, time and a number. The date and time are when the series was opened. The number increments with each file. This guarantees unique file names are created.

- Append Series Start/Date & File Number:

  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) and file number (001) when capturing a series of files.

- Append File Start Date/Time:

  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) when capturing a single file.

- Maximum number of files:

  Set the maximum number of files in the series in the Maximum number of files box. The next file starts when the currently open file is full.

- Start new file after:

  If you want to start a new file on a periodic basis, check the box for Start new file after and put in the number of hours after which a new file is started. Note that if the currently open file becomes full before the time limit has been reached, a new file is opened immediately rather than lose data. Capturing stops if the maximum number of files has been used unless Wrap Files has been checked. If Wrap Files has been checked the analyzer erases the oldest file in the series and makes a new file.

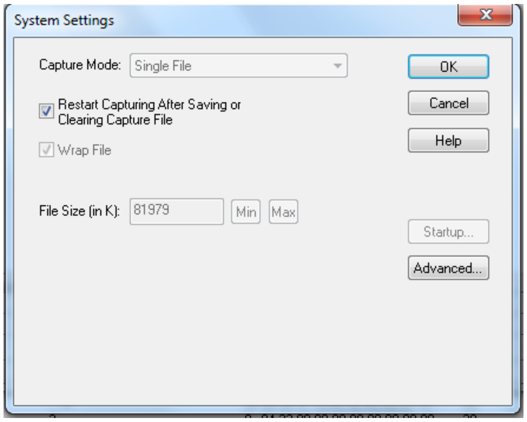
- Start up

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

- Advanced

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

7.1.1.2 Single File

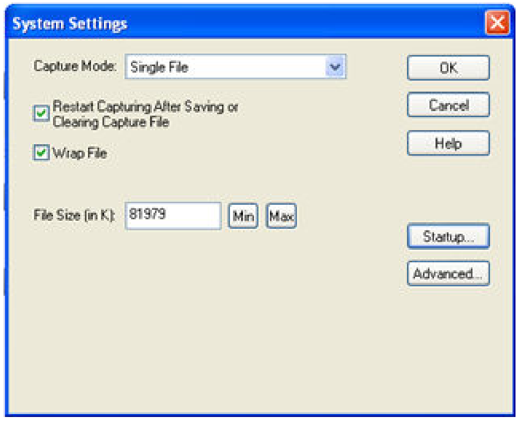

System Settings

Capture Mode: Single File

☑ Restart Capturing After Saving or Clearing Capture File

☑ Wrap File

File Size (in K): 81979


System Settings

Capture Mode: Single File

☑ Restart Capturing After Saving or Clearing Capture File

☑ Wrap File

File Size (in K): 81979

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

7.1.1.3 Common Options

- Restart Capturing After Saving or Clearing Capture File

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

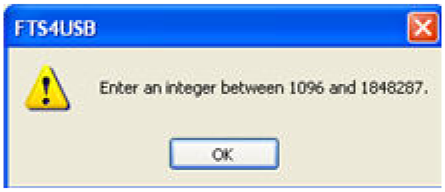
- Wrap File

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

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

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

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


FTS4USB

Enter an integer between 1096 and 1848287.

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

- Start up

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

- Advanced

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

7.1.1.4 System Settings - Disabled/Enabled Options

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

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

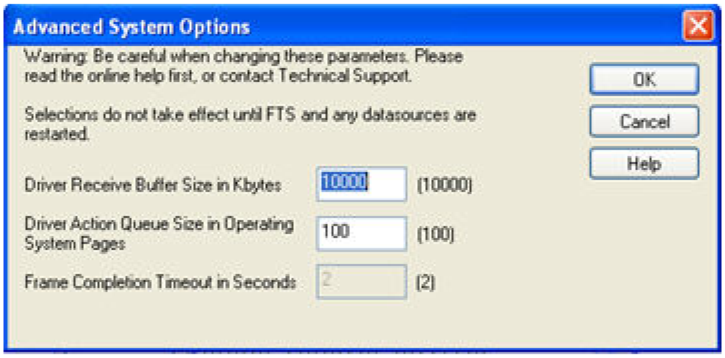
7.1.1.5 Advanced System Options

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

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

To access the Advanced System Options:

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



Advanced System Options

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

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

Driver Receive Buffer Size in Kbytes: 10000 (10000)

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

Frame Completion Timeout in Seconds: 2 (2)

Figure 104. Advanced System Options dialog

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

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

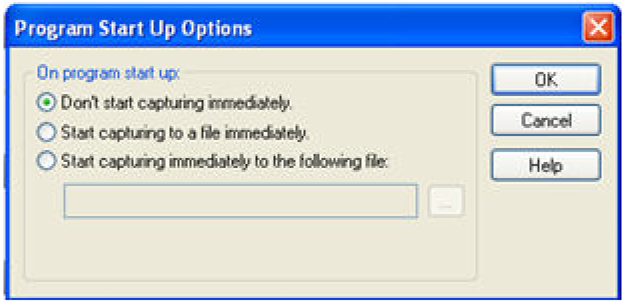
  The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

Note: This option is currently disabled.

7.1.1.6 Selecting Start Up Options

To open this window:

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



Program Start Up Options

On program start up:

● Don't start capturing immediately.

○ Start capturing to a file immediately.

○ Start capturing immediately to the following file:

Figure 105. Start Up Options dialog

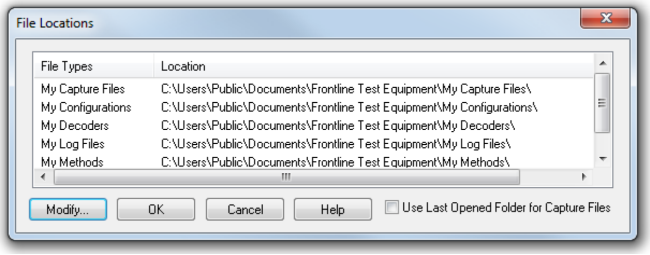
- Don't start capturing immediately - This is the default setting. The analyzer begins monitoring data but does not begin capturing data until clicking the Start Capture ● icon on the Control, Event Display or Frame Display windows.
- Start capturing to a file immediately - When the analyzer starts up,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

7.1.2 Changing Default File Locations

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

Follow the steps below to change the default locations.

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



File Locations

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

□ Use Last Opened Folder for Capture Files

Figure 106. File Locations dialog

2. Select the default location you wish to change.
3. Click Modify.

4. Browse to a new location.

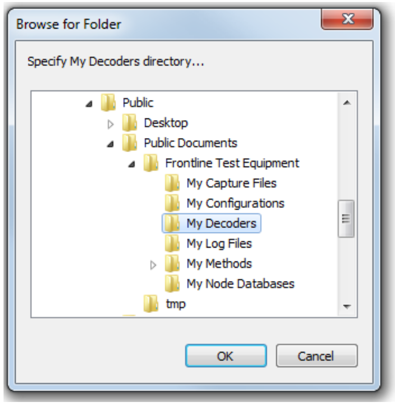


Figure 107. File Locations Browse dialog

5. Click OK.

6. Click OK when finished.

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

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

Default Capture File Folder Checkbox

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

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

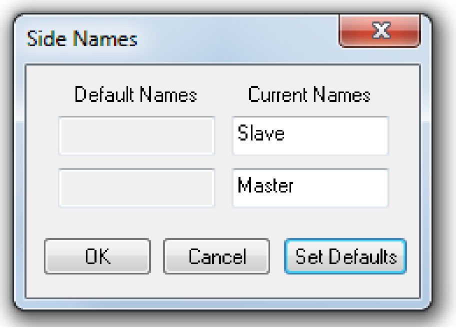
where the last file was opened from or saved to, if Use Last Opened Folder for Capture Files is checked. If, however, the location is not accessible, files are saved to the default directory that is set at installation.

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

7.1.3 Side Names

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

Changes to the Names are used throughout the program.



Default Names	Current Names
	Slave
	Master

Figure 108. Example: Side Names Where "Slave" and "Master" are current

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

7.1.4 Timestamping

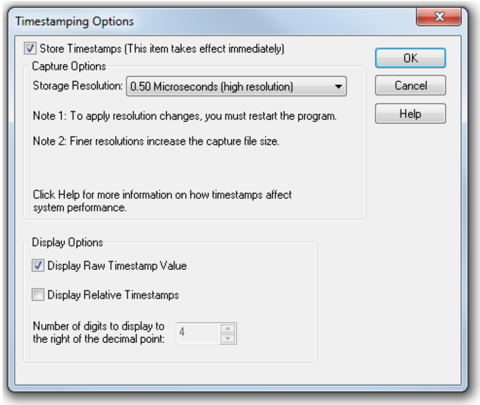
Timestamping is the process of precise recording in time of packet arrival. Timestamps is an optional parameter in the Frame Display and Event Display that can assist in troubleshooting a network link.

7.1.4.1 Timestamping Options

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

To open this window:

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



☑ Store Timestamps (This item takes effect immediately)

Capture Options

Storage Resolution: 0.50 Microseconds (high resolution)

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

Note 2: Finer resolutions increase the capture file size.

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

Display Options

☑ Display Raw Timestamp Value

□ Display Relative Timestamps

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

Figure 109. Timestamping Options dialog

7.1.4.1.1 Enabling/Disabling Timestamp

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

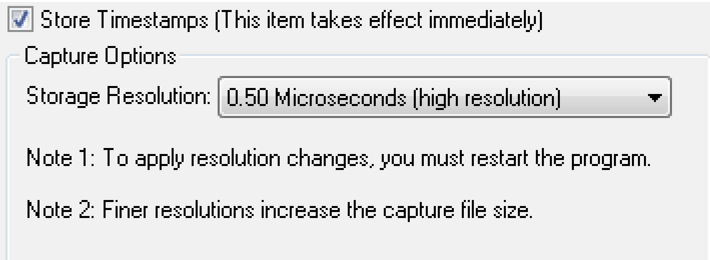
7.1.4.1.2 Changing the Timestamp Resolution

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

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

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

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



☑ Store Timestamps (This item takes effect immediately)

Capture Options

Storage Resolution: 0.50 Microseconds (high resolution)

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

Note 2: Finer resolutions increase the capture file size.

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

7.1.4.1.2.1 Performance Issues with High Resolution Timestamp

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

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

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

7.1.4.1.3 Switching Between Relative and Absolute Time

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

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

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

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

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

7.1.4.1.4 Displaying Fractions of a Second

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

7.2 Technical Information

7.2.1 Performance Notes

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

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

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

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

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

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

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

7.2.2 Progress Bars

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

The title on the progress bar indicates the process underway.

7.2.3 Event Numbering

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

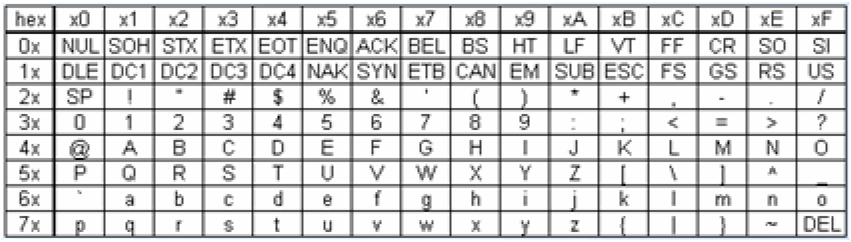
When the analyzer captures an event, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8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

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

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

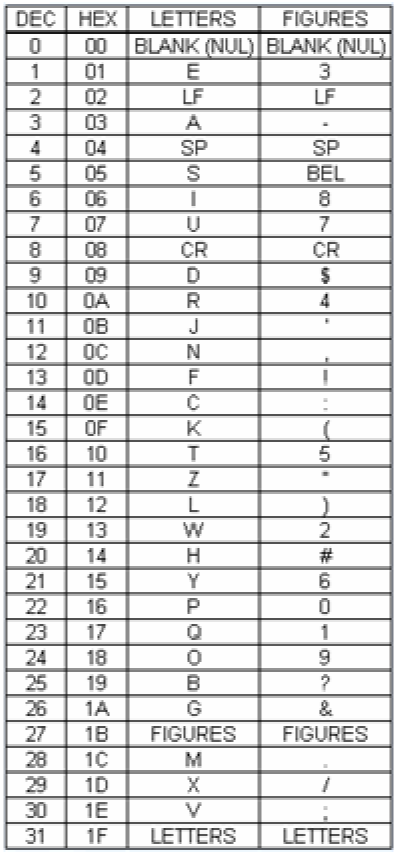
7.2.4 Useful Character Tables

7.2.4.1 ASCII Codes



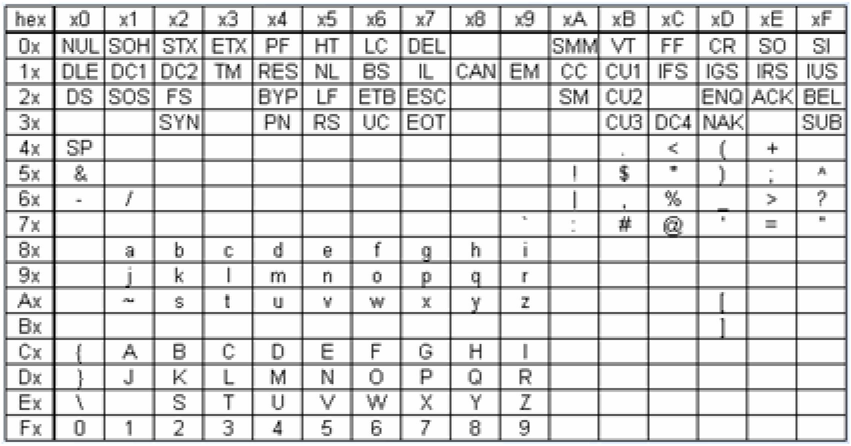
hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y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

7.2.4.2 Baudot Codes



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

7.2.4.3 EBCDIC Codes



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

7.2.4.4 Communication Control Characters

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

Communications Control Characters

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

Communications Control Characters(continued)

Abbreviation	Control Character	Text
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit Separator
VT	VT	Vertical Tabulation

7.2.5 The Frontline Serial Driver

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

7.3 Contacting Technical Support

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

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

Email: tech_support@fte.com

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

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

7.3.1 Instructional Videos

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

Appendix A: Application Notes

A.1 Decrypting Encrypted Bluetooth low energy

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

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

A.1.2 Pairing

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

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

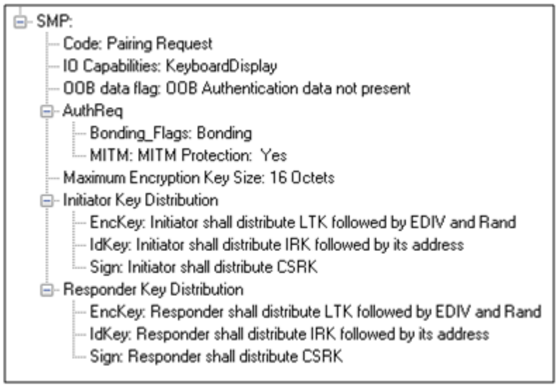
This paper will focus on the LTK.

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

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

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

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



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

Figure 110. Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

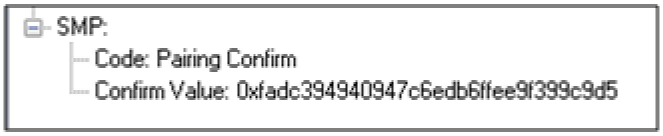
Of particular importance to decrypting the encrypted data on a Bluetooth low energy link is LTK, EDIV, and Rand.

A.1.3 Pairing Methods

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

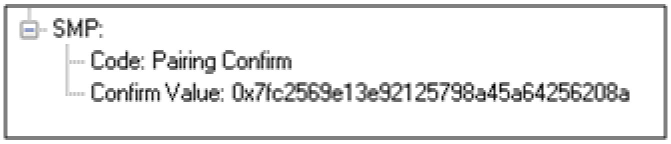
In **Just Works** the TK = 0. In the **Passkey Entry** method,

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



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

Initiator Pairing Confirm Example (ComProbeFrame Display, BPA 600 low energy capture)



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

.

Responder Pairing Confirm Example (ComProbeFrame Display, BPA 600 low energy capture)

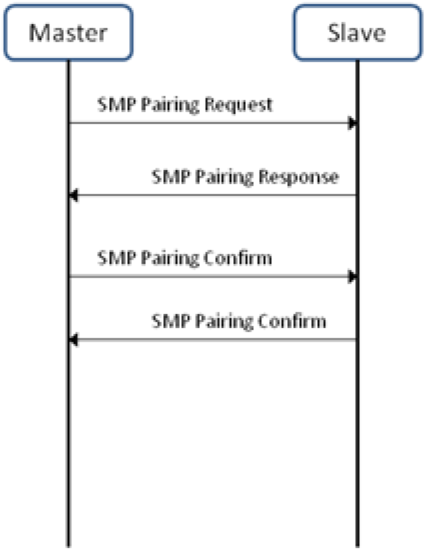


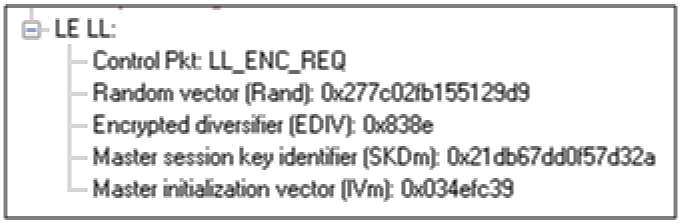
Figure 111. Message Sequence Chart: SMP Pairing

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

A.1.4 Encrypting the Link

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

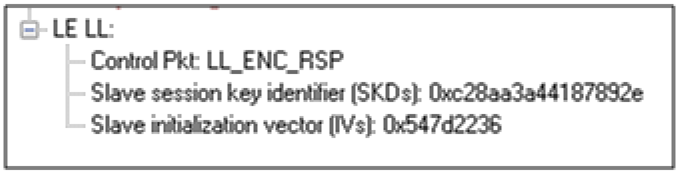
A.1.5 Encryption Key Generation and Distribution



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

Figure 112. Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

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



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

Figure 113. Encryption Response from Slave, Example (ComProbe Frame Display, BPA 600 low energy capture)

A.1.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The SK is created using a session key diversifier (SKD). The first step in a link encryption is for the master device to send Link Layer encryption request message (LL_ENC_REQ) that contains the SKD$_{master}$. TheSKD$_{master}$ is generated using the LTK. The slave receives SKD$_{master}$, generates SKD$_{slave}$, and generates SK by concatenating parts ofSKD$_{master}$ and SKD$_{slave}$. The slave device responds with an encryption response message (LL_ENC_RESP) that contains SKD$_{slave}$; the master will create the same SK.

The master and slave devices will now begin a handshake process. In this instance the master wants to transmit encrypted data, so the master will transmit unencrypted LL_START_ENC_REQ, but is set to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_RESP that uses the same SK just calculated and setting up to receive encrypted data. Once the slave receives the master’s encrypted LL_START_RESP message and responds with an encrypted LL_START_RESP message. The Bluetooth low energy devices can now begin transmitting and receiving encrypted data. This process is reversed should the slave want to transmit encrypted data.

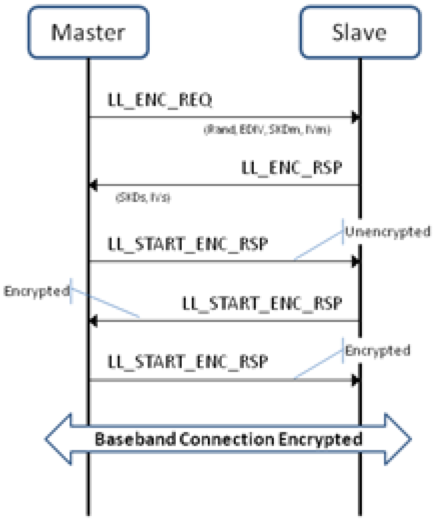


Figure 114. Message Sequence Chart: Link Layer Encryption

A.1.7 Decrypting Encrypted Data Using ComProbe® BPA 600 low energy Capture

Note: The following discussion uses the ComProbe BPA 600 in low energy capture mode to illustrate how to identify the encryption process and to view decrypted data. However any of the ComProbe devices (BPA 500, BPA low energy, or Sodera) that are low energy capable will accomplish the same objectives, although the datasource setup will be slightly different for each device.

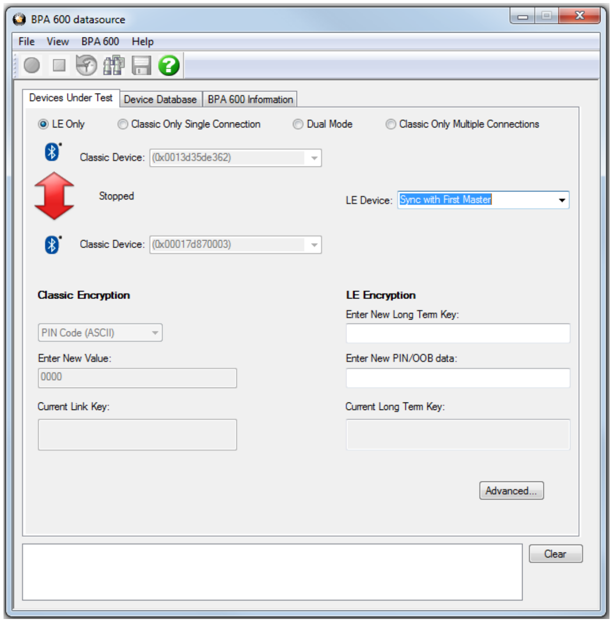
A.1.7.1 Setting up the BPA 600

1. Run the ComProbe Protocol Analysis Software and select Bluetooth Classic/low energy (BPA 600). This will bring up the BPA 600 datasource window. This is where the parameters are set for sniffing, including the devices to be sniffed and how the link is to be decrypted.

2. Select Devices Under Test tab on the Datasource window.

3. Click/select LE Only.

4. To decrypt encrypted data transmissions between the Bluetooth low energy devices the ComProbe analyzer needs to know the LTK because this is the shared secret used to encrypt the session. There are two ways to provide this information and which to select will depend on the pairing method: **Just Works** or **Passkey Entry**.



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

Classic Device: (0x0013d35de362)

Stopped

LE Device: Sync with First Master

Classic Device: (0x00017d870003)

Classic Encryption

PIN Code (ASCII)

Enter New Value: 0000

Current Link Key:

LE Encryption

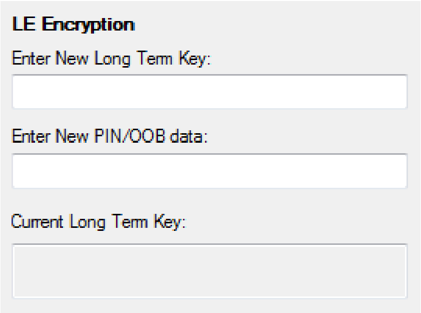
Enter New Long Term Key:

Enter New PIN/OOB data:

Current Long Term Key:

Figure 115. ComProbe BPA 600 low energy only datasource settings

a. **Passkey Entry** is easiest if you have the code that was displayed or entered during device pairing. The code is what is used to generate the LTK. Under LE Encryption enter the code in the Enter New PIN/OOB data text box.



LE Encryption

Enter New Long Term Key:

Enter New PIN/OOB data:

Current Long Term Key:

Figure 116. BPA 600 datasource Encryption Key Entry

b. **Just Works** is more of a challenge because you must know the LTK that is created at the time of pairing and identification of an encrypted link.

- If your device was previously used in an encrypted capture session, the device information including LTK can be found in the Device Database tab.

- In a design and development environment the LTK is often known beforehand.

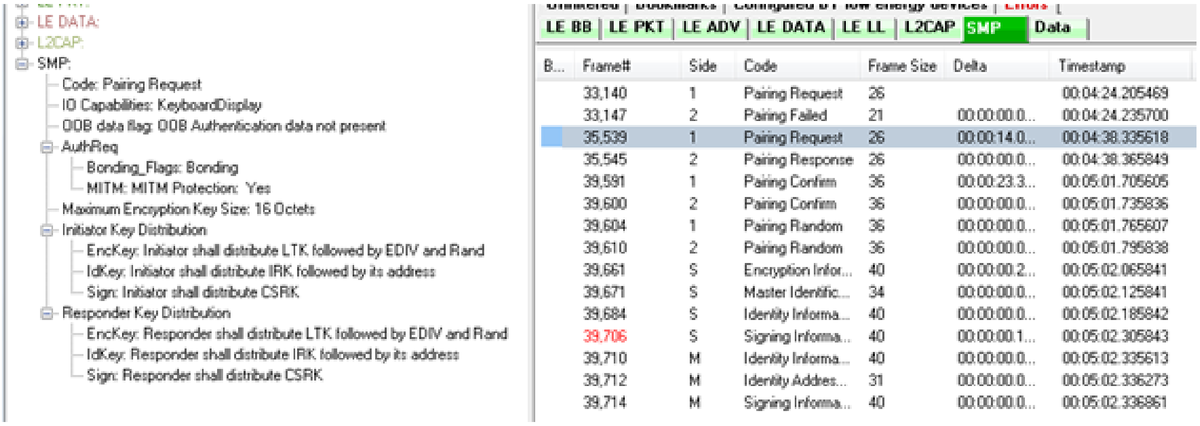
- Capture of Host Controller Interface (HCI) events using ComProbe HSU can reveal the LTK, which is contained in the HCI_Link_Key_Request_Reply command. HCI capture is through direct connection to the device host controller. The information obtained in a direct connection can later be used in a wireless encrypted capture session that requires prior knowledge of encryption keys.

5. To start capture click on the Start Sniffing button ● on the BPA 600 datasource toolbar.

A.1.7.2 Use Frame Display to View Encryption/Decryption Process

A.1.7.2.1 Security Manager Protocol

The Security Manager Protocol (SMP) controls the process for pairing and key distribution. The results of a pairing and key distribution can be observed in the ComProbe software **Frame Display**. Activate the **Frame Display** by clicking on the icon on the **Control** window toolbar. On the **Frame Display** low energy protocols are shown in light green tabs. Click on the **SMP** protocol tab that will show only the SMP commands from the full data set.



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

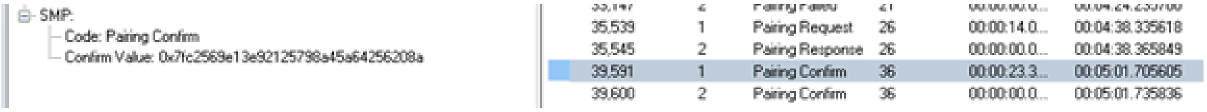
B...	Frame#	Side	Code	Frame Size	Delta	Timestamp
	33,140	1	Pairing Request	26		00:04:24.205469
	33,147	2	Pairing Failed	21	00:00:00.0...	00:04:24.235700
	35,539	1	Pairing Request	26	00:00:14.0...	00:04:38.335618
	35,545	2	Pairing Response	26	00:00:00.0...	00:04:38.365849
	39,591	1	Pairing Confirm	36	00:00:23.3...	00:05:01.705605
	39,600	2	Pairing Confirm	36	00:00:00.0...	00:05:01.735836
	39,604	1	Pairing Random	36	00:00:00.0...	00:05:01.765607
	39,610	2	Pairing Random	36	00:00:00.0...	00:05:01.795838
	39,661	S	Encryption Infor...	40	00:00:00.2...	00:05:02.065841
	39,671	S	Master Identific...	34	00:00:00.0...	00:05:02.125841
	39,684	S	Identity Informa...	40	00:00:00.0...	00:05:02.185842
	39,706	S	Signing Informa...	40	00:00:00.1...	00:05:02.305843
	39,710	M	Identity Informa...	40	00:00:00.0...	00:05:02.335613
	39,712	M	Identity Addres...	31	00:00:00.0...	00:05:02.336273
	39,714	M	Signing Informa...	40	00:00:00.0...	00:05:02.336861

Figure 117. SMP Pairing Request (Frame# 35,539) from Initiator (Side 1)

On the left side of the figure above is the Frame Display Decoder pane that shows the decoded information supplied in the selected frame in the Summary pane, Frame# 35,539. Shown is the SMP data associated with and encrypted link (MITM Protection = Yes). The requested keys are also shown. Selecting Frame# 35,545 would provide the response from the responder (Side 2) and would contain similar information.

Selecting Frame# 39,591 will display the Pairing Confirm from the initiator (Side 1) in the Decoder pane. The Confirm Value shown is the Mconfirm 128-bit random number that contains TK, Pairing Request command, Pairing Response command, initiating device address, and the responding device address. Selecting Frame# 39,600 would provide the Sconfirm random number from the responder (Side 2) with similar information from that device but the random number would be different than Mconfirm.

Once pairing is complete and an encrypted session established, the keys are distributed by the master and slave now identified by Side = M and Side = S respectively in the Summary pane. In Frame# 39,661 the slave has distributed LTK to the master to allow exchange of encrypted data. Frame# 39,661 through 39,714 in the Summary pane SMP tab are the key distribution frames.

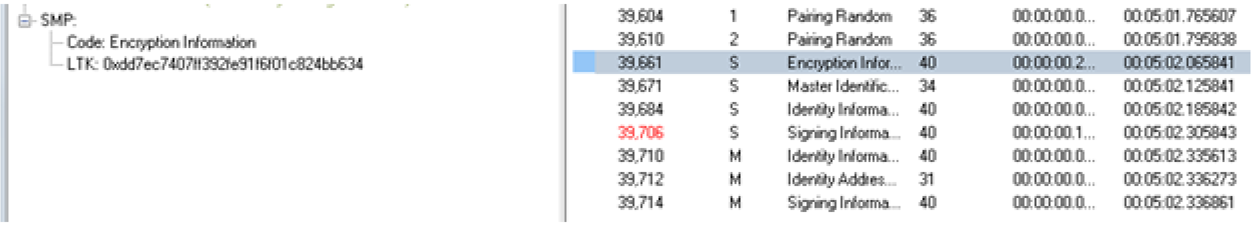


```
SMP:
  Code: Pairing Confirm
  Confirm Value: 0x7fc2569e13e92125798a45a64256208a
```

```
35,539    1    Pairing Request     26    00:00:14.0...    00:04:38.335618
35,545    2    Pairing Response    26    00:00:00.0...    00:04:38.365849
39,591    1    Pairing Confirm     36    00:00:23.3...    00:05:01.705605
39,600    2    Pairing Confirm     36    00:00:00.0...    00:05:01.735836
```

Figure 118. SMP Pairing Confirm (Frame# 39,591) from Initiator (Side 1)

Figure 119.



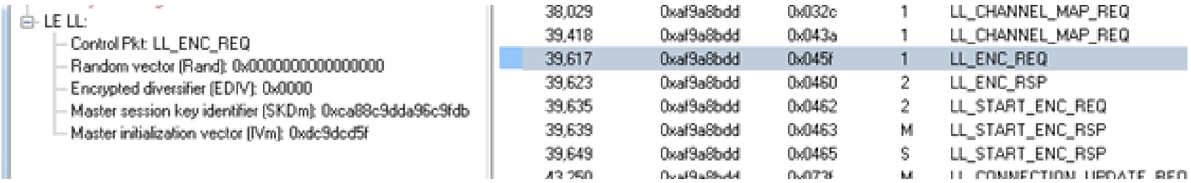
```
SMP:
  Code: Encryption Information
  LTK: 0xdd7ec7407ff392fe91f6f01c824bb634
```

```
39,604    1    Pairing Random        36    00:00:00.0...    00:05:01.765607
39,610    2    Pairing Random        36    00:00:00.0...    00:05:01.795838
39,661    S    Encryption Infor...   40    00:00:00.2...    00:05:02.065841
39,671    S    Master Identific...   34    00:00:00.0...    00:05:02.125841
39,684    S    Identity Informa...   40    00:00:00.0...    00:05:02.185842
39,706    S    Signing Informa...    40    00:00:00.1...    00:05:02.305843
39,710    M    Identity Informa...   40    00:00:00.0...    00:05:02.335613
39,712    M    Identity Addres...    31    00:00:00.0...    00:05:02.336273
39,714    M    Signing Informa...    40    00:00:00.0...    00:05:02.336861
```

Figure 120. SMP Key Distribution Frames

A.1.7.2.2 Link Layer

The Link Layer (LL) protocol manages the Bluetooth low energy radio transmissions and is involved in starting link encryption. To observe the decoded LL commands, click on the Frame Display LE LL tab, search for and select ControlPkt "LL_ENC_REQ". This command should originate with Side 1, the initiator of the encryption link. In Figure 11 Frame# 39,617 is selected in the Summary pane and we see the decoded LE LL frame is display in the Decoder pane. Shown in this frame packet is the SKDm that is the Master Session Key Diversifier (SKDmaster). In Frame# 39,623 you will find SKDslave that is combined with SKDmaster to create the Session Key (SK). Both SDKs were created using the LTK. Frame# 39,635 through 39,649 in the LE LL tab completes starting of the encryption process. After the slave sends LL_START_ENC_RSP (Frame# 36,649) the Bluetooth devices can exchange encrypted data, and the ComProbe sniffing device can also receive and decrypt the encrypted data because the appropriate "key" is provided in the BPA 600 Datasource window.



```
LE LL:
  Control Pkt: LL_ENC_REQ
  Random vector (Rand): 0x0000000000000000
  Encrypted diversifier (EDIV): 0x0000
  Master session key identifier (SKDm): 0xca88c9dda96c9fdb
  Master initialization vector (IVm): 0xdc9dcd5f
```

```
38,029    0xaf9a8bdd    0x032c    1    LL_CHANNEL_MAP_REQ
39,418    0xaf9a8bdd    0x043a    1    LL_CHANNEL_MAP_REQ
39,617    0xaf9a8bdd    0x045f    1    LL_ENC_REQ
39,623    0xaf9a8bdd    0x0460    2    LL_ENC_RSP
39,635    0xaf9a8bdd    0x0462    2    LL_START_ENC_REQ
39,639    0xaf9a8bdd    0x0463    M    LL_START_ENC_RSP
39,649    0xaf9a8bdd    0x0465    S    LL_START_ENC_RSP
```

Figure 121. LE LL Tab Encryption Request (Frame# 39,617) from Initiator (Side 1)

A.1.7.3 Viewing Encryption in the Message Sequence Chart

The ComProbe software Message Sequence Chart (MSC) links directly to frames being viewed in the Frame Display. Similarly MSC will display the same information as the Frame Display Decoder pane. Frames are synchronized between the Frame Display Summary pane and the MSC, so clicking on a frame in either window will select that same frame in the other window. Also the protocol tabs are the same in each window. To see the pairing process, click on the SMP tab.

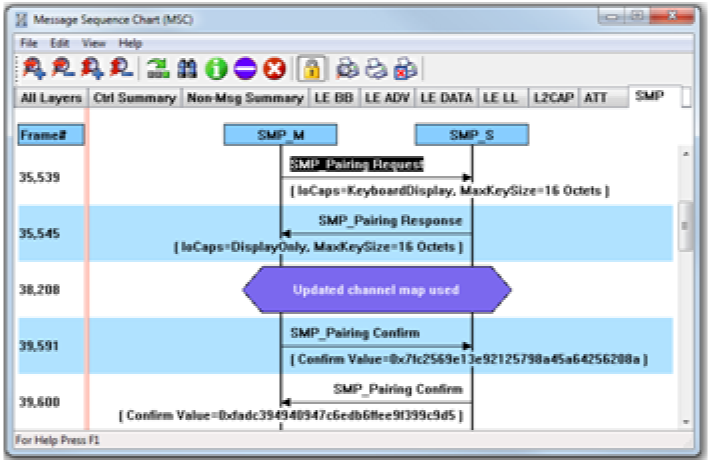

Message Sequence Chart (MSC)
File Edit View Help
All Layers | Ctrl Summary | Non-Msg Summary | LE BB | LE ADV | LE DATA | LE LL | L2CAP | ATT | SMP
Frame#
SMP_M
SMP_S
35,539
SMP_Pairing Request
[IoCaps=KeyboardDisplay, MaxKeySize=16 Octets]
35,545
SMP_Pairing Response
[IoCaps=DisplayOnly, MaxKeySize=16 Octets]
38,208
Updated channel map used
39,591
SMP_Pairing Confirm
[Confirm Value=0x7fc2569e13e92125798a45a64256208a]
39,600
SMP_Pairing Confirm
[Confirm Value=0xdadc394940947c6edb6ffee9f399c9d5]
For Help Press F1

Figure 122. MSC SMP Paring (BPA 600 low energy capture)

In the image above we see Frame# 35,539 initiating the pairing from the master device. The response, SMP_Pairing Response, is sent from the slave in Frame# 35,545. SMP_Pairing Confirm occurs between the master and the slave devices at Frame# 39,591 and 39,600 respectively.

Clicking on the MSC LE LL tab will show the process of encrypting a session link. Clicking on Frame# 39,617 displays the LL_ENC_REQ command from the master to the slave. In the MSC below this command you will see the data transferred that includes SKD_{master} used to generate the LTK. At Frame# 39,623 the slave responds with LL_ENC_RSP sending SKD_{slave} to generate LTK at the master. Up to this point all transmissions are unencrypted. For this example the slave sends the request to start encryption, LL_START_ENC_REQ, at Frame#39,635. The master responds with LL_START_ENC_RSP at Frame# 39,639, and finally the slave responds with LL_START_ENC_RSP at Frame# 36,649. At this point the session link is encrypted.

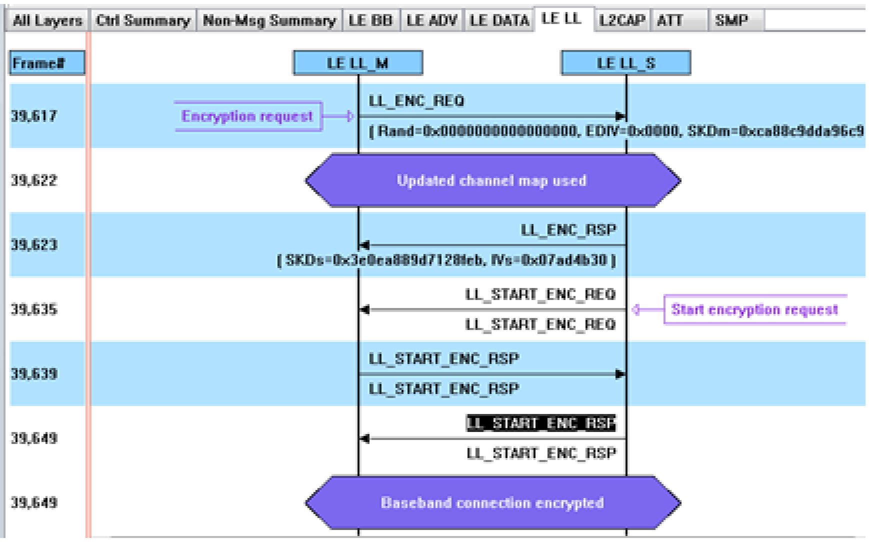
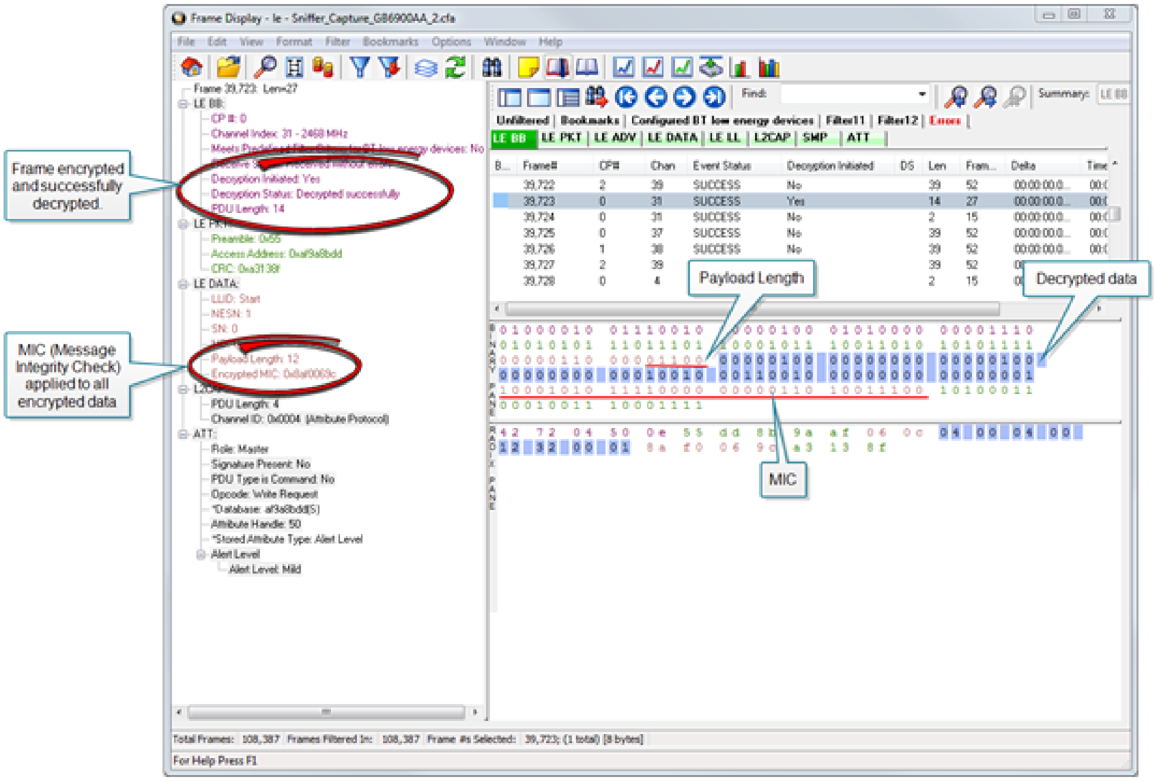


Figure 123. MSC link Layer Encryption (BPA 600 low energy capture)

A.1.7.4 Viewing Decrypted Data

In the ComProbe software Frame Display click on the LE BB tab. Search in the Summary pane for Decryption Initiated = Yes frames. In the example depicted in the following figure, Frame# 39723 is selected. In the Decoder pane LE BB shows that the decryption was initiated and decryption was successful. In LE Data we see the Encrypted MIC value. The MIC value is used to authenticate the sender of the data packet to ensure that the data was sent by a peer device in the link and not by a third party attacker. The actual decrypted data appears between the Payload Length and the MIC in the packet. This is shown in the Binary pane below the Summary pane.


Frame encrypted and successfully decrypted.
MIC (Message Integrity Check) applied to all encrypted data
Payload Length
Decrypted data
MIC
Frame Display - le - Sniffer_Capture_GB6900AA_2.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: LE BB
Unfiltered | Bookmarks | Configured BT low energy devices | Filter11 | Filter12 | Errors
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | ATT
BINARY PANE
RADIX PANE

```
Frame 39,723: Len=27
LE BB:
    CP #: 0
    Channel Index: 31 - 2468 MHz
    Meets Predefined Filter Criteria for BT low energy devices: No
    Receive S... Received without error
    Decryption Initiated: Yes
    Decryption Status: Decrypted successfully
    PDU Length: 14
LE PKT:
    Preamble: 0x55
    Access Address: 0xaf9a8bdd
    CRC: 0xa3138f
LE DATA:
    LLID: Start
    NESN: 1
    SN: 0
    Payload Length: 12
    Encrypted MIC: 0x8af0069c
L2CAP:
    PDU Length: 4
    Channel ID: 0x0004 (Attribute Protocol)
ATT:
    Role: Master
    Signature Present: No
    PDU Type is Command: No
    Opcode: Write Request
    *Database: af9a8bdd[5]
    Attribute Handle: 50
    *Stored Attribute Type: Alert Level
    Alert Level
        Alert Level: Mild
```

B...	Frame#	CP#	Chan	Event Status	Decryption Initiated	DS	Len	Fram...	Delta	Time
	39,722	2	39	SUCCESS	No		39	52	00:00:00.0...	00:(
	39,723	0	31	SUCCESS	Yes		14	27	00:00:00.0...	00:(
	39,724	0	31	SUCCESS	No		2	15	00:00:00.0...	00:(
	39,725	0	37	SUCCESS	No		39	52	00:00:00.0...	00:(
	39,726	1	38	SUCCESS	No		39	52	00:00:00.0...	00:(
	39,727	2	39				39	52	0(	
	39,728	0	4				2	15	0(	

```
01000010  01110010  00000100  01010000  00001110
01010101  11011101  10001011  10011010  10101111
00000110  00001100  00000100  00000000  00000100
00000000  00010010  00110010  00000000  00000001
10001010  11110000  00000110  10011100  10100011
00010011  10001111

42 72 04 50 0e 55 dd 8b 9a af 06 0c 04 00 04 00
12 32 00 01 8a f0 06 9c a3 13 8f
```

```
Total Frames: 108,387   Frames Filtered In: 108,387   Frame #s Selected: 39,723; (1 total) [8 bytes]
For Help Press F1
```

Figure 124. Decrypted Data Example (Frame# 39,723)

A.1.8 Technical Support

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

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

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Author: John Trinkle

Publish Date: 9 April 2014

A.2 Bluetooth Virtual Sniffing

A.2.1 Introduction

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

This white paper discusses:

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

A.2.2 Why HCI Sniffing and Virtual Sniffing are Useful

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

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

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

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

A.2.3 *Bluetooth* Sniffing History

Frontline has a strong appreciation for the importance of HCI sniffing because of the way we got involved with *Bluetooth*. Because of our company history, we are uniquely qualified to offer a multi-mode analyzer that provides many ways to sniff and supports a wide variety of protocols. This brief *Bluetooth* sniffing history should help you understand our approach to *Bluetooth* protocol analysis.

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

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

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

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

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

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

A.2.4 Virtual Sniffing—What is it?

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

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

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

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

A.2.5 The Convenience and Reliability of Virtual Sniffing

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

This means:

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

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

A.2.6 How Virtual Sniffing Works

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

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

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

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

A.2.7 Virtual Sniffing and *Bluetooth* Stack Vendors

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

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

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

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

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

A.2.8 Case Studies: Virtual Sniffing and *Bluetooth* Mobile Phone Makers

Case Study # 1

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

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

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

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

Case Study # 2

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

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

A.2.9 Virtual Sniffing and You

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

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

Author: Eric Kaplan

Publish Date: May 2003

Revised: December 2013

Index