



BLUETOOTH[®] PROTOCOL ANALYZER
DUAL MODE EDITION

BPA[™] 500 Bluetooth Protocol Analyzer **Quick Start Guide**

Copyright © 2000-2011 Frontline Test Equipment, Inc. All rights reserved. You may not reproduce, transmit, or store on magnetic media any part of this publication in any way without prior written authorization of Frontline Test Equipment, Inc. FTS, Frontline, Frontline Test System, and ComProbe are registered trademarks of Frontline Test Equipment, Inc. FTS4BT is a trademark of Frontline Test Equipment, Inc. The Bluetooth SIG, Inc. owns the *Bluetooth* word mark and logos, and any use of such marks by Frontline is under license. All other trademarks and registered trademarks are property of their respective owners.



CONTENTS

Minimum System Requirements	1
Declaration of Conformity (EU).....	1
Purpose	2
Introduction	3
Hardware Installation/ComProbe placement.....	4
Attaching Antennas.....	4
Connecting/Powering ComProbe	4
Opening/Selecting Data Capture Method	6
Setting Up BPA 500 Datasource.....	9
Device Database.....	9
BPA 500 Information.....	10
Devices Under Test	11
Dual Mode.....	12
Classic Only	16
<i>Bluetooth</i> low energy only	18
Start Sniffing.....	20
Analyzing Data	22
Control Window	22
Frame Display.....	23
Data Extraction	26
Message Sequence Chart.....	30
How do I access the chart?	30
What do I see?	30
Search.....	32
PER Stats	34
<i>Bluetooth</i> Timeline.....	36
Timeline.....	37
Legend.....	37
Indicators	37
Throughput Graph	38
Low Energy Timeline	38
Coexistence View	39
Timeline.....	40



Legend..... 40

Indicators 41

Throughput Graph 41

Display Synchronization 42

Duplicate Displays 42

Bookmarks 42

Technical Support 43



MINIMUM SYSTEM REQUIREMENTS

- PC with Windows XP 32 bit, (Service Pack 2 or higher), Windows 7 (32 and 64 bit).
- Pentium 2 GHz processor
- RAM Requirements: 2 GB minimum
- 50 MB free Hard Disk Space (capture file size is limited only by disk size)
- USB 2.0 High Speed enabled port

DECLARATION OF CONFORMITY (EU)

We hereby declare that all essential radio test suites have been carried out for the **BPA 500 Dual Mode Bluetooth Protocol Analyzer** and that it is in conformity to all essential requirements of the directive 199/5/EC.

The conformity assessment procedure referred to in Article 10 and detailed in Annex III or IV of Directive 1999/5/EC has been followed with the involvement of the following Notified Body (ies):

BABT, Forsyth House, Churchfield Road, Walton-on-Thames, Surrey, KT12 2TD, UK

See complete Declaration of Conformity (DOC) document at:

[http://www.fte.com/docs/DECLARATION_OF_CONFORMITY - BPA 500.pdf](http://www.fte.com/docs/DECLARATION_OF_CONFORMITY_-_BPA_500.pdf)



PURPOSE

This document is designed to get your data capture and analysis feet wet. What we are going to do in this guide is go through one of the data capture methods available in BPA 500. We will explain how to set up devices, install hardware, configure BPA 500, and capture data for each one. In later sections you will see how to use BPA 500 to analyze the captured data.

What this document does not do is cover all methods of data capture or data analysis for BPA. We wanted to provide a solid foundation for early success in capturing data and using some of the tools to view and analyze what you capture.



INTRODUCTION

The BPA 500 Dual Mode *Bluetooth* Protocol Analyzer combines and displays *Bluetooth* low energy and classic data in Frontline's intuitive display, simplifying and accelerating the debugging process. With Dual Mode, engineers can capture and display live data streams from both *Bluetooth* low energy devices and Basic Rate/Enhanced Data Rate (BR/EDR) "Classic" *Bluetooth* devices within a single interface and in a single graphical coexistence view.

You have six general options with BPA 500.

- **Classic- low energy Air Sniffing** uses one BPA 500 ComProbe[®] to sniff Classic and low energy data.
- **Classic/low energy/802.11 Air Sniffing (optional)** uses one BPA 500 ComProbe[®] to sniff Classic, low energy, and additional hardware to sniff 802.11 data.
- **High Speed Serial Sniffing** is used to monitor data going between a Host and Host controller, BPA 500 includes a set of custom cables for Serial RS-232 sniffing. Using HCI sniffing in conjunction with air sniffing, a complete picture of the *Bluetooth* transmission can be captured.
- **SDIO Sniffing (optional)** captures and decodes Bluetooth and SD/SDIO/SPI/MMC data.
- **USB HCI Sniffing** captures data via UART transports for debugging Host to Host Controller issues.
- The **Virtual Sniffer** is a live import facility within BPA 500 that makes it possible to access any layer in a stack that the programmer has access to and feed this data into the Virtual Sniffer.

For this document we will assume that you have already loaded the device drivers and installed the software for BPA 500. If our assumption is correct, you can move to the next section and we will get started. If, however, you haven't installed drivers and software, you need to stop here and follow the **Software and Device Driver installation Instructions** included with the software to take care of installation.



HARDWARE INSTALLATION/COMPROBE PLACEMENT

Attaching Antennas

When you remove the ComProbe from the box, the first step is to attach the antennas (Figure 1).

Figure 1



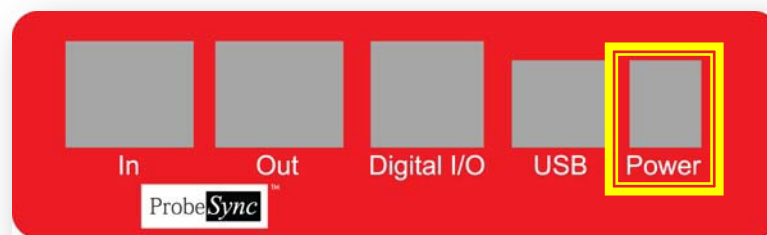
1. Attach antennas to "RF" under LE" and "RF under Classic".

Connecting/Powering ComProbe

Once you have attached the antenna, the next step is to power up and connect the BPA 500 ComProbe to the computer.

2. Insert the power cable (DC connector) from the AC adapter into the "Power" port on the ComProbe (Figure 2).

Figure 2



3. Plug the AC adapter into the AC power source.

AC Adapter Details:

ECOPAC (UK) POWER LTD, Switch Mode Power Supply –

Model: 3A-181WP09

P/N: T3508ST

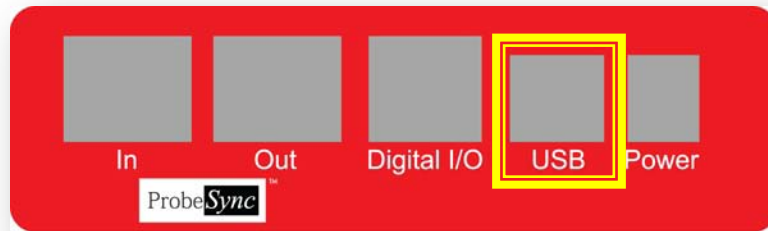
Input: 100-240V~, 50-60Hz, 0.6A

Output: +9V-2.0A



4. Insert the "USB cable" into the USB port on the ComProbe (Figure 3).

Figure 3



IMPORTANT NOTE: The ComProbe WILL NOT function properly when only the USB is plugged in. The AC power must also be connected.

5. Insert the "other end of the USB cable" into the PC.
6. The next thing to do is to turn on the devices that you want to test.
7. Finally, position the BPA 500 ComProbe between the devices.

IMPORTANT NOTE: It is easier to sync and then capture data if the devices are somewhat separated because *Bluetooth* adjusts power levels on devices that are in close proximity, which can affect the ability to sync and the quality of the trace. Also, don't place the BPA 500 right next to the computer; close proximity to the computer could cause some interference.



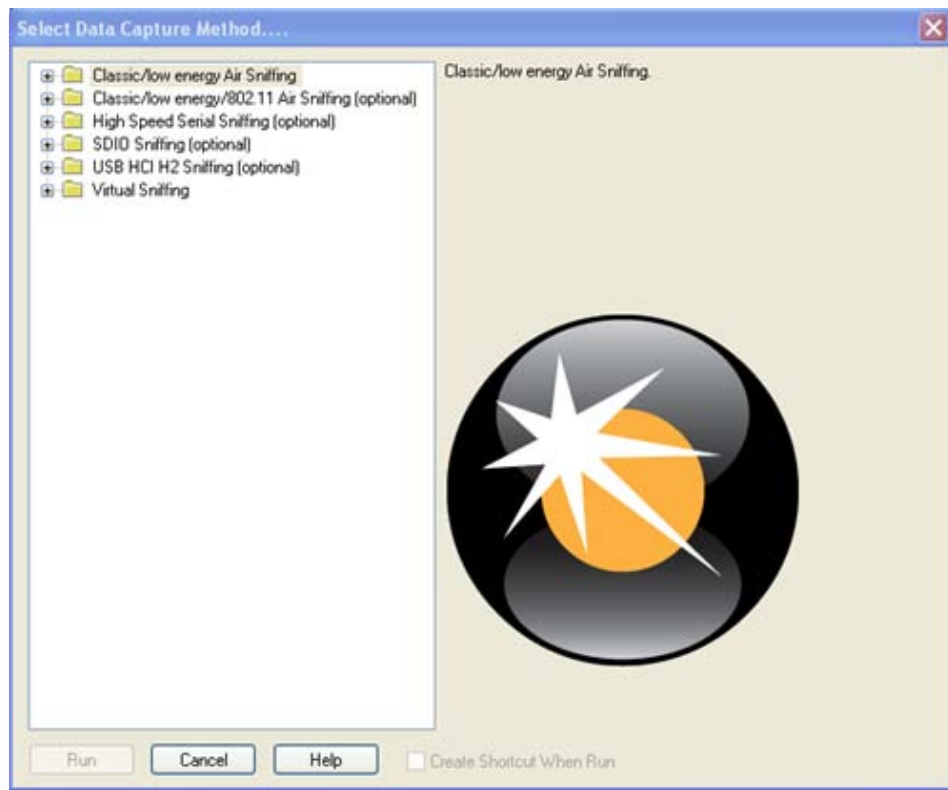
OPENING/SELECTING DATA CAPTURE METHOD

Now that the devices are on, the ComProbe fired up and positioned correctly, the next step is to open BPA 500 and select the data capture method.

1. Open "BPA 500" from the Start menu or from the Desktop folder.
2. Select "Frontline BPA 500".

The Select Data Capture Method dialog appears (Figure 4).

Figure 4



Notice that the six sniffing methods that we identified in the Introduction are displayed here:

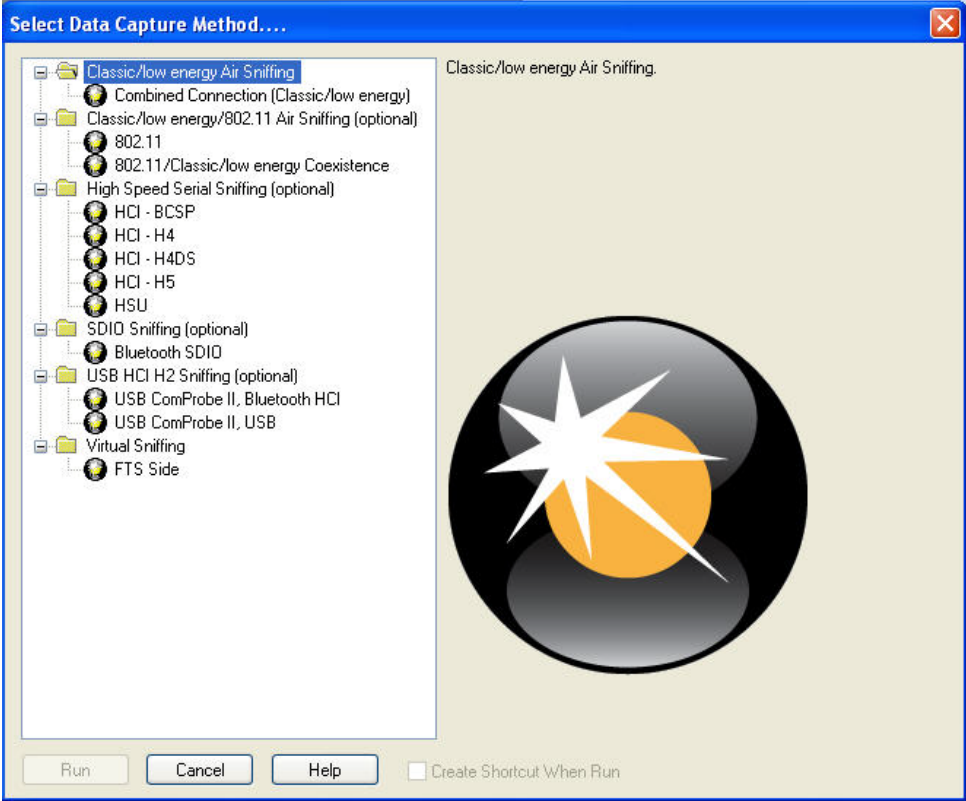
- Classic/low energy Air Sniffing
- Classis/low energy/802.11 Air Sniffing (optional) Requires optional hardware
- High Speed Serial Sniffing (optional) – Requires optional hardware
- SDIO Sniffing (optional) Requires optional hardware
- USB HCI H2 Sniffing (optional) – Requires optional hardware
- Virtual Sniffing



- 3. Expand the tree for Classic/low energy Air Sniffing (Figure 5).

Notice the options available for each method. If you click on an option, a short description appears on the right of the dialog.

Figure 5



As we mentioned earlier in the Introduction, in this guide we are going to select one of the options (the most commonly used), explain how to configure the software, prepare the hardware, capture the data, and analyze the results. So, let's get started.

- 4. Select "Combined Connection (Classic/low energy)".
- 5. Select "Run".

BPA 500 will open with the Control Window (Figure 6) and the BPA 500 datasource dialog (Figure 7) visible.

Figure 6

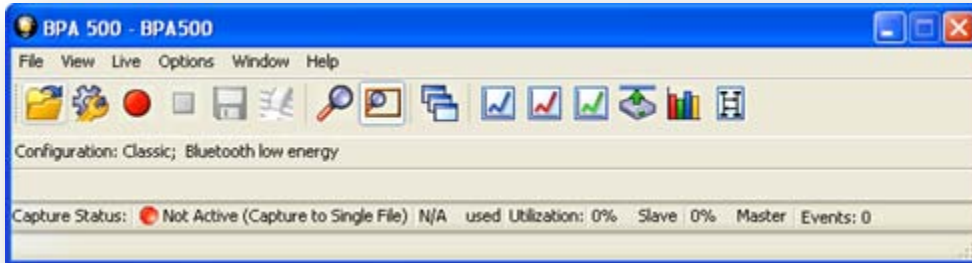
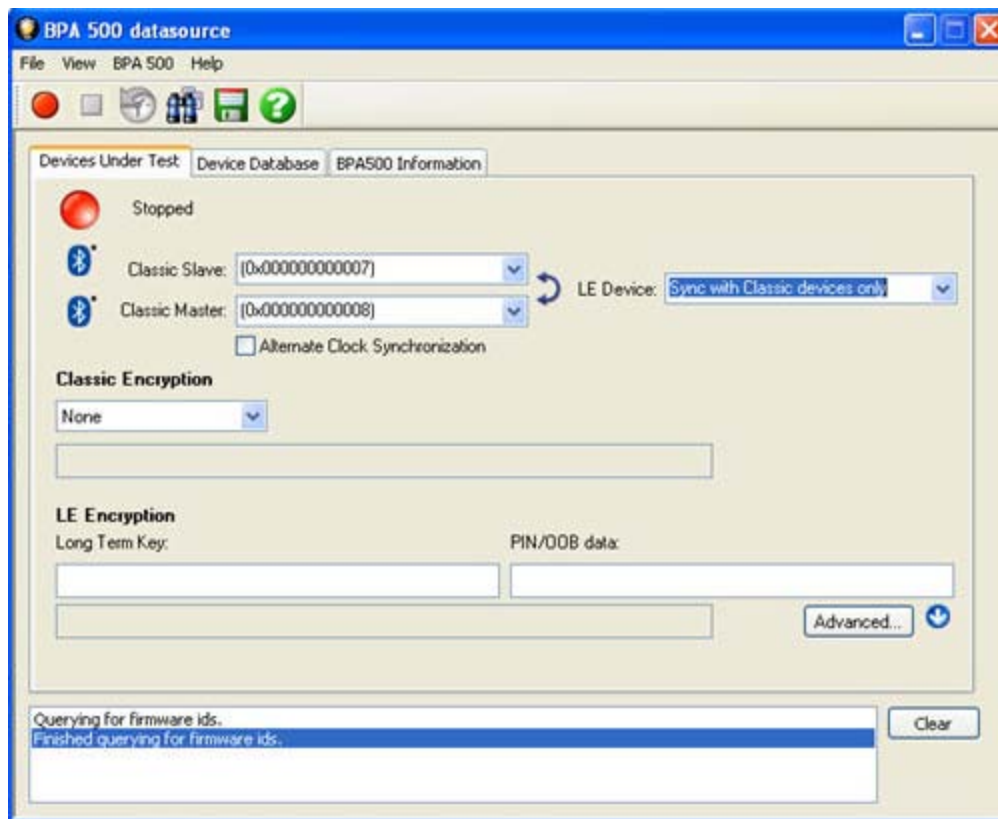


Figure 7





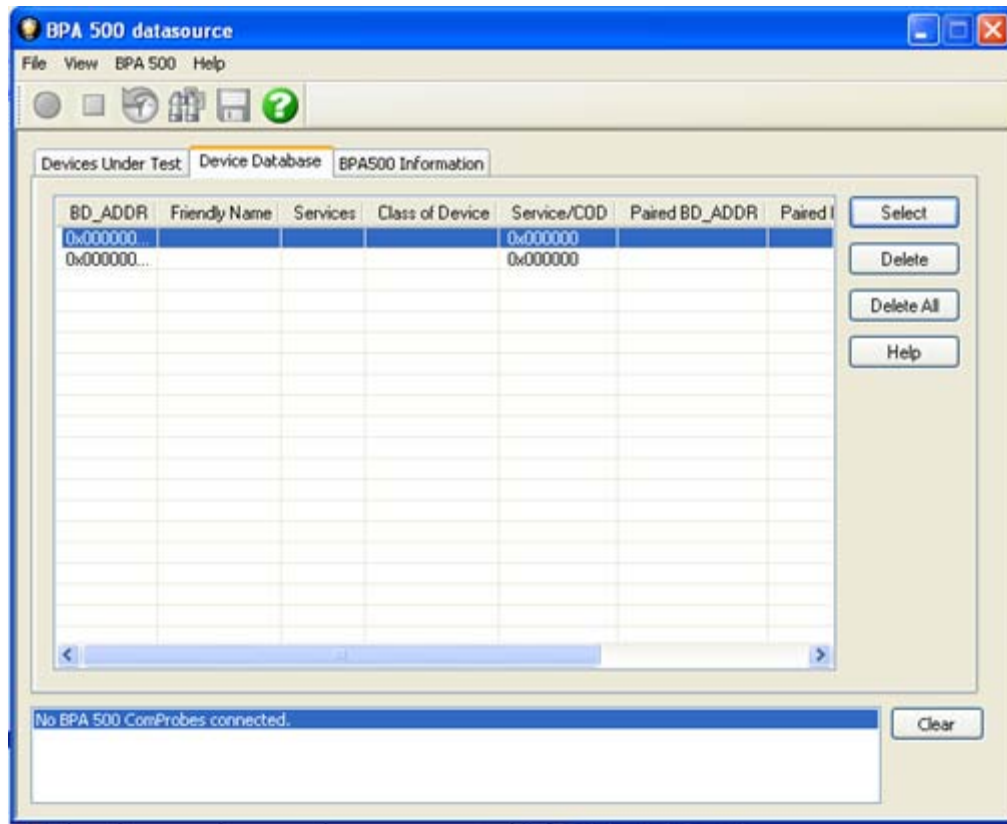
SETTING UP BPA 500 DATASOURCE

There are three tabs on the BPA 500 datasource dialog. Most of the configuration will be done on the *Devices Under Test* dialog, which we will look at in a moment. Before that, let's take a quick look at the two other dialogs.

Device Database

The Device Database (Figure 8) contains information about the devices that have been discovered or entered by the user.

Figure 8



There are several things you can do on the Device Database dialog.

- When you select the **Discover** button, BPA 500 lists all the discoverable *Bluetooth* devices.
- When you select a device from the list, then click **Select**, the information is transferred to the *Devices Under Test* dialog.
- You can delete records one at a time by selecting the record, then selecting **Delete**.
- You can also delete all the records by selecting **Delete All**.
- Select **Close** to close the dialog.
- The **Help** button brings up more Help information.

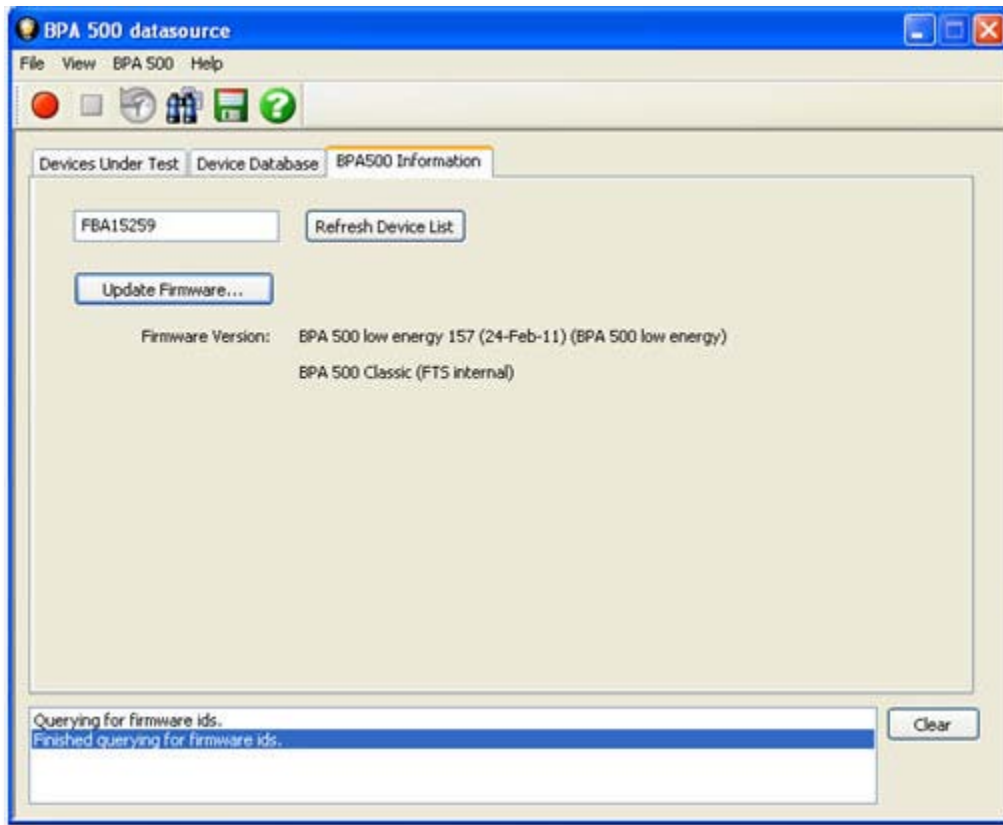


There is really nothing to do with this dialog right now, so let's move to the BPA 500 Information dialog.

BPA 500 Information

The BPA 500 Information dialog (Figure 9) displays information about devices and firmware.

Figure 9



There are several pieces of information on this display:

- The current 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 List**.
- If you want to load the latest firmware, you select the Update Firmware button.

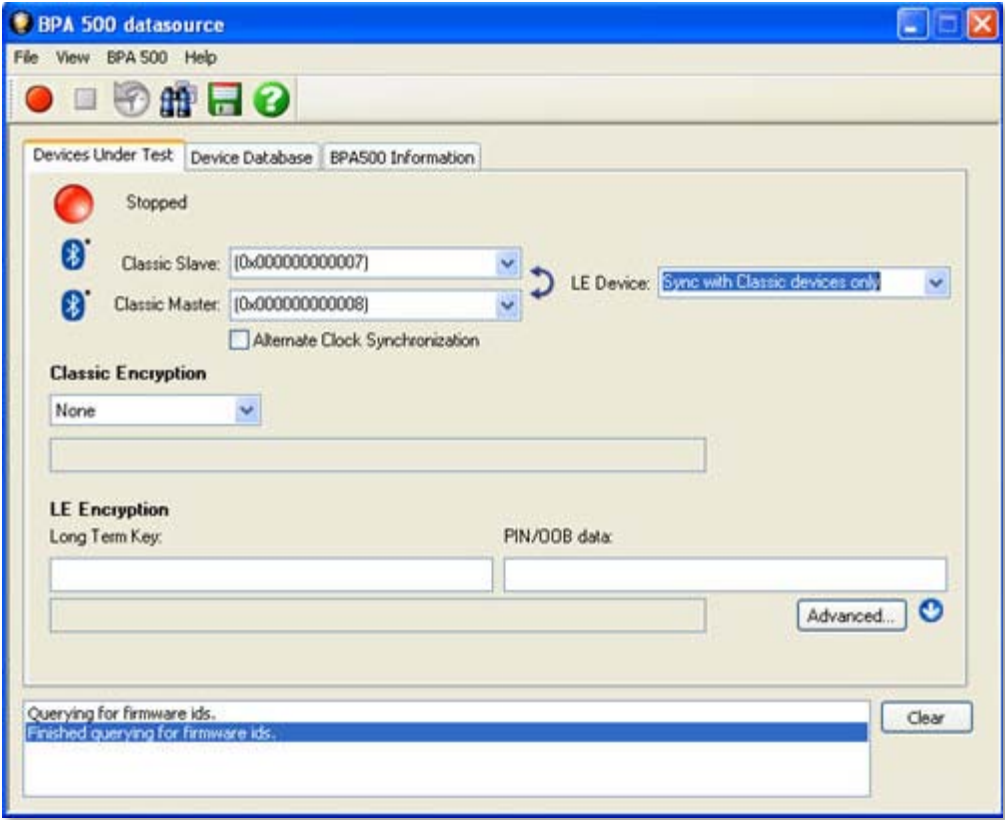
You can take a look at the electronic help files to learn more about updating firmware and refreshing the device list, but for now we really don't need to do anything with this dialog. What we need to concentrate on is the **Devices Under Test** on the next page.



Devices Under Test

The **Devices Under Test** dialog (Figure 10) has all the setup information the analyzer needs in order to synchronize with the piconet and capture data. The analyzer requires information on the clock synchronization method and the device address of the devices that you want to test.

Figure 10



You can choose to capture data using:

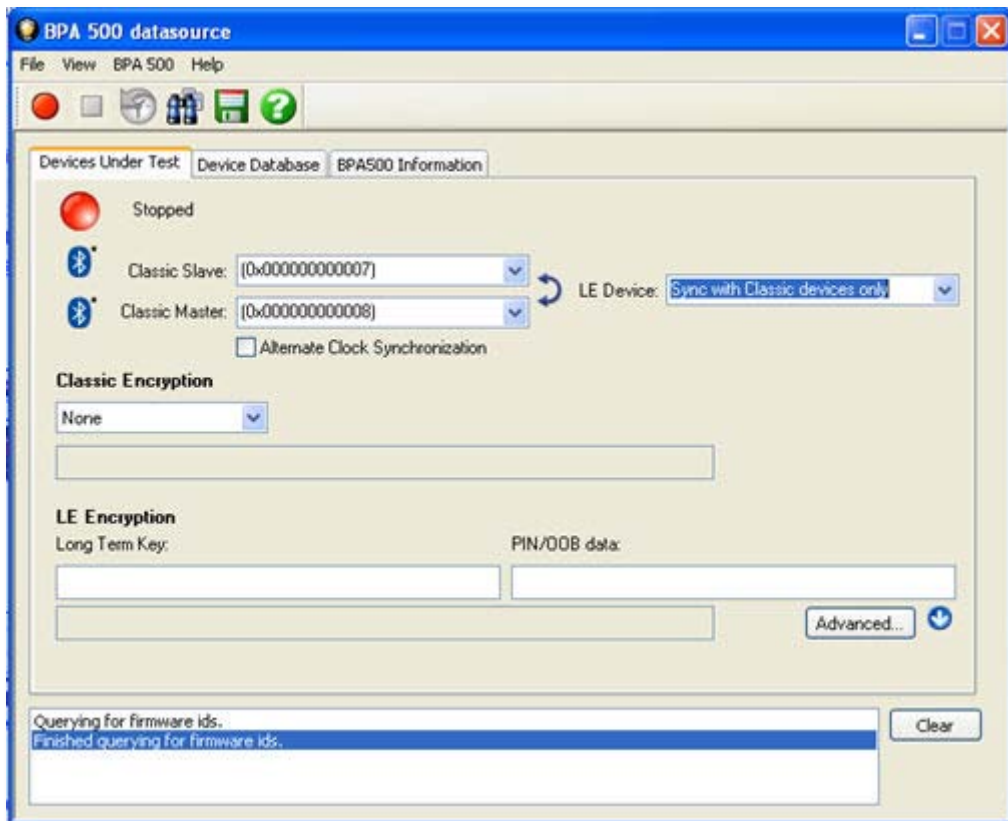
- Dual Mode - Combination of Classic (BR/EDR) and low energy
- Classic (BR/EDR) only
- low energy only

Let's take a quick look at how to set up a basic configuration for each one.

Dual Mode

BPA 500 is designed to capture classic **Bluetooth** and *low energy* at the same time. In order to do that you have to make several configuration settings.

Figure 11



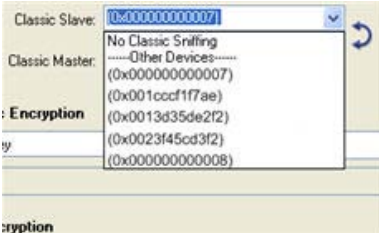
Specifying the Bluetooth Device Address (BD_ADDR)

The analyzer needs to know the Bluetooth® Device Address (BD_ADDR) for the Slave. You can specify the Bluetooth Device Address in multiple ways.

1. Select the Bluetooth Device Address (BD_ADDR) for **Classic Slave**: from a list of available devices from the Device Database. You can also type in the address as a 14 digit hex number. The "0x" is automatically typed in by the control. Any device entered this way is added to the Device Database.

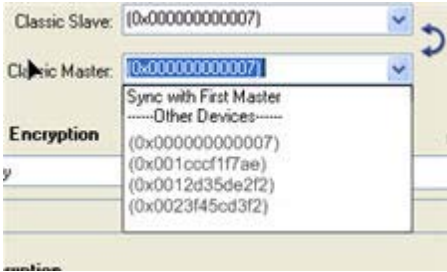


Figure 12



- 2. Select the Bluetooth Device Address (BD_ADDR) for **Classic Master:** from a list of available devices from the Device Database. You can also type in the address as a 14 digit hex number. The "0x" is automatically typed in by the control. Any device entered this way is added to the Device Database.

Figure 13



Important Note: You do not have to enter a Master Address. If you do not enter a Master address, Frontline will follow the first connection made from the selected Slave. If a Master is selected, Frontline will only capture a connection made between the designated Master and Slave.

Also, generally you will not use Alternate Clock Synchronization, so it should be left unchecked. Using the pairing process described above, you will sync successfully almost every time. If you cannot sync using the steps above, contact Technical Support for additional help on how to use Alternate Clock Synchronization.



Note: You can select the Swap button to exchange the Master and Slave addresses. The button is only active if there is an address for both the Master and Slave. You can use the button when the dialog is static or "on the fly", when you are attempting to sync. The button will only work "on the fly", however when the color of the ComProbe icon is green, indicating that the application is waiting for the piconet to form or reform.

- 3. Specify the "BD_ADDR for the LE Device" by selecting "Sync with Classic Devices Only". By doing this, the low energy device will follow the first Classic Master that requests a response.

Figure 14



Classic Encryption

Figure 15



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

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

- None
- PIN Code (ASCII)
- PIN Code (Hex)
- Link Key

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

- **First**, you can choose None as the encryption method when neither of the devices has encryption enabled.
- The **second** and **third ways** are to use a PIN Code to generate the Link Key. The devices generate link Keys during the Pairing Process based on a PIN Code. The Link Key generated from this process is also based on a random number so the security cannot be compromised. If the analyzer is given the PIN Code it can determine the Link Key using the same algorithm. Since the analyzer also needs the random number, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

Example:

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

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

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

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

LE Encryption

Figure 16

The screenshot shows a form titled "LE Encryption" with two input fields. The first field is labeled "Long Term Key:" and the second field is labeled "PIN/OOB data:". Both fields are currently empty.

6. 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.

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

This is extra information that can make the pairing process more efficient and consistent.

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

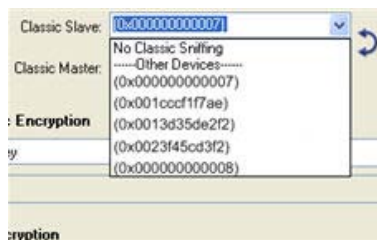


Classic Only

The analyzer needs to know the Bluetooth® Device Address (BD_ADDR) for the Slave. You can specify the Bluetooth Device Address in multiple ways.

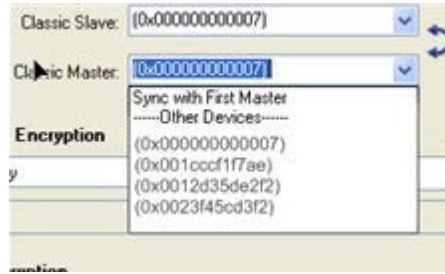
1. Select the Bluetooth Device Address (BD_ADDR) for **Classic Slave**: from a list of available devices from the Device Database. You can also type in the address as a 14 digit hex number. The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.

Figure 17




2. Select the Bluetooth Device Address (BD_ADDR) for **Classic Master**: from a list of available devices from the Device Database. You can also type in the address as a 14 digit hex number. The "0x" is automatically typed in by the control. Any device entered this way is added to the Device Database.

Figure 18



Important Note: You do not have to enter a Master Address. If you do not enter a Master address, Frontline will follow the first connection made from the selected Slave. If a Master is selected, Frontline will only capture a connection made between the designated Master and Slave.

Also, generally you will not use Alternate Clock Synchronization, so it should be left unchecked. Using the pairing process described above, you will sync successfully almost every time. If you cannot sync using the steps above, contact Technical Support for additional help on how to use Alternate Clock Synchronization.

Note: You can select the Swap button  to exchange the Master and Slave addresses. The button is only active if there is an address for both the Master and Slave. You can use the button when the dialog is static or "on the fly", when you are attempting to sync. The button will only work "on the fly", however when the color of the ComProbe icon is green, indicating that the application is waiting for the piconet to form or reform.

3. Select "No LE Sniffing" from the LE Device drop-down (Figure 19).

Figure 19



Classic Encryption

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

To learn more, look at the description of **Classic Encryption** on the previous pages within the discussion of Dual Mode. The settings would be the same.

4. Select an Encryption **option**.
5. Enter a **value** for the encryption.



That takes care of the setup for Classic only. Next let's look at how to capture low energy data only.

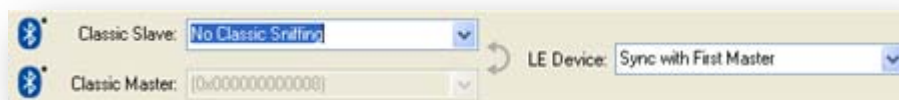
Bluetooth low energy only

Finally, you can use BPA 500 to sniff low energy by itself.

1. Select "No Classic Sniffing" from the Classic Slave drop-down (Figure 20).
2. Specify the BD_ADDR for the LE Device by selecting "Sync with First Master" (Figure 20).

By using this setting, you will capture LE advertising traffic and the sniffer will follow (and lock onto) the first connection it sees.

Figure 20



LE Encryption

The **Long Term Key** (Figure 21) is similar to the Link key in Classic.

Figure 21

The screenshot shows a software window titled "LE Encryption". Inside the window, there are two input fields. The first field is labeled "Long Term Key:" and the second field is labeled "PIN/OOB data:". Both fields are currently empty.

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.

3. Enter the "Long Term Key" for the LE Encryption.

In low energy Encryption there are two extra pieces of information that you can use in pairing:

- PIN
- Out-of-Band (OOB) data

In the case of PIN Entry, the extra information is a six digit (or less if leading zeroes are omitted) decimal PIN which can be entered in the field.

In the second case of out-of-band (OOB), there is a 16-digit (hexadecimal) code which the devices exchange via a channel that is different than the low energy transmission itself. This channel is called out-of-band and therefore the code is called out-of-band data.

On off-the-shelf devices we cannot sniff the OOB data, but in the lab you may have access to the data which is exchanged through this other channel. Therefore, we allow you to input either a six (or less) decimal digit PIN or a 16 hexadecimal digit code in this field.

4. Enter a PIN or OOB code (Optional).

That's it for the setup. Now you are ready to capture some data.



START SNIFFING

So, now we have our ComProbe installed, devices turned on and identified in BPA 500. It's time to sniff the communication between the devices.

1. Select "Start Sniffing" on the Datasource dialog from the toolbar or from the BPA 500 menu (Figure 22).

Figure 22



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

As data is being captured, the Status message at the top of the window indicates the synchronization status of the *BPA 500 ComProbe*. Also, the color of the ComProbe icon changes depending on the synchronization state. There are four states:



Blue = running and in sync with the piconet.



Green = running and waiting for piconet to form or reform





Red = initializing



White = stopped.

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

- Files are placed in My Capture Files by default and have a .cfa extension. Choose Directories from the Options menu on the Control window to change the default file location.
- Watch the status bar on the Control window to monitor how full the file is. When the file is full, it begins to *wrap*, which means the oldest data will be overwritten by new data.
- Click the Stop icon  to temporarily stop data capture. Click the Start Capture icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured data remains in the file.
- To clear captured data, click the Clear icon .
- If you select Clear after selecting Stop, a dialog appears asking whether you want to save the data.
 - You can click Save File and enter a file name when prompted.
 - If you choose Do Not Save, all data will be cleared.
 - If you choose Cancel, the dialog closes with no changes.
- 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.

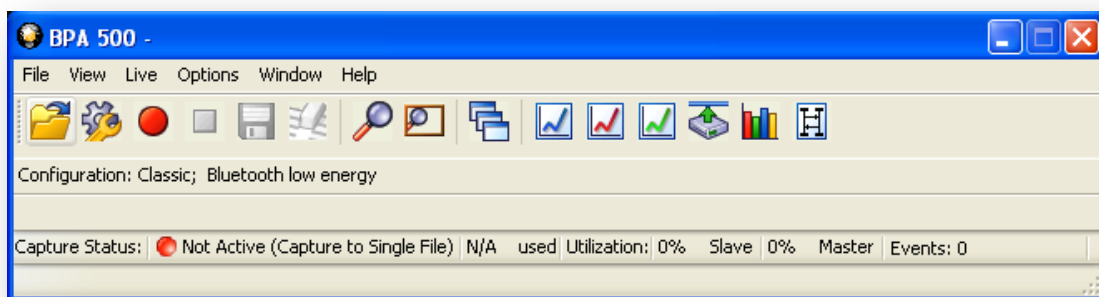
If you have done everything correctly, you will start capturing data. In the next section we will explain a little about the many different options you have for viewing and analyzing the data. Go to the [Analyzing Data](#) section next in this guide to learn how to use Frontline analysis tools.

ANALYZING DATA

Control Window

First of all, we have the Control window, which appears as the small rectangular window at the top of your screen (Figure 23).

Figure 23



BPA 500 is organized around this window. The Control window allows you to control data capture and access the other windows used to view data.

While there are a number of dialogs you can use to analyze the data, let's look quickly at some of the options you have.

Frame Display


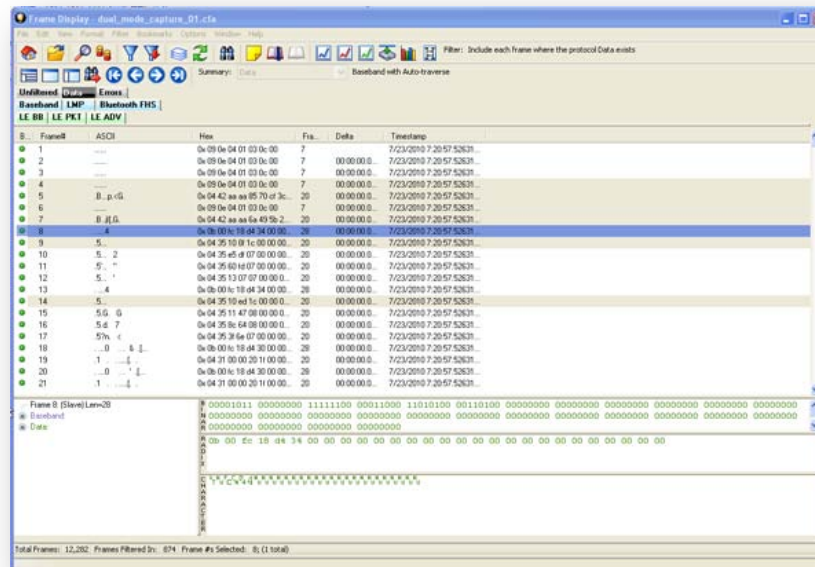
Click the Frame Display icon  on the Control window toolbar to open Frame Display (Figure 24).

Figure 24



Protocol Tabs

The Frame Display adds a tab to the top of the Summary Pane for every protocol found in the in the data. You can click on these tabs to filter on the protocol. Protocols are also arranged by technology groups. When the same protocol appears in multiple technologies, the data will be displayed in separate groups. For example, if there are Classic, low energy, and/or 802.11 data, they will be displayed within a Classic, low energy, and 802.11 group. Clicking on a protocol tab within a group shows all packets for that protocol and technology. The groups are arranged from top to bottom as General, Classic, low energy, and 802.11. They are also color-coded: General/Gray, Classic/Light Blue, low energy/Light Green, and Wi-Fi/Orange.

If a protocol appears in multiple technologies, then a tab for that protocol will appear in the specific technology group and in the General group.

Select the Unfiltered tab to display all protocols. The Unfiltered tab is automatically selected when multiple protocols are being *filtered-in* using other filtering methods.

There are several special tabs that appear in the Summary Pane when certain conditions are met. These include:

- **Bookmarks** appear when a bookmark is first seen.

- **Errors** appear when an error is first seen. Errors include decode errors (failure of Verify methods), DRF error bits, and PDA complaints about decoders (CFrameConstructor::AddCompilingErrorMessage). The Errors tab is displayed in **red**.
- **Info** appears when a frame containing an *Information* field is first seen.
- A **shown technology** has the icon to the left of the first row. A hidden technology has the icon to the right of the first row of the general tab group.

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

Panes

Frame display allows you to see an amazing amount of information from your protocol. The Frame Display is divided into panes, where each pane shows a different view of the data.

- The Summary pane (Figure 25) stretches across the top of the display. Each line in the Summary Pane represents one frame, except when running in one of the USB HCI Sniffing modes where each line represents one transaction.

Figure 25

Bookmark	Frame#	Chan	Type	AddTypeI	InitA/ScanA	AddTypeA	AdvA	Len	Frame Size	Delta	Timestamp
●	8	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.020001	2/23/2011 1:44:47.42700...
●	9	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.018751	2/23/2011 1:44:47.44575...
●	10	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.021251	2/23/2011 1:44:47.46700...
●	11	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.025003	2/23/2011 1:44:47.49200...
●	12	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.018751	2/23/2011 1:44:47.51075...
●	13	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.026243	2/23/2011 1:44:47.53700...
●	14	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.022500	2/23/2011 1:44:47.55950...
●	15	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.020001	2/23/2011 1:44:47.57950...
●	16	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.020001	2/23/2011 1:44:47.59950...
●	17	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.021251	2/23/2011 1:44:47.62075...
●	18	37	ADV_IND			(pub)	0x00025b00ed01	18	33	00:00:00.004826	2/23/2011 1:44:47.62558...
●	19	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.063922	2/23/2011 1:44:47.68950...
●	20	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.023749	2/23/2011 1:44:47.71325...
●	23	38	ADV_IND			(pub)	0x00025b00ed02	19	34	00:00:00.026250	2/23/2011 1:44:47.73950...

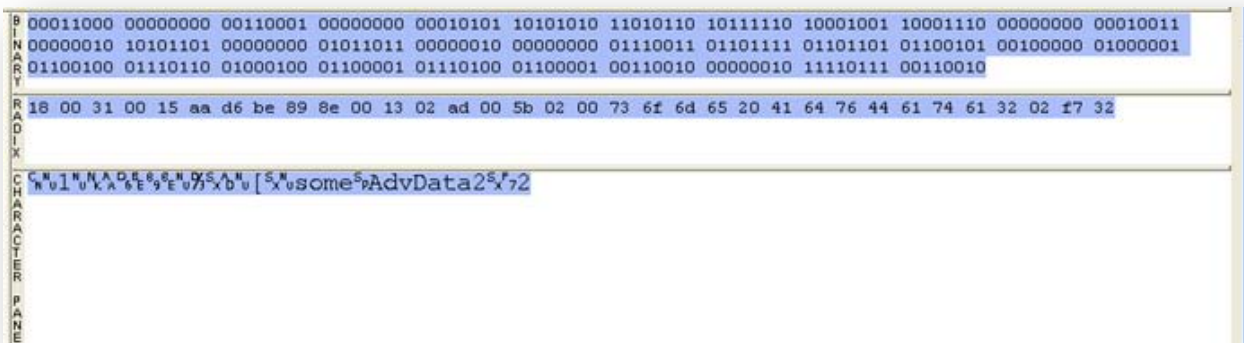
- The Decode pane (Figure 26) contains a detailed decode of the frame/transaction selected in the Summary pane, and is located on the left side of the Frame Display window.

Figure 26



- The three smaller panes on the bottom right of the Frame Display show the data in hex, binary and ASCII (Figure 27). The user can choose to have these panes show the data in other radices or character sets. Select any field in the Decode pane and the corresponding bit(s) or byte(s) will be selected in the data panes.


Figure 27



Frame Errors

Frame numbers in red indicate an error in the frame. Select the frame, and look at the top of the Decode pane to determine the type of error.

Scrolling versus Static View

Click the *Lock/Resume* icon  to have the Summary pane scroll to always show the latest frames captured. Click the *Lock/Resume* icon again to stop the Summary pane from scrolling.

Protocol Tabs

The frame display has a series of Protocol Tabs that allow you to filter on a specific protocol quickly and easily. For more advanced filtering option please consult the online *Help*.



Data Extraction

You use Data/Audio Extraction to pull out data from various decoded *Bluetooth*[®] protocols. Once the data are extracted, you can save them into different file types, such as text files, graphic files, email files, .mp3 files, and more.


1. You access this dialog by selecting Extract Data/Audio from the View menu or by clicking on the icon from the toolbar  .
2. Choose a checkbox or checkboxes on the left side of the dialog to identify those **profile(s)** from which you want to extract data (Figure 28).

Figure 28



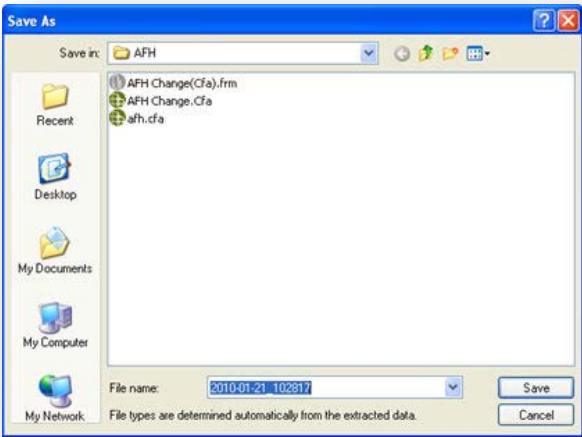
It's important to note that if there is no data for the profile(s) you select, no extracted file is created.

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**. This 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.
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. *This option is active for SCO/eSCO only.*
7. Select **Extract**.

A *Save As* dialog appears (Figure 29).



Figure 29

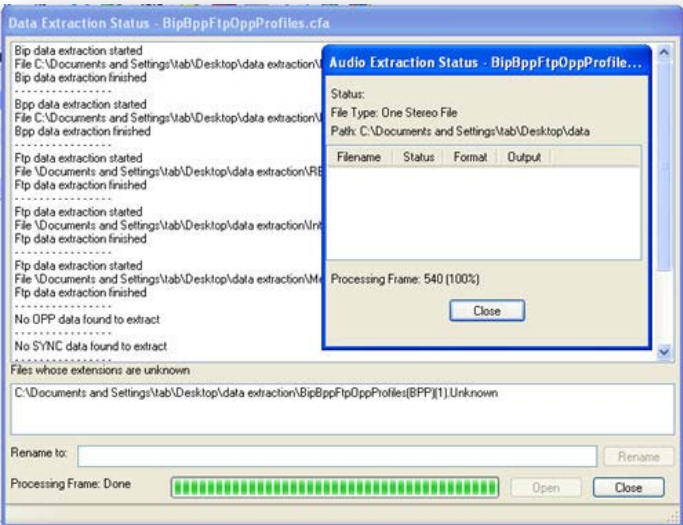


The application will assign a file name and file type for each profile you select in Step 1 above. The file type varies depending on the original profile. A separate file for each profile will be created, but only for those profiles with available data.

- 8. Select a **location** for the file(s).
- 9. Click **Save**.

The *Data Extraction Status* and *Audio Extraction Status* dialogs appear (Figure 30). When the process is complete the dialogs display what files have been created and where they are located.

Figure 30



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



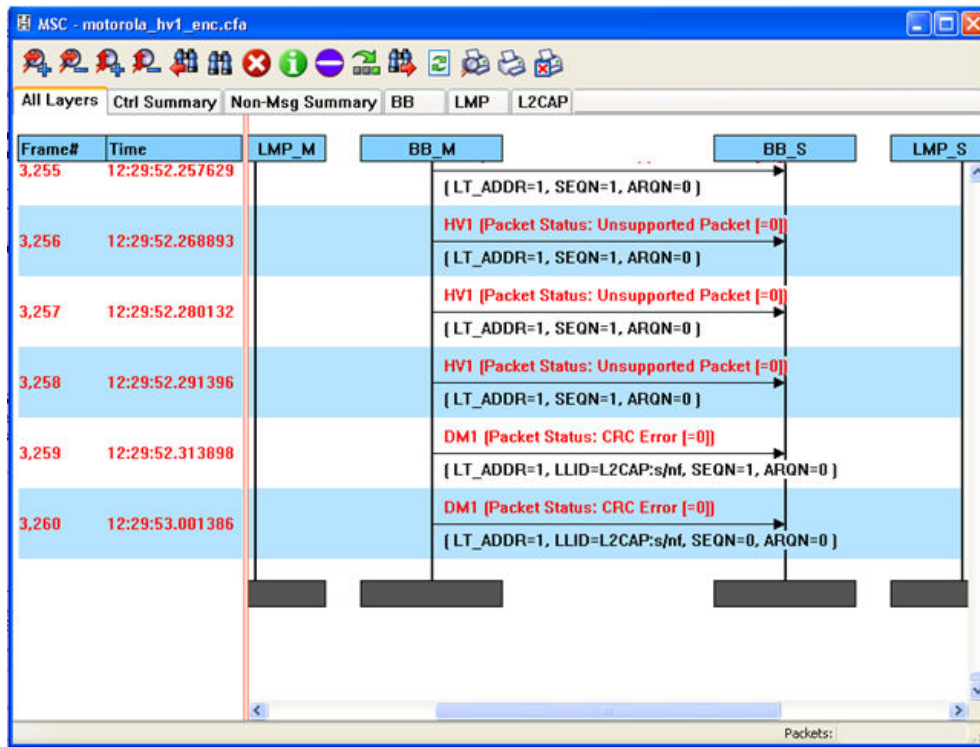
10. If you did not select this option, you can open a file by simply double-clicking on the name.

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


Message Sequence Chart

The Message Sequence Chart (MSC) displays a concise overview of a *Bluetooth* connection, highlighting the essential elements of 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 in the capture, or filter by protocol/profile. The MSC is color coded for a clear and easy to use view of your data (Figure 31).

Figure 31



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?

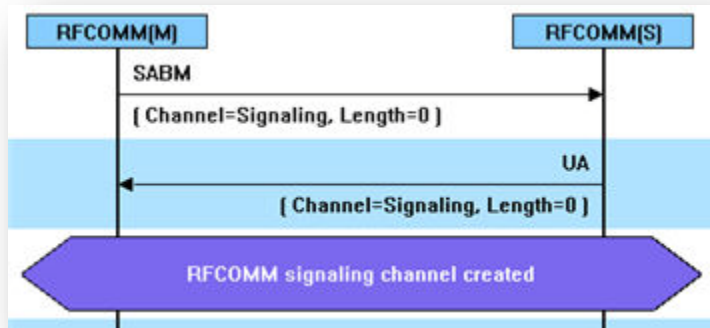
Along the top of the dialog are a series of tabs, which will vary depending on the protocols.





Clicking on a tab displays the messaging between the master and slave for that protocol (Figure 32). For example, if you select RFCOMM, you will see the messaging between the RECOMM{M} Master, and the RECOMM{S} Slave.

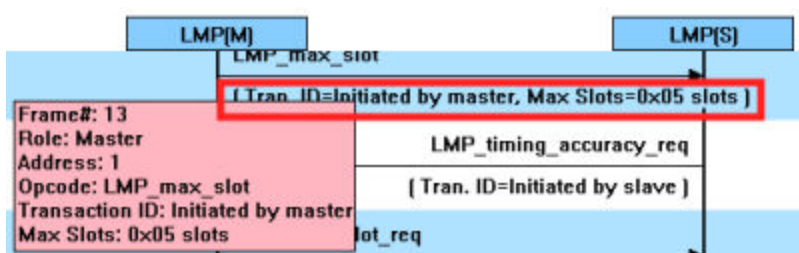
Figure 32



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

When you position the mouse over the message description, you will see an expanded tool tip (Figure 33).

Figure 33



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 within the dialog, which brings up a directional arrow that you can use to move left/right and up/down.

Search

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

You access this dialog by selecting the Search icon  or **F3**, the Search dialog appears (Figure 34).

Figure 34



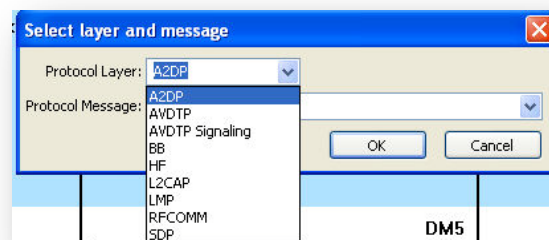
From this dialog you can search for specific protocol messages or search for the first error frame. To use the dialog:

1. Select one of the **protocol tabs** at the top of the dialog.
2. Open the **Search dialog** using one of the three methods.

*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.*

3. Select a specific **Protocol Message** from the drop-down list (Figure 35).

Figure 35



4. Once you select the Protocol Message, click **OK**.



The Search dialog disappears and the first search result is highlight in the Message Sequence Chart (Figure 36).



Figure 36



If there is no instance of the search value, you see the following dialog (Figure 37).

Figure 37



Once you have set the search value, you can 1) use the Search Previous  and Search Next  buttons or 2) **F2** and **F3** to move to the next or previous frame in the chart.

PER Stats

The Packet Error Rate Stats (PER Stats) Plug-in provides a dynamic graphical representation of the Packet Error Rate for each channel (Figure 38).

Figure 38



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.

- Each channel contains a bar that displays the number of packets with no errors in **green**, packets with Header Errors in **red**, packets with Payload or CRC errors in **dark red**, and Retransmitted packets in **yellow**.




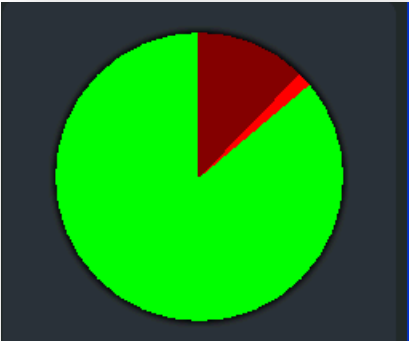

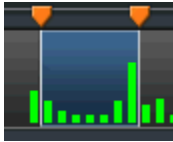
- When you select a channel, detailed information for that channel is displayed in the expanded channel chart on the upper right.
 - The number of packets with no errors is displayed in light green in the bar chart.
 - The number of packets that have header errors is displayed in red in the bar chart.
 - The number of payload errors is displayed in dark red in the bar chart.
 - The number of re-transmits is displayed in yellow in the bar chart.
- When you select the  in the upper-right corner, the bar chart is replaced by a pie chart (Figure 39). To return to the bar chart, click on the channel again.

Figure 39



- In the 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.

- The Viewport is used to select single or multiple vertical bars . Clicking on a vertical bar left justifies the Viewport to that bar. 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.

Bluetooth Timeline


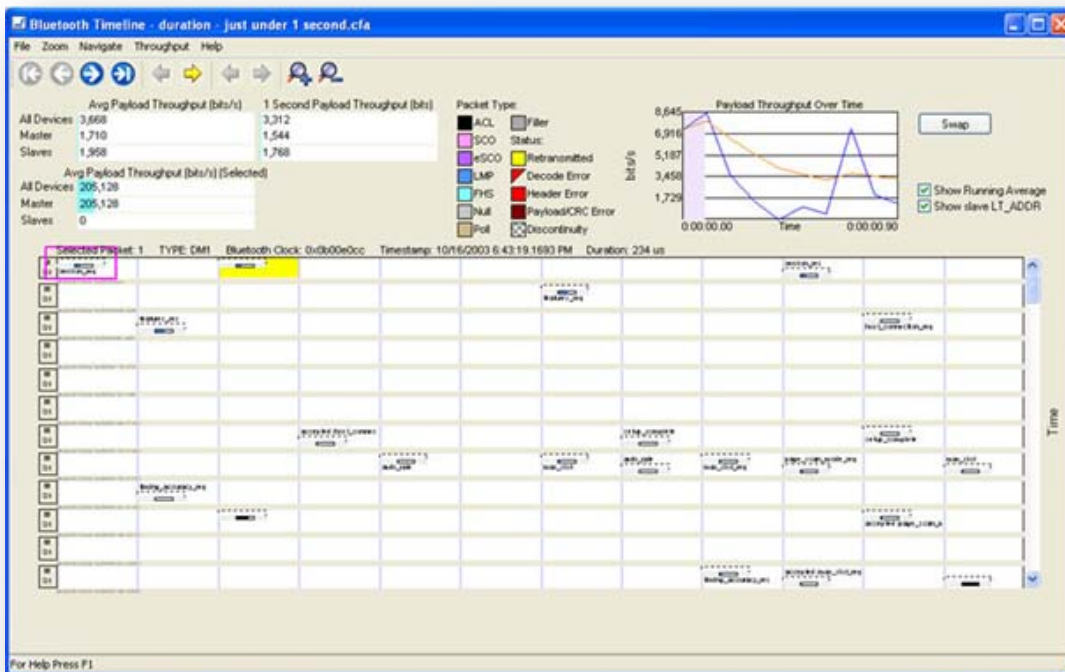

The *Bluetooth Timeline*  displays packet information in a main timeline that can display data over different periods of time and also in graph and chart form. Instead of just raw numbers and characters, the Timeline displays when packets occur, their speed, type, their payload, errors, retransmits, and more (Figure 41).

Figure 40



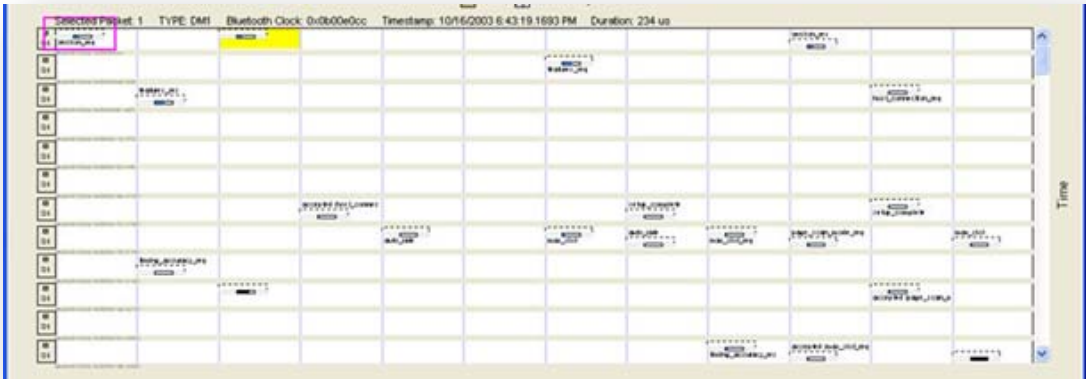
You access the *Bluetooth Timeline* by selecting the icon  from the Control Window or Frame Display toolbars or **Bluetooth Timeline** from the View menus.



Timeline

The timeline displays multiple rows of time, from left to right, top to bottom, just like a book. Information for the Master and Slave are shown on separate lines. Each packet type is a different color. The packet and corresponding color are shown on the legend (Figure 42).

Figure 41



Legend

This legend identifies the color coding found in the timeline (Figure 43).

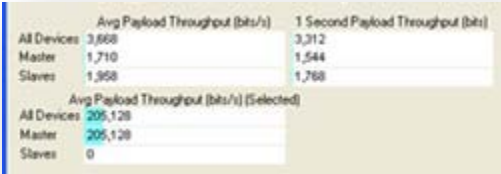
Figure 42



Indicators

There are three throughput indicators (Figure 44).

Figure 43

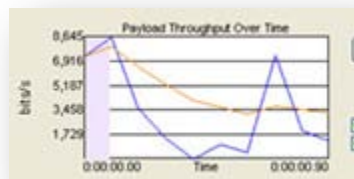


- Average throughput is the total payload over the entire session divided by the total time.
- 1-Second Payload Throughput is the total payload over the most recent one second of duration.
- Average Throughput for a selected packet range displays the data for a single packet when you select that packet from the Timeline.


Throughput Graph

Payload Throughput over Time shows throughput over a period of time in a graph (Figure 45).

Figure 44



Low Energy Timeline

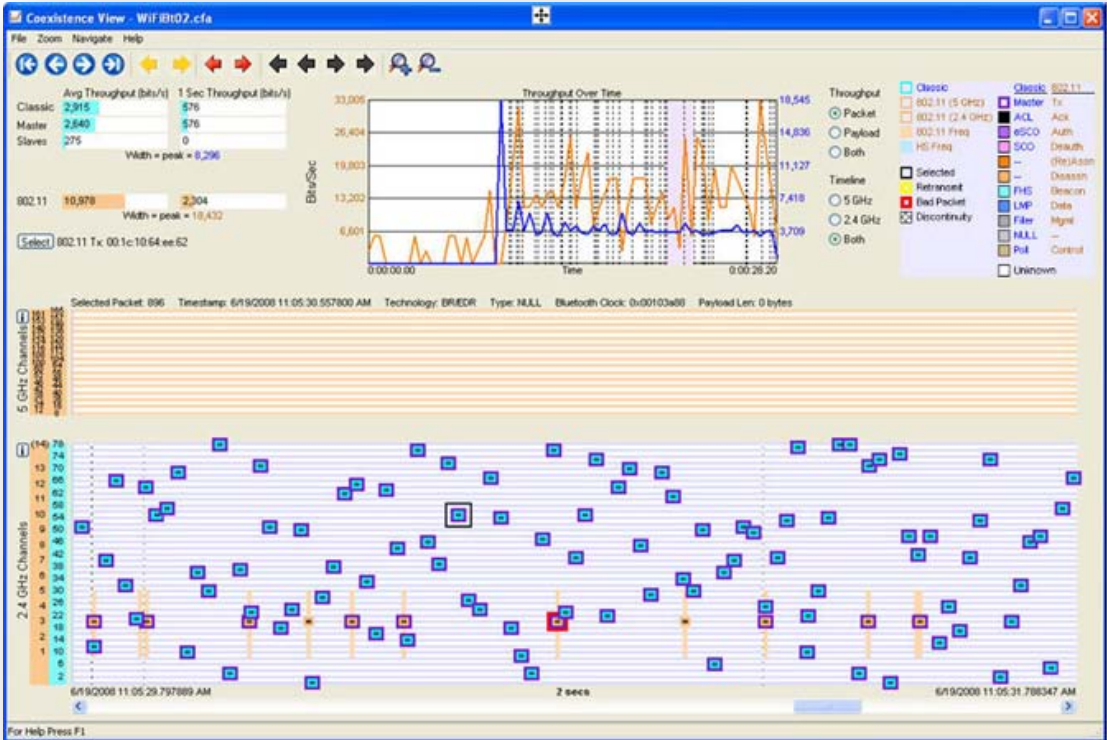
There is also a low energy Timeline . It is very similar to the *Bluetooth* Timeline.




Coexistence View

The Coexistence View displays *Bluetooth*® and the 802.11 channels frequencies in one view or separately (Figure 46).

Figure 45



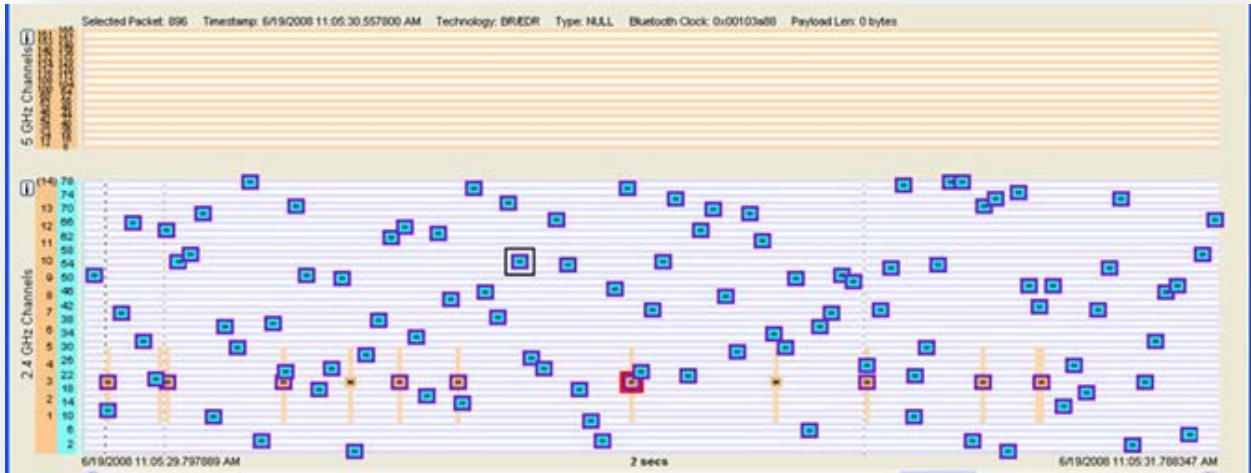
You access the Coexistence View by selecting the icon  from the Control Window or Frame Display toolbars or **Coexistence View** from the View menus.



Timeline

In the Timeline you can see what packets were being transmitted, when they were transmitted, and how they relate to each other (Figure 47).

Figure 46



You can see Classic *Bluetooth* and Wi-Fi together in the 2.4 gigahertz range, the *Bluetooth* channels being blue and the Wi-Fi being orange, or you can view only Wi-Fi in the 5 gigahertz range. The packets are color coded, which you can match up to the Legend to see the packet type.

Legend

Any packet type that is seen in the current session is shown in bold in the Legend. When you select a packet type, the attributes for the packet are highlight in the legend. Blue is for *Bluetooth* and orange is for 802.11 (Figure 48).

Figure 47





Indicators

The throughput indicators show average throughput and One second throughput for both *Bluetooth* and Wi-Fi. For *Bluetooth* these indicators segregate the master and slave values (Figure 49).

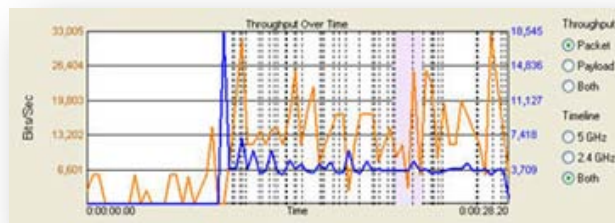
Figure 48



Throughput Graph

The throughput graph displays throughput over time (Figure 50).

Figure 49




You can see a line that displays the packet throughput for *Bluetooth* and Wi-Fi. You can also see a line that displays the payload throughput for both *Bluetooth* and Wi-Fi.



Display Synchronization

The system synchronizes the display in the Frame Display with the Event Display. Select a frame in the Frame Display and the other windows automatically update to highlight the bytes in the selected frame. Select a byte in the Message Sequencing Chart and the Frame Display and Event Display updates to show the frame containing the byte.


Duplicate Displays

The *Duplicate* icon  creates a second window of the same type, identical to the first. The advantage of additional Displays is that you can look at two different groups of data at the same time. For example, you can look at the start of an interaction in one Frame Display and the end of that same interaction in the other and compare the two.

Bookmarks

Bookmarks let you mark frames of interest so they can be easily found later. Bookmarked frames appear with a magenta triangle icon next to them except in the Event Display where they appear as a dashed line around the start of frame marker. You can navigate between bookmarks using the Find feature or by pressing F2 to go to the next bookmark. To make a new bookmark, right-click on the frame and choose *Add Bookmark* from the menu.

You can search for strings or patterns in your data or in the frame decode, for errors, control signal

changes, bookmarks, special events, and time. Click the Find  icon to open the Find window. Click the *Help* button for more information on the different types of searches.



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