

# **Wireless Protocol Suite Hardware and Software User Manual**

## Document Disclaimer

The information contained in this document has been carefully checked and is believed to be reliable. However, no responsibility can be assumed for inaccuracies that may not have been detected.

Teledyne LeCroy reserves the right to revise the information presented in this document without notice or penalty.

## Trademarks and Servicemarks

Teledyne LeCroy, Frontline, Frontline Test System and Wireless Protocol Suite are registered trademarks of Teledyne LeCroy, Inc.

The following are trademarks of Teledyne LeCroy, Inc.

- Sodera™
- Sodera LE™
- 802.11™
- X240™
- Audio Expert System™
- Audio Rating Metric™
- ProbeSync™

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

Microsoft and Windows are registered trademarks of Microsoft Inc.

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

## Copyright

© 2020 Teledyne LeCroy, Inc. All Rights Reserved

This document may be printed and reproduced without additional permission, but all copies should contain this copyright notice.

# Contents

---

<b>Chapter 1 Frontline Hardware and Wireless Protocol Suite Software</b> .....	<b>13</b>
1.1 What is in this manual .....	13
1.2 Computer Minimum System Requirements .....	14
1.3 Software Installation .....	14
<b>Chapter 2 Getting Started</b> .....	<b>15</b>
2.1 X500 Hardware .....	15
2.1.1 Front Panel Controls and Connectors .....	15
2.1.2 Front Panel Connectors .....	15
2.1.3 Rear Panel Connectors .....	17
2.1.4 Attach Antennas .....	18
2.1.5 Applying Power .....	19
2.1.5.1 Applying Power using X500 Battery Pack .....	19
2.1.6 Recovery Mode .....	20
2.1.7 Connecting X500 for HCI and Logic Capture .....	20
2.1.7.1 UART Capture Configuration .....	24
2.1.7.2 Logic Event Capture Configuration .....	25
2.1.7.3 SPI Capture Configuration .....	26
2.2 X240™ Hardware .....	26
2.2.1 Front Panel Controls and Connectors .....	26
2.2.2 Rear Panel Connectors .....	28
2.2.3 Attach Antenna .....	30
2.2.4 Applying Power .....	30
2.2.5 Recovery Mode .....	30
2.2.6 Connecting X240 for HCI and Logic Capture .....	31
2.2.6.1 UART Capture Configuration .....	35
2.2.6.2 Logic Event Capture Configuration .....	36
2.2.6.3 SPI Capture Configuration .....	37
2.2.7 Setting Up for Synchronized X240 (2) Capture .....	37
2.2.8 Setting Up for Synchronized X240 (3) Capture .....	38
2.3 Soderia™ Hardware .....	40

---

2.3.1 Front Panel Controls .....	40
2.3.2 Rear Panel Connectors .....	42
2.3.3 Attach Antenna .....	44
2.3.4 Applying Power .....	44
2.3.5 Battery Power .....	46
2.3.5.1 Battery Install .....	46
2.3.6 Connecting for HCI & Logic Capture .....	52
2.3.7 Connecting for USB Capture .....	55
2.4 Soder LE Hardware .....	57
2.4.1 Soder LE Front Panel .....	57
2.4.2 Soder LE Rear Panel Connectors .....	58
2.4.3 Attach Antenna .....	59
2.4.4 Applying Power .....	59
2.5 802.11 Hardware .....	60
2.5.1 Attaching Antennas .....	60
2.5.2 Connecting/Powering the Frontline 802.11 .....	61
2.5.3 Setting Up for ProbeSync .....	62
2.6 Data Capture Methods .....	64
2.6.1 Opening Wireless Protocol Suite .....	64
2.6.2 X240 Data Capture Method .....	65
2.6.2.1 Single Technology Capture, Single X240 (1) .....	65
2.6.2.2 Synchronized X240 (2) Data Capture Method .....	66
2.6.2.3 Synchronized X240 (3) Data Capture Method .....	69
2.6.3 Soder Data Capture Method .....	72
2.6.4 Soder LE Data Capture Method .....	72
2.6.5 Frontline® 802.11 Data Capture Method .....	73
2.6.6 Using Sample Capture Files .....	77
2.7 NewTopic .....	78
<b>Chapter 3 Configuration Settings .....</b>	<b>79</b>
3.1 Configuration and I/O for Bluetooth Data Capture .....	79
3.1.1 User Configuration Overview .....	79



---

3.1.1.1 Standard Capture Scenario .....	80
3.1.2 Wireless Protocol Suite Analyzer Toolbars .....	80
3.1.2.1 Menu & Toolbars .....	81
3.1.2.1.1 Analyzer Toolbar Menu and Icons .....	81
3.1.2.1.1.1 Record Options Dialog .....	87
3.1.2.1.1.1.1 Record Options Dialog: X500 .....	87
3.1.2.1.1.1.2 Record Options Dialog: X240 .....	107
3.1.2.1.1.1.3 Record Options Dialog: Sodera .....	124
3.1.2.1.1.1.4 Record Options Dialog: Sodera LE .....	133
3.1.2.2 Device Database View .....	135
3.1.2.2.1 Reorder Identity Resolving Key (IRK) .....	145
3.1.2.2.2 Clean Device Database .....	148
3.1.2.2.2.1 Clean Device Database on Start Application .....	148
3.1.2.3 Wired Devices View .....	150
3.1.2.4 Security View .....	152
3.1.2.4.1 Classic Bluetooth Encryption and Decryption .....	154
3.1.2.4.2 Bluetooth Low Energy Encryption and Decryption .....	156
3.1.2.5 Private Keys View .....	159
3.1.2.6 Bluetooth Privacy Codes View .....	162
3.1.2.7 Event Log View .....	165
3.1.3 Excursion Mode .....	166
3.2 802.11 Configuration .....	168
3.2.1 Wi-Fi Scanner Hardware Settings .....	168
3.2.2 802.11 Datasource .....	168
3.2.2.1 Settings .....	169
3.2.2.2 Status .....	171
3.2.2.3 Capture Filters .....	171
3.2.2.4 Firmware Update .....	174
3.2.2.5 Wi-Fi Security .....	178
3.2.2.5.1 Wi-Fi Device Scanner .....	179
3.2.3 Wi-Fi Device - MAC Address Editor .....	185

---

3.3 802.15.4 Configuration .....	185
3.4 Decoder Parameters .....	186
3.4.1 Decoder Parameter Templates .....	190
3.4.1.1 Select and Apply a Decoder Template .....	190
3.4.1.2 Adding a New or Saving an Existing Template .....	191
3.4.1.3 Deleting a Template .....	192
3.4.2 Selecting A2DP Decoder Parameters .....	192
3.4.3 AVDTP Decoder Parameters .....	193
3.4.3.1 About AVDTP Decoder Parameters .....	193
3.4.3.2 AVDTP Missing Decode Information .....	194
3.4.3.3 AVDTP Override Decode Information .....	195
3.4.4 L2CAP Decoder Parameters .....	197
3.4.4.1 About L2CAP Decoder Parameters .....	197
3.4.4.2 L2CAP Override Decode Information .....	199
3.4.5 RFCOMM Decoder Parameters .....	200
3.4.5.1 About RFCOMM Decoder Parameters .....	200
3.4.5.2 RFCOMM Missing Decode Information .....	202
3.4.5.3 RFCOMM Override Decode Information .....	203
3.4.6 Determining Central and Peripheral .....	204
3.5 Conductive Testing .....	204
3.5.1 Classic Bluetooth Transmitter Classes .....	205
3.5.2 Bluetooth Low Energy Transmitter .....	205
3.5.3 Conductive Testing .....	206
3.5.4 Soder LE Conductive Testing .....	207
3.5.5 Bluetooth Conductive Test Process .....	210
3.5.6 802.11 Wi-Fi Conductive Testing .....	210
<b>Chapter 4 Capturing Data .....</b>	<b>212</b>
4.1 Air Sniffing: Positioning Devices .....	212
4.1.1 Capturing using X500 with Antenna Diversity .....	212
4.1.2 Using the x240 and Soder with indoor radio propagation .....	213
4.2 Capturing Data: Introduction .....	216

---

4.2.1 Record: Begin Capture .....	216
4.2.2 Selecting Devices for Analysis .....	217
4.2.3 Starting Analysis .....	219
4.2.4 Hardware Signal Too Strong Indication .....	220
4.2.5 Excursion Mode Capture & Analysis .....	222
4.2.6 Soderia Logic Event Capture and Analysis .....	227
4.2.7 Spectrum Analysis .....	228
4.2.8 Critical Packets and Information for Decryption .....	230
4.2.9 Saving Analyzed Data to Disk .....	231
4.3 Extended Inquiry Response .....	232
<b>Chapter 5 Analyzing Data .....</b>	<b>234</b>
5.1 Tool Bar .....	235
5.2 Analyzer Toolbar .....	238
5.3 Status Bar .....	238
5.3.1 Application Status .....	239
5.3.1.1 Device information block .....	239
5.3.2 Selected Frames Information .....	240
5.3.2.1 Information for one packet: .....	240
5.3.2.2 Information for several packets: .....	240
5.3.3 Total Frames Information .....	241
5.4 Panes in the Wireless Protocol Suite Main windows .....	242
5.4.1 Summary .....	243
5.4.1.1 Protocol Tabs .....	245
5.4.1.2 Bluetooth Low Energy Data Encryption/Central and Peripheral Assignment .....	246
5.4.1.3 Bluetooth Low Energy Decryption Status .....	246
5.4.1.4 Column Filtering/Sorting .....	247
5.4.1.4.1 Sorting .....	247
5.4.1.4.2 Filtering .....	247
5.4.1.5 Filtering .....	248
5.4.1.5.1 Display Filters .....	250
5.4.1.5.1.5 Defining Node and Conversation Filters .....	255

---

5.4.1.5.1.6 Editing Filters .....	255
5.4.1.5.2 Protocol Filtering from the Main windows .....	258
5.4.1.5.2.1 Quick Filtering on a Protocol Layer .....	258
5.4.1.5.2.2 Easy Protocol Filtering .....	259
5.4.2 Decode Pane .....	260
5.4.3 Raw Data Pane .....	262
5.4.4 Bluetooth Timeline .....	269
5.4.4.1 Bluetooth Timeline Packet Depiction .....	270
5.4.4.2 Bluetooth Timeline Packet Navigation and Selection .....	274
5.4.4.3 Bluetooth Timeline Visual Elements .....	274
5.4.4.4 Bluetooth Timeline Discontinuities .....	276
5.4.5 Low Energy (LE) Timeline .....	277
5.4.5.1 Low Energy Timeline Visual Elements .....	278
5.4.5.2 Low Energy Timeline Zooming .....	280
5.4.6 Coexistence View .....	281
5.4.6.1 Packets .....	283
5.4.6.2 Zoom .....	286
5.4.6.3 Coexistence View - No Packets Displayed with Missing Channel Numbers .....	287
5.4.6.4 Coexistence View - Spectrum .....	288
5.4.6.5 Show Legend .....	290
5.4.7 Statistics .....	290
5.4.8 Packet Error Rate Statistics .....	294
5.4.9 Throughput .....	298
5.4.10 Airtime Utilization .....	299
5.4.11 Message Sequence Chart (MSC) .....	303
5.4.11.1 Message Sequence Chart Toolbar .....	313
5.4.11.2 Message Sequence Chart - Search .....	314
5.4.11.3 Message Sequence Chart - Go To Frame .....	315
5.4.11.4 Message Sequence Chart - First Error Frame .....	316
5.5 Bluetooth Protocol Expert System .....	316
5.5.1 Starting the Bluetooth Protocol Expert System .....	317

---

5.5.2 Bluetooth Protocol Expert System Window .....	318
5.5.2.1 Expert System Connections Pane .....	319
5.5.2.2 Expert System Statistics Pane .....	320
5.5.2.3 Expert System Protocol Events Pane .....	323
5.5.2.4 Expert System Window Scroll Bar Navigation .....	324
5.5.2.5 Expert System Table Sorting .....	325
5.5.3 Bluetooth Protocol Expert System Toolbox .....	327
5.5.3.1 Toolbox Hardware Setup .....	327
5.5.3.2 Toolbox Pane .....	330
5.5.3.2.1 A2DP Tool .....	330
5.5.3.2.2 LE Tool .....	333
5.6 Bluetooth Audio Expert System™ .....	336
5.6.1 Supported Codec Parameters .....	337
5.6.2 Operating Modes .....	338
5.6.2.1 Non-Referenced Mode .....	338
5.6.2.2 Referenced Mode .....	338
5.6.2.3 Referenced Mode Testing Processes .....	341
5.6.2.3.1 System Calibration for Referenced Mode .....	343
5.6.2.3.2 Adjusting for Optimal Volume Levels .....	345
5.6.3 Audio Expert System™ Event Type .....	346
5.6.3.1 Event Type: Bluetooth Protocol .....	346
5.6.3.2 Event Type: Codec .....	347
5.6.3.3 Event Type: Audio .....	349
5.6.4 Audio Expert System™ Window .....	354
5.6.4.1 Global Toolbar .....	356
5.6.4.2 Wave Panel .....	358
5.6.4.2.1 Audio Stream Info .....	359
5.6.4.2.2 Local Controls .....	360
5.6.4.2.3 Audio Waveform Panel .....	361
5.6.4.2.4 Event Timeline .....	365
5.6.4.3 Event Table .....	366

---

5.6.4.4 Wave Panel & Event Table Pop-up Menu .....	368
5.6.4.5 Export Audio Data .....	369
5.6.4.6 Export Event Table .....	371
5.6.5 Frame, Packet, and Protocol Analysis Synchronization .....	371
5.7 Timing Analysis .....	372
5.7.1 Timing Analysis Navigation Toolbar .....	373
5.7.2 Timing Analysis Navigation Bar .....	376
5.7.3 Timing Analysis Timeline View .....	377
5.7.3.1 Logic Signals in Timeline View .....	382
5.7.3.2 Bluetooth, Wi-Fi & HCI Signals in Timeline View .....	382
5.7.3.3 Zooming in Timeline View .....	383
5.7.3.4 Timing Cursors & Measuring in Timeline View .....	385
5.7.3.5 Arranging Rows in Timeline View .....	387
5.8 Protocol Stacks .....	388
5.8.1 Protocol Stack .....	388
5.8.2 Creating and Removing a Custom Stack .....	391
5.8.3 How the Analyzer Auto-traverses the Protocol Stack .....	392
5.8.4 Providing Context For Decoding When Frame Information Is Missing .....	392
<b>Chapter 6 Navigating and Searching the Data .....</b>	<b>394</b>
6.1 Searching .....	394
6.2 Bookmarks .....	399
6.2.1 Adding a Bookmark .....	399
6.2.2 Showing Bookmarks on Views .....	402
<b>Chapter 7 Saving and Importing Data .....</b>	<b>405</b>
7.1 Saving Your Soder Data .....	405
7.1.1 Saving the Capture File .....	405
7.1.2 Saving the Entire Capture File with Save Selection .....	405
7.1.3 Save a Portion of Capture File with Save Selection .....	407
7.2 Adding Comments to a Capture File .....	410
7.3 Confirm Capture File (CFA) Changes .....	411
7.4 Loading and Importing a Capture File .....	412

---

7.4.1 Loading a Capture File .....	412
7.4.2 Importing Capture Files .....	413
7.5 Printing .....	414
7.5.1 Printing from the Frame Display/HTML Export .....	414
7.6 Exporting .....	416
7.6.1 Main windows - Byte Export .....	416
7.6.2 Export .....	419
7.6.3 Export to pcapng Format .....	420
<b>Chapter 8 General Information .....</b>	<b>426</b>
8.1 System Settings and Program Options .....	426
8.1.1 System Settings .....	426
8.1.2 Changing Default File Locations .....	427
8.1.3 Timestamping .....	430
8.1.3.1 Timestamping Options .....	430
8.2 Technical Information .....	434
8.2.1 BTSnoop File Format .....	434
8.2.2 Ring Indicator .....	437
8.2.3 Useful Character Tables .....	437
8.2.3.1 ASCII Codes .....	437
8.2.3.2 Baudot Codes .....	438
8.2.3.3 EBCDIC Codes .....	438
8.2.3.4 Communication Control Characters .....	439
8.2.4 Bluetooth Low Energy ATT Decoder Handle Mapping .....	440
8.3 Contacting Teledyne LeCroy Frontline Technical Support .....	441
8.4 License Manager .....	442
8.4.1 Introduction .....	442
8.4.2 Manage License Dialog .....	442
8.4.3 Trial Licenses .....	447
8.5 What's New .....	448
<b>Appendices .....</b>	<b>450</b>
Appendix A: X500 Technical Specifications/Service Information .....	450

---

Appendix B: X240 Technical Specifications/Service Information .....	451
Appendix C: Sodera Technical Specifications/Service Information .....	452
Appendix D: Sodera LE Technical Specifications/Service Information .....	453
Appendix E: File Extension Descriptions .....	453
Appendix F: Application Notes .....	454
F.1 Audio Expert System: aptX 'hiccup' Detected .....	455
F.1.1 Background .....	455
F.1.2 Test Setup .....	455
F.1.3 Discussion .....	456
F.1.4 Conclusions .....	459
F.2 Getting the Android Link Key for Classic Decryption .....	460
F.2.1 What You Need to Get the Android Link Key .....	460
F.2.2 Activating Developer options .....	460
F.2.3 Retrieving the HCI Log .....	460
F.2.4 Using the Wireless Protocol Suite software to Get the Link Key .....	462
F.3 Decrypting Encrypted Bluetooth® Low Energy .....	464
F.3.1 How Encryption Works in Bluetooth Low Energy .....	464
F.3.2 Bluetooth® Low Energy Security .....	466
F.3.3 Pairing .....	467
F.3.4 Pairing Methods .....	468
F.3.5 Encrypting the Link .....	469
F.3.6 Encryption Key Generation and Distribution .....	469
F.3.7 Encrypting The Data Transmission .....	469
F.3.8 IRK and CSRK Revisited .....	470
F.4 Table of Acronyms .....	470
Appendix G: ra X500 Wi-Fi 6E Frequencies .....	471



## Chapter 1 Frontline Hardware and Wireless Protocol Suite Software

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

- Classic *Bluetooth*
- *Bluetooth* Low Energy
- Dual Mode *Bluetooth* (simultaneous Classic and Low Energy)
- Wi-Fi
- 802.15.4

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

Wireless Protocol Suite software is an easy to use and powerful protocol analysis platform. Simply use the appropriate Frontline hardware or write your own proprietary code to pump communication streams directly into the Wireless Protocol Suite software where they are decoded, decrypted, and analyzed. Within the Wireless Protocol Suite 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 Wireless Protocol Suite software functions for your Frontline hardware. Should you have any questions contact the [Frontline Technical Support Team](#).

### 1.1 What is in this manual

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

- **Chapter 1 Frontline Hardware and Wireless Protocol Suite** 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 Wireless Protocol Suite software in Data Capture Methods. You will be introduced to the Main window that is the primary operating dialog in the Wireless Protocol Suite software.
- **Chapter 3 Configuration Settings**. The software and hardware are configured to capture data. Configuration settings may vary for a particular Frontline analyzer depending on the technology and network being sniffed. There are topics on configuring protocol decoders used to disassemble packets into frames and events.

- **Chapter 4 Capturing Data.** This Chapter describes how to start a capture session using the **Wireless Protocol Suite** software.
- **Chapter 5 Analyzing Data.** This chapter describes how to observe the captured packets, frames, layers and events using the **Wireless Protocol Suite** software.
- **Chapter 6 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 7 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 8 General Information.** This chapter provides advanced system set up and configuration information, timestamping information, and general reference information such as ASCII, Baudot, and EBCDIC codes. This chapter also provides information on how to contact Frontline's Technical Support team should you need assistance.

## 1.2 Computer Minimum System Requirements

Frontline hardware supports the following computer systems configurations:

- Operating System: Windows 10
- USB Port: USB 2.0 High-Speed or later

The Wireless Protocol Suite software must operate on a computer with the following minimum characteristics.

- Processor: Core i5 processor at 2.7 GHz
- RAM: 4 GB
- Free Hard Disk Space on C: drive: 20 GB

## 1.3 Software Installation

Download the installation software from [FTE.com](http://FTE.com). Once downloaded, double-click the installer and follow the directions.

Use this link: <http://www.fte.com/<product identifier, e.g. sodera>-soft>.

## Chapter 2 Getting Started

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

### 2.1 X500 Hardware

#### 2.1.1 Front Panel Controls and Connectors

The Frontline X500™ front panel is shown below. The panel provides controls to power up and shut down the Frontline X500 hardware, and it provides indicators to show the power and capture status.

#### 2.1.2 Front Panel Connectors

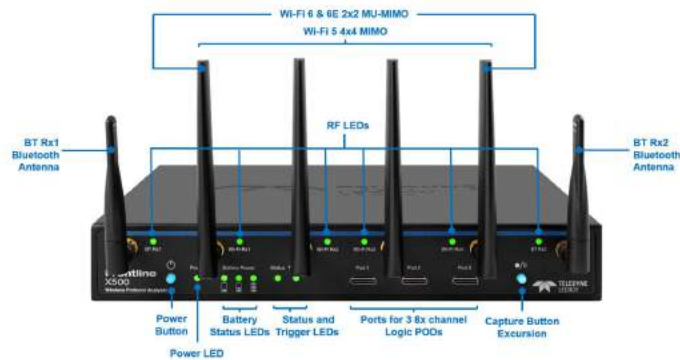


Figure 2.1 - X500 Front Panel Controls and Indicators

**Power Button:** The Power button illuminates when the unit is connected to a power source. Press and release the button to power on or power off the system.

**Status Indicators:** Colored LEDs show the status of power, capture and RF status.

Table 2.1 - X500 Front Panel Status Indicators

Indicator	Color	State	Status Indicated
<b>Power</b>	<b>None</b>	OFF	Unit is powered off.
	<b>Green</b>	Constant	Unit powered on with sufficient power source plugged in.
	<b>Blue</b>	Constant	Unit powered off with sufficient power source plugged in.
	<b>Red</b>	Fast Flash	Thermal warning threshold reached.
		Constant	System reaches thermal overload. Unit has started a controlled/sequenced power down.
<b>Battery Level 1</b>	<b>None</b>	OFF	Battery not present OR Battery not charged.
	<b>Green</b>	Constant	Battery discharging. Capacity 20% - 45%.
		Slow Flash	Battery charging. Capacity 20% - 45%.
	<b>Yellow</b>	Slow Flash	Battery charging. Capacity <20%..
		Fast Flash	Battery discharging. Capacity <20%.
<b>Battery Level 2</b>	<b>None</b>	OFF	Battery not present OR Battery <45% capacity, and not charging.
	<b>Green</b>	Constant	Battery discharging. Capacity 45% - 70%.
		Flash	Battery charging. Capacity 45% - 70%.
<b>Battery Level 3</b>	<b>None</b>	OFF	Battery not present OR Battery <70% capacity, and not charging.
	<b>Green</b>	Constant	Battery discharging. Capacity 70% - 100%.
		Flash	Battery charging. Capacity 70% - 100%.
<b>Status</b>	<b>None</b>	Off	Unit is powered off.
	<b>Yellow</b>	Slow Flash	Initializing (may not be seen if initialization is quick).
		Fast Flash	Unit is shutting down.
		Constant	Unit is in Recovery Mode.
	<b>Green</b>	Constant	Unit is initialized and ready to capture.
	<b>Blue</b>	Slow Flash	Unit is waiting for a Trigger (future).
		Fast Flash	Unit is capturing in Excursion mode or capture is not "OK" (future).
		Constant	Unit is capturing data.
<b>Red</b>	Constant	The unit failed to initialize or has a System Error.	
<b>Trigger</b>	<b>None</b>	Off	Reserved for future use.

Table 2.1 - X500 Front Panel Status Indicators(continued)

Indicator	Color	State	Status Indicated
BT Rx1	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing any combination of the following: Bluetooth data, 802.15.4 data, and/or spectrum.
	Red	Solid	The RF signal is too strong.
Wi-Fi Rx1	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing Wi-Fi 5 or Wi-Fi 6 data.
Wi-Fi Rx2	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing Wi-Fi 5 data.
Wi-Fi Rx3	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing Wi-Fi 5 data.
Wi-Fi Rx4	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing Wi-Fi 5 or Wi-Fi 6 data.
BT Rx2	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing any combination of the following: Bluetooth data, 802.15.4 data, and/or spectrum.
	Red	Solid	The RF signal is too strong.

**PODs with Oculink Connectors:** There are 3 PODs to connect x8 channel logic cable to capture HCI UART/SPI and logic signals.

**Capture Button for Excursion Mode:** The capture button for excursion captures illuminates when the unit is connected to a power source. Pressing this button will begin data capture - the same as the Record button in the Wireless Protocol Suite. The Excursion Mode button is inactive when X500 is connected to a computer.

To operate in the Excursion mode, the X500 hardware must have been previously configured from the Wireless Protocol Suite prior to disconnecting from the computer. The X500 hardware will retain those configuration settings when disconnected from the computer. Refer to the Wireless Protocol Suite Hardware and Software User Manual for Excursion mode operating details.

**Antenna SMA Connectors:** Antenna attaching point for Bluetooth and Wi-Fi capture.

### 2.1.3 Rear Panel Connectors

The rear panel is shown below. The panel provides connectors for external power and for a connection to the computer hosting the **Wireless Protocol Suite** software.



Figure 2.2 - Frontline X500 Rear Panel Connectors

**Trigger In and Out:** Reserved for future use.

**Sync/Data Connector:** The MicroD25 connector will be used in a future release to connect multiple X500 or other PSG analyzers to capture time synced data using CrossSync technology.

**HC USB1/HCI USB2:** USB Type A and USB Type mini-B connectors allow capture of HCI USB data.

**Ethernet:** The Ethernet connector is reserved for a future use.

**Host:** USB C 3.0 port for connecting X500 to the host computer where the Wireless Protocol Suite resides. This connector provides host computer command, control, and data transfer

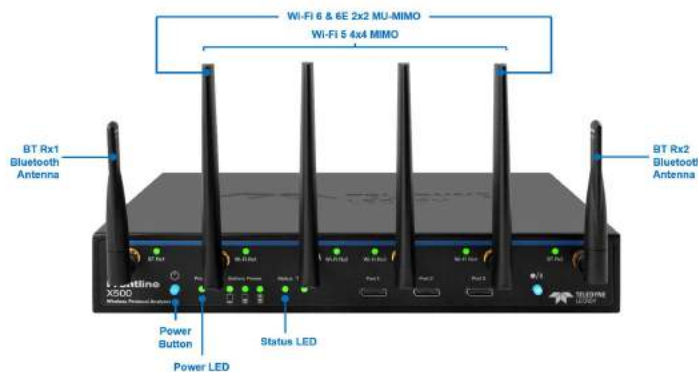
**Auto-boot ON/OFF :** When the Auto-boot is ON, it allows powering the unit automatically when an external power is applied. The feature is particularly useful during a remote setup.

**Power:** The Frontline X500 use a DC supply of 15V 6A.

### 2.1.4 Attach Antennas

Remove the Frontline X500 hardware from the box and attach the six antennas to the SMA connectors on the front panel. As name indicates, BT Rx1 and BT Rx2 are Bluetooth antenna connectors and Wi-Fi Rx1, 2, 3, and 4 are Wi-Fi antenna to capture Wi-Fi 5 and Wi-Fi Rx 1 and 4 to capture Wi-Fi 6/6E. The base of the antennas can be carefully rotated by 90 degrees so that the antenna points upward.

The X500 is configured to use Antenna Diversity for capture to intelligently improve performance and eliminate the need to place the unit in a specific position when wireless channels are affected by multipath, fading, and interference. See Section 4.1.1 for more information about Antenna Diversity.



## 2.1.5 Applying Power

Connect the 15V Power adapter supplied with the product to the X500 hardware. The front panel Power indicator LED will be a constant blue indicating that there is sufficient power. To turn on the X500 hardware press and release the Power button on the front panel. This action will provide a clean start for X500 hardware. The front panel six antenna LEDs will blink green three times and the Status indicator LED will be a constant green once the unit has completely booted up. If the front panel Power indicator begins blinking red, the X500 hardware is approaching thermal overload temperature, between 70° C and 80° C (158° F and 185° F), and should be shutdown. When the hardware reaches thermal overload, it will automatically shut down and the Power indicator will turn off.

**Note:** For information on installing a Frontline X500 Battery Pack as an external power source for the Frontline X500 protocol Analyzer, see the *Frontline X500™ Battery Installation Guide*.

### 2.1.5.1 Applying Power using X500 Battery Pack

Refer to the Frontline X500 Installation Guide to install the X500 battery.

After installing the battery, apply power to the X500 by switching the dip switch to the ON state. Check the battery charge on the front panel Battery Charge LEDs.



Figure 2.3 - X500 Battery in the ON state

If a charge is necessary, connect the external power source until the battery is fully charged. Once you connect the power source the LEDs will start blinking based on the charge level.

Table 2.2 - X500 Battery Level Indicators

Indicator	Color	State	Status Indicated
Battery Level 1	None	OFF	Battery not present OR Battery not charged.
	Green	Constant	Battery discharging. Capacity 20% - 45%.
		Slow Flash	Battery charging. Capacity 20% - 45%.
	Yellow	Slow Flash	Battery charging. Capacity <20%..
Fast Flash		Battery discharging. Capacity <20%.	

Table 2.2 - X500 Battery Level Indicators(continued)

Indicator	Color	State	Status Indicated
Battery Level 2	None	OFF	Battery not present OR Battery <45% capacity, and not charging.
	Green	Constant	Battery discharging. Capacity 45% - 70%.
		Flash	Battery charging. Capacity 45% - 70%.
Battery Level 3	None	OFF	Battery not present OR Battery <70% capacity, and not charging.
	Green	Constant	Battery discharging. Capacity 70% - 100%.
		Flash	Battery charging. Capacity 70% - 100%.

### 2.1.6 Recovery Mode

Recovery mode occurs when something prevents the X500 unit from successfully loading the firmware images during power up. In this state, the X500 powers on with an alternate recovery firmware image. When the unit is in recovery mode, the status indicator light is a constant purple. In recovery mode, the system prevents the user from capturing data. However, the user can upgrade the firmware. The upgrade process should correct the problem allowing the unit to power on normally. When the Wireless Protocol Suite software starts, the software automatically prompts the user to update the firmware.

### 2.1.7 Connecting X500 for HCI and Logic Capture

**Warning:** The X500 Logic Analyzer Pods are designed for use with TTL voltage levels, 0 to 3.3 volts maximum. Exceeding the 3.3 volts maximum may damage the pods.

To capture UART and logic data at the Bluetooth Host Controller processor interface using a wired connection:

- Connect a Logic Analyzer Pod to one of the Oculink connectors on the front panel of the X500. A Logic Analyzer Pod can be connected to either Oculink connector or two/three pods can be connected to the Oculink connectors at the same time.





Figure 2.4 - X500 Logic Analyzer Pods Installed on X500

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



Figure 2.5 - X500 Logic Analyzer Pod with Flying Lead Assembly



Figure 2.6 - Installing the Flying Lead Assembly on the X500 Logic Analyzer Pod

- Attach an appropriate Flying Lead Assembly micro-clip to the Bluetooth logic or HCI signal test point in accordance with the following table.

Table 2.3 - X500 Logic Analyzer Pod Interface Pins

Pin	Label
1	Ground
2	Data 0
3	Data 1
4	Data 2
5	Data 3
6	Ground
7	Data 4
8	Data 5
9	Data 6
10	Data 7
11	Ground

- To remove the Flying Lead Assembly from the Logic Analyzer Pod, depress the release key on the Flying Lead Assembly.

Figure 2.7 - Flying Lead Assembly Header Release

- To remove the Logic Analyzer Pod from the X500, depress the release key on the Oculink connector.



Figure 2.8 - Oculink Connector Release

### 2.1.7.1 UART Capture Configuration

Successful HCI UART capture requires the following Logic Analyzer Pod connections.

Table 2.4 - Required UART Layer Connections

UART Signal	Logic Analyzer Pod Pin	Comment
Tx	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the Device Under Test (DUT) TX pin. Only 1 data pin can be used. That pin cannot be used for Rx. Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
Rx	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the DUT Rx pin. Only 1 data pin can be used. That pin cannot be used for Tx. Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .

Table 2.4 - Required UART Layer Connections(continued)

UART Signal	Logic Analyzer Pod Pin	Comment
<b>GND</b>	Any line labeled Ground	Any of the three Ground pins can be used to connect the DUT ground to the Logic Analyzer Pod.

### 2.1.7.2 Logic Event Capture Configuration

Successful logic event capture requires the following Logic Analyzer Pod connections. The Logic Analyzer Pod has up to eight pins that can be used for logic event capture. When capturing many rapidly occurring events, WPS may not update in real time. The analyzer buffers unsent events and continue to send them to WPS until the buffer is cleared. Therefore, after stopping the recording the user may see additional events received.

Table 2.5 - Required Logic Connections

Logic Signal	Logic Analyzer Pod Pin	Comment
<b>0</b>	<b>Data 0</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
<b>1</b>	<b>Data 1</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
<b>2</b>	<b>Data 2</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
<b>3</b>	<b>Data 3</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
<b>4</b>	<b>Data 4</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
<b>5</b>	<b>Data 5</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
<b>6</b>	<b>Data 6</b>	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .

Table 2.5 - Required Logic Connections(continued)

Logic Signal	Logic Analyzer Pod Pin	Comment
7	Data 7	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Capture Options. See <a href="#">Capture Options -&gt; Wired Tab: X500</a> .
GND	Any line labeled Ground	Any of the three Ground pins can be used to connect the DUT ground to the Logic Analyzer Pod.

### 2.1.7.3 SPI Capture Configuration

Successful HCI SPI capture requires the following Logic Analyzer Pod connections.

Table 2.6 - Required Logic Connections

SPI Signal	Logic Analyzer Pod Pin	Comment
SCLK	Any single line labeled Data 0 through Data 7	Connect to the Device Under Test (DUT) CLK pin. Only 1 data pin can be used.
MOSI	Any single line labeled Data 0 through Data 7	Connect to the Device Under Test (DUT) MOSI pin. Only 1 data pin can be used.
MISO	Any single line labeled Data 0 through Data 7	Connect to the Device Under Test (DUT) MISO pin. Only 1 data pin can be used.
SS/CS	Any single line labeled Data 0 through Data 7	Connect to the Device Under Test (DUT) SS/CC pin. Only 1 data pin can be used.
GND	Any line labeled Ground	Any of the three Ground pins can be used to connect the DUT ground to the Logic Analyzer Pod.

## 2.2 X240™ Hardware

### 2.2.1 Front Panel Controls and Connectors

The Frontline X240™ front panel is shown below. The panel provides controls to power up and shut down the Frontline X240 hardware, and it provides indicators to show the power, battery, and capture status.

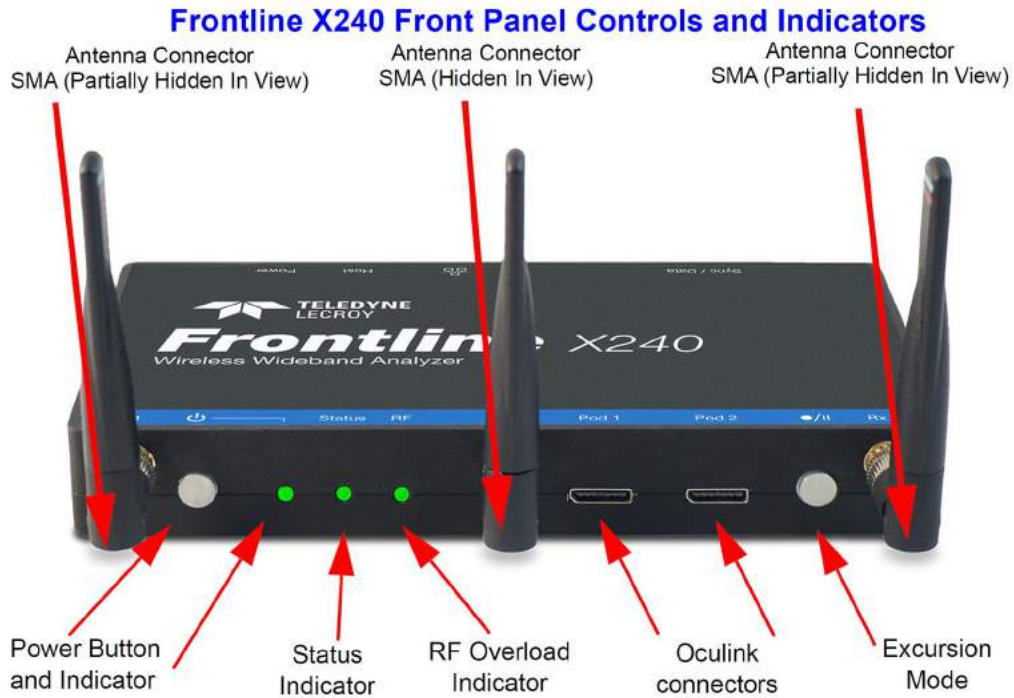


Figure 2.9 - X240 Front Panel Controls and Indicators

**Power On/Off Button:** Press and release the button to power on or power off the system.

**Status Indicators:** Colored LEDs show the status of power and capture.

Table 2.7 - X240 Front Panel Status Indicators

Indicator	Color	State	Status Indicated
Power	Blue	Constant	Unit is connected to power source but powered off.
	Purple	Constant	Insufficient Power
	Green	Constant	Unit is switched on.
	Red	Fast Flash	Unit is approaching its maximum thermal load and should be shut down.
		Constant	Unit has reached thermal overload or Unit has started a controlled/sequenced shutdown.
Status	None	Off	Unit is powered off.
	Yellow	Slow Flash	Initializing (may not be seen if initialization is quick).
		Fast Flash	Unit is shutting down.
		Constant	Unit is in Recovery Mode.
	Green	Constant	Unit is initialized and ready to capture.
	Blue	Slow Flash	Unit is waiting for a Trigger (future).
		Fast Flash	Unit is capturing in Excursion mode or capture is not "OK" (future).
		Constant	Unit is capturing data.
Red	Constant	The unit failed to initialize or has a System Error.	
RF	None	Off	Unit is powered off or Unit is not actively capturing data.
	Green	Constant	Unit is capturing Bluetooth data.
	Red	Fast Flash	The RF signal is too strong.

**Antenna SMA Connector:** Antenna attaching point.

**Excursion Mode** When configured Excursion mode, pressing this button will begin data capture - the same as the Record/Recording button on the X240 Window Datasource toolbar. The **Excursion Mode** button is inactive when X240 is connected to a computer. To operate in the Excursion mode, the X240 hardware must have been previously configured from the **Wireless Protocol Suite** prior to disconnecting from the computer. The X240 hardware will retain those configuration settings when disconnected from the computer. Refer to the Wireless Protocol Suite Hardware and Software User Manual for Excursion mode operating details.

**Oculink Connectors:** For connection to eight (8) channel PODs used for hardwired connection to user's equipment under test.

## 2.2.2 Rear Panel Connectors

The rear panel is shown below. The panel provides connectors for external power and for a connection to the computer hosting the **Wireless Protocol Suite** software.



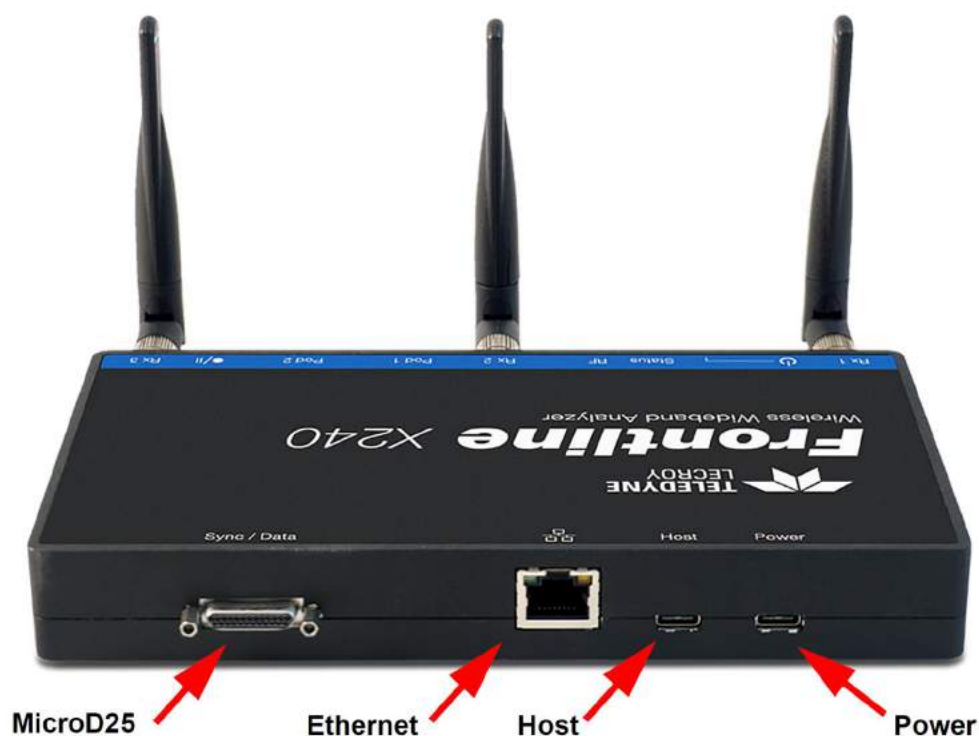


Figure 2.10 - Frontline X240 Rear Panel Connectors

**Host:** USB C 2.0/3.0 port for connecting X240 to the host computer where the **Wireless Protocol Suite** resides. This connector provides host computer command, control, and data transfer. If the USB cable is connected to a computer with a USB C 3.0 with power delivery or higher then the X240 can be powered through this port as well and will not need a USB cable connected to the Power connector on the X240.

**Power:** Type C PD power adapter—preferably the adapter/s supplied with the X240—is required.

**Ethernet:** The Ethernet connector is for a future release to support PoE (Power over Ethernet) and Host communications.

**MicroD25:** The **MicroD25** connector is used to connect two X240s to provide Synchronized X240(2) technology (BLE & BR/EDR or BLE & Wi-Fi as examples) captures timesynced via the CATC Sync cable. The MicroD25 connector can also be used to connect three X240s to provide Synchronized X240 (3) technology (BLE & BR/EDR & Wi-Fi) captures timesynced via the CrossSync cable kit.

**PC HOST :** USB 2.0 port for connecting X240 too the host computer where the **Wireless Protocol Suite** software resides. This connector provides host computer command, control, and data transfer.

### 2.2.3 Attach Antenna



Figure 2.11 - Frontline X240 Antenna Attachment Points on Front Panel

Remove the Frontline X240 hardware from the box and attach the three ANTENNAS to the SMA connectors on the front panel. The base of the antennas can be carefully rotated by 90 degrees, so that the antenna points upward.

### 2.2.4 Applying Power

Teledyne LeCroy recommends that the X240 hardware be powered by the supplied PD adapters or equivalent. Connect the USB C cable to the connector labeled **Power** on the back panel of the X240.

To apply power to X240 hardware depress and release the Power button on the front panel. This action will provide a clean start for X240 hardware. The front panel **Power** indicator LED will be a constant green. Should the front panel **Power** indicator begin blinking red, the X240 hardware is approaching thermal overload temperature between 70° C and 80° C (158° F and 185° F) and should be shutdown. When the hardware reaches thermal overload it will automatically shut down and the **Power** indicator will turn off.

### 2.2.5 Recovery Mode

Recovery mode occurs when something prevents the x240 unit from successfully loading the firmware images during power up. In this state, the x240 powers on with an alternate recovery firmware image. When the unit is in recovery mode, the status indicator light is a constant yellow.

In recovery mode, the system prevents the user from capturing data. However, the user can upgrade the firmware. The upgrade process should correct the problem allowing the unit to power on normally. When the Wireless Protocol Suite software starts, the software automatically prompts the user to update the firmware.

## 2.2.6 Connecting X240 for HCI and Logic Capture

**Warning:** The X240 Logic Analyzer Pods are designed for use with TTL voltage levels, 0 to 3.3 volts maximum. Exceeding the 3.3 volts maximum may damage the pods.

To capture UART, SPI and logic data at the Bluetooth Host Controller processor interface using a wired connection:

- Connect a Logic Analyzer Pod to one of the Oculink connectors on the front panel of the X240. A Logic Analyzer Pod can be connected to either Oculink connector or two pods can be connected to both Oculink connectors at the same time.



Figure 2.12 - X240 Logic Analyzer Pods Installed on X240

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



Figure 2.13 - X240 Logic Analyzer Pod with Flying Lead Assembly



Figure 2.14 - Installing the Flying Lead Assembly on the X240 Logic Analyzer Pod

- Attach an appropriate Flying Lead Assembly micro-clip to the Bluetooth logic or HCI signal test point in accordance with the following table.

Table 2.8 - X240 Logic Analyzer Pod Interface Pins

Pin	Label
1	Ground
2	Data 0
3	Data 1
4	Data 2
5	Data 3
6	Ground
7	Data 4
8	Data 5
9	Data 6
10	Data 7
11	Ground

- To remove the Flying Lead Assembly from the Logic Analyzer Pod, depress the release key on the Flying Lead Assembly.



Figure 2.15 - Flying Lead Assembly Header Release

- To remove the Logic Analyzer Pod from the X240, depress the release key on the Oculink connector.



Figure 2.16 - Oculink Connector Release

### 2.2.6.1 UART Capture Configuration

Successful HCI UART capture requires the following Logic Analyzer Pod connections.

Table 2.9 - Required UART Layer Connections

UART Signal	Logic Analyzer Pod Pin	Comment
<b>Tx</b>	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the Device Under Test (DUT) TX pin. Only 1 data pin can be used. That pin cannot be used for Rx. Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
<b>Rx</b>	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the DUT Rx pin. Only 1 data pin can be used. That pin cannot be used for Tx. Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
<b>GND</b>	Any line labeled Ground	Any of the three Ground pins can be used to connect the DUT ground to the Logic Analyzer Pod.



### 2.2.6.2 Logic Event Capture Configuration

Successful logic event capture requires the following Logic Analyzer Pod connections. The Logic Analyzer Pod has up to eight pins that can be used for logic event capture.

Table 2.10 - Required Logic Connections

Logic Signal	Logic Analyzer Pod Pin	Comment
0	Data 0	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
1	Data 1	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
2	Data 2	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
3	Data 3	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
4	Data 4	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
5	Data 5	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
6	Data 6	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
7	Data 7	TTL logic input. Connect to the Device Under Test (DUT). Also select this pin in the Wired tab of the Record Options. See <a href="#">Record Options -&gt; Wired Tab: X240</a> .
GND	Any line labeled Ground	Any of the three Ground pins can be used to connect the DUT ground to the Logic Analyzer Pod.



### 2.2.6.3 SPI Capture Configuration

Successful HCI SPI capture requires the following Logic Analyzer Pod connections.

Table 2.11 - Required Logic Connections

SPI Signal	Logic Analyzer Pod Pin	Comment
<b>SCLK</b>	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the Device Under Test (DUT) CLK pin. Only 1 data pin can be used.
<b>MOSI</b>	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the Device Under Test (DUT) MOSI pin. Only 1 data pin can be used.
<b>MISO</b>	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the Device Under Test (DUT) MISO pin. Only 1 data pin can be used.
<b>SS/CS</b>	Any single line labeled <b>Data 0</b> through <b>Data 7</b>	Connect to the Device Under Test (DUT) SS/CC pin. Only 1 data pin can be used.
<b>GND</b>	Any line labeled <b>Ground</b>	Any of the three Ground pins can be used to connect the DUT ground to the Logic Analyzer Pod.

### 2.2.7 Setting Up for Synchronized X240 (2) Capture

The Frontline X240 hardware allows for synchronization of X240 hardware clocks and timestamping. The CATC Sync cable connected to the MicroD25 connectors on the backs of two X240 hardware allows both the X240 hardware to run off a common clock, ensuring precise timestamp synchronization while capturing multiple wireless technologies such as *Bluetooth BR/EDR* and *Bluetooth LE*.



Figure 2.17 - CATC Sync Cable

Connect one end of the CATC Sync Cable to the MicroD25 port on the back of one X240 and the other end of the CATC Sync Cable to the MicroD25 port on the back of the other X240.



Figure 2.18 - Two X240 Units connected with the CATC Sync Cable

Refer to the [Rear Panel Connectors on page 28](#).

### Troubleshooting

If the X240 indicates that synchronization cables are not properly connected, these are actions to take to reestablish synchronization:

- Reseat the MicroD25 cable on the back of each X240.
- Rebooting each X240.

### 2.2.8 Setting Up for Synchronized X240 (3) Capture

The Frontline X240 hardware allows for synchronization of X240 hardware clocks and timestamping. The CATC Sync cable kit connected to the MicroD25 connectors on the backs of three X240 hardware allows all the X240 hardware to run off a common clock, ensuring precise timestamp synchronization while simultaneously capturing three wireless technologies, *Bluetooth* (Le, Classic or Dual mode), *Wi-Fi* and 802.15.4.



Figure 2.19 - CATC Sync Cable Kit

Connect the 3 CATC Sync Cable Kits together by connecting the DB9 Sync Out connector of one kit to the DB9 Sync In connector of the second kit. Connect the DB9 Sync Out connector of the second kit to the DB9 Sync In connector of the third kit.

Connect MicroD25 connector of the first CATC Sync Cable kit to the MicroD25 port on the back of one X240. Connect the MicroD25 connector of the second kit to the MicroD25 port on the back of the second X240. Connect the MicroD25 connector of the third kit to the MicroD25 port on the back of the third X240.

The X240s are now ready for Synchronized X240 (3) capture.



Figure 2.20 - Three X240 Units connected with CATC Sync Cable Kits

Refer to the [Rear Panel Connectors on page 28](#).

### Troubleshooting

If the X240 indicates that synchronization cables are not properly connected, these are actions to take to reestablish synchronization:

- Reseat the MicroD25 cable on the back of each X240.
- Reseat the DB9 connections between the CATC Sync Cable kits.
- Rebooting each X240.

## 2.3 Soderia™ Hardware

### 2.3.1 Front Panel Controls

The Teledyne LeCroy Soderia™ front panel is shown below. The panel provides controls to power up and shut down the Frontline Soderia hardware, and it provides indicators to show the power, battery, and capture status.

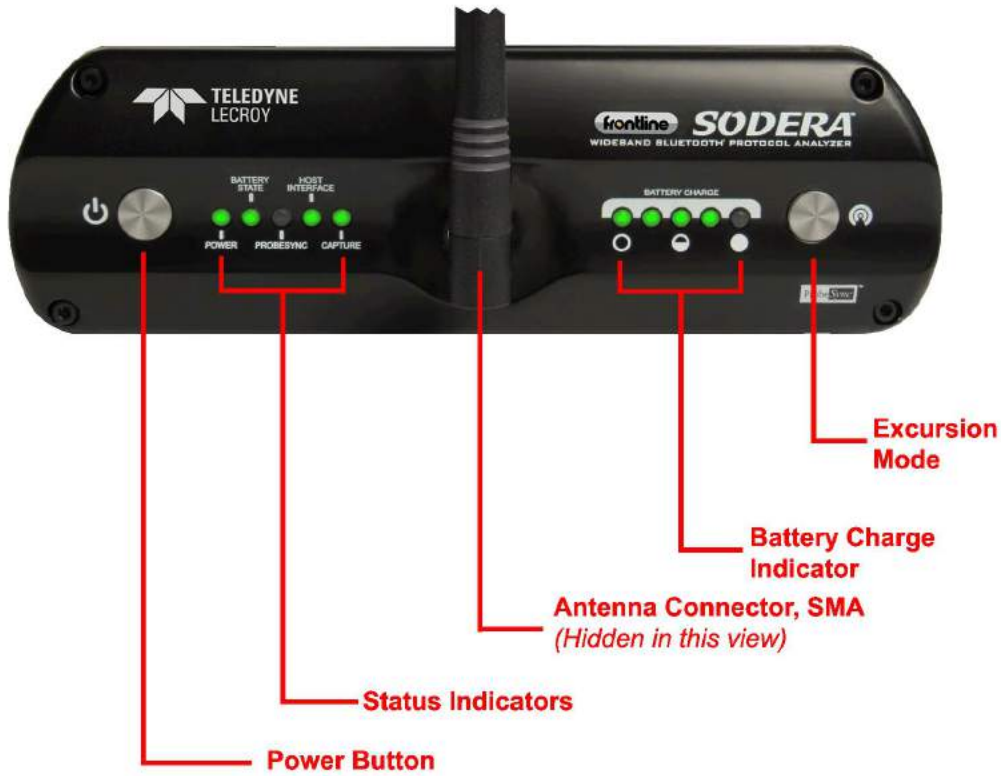


Figure 2.21 - Soderas Front Panel Controls and Indicators

**Power On/Off Button:** Press and hold the button for at least 1/2 second, and then release the button to power on or power off the system.

Pressing and holding the button for at least five seconds will initiate an **emergency shut down** sequence.

**Status Indicators:** Colored LEDs show the status of power and capture.

Table 2.12 - Soderas Front Panel Status Indicators

Indicator	Color	State	Status Indicated
Power	None	Off	Unit is powered off
	Green	Constant	Unit is switched on
	Red	Blinking	Unit is approaching its maximum thermal load and should be shut down.
		Constant	Unit has been automatically disabled due to thermal overload.
	Amber	Constant	Unit is powering down.
Battery State	None	Off	No battery present
	Green	Constant	Battery present and is at normal operating voltage
		Slow Flash	Battery charging
Amber	Fast Flash	Battery fault	

Table 2.12 - Sodera Front Panel Status Indicators(continued)

Indicator	Color	State	Status Indicated
Host Interface	None	Off	No host interface is connected.
	Green	Constant	Host interface is connected.
	Amber	Constant	Internal error
Capture	None	Off	Unit is not actively capturing data
	Green	Constant	Unit is capturing data
	Red	Constant	Unit has engaged RF overload protection; the RF signal is too strong.

**Antenna SMA Connector:** Antenna attaching point.

**Battery Charge :** The following table shows the charge state of the installed battery. When the battery is not installed, all LEDs are off except when the unit is in the process of powering up. In that case they repeatedly light up in sequence.

Table 2.13 - Sodera Battery Charge State LED Indicators

Indicator LEDs	Charge Status
	Greater than 80%
	Between 60 and 80%
	Between 40 and 60%
	Between 20 and 40%
	Less than 20%
	Not Active

**Excursion Mode:** When configured for Excursion mode, pressing this button will begin data capture—the same as the **Record/Recording** button on the Sodera Window DatasourceToolbar. The **Excursion Mode** button is inactive when Sodera is connected to a computer. To operate in the Excursion mode, the Sodera hardware must have been previously configured from the Wireless Protocol Suite prior to disconnecting from the computer. Refer to the Wireless Protocol Suite Hardware and Software User Manual for Excursion mode operating details.

### 2.3.2 Rear Panel Connectors

The rear panel is shown below. The panel provides connectors for external power, **ProbeSync™**, HCI, and for connection to the computer hosting the **Wireless Protocol Suite**.



Figure 2.22 - Sodera Rear Panel Connectors

**+12 VDC:** Connection to the Teledyne LeCroy supplied AC-to-DC power adapter, or a 12 VDC auxiliary vehicle outlet system can be used.

**ProbeSync™ IN/OUT:** Used for synchronizing multiple capture devices. Sodera can act as a clock source (central) device providing the clock to synchronize timestamping with connected target (peripheral) devices. When operating as a central device the **OUT** RJ-45 connector provides the synchronizing clock. The synchronizing clock can be attached to a peripheral Sodera or a Frontline 802.11, for example. When operating as a peripheral device, the IN RJ-45 connector receives the synchronizing clock from the central Sodera unit.

**HCI USB 1/HCI USB 2:** USB Type B and a USB Type A connectors allow capture of HCI USB data. HCI USB 1 and HCI USB 2 are independent groupings of the Type A and Type B connectors. The HCI USB 1 connectors use the same Sodera unit internal interface as the Sodera HCI POD1 UART pins. Likewise the HCI USB 2 connectors use the same internal interface as the Sodera HCI POD2 UART pins. Therefore you cannot simultaneously capture USB and UART on the "1" interface or on the "2" interface. Refer to Connecting for USB Capture and Connecting for HCI/WCI-2 & Logic Capture in the Wireless Protocol Suite Hardware and Software User Manual.

**PC HOST :** USB 2.0 port for connecting Sodera to the host computer where the Wireless Protocol Suite resides. This connector provides host computer command, control, and data transfer.

**Note:** At this time all other rear panel connectors are inactive.



### 2.3.3 Attach Antenna



Figure 2.23 - Antenna Attachment Point

Remove the Frontline Soderas™ hardware from the box and attach the antenna to the SMA connector on the front panel. The base of the antenna can be carefully rotated by 90 degrees, so that the antenna points upward.

### 2.3.4 Applying Power

The Soderas hardware is powered by three methods: the Teledyne LeCroy supplied AC-to-DC adapter, an external DC power source that can include power from an automobile auxiliary power source and an optional internal battery.

To apply power to Soderas use one of the three methods:

1. Connect the provided AC-to-DC power adapter to the **+12VDC** connector on the rear panel and then connect the adapter into an AC source.
2. Connect a DC power source supplying +12 VDC directly to the **+12VDC** connector on the rear panel.
3. Install the battery.

To start the Soderas Analyzer, depress the Power button on the front panel for at least 1/2 second and then release. This action will provide a clean start for Soderas hardware. The battery charge state indicator LEDs will repeatedly flash in sequence while the unit powers up.

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



Should the front panel **Power** indicator begin blinking red, the Sodera hardware is approaching thermal overload temperature between 50 °C and 60 °C (122 °F and 140 °F) and should be shut down. When the hardware reaches thermal overload it will automatically shut down and the **Power** indicator will be a constant red.

### 2.3.5 Battery Power

Frontline Soderas™ has an internal battery power option that allows the user to extend the range of the analyzer to include locations without easy access to external power sources. The battery installation is not necessary to operate Soderas with an external AC or DC power source.

The battery is an intelligent lithium rechargeable battery. Frontline Soderas hardware will operate solely on battery power for at least one hour. The battery is charged with an external charging unit or can be charged when installed provided Soderas is connected to an external power source.

#### 2.3.5.1 Battery Install

Turn off power and disconnect the external power source.



Figure 2.24 - Soderas Battery Compartment with Cover Opened

To change or install a battery, start by opening the battery compartment by turning the fastener counterclockwise. The cover is held in place by two tabs on the side opposite the fastener. Slide the cover towards the rear connector panel.



Figure 2.25 - Sodera Battery Removal Using the Tab

If changing the battery, remove the battery from the compartment by lifting on the tab attached to the battery and carefully lifting it upwards until free of the contacts.



Figure 2.26 - Sodera Battery Connectors, bottom side shown.

To install the battery, position the battery connectors over the connectors in the Sodera battery compartment. Gently press down until the battery makes firm contact.



Figure 2.27 - Sodera Battery: Press to Make Contact

Insert the battery cover tabs in the slots towards the Sodera front panel. Lower the cover and use a screw driver to turn the fastener clockwise until it is firmly engaged.



Figure 2.28 - Sodera Battery Cover: Insert Tabs



Figure 2.29 - Sodera Battery Cover, turn clockwise to secure

After installing the battery, apply power to the Sodera and power it up. Check the battery charge on the front panel **Battery Charge** LEDs. If a charge is necessary, keep the Sodera connected to an external power source until the battery is fully charged.

**Note:** When using the Sodera in Excursion mode and powered by the battery, it is recommended to have a fully charged battery before beginning data capture.

### 2.3.6 Connecting for HCI & Logic Capture

To capture UART and logic data at the *Bluetooth* Host Controller processor interface using a wired connection:

**Note:** SPI and SDIO are not supported on Sodera Analyzers.

- Connect an HCI Pod to the bottom of the Sodera unit in **POD 1** or **POD 2**.



Figure 2.30 - HCI Pods Installed on Soderia

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



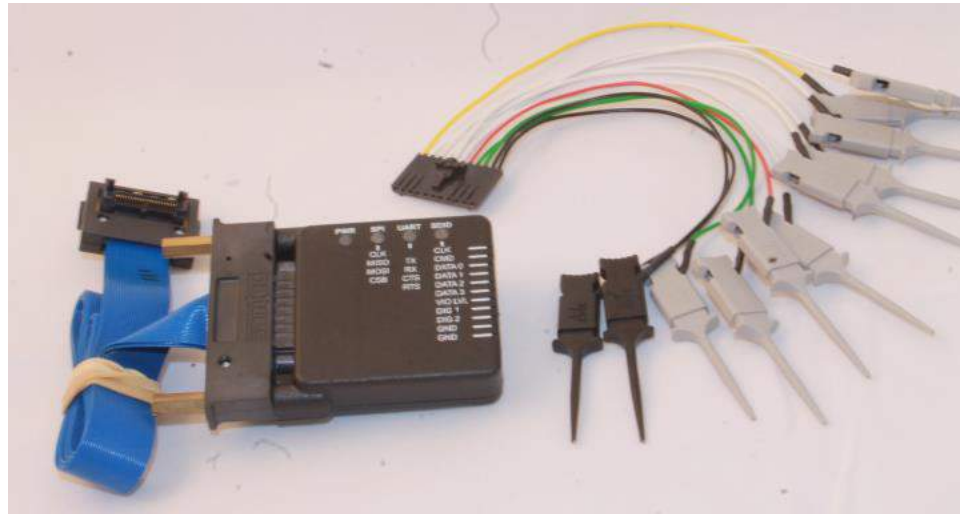


Figure 2.31 - HCI Pod with Flying Lead Assembly

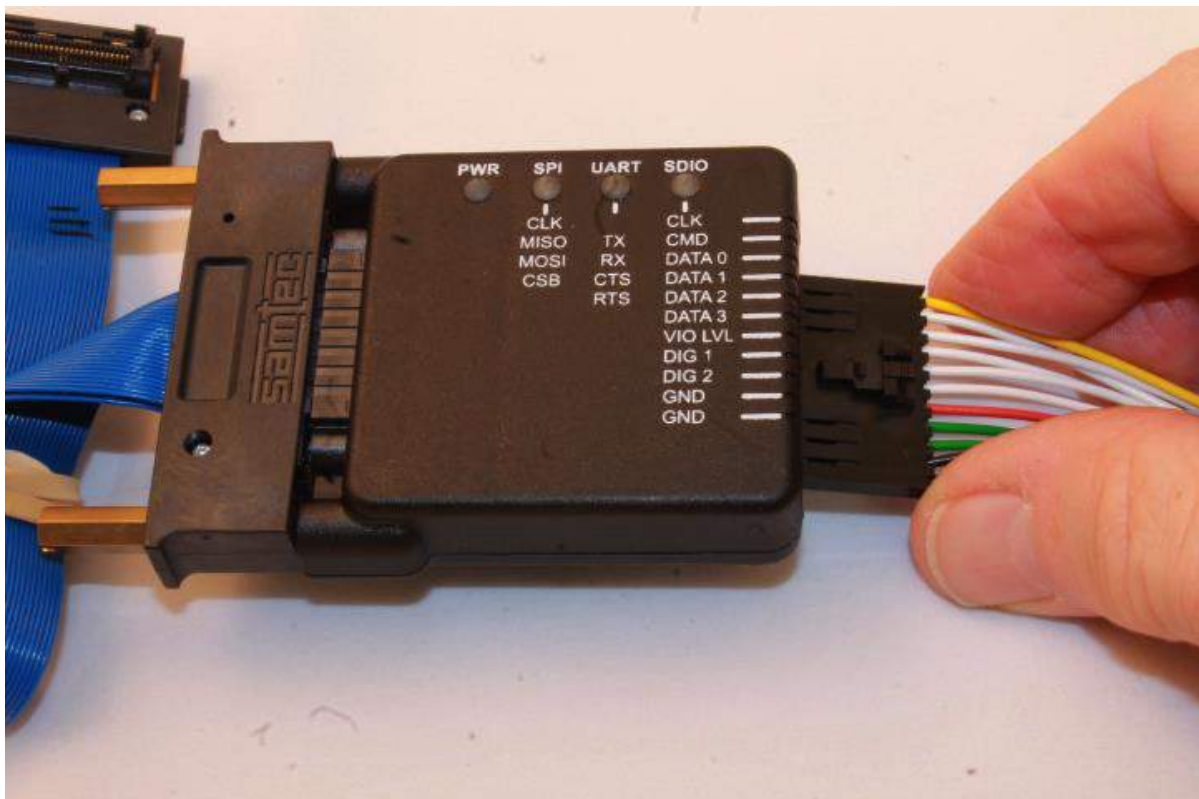


Figure 2.32 - Installing the Flying Lead Assembly on the HCI Pod

- Attach an appropriate Flying Lead Assembly micro-clip to the *Bluetooth* HCI signal test point in accordance with the following table.

Table 2.14 - Sodera HCI Interface Pins

Transport Layer			Logic	Pin	Wire Color
SPI	UART	SDIO			
CLK		CLK		1	Yellow
MISO	TX	CMD		2	White
MOSI	RX	DATA 0		3	White
CSB	CTS	DATA 1		4	White
	RTS	DATA 2		5	White
		DATA 3		6	White
	VIO LVL	VIO LVL	VIO LVL	7	Red
		DIG 1	DIG 1	8	Green
		DIG 2	DiG 2	9	Green
	GND	GND	GND	10	Black
	GND	GND	GND	11	Black

**Note:** SPI and SDIO are not supported on Sodera Analyzers.

- To remove the Flying Lead Assembly from the HCI Pod, depress the release key on the Flying Lead Assembly.

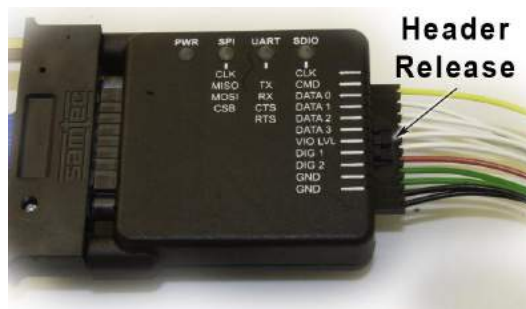


Figure 2.33 - Flying Lead Assembly Header Release

### UART Capture Configuration

Successful HCI UART capture requires the following Pod connections.

Table 2.15 - Required UART Layer Connections

Signal Name	Pin	Wire Color	Comment
TX	2	White	Connect to the Device Under Test (DUT) TX pin.
RX	3	White	Connect to the DUT RX pin.

Table 2.15 - Required UART Layer Connections (continued)

Signal Name	Pin	Wire Color	Comment
VIO LVL	7	Red	I/O voltage reference that designates the threshold for a logic level "1".. The VIO LVL minimum voltage is 1.65 Vdc. The supplied voltage needs to be the DUT logic signal level that designates a logic level "1". Some DUTs will have a VIO signal/tap. If a VIO tap is not available, use the DUT rail/power supply (Vcc/Vdd). If an I/O reference tap is available, use that as the VIO LVL source.
GND	10	Black	Either one of these pins can be used to connect the DUT ground to the HCI pod.
GND	11	Black	

### Logic Event Capture Configuration

Successful logic event capture requires the following Pod connections.

Table 2.16 - Required Logic Connections

Signal Name	Pin	Wire Color	Comment
DIG 1	8	Green	TTL logic input. Connect to the Device Under Test (DUT)
DIG 2	9	Green	TTL logic input. Connect to the DUT.
VIO LVL	7	Red	I/O voltage reference that designates the threshold for a logic level "1".. The VIO LVL minimum voltage is 1.65 Vdc. The supplied voltage needs to be the DUT logic signal level that designates a logic level "1". Some DUTs will have a VIO signal/tap. If a VIO tap is not available, use the DUT rail/power supply (Vcc/Vdd). If an I/O reference tap is available, use that as the VIO LVL source.
GND	10	Black	Either one of these pins can be used to connect the DUT ground to the HCI pod.
GND	11	Black	

### 2.3.7 Connecting for USB Capture

The HCI USB connectors are located on the Soderia rear panel connectors (see [2.3.2 Rear Panel Connectors on page 42](#)). USB testing is normally performed by capturing the USB traffic between a USB device and a host computer or controlling device. In the image below we see the normal configuration of a *Bluetooth* dongle connected to the USB port of a laptop computer. To capture the USB traffic, the Soderia unit is placed between the dongle and laptop computer. Any traffic between the devices is captured through the Soderia HCI interface.

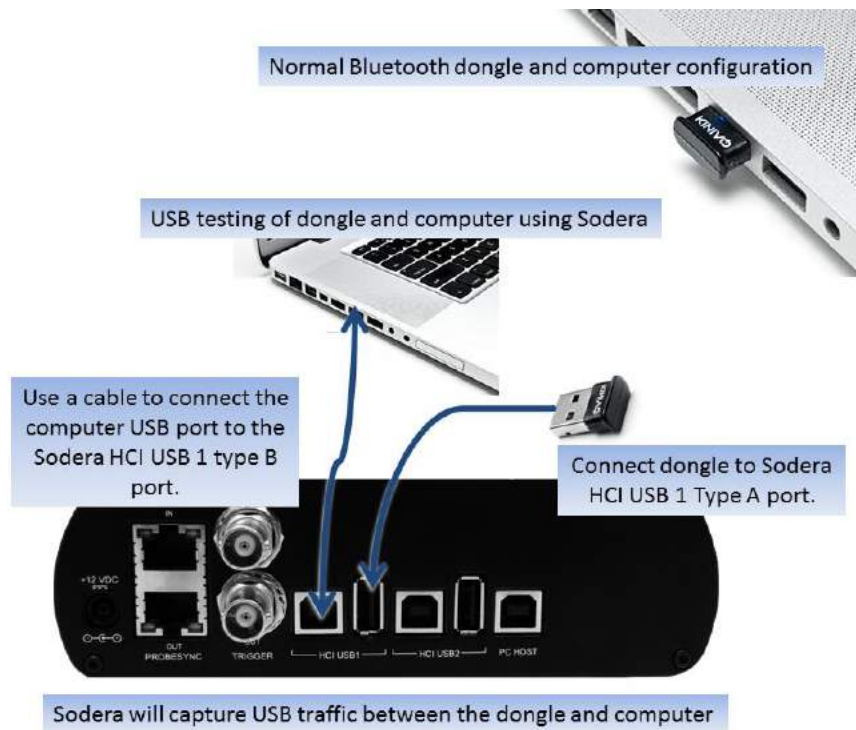


Figure 2.34 - Example: Sodera HCI USB Capture Setup

The HCI USB 1 connectors use the same Sodera unit internal interface as the Sodera HCI POD1 UART pins. Likewise the HCI USB 2 connectors use the same internal interface as the Sodera HCI POD2 UART pins. Therefore you cannot simultaneously capture USB and UART on the "1" interface or on the "2" interface. You can simultaneously capture from the HCI USB 1 connectors and the HCI POD2 UART pins and vice versa. Refer to [3.1.2.1.1 Analyzer Toolbar Menu and Icons on page 81](#).

## 2.4 Sodera LE Hardware

### 2.4.1 Sodera LE Front Panel

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



Figure 2.35 - Sodera LE Front Panel Controls and Indicators

Table 2.17 - Sodera LE Front Panel Controls

Control	Description
<b>ANTENNA</b>	Connect to the front panel antenna SMA connector. Used for wideband wireless capture of <i>Bluetooth</i> Low Energy transmissions.  Maximum useable signal level: -10 dBm.
<b>WIRED</b>	Low sensitivity RF input suitable for conductive testing that utilizes a wired connection from the devices under test (DUTs). Conductive testing allows for isolation of the DUTs from environmental interference.  Maximum useable signal level: 27 dBm.
<b>OVERLOAD</b>	RF overload indicator. If the RF signal level on either the ANTENNA or WIRED connector is too high, then this LED will light red. RF overload occurs when the signal level is greater than 27 dBm. Should an RF overload occur with the ANTENNA in use, try switching to the less sensitive WIRED connector to relieve the problem.
<b>POWER</b>	LED illuminates when the Sodera LE unit has been powered up using the power button. See <a href="#">Table 2.18 - Sodera LE Front Panel Power and Overload Indicators on page 58</a> for more information.
<b>EXT CLOCK</b>	Not used.
<b>Power Button</b>	Press and then release the button to power on or power off the system.

Table 2.18 - Soder LE Front Panel Power and Overload Indicators

Indicator	Color	State	Status Indicated
Power	None	Off	Unit is powered off.
	Green	Constant	Unit is powered on.
	Amber	Constant	Unit is powering on.
	Red	Blinking	Unit has reached thermal overload. See <a href="#">Applying Power on page 59</a> .
		Constant	Unit has reach thermal overload and has shut down. See <a href="#">Applying Power on page 59</a> .
Overload	Red	Occassional	Illuminates each time RF power at the Antenna or Wired connectors has exceeded 27 dBm.

### 2.4.2 Soder LE Rear Panel Connectors

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

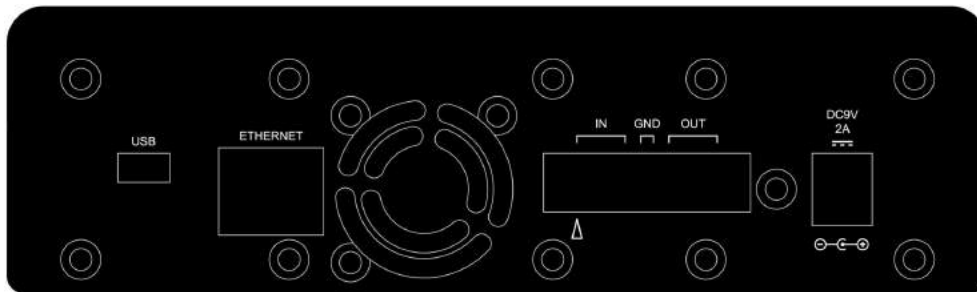


Figure 2.36 - Soder LE Rear Panel Connectors

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

**USB :** USB 2.0 port for connecting the Soder LE unit to the host computer where the Wireless Protocol Suite software resides. This connector provides host computer command, control, and data transfer.

**Note:** All other connectors are not used.

### 2.4.3 Attach Antenna



Figure 2.37 - Antenna Attachment Point

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

### 2.4.4 Applying Power

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

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

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

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

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

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





Figure 2.38 - Sodera LE Rear Panel Airflow

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

## 2.5 802.11 Hardware

### 2.5.1 Attaching Antennas

When you remove the Frontline 802.11 from the box, the first step is to attach the antennas (Figure 2.39).



Figure 2.39 - Front Panel

1. Attach an antenna to each front panel connector.





Figure 2.40 - Frontline 802.11 with all antennas attached

## 2.5.2 Connecting/Powering the Frontline 802.11

Once you have attached the antennas, the next step is to power up and connect the Frontline 802.11 to the computer.

1. Insert the power cable (DC connector) from the 12 volt AC adapter into the **Power** port on the Frontline 802.11 back panel (Figure 2.41).



Figure 2.41 - Back Panel - Power

2. Plug the 12 volt AC adapter into the AC power source. The front panel **Power** light illuminate (Figure 2.39).
3. Insert the USB cable into the **USB** port on the Frontline 802.11 back panel (Figure 2.42).



Figure 2.42 - Back Panel - USB

4. Insert the other end of the USB cable into the PC.
5. It may take as long as thirty seconds for Windows to recognize that the Frontline 802.11 hardware is connected to the PC. The **Activity** light on the Frontline 802.11 front panel (Figure 2.39) will blink during this period, when the light is steady, the Frontline 802.11 hardware is ready to communicate with the Wireless Protocol Suite software.

### 2.5.3 Setting Up for ProbeSync

The Frontline 802.11 hardware has ProbeSync™ which allows for synchronization of Frontline hardware clocks and timestamping. One Frontline device will act as the central device by providing the clock to the central device receiving the clock. Do not confuse "central" and "central" with the *Bluetooth* device central and central relationships. Refer to the following tables.

Table 2.19 - 802.11<sub>1</sub> Synced to 802.11<sub>2</sub>

802.11 <sub>1</sub>	802.11 <sub>2</sub>	802.11 <sub>1</sub>		802.11 <sub>2</sub>	
		OUT	IN	OUT	IN
Central	Peripheral	X			X
Peripheral	Central		X	X	

Table 2.20 - Sodera Synced to 802.11

Sodera	802.11	Sodera		802.11	
		OUT	IN	OUT	IN
Central	Peripheral	X			X

**Note:** The Frontline Sodera device must always be the central node in ProbeSync mode.

ProbeSync allows a Frontline Sodera and a 802.11 hardware to be connected together to run off of a common clock, ensuring precise timestamp synchronization while capturing multiple wireless technologies such as *Bluetooth* and 802.11. One device will act as the *central* device by providing the clock to the *central* device receiving the clock. The devices are connected in a daisy-chain configuration. Refer to the following table, to [Rear Panel Connectors on page 42](#), and to [Connecting/Powering the Frontline 802.11 on page 61](#).

Table 2.21 - Sodera Synced to 802.11

Sodera	802.11	Sodera		802.11	
		PROBESYNC OUT	PROBESYNC IN	OUT	IN
Central	Peripheral	X			X

1. Using a CAT 5 Ethernet cable (less than 1.5 meters (4.9 feet)) insert one end to the central Frontline Sodera device OUT jack.
2. Insert the other end of the cable into the central Frontline 802.11 device IN jack.



Figure 2.43 - Back Panel - ProbeSync with Sodera and 802.11

## 2.6 Data Capture Methods

This section describes how to load Teledyne LeCroy Wireless Protocol Suite software, and how to select the data capture method for your specific application.

### 2.6.1 Opening Wireless Protocol Suite

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

1. Double-click the "**Wireless Protocol Suite <version #>**" desktop folder.

This opens a standard Windows file folder window.

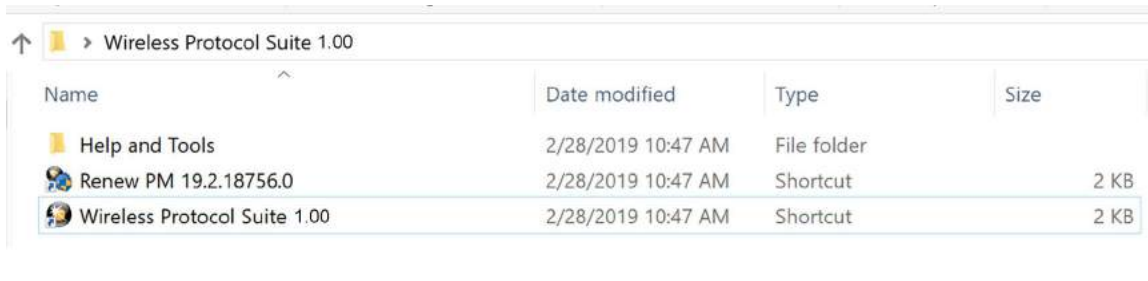


Figure 2.44 - Desktop Folder Link

2. Double-click on **Wireless Protocol Suite** Icon and the system displays the **Start Page** dialog.

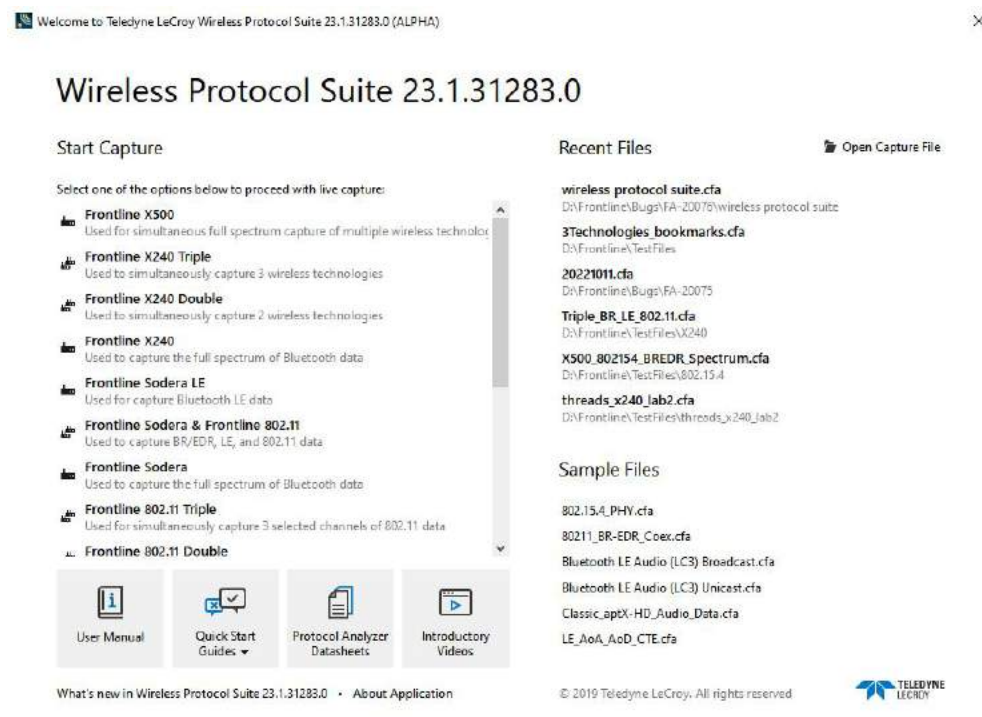


Figure 2.45 - Example: Wireless Protocol Suite Start Page

**Note:** You can also access this dialog by selecting Start > All Programs > Teledyne LeCroy Wireless > Wireless Protocol Suite<version #>

Select the Sodera and the Main Application Window will be displayed.

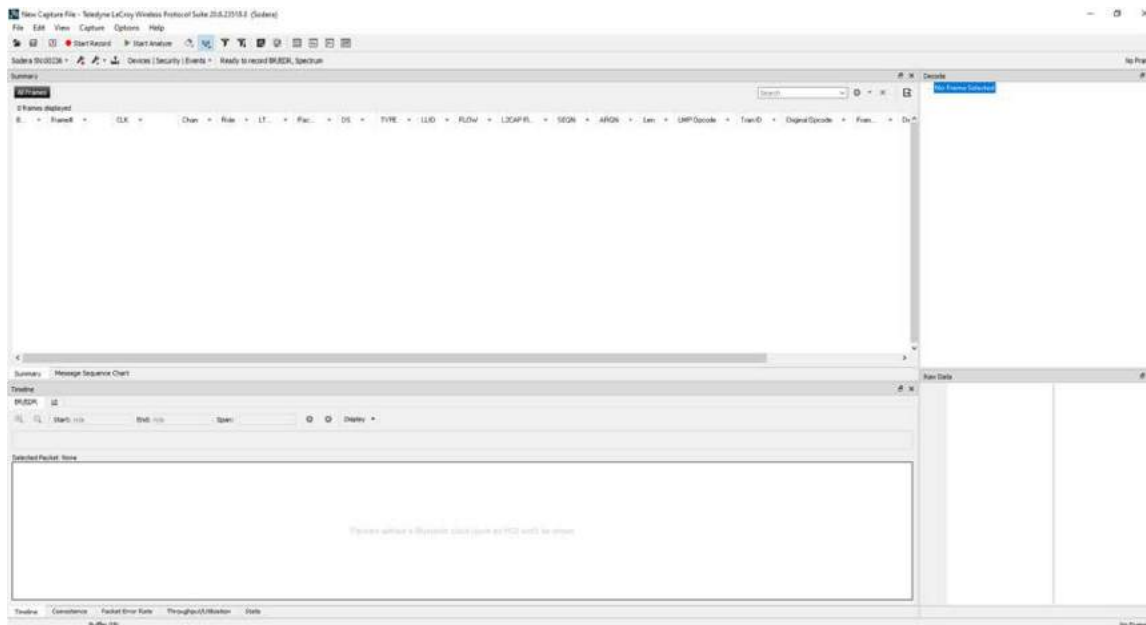


Figure 2.46 - Main Application Window with Capture Screen

## Supporting Documentation

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

### 2.6.2 X240 Data Capture Method

**X240** can be set up for a single technology capture or with two **X240** units for synchronized capture of multiple technologies.

#### 2.6.2.1 Single Technology Capture, Single X240 (1)

Connect a USB C cable to the USB connector labeled **Host** on the rear of the **X240** and the other end of the cable to the Host PC. When the **X240** Analyzer is connected to the Host PC running the **Wireless Protocol Suite** the **Start Page** window will display the **X240** option.

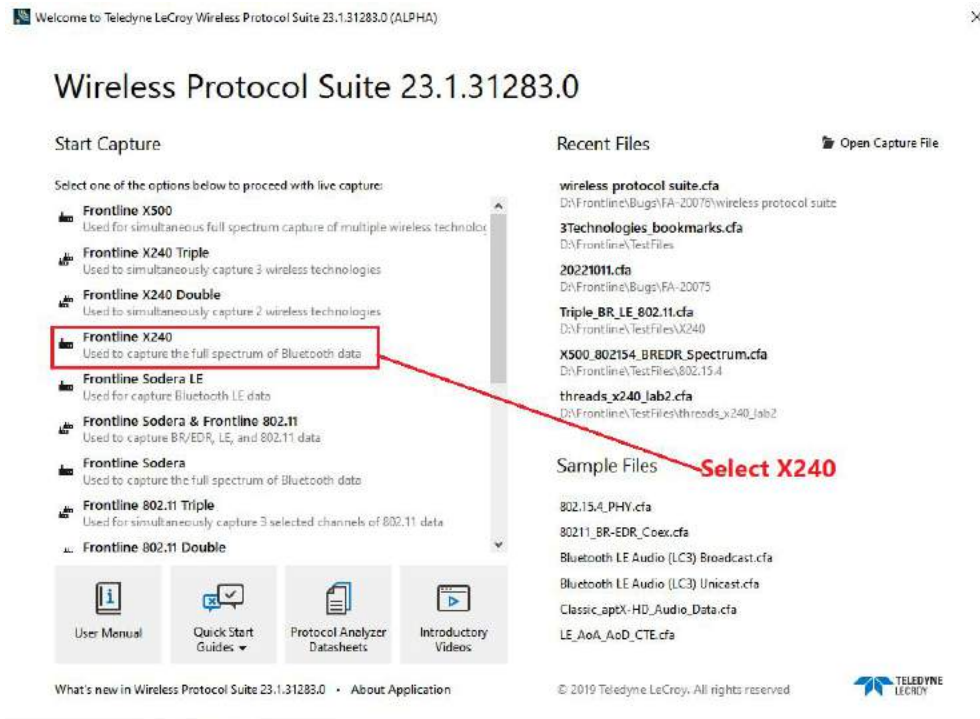


Figure 2.47 - Start Page Single Technology Capture

Select **X240** to bring up the **X240** Main Window. When the Main Window is displayed, you will see Toolbars with the following functions:

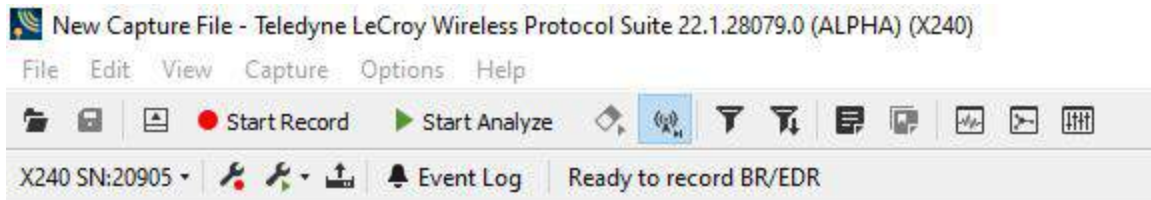


Figure 2.48 - X240 Toolbars

To begin recording *Bluetooth* traffic, click on the **Start Record** button. Addresses of captured *Bluetooth* devices will appear on the **Device Database** View. The view is accessible via **Main menu** View.

### 2.6.2.2 Synchronized X240 (2) Data Capture Method

On both **X240** Analyzer units, connect a USB C cable to the USB connector labeled Host on the back of the **X240** and the other end of the cable to the Host PC. Connect the CATC Sync cable to the MicroD25 port on the back of each **X240**. See [Setting Up for Synchronized X240 \(2\) Capture on page 37](#) .

When the **X240** Analyzers are connected to the Host PC running the **Wireless Protocol Suite** the **Start Page** window will display the **Synchronized X240 (2)** option.



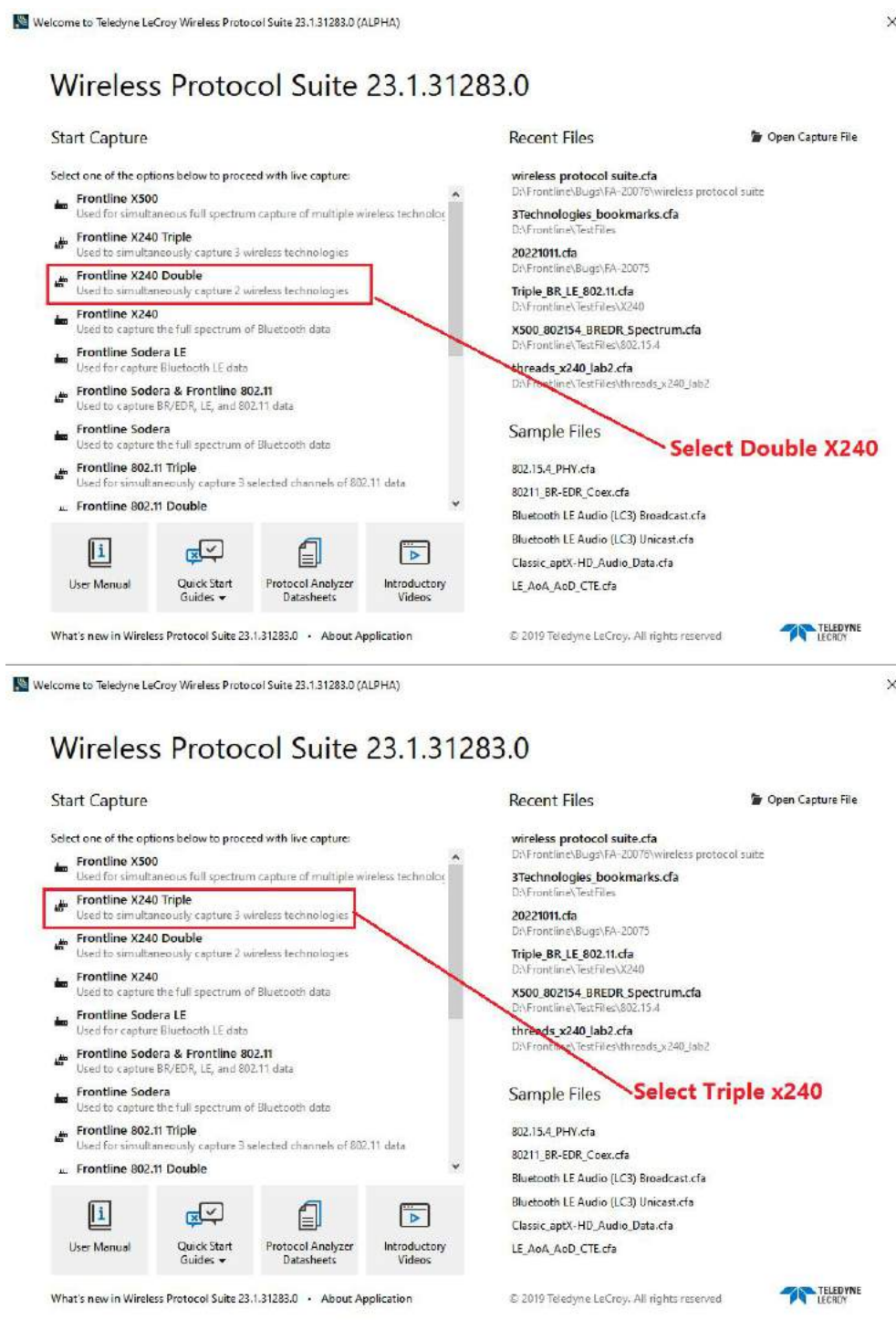


Figure 2.49 - Wireless Protocol Suite: Start Page

Select **Synchronized X240 (2)** to start the **Wireless Protocol Suite** using both **X240** Analyzer units.

Each **X240** will be represented by an Analyzer Toolbar in the **Wireless Protocol Suite** from which it can be configured

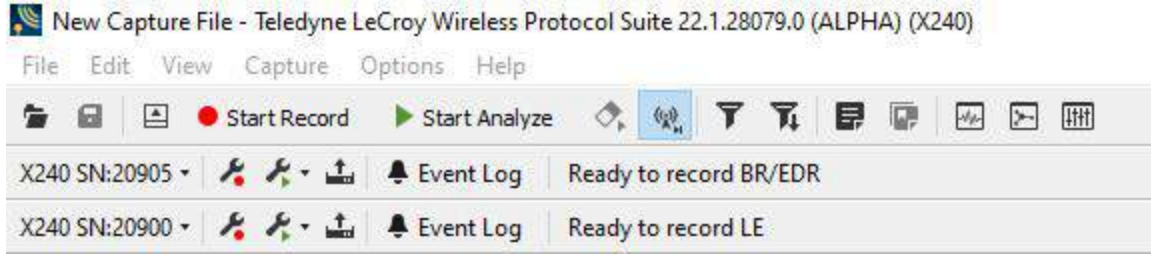


Figure 2.50 - New Capture File

When using **Synchronized X240 (2)**, each **X240** should be configured to conform to the following rules of synchronized capture.

Table 2.22 - **Synchronized X240 (2)** Capture Configuration Rules

Synchronized X240 (2) Capture Configuration Rules
No X240 can have Excursion Mode enabled.
Only one X240 can have Logic Signals and HCI enabled.
Only one X240 can have Spectrum enabled.
Only one X240 can have Low Energy (LE) Bluetooth enabled.
Only one X240 can have Classic (BR/EDR) Bluetooth enabled.
Only one X240 can have Dual mode (BR/EDR and LE) Bluetooth enabled.
Only one X240 can have Wi-Fi enabled.
Only one X240 can have 802.15.4 enabled.

To begin recording Bluetooth traffic, click on the **Start Record** button in the **Wireless Protocol Suite**.

If any rule of synchronized capture is not followed in the capture configuration of the **X240** Analyzer units, an error message is displayed detailing each rule that is not followed. The capture configuration of the **X240** Analyzer units must be changed to conform to the synchronization rules. The **Start Record** button in the **Wireless Protocol Suite** must be clicked again to begin recording.

If the Event Log of either X240 indicates that the synchronization cable is not properly connected, refer to **Troubleshooting** in [Setting Up for Synchronized X240 \(2\) Capture on page 37](#)

**Synchronized X240 (2) Capture Modes**

The X240 can be configured for either LE or BR/EDR or Dual mode or Wi-Fi or 802.15.4. This offers the opportunity to capture with two X240s in these configurations or modes:

- LE and BR/EDR
- LE and Wi-Fi
- LE and 802.15.4
- BR/EDR and Wi-Fi
- BR/EDR and 802.15.4



- Dual mode (BR/EDR and LE) and Wi-Fi
- Dual mode (BR/EDR and LE) and 802.15.4
- Wi-Fi and 802.15.4

Spectrum capture can be enabled on any one X240 in the each of the above modes.

### 2.6.2.3 Synchronized X240 (3) Data Capture Method

Connect three **X240** units using three CATC Sync Cable kits as described in [Setting Up for Synchronized X240 \(3\) Capture on page 38](#)

When the **X240** Analyzers are connected to the Host PC running the **Wireless Protocol Suite**, the **Start Page** window will display the Synchronized X240 (3) option.

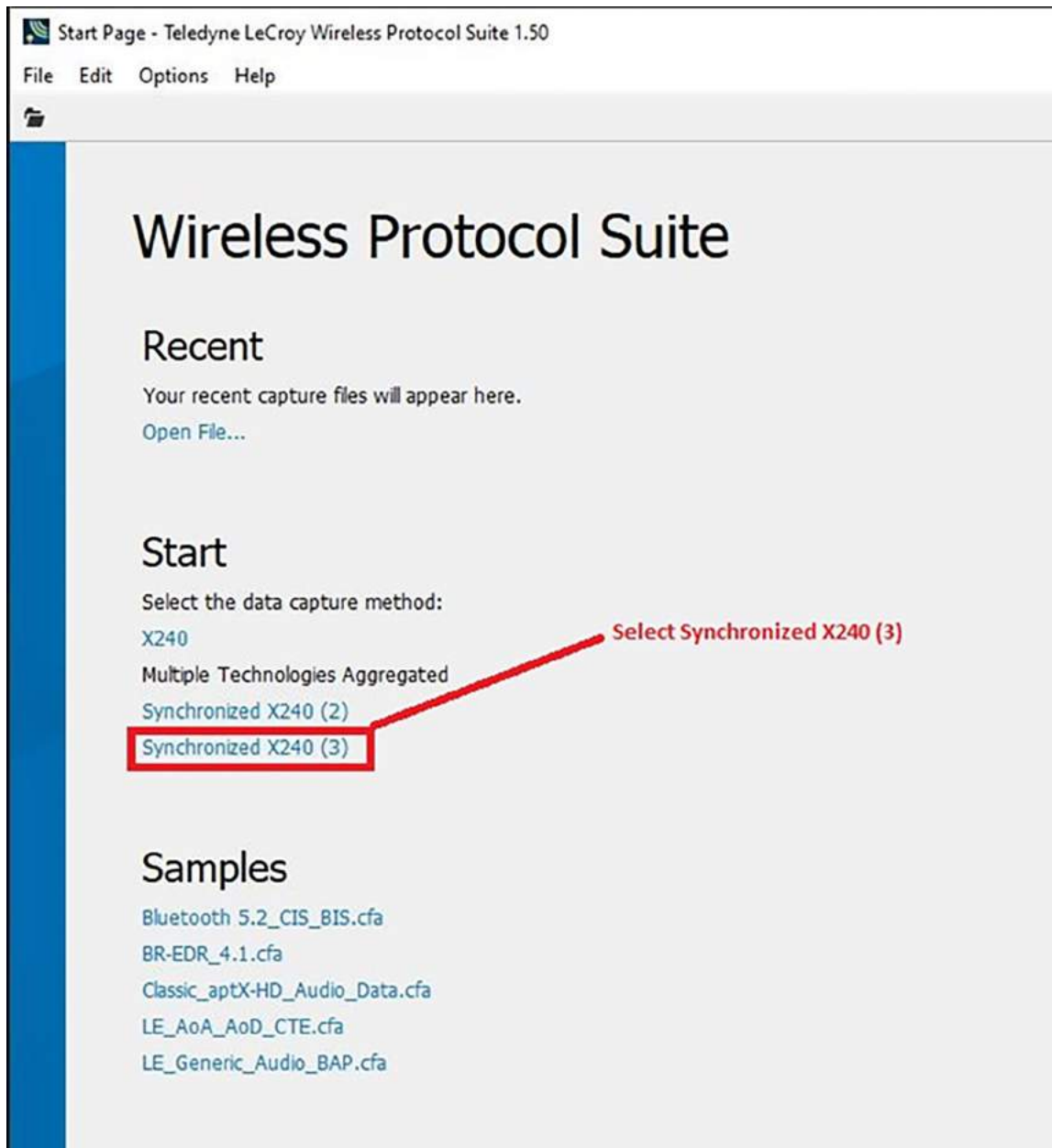


Figure 2.51 - Wireless Protocol Suite: Start Page

Select **Synchronized X240 (3)** to start the **Wireless Protocol Suite** using three **X240** Analyzer units.

Each **X240** will be represented by an Analyzer Toolbar in the **Wireless Protocol Suite** from which it can be configured.

When using Synchronized X240 (3), each X240 should be configured to conform to the following rules of synchronized capture.

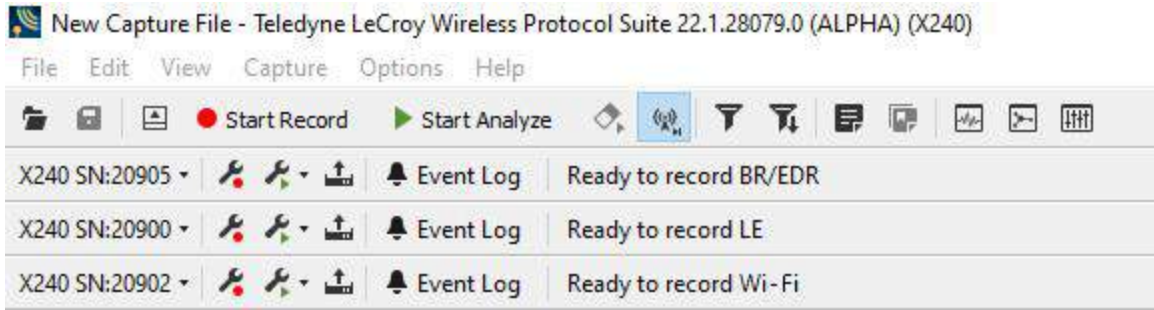


Figure 2.52 - Synchronized X240 Toolbars

Table 2.23 - **Synchronized X240 (3) Capture Configuration Rules**

Synchronized X240 (3) Capture Configuration Rules
No X240 can have Excursion Mode enabled.
Only one X240 can have Logic Signals and HCI enabled.
Only one X240 can have Spectrum enabled.
Only one X240 can have Low Energy (LE) Bluetooth enabled.
Only one X240 can have Classic (BR/EDR) Bluetooth enabled.
Only one X240 can have Dual mode (BR/EDR and LE) Bluetooth enabled.
Only one X240 can have Wi-Fi enabled.
Only one X240 can have 802.15.4 enabled.

To begin recording Bluetooth traffic, click on the **Start Record** button in the **Wireless Protocol Suite**.

If any rule of synchronized capture is not followed in the capture configuration of the **X240** Analyzer units, an error message is displayed detailing each rule that is not followed. The capture configuration of the **X240** Analyzer units must be changed to conform to the synchronization rules. The **Start Record** button in the **Wireless Protocol Suite** must be clicked again to begin recording.

If any **X240** indicates, in its Event Log window, that the synchronization cable is not properly connected, refer to **Troubleshooting** in [Setting Up for Synchronized X240 \(3\) Capture on page 38](#)

### 2.6.3 Sodera Data Capture Method

When the **Sodera Analyzer** is connected to the Host PC running the **Wireless Protocol Suite** the **Start Page** window will display the **Sodera** option.

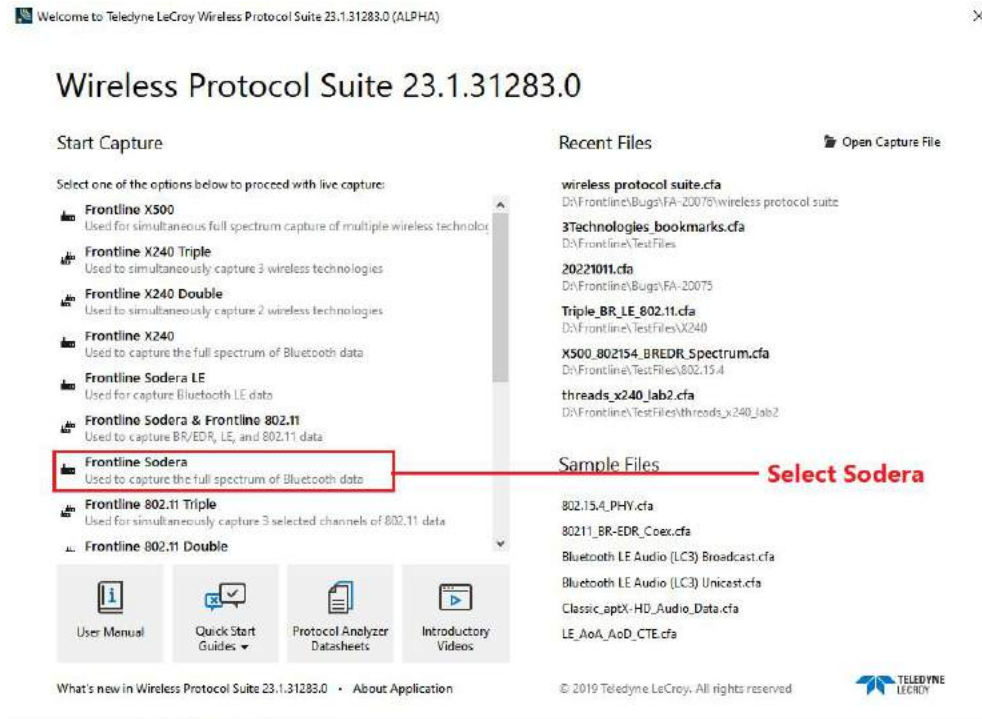


Figure 2.53 - Wireless Protocol Suite: Start Page

Select **Sodera** to bring up the **Wireless Protocol Suite** window. The Wireless Protocol Suite Application icon will be placed in your taskbar at the bottom of your screen.



Wireless Protocol Suite Application Icon

### 2.6.4 Sodera LE Data Capture Method

When the **Sodera LE Analyzer** is connected to the Host PC running the **Wireless Protocol Suite** the **Start Page** window will display the **Sodera LE** option.

Select Sodera LE to bring up the Wireless Protocol Suite window. When the Main Application Window is Displayed, you will see toolbars with the following functions:

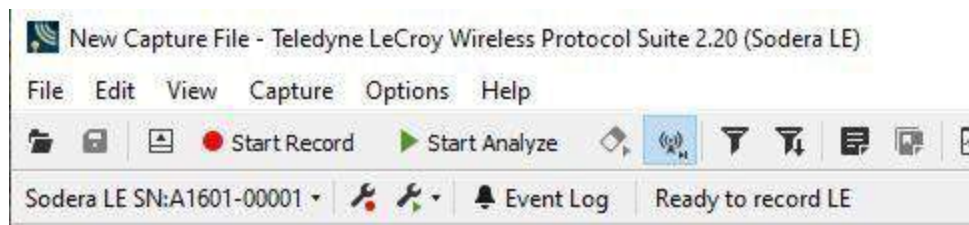


Figure 2.54 - Sodera LE Toolbars

To begin recording Bluetooth traffic, click on the **Start Record** button. Addresses of captured *Bluetooth* devices will appear on the **Device Database** View. The Device Database is available from menu in the toolbar.

Select **Sodera LE** to bring up the **Wireless Protocol Suite** window. The **Sodera Main window** icon will be placed in your taskbar at the bottom of your screen.



Wireless Protocol Suite Application Icon

## 2.6.5 Frontline® 802.11 Data Capture Method

When the **802.11 Analyzer** is connected to the Host PC running the **Wireless Protocol Suite** the **Start Page** will display the **802.11** option.

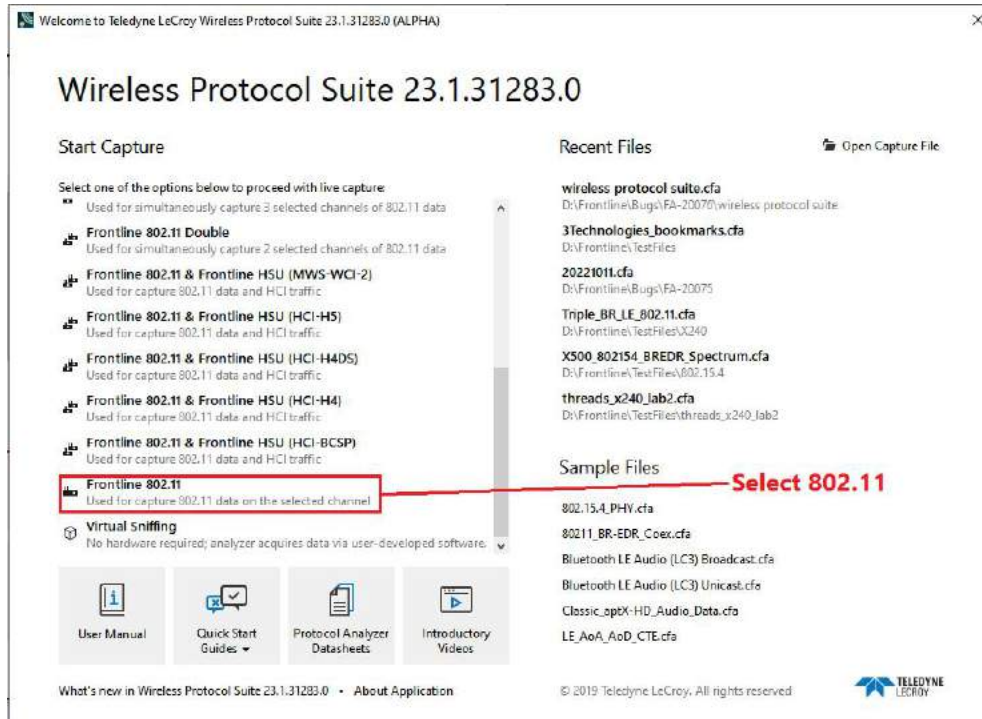


Figure 2.55 - Wireless Protocol Suite: Start Page

Click on **802.11**.

The **Teledyne LeCroy Wireless Protocol Suite** software will display the **802.11 Main window**. From this window you can choose the **Start Record** button.

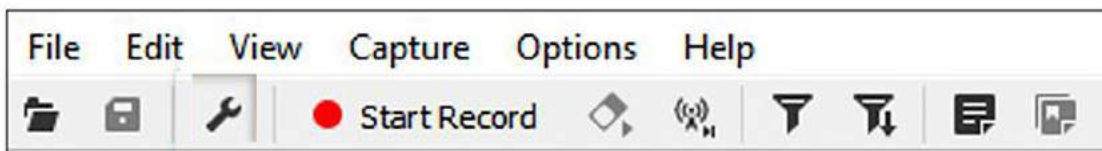


Figure 2.56 - 802.11 Start Record button

- 802.11
  - Requires one Frontline 802.11 hardware.
  - Captures 802.11 data on the selected channel.

- 802.11 Double
  - Requires two Frontline 802.11 hardware with **ProbeSync™**.

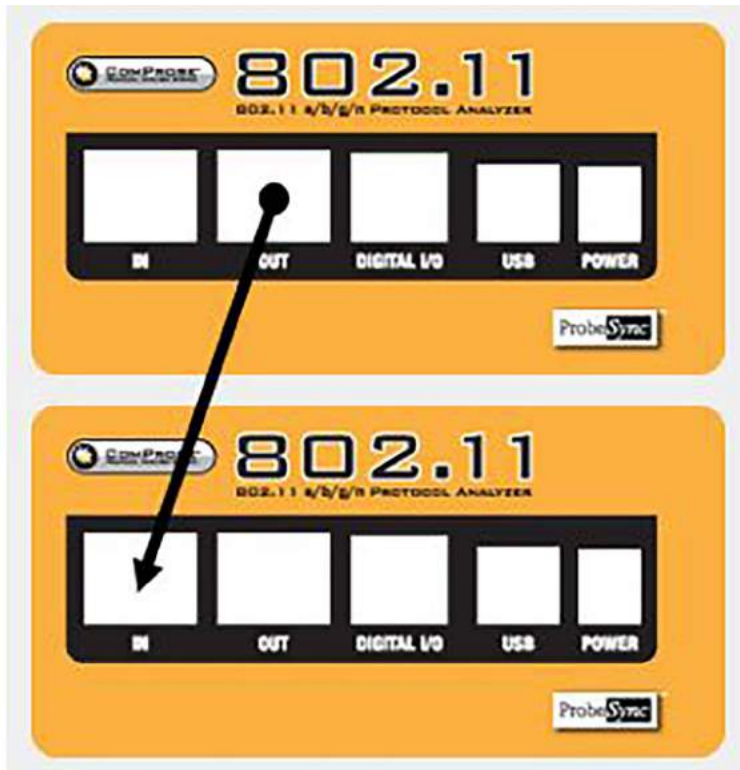


Figure 2.57 - 802.11 Double

- 802.11 Triple
  - Requires three Frontline 802.11 hardware with **ProbeSync™**.

To begin recording **802.11** traffic, click on the **Start Record** button. 802.11 traffic will be shown in the Summary Window.



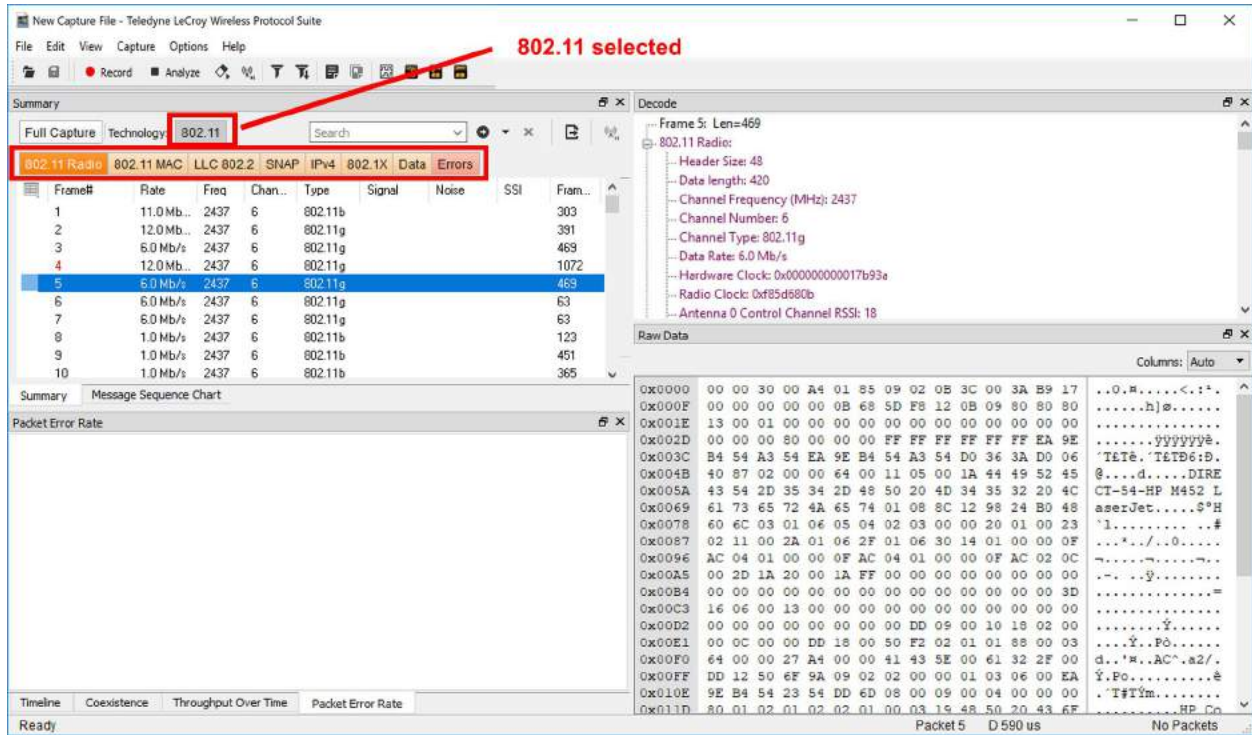


Figure 2.58 - 802.11 Capture / Analysis Windows



## 2.6.6 Using Sample Capture Files

There are several sample capture files in the Wireless Protocol Suite installation.

Each file has a self descriptive name regarding used device and traffic type. You can open these files using the Samples section in the Start Page.

### Caution:

Wireless Protocol Suite software treats sample files in the same way as other user recorded capture files, i.e. it preserves all your changes in the original sample file: you may make a copy of the desired file and save it before any experiment that may corrupt it.

By default sample files stored in the Public Documents folder more precise path you can find out from path hint:

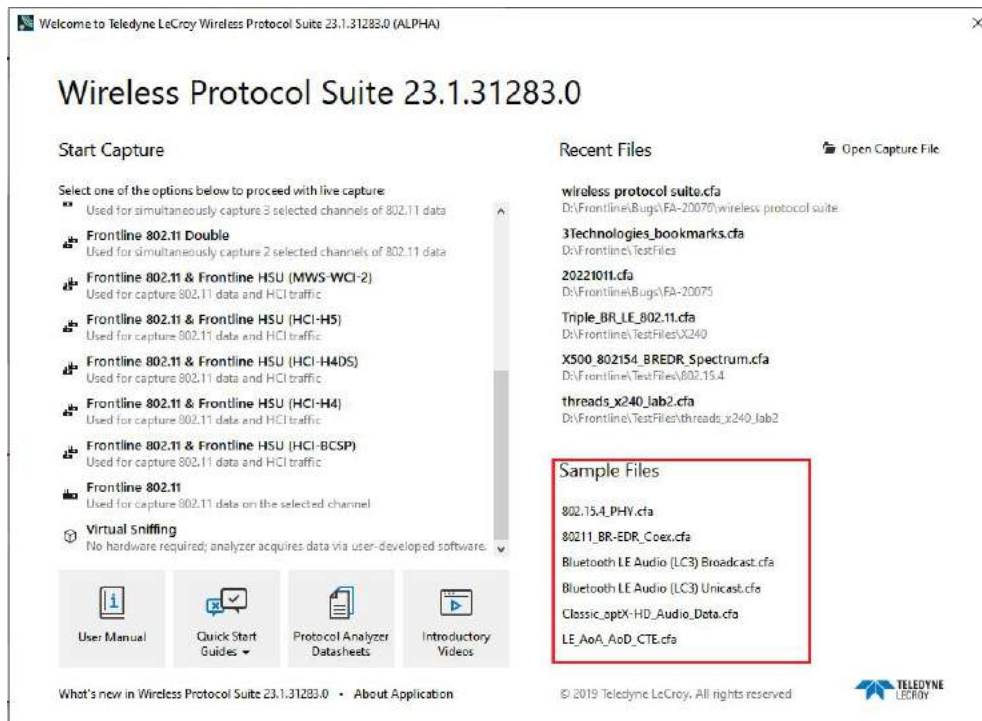


Figure 2.59 - Start Page -> Sample Files

Click on the file name and the main application window of the Wireless Protocol Suite software will open with the Captured File loaded.

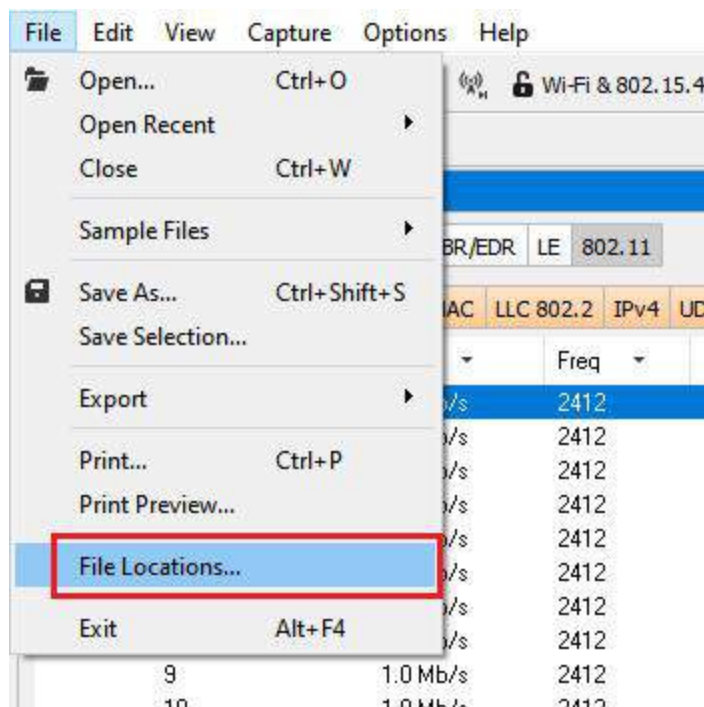


Figure 2.60 - File Location Options

You can also discover the path to "My Captured Files " by selecting **File -> File Locations** from the Main Page.

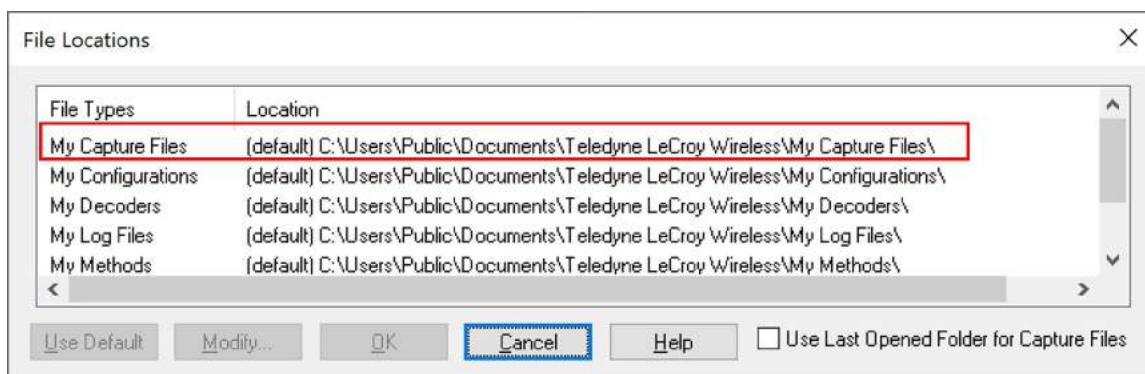


Figure 2.61 - File Locations

## 2.7 NewTopic

## Chapter 3 Configuration Settings

In this section the Wireless Protocol Suite software is used to configure an analyzer for capturing data.

### 3.1 Configuration and I/O for Bluetooth Data Capture

#### 3.1.1 User Configuration Overview

The Frontline Bluetooth Protocol Analyzer is capable of simultaneously capturing and demodulating RF channels and packet types defined in Bluetooth Specifications up to and including 5.1. The user is not required to specify the addresses of the devices to be captured or their roles (central or peripheral) during the connection lifetime. Prior to capturing data the user does not need to enter any information (PIN, OOB, long term key, link key) used to encrypt or decrypt data. The Analyzer provides live simultaneous capture of all 79 Classic Bluetooth channels and 40 Bluetooth low energy channels storing data for both live and post capture analysis.

The Analyzer uses a two-stage capture-analysis process. First, **Record** will activate the analyzer to begin capturing data from all Bluetooth devices in range. In the Analyze stage, the user selects one or more wireless or wired devices for analysis and the analyzer will begin sending captured data that is to/from those devices to the Wireless Protocol Suite software. The data appears in various views:

**Summary Pane, Message Sequence Chart, Coexistence View, Bluetooth Timeline, Low Energy Bluetooth Timeline, PER Stats, etc.**

If any keys needed for decryption are known from past captures those keys are automatically applied to the devices under test. Prior to protocol analysis the user can enter any unknown keys. The analyzer will identify the specific key necessary for data decryption, for example Link Key, Passkey, PIN, Temporary Key. Decryption keys are entered into the **Security** pane. The Security pane is available from the View menu.

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
4/19/2021 2:28:57.589...	xxxxxxxx:93:76:76:FC	N/A	Missing Peripheral Address		N/A
4/19/2021 2:29:02.260...	Enter Peripheral Address				
4/19/2021 2:29:25.268...	"Echo-BH0" 74:C2:46:0E:41:F4	N/A	0x6238236F3988FDD40DD05E732A3A9...	0x9C5D:C900...	N/A
4/19/2021 2:29:25.367...	08:AE:D6:57:9B:10				
4/19/2021 2:29:25.367...	"Echo-BH0" 74:C2:46:0E:41:F4	N/A	0x6238236F3988FDD40DD05E732A3A9...	0xC285:3956...	N/A
4/19/2021 2:30:11.890...	08:AE:D6:57:9B:10				
4/19/2021 2:30:12.062...	08:AE:D6:57:9B:10	N/A	0x6238236F3988FDD40DD05E732A3A9...	0xC285:3956...	N/A
4/19/2021 2:39:18.962...	"Echo-BH0" 74:C2:46:0E:41:F4				
4/19/2021 2:30:20.900...	28:A0:2B:D9:46:0C	N/A	Unable to validate		N/A
4/19/2021 2:40:06.261...	F0:5C:D5:A8:C5:65				
4/19/2021 2:30:26.345...	F0:5C:D5:A8:C5:65	N/A	Unable to validate		N/A
4/19/2021 2:39:57.934...	F0:5C:D5:A8:C5:65				
4/19/2021 2:39:31.165...	08:AE:D6:57:9B:10	N/A	0x6238236F3988FDD40DD05E732A3A9...	0x3F96:4238:E...	N/A
4/19/2021 2:39:31.917...	"Echo-BH0" 74:C2:46:0E:41:F4				
4/19/2021 2:39:31.917...	08:AE:D6:57:9B:10	N/A	0x6238236F3988FDD40DD05E732A3A9...	0x0E3A:4F12...	N/A

Figure 3.1 - Security Pane

The user can configure the record options from the Analyzer Toolbar. The default settings are sufficient for capturing most Bluetooth connections. Details of the configuration settings are in the Wireless Protocol Suite Hardware and Software User Manual available to download from [FTE.com](http://FTE.com) or in Frontline on-line help.

### 3.1.1.1 Standard Capture Scenario

In the standard capture scenario, the analyzer is connected to a host computer via the rear panel **PC HOST** interface and captures live “over the air” data exchanged between two *Bluetooth* devices.

### 3.1.2 Wireless Protocol Suite Analyzer Toolbars

When the Wireless Protocol Suite software is loaded and started on the host computer the Wireless Protocol Suite Main Windows with Analyzer toolbar(s) will open. It allows users to control and view the status of a connected X240 / X500 /Sodera / Sodera LE hardware from within the main application window of the Wireless Protocol Suite.

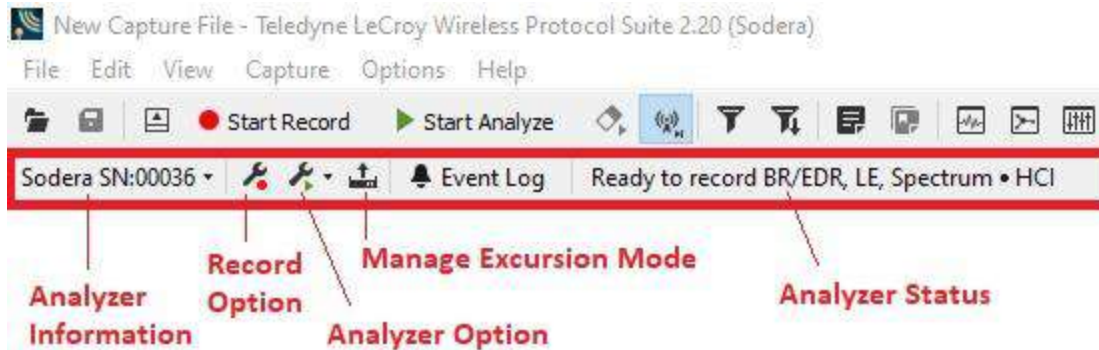


Figure 3.2 - Wireless Protocol Suite Analyzer Toolbar

From within the Wireless Protocol Suite application, the user now has the same options and capabilities previously provided via the separate Datasource application window. These include the following:

- Display of X240 / X500 /Sodera / Sodera LE product information
- Display of current status of X240 / X500 /Sodera / Sodera LE
- Ability to configure Record options
- Ability to configure Analyze options (including selecting which devices to analyze)
- Display of Wireless devices captured (current and previously captured)
- Display of Wired devices configured/captured
- Display of captured Security Events
- Ability to configure Bluetooth Privacy Keys
- Ability to configure Private Keys
- Display of Datasource event messages
- Ability to apply feature licenses
- Ability to manage excursion mode captures

In addition, as a result of removing the Datasource application window, the user is now only presented with a single button for Start Record and for Start Analyze (the current buttons in the Wireless Protocol Suite).

The Analyzer toolbars are presented for each connected Datasource. E.g., for the Synchronized X240 mode two analyzer toolbars will be displayed:

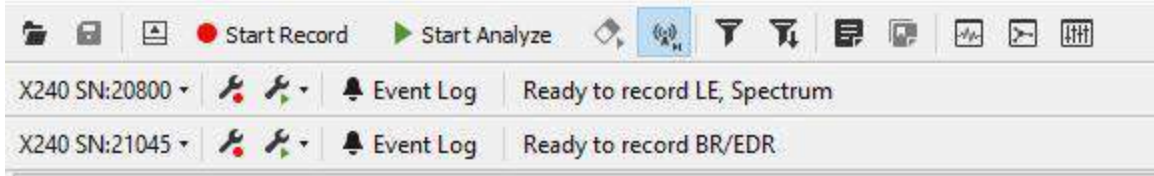


Figure 3.3 - Wireless Protocol Suite with Two Analyzer Toolbars

The Analyzer toolbars are presented in live mode and when a capture file is opened. A Datasource file (.scap) is required to display the toolbars. When opening a capture file without corresponding Datasource file, the Wireless Protocol Suite will not display Analyzer toolbars.

When opening a capture file, the **Record Options**, **Excursion Mode Captures** menus, and the Analyzer **Status** indicator will not be displayed.

### 3.1.2.1 Menu & Toolbars

Access to the various capture and analysis functions and displays is through the various menus and toolbars in the Wireless Protocol Suite software.

#### 3.1.2.1.1 Analyzer Toolbar Menu and Icons

The Analyzer toolbar menu is fixed in position and always in view. When selected, the **Analyzer Information** and **Analyzer Options** form pull-down menus with options for each topic. The Analyzer Toolbar icons and pull-down menu items are described in the table below.

Table 3.1 - Wireless Protocol Suite Analyzer Toolbar Icons and Menus

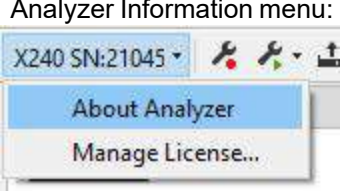

Icon/Menu	Description
	<p><b>About Analyzer</b> - Opens a popup window with version and configuration information</p> <p><b>Manage License</b> (X500 and X240 only) – Opens Manage License dialog that allows to view the details of a currently installed license file or update the license file.</p>
	<p>Opens the <b>Record Options</b> dialog where the attached hardware can be configured for <i>Bluetooth</i> technologies and other capture modes. For additional information see <a href="#">Record Options Dialog on page 87</a></p>

Table 3.1 - -Wireless Protocol Suite Analyzer Toolbar Icons and Menus (continued)

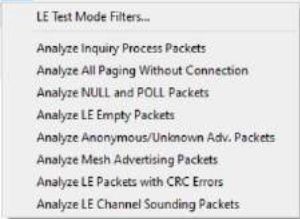

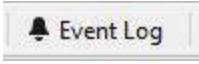
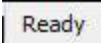
Icon/Menu	Description	
<p>Analyze Options menu</p> 	<p><b>LE Test Mode Filters...</b></p>	<p>Allows filtering in or out LE Test Mode PDUs and will allow filtering in selective LE Test Mode PDUs by channel number. For additional information see <a href="#">Record Options Dialog on page 87</a></p>
	<p><b>Analyze Inquiry Process Packets</b></p>	<p>When checked will include inquiry packets in the analysis. Inquiry packets are normally ignored, so not-checked is the default. This feature is unavailable with Sodera LE hardware.</p>
	<p><b>Analyze All Paging Without Connection</b></p>	<p>Includes traffic from all failed BR/EDR connection attempts. This feature is unavailable with Sodera LE hardware.</p>
	<p><b>Analyze NULL and POLL Packets</b></p>	<p>When checked will include NULL and POLL packets. NULL and POLL packets are normally ignored, so not-checked is the default.</p>
	<p><b>Analyze LE Empty Packets</b></p>	<p>When checked will include Bluetooth Low Energy empty packets. Empty packets are normally ignored, so not-checked is the default.</p>

Table 3.1 - Wireless Protocol Suite Analyzer Toolbar Icons and Menus (continued)

Icon/Menu	Description	
	<b>Analyze Anonymous/ Unknown Adv. Packets</b>	<p>When checked the Wireless Protocol Suite software identifies <i>Bluetooth</i> Low Energy anonymous advertising packets. An anonymous advertising packet does not contain the AdvA field and its corresponding auxiliary packet also does not contain an AdvA field. With no address, there is nothing to select for analysis in the Device Database pane. The Wireless Protocol Suite software groups anonymous packets and this option allows the user to include or exclude those packets for analyzing.</p> <p>If the Frontline system captures either the extended advertising packet or its corresponding auxiliary packet but not both and the AdvA field is not present in</p>
	<b>Analyze Mesh Advertising Packets</b>	<p>When checked, all captured Mesh Advertising packets are included in the analysis. This includes advertising packets for both Mesh Provisioning and the Mesh Proxy Service. The default setting is unchecked. Settings are persistent.</p>
	<b>Analyze LE Packets with CRC Errors</b>	<p>When checked, LE packets with CRC errors are included in analysis and a partial decode of those packets is provided.</p>



Table 3.1 - Wireless Protocol Suite Analyzer Toolbar Icons and Menus (continued)

Icon/Menu	Description	
	<b>Analyze LE Channel Sounding Packets</b>	When checked, LE Channel Sounding packets are included in analysis. Those not interested in Channel Sounding feature are recommended to disable this option to improve quality of capture.
	Record or delete captures from the Sodera hardware that were created using excursion mode. Opens the Manage excursion mode captures dialog.  This selection is disabled during live capture.	
<b>Event Log</b> button  	<b>Event Log</b>	Opens up the Event Log view.
	The Analyzer current status. The following statuses are available:  <b>Ready</b> – the Analyzer is connected and ready to record traffic.  <b>Recording</b> – the Analyzer is recording traffic.  <b>Disconnected</b> – the Analyzer was disconnected from the system.	

**Manage Excursion Mode captures dialog**

This dialog provides the user with a means to record or delete captures previously created and saved on the hardware using Excursion Mode. The Excursion Mode feature is only supported on Sodera and X240 analyzers. This option is unavailable with Sodera LE hardware.



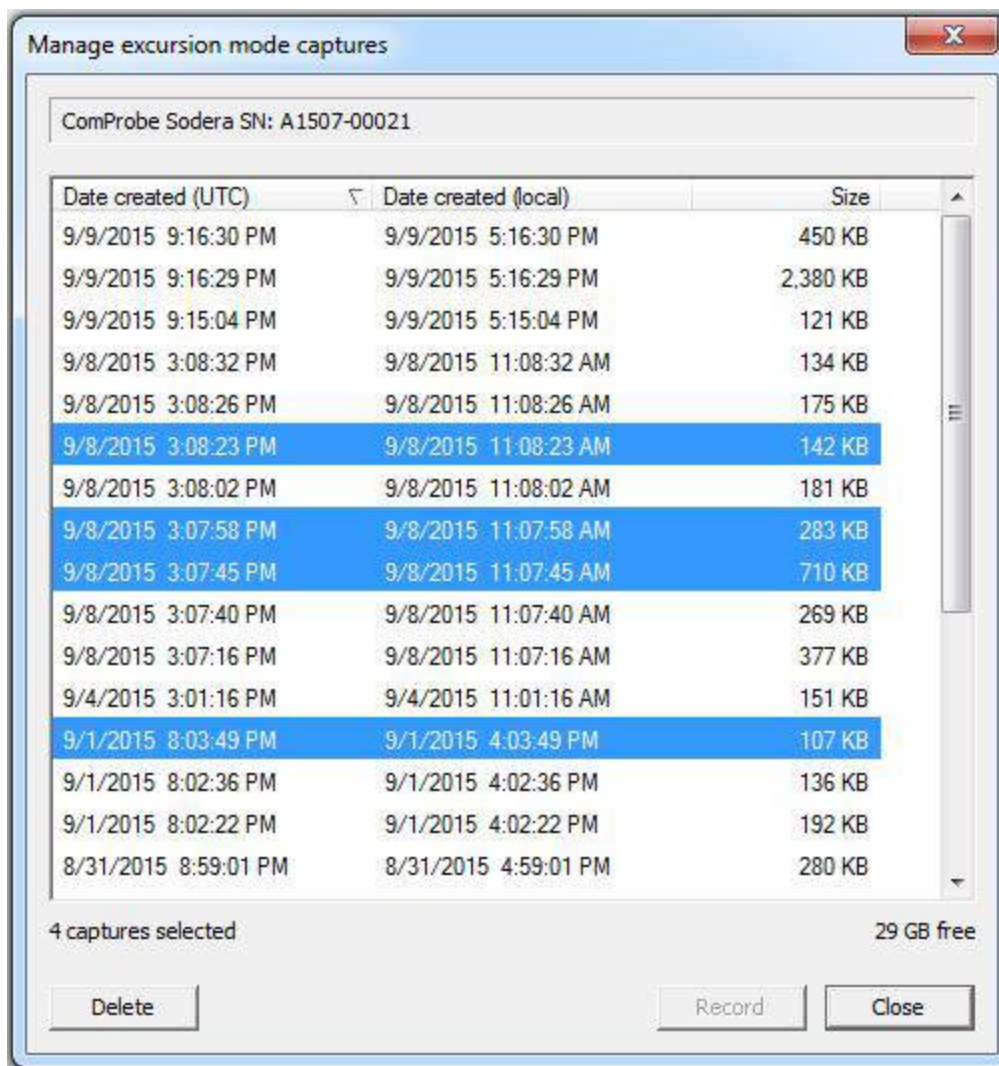


Figure 3.4 - Manage Excursion Mode Captures Dialog

If a hardware unit is connected to the computer the dialog displays

- The serial number of the hardware.
- A listing of all Excursion mode capture files stored on the currently connected Sodera hardware. If no files are stored, the list will be empty.

The listed files display the following information.

- **Date Created (UTC)** - the date and time in the UTC time zone that the excursion mode capture was started.
- **Date Created (local)** - The capture's starting date and time in the local time zone of the user's computer.
- **Size** - the size of the excursion mode capture.

Select Excursion mode capture files by

- Click to select a single file.
- Shift-click to select a contiguous range of files starting with the most recently selected file.
- Ctrl-click to select an additional file or non-contiguous file to the selection.
- Select all files by:
  - right-clicking and selecting **Select All Ctrl-A** from the context menu, or.
  - Typing Ctrl-a.

Delete selected files from the connected Soderia hardware by

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

A delete operation will display a confirming dialog that requires the user to confirm the operation before the files are actually deleted. Clicking on **Yes** will permanently delete the files from the connected Soderia hardware. Clicking on **Cancel** will abort the delete operation.

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

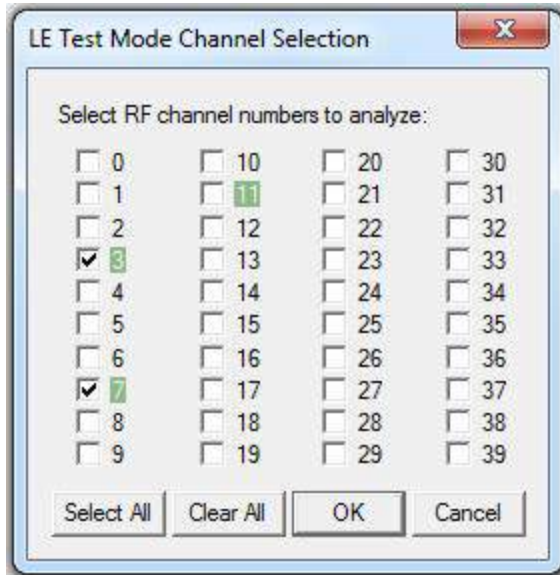
### Right-click pop-up menu

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



Figure 3.5 - Excursion Mode Pop Up Menu

### LE Test Mode Channel Selection dialog



In this image , three channels have detected LE Test Mode PDUs and the channels are highlighted: channel 3, 7, and 11. Channels 3 and 7 are checked, so their PDUs are filtered "in" for analysis. Channel 11 has not been checked, so its PDUs are filtered "out" from the analysis.

These channel filter selections are persistent for the current session. Another **Record** action in this same session can be performed and the same channel filter selection will be applied unless changed.

Table 3.2 - LE Test Mode Channel Selection Buttons

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

#### 3.1.2.1.1.1 Record Options Dialog

The Record Options dialog is used to configure the unit prior to data capture. The record options are stored on the hardware and these setting will persist until changed. The Record Options dialog is only active when a unit is connected to the computer running the Wireless Protocol Suite software.

**Note:** If a hardware unit is not connected then these settings can neither be viewed nor changed.

##### 3.1.2.1.1.1.1 Record Options Dialog: X500

The Record Options dialog is used to configure the X500 unit prior to data capture. The record options are stored on the X500 hardware and these setting will persist until changed. The Record Options dialog is only active when a X500 unit is connected to the computer running the Wireless Protocol Suite software.

**Note:** If a X500 hardware unit is not connected then these settings can neither be viewed nor changed.

Clicking on **OK** will save the **Record Options** settings on the connected X500 unit. Any **Record Options** parameter changes made will overwrite the previously saved **Record Options**.

### Wireless Tab

The X500 Wireless tab is scrollable.

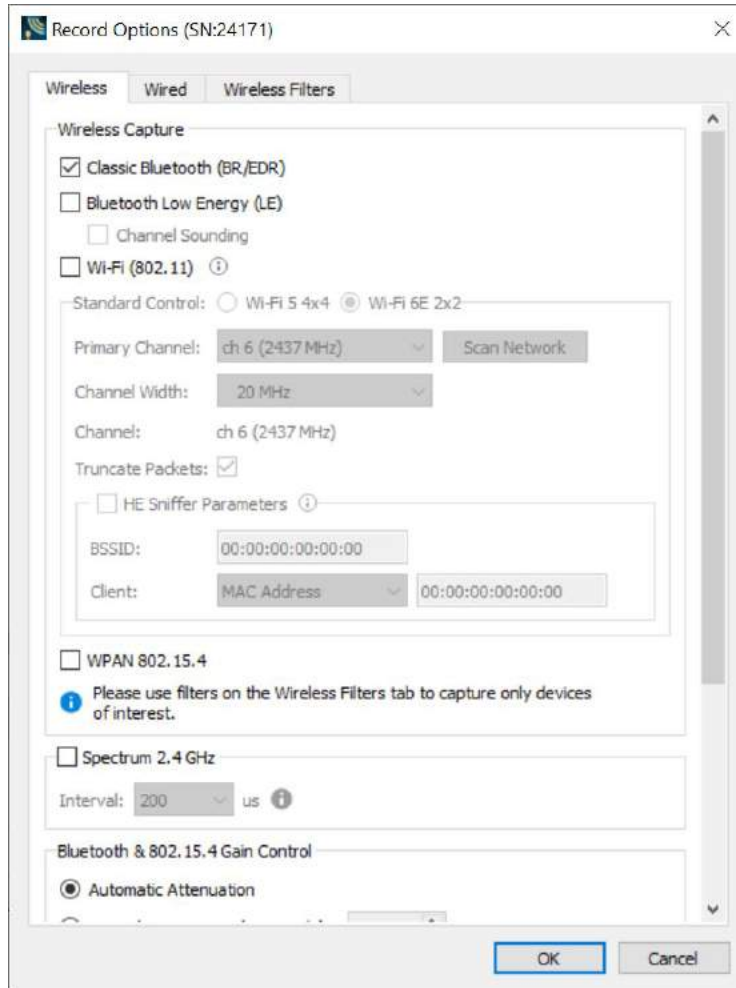


Figure 3.6 - X500 Record Options - Wireless tab (not scrolled).

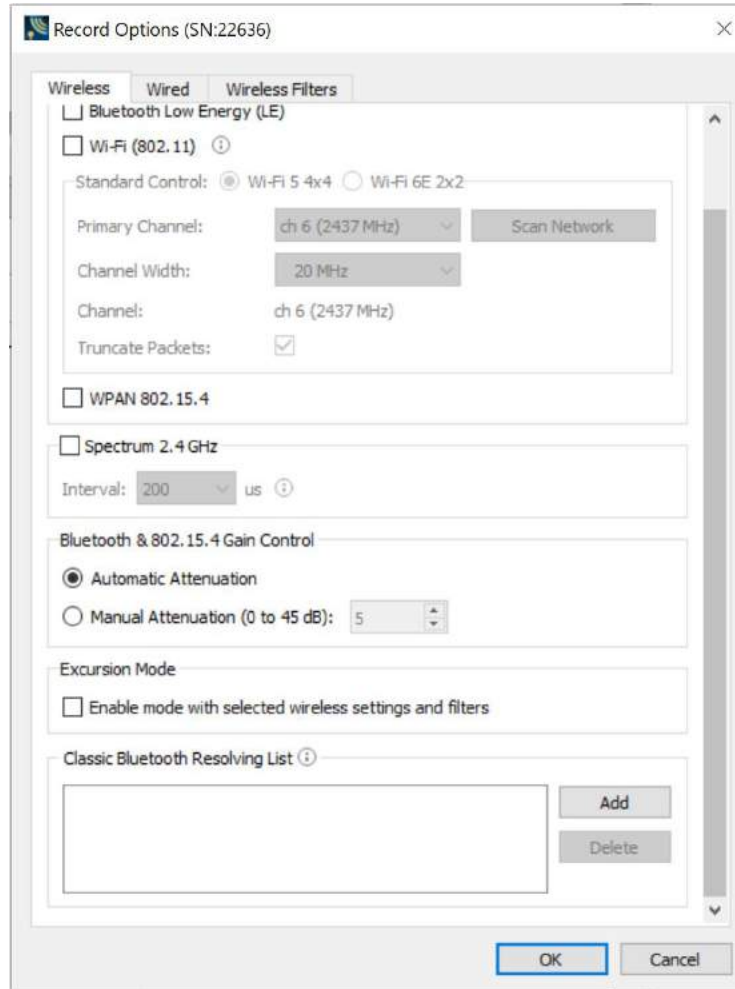




Figure 3.7 - X500 Record Options - Wireless tab (scrolled).

Table 3.3 - X500 Record Options Wireless Tab Selections

Section	Selection	Description
Wireless Capture	Classic Bluetooth	When checked, will capture data from Classic Bluetooth devices.
	Bluetooth Low Energy	When checked, will capture data from Bluetooth Low Energy devices. The sub menu for Bluetooth LE Channel Sounding (CS) is provided to configure Channel Sounding (CS) data capture. By default the check box for Channel Sounding is unchecked so no CS packets are captured.
	Wi-Fi	When checked, will enable configuring either Wi-Fi 5 4x4 or Wi-Fi 6E 2x2 capture. See the section titled Wi-Fi Configuration following this table.
	WPAN 802.15.4	When checked, will capture data from 802.15.4 devices.

Table 3.3 - X500 Record Options Wireless Tab Selections(continued)

Section	Selection	Description
<p><b>Spectrum 2.4 GHz</b></p>		<p>When checked this selection provides the user with the ability to capture samples of the 2.4 GHz RF present at the X500 antenna. The spectrum data represents the RSSI and it is automatically saved when the capture is saved. It can be optionally viewed in the Coexistence View. Spectrum sampling is set at 20, 50, 100, or 200 microsecond intervals using the <b>Interval</b> control.</p>  <p>Capturing spectrum data will use additional memory, and the smaller the sample interval, the more memory that is used, So when using sample rates less than 200 microseconds the X500 unit must be connected to a computer and not being used in Excursion Mode. See <a href="#">Spectrum Analysis on page 228</a> and <a href="#">Coexistence View - Spectrum on page 288</a> for more information.</p>
<p><b>Bluetooth &amp; 802.15.4 Gain Control</b></p>	<p><b>Automatic Attenuation</b></p> <p><b>Manual Attenuation)</b></p>	<p>The X500 unit will automatically adjust the attenuation of the received RF signal to estimated levels suitable for effective data capture.</p> <p>Manual Attenuation may be necessary if the capture does not provide reliable results. Attenuation can be adjusted from 0 to 45 dB in 1 dB steps. For example, in the presence of a strong Wi-Fi signal the user may have to increase the attenuation to achieve a reliable Bluetooth or 802.15.4 data capture. The user should adjust the attenuation and then capture the data again. Repeat, if necessary, until a reliable data capture is achieved.</p>  <p>The X500 default Manual Attenuation is 5dB.</p>
<p><b>Excursion Mode</b></p>		<p>When <b>Excursion Mode</b> is checked the X500 hardware will support Excursion mode captures where the hardware can capture data without being connected to a computer. The configured traffic is captured for later upload and analysis using a computer running the Wireless Protocol Suite software. Refer to <a href="#">Excursion Mode on page 166</a> for more information about the Excursion Mode.</p>
<p><b>Classic Bluetooth Resolving List</b></p>		<p>This is a list of Classic Bluetooth device addresses used to resolve packet source BD_ADDRs (Bluetooth Device ADDResses) during capture. The datasource maintains a database of known device BD_ADDRs indexed on the least significant 4 bytes of the BD_ADDR – the UAP and LAP. Over time, the device database will grow and may contain multiple devices with BD_ADDRs with the same UAP and LAP. The resolving list is used to specify a known set of device BD_ADDRs that will be encountered in a capture session. This list will be checked first for matching device BD_ADDRs. Each BD_ADDR on the resolving list must have a unique value for the least significant 4 bytes of the BD_ADDR (UAP and LAP).</p>

### Classic Bluetooth Resolving List Configuration

To add a Classic Bluetooth Device Address to the resolving list, select the “Add” button. Enter the Classic Bluetooth Address. Click OK. See figure below.



Figure 3.8 - Enter Bluetooth Address



Figure 3.9 - After Entering Bluetooth Address

To edit a Classic Bluetooth Device Address that is already on the list, select that address and click the “Edit” button. Change the address, then click **OK**.

To remove a Classic Bluetooth Device Address that is on the list, select that address and click the “Delete” button

### Wi-Fi Configuration

Either Wi-Fi 5 4x4 or Wi-Fi 6E 2x2 can be selected. For either of these selections, Primary 20 MHz Channel and Channel Width on which to capture Wi-Fi can be configured.

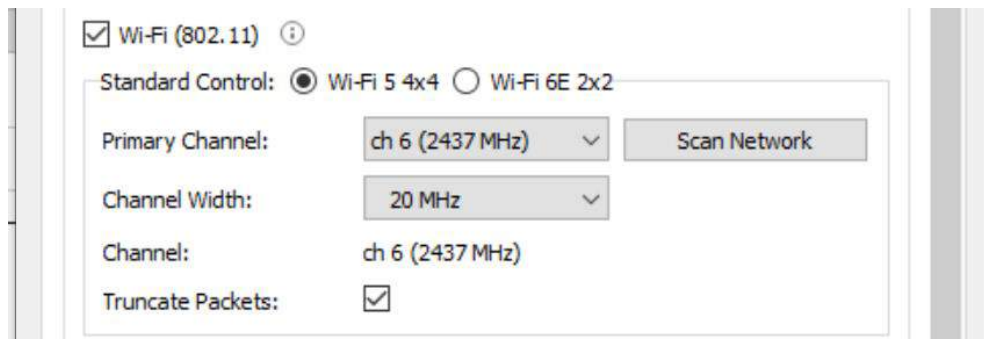


Figure 3.10 - X500 Wi-Fi 5 4x4 Options



Table 3.4 -  
X500 Wi-Fi 5 4x4 Option Selections

Section	Description
<b>Primary Channel</b>	Select from the 2.4 GHz, 5 GHz, or 6 GHz primary channels. The primary channels are 20 MHz wide. They are used for signaling and backwards compatibility.  The 6 GHz channels are only available with the Wi-Fi 6E standard selection.
<b>Channel Width</b>	The possible <b>Channel Width</b> options are enabled based on the <b>Primary Channel</b> selection.  For a 2.4 GHz channel, the possible options are 20 MHz, +40 MHz (expanded above the primary channel), and -40 MHz (expanded below the primary channel).  For a 5 GHz channel with the Wi-Fi 5 Standard, the possible options are 20 MHz, 40 MHz, 80 MHz.  For a 5 or 6 GHz channel, with the Wi-Fi 6E Standard, the possible options are 20 MHz, 40 MHz, 80 MHz and 160 MHz.
<b>Channel</b>	This is the center frequency, automatically calculated from the <b>Primary Channel</b> and the <b>Channel Width</b> selections.
<b>Truncate Packets</b>	When checked, the system truncates Wi-Fi data packets. The system does not truncate management or control type packets.  In summary view, a user will only see the decoding for the Radio Tap and MAC header of truncated packets. This allows for smaller capture files.

**For Wi-Fi 6E**

For Wi-Fi 6E, you can specify additional parameters for capturing OFDMA packets associated to one device. OFDMA is a Wi-6E feature that allows subdividing the wireless channel bandwidth. This allows multiple clients to use the channel at the same time. The settings identify these additional parameters as HE Sniffer parameters.

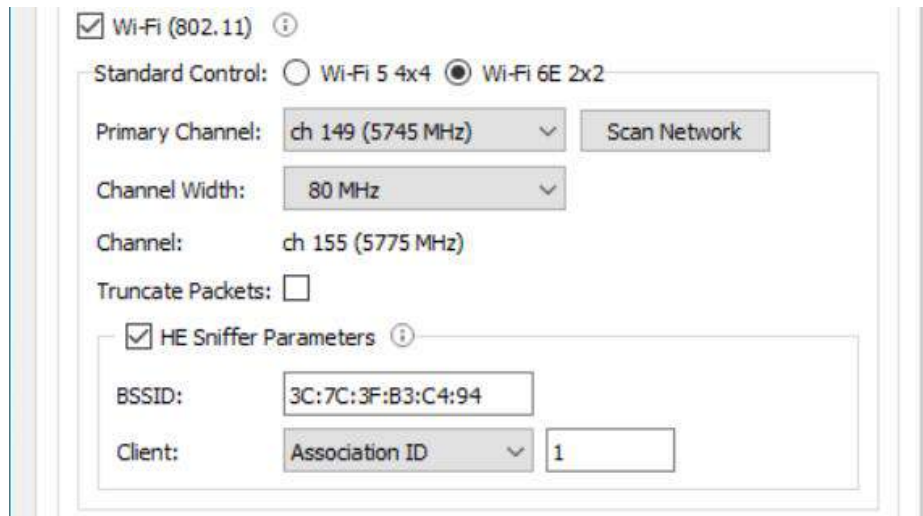


Figure 3.11 - X500 Wi-Fi 6E Options



Table 3.5 -  
HE Sniffer Parameters

<b>Section</b>	<b>Description</b>
<b>HE Sniffer Parameters</b>	This enables capturing OFDMA packets from one client device that's associated to a BSSID. When this is enabled, the system can capture Wi-Fi 6 packets that have physical types of HE_MU and HE_TRIG.
<b>BSSID</b>	This is the address of the access point in the connection.
<b>Client</b>	This indicates if the client is identified with its association ID or its MAC address.
<b>Client MAC Address</b>	This is the MAC address of the client. When a user specifies this parameter, the system extracts the association ID from an association response packet. After capturing the association response packet, the system will capture the OFDMA packets for this device.
<b>Client Association ID</b>	This is the association ID of the client. If a client device is already connected to an access point and the client's association ID is known, then use this configuration option.

### Wired Tab

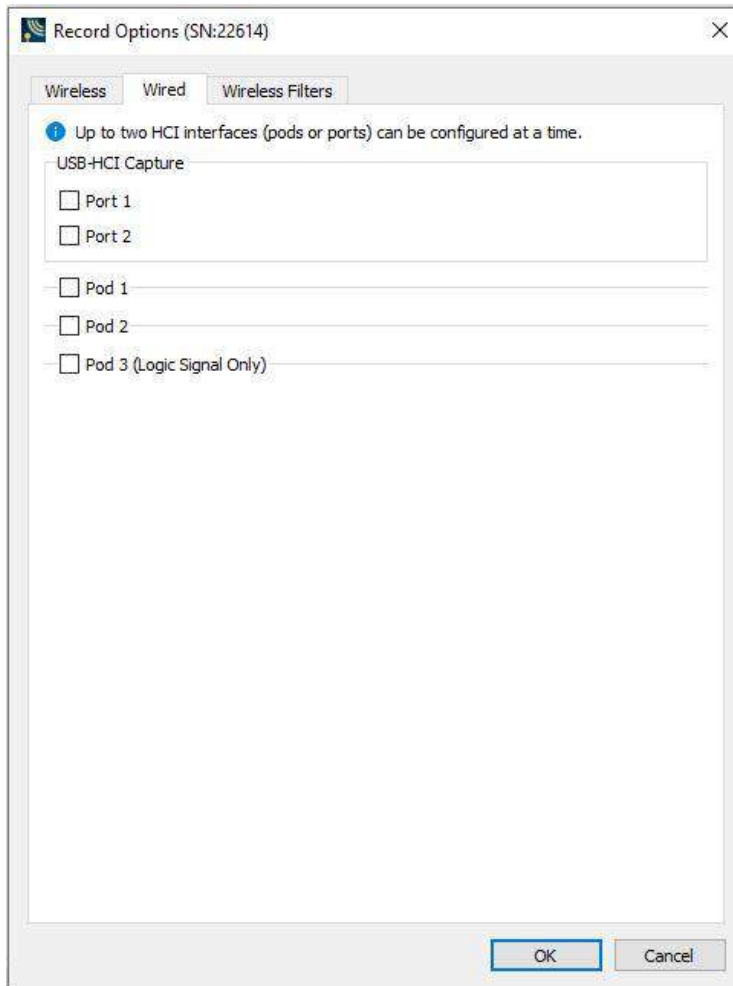


Figure 3.12 - X500 Record Options – Wired tab

Initially, without any pod selected for capture, the dialog will appear in a compressed state. Selecting a pod for capture will open the pod's options.

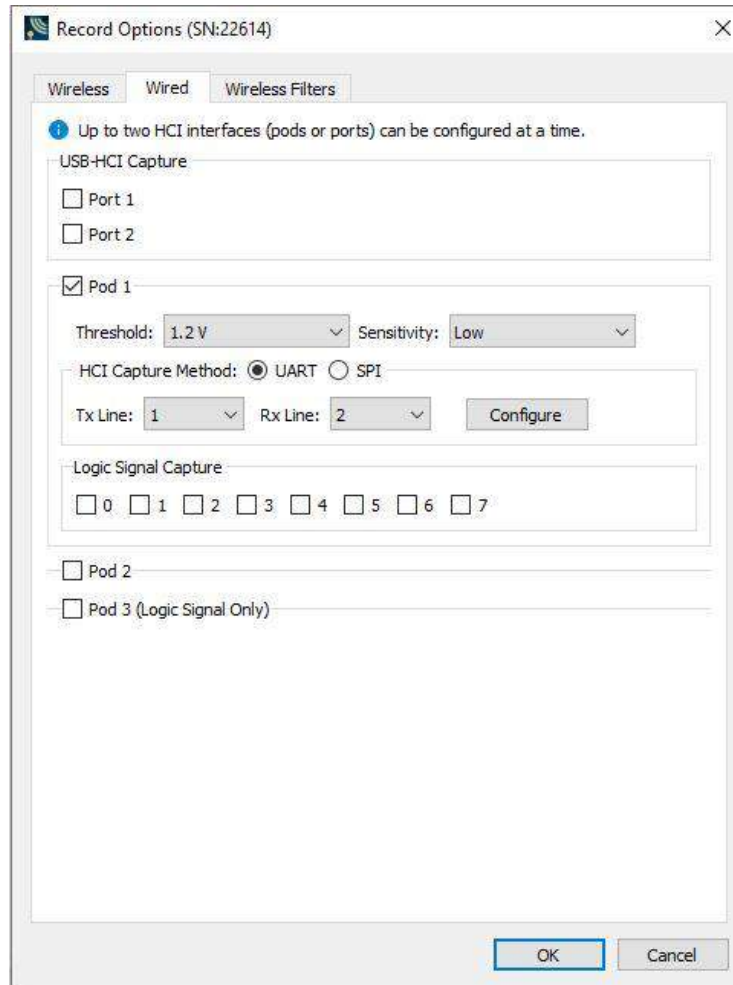


Figure 3.13 - X500 Record Options – Wired tab with Pod 1 selected for capture

When all pods are selected for capture, the dialog is scrollable.

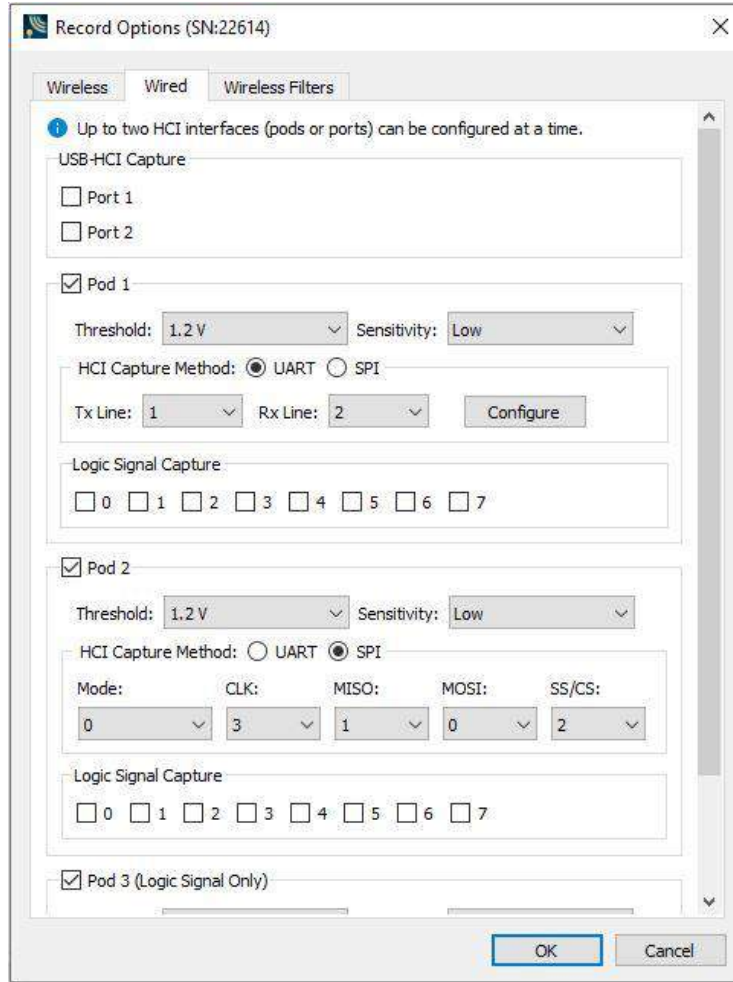


Figure 3.14 - X500 Record Options – Wired tab (not scrolled)

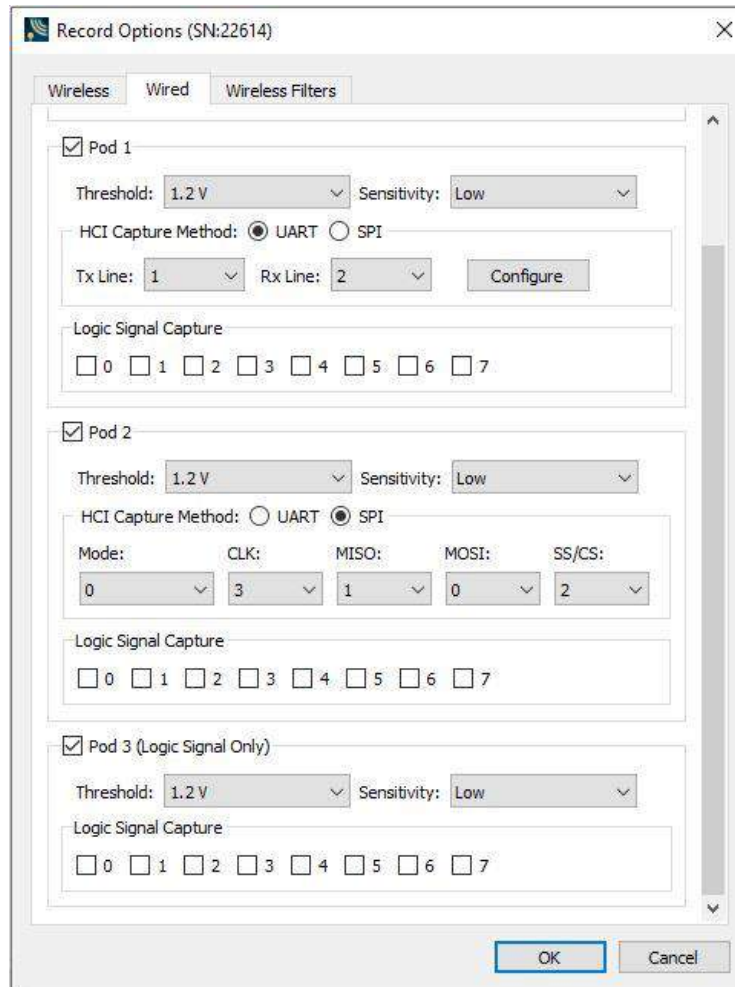


Figure 3.15 - X500 Record Options – Wired tab (scrolled)

Table 3.6 - X500 Record Options Wired Tab Selections

Pod Selection	Section	Description	
Pod 1		When checked, Pod 1 is enabled for both Logic Signal and HCI capture.	
	<b>Threshold (V)</b>	Threshold voltage at which a line is considered to be in an on state. The default value is set to 1.2 V (recommended). Users can select threshold value starting at 0.4 V and go up to 2.7 V. Using a value that's close to half the signaling level will work for most applications. Please check your hardware datasheet or vendor to learn about the settings to use.	
	<b>Sensitivity</b>	Sensitivity to changes in voltage level around the threshold voltage. The default value is set to "low" (recommended) indicating lowest sensitivity to noise or maximum hysteresis. Please check your hardware datasheet or vendor to learn about the settings to use.	
	<b>HCI Capture Method: UART</b>	<b>Tx line</b>	Data line selected for UART transmit
		<b>Rx line</b>	Data line selected for UART receive
		<b>Configure</b>	HCI UART I/O Settings . See HCI-UART I/O Settings following this table.
	<b>HCI Capture Method: SPI</b>	<b>Mode</b>	SPI Mode 0 – 3.
		<b>CLK</b>	Data line selected for clock signal.
		<b>MISO</b>	Data line selected for central output central input.
		<b>MOSI</b>	Data line selected for central input central output.
		<b>SS/CS</b>	Data line selected for central select signal.
<b>Logic Signal Capture</b>	<b>0-7</b>	These are Logic Signal data lines 0-7 corresponding to Data 0-Data 7 on the Logic Analyzer Pod. When any data lines are selected, logic signal transitions on those lines will be captured. None or one or any number of data lines can be selected.	

Table 3.6 - X500 Record Options Wired Tab Selections(continued)

Pod Selection	Section	Description	
Pod 2		When checked, Pod 2 is enabled for both Logic Signal and HCI capture.	
	Threshold (V)	Threshold voltage at which a line is considered to be in an on state. The default value is set to 1.2 V (recommended). Users can select threshold value starting at 0.4 V and go up to 2.7 V. Using a value that's close to half the signaling level will work for most applications. Please check your hardware datasheet or vendor to learn about the settings to use.	
	Sensitivity	Sensitivity to changes in voltage level around the threshold voltage. The default value is set to "low" (recommended) indicating lowest sensitivity to noise or maximum hysteresis. Please check your hardware datasheet or vendor to learn about the settings to use.	
	HCI Capture Method: UART	Tx line	Data line selected for UART transmit
		Rx line	Data line selected for UART receive
		Configure	HCI UART I/O Settings . See HCI-UART I/O Settings following this table.
	HCI Capture Method: SPI	Mode	SPI Mode 0 – 3.
		CLK	Data line selected for clock signal.
		MISO	Data line selected for central output central input.
		MOSI	Data line selected for central input central output.
		SS/CS	Data line selected for central select signal.
Logic Signal Capture	0-7	These are Logic Signal data lines 0-7 corresponding to Data 0-Data 7 on the Logic Analyzer Pod. When any data lines are selected, logic signal transitions on those lines will be captured. None or one or any number of data lines can be selected.	

Table 3.6 - X500 Record Options Wired Tab Selections(continued)

Pod Selection	Section	Description	
Pod 3		When checked, Pod 3 is enabled for both Logic Signal and HCI capture.	
	<b>Threshold (V)</b>	Threshold voltage at which a line is considered to be in an on state. The default value is set to 1.2 V (recommended). Users can select threshold value starting at 0.4 V and go up to 2.7 V. Using a value that's close to half the signaling level will work for most applications. Please check your hardware datasheet or vendor to learn about the settings to use.	
	<b>Sensitivity</b>	Sensitivity to changes in voltage level around the threshold voltage. The default value is set to "low" (recommended) indicating lowest sensitivity to noise or maximum hysteresis. Please check your hardware datasheet or vendor to learn about the settings to use.	
	<b>HCI Capture Method: UART</b>	<b>Tx line</b>	Data line selected for UART transmit
		<b>Rx line</b>	Data line selected for UART receive
		<b>Configure</b>	HCI UART I/O Settings . See HCI-UART I/O Settings following this table.
	<b>HCI Capture Method: SPI</b>	<b>Mode</b>	SPI Mode 0 – 3.
		<b>CLK</b>	Data line selected for clock signal.
		<b>MISO</b>	Data line selected for central output central input.
		<b>MOSI</b>	Data line selected for central input central output.
		<b>SS/CS</b>	Data line selected for central select signal.
	<b>Logic Signal Capture</b>	<b>0-7</b>	These are Logic Signal data lines 0-7 corresponding to Data 0-Data 7 on the Logic Analyzer Pod. When any data lines are selected, logic signal transitions on those lines will be captured. None or one or any number of data lines can be selected.

### HCI UART I/O Settings

After clicking on the Configure button, the I/O Settings for UART can be configured without an HCI pod being connected to the Soderia. When you click on the OK button the configuration information is saved but is not stored on the Soderia hardware.



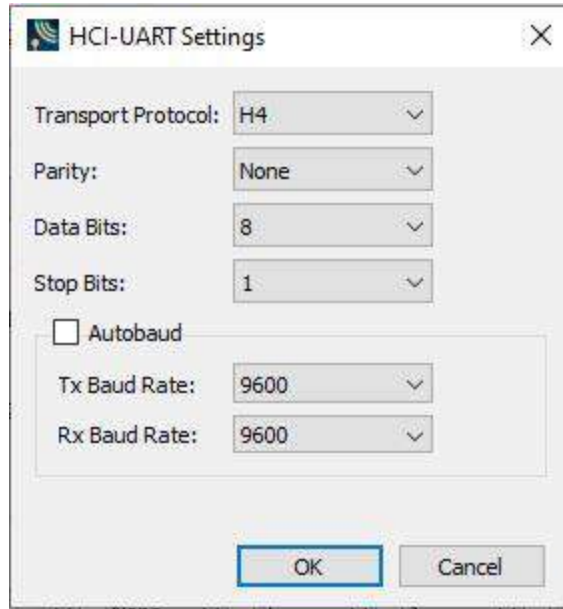


Figure 3.16 - HCI UART Settings

Table 3.7 - HCI-UART Settings

Setting	Value	Description
<b>Transport Protocol</b>	<b>H4</b>	The simplest protocol designed to operate over RS-232 with no parity in a 5-wire configuration.
	<b>BCSP</b>	BlueCore Serial Protocol, developed by CSR, provides a more reliable alternative to H4. The protocol is defined to run a 3-wire connection, and can optionally use a 5-wire UART connection with two flow control lines.
	<b>3-Wire (H5)</b>	A 3-wire protocol that provides error detection and correction.
	<b>MWS WCI-2</b>	The Wireless Coexistence Interface (WCI) is a full duplex UART carrying logic signals framed as UART characters.
<b>Parity</b>	<b>None</b>	No parity check occurs
	<b>Even</b>	The count of bits set is an even number.
	<b>Odd</b>	The count of bits set is an odd number.
<b>Data Bits</b>	<b>8</b>	The number of data bits in the expected packet.
	<b>7</b>	
	<b>6</b>	
	<b>5</b>	
<b>Stop Bits</b>	<b>1</b>	The number of data bits held in the mark (logic 1) condition at the end of the expected packet.
	<b>1.5</b>	
	<b>2</b>	

Table 3.7 - HCI-UART Settings (continued)

Setting	Value	Description
<b>Autobaud</b>		The X500 can automatically determine the baud rate of the HCI UART when the Autobaud is selected. When the Autobaud checkbox is checked in the “HCI-UART Settings” dialog box the analyzer automatically determines the baud rate. Once a baud rate has been determined, it is applied to both the TX and RX lines. The baud rate is continually monitored during the capture and automatically adjusted if the baud rate of the received data changes. If Autobaud is used on multiple pods simultaneously then Autobaud determines the baud rate of each pod independently of the other pods. Additionally, if Autobaud is being used then other pods can still use fixed baud rates. It is possible that when starting the baud search very short packets may be missed.
<b>TX Baud Rate</b>	<b>Disabled</b>	The baud rates displayed are nominal baud rates as opposed to the precise values internal to the analyzer which may differ slightly with a mean absolute average difference of less than half a percent. If autobaud is used the difference may be more depending on how much the actual baud rate differs from those listed in the table.
	<b>9,600</b>	
	<b>14,400</b>	
	<b>19,200</b>	
	<b>28,800</b>	
	<b>38,400</b>	
	<b>57,600</b>	
	<b>115,200</b>	
	<b>230,400</b>	
	<b>460,800</b>	
	<b>921,600</b>	
	<b>1,000,000</b>	
	<b>1,250,000</b>	
	<b>1,500,000</b>	
	<b>1,750,000</b>	
	<b>2,000,000</b>	
	<b>2,250,000</b>	
<b>2,500,000</b>		
<b>2,750,000</b>		
<b>3,000,000</b>		
<b>3,250,000</b>		
<b>3,500,000</b>		
<b>3,750,000</b>		
<b>4,000,000</b>		
<b>RX Baud Rate</b>		Same as <b>TX Baud Rate</b> .

**Wireless Filters Tab**

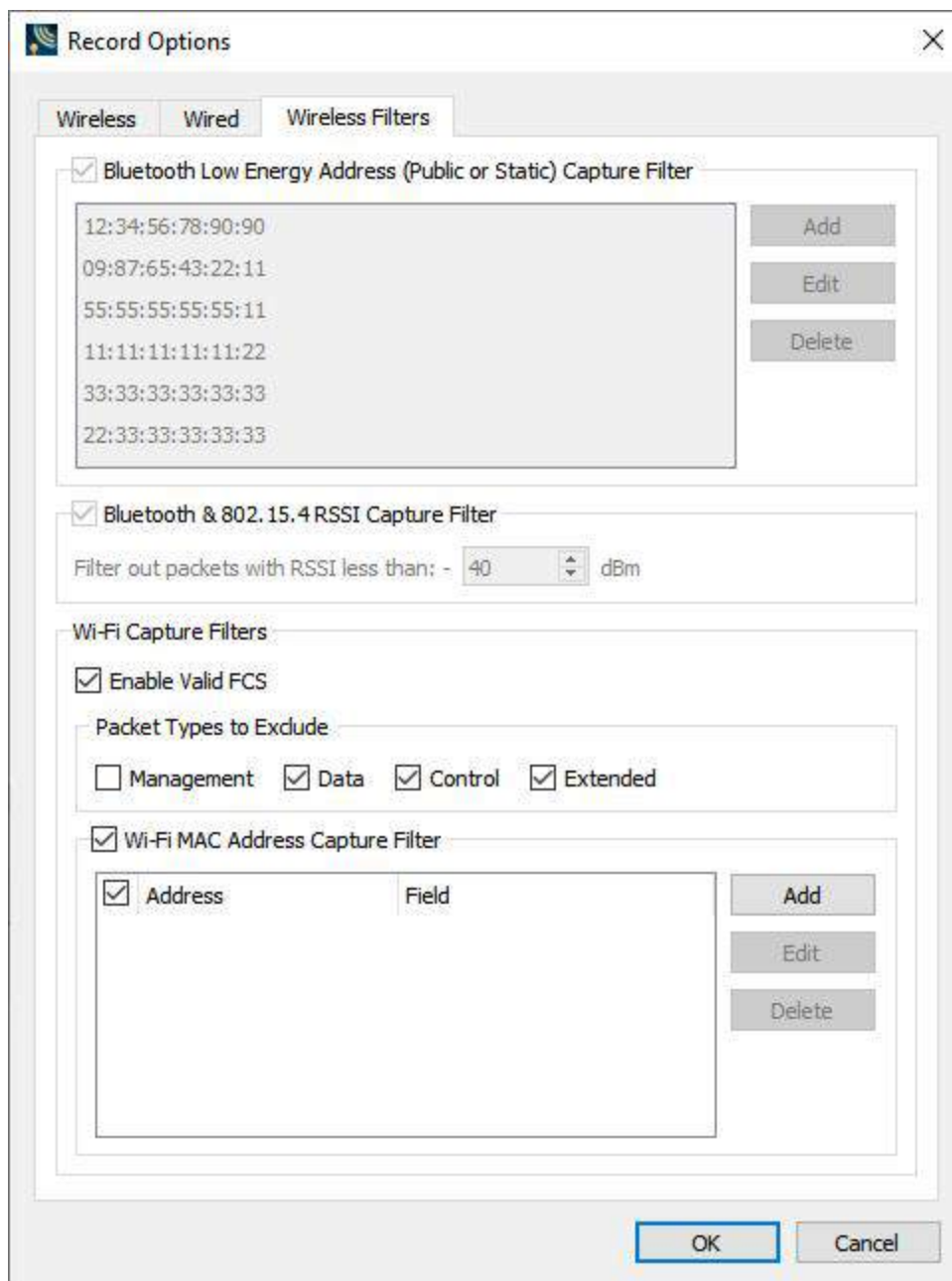
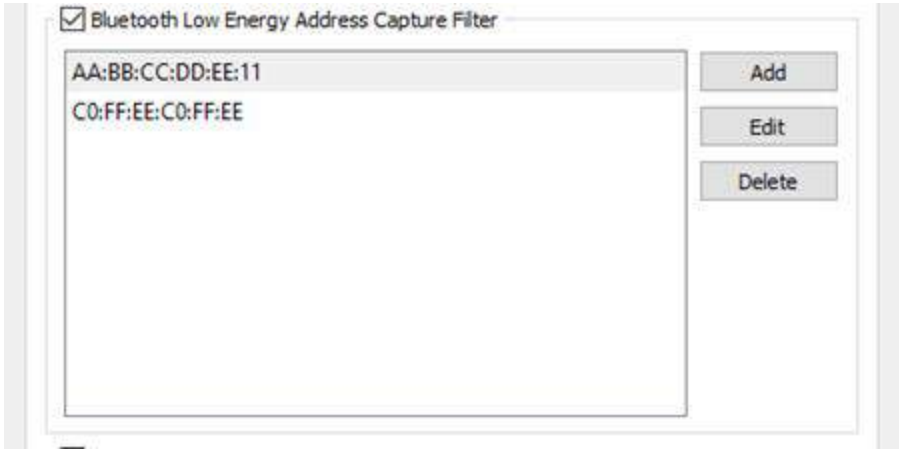



Figure 3.17 - X500 Record Options – Wireless Filters Tab

Table 3.8 - X500 Record Options Wireless Filters Selections

Section	Description
<p><b>Bluetooth Low Energy Address Capture Filter</b></p>	<p>By enabling the Bluetooth Low Energy Address Capture Filter, only Low Energy packets from the listed Bluetooth Addresses will be processed into the capture. Addresses can be added, selected and edited, and selected and deleted by using the Add, Edit, Delete buttons respectively.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>
<p><b>RSSI Capture Filter</b></p>	<p>By enabling the RSSI Capture Filter, only those packets with RSSI greater than the entered dBm value will be processed into the capture.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>
<p><b>Wi-Fi Capture Filters</b></p>	
<p><b>Enable Valid FCS</b></p>	<p>When checked, the system only captures Wi-Fi packets with a valid checksum. This allows a user to filter out bad packets.</p>
<p><b>Packet Types to Exclude</b></p>	<p>When a type is checked, the system does not capture this type of Wi-Fi packet. This allows a user to filter out unnecessary packet types. For example, a user may only want to see Management type packets.</p>
<p><b>Wi-Fi MAC Address Capture Filter</b></p>	<p>See Wi-Fi MAC Address Filtering following this table.</p>

**Wi-Fi MAC Address Filtering**

In environments where many Wi-Fi signals can make it hard to focus analysis on only a few signals of interest, the Wi-Fi MAC Address Capture Filter options allow configuration of only the signals of interest.

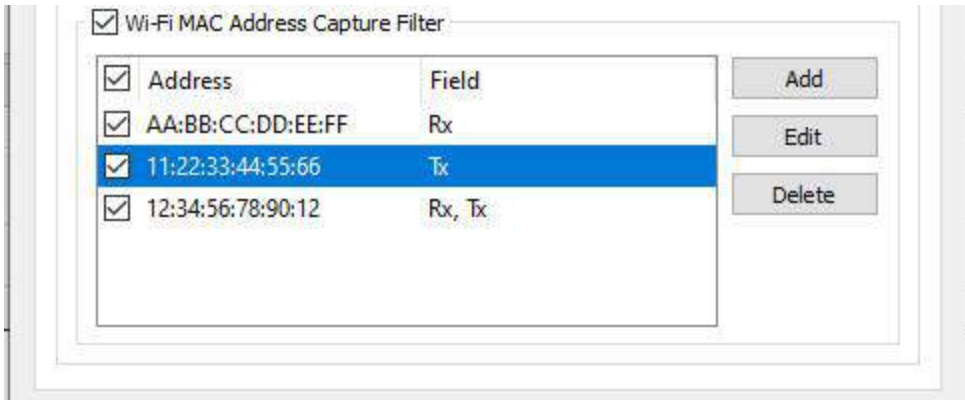


Figure 3.18 - X500 Wireless Filters Tab – Wi-Fi MAC Address Capture Filter

Table 3.9 - X500 Wi-Fi Tab MAC Address Filtering

Setting	Description
<b>Wi-Fi MAC Address Capture Filters</b>	This must be checked in order to enable the filtering of MAC Addresses on the X500. Unchecking this disables MAC Address filtering on the X500, allowing all Wi-Fi signals captured into WPS for analysis.
<b>Add</b>	Displays a dialog in which the MAC Address can be entered and controls for selecting TX/RX. See Wi-Fi MAC Address Editing following this table.
<b>Edit</b>	After selecting one of the MAC Addresses in the table, this will display a dialog in which the MAC Address and the TX/RX can be changed. See Wi-Fi MAC Address Editing following this table.
<b>Delete</b>	After selection one of the MAC Addresses in the table, this will delete that MAC Address filter.

**Wi-Fi MAC Address Editing**

The MAC Address table displays the MAC Address and the Fields which indicates whether the MAC Address is filtered by the Rx (Receive) and/or Tx (Transmit) Field in the MAC Frame.

There is an Enable checkbox for each MAC Address so that each one can be enabled or disabled for filtering.

Up to eight MAC Addresses can be entered for filtering.

To add a MAC Address, click the **Add** button. The **New Address** dialog is displayed.

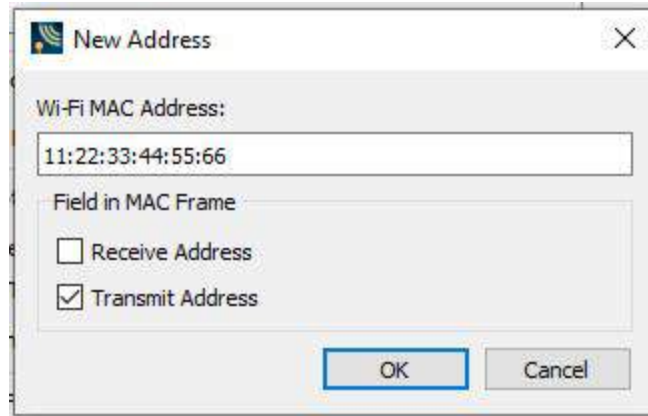


Figure 3.19 - X500 New Address dialog for a new MAC Address

Enter the MAC Address into the edit field as indicated and select whether to filter that address as Receive and/or Transmit. Click **OK** and the MAC Address will appear in the MAC Address table with its Enable checkbox checked by default.

To edit a MAC Address, click on one of the MAC Addresses in the table to select it and click the **Edit** button. The same **New Address** dialog as above will display with all the information from the table already entered. Edit then click OK. The changes to the MAC Address appear in the MAC Address table.

If the **Wi-Fi MAC Address Capture Filter** checkbox is turned off, the MAC Address filters themselves are still retained on the X500 for re-enabling later.

### 3.1.2.1.1.2 Record Options Dialog: X240

The Record Options dialog is used to configure the X240 unit prior to data capture. The record options are stored on the X240 hardware and these settings will persist until changed. The Record Options dialog is only active when a X240 unit is connected to the computer running the Wireless Protocol Suite software.

**Note:** If a X240 hardware unit is not connected then these settings can neither be viewed nor changed.

Clicking on **OK** will save the **Record Options** settings on the connected X240 unit. Any **Record Options** parameter changes made will overwrite the previously saved **Record Options**.

#### Wireless Tab X240

The X240 Wireless tab is scrollable.

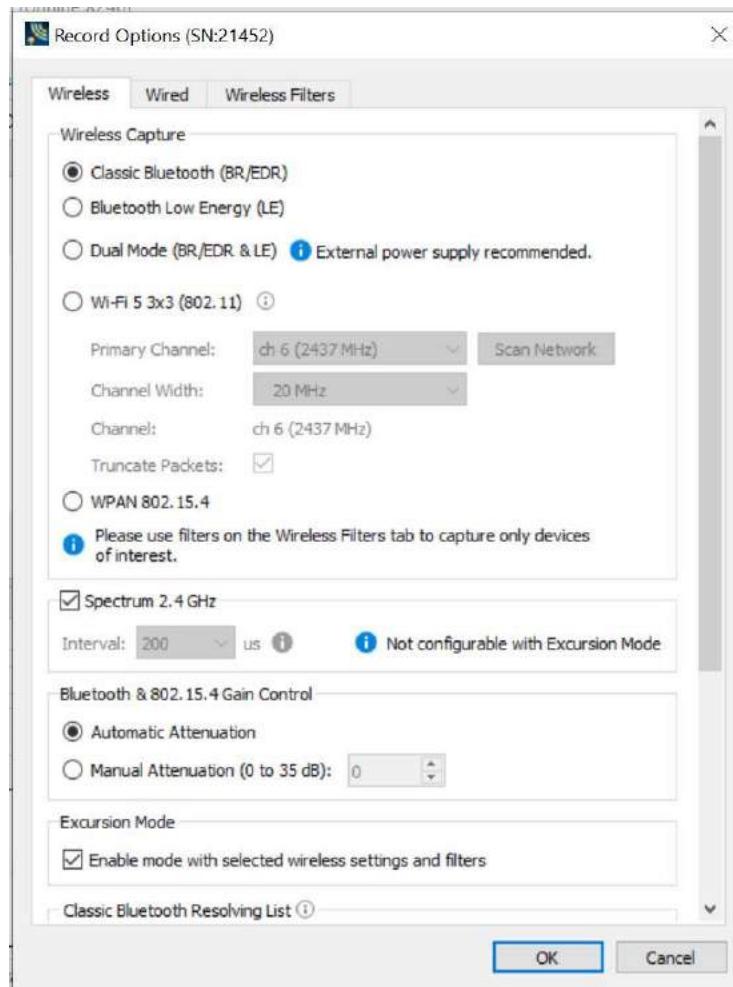


Figure 3.20 - X240 Record Options - Wireless tab (not scrolled).

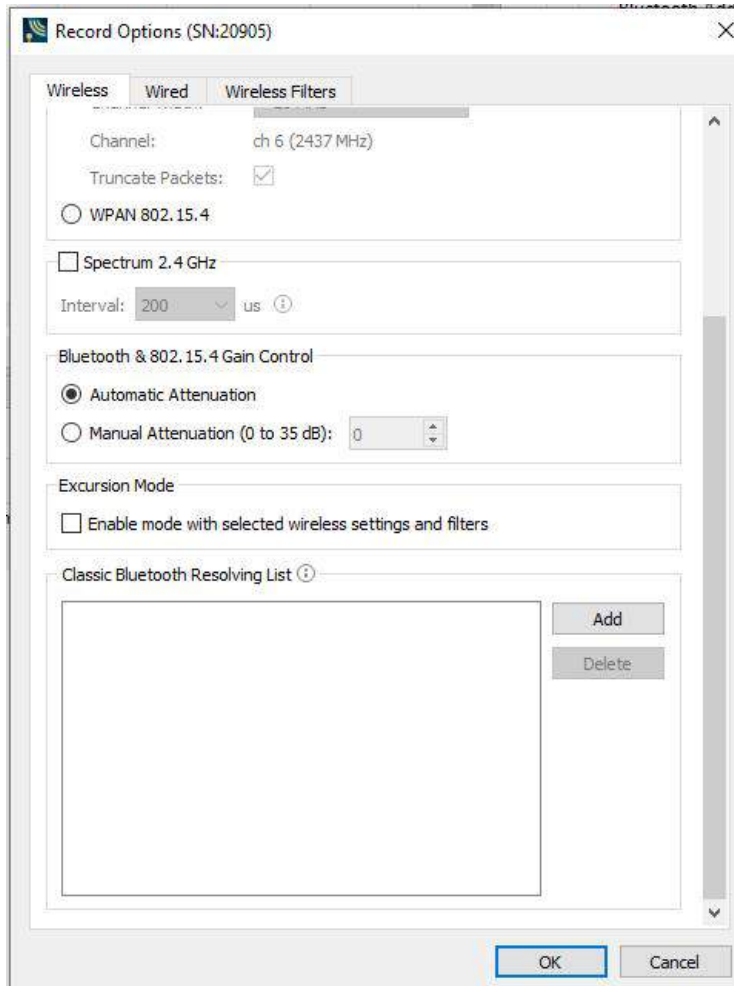


Figure 3.21 - X240 Record Options - Wireless tab (scrolled).



Table 3.10 - X240 Record Options Wireless Tab Selections



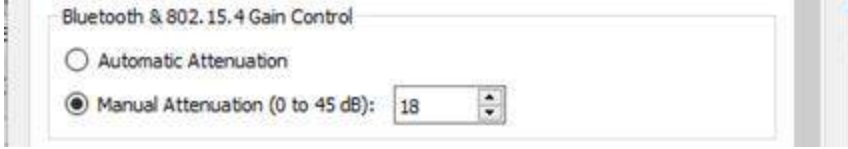
Section	Selection	Description
<b>Wireless Capture</b>	<b>Classic Bluetooth</b>	When checked, will capture data from Classic Bluetooth devices.
	<b>Bluetooth Low Energy</b>	When checked, will capture data from Bluetooth Low Energy devices.
	<b>Bluetooth Dual Mode (BR/EDR and LE)</b>	When checked, will capture data from both Bluetooth Classic and LE devices. <b>NOTE:</b> It is recommended to use an external power supply when capturing using X240 in dual mode configuration. The X240 hardware may shut down if the PC cannot deliver at least 15W to the hardware consistently. It is also recommended to use certified USB cables provided by Teledyne LeCroy for optimal performance.
	<b>Wi-Fi 5 3x3</b>	When checked, will capture data from 802.11 devices. See the section titled Wi-Fi 5 3x3 Configuration following this table.
	<b>WPAN 802.15.4</b>	When checked, will capture data from 802.15.4 devices. <b>NOTE:</b> When the Wireless Capture technology is changed, a dialog will appear indicating that the selected Wireless Capture technology is being enabled. 
<b>Spectrum 2.4 GHz</b>		When checked this selection provides the user with the ability to capture samples of the 2.4 GHz RF present at the X240 antenna. The spectrum data represents the RSSI and it is automatically saved when the capture is saved. It can be optionally viewed in the Coexistence View. Spectrum sampling is set at 20, 50, 100, or 200 microsecond intervals using the <b>Interval</b> control.  Capturing spectrum data will use additional memory, and the smaller the sample interval, the more memory that is used, So when using sample rates less than 200 microseconds the X240 unit must be connected to a computer and not being used in Excursion Mode. See <a href="#">Spectrum Analysis on page 228</a> and <a href="#">Coexistence View - Spectrum on page 288</a> for more information.

Table 3.10 - X240 Record Options Wireless Tab Selections(continued)

Section	Selection	Description
<b>Bluetooth &amp; 802.15.4 Gain Control</b>	<b>Automatic Attenuation</b>	The X240 unit will automatically adjust the attenuation of the received RF signal to estimated levels suitable for effective data capture.
	<b>Manual Attenuation)</b>	Manual Attenuation may be necessary if the capture does not provide reliable results. Attenuation can be adjusted from 0 to 45 dB in 1 dB steps. For example, in the presence of a strong Wi-Fi signal the user may have to increase the attenuation to achieve a reliable Bluetooth or 802.15.4 data capture. The user should adjust the attenuation and then capture the data again. Repeat, if necessary, until a reliable data capture is achieved.   The X240 default Manual Attenuation is 0dB.
<b>Excursion Mode</b>		When <b>Excursion Mode</b> is checked the X240 hardware will support Excursion mode captures where the hardware can capture data without being connected to a computer. The configured traffic is captured for later upload and analysis using a computer running the Wireless Protocol Suite software. Refer to <a href="#">Excursion Mode on page 166</a> for more information about the Excursion Mode.
<b>Classic Bluetooth Resolving List</b>		This is a list of Classic Bluetooth device addresses used to resolve packet source BD_ADDRs (Bluetooth Device ADDresses) during capture. The datasource maintains a database of known device BD_ADDRs indexed on the least significant 4 bytes of the BD_ADDR – the UAP and LAP. Over time, the device database will grow and may contain multiple devices with BD_ADDRs with the same UAP and LAP. The resolving list is used to specify a known set of device BD_ADDRs that will be encountered in a capture session. This list will be checked first for matching device BD_ADDRs. Each BD_ADDR on the resolving list must have a unique value for the least significant 4 bytes of the BD_ADDR (UAP and LAP).

### Classic Bluetooth Resolving List Configuration

To add a Classic Bluetooth Device Address to the resolving list, select the “Add” button. Enter the Classic Bluetooth Address. Click OK. See figure below.



Figure 3.22 - Enter Bluetooth Address



Figure 3.23 - After Entering Bluetooth Address

To edit a Classic Bluetooth Device Address that is already on the list, select that address and click the “Edit” button. Change the address, then click **OK**.

To remove a Classic Bluetooth Device Address that is on the list, select that address and click the “Delete” button

### Wi-Fi 5 3x3 Configuration

The Wi-Fi 5 3x3 options permit configuration of the Primary 20 MHz Channel and Channel Width on which to capture Wi-Fi.

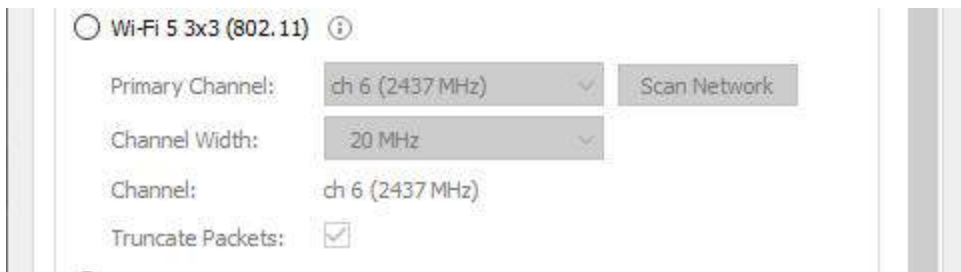


Figure 3.24 - X240 5 3x3Wi-Fi Options

Table 3.11 - X240 Wi-Fi 5 3x3 Option Selections

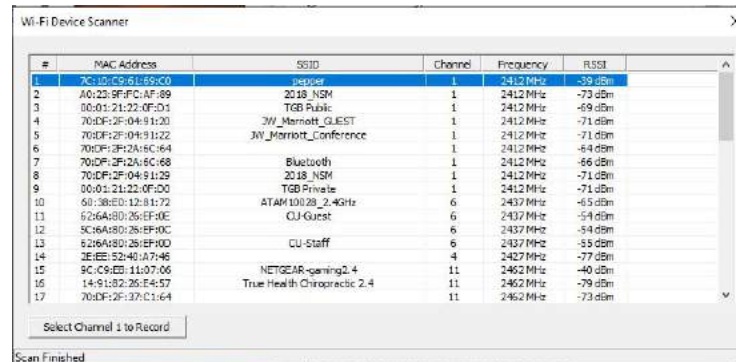
<b>Section</b>	<b>Description</b>
<b>Primary Channel</b>	Select from the 2.4 GHz or 5 GHz primary channels. The primary channels are 20 MHz wide. They are used for signaling and backwards compatibility.
<b>Channel Width</b>	<p>The possible <b>Channel Width</b> options are enabled based on the <b>Primary Channel</b> selection.</p> <p>For a 2.4 GHz channel, the possible options are 20 MHz, +40 MHz (expanded above the primary channel), and -40 MHz (expanded below the primary channel).</p> <p>For a 5 GHz channel, the possible options are 20 MHz, 40 MHz, and 80 MHz.</p>
<b>Channel</b>	This is the center frequency, automatically calculated from the <b>Primary Channel</b> and the <b>Channel Width</b> selections.
<b>Truncate Packets</b>	<p>When checked, the system truncates Wi-Fi data packets. The system does not truncate management or control type packets.</p> <p>In summary view, a user will only see the decoding for the Radio Tap and MAC header of truncated packets. This allows for smaller capture files.</p> <p><b>NOTE:</b> The system only allows capturing spectrum data when Wi-Fi packets are truncated.</p>

### Wi-Fi Device Scanner

The “Scan Network” button allows a user to scan Wi-Fi channels for Wireless networks. The scanner scans channels on both the 2.4 GHz and 5.0 GHz frequency bands. After the scanning completes, the user can choose the primary channel to record. This is helpful if one doesn’t know before recording what channel to use.

The Wi-Fi tab only enables the “Scan Network” button when the current firmware image in the X240 supports Wi-Fi 5 3x3 capture.

Scanning takes a few seconds to complete before displaying a list of Wireless networks.



#	MAC Address	SSID	Channel	Frequency	RSSI
1	7C:30:40:01:55:C0	Verizon	1	2412 MHz	-59 dBm
2	A0:22:8F:FC:AF:89	2018_NSM	1	2412 MHz	-73 dBm
3	00:01:21:22:0F:5D	TGB Public	1	2412 MHz	-69 dBm
4	70:DF:2F:04:91:20	3W_Marriott_GUEST	1	2412 MHz	-71 dBm
5	70:DF:2F:04:91:22	3W_Marriott_Conference	1	2412 MHz	-71 dBm
6	70:DF:2F:2A:6C:64		1	2412 MHz	-64 dBm
7	70:DF:2F:2A:6C:68	Bluetooth	1	2412 MHz	-66 dBm
8	70:DF:2F:04:91:29	2018_NSM	1	2412 MHz	-71 dBm
9	00:01:21:22:0F:5D	TGB Private	1	2412 MHz	-71 dBm
10	60:38:ED:12:81:72	AT&T10028_2.4GHz	6	2437 MHz	-65 dBm
11	52:6A:8D:26:EF:0E	CJ-Guest	6	2437 MHz	-54 dBm
12	52:6A:8D:26:EF:0C		6	2437 MHz	-54 dBm
13	52:6A:8D:26:EF:0D	CJ-staff	6	2437 MHz	-55 dBm
14	2E:EE:52:40:A7:46		4	2427 MHz	-77 dBm
15	9C:C9:ED:11:07:06	NETGEAR-gaming2.4	11	2462 MHz	-40 dBm
16	14:51:52:26:2E:57	True Health Chromecast 2.4	11	2462 MHz	-79 dBm
17	70:DF:2F:37:C1:64		11	2462 MHz	-73 dBm

Select Channel 1 to Record

Scan Finished

Figure 3.25 - X240 Wi-Fi 5 3x3 Device Scanner

Select an entry and click the “Select Channel to Record” button.

Wired Tab

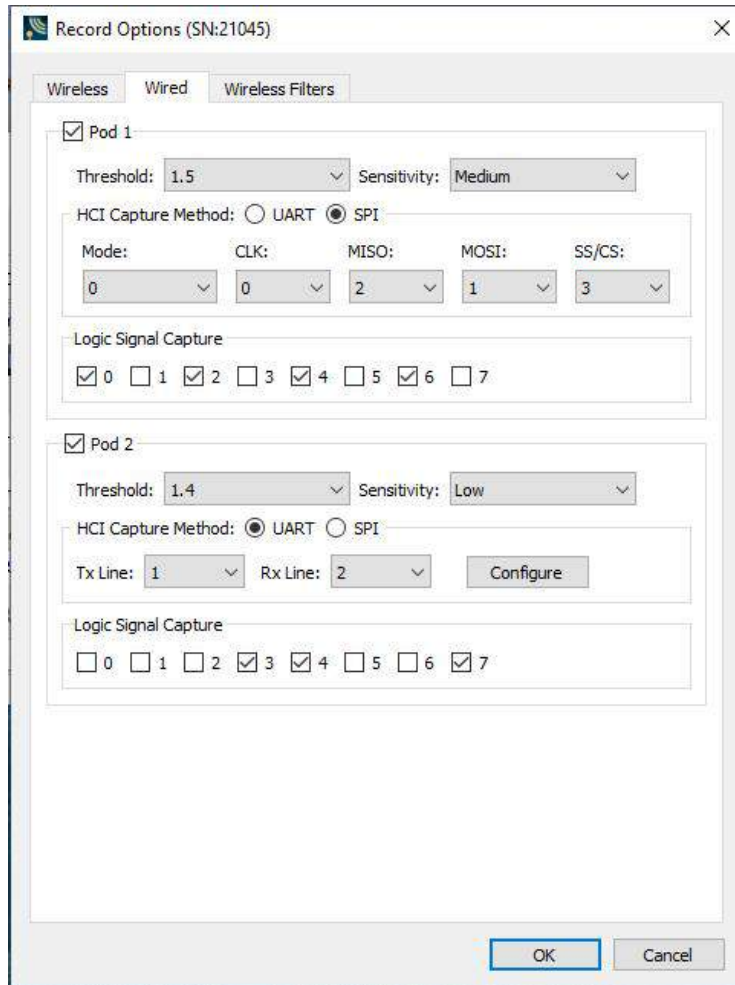


Figure 3.26 - X240 Record Options – Wired tab (scrolled)

Table 3.12 - X240 Record Options Wired Tab Selections

Pod Selection	Section	Description	
Pod 1		When checked, Pod 1 is enabled for both Logic Signal and HCI capture.	
	Threshold (V)	Threshold voltage at which a line is considered to be in an on state. The default value is set to 1.2 V (recommended). Users can select threshold value starting at 0.4 V and go up to 2.7 V. Using a value that's close to half the signaling level will work for most applications. Please check your hardware datasheet or vendor to learn about the settings to use.	
	Sensitivity	Sensitivity to changes in voltage level around the threshold voltage. The default value is set to "low" (recommended) indicating lowest sensitivity to noise or maximum hysteresis. Please check your hardware datasheet or vendor to learn about the settings to use.	
	HCI Capture Method: UART	Tx line	Data line selected for UART transmit
		Rx line	Data line selected for UART receive
		Configure	HCI UART I/O Settings . See HCI-UART I/O Settings following this table.
	HCI Capture Method: SPI	Mode	SPI Mode 0 – 3.
		CLK	Data line selected for clock signal.
		MISO	Data line selected for central output central input.
		MOSI	Data line selected for central input central output.
		SS/CS	Data line selected for central select signal.
Logic Signal Capture	0-7	These are Logic Signal data lines 0-7 corresponding to Data 0-Data 7 on the Logic Analyzer Pod. When any data lines are selected, logic signal transitions on those lines will be captured. None or one or any number of data lines can be selected.	

Table 3.12 - X240 Record Options Wired Tab Selections(continued)

Pod Selection	Section	Description	
Pod 2		When checked, Pod 2 is enabled for both Logic Signal and HCI capture.	
	<b>Threshold (V)</b>	Threshold voltage at which a line is considered to be in an on state. The default value is set to 1.2 V (recommended). Users can select threshold value starting at 0.4 V and go up to 2.7 V. Using a value that's close to half the signaling level will work for most applications. Please check your hardware datasheet or vendor to learn about the settings to use.	
	<b>Sensitivity</b>	Sensitivity to changes in voltage level around the threshold voltage. The default value is set to "low" (recommended) indicating lowest sensitivity to noise or maximum hysteresis. Please check your hardware datasheet or vendor to learn about the settings to use.	
	<b>HCI Capture Method: UART</b>	<b>Tx line</b>	Data line selected for UART transmit
		<b>Rx line</b>	Data line selected for UART receive
		<b>Configure</b>	HCI UART I/O Settings . See HCI-UART I/O Settings following this table.
	<b>HCI Capture Method: SPI</b>	<b>Mode</b>	SPI Mode 0 – 3.
		<b>CLK</b>	Data line selected for clock signal.
		<b>MISO</b>	Data line selected for central output central input.
		<b>MOSI</b>	Data line selected for central input central output.
		<b>SS/CS</b>	Data line selected for central select signal.
<b>Logic Signal Capture</b>	<b>0-7</b>	These are Logic Signal data lines 0-7 corresponding to Data 0-Data 7 on the Logic Analyzer Pod. When any data lines are selected, logic signal transitions on those lines will be captured. None or one or any number of data lines can be selected.	



## HCI UART I/O Settings

After clicking on the Configure button, the I/O Settings for UART can be configured without an HCI pod being connected to the Sodera. When you click on the OK button the configuration information is saved but is not stored on the Sodera hardware.

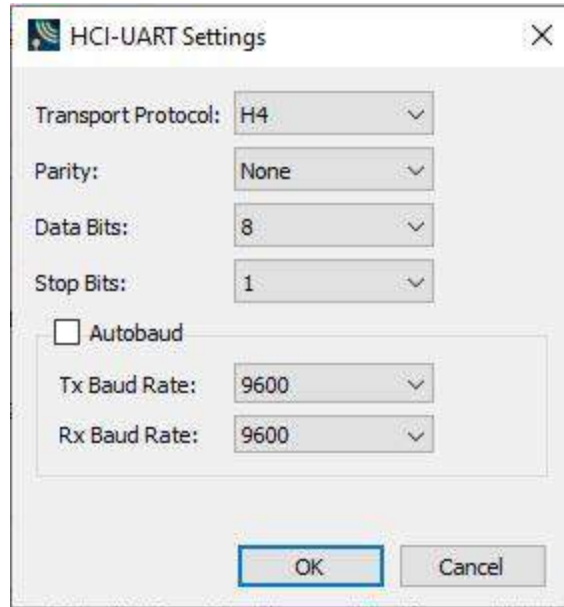


Figure 3.27 - HCI UART Settings

Table 3.13 - HCI-UART Settings

Setting	Value	Description
Transport Protocol	H4	The simplest protocol designed to operate over RS-232 with no parity in a 5-wire configuration.
	BCSP	BlueCore Serial Protocol, developed by CSR, provides a more reliable alternative to H4. The protocol is defined to run a 3-wire connection, and can optionally use a 5-wire UART connection with two flow control lines.
	3-Wire (H5)	A 3-wire protocol that provides error detection and correction.
	MWS WCI-2	The Wireless Coexistence Interface (WCI) is a full duplex UART carrying logic signals framed as UART characters.
Parity	None	No parity check occurs
	Even	The count of bits set is an even number.
	Odd	The count of bits set is an odd number.

Table 3.13 - HCI-UART Settings (continued)

Setting	Value	Description
<b>Data Bits</b>	8	The number of data bits in the expected packet.
	7	
	6	
	5	
<b>Stop Bits</b>	1	The number of data bits held in the mark (logic 1) condition at the end of the expected packet.
	1.5	
	2	
<b>Autobaud</b>		The X240 can automatically determine the baud rate of the HCI UART when the Autobaud is selected. When the Autobaud checkbox is checked in the “HCI-UART Settings” dialog box the analyzer will automatically determine the baud rate. Once a baud rate has been determined, it will be applied to both the TX and RX lines. The baud rate will be continually monitored during the capture and automatically adjusted if the baud rate of the received data changes. If Autobaud is used on multiple pods simultaneously then Autobaud will determine the baud rate of each pod independently of the other pods. Additionally, if Autobaud is being used then other pods can still use fixed baud rates. It is possible that when starting the baud search very short packets may be missed.

Table 3.13 - HCI-UART Settings (continued)

Setting	Value	Description
<b>TX Baud Rate</b>	<b>Disabled</b>	The baud rates displayed are nominal baud rates as opposed to the precise values internal to the analyzer which may differ slightly with a mean absolute average difference of less than half a percent. If autobaud is used the difference may be more depending on how much the actual baud rate differs from those listed in the table.
	<b>9,600</b>	
	<b>14,400</b>	
	<b>19,200</b>	
	<b>28,800</b>	
	<b>38,400</b>	
	<b>57,600</b>	
	<b>115,200</b>	
	<b>230,400</b>	
	<b>460,800</b>	
	<b>921,600</b>	
	<b>1,000,000</b>	
	<b>1,250,000</b>	
	<b>1,500,000</b>	
	<b>1,750,000</b>	
	<b>2,000,000</b>	
	<b>2,250,000</b>	
	<b>2,500,000</b>	
	<b>2,750,000</b>	
<b>3,000,000</b>		
<b>3,250,000</b>		
<b>3,500,000</b>		
<b>3,750,000</b>		
<b>4,000,000</b>		
<b>RX Baud Rate</b>		Same as <b>TX Baud Rate</b> .

### Wireless Filters Tab

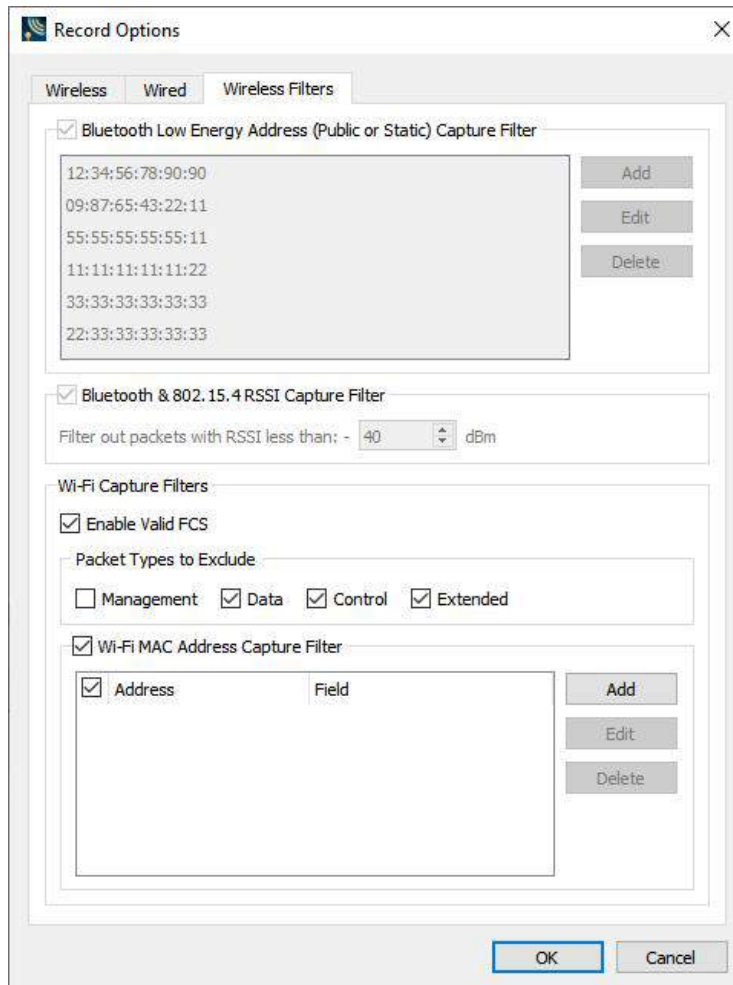
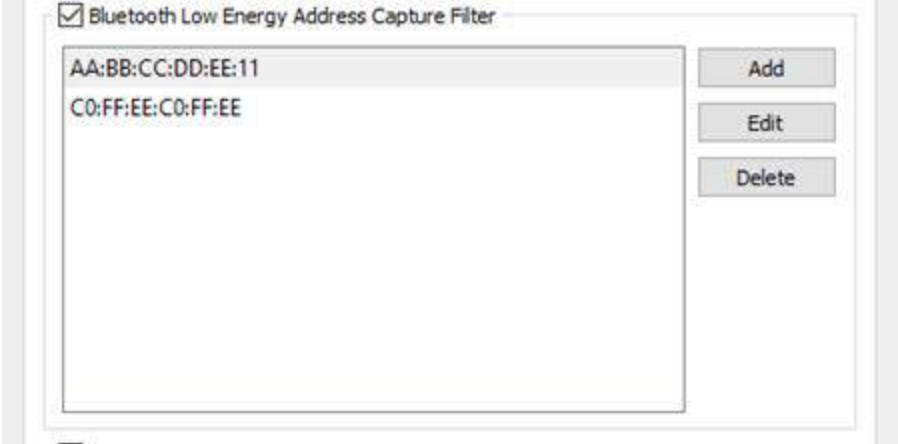



Figure 3.28 - Record Options – Wireless Filters Tab

Table 3.14 - X240 Record Options Wireless Filters Selections

Section	Description
<p><b>Bluetooth Low Energy Address Capture Filter</b></p>	<p>By enabling the Bluetooth Low Energy Address Capture Filter, only Low Energy packets from the listed Bluetooth Addresses will be processed into the capture. Addresses can be added, selected and edited, and selected and deleted by using the Add, Edit, Delete buttons respectively.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>
<p><b>RSSI Capture Filter</b></p>	<p>By enabling the RSSI Capture Filter, only those packets with RSSI greater than the entered dBm value will be processed into the capture.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>
<p><b>Wi-Fi Capture Filters</b></p>	
<p><b>Enable Valid FCS</b></p>	<p>When checked, the system only captures Wi-Fi packets with a valid checksum. This allows a user to filter out bad packets.</p>
<p><b>Packet Types to Exclude</b></p>	<p>When a type is checked, the system does not capture this type of Wi-Fi packet. This allows a user to filter out unnecessary packet types. For example, a user may only want to see Management type packets.</p>
<p><b>Wi-Fi MAC Address Capture Filter</b></p>	<p>See Wi-Fi MAC Address Filtering following this table.</p>

**Wi-Fi MAC Address Filtering**

In environments where many Wi-Fi signals can make it hard to focus analysis on only a few signals of interest, the Wi-Fi MAC Address Capture Filter options allow configuration of only the signals of interest.

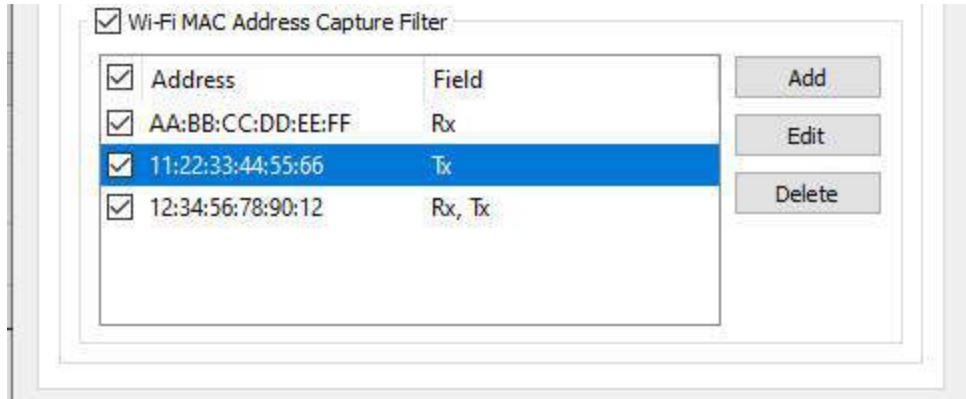


Figure 3.29 - X240 Wireless Filters Tab – Wi-Fi MAC Address Capture Filter

Table 3.15 - X240 Wi-Fi Tab MAC Address Filtering

Setting	Description
<b>Wi-Fi MAC Address Capture Filters</b>	This must be checked in order to enable the filtering of MAC Addresses on the X240. Unchecking this disables MAC Address filtering on the X240, allowing all Wi-Fi signals captured into WPS for analysis.
<b>Add</b>	Displays a dialog in which the MAC Address can be entered and controls for selecting TX/RX. See Wi-Fi MAC Address Editing following this table.
<b>Edit</b>	After selecting one of the MAC Addresses in the table, this will display a dialog in which the MAC Address and the TX/RX can be changed. See Wi-Fi MAC Address Editing following this table.
<b>Delete</b>	After selection one of the MAC Addresses in the table, this will delete that MAC Address filter.

**Wi-Fi MAC Address Editing**

The MAC Address table displays the MAC Address and the Fields which indicates whether the MAC Address is filtered by the Rx (Receive) and/or Tx (Transmit) Field in the MAC Frame.

There is an Enable checkbox for each MAC Address so that each one can be enabled or disabled for filtering.

Up to eight MAC Addresses can be entered for filtering.

To add a MAC Address, click the **Add** button. The **New Address** dialog is displayed.

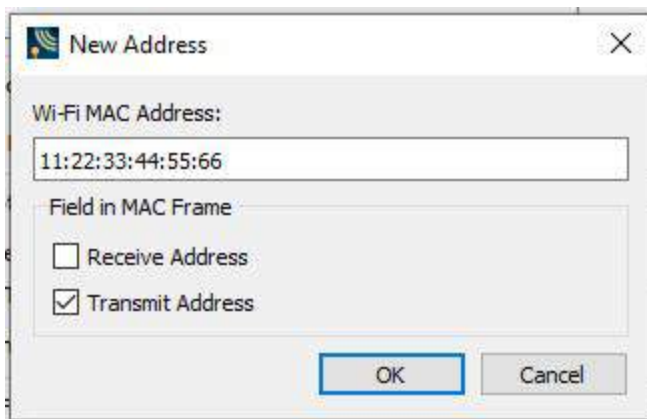


Figure 3.30 - X240 New Address dialog for a new MAC Address

Enter the MAC Address into the edit field as indicated and select whether to filter that address as Receive and/or Transmit. Click **OK** and the MAC Address will appear in the MAC Address table with its Enable checkbox checked by default.

To edit a MAC Address, click on one of the MAC Addresses in the table to select it and click the **Edit** button. The same **New Address** dialog as above will display with all the information from the table already entered. Edit then click OK. The changes to the MAC Address appear in the MAC Address table.

If the **Wi-Fi MAC Address Capture Filter** checkbox is turned off, the MAC Address filters themselves are still retained on the X240 for re-enabling later.

### 3.1.2.1.1.3 Record Options Dialog: Sodera

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

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

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

#### Wireless Tab.

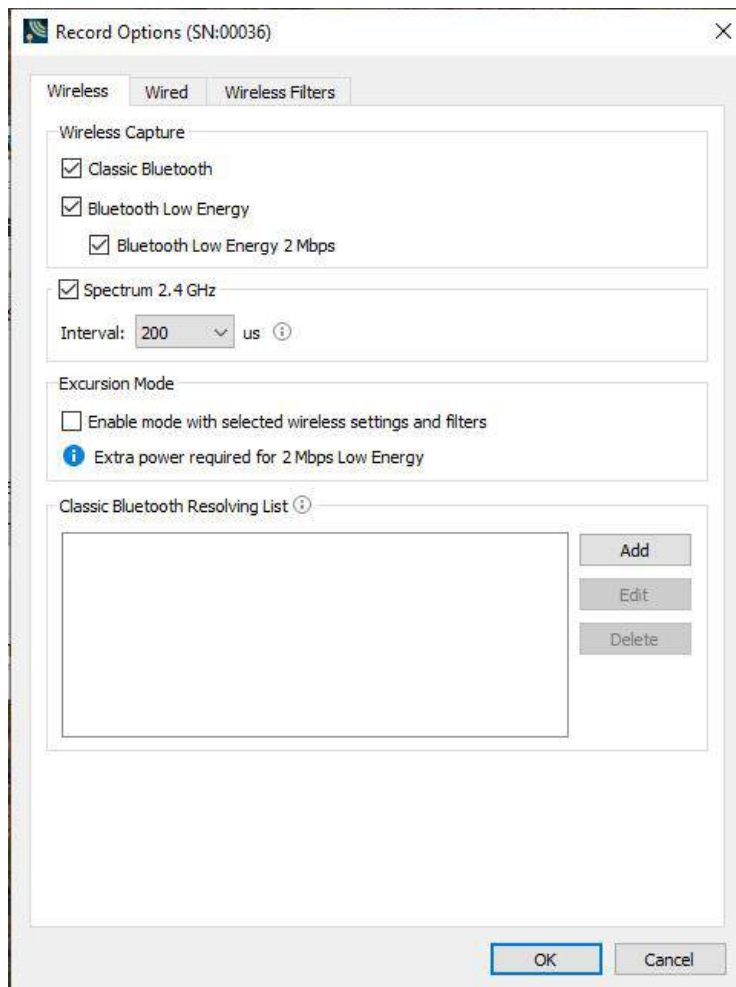
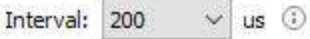


Figure 3.31 - Sodera Record Options - Wireless tab.



Table 3.16 - Soder Record Options Wireless Tab Selections

Section	Selection	Description
Wireless Capture	Classic Bluetooth	When checked, will capture data from Classic Bluetooth devices.
	Bluetooth Low Energy	When checked, will capture data from Bluetooth Low Energy devices.
	Bluetooth Low Energy 2 Mbps	When checked captures Bluetooth Low Energy 2 Mbps data rate. When this option is selected the Soder unit must be connected to an external power source. Refer to <a href="#">Applying Power on page 44</a> .
Spectrum 2.4 GHz		<p>When checked this selection provides the user with the ability to capture samples of the 2.4 GHz RF present at the Soder antenna. The spectrum data represents the RSSI and it is automatically saved when the capture is saved. It can be optionally viewed in the Coexistence View. Spectrum sampling is set at 20, 50, 100, or 200 microsecond intervals using the <b>Interval</b> control.</p>  <p>Interval: 200 us ⓘ</p> <p>Capturing spectrum data will use additional memory, and the smaller the sample interval, the more memory that is used, So when using sample rates less than 200 microseconds the Soder unit must be connected to a computer and not being used in Excursion Mode. See <a href="#">Spectrum Analysis on page 228</a> and <a href="#">Coexistence View - Spectrum on page 288</a> for more information.</p>
Excursion Mode		When <b>Excursion Mode</b> is checked the Soder hardware will support Excursion mode captures where the hardware can capture data without being connected to a computer. The configured traffic is captured for later upload and analysis using a computer running the Wireless Protocol Suite software. Refer to <a href="#">Excursion Mode on page 166</a> for more information about the Excursion Mode.
Classic Bluetooth Resolving List		This is a list of Classic Bluetooth device addresses used to resolve packet source BD_ADDRs (Bluetooth Device ADDresses) during capture. The datasource maintains a database of known device BD_ADDRs indexed on the least significant 4 bytes of the BD_ADDR – the UAP and LAP. Over time, the device database will grow and may contain multiple devices with BD_ADDRs with the same UAP and LAP. The resolving list is used to specify a known set of device BD_ADDRs that will be encountered in a capture session. This list will be checked first for matching device BD_ADDRs. Each BD_ADDR on the resolving list must have a unique value for the least significant 4 bytes of the BD_ADDR (UAP and LAP).

### Classic Bluetooth Resolving List Configuration

To add a Classic Bluetooth Device Address to the resolving list, select the “Add” button. Enter the Classic Bluetooth Address. Click OK. See figure below.

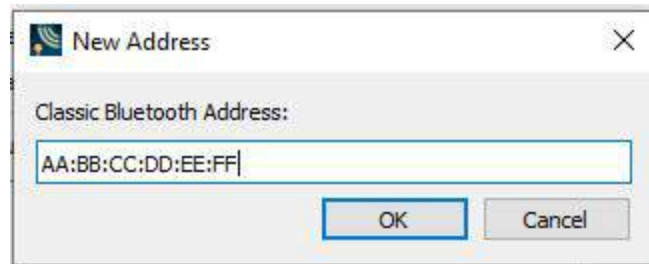


Figure 3.32 - Enter Bluetooth Address



Figure 3.33 - After Entering Bluetooth Address

To edit a Classic Bluetooth Device Address that is already on the list, select that address and click the “Edit” button. Change the address, then click **OK**.

To remove a Classic Bluetooth Device Address that is on the list, select that address and click the “Delete” button

### Wired Tab

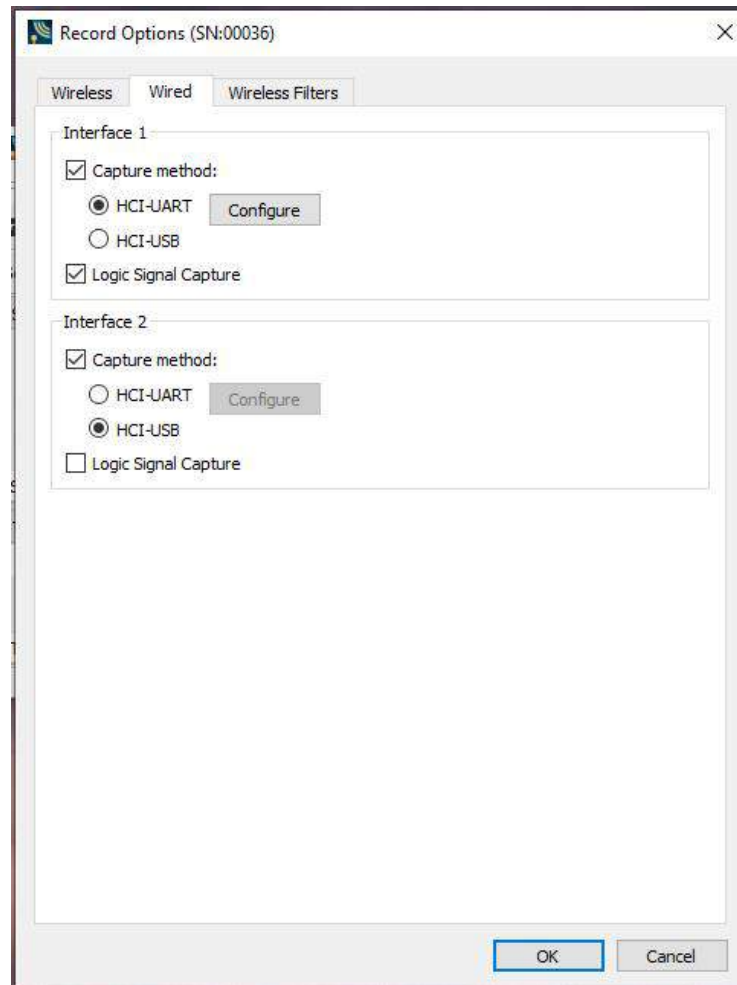


Figure 3.34 - Soderia Record Options – Wired tab

Table 3.17 - Record Options Wired Tab Selections

Section	Selection	Description
Interface 1	Capture method	Control whether or not HCI traffic on <b>POD1</b> will be captured. Available options are: <ul style="list-style-type: none"> <li>HCI-UART. See <a href="#">Connecting for HCI &amp; Logic Capture on page 52</a>. Click on the Configure button to setup the HCI-UART capture parameters for Interface 1. See HCI-UART I/O Settings following this table.</li> <li>HCI-USB. See <a href="#">Connecting for USB Capture on page 55</a>.</li> </ul>
	Logic Signal Capture	When checked, the Soderia unit HCI POD1 is configured to capture logic events. Refer to <a href="#">Logic Event Capture Configuration on page 55</a> .
Interface 2	Capture method	Control whether or not HCI traffic on <b>POD1</b> will be captured. Available options are: <ul style="list-style-type: none"> <li>HCI-UART. See <a href="#">Connecting for HCI &amp; Logic Capture on page 52</a>. Click on the Configure button to setup the HCI-UART capture parameters for Interface 1. See HCI-UART I/O Settings following this table.</li> <li>HCI-USB. See <a href="#">Connecting for USB Capture on page 55</a>.</li> </ul>
	Logic Signal Capture	When checked, the Soderia unit HCI POD2 is configured to capture logic events. Refer to <a href="#">Logic Event Capture Configuration on page 55</a> .

### HCI UART I/O Settings

After clicking on the **Configure** button, the I/O Settings for UART can be configured without an HCI pod being connected to the Soderia. When you click on the OK button the configuration information is saved, but is not stored on the Soderia hardware.

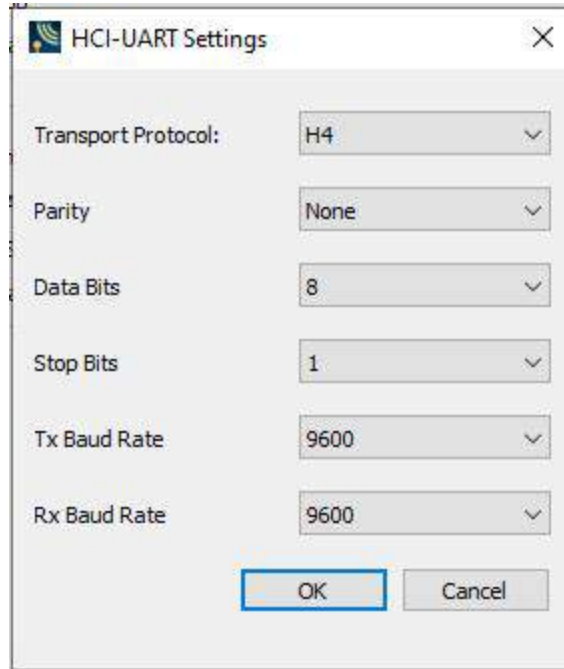


Figure 3.35 - HCI UART Settings

Table 3.18 - HCI Settings for UART

Setting	Value	Description
Transport Protocol	H4	The simplest protocol designed to operate over RS-232 with no parity in a 5-wire configuration.
	BCSP	BlueCore Serial Protocol, developed by CSR, provides a more reliable alternative to H4. The protocol is defined to run a 3-wire connection, and can optionally use a 5-wire UART connection with two flow control lines.
	3-Wire (H5)	A 3-wire protocol that provides error detection and correction.
	MWS WCI-2	The Wireless Coexistence Interface (WCI) is a full duplex UART carrying logic signals framed as UART characters.
Parity	None	No parity check occurs
	Even	The count of bits set is an even number.
	Odd	The count of bits set is an odd number.

Table 3.18 - HCI Settings for UART (continued)

Setting	Value	Description
<b>Data Bits</b>	8	The number of data bits in the expected packet.
	7	
	6	
	5	
<b>Stop Bits</b>	1	The number of data bits held in the mark (logic 1) condition at the end of the expected packet.
	1.5	
	2	
<b>TX Baud Rate</b>	<b>Disabled</b>	The baud rates displayed are nominal baud rates as opposed to the precise values internal to the analyzer which may differ slightly with a mean absolute average difference of less than half a percent. If autobaud is used the difference may be more depending on how much the actual baud rate differs from those listed in the table.
	<b>9,600</b>	
	<b>14,400</b>	
	<b>19,200</b>	
	<b>28,800</b>	
	<b>38,400</b>	
	<b>57,600</b>	
	<b>115,200</b>	
	<b>230,400</b>	
	<b>460,800</b>	
	<b>921,600</b>	
	<b>1,000,000</b>	
	<b>1,250,000</b>	
	<b>1,500,000</b>	
	<b>1,750,000</b>	
	<b>2,000,000</b>	
	<b>2,250,000</b>	
	<b>2,500,000</b>	
	<b>2,750,000</b>	
	<b>3,000,000</b>	
<b>3,250,000</b>		
<b>3,500,000</b>		
<b>3,750,000</b>		
<b>4,000,000</b>		
<b>RX Baud Rate</b>		Value selections same as <b>TX Baud Rate</b> .

### Wireless Filters Tab

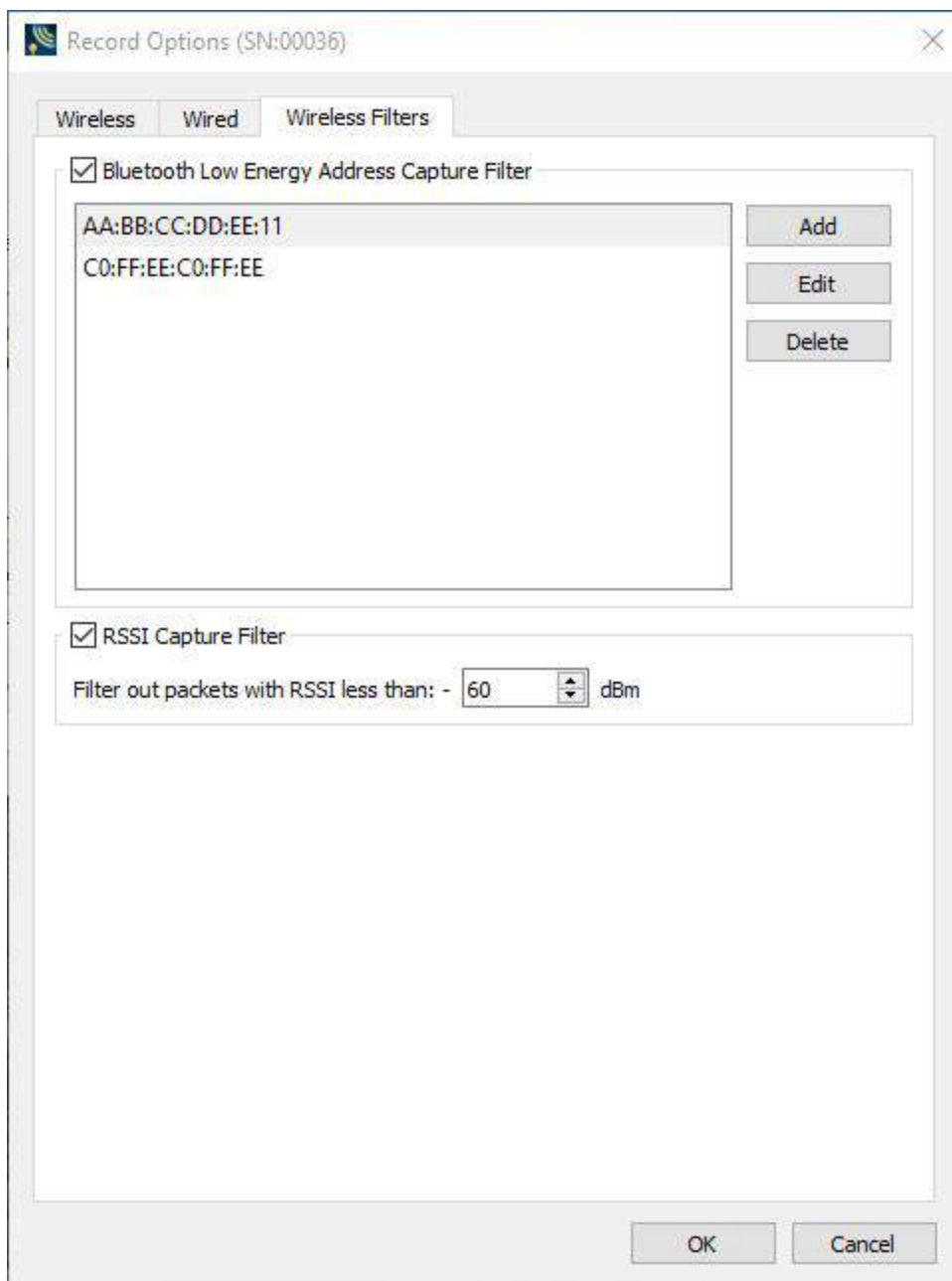
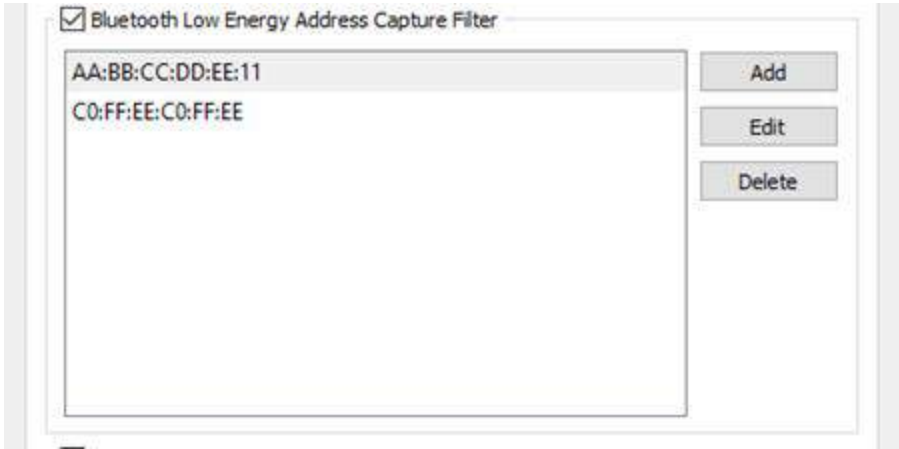



Figure 3.36 - Soderia Record Options – Wireless Filters Tab

Table 3.19 - Soderia Record Options Wireless Filters Selections

Section	Description
<p><b>Bluetooth Low Energy Address Capture Filter</b></p>	<p>By enabling the Bluetooth Low Energy Address Capture Filter, only Low Energy packets from the listed Bluetooth Addresses will be processed into the capture. Addresses can be added, selected and edited, and selected and deleted by using the Add, Edit, Delete buttons respectively.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>
<p><b>RSSI Capture Filter</b></p>	<p>By enabling the RSSI Capture Filter, only those packets with RSSI greater than the entered dBm value will be processed into the capture.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>



### 3.1.2.1.1.4 Record Options Dialog: Sodera LE

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

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

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

#### Wireless Tab

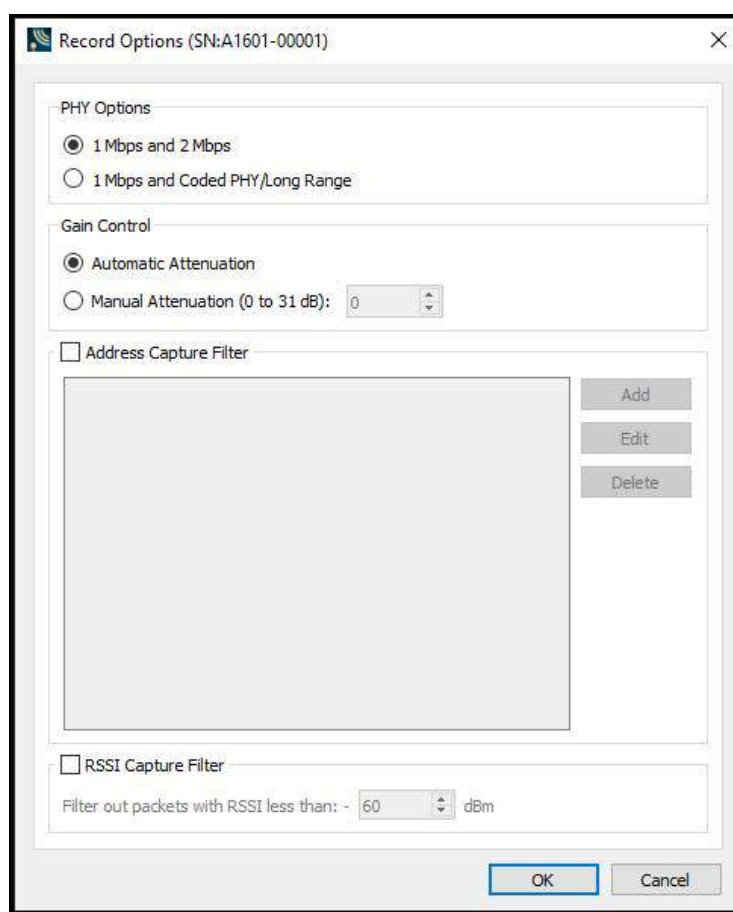


Figure 3.37 - Sodera LE Record Options - Wireless tab.

Table 3.20 - Sodera LE Record Options - Wireless Tab Selections


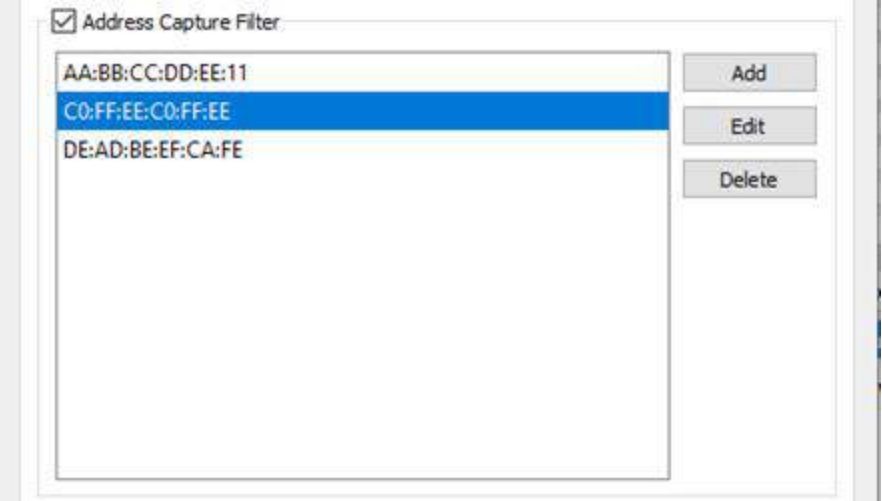

Section	Selection	Description
PHY Options	1M and 2M LE	Capture and record at 1 Mbps or 2 Mbps.
	1M and Coded PHY/Long Range LE	Allows for capture of Long Range <i>Bluetooth</i> Low Energy, also called Coded PHY. Long Range LE can only be captured with 1Mbps PHY.
Gain Control	Automatic Attenuation	The Sodera LE unit will automatically adjust the gain of the received RF signal to estimated levels suitable for effective data capture..
	Manual Attenuation	<p>Manual Selection of gain may be necessary if the capture does not provide reliable results. Attenuation can be adjusted from 0 to 31 dB in 1 dB steps. For example, in the presence of a strong Wi-Fi signal the user may have to increase the attenuation to achieve a reliable <i>Bluetooth</i> Low Energy data capture. The user should adjust the attenuation and then capture the data again. Repeat, if necessary, until a reliable data capture is achieved..</p> 
Address Capture Filter		<p>By enabling the Address Capture Filter, only packets from the listed Bluetooth Addresses will be processed into the capture. Addresses can be added, selected and edited, and selected and deleted by using the Add, Edit, Delete buttons respectively.</p> 

Table 3.20 - Soder LE Record Options - Wireless Tab Selections (continued)

Section	Selection	Description
RSSI Capture Filter		<p>By enabling the RSSI Capture Filter, only those packets with RSSI greater than the entered dBm value will be processed into the capture.</p>  <p>This filter can be useful in a crowded Bluetooth environment.</p>

### 3.1.2.2 Device Database View

The Device Database View is shown in top right corner of WPS main window. In case it was closed, the Device Database View can be open from menu View

The Device Database View provides the user with information on active, inactive, and previously detected Bluetooth devices within range of the Soder/X240 wide band receiver. The Device Database View provides information from all connected Bluetooth receivers.

Also the Device Database View gives access to Wired Devices view.

In performing analysis the user will filter the captured data by selecting which devices the Wireless Protocol Suite software will use.

The Device Database View is a list populated by wireless devices that are:

- captured devices,
- previously captured devices, or
- added by the user.

Devices are shown in a corresponding group: User-Added Devices, Captured Devices or Previously Captured Devices.

A new device/BD\_ADDR is automatically added to the Device Database View when:

- For BR/EDR, the full BD\_ADDR encapsulated in the FHS Packet is added to the Device Database View when Soder/X240 captures an FHS packet that is successfully dewhitened with the CRC checked.
- A partial BD\_ADDR—just the Lower Address Part(LAP) and Upper Address Part(UAP)—may be added when we do not observe paging such as when a conversation is already ongoing at the time capturing is started. If Soder/X240 is able to successfully dewhitene a BR/EDR packet using the payload CRC to check repeated dewhitening attempts, then the partial BD\_ADDR will be added.
- For Bluetooth Low Energy, the full BD\_ADDR is always displayed.

Added devices are retained by the Wireless Protocol Suite software. When devices are added and appear in the Device Database View they must be removed by the user or, in the case of a subsequent session, the devices will appear again. If not used in the current session the devices will be shown in or Previously Captured Devices group, otherwise it will be active and shown in Captured Devices group.

Retaining past added devices allows the user to select devices prior to starting a session with the Start Record button.

When using a .cfa(capture) file, e.g. using the Viewer, the set of devices shown will only be the devices in that capture file. All devices will be shown in Captured Devices group. Any device changes made can be saved to that file, but do not affect the “live capture” database of devices.

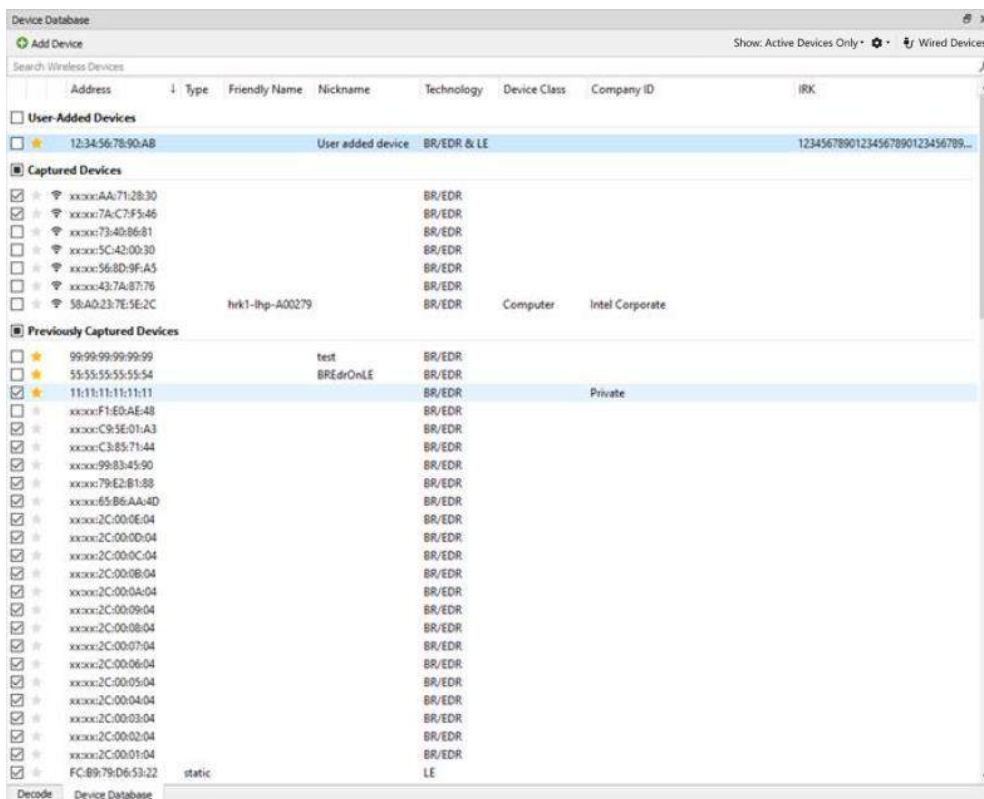


Figure 3.38 - Device Database View in Viewer Mode

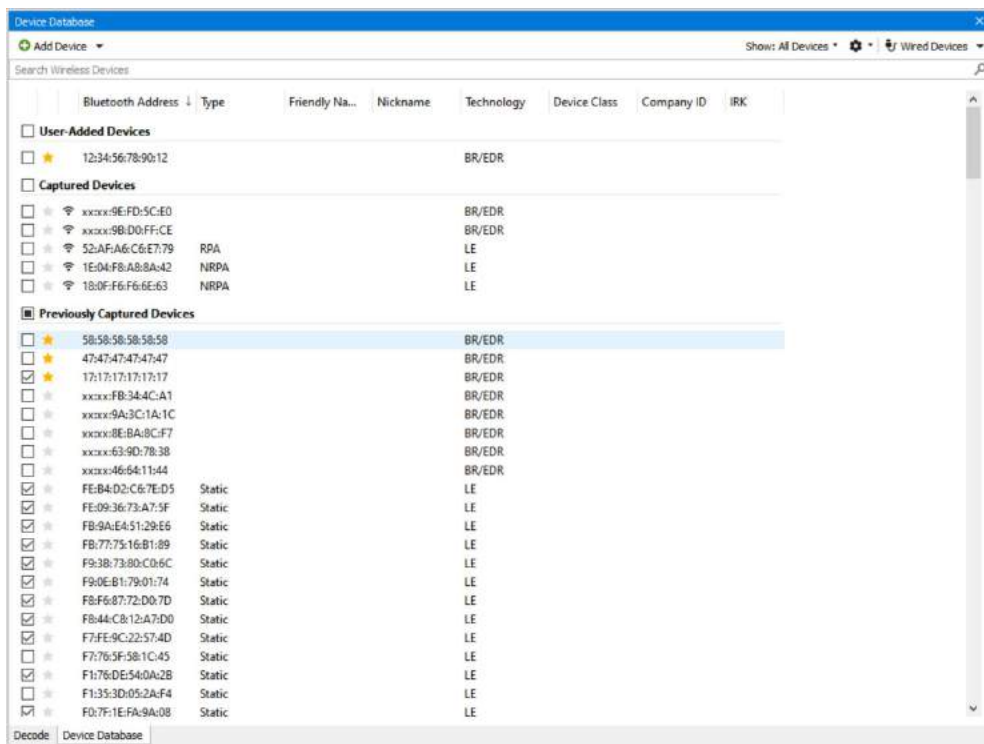


Figure 3.39 - Device Database View in Live Mode

Table 3.21 - Device Database Table Columns



Column	Description
<b>Filter Selection</b> <input type="checkbox"/> / <input checked="" type="checkbox"/>	The filter is an on/off selection. When checked, the device is selected for data analysis, that is the data is filtered into the Wireless Protocol Suite when the Standard Toolbar Start Analyze button is clicked.
<b>Favorites</b>  / 	The device's Bluetooth address.
<b>Address</b>	When a star is activated by clicking on it, the device is designated as a "favorite". A "favorite" device will have a gold star. The "favorites" serve to identify devices key to the user's analysis. Favorite devices are always displayed regardless of their active/inactive status.
<b>Type</b>	Type of the address
<b>Friendly Name</b>	The device name. This field is blank if no friendly name has been observed.
<b>Nickname</b>	The nickname allows the user to organize the display of captured devices in the Device Database and Timing Analysis panels.
<b>Technology</b>	Device technology to include one of the following. <ul style="list-style-type: none"> <li>• BR/EDR</li> <li>• Smart(LE)</li> <li>• Smart Ready (LE &amp; BR/EDR)</li> </ul>
<b>Device Class</b>	A general use-classification for the wireless device. _list the classes by Bluetooth technology.
<b>Company ID</b>	Obtained by OUI Company name.
<b>IRK</b>	Bluetooth Low Energy only, allows the user to determine which devices are actually the same physical device. The Identity Resolving Key allows peer devices to determine their identities when using random addresses to maintain privacy.

Table 3.22 - Device Classes

Class	BR/EDR	Low Energy
Audio/Video	X	
Barcode Scanner		X
Barcode Scanner		X
Blood Pressure		X
Blood Pressure: Arm		X
Blood Pressure: Wrist		X
Card Reader		X

Table 3.22 - Device Classes (continued)

<b>Class</b>	<b>BR/EDR</b>	<b>Low Energy</b>
Clock		X
Computer	X	X
Cycling		X
Cycling: Cadence Sensor		X
Cycling: Cycling Computer		X
Cycling: Power Sensor		X
Cycling: Speed Cadence Sensor		X
Cycling: Speed Sensor		X
Digital Pen		X
Digitizer Tablet		X
Display		X
Eye-Glasses		X
Gamepad		X
Glucose Meter		X
Health	X	
Heart Rate Sensor		X
Heart Rate Sensor: Heart Rate Belt		X
Human Interface Device (HID)		X
Imaging	X	
Joystick		X
Keyboard		X
Keyring		X
LAN/Network Access Point	X	
Media Player		X
Miscellaneous	X	
Mouse		X
Outdoor Sports Activity		X
Outdoor Sports: Location and Navigation Display		X
Outdoor Sports: Location and Navigation Pod		X

Table 3.22 - Device Classes (continued)

Class	BR/EDR	Low Energy
Outdoor Sports: Location Display		X
Outdoor Sports: Location Pod		X
Peripheral	X	
Phone	X	X
Pulse Oximeter		X
Pulse Oximeter: Fingertip		X
Pulse Oximeter: Wrist		X
Remote Control		X
Reserved	X	
Running Walking Sensor		X
Running Walking Sensor : On Shoe		X
Running Walking Sensor: In Shoe		X
Running Walking Sensor: On Hip		X
Sports Watch		X
Tag		X
Generic Thermometer		X
Thermometer: Ear		X
Toy	X	
Uncategorized	X	
Unknown		X
Watch		X
Wearable	X	
Weight Scale		X

### Sorting Device Database Columns

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

Clicking on the column header will initiate the sort. An arrow head will appear on the right of the column. An upward pointing arrow head indicates that the sort is in ascending order top to bottom. Clicking the column header again will toggle the sort to descending order top to bottom.

**Note:** Devices added after a sort will not appear in the last sort order, and are appended to the current list. The sort process must be repeated to place the new devices in sorted order.



Favorite devices will always be grouped together at the top of the Device Database Table in a sorted order. Non-favorite devices will appear immediately below the favorite devices in a sorted order.




### Group Checked Indication.

Each group has a checked indication.



Figure 3.40 - Group checked indication

This indication shows:

-  no devices are checked in group
-  some devices are checked in group
-  all devices are checked in group

All devices in a group can be checked/unchecked at once by clicking on a group checkbox.

### Device Management Toolbar

At the top of the Device Database View are tools for managing the devices in the View. You can add devices, hide/unhide inactive devices and search by content of any column. Also there is a button/dropdown menu to open the Wired Devices View. During Analyzing device management, Except Search Wireless Devices is not available for use.



Figure 3.41 - Devices Management Toolbar in View mode

In view mode, the Device Toolbar allows searching Wireless devices in the wireless table or opening the Wired Devices View.



Figure 3.42 - Devices Management Toolbar in Live mode

In Live mode, the Device Toolbar allows adding devices, showing All/Active devices, managing maintenance settings for inactive devices, searching Wireless devices in the wireless table, maintenance device settings, clean device database or opening a Wired Devices View.

Table 3.23 - Devices Management Tools

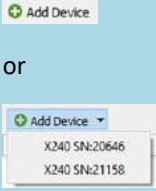

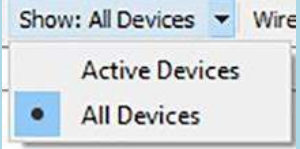

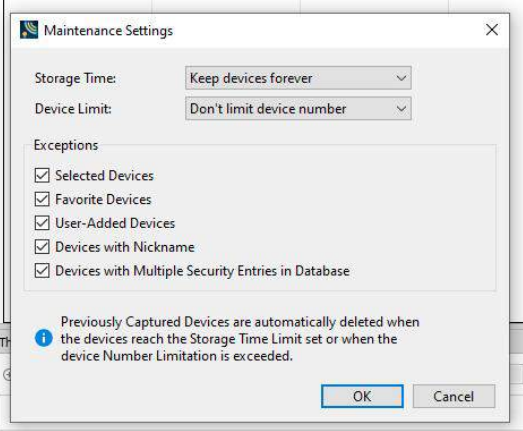

Tool	Icon/Menu	Description
Add new device		<p>Single button in single analyzer personality. Dropdown menu with possibility to choose analyzer in multi analyzer personality. Clicking this tool will open the Edit Device Details dialog. Enter the new device’s Bluetooth address and other relate data and press OK.</p>
Gear		<p>“Maintenance Settings...” opens dialog for device cleanup setting maintenance, which allows users to change Bluetooth device store capacity, storage time and device exceptions when cleaning. Cleaning is performed each time when the user closes the application or returns to the welcome screen. See Figure 3.51</p> <p>“Clean Device Database...” open dialog for starting immediately cleaning the Bluetooth device database with some device exceptions. See Figure 3.52</p>
Show All/Active devices		<p>Show All Devices. All devices are shown.</p> <p>Show Active Devices. All inactive devices are hidden. Favorite devices are always displayed without regard to their active/inactive status.</p> <p>If inactive devices are selected and the control is toggled to Hide, the selected devices are deselected.</p>
Maintenance Settings		<p>The user can manage the maintenance settings for inactive Bluetooth devices, as well as completely clear this list.</p> <p>By default, the application saves all captured devices. The user can set limits on the storage time since the capture of the device or on the device limit. In addition the user can set exceptions to these two main parameters.</p> 

Table 3.23 - Devices Management Tools (continued)

Tool	Icon/Menu	Description
Wired Devices	 <p>Wired Devices icon and menu showing a dropdown with options: SN:20646, SN:21158, SN:21217.</p>	Open Wired Devices View. In multi analyzer personality. Its need to be chosen for which analyzer Wired Device View should be opened.

### Search Wireless Devices



Figure 3.43 - Search Wireless Devices

Search wireless devices allow filtering all devices by any column, i.e. if data in any column has a match with a search string, this device will be shown in Wireless Devices Table.

Search Wireless Devices edit has a delay between inputting text and search, so the search result will be available in 0.5 seconds after the input data searching.

Data searching could be deleted by removing text or pressing the right corner of the search for this icon:



Search input has a standard text edit popup menu.



Figure 3.44 - Search input popup menu

## Edit Device Details

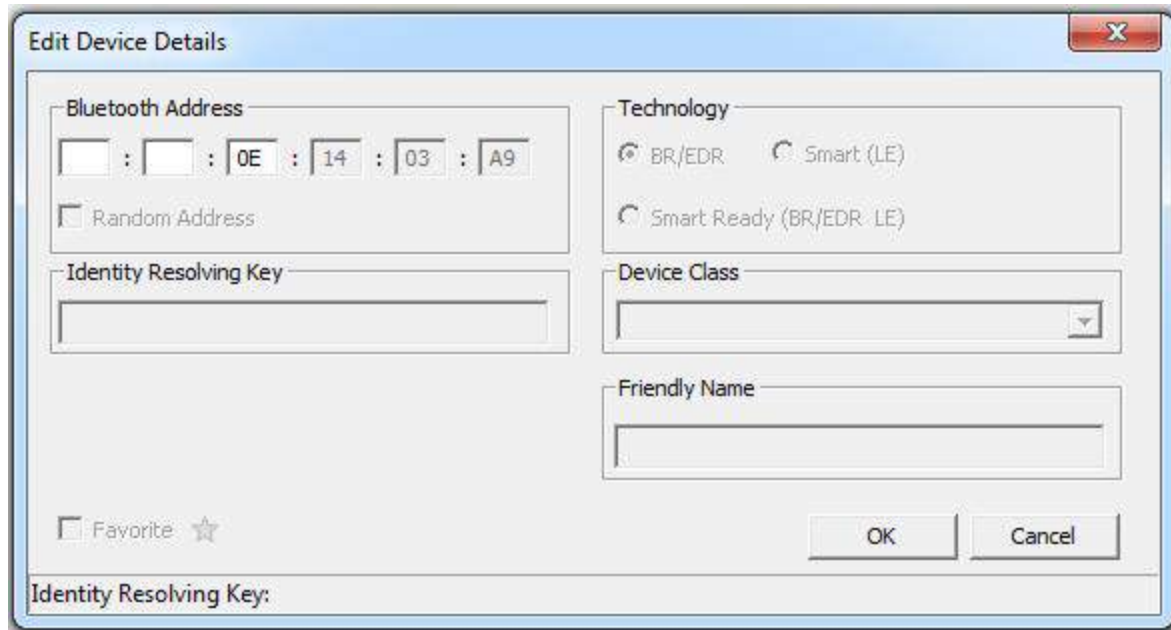



Figure 3.45 - Edit Device Details Dialog

When a device is selected in the window and the **Edit Device Details** tool  is selected, a dialog opens showing all the editable fields. Double clicking on a selected field will also open the dialog. If a dialog field is grayed-out, the field is not editable.

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

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

### Identity Resolving Key (IRK) Field:

- This field is enabled for devices with a random resolving address or public address. These devices are either Smart (LE) or Smart Ready (LE & BR/EDR) technology. The **Bluetooth Address** will be enabled and checked.
- This field is disabled if the device selected for edit has a valid IRK.
- For random resolving address, entered IRK values are validated against the BD\_ADDR. User entered IRK values are automatically reordered when the a secure connection is validated using the IRK. Refer to [Reorder Identity Resolving Key \(IRK\) on page 145](#) for details on reordering.
- Entering an invalid IRK results in an error message and the field background displays red. The **OK** button is disabled.
- Entering a valid IRK displays a green background and the **OK** button is enabled.
- Valid IRK entries are persisted to the Sodera devices database.



**Nickname Field:** User-defined name or identification, which may be useful for organizing analysis projects. The assigned nickname is also displayed next to the address in the Timing Analysis panel as well.

**Right-Click Pop-Up Menu**



After selecting a device or devices, right-clicking the mouse will open a pop-up menu that includes functions Edit Device and Delete. The menu active selections will vary depending on the status of the selected devices. For example, selecting multiple devices will inactivate the Edit devices menu selections.

Table 3.24 - Right-Click Pop-Up Menu Selections

Selection	Description
Edit device	Active when a single device has been selected. Allows the user to edit partially known BD_ADDRs, Technology type, Identity Resolving Key (IRK), Device Class and Friendly Name discovered during capture, and for entering a custom Nickname. Clicking this tool will open the Edit Device Details dialog.
Delete	<p>Deletes the selected inactive devices from the wireless devices list. Only active when inactive devices are selected. If a device is marked as a Favorite, it will not be deleted even if it is inactive. When clicked, a warning appears asking for confirmation of the action. Warning can be of two types:</p> <p>1) Single device will be removed:</p>  <p>(devices MAC address will be shown in dialog)</p> <p>2) More than one device will be removed</p>  <p>(Count of devices to remove will be shown in dialog).</p>

**3.1.2.2.1 Reorder Identity Resolving Key (IRK)**

When editing a *Bluetooth* Low Energy device from the **Device Database** table using the Edit Device Details dialog, the Wireless Protocol Suite software will automatically reorder the user entry. When the user provides an IRK that is in reverse order, the software applies the correct order when validating a secure connection using the IRK.

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

When the user enters a complete IRK in the **Identity Resolving Key** field, a validation of the reversed IRK will occur under the following conditions:

- The device BD\_ADDR is a random resolvable private address (RPA), and
- Validation of the IRK in the user-entered order has failed.

The IRK field is also enabled for *Bluetooth* Low Energy devices with public address, however automatic validation does not occur

If the reversed IRK validates successfully, the **Identity Resolving Key** field turns green and becomes inactive (read only). The status bar at the bottom of the dialog displays "Identity Resolving Key: Valid (Reordered) - Properly resolves the random address". In the Device Database pane, the IRK will now appear for the selected device with "(Reordered)" appended.

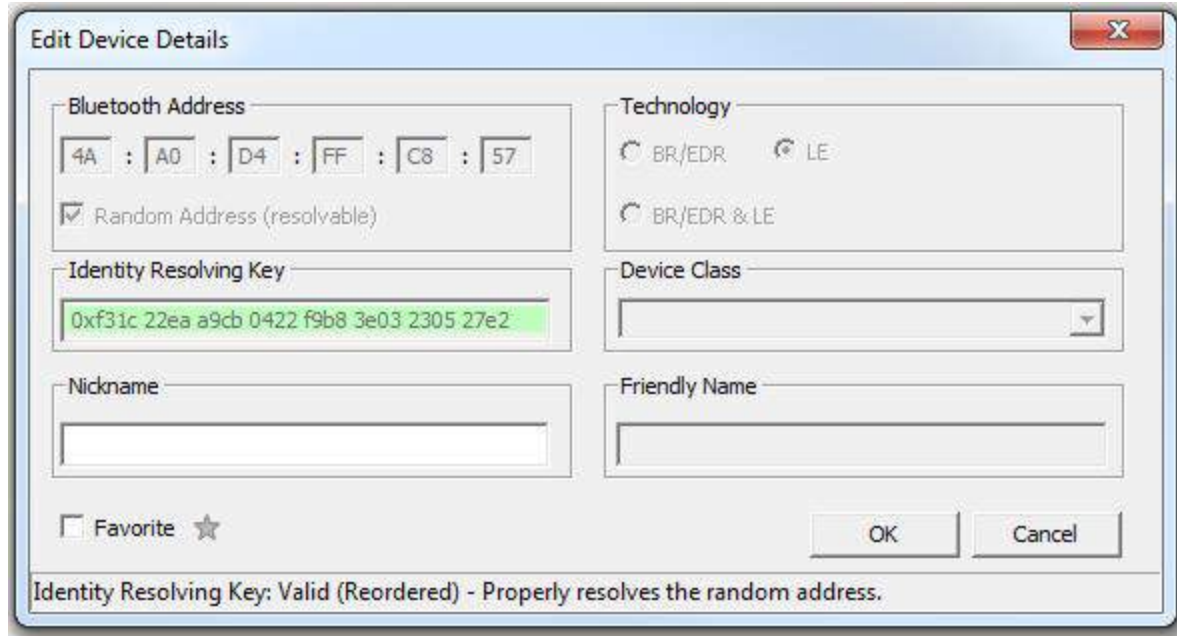


Figure 3.46 - RPA Device IRK Valid and Reordered

	BD_ADDR	Friendly Name	Nickname	Device Cla...	Technology	IRK
<input checked="" type="checkbox"/>	5C:F3:70:62:A9:BB				LE	
<input checked="" type="checkbox"/>	4A:A0:D4:FF:C8:57 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3 (Reordered)
<input checked="" type="checkbox"/>	6D:BB:28:60:92:01 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3 (Reordered)
<input checked="" type="checkbox"/>	64:2B:CD:69:F9:BE (RPA)				LE	

Figure 3.47 - RPA Wireless Device IRK Reordered and Matched

In the **Device Database** table, when the user selects a device for filtering for analysis, if that device has an IRK, other devices will also be selected if they match. Two devices match if they satisfy any of the following conditions:

- If two devices have equal IRKs, they are considered to match.
- If one device has a user-entered IRK and its BD\_ADDR is not a random resolvable private address (i.e., it is not either a public address or a random static address, and therefore the IRK cannot be validated), it matches if either its IRK is equal or the reverse of its IRK is equal to the other device.

In this next example, we have selected a device with a public address. Entering the IRK in the **Edit Device Details** dialog will indicate "Identity Resolving Key: Complete - Unable to determine if valid." and the **Identity Resolving Key** field remains white and editable but the **OK** button is active. Clicking OK closes the dialog, and the reordered IRK appears in with the public address device with "(Reordered)" appended and matching addresses will display the same reordered IRK.

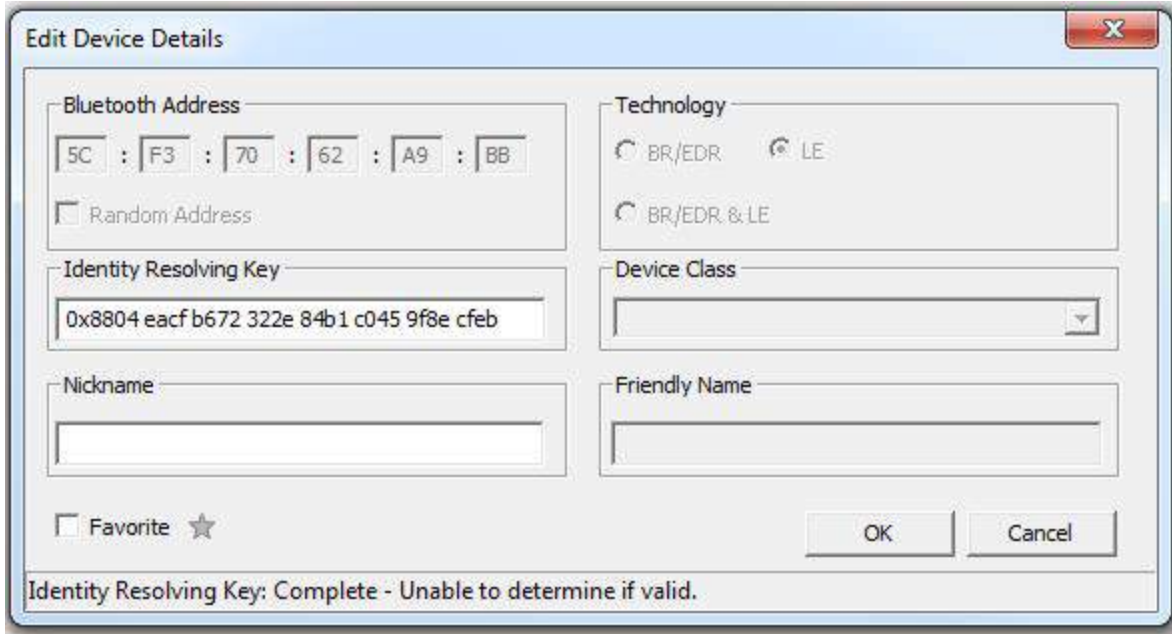


Figure 3.48 - Public Address Device IRK: Unable to Determine if Valid

	BD_ADDR	Friendly Name	Nickname	Device Class	Technology	IRK
<input checked="" type="checkbox"/>	5C:F3:70:62:A9:BB				LE	ebcf8e9f45c0b1842e3272b6cfea0488 (Reordered)
<input checked="" type="checkbox"/>	4A:A0:D4:FF:C8:57 (RPA)				LE	
<input checked="" type="checkbox"/>	6D:BB:28:60:92:01 (RPA)				LE	
<input checked="" type="checkbox"/>	64:2B:CD:69:F9:BE (RPA)				LE	ebcf8e9f45c0b1842e3272b6cfea0488 (Reordered)

Public Address Device IRK Reordered

Open the **Security** pane. In the first security context for the public address device, enter the LTK into the **Link Key** field. If valid, the IRK for the public address device will appear with "(Reordered)" removed.

Status	Time	Master	Slave	PIN / TK	Link Key
	1/20/2017 7:28:41.334597 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	n/a	0xccc768dec829ade50842ba3021df44ce
	1/20/2017 7:28:42.894620 AM				Valid
	1/20/2017 7:28:42.894620 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	Just Works	0xccc768dec829ade50842ba3021df44ce
	1/20/2017 7:28:43.236106 AM				Valid
	1/20/2017 7:28:43.333376 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	n/a	0xf08bf51a54efb35405d4f4ba07c95ea7
	1/20/2017 7:28:44.942150 AM				Valid STK
	1/20/2017 7:28:45.429657 AM	5C:F3:70:62:A9:BB	4A:A0:D4:FF:C8:57 (RPA)	n/a	0x7b230f446efe2fadaee1388ac9a53c26
	1/20/2017 7:28:46.989680 AM				Valid
	1/20/2017 7:28:47.574689 AM	64:2B:CD:69:F9:BE (RPA)	6D:BB:28:60:92:01 (RPA)	n/a	0x7b230f446efe2fadaee1388ac9a53c26
	1/20/2017 7:28:49.037211 AM				Valid

Figure 3.49 - Public Address Device: LTK Entered in Security pane to Validate IRK



	BD_ADDR	Friendly Name	Nickname	Device Class	Technology	IRK
<input checked="" type="checkbox"/>	5C:F3:70:62:A9:BB				LE	ebcf8e9f45c0b1842e3272b6cfea0488
<input checked="" type="checkbox"/>	4A:A0:D4:FF:C8:57 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3
<input checked="" type="checkbox"/>	6D:BB:28:60:92:01 (RPA)				LE	e2270523033eb8f92204cba9ea221cf3

Figure 3.50 - Public Address Device: IRK Reordered and Validated

### 3.1.2.2.2 Clean Device Database

The following section shows how to clean a device database.

#### 3.1.2.2.2.1 Clean Device Database on Start Application

In case the device store contains more than 5000 devices the application will show the dialog with suggestion to clean the device database.

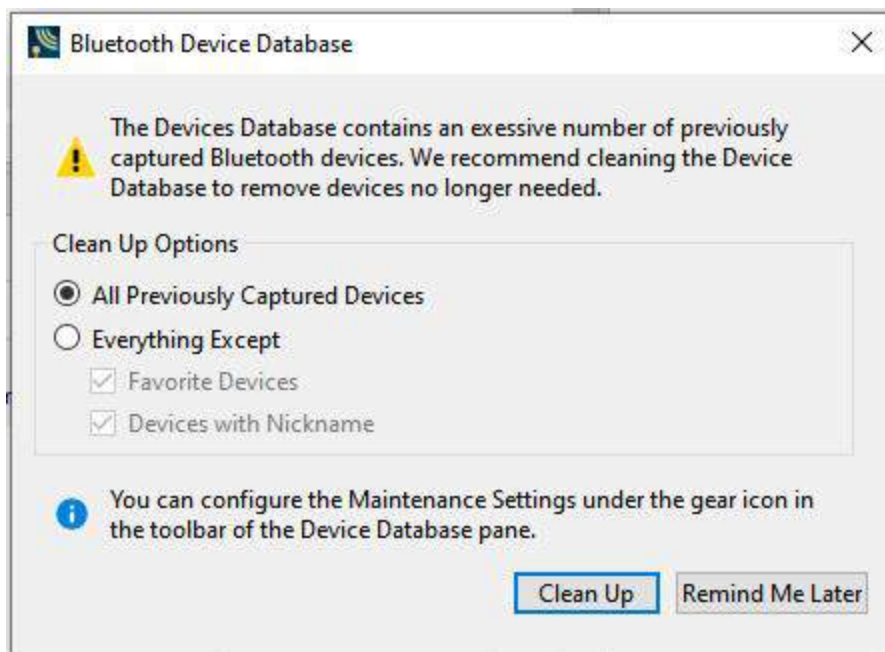


Figure 3.51 - Bluetooth device database cleanup

You can choose: cleanup all previous captured devices, cleanup all previous captured devices except Favorite Devices and/or Devices with Nickname, or leave database as is.

Using the Gear menu on Device Database toolbar you can call Maintenance Settings dialog to managing device cleanup functionality which start every time when user close WPS, file or personality.



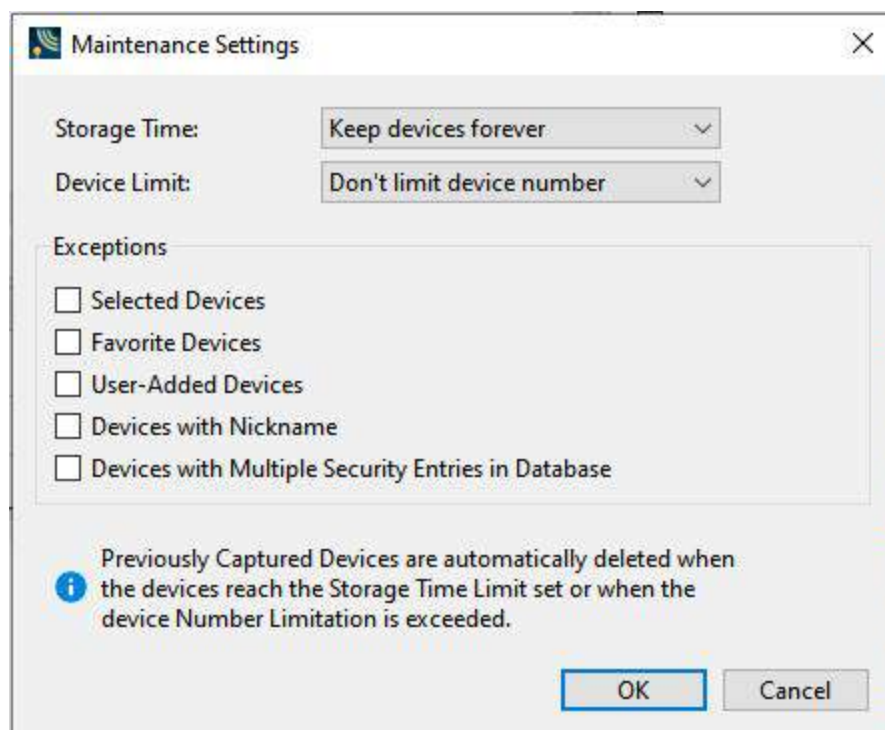


Figure 3.52 - Bluetooth device database maintenance settings

In this dialog user can choose device storage time:

- Keep devices forever – this means that devices will never be removed;
- 1 year;
- 6 months;
- 1 month;
- 2 weeks;
- 1 week
- Devices seen within the last day – this means that on exit all devices which were captured earlier than today will be removed;
- Keep current devices only – this means that on exit all devices which were captured in previous sessions will be removed.

For all choices checked exceptions will be applied.

Also user can choose limit of devices which can be stored:

- Don't limit device number
- 1000
- 500
- 250

- 100
- 50
- 25
- 10

For all choices checked exceptions will be applied.

Exceptions section allows users to except devices with specified parameters from the list of devices which should be deleted.

You can choose: cleanup all previous captured devices, cleanup all previous captured devices except Favorite Devices and/or Devices with Nickname, or leave the database as is.

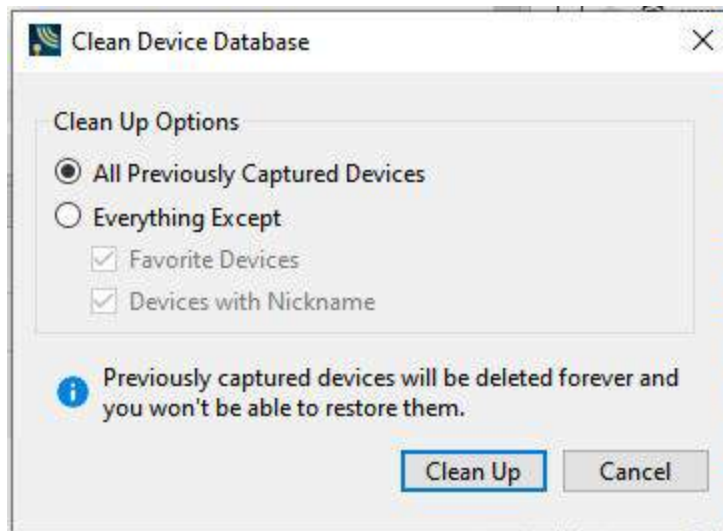


Figure 3.53 - Force Bluetooth device database cleanup

By default all devices store in Device Database without any limitations.

All changes in cleanup settings keep between WPS sessions.

### 3.1.2.3 Wired Devices View

**Note:** The **Wired Devices** View is available with Sodera and X240 hardware. The wired technologies are not supported on Sodera LE.

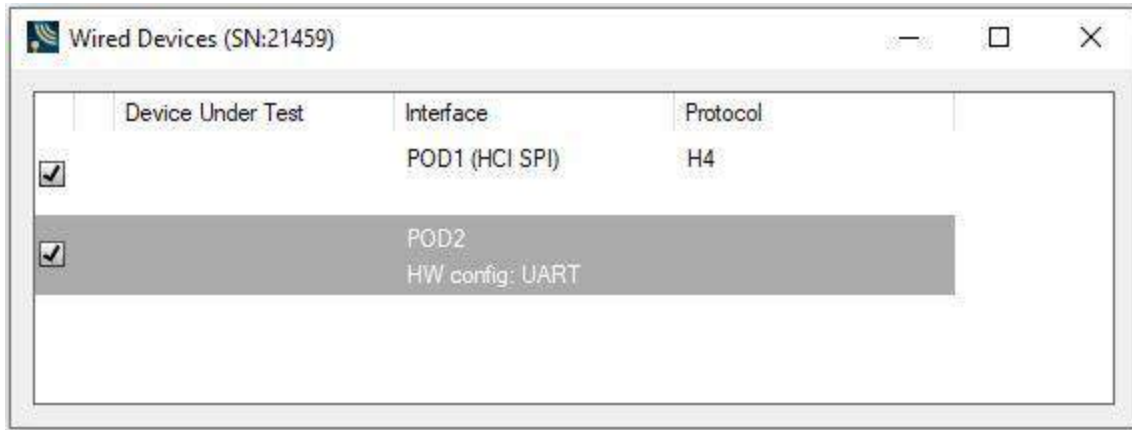


Figure 3.54 - **Wired Devices** View

The **Wired Devices** view can be opened by selecting the corresponding menu item in the **Wired Devices** menu on the **Device Database** view toolbar.

The **Wired Devices** View provides information about devices connected to **POD 1** and **POD 2**, on the bottom of the **Sodera** unit. These connectors are used to capture **Host Controller Interface** traffic through a direct wired connection. The **HCI UART** will capture **Protocol Transports H4, BCSP, and 3-wire (H5)**.

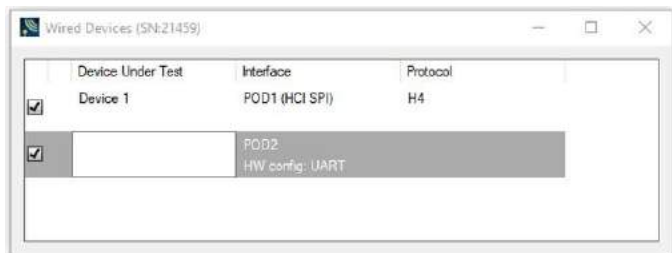
The **Wired Devices** View contains five columns. Their functions are listed below.

Table 3.25 - **Sodera Wired Devices** View Columns

Column	Description
Filter Selection <input type="checkbox"/> / <input checked="" type="checkbox"/>	The filter is an on/off selection . When checked , the device is selected for data analysis, that is the data is filtered into the <b>Frontline</b> protocol analyzer when the <b>Standard Toolbar Start Analyze</b> button is clicked.
Traffic Captured 	If the a "traffic captured" icon is present traffic has been captured that involves the device. If the icon is not present then <b>Sodera</b> has not captured any traffic that involves that device. Only wired devices with traffic captured can be used for <b>Frontline</b> protocol analysis.
<b>Device Under Test</b>	The is an area where the user can optionally document which device they were connected to at the time of the capture.
<b>Interface</b>	For each device, this column lists the <b>Sodera</b> interface connection and the protocol configured for that connection.
<b>Protocol</b>	For each device, this column lists the configured interface protocol transport.

### Naming the Device Under Test

In the **Device Under Test** column, you can optionally document which device they were connected to at the time of the capture. To do this, click in the **Device Under Test** field in a device row. Type an identifying name, and press **Enter** on the keyboard to click in another field.



For more information on configuring the wired devices, see [Analyzer Toolbar Menu and Icons on page 81](#).

### 3.1.2.4 Security View

The **Security** View is where the Wireless Protocol Suite software identifies devices with captured traffic (📶) that contain pairing, authentication, or encrypted data. The pane will show fields for entering keys, and will show if the keys are valid or invalid.

Successful decryption of captured data requires datasource receipt of all the critical packets and either :

- be given the link key by the user, or
- observe the pairing process and determine the link key.

See [Critical Packets and Information for Decryption on page 230](#) for a description of the critical packets. The **Security** View will identify the type of key required for decryption.



Figure 3.55 - Security View

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



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

Icon	Description
	Pairing/Authentication attempt observed but was unsuccessful
	Devices successfully Paired/Authenticated.
	Encrypted: traffic is encrypted but there is insufficient information to decrypt. See <a href="#">Critical Packets and Information for Decryption on page 230</a> for a description of the critical packets.
	Decrypted

- **Time:** Beginning and end time of the security context. No end time is indicated by an "...". Beginning time is shown in the first row of the grouping. End time is shown in the second row.
- **Central and Peripheral:** The BD\_ADDR of the Central and Peripheral (central and central) device in the link. If the friendly name is available it will show on the second line.

- **PIN/TK:**
  - Classic *Bluetooth*<sup>®</sup> :
    - Legacy Pairing PIN: 1 to 16 alphanumeric character PIN
  - Bluetooth Low Energy
    - PIN: 6 digit numeric passkey (000000 - 999999)
    - Out-of-Band Temporary Key (OOB TK): 32 digit hexadecimal number
- **Link Key**
  - Classic *Bluetooth*<sup>®</sup> , 32 digit hexadecimal number
  - Bluetooth Low Energy, 32 digit hexadecimal number
  - The **Link Key** cell displays "*Enter link key*" in gray when the link key is unknown. When a link is invalid the cell has a light red background and indented gray text under the link key says "*Invalid*". When a link key is valid the cell has a light green background and indented gray text under the link key says "*Valid*" (if the link key was transformed from the entered link key the text is "*Valid (Reordered)*").
  - If Soderia is Analyzing and a link key has not been entered, "Stop analyzing to enter link key" appears in the device **Link Key** cell. Click the **Stop Analyze** button to stop the analysis, and type or paste in the link key.
  - Users can enter the device security information by typing directly on the device fields **PIN/TK** and **Link Key**. An invalid entry will display a red background and a warning **Invalid**.
- **ACO:** Authenticated Ciphering Offset is used by the devices for generation of the encryption key in Classic *Bluetooth*.
- **IV:** Initialization Vector is displayed for both *Bluetooth* Low Energy encryption and Classic *Bluetooth* Secure Connections/AES encryption.. The central will use the IV in starting the encrypted communications.

**Security View Toolbar**

The **Security** View toolbar appears at the top of the pane. The **Security** View Toolbar items are described below.

Table 3.26 - **Security View** View Toolbar



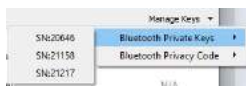

Menu	Description
	<p>Available in the multiple analyzers mode. All analyzers or analyzer by serial number items can be selected. In case item with analyzer serial number is selected, the security contexts associated with this analyzer will be shown. In case "All Analyzers" item is selected all available security contexts will be shown.</p>

Table 3.26 - Security View View Toolbar (continued)

Menu	Description
	<p>The default state of the tool is “Selected devices only”, shows available security information for selected active devices in the Wireless Devices table. In case the state was changed, the new state will be saved between sessions. When the tool is clicked, that is active, only the available Security View only shows the security context associated with the wireless devices that have been selected for analysis. Should device selection change by selecting or deselecting devices, the Security View display will change with the device context.</p>
 <p>Or</p> 	<p>Manage Keys menu can be used for Bluetooth Privacy Code and Bluetooth Private Key windows opening. For multiple analyzers mode submenu with analyzer serial number should be used for appropriate window opening.</p>

Users can select Bluetooth devices to filter data in Summary pane from the Bluetooth Security pane by using the right click menu item “Start Analyzing these Devices”. This will allow selecting devices in the Bluetooth Device Database automatically.



Figure 3.56 - Start analyzing using context menu

### 3.1.2.4.1 Classic *Bluetooth* Encryption and Decryption

**Note:** This section is not applicable to Soder LE analyzer as it support LE technology only.

To decrypt a Classic *Bluetooth* link there are two options in the **Security** pane.

1. PIN : Enter into the **PIN/TK** field; legacy pairing only.

**Note:** The only time a PIN can be used is when the datasource has captured Legacy Pairing in the current trace. The datasource uses information transferred during the Legacy Pairing process to calculate a Link Key.

2. Link Key: Enter into the **Link Key** field.

#### Passkey/PIN

The first option uses a PIN to generate the Link Key. If the analyzer is given the PIN and has observed complete pairing it can determine the Link Key. Since the analyzer also needs other information exchanged between the

two devices, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

The **PIN/TK** can be up to a maximum of 16 alphanumeric ASCII characters or a hexadecimal value that the user enters. When entering a hexadecimal value it must include a "0x" prefix, for example, "0x1234ABCD".

### Link Key

If you know the Link Key in advance you may enter it directly. To enter the [Link Key](#) click on the device row **Link Key** field and enter the Link Key in hex followed by the keyboard Enter key. If the link key has previously been entered it is automatically entered in the edit box after the Central and Peripheral have been selected. Once the Link Key is entered the ACO automatically appears in the **Security** pane for the devices in the link.

**Note:** The Link Key does not have to be prefixed with "0x" because the Link Key field will only accept hex format, and the "0x" prefix is added automatically. Entering "0x..." will result in an invalid entry result.

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
4/2/2021 11:47:56.907...	F0:5C:77:F4:61:0E	N/A			N/A
4/2/2021 11:48:38.244...	"Bose QuietComfort 35 Series II" 4C:87:...				
4/2/2021 11:48:53.960...	"Bose QuietComfort 35 Series II" 4C:87:... Enter Peripheral Address	N/A	Missing Peripheral Address		N/A

Figure 3.57 - Classic Bluetooth Link Key Entry

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
4/2/2021 11:47:56.907...	F0:5C:77:F4:61:0E	N/A	0x3A84E5F50C59862195FC1A5A01B51E87	0x84E8:82E3:E...	N/A
4/2/2021 11:48:38.244...	"Bose QuietComfort 35 Series II" 4C:87:...				
4/2/2021 11:48:53.960...	"Bose QuietComfort 35 Series II" 4C:87:... F0:5C:77:F4:61:0E	N/A	0x3A84E5F50C59862195FC1A5A01B51E87	0x5A39:09BA:...	N/A

Figure 3.58 - Classic Bluetooth Valid Link Key Entered and ACO Automatically Calculated

If the Link Key is correct the **Link Key** field for the devices in the encrypted link will appear green with "valid" below the link key. If the Link Key is not correct the **Link Key** field will appear red with "invalid" below the link key. To re-enter the Link Key click on the **Link Key** field and follow the procedure above.

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
3/14/2017 2:34:13.0285...	"Skip's CSR8510 A10" 00:1A:7D:11:11:11	N/A	0x11111111111111111111111111111111		N/A
3/14/2017 2:35:22.7488...	xxxxxx:7D:DA:71:09				
3/14/2017 2:36:47.9855...	"Skip's CSR8510 A10" 00:1A:7D:11:11:11	N/A	0x1212EEEE33333333333333311		N/A
3/14/2017 2:37:55.5995...	xxxxxx:7D:DA:71:09				

Figure 3.59 - Classic Bluetooth Invalid Link Key Entered

### SSP Debug Mode

If one of the *Bluetooth* devices is in SSP Debug Mode then the Wireless Protocol Suite software in the Soderia analyzer can automatically figure out the Link Key, under certain conditions. To obtain the information for figuring



out the Link Key, the software must actively observe the SSP pairing process in the capture. If the SSP pairing previously took place and encrypted data is later captured the software does not have the necessary information to figure out the Link Key. The only alternatives are

- to again pair the devices in SSP Debug Mode, or
- to independently determine the Link Key and enter it directly.

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

If the Bluetooth devices do not allow Debug Mode activation, enter the Link Key as described above.

### 3.1.2.4.2 Bluetooth Low Energy Encryption and Decryption

#### Long Term Key

The Long Term Key (LTK) in *Bluetooth* Low Energy is similar to the Link Key in Classic Bluetooth. It is a persistent key that is stored in both devices and used to derive a fresh encryption key each time the devices go encrypted. In the Soder Security pane the LTK is entered in the **Link Key** field so the following discussion will use Link Key instead of LTK.



Figure 3.60 - Bluetooth Low Energy Static Address Link Key Required

In this example a Low Energy device requires Link Key entry for the Wireless Protocol Suite software to decrypt the data. To enter the Link Key click on **Enter link key** and type or paste in the Link Key in hex format.

**Note:** It is not necessary to precede the Link Key with "0x" to signify a hex format. The software will automatically add "0x" to the front of the Link Key.

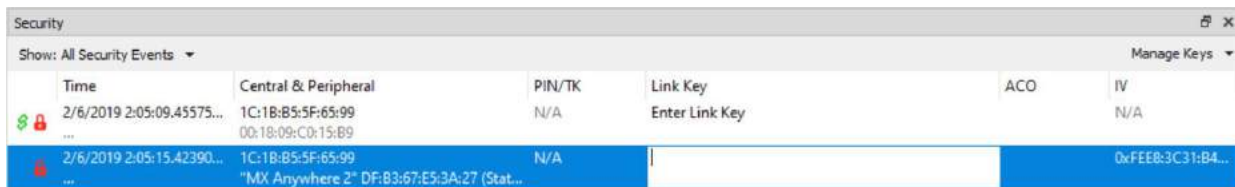


Figure 3.61 - Bluetooth Low Energy Enter Link Key

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



If the Link Key is not valid the box will be red, beneath the entered Link Key will appear "Invalid", and the Status will show a closed, red lock indicating that decryption is not enabled.

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
9/22/2020 11:49:36.7770...	3C:F7:A4:A5:46:EE "WH-CH400" 00:18:09:C0:15:B9	N/A	Enter Link Key		N/A
9/22/2020 11:49:11.1302...	57:CB:1B:2B:C7:7D (RPA) "MX Anywhere 2" DF:B3:67:E5:3A:3D (Static)	N/A	0xCCC768DEC829ADE50842BA3021DF44CE		0x4DFC:9404:A2...

Figure 3.62 - Bluetooth Low Energy Valid Link Key

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
9/22/2020 11:49:36.7770...	3C:F7:A4:A5:46:EE "WH-CH400" 00:18:09:C0:15:B9	N/A	Enter Link Key		N/A
9/22/2020 11:49:11.1302...	57:CB:1B:2B:C7:7D (RPA) "MX Anywhere 2" DF:B3:67:E5:3A:3D (Static)	N/A	0xCCC768DEC829ADE50842BA3021DF44C1		0x4DFC:9404:A2...

Figure 3.63 - Bluetooth Low Energy Invalid Link Key

### Legacy Just Works Pairing

In this example the devices under test use Legacy Just Works pairing to calculate a Short-Term Key (STK) in order to securely transfer the device's Long-Term Key (LTK). The LTK is then used to encrypt the subsequent security contexts.

Time	Central & Peripheral	PIN/TK	Link Key	ACO	IV
4/6/2021 3:11:12.9476...	80:7A:BF:1A:BF:99	Just Works	0xD81A6D1777CAA534933F6C8FCFE013B0	0xDA8D:45C9...	N/A
4/6/2021 3:12:12.7106...	"Samsung WEP460" D4:88:90:81:88:CE				

Figure 3.64 - Bluetooth Low Energy Piconet Public Key and Private Key Encryption

### Legacy Passkey Pairing

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

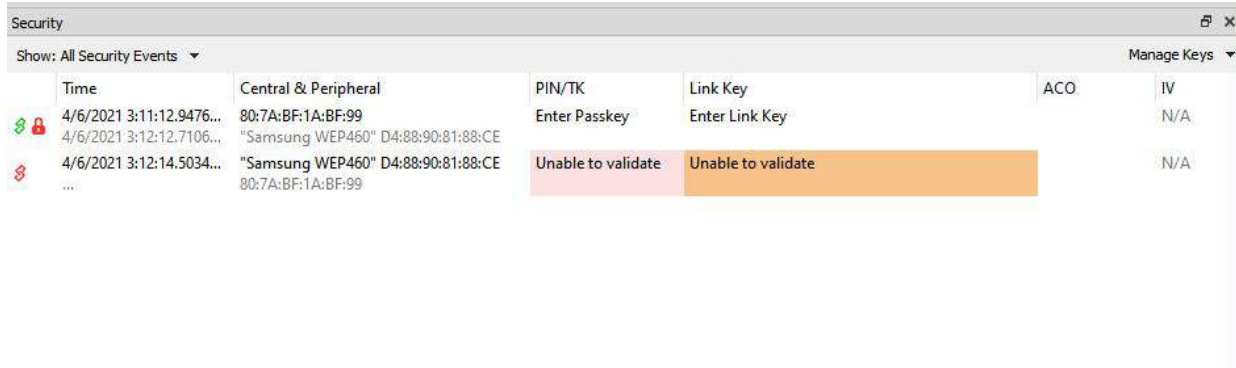


Figure 3.65 - Bluetooth Low Energy Passkey Decryption Not Enabled

This example uses Passkey Pairing to enable decryption. The user clicks on "Enter passkey" in the device **PIN/TK** field.

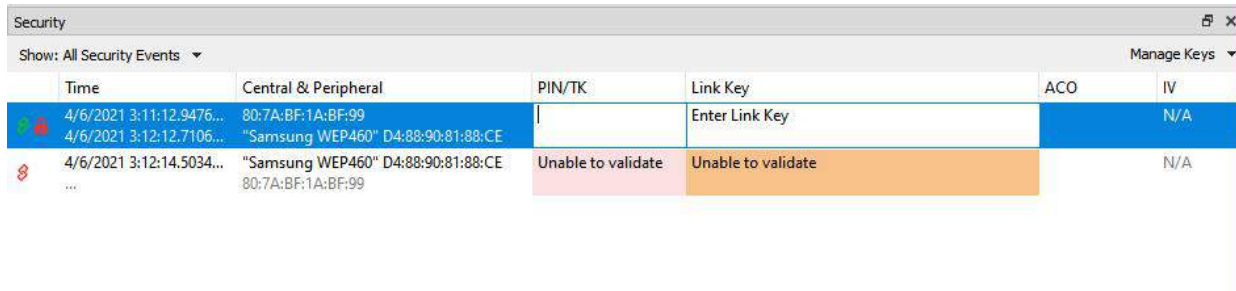


Figure 3.66 - Bluetooth Low Energy Passkey Entry

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

If the entered Passkey is incorrect, the **PIN/TK** field will be red and "Invalid" will appear below the entered PIN. The **Status** field will show a closed, red lock to indicate that encryption is not enabled.

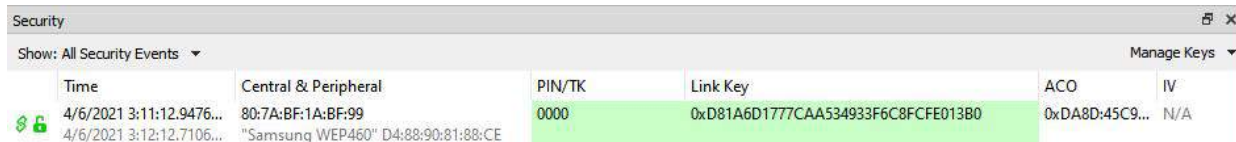


Figure 3.67 - Bluetooth Low Energy Passkey Decryption Enabled



Figure 3.68 - Bluetooth Low Energy Passkey Invalid

### Legacy Out-of-Band(OOB) Pairing

Out-of-Band (OOB) data is a 16-digit hexadecimal code preceded by "0x" which the devices exchange via a channel that is different than the le transmission itself. This channel is called OOB. For off-the-shelf devices we cannot sniff OOB data, but in the lab you may have access to the data exchanged through this channel.

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

#### 3.1.2.5 Private Keys View

For Soderia captures that include Bluetooth Low Energy Secure Connections Pairing between one or more pairs of devices, users will be able to manually enter Private Keys for both legacy and Secure Connections. The Private/Public keys are stored for use by discovered *Bluetooth* Low Energy devices. Duplicate keys cannot be stored.

When Debug key is not used during pairing, the datasource will look for a matching Public key in the set of Private/Public key pairs. If a match is found, the datasource will use the corresponding Private Key to compute the Diffie-Hellman Key.

The Private Keys pane can be viewed or hidden from the **View** menu and can be docked like the other optionally viewable panes. While operating in live mode, Private Keys are saved to persistent storage when the **Wireless Protocol Suite Soderia** window is closed . When the window is opened while in live mode, saved Private Keys are loaded from persistent storage.



Figure 3.69 - Private Keys View

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

Table 3.27 - Private Keys Pane Columns

Column	Description
Key Type	P192 if the key is used for Legacy pairing. P256 if the key is used for Secure Connection pairing.

Table 3.27 - Private Keys Pane Columns(continued)

Column	Description
Private Key	The key entered by the user. 24 octets for P192 (Legacy) 32 octets for P256 (Secure Connection)
Public Key	The two parts of the public key automatically generated when the complete Private Key is entered. X - the first half of the Public Key y - the second half of the Public Key

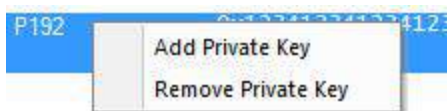
**Private Key management tools**



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

Table 3.28 - Private Keys Management Tools

Tool	Icon	Description
Add Private Key		Used to add a Private Key to the pane. When clicked, it opens the <b>Private Keys Entry</b> dialog. See <a href="#">Private Key Entry dialog on page 160</a>
Edit Selected Private Key		Enabled when a private key in the pane is selected. When clicked, it opens the <b>Private Keys Entry</b> dialog with the selected Private and Public Key filled in. See <a href="#">Private Key Entry dialog on page 160</a>
Reverse Private Key		Enabled with a private key in the pane is selected. When checked, it allows the user to switch between big endian and little endian format. The public key will be updated to reflect the changes made to the private key.
Remove Private Key		Enabled when a private key in the pane is selected. When clicked the selected key row is removed from the pane.



Right-clicking on a selected Private Key entry in the pane or right clicking anywhere in the pane will open a Private Key Management tools menu. The menu selections perform the same functions as the Private Key Management tools.

**Private Key Entry dialog**

The **Private Key Entry** dialog opens when the user selects **Add Private Key** from the **Private Keys** Management Tools or from the right-click menu.

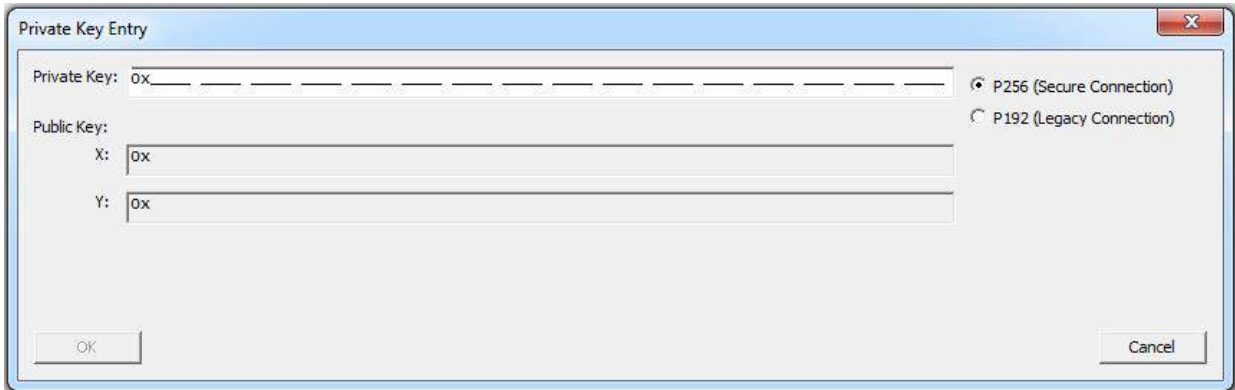
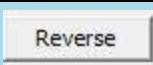


Figure 3.70 - Private Key Entry Dialog

Table 3.29 - Private Key Entry Dialog Fields

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

To Add  a Private Key:

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


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

The **Private Key** may also be pasted in. The copied key pasted in may have been in either big endian or little endian format. The **Reverse** button allows the user to reverse the format for use with their particular device.

3. Once the **Private Key** field is completely filled in, the **Public Key X:** and **Y:** fields are automatically calculated and filled in.
4. Click the **OK** button, the dialog will close, and the added Private and Public keys appear in the **Private Keys** pane.

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

To Remove  a Private Key:

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

### 3.1.2.6 Bluetooth Privacy Codes View

For captures that include encrypted Broadcast Isochronous Streams, the Bluetooth Privacy Code used to decrypt the packets in the streams can be entered on the **Bluetooth Privacy Codes** View. The **Bluetooth Privacy Codes** View can be viewed or hidden from the **View** menu and can be docked like the other optionally viewable panes. While operating in live mode, Bluetooth Privacy Codes are saved to persistent storage when the **Wireless Protocol Suite** window is closed. When the window is opened while in live mode, saved Bluetooth Privacy Codes are loaded from persistent storage.

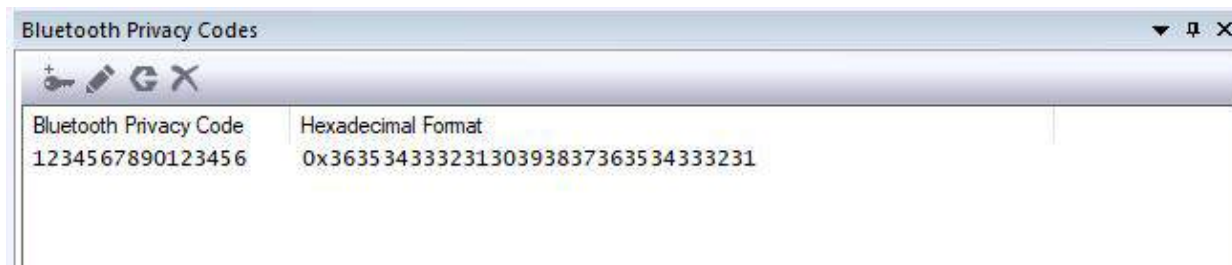


Figure 3.71 - **Bluetooth Privacy Codes** View

The **Bluetooth Privacy Codes** View has two columns that list one entry for each privacy code. Currently, only one code can be entered.

Table 3.30 - **Bluetooth Privacy Codes** View Columns

Column	Description
<b>Bluetooth Privacy Code</b>	UTF-8 character representation of the code
<b>Hexadecimal Format</b>	Hexadecimal representation of the code

The Bluetooth Privacy Code can be between 4 and 16 octets and represented as UTF-8 characters and in hexadecimal format.

**Bluetooth Privacy Code management tools**



In the header of the **Bluetooth Privacy Codes** View is a toolbar for adding or deleting codes.

Table 3.31 - Bluetooth Privacy Codes Management Tools

Tool	Icon	Description
Add Bluetooth Privacy Code		Used to add a Bluetooth Privacy Code to the View. When checked, it opens the Add Bluetooth Privacy Code dialog. See Add Bluetooth Privacy Code dialog below.  Currently only one Bluetooth Privacy Code can be entered.. To add anew code, select the current code and remove it. The <b>Add</b> button will become active and a new code can be entered.
Edit Selected Bluetooth Privacy Code		Enabled when a Bluetooth Privacy Code in the View is selected. When clicked, it opens the <b>Add Bluetooth Privacy Code</b> dialog with the selected Bluetooth Privacy Code and hexadecimal filled in. See <b>Add Bluetooth Privacy</b> dialog below.
<b>Reverse Selected Bluetooth Privacy Code</b>		Enabled when a Bluetooth Privacy Code in the View is selected. When checked, it reverses the content of the code. (EX: A-BCDE becomes EDCB-A when reversed.) Both fields of the selected code in the View are updated to reflect the change.
Remove Bluetooth Privacy Code		Enabled when a Bluetooth Privacy Code in the View is selected. When checked, the selected code row is removed from the View.

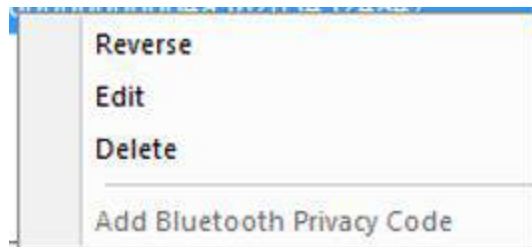


Figure 3.72 - Right Click Bluetooth Privacy Codes Management Tools Pop-Up



Right Clicking on a selected Bluetooth Privacy Code entry in the View or right clicking anywhere in the View will open a Bluetooth Privacy Code management tools menu. The Menu selections perform the same functions as the Bluetooth Privacy Code Management Tools.

### Add Bluetooth Privacy Code dialog

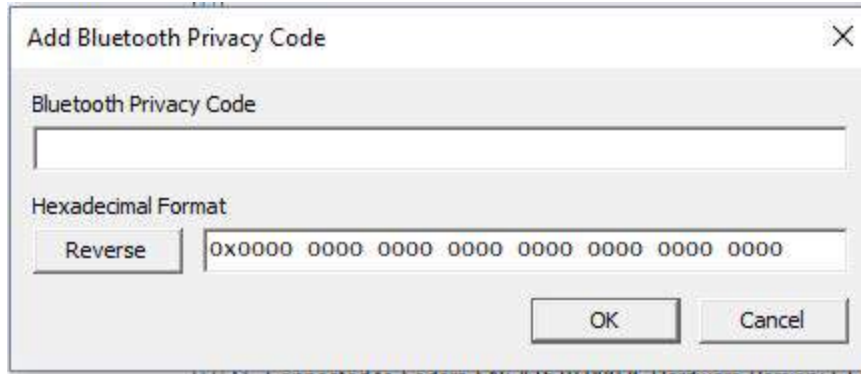






Figure 3.73 - Add Bluetooth Privacy Code Dialog

Table 3.32 - Add Bluetooth Privacy Code Dialog Fields


Section	Field	Description
Bluetooth Privacy Code	Bluetooth Privacy Code	Enter the Bluetooth Privacy Code in text.
Hexadecimal Format		Enter the Bluetooth Privacy Code in hexadecimal.
	Reverse	Allows the user to reverse the Bluetooth Privacy Code (ex: A-BCDE becomes EDCB-A when reversed.) Both fields will be updated to reflect the changes.


To Add  a bluetooth Privacy Code:

1. If a Bluetooth Privacy Code already exists, select it and click the **Remove** button .
2. Click the **Add**  button.
3. Enter the Bluetooth Privacy Code in either the **Bluetooth Privacy Code** field or the **Hexadecimal Format** field of the **Add Bluetooth Privacy Code** dialog.
4. Click the **OK** button, the dialog will close, and the added code will appear in the **Bluetooth Privacy Codes** View.

To Remove  a Bluetooth Privacy Code:



1. Select a Bluetooth Privacy Code row in the **Bluetooth Privacy Codes** View.
2. Click the **Remove**  button.
3. The Bluetooth Privacy Code will be removed from the **Bluetooth Privacy Codes** View.


To Edit  a Bluetooth Privacy Code:

1. On the **Bluetooth Privacy Codes** View, click on either of the following:
  - The selected entry in the **Bluetooth Privacy Code** field.
  - The selected entry in the **Hexadecimal Format** field.
2. Edit the field selected.
3. Press the keyboard Enter key or click the mouse pointer anywhere outside the edited row of the **Bluetooth Privacy Codes** View.

To in-place Edit a Bluetooth Privacy Code:

1. Click either on the Bluetooth Privacy Code field of the selected entry in the **Bluetooth Privacy Codes** View.
2. Edit the selected field.
3. Press the **Enter** key on the keyboard or click the mouse anywhere outside of the edited row of the **Bluetooth Privacy Codes** View.

To Reverse  a Bluetooth Privacy Code:

1. Select a Bluetooth Privacy Code in the **Bluetooth Privacy Codes** View.
2. Click the **Reverse**  button.
3. The content of the selected Bluetooth Privacy Code is reversed. For example, code A-BCDE becomes EDCB-A when reversed.

### 3.1.2.7 Event Log View

The Event Log is a record of significant events that occurred at any time the Soderas datasource software is running. The log is recorded in time sequence using the computer clock. Log event descriptions provide information, warnings, and error notifications. The Event Log provides the user with a history of their analysis process. This history may be useful for process documentation or for troubleshooting capture issues and problems.

Information messages can include the starting and stopping of recording and the time that this event took place. Warnings in the log could be notifying the user that the capture file just opened contains unsupported content. Event Log error events include, for example, telling the user that the capture file is invalid.

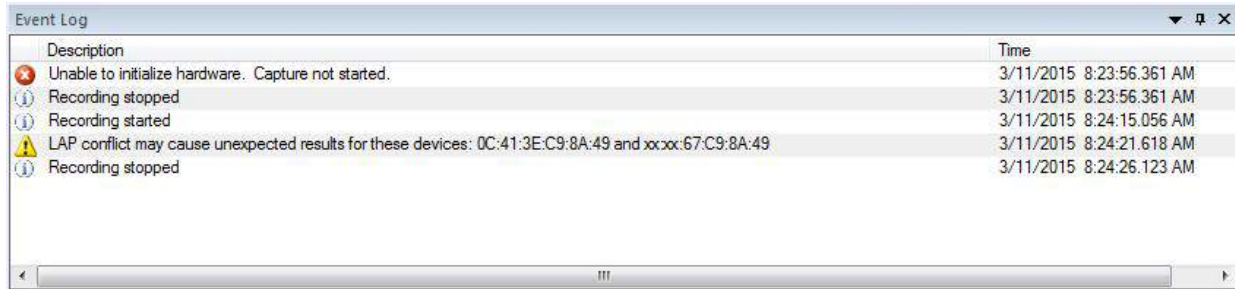


Figure 3.74 - Sodera Event Log View

The **Event Log** View contains event icons in the first column (no heading), event descriptions in the second column (**Description**), and the time the event occurred in the third column (**Time**).

A description of each **Event Log** column is in the following table.

Table 3.33 - Event Log Columns

Heading	Icon	Description
<b>Event</b>		Information: Events related to the normal flow of the capture process, e.g. "Start Capture", "Stop Capture", "Sodera hardware not found"
		Warning: Events that raise concern about the capture process integrity
		Error: Events that compromise the capture process or that may invalidate some of the captured data.
<b>Description</b>	—	Description of the event with additional information related to the Event icon.
<b>Time</b>	—	The actual time of the event in live capture mode, or the recorded time when running a previously captured file. The recorded time is based on the clock of the computer running the Wireless Protocol Suite software.

### Saving the Event Log

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

### 3.1.3 Excursion Mode

**Note:** The Excursion Mode feature is not supported on Sodera LE hardware.

Excursion Mode allows the user to capture *Bluetooth* data while untethered from a computer. This feature can make it easier to capture data while in a moving vehicle, to capture data in places where a laptop cannot readily be used, or to capture data in confined spaces, for example. Sodera’s internal battery complements Excursion mode by providing sufficient power to capture data for up to an hour without being connected to an external power source

#### Enable Excursion mode

1. Connect the Sodera hardware to a computer with a USB cable and start the Wireless Protocol Suite software.
2. In the Sodera window, select **Record Options...** from the **Options** menu.

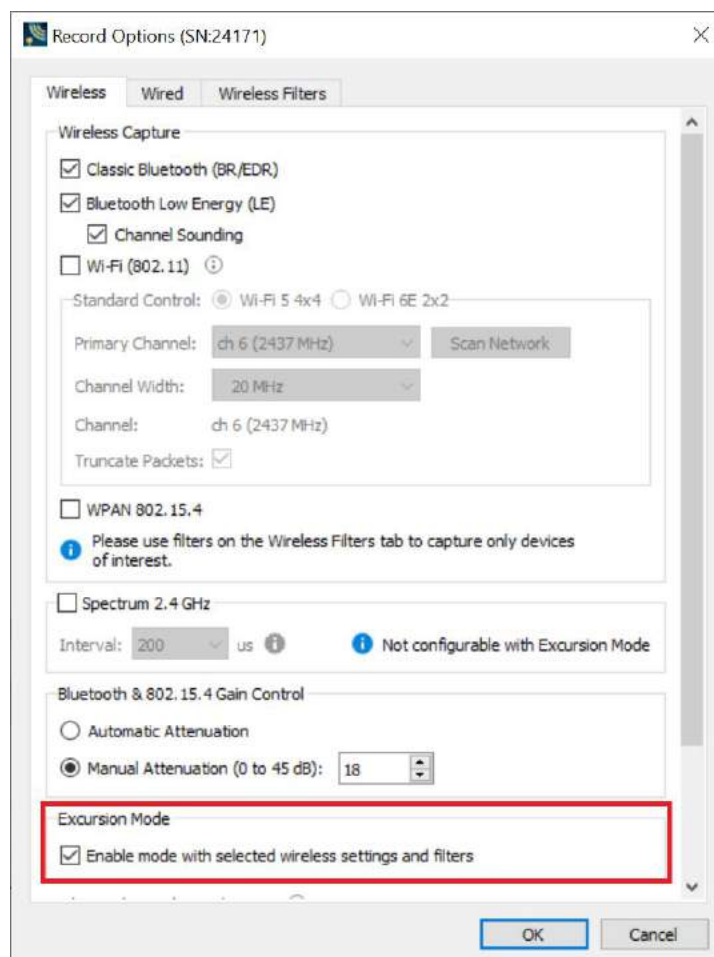


Figure 3.75 - X500 Record Options - Excursion Mode

3. Verify that the status message on the pop-up indicates the serial number of the connected hardware.
4. Check the box next to **Enable Excursion mode** and press **OK**. The pop-up will close and the **Record Options** are saved to the connected Soder hardware. The saved **Record Options** will travel with that specific Soder hardware module and affect all subsequent captures performed with that unit, regardless of whether they are performed using Excursion mode or using a connected computer.

### Disable Excursion mode

1. Connect the Soder hardware to a computer with a USB cable and start the Wireless Protocol Suite software.
2. In the Soder window, select **Record Options...** from the **Options** menu.
3. Verify that the status message on the pop-up indicates the serial number of the connected hardware.
4. Uncheck the box next to **Enable Excursion mode** and press **OK**. The pop-up will close and the **Record Options** are saved to the connected Soder hardware.

### Start Capturing Data in Excursion mode

1. With the Sodera hardware disconnected from a computer, hold for at least 1/2 second and then release the Power button on the front panel. The battery charge state indicator LEDs will repeatedly flash in sequence while the unit powers up.
2. Once the unit is powered up, press the Capture button on the front panel (right side). The Capture LED will be a constant green when capturing data.

### Stop Capturing Data in Excursion mode

1. Press the Capture button on the front panel (right side). There may be a brief delay, and the Capture LED will turn off.

## 3.2 802.11 Configuration

### 3.2.1 Wi-Fi Scanner Hardware Settings

The Hardware Settings dialog provides the ability to select a device to sniff/scan. The dialog only lists devices with a MAC address that match the Frontline devices. To access the Hardware Settings dialog:

1. Select Hardware Settings from the Options menu on the 802.11 Main window.

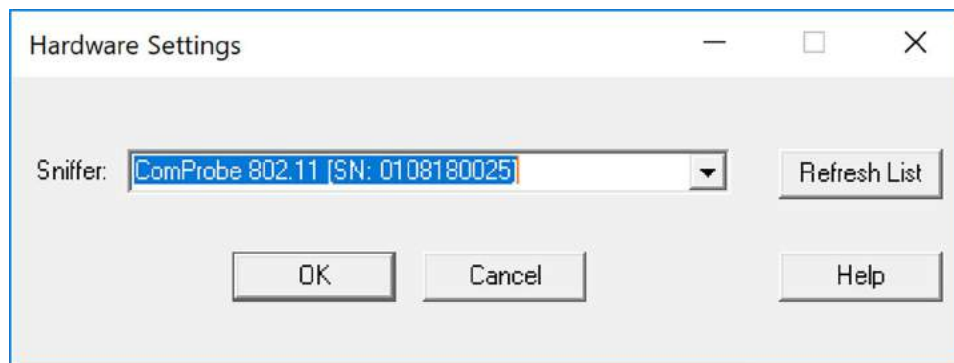


Figure 3.76 - Wi-Fi Scanner Hardware Settings Dialog

2. Select a device from the drop-down list.
3. Select OK

If no devices are found, the list is blank.

**Note:** Upon launching the Air Sniffer, the first device in the drop-down is the default device.

### 3.2.2 802.11 Datasource

1. Select **Capture -> Options** menu on the **Main windows**.

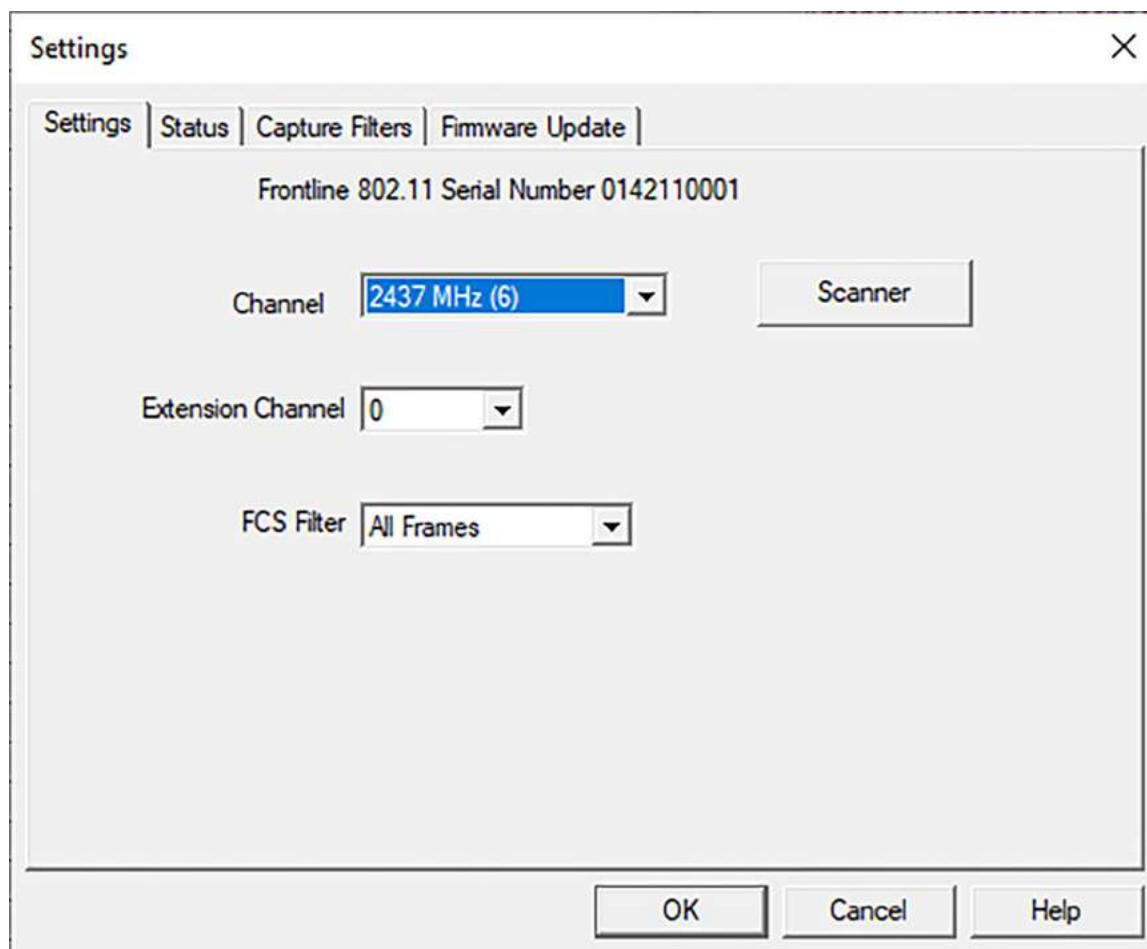


Figure 3.77 - 802.11 Settings Dialog

There are several things to remember about **Settings**:

- The **Settings** are specific to the device selected in the **Hardware Settings**.
- Two 802.11 devices attached to a computer have different settings.
- Changing the settings changes the devices' default settings.
- If a parameter is changed (e.g. Channel 1 is changed to 6), the new setting appears the next time the **Settings** dialog is opened for the device.
- The settings are saved when the **OK** button is pressed.

### 3.2.2.1 Settings

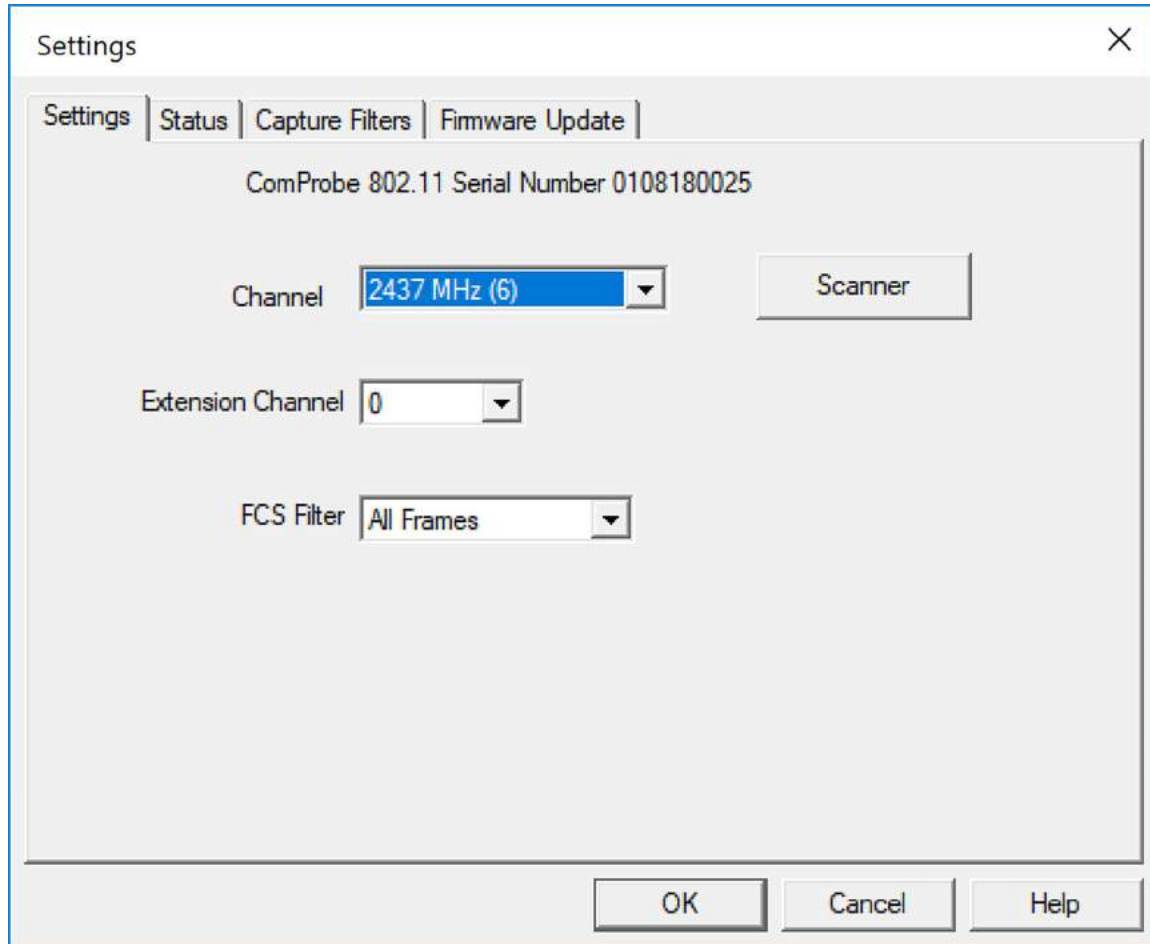


Figure 3.78 - 802.11 Settings Tab

The Settings dialog allows you to change and observe basic configuration values. These include the **Channel**, **Extension Channel**, **FCS Filter** and **Capture Type**.

- **Channel** - Select the channel from the drop-down list. Channels have been extended to the 5Ghz range.
- **Extension**- allows you to extend the range of channels available
  - 0 = Standard 1-13 Wi-Fi channels
  - -1 = Expanded channels below the standard range
  - +1 = Expanded channels above the standard range
- **FCS Filter** - The Frame Check Sequence filter indicates if the device should capture frames with an invalid FCS. Select **All Frames** or **Valid Frames**

Clicking on the **Scanner** button will open the **Wi-Fi Scanner** dialog. This action is useful if you do not know the channel to sniff. Once you have selected a channel in the **Wi-Fi Scanner** dialog and confirmed your selection the selected channel will appear in **Channel**.

### 3.2.2.2 Status

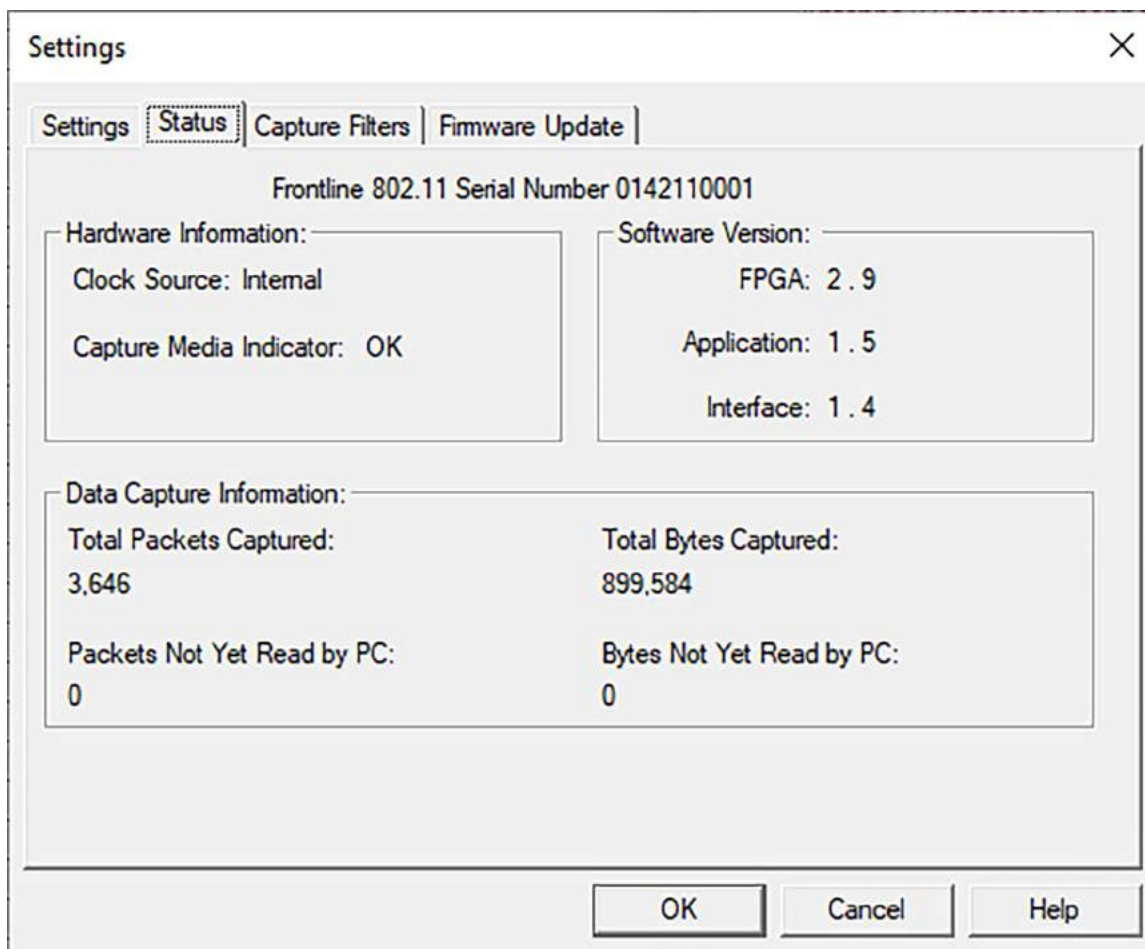


Figure 3.79 - 802.11 Settings Status Tab

The Status dialog provides current information about the Frontline device. There are no settings for this dialog.

### 3.2.2.3 Capture Filters

The **Capture Filters** dialog allows you create, modify, and delete capture filters. The dialog initially displays the existing MAC address Capture Filters.

- To activate the capture filters and to be able to create/modify additional filters, you first must select the **Enable MAC Address Capture Filters** check box.
- You can select/deselect which filters are active by checking/unchecking the **Enable** checkbox in the first column in the table.
- You can also select to ignore **Management**, **Control**, **Data**, and **Reserved** frame types by selecting one or more the checkboxes.

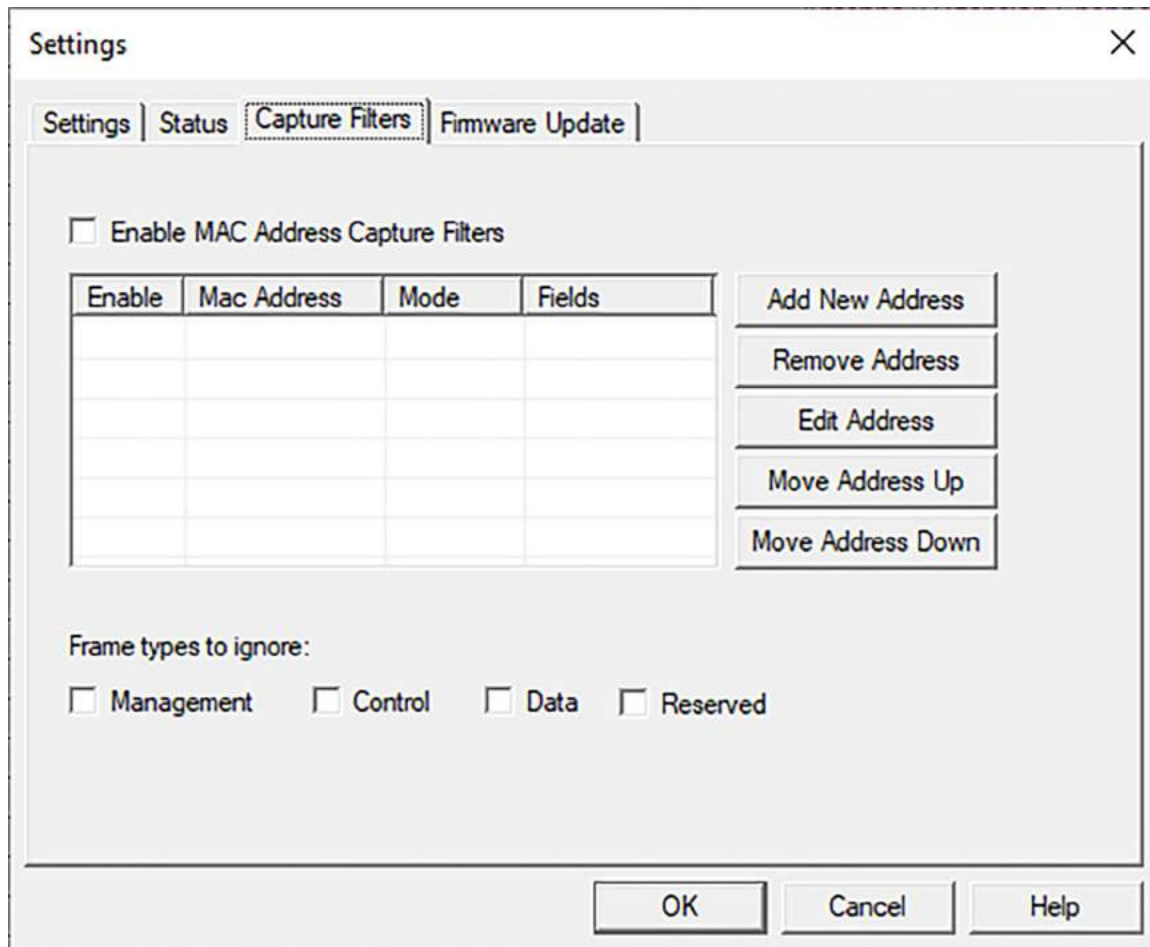


Figure 3.80 - 802.11 Settings Capture Filters Tab

To create a key, select one of the following options:

- **Add New Address** - displays a text box where you can enter the address



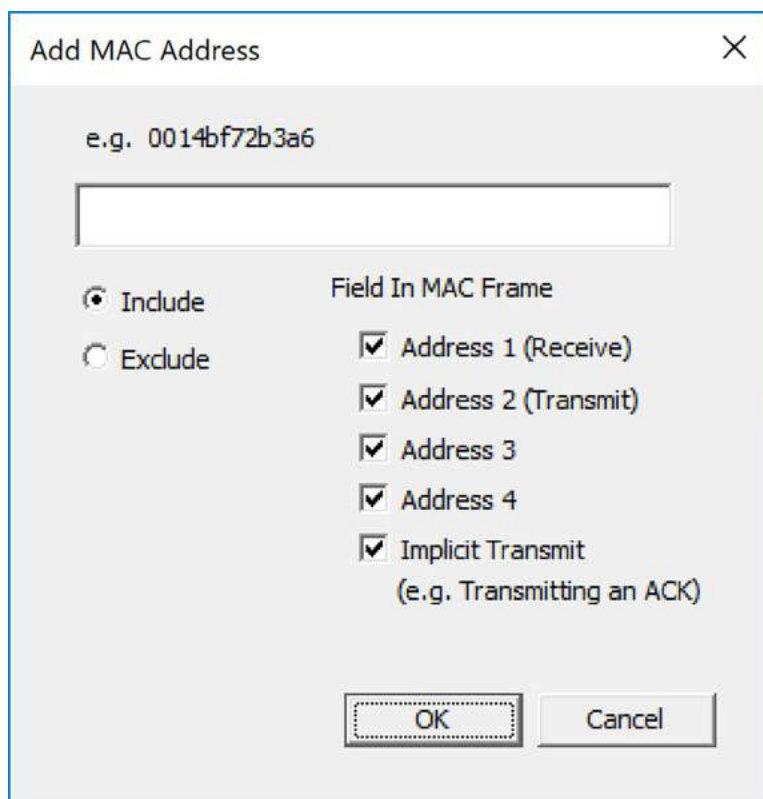


Figure 3.81 - 802.11 Settings Capture Filters Add New Address Dialog

1. Enter a MAC Address in the text field.
2. Select the **Include** radio button to only capture packets with this MAC address.
3. Select the **Exclude** radio button to capture packets with other filters, but not ones with this MAC address.
4. Select one or more check boxes to identify which fields in the MAC Frame to include.

The MAC header for an 802.11 frame can contain up to 4 address fields. Most frames do not have that many. In general, the first address is the intended receiver and the second address is the device that transmits the frame. The third and fourth address fields depend on the context of the frame. Some of the control type frames do not include the transmitter address but they may be determined from previous frames.

5. Select **OK** to close the dialog.

Once you have MAC addresses on the main dialog, you can modify them using four options.

- **Remove Address** - Highlight an address that you want to delete and select Remove Address to remove it from the list.
- **Edit Address** - Highlight an address that you want to edit and select Edit to bring up a dialog where you can edit the address. The address and any of the prior settings may be changes. Click **OK** to save and close.

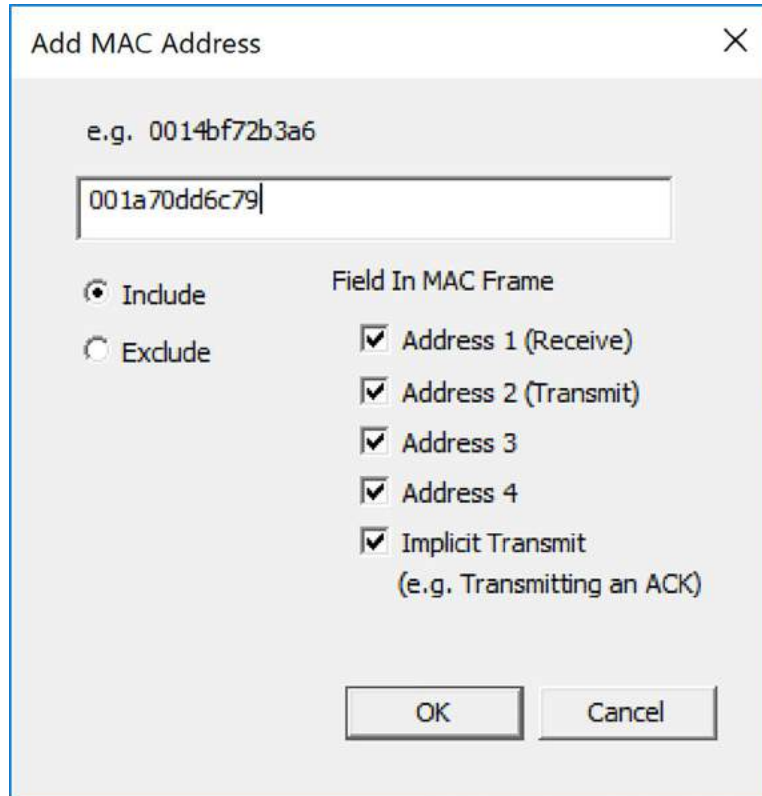


Figure 3.82 - 802.11 Settings Capture Filters Edit MAC Address Dialog

- **Move Address Up** - moves the selected address up in the queue.
- **Move Address Down** - moves the selected address down in the queue.

### 3.2.2.4 Firmware Update

To take full advantage of the improvements to the Frontline 802.11 with Wireless Protocol Suite software you must update the firmware on the Frontline .

**Note:** With the release of Wireless Protocol Suite software, an update to the firmware is required upon installation of the software. For that version, the full update requires three complete passes through the update process followed by a power cycle of the Frontline 802.11. Subsequent firmware updates may not require three firmware update cycles. This procedure is designed to take you through one to three firmware update cycles. Follow the procedure carefully, paying attention to jumps around unnecessary steps, and you should have no difficulty updating the firmware.

1. This tab displays the current firmware version in the hardware. You can check for the firmware updates by first noting the current version and then clicking on the **Check For Updates** button.

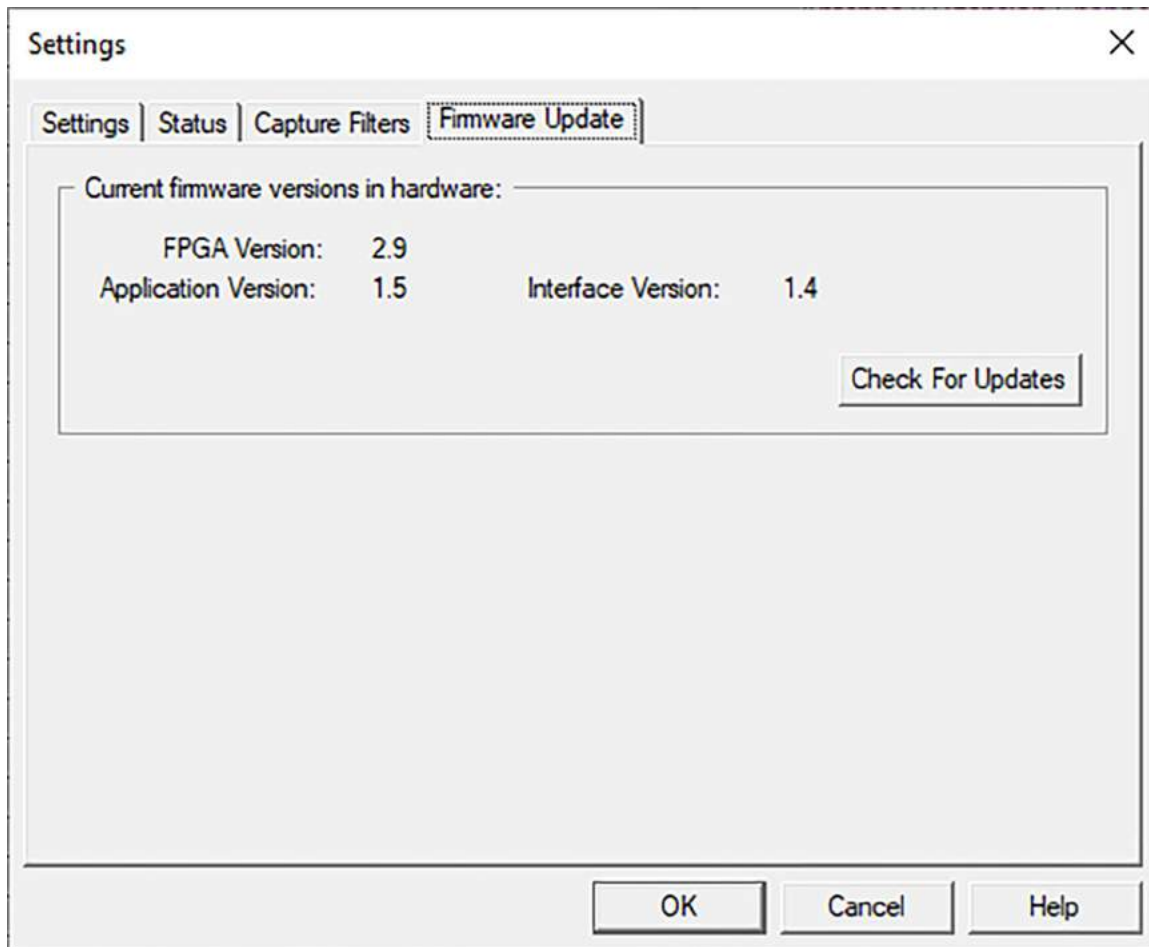


Figure 3.83 - 802.11 Settings Firmware Update Tab

2. The **Check for Updates** dialog will open. If an update is available you can install it by clicking on the **Start Update** button.

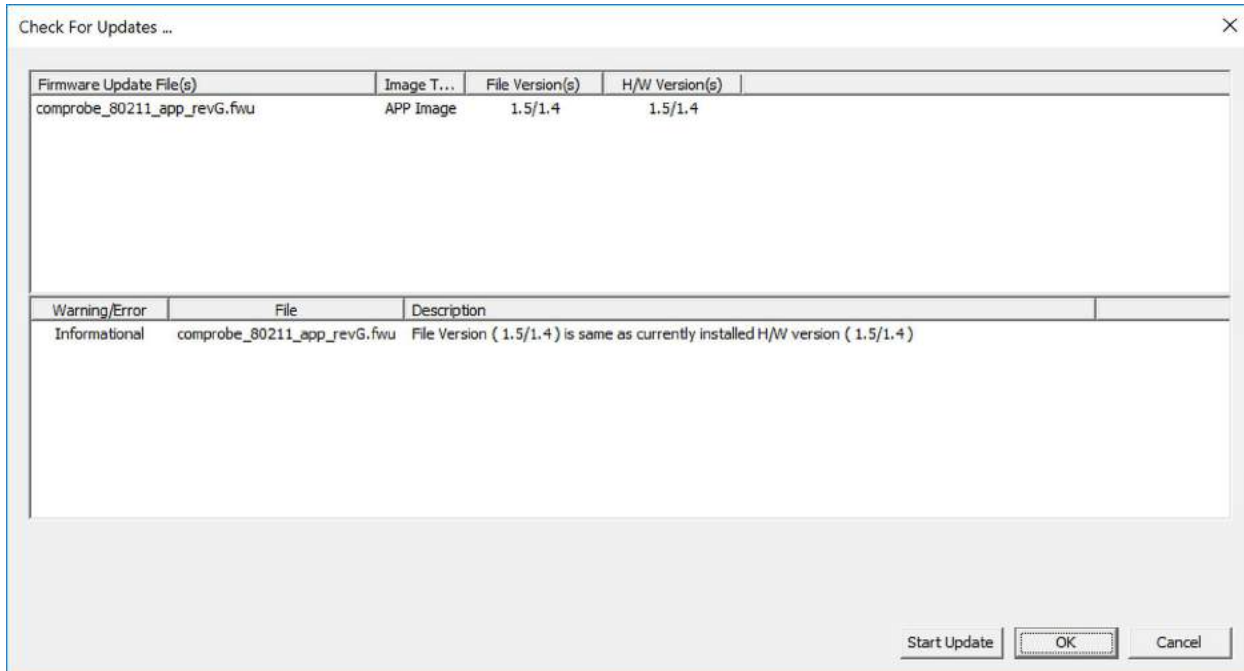


Figure 3.84 - 802.11 Settings Firmware Check For Updates

3. When the update is complete, two situations can occur.
  - a. If more firmware updates are required the following dialog will appear. Click on OK, and continue to step 4.

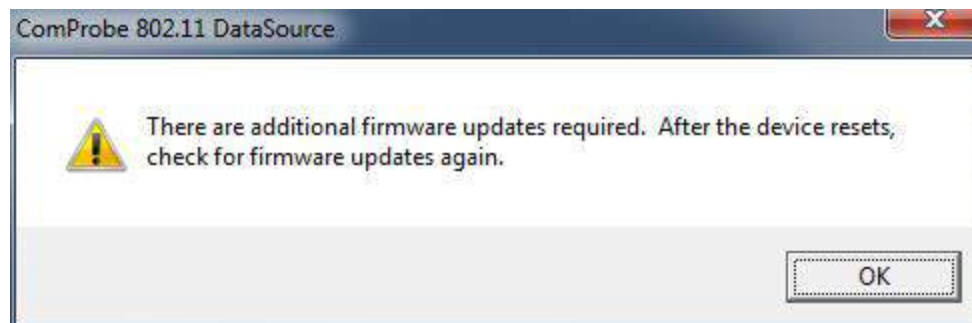


Figure 3.85 - 802.11 Settings Check for Updates Again, second cycle.

- b. If there are no more firmware updates, continue to step 15.
4. Click **OK** on the **Check for Updates** dialog.
5. Click **Cancel** on the **Settings** dialog **Settings** tab (See [Settings on page 169](#)). The Frontline 802.11 will reset. Wait for a constant **Activity** LED on the Frontline hardware .
6. Once the Frontline 802.11 has reset, select **Settings** from the Main window **Options** menu.
7. Click on the **Settings** dialog **Firmware Update** tab and then click on the **Check for Updates** button. The Check for Updates dialog will appear.

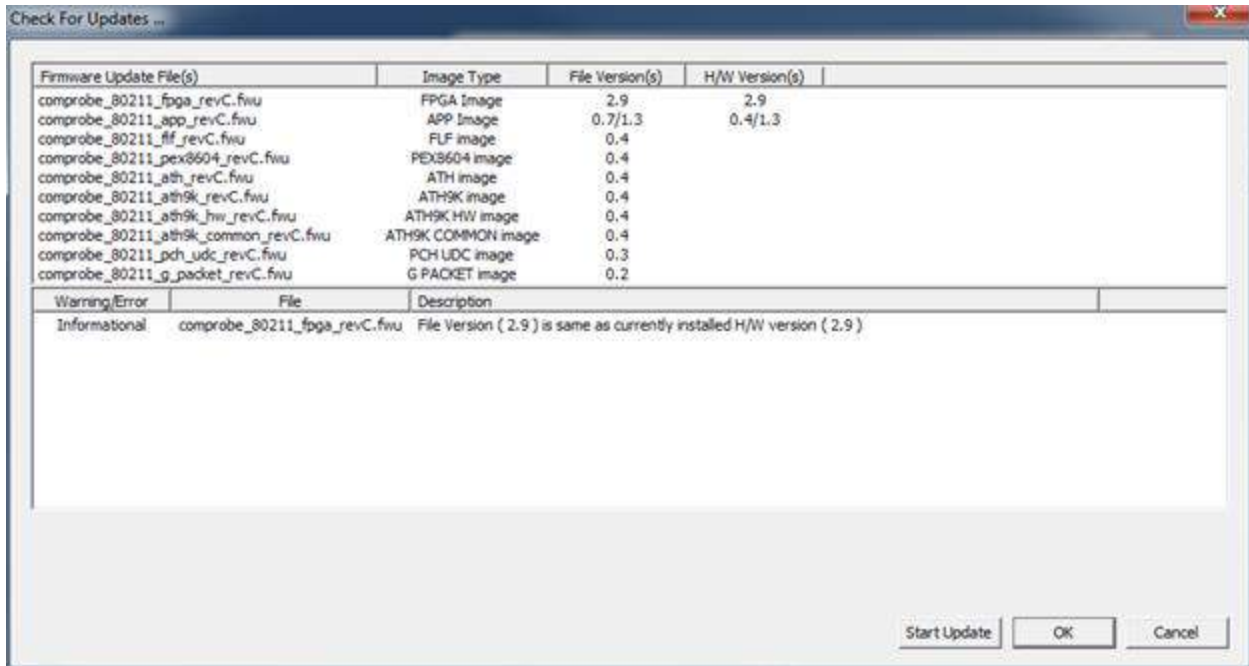


Figure 3.86 - 802.11 Settings Firmware Check For Updates, second cycle.

8. Click the **Start Update** button.
9. Again, when the update is complete, two situations can occur.
  - a. If there are more firmware updates the following dialog will be displayed. Click on **OK** and continue to step 10.

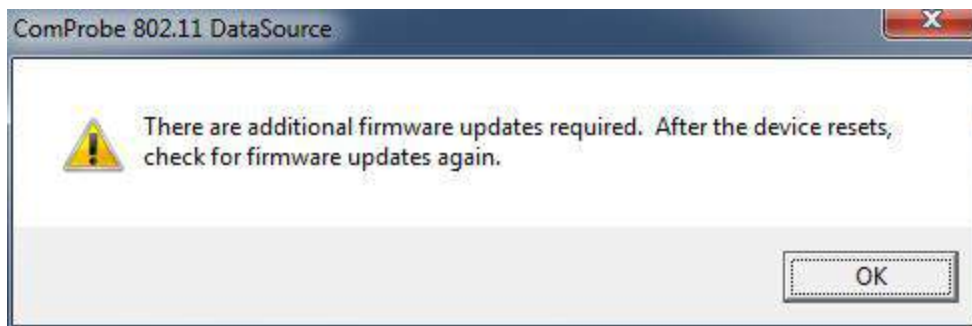


Figure 3.87 - 802.11 Settings Check for Updates Again, third cycle.

- b. If there are no more firmware updates, continue to step 15.
10. Click **OK** on the **Check for Updates** dialog.
11. Click **Cancel** on the **Settings** dialog **Settings** tab (See [Settings on page 169](#)). The Frontline 802.11 will reset. Wait for a constant **Activity** LED on the Frontline hardware .
12. Once the Frontline 802.11 has reset, select **Settings** from the Main window **Options** menu.
13. Click on the **Settings** dialog **Firmware Update** tab and then click on the **Check for Updates** button. The **Check for Updates** dialog will appear again.

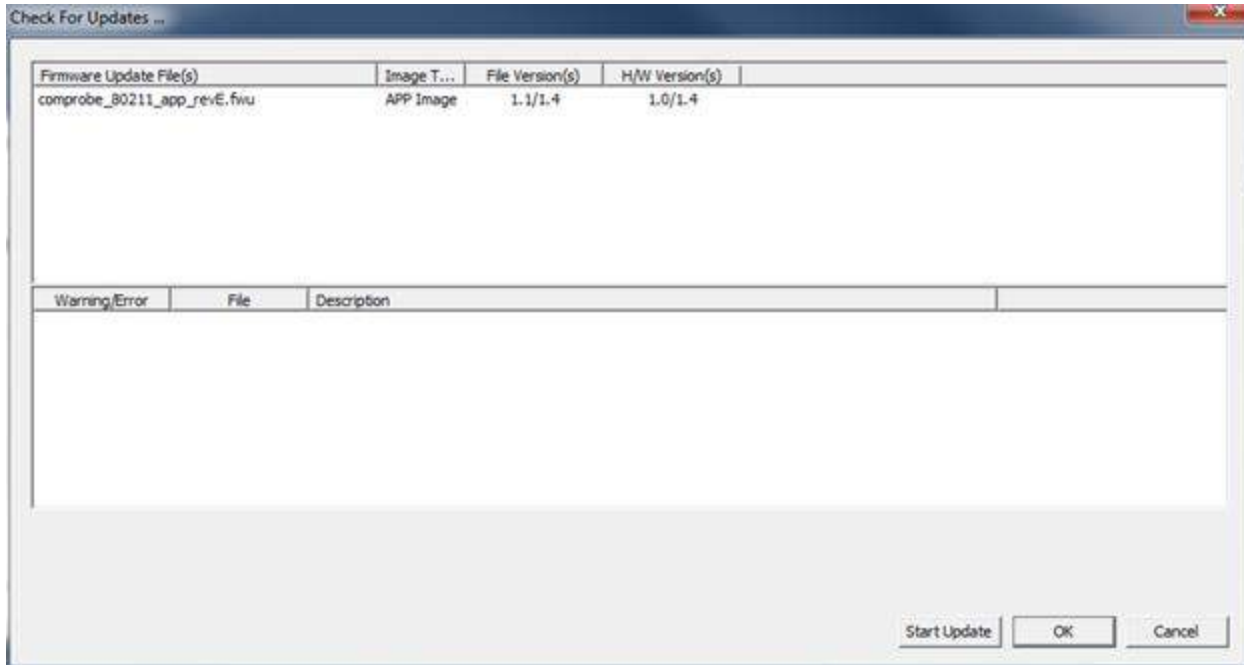


Figure 3.88 - 802.11 Settings Firmware Check For Updates, third cycle.

14. Click the **Start Update** button.
15. When the update is complete the **OK** button will be enabled. Click the **OK** button.
16. Remove power from the Frontline 802.11 unit, and then reapply power. Wait until the **Activity** LED comes back on and resume normal Frontline operation. When the Frontline 802.11 serial number shows in the Main window again, the firmware update is complete.

### 3.2.2.5 Wi-Fi Security

Security information is provided in the **Wi-Fi Security Window**.

The window is opened using the **Wi-Fi Security** button on the main toolbar.



Figure 3.89 - Wi-Fi & 802.15.4 Keys button on the main toolbar.

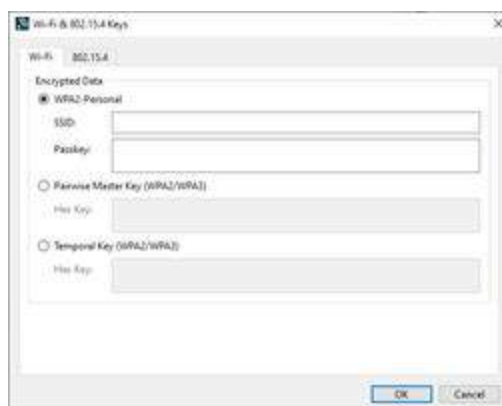


Figure 3.90 - Wi-Fi security configuration tab.

In the **Wi-Fi Security** dialog, select the encryption method being using with your device under test (DUT) by clicking on the radio button in the **Encrypted Data** section.

Table 3.34 - Wi-Fi Encrypted Data Options

Encrypted Data Option	Field	Description
<b>WPA2-Personal</b>	SSID	The station ID of the 802.11 communications link.
	Passkey	The shared passkey phrase used in communications.
<b>Pairwise Master Key</b>	key	The key is established between the wireless station and the access point. The key size is 32 Bytes for WPA2, the key size is 48 bytes for WPA3.
<b>Temporal Key</b>		A temporary key used to encrypt data for only the current session.

Within the **Set Initial Decodekey Parameters...** dialog **Security** tab, the fields available will depend on the **Encrypted Data** option selected.

### 3.2.2.5.1 Wi-Fi Device Scanner

1. On the **Settings** dialog click on the **Settings** tab, and then click on the Scanner button. The **Wi-Fi Device Scanner** dialog will open.

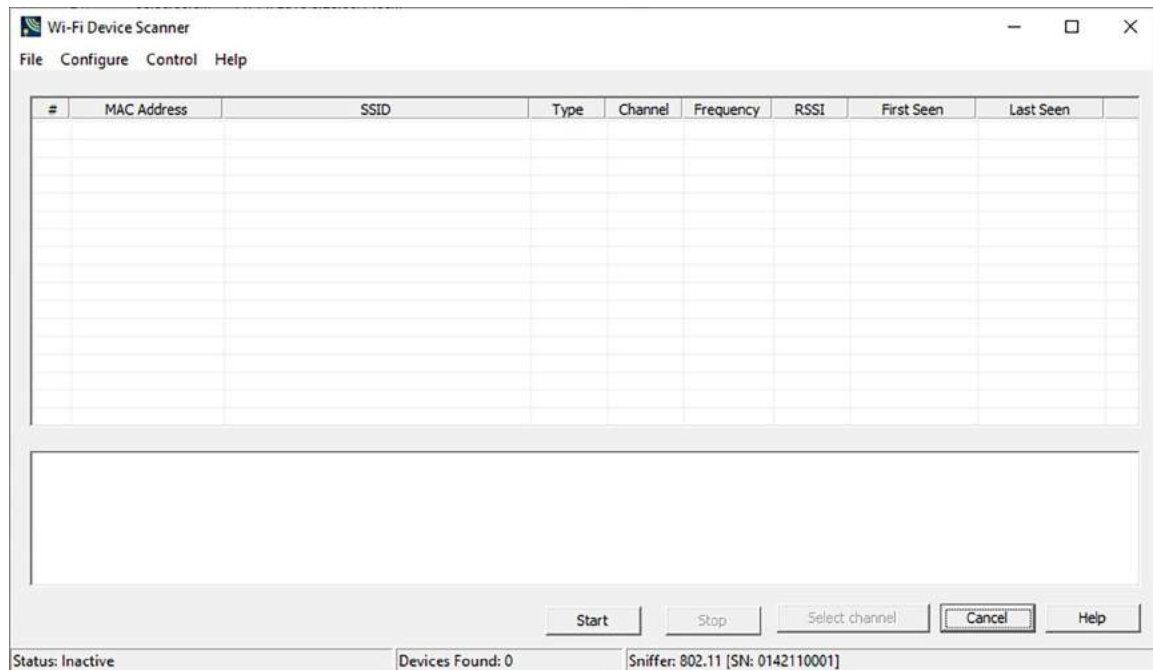


Figure 3.91 - 802.11 Device Scanner with no Devices Detected

2. On the **Wi-Fi Device Scanner** dialog Select the **Start** button or select **Start Scanning** from the **Main windows** menu to begin populating the list .

The **Wi-Fi Device Scanner** dialog displays a list of discoverable Wi-Fi devices in a table. The devices are identified by:

- MAC Address
- SSID
- Type
- Channel
- Frequency
- [RSSI](#)
- First Seen
- Last Seen

**Note:** You can select the **Stop** or **Stop Scanning** from the **Configure** menu anytime to stop the device search.



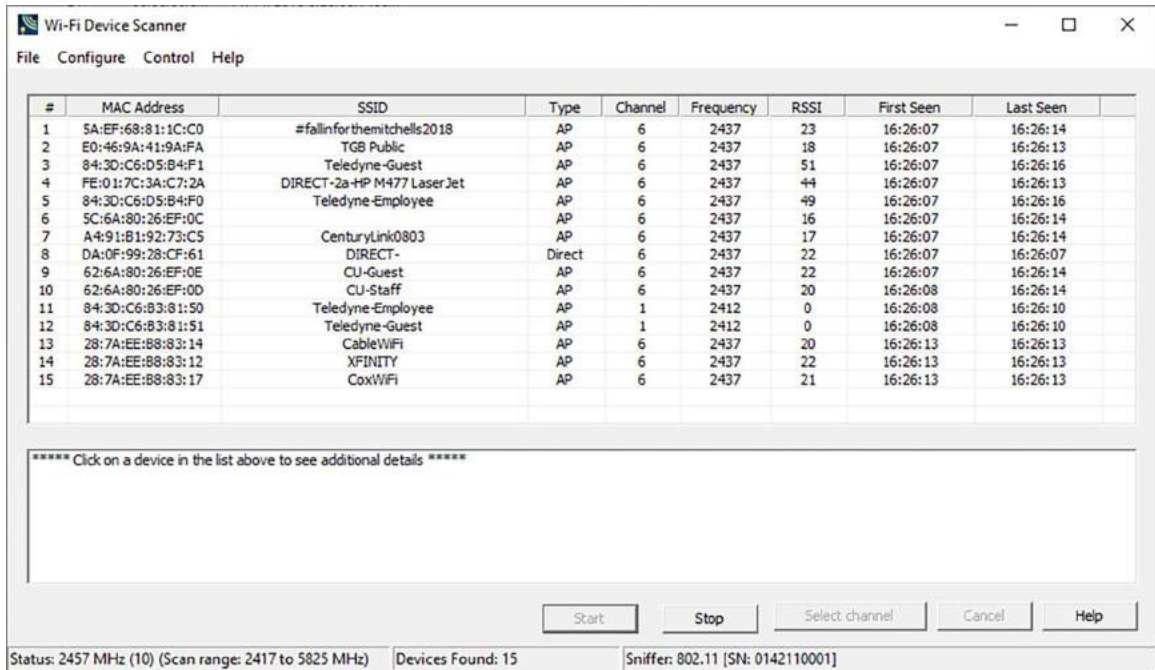
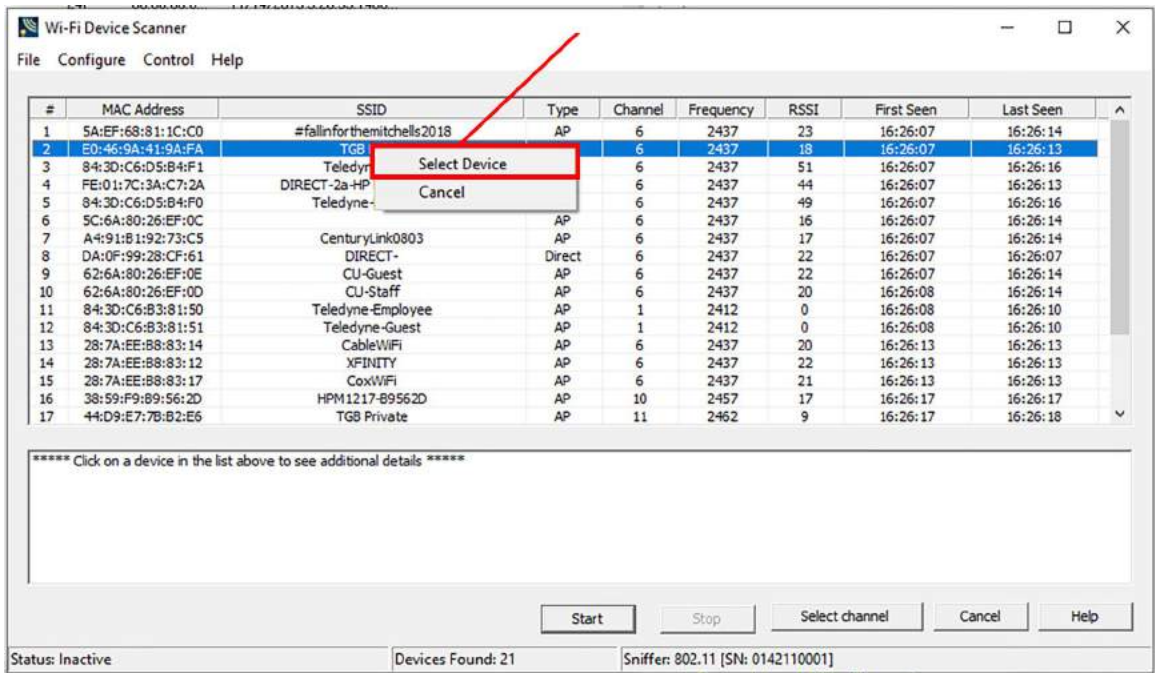
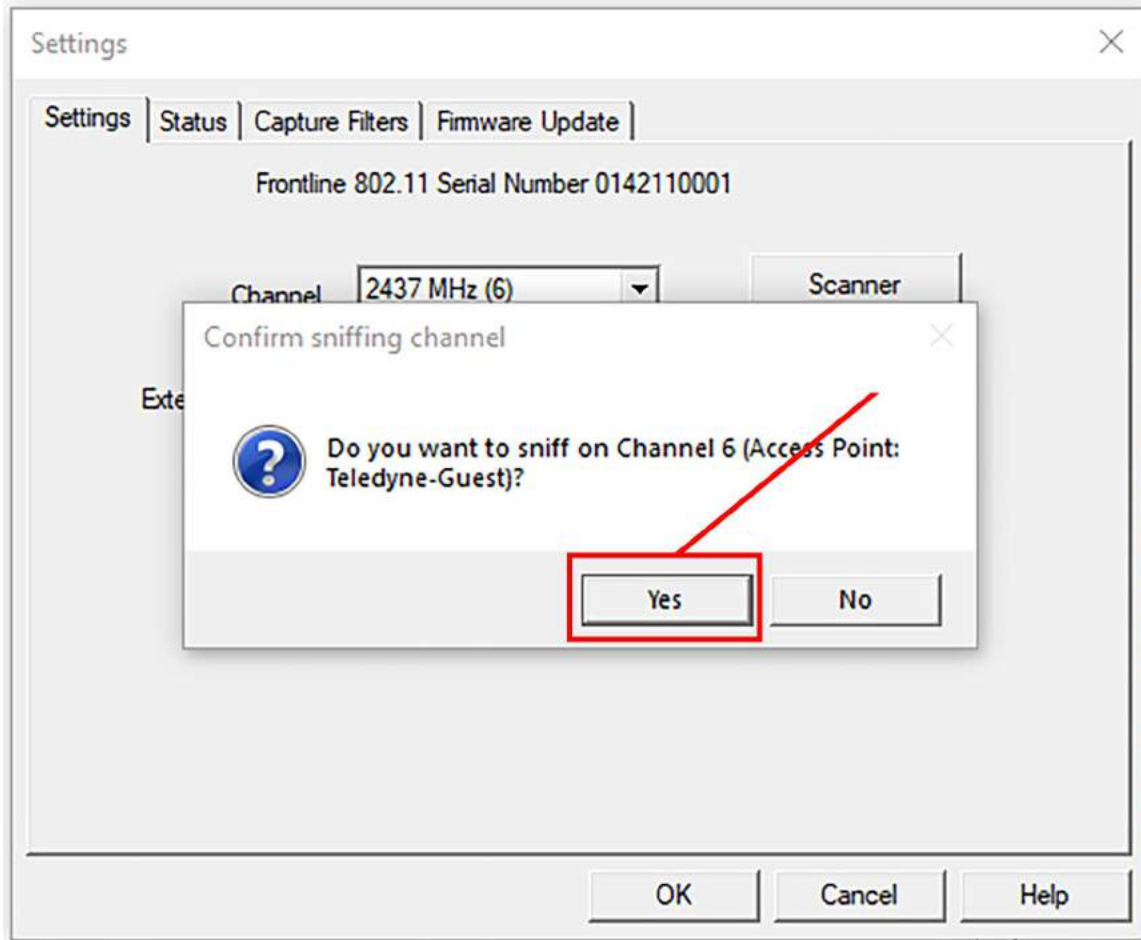


Figure 3.92 - 802.11 Device Scanner with Devices Detected

3. Select the device.



4. Click on **Select channel <no>**, where <no> is the channel number selected. The **Confirm Sniffing Channel** confirmation will appear. Click on **Yes** will close the **Wi-Fi Device Scanner** and the Frontline analyzer will use the selected channel.



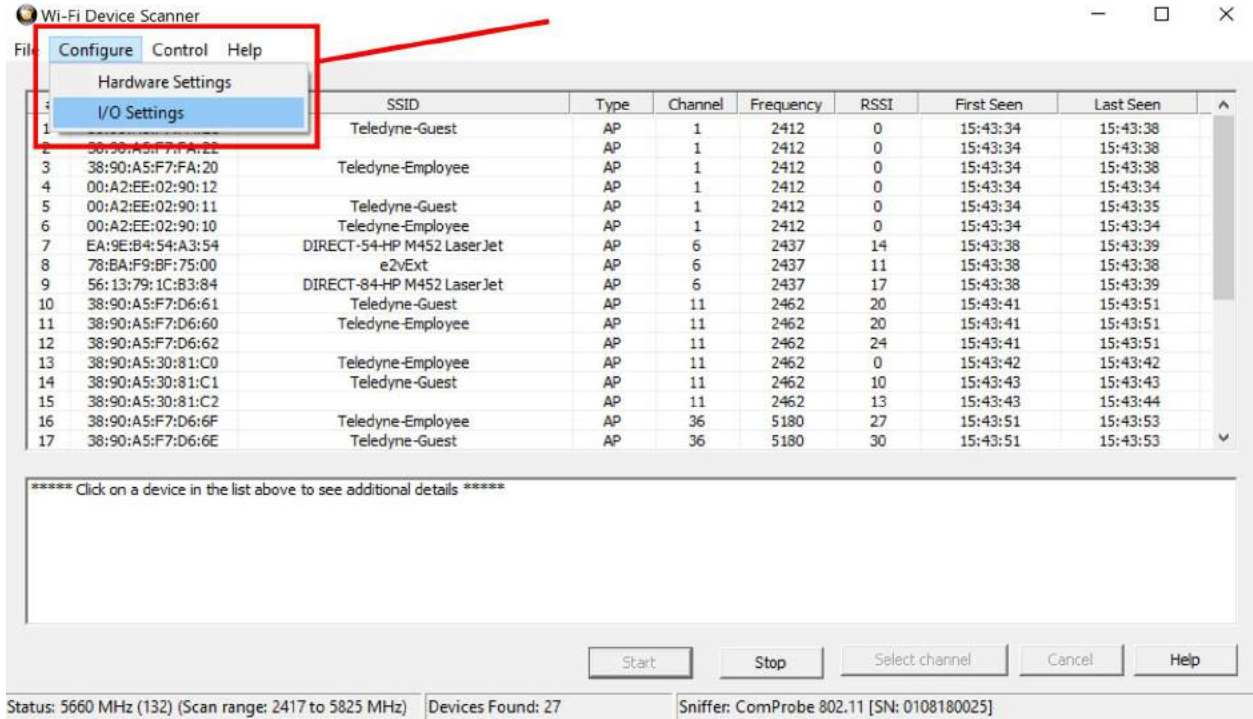
## File Menu

Under the File menu you can select **Export to file** which converts the information in the table to a text file.

1. Select **Export to CSV file**. The **Save As** menu appears
2. Select where you want to save the file in **Save in**.
3. Enter a **File Name**.
4. Select **Save**.

## Configure

From the Configure menu you can select [Hardware Settings](#) and [Settings](#). See the diagram below.



### 3.2.2.5.2 Wi-Fi Device Scanner - I/O Settings

The Device Scanner I/O Settings dialog is used to set a listening time and to activate a probe request. To access the I/O Settings dialog:

1. Select **I/O Settings** from the Configure menu on the [Wi-Fi Device Scanner](#) window.

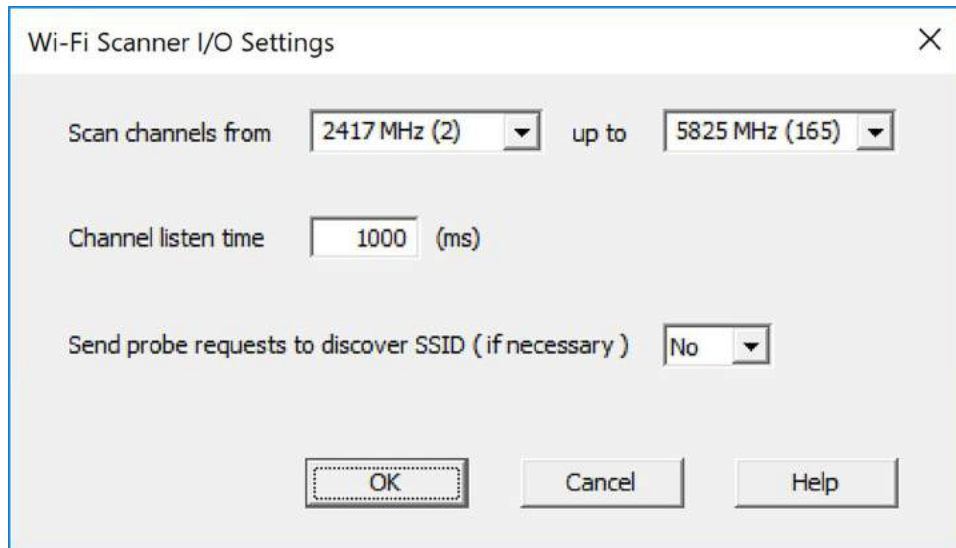


Figure 3.93 - Wi-Fi Device Scanner I/O Settings Dialog

2. **Scan Channels from:** Pick a lower and upper limit to scan a specific subset of frequencies. By default all channels are selected. Choosing a subset of frequencies to scan saves time and can be used when the user is interested in scanning only a certain range of frequencies.
3. Enter an amount, in msec, for **Channel listen time**.

**Channel listen time** is how long **Frontline**® 802.11 will listen on a channel to discover devices before moving on to the next channel.

4. Select **Yes** or **No** to choose whether to send a probe sync request.

Sometimes an Access Point will intentionally not send its SSID in a beacon to conceal its identity. Selecting **Yes** for this option will send the MAC address, the SSID will be part of the Probe Response it sends back.

5. Select **OK** to save the options and close the dialog or **Cancel** to close the dialog without saving your choices.

### 3.2.2.5.3 Device Scanner RSSI Values

The 802.11 specification does not provide a relationship between the RSSI value and the actual power value. Here are the definitions from the specification.

1. RSSI in FHSS PHY: The RSSI is an optional parameter that has a value of 0 through RSSI Max. This parameter is a measure by the PHY of the energy observed at the antenna used to receive the current PPDU. RSSI shall be measured between the beginning of the SFD and the end of the PLCP HEC. RSSI is intended to be used in a relative manner. Absolute accuracy of the RSSI reading is not specified.
2. RSSI in DSSS PHY: The RSSI shall be a measure of the RF energy received by the DSSS PHY. RSSI indications of up to 8 bits (256 levels) are supported.
3. RSSI in OFDM PHY: The allowed values for the RSSI parameter are in the range from 0 through RSSI maximum. This parameter is a measure by the PHY of the energy observed at the antenna used to receive the current PPDU. RSSI shall be measured during the reception of the PLCP preamble. RSSI is intended to be used in a relative manner, and it shall be a monotonically increasing function of the received power.

Different vendors implement these value in their own way. The Frontline 802.11 uses an Atheros chipset which provides RSSI values in the range of 0 to 128. The radio hardware in the Frontline 802.11 has two receive chains (one for each antenna). Each received packet has RSSI values for both antennas as well as the combined value.

The hardware provides the following five values:

1. rssi\_ant00: Receive signal strength indicator of control channel chain 0.
2. rssi\_ant01: Receive signal strength indicator of control channel chain 1.
3. rssi\_ant10: Receive signal strength indicator of extension channel chain 0.
4. rssi\_ant11: Receive signal strength indicator of extension channel chain 1
5. rssi\_combined: Receive signal strength indicator of combination of all active chains on the control and extension channels.

All five of these values are shown in the PHY layer decoder for every packet. The Wi-Fi scanner shows the combined value.

### 3.2.3 Wi-Fi Device - MAC Address Editor

If you know the MAC Address of the device you can enter it manually.

1. From the Settings dialog select the "Edit" button.
2. On the MAC Address Editor enter the MAC Address for the device.



Figure 3.94 - Wi-Fi Direct MAC Address Editor

3. Enter a channel number in Listen Channel.
4. Select "OK".

The MAC Address appears on the Settings dialog.

Once you close the dialog, the last MAC Address shown will appear when you reopen the dialog.

## 3.3 802.15.4 Configuration

Security information for 802.15.4 protocols are configured in the Wi-Fi & 802.15.4 Keys window. The window is opened using the Wi-Fi & 802.15.4 Keys button on the main toolbar ( [Figure 3.95 -](#) ) or by selecting "Wi-Fi & 802.15.4 Keys" from the View menu.

The window is opened using the **Wi-Fi Security** button on the main toolbar.



Figure 3.95 - Wi-Fi & 802.15.4 Keys button on the main toolbar.

Once the window is open ( [Figure 3.96 -](#) ) select the 802.15.4 tab and to add a key:

1. Select add a new key ( [Figure 3.96 -](#) )
1. Enter the key into the key value text box ( [Figure 3.96 -](#) ).
1. Select the key hash type ( [Figure 3.96 -](#) ). Currently the choices are "No Hash" and "Thread". The Thread hash type should be selected for the Thread protocol.

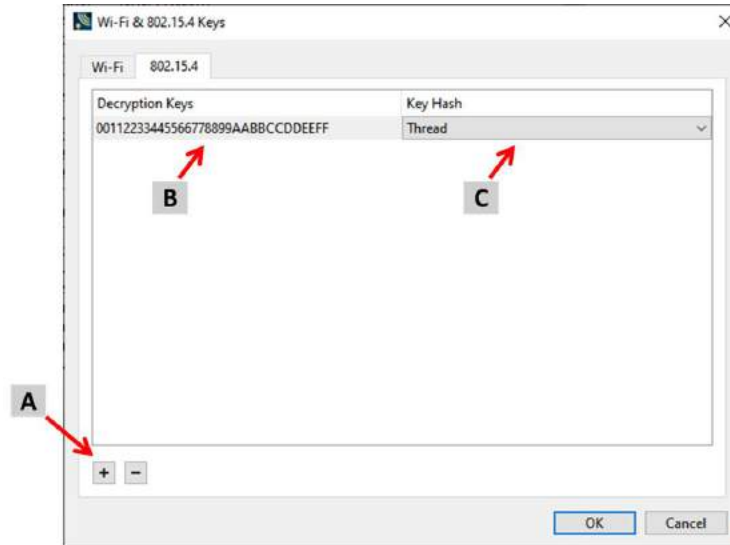


Figure 3.96 - 802.15.4 security configuration tab. (A) Add a new key. (B) key value text box. (C) Key hash type.

### 3.4 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*<sup>®</sup> 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 Options -> Decoders -> Initial Decoder Parameters....

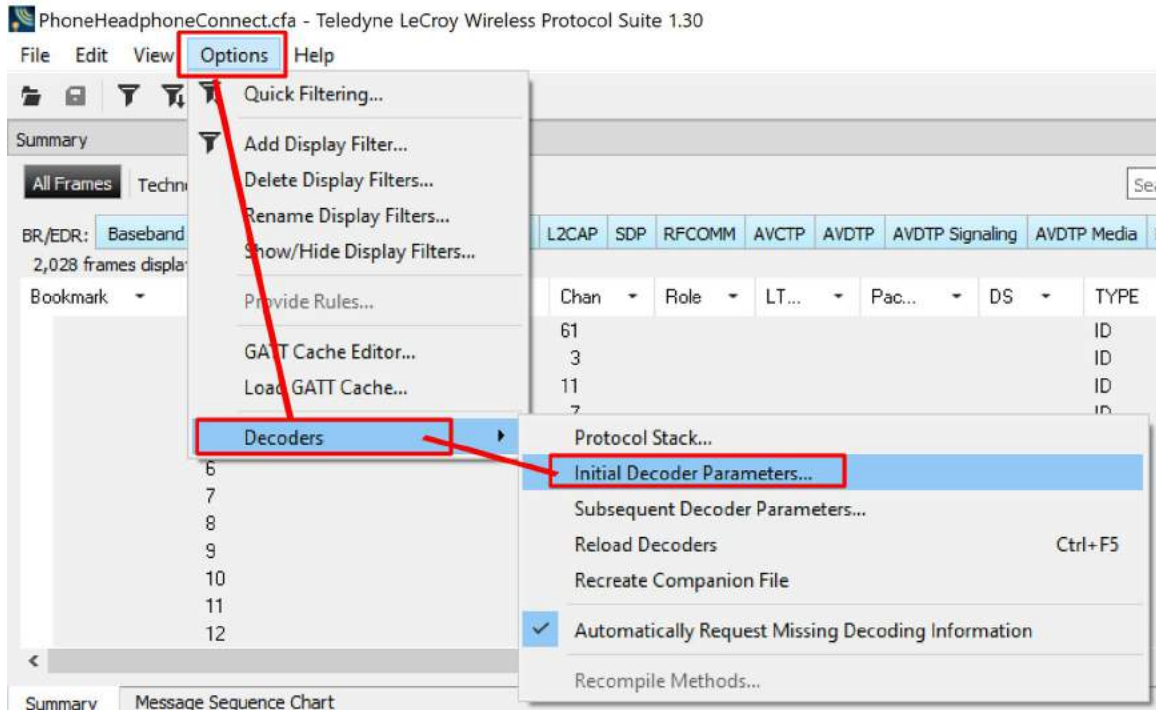


Figure 3.97 - Select **Set Initial Decoder Parameters...** from **Main windows** window

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

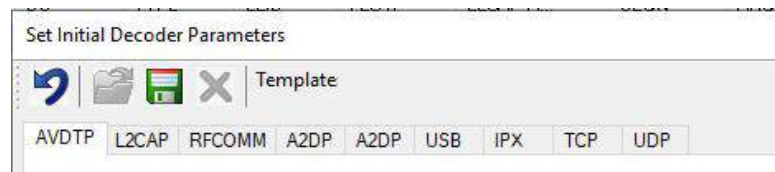


Figure 3.98 - Tabs for each decoder requiring parameters.

- 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 > Decoders > Subsequent Decoder Parameters** menu, and make the needed changes. You can also right-click on the frame to select the same option.



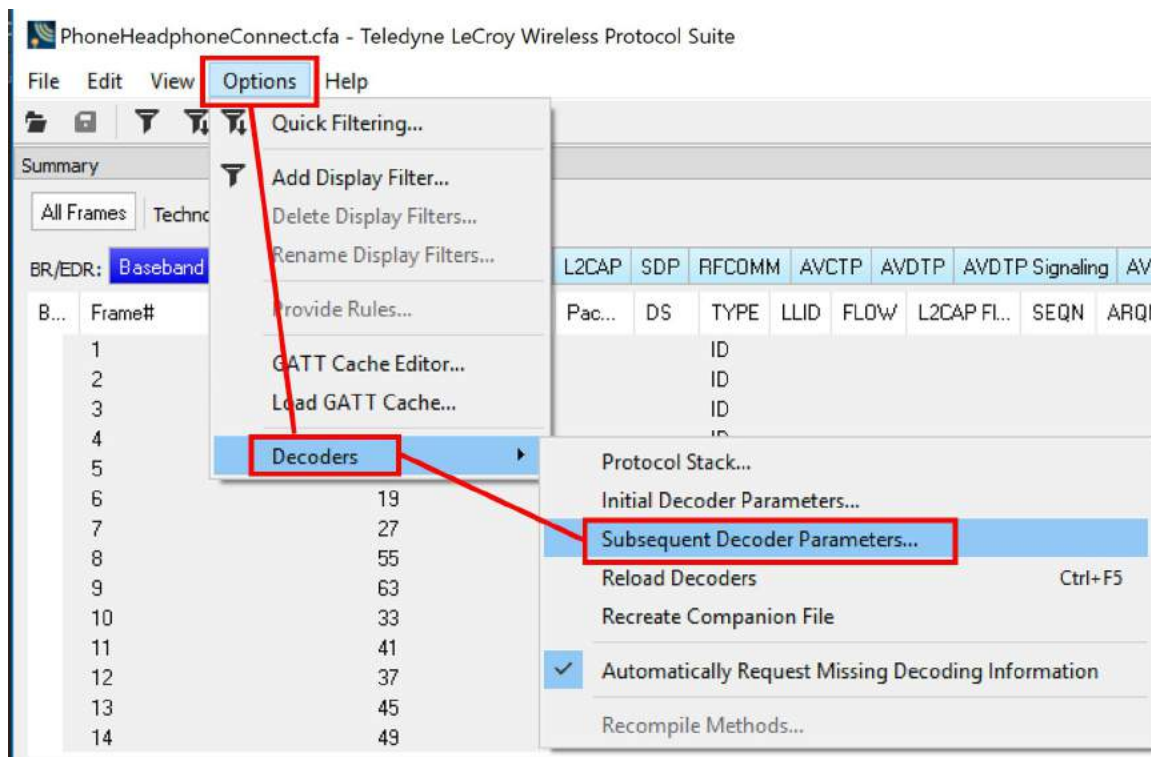


Figure 3.99 - Options -> Decoders -> Subsequent Decoder Parameters



You can also right-click on the frame to select the same option.

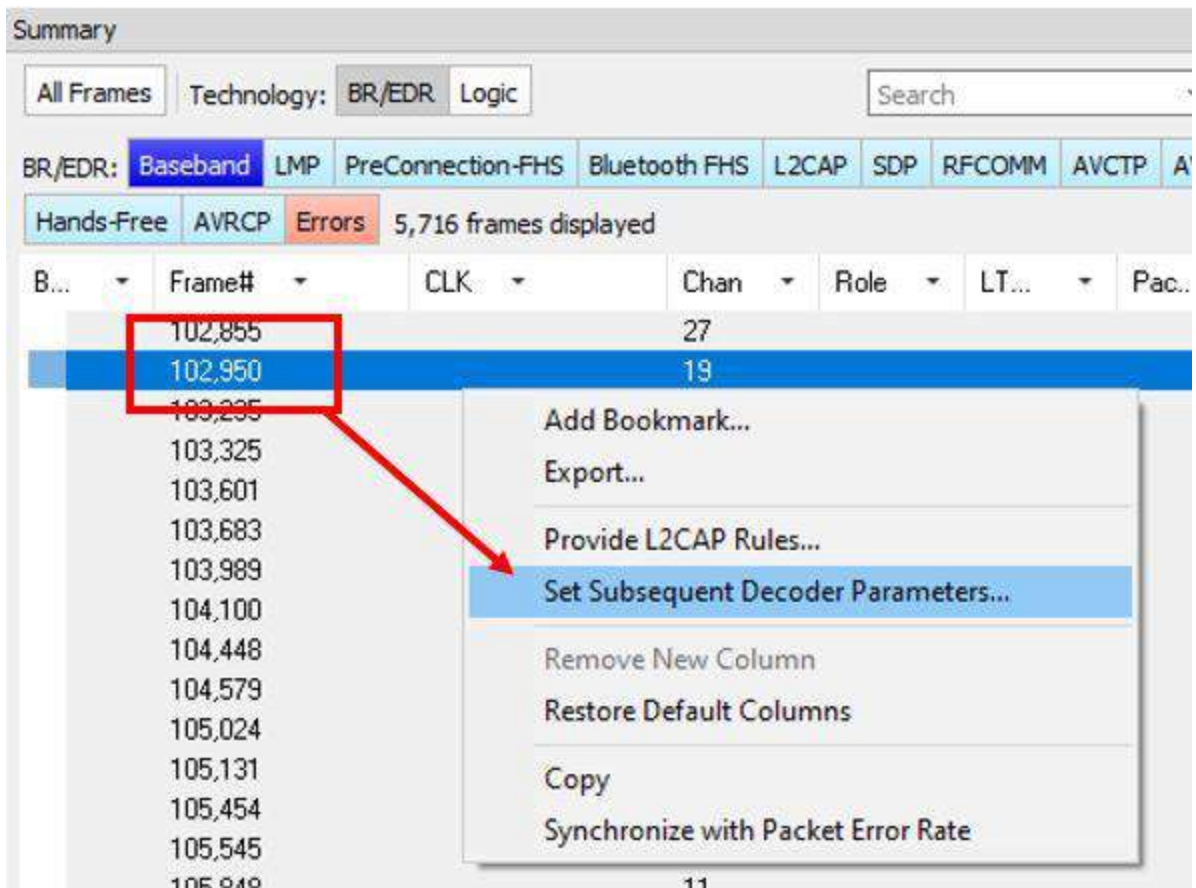


Figure 3.100 - **Set Subsequent Decoder Parameters...** from Main windows

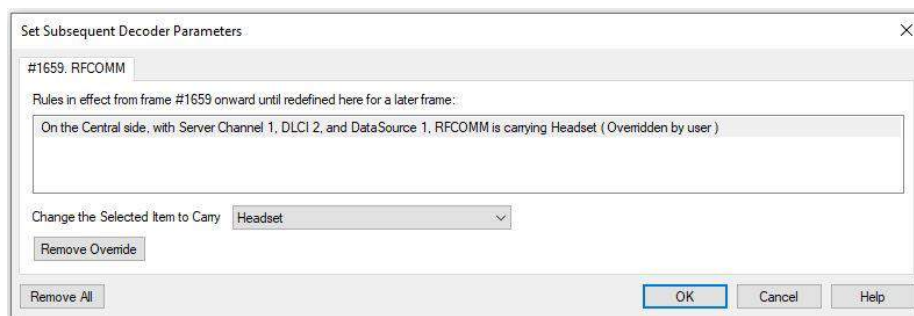


Figure 3.101 - Example: Set Subsequent Decode Parameters for Frame #52, RFCOMM

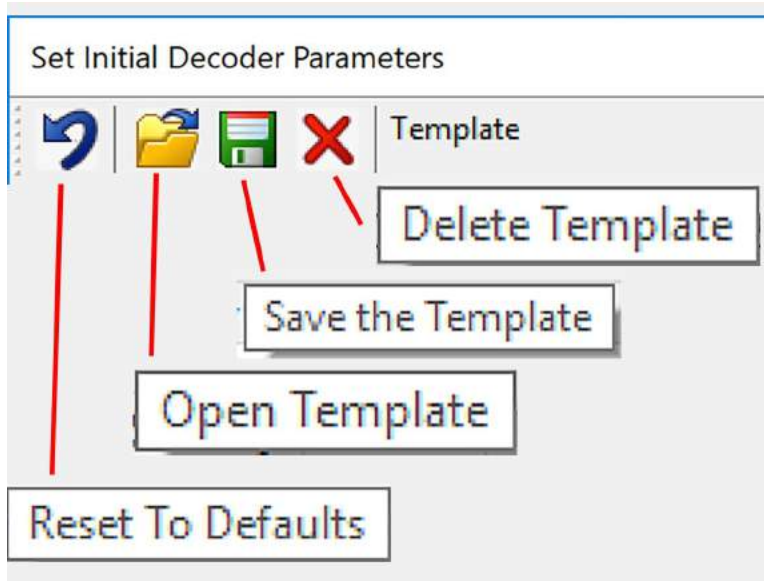
- Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.
- The **Remove Override** button will remove the selected decode parameter override.
- The **Remove All** button will remove all decoder overrides.

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.

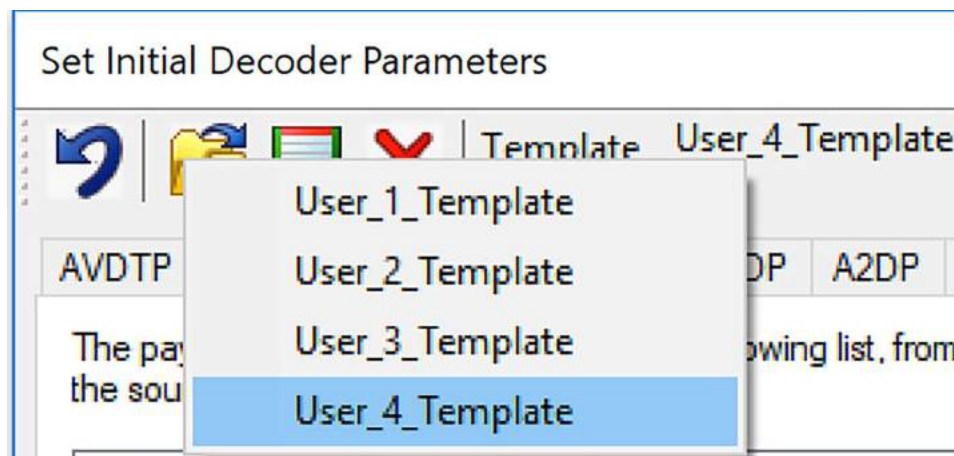
### 3.4.1 Decoder Parameter Templates

#### 3.4.1.1 Select and Apply a Decoder Template

1. Select **Set Initial Decoder Parameters...** from the **Options -> Decoders -> Initial Decoder Parameters....** menu on the **Main 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 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.

### 3.4.1.2 Adding a New or Saving an Existing Template

#### Add a Template

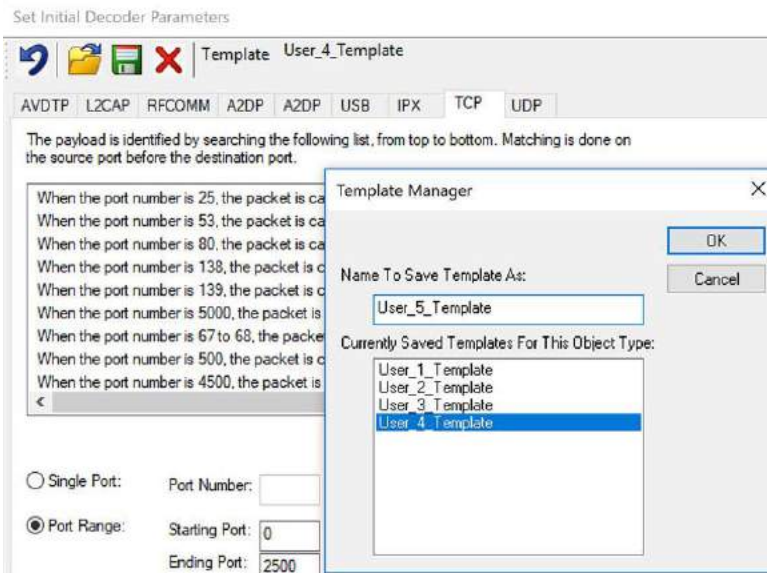
A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

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.



#### 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.

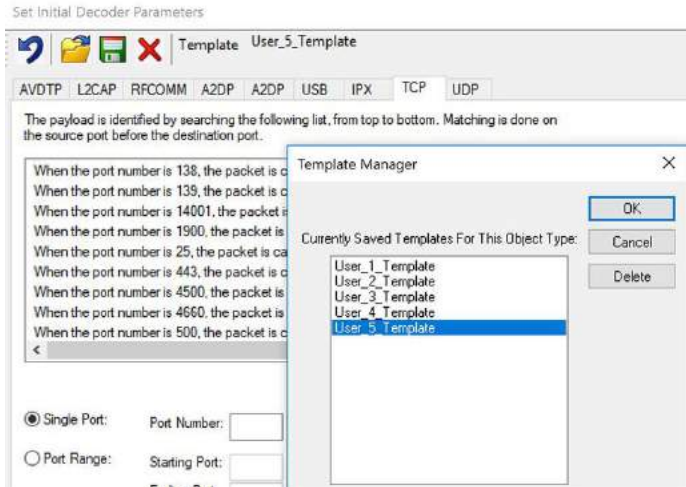
4. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the template and close the window.

### 3.4.1.3 Deleting a Template

1. After opening the **Set Initial Decoder Parameters** window click the **Delete**  button in the toolbar.

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

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



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

3. Click the **OK** button to complete the deletion process and close the Delete dialog.
4. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the deletion and close the dialog.

### 3.4.2 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 **Main windows** or the **Datasource** window.
2. Click on the **A2DP** tab.
3. Choose the desired decoding method.

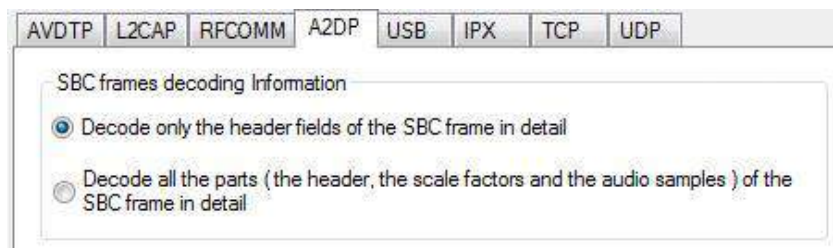


Figure 3.102 - A2DP Decoder Settings

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.

### 3.4.3 AVDTP Decoder Parameters

#### 3.4.3.1 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.

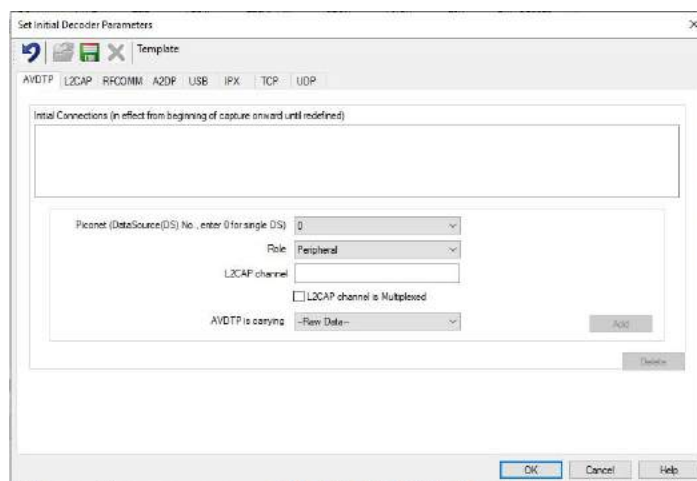


Figure 3.103 - AVDTP parameters tab

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 (**Central** or **Peripheral**)
- **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 Initial Connection window displays the added parameters.

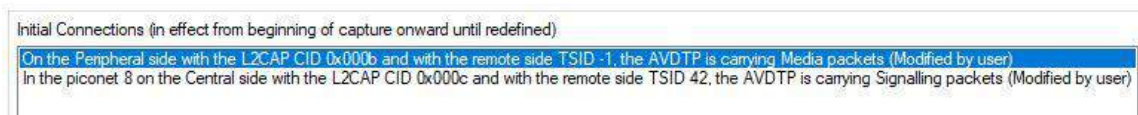


Figure 3.104 - Parameters Added to Decoder

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 191](#) [Adding a New or Saving an Existing Template on page 191](#)

#### 3.4.3.2 AVDTP Missing Decode Information

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

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

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

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

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



If you are not sure of the payload carried by the subject frame, look at the raw data shown “data” in the [Decode](#) pane. 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.

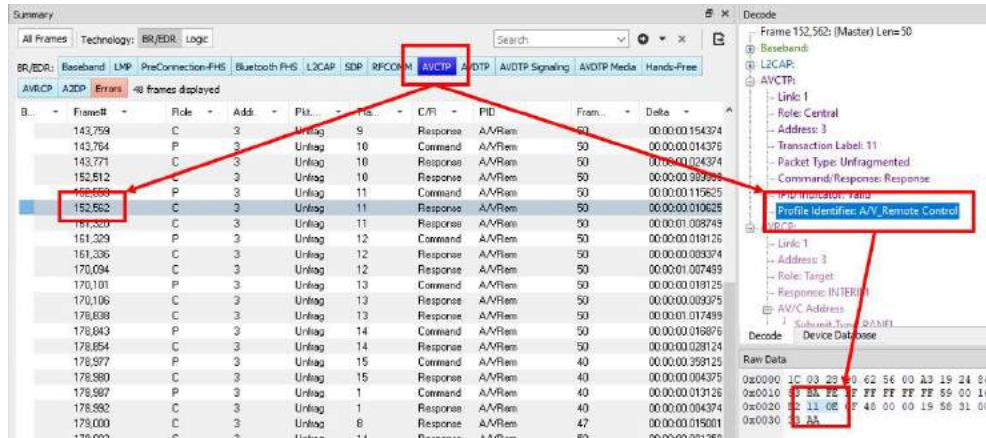


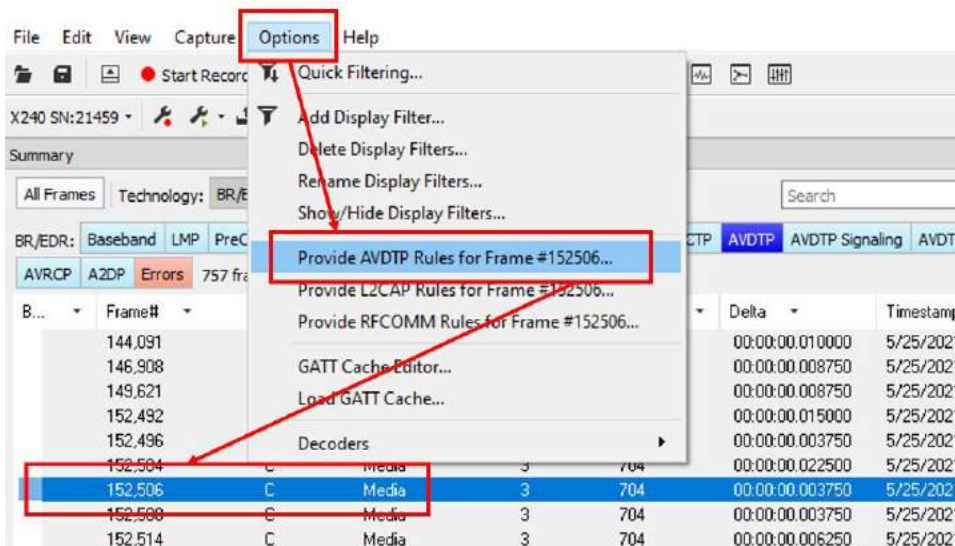
Figure 3.105 - Look in Decoder pane for profile hints

### 3.4.3.3 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 > Decoders > Subsequent Decoder Parameters** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.



- 3. Select the rule you wish to modify from the list of rules.
- 4. Choose the protocol the selected item carries from the drop-down list, and click **OK**.

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

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

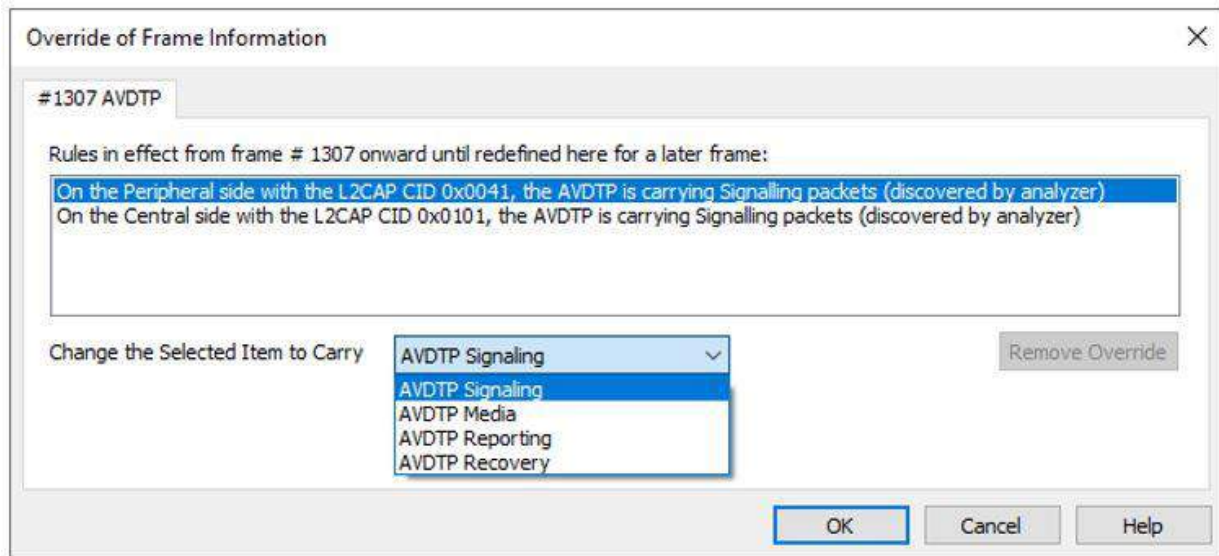


Figure 3.106 - AVDTP Override of Frame Information, Item to Carry

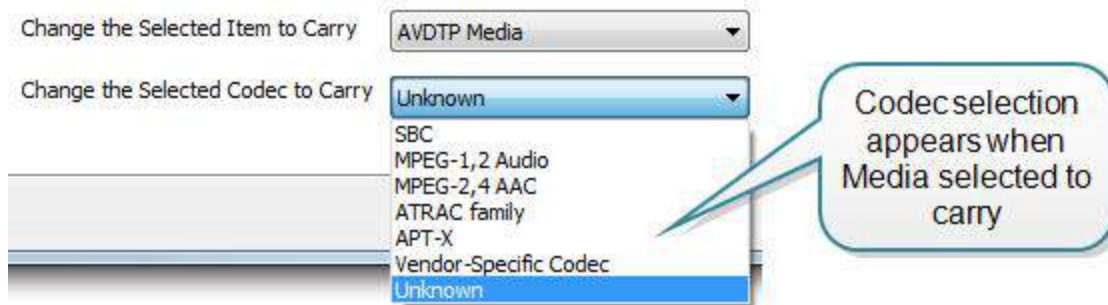


Figure 3.107 - AVDTP Override of Frame Information, Media Codec Selection



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.

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

### 3.4.4 L2CAP Decoder Parameters

#### 3.4.4.1 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. You get to the menu below by selecting **Options -> Decoders -> Initial Decoding Parameters**. This will bring up the Set Initial Decoder Parameters menu below:

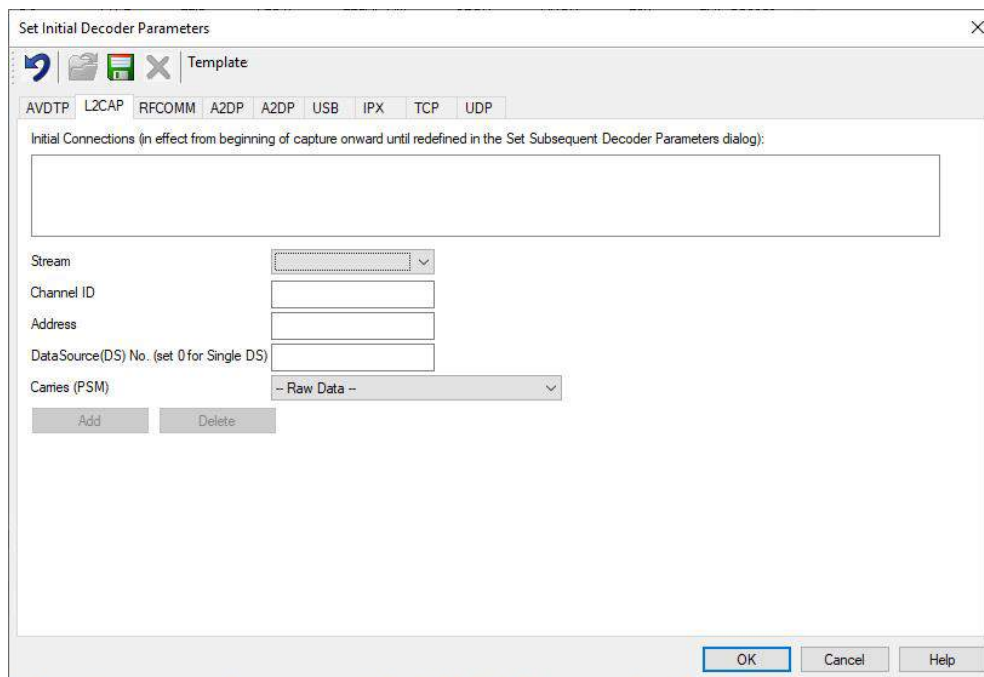
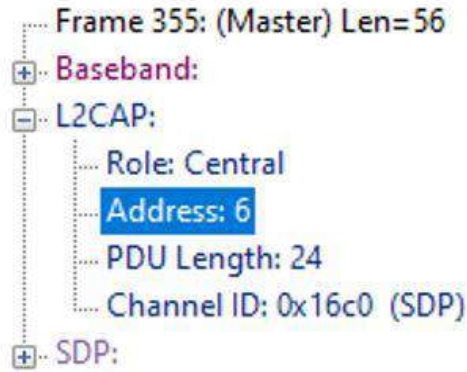


Figure 3.108 - L2CAP Decoder parameters tab

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 (central or central)
- **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 **Main windows** can provide address information.
- **Data Source (DS) No.** -When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source number.



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

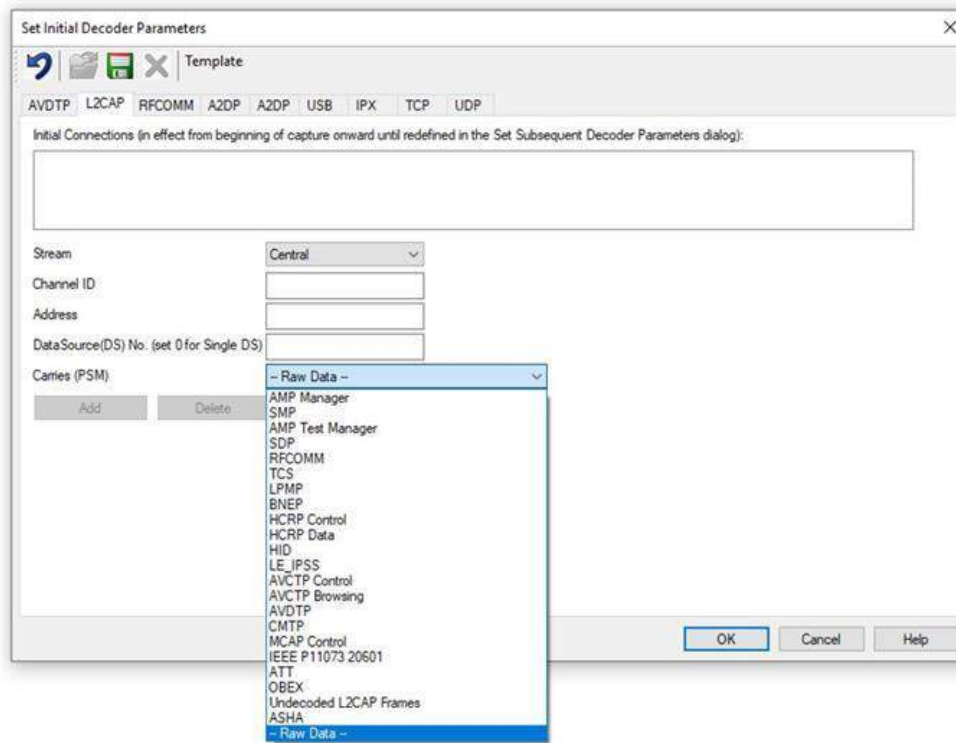


Figure 3.109 - List of Carries (PSM) Protocols

### Adding, Deleting, and Saving L2CAP Parameters

1. From the **Set Initial Decoder Parameters** window, click on the **L2CAP** tab.
2. Set or select the **L2CAP** decoder parameters.

3. Click on the **ADD** button. The Initial Connection window displays the added parameters.

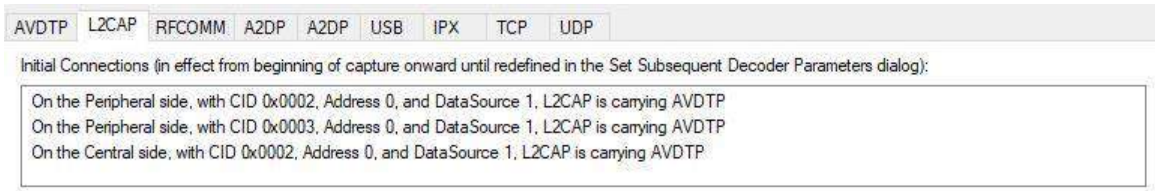


Figure 3.110 - Parameters Added to Decoder

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

### 3.4.4.2 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 -> Decoders -> Set Subsequent Decode Parameters** 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 figure below:

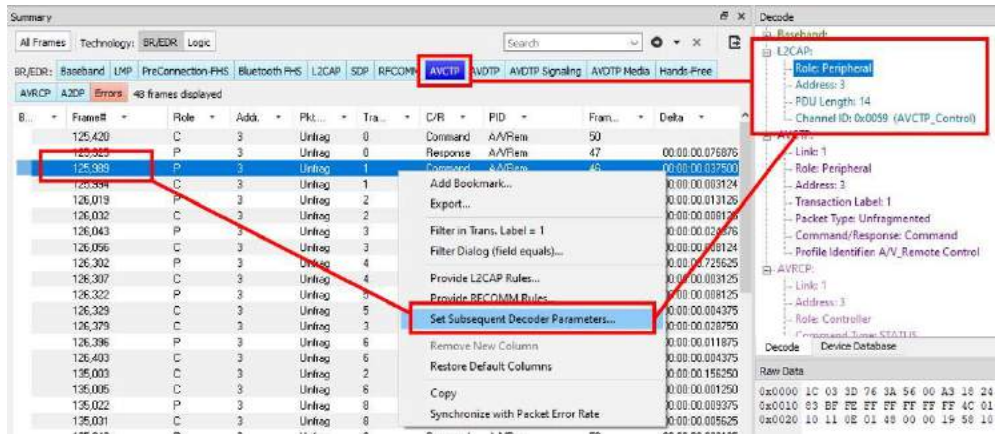


Figure 3.111 - L2CAP Set Subsequent Decoder Parameters

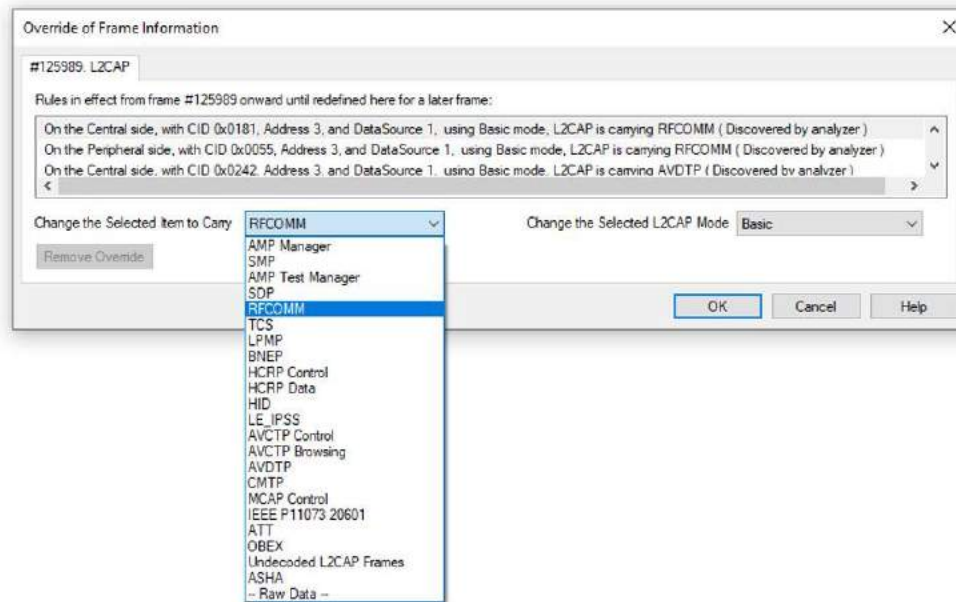


Figure 3.112 - Options to Choose From

1. Change the L2CAP parameter by selecting from the rule to change, and click on the listed parameters.
2. 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**.
3. Click **OK**.

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

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

### 3.4.5 RFCOMM Decoder Parameters

#### 3.4.5.1 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.

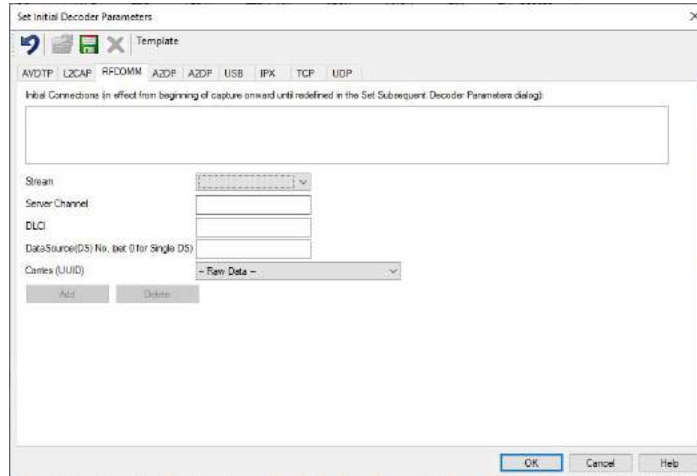


Figure 3.113 - RFCOMM parameters tab

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 (central or central)
- **Server Channel** - The *Bluetooth*<sup>®</sup> channel number 0 through 78
- **DLCI** - This is the Data Link Connection Identifier and identifies the ongoing connection between a client and a server
- **Data Source (DS) No.**- When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source

**Carries (UUID)** - Select from the list to apply the Universal Unique Identifier (UUID) of the application layer that RFCOMM traverses to from the following:

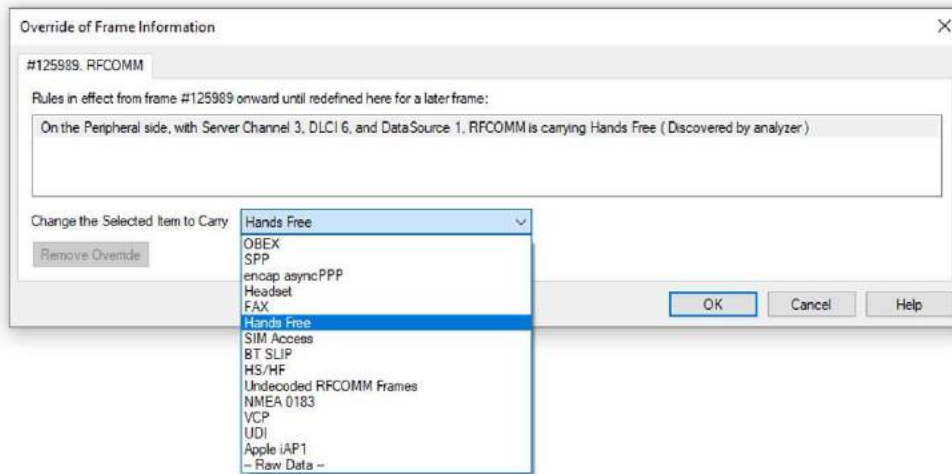


Figure 3.114 - RFCOMM Selected Item to Carry

## Adding, Deleting, and Saving RFCOMM Parameters

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

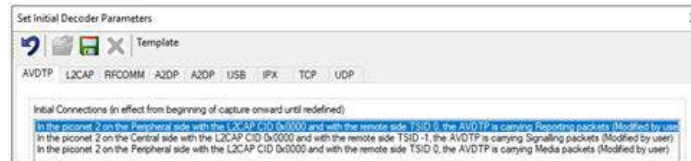


Figure 3.115 - Initial Decoder Parameters window

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 191](#)

### 3.4.5.2 RFCOMM Missing Decode Information

Wireless Protocol Suite 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 **Summary 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.

### 3.4.5.3 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 -> Decoders -> Subsequent Decoder Parameters** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.

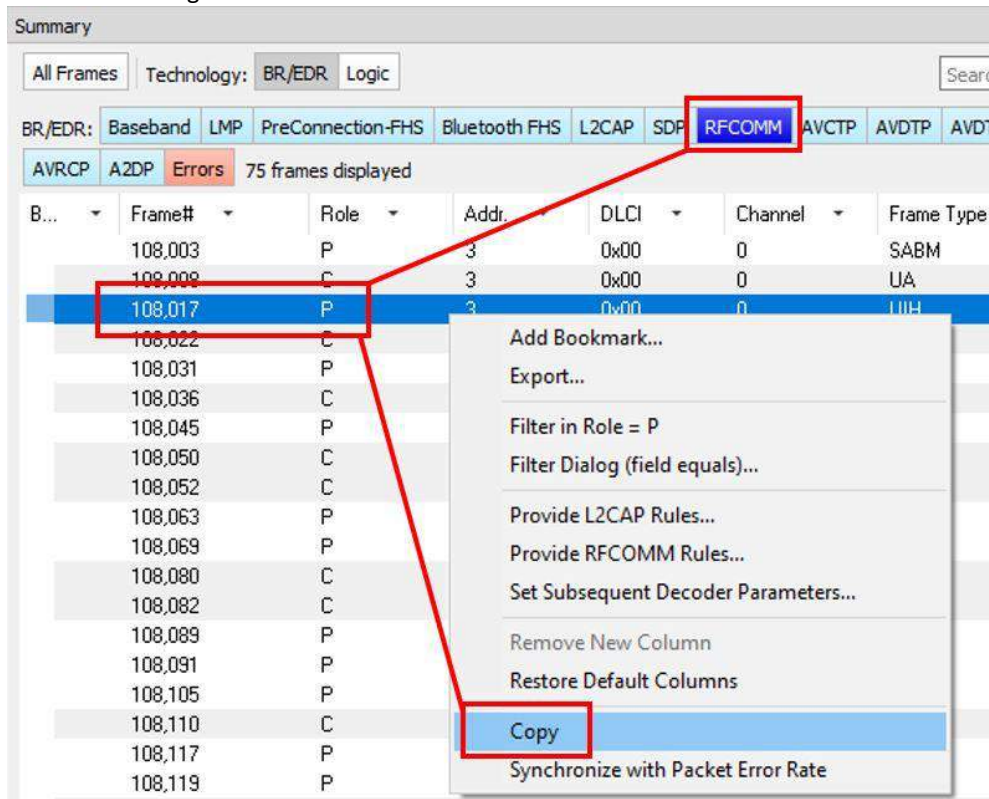


Figure 3.116 - Drop Down Menu

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.



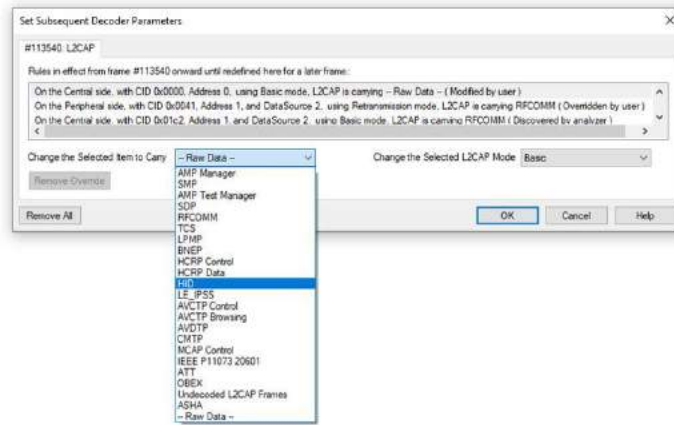


Figure 3.117 - Set Subsequent Decoder Parameters selection list

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

### 3.4.6 Determining Central and Peripheral

In *Bluetooth*, the device that initiates the connection is always the central at connection time. You only need to know the central and peripheral at connection time when setting up the I/O Settings. Afterward, a role switch may occur, but the analyzer automatically follows the role switch.

**Note:** You do not have to identify a Central address if you are using Firmware Version 62 or newer.

### Role Switches

After the connection has been made, a role switch can take place. A good example of why this happens would be when a mouse connects to the PC. The mouse initiates the connection, so it is the central. After the connection is made, a role switch occurs so that the PC becomes the central and the mouse becomes a peripheral. The role switch takes place because the PC may be working with multiple devices at the same time, and as such, the PC would not be a central of more than one device.

Let us say that a link exists between a PC and a keyboard with the PC as central. If the mouse wants to become a member of the link, it initiates the connection. Since the mouse initiated the connection, it is the central of a new link and the PC is the peripheral. The PC is still the central of the link between the PC and keyboard. A role switch now occurs between the PC and the mouse, and the PC is now the central of a link with two peripherals: the mouse and keyboard.

### 3.5 Conductive Testing

Conductive testing could be used for many reasons, but the most common use is to isolate the Bluetooth or Wi-Fi test setup from the surrounding environment. Interference from radio frequency (RF) sources is the most common reason for isolating the test from the environment. This is especially important when the environment contains RF sources using the industrial, scientific, and medical (ISM) radio bands from 2.4 to 2.485 GHz that are the bands used for Bluetooth or Wi-Fi.



“Conductive” in this context means that you are not “air sniffing”, that is, capturing Bluetooth or Wi-Fi transmissions on the Frontline analyzer's antenna. The conductive test setup uses coaxial cable to directly connect the Device Under Test (DUT) to the analyzer's antenna connectors. The coaxial cable provides the isolation from the environment through shielding.

### 3.5.1 Classic *Bluetooth* Transmitter Classes

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

[Table 3.35 - Classic Bluetooth Power Classes below](#) lists the maximum power and operating range for each Classic *Bluetooth* Class.

Table 3.35 - Classic *Bluetooth* Power Classes

Class	Maximum Power	Operating Range
1	100 mW (20 dBm)	100 meters
2	2.5 mW (4 dBm)	10 meters
3	1 mW (0 dBm)	1 meter



**Caution:** Good engineering judgment is essential to protecting both the Frontline Bluetooth analyzer and the devices under test from power levels that could cause damage. The procedures contained here are general guidelines for connecting the equipment for conductive testing.

### 3.5.2 *Bluetooth* Low Energy Transmitter

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

[Table 3.36 - Bluetooth Low Energy Transmitter below](#) lists the maximum power and operating range for *Bluetooth* Low Energy transmitters.

Table 3.36 - *Bluetooth* Low Energy Transmitter

Bluetooth SIG Specification	Maximum Power	Operating Range
Up to 4	10 dBm (5 mW)	50 meters



**Caution:** Good engineering judgment is essential to protecting both the Frontline Bluetooth analyzers (Sodera, Sodera LE, X240 and X500) and the devices under test from power levels that could cause damage. The procedures contained here are general guidelines for connecting the equipment for conductive testing.

### 3.5.3 Conductive Testing

#### Test Equipment

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

1. Coaxial cable with adapter for connecting to DUT 1.
2. Coaxial cable with adapter for connecting to DUT 2.
3. Coaxial T-connector.
4. SMA adapters for connecting coaxial cable or attenuators to the Frontline antenna connectors.
5. Attenuators, values depending on the *Bluetooth* technology or DUT power output levels.
6. Sodera Wideband *Bluetooth* Protocol Analyzer.
7. Personal computer for running Wireless Protocol Suite software.

#### Test Setup

[Figure 3.118 below](#) shows the conductive test setup. The values of AT1, AT2, and AT3 depend on the power transmitted by DTU 1 and DTU 2.

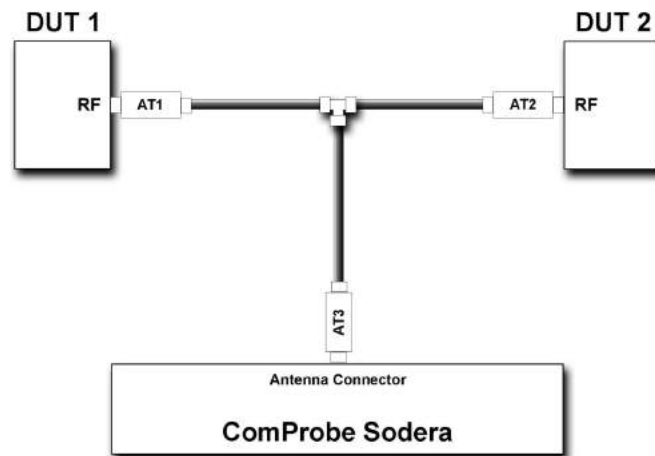


Figure 3.118 - Sodera/X240/X500 Conductive Test Setup

The AT1 through AT3 attenuator values will depend on the DUT1 and DUT2 transmitter Class or the transmit power from each device. At higher power levels, all three attenuators may be needed. In all cases, use good engineering practices to protect the devices under test and the Sodera hardware from damage, to ensure reliable operation.

For example, assume that there is no attenuation in the test setup:

- At the T-connector, the power will split in half. For example, if DUT1 is a Class 1 device transmitting +20 dBm (100 mW) (at the T-connector) the power will be split with +17 dBm (50 mW) going to DUT2 and +17 dBm (50 mW) going to the antenna connector. Adding additional attenuation with AT1, AT2, AT3, and the **Record**

**Options** -> **RSSI Threshold** selection will further reduce the input power level to the Soderaradio.

- If DUT1 or DUT2 is a Class 2 device, +10 dBm (12.5 mW) will reach the antenna connector. If they are Class 3 devices, -3 dBm (0.5 mW) will reach the antenna connector.

If the protocol analysis results prove to be unreliable, adjust the AT1, AT2, or AT3 values and the Soderaradio **Record Options** -> **RSSI Threshold** settings to achieve reliable results.

### 3.5.4 Soderaradio LE Conductive Testing

#### Test Equipment

While exact conductive test setups are dependent on the specific circumstances surrounding the DUT RF interface, the following equipment is required for all testing situations.

1. Coaxial cable with adapter for connecting to DUT 1.
2. Coaxial cable with adapter for connecting to DUT 2.
3. Coaxial T-connector.
4. SMA adapters for connecting coaxial cable or attenuators to the Soderaradio LE **Antenna** and **Wired** connectors.
5. Attenuators, values depending on the *Bluetooth* technology or Class being tested.
6. Frontline Soderaradio LE Wideband *Bluetooth* Low Energy Protocol Analyzer.
7. Personal computer for running Wireless Protocol Suite software.

#### Test Setup

The following figures show the conductive test setup. The values of AT1, AT2, and AT3 depend on the power transmitted by DUT1 and DUT2 and which setup is used.

**Note:** Internal Soderaradio LE attenuation options are likely to preclude the use of external attenuators when using typical *Bluetooth* Low Energy power levels.

#### Wired Input Test Setup

[Figure 3.119 - Soderaradio LE Conductive Test Setup \(a\) on the next page](#) connects the test signal to the Soderaradio LE **Wired** input connector. This input provides internal 27 dB attenuation, so AT3 may not be necessary depending on the DUT1 and DUT2 transmitted power.

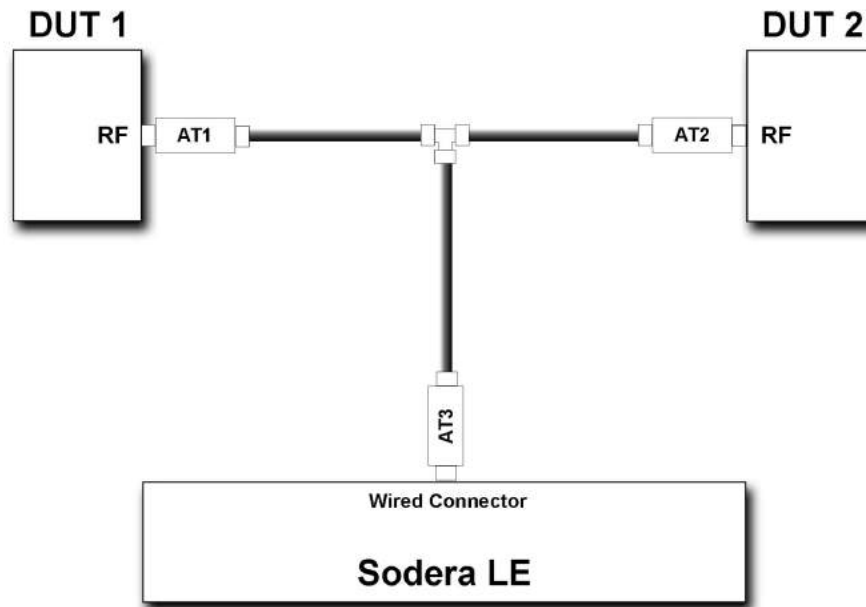


Figure 3.119 - Sodera LE Conductive Test Setup (a)

The AT1 through AT3 attenuator values will depend on the DUT 1 and DUT 2 transmitter Class or the transmit power from each device. At higher power levels, all three attenuators may be needed. In all cases, use good engineering practices to protect the devices under test, the Sodera hardware from damage and to ensure reliable operation.

For example, assume that there is no attenuation in the test setup (a): At the T-connector, the power will split in half. For example, if DUT 1 is transmitting +20 dBm (100 mW), at the T-connector it will split with +17 dBm (50 mW) going to DUT 2 and +17 dBm (50 mW) going to the Sodera LE **Wired** connector. The Wired connector will provide an additional 27 dB attenuation after the connector reducing the 50 mW to -283 dBm ( $5 \times 10^{-26}$  mW). This example points out that for conductive testing, the **Wired** connector is best for larger RF signals.

#### Antenna Input Test Setup

[Sodera LE Conductive Test Setup \(b\) on page 209](#) shows an alternate test setup that connects the devices under test to the Sodera LE **Antenna** connector. This setup provides a wider range of control over the internal attenuation. To use the variable attenuator on the **Antenna** input, the Sodera LE unit must be configured by selecting **Record Options** from the **Options** menu. Select the **Manual Attenuation** in the **Gain Control** section. With this control you can select Sodera LE internal attenuation between 0 and 32 dB in 1 dB steps. Refer to Sodera LE [Record Options dialog on page 1](#) for additional information about this control.

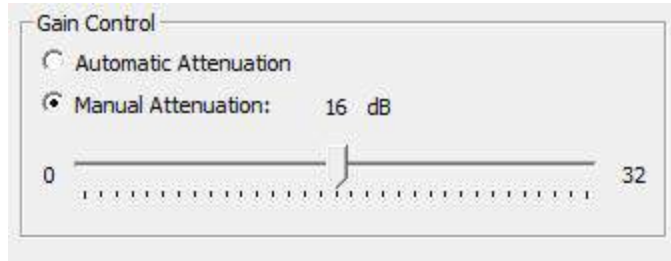


Figure 3.120 - Sodera LE Record Options Gain Controls

The AT1 through AT3 attenuator values will depend on the DUT1 and DUT2 transmitter Class or the transmit power from each device. At higher power levels all three attenuators may be needed. In all cases, use good engineering practices to protect the devices under test and the Sodera hardware from damage, and to ensure reliable operation.

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

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

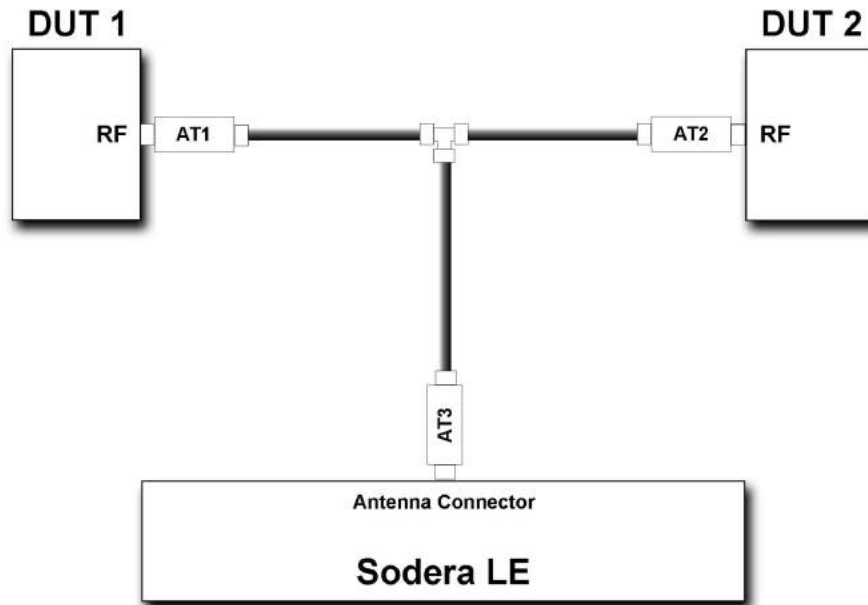


Figure 3.121 - Sodera LE Conductive Test Setup (b)

### 3.5.5 Bluetooth Conductive Test Process

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

**Note:** For the X500 the connection should be to BT Rx1.

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

### 3.5.6 802.11 Wi-Fi Conductive Testing

“Conductive” in this context means that you are not “air sniffing”, that is, capturing 802.11 transmissions on the Frontline 802,11 analyzer antenna. The conductive test setup uses coaxial cable to directly connect the DUT (Device Under Test) to the analyzer antenna connectors. The coaxial cable provides the isolation from the environment through shielding.

#### Test Equipment

The following equipment is required for the test setup. All cables, connectors and adapters, and attenuators should be relatively flat from 2 GHz to 6 GHz.

1. Coaxial cable All cable must be 50Ω and should be double shielded.
2. Coaxial T-connectors, 50Ω.
3. RP.SMA adapters for connecting coaxial cable or attenuators to the antenna connectors, 50Ω.
4. AT1 - AT9: 20 dB attenuators, 50Ω.
5. Frontline 802.11 Wi-Fi protocol analyzer.
6. Computer for running Wireless Protocol Suite software.

#### Test Setup

[Figure 3.122 on the facing page](#) shows the 802,11 conductive test setup.

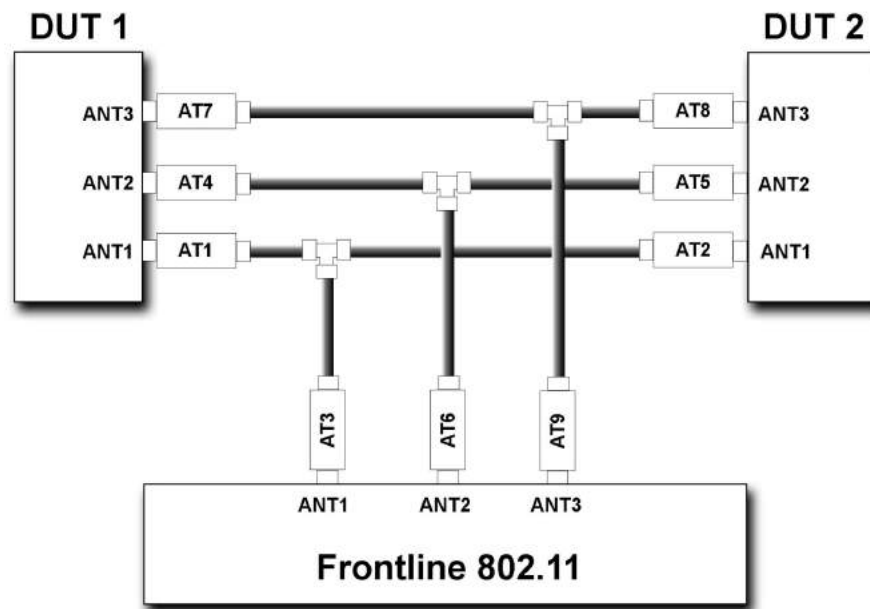


Figure 3.122 - Frontline 802.11 Conductive Test Setup for 3X3 MIMO

The above test setup is for 3X3 MIMO 802.11 devices. If not testing this configuration, the ANT3 connection to the DUTs and the Frontline 802.11 is not used.

### Test Process

After connecting DUT1, DUT2, and the Frontline 802.11, follow these steps to capture Wi-Fi data.

1. Establish data transmission between DUT 1 and DUT 2.
2. Begin capture of the data with the Frontline 802.11.
3. Conduct protocol analysis with the Wireless Protocol Suite software on the personal computer or save the capture file for future analysis.

## Chapter 4 Capturing Data

The following sections describe the **Wireless Protocol Suite** software functions that capture data packets.

### 4.1 Air Sniffing: Positioning Devices

When capturing over the air packets, proper positioning of the Frontline hardware and the Devices Under Test (DUTs) will result in the best possible captures and will mitigate sources of path loss and interference. The X500 uses Antenna Diversity to simplify these issues. Section 4.1.1 elaborates on using Antenna Diversity with the X500, while Section 4.1.2 describes procedures with the X240 and Soderia to help optimize the capture process especially if you have problems obtaining reliable captures.

#### 4.1.1 Capturing using X500 with Antenna Diversity

The X500 is configured to use Antenna Diversity for capture to improve performance and eliminate the need to place the unit in a specific position when wireless channels are affected by multipath, fading, and interference. The signal received from the two antennas (BT Rx1 and BT Rx2) are added by an intelligent algorithm which adjusts the antenna weighting to maximize signal strength. The algorithm uses the spatial diversity of the antennas for three benefits. First, it increases the probability of having a channel which isn't in a fading null. Second, it reduces the probability that a channel is interference-limited from another transmitter on the same or nearby frequency. Third, the extra antenna increases the chance of less interference because generally the source of the interference isn't physically co-located with the wanted transmission. The Antenna Diversity algorithm runs on packet level granularity so that the improvement can be maintained over wide-band operation when capturing signals from multiple devices.

Antenna Diversity doesn't require a special setup by the user and is enabled by default in both AGC Manual and Auto modes. In AGC Manual mode a set attenuation is applied to both antenna channels. In AGC Auto mode the Antenna Diversity algorithm automatically determines attenuation to be applied to RF chain so that signal doesn't saturate.

For the general scenario, (See [Figure 4.1 below](#)) position the analyzer between the DUTs so each antenna will receive a better signal from the DUT which it is near as shown. Either DUT can be paired with either antenna (BT Rx1 or BT Rx2). The algorithm will automatically recognize and take advantage of this setup. No additional setup is required in the Wireless Protocol Suite software.



Figure 4.1 - Capture setup with Frontline X500 using Antenna Diversity



### 4.1.2 Using the x240 and Soderia with indoor radio propagation

#### Problems with indoor radio propagation

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

#### Estimating indoor propagation loss

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

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

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

#### Mitigating path loss and interference

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

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

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

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

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



Figure 4.2 - Devices Equally Spaced in the Same Horizontal Plane

Finally, eliminate other RF sources.

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

### Positioning for wideband capture

Frontline Bluetooth analyzers (Sodera, Sodera LE, X240) can capture from multiple devices, which requires a different approach to position the DUTs and the analyzer. When testing more than two devices, arrange the DUTs on the perimeter of a circle 1-2 meters in diameter for Bluetooth transmitter Class 1 and 2 devices. For transmitter Class 3 DUTs, the circle should be 1/2 meter in diameter. Equally space the DUTs on the perimeter. Place the Sodera in the center of the circle. If not using the Sodera Excursion mode, connect the computer and place it outside the circle as far away from the DUTs as possible.

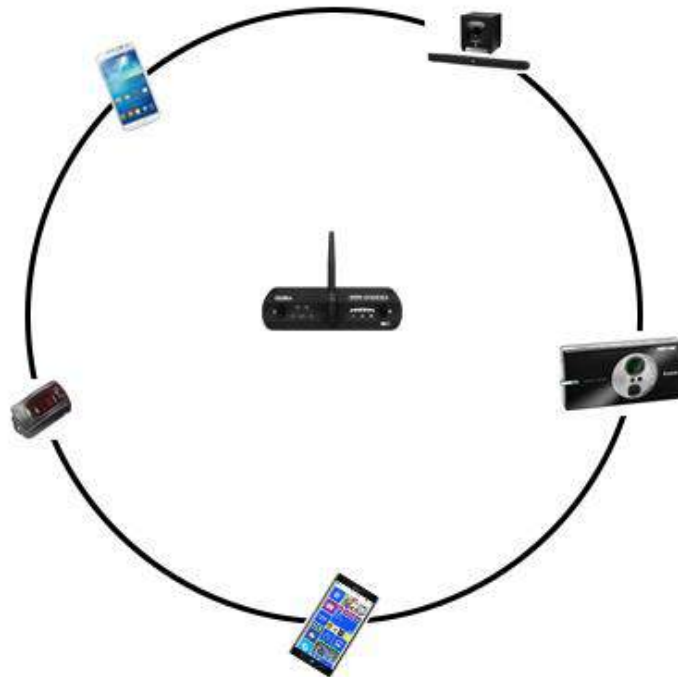


Figure 4.3 - Wideband Capture: Devices Equally Spaced in the Same Horizontal Plane

### Positioning for audio capture

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

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

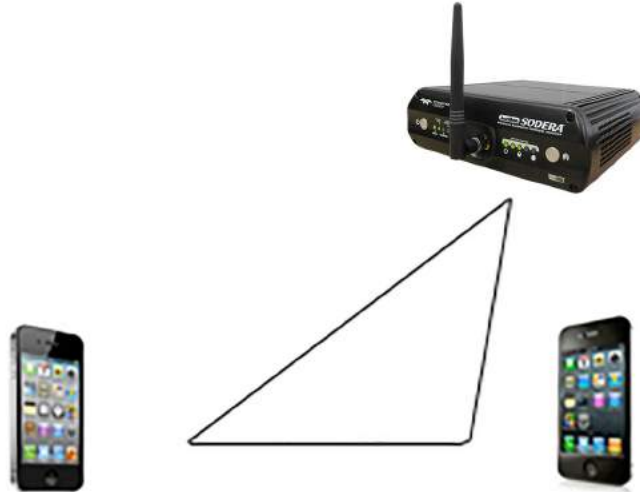


Figure 4.4 - For Audio A2DP, Position Closer to SINK DUT

### Poor Placement

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

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

## 4.2 Capturing Data: Introduction

Data capture using Frontline *Bluetooth* analyzers (Sodera, Sodera LE, X240) will capture data from all devices with active connections within range of the analyzer. Once a session is started, the capture is initiated and the data is recorded. The analysis mode can begin. The user must select specific devices. The user can select from all devices that are actively communicating. The user can also select devices from a prior capture, when available, before recording. The data captured only from selected devices is sent to the **Wireless Protocol Suite** for event- and protocol-level analysis.

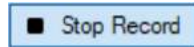
### 4.2.1 Record: Begin Capture

When starting a capture session all of these actions occur:

- The active status of all devices is cleared in the **Device Database** pane and the **Wired Devices** pane.
- The **Security** pane is emptied.
- The **Event Log** pane retains all prior logged events.



On the **Wireless Protocol Suite** Toolbar, click on the **Start Record** button or select **Start Record** from the **Capture** menu option. The **Start Record** button is also available in the **Wireless Protocol Suite** main window. In the Main window you can also select **Start Recording** from the **Capture** menu option. When the **Start Record** button changes to **Stop Record**, the Soderia hardware is capturing data from all active *Bluetooth* devices within range and is recording data on the PC.



On the **Wireless Protocol Suite** Toolbar, clicking on the **Stop Record** button, or selecting **Stop Recording** from the **Capture** menu options will halt live capture. From the Main window you can click the **Stop Record** button or select **Stop Recording** from the **Capture** menu list to stop recording as well. Alternately Start Record/Stop Record can be activated by the keyboard shortcut of Ctrl+E.

The **Device Database** View populates with any newly discovered devices. Selecting devices for analysis can be done while recording.

The **Security** View will show all encrypted *Bluetooth* links.

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

The **Status Bar** will show a running total of captured packets.

**Note:** Starting a new capture session will clear all unsaved data from both the Soderia hardware and the **Wireless Protocol Suite**. If it has not been saved, then a pop-up warning message will appear.

## 4.2.2 Selecting Devices for Analysis

Once a capture session starts by clicking on **Start Record** on the Main Window Toolbar, data from all active devices within range or data from wireless or wired connections is being captured. To analyze the data using the **Wireless Protocol Suite**, select specific devices of interest to include in the analysis.

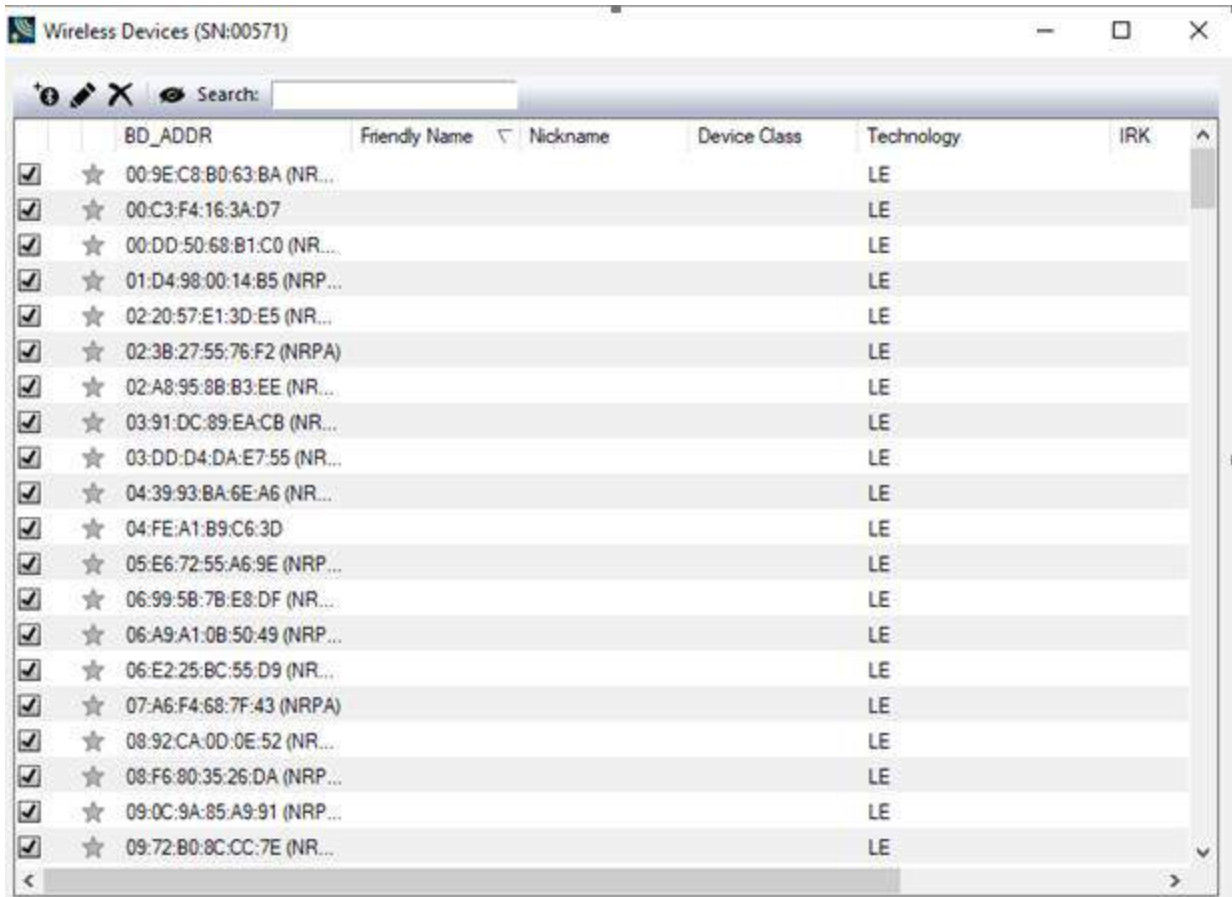


Figure 4.5 - Device Database View

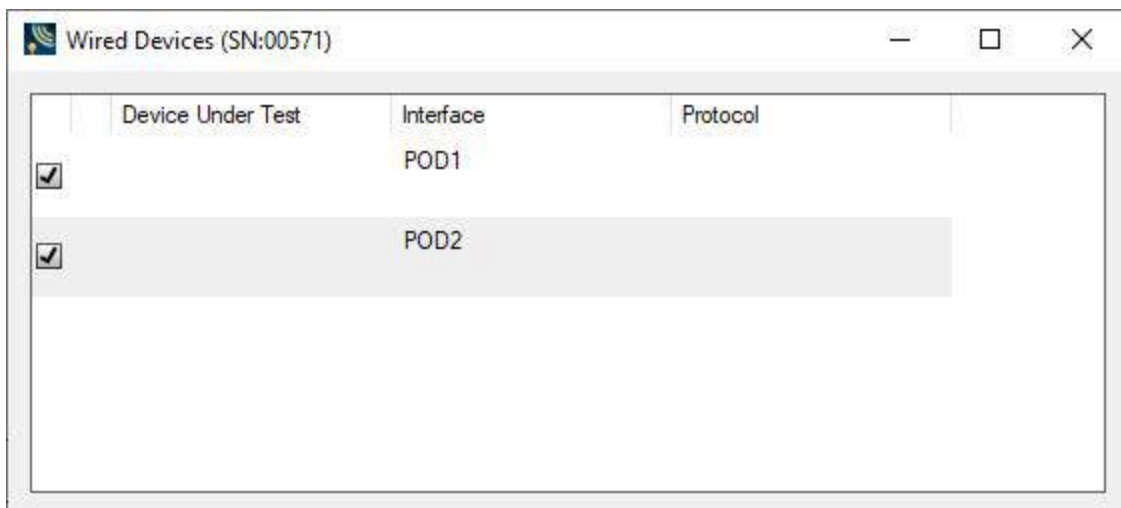




Figure 4.6 - Wired Devices View

In the **Device Database** view, place a check in the row of each active device   to be analyzed. Active devices can also be selected while the recording is in process.

**Note:** Data filtered by the device selection is an “OR” function, not an “AND” function. When selecting device1, device2, device3,... the recorded data filtered into the analyzer is data involving device1 OR device2 OR device3 OR .... However, if in the Options menu, analysis of LE Empty packets is selected, an AND function is included. For example: (device2 AND LE Empty packets) OR (device3 AND LE Empty packets).

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

Table 4.1 - Common Data Capture and Device Selection Scenarios

Scenario	Wireless/Wired Devices View Selection
Analyzing traffic between a Peripheral Device Under Test (DUT) and its Central.	Select only the Peripheral DUT for analysis
Analyzing all traffic involved in Inquiries	In the Options menu select <b>Analyze Inquiry Process Packets</b>

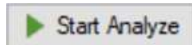
The Frontline Bluetooth analyzer is now ready to begin protocol- and event-level analysis.

Once Devices are selected, analysis of the capture can begin.

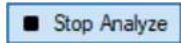
### 4.2.3 Starting Analysis



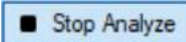
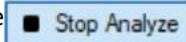
The analysis begins by clicking on the **Start Analyze** button in the **Wireless Protocol Suite** Main window. The Soder LE analyzer will begin sending captured packets involving the selected device to the **Wireless Protocol Suite**.



The analysis begins by clicking on the **Start Analyze** button or Selecting **Start Analyze** from the **Capture** menu. Alternatively, click on the **Start Analyze** button in the **Wireless Protocol Suite** Main window. In the Main window you can also select **Start Analyzing** from the **Capture** menu. The Soder analyzer will begin sending captured packets involving the selected device (s) to the Wireless Protocol Suite software.

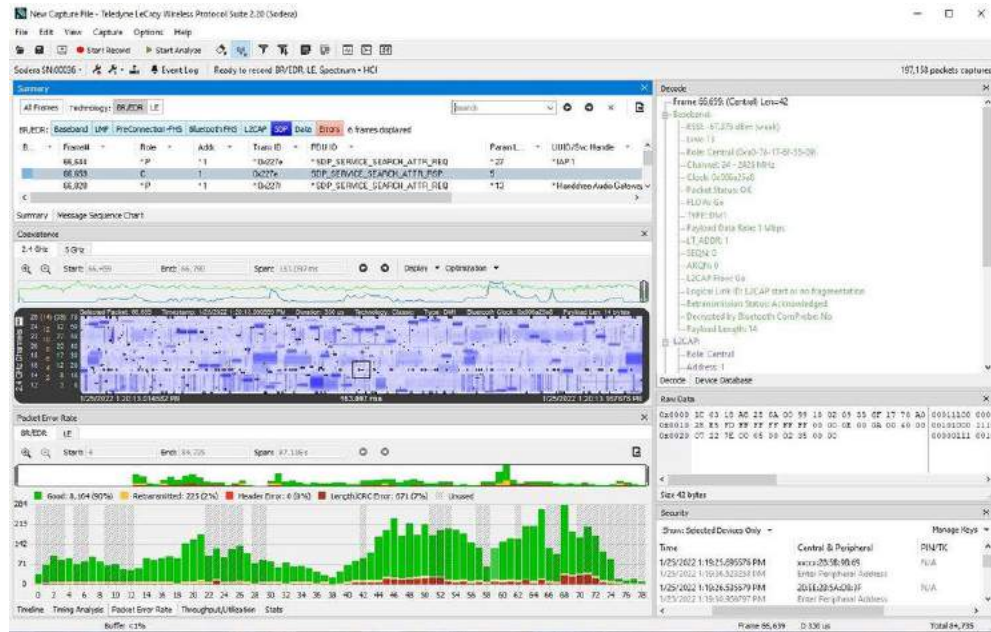


Once analysis has begun, you cannot change the device selection. All device rows in the **Device Database** View are grayed-out. To stop the analysis, click on the **Stop Analyze** button. You can then change your device selection and restart analysis by clicking on the **Start Analyze** button.

To stop the analysis, click on the  button in the Soder datasource or click the  button on the **Wireless Protocol Suite** Main window You can also select the **Stop Analyze** option in the **Capture** menu or **Stop Analyzing** option in the **Capture** menu in the Main window as well. Alternately Start Analyze/Stop Analyze can be activated by the keyboard shortcut of Ctrl+Shift+E.


Conducting analysis from a capture file is identical to the live capture method.

#### Wireless Protocol Suite: Main Window



## 4.2.4 Hardware Signal Too Strong Indication

When the software has detected an RF signal that is *too strong*, warnings will appear in several places.

- [Event Log View on page 165](#) - Displays "Received signal too strong to capture data reliably." with a Warning icon . The event is added to the log as soon as the conditions for a *too strong* signal have been detected. A signal that is *too strong* can cause errors in the decoding process.



**Caution:** The Frontline Bluetooth analyzers (Sodera, Sodera LE, X240 and X500) will continue to capture after a *too strong* signal detection, which may compromise the decoded packet integrity.

- Status Bar (see [Wireless Protocol Suite Analyzer Toolbars on page 80](#),) - Displays "SIGNAL TOO STRONG".

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

### Conditions for "too strong" RF signal

The software will determine that a received signal is too strong based on the following conditions.

- X500, X240, Sodera:
  - o Normal Gain **Record Options** setting (see [Analyzer Toolbar on page 238](#)) - 5 or more packets with RSSI greater than or equal to -20 dBm within the past 5 seconds.




o Reduced Gain **Record Options** settings (see [Analyzer Toolbar on page 238](#)) - 5 or more packets with RSSI greater than or equal to -0.5dBm or higher within the past 5 seconds.

- Sodera LE: a packet with a RSSI greater than -27 dBm.

### Signal too Strong reset

When the software has determined that the RF signal has returned to a *safe* condition from a *too strong* condition, the following will occur.

- [Event Log View on page 165](#) - Displays "Received Signal Strength OK" with an Information icon . The event is added to the log as soon as the conditions for a *safe* signal have been detected.
- Status Bar - No display of signal strength.

### Conditions for Signal too Strong reset

The software will determine that a *too strong* signal has returned to a *safe* status based on the following conditions.

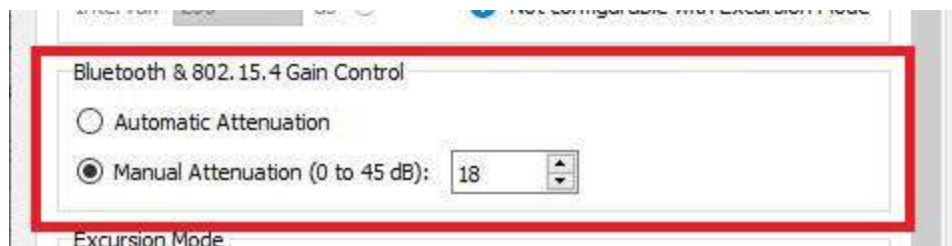
- Normal Gain **Record Options** setting (see [Analyzer Toolbar Menu and Icons on page 81](#))- No packets with RSSI greater than -24 dBm within the last 5 seconds.
- Reduced Gain **Record Options** -> **General** settings (see [Analyzer Toolbar Menu and Icons on page 81](#)) - No packets with RSSI greater than -4.5 dBm within the last 5 seconds.

### Suggested Corrective Action

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

On X500, X240, and Sodera LE, the gain can be adjusted by using the Record Options Gain controls.

Example Gain controls from X500 are shown below. Similar controls exist for X240 and Sodera LE.



Try adjusting the Manual Attenuation from the Record Options dialog then try capturing again. Repeat until successful capture is achieved.

For the Sodera LE, another action to take is to move the antenna from the Antenna connector to the Wired connector. Try capturing again.

## 4.2.5 Excursion Mode Capture & Analysis

**Note:** The Excursion Mode feature is supported on Sodera and X240 hardware only.

Capturing data in Excursion mode is accomplished without the hardware being connected to a computer. The captured data is stored on the hardware for later access and analysis when connected to a computer.

The hardware must be configured for Excursion mode while connected to a computer running the **Wireless Protocol Suite** software.

### Excursion Data Capture Mode

To enable Excursion Data Capture Mode, follow the steps below:

Configure the record options for the hardware using the **Record Options** dialog. The record options you select will be stored to the hardware and applied during the excursion mode capture. For example, if you wish to only capture LE traffic, then you must make sure the hardware is configured to only capture LE traffic using the **Record Options** dialog. Finally, to enable Excursion mode on the hardware, you must select the "Enable Excursion Mode" record options, as shown in Figure 4.7.

The figures below show the Excursion Mode option using the X500 analyzer.



Figure 4.7 - Wireless Protocol Suite: Record Options

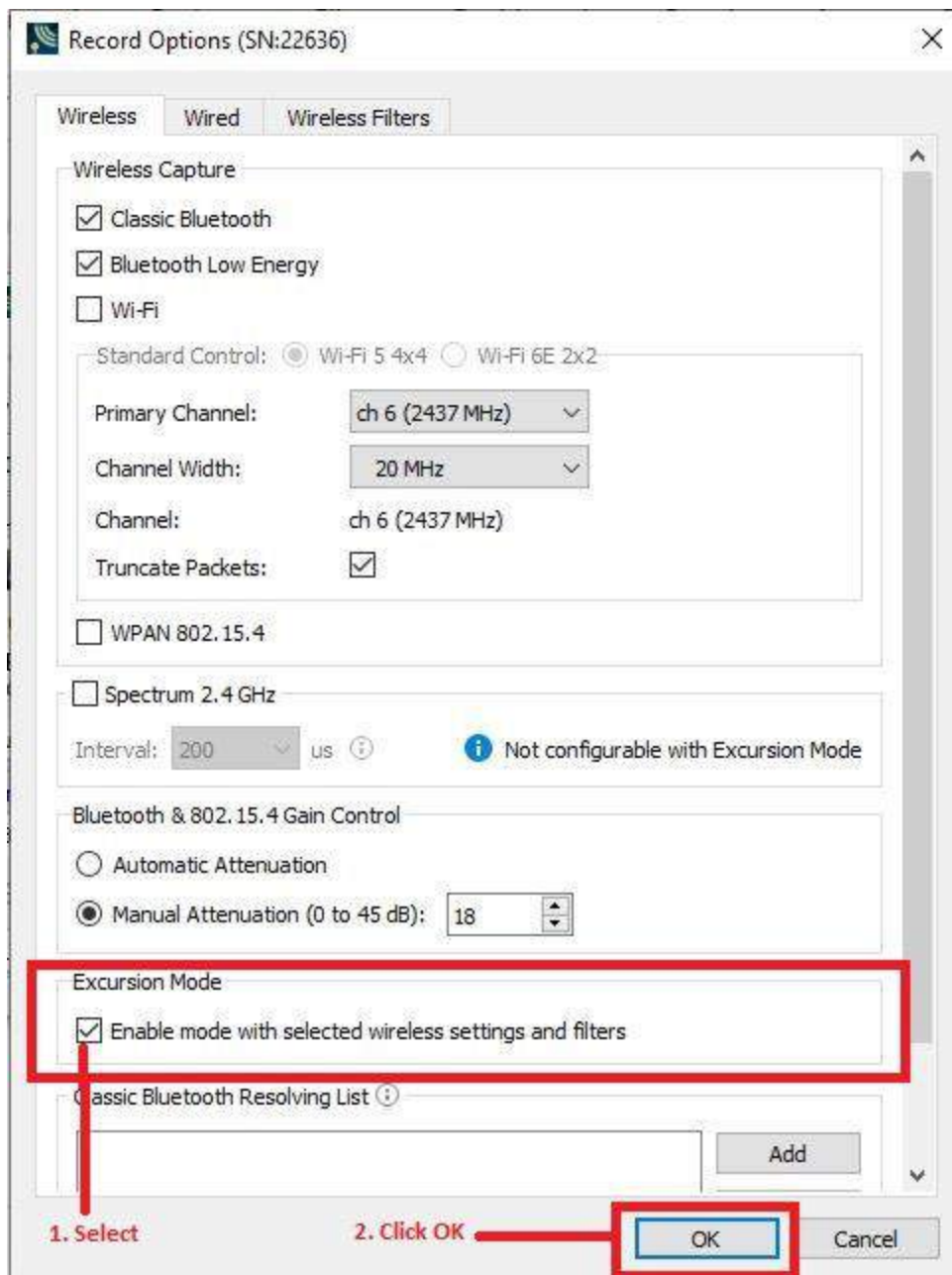


Figure 4.8 - Excursion Mode Enabled

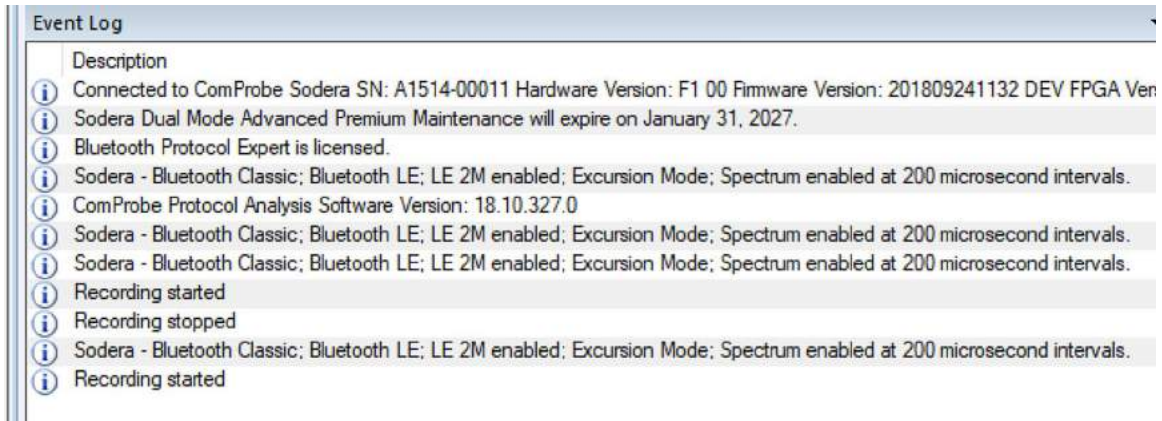


Figure 4.9 - Event Log Shows Sodera in Excursion Mode

To capture in Excursion mode, disconnect the hardware from the computer.

1. Apply power to the hardware with external power or using the internal battery power. See [Applying Power on page 44](#).
2. Press the Capture button on the front panel (right side). The **Capture** LED will illuminate a steady green light when capturing data.

To stop capturing data,

1. Press the Capture button on the analyzer's front panel.
2. After a brief delay, the **Capture** LED will turn off. The capture file is saved to the hardware.

Starting a new capture will save the captured data in a new capture file.

Each capture collected in Excursion mode (a start/stop sequence) is stored as a separate date and timestamped capture file in the hardware. Each capture file can be selectively analyzed upon reconnecting to the **Wireless Protocol Suite**, (see following section).

### Limitations to Excursion Mode Capture

The only limitations to Excursion mode capture are:

- Battery life in X500: X500 hardware has an external battery which has about two hours operating life under typical RF conditions. In the case of capture periods exceeding two hours, connect the X500 hardware to an external power source.
- Battery life in Sodera: Sodera hardware has an internal battery which has an hour operating life. In the case of capture periods exceeding one hour, connect the Sodera hardware to an external power source.
- Battery life in the X240: The X240 does not have an internal battery. It can be powered via a USB Type C PD external battery backup, such as HYPERLINK "<https://a.co/d/bpMZqXP>" Charmast USB C Power Bank, 26800mAh, for Excursion mode. Under typical RF conditions, the 26800mAh battery allows about 4 hours of capture time in the dual mode configuration.

- Internal memory - The X240, and X500 analyzers have 64 GB of internal storage that is used to hold Excursion Mode captures. Soderia has 32GB of internal storage. This storage can be managed using the Wireless Protocol Suite on a computer. This storage can be managed using the **Wireless Protocol Suite** on a computer.
- Number of Excursion Mode captures - There can be no more than 255 Excursion mode captures stored on the hardware. Refer to [Manage Excursion Mode captures dialog on page 84](#) for instruction on how to delete Excursion mode capture files from the hardware unit.

### Analyzing Data from Excursion Mode Capture

The procedure for protocol analysis of data captured in Excursion mode involves connecting the hardware to a computer, recording a capture that was previously stored on that hardware unit, and analyzing the data using the **Wireless Protocol Suite**.

1. Connect the hardware that contains the Excursion Mode capture to be analyzed, to a computer.
2. Apply power to the hardware.
3. Open the **Wireless Protocol Suite**.
4. When the Main application window opens, press **Manage Excursion Mode** captures button on the analyzer toolbar. See the figures below as an example.



Figure 4.10 - Analyzer toolbar -> Manage excursion mode captures

The list of files recorded during **Excursion Mode** is shown below.

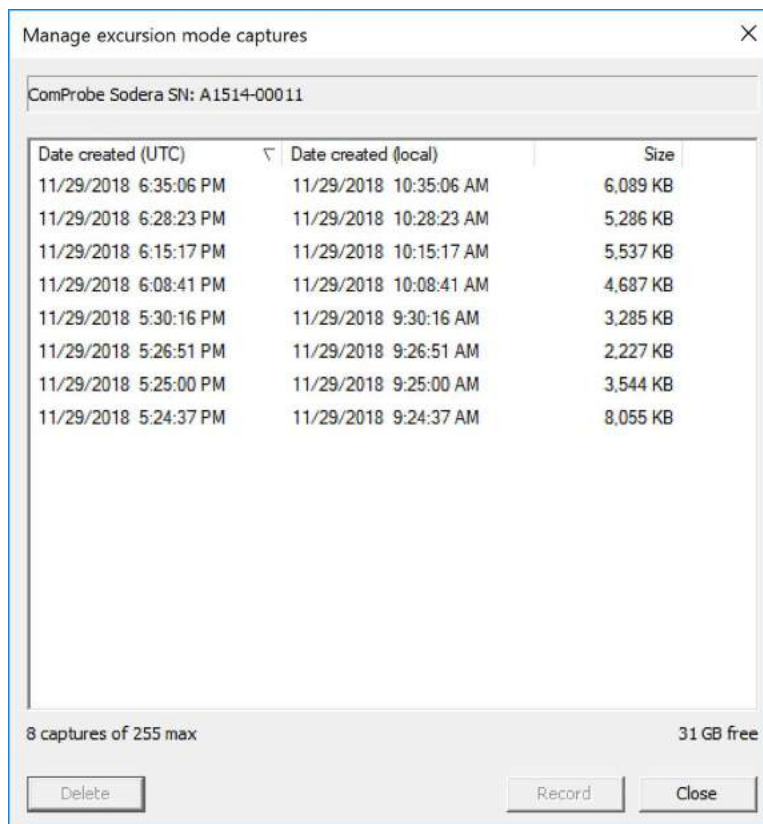


Figure 4.11 - Excursion Mode Files Captured

5. When the **Manage excursion mode captures...** dialog opens, select a capture to analyze. Click on the **Record** button, and the dialog will close. The hardware will begin behaving identically to how it handles a live capture. The Device Database View and Security View will populate with information from the selected Excursion Mode capture.
6. Follow the procedures in [Selecting Devices for Analysis on page 217](#).
7. Follow the procedures in [Record: Begin Capture on page 216](#).

## 4.2.6 Sodera Logic Event Capture and Analysis

Logic signal analysis is accomplished by capturing the logic signal using the Sodera HCI Pods. Captured logic event changes are mapped to packets that are recorded to the **Wireless Protocol Suite** software. To configure logic signal capture and analysis, select the POD(s) which are to be used for capture in **the Record Options** dialog as shown in the figure below.

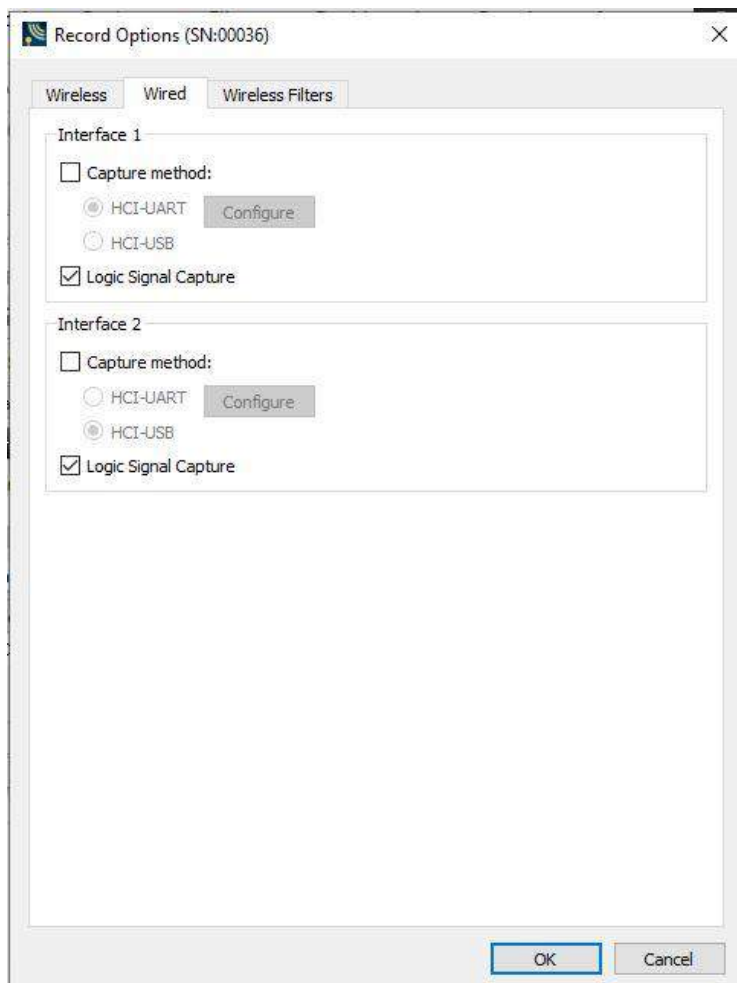


Figure 4.12 - Record Options: Wired Logic Analyzer

### Hardware Setup

Follow the procedures in [Logic Event Capture Configuration on page 55](#).

### Sodera Unit Configuration

On the Analyzer toolbar, press **Record Options** button and the **Record Options** dialog will open. Select the **Wired** tab and then select the **Logic Analyzer** Signal Pod(s) being used to capture the logic events.

Click **OK** to close the dialog.



## Recording the Capture

Click on the **Start Record** button. Logic events captured at the pods are placed in packets and sent to the host computer.

The captured logic events can be saved as a capture file for future analysis.

## Analyzing the Recorded Events

Logic level changes are recorded into packets. Each packet contains a single logic level change. View the packets in the **Wireless Protocol Suite Summary** view. Logic frames will have their own protocol tabs in the **Wireless Protocol Suite Summary** view.

### 4.2.7 Spectrum Analysis

Both Sodera and X240 hardware have an option to sample the 2.4 GHz RF spectrum at the hardware unit's antenna connector. The spectrum data represents the Received Signal Strength Indicator (RSSI) and is automatically saved when the capture is saved.

The spectrum data is synchronized in time to the received packets and is displayed in the Coexistence View 2.4 GHz Timeline when **Show Spectrum** is selected in the **Spectrum** menu on the **Coexistence View**.

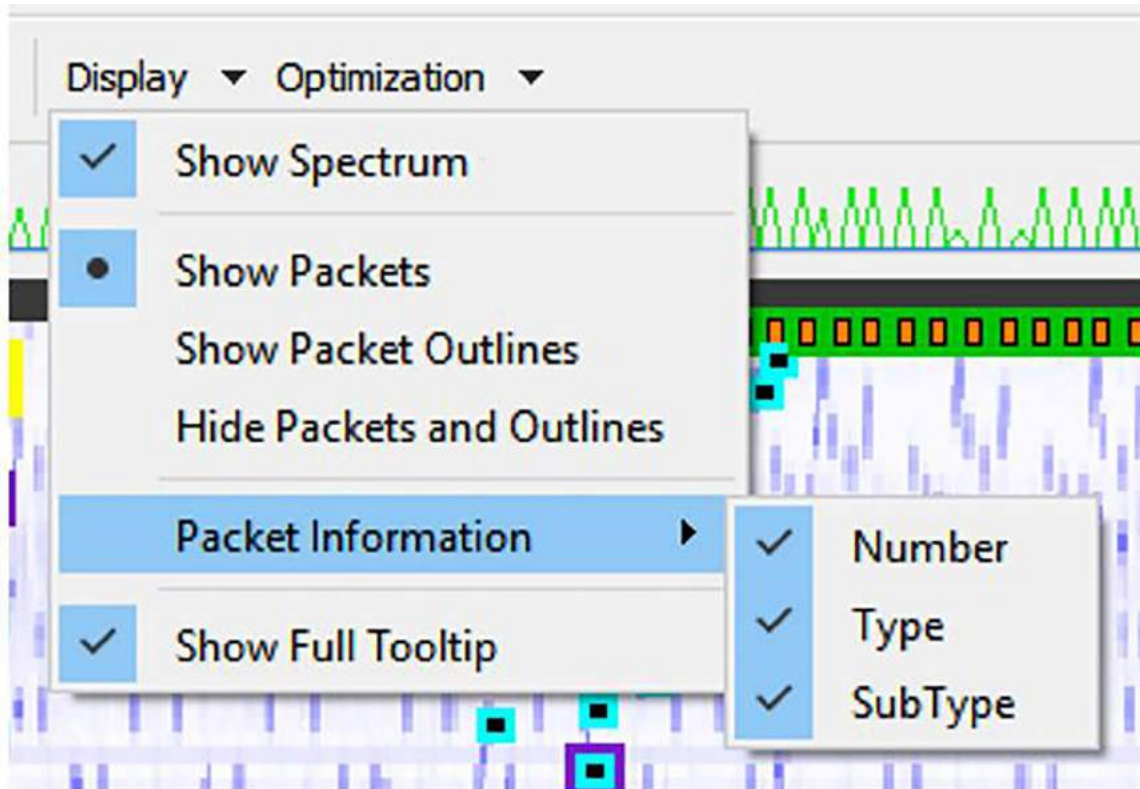


Figure 4.13 - Coexistence View: Spectrum Display

The spectrum power level is shown as a "heat map" behind the timeline packets. The "heat map" appears in shades of blue with darker blues representing higher power levels and lighter blues representing lower power levels (white represents the lowest power level). The darkest shade of blue represents -15dBm and above, while white represents -100 dBm and below.



**Note:** Too strong of a signal level is detected and noted in the Events Log View. See [Hardware Signal Too Strong Indication on page 220](#) for more information.

Spectrum data appearing in the **Coexistence View** that is not synchronized to a packet may indicate the presence of RF interference. Interference has the potential to degrade the *Bluetooth* signal.

The spectrum can be sampled at 20, 50, 100, or 200 microseconds. The Spectrum option and sample rate is set in the **Record Options** dialog. Refer to [Capture Toolbar on page 1](#) for information on capture settings. Smaller sample rate will cause an increase in memory used. However, identifying potential sources of interference may require more samples to avoid missing a signal.

**Note:** For Spectrum sample intervals less than 200 microseconds, the Soderia unit must be connected to a computer.

The spectrum data is saved automatically when the capture is saved. The saved spectrum data file has the file extension .swsd with the same basename as the .cfa file and in the same directory. (See [Changing Default File Locations on page 427](#) for information on default file locations.)

Currently, if a user opens a capture file and chooses to save the capture under a different name, a new.swsd file will not be created.

When copying capture files (.cfa, .scap, etc.) to a different directory, the user must also copy the spectrum data file (.swsd). If the spectrum data file is not present at the time the capture file is opened, spectrum data will not be available in the **Coexistence View**.

## 4.2.8 Critical Packets and Information for Decryption

After two Bluetooth devices are paired and the Bluetooth analyzers (Sodera/Sodera LE/X240) have captured data, the Wireless Protocol Suite software requires certain packets and information for successful post capture decryption.

### BR/EDR Legacy Encryption (E0)

The following information and packets are needed to follow decryption:

- Link Key
- Full Central BD\_ADDR, Full Peripheral BD\_ADDR
- All packets from the last authentication (central or central) before encryption starts (LMP\_au\_rand, and LMP\_sres)
- LMP\_en\_rand, negotiated LMP\_encryption\_key\_size
- LMP\_start\_encryption\_req, LMP\_accepted(LMP\_start\_encryption\_req)
- LMP\_stop\_encryption\_req, LMP\_accepted(LMP\_stop\_encryption\_req)

### BR/EDR Secure Encryption (AES)

The following information and packets are needed to follow decryption:

- Link Key
- Full Central BD\_ADDR, Full Peripheral BD\_ADDR
- Complete mutual authentication (LMP\_au\_rand from the central as well as LMP\_sres from the peripheral)
- Negotiated LMP\_encryption\_key\_size
- LMP\_start\_encryption\_req, LMP\_accepted(LMP\_start\_encryption\_req)
- LMP\_pause\_encryption\_aes\_req (if pausing and resuming AES encryption)
- LMP\_stop\_encryption\_req, LMP\_accepted(LMP\_stop\_encryption\_req)

### Bluetooth Low Energy Encryption (AES)

The following information and packets are needed to follow decryption:

- Long-Term Key (LTK)
- LL\_ENC\_REQ, LL\_ENC\_RSP
- LL\_START\_ENC\_REQ, LL\_START\_ENC\_RSP
- LL\_PAUSE\_ENC\_REQ, LL\_PAUSE\_ENC\_RSP

## 4.2.9 Saving Analyzed Data to Disk

**Note:** **Start Record** is not available when viewing a previously recorded Capture file. **Start Analyze/Stop Analyze** is available in **Wireless Protocol Suite** application window, allowing different analyses to be performed on previously recorded and saved captures.

**Note:** Choose File Location from the File menu to change the default file location.


1. Click on either
  - the **Start Record** button on the datasource toolbar.,
  - or the **Start Record** under Capture in the datasource,,
  - or the Start Recording under the Capture option in the Main window.

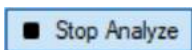
The Soderas Soderas LE analyzer will begin capturing data from all wireless devices within range and from all connected wired devices.

2. In the **Device Database** and **Wired Devices** View select the active devices for analysis.
3. : Click on either
  - the **Start Analyze** button Start Analyze under the Capture menu in the SoderasSoderas LE datasource window,
  - or click on Start Analyze button in the Wireless Protocol Suite Main window,
  - or Start Analyzing under Capture menu

to begin capturing data traffic.

4. Files are placed in **My Capture Files** folder by default and have a .cfa extension.
5. Watch the Status Bar on the Wireless Protocol Suite Main window to monitor how full the file is.

6. Click on **Stop Record**  button to stop recording.

7. Click the **Stop Analyze**  button to stop analyzing.



8. To clear captured data, click the **Clear** icon .
- If you select **Clear** after stopping analysis, a dialog appears asking whether you want to save the data.
    - You can click **Save File** and enter a file name when prompted .
    - If you choose **Do Not Save**, all data will be cleared.
    - If you choose **Cancel**, the dialog closes with no changes.
  - If you select the **Clear** icon while a capture is occurring:
    - The capture stops.
    - A dialog appears asking if you want to save the capture.
    - You can select **Yes** and save the capture or select **No** and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
    - If you choose **Cancel**, the dialog closes with no changes.
  - Alternately Clear can be selected from the keyboard shortcut Ctrl+R.

### 4.3 Extended Inquiry Response

**Extended Inquiry Response** (EIR) is a tab that appears automatically in the Summary pane of the Wireless Protocol Suite software when you capture data.

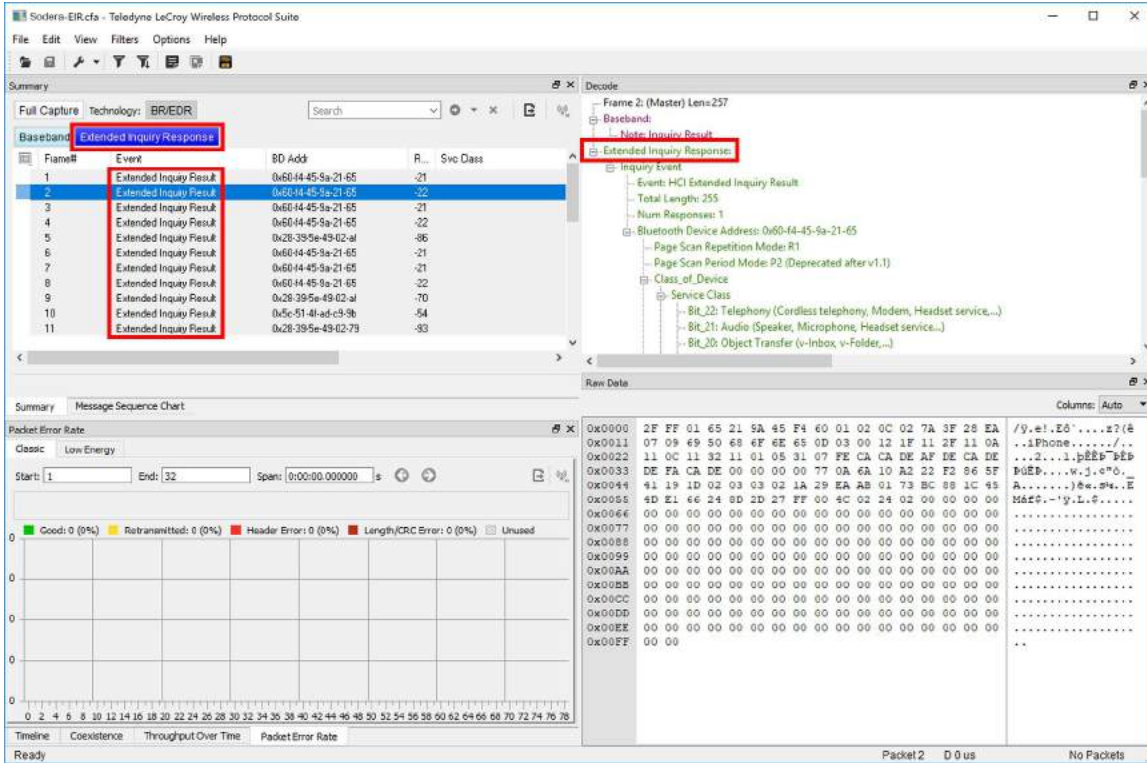


Figure 4.14 - Main windows Extended Inquiry Response

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

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

## Chapter 5 Analyzing Data

The main application window of the **Wireless Protocol Suite** is used for analyzing captured frames. The main components of this window are shown below and are described in more detail in the following sections.

### The Wireless Protocol Suite: Main Window

By default, the Menu Bar, the Tool Bar, the Analyzer Toolbar four separate Panes and the Status Bar are displayed when the Main window first opens. Any of the panes can be selected and moved around on the Main window. If you click and drag on the top of the pane you can attach to another existing pane, or create a new pane. The figure below shows the default set of panes and bars.

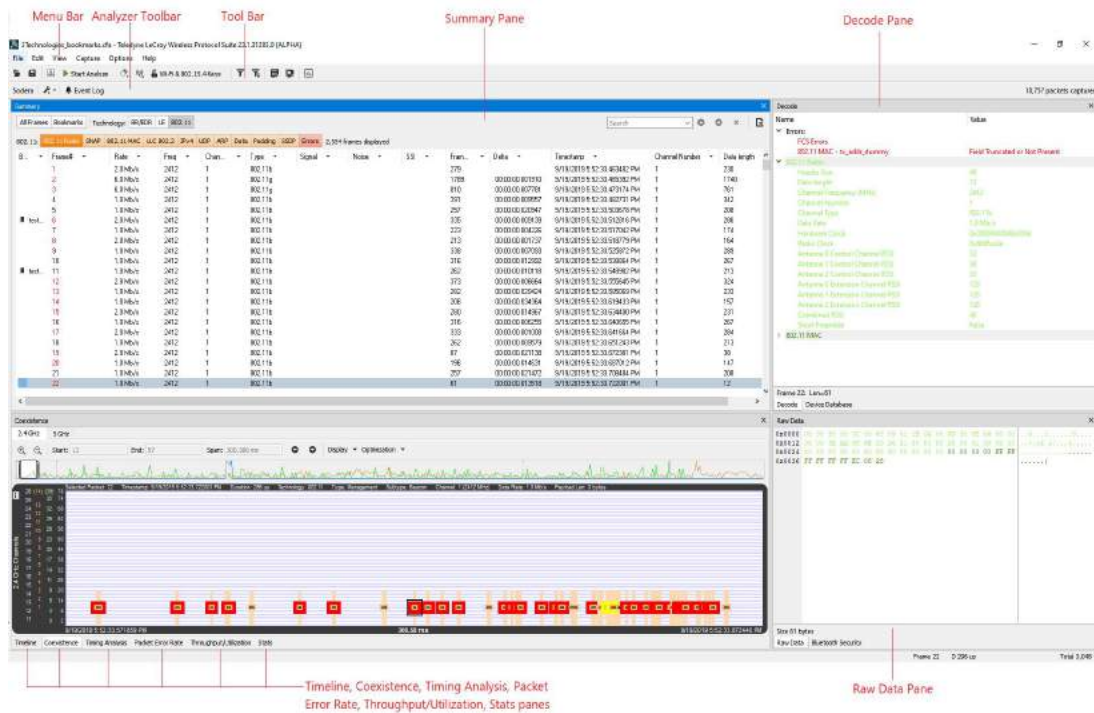


Figure 5.1 - Main window with all Panes active

### Protocol Filter Tabs

- 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.

### 5.1 Tool Bar

The tabs that appear in the **Wireless Protocol Suite** Main window vary according to the particular configuration of the analyzer. For controls not available the icons will be grayed-out.

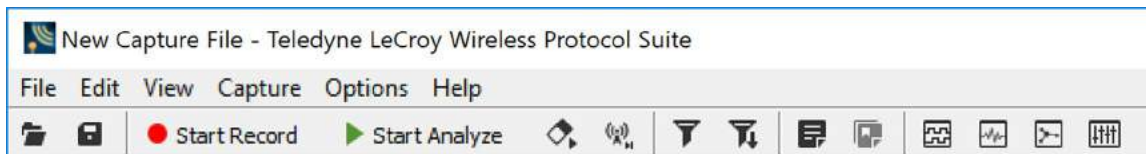


Figure 5.2 - **Wireless Protocol Suite** Main window Functions and Toolbar

When selected, the File, Edit, View, Capture, Options and Help menu items form pull down menus with options for each topic.







The icons below the tabs are described in the table below.

Table 5.1 - Wireless Protocol Suite Main window Toolbar Icons

Icon	Description
	Open a captured file.
	Save As – Save a captured file
	Start / Stop a Recording
	Start / Stop Analysis of Recording
	<p>The Clear button allows to to selectively remove the following panes from the Main window:</p> <ul style="list-style-type: none"> <li>Message Sequence Chart</li> <li>Packet Error Rate</li> <li>Throughput</li> <li>Coexistence</li> <li>Timeline</li> <li>Summary</li> <li>Decode</li> <li>Raw Data</li> </ul> <p>Toolbar (If you select Clear -&gt; Toolbar to display the toolbar again right click in the area to the right of the Help menu item and the Toolbar with be visible again).</p> <p>Alternately Clear can be selected from the keyboard shortcut Ctrl+R.</p>
	<p>When you are actively Capturing traffic, clicking on the Follow Live button will freeze the Summary Pane, the Coexistence pane, the Packet Error Rate pane and the Throughput pane so you can take a look at a Frame you're interested in while the tool continues capturing traffic.</p> <p>When you click on the Follow Live button again the panes will all display the latest traffic captured.</p> <p>Alternately Follow Live can be selected by pressing the space bar.</p>



Table 5.1 - Wireless Protocol Suite Main window Toolbar Icons (continued)







Icon	Description
	Apply/Modify Display Filters - Opens the Display Filter dialog.
	Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.
	Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.
	Audio Expert System - Opens Audio Expert System Window
	<i>Bluetooth</i> Expert System - Opens <i>Bluetooth</i> Expert System window
	<i>Bluetooth</i> Toolbox - Includes the ability to emulate an A2DP sink device and the ability to generate and inject Low Energy packets directly into in the 2.4 GHz spectrum.

**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.

## 5.2 Analyzer Toolbar

The Analyzer Toolbar appears under the main Toolbar. The Analyzer Toolbars are described in detail in section [Analyzer Toolbar Menu and Icons on page 81](#) . Below is the summary table of the Analyzer Toolbar icons and menus:

Table 5.2 - Wireless Protocol Suite Analyzer Toolbar Icons

Icon/Menu	Description or Summary
Analyzer Information menu: 	<p><b>About Analyzer</b> - Opens a pop-up window with version and configuration information</p> <p><b>Manage License</b> (X240 only) – Opens Manage License dialog that allows to view the details of a currently installed license file or update the X240 license file.</p>
	Opens the <b>Record Options</b> dialog where the attached hardware can be configured for <i>Bluetooth</i> technologies and other capture modes. For additional information see <a href="#">Record Options Dialog: X240 on page 107</a>
Analyze Options menu 	Allows to turn on/off various analyzing options
	Record or delete captures from the Soderia hardware that were created using excursion mode. Opens the Manage excursion mode captures dialog.  This selection is disabled during live capture.
<b>Event Log</b> menu	Opens up Event Log view.
	Displays the analyzer current status.
<b>Update</b> button 	Press this button to update your license.

## 5.3 Status Bar

The **Main windows Status Bar** appears at the bottom of the **Main windows**. It contains the following information:

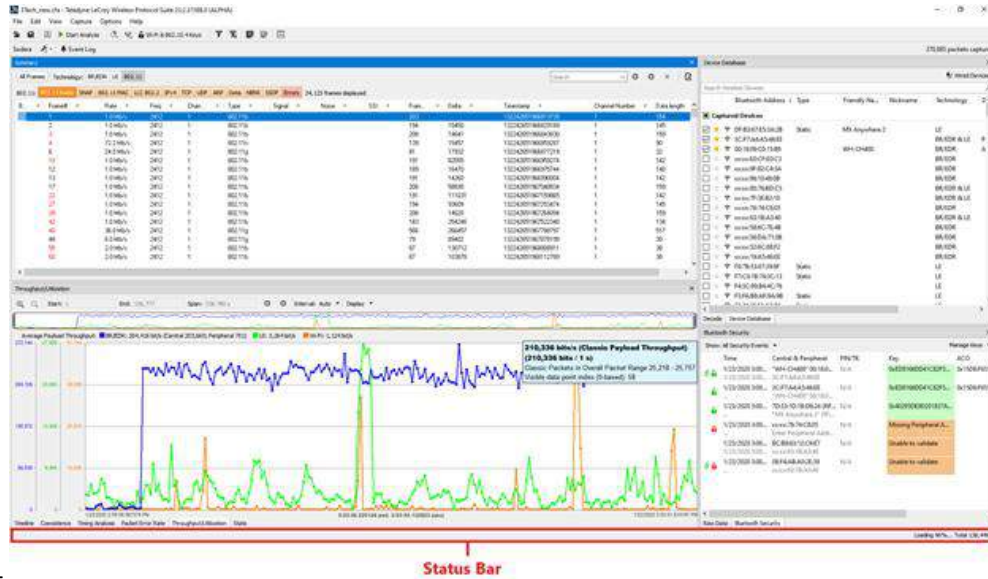


Figure 5.3 -

Figure 5.4 - Main windows: Status Bar



Figure 5.5 - Main windows: Status Bar Zoomed In

### 5.3.1 Application Status

The **Wireless Protocol Suite** software status is shown at the bottom of the Main window. The software can be in one of several states as shown below:

- Ready: The Wireless Protocol Suite software is not active
- Recording: The Wireless Protocol Suite software is recording traffic
- Filtering: The Wireless Protocol Suite software is filtering the incoming traffic before it can be analyzed
- Analyzing: the Wireless Protocol Suite software is analyzing the currently recorded traffic

#### 5.3.1.1 Device information block

Items of this area are displayed only in live mode (live mode – when a device is connected).

- The device information block consists of the following items:

**Buffer** – this 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 window. Buffer is displayed in the format “Buffer /percentage of fill/%”. Example: “Buffer 5%”.

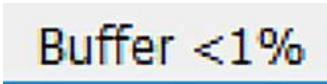


Figure 5.6 - Status Bar: Buffer

### 5.3.2 Selected Frames Information

- This part of the Status Bar is displayed only when packet(s) have been selected.
- The user can see information for one or several packets. In the Summary view, you can select multiple sequential packets or several non-sequential packets.

#### 5.3.2.1 Information for one packet:

- Packet number in the format "Packet /Number/". Example: "Packet 880".
- Duration in the format "D /Time/ /Time Unit/". Example: "D 376 us".

#### 5.3.2.2 Information for several packets:

- The number of selected packets in the format "/Number of packets/ packets". Example: "3 packets".
- Gap - Duration between the end of the first selected packet and the beginning of the last selected packet in the format "G /Time/ /Time Unit/". Example: "G 317 us".
- Delta - Duration between the beginnings of the first and last packets selected. Delta in the format "Δ /Time/ /Time Unit/". Example: "Δ 623 us".
- Span - Duration between the beginning of the first selected packet and the end of the last selected packet. Span in the format "S /Time/ /Time Unit/". Example: "S 749 us".
- Duration - Duration is the beginning of the first packet to the end of the last packet.
- Time for Duration, Gap, Delta and Span are shown in "000.000" format. If the number is an integer, then decimal is not displayed.
- If the time exceeds 999.999, the unit of measurement switches to the higher unit of measurement.
- Time is shown in second, millisecond, microsecond and nanosecond. Second – s, Millisecond – ms, Microsecond – us, Nanosecond – ns. There must be a space between the number and the measurement unit.
- The figures below shows that a number of packets have been selected (highlighted) and the data from those packets in the Status Bar.

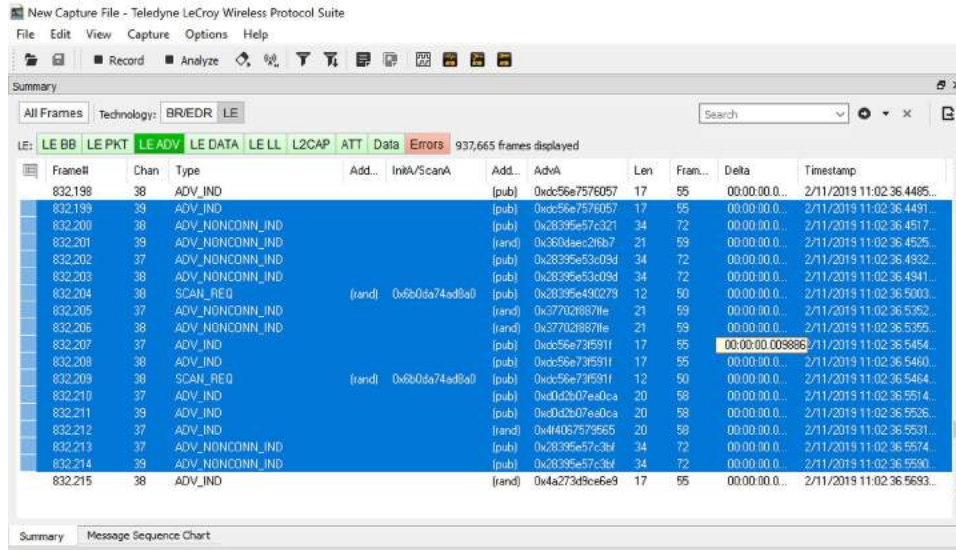


Figure 5.7 - Selected Frames in Summary Pane

- Information about selected frames is shown below.

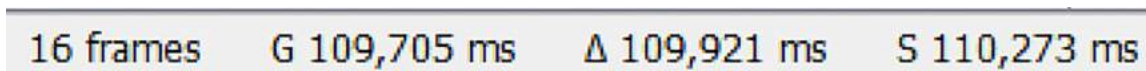


Figure 5.8 - 16 Frames Selected with: Gap/Delta/Span Times

### 5.3.3 Total Frames Information

- This part shows information about the number of analyzed frames in the capture file and the process of their decoding.
- Information is displayed in the “Total /Number of frames/” format. Every third character is separated by a comma. Example: “Total 1,042,857”.
- If there are no frames (this may be the case when the user has just opened an interface of connected a device), then “No Frames” is displayed.
- The decoding process is displayed when opening or analyzing a capture file.
- The decoding process is displayed in the format “Decoding (/Decoding percentage/%) ... /Number of frames/”. Example: “Decoding (32%)... 1,042,857”.

**Total Number of Frames Information:** Displays the total number of frames, the analysis process currently underway and the percent completion. The image below shows that 100,523 frames have been analyzed and that the analysis has been completed.

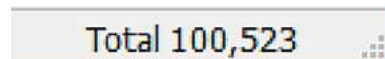


Figure 5.9 - Total Number of Frames Analyzed

## 5.4 Panes in the Wireless Protocol Suite Main windows

The **Wireless Protocol Suite** is used to view all frame related information. It is composed of a number of different sections or "views" where each pane shows a different type of information about a frame. A short description of each pane or view is given here with a more detailed explanation later in the User Manual.

**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.

**Message Sequence Chart** - Displays information about the messages passed between protocol layers. MSC displays a concise overview of a Bluetooth connection, highlighting the essential elements for 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 or profile. The MSC is color coded for a clear and easy view of your data.

**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 Raw Data Pane.

**Raw Data Pane**- Displays the logical data bytes in the selected frame in either hexadecimal, decimal, binary or ASCII.

**Throughput View** - Displays Packet Payload Throughput.

**Timeline View** - Displays packet information with an emphasis on temporal information and payload throughput. The timelines also provide selected information from Summary Pane.

**Coexistence View** - Displays Classic Bluetooth and Bluetooth Low Energy packets and throughput in one view.

**Packet Error Rate View** - Displays a graph for each Classic Bluetooth channel numbered 0 through 78 and for each Bluetooth Low Energy channel numbered 0 through 39.

### Working with Panes on the Main windows

When the **Main windows** first opens, all panes are displayed.

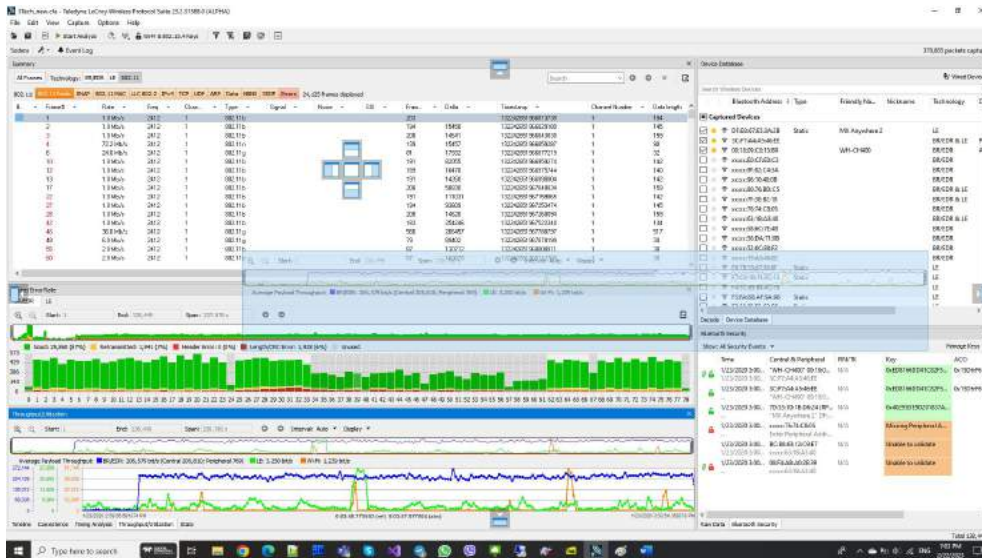


Figure 5.10 - Docking Frame

The docking frame supports the following features

- Allows docking panes in an undocked pane.
- Indicates which pane is in focus with color coding.
- Allows any number of splits horizontally and vertically.
- Allows changing the width and height of the panes.
- Allows docking panes by grabbing the top or bottom of a pane. Packet Error Rate, Timeline and Coexistence panels allows user to change the order of nested tabs: BR/EDR and LE for Timeline and PER panels/ 2,4 and 5 GHz for CoEx panel. The orders save between session.

To get back to the original default set of panes, just select **View -> Reset Window Layout**.

Device Database View - Displays Active/Previous/User added wireless devices. It also allows you to add/edit/delete wireless devices, set devices properties and configure check/uncheck devices for analysis.

### 5.4.1 Summary

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.



Frame#	CP#	RF Chan	Chan	Event Status	Decryption Initiated	DS	PHY	PD...	Fram...	Delta	Timestamp
396,146	1	12	38	SUCCESS	No		1M	38	74	00:00:00.0...	1/3/2019 4:02:49.016466 ...
396,147	1	0	37	SUCCESS	No		1M	36	72	00:00:00.0...	1/3/2019 4:02:49.021215 ...
396,149	1	12	38	SUCCESS	No		1M	36	72	00:00:00.0...	1/3/2019 4:02:49.022022 ...
396,150	1	39	39	SUCCESS	No		1M	36	72	00:00:00.0...	1/3/2019 4:02:49.022830 ...
396,155	1	0	37	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.037111 ...
396,156	1	12	38	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.037651 ...
396,157	1	39	39	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.038209 ...
396,158	1	0	37	SUCCESS	No		1M	38	74	00:00:00.0...	1/3/2019 4:02:49.038292 ...
396,159	1	0	37	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.040454 ...
396,160	1	12	38	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.040995 ...
396,161	1	39	39	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.041536 ...
396,162	1	0	37	SUCCESS	No		1M	34	70	00:00:00.0...	1/3/2019 4:02:49.042169 ...
396,164	1	0	37	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.042617 ...
396,165	1	12	38	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.043158 ...
396,167	1	39	39	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.043699 ...
396,168	1	12	38	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.044042 ...
396,169	1	0	37	SUCCESS	No		1M	19	55	00:00:00.0...	1/3/2019 4:02:49.044584 ...
396,170	1	39	39	SUCCESS	No		1M	39	75	00:00:00.0...	1/3/2019 4:02:49.044591 ...
396,171	1	12	38	SUCCESS	No		1M	19	55	00:00:00.0...	1/3/2019 4:02:49.045168 ...
396,172	1	39	39	SUCCESS	No		1M	19	55	00:00:00.0...	1/3/2019 4:02:49.045752 ...
396,178	1	12	38	SUCCESS	No		1M	38	74	00:00:00.0...	1/3/2019 4:02:49.059265 ...
396,179	1	0	37	SUCCESS	No		1M	36	72	00:00:00.0...	1/3/2019 4:02:49.061955 ...
396,180	1	39	39	SUCCESS	No		1M	36	72	00:00:00.0...	1/3/2019 4:02:49.063570 ...
396,184	1	0	37	SUCCESS	No		1M	23	59	00:00:00.0...	1/3/2019 4:02:49.074448 ...
396,185	1	39	39	SUCCESS	No		1M	23	59	00:00:00.0...	1/3/2019 4:02:49.075208 ...

Figure 5.11 - Summary Pane

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

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

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

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

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

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

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

The **Summary** pane is synchronized with the other panes in this window. Click on a frame in the **Summary** pane, and the bytes for that frame is highlighted in the **Event** pane while the **Decode** pane displays the full



decode for that frame. Any other panes which are being viewed are updated accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame is highlighted in the other panes.

### 5.4.1.1 Protocol Tabs

Protocol filter tabs are displayed in the Main windows 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), Wi-Fi (orange) and 802.15.4 (purple). The General group applies to all technologies. The other groups are technology-specific.

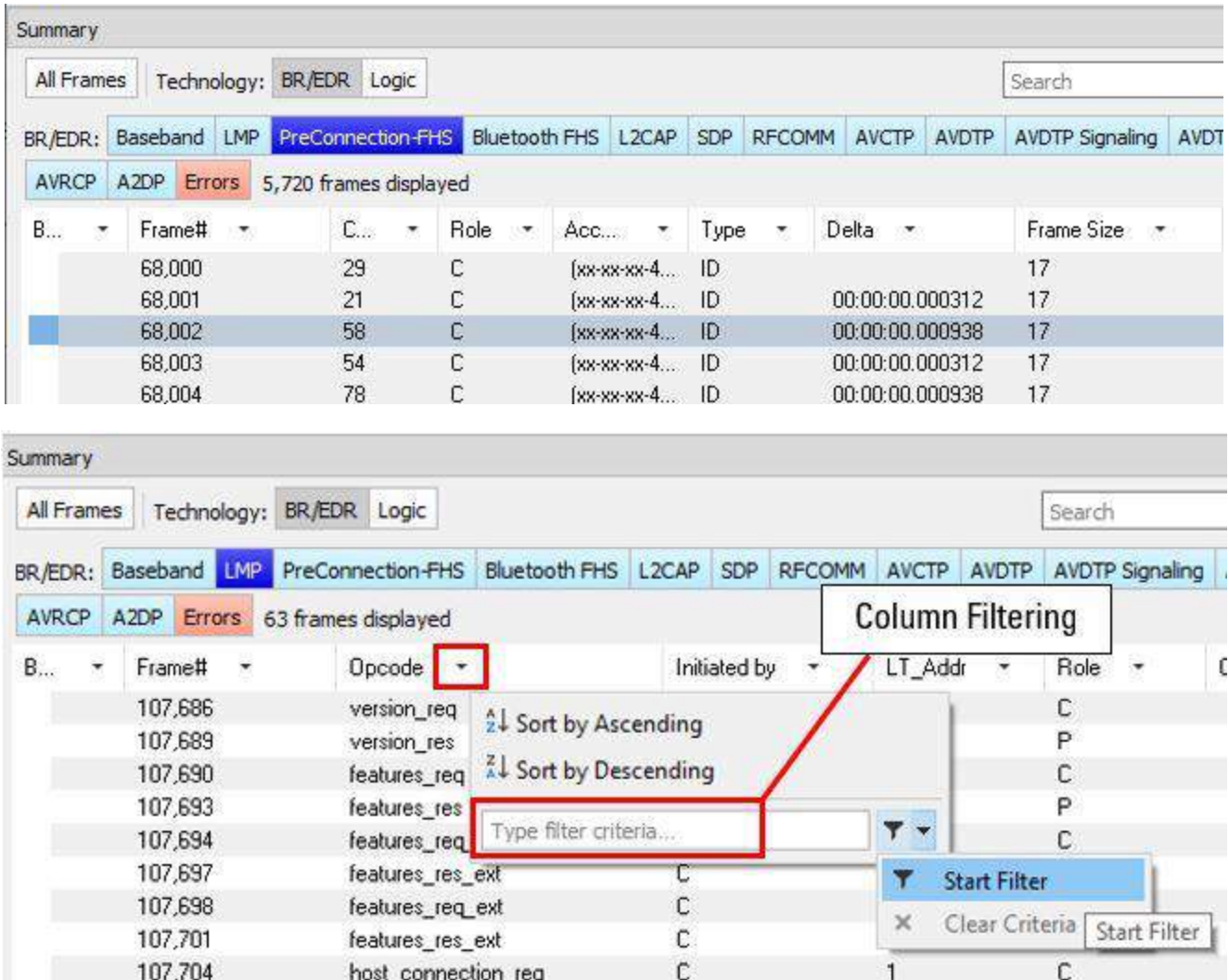


Figure 5.12 - Example Protocol Tabs

- 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.

### 5.4.1.2 *Bluetooth Low Energy Data Encryption/Central and Peripheral Assignment*

A Bluetooth Low Energy data connection consists of connection events, which are a series of transmissions on the same channel. In each connection event the central transmits first, then the peripheral, 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 master 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 master device are labeled '1' and packets sent by the slave 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".

### 5.4.1.3 *Bluetooth Low Energy Decryption Status*

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

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

#### 5.4.1.4 Column Filtering/Sorting

The Column Filter/Sort provides an easy way to sort/filter specific information from the Summary View making it easier to find information. Clicking on a column header provides options to either sort or filter data.

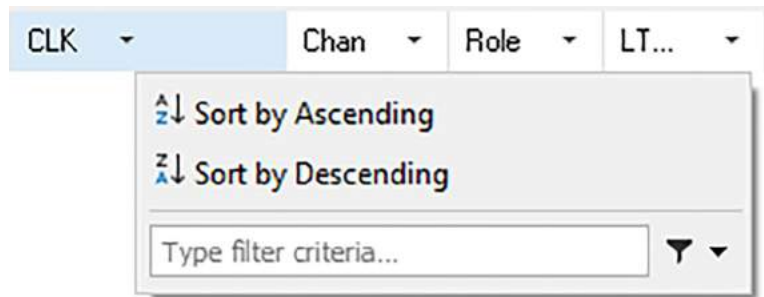


Figure 5.13 - Column Filtering/Sorting Popup Dialog

##### 5.4.1.4.1 Sorting

By default, frames are sorted in ascending numerical sequence by frame number. Click on “Sort by Ascending” or “Sort by Descending” to sort data in the desired order. Note that it may take some time to sort large numbers of frames.

##### 5.4.1.4.2 Filtering

A value or range of values can be used to filter data. Multiple column filters can be applied to the current protocol tab which are combined using “AND” operation. The column filters for a protocol tab resets when the tab changes or the current tab is re-selected.

###### To apply a filter:

1. Click on the column header.
2. Type filter criteria into the edit field.
3. Then press “Enter” or click on the filter icon.

To change the current filter, click on the column header again.

To clear a filter:

To reset a filter, click on a column header. From the drop-down menu,

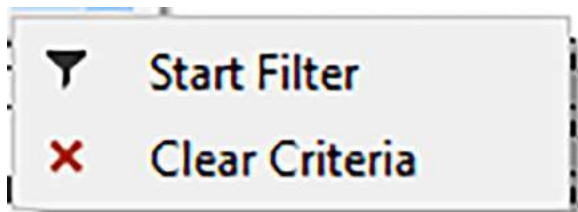


Figure 5.14 - Start Filter/Clear Criteria Drop Down Box

click on



Figure 5.15 - Clear Icon

icon or clear edit field and click on the drop-down arrow and select “Start Filter”.

To reset all header filters click on the current tab or another tab (protocol or technology).

The columns “Frame#” and “Frame size” can be filtered with range, such as value1 – value2. If value1 is skipped then 0 is used as a low boundary. If value2 is skipped, the max value is used as an upper boundary.

The column filters cannot be used on Bookmark tab or Delta column. The filter on columns such as “Channel”, “Chan”, “Frame#”, “Frame size” use full match criteria for a field value. To filter on columns such as “Timestamp”, “Hardware Clock”, “Src SAP”, “Dest SAP”, “Access code LAP”, “AddrTypeI”, “AddrTypeA”, “Opcode”, “Original Opcode”, “Signal ID”, “Error Code”, “Command”, “Code”, apply partial match criteria in any part of corresponding field in frames. Filters for all other columns apply match from the beginning of the field data.

### 5.4.1.5 Filtering

Filtering allows the user to control the way in which the capture frames are displayed. Filters fall into two general categories: Quick Filters and Apply/Modify Display Filters.

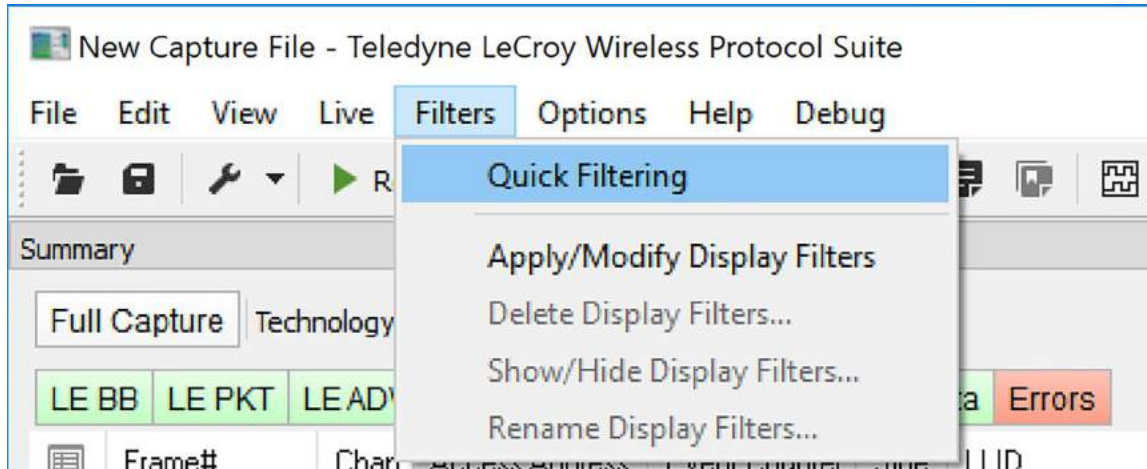
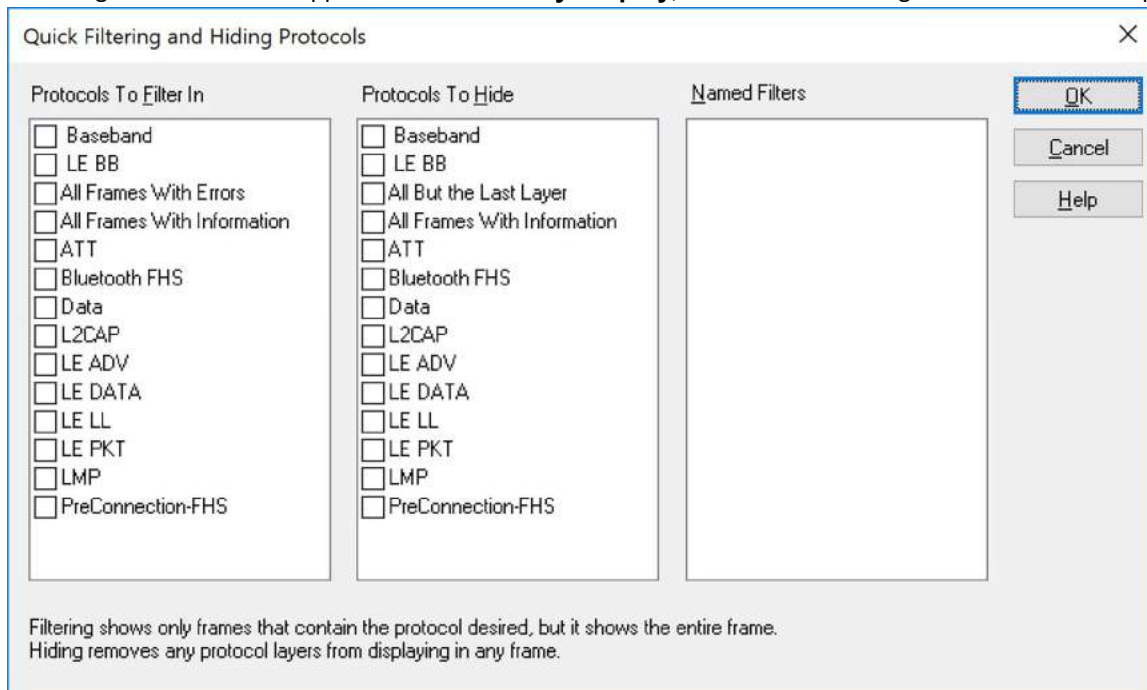


Figure 5.16 - Filtering: Quick and Apply/Modify Display Filters

**Quick Filters** allow a user to look at a subset of captured data without affecting the capture content. Frames matching the filter criteria appear in the **Summary Display**; frames not matching the criteria will not appear.



**Connection filters** - Two options are available.

A *Bluetooth* connection: Displays only the frames associated with a Classic Bluetooth link or a *Bluetooth* Low Energy access address. A new Main windows will open showing only the protocol tabs, frames, summary, and events associated with that particular *Bluetooth* connection.

A specific wireless or wired technology displays all of the frames associated with:

Classic *Bluetooth*

*Bluetooth* Low Energy

A new Main windows will open showing only the protocol tabs, frames, summary and events associated with the selected technology.

#### 5.4.1.5.1 Display Filters

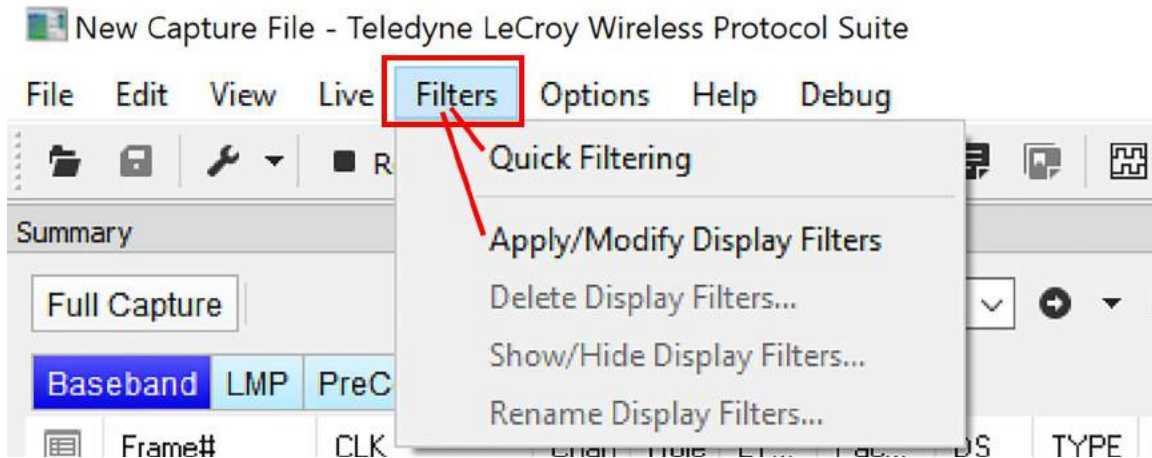


Figure 5.17 - Filter Options

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.

**5.4.1.5.1 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 **Wireless Protocol Suite Main Toolbar** window 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.

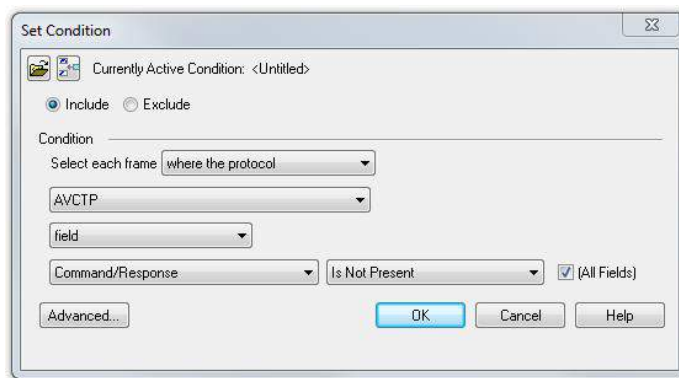


Figure 5.18 - Example: Set Conditions Self Configuring Based on Protocol Selection

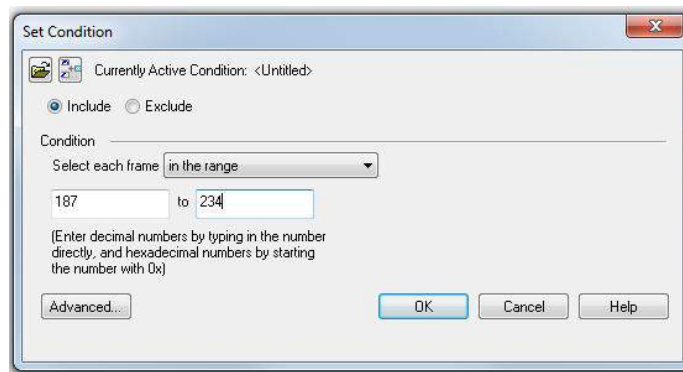


Figure 5.19 - Example: Set Conditions Self Configuring Based on Frame Range

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 **Main windows** 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 **Main windows**.

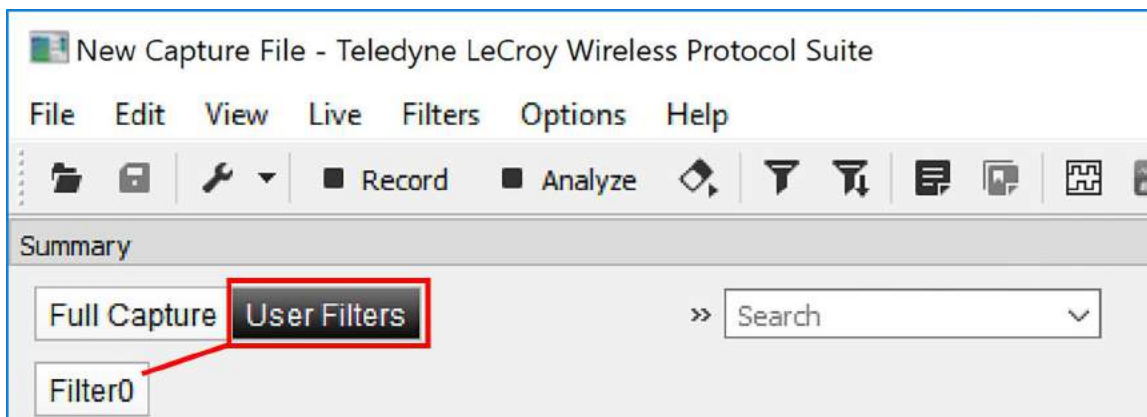


Figure 5.20 - Filter Displayed in Analysis Pane

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 Main windows](#) with a display filter or filters, those filter do not automatically appear in other **Main windows**. You must use the [Hide/Reveal](#) feature to display a filter created in one **Main windows** in different **Main windows**.

#### 5.4.1.5.1.2 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.

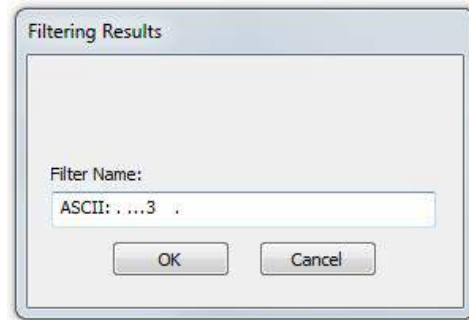


### 5.4.1.5.1.3 Named Display Filters

You can create a unique display filter by selecting a data type on the **Main windows** and using a right click menu. When you create a **Name Filter**, it appears in the [Quick Filtering](#) dialog, where you can use it to customize the data you see in the **Main windows** panes.

1. Select a frame in the **Main windows Summary** Pane.
2. Right click in 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.




### 5.4.1.5.1.4 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**.

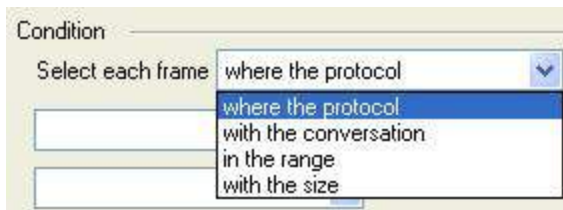
The **AND** operator narrows the filter, the **OR** operator broadens the filter, and the **NOT** operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets and force the filter-processing order.

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

Now you can set the conditions for the filter.

4. Select the initial condition for the filter from the combo box at the bottom of the dialog for **Select each frame**.
5. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.



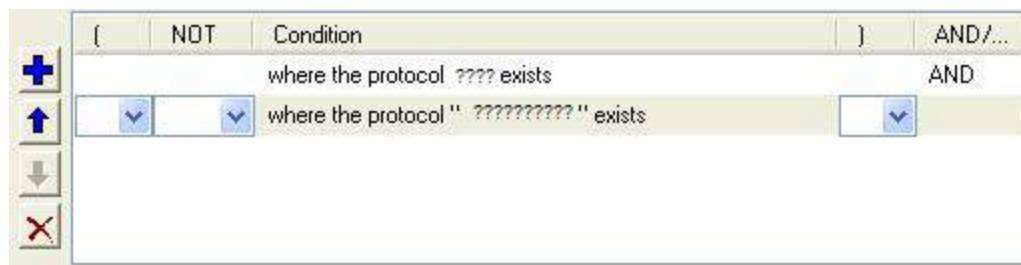


Figure 5.21 - Two Filter Conditions Added with an AND Operator





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 5.22 - Save Named Filter Condition Dialog

The **Set Condition** dialog box closes, creates a tab on the **Main windows** 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 **Main windows**.

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

### 5.4.1.5.1.5 Defining Node and Conversation Filters

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



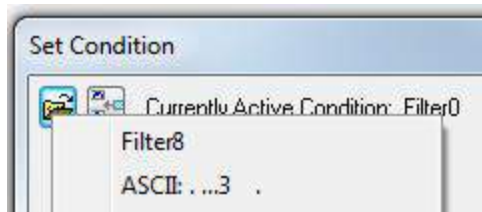
1. Click the **Display Filters** icon  on the **Wireless Protocol Suite Main Toolbar** window to open the **Set Condition** dialog box.
2. From the **Select each frame** combo box choose frames **with the conversation** as the initial condition.
3. Select an address type—IP, MAC, TCP/UDP—from the **Type** combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first **Address** combo box.
5. Choose a direction arrow from the direction box . The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination. 
6. If you want to filter on just one node address, skip step 7 and continue with step 8.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select a node address from the second Address combo box.
8. Click **OK**. The **Set Condition** dialog box closes and the analyzer applies the filter.

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

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

### 5.4.1.5.1.6 Editing Filters

#### Modifying a Condition in a Filter

1. Click the **Display Filters** icon  on the **Main windows** 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,

provide a new name for the filter condition or accept the default name provided by the system and click **OK.**) The **Set Condition** dialog box closes and the system applies the modified filter.

**Note:** When a display filter is applied, the name of the filter appears to the right of the toolbar in the Main windows.

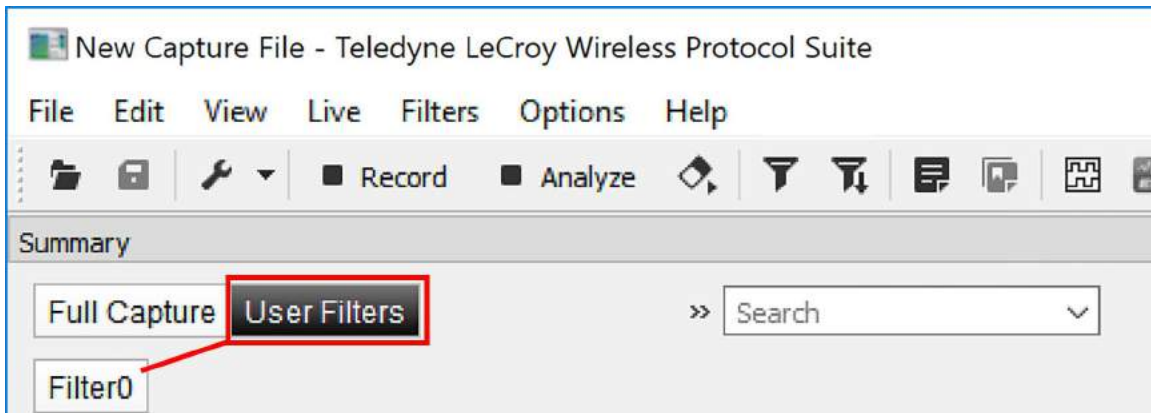




Figure 5.23 - Name of Filter Displayed

### 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 **Main windows** 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.
2. Select the desired condition from the filter definition.

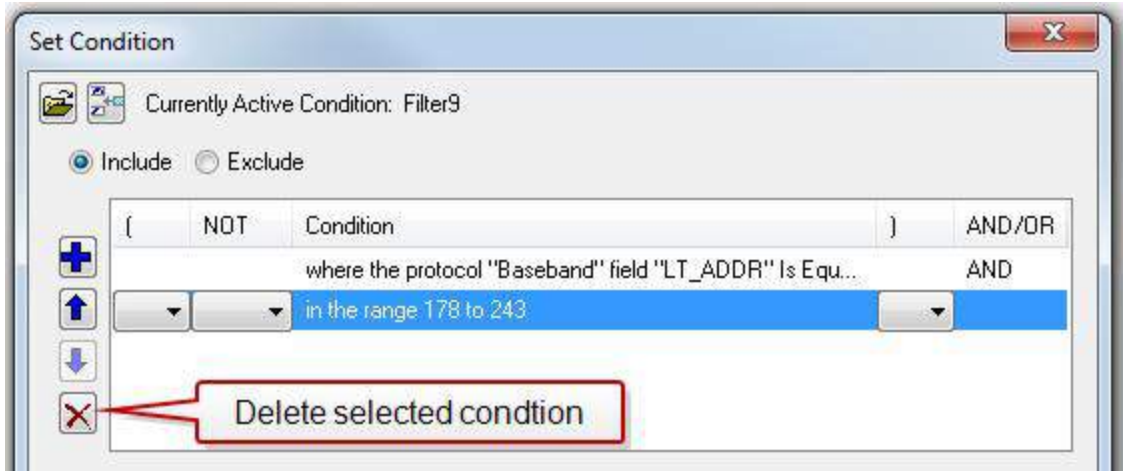



Figure 5.24 - Set Condition Dialog in Advanced View

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

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

### Renaming a Display Filter

1. Select **Rename Display Filters...** from the **Filter** menu in the **Main windows** 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.

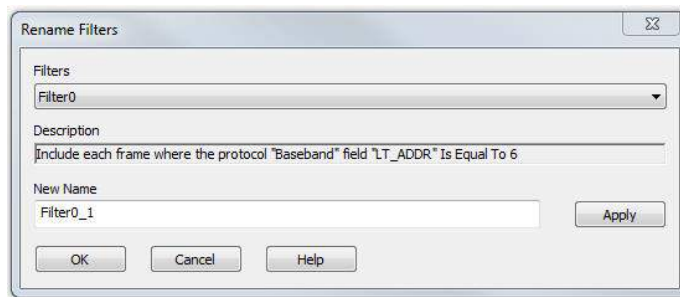


Figure 5.25 - Rename Filters Dialog

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.

### 5.4.1.5.2 Protocol Filtering from the Main windows

Protocol filtering allows for customized view of captured protocols to facilitate effective and efficient analysis.

#### 5.4.1.5.2.1 Quick Filtering on a Protocol Layer

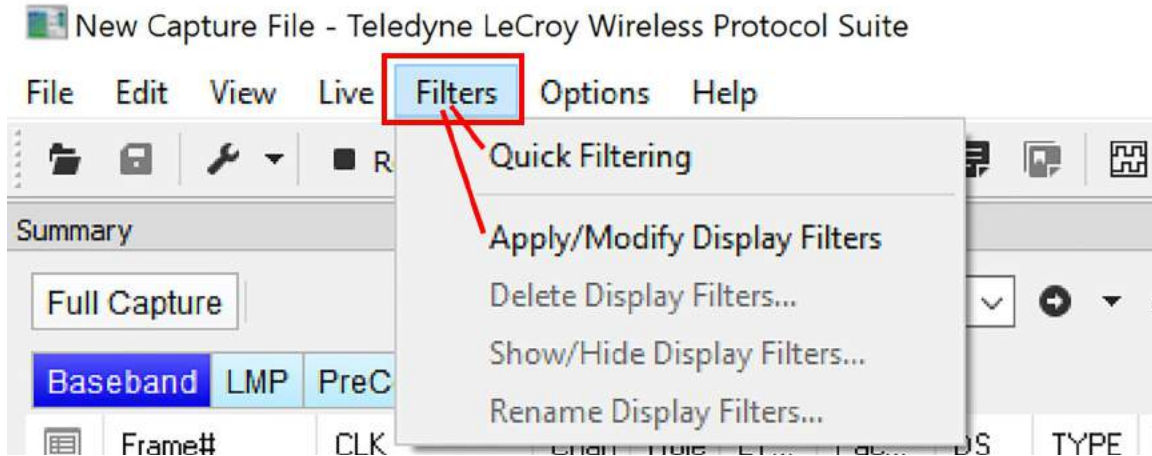



Figure 5.26 - Quick Filtering

On the **Main windows**, 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.

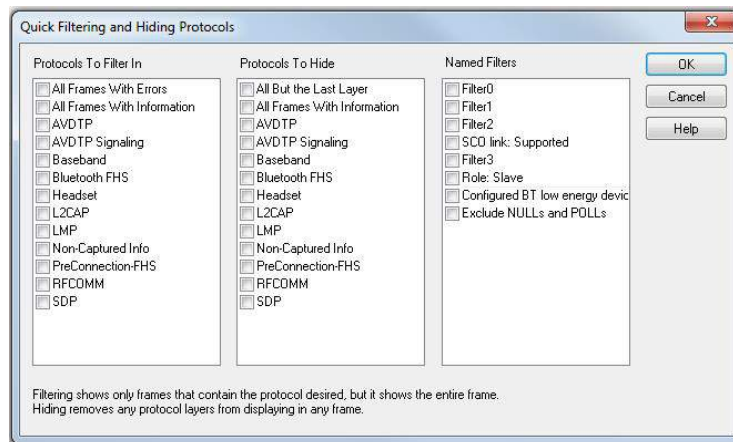


Figure 5.27 - Main windows Quick Filtering and Hiding Protocols Dialog

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 **Main windows**. 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 of data will still appear in the **Summary** pane, but not in the **Decode**, **Binary**, **Radix**, and **Character** panes.

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 Main windows Summary Pane unless you hide it using the Hide/Show Display Filters dialog.



With Low Energy, the Configured *Bluetooth* 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 the **Named Filter** to display. Then click **OK**.

#### 5.4.1.5.2.2 Easy Protocol Filtering

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



##### Filtering on the Summary Layer Protocol

To filter on the protocol in the **Summary** in the **Main windows** pane:

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

##### Filtering on all Frames with Errors

To filter on all frames with errors:

1. Open the **Main windows**  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 **Main windows** labeled "Errors" that displays the results of the **All Frames With Errors** filter.





**Note:** When you have multiple Main 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.

## 5.4.2 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. By default, the layer selected in the Summary Pane is the only opened layer in Decoding Pane, however you can set default option for any layer by expanding/collapsing it. Click on the right arrow to expand a layer. The right arrow changes to a down arrow. Click on the down arrow to collapse a layer. Layers retain their expanded or collapsed state between frames.

Name	Value
RSSI	-49.375 dBm (medium)
Link	1
Role	Central (0x3c-f7-a4-a5-46-ee)
Channel	46 - 2448 MHz
Clock	0x0ca00e68
Packet Status	OK
FLOW	Go
TYPE	2-DH5
Payload Data Rate	2 Mbps
LT_ADDR	3
SEQN	0
ARQN	0
L2CAP Flow	Go
Logical Link ID	L2CAP start or no fragmentation
Decrypted by Bluetooth ComProbe	Yes
Pa	676
▼ L2CAP	
Ro	Central
Ad	3
PD	672
Channel ID	0x0048 (AVDTP)
▼ AVDTP	
Link	1
Role	Central
Address	3

Figure 5.28 - Decode Pane : All Options Collapsed

- Add to Summary View: Add selected field to the Summary Pane
  - An alternative way of adding columns to Summary View is to drag and drop them from Decode Pane.
- Filter In: Create a quick filter based on the selected field



- Filter Dialog: Create a custom filter based on the selected field
- Collapse All: Collapse Decode Pane tree
- Expand All: Expand Decode Pane tree
- Copy Selection: Copy selected data to clipboard. Copy menu includes such items:
  - All selection: allows to copy Field Name and Value
  - Field Name: allows to copy Field Name
  - Value: allows to copy Field Value

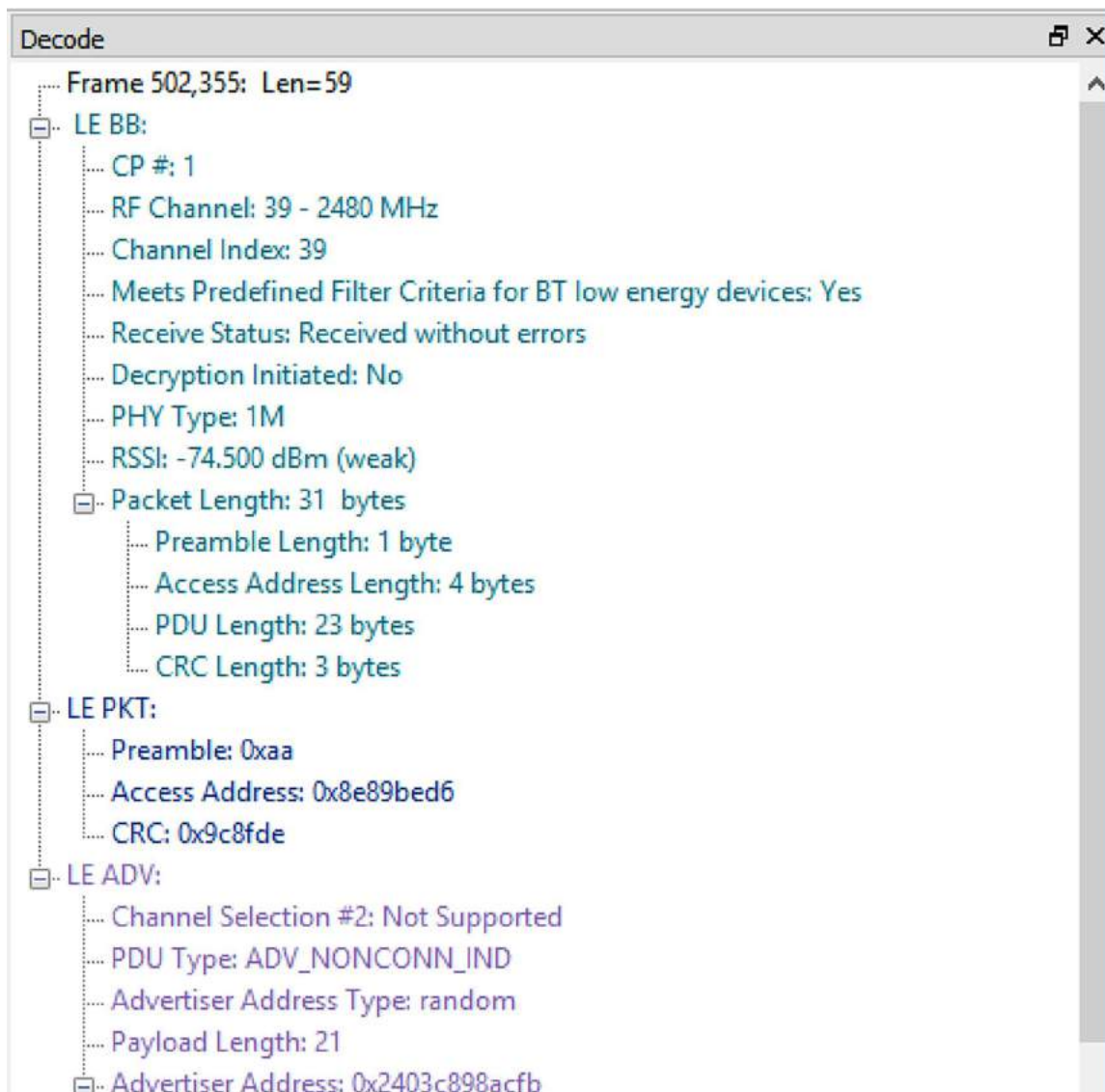


Figure 5.29 - Decode Pane: All Options Expanded

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

Each protocol layer is represented by a [color](#), which is used to highlight the bytes that belong to that protocol. The fields which do not represent the frame itself, but represent metadata, are represented in a gray color.

When a payload in particular packet is reconstructed, the legend “\* means that the data were reconstructed”, is displayed at the top of the Decode Pane after the Frame Number. The asterisk character is also displayed in front of each field when the content of that particular field is coming from a previous packet. The reconstruction is dependent on the protocol and can be due to number of reasons such as reassembly, fragmentation/defragmentation or encryption/decryption.

Consider the following example,

- Packet #1 has layers A and B where B’s payload contains the first fragment ‘f1’ (0x112233).
- Packet #2 has the same layers A & B, where B’s payload contains the last fragment ‘f2’ (0x445566).

Then B’s payload in packet #2 will be reconstructed and f2 will be transformed to f1+f2 (0x112233445566). The fields that are decoded and part of fragment f1 will bear an asterisk in front of it (Example: \*f1\_field1: 0x11) because these fields are not part of packet #2 but is required for the complete decoding of Layer B.

The Raw Data Pane also exhibits the same behavior. In the above example, if you click on Packet #2 and Layer A, all the original octets transmitted in this packet shall be displayed in the Raw Data Pane. The moment you click on Layer B, the octets in the Raw Data Pane is transformed and the reconstructed octets are shown instead.

In the case of certain specific protocols, an encrypted payload (for example) 0x2233445566 maybe decrypted as (for example) 0x1111111111. Since the entire payload is transformed, all the fields will bear an asterisk implying that they were reconstructed.

### 5.4.3 Raw Data Pane

The Raw Data Pane displays the logical bytes in the frame in various formats. It has three sub-panes and the data format for each can be changed independently by right-clicking on the pane.

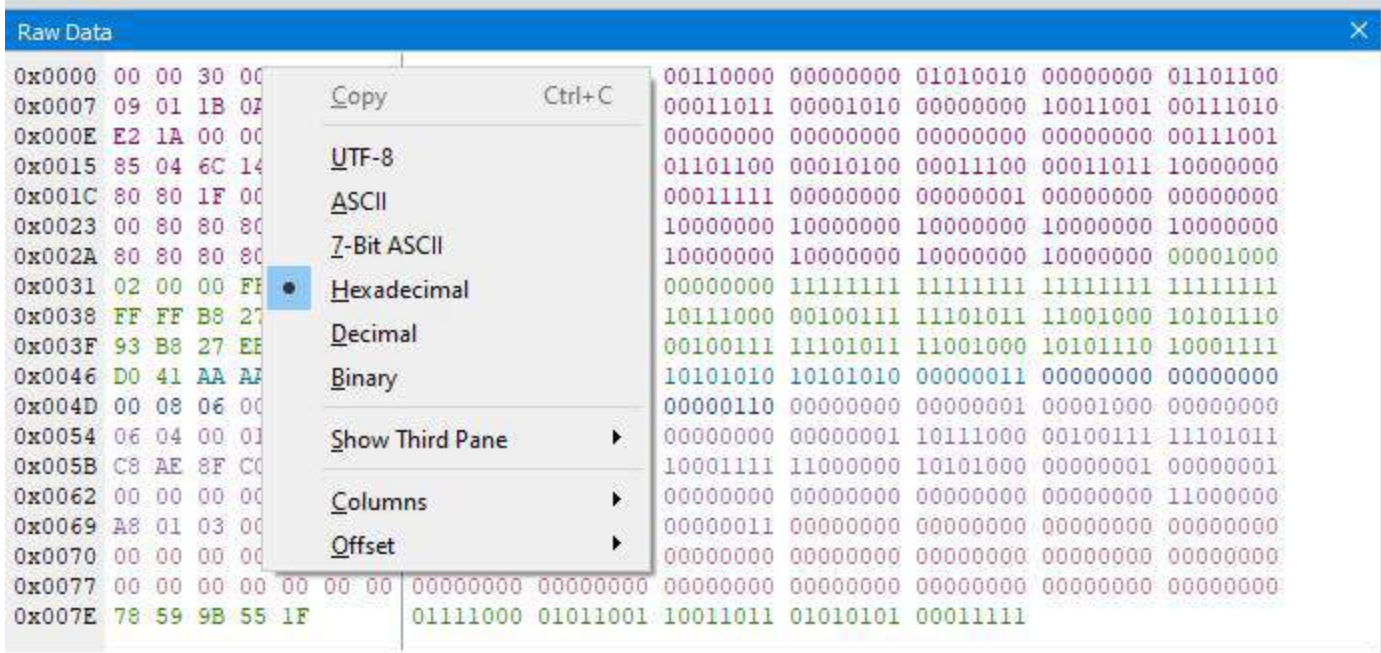


Figure 5.30 - Raw Data Pane: Options Shown

The data format for all sub-panes can be set to UTF-8, ASCII, 7-Bit ASCII, Hexadecimal, Decimal, or Binary.

Note that Raw Data view supports UTF-8 data display, which can be useful when there are non-ASCII symbols in the data stream, like Japanese, Korean or Chinese characters.

**Note:** Not all the fields in the decode pane will highlight values in the raw data pane. Some of the decode pane values are added to improve readability, such as the LE Uncoded PHYs mandatory fields "Preamble" and "Access Address" which are not included in the decoded packet values. Additionally, some of the displayed raw data values at the start of the frame are metadata, such as RSSI and not decoded packet values.

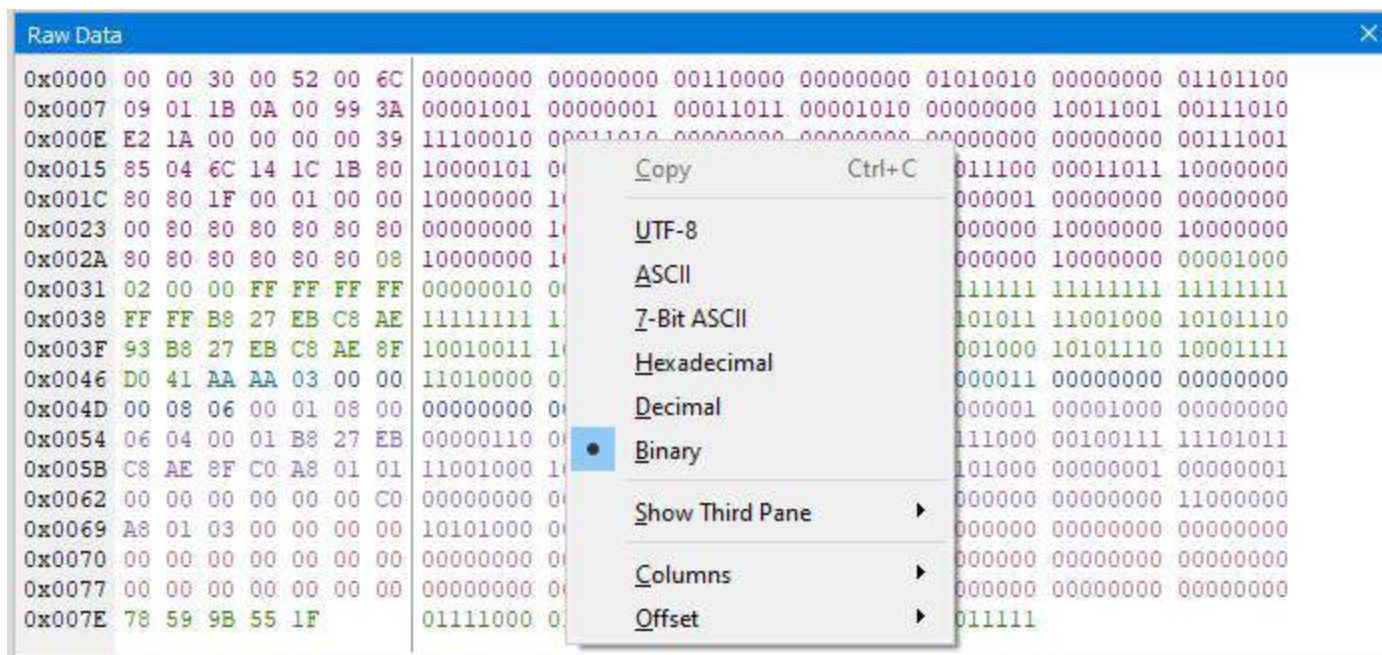


Figure 5.31 - Raw Data Pane: Binary Option Chosen

The number of columns in the first sub-pane is set to “Auto” to adjust automatically according to the width of the pane. Users can change the number of columns by right-click and choose “Columns” and options 4, 8, 16 or 32 columns.





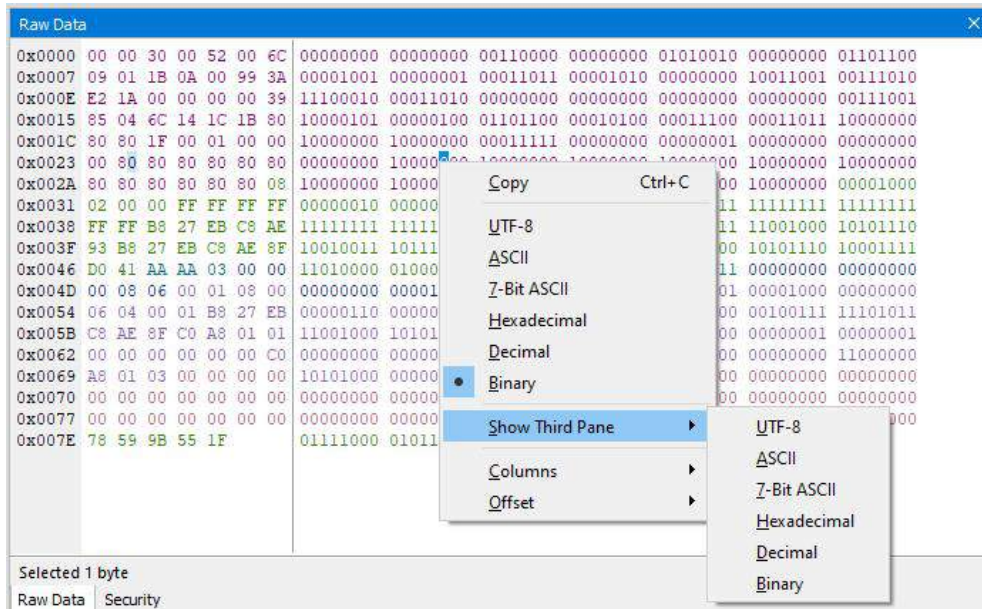


Figure 5.33 - Third sub pane option shown

The third sub-pane always opens in the rightmost position of the Raw Data Pane.

In three sub-pane mode you can close one sub pane using the “Hide This Pane” menu item from the context menu. The sub-pane for which the context menu is called closes.

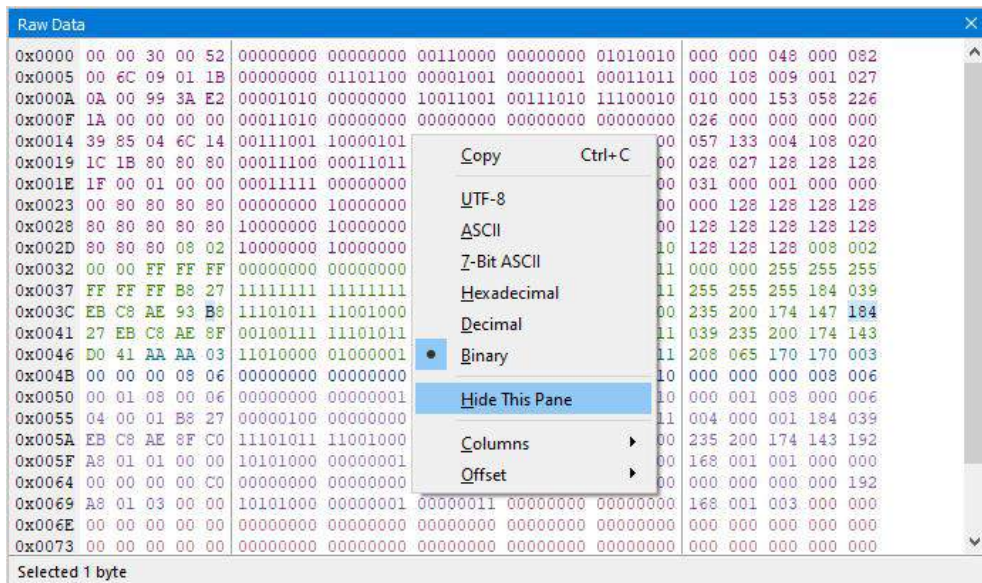


Figure 5.34 - Third sub pane hide option





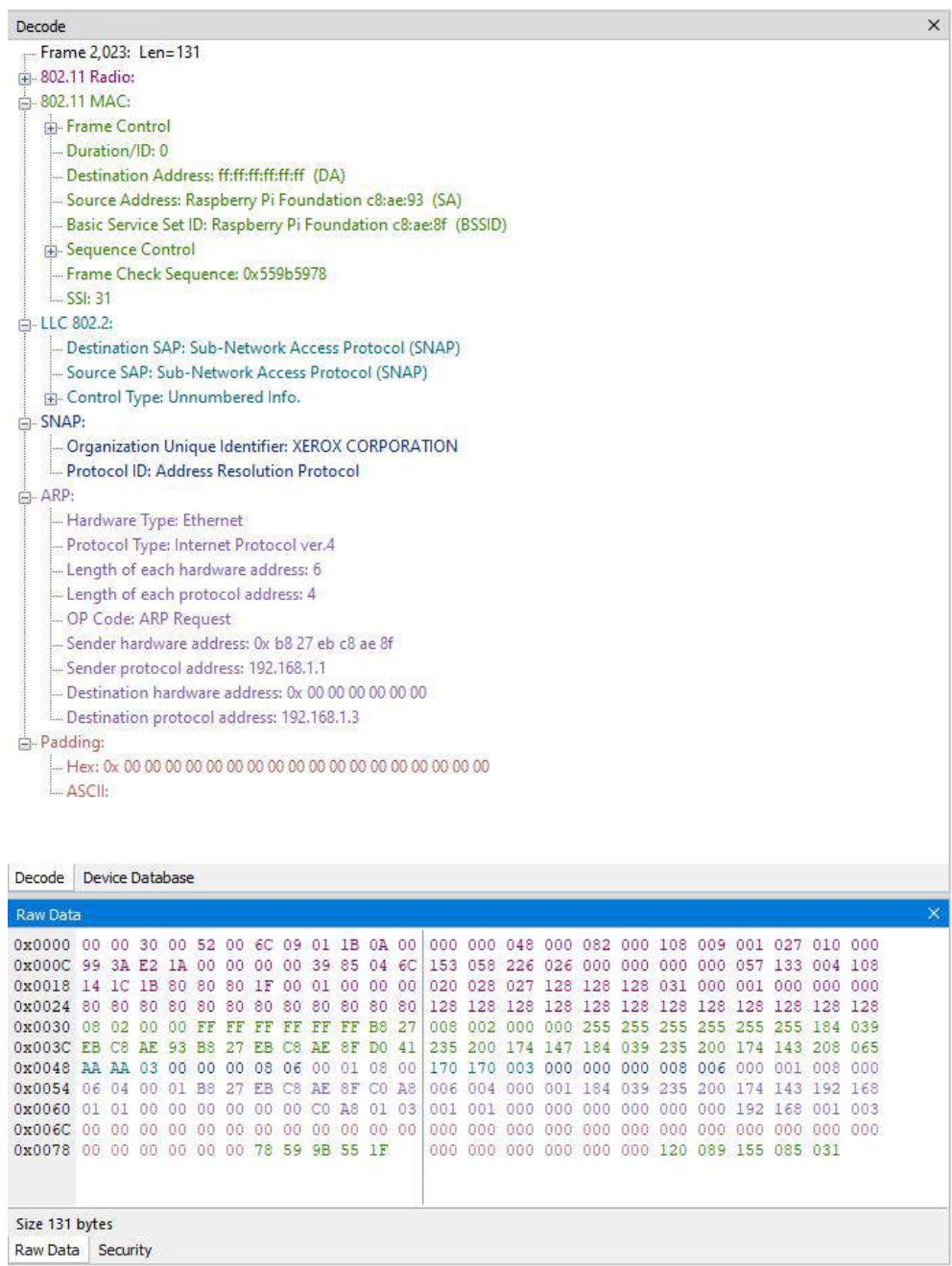


Figure 5.36 - Raw Data Pane: Data color coding



### 5.4.4 Bluetooth Timeline

The *Bluetooth Timeline* displays packet information with an emphasis on temporal information and payload throughput. The timelines also provide selected information from Main windows.

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

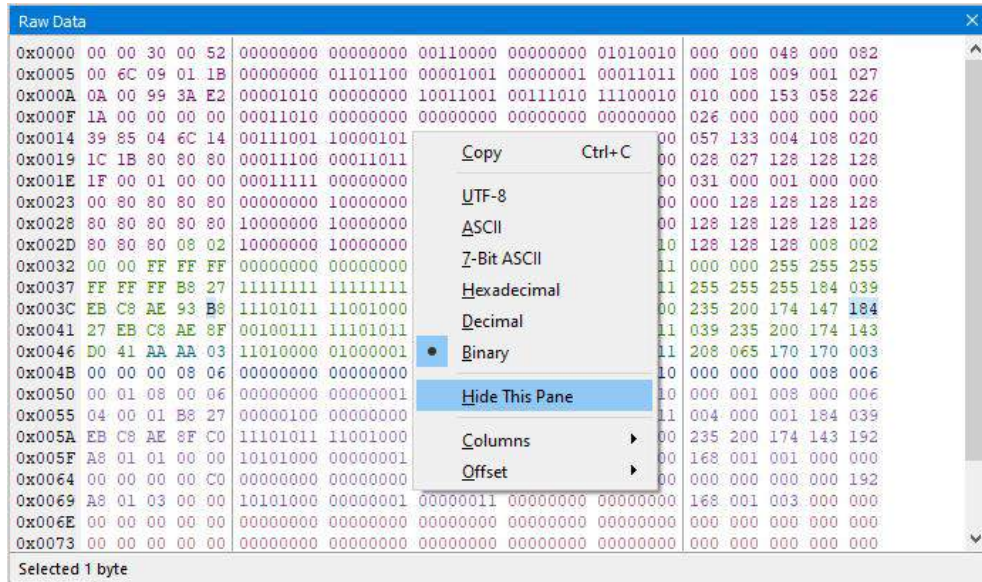


Figure 5.37 - Bluetooth Timeline: Classic View

### 5.4.4.1 Bluetooth Timeline Packet Depiction

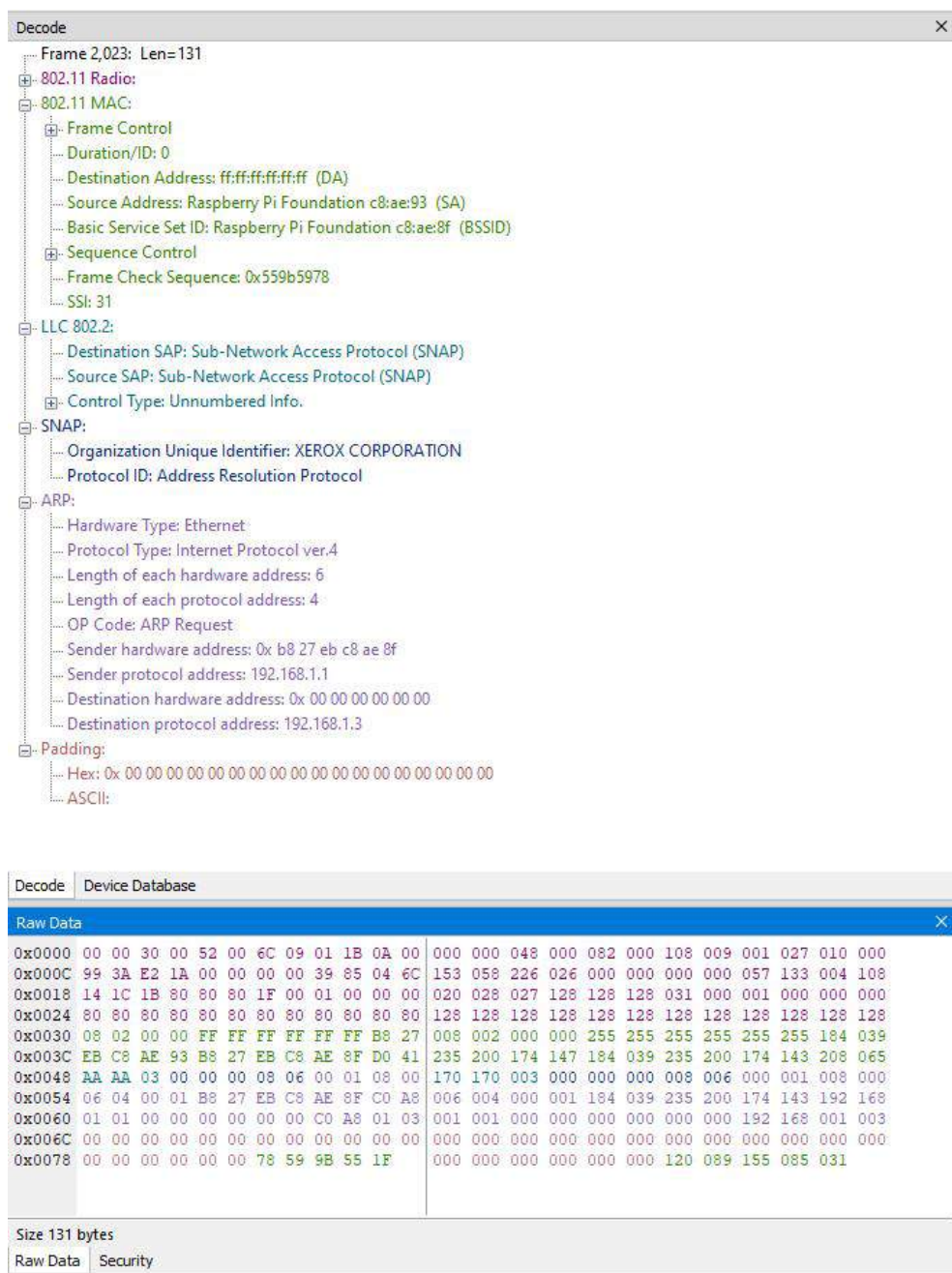


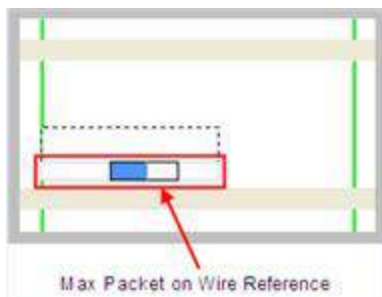
Figure 5.38 - Bluetooth Timeline Packet Depiction with Packet Information Shown

- The timeline shows *Bluetooth* packets within a specific period of time.
- Within each row are two divisions: **C** (central) and **P** (Peripheral). Packets are placed on **C** or **P** depending on the data's role.
- Placing the mouse pointer on a packet displays information about that packet in an information box.

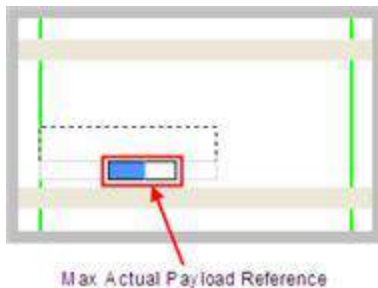
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet. You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline horizontally. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu. User can also Zoom IN/OUT by holding the CTRL key and scroll wheel on the mouse.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625- $\mu$ s). Packet height and length together indicate size (speed times duration).

A packet is drawn using the following components:

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

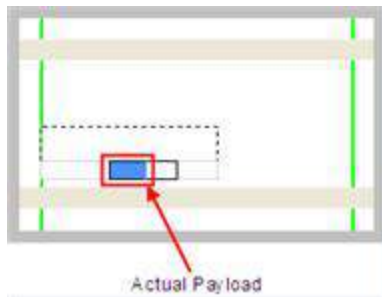


- A “max actual payload reference” rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload in the air contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates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

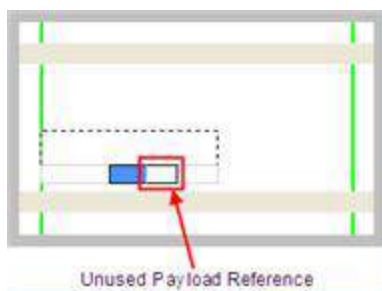


- An “actual payload” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference”

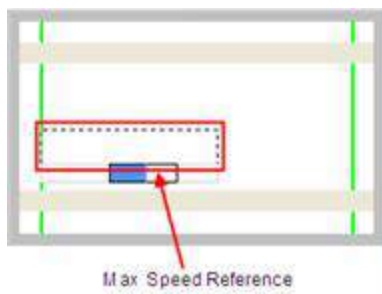
rectangle. If the actual payload is of max size, the entire “max actual payload reference” rectangle is colored.



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

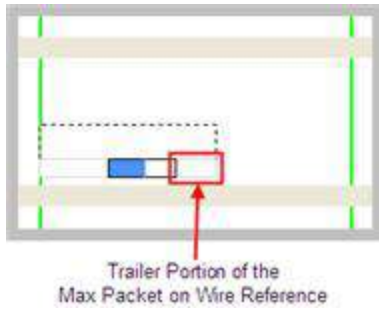


- A “max speed reference” rectangle (dashed lines). This is used to extend the height to that of a 3 Mbits/sec packet and appears only for packets whose speed is less than that. The packet shown here has a speed of 1 Mbit/sec because the height of the other rectangles is 1/3 of the total height.



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

and pixel granularity) between the ends of the two rectangles.



This table shows how packets are colored:

Table 5.3 - Packet Type Colors

Packet Category	Packet Types	Color
ALC	DM1, DM3, DM5, DH1, 2-DH1, 3-DH1, DH3, 2-DH3, 3-DH3, DH5, 2-DH5, 3-DH5, AUX1	Black
SCO	HV1, HV2, HV3, DV	Pink
eSCO	EV3, 2-EV3, 3-EV3, EV4, EV5, 2-EV5, 3-EV5	Purple
LMP*	DM1, DV	Dark Blue
FHS	FHS	Light Blue
NULL	NULL	Light Gray
POLL	POLL	Light Brown
Filler	Filler provided by Wireless Protocol Suite software	Dark Gray

\*LMP is a protocol layer that uses either DM1 or DV packets. If a packet has an LMP layer, the LMP color is used instead of the packet type color.

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

Table 5.4 - Packet Information Presentation





Information	Text	Color	Graphic size	Position
Packet Type	X			
Packet Category		X		
Protocol	X	X		

Table 5.4 - Packet Information Presentation (continued)

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

#### 5.4.4.2 Bluetooth Timeline Packet Navigation and Selection

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

- If there is no selected packet in the timeline, **First Packet** , **Next Packet** , and **Last Packet**  are enabled, but **Previous Packet**  is not.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the **Main windows**. Selecting a packet activates **Previous Packet**.
- Selecting **Previous Packet** with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).
- Selecting **Next Packet** with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).
- Selecting **Previous Packet** or **Next Packet** for a packet that's currently visible selects it without scrolling.
- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline, it is also becomes selected in the **Main windows**. When multiple packets are selected in the timeline, only one of them is selected in the **Main windows**.
- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

#### 5.4.4.3 Bluetooth Timeline Visual Elements

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

- The timeline shows *Bluetooth* packets within a specific period of time.
- Within each row are two divisions: **C** (central) and **P** (Peripheral). Packets are placed on **C** or **P** depending on source of the data within the link.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet. You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- The mouse wheel performs a zoom in and zoom out. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu. You can also Zoom IN/OUT by holding the CTRL key and scroll wheel on the mouse.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625- $\mu$ s). Packet height and length together indicate size (speed times duration).
- Rows of *Bluetooth* Slots: Each slot begins at the left edge of the vertical blue bar. There are two *Bluetooth* clocks per slot. Each slot represents 0.000625 seconds, or 625  $\mu$ s.
- **C** and **P** labels: Within each row, central and peripheral packets are indicated on the left side of the row. By default, all possible central devices (there can be up to 7) are put on the **P** sub-row, but checking the **Show central LT\_ADDR** checkbox shows all existing central device sub-rows with numbered labels (some or all of S1, S2, ..., S7).

- **Contents of Status Bar:** The packet info line appears just above the timeline and displays information for the currently selected packet(s). If only one packet is selected, this information consists of the **packet number**, **packet type**, *Bluetooth clock* (*Bluetooth* only), **Timestamp**, and **Duration**. **Duration** is shown as "Unknown" when the selected packet has an error.

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

Selected packets are bounded by a magenta rectangle. See the [Bluetooth Timeline Packet Navigation and Selection on page 274](#).

- Floating Information Window (aka Tooltip): The information window displays when the mouse cursor hovers on a packet (not slot). It persists as long as the mouse cursor stays on the packet or tooltip. For *Bluetooth*, the tooltip shows the packet number (in bold), the Baseband layer decode from the decode pane of the Main windows (with the percentage of the Payload Length max added).

Discontinuities are indicated by cross-hatched slots. See the [Bluetooth Timeline Discontinuities on page 276](#) section.

- Zoom Tools: **Zoom** tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See [Bluetooth Timeline Zooming, on page 1](#).
- Packet Status: Packet status is indicated by color codes. A yellow slot indicates a re-transmitted packet, a dark red slot indicates a CRC error, and a small red triangle in the upper-left corner of the packet (not the slot) indicates a decode error.



- Right-Click Menu: The right-click menu provides zooming and tool selection. See the [Bluetooth Timeline Discontinuities on page 276](#).
- Graphical Packet Depiction: Each packet within the visible range is graphically depicted. See the [Bluetooth Timeline Packet Depiction on page 270](#).
- Show Running Average: Selecting this check box shows a running average in the Throughput graph as an orange line.
- Show central LT\_ADDR: Selecting this checkbox displays the Peripheral LT\_ADDR in the timeline row labels

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

## Show Legend

The legend can be turned on/off from the Display menu in the toolbar. The settings are saved between sessions.

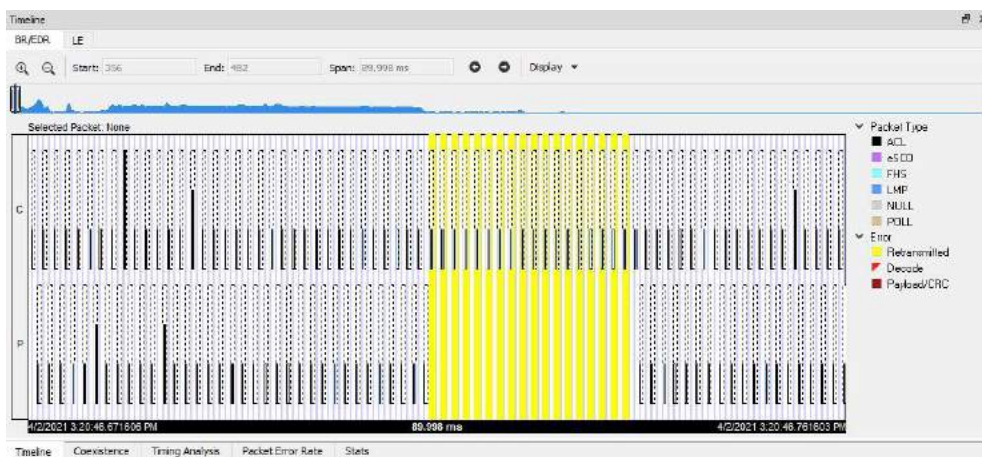


Figure 5.39 - Classic Timeline with Legend

### 5.4.4.4 Bluetooth Timeline Discontinuities

The following figure depicts a discontinuity between two packets.



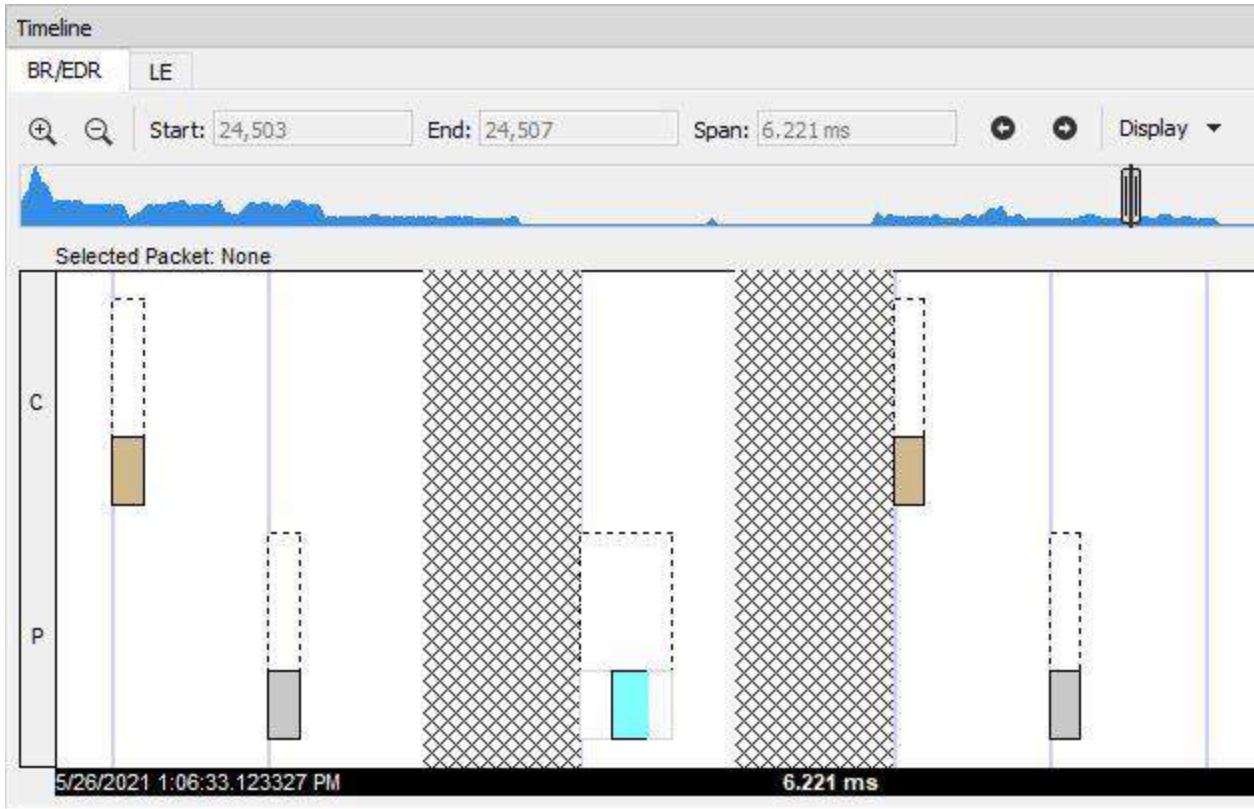


Figure 5.40 - *Bluetooth* Timeline Packet Discontinuity, cross-hatched area.

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

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

### 5.4.5 Low Energy (LE) 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 **Summary Pane**.

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.

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

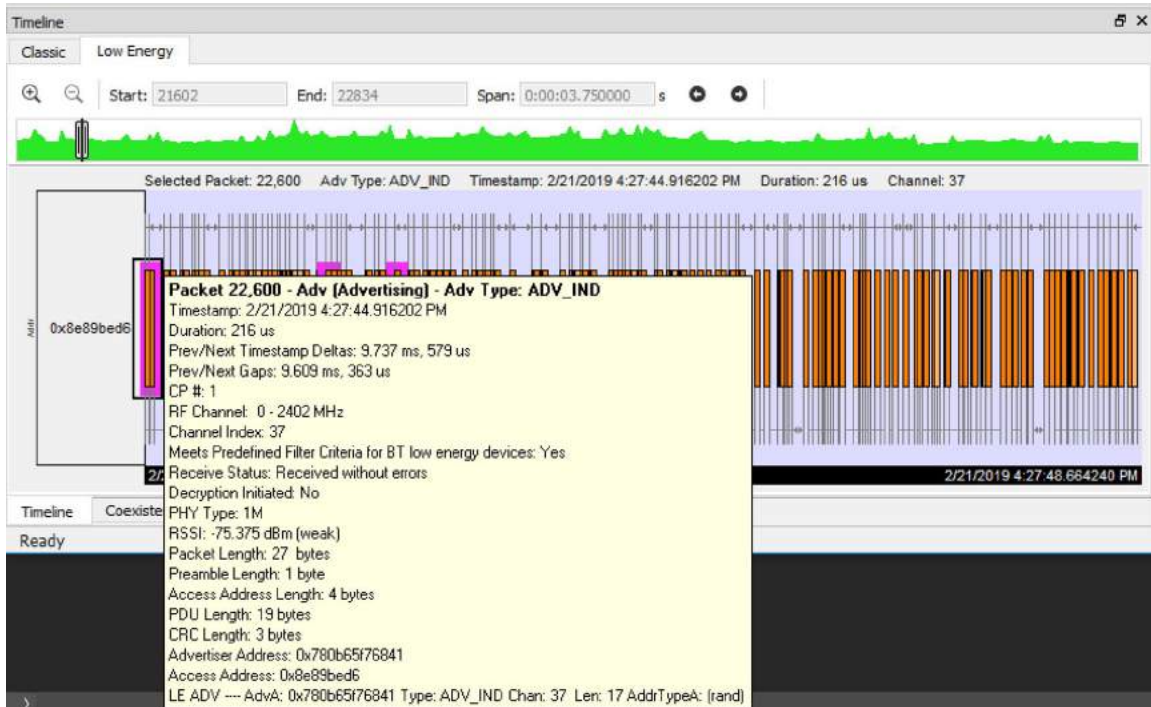


Figure 5.41 - Low Energy Timeline

### 5.4.5.1 Low Energy Timeline Visual Elements

The Low Energy Timeline consists of the following visual elements:

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

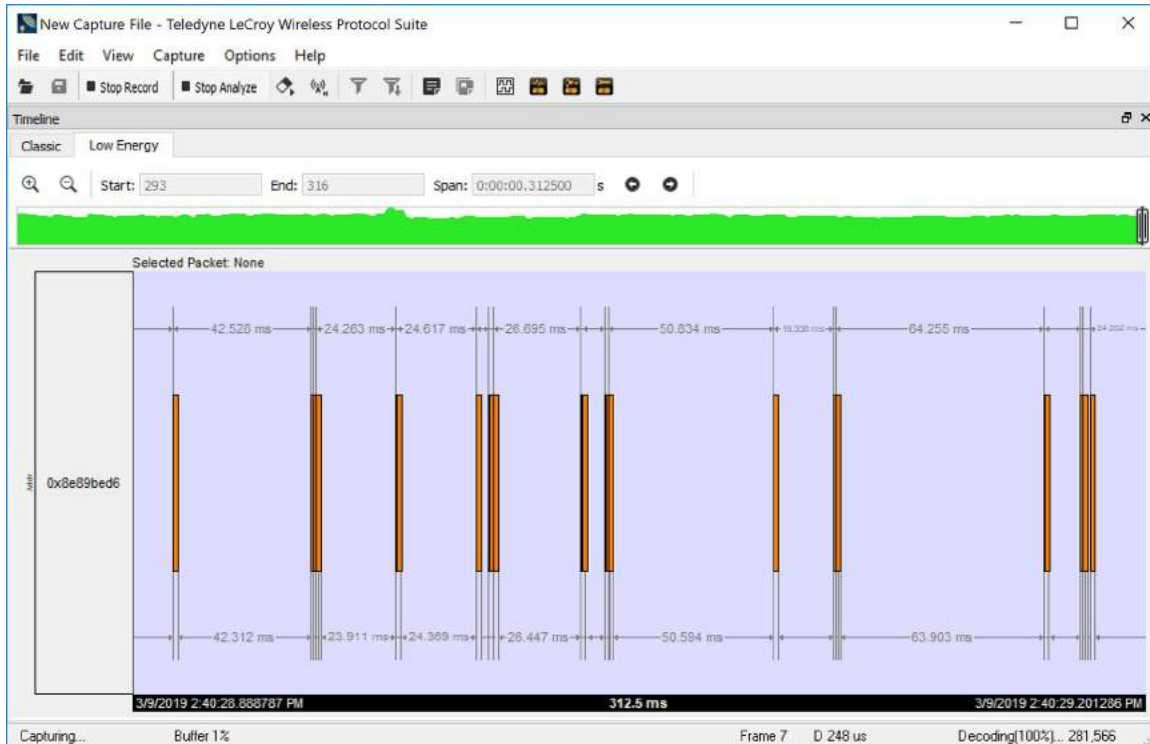


Figure 5.42 - Low Energy Timeline

- **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.

**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.
- 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
- **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.

**Show Legend:** The legend can be turned on/off from the Display menu in the toolbar. The settings are saved between sessions.

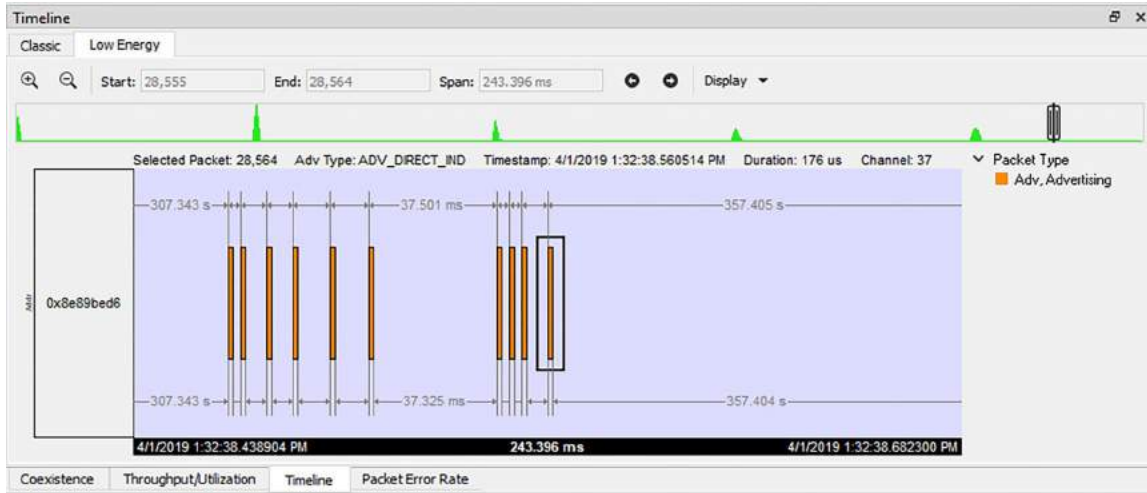


Figure 5.43 - Timeline Low Energy Legend

### 5.4.5.2 Low Energy Timeline Zooming

In Wireless Protocol Suite, the user can select the icon + and - on the toolbar of view which are located to the left of the inputs start/end/span to zoom in and zoom out. Also the user can use right-click menu of view. The following menu will pop up to select the amount of time to be displayed.

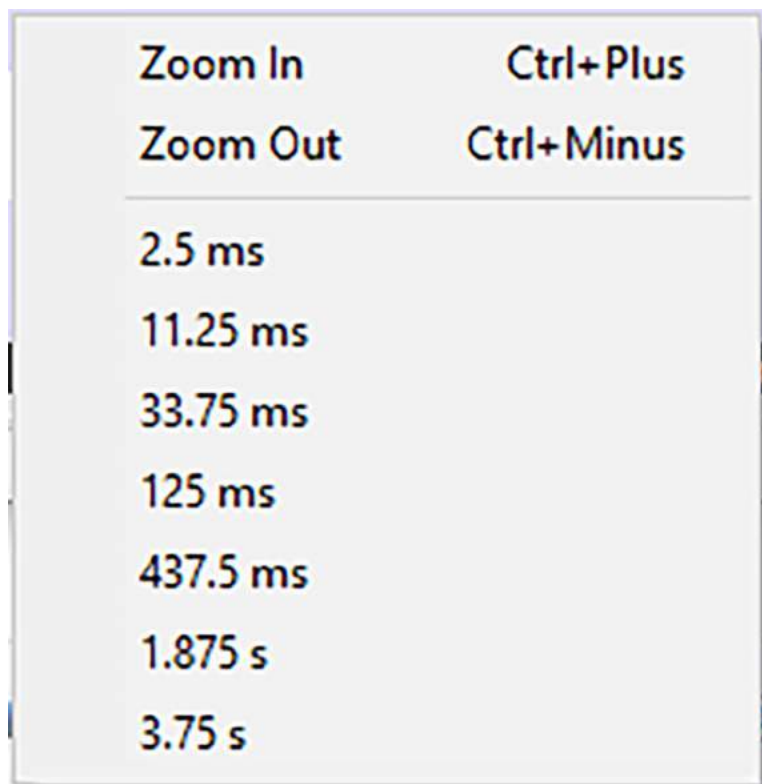


Figure 5.44 - Low Energy Timeline Zoom menu

**Zoom IN/OUT** can also be achieved by holding the CTRL key and moving the scroll wheel on the mouse.

### 5.4.6 Coexistence View

The **Coexistence View** displays Classic Bluetooth, Bluetooth Low Energy, Wi-Fi and 802.15.4 packets by channel and time. You access the **Coexistence View** by clicking its tab below the Summary Pane.

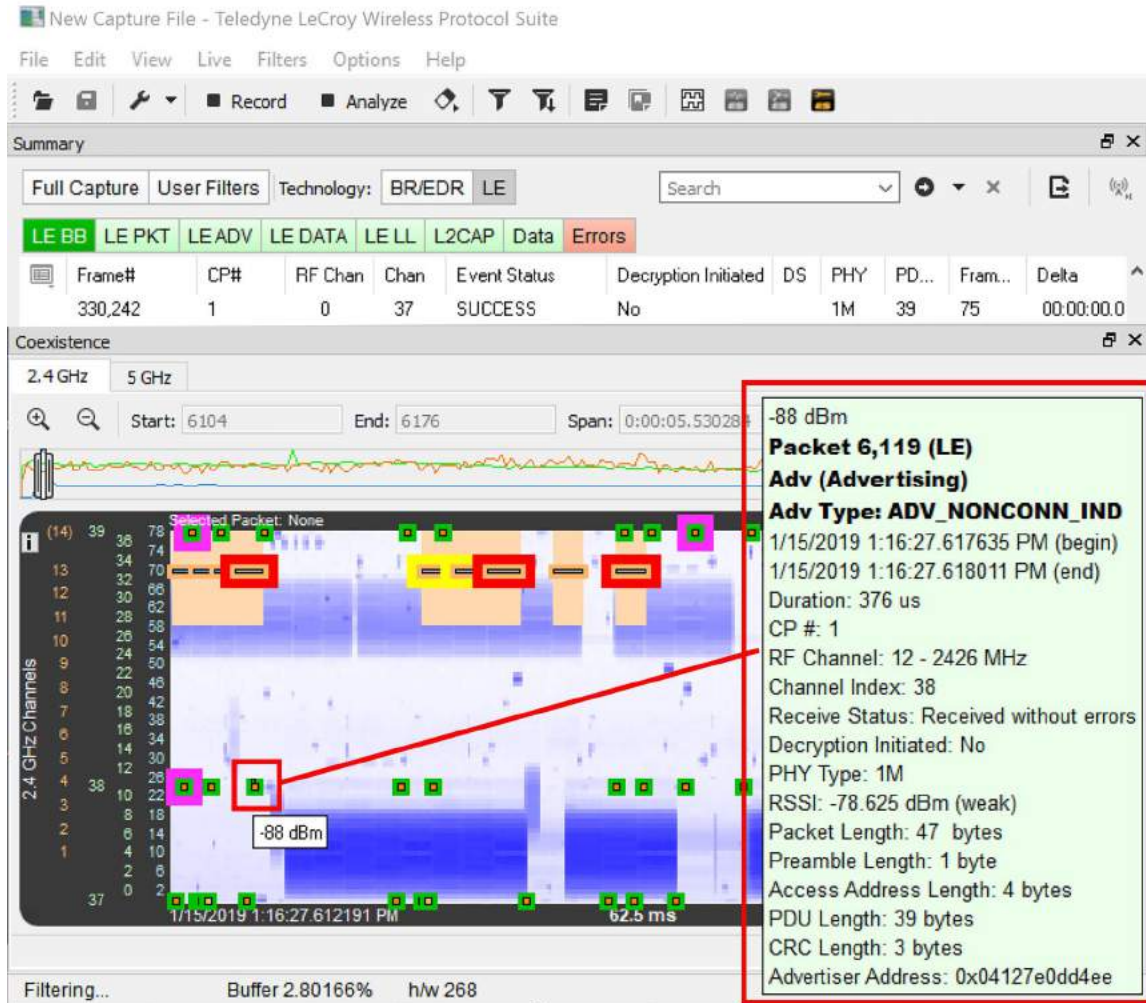


Figure 5.45 - Coexistence View Window 2.4 GHz Bluetooth LE

**Show Legend:** The legend can be turned on/off from the Display menu in the toolbar. The settings are saved between sessions.



Figure 5.46 - Coexistence View: Legend Shown

### 5.4.6.1 Packets

If you select a packet in the Coexistence View, you see information about that Packet:



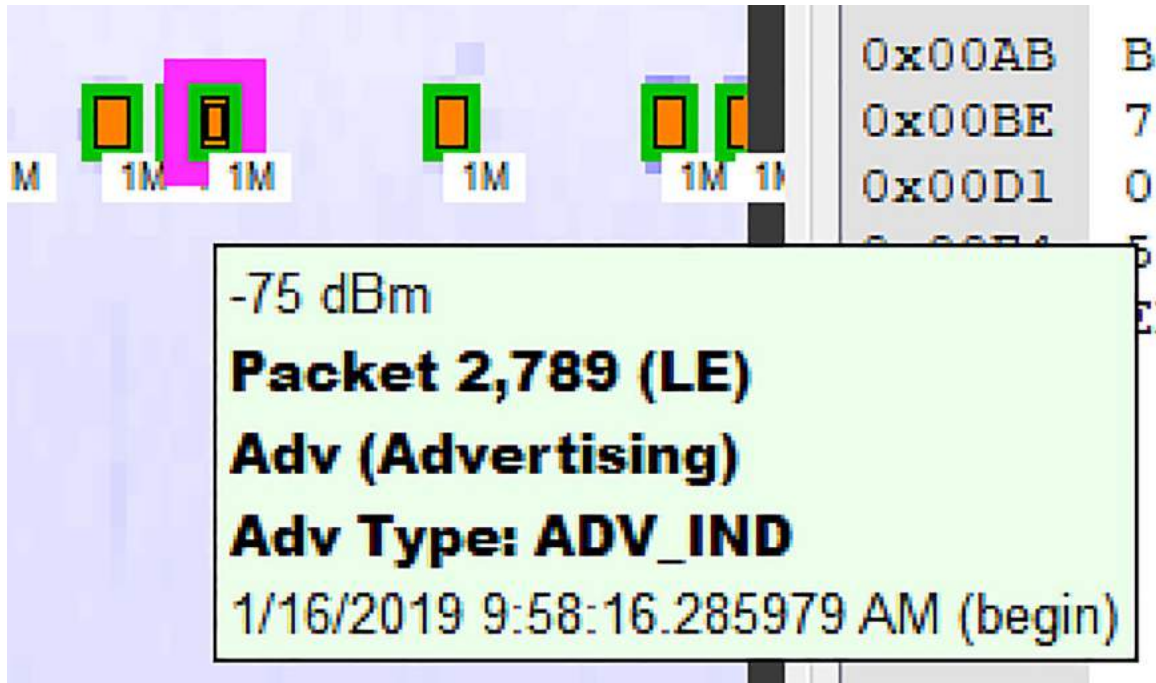


Figure 5.47 - Packet : LE

If you right click on a Packet the following context menu will pop up.



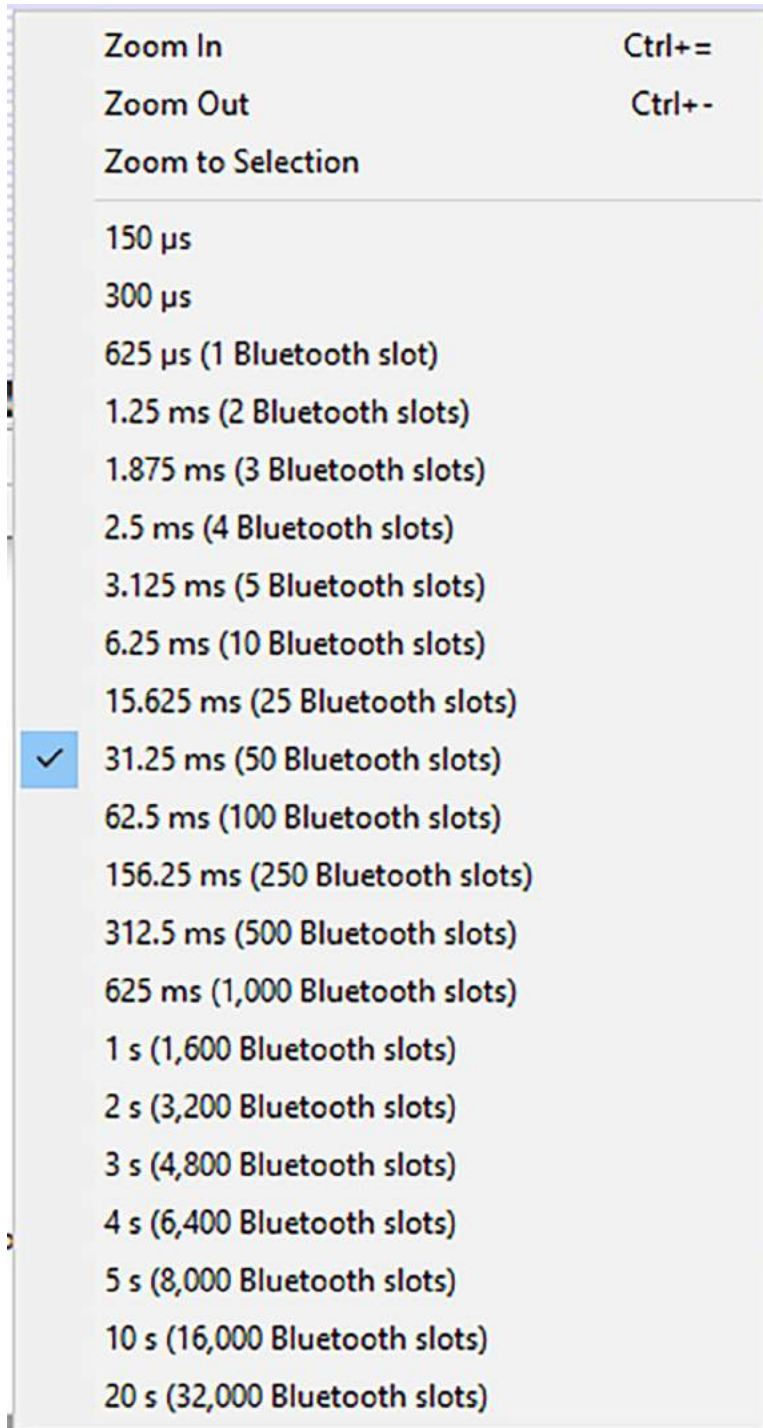


Figure 5.48 - Context Menu Options

If you select the Show Full Tooltip, you'll get details about the Packet.

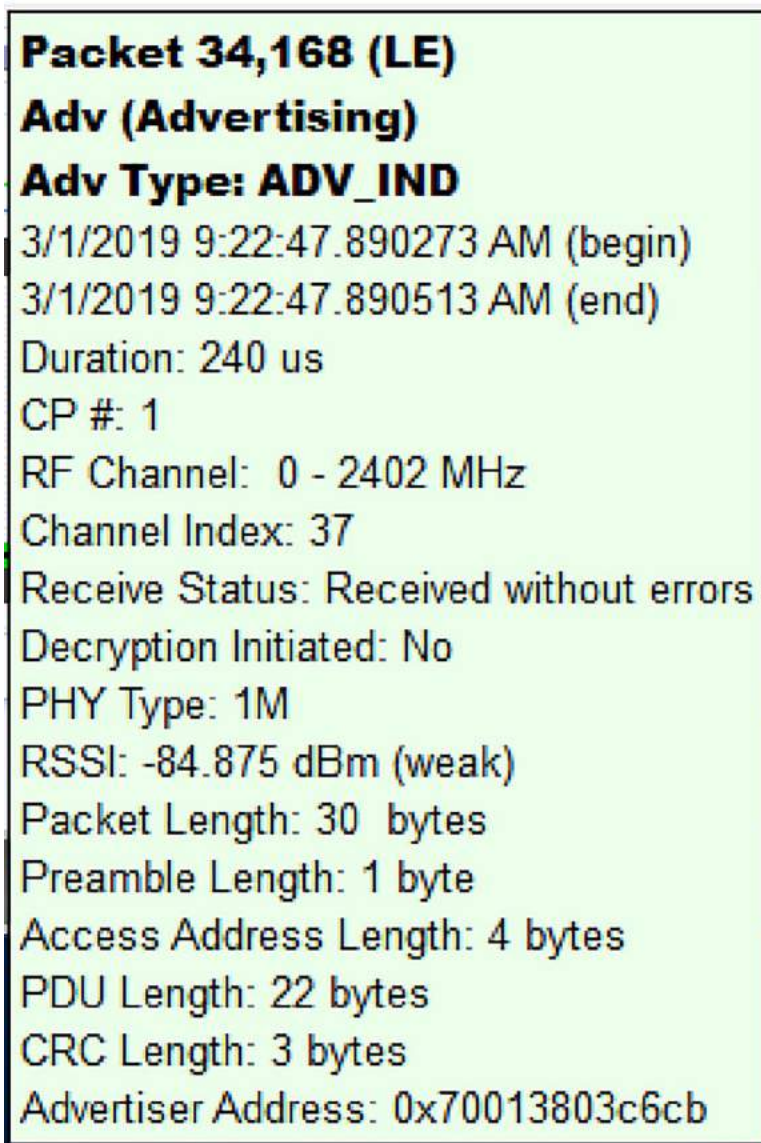


Figure 5.49 - Detailed Tooltip about Packet

**Zoom** IN/OUT can also be achieved by holding the CTRL key and moving the scroll wheel on the mouse.

#### 5.4.6.2 Zoom

In Wireless Protocol Suite, the user can select the icon + and - on the toolbar of the view, which are located to the left of the inputs start/end/span, to zoom in and out.

### 5.4.6.3 Coexistence View - No Packets Displayed with Missing Channel Numbers

**Note:** This topic applies only to Classic *Bluetooth*.

Captured packets that don't contain a channel number, such as HCI, will not be displayed. When no packets have a channel number the **Throughput View** and **Coexistence View** will display a message: "Packets without a channel number (such as HCI) won't be shown."

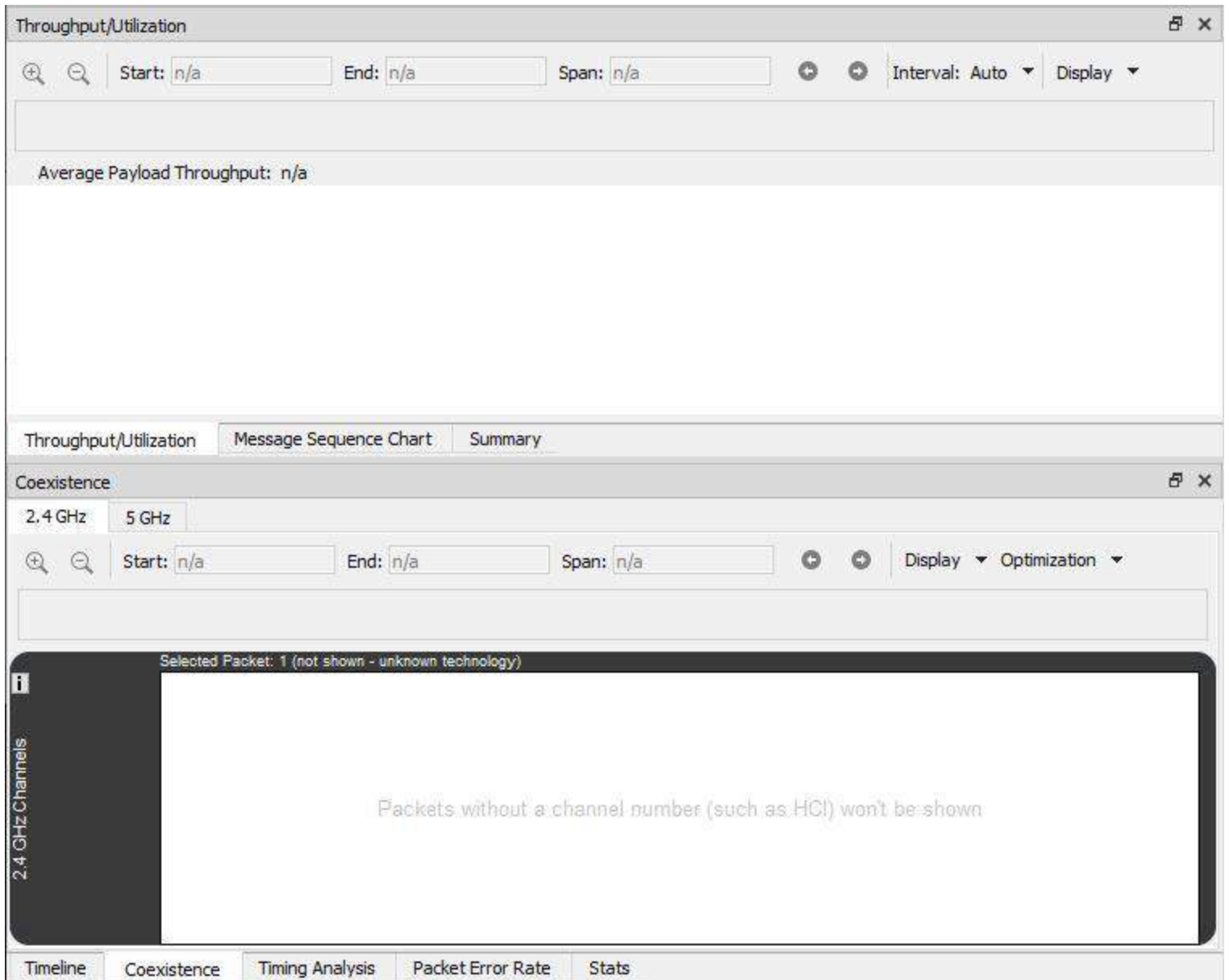


Figure 5.50 - Missing Channel Numbers Message in Views

### 5.4.6.4 Coexistence View - Spectrum

Both the Soderia and the X240 hardware have an option to sample the 2.4 GHz RF spectrum at the unit's antenna connector. The spectrum data represents the Received Signal Strength Indicator (RSSI). The spectrum data is synchronized in time to the captured *Bluetooth* packets and is displayed in the **Coexistence View** 2.4 GHz Timeline. The spectrum power level is shown as a "heat map" behind the timeline packets. The "heat map" appears in shades of blue with darker blues representing higher power levels and lighter blues representing lower power levels (white represents the lowest power level). The darkest shade of blue represents -15dBm and above, while white represents -100 dBm and below.

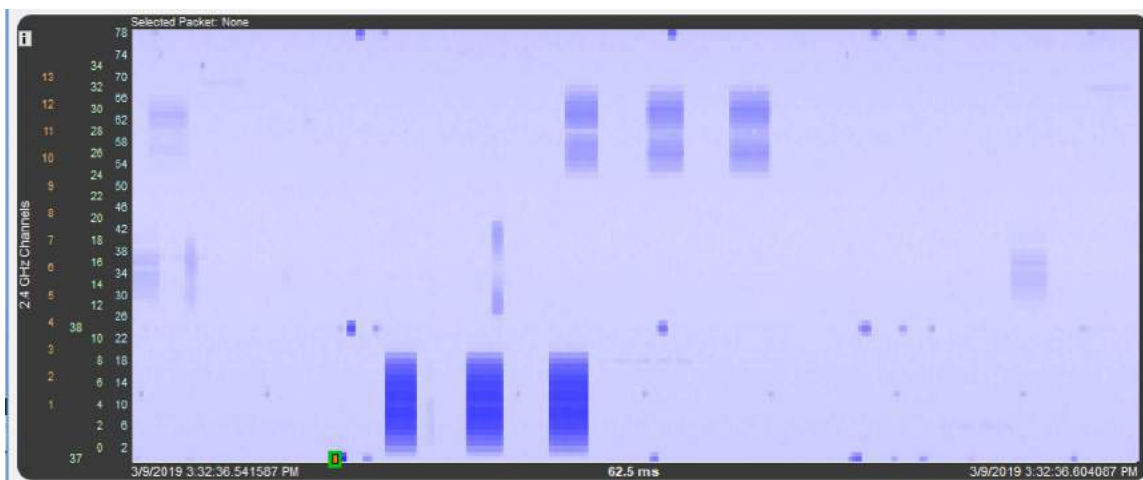


Figure 5.51 - Coexistence View Timeline with Packets and Spectrum Heat Map

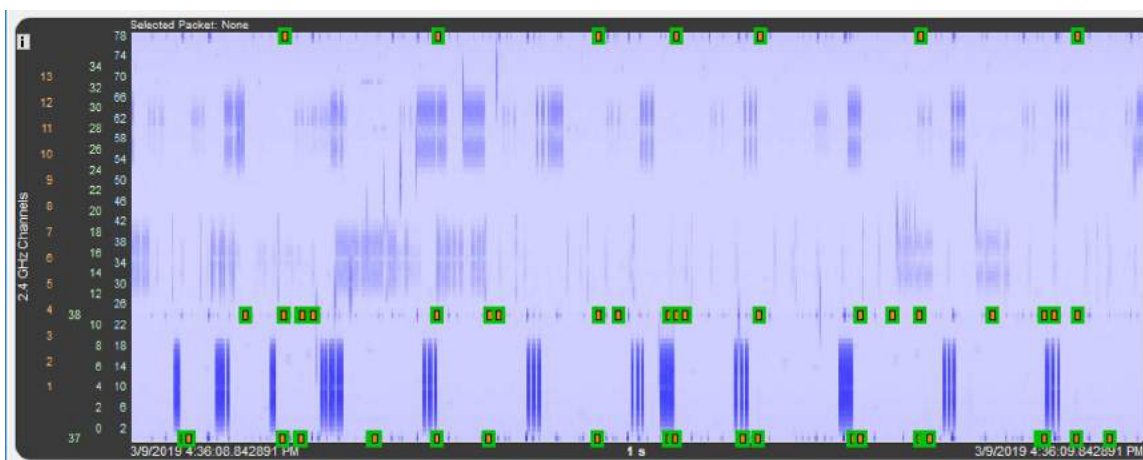


Figure 5.52 - Coexistence View Timeline with Packet Outlines, Packet Selection Boxes, and Spectrum Heat Map

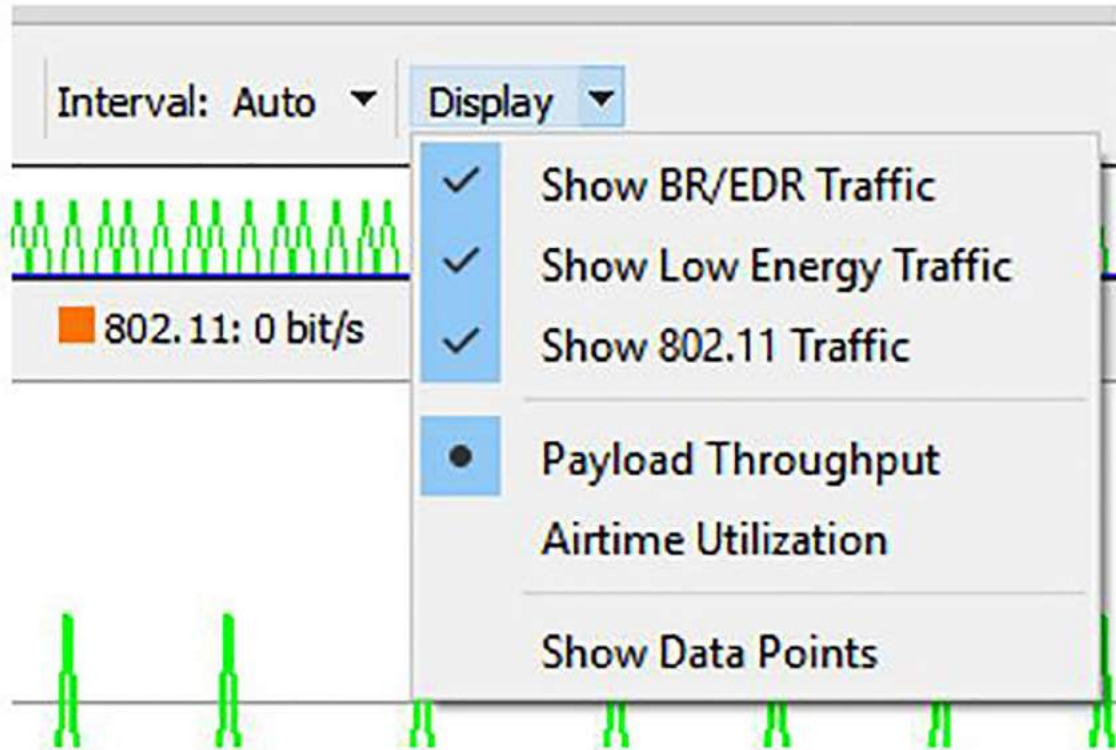


Figure 5.53 - Coexistence Timeline Display Options

The Spectrum heat map view is controlled from the **Spectrum** menu. If spectrum data is available, the spectrum heat map is shown with the packets by default. To hide the spectrum data heat map, uncheck the **Show Spectrum** option.

When displaying the heat map, the user can control how the packets are displayed. The following table describes the options for packet display. These options are mutually exclusive and they are available only when **Show Spectrum** is checked.

Table 5.5 - Spectrum Menu Packet Display Options

Option	Description
<b>Show Packets</b>	Displays each packet. Tooltips, packet text, and selection boxes are available as usual.
<b>Show Packet Outlines</b>	Displays an outline of each packet. In this mode the spectrum data comprising each packet is clearly visible and indicated. Tooltips, packet text, and selection boxes are available as usual.
<b>Hide Packets and Outlines</b>	Packets and packet outlines are not displayed. Tooltips, packet text, and selection boxes are available as usual.



### 5.4.6.5 Show Legend

The legend can be turned on/off from the Display menu in the toolbar. The settings are saved between sessions.



## 5.4.7 Statistics

### Stats View

#### Introduction

The Stats View is a dockable and scrollable pane that shows packet counts and packet count percentages as both text and a bar graph for each technology and for each data rate, NSS (Number of Spatial Streams), MCS (Modulation Coding Scheme), and packet type within each technology. Retransmits can be optionally indicated..

#### Technologies

Supported technologies are BR/EDR, LE, Wi-Fi 1-3 (802.11a/b/g), and Wi-Fi 4 (802.11n).

In BR/EDR, LE, and Wi-Fi 1-3, packet types are grouped by data rate. Data rates are shown in ascending order.

In Wi-Fi 4, packet types are grouped by NSS (Number of Spatial Streams) and MCS (Modulation Coding Scheme).

In each technology, bad packets are shown on a separate row.

#### Retransmits

Retransmits are optionally indicated by selecting Indicate Retransmits in the Display menu. When retransmits are being indicated, the overall length of each bar doesn't change, but the ending portion of it becomes yellow to indicate the percentage of retransmits (if any).

#### Percentages and Packet Counts

All packet count percentages in parentheses are calculated with respect to all packets in the entire capture. Such percentages are used only in technology rows ("BR/EDR", "LE", "Wi-Fi 1-3", and "Wi-Fi 4").

All other packet count percentages are calculated with respect to all packets in the associated technology.

The packet count of each row is equal to the sum of the packet counts in the rows that are grouped below it at the next indentation level.

The packet count of a Total Packets entry is equal to either the sum of its good packets and retransmitted packets or, in the case of a Bad Packets row, the number of bad packets.

Percentages are shown as rounded whole values except that a value between 0% and 1% exclusive is shown as "<1%", and a value between 99% and 100% exclusive is shown as ">99%". This ensures that "0%" is shown only when the packet count is 0, and that "100%" is shown only when the packet count is all applicable packets.

Since percentages are rounded, a sum of percentages can appear to be wrong. For example, a particular data rate's percentage can be displayed as 47% when the percentages of its packet types are displayed as 30% and 16% if, for example, the unrounded percentages of the packet types are 30.32% and 16.47% which equals 46.79% which rounds to 47%.

### Graph Bars

A graph bar consists of either (1) good packets and/or retransmitted packets, or (2) only bad packets in the case of a Bad Packets row.

A Bad Packets bar (1) never indicates retransmits, and (2) is color-coded by technology (blue for BR/EDR, green for LE, and orange for Wi-Fi) and has red text.

All other bars contain good and/or retransmitted packets and have black text. If Indicate Retransmits is selected in the Display menu then each graph bar is color-coded by technology for good packets and has a yellow portion for any retransmits. If Indicate Retransmits is not selected then the entire bar is color-coded by technology.

The length of a bar indicates the total packets percentage, where the percentage is of all packets in the entire capture for a technology row ("BR/EDR", "LE", "Wi-Fi 1-3", and "Wi-Fi 4"), and is of all packets in the associated technology for all other rows.

### Navigation

As in many other views, Stats View has a Navigation Bar whose slider indicates the displayed time range. The time range can be changed by clicking the zoom buttons, selecting the Zoom In or Zoom Out entries in the right-click menu, selecting the zoom presets in the right-click menu, dragging the Navigation Bar slider to a different position, or dragging either side of the Navigation Bar slider to resize it.

To display a specific packet range in the Stats Graph, select the desired packet range in the Summary pane by clicking on one packet and then shift-clicking on another packet, then select Zoom to Selection in the Stats View's Display menu.

The Navigation Bar contains a color-coded graph of the entire capture that shows packets per second for BR/EDR, LE, Wi-Fi, and 802.15.4.

### Nodes

With the exception of packet type nodes, which are endpoints, any node can be collapsed or expanded by clicking on the node label or on the icon that precedes the label. To collapse or expand all nodes in one operation, click on Collapse All Nodes or Expand All Nodes respectively in the Display menu.

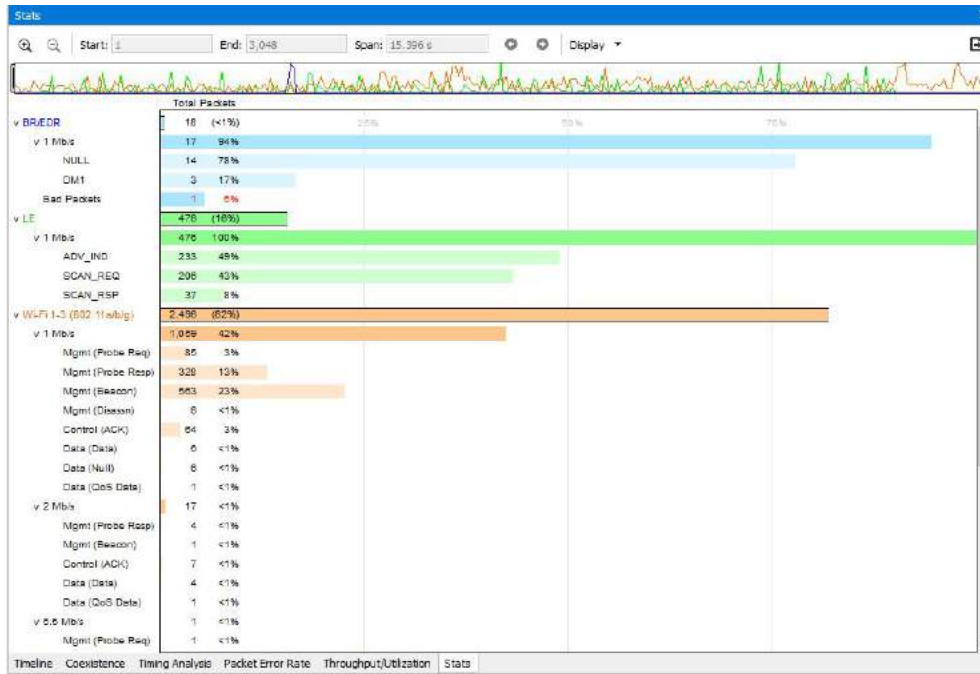


Figure 5.54 - Stats View Pane

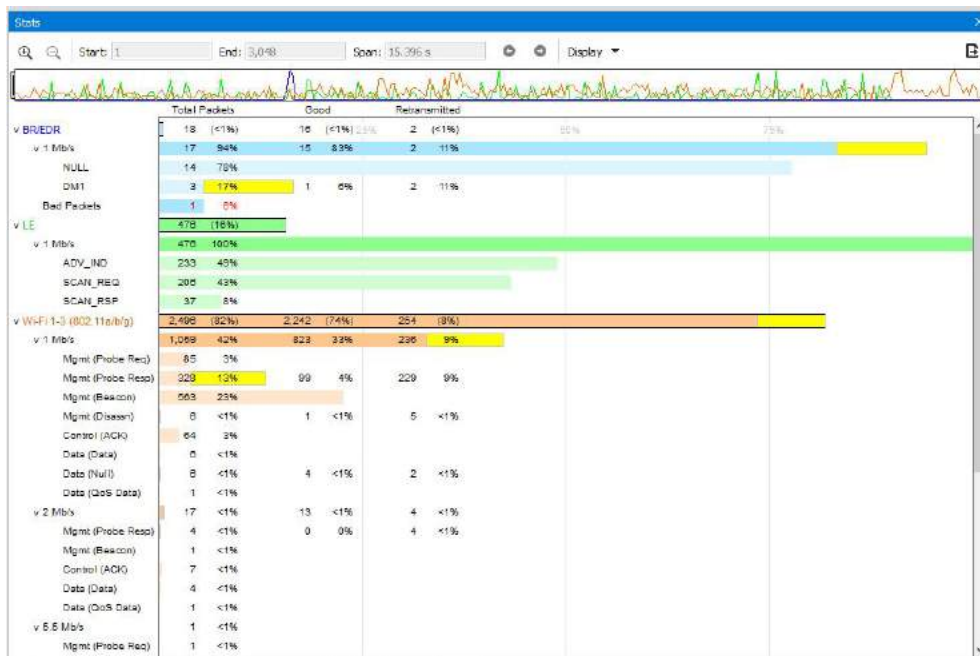


Figure 5.55 - Stats View with Good Packets and Retransmitted Packets indicated separately

Statistics can be exported to a csv file using button on the Navigation toolbar.



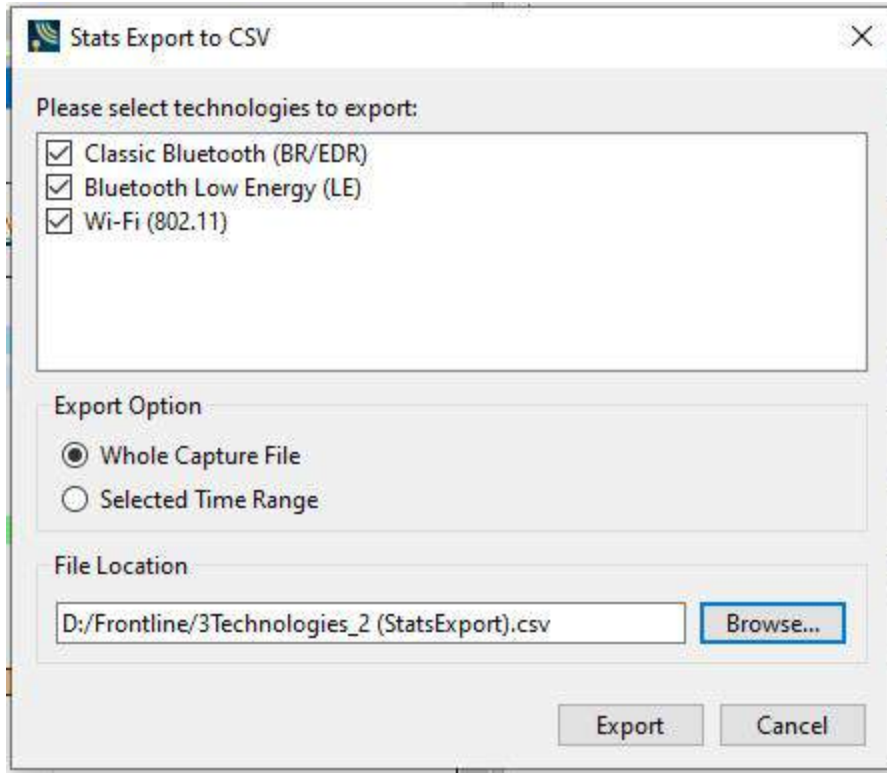


Figure 5.56 - Stats view export dialog

The Stats view export dialog has several options. You can select technologies to export as well as range to export (whole file or range selected with Navigation bar). Choose path and filename to save.

### 5.4.8 Packet Error Rate Statistics

**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 from View -> Packet Error Rate

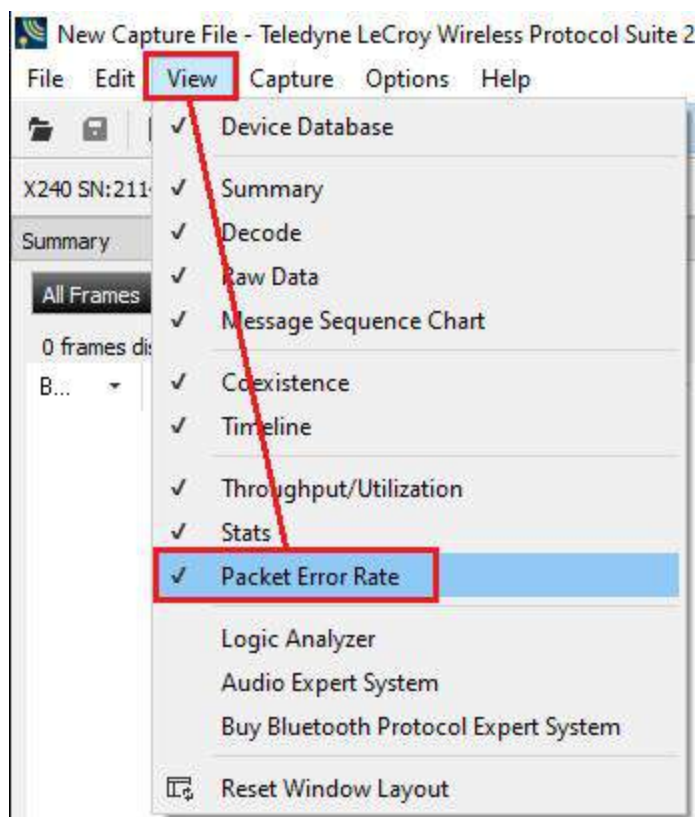


Figure 5.57 - Packet Error Rate

## Packet Error Rate Statistics View by Channel

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 Classic *Bluetooth* channel numbered 0 through 78 and for each *Bluetooth* Low Energy channel numbered 0 through 39. Similarly a graph for Bluetooth BR/EDR data will show channel 0 through 78. You can scroll on the PER stats View using the mouse wheel. Each scroll step equals 1 bar on the graph. You can zoom on the graph by holding the CTRL key and using the scroll wheel on the mouse.

### Each channel is rated:

- Good
- Retransmitted
- Header Error
- Length/CRC Error
- Unused

### Bluetooth Classic Packet Error Rate



Figure 5.58 - Classic Bluetooth Packet Error Rate Statistics Window

### Bluetooth Low Energy Packet Error Rate

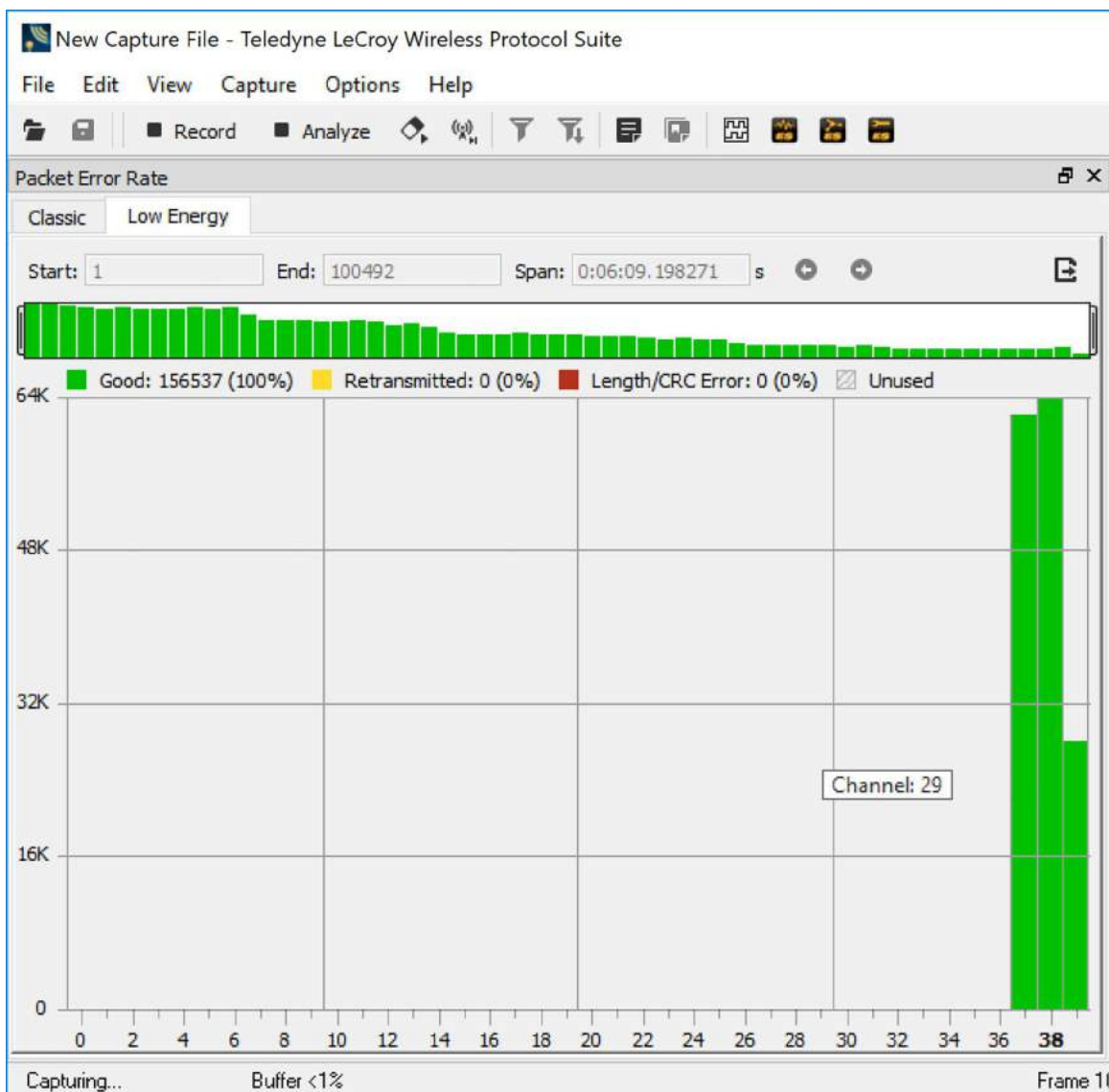


Figure 5.59 - Bluetooth Low Energy PER Stats Window

## 5.4.9 Throughput

In general, throughput is the rate of successful message delivery over a communication channel. In this case, we are interested in the rate of successful message delivery over a Bluetooth data channel.

The figure depicts the **Throughput** display with the **Average Throughput** and the **Payload Throughput** for both Classic and Low Energy *Bluetooth* traffic.

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

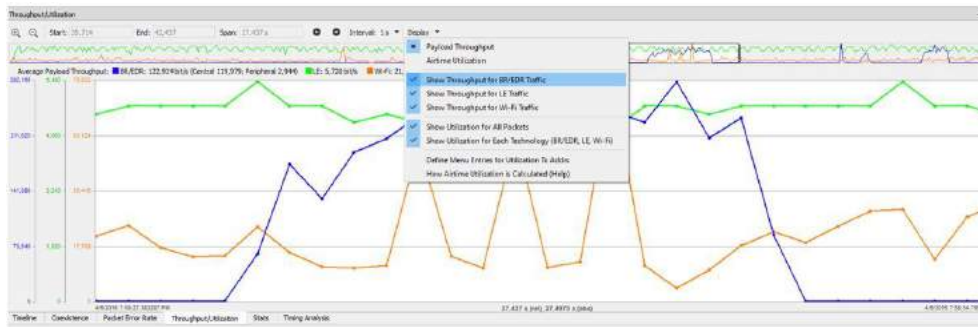


Figure 5.60 - Payload Throughput:Bluetooth LE

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

- **Average Throughput** is shown as 0 when there is only one packet, because in that case the timestamp difference is 0 and an average cannot be computed.
- **Duration** is from the beginning of the first packet to the end of the last packet.
- **Duration for average throughput** is from the beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- **Average Throughput** is shown for all devices, central devices, and central devices.

The user can move left or right in the **Throughput Pane** using the mouse wheel.

The user can also **Zoom** using the + and - buttons or using the ctrl + mouse scroll wheel just like in other panes.

### 5.4.10 Airtime Utilization

Airtime Utilization is the percentage of the duration of a data point that is occupied by applicable packets. A packet is "applicable" if it has the specified address or attribute as described below. Bad packets are excluded. Retransmitted packets are included.

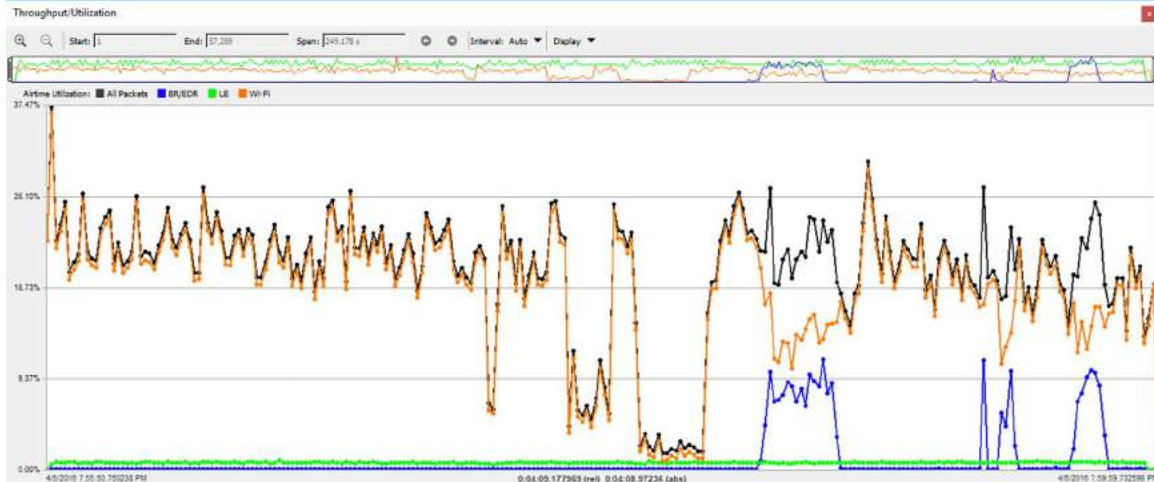


Figure 5.61 - Utilization Graph

Utilization Graph showing plots for all packets regardless of technology (black), all BR/EDR packets (blue), all LE packets (green), and all Wi-Fi packets (orange). Plots for individual devices can also be shown.

For example, if the data point duration is 1ms and the total duration of applicable packets within that data point is 200us, the airtime utilization is 200us / 1ms = 20%. The tooltip of each data point shows both the duration of the data point and the total duration of the applicable packets within that data point.

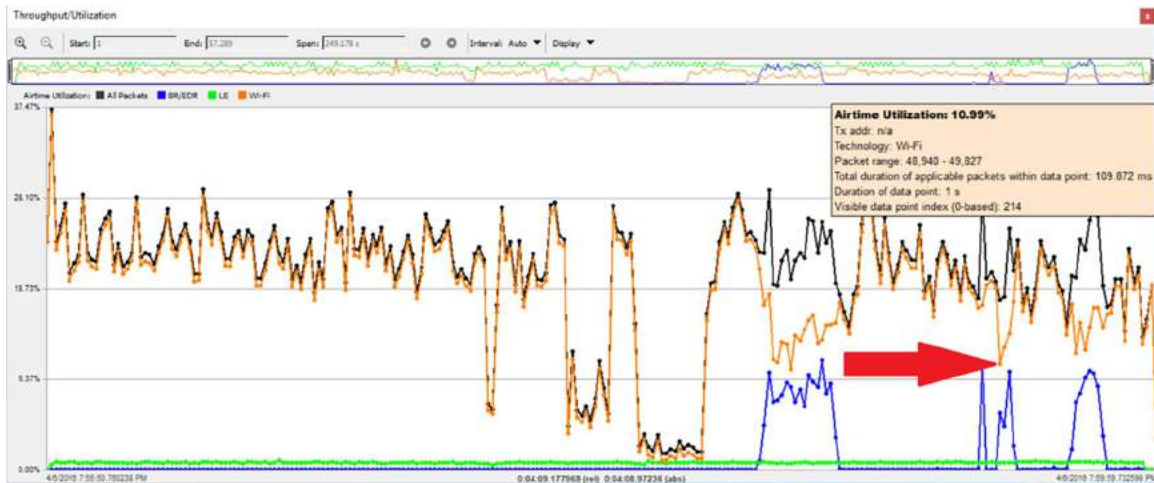


Figure 5.62 - Tooltip Displayed

Tooltip displayed when mouse hovered on the data point indicated by the red arrow.



For a single device the airtime utilization cannot exceed 100% since a device sends only one packet at a time. If the data point duration is small enough that it's filled by an applicable packet or a portion of an applicable packet then the airtime utilization is 100%. For larger data point durations the airtime utilization will always be less than 100%. To display the airtime utilization for a single device define a menu entry for it by selecting Define Menu Entries for Utilization Tx Addr in the Display menu. Up to 10 such menu entries can be defined. They appear in the Display menu after starting a new live capture or opening a capture file. They persist until removed by the user.



Figure 5.63 - Define Menu Entries for Utilization Tx Addr



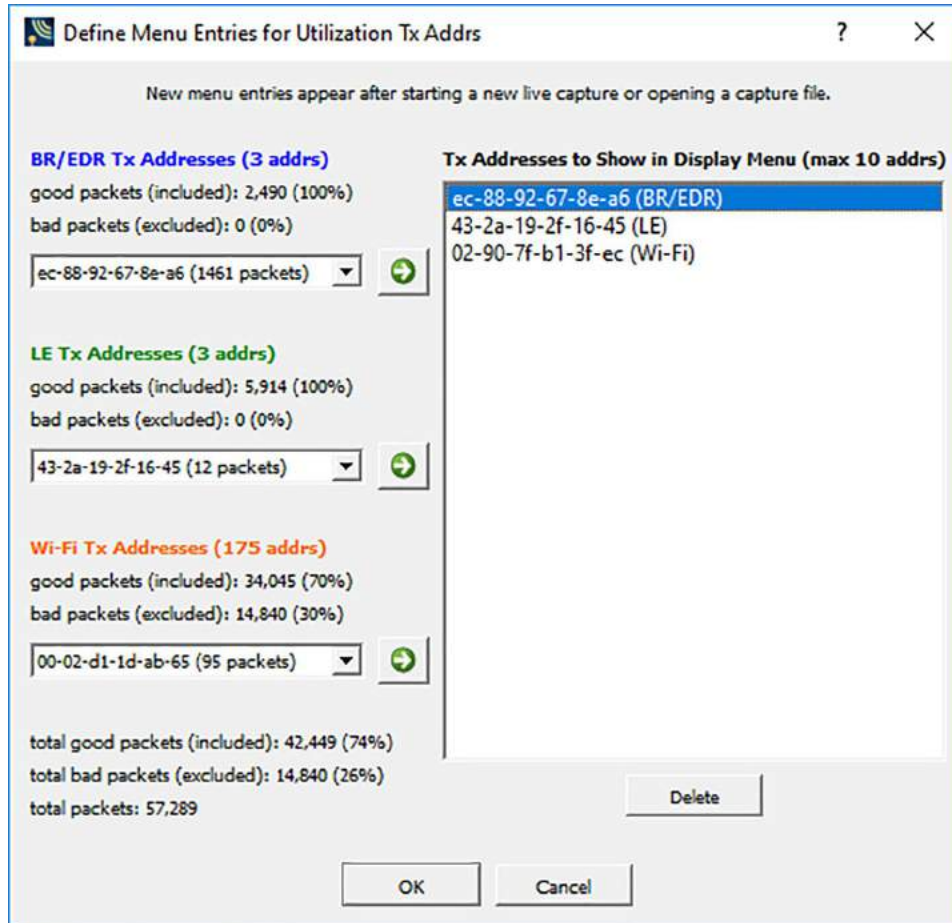


Figure 5.64 - Define Menu Entries for Utilization Tx Addr

The “Define Menu Entries for Utilization Tx Addr” dialog is used to define menu entries to show airtime utilization for individual devices. Here there are two existing entries and a new entry is being added.

For multiple devices the airtime utilization can exceed 100% since the utilizations of each device are added together. This is the case with the “all packets” and “all packets in each technology” plots, which are displayed by selecting Show Utilization for All Packets and Show Utilization for Each Technology (BR/EDR, LE, Wi-Fi) respectively in the Display menu. The screenshots above show plots for all packets regardless of technology (black), all BR/EDR packets (blue), all LE packets (green), and all Wi-Fi packets (orange). The Tx Addr field in the tooltip is set to “n/a” in all those cases.

The plot for a single device uses the same technology-specific color coding. The Tx Addr field in the tooltip shows the device address.



Figure 5.65 - Tooltip for Single Device

*Tooltip displayed for a plot of a single device when mouse hovered on the data point indicated by the red arrow.*

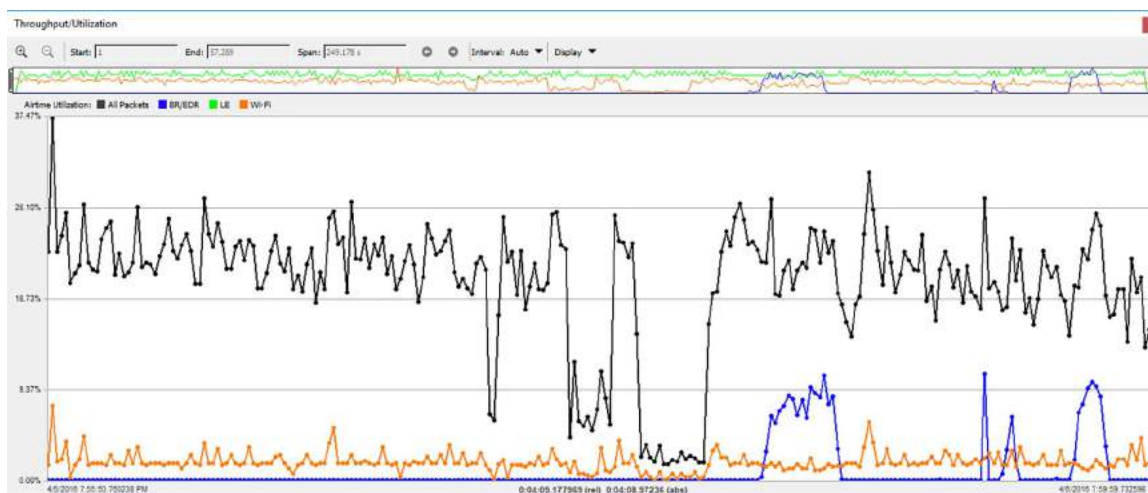


Figure 5.66 - Plot of Same Device

*The plot of the same device plus plots for all packets (black) and for a Wi-Fi device (orange). The percentage scale on the y-axis adjusts automatically.*

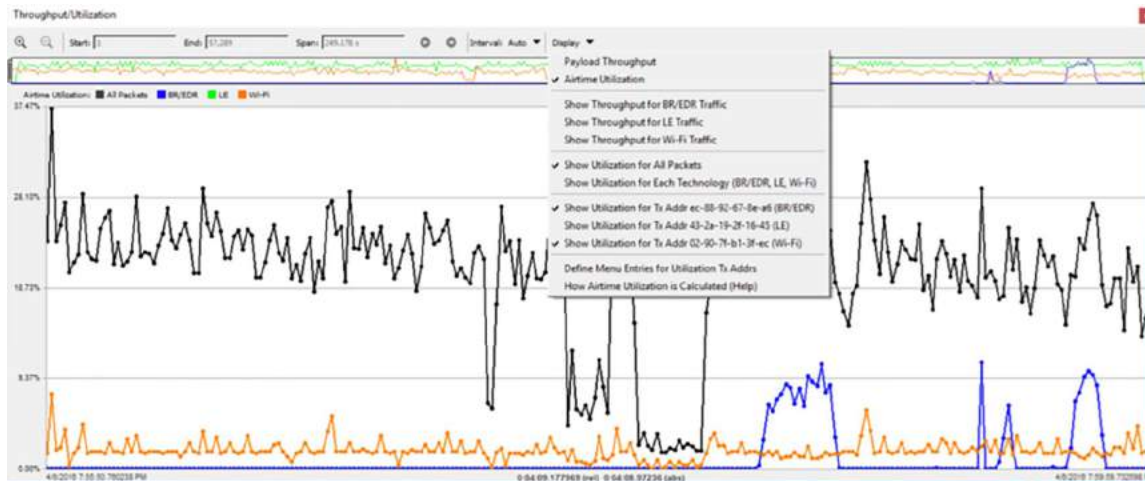


Figure 5.67 - Display Menu

*The Display menu selections that produce these plots.*

### 5.4.11 Message Sequence Chart (MSC)

The **Message Sequence Chart (MSC)** displays information about the messages passed between protocol layers. MSC displays a concise overview of a *Bluetooth* connection, highlighting the essential elements for 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 or profile. the MSC is color coded for a clear and easy view of your data. You access the Message Sequence Chart from the View tab on the main toolbar.

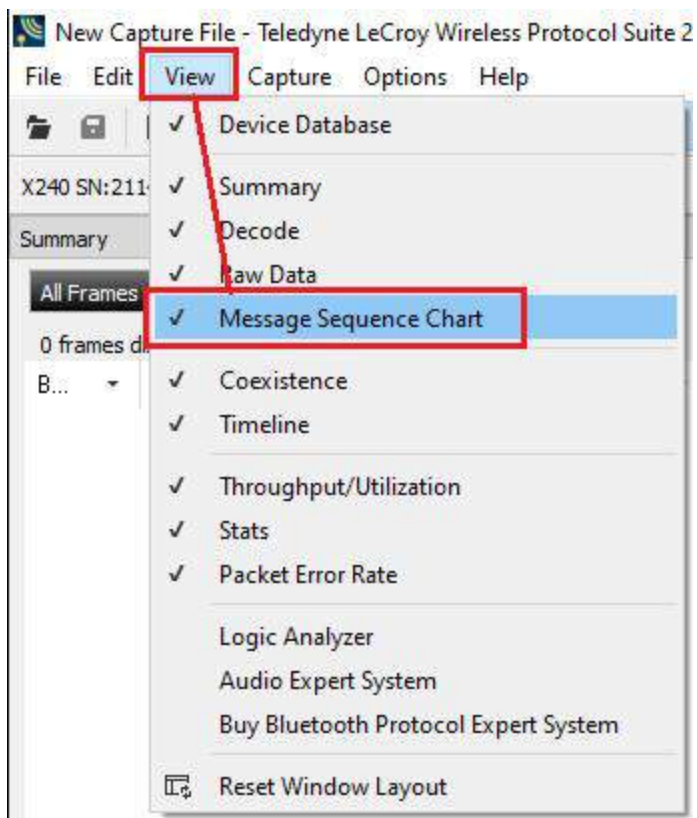


Figure 5.68 - View -> Message Sequence Chart

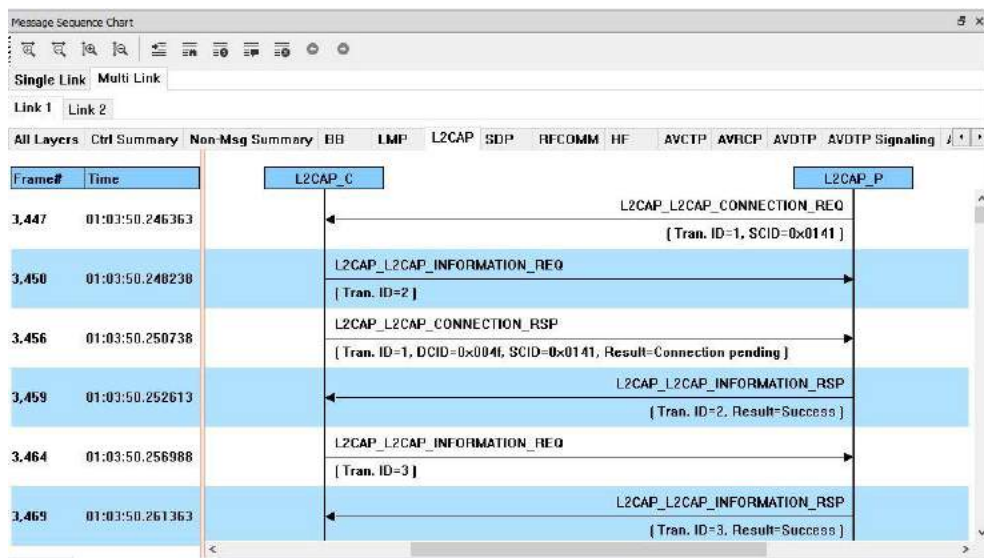
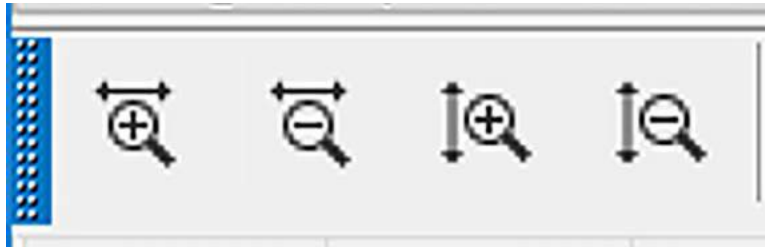


Figure 5.69 - Message Sequence Chart Window


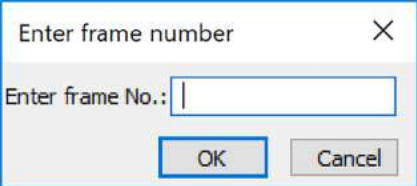

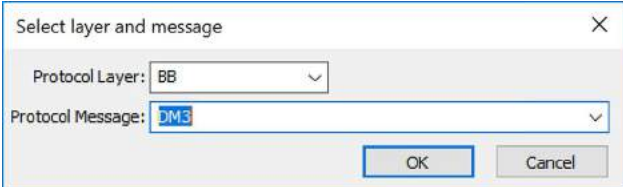





**What do I see on the dialog?**

At the top of the dialog you see four icons that you use to zoom in and out of the display vertically and horizontally.



There are seven navigation icons also on the toolbar.

1. Go to Frame Number: Brings up a box to enter a Frame number
2. Search: Brings up a box to Select Layer and Message
3. Go to First Information Message
4. Go to First Protocol State Message
5. Go to First Error Frame
6. Go to the previous occurrence of a selected item
7. Go to the next occurrence of a selected item

	This icon pops up an Enter frame number box.	
	This icon pops up a Select layer and message box.	
	This icon takes you to the First Information Message.	
	This icon takes you to the first Protocol State Message.	
	This icon takes you to the First Error Message.	
	This icon will search for a previous occurrence of an item.	
	This icon will search for the next occurrence of an item.	

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

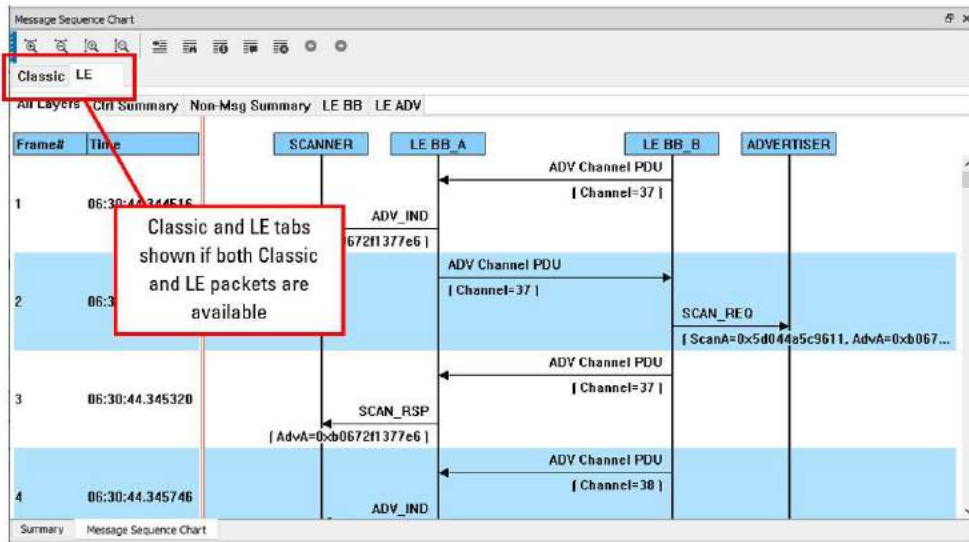
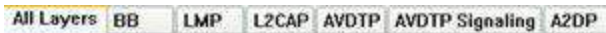


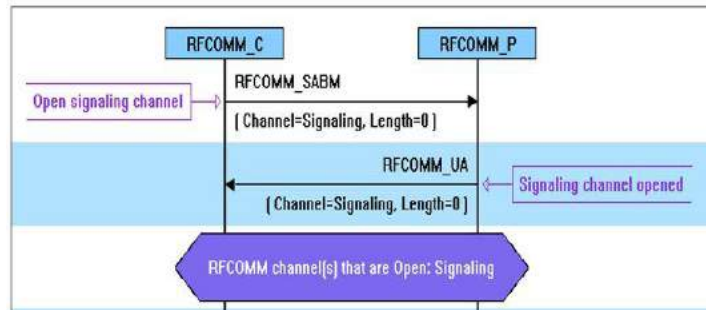
Figure 5.70 - Classic and LE tabs

If the **Classic** tab is selected, you will see Classic protocols. If you select the **LE** tab, you will see LE Protocols. If there are no packets for that protocol, its tab will not appear.



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

Clicking on a tab displays the messaging between the central and peripheral for that protocol. For example, if you select **RFCOMM**, you will see the messaging between the **RFCOMM{C}** Central, and the **RFCOMM{P}** Peripheral.



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.

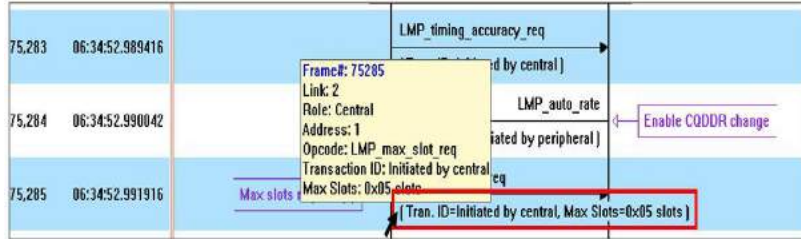
If you want to see all the messaging in one dialog, you select the **All Layers** tab.



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

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

However, if 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.

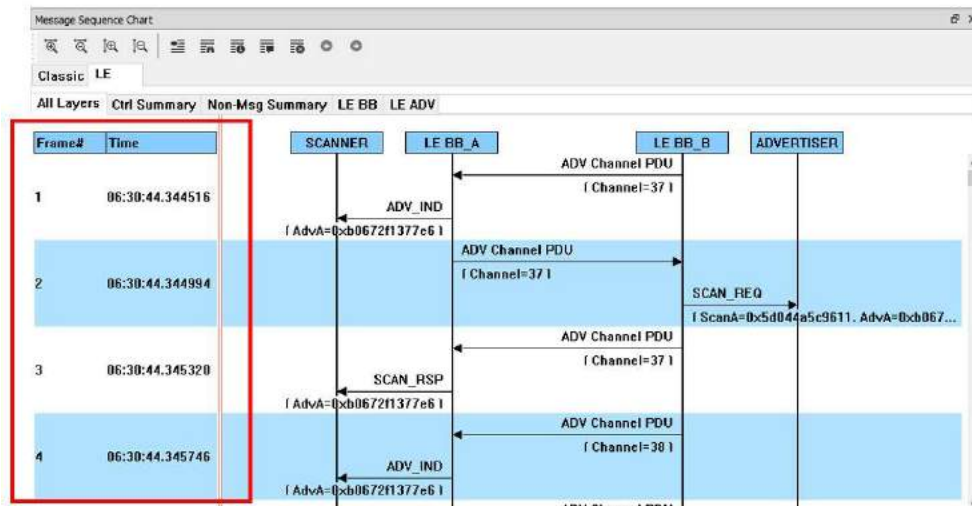


Figure 5.71 - Frame# and Time Display, inside red box.

### 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. The mouse wheel also moves the dialog up and 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.



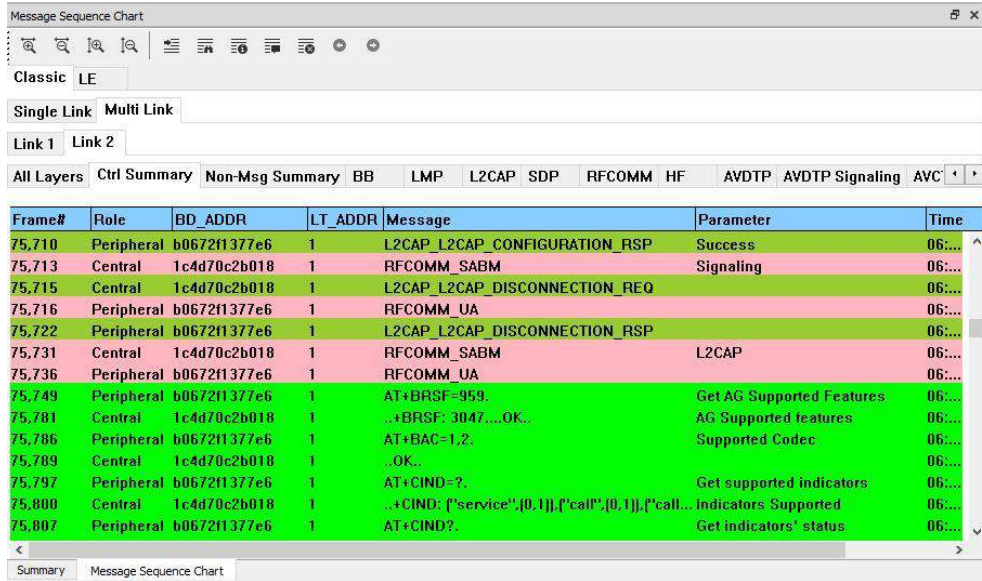


Figure 5.72 - Main windows and Signaling Frames Summary

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

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

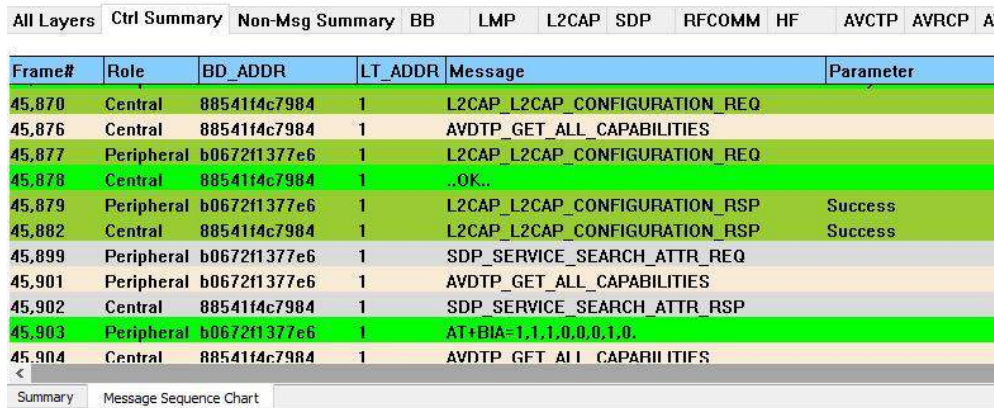


Figure 5.73 - Packet Layers Shown in Different Colors

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

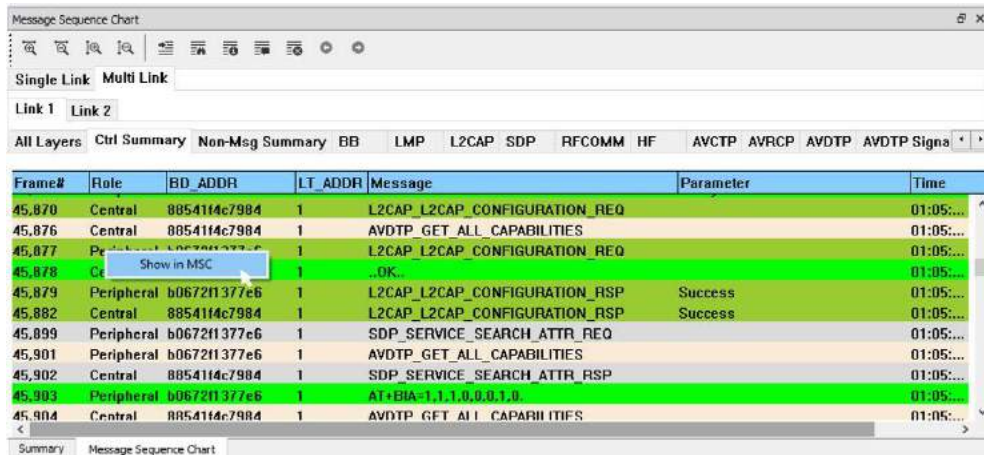


Figure 5.74 - Right-Click in Ctrl Summary to Display Show in MSC

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

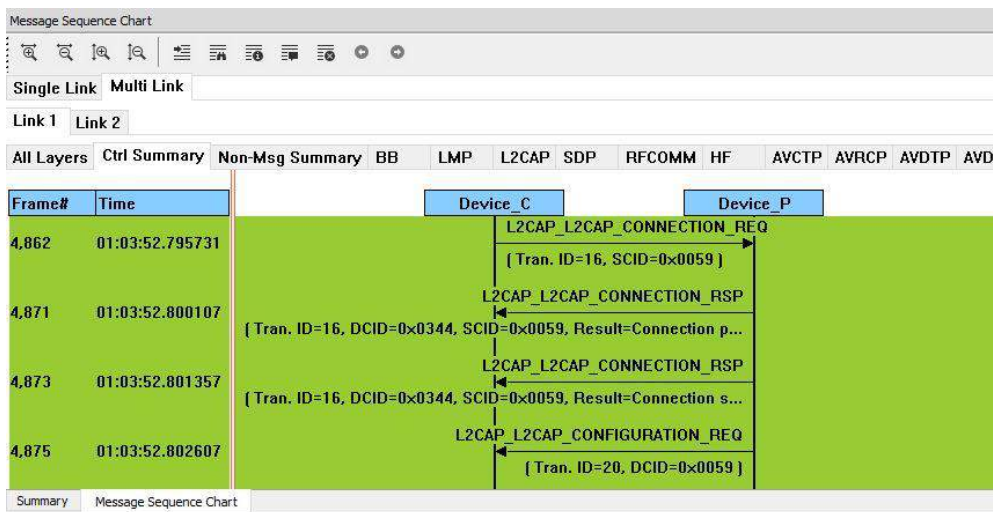


Figure 5.75 - MSC View of Selected Packet from Ctrl Summary

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

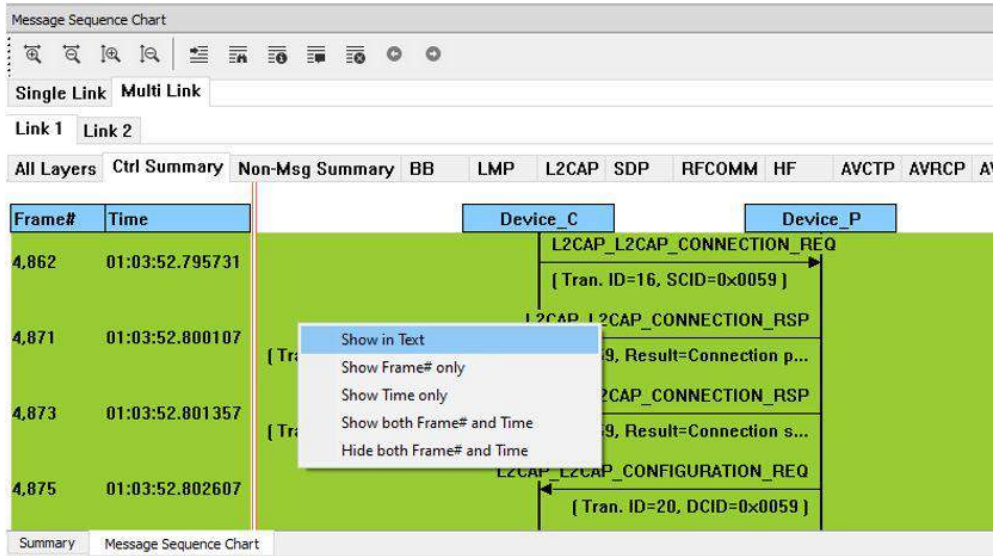


Figure 5.76 - Return to Text View Using Right-Click Menu

You can also choose:

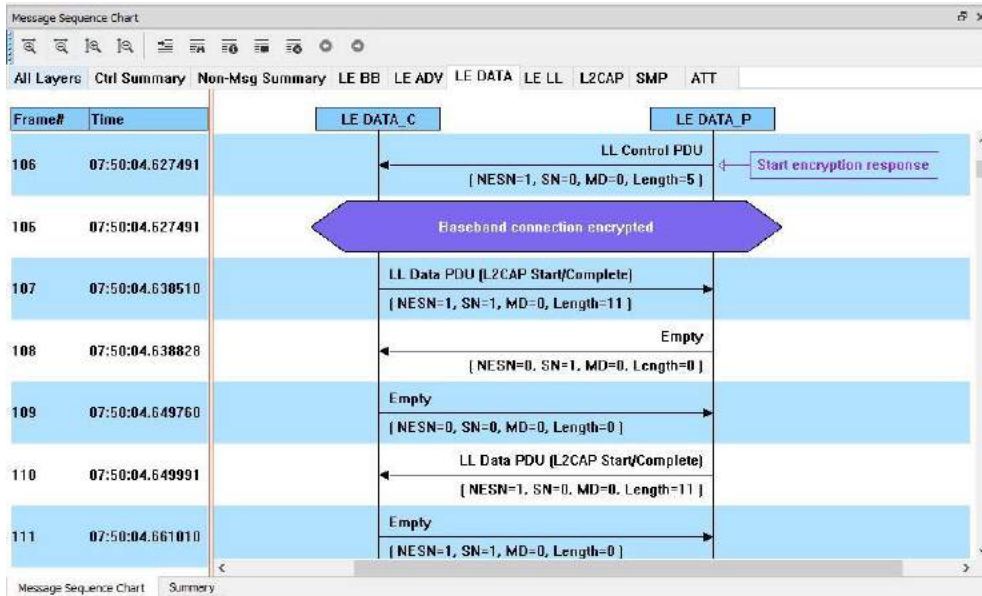


Figure 5.77 - LE DATA Messages

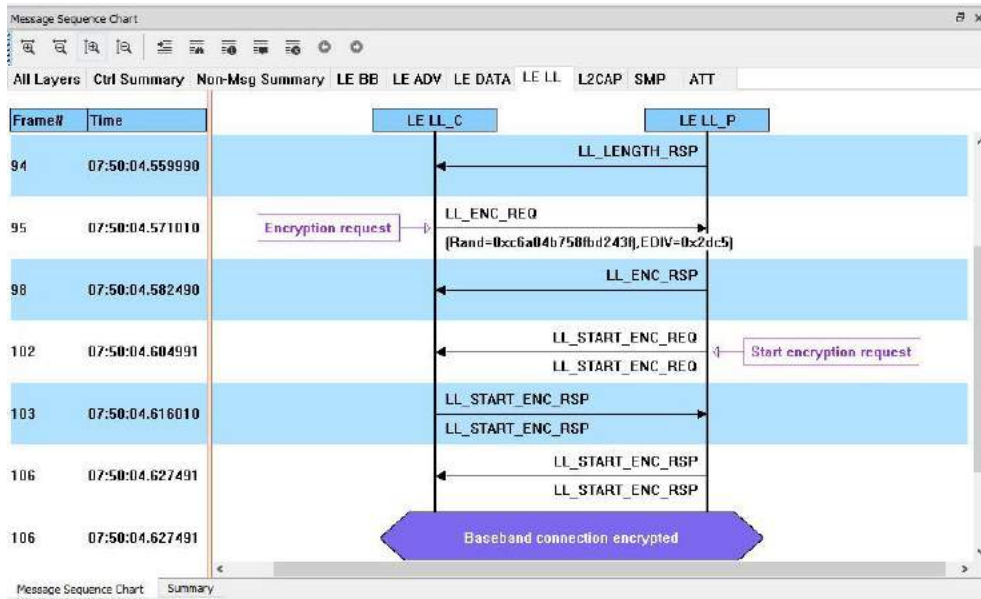


Figure 5.78 - LE LL Message Summary

• L2CAP

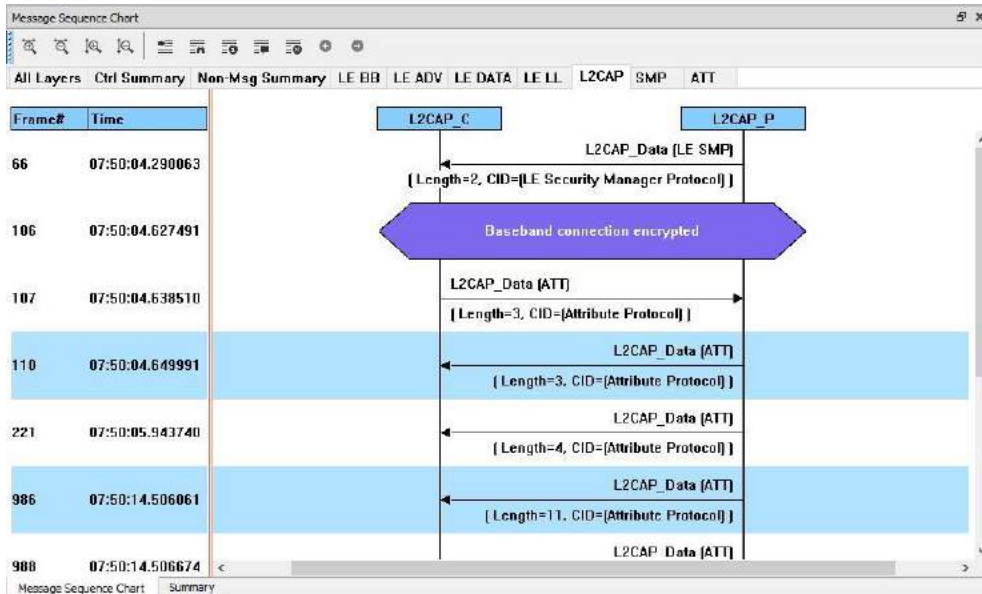


Figure 5.79 - L2 CAP Message Summary

• ATT

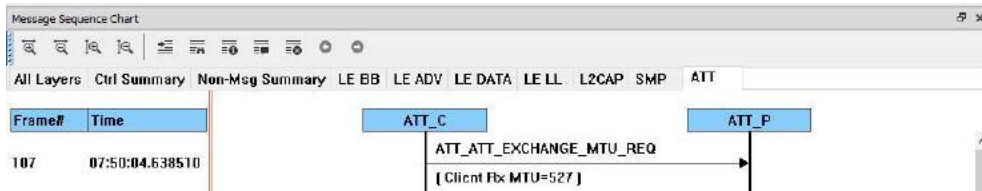


Figure 5.80 - ATT Message Summary

5.4.11.1 Message Sequence Chart Toolbar

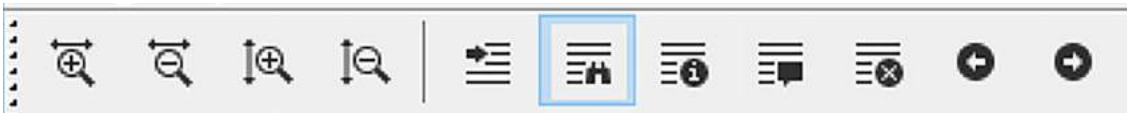











Figure 5.81 - Message Sequence Chart Toolbar

Table 5.6 - Message Sequence Chart Tools


Tool	Keyboard	Description
	Ctrl + H	Zoom in horizontal - expands the chart horizontal view
	Shift + H	Zoom out horizontal - compresses the chart horizontal view

Table 5.6 - Message Sequence Chart Tools (continued)

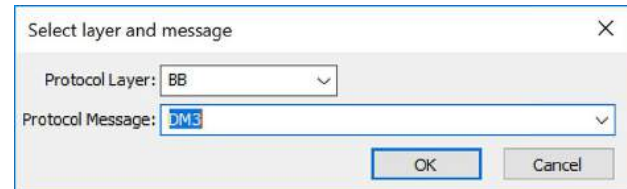
Tool	Keyboard	Description
	Ctrl + V	Zoom in vertical - expands the chart vertical view
	Shift + V	Zoom out vertical - compresses the chart vertical view
	Shift + F	Go to frame
	F3	Search
	Ctrl + I	Go to first information message
	Ctrl + S	Go to first protocol state message
	Ctrl + E	Go to first error frame
	F2	Search for prior using Search criteria.
	F4	Search for Next using Search criteria

### 5.4.11.2 Message Sequence Chart - Search

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

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

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



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

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

2. Or Open the Search dialog using the Search icon or the **F3** key.



3. Select a specific Protocol Message from the drop-down list.
4. Once you select the Protocol Message, click **OK**

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

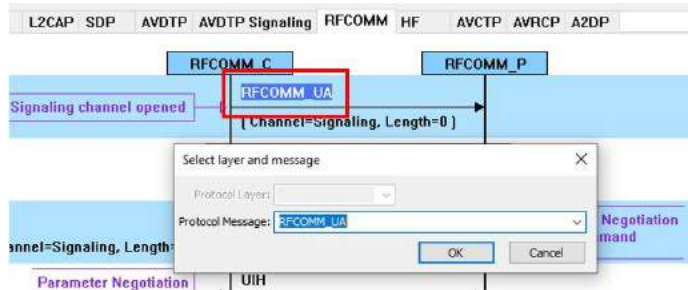


Figure 5.82 - Highlighted First Search Result

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



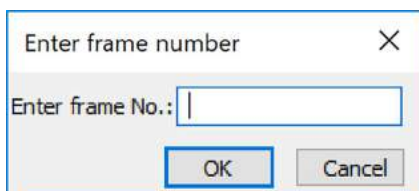
Once you have set the search value, you can 1) use the **Search Previous** and **Search Next** buttons or 2) **F2** and **F4** to move to the next or previous frame in the chart.

### 5.4.11.3 Message Sequence Chart - Go To Frame

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



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

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




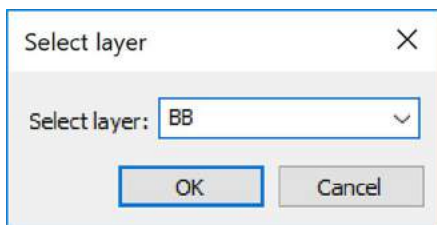
3. Click **OK**.

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

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

#### 5.4.11.4 Message Sequence Chart - First Error Frame

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

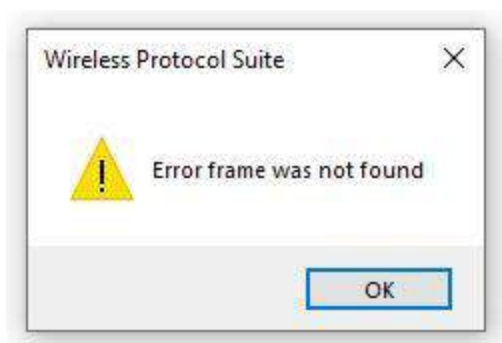


You have to select a layer from the drop down list to choose what layer you want to search for the error.



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.



## 5.5 Bluetooth Protocol Expert System



The *Bluetooth* Protocol Expert System is used to debug protocol-related events for *Bluetooth* protocols. The Expert System provides the ability to interactively select protocol events from a table of events in live capture



mode or in analyzing a previously captured file. The expert system automatically analyzes *Bluetooth* packets to reveal when your implementations is violating protocol (currently A2DP and L2CAP with more coming), and identifies with reference to the relevant entries in the Bluetooth specification, violations of best practices and protocol ambiguities.

Protocol error events appearing in the **Protocol Events** pane identify the related *Bluetooth* specification reference that is likely to point to a solution to the error. The expert system references *Bluetooth* specification 5.0 and the following protocols for both Classic *Bluetooth* and *Bluetooth* Low Energy.

- L2CAP
- A2DP
- SDP
- SMP
- ATT

Selecting an event will dynamically link the related packet selection to the Wireless Protocol Suite software **Main windows, Coexistence View, Message Sequence Chart, Bluetooth Timeline, and Packet Error Rate Statistics (PER Stats)**.

The expert system **Toolbox** includes tools for greater precision and more control over your testing environment. The **A2DP** tool allows the Soderia or Soderia LE units to become a user-controlled sink device. This tool provides a much more accurate depiction of the source device's *Bluetooth* audio score. The **LE** tool is useful for the Soderia or Soderia LE creating random or sequential jammer traffic on all *Bluetooth* channels. This gives the user the ability to see how their device's communications performs on each channel in a very noisy environment.


### 5.5.1 Starting the *Bluetooth* Protocol Expert System


To use the *Bluetooth* Protocol Expert System the user must have Soderia or Soderia LE hardware with *Bluetooth* Protocol Expert System license installed and connected to the PC. This is a requirement for both live capture and when viewing a saved capture file.

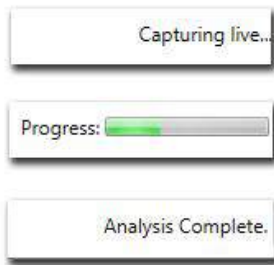
For live capture, set up the Soderia or Soderia LE device datasource and begin capturing data. The Soderia or Soderia LE must be capturing before the expert system can be started.

For viewing a capture file, load the saved file from the **Main windows File** menu.

**Note:** To use the *Bluetooth* Protocol Expert System with a capture file, Soderia or Soderia LE hardware with *Bluetooth* Protocol Expert System license installed must be connected to the PC.

*Bluetooth* Protocol Expert System Window is opened by clicking on  on the **Main windows** toolbar. If the Soderia or Soderia LE hardware is not licensed for *Bluetooth* Protocol Expert System, a tooltip will appear with

"Bluetooth Protocol Expert System is not licensed. Please contact sales@fte.com." Click on the  or select **Bluetooth Protocol Expert** from the **View** menu. The *Bluetooth* Protocol Expert System window will open.



When the protocol analyzer begins analysis of the captured data, the **Bluetooth Protocol Expert System** window status bar (bottom of the window) will show **Capturing live....** The expert system does not get any frames until after the frames are analyzed. When a complete captured frame set is available, the expert system knows the file size so a **Progress** bar appears while the expert system analyzes. The expert system will search and evaluate for protocol events for warnings and errors. When the expert system has completed analyzing frames, the status bar will show **Analysis Complete** indicating that all frames have been analyzed.

If no protocol warnings or errors are detected, the window will remain empty of data.

For instructions on using the expert system Toolbox with the Frontline Soderia, see [Bluetooth Protocol Expert System Toolbox on page 327](#).

## 5.5.2 Bluetooth Protocol Expert System Window


This window is the working space for the *Bluetooth* Protocol Expert System. Upon opening *Bluetooth* Protocol Expert System by clicking on the **Main windows**  button, the window shown below will open with four main areas displayed described in the table below. Detailed explanations of each window section follow.

Table 5.7 - *Bluetooth* Protocol Expert System Window Panes

Section	Description
<a href="#">Connections</a>	Displays the <i>Bluetooth</i> central and central device connections with associated link layer logic transport type.
<a href="#">Statistics</a>	Displays the protocol statistics associated with the warning or error selected in the <b>Protocol Events</b> pane, or associated with the selected <i>Bluetooth</i> address and protocols selected in <b>Connections</b> pane. Tabbed sections contain the statistics for the protocols associated with the analyzed data. Statistics will vary depending on the protocol.
<a href="#">Protocol Events</a>	Displays the <i>Bluetooth</i> protocol warnings and errors. Clicking on an event will select the associated protocol tab in the Statistics pane.
<b>Toolbox</b>	Used for testing audio when using the <i>Bluetooth</i> USB adapter on the HCI USB ports. See <a href="#">Bluetooth Protocol Expert System Toolbox on page 327</a>

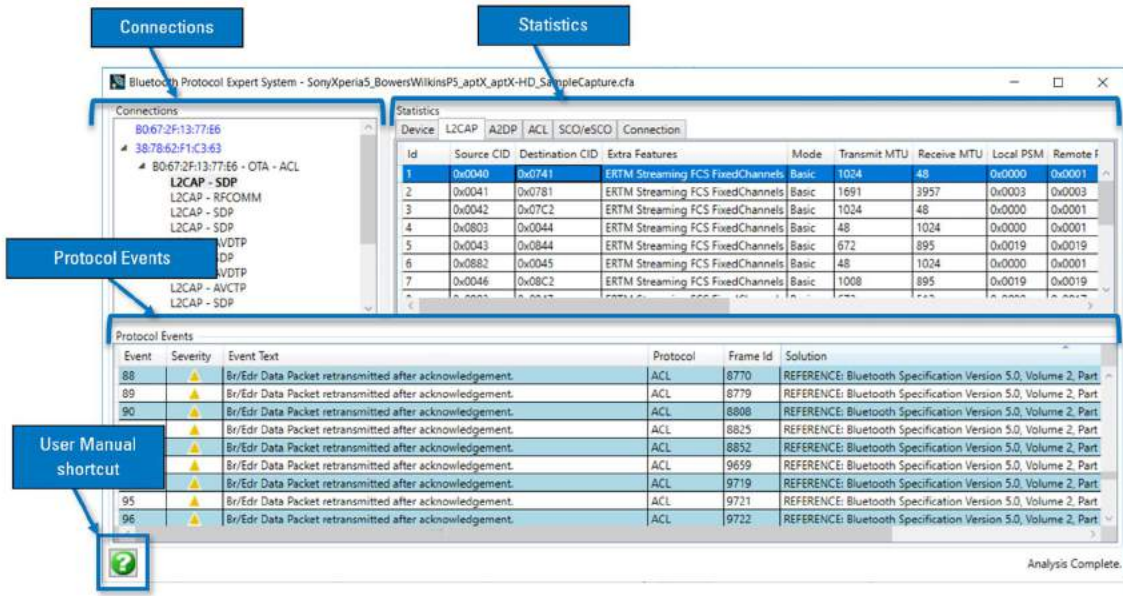


Figure 5.83 - Bluetooth Protocol Expert System Window

### 5.5.2.1 Expert System Connections Pane

The **Connections** pane provides a chart of all the connected devices from the current live recording session or from a loaded capture file that have a protocol error or warning appearing in the **Protocol Events** pane. Devices are identified by their BD\_ADDR. A device address with an arrow symbol will expand to show the connected devices and the link layer logical transport type.

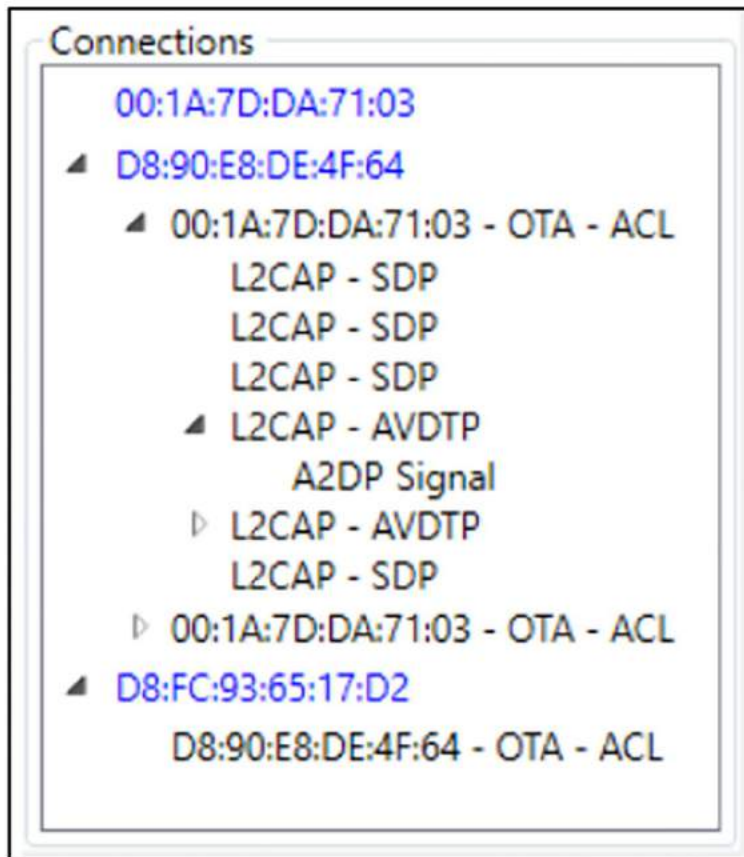


Figure 5.84 - BPES Connections Pane

### 5.5.2.2 Expert System Statistics Pane

The Statistics pane contains detailed information about the links, protocols, and connections associated with frames or range of frames and devices of detected events. The tabs across the top list the links and protocols.

Statistics												
<span>ACL</span> <span>L2CAP</span> <span>A2DP</span> <span>Connection</span> <span>SCO/eSCO</span> <span>Device</span>												
Id	Source CCID	Destination CCID	Extra Features	Mode	Transmit MTU	Receive MTU	Local PSM	Remote PSM	Data Transmitted	Data Received	Transmit Mps	
1	40	0	""	""	668	256	0	0	0	0	0	
2	41	0	""	""	1013	2048	0	0	0	0	0	
3	40	0	""	""	668	256	0	0	0	0	0	
4	40	0	""	""	668	256	0	0	0	0	0	
5	40	0	""	""	668	256	0	0	0	0	0	
6	40	0	""	""	668	256	1	0	0	0	0	
7	40	0	""	""	668	256	1	0	0	0	0	

Figure 5.85 - Bluetooth Protocol Expert System **Statistics** Pane

Table 5.8 - Bluetooth Protocol Expert System Statistics Pane

Tab	Tab Description	Column	Column Description
<b>ACL</b>	An asynchronous (packet switched) connection between devices created on LMP level.	<b>ID</b>	System assigned identifier for ACL connections.
		<b>Device A</b>	Contains the BD_Addr of a device in the connection.
		<b>Device B</b>	Contains the BD_Addr of a device in the connection.
		<b>AddrType</b>	BR_EDR or LE
		<b>Handle</b>	
		<b>Active</b>	
		<b>Errors</b>	

Table 5.8 - Bluetooth Protocol Expert System Statistics Pane (Continued)

Tab	Tab Description	Column	Column Description
<b>L2CAP</b>	L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions.	<b>ID</b>	System assigned identifier for ACL connections
		<b>Source CID</b>	Channel Identifier for the source device.
		<b>Destination CID</b>	Channel Identifier for the destination device.
		<b>Extra Features</b>	
		<b>Mode</b>	
		<b>Transmit MTU</b>	Maximum Transmission Unit in bytes during transmission.
		<b>Receive MTU</b>	Maximum Transmission Unit in bytes during receive.
		<b>Local PSM</b>	Local device Protocol and Service Multiplexer.
		<b>Remote PSM</b>	Remote device Protocol and Service Multiplexer.
		<b>Data Transmitted</b>	
		<b>Data Received</b>	
		<b>Transmit Mps</b>	
		<b>Receive Mps</b>	
		<b>Transmit Window</b>	
		<b>Receive Window</b>	
		<b>Number of Retransmissions</b>	
<b>Active</b>			
<b>Error Count</b>	Number of errors associated with this <b>L2CAP Id.</b>		
<b>A2DP</b>	Advanced Audio Distribution Profile event parameters.		

Table 5.8 - Bluetooth Protocol Expert System Statistics Pane (Continued)

Tab	Tab Description	Column	Column Description
<b>SCO/eSCO</b>	Synchronous Connection-oriented (SCO)/extended SCO.	<b>Id</b>	System assigned identification.
		<b>Type</b>	SCO or eSCO
		<b>Air Mode</b>	Part of the <i>voice_settings</i> parameter in the air mode negotiations designed to improve or optimize audio quality during transmissions.  SCO: CVSD, A-law, $\mu$ -law.  eSCO: CVSD, A-law, $\mu$ -law, transparent.
		<b>Handle</b>	
		<b>Active</b>	
		<b>Error Count</b>	
<b>Device</b>	This tab serves the purpose of assigning a unique expert system identification to the devices listed in the <b>Connections</b> pane.	<b>Id</b>	System assigned identification.
		<b>Address</b>	BD_ADDR of a device found in the <b>Connections</b> pane.

### 5.5.2.3 Expert System Protocol Events Pane

Event	Severity	Event Text	Protocol	Frame Id	Solution	Time
1	●	Unable to negotiate L2CAP lir	L2CAP	1383	REFERENCE: Bluetooth Specification Version 5.0, Volume 3,	May-29-2015 01:46:13.043601 PM
2	●	Unable to negotiate L2CAP lir	L2CAP	1521	REFERENCE: Bluetooth Specification Version 5.0, Volume 3,	May-29-2015 01:46:14.484855 PM
3	●	Unable to negotiate L2CAP lir	L2CAP	1561	REFERENCE: Bluetooth Specification Version 5.0, Volume 3,	May-29-2015 01:46:14.973606 PM
4	●	Unable to negotiate L2CAP lir	L2CAP	1621	REFERENCE: Bluetooth Specification Version 5.0, Volume 3,	May-29-2015 01:46:16.493610 PM
5	●	Invalid SCO connection paran		11207	REFERENCE: Bluetooth Specification Version 4.1, Volume 2,	May-29-2015 01:47:40.391315 PM

Figure 5.86 - Protocol Events Pane

Bluetooth protocol events that generate a warning or an error in the expert system are listed in the **Protocol Events** pane. Events are listed in the order that they occur.

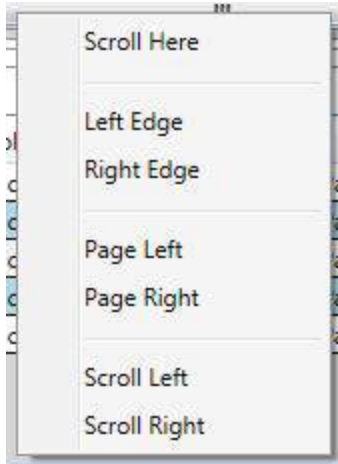
Table 5.9 - Protocol Events Pane Fields

Row Field	Description
<b>Event</b>	System assigned event number. Events are numbered in the order that they appear.

Table 5.9 - Protocol Events Pane Fields (Continued)

Row Field	Description
<b>Severity</b>	<p>▲ = Warning. The event has not created a failure, but should receive some attention and further investigation..</p> <p>● = Error. The event has identified a situation that does not conform to the <i>Bluetooth</i> specification. Corrective action is required.</p>
<b>Event Text</b>	Event description.
<b>Protocol</b>	Protocol in which the event occurred.
<b>Frame Id</b>	Frame where the event occurred. Clicking in the event row will select the related <b>Statistics</b> pane protocol tab and protocol <b>Id</b> . The corresponding frame is selected in the <b>Main windows, Event Display, Message Sequence Chart, Coexistence View, and Bluetooth Timeline or Bluetooth Low Energy Timeline</b> .
<b>Solution</b>	A solution to the event is provided by reference to the Bluetooth specification that applies to the Event Text content.
<b>Time</b>	Event timestamp.

### 5.5.2.4 Expert System Window Scroll Bar Navigation



Some tabs in the Statistics pane display a horizontal scroll bar that can be clicked and dragged to view the tab columns. An alternative scroll navigation is to right-click the mouse cursor on the scroll bar. A navigation menu will appear, and you click on the direction and amount of scrolling to move the horizontal scroll bar in discrete steps.

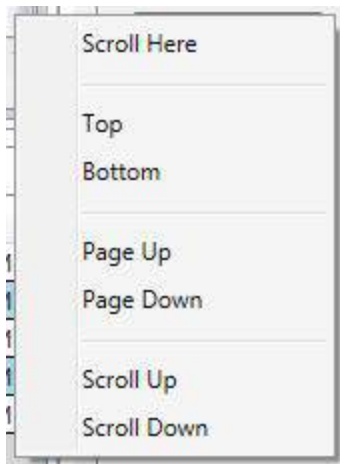
Table 5.10 - Horizontal Scroll Bar Navigation Sections

Selection	Description
Scroll Here	Scrolls to the point on the scroll pane where the mouse was last positioned.
Left/Right Edge	Scrolls the table to the beginning (left edge) or to the end (right edge)



Table 5.10 - Horizontal Scroll Bar Navigation Sections (Continued)

Selection	Description
Page Left/Right	Left: Moves the current right edge to the left edge of the current view range.  Right: Moves the current left edge to the right edge of the current view range.
Scroll Left/Right	Moves the table is small increment to the left or right. Same action as the left/right scroll arrows at the ends of the scroll bar.



Some tabs in the Statistics pane display a vertical scroll bar that can be clicked and dragged to view the tab columns. An alternative scroll navigation is to right-click the mouse cursor on the vertical scroll bar. A navigation menu will appear, and you click on the direction and amount of scrolling to move the scroll bar vertically in discrete steps.

Table 5.11 - Vertical Scroll Bar Navigation Sections

Selection	Description
Scroll Here	Scrolls to the point on the scroll pane where the mouse was last positioned.
Top/Bottom	Scrolls the table to the first row (top) or to the last row (bottom)
Page Up/Down	Up: moves the current view bottom row to the top row of the current view range.  Down: Moves the current view top row to the bottom row of the current view range.
Scroll Up/Down	Moves the table one row up or down.

### 5.5.2.5 Expert System Table Sorting

Tables in the Bluetooth Protocol Expert System can be sorted in ascending or descending order. This process includes tables in the **Statistics** pane and the **Protocol Events** pane.

1. In any table click in the header for the column you want to sort. The column header will turn blue and an arrow head will appear.
2. If the arrow head is pointing up, the column is sorted in ascending order. If the arrow head is pointing down the column is sorted in descending order.
3. To change the direction of the sort, click in the column header to change the arrow head direction accordingly.

All other columns in the table are sorted relative to the selected column sort. Refer to the following Statistics pane images for an example.

Id	Type	Air Mode	Handle	Active	Error Count
1	eSCO	Transparent	1	False	0
2	SCO	CVSD	1	False	0
3	eSCO	Transparent	1	False	0
4	SCO	CVSD	1	False	0

Figure 5.87 - Sorting **Id** Ascending

Id	Type	Air Mode	Handle	Active	Error Count
4	SCO	CVSD	1	False	0
2	SCO	CVSD	1	False	0
1	eSCO	Transparent	1	False	0
3	eSCO	Transparent	1	False	0

Figure 5.88 - Sorting **Air Mode** Ascending; Note **Id** Sort

Id	Type	Air Mode	Handle	Active	Error Count
3	eSCO	Transparent	1	False	0
1	eSCO	Transparent	1	False	0
4	SCO	CVSD	1	False	0
2	SCO	CVSD	1	False	0

Figure 5.89 - Sorting **Air Mode** Descending; Note how other columns follow.

### 5.5.3 Bluetooth Protocol Expert System Toolbox

The Bluetooth Protocol Expert System includes Toolbox that includes the ability to emulate an A2DP sink device and the ability to generate and inject Low Energy packets directly into in the 2.4 GHz spectrum.

The USB adapter that is provided with your protocol expert system license is a generic Bluetooth radio. This adapter is inserted into:

- Sodera: one of the HCI USB connectors on the rear panel (See [Rear Panel Connectors on page 42.](#)), or a USB port on the host PC.
- Sodera le: a USB port on the host PC.

#### A2DP Sink

The A2DP sink functionality dramatically simplifies the troubleshooting A2DP source devices by providing engineers fine grain control of an emulated A2DP sink device. Once Toolbox A2DP is running, the user can connect to the *Bluetooth* address displayed at the top of the toolbox or by scanning for 'Frontline Test Device' friendly name.

Toolbox A2DP does not render the audio stream it receives. If the protocol stream generated by Toolbox A2DP is being captured with the OTA or HCI sniffer, audio can be extracted or analyzed via the [Bluetooth Audio Expert System™ on page 336.](#)

#### LE Jammer/Packet Generator

The Low Energy jammer or packet generation functionality provides engineers the means to test devices in a “noisy” environment by generating packets or “noise”, forcing the device under test to accommodate and adjust as it would in the real world.

### 5.5.3.1 Toolbox Hardware Setup

#### Set up the Sodera unit to use the Toolbox:

Required equipment:

- Provided Teledyne LeCroy Bluetooth USB adapter.
- USB cable with Type A and Type B connectors.
- Host PC with 2 USB ports.

Follow these steps to prepare for using the Toolbox

1. Connect the *Bluetooth* USB adapter to the Sodera **HCI USB1** or **USB2** connector group (See [Rear Panel Connectors on page 42.](#)). Each HCI USB connector group has two ports with a USB Type A and USB Type B connector. The Bluetooth USB adapter is "keyed" to the Sodera unit.
2. Insert the provided Bluetooth adapter into the **HCI USB** group Type A connector.
3. Connect a USB cable from the same **HCI USB** group Type B connector and other end to the host PC USB connector. .

**Note:** The adapter must be inserted prior to using the **A2DP** tool or the **LE** tool.

The Sodera hardware must also be connected to the PC Host connector via an additional USB connector, since the Bluetooth Protocol Expert System is licensed for a specific Sodera hardware unit.

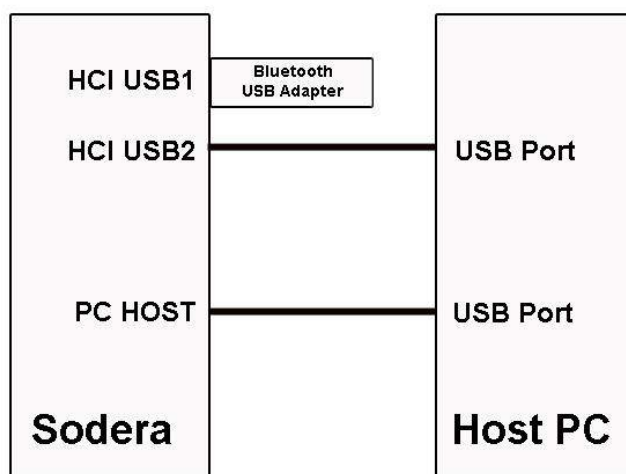


Figure 5.90 - Sodera Toolbox USB Adapter Test Setup.

It is not necessary to connect the *Bluetooth* USB adapter to the Sodera unit. Alternatively, the USB adapter may be connected directly to a Host PC USB port. However, an advantage to using the **HCI USB** connectors is the ability of the Sodera unit to HCI capture of the Toolbox sessions.

### Set up the Sodera LE unit to use the Toolbox:

Required equipment:

- Provided Teledyne LeCroy Bluetooth USB adapter.
- Host PC with 2 USB ports.

Follow these steps to prepare for using the Toolbox

1. Connect the *Bluetooth* USB adapter to a Host PC USB port.

**Note:** The adapter must be inserted prior to using the **A2DP** tool or the **LE** tool.

The Soderale hardware must also be connected to the PC Host connector via an additional USB connector, since the Bluetooth Protocol Expert System is licensed for a specific Soderale hardware unit.

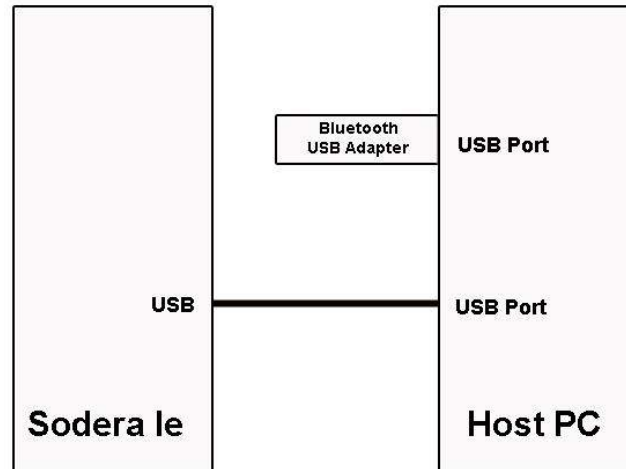
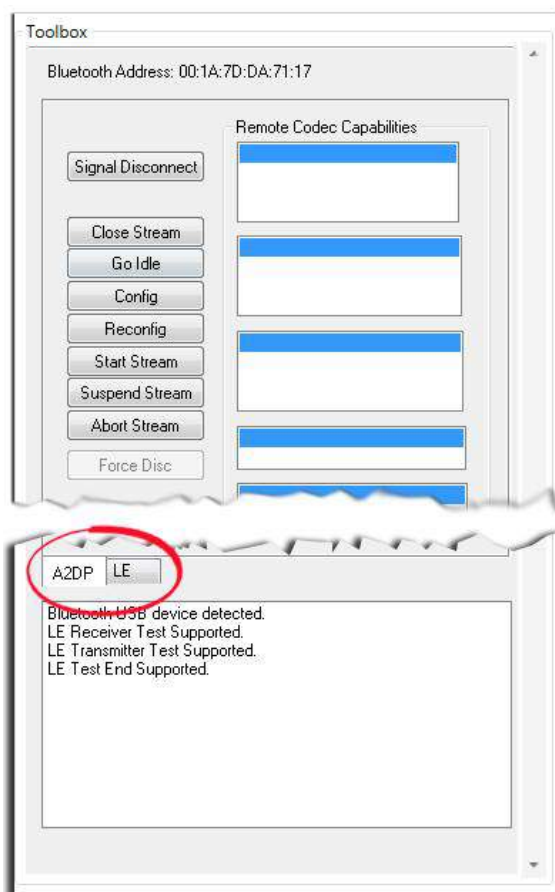


Figure 5.91 - Soderale Toolbox USB Adapter Test Setup.

### 5.5.3.2 Toolbox Pane



The Bluetooth Protocol Expert System Test Tools pane has two tabs: **A2DP** and **LE**. Each tab has a unique set of controls. The following topics describe the controls and displays for each tab selection.

At the top of the Toolbox pane is a **Bluetooth Address**. This is the BD\_ADDR of the provided Bluetooth USB Adapter. When connecting a source device this is the address to which the source is linked.

#### 5.5.3.2.1 A2DP Tool

The A2DP tool uses the Sodera or Sodera LE unit to simulate a sink device in a *Bluetooth* connection, which makes the Sodera or Sodera LE unit an integral party in the link instead of operating as a third-party sniffing the over-the-air traffic. When the provided *Bluetooth* USB adapter is inserted into one of the Sodera HCI USB connectors or the a Host PC USB port and the A2DP tool is running, the user can connect to the *Bluetooth* address displayed at the top of the Toolbox or by scanning for 'Frontline Test Device' friendly name.

The Sodera or Sodera LE must be recording to capture the stream over the A2DP tool.

Bluetooth Address: 5C:F3:70:67:D3:1B

Signal Disconnect

Close Stream

Go Idle

Config

Reconfig

Start Stream

Suspend Stream

Abort Stream

Force Disc

Remote Codec Capabilities

48000 HZ

44100 HZ

32000 HZ

16000 HZ

JOINT STEREO

STEREO

DUAL CHANNEL

MONO

16 BLOCKS

12 BLOCKS

8 BLOCKS

4 BLOCKS

8 SUBBANDS

4 SUBBANDS

LOUDNESS

SNR

Stream	In Use	Media Type	Stream Type
0	TRUE	AUDIO	SINK

Registered Stream Capabilities

Codec: SBC

Configured Content Protection

Stream Status

Source:	Closed	0 Kbps	0 Khz
Sink:	Open	0 Kbps	0 Khz

A2DP LE

```

Stream Open
Delay (Source) = 0 ms
InterArrivalTime = 5 ms
A2DP_SetBrEdrFlowSpec() returned Success.
Stream Start Indication
A2DP_StartStreamRsp() returned Pending.
Stream Started
Stream Suspended
Stream Start Indication
A2DP_StartStreamRsp() returned Pending.
Stream Started
Stream Suspended
    
```

## A2DP Tool Pane, top half

**Remote Codec Capabilities**

These series of lists, on the right top half of the A2DP tool, are used to display the codec capabilities reported to the remote A2DP source when it performs stream discovery. The lists are selectable to allow the user to choose a codec configuration when configuring an AVDTP stream.

Remote Code Capabilities text boxes are only populated after the provided Bluetooth USB adapter has been inserted into one of the HCI USB connectors or a Host PC USB port and a link with the remote source has been established.

To configure the remote source capabilities, click on the desired capability in each list.

**Function buttons**

The Function buttons, on the left top half of the A2DP tool, allow the user to control how the A2DP sink uses AVDTP to interact with the A2DP Source.

Table 5.12 - A2DP Tool Function Buttons

Function Button	Description
<b>Signal Disconnect</b>	Disconnects the AVDTP signaling L2CAP channel. Useful for stress testing to verify A2DP source implementations correctly handle spontaneous disconnection of the signal channel.
<b>Close Stream</b>	Sends a CLOSE AVDTP command and if accepted terminates the AVDTP connection.
<b>Go Idle</b>	Places the stream in an idle state. If actively streaming, suspends the stream and prepares the stream for configuration.
<b>Config</b>	Sends an AVDTP SET_CONFIGURATION command using the CODEC parameters selected from 'Remote Codec Capabilities'
<b>Reconfig</b>	Sends an AVDTP RECONFIGURE command using the CODEC parameters selected from 'Remote Codec Capabilities'
<b>Start Stream</b>	Sends an AVDTP START command.
<b>Suspend Stream</b>	Sends an AVDTP SUSPEND command
<b>Abort Stream</b>	Sends and AVDTP ABORT command.
<b>Force Disc</b>	Forcibly disconnects the ACL without disconnecting AVDTP first. Useful for stress testing error handling.



**Local Streams**

Displays the streams supported by the A2DP Tool. Currently, only a single audio stream is supported. More streams will be added in the future.

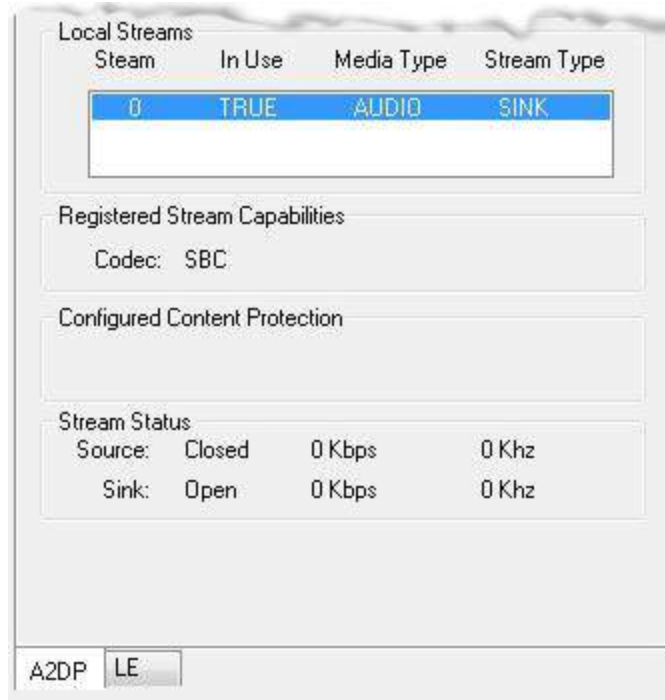


Figure 5.92 - A2DP Tool Pane, bottom half

**Registered Stream Capabilities**

Displays the current codec capabilities supported by the A2DP tool. Currently, only SBC audio is supported.

**Configured Content Protection**

Displays the type of content protection being used by the active stream.

**Stream Status**

Statistics for the current stream that include stream state, throughput, and sampling frequency.

**5.5.3.2.2 LE Tool**

The LE tool provides the user with the ability to generate and inject Low Energy packets directly into in the 2.4 GHz spectrum. The Toolbox LE tab is used to configure the LE tool for Low Energy channel, packet patterns, and pattern burst parameters.

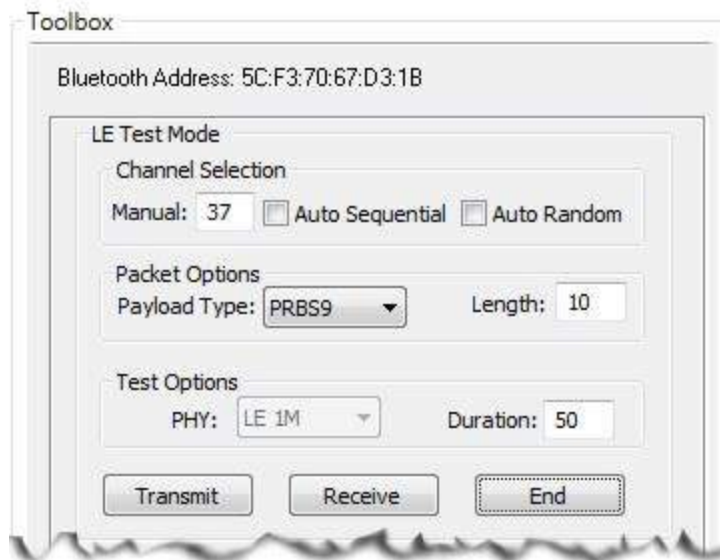


Figure 5.93 - LE Tool Pane, example

LE Tool Test Mode Options

Category	Option	Description
Channel Selection	Manual	Select a single channel 0-39. Not active when <b>Auto Sequential</b> and <b>Auto Random</b> are selected.
	Auto Sequential	Channels 0 - 39 are sequentially transmitted.
	Auto Random	Channels withing the range of 0 - 39 are transmitted in groups of three . The next sequence of three is randomly transmitted. For example, channels 5,6,7 then channels 34,35,36 then channels 12,13,14, and so forth.
Packet Options	Payload Type	Select a sequence from the drop-down list: <ul style="list-style-type: none"> <li>• Pseudo-random bit sequence 9</li> <li>• Pattern of alternating bits '11110000'</li> <li>• Pattern of alternating bits '10101010'</li> <li>• Pseudo-random bit sequence 15</li> <li>• Pattern of all '1' bits</li> <li>• Pattern of all '0' bits</li> <li>• Pattern of alternating bits '00001111'</li> <li>• Pattern of alternating bits '0101'</li> </ul>

LE Tool Test Mode Options (continued)

Category	Option	Description
	Length	Number of bytes to send in the burst.
Test Options	PHY	Available only for Bluetooth 5.0 and later, LE 1M - 1 Mbps data rate LE 2M - 2 Mbps data rate
	Duration	The wait time in milliseconds between each burst of data.
Transmit	Pressing this button triggers the LE tool to start transmitting test packets as configured. When in Auto Sequential or Auto Random modes, the LE tool continues to transmit until the end button is pressed.	
Receive	Using this function instructs the LE tool to monitor receiving test packets. Packets are received only on one channels set in the Channel Selection Manual mode.  The LE tool does not render the packets received. To view the packets, use the <b>Main windows</b> .	
End	Stops the Transmit mode.	

### Steps to transmit LE test data

Follow these steps to transmit on one channel when using a Bluetooth 4.0 USB adapter.

1. Enter the transmit channel in the text box next to **Channel Selection Manual**.
2. Select the **Packet Options Payload Type**.
3. In the **Packet Options Length** text box enter the burst length in bytes.
4. In the **Test Options Duration** text box the enter the wait time between bursts in milliseconds.
5. Click on the **Transmit** button.

The LE tool will transmit the selected payload for the selected number of bytes with a selected wait time between the bursts.

Follow these steps to broadcast simulated noise on random channels when using a Bluetooth 4.0 USB adapter.

1. Select **Channel Selection Auto Random**.
2. Select the **Packet Options Payload Type PRBS9** (pseudo-random bit sequence 9).
3. In the **Packet Options Length** text box enter the burst length in bytes.
4. In the **Test Options Duration** text box the enter the wait time between bursts in milliseconds.
5. Click on the **Transmit** button. The LE tool will continuously transmit the pseudo-random bit sequence over groups of three sequential channels for the selected burst length with the selected wait time between the bursts.
6. To end the transmission click on the **End** button.

## Capturing LE tools transmissions

You can use the Sodera or Sodera LE to capture the LE tools transmissions, however you must use the Sodera **Options** menu to select the **LE Test Mode Filters....** After Recording the data transmissions, select **LE Test Mode Filters...** and click on **Select All**. Then click on the **Analyze** button. In the **Main windows** the **LE Test Mode Filters** tab will contain the captured LE tool transmissions. For additional information see [LE Test Mode Channel Selection dialog on page 87](#).

## 5.6 Bluetooth Audio Expert System™

The *Bluetooth* Audio Expert System™ monitors and analyzes *Bluetooth* audio streams with the purpose of detecting and reporting audio impairments. The primary goal of the Audio Expert System™ is to expedite the detection and resolution of *Bluetooth* protocol related audio impairments. To achieve this, the system automatically identifies audio impairments and reports them to a user as “events”. It also correlates the audio events with any detected codec or *Bluetooth* protocol anomalies (events). The system allows a user to view the audio waveform, audio events, codec events, and *Bluetooth* protocol events on a time-aligned display.

An Audio Expert System™ event identifies to the user information, warnings, and errors. Event categories are shown in the following table.

Table 5.13 - Audio Expert System™ General Events

Event Category	General Events Reported
<i>Bluetooth</i> Protocol	Protocol violations
	Best practice violations
Codec	Configuration changes
	errors
Audio	impairments (errors)
	information data

When the Frontline software captures data, if there is audio content that must be debugged this data must be systematically examined when looking for the problem source. The effort to identify and correlate the audio related data can be daunting because the problem source may be caused by protocol, codec, or the audio itself. Using the Audio Expert System™ identifies events that are likely candidates for audio root cause analysis. The expert system examines all captured frames—in live capture or in capture file viewer—and selects audio-related protocol, codec, and audio events. The events are time correlated to the audio stream and identified with specific frames. In general, a cluster of events suggests an area for investigation, and in the presence of multiple event clusters the cluster with the most events suggests the best starting point.

The expert system works in conjunction with Frontline software that is operating in live capture mode or in capture file viewer mode. Selecting an event in the Audio Expert System™ will simultaneously highlight related packets in the Frontline software **Main windows**, **Coexistence View**, **Message Sequence Chart**, **Bluetooth Timeline**, and **Packet Error Rate Statistics (PER Stats)** windows.

## 5.6.1 Supported Codec Parameters

Table 5.14 - Timing Analysis Supported Codec Parameters

Codec	Sample Frequency	Channel Modes	Data Rate	Other Information
SBC	16 kHz*, 32 kHz*, 44.1 kHz, 48 kHz	Mono, Dual, Stereo, Joint Stereo		Block Length: 4, 8, 12, 16 Number of subbands: 4, 8 Allocation Method: SNR, Loudness Minimum Bitpool Value: 2 Maximum Bitpool Value: 53
CVSD	8 kHz	Mono	64 kbps	
mSBC	16 kHz	Mono		Allocation method: Loudness Subbands: 8 Block Length: 15 Bitpool: 26
G.711	8 kHz	Mono	64 kbps	
G.726	8 kHz	Mono	32 kbps	
G.722 (ASHA)	8 kHz , 16 kHz	Mono	48 kbps, 64 kbps	
MPEG-4 AAC LC	44.1 KHz, 48 KHz, 8 KHz*, 11.025 KHz*, 12 KHz*, 16 KHz*, 22.050 KHz*, 24 KHz*, 32 KHz*, 64 KHz*, 88.2 KHz*, 96 KHz*	Mono, Dual		Variable Bit Rate and Specified Bit rate
AAC-ELD	16 kHz, 24 kHz	Mono	32 kbps, 44.8 kbps, 48 kbps, 64 kbps	
LDAC	44.1 kHz, 48 kHz, 88.2 kHz, 96 kHz	Mono, Dual, Stereo	Up to 990 kbps	Sample Resolutions: 24 bits, 32 bits
aptX-Classic and LL	44.1kHz	Stereo	352 kbps	Sample Resolution: 16-bit both content protected and non-content protected
aptX-HD	44.1 kHz, 48 kHz	Stereo	576 kbps	Sample Resolution: 24-bit
LC3	8 kHz, 16 kHz, 24 kHz, 32 kHz, 44.1 kHz, 48 kHz	Mono		Frame Durations: 7.5 ms, 10 ms
GN ReSound 'Heimdall'	16 kHz	Mono	48 kbps, 64 kbps	
LC3-SWB	32 kHz	Mono	61867 bits/s	Frame Duration: 7.5 ms

\* Audio Analysis not supported, though you are able to play back the audio live.

## 5.6.2 Operating Modes

The *Bluetooth* audio analysis can be accomplished in two modes: 1) unreferenced mode, and 2) referenced mode.

Table 5.15 - Audio Expert System Operating Modes

Mode	Description
Non-referenced	Processing audio of completely unknown program content (e.g. arbitrary music or speech content). Since the system does not have any prior knowledge of the audio being analyzed, the types of audio analysis that can be performed is limited.
Referenced	A “pseudo closed loop” test scenario where the user plays specific Reference Audio files (pre-recorded audio test files provided by Frontline) on the Source DUT (Device Under test). The analysis of the received audio results in a series of “Audio Events” being reported by comparing changes in the received audio to expected changes of the Reference Audio, and reporting deviation events when they occur.

Reference mode detects a larger number of events because the reference audio has specific frequency, amplitude, and duration occurring at known points in time allowing for precise comparison.

### 5.6.2.1 Non-Referenced Mode

In Non-Referenced Mode, the system is typically processing audio of completely unknown program content (e.g. arbitrary music or speech content). Since the system does not have any prior knowledge of the audio being analyzed, the types of audio analysis that can be performed is limited.

The following events are reported whenever the system is operating in Non-Reference mode. These are the meaningful audio analysis that the system can perform without reporting too many false positive results.

- Volume Level (Low Volume or High Volume): Reported if the average volume level is not in a range conducive to performing meaningful audio analysis.
- Clipping: Amplitude distortion due to a signal amplitude exceeding the maximum value that can be represented by the digital system
- Dropout: Abrupt and very short duration intervals of silence
- Glitch: Extremely large sample-to-sample audio amplitude transitions that have little probability of occurring within natural speech or music

### 5.6.2.2 Referenced Mode

In Referenced Mode, the system operates in a “pseudo closed loop” test scenario where the user plays a specific Reference Audio file on the Source DUT. The Source DUT negotiates with the Sink DUT to determine the appropriate codec and audio parameters to use and will then process the Reference Audio file accordingly before transmitting the resulting audio via *Bluetooth*. The Reference Audio is a pre-recorded audio test file provided in the Wireless Protocol Suite software installer.

The Sink DUT receives the encoded audio, decodes it, and processes it for playback. In parallel, the Frontline analyzer unit snoops the over-the-air signal between the Source DUT and Sink DUT and emulates the RF reception and decoding done inside the Sink DUT. The Audio Expert System™ automatically detects that a Reference Audio file is being received and then analyzes the resulting audio for deviations from expected parameters.

Referenced Audio files are protocol specific.

The following events are reported whenever the system is operating in the Referenced mode.

- Test ID Found
- Test Script Not Found
- Invalid Test Script
- Synchronization Lost
- Unexpected Frequency
- Unexpected Level
- Unexpected Duration
- Amplitude Fluctuation
- Unexpected Phase Change
- Clipping
- Excess Noise
- CVSD HF Level Too High
- End of Test

### Reference Audio Test Files

The Reference Audio files are specific audio files that exercise the system so that audio impairments can more efficiently and accurately be identified and reported. The Reference Audio files are composed of a series of back-to-back and relatively short duration tones of changing amplitude, frequency, and duration.

The test files are stored on the users computer In the directory "\\Frontline <version #>\Development Tools\Audio Expert Test Files\". For example,

Test\_1.03\_48kHz\_16Bit\_3Loops\_2Ch.wav

**Note:** Reference test files are periodically updated. Shown here is an example. Files delivered with your latest Wireless Protocol Suite software version may have changed. Contact Frontline Technical Support for information on the latest reference file versions.

The test files have a set of tones forming a unique Test ID that lets the analyzer know that it is capturing a test file instead of an arbitrary audio stream. There is no need for special configuration of the analyzer. The Test ID will have the identifier notation N.vv, where N = the file number and vv = a two digit version, for example 1.02.

### Using the Test Files

The analysis of the received audio results in a series of Audio Events being reported by comparing changes in the received audio to expected changes of the Reference Audio, and reporting deviation events when they occur.

The system starts up in Non-Referenced mode, and is continuously looking for a valid Reference Audio file by measuring frequency and amplitude of the received over-the-air audio. Transitioning to Referenced mode requires the successful detection of a Test ID tone sequence of proper frequency, duration, and value.

Once the Referenced Mode state is achieved, the expectation is that all tones encountered will conform to the script identified by the Collected Digits (the "Test ID"). The system remains in the Referenced Mode state until either the end of test is reached, or a loss of synchronization occurs.

The synchronization of the received audio (from the Reference Audio files) versus the internal Test Script is achieved based on changes in frequency of the tones in the Reference Audio file. Frequency changes are used because this parameter is relatively immune to the configuration of the network.

For a comparison of reference mode detectable problems to unreferenced detectable problems see the table in [the audio event type table](#).

### The Test Script

The Reference Audio used for Referenced Mode testing is generated from scripts that define a series of audio segments. Each segment provides an audio tone parameters including frequency, amplitude, duration, fade in and fade out durations, and start time. The script is an XML file delivered with the Wireless Protocol Suite software. This file is used during Referenced mode testing for comparison to the "sniffed" Reference Audio parameters of frequency, amplitude, duration, etc.

Below is a sample script table and the resulting sample Reference Audio .wav file. The generated .wav file begins with a Test ID that is used to identify the "sniffed" audio as a Reference Audio file, and the Audio Expert System™ automatically switches from Non-Referenced mode to Referenced mode.

```
<?xml version="1.0" encoding="UTF-8"?>
- <SegmentArray>
  - <Segment>
    <SegID>0</SegID>
    <Opcode>F</Opcode>
    <Frequency>100</Frequency>
    <Level>-95</Level>
    <Cycles>10</Cycles>
    <Duration>0.1</Duration>
    <FadeIn>0</FadeIn>
    <FadeOut>0</FadeOut>
    <StartTime>0</StartTime>
  </Segment>
  - <Segment>
    <SegID>1</SegID>
    <Opcode>F</Opcode>
    <Frequency>210</Frequency>
    <Level>-3</Level>
    <Cycles>21</Cycles>
    <Duration>0.1</Duration>
    <FadeIn>0</FadeIn>
    <FadeOut>0</FadeOut>
    <StartTime>0.1</StartTime>
  </Segment>
  - <Segment>
    <SegID>2</SegID>
    <Opcode>F</Opcode>
```

Table 5.16 - Sample Test Script Table

Segment	OpCode	Frequency	Level	Cycles	Duration	Fade in	Fade Out	Start Time
1	F	200	0	5	0.025	0	0	0.000
2	F	1000	0	25	0.025	0	0	0.025
3	F	300	-12	15	0.050	0	0	0.050
4	F	600	0	30	0.050	0	0	0.100
5	F+	880	-6	44	0.050	0	0	0.150
6	F+	240	-6	12	0.050	0	0	0.150
7	F	600	-95	30	0.050	0	0	0.200
8	F	600	0	30	0.050	0	10	0.200



### 5.6.2.3 Referenced Mode Testing Processes

In the Referenced mode, the devices under test use a specific audio file (called reference file or test file) provided by Frontline whose contents are already known to the Wireless Protocol Suite software. The software compares the parameters of the received audio data against its parameters and presents analysis for the user. Commonly, in Bluetooth technology the music sent via A2DP and speech sent via HFP. There are a few ways users can conduct referenced mode testing depending upon what profile they are using. The figure 17 shows the source of the audio and the medium through which it can be accessed by Source device to send to sink device via Bluetooth.

Table 5.17 - Referenced Mode Testing Process Between Two DUTs

Audio Source	Process to Send Using A2DP	Process to Send Using HFP
A file stored on the device's local memory	Play the locally stored file on the audio source device	Play using the third party App that transmits music data on HFP.
Streaming audio over a cellular network	Play the test in a browser on the audio source device <a href="https://youtu.be/rmirDbikrtM">https://youtu.be/rmirDbikrtM</a>	Make a call to 434-964-1407 or 434-964-1304 through a cellular network. The phone number receiving the call playbacks recorded test signal.
Streaming audio over a Wi-Fi network	Play the test in a browser on the audio source device <a href="https://youtu.be/rmirDbikrtM">https://youtu.be/rmirDbikrtM</a>	Make a call to 434-964-1407 or 434-964-1304 through a VoIP provider such as Skype. The phone number receiving the call playbacks recorded test signal.  <b>Potential problem:</b> The VoIP provider might use custom codecs and cause undesirable behavior.

#### A2DP

##### Playing the test file locally

The simplest way to perform music data testing is to directly play the reference file from DUT1 to DUT2. To do that, save the reference file provided with the Wireless Protocol Suite software on the Source device. Then connect the Bluetooth enabled devices and play the music file from one device to the other. The software will automatically detect the mode and present analysis for the user.

##### Playing the test file via Internet

If the user is testing a scenario where they need to analyze audio played through the internet (either using Wi-Fi or cellular data plan), they may access the reference file on YouTube provided by Frontline - <https://youtu.be/rmirDbikrtM>. Note that the software is only analyzing the Bluetooth link between the two DUTs. Any abnormalities at the Wi-Fi and cellular network level will affect the audio quality that may not be Bluetooth protocol related and the software will not be able to detect that.

## HFP

### Playing the test file by calling a phone number

Frontline provides the following phone numbers - 434-964-1407 and 434-964-1304 that users can call, to conduct speech audio data analysis over Bluetooth. The calls can be made using the cellular network (most common method) or VoIP. Again, the VoIP provider might use custom codecs and cause undesirable behavior which cannot be detected by Audio Expert System™ software.

### Playing the test file using Third party Apps

*Bluetooth* Audio Expert System™ Reference mode testing can be accomplished using third party apps on Android, iOS, and Windows phones. The following apps are available from their respective App stores:

- [BTmono, Android](#)
- [Blue2Car, IOS](#)
- [Windows Headset player lite](#)


**Note:** When selecting and using these apps, thoroughly review all the vendor documentation. While Teledyne LeCroy has conducted testing of these apps, Teledyne LeCroy has not completed full interoperability testing with our library of *Bluetooth* devices and does not warrant the use of these apps with every device when using the following procedures. Teledyne LeCroy does not provide support or maintenance for third party apps. Any issues or questions should be directed to the app developer.

1. In the following steps Device Under Test 1 (DUT1) is the device sending the reference test file to DUT2.
2. Download the third party app to DUT1 and follow the app vendor's instructions for installation and use.
3. Load the Audio Expert System reference test file

"Test\_1.02\_64.1kHz\_16Bit.wav"

on DUT1. The test file is stored on the users computer In the directory "\\Frontline <version #>\Development Tools\Audio Expert Test Files\".

**Note:** Reference test files are periodically updated. Shown here is an example. Files delivered with your latest Wireless Protocol Suite software version may have changed. Contact Teledyne LeCroy Technical Support for information on the latest reference file versions.

4. With the Soderia Soderia LE connected to the computer, configure the datasource, and follow procedures to capture data.
5. Launch Audio Expert System by clicking on the **Main windows** .
6. Turn on Bluetooth on your DUTs, DUT1 and DUT2. Turn on the third party *Bluetooth* app for routing the reference file over A2DP or HFP by following the vendor's directions.
7. Send the reference test file from DUT1 to DUT2 via the third party app.
8. Observe the events in the Audio Expert System™ **Events Table**. Look for an event **Description**:

“TestIDFound : REF: Test ID 1.02, Channel Gain = -11.8 dB TermFreq=400.0”.

**Note:** This is an example. The display may vary with the reference file version.

The Frontline analyzer has successfully detected the reference test signal and the system is locked into reference mode.

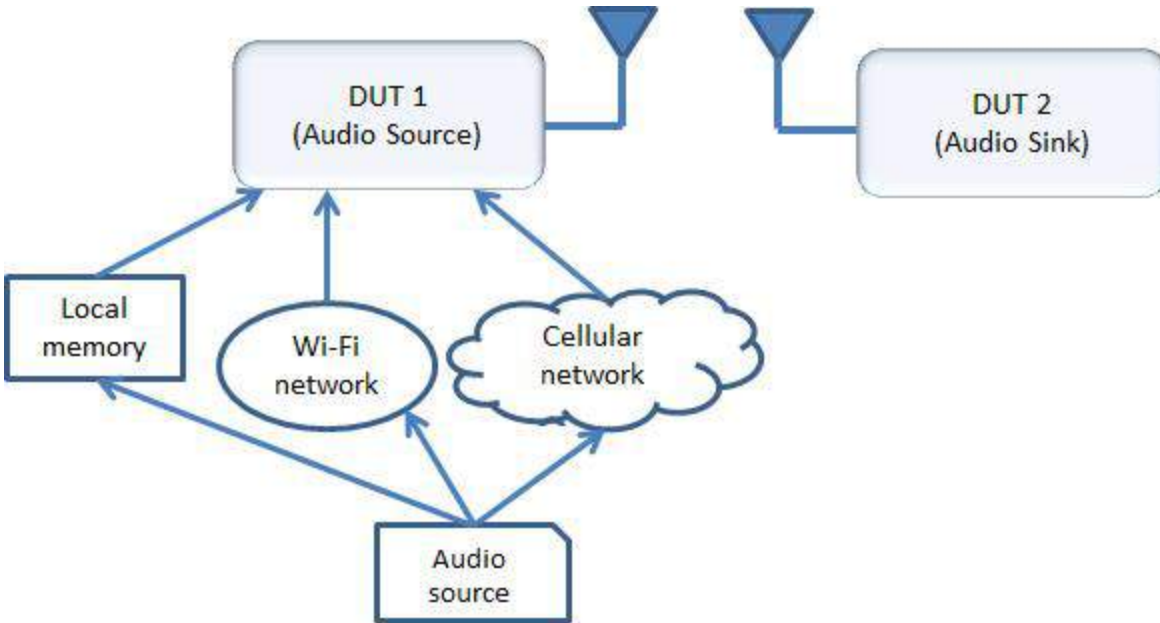


Figure 5.94 - Test Cases for Referenced Mode Testing

### 5.6.2.3.1 System Calibration for Referenced Mode

The objective is to achieve settings at the *Bluetooth* source device (DUT1) that bring the PCM sample levels of tones in the Reference Audio files sent over-the-air as close as possible to the levels at which they were created, without exceeding them. Test ID tones, and the tones in test file sequences for Referenced Mode are generally recorded with a maximum tone segment level of -3 dBFS, although there are a few exceptions where signal levels may be as high as -1 dBFS.

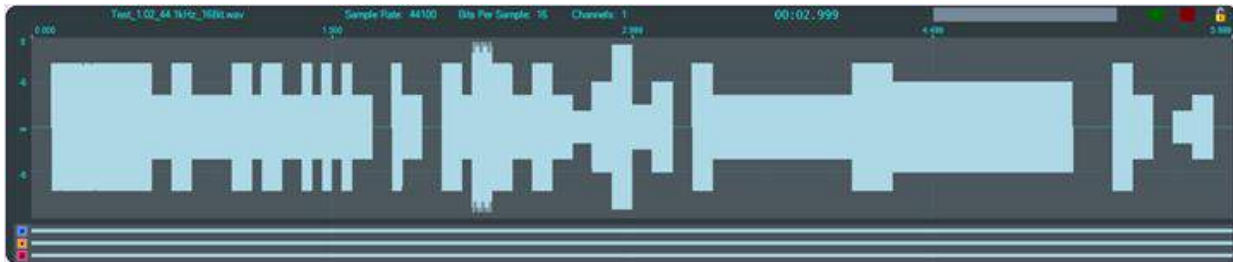


Figure 5.95 - Test\_1.02\_44.1kHz\_16Bit.wav Waveform

Show in the image above, is a graphic of the overall envelope of the Reference Audio test file “Test\_1.02\_44.1kHz\_16Bit.wav. Test 1.02 is a test file that enables a wide range of tests that includes a number amplitude changes, frequency changes, intentional silence, and multi-frequency tone segments. Its goal is to flush out the audio chain’s general ability to convey amplitude, frequency, silence, and duration.

The ideal calibration for this file is one where the waveform visualization on Frontline’s Expert System User Interface (UI) looks identical to the one shown below with respect to maximum levels. In particular, there are three segments in this test whose peaks are at exactly -6 dBFS. That is, there is zero loss or gain through the chain.

Table 5.18 - Test 1.02 -6 dBFS Segments

SegmentID	Frequency, Hz	Start Time, sec.	Duration, sec.
32	800	2.800	0.100
35	1120	3.100	0.100
40	400	4.300	0.900

These -6 dBFS segments are described in the Test 1.02 -6dBFS Segments table . These segments serve as a convenient and quick visual indicator that levels are appropriate, especially the longer 3rd case which is evident at the 4.999 second reference time of the above image(a little over 2/3 of the way through the test).

The first 0.500 seconds of Test 1.02, which contains the Test ID value “1.02” is shown below. The three digits ‘1’, ‘0’, and ‘2’ are represented by the low frequencies 210Hz, 200Hz, and 220Hz, respectively, which are 100 milliseconds in duration, and are separated by 1 kHz digit delimiters of 50 milliseconds duration. The final tone is a 100 millisecond segment at 400 Hz, defined as a “Test ID Terminator”. Note that since the levels of all of these tones are at exactly -3 dBFS, the peak levels should be exactly halfway between any available -6 dBFS (50%) gridline.

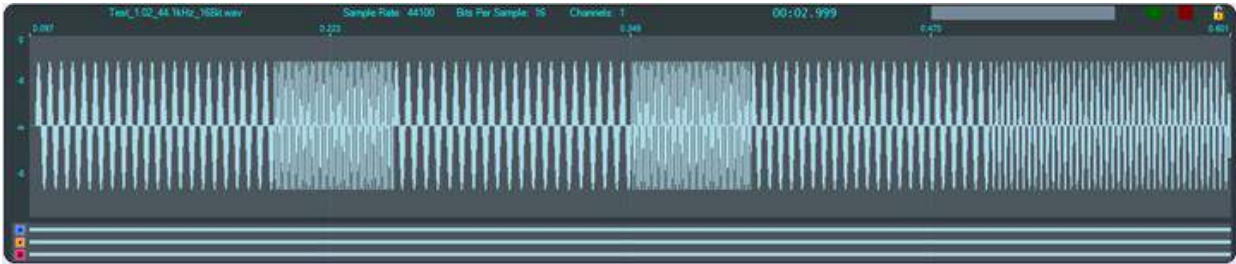


Figure 5.96 - Test 1.02 Test ID Segment

The three digits ‘1’, ‘0’, and ‘2’ are represented by the low frequencies 210 Hz, 200 Hz, and 220 Hz, respectively, which are 100 ms in duration, and are separated by 1 kHz digit delimiters of 50 ms duration. The final tone is a 100 ms segment at 400 Hz, defined as a “Test ID Terminator”. Note that since the levels of all of these tones are at exactly -3 dBFS, the peak levels -3 dBFS.

The value in the Info1 parameter of the “Test ID Found” event is optimally the value 23196 and may be converted to dBFS by the relationship

$$\text{dBFS} = 20 \log_{10} \left( \frac{\text{info1}}{32767.0} \right)$$

Optionally the value can be interpreted as “Channel Gain” via the relationship

$$\text{dB} = 20 \log_{10} \left( \frac{\text{info1}}{23196.0} \right)$$

Table 5.19 - "Test ID Found" Event "info1" Maximum and Minimum Values

Format	Application	Maximum	Minimum
Integer	Speech	23196	5826
	Music	23196	3297
Level	Speech	-3 dBFS	-15 dBFS
	Music	-3 dBFS	-20 dBFS
Chanel Gain	Speech	0 dB	-12 dB
	Music	0 dB	-17 dB

This table indicates the maximum and minimum acceptable levels for the "Test ID Found" Info1 parameter in integer form, decibel level in dBFS, and Channel Gain in dB.

**Example 1:** For the case where the Info1 parameter is converted to "Channel Gain", if the audio is speech (i.e. transported via a SCO channel), then a value of -11.9 dB is acceptable, and a value of -12.1 dB is not.

**Example 2:** For the case where the Info1 parameter is converted to "Channel Gain", if the audio is music (i.e. transported via an A2DP connection), then a value of -16.9 dB is acceptable, and a value

of -17.1 dB is not.

For both cases, at the high volume end, a value of -0.1 dB is acceptable, a value of 0.1 dB is not.

The dynamic range of the audio path is important to understand because it has a direct impact on measurement accuracy. Only levels at or above the minimum and at or below the maximum are examined for expected level and frequency.

### 5.6.2.3.2 Adjusting for Optimal Volume Levels

The exact steps that need to be taken depend on the exact devices being used, and their device specific setup requirements, and the speech or audio configuration under test. For the simplest case where, for example, a "music" audio file is to be played by a smartphone to a set of *Bluetooth* speakers, the typical steps would include the following.

1. Choose an audio reference file to be played at DUT1 appropriate for the configuration to be tested.

The test files are stored on the users computer In the directory. For example -> C:\Program Files (x86)\Teledyne LeCroy Wireless\Wireless Protocol Suite 19.3.18837.0\Help and Tools\Audio Expert Test Files

Test\_1.03\_48kHz\_16Bit\_3Loops\_2Ch.wav

**Note:** Reference test files are periodically updated. Shown here is an example. Files delivered with your latest Wireless Protocol Suite software version may have changed. Contact Frontline Technical Support for information on the latest reference file versions.

2. Before establishing the *Bluetooth* connection, play the file while listening to it on the DUT1 device itself, and become familiar with the overall sound quality, generally ignoring exact volume.
3. Set the playback volume at DUT1 to maximum.
4. Set the playback volume at DUT2 to minimum.
5. Establish the *Bluetooth* connection and begin playback of the file on DUT1, if possible in "Loop" or "Repeat" mode to avoid having to continuously restart.
6. Slowly increase the volume on DUT2 until it is at a comfortable level.

7. If the audio sounds distorted, reduce the playback volume at DUT1, and repeat Step 6.
8. When the clarity of the audio is comparable to that heard when listening to the DUT1 device, proceed with using the Frontline software enabled to capture and analyze the Bluetooth data.
9. Visually observe the waveform in the Audio Expert System **Wave Panel** comparing it to the image above, Figure 1.1. If the level of the -6 dB, 0.9 sec duration, 400 Hz tone (a little over 2/3 of the way through the test) is grossly above or below the -6 dB (50% volume) grid line, adjust the DUT1 volume accordingly and repeat this step. Optimally it would be on or just below the -6 dB gridline, but not above. The peak should never hit the maximum positive or negative limits of the display.
10. Find the “Test ID Found” event in the **Event Table** to verify that the system has transitioned to Referenced Mode, and verify that the value for “Channel Gain” (or “Level” as implemented in the UI) is within the range of values specified in Table 1-2.

If the observed (captured) waveforms do not reasonably conform to the above graphic for Test\_1.02, or the “Test ID Found” event is not reported, there is a problem along the audio chain. This could be as simple as a configuration setting, or more subtle such as an encoder/decoder incompatibility.

### 5.6.3 Audio Expert System™ Event Type

The following tables list the Audio Expert System™ *Bluetooth*, *Codec*, and audio events with description. Included in the tables is the event severity that can have three values: Information, Warning, and Error. The event severity will appear as icons and text in the Audio Event System once an audio streams has been captured. Refer to [5.6.4.3 Event Table, Event Table Columns on page 367](#) for an explanation of the severity types.

#### 5.6.3.1 Event Type: *Bluetooth* Protocol

Table 5.20 - Event Type: *Bluetooth* Protocol

Protocol	Severity	Description
A2DP	Warning	AVDTP signal response received for unknown command.
A2DP	Warning	Unrecognized capability type
A2DP	Error	eSCO parameters requested.
A2DP	Error	Profile TX PDUs larger than available bandwidth for active A2DP Streaming interval.
A2DP	Error	Bitpool value does not match configured bitpool range.
A2DP	Error	Attempt to suspend inactive stream.
A2DP	Error	Configuration attempt using unsupported CODEC.
A2DP	Error	Incorrect AVTDP command length.
A2DP	Error	Unknown command Stream End Point Identifier (SEID).
A2DP	Error	A2DP stream configuration attempt using invalid CODEC parameters.
A2DP	Error	A2DP stream configuration request sent during active stream.
A2DP	Error	Audio data length does not match length header.
A2DP	Error	Incorrect A2DP SBC frame fragmentation.
A2DP	Error	A2DP SBC frame header contents does not match stream configuration.

Table 5.20 - Event Type: Bluetooth Protocol(continued)

Protocol	Severity	Description
A2DP	Error	Attempt to configure A2DP stream with unsupported configuration.
A2DP	Error	Reported A2DP stream capabilities do not contain mandatory features.
A2DP	Error	A2DP streaming L2CAP channel not disconnected after ABORT operation.
A2DP	Error	Fragmented AVDTP packet not terminated before sending next packet.
A2DP	Error	Invalid AVDTP transaction ID.
A2DP	Error	Missing AVDTP command response.
A2DP	Error	Unrecognized A2DP content protection type.
A2DP	Error	Attempt to configure delay reporting during incorrect stream state.
A2DP	Error	Attempt to open A2DP stream that has not been configured.
A2DP	Error	Attempt to close A2DP stream that is not active.
A2DP	Error	A2DP streaming channel created before configuration completed.
A2DP	Error	Configuration command contains invalid length parameter.
A2DP	Error	Configuration command contains invalid media transport format.
A2DP	Error	SBC CRC Error.
A2DP	Error	SBC invalid channel mode.
A2DP	Error	SBC invalid header.
A2DP	Error	Invalid AVDTP configuration parameter.
A2DP	Error	Invalid AVDTP stream state

### 5.6.3.2 Event Type: Codec

Table 5.21 - Event Type: Codec

Codec	Severity	Event	Description
SBC	Information	Codec Initialization	Codec session started
SBC	Information	Codec tear-down	Codec session ended
SBC	Information	Stream Re-configuration	Stream Re-configuration
SBC	Error	Incorrect Configuration Detected	SBC Codec detected a change in audio parameters
SBC	Error	Lost Sync	SBC Codec expected to find synch word: 0x9C instead found: 0x: typically due to corrupted data
SBC	Error	Bad Header	SBC Codec detected corrupted header: typically due to corrupted data
SBC	Error	CRC Failure	SBC Codec detected bad CRC: typically due to corrupted data



Table 5.21 - Event Type: Codec(continued)

Codec	Severity	Event	Description
SBC	Error	No output	SBC Codec generated no output due to corrupted data
mSBC	Information	Codec tear-down	Codec Session Ended
mSBC	Information	Stream Re-configuration	Stream Re-configuration
mSBC	Warning	Packet Loss Concealment	mSBC Codec detected a bad frame and generated substitute data to compensate for it
mSBC	Error	Incorrect Configuration Detected	mSBC Codec detected a change in audio parameters
mSBC	Error	Lost Sync	mSBC Codec expected to find synch word: 0xAD instead found: 0x: typically due to corrupted data
mSBC	Error	Bad Header	mSBC Codec detected corrupted header: typically due to corrupted data
mSBC	Error	CRC Failure	mSBC Codec detected bad CRC: typically due to corrupted data
mSBC	Error	No output	mSBC Codec generated no output due to corrupted data when PLC not configured
AAC	Information	Codec initialization	Codec session started
AAC	Information	Codec tear-down	Codec session ended
AAC	Information	Bitstream type set	The bitstream type has been set. For Bluetooth, it should be LATM.
AAC	Warning	Single frame error, concealment triggered.	During decoding, a single frame error was detected which triggered built in concealment processing.
AAC	Error	Codec setting change	The codec has been re-initialized due to a setting change.
AAC	Error	Unframed stream error	A frame error was detected for an unframed stream. The codec is being reset in order to continue processing.
AAC	Error	Transport not initialized	The codec cannot be initialized for the given transport.
AAC	Error	Transport not supported	The selected transport is not supported. This could occur when an out of band LATM is selected opposed to in band.
AAC	Error	Transport failure	General failure in the transport.



Table 5.21 - Event Type: Codec(continued)

Codec	Severity	Event	Description
AAC	Error	Transport error	This typically occurs when there isn't any configuration information available.
AptX	Information	Codec initialization	Codec session started
AptX	Information	Codec tear-down	Codec session ended
AptX	Error	Bad Data	Non-stereo data has been detected for incoming data stream.
LC3	Error	Invalid payload length	Codec received a frame with less data than configured
LC3	Error	Unable to decode a frame	Codec was unable to decode the data
LC3	Error	Invalid codec configuration	Codec configuration data is corrupted
LC3	Warning	LC3 codec applied PLC on this frame	Codec detected bit stream error and applied PLC to the frame

**5.6.3.3 Event Type: Audio**

Table 5.22 - Event Type: Audio

Test Mode	Severity	Event	Description
Non-Referenced	Warning	Low Volume Alarm	Warn the user that the volume level of the detected audio is below the best range for performing meaningful audio analysis. Alarm is initialized when volume level above the "Measurement Threshold" level is detected. Alarm is activated when the detected volume drops below the "Measurement Threshold" level for 10 consecutive 0.5 sec measurement intervals.
Non-Referenced	Warning	<a href="#">Clipping</a>	Reports the detection of suspected distortion that occurs when the amplitude of a signal exceeds a digital systems ability to represent it accurately. Clipping is a type of amplitude distortion. The system reports a Clipping event when consecutive samples at the maximum value that can be represented by the digital system have been detected. Note that the maximum value that can be represented is different depending on the number of <a href="#">bits per sample</a> (i.e. bits of resolution) of the audio stream. The system limits the number of reported Clipping events to typically 10 to 20 per sec.

Table 5.22 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Non-Referenced	Warning	High Volume Alarm	Warn the user that the volume level of the detected audio is above the best range for performing meaningful audio analysis (i.e. above a level where the audio will likely become distorted). Alarm is activated when the detected audio volume is continuously above the high volume threshold (see Figure 2) for 10 consecutive 0.5 sec measurement intervals (i.e. 5 sec total). The event will not be repeated again until the detected volume level drops below the high volume threshold for 10 more consecutive 0.5 sec measurement connections.
Non-Referenced	Warning	<a href="#">Dropout</a>	Reports the detection of an unusual brief silence period where the brief silence is preceded and followed by “normal” audio levels. A typical definition of Dropout is the short dramatic loss of volume typically caused by lost digital information. Root causes include transmission system errors resulting in lost data packets, transmission channel reconfigurations, bad sections of memory, processor overloads that temporarily interrupt the flow of information, and so on.
Non-Referenced	Warning	<a href="#">Glitch</a>	Extremely large sample-to-sample audio amplitude transitions that have little probability of occurring within natural speech or music. Such dramatic changes would typically happen only in situations of dropped samples.
Referenced	Info	TestID Found	Occurs when a valid Test ID has been recognized. A valid Test ID must meet the level, frequency, duration, and delimiter requirements. If any of these parameters do not match, the process is terminated and is reset to the initial conditions. Until a Test ID is successfully recognized, the system will continue to operate in Non Referenced Mode; therefore, no events related to false starts are reported. This is because for arbitrary audio there is no expectation of any Test ID.
Referenced	Warning	Test Script Not Found	Occurs if a valid Test ID was found , but the script for that Test ID was not found. The system reverts to Non-Referenced Mode if this happens. This event should not occur if using a valid Reference Audio file provided by Frontline.
Referenced	Error	Invalid Test Script	This event is generated when an error occurs while accessing information in a script. This event should not occur if using a valid reference audio file provided by Frontline.

Table 5.22 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Error	Synchronization Lost	Generated when after a successful TestID recognition the system encounters unexpected frequencies or durations of audio segments while analyzing a received Reference Audio file. If this situation occurs, the internal segment tracking logic attempts to look forward and/or backward in the test script to determine if the currently measured characteristics are consistent with the previous or next segment of the script. If there is a match, the internal segment pointer is advanced or retarded appropriately, the Synchronization Lost event is not generated, and the audio analysis continues. However, if a match cannot be found, the system declares itself out of sync and generates the Synchronization Lost Event, terminates any active test script, and reverts to Non-Referenced Mode.
Referenced	Error	Unexpected Frequency	Reported when a measured frequency deviates from an expected frequency by a specific percentage (determined by the negotiated parameters of the over-the-air audio stream). The system knows the Reference Audio file that is being played on the Source DUT; therefore, the system knows which frequencies (tones) to expect at a given time.
Referenced	Error	Unexpected Level	Reported when the measured level at the start of a tone segment is not within tolerance. The tolerance is dependent on sample rate and bits per sample, but it generally is +/- 3 dB for speech and +/-11 dB for music. The system knows the Reference Audio file that is being played on the Source DUT; therefore, the system knows which amplitude level to expect at a given time.
Referenced	Error	Unexpected Duration	Reported when a tone segment of the Reference Audio file is shorter or longer than expected. The system knows the Reference Audio file that is being played on the Source DUT and therefore knows how long a specific tone segment should last. If either a change of amplitude or frequency arrives either before or after that programmed duration, then the change is by definition unexpected. This type of audio impairment can be caused by lost or corrupted data, repeated data, faulty packet loss concealment algorithms, etc.

Table 5.22 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Error	Amplitude Fluctuations	Reported if the system detects unexpected amplitude changes over a given interval. The test tones in Frontline's Reference Audio files have a fixed amplitude level over their duration. Therefore, if the corresponding audio levels received over the air by the system fluctuates more than a specified level (this level is based on the received audio stream parameters), then the system generates an Amplitude Fluctuations event.
Referenced	Error	Unexpected Phase Change	Provides a fine-grained indication of lost or repeated energy. The system knows when a specific tone should be expected. During this interval, the system checks that the measured average frequency is the same as the expected frequency. If this is correct, the system will continue to monitor the instantaneous frequency. If the instantaneous frequency deviates sufficiently from the current average frequency, the frequency measurement state machine will reset and begin re-measuring. Typically, the outcome is the discovery of the next scripted (expected) frequency. However, another outcome can be that the same frequency as the previous average frequency is rediscovered, and this is reported as an Unexpected Phase Change event. Such phase changes are an indicator of losses of signal that do not result in amplitude dropouts, or signal substitution (repetition) of previous audio energy due to things such as "packet loss concealment" tactics.
Referenced	Error	Excess Noise	The Excess Noise event is reported when energy sufficiently above the "Silence Threshold" is detected during programmed segments of silence. Excess noise can indicate a poor analog audio chain with an inherently poor noise floor, glitches occurring during silence intervals, or codecs that do not transition to silence instantaneously.

Table 5.22 - Event Type: Audio(continued)

Test Mode	Severity	Event	Description
Referenced	Error	<a href="#">Clipping</a>	Reports the detection of suspected distortion that occurs when the amplitude of a signal exceeds a digital systems ability to represent it accurately. Clipping is a type of amplitude distortion. The system reports a Clipping event when consecutive samples at the maximum value that can be represented by the digital system have been detected. Note that the maximum value that can be represented is different depending on the number of <a href="#">bits per sample</a> (i.e. bits of resolution) of the audio stream. The system limits the number of reported Clipping events to typically 10 to 20 per sec.
Referenced	Error	CVSD HF Level Too High	Reported when a CVSD encoded audio stream is detected and there is high frequency energy above 4 kHz that is greater than -20 dBFS.
Referenced	Info	End of Test Event	Reported to indicate that the system has completed processing a test script for a Reference Audio file, and that the system has exited Reference Mode. This event is generated when the elapsed time from the start of test is equal to or greater than the scripted duration of a test. It is reached when the number of samples processed equals the number of samples associated with the test duration.

**Clipping**

The number of consecutive samples needed to qualify as a clipping event depends on both sample rate and number of bits per sample. Table 1 specifies the number of consecutive samples at the maximum value level that will generate a Clipping event.

Table 5.23 - Clipping Event Thresholds

Consecutive Samples	Sample Rate, Samples/sec	Resolution, bits
3	8000	16
5	16000	16
11	41000	16
2	64000	16
12	48000	16
24	96000	16

Table 5.24 - Clipping Event Thresholds

Consecutive Samples	Sample Rate, Samples/sec	Resolution, bits
3	8000	16

Table 5.24 - Clipping Event Thresholds (continued)

Consecutive Samples	Sample Rate, Samples/sec	Resolution, bits
5	16000	16
11	41000	16
2	64000	16
12	48000	16
24	96000	16

### Dropout

Dropout events are reported when the average audio level (RMS) is initially above the Measurement Threshold, then falls below the Silence Threshold, and then quickly rises above the Measurement Threshold again). This approach largely disqualifies the natural inter-syllable silence and pauses that occur in natural speech, but will detect gaps caused by dropped data. Note that the system does not report dropouts that begin at very Low Energy levels.

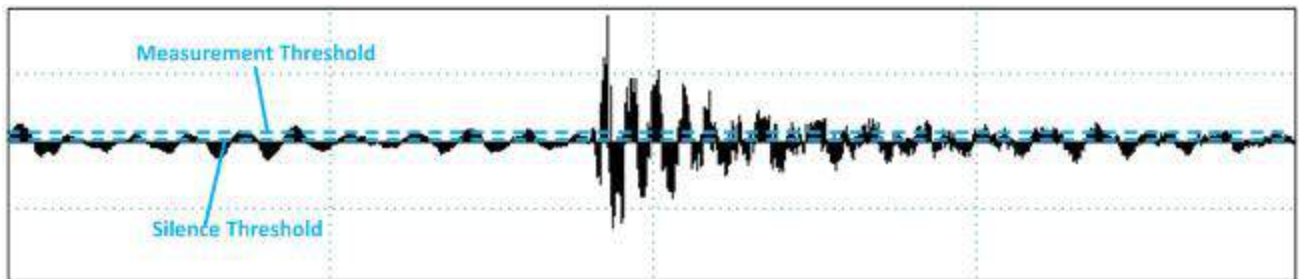


Figure 5.97 - Dropout: Measurement and Silence Threshold

### Glitch

The Glitch event is reported whenever an extremely large sample to sample amplitude transition occurs that has little or no probability of occurring within natural speech or music. As illustration, back to back +N, -N, ..., +N, -N values (where N is any non-zero number), represents energy at the Nyquist frequency, or  $\frac{1}{2}$  the sample rate. Neither speech nor music contain average energy levels at this frequency more the 20 dB below nominal. However, moderately large sample to sample changes in amplitude do occur, and these naturally limit how sensitive this measure can be configured.

The system uses back to back transition levels of 90 dB for music and 40 dB for speech as the threshold for reporting the Glitch event.

Such dramatic changes would typically happen only in the face of dropped samples, and serve as an additional means of detecting gross abnormalities

## 5.6.4 Audio Expert System™ Window

This window is the working space for the Audio Expert System™. Upon opening Audio Expert System™ the window shown below will open with four main areas displayed :

- Global Toolbar - Provides play cursor controls, waveform viewing controls, and volume controls that affect all Wave Panels.

- Wave Panel - Displays the waveforms for each captured audio stream. There is a separate Wave Panel for each stream. Each panel contains local information, controls, and an event timeline specific to the displayed audio stream being shown. Other Wave Panels that may be off screen may be viewed using the vertical scroll control or by collapsing other Wave Panels.
- Event Timeline - The Event Timeline shows *Bluetooth* events, Codec events, and Audio events synchronized to the displayed waveform. There is an Event Timeline in each Wave Panel.
- Event Table – A tabular listing of *Bluetooth*, codec, and audio events with information on event severity, related *Bluetooth* frame, timestamp, and event information.

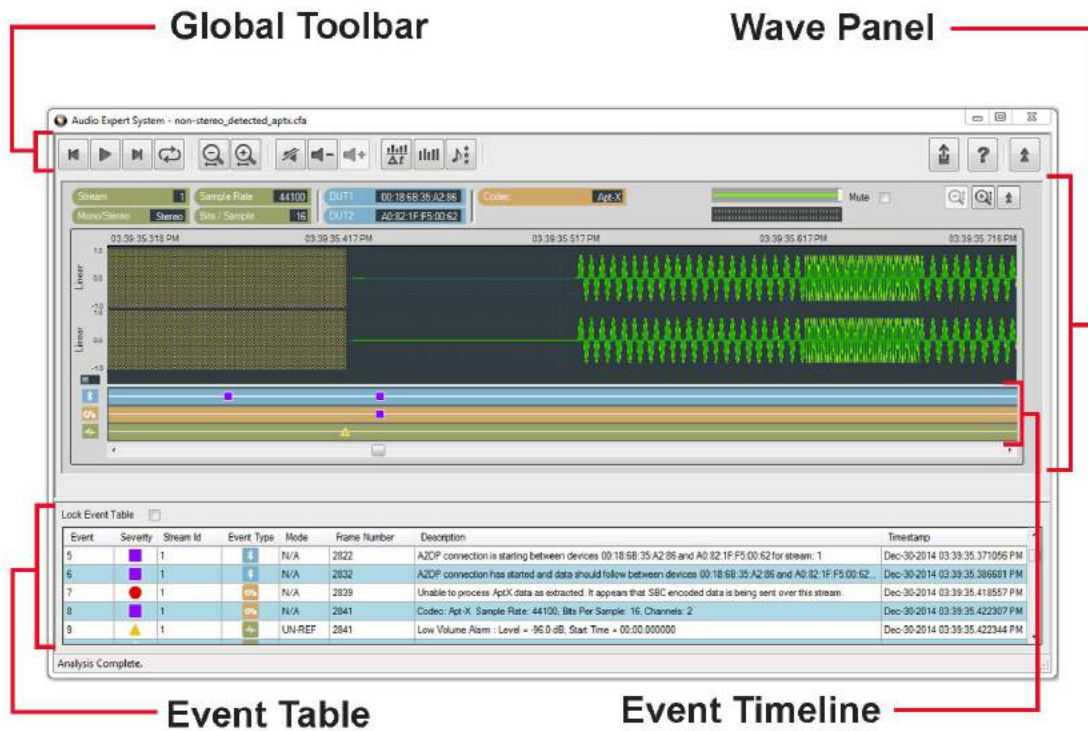


Figure 5.98 - Audio Expert System™ Window

**Color Codes and Icons**




The Audio Expert System™ uses standard color codes and icons to assist the user in focusing on specific issues.

Table 5.25 - Audio Expert System™ Color Codes and Icons

Category	Sub-Category	Color Code	Icon
Technology	Bluetooth	blue	
	Codec	orange	
	Audio	green	



Table 5.25 - Audio Expert System™ Color Codes and Icons (continued)

Category	Sub-Category	Color Code	Icon
Event Severity	Information	purple	
	Warning	yellow	
	Error	red	

**Note:** If an Event Severity icon is surrounded by a dark line, the event is a global event and not applying to a particular captured waveform. The event is assigned to "Stream 0" in the Event Table.

The following topics describe the Global Toolbar, Wave Panel, Event Timeline and Event Table in more detail.

### 5.6.4.1 Global Toolbar

The global toolbar provides audio play controls, audio play cursor positioning controls, waveform viewing controls, and volume controls. Global toolbar controls apply simultaneously to all waveform panels.



Table 5.26 - Global Toolbar Controls






Icon	Description
	Home: Moves play cursor to beginning of the waveform
	Play : Start playing the audio from the current play cursor position. Toggles to Pause when clicked. Pause: Stops audio play back at its current position, toggles to Play when clicked.
	End: Moves the play cursor to the end of the waveform
	Loop: Loops waveform playback continuously. If the Play button is visible it will toggle to the Pause. Clicking the Pause button will stop Loop playback. Clicking on the Loop button will stop the loop and the playback. If there is a selection on the waveform, only the selection will loop.
	Horizontal Zoom Out: Increases the amount of data that is visible on the screen; however, less detail is discernible.



Table 5.26 - Global Toolbar Controls (continued)












Icon	Description
	Horizontal Zoom In: Decreases the amount of data that is visible on the screen; however, more detail is discernible
	Lock/Unlock (Operational in live mode only): Selecting Lock will freeze the waveform display; however, the Audio Expert System™ will still continue to analysis new audio data..  Selecting Unlock will jump to the waveform end and then resume following the waveform.
	Mute: Mute will mute / unmute audio playback for all Wave Panels. Individual Wave Panel Mute control will override the Global Toolbar Mute for that panel only.
	Volume Down: Decreases the audio playback volume of all Wave Panels based on the current volume level setting for each individual Wave Panel.
	Volume Up: Increases the audio playback volume of all Wave Panels based on the current volume level setting for each individual Wave Panel.
	Average Bit Rate Overlay: Displays an overlay graph of the average bit rate for the audio stream in each Wave Panel. The average is based on a 0.10 second moving window.  When active, will deactivate Actual Bit Rate Overlay and Audio Rating Metric.
	Actual Bit Rate Overlay: Displays an overlay graph of the instantaneous bit rate for the audio stream in each Wave Panel.  When active, will deactivate Average Bit Rate Overlay and Audio Rating Metric
	Audio Rating Metric™. Used only when a Referenced Mode file is detected (See <a href="#">Referenced Mode on page 338</a> ). Displays an overlay graph of audio quality on a scale of 1 to 5, with 5 being excellent quality and 1 indicating bad quality.  When active, will deactivate Actual Bit Rate Overlay and Average Bit Rate Overlay.
	Export Data: Exports audio data in .raw and/or .wav format for selected Wave Panels or all the Wave Panels. This button also lets user export Event Table data in .csv format. Refer to <a href="#">Waveform Export Audio Data</a> for more details .

Table 5.26 - Global Toolbar Controls (continued)

Icon	Description
	Help - Opens Frontline software help.
	Collapse/Expand: Toggles between collapsing and expanding all Wave Panels. Note that the Wave Panel Local Controls Collapse/Expand control will locally override the Global Toolbar Collapse/Expand control.

### 5.6.4.2 Wave Panel

The Stream Panel is where the details of the captured audio stream are presented. The Stream Panel displays the captured audio waveform along with an event timeline that displays discrete *Bluetooth*, *Codec*, and *Audio* events synchronized to the captured waveform. .

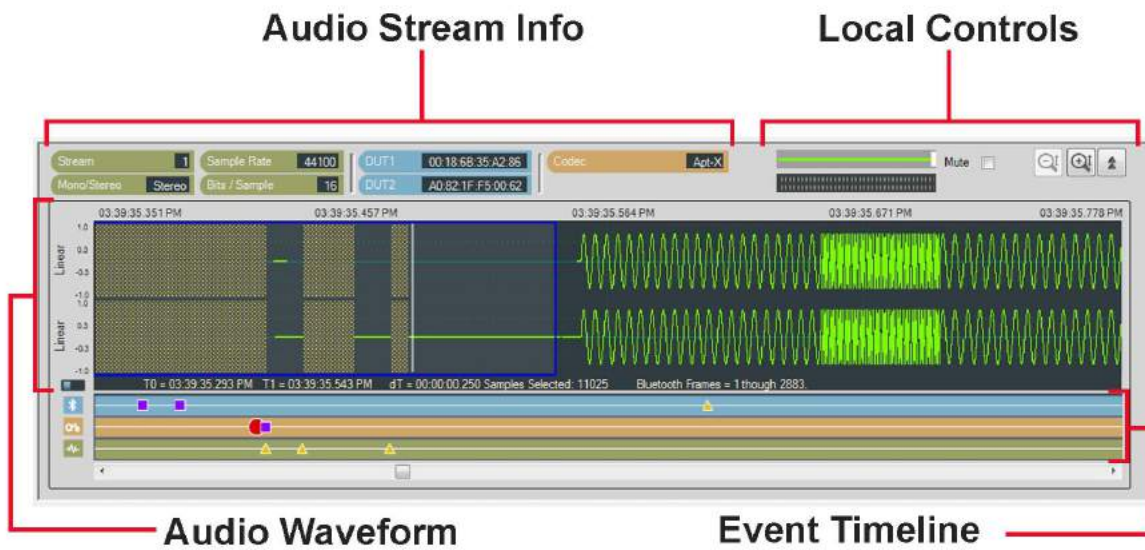





Figure 5.99 - Wave Panel

The Wave Panel contains four sections.

1. Audio Stream Info that provides users with information, such as sample rate, bit/sample, codec and DUT (Device Under Test) addresses.
2. Local Controls include audio volume controls and Indicators, “Mute”, “Vertical Zoom” and “Collapse/Expand”
3. An Audio Waveform which is plotted as amplitude (linear or dB) versus time and an interactive play cursor. The play cursor appears as a white vertical line across the waveform.
4. Event Timeline that shows color coded *Bluetooth* , *Codec* , and *Audio*  events. Details of these events are listed in the Audio Expert System™ Event Table.

### 5.6.4.2.1 Audio Stream Info

The Audio Stream Info displays Audio, *Bluetooth*, and Codec information (left to right in the image below) about the audio waveform displayed in the panel. This information is discovered during AVDTP signaling when the devices under test (DUT) negotiate audio streaming parameters.

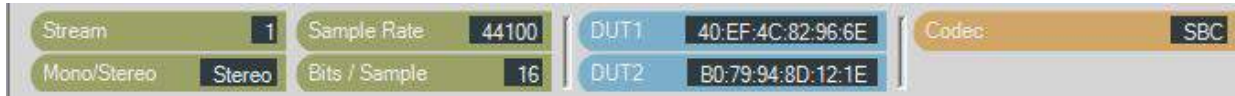


Figure 5.100 - Audio Stream Info in the Wave Panel

Table 5.27 - Audio Stream Info Tags

Category	Name	Description
Audio	<b>Stream</b>	A system assigned index number that represents an audio waveform between a pair of Bluetooth devices. This number appears in the Event Table for easy cross-referencing.
	<b>Sample Rate</b>	Displays the sampling frequency used to digitize the original audio.
	<b>Mono/Stereo</b>	Indicates if the audio data is monaural or stereophonic.
	<b>Bits/Sample</b>	Displays the number of bits per sample of the audio data.
<i>Bluetooth</i>	<b>DUT1</b>	<i>Bluetooth</i> address of one device in the connection. Can be either sending or receiving the audio data.
	<b>DUT2</b>	<i>Bluetooth</i> address of the other device in the connection. Can be either sending or receiving the audio data.
Codec	<b>Codec</b>	Displays the Codec type used by the captured audio stream. The supported codecs include SBC, AAC, aptX-Classic, aptx-LL, aptX-HD, LC3, mSBC, and CVSD.

#### SBC Codec Information Pop-up

When you hover over the **Codec** tag and the Codec = SBC a pop up will appear that shows additional information about which SBC parameters can be used. The pop-up is visible as long as the cursor hovers over the **Codec** tag.

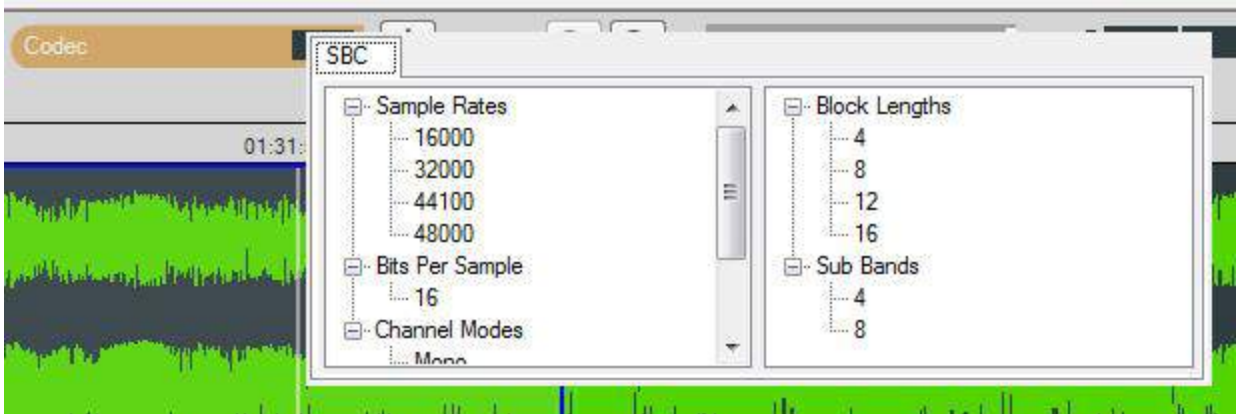


Figure 5.101 - SBC Codec Information Pop-Up on Cursor Hover Over

### 5.6.4.2.2 Local Controls

The Local Controls in each Wave Panel provide the user with indicators and controls for waveform display and audio play back.



Figure 5.102 - Wave Panel Local Controls

#### Waveform Play Back Volume



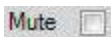
The volume slider controls the playback volume for the audio in each Wave Panel.

#### Audio Volume Indicator



The volume indicator shows the relative audio volume at the waveform display play cursor. When the green bars completely fill the indicator the audio volume is at its highest level. As the volume decreases, the bars will move to the right linearly, with no visible green bar indicating no audio. The volume indicator will continue to operate if the audio stream has been muted.

#### Mute



Checking the **Mute** check box will silence the Wave Panel's audio output. The volume indicator will respond to the audio volume but nothing will be heard. All panels can be simultaneously muted using the Audio Expert System™ Global Toolbar. The Wave Panel mute is a local control only. However, the Global Toolbar mute control will set the Stream Panel's Local Controls mute.

### Vertical Zoom



Each Wave Panel contains local Vertical Zoom controls that expands or reduces the waveform display vertically. The waveform amplitude is always visible, and the Vertical Zoom controls increases or decreases the entire vertical size of the display. The vertical zoom buttons will turn gray and become inactive when the maximum and minimum values are reached.

### Collapse/Expand Control



Collapse/Expand button toggles between two views. The top image indicates that the Wave Panel is expanded. When the bottom image is visible it indicates that the Wave Panel is collapsed.



When the top image is visible, clicking on it will collapse the Wave Panel to the minimum size that shows only the Stream Info and the Local Controls. When the bottom image is visible, clicking on it expands the Wave Panel to full size.



Figure 5.103 - Collapsed Wave Panel

### 5.6.4.2.3 Audio Waveform Panel

The Audio Waveform Panel displays the captured audio waveform. If the waveform is stereo, both channels are visible in the Wave Panel. The user can view the entire waveform or can zoom to view a portion of the waveform in more detail.

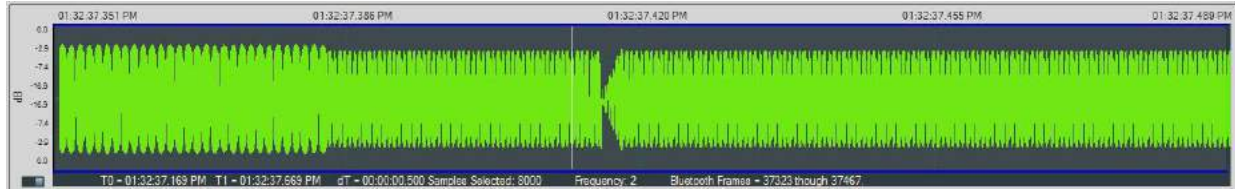


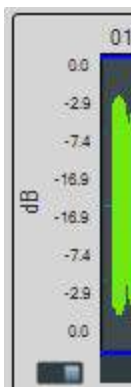


Figure 5.104 - Audio Waveform Panel in the Wave Panel

Table 5.28 - Global Toolbar Waveform Horizontal Zoom Controls

Control	Description
	Horizontal Zoom: Increases the amount of data that is visible on the screen; however, less detail is discernible.
	Horizontal Zoom: Decreases the amount of data that is visible on the screen; however, more detail is discernible.

## Waveform



The audio waveform is plotted as amplitude versus time on the Wave Panel. The amplitude scale is located on the left edge of the Wave Panel. The waveform's amplitude can be linear or in decibels. The linear range is -1.0 to +1.0. The range for the dB scale is 0 dB for the maximum positive and maximum negative values, and silence is negative infinity. A toggle switch at the bottom of the amplitude scale will switch between **Linear** scale and **dB** scale. Moving the switch to the left will display the **Linear** scale and moving it to the right will display the **dB** scale.

## Play Cursor

The Play Cursor is identified by a white vertical line on the Wave Panel. The Play Cursor appears when user clicks on any point in the waveform, or, if the cursor is already present it can be dragged to another position. To drag the Play Cursor, hover the mouse cursor over the Play Cursor until the mouse cursor changes to a pointing hand; click and drag the cursor to a new position.

## Waveform Segment Selection

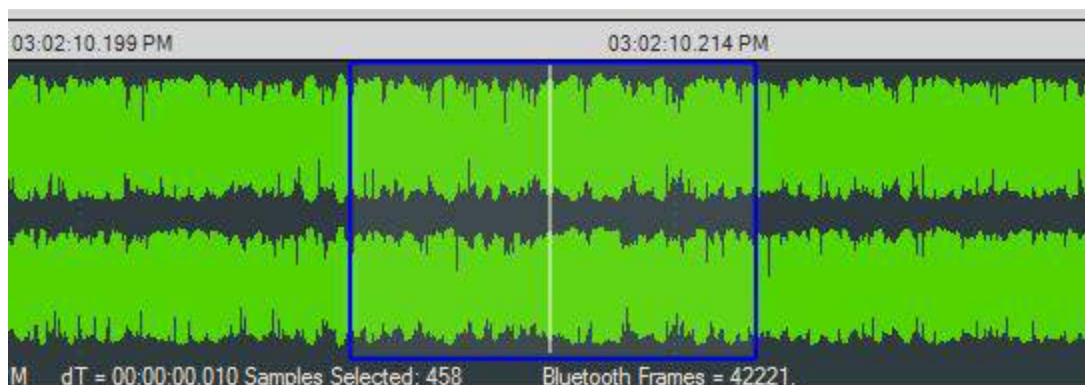


Figure 5.105 - Selection in the Audio Waveform

A waveform segment selection is identified by a blue border surrounding the selection. Procedures for selecting a segment depend on the desired actions.



Table 5.29 - Segment Selection Procedures

Desired Action	Procedure
Loop play back	<ol style="list-style-type: none"> <li>1. Zoom in to the waveform segment of interest.</li> <li>2. Click in the approximate center of the proposed selection. This will place the Play Cursor in the area to be selected.</li> <li>3. Move the mouse cursor to the right or left of the Play Cursor, click and hold, then drag over the waveform segment of interest. Release the mouse key. The selection is surrounded by a blue border.</li> </ol>
View waveform details	<ol style="list-style-type: none"> <li>1. Zoom in to the segment of interest.</li> <li>2. Move the mouse cursor to the right or left limit of the waveform segment of interest; click and hold, then drag over the waveform segment of interest. Release the mouse key. The selection is surrounded by a blue border.</li> </ol>

For either of the procedures described in the table above, once the selection is made details of the segment appear below and to the left of the waveform. These details include selection start and stop range ("T0" and "T1"), the time difference ("dT"), samples selected, frequency, and "Bluetooth Frames" selected.

Right-clicking in the Waveform panel will open a pop up menu (see [Wave Panel & Event Table Pop-up Menu on page 368](#)). Selecting **Zoom to Selection** will expand the selection to the full width of the Wave Panel. Other selection option in the pop up are **Select Area**, **Clear Selection**, and **Copy Selection**.

### Actual Bitrate Overlay Display

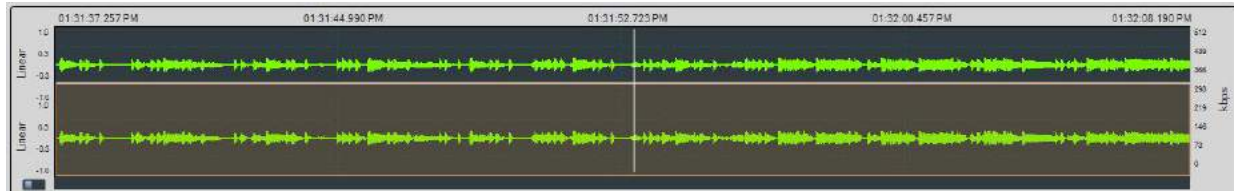




Figure 5.106 - Actual Bitrate Overlay

The Average and Actual audio stream bitrate graphs can be displayed over the audio waveform using the Global Toolbar Average Bitrate Overlay  and Actual Bitrate Overlay  buttons respectively. These are presented as overlays onto the main Wave Panel so the user can correlate audio issues with bitrate changes and the like. The scale is in kbps (kilo bits per second). Hovering over the bitrate scale will display a pop-up showing the bitrate at the play cursor position.

Actual Bitrate is based on the throughput at the Codec level.

The Average Bitrate is the moving average over 0.1 sliding-second window.

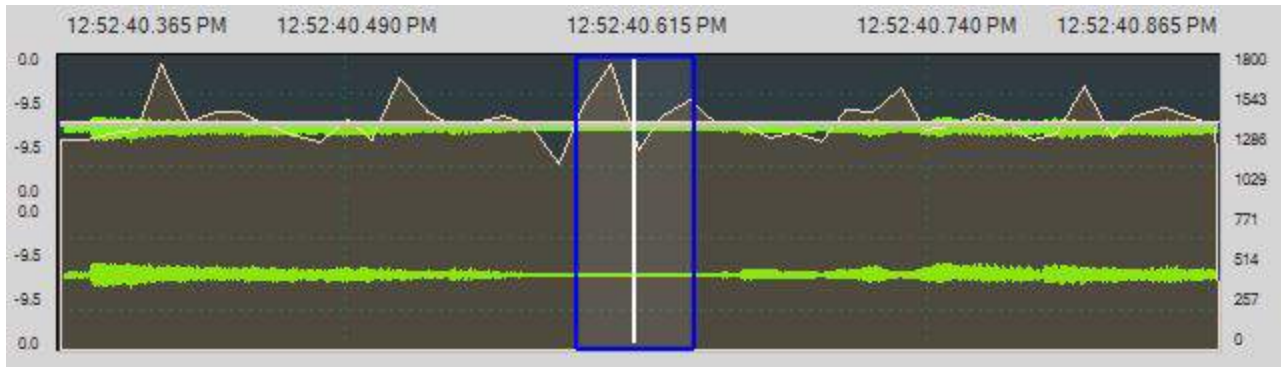
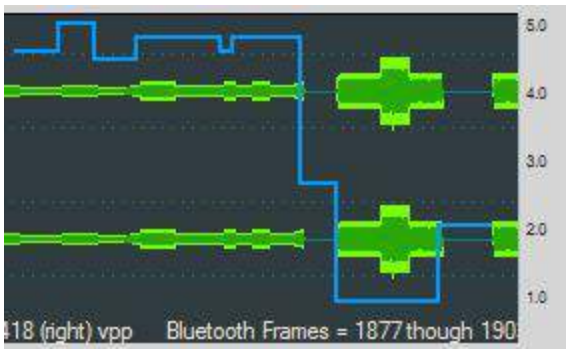



Figure 5.107 - Average Bitrate Overlay

All of the information for calculating the Actual and Average Bitrate is in the codec data frame header.

**Audio Rating Metric (Referenced Mode Only)**



The Audio Rating Metric is only available in referenced mode operation when a reference audio has been detected with a Test ID Found event. When the Audio

Rating Metric button  on the Global Toolbar is activated, a metric scale appears on the right of the Audio Wave Panel and a blue graph line is overlaid onto displayed waveform. This graph represents an objective score of the captured audio compared to the original reference audio. The score is based on a set of six Audio Expert System™ real-time measurements that include, for example, the number of frequency resets. Individual scores are computed frequently for sub-second segments

of reference mode audio; these segments can be as small as 50 milliseconds. Scores are computed for a frequency change, for silence, for multi frequency segments. or for level changes.

The Audio Rating Scale ranges from 1 to 5. [Audio Rating Metric Scale Interpretation below](#) provides an interpretation of the major scale points in quality and in the hearer's perception of the difference between the reference signal and the playback. At a scale value of 5, the reference signal in the audio waveform panel would represent excellent quality because, when hearing the audio played, the difference between the playback and the original reference audio is imperceptible.







Table 5.30 - Audio Rating Metric Scale Interpretation

Major Scale Point	Quality	Hearer's Perception of Difference
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The Audio Rating Metric is best used for making relative comparisons and for localizing problem areas.



### 5.6.4.2.4 Event Timeline

The Event Timeline in the Wave Panel shows the *Bluetooth* , *Codec* , and *Audio*  events related to the waveform being viewed. The events are synchronized in time to the waveform displayed in the Wave Panel. The event severity is displayed as Information , Warning , and Error .

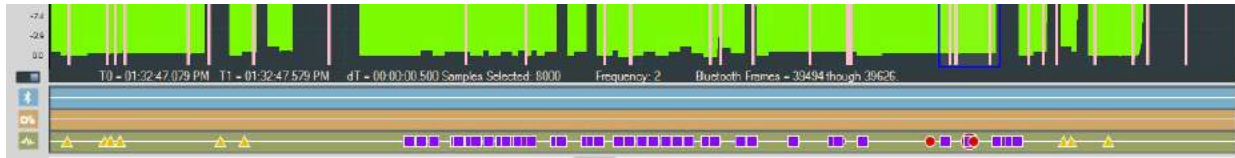


Figure 5.108 - Event Timeline Shown with Wave Panel

Clicking on an event in the Event Timeline shows a relevant selection in the Audio Waveform Panel. The size of the selection depends on the number of frames associated with the selected event. This selection will appear in all Wave Panels; however, the event severity icon will only appear in the Wave Panel associated with the event.

To assist the user with viewing events in detail, the Event Timeline will zoom in and out in sync with the Wave Panel.

### Event Timeline Example

This example shows that event 159 was selected in the Event Table resulting in the severity icon being enlarged in the Event Timeline. The system automatically selected the surrounding area—the blue outline.

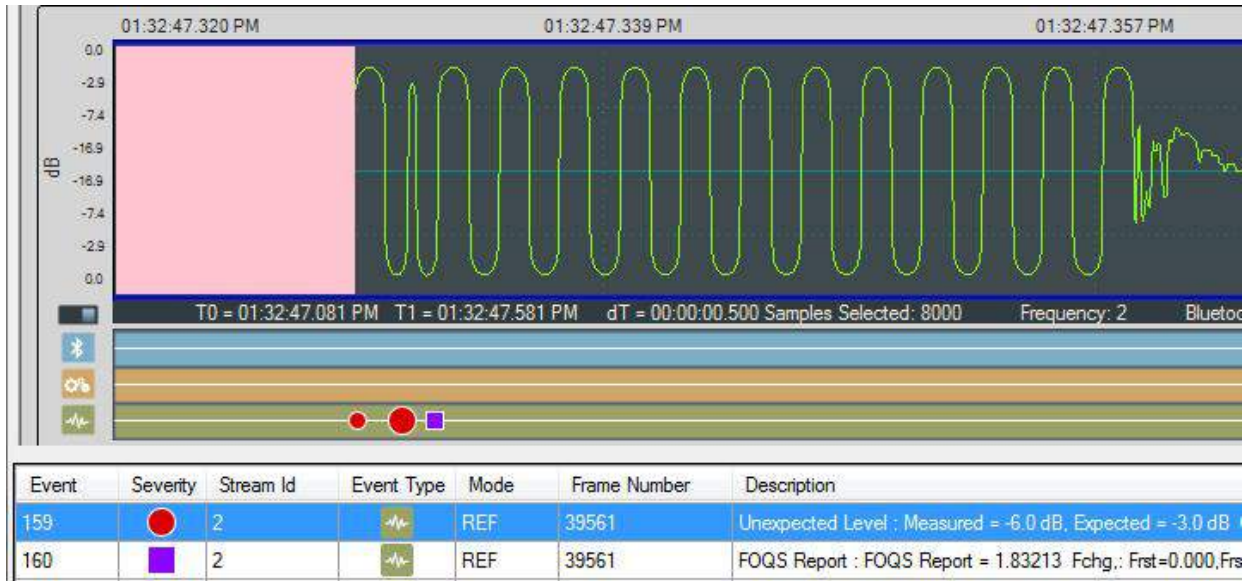


Figure 5.109 - Example: Event Table Selection Shown in Event Timeline

### Event Pop Up

When the cursor hovers over a selected event severity icon in the Event Timeline, a pop-up will display the event class, severity, and associated *Bluetooth* frame.

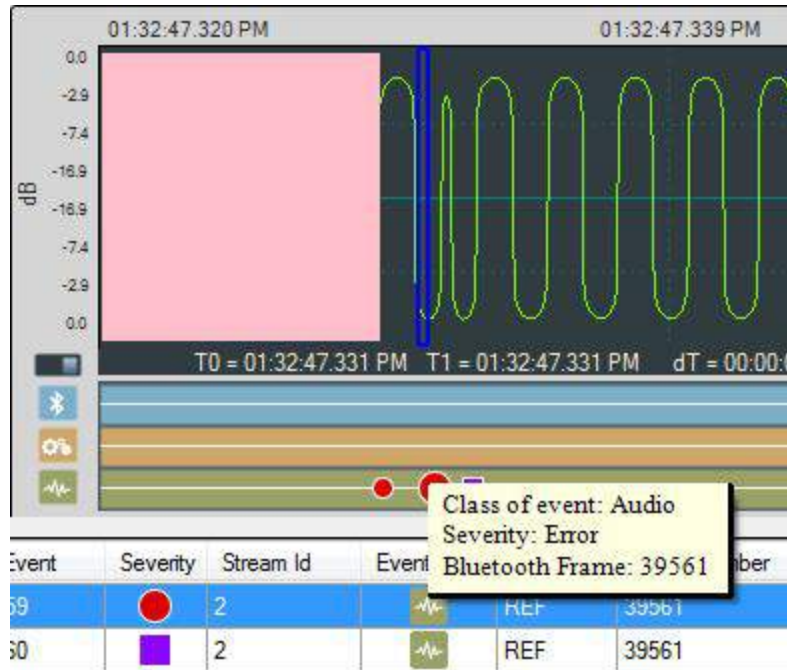


Figure 5.110 - Event Timeline Selected Event Pop Up

### 5.6.4.3 Event Table

The Event Table lists all audio stream events. Clicking on an event will select that event in the Event Timeline in the Wave Panel. If the selected event is outside the visible area of the waveform, the waveform will move and bring the selected event to the center of the display. The event icon in the Event Timeline is also centered and the selected icon will be larger than the non-selected event icons. Selecting one or more events in the table will highlight the associated frames in the standard Frontline software windows, such as **Main windows**, **Coexistence View**, **Bluetooth Timeline**, etc. .

Event	Severity	Stream Id	Event Type	Mode	Frame Number	Description	Timestamp
17	Yellow Triangle	1	Bluetooth	N/A	3039	Packet retransmission.	Mar-31-2014 12:52:38.080991 PM
18	Purple Square	1	Bluetooth	N/A	4094	A2DP paused between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:52:45.553569 PM
19	Purple Square	1	Bluetooth	N/A	4095	A2DP paused between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:52:45.617944 PM
20	Yellow Triangle	0	Bluetooth	N/A	4101	SCO connection request.	Mar-31-2014 12:52:46.151071 PM
21	Purple Square	2	Bluetooth	N/A	4105	SCO connection established between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 2 using cod...	Mar-31-2014 12:52:46.504191 PM
22	Purple Square	3	Bluetooth	N/A	4105	SCO connection established between devices 00:07:62:0F:00:00 and 98:0D:2E:23:B6:2E for stream: 3 using cod...	Mar-31-2014 12:52:46.504191 PM
23	Purple Square	2	Audio	N/A	4108	Codec: CVSD Frequency: 64000, Bits Per Sample: 16, Channels: 1	Mar-31-2014 12:52:46.806067 PM
24	Purple Square	3	Audio	N/A	4256	Codec: CVSD Frequency: 64000, Bits Per Sample: 16, Channels: 1	Mar-31-2014 12:52:47.357946 PM
25	Purple Square	2	Bluetooth	N/A	13222	SCO disconnected between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 2 using codec: CVSD	Mar-31-2014 12:53:04.151789 PM
26	Purple Square	3	Bluetooth	N/A	13222	SCO disconnected between devices 00:07:62:0F:00:00 and 98:0D:2E:23:B6:2E for stream: 3 using codec: CVSD	Mar-31-2014 12:53:04.151789 PM
27	Purple Square	1	Bluetooth	N/A	13253	A2DP resumed between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:53:05.446738 PM
28	Purple Square	1	Bluetooth	N/A	13254	A2DP resumed between devices 98:0D:2E:23:B6:2E and 00:07:62:0F:00:00 for stream: 1 using codec: SBC	Mar-31-2014 12:53:05.474864 PM
29	Yellow Triangle	0	Bluetooth	N/A	13479	Packet retransmission for unknown CID.	Mar-31-2014 12:53:07.712976 PM
30	Yellow Triangle	1	Bluetooth	N/A	14187	AVDTP packet loss detected based on missing packet sequence number.	Mar-31-2014 12:53:13.742943 PM
31	Yellow Triangle	1	Bluetooth	N/A	14351	AVDTP packet loss detected based on missing packet sequence number.	Mar-31-2014 12:53:15.385434 PM







Figure 5.111 - Event Table

Several events can be selected by clicking and dragging over the events, or by holding down the Shift key and clicking on events. To select events that are not adjacent hold down the Ctrl key and click on the events.

When selecting multiple events, the Wave Panels will not scroll to the selected events.

The Event Table contains eight columns.

Table 5.31 - Event Table Columns

Name	Value	Description
<b>Event</b>	integer	System generated sequential numbering of events.
<b>Severity</b>		<b>Information</b> - provides information of interest but does not indicate a problem event.
		<b>Warning</b> -identifies a potential problem where further investigation may be appropriate
		<b>Error</b> - identifies a definite problem.
<b>Stream Id</b>	integer	A system generated ID that is assigned in the order that the audio streams are detected. The ID is not maintained between captures for the same device with the same audio. It identifies the Wave Panel where the event can be viewed. The ID appears in the Audio Stream Info of the Wave Panel.
<b>Event Type</b>		<i>Bluetooth</i> -Events generated by analyzing Bluetooth protocol activities.
		Codec -Events generated from analyzing the audio coding/decoding activities.
		Audio -Events generated by analyzing the audio data.
<b>Mode</b>	N/A	Mode does not apply to this event.
	REF	Referenced Mode. Refer to <a href="#">5.6.2.2 Referenced Mode on page 338</a> .
	UN-REF	Non-Referenced Mode. Refer to <a href="#">5.6.2.1 Non-Referenced Mode on page 338</a> .
<b>Frame Number</b>	integer	The system generated identification for a specific frame.
<b>Description</b>		Details and explanation about this event.
<b>Timestamp</b>	clock date and time	A system generated time stamp for each frame.

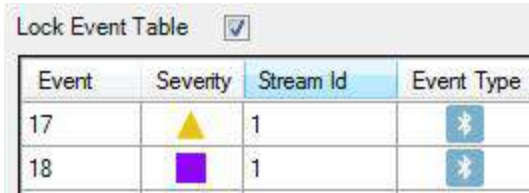
### Sorting

Event table entries are sortable by column. Left-click on the column heading to sort.

### Event Table Pop-Up Menu

Right-clicking with the cursor over the Event Table will open a menu of additional options. For more on this option see [Wave Panel & Event Table Pop-up Menu on page 368](#).

### Lock Event Table

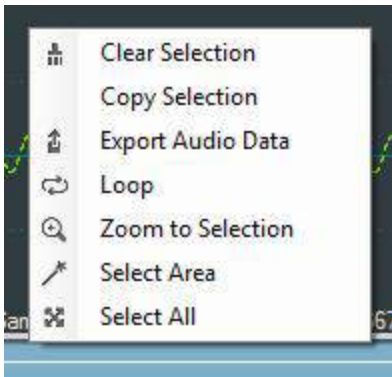


The **Lock Event Table** checkbox is available in live mode only. Clicking to check the box will prevent the Event Table from scrolling during live capture. Un-checking the box will resume scrolling of events as they are detected. When analyzing a capture file the checkbox has no effect.

### 5.6.4.4 Wave Panel & Event Table Pop-up Menu

Additional Wave Panel and Event Table options are available by right clicking the mouse with the cursor anywhere in the Wave Panel or in the Event Table.

#### Wave Panel Pop-up Menu Actions



Right-clicking anywhere in the Wave Panel will provide you with a selection of the following actions.

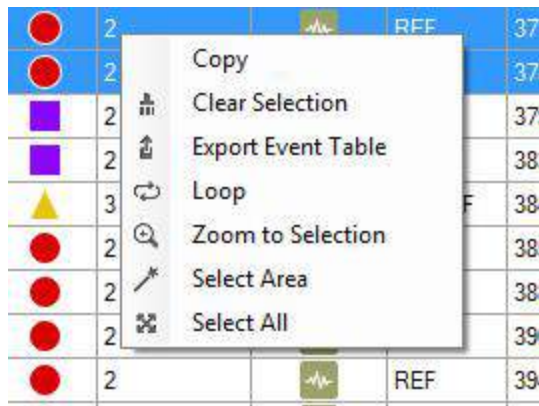
Table 5.32 - Wave Panel Pop-up Menu Selections

Option	Description
Clear Selection	Clears the current selection in the viewer
Copy Selection	Saves a copy of the selection to the computer clipboard. The clipboard can be pasted into a Word document, an e-mail, or other Windows clipboard-compatible application.
Export Audio Data	Opens the Export pop-up menu with options to export the waveform as a .raw, .wav, or Event Data. For additional details on exporting refer to <a href="#">Waveform Display Export</a> .
Loop	Loops through the audio selected on the Wave Panel.

Table 5.32 - Wave Panel Pop-up Menu Selections (continued)

Option	Description
Zoom to Selection	Expands or compresses the selection to fill the Wave Panel view.
Select Area	When the mouse cursor is positioned over data (not fill, pause, or gaps) in the Wave Panel and selecting this option will select all the data between and fills, pauses, or gaps.
Select All	Selects the entire waveform

**Event Table Pop-up Menu Actions**




Right-clicking in the Event Table will provide you with a selection of the following actions.

Table 5.33 - Event Table Pop-up Menu Selection

Options	Description
Copy	Copies the selected events to Windows clipboard as text.
Clear Selection	Clears the current event selection in the table
Export Event Table	Copies the current event selection and saves it as a .csv file. For additional details on exporting refer to <a href="#">Event Table Export</a> .
Loop	Loops through the audio selected on the Wave Panel.
Zoom to Selection	Expands the Event Table selection to fill the Wave Panel view.
Select Area	Expands the selection.
Select All	Selects all events.

**5.6.4.5 Export Audio Data**

There are two ways to export audio data:

1. Clicking the Audio Expert System™ window **Global Toolbar** Export button .
2. Right-click in a Stream Panel Wave Panel and a pop-up menu will appear. Select **Export**.

Two windows will appear:

1. The standard Windows Save As.
2. The **Export Audio Data** dialog.

In the Windows Save As window enter a **File name** and directory location. Click on **Save**.

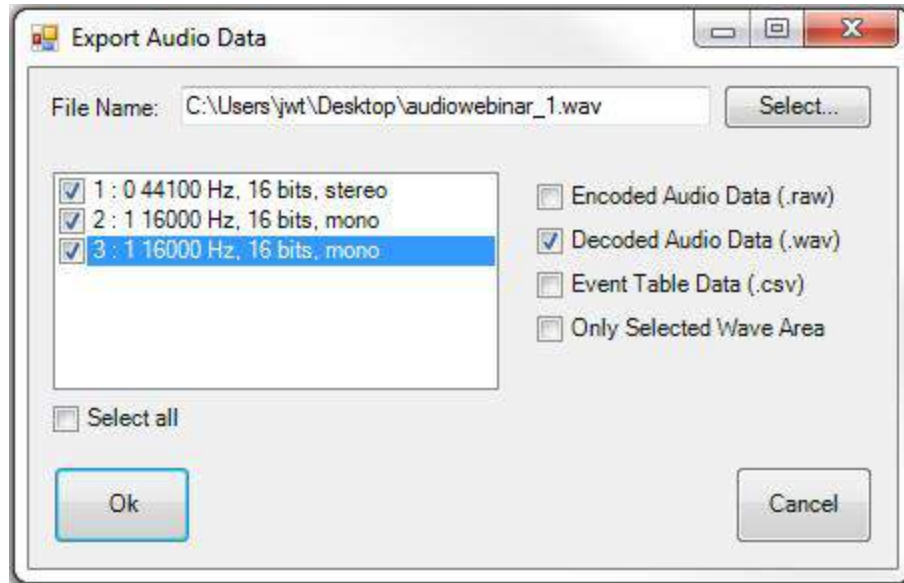


Figure 5.112 - Export Audio Data dialog

The Save As window will close, and the file name will appear in the **File Name** field in the **Export Audio Data** window. Should the file name need to be changed, click on the **Select** button and the Windows Save As dialog will open. By default the .wav file extension is used in the file name.

In the window below **File Name** will appear a list of **Stream Ids** with a description from the Audio Stream Info . If opening from the Audio Expert System™ **Global Toolbar** all **Stream IDs** are checked by default. If opening from a Wave Panel, the **Stream ID** where the export dialog was opened is automatically checked. You can check each stream that is to be exported. For convenience checking **Select all** below the stream list window will place checks in all streams.

### Export Options

After selecting the streams to export, select the desired formats to export.

Table 5.34 - Export Audio Data Format Options

Option	Description
Encoded Audio Data	Exports the selected files as .raw format. The audio data is in an encrypted format and user will need a codec to decode it.



Table 5.34 - Export Audio Data Format Options (continued)

Option	Description
Decoded Audio Data	Exports the selected files as .wav format that can be played on a wide variety of media players.
Event Table Data	Exports a text .csv file of all the detected events
Only Selected Wave Area	Exports the Encoded, Decoded, or Event Data for the selected waveform. This option is only active if a selection has been made in one of the Wave Panels

 audiowebinar_1.csv	39 KB	Microsoft Excel C...
 audiowebinar_1.raw	5,439 KB	RAW File
 audiowebinar_1.wav	38,652 KB	Wave Sound
 audiowebinar_2.csv	39 KB	Microsoft Excel C...
 audiowebinar_2.raw	299 KB	RAW File
 audiowebinar_2.wav	7,227 KB	Wave Sound

Click on **OK** to save the waveform. The dialog will close and a series of progress bars will appear. Each progress bar is associated with a file for each export option. The exported files will have the following syntax: *<filename>\_n.<filetype>*, where *<filename>* = the name entered into the File Name field, *n* = the stream id number (1, 2, 3, ...), and *<filetype>* = "raw", "wav", and "csv". The image shows an example where the user exported **Stream**

**Id's 1 and 2** in Encoded Audio , Decoded Audio , and Event Table data to filename "audiowebinar".

Click on **Cancel** to close the window without exporting.

### 5.6.4.6 Export Event Table

Right-clicking in the Event table will open a pop-up menu with the option to **Export Event Table**. This option will export selected events in the in comma separated variable (.csv) format for used in Microsoft Excel or any other Windows .csv compatible application.

First select the events to export. Multiple events are selectable by selecting an event then holding the Shift key while clicking on another event. This will select all events between the two selections. If the selections are not adjacent you can hold the Ctrl (control) key while clicking events.

Next right-click anywhere in the Event Table to open the pop-up menu and click on the **Export Event Table** option. A Windows **Save As** dialog will open. Enter a file name and select a file location and click on **Save**. A confirmation dialog will open. Click **OK** to close the confirmation dialog.

If you have not selected an event in the table before exporting, a warning to "Please select an event row first." appears.

### 5.6.5 Frame, Packet, and Protocol Analysis Synchronization

The Audio Expert System™ module integrates seamlessly with Frontline software with common timestamping of *Bluetooth* protocol data, audio events, audio waveform display, and codec events. The audio expert data and results are synchronized and coordinated with the existing Frontline software data views, such as **Main windows, Bluetooth Timeline**, etc. to expedite the root-cause analysis of *Bluetooth* protocol related audio issues. When a frame is selected in any Frontline software data views, the corresponding audio data associated with those frames is also selected in the Wave Panel, Event Timeline and Event Table and vice-versa.

Protocol analysis tools synchronized to the Audio Expert System™ include:

- **Main windows**
- **Coexistence View**
- **Bluetooth Timeline**
- **Message Sequence Chart**
- **Packet Error Rate Statistics**

When a portion of the waveform is selected in the Wave Panel, all frames within the selection will be highlighted in the **Main windows**, **Coexistence View**, and **Bluetooth Timeline**.

**Note:** If the **Main windows** is filtered to show non-audio events then the frames associated with selected audio events may not show.

## 5.7 Timing Analysis

The **Timing Analysis** provides a display and measurement tool for logic signals captured using the Soderia HCI pods and HCI UART, SPI, and USB data. In addition, the view can include graphical display of Classic *Bluetooth*, *Bluetooth*, Low Energy and Wi-Fi packets. The packets are displayed simultaneously and time synchronized with captured logic signals.

The **Timing Analysis View** is shown in bottom left corner of WPS main window. In case it was closed, the **Timing Analysis View** can be open from menu **View**

The **Timing Analysis** displays signals/protocols available to the **Main windows**. This means you will see only the recorded data for devices in the X240 / Soderia **Wireless** and **Wired** panes selected for analysis and for *Bluetooth* technologies selected in the **Record Options Wireless** and **Wired** tabs. If the data filter changes due to changes in device selection and/or technology selection, the **Timing Analysis** display will refresh with the next analysis.

**Note:** Filters applied in the **Main windows** do not apply to the signals/protocols displayed in the **Timing Analysis**.

See [Logic Event Capture Configuration on page 55](#), and [Record Options Dialog: X240 on page 107](#) procedures for configuring the Soderia HCI pod hardware and the Wireless Protocol Suite software. See [Soderia Logic Event Capture and Analysis on page 227](#) for information on logic capture, recording, and analysis procedures. See [UART Capture Configuration on page 54](#) for information on capturing UART. See [Connecting for USB Capture on page 55](#) for information on capturing USB.

See [Connecting X240 for HCI and Logic Capture on page 31](#), and [Record Options Dialog: X240 on page 107](#) procedures for configuring the X240 Logic Analyzer pod hardware and the Wireless Protocol Suite software.



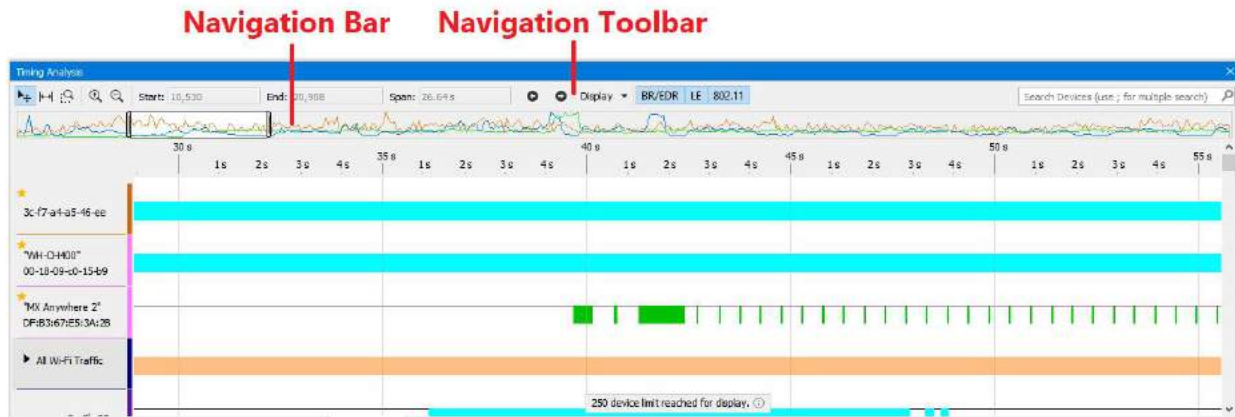


Figure 5.113 - Timing Analysis Window

The **Timing Analysis** window has three major areas:

- Navigation Toolbar - provides tools for positioning, displaying, filtering and measuring elements in the Timeline View.
- Timeline View- Displays the logic signal waveform, the packets, and measurements.
- Navigation Bar - Contains a viewport that represents the range of the Timeline View. Timing cursor timeline locations are represented in the Navigation Bar.

**Acknowledgment:** The Frontline Logic Analyzer contains features utilizing the Qt open source library, licensed under LGPL. To obtain the utilized Qt library source code , please contact Teledyne LeCroy [Technical Support](#).

### 5.7.1 Timing Analysis Navigation Toolbar

The tools control the display of the Timeline View. Detailed information on how to use the tools is contained in [Timing Analysis Timeline View on page 377](#).



Figure 5.114 - Timing Analysis Navigation Toolbar

Table 5.35 - Tools Pane Selections

Icon	Selection	Description
	Move Tool	In movement mode, the button allows you to move the timeline left/right by pressing the left mouse button and moving the mouse left/right respectively. This is default state.

Table 5.35 - Tools Pane Selections (continued)










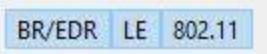

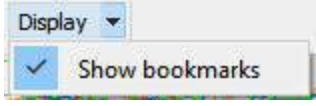
Icon	Selection	Description
	Timing	Places cursor in the timeline. A pair of cursors—left (X) and right (Y)—will display the time between them. Multiple pairs of cursors can be placed on the timeline. See <a href="#">Timing Cursors &amp; Measuring in Timeline View on page 385</a> .
	Zoom In	Clicking on these buttons will zoom the Timeline View in or out. The buttons will turn gray when the timeline display is zoomed to at either its maximum or minimum. See <a href="#">Zooming in Timeline View on page 383</a> .
	Zoom Out	
	Zoom Box	This button toggles between enabling and disabling the zoom box mode. The zoom box allows you to zoom in or out by dragging your mouse around an area of the Timeline View. See <a href="#">Zooming in Timeline View on page 383</a> .
	Start Packet Number	Shows start packets which could be found in shown time range.
	End Packet Number	Shows end packets which could be found in shown time range.
	Time Interval	Displays shown in timeline view time interval.
	Move Backward	Scrolls the viewport across the Navigation Bar.
	Move Forward	
	Selector	Allows you to select technologies which will be shown in Timing Analysis view.
	Line addresses/names filtering	Allows you to filter lines in TA by addresses or Nicknames/Friendly names. Addresses delimiters (":", "-") will be ignored. User can input multiple addresses filters using ";". All filters will be applied using "or".

Table 5.35 - Tools Pane Selections (continued)

Icon	Selection	Description
	<p>Display menu</p>	<p>Allows user to show/hide bookmarks on Timing Analysis. By default, bookmarks will be shown. The state of menu item does not save between sessions.</p>


## 5.7.2 Timing Analysis Navigation Bar

The Navigation Bar spans the entire duration of the capture session from the beginning of the first packet or logic signal to the end of the last packet or logic signal. Within the Navigation Bar viewport appears that represents the visible Timeline View . The viewport is a moveable and resizable slider.



Figure 5.115 - Timing Analysis Navigation Bar

Within the Navigation Bar you will see

- The viewport, which is discussed in detail below.
- Timing cursor markers placed in the timeline using the Timing button in the Navigation Toolbar . See [Timing Analysis Navigation Toolbar on page 373](#). When a measurement is set the Navigation Bar will display  at each location of a timing cursor.

**Note:** Technology filters applied in the Timing Analysis Navigation toolbar do not affect Navigation bar lines. Technology lines in the navigation bar will appear regardless of technology filter.

### Moving the viewport

By moving the viewport along the Navigation Bar you horizontally scroll the Timeline View. There are four methods for moving the viewport.

- Click on the Scroll left or right buttons on the Navigation Bar to move the viewport. The viewport will jump left or right respectively.
- Position the cursor inside the viewport ; the cursor changes to a hand. Hold down the left mouse button and drag the viewport along the Navigation Bar.
- Left click the mouse with the cursor outside the viewport but inside the Navigation Bar. The viewport center will jump to the cursor location.
- Use mouse while cursor is in the Navigation Bar.

### Expanding or Collapsing the viewport

Expanding or collapsing the viewport has the effect of zooming the Timeline View out or in, respectively.

- Position the mouse cursor over either the viewport's left or right edge; the cursor changes to a double-headed arrow ( $\leftrightarrow$ ). Hold down the left mouse button and drag the viewport edge to collapse or expand the viewport thereby zooming the Timeline View in or out respectively.

You can anchor the viewport to the beginning or end of the timeline.

- Position the mouse cursor inside the viewport; the cursor changes to a hand. Holding down the left mouse button, drag the viewport along the Navigation Bar to the left edge, which is time zero. Position the cursor on the viewport right edge and drag to expand or collapse the viewport.

- Position the mouse cursor inside the viewport; the cursor changes to a hand. Holding down the left mouse button, drag the viewport along the Navigation Bar to the right edge, which is the maximum time. Position the cursor on the viewport left edge and drag to expand or collapse the viewport.

Dragging the viewport edges has the same effect as using the Timing Analysis zooming tools. When you use the zooming tools the viewport will expand when zooming out or collapse when zooming in. See [5.7.1 Timing Analysis Navigation Toolbar on page 373](#)

### 5.7.3 Timing Analysis Timeline View

Timeline View displays captured logic signals, Classic *Bluetooth*, *Bluetooth* Low Energy, Wi-Fi and HCI packets. The signals and packets are synchronized and displayed on a horizontal time axis. The amount of time displayed in the view is controlled by the Navigation Bar viewport. As the viewport expands, more of the timeline is displayed and the signals and packets will compress. Conversely, as the viewport collapses—gets smaller—less of the timeline displays and the logic signals and packets will expand.

Each signal or packet set displayed in the Timeline View appears on a single row. All logic signals, *Bluetooth*, Wi-Fi and HCI UART/USB packets available in the **Main windows Unfiltered** tab will appear in the Timeline View from both live capture and a capture file.

**Note:** Filters applied in the **Main windows** do not apply to the signals/protocols displayed in the **Timing Analysis**.

Each Timeline View protocol row contains the packets from a single source device selected for analysis from the Device Database or Wired Devices views. If a *Bluetooth* device cannot be determined, packets will be placed in an appropriate aggregate row— "BR/EDR Other" or "LE Other". Bluetooth packets have the following characteristics and information:

- Wireless packet width indicates the in-air duration. HCI packet width is computed assuming a bus rate of 12 Mbps that is 100% utilized (utilization is always less than 100%, but exact utilization is unknowable, so this method provides a reasonable approximation).
- Packet type.
- Frame number.

Wi-Fi packets have the following characteristics and information:

- Packet width indicates the in-air duration.
- Wi-Fi frame type.
- Frame number.

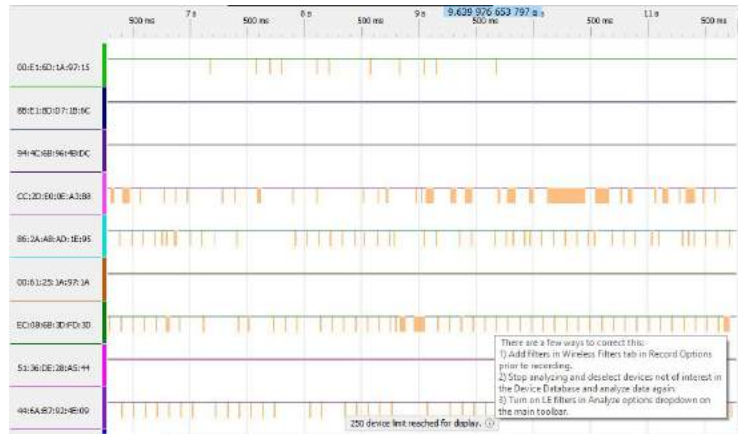


Figure 5.116 - Timing Analysis Timeline View

At the top of the Timeline View is a time scale. its time range is the time span of the viewport. The Timing Analysis view shows 250 devices maximum. Information label with hint will be shown at the bottom of TA view if there are more devices in analyzed traffic.

**Row Label**



HCI POD 1 (H440)

08:96:AD:0B:02:74

On the left of each row is a row label. There are two label categories: Soderia Wired capture (either logic, UART, or USB), and Wireless. The row labels are color coded for easy identification and the color carries through in the signal/packet timeline. [Timing Analysis Timeline Row Labels on page 379](#) provides details of the label format.

You can add and manage nicknames for the devices and signals. Please call the context menu in the left column next to the device address to open the editing window. The entered nicknames are synchronized with the Device Database panel.

Table 5.36 - Timing Analysis Timeline Row Labels

Category	Type	Label	Source Connector
Wired	Logic	<HCI Pod#> : <Line#>	Pod 1 or Pod 2 Digital 1
		Where: Pod# = "Pod 1" or "Pod 2"	Pod 1 or Pod 2 Digital 2
		Line# = "Data 0"-"Data 1", etc.	
	UART	HCI POD 1 (Host)	Pod 1
		Message direction is from the host to the controller.	
		HCI POD 1 (Ctrl)	
		Message direction is from the controller to the host.	
		HCI POD 2 (Host)	Pod 2
		Message direction is from the host to the controller.	
	SPI	HCI POD 2 (Ctrl)	
		Message direction is from the controller to the host.	
		HCI POD 2 (Host)	Pod 2
Message direction is from the host to the controller.			
		HCI POD 2 (Ctrl)	
		Message direction is from the controller to the host.	

Table 5.36 - Timing Analysis Timeline Row Labels (continued)

Category	Type	Label	Source Connector
	USB	HCI USB 1 (Host) Message direction is from the host to the controller.	USB 1
		HCI USB 1 (Ctrl) Message direction is from the controller to the host.	
		HCI USB 2 (Host) Message direction is from the host to the controller.	USB 2
		HCI USB 2 (Ctrl) Message direction is from the controller to the host.	
Wireless	<i>Bluetooth</i>	A <i>Bluetooth</i> label is either a BD_ADDR (full or partial) or, if the address is not known, an aggregate label (“BR/EDR Other” or “LE Other”)	Antenna
	Wi-Fi	A Wi-Fi label is either a MAC address (full or partial) or, if the address is not known, an aggregate label “Wi-Fi Other”	

## Timeline

In the Timeline appears a representation of the captured logic signal or HCI UART/USB and *Bluetooth* or *Wi-Fi* packets. Synchronization of these timelines provides for a means of accurate timing analysis. The viewport and the zoom tools controls the amount of signals and packets displayed in the Timeline View. The larger the viewport—zooming out—the more of the captured range that is displayed, and the smaller the signals and packets will appear. As the resolution decreases, logic signals will become smaller and smaller until they become a gray-hash bar.

Decreasing the viewport size by zooming in will decrease the time duration covered by the timeline, and the signals will appear with greater resolution. Should a logic signal or signal be not differentiable from adjacent signals or packets they are displayed as a hash-bar. This ensures that all signals and packets are visible when the



timeline displays the complete capture session. [Figure 5.117 below](#) and [Figure 5.118 below](#) show examples of the same display in hash-bars and zoomed in to show the actual logic signals and packets in the same time frame.



Figure 5.117 - Example: Timeline View Hash-Bar at Low Resolution

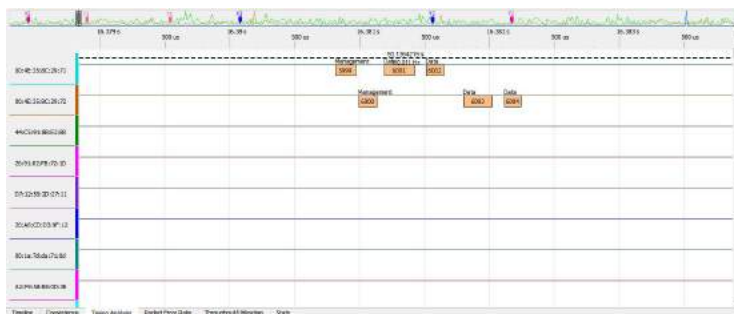



Figure 5.118 - Example: Timeline View at Higher Resolution, Zoomed In to same area.

### Repositioning the Timeline

The Navigation Bar viewport can be used to reposition the timeline, however this is best used for large changes to the view. For small changes to the view port, disable the Navigation Toolbar Zoom Box and click the mouse pointer anywhere in the timeline view. The cursor will change to a grabbing hand, . While holding the mouse left key down, move the timeline view.

At the top of the Timeline View is a time scale. The visible time range of the Timeline View corresponds to the time covered by the viewport.



When moving the cursor over the Timeline, a blue box appears just above the time scale. The time shown in this box is the time corresponding to the cursor position within the timeline.

To the right of the timeline is vertical scroll bar that is useful when displaying a large number of devices.

### Keyboard and Mouse Controls

Table 5.37 - Timeline View Keyboard Controls

Keys	Action
Left/Right Arrow	Moves timeline left/right. Equivalent to moving the viewport. If a packet is selected, then pressing Left or Right Arrow key will move selection to the previous or next packet.

Table 5.37 - Timeline View Keyboard Controls (continued)

Keys	Action
Up/Down Arrow	Scrolls timeline rows up/down. Equivalent to using the Timeline View scroll bar.
Up/Down Arrow + Ctrl	Zooms timeline in/out. Equivalent to using the Navigation Toolbar Zoom In/Out buttons, or collapsing/expanding the viewport.
Page Up/Down	Pages the timeline left/right. Paging Up moves the timeline left side over to the right side, that is jumping to the left. Paging Down moves the timeline right side over to the left side, that is jumping to the right.
Home	Moves the timeline and viewport to the beginning of the capture.
End	Moves the timeline and viewport to the end of the capture.

Table 5.38 - Timeline View Mouse Controls

Keys	Action
Left Click on a packet	Selects the packet.
Scroll Wheel	Scrolls timeline left/ right
Scroll Wheel + Ctrl	Zooms timeline in/out. Equivalent to using the Tools Zoom In/Out buttons.
Scroll Wheel + Shift	Moves rows up and down. Equivalent to using the Timeline View scroll bar.

### 5.7.3.1 Logic Signals in Timeline View

A logic signal timeline is shown as a high/low representation of the captured signal. A high level appears beginning at the time when the captured signal transitioned from a low state up through the logic-high threshold voltage. The high state is shown at the row label top edge. The logic low state occurs when the captured logic signal transitions from a high state down through the logic-high threshold voltage. A logic low state is shown at the row label bottom edge. State transition is displayed as instantaneous.

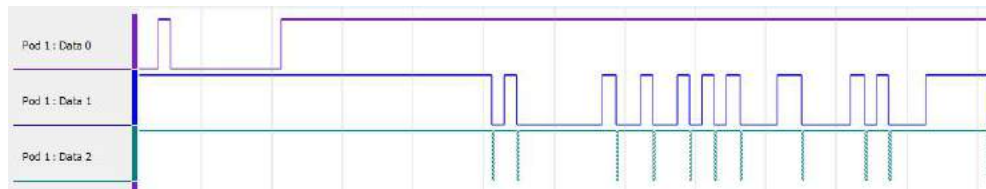


Figure 5.119 - Example: Logic State Transition

The high level threshold is determined by the HCI POD **LIO LVL** voltage. The minimum threshold voltage is 1.65 Vdc. Refer to [Logic Event Capture Configuration on page 55](#) for more information about the threshold level.

### 5.7.3.2 Bluetooth, Wi-Fi & HCI Signals in Timeline View

A protocol row in the Timeline View shows the packets associated with a single source device. The devices appearing in the row labels were selected for analysis in the Device Database or Wired Devices views.

The packets for each device appear as color-coded rectangles on the timeline.

Table 5.39 - Timeline Packet Color Codes

Category	Color	Description
Bluetooth	Blue	Classic <i>Bluetooth</i>
	Green	Bluetooth Low Energy
Wi-Fi	Orange	Wi-Fi frames
HCI	Purple	UART
		USB
Error	Red	Surrounding dashed line. Status errors, e.g. CRC or link errors.
Selected	Black	Surrounding line. Selected packet. Can result from selection in <b>Main windows</b> or one of the <b>Timeline</b> views.
802.15.4	Violet	802.15.4. frames

Packet information appearing on the rectangle is

- Packet type - Above the packet rectangle top border. HCI will show packet type and, for HCI ALC and SCO data, the source.
- Frame number - In the rectangle center.
- Frame selection - If a dashed yellow line appears surrounding the packet, that packet has been selected in either the **Main windows**, **Coexistence View**, **Bluetooth Timeline**, or **Bluetooth Low Energy Timeline**.

The length of the rectangle represents the *Bluetooth* or Wi-Fi packet in-the-air duration or the HCI packet duration.

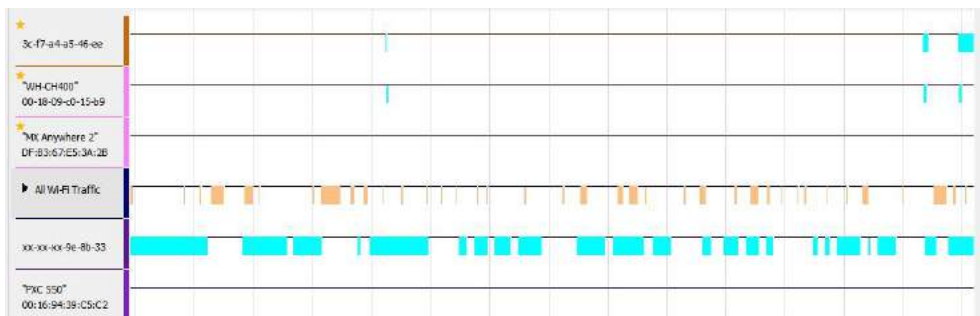



Figure 5.120 - Example: Timeline View Protocol Rows

The "All Wi-Fi traffic" row includes all Wi-Fi packets from all addresses available on Timing Analysis. This row can expand/collapse using the arrow icon on the row header. In the expanded state Wi-Fi rows are shown below the "All Wi-Fi Traffic" row. You can drag any devices out of this grouping for easier navigation and analysis. To do that, simply left click on the device of interest and drag it out to place anywhere in the left column.

### 5.7.3.3 Zooming in Timeline View

Zooming the timeline display in or out is accomplished using four methods:

1. Drag the edges of the viewport. The Timeline will expand or decrease with the size of the viewport. See [5.7.2 Timing Analysis Navigation Bar on page 376](#).
2. Enable the Tools Zoom Box , and then drag a zoom area with the mouse cursor.

**Zoom In:** After enabling the Zoom Box, click and hold anywhere in the Timeline. When the cursor changes to a "+", drag to the right and down and a box will appear along with text showing the start and end times of the box. Release the mouse key and the timeline will zoom in to the time range covered by the box.




Figure 5.121 - Zoom Box Tool - Zoom In


**Zoom Out:** After enabling the Zoom Box, click the mouse and hold anywhere in the Timeline. When the cursor changes to a "+", drag to the left and up and a box will appear with the start and times of the box. Release the mouse key and the timeline will zoom out.



Figure 5.122 - Zoom Box Tool - Zoom Out

3. Clicking on the Tools Zoom In and Zoom Out buttons.

**Zoom In:** Click on the Zoom In tool  and the displayed timeline's duration incrementally decreases.

**Zoom Out:** Click on the Zoom Out tool  and the displayed timeline's duration incrementally increases.

4. Hold down the keyboard Ctrl key and use the mouse scroll wheel to zoom in and out.

Zooming the timeline display in or out uses current mouse position as a zooming anchor point. If a packet or a group of packets are selected then zooming is performed to the center of the selection.

**Note:** The timeline view can be zoomed in to nanosecond resolution.

### 5.7.3.4 Timing Cursors & Measuring in Timeline View

The Logic Analyzer Timeline view provides a way to quickly see basic timing information by hovering mouse cursor over the timeline. When a user hovers mouse over a packet/signal or over a gap between two adjacent packets/signals, the following information is displayed along with gray dimension and extension lines:

- The *Duration* of the packet /signal
- The *Gap* between the end of the packet/signal and the beginning of the next packet/signal
- The *Delta* between the beginning of the packet/signal and the beginning of the next packet/signal
- The *Gap* between the end of the previous packet/signal and the beginning of the packet/signal
- The *Delta* between the beginning of the previous packet/signal and the beginning of the packet/signal

The following is true:  $Duration(\text{Current}) + Gap(\text{Current}, \text{Next}) = Delta(\text{Current}, \text{Next})$ ;

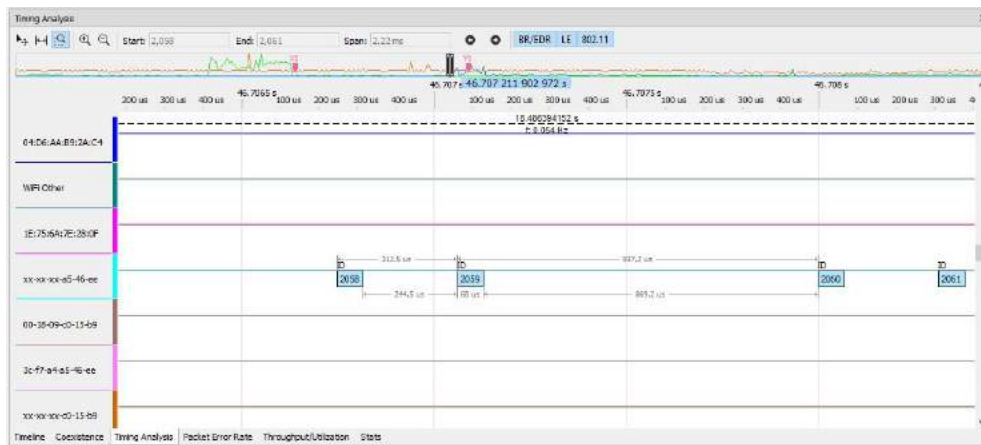



Figure 5.123 - Timing information on Logic Analyzer timeline

The timing information is not shown if a packet is displayed as a hash-bar at the current zoom level. Also, only gap between signals is shown if a signal is displayed as a hash-bar at the current zoom level.



Figure 5.124 - Signals timing information on Logic Analyzer timeline

An advanced method to perform timing measurements on Logic Analyzer is to use timing cursors. Using the Navigation Toolbar Timing button (see [Timing Analysis Navigation Toolbar on page 373](#)) you can place a set of left and right timing cursors on the timeline. The timing cursors provide a means to measure relative time differences between logic signals, packets, or both, or arbitrary positions on the timeline.

1. Enable the Timing button .
2. With the mouse cursor In the Timeline, click the left mouse button to place the left ("X") timing cursor.

- Then, anywhere in the Timeline, click the right mouse button to place the right ("Y") timing cursor. The time between the X/Y pair is displayed on a connecting line.

When the + cursor is near a logic signal transition or a packet right or left edge, a down-pointing triangle appears on the transition. Releasing the mouse when the triangle appears, results in the timing cursor snapping to the transition. If there is no snapping triangle, the timing cursor is placed at the location of the + cursor.

You can place multiple timing cursor pairs on the timeline. The timing cursor pairs are identified with subscript notation: X1/Y1, X2/Y2...Xn/yn. The timing cursor pairs are locked to the timeline and will expand or collapse with the timeline display.

Timing cursor X/Y pair tags appear at the top of the time scale and are color coded. Vertical lines extend from the tag through the timeline and the lines are color matched to their tags. Between the tag lines is a white dashed connecting line with the time span of the tag pair above the line, and the frequency of the time span (reciprocal of the time) below the line. If the Y-cursor is placed to the left of the X-cursor the time value will be negative, however, the frequency is the absolute time span reciprocal.

Timing cursors can be moved by positioning the mouse cursor over the timing cursor tag, holding and dragging the tag to a new position. When a cursor pair is selected the cursor tag color changes to white.

To remove the timing cursors, click on the red circle "x" in the cursor tag **X1** at the top of the timeline. Clicking in either the X or the Y tag will remove the X/Y cursor pair.

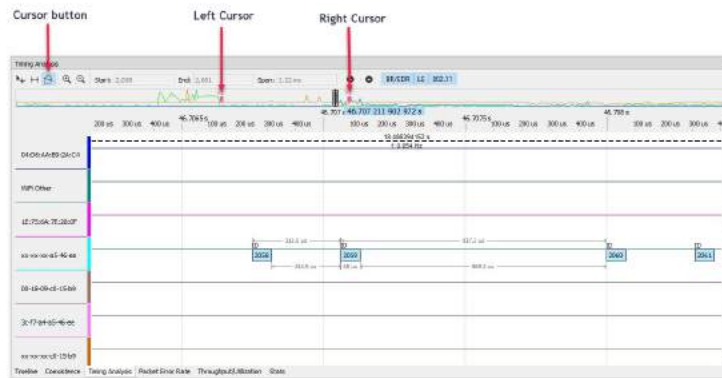


Figure 5.125 - Example: Timing Analysis Cursor Pairs

If you click on the cursor connecting time line a navigation bar appears. This bar is especially useful when both cursor are not visible within the Timeline View, such as when you have zoomed in; or for when there are multiple cursor pairs within the same view. Clicking on one of the navigation buttons moves a cursor into the Timeline View.

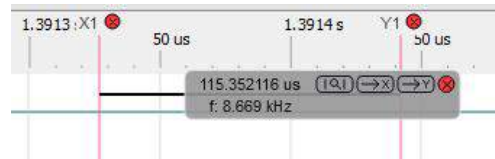






Figure 5.126 - Navigation Bar Time Measurement Cursor Markers

The following table provides a description of the navigation actions.

Table 5.40 - Cursor Timeline Navigation Bar Buttons

Button	Description/Action
	Search for Cursor Pair: Adjusts the Timeline View to display both the X- and Y-cursor. The cursors are centered around the middle of the Timeline View.
	Search for X-Cursor: scrolls the X-cursor to the middle of the Timeline View without changing the current range of the Timeline view.
	Search for Y-Cursor: scrolls the Y-cursor to the middle of the Timeline View without changing the current range of the Timeline View.
	Delete the Cursor Pair: Deletes the cursor pair without changing the current range of the Timeline View.

When a X/Y cursor pair is created, a marker appears in the Navigation Bar. The marker has the same color code as the cursor pair tags. This feature aids in quickly navigating to important parts of the capture time range.

### 5.7.3.5 Arranging Rows in Timeline View

#### Resizing

The Timeline View can be scrolled vertically by using the scroll bar on the right side of the view. Additionally the rows can be rearranged to aid in analysis and measurement. Click and hold the mouse cursor on a row label and drag it to a new position. A white horizontal bar will appear between row labels to indicate where the row you are moving will be dropped when the mouse key is released.

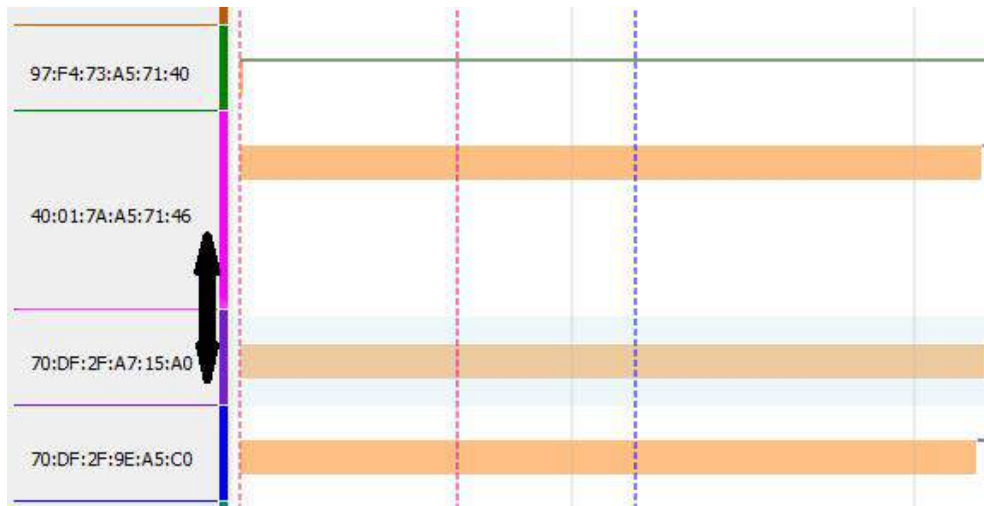


Figure 5.127 - Navigation Bar Time Measurement Cursor Markers

Rows can be resized by dragging the bottom of the row label. The row data also resizes with the row label.

## Positioning

Rows can be moved up or down to change the order. Click and hold anywhere in a row label. Drag the mouse cursor up or down the rows over the labels. A line with the same color as the row label that you clicked on will appear. Position the line where you want to move the row and release the mouse key. The row will snap to the new location.

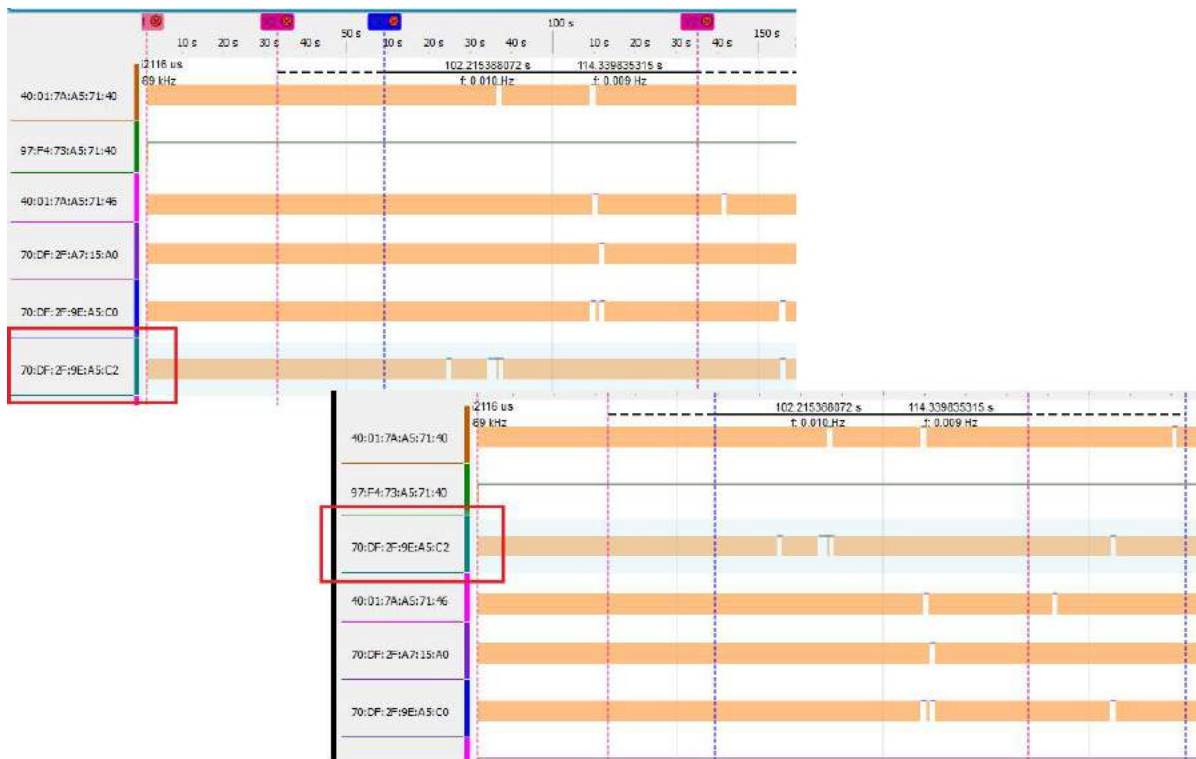


Figure 5.128 - Positioning Rows in the Timeline View

## 5.8 Protocol Stacks

### 5.8.1 Protocol Stack

You can define the protocol stack you want the analyzer to use when decoding frames.

From the Main window using any of the products described in this manual (Sodera and Sodera LE) select

**Options -> Decoders -> Protocol Stack...** and a menu with typical **Protocol Stacks** will pop up.



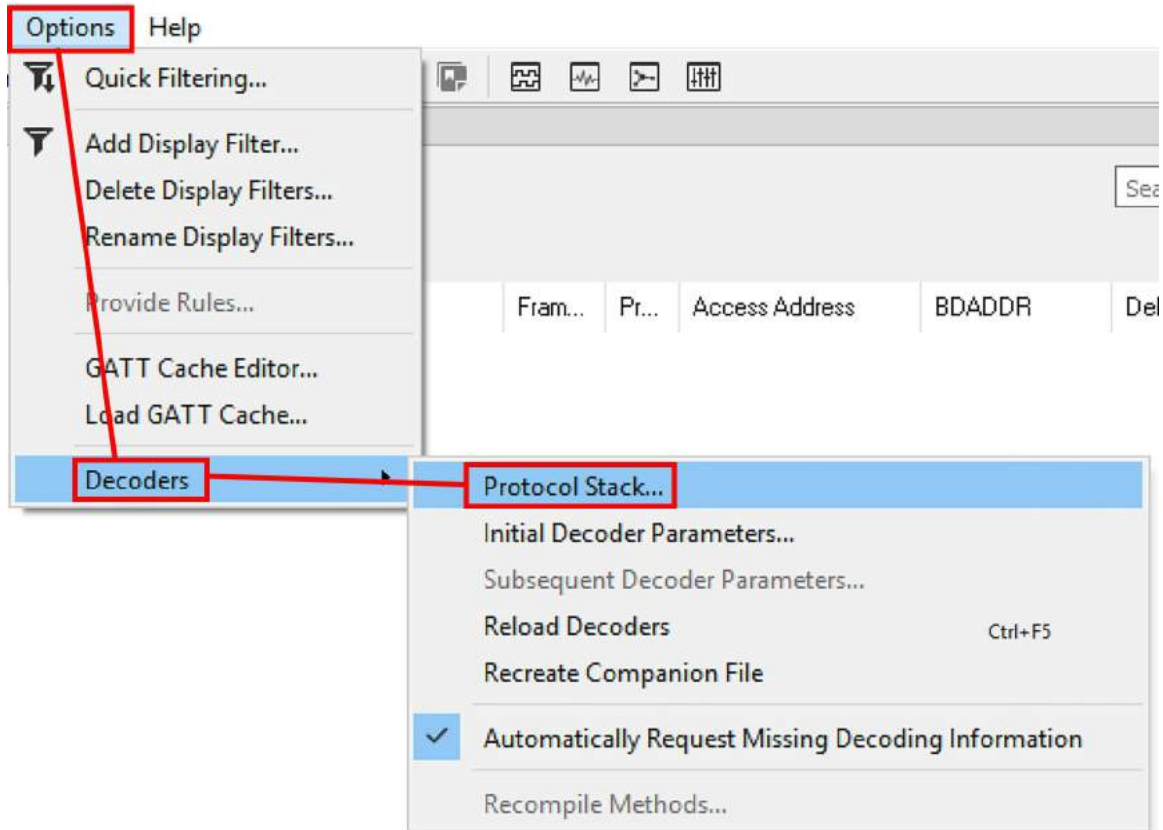


Figure 5.129 - Main window: Options -> Decoders -> Protocol Stack...

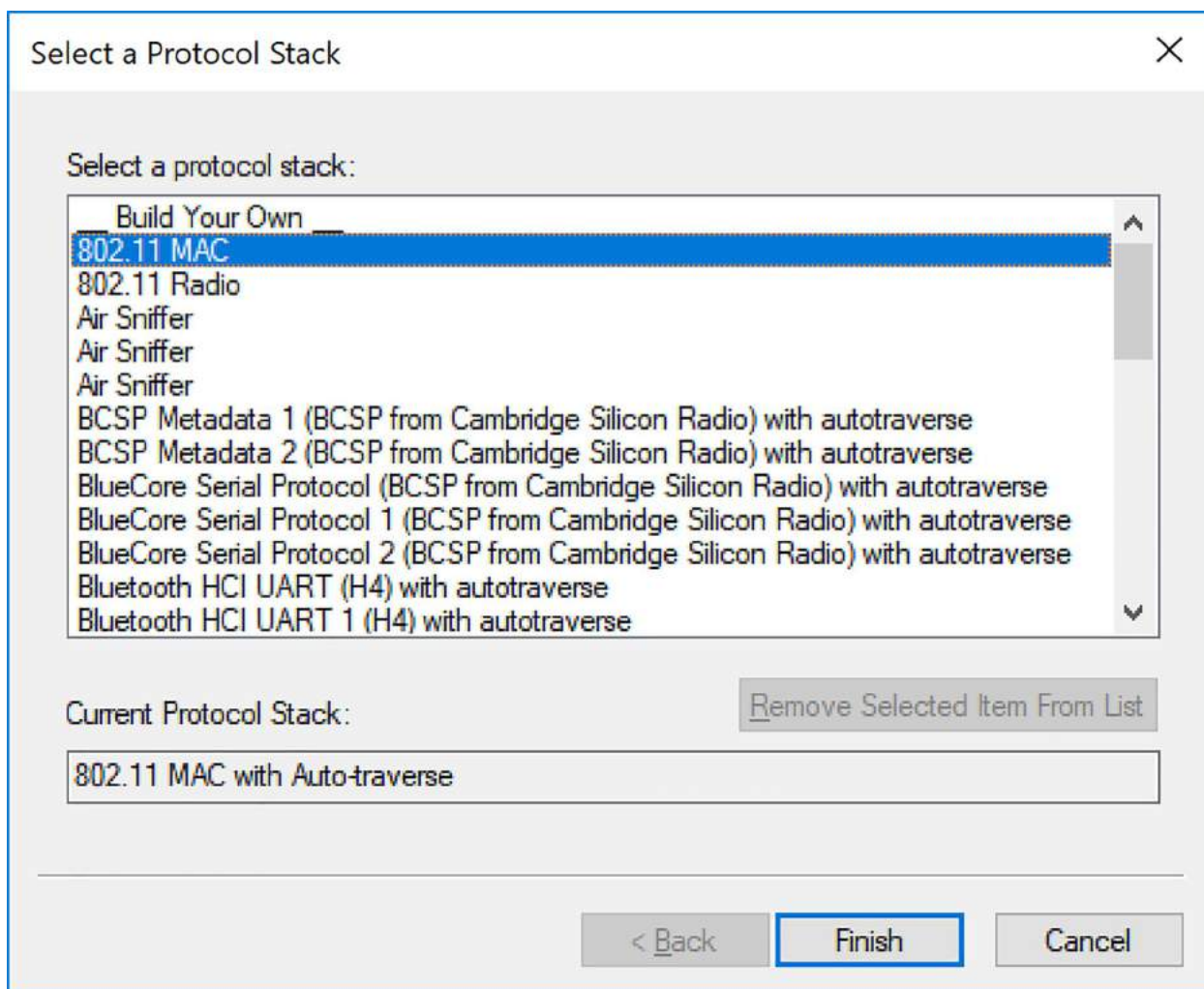


Figure 5.130 - Select Protocol Stack or Define Your Own

You can use a pre-defined **Protocol Stack** or you can define your own.

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

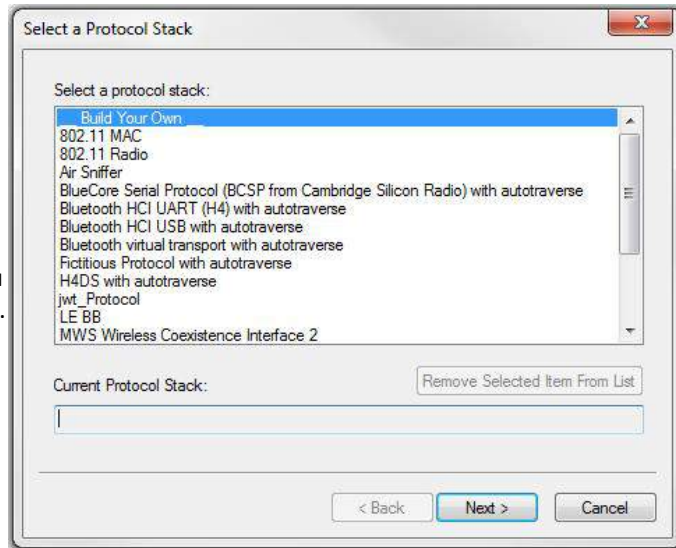
You cannot select a stack or change an existing one for a capture file loaded into the Main windows.

Protocol Stack changes can only be made from a live session.

## 5.8.2 Creating and Removing a Custom Stack

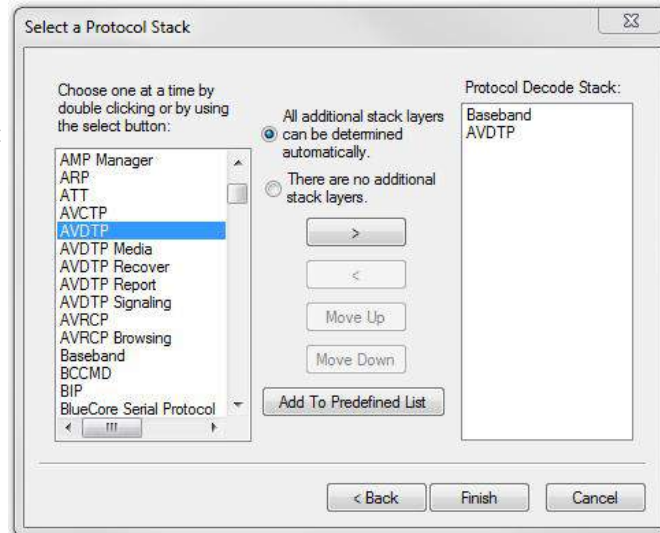
### To create a custom stack:

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



### Select Protocols

1. Select a protocol from the list on the left.
2. Click the right arrow button to move it to the **Protocol Decode Stack** box on the right, or double-click the protocol to move it to the right.
3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.
4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the **Move Up** and **Move Down** buttons until the protocol is in the correct position.



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

### Auto-traversal (Have the analyzer Determine Higher Layers)

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

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

### Save the Stack

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

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

### Remove a Stack

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

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

## 5.8.3 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.

## 5.8.4 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. 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 Summary View window.
2. Choose Provide <context name>.

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

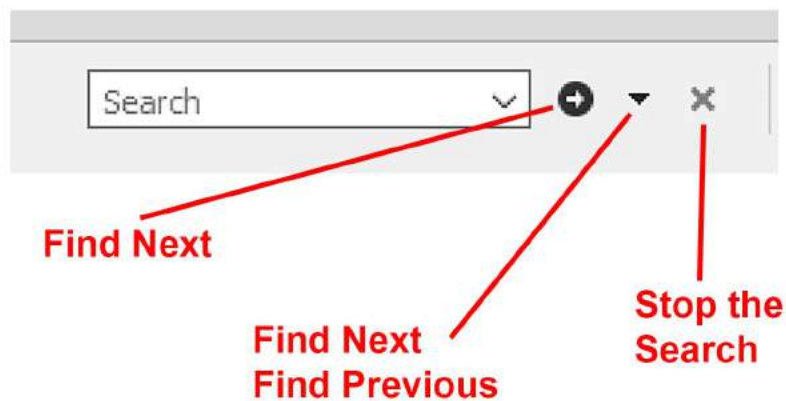
3. This option brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check **Automatically Request Missing Decoding Information**.
5. When unchecked, the analyzer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

## Chapter 6 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.

### 6.1 Searching

The **Wireless Protocol Suite** Analysis software has a simple **Search** function that you can use to search the Summary and Decode Panes for any alpha numeric value.



There is also a more complex **Find** function.

The **Find** function is located by selecting **Edit** -> **Go to** in the main Main windows menu, see below:

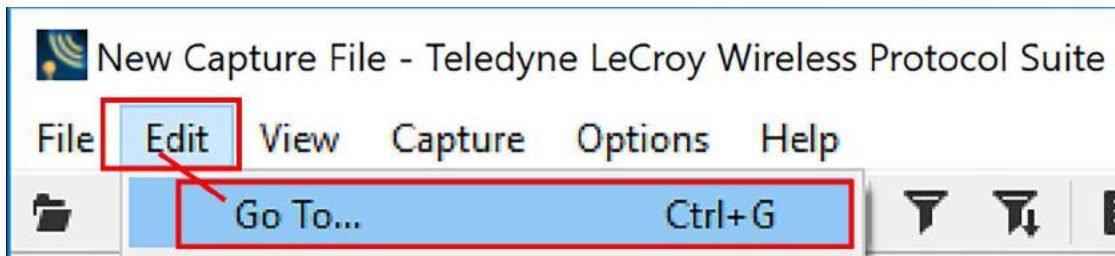


Figure 6.1 - Main windows Find text entry field

Where the more powerful **Find** functionality searches the **Raw Data**, **Go To** and **Bookmark** tabs. See figure below.

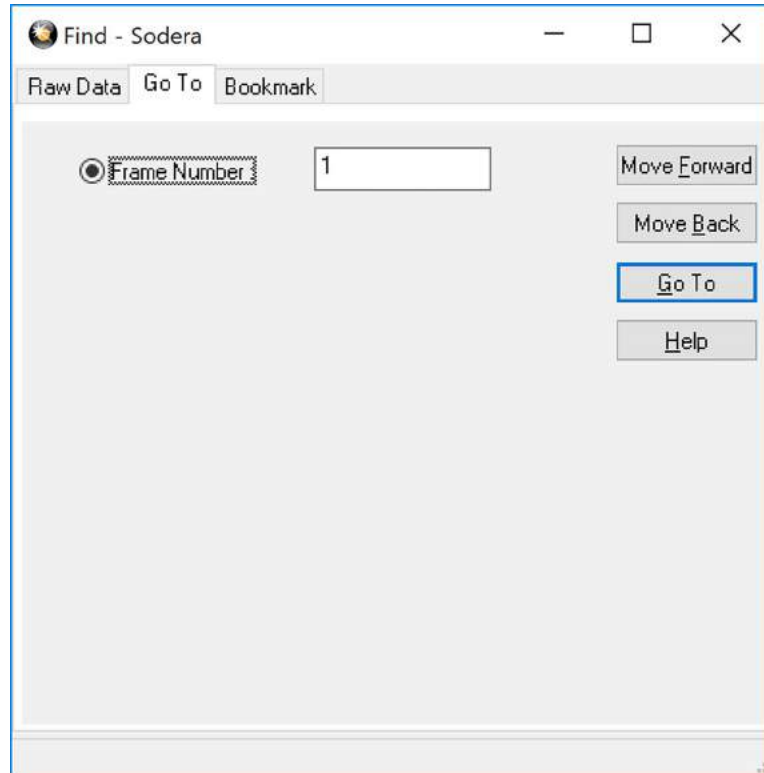


Figure 6.2 - Find Dialog: Go To

**Go To** searches for a **Frame** number in the **Summary** pane.

For each of these finds, upon finding a match, the frame found will be shown selected in the Summary Pane, and all the other frames will update as well to show their respective information about the selected pane.

The "Raw Data" find finds a user-supplied data pattern in the raw data bytes of a frame. The found bytes should be highlighted in the Raw Data pane.

The "Go To" find is a way for the user to jump to a specific frame by frame number.

The "Bookmark" find is a way to jump to a specific bookmark in the capture.

Select **Go To Move Forward** or **Go To Move Back** to continue the search.

The "Move Forward" and "Move Back" buttons appear to jump forward or back by the number of frames equal to the frame number the user entered in the dialog box. While "Go To" always jumps to the exact frame number provided.

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 **Move Forward**, 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.

- If you select **Move Back**, 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. You cannot search while data is being captured.
- After a capture is completed, you cannot search until Main windows 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. The search is canceled when you select a different protocol tab during a search
- You can cancel the search at any time by selecting the **Stop the Search** button.

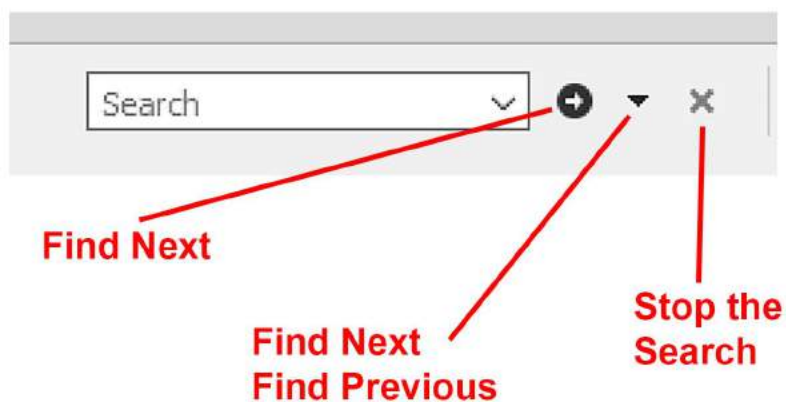


Figure 6.3 - Stop the Search Button



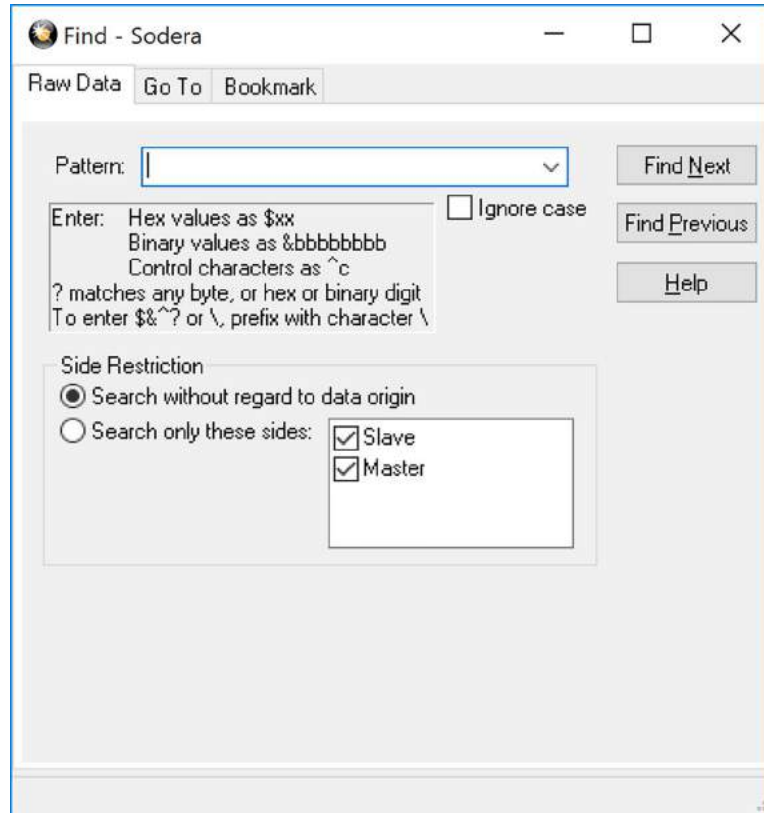


Figure 6.4 - Find Dialog: Raw Data

Raw Data 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 Wireless Protocol Suite analysis 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.

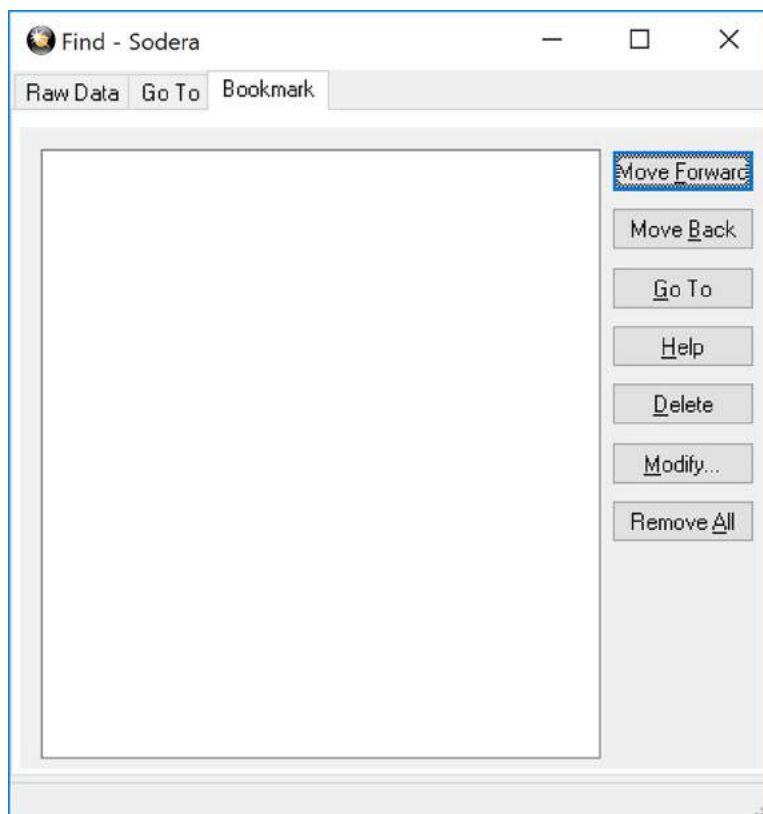



Figure 6.5 - Find Dialog: Bookmark

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.

## 6.2 Bookmarks

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

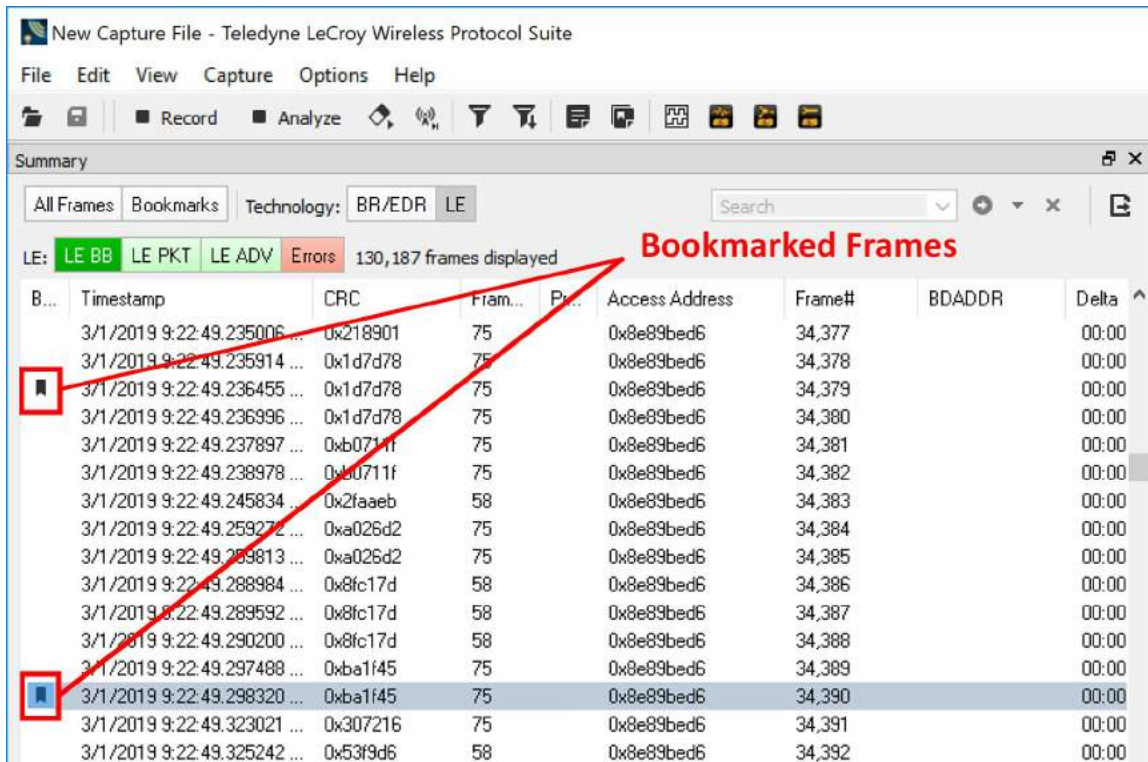


Figure 6.6 - Bookmarked Frame (3) in the Main windows

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 Bookmark Tab to [locate and move](#) among them.

### 6.2.1 Adding a Bookmark

You can add bookmarks from the **Summary pane**.

1. There are two ways to **Add a Bookmark** .

**Select Edit -> Add Bookmark** from the Main windows toolbar as shown below:

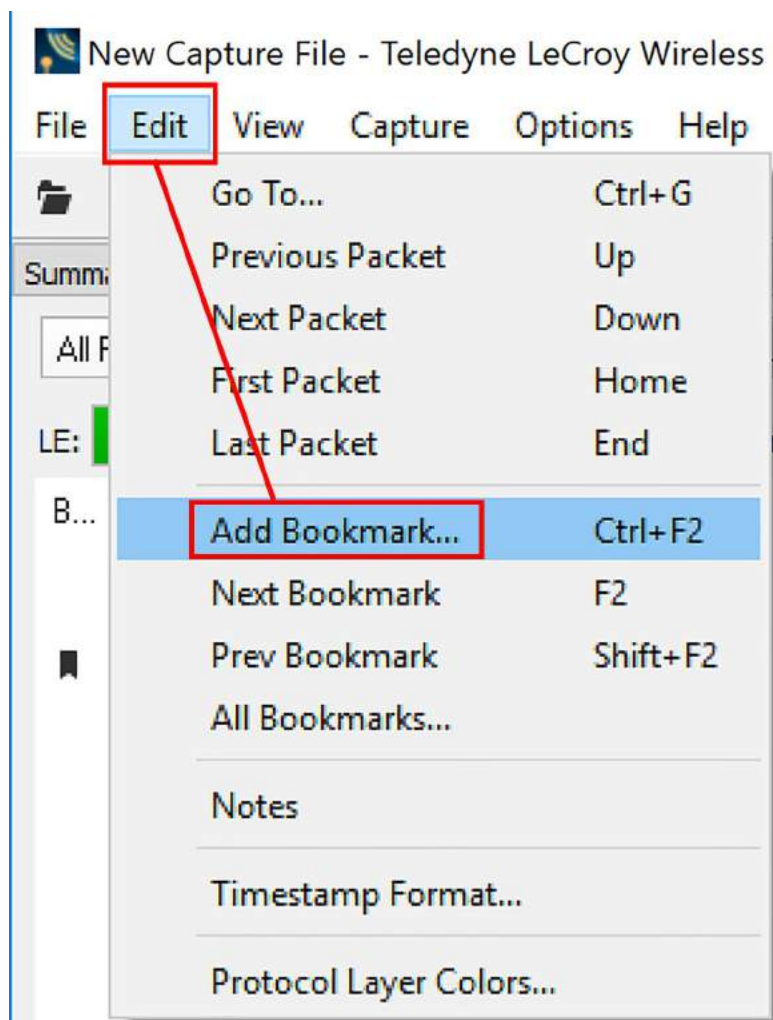


Figure 6.7 - Edit -&gt; Add a Bookmark

Or select a frame and right click on the mouse. The same Add Bookmark dialog will pop up. See the figure below:

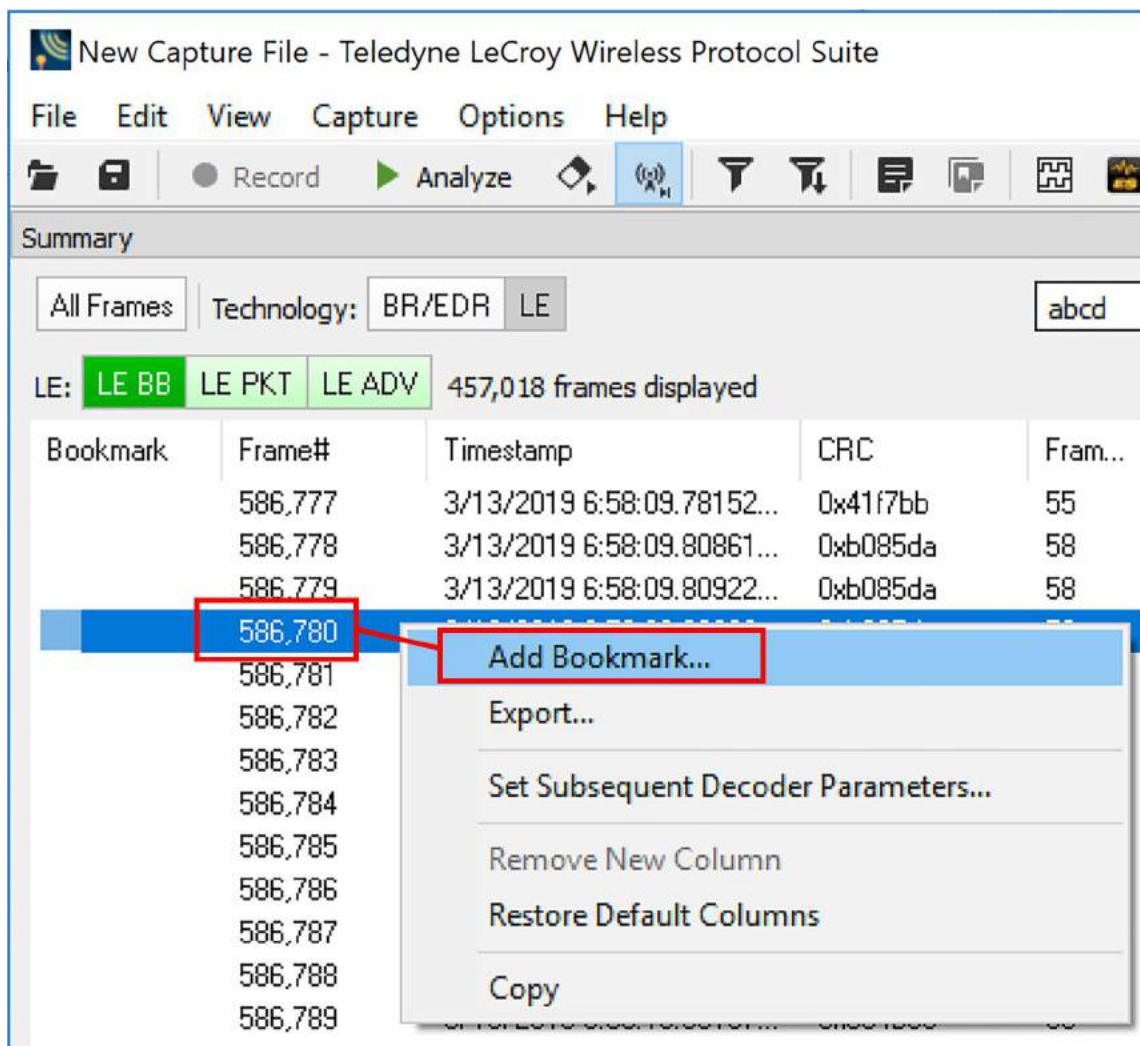


Figure 6.8 - Edit -> Add a Bookmark from Selected Frame

Either way will get you to the Add a Bookmark pop up dialog:

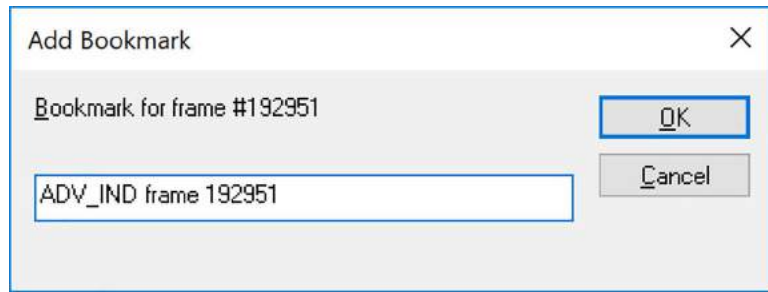


Figure 6.9 - Bookmark Pop Up Dialog

After you have generated several bookmarks you can select only the Bookmarked Frames by click on the Bookmark tab. See the figure below:

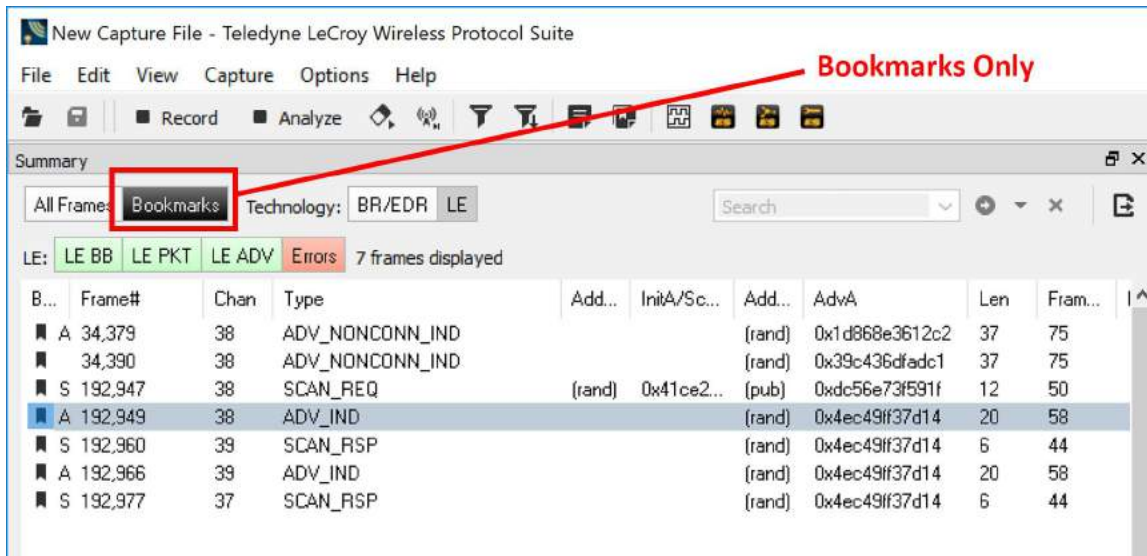


Figure 6.10 - Bookmark Only Frames Displayed

## 6.2.2 Showing Bookmarks on Views

Bookmarks appear on the Viewport and the Navigation Bars of LE/Classic Timelines, Coexistence, Throughput and Timing Analysis views. Also, Bookmarks appear on the Navigation bar of Stats view and Packet Error Rate view. If a packet is bookmarked, the bookmark shows up at the beginning of the packet. See [Figure 6.11](#) - for Bookmarks on Coexistence view, Timeline, Packet Error Rate and Stats view. See [Figure 6.12](#) - for Bookmarks on Timing Analysis and Throughput view.



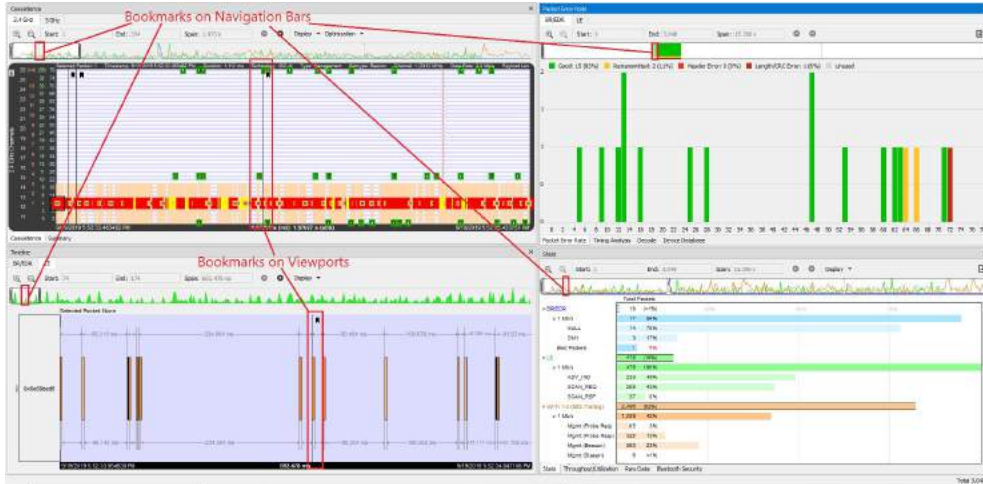


Figure 6.11 - Bookmarks on Coexistence view, Timeline, Packet Error Rate and Stats view.

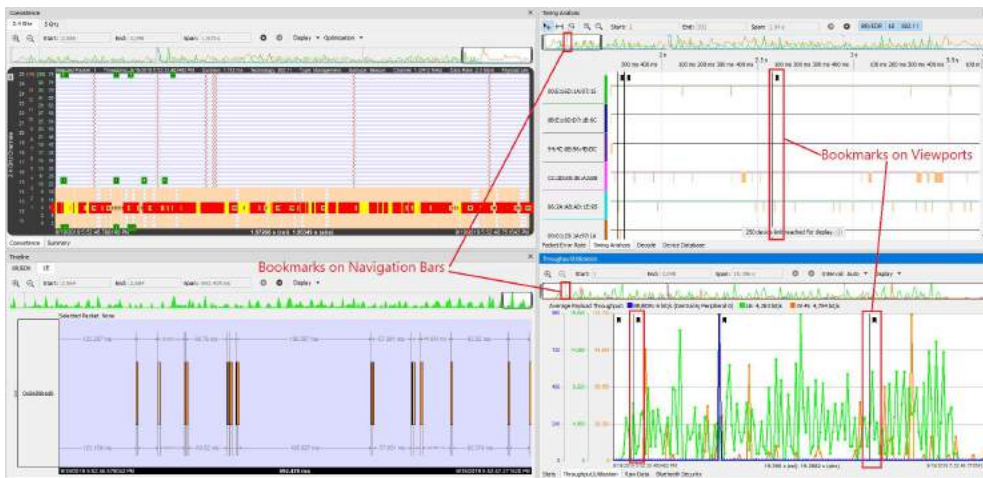


Figure 6.12 - Bookmarks on Timing Analysis and Throughput view.

The Classic and LE Timelines show bookmarks for the specific technology. All other views show bookmarks for all technologies.

The tooltip with general information about the bookmark (Bookmark name and the packet number the tooltip is assigned to) is displayed by hovering on the tooltip sign on viewport as shown in [Figure 6.13](#) - .

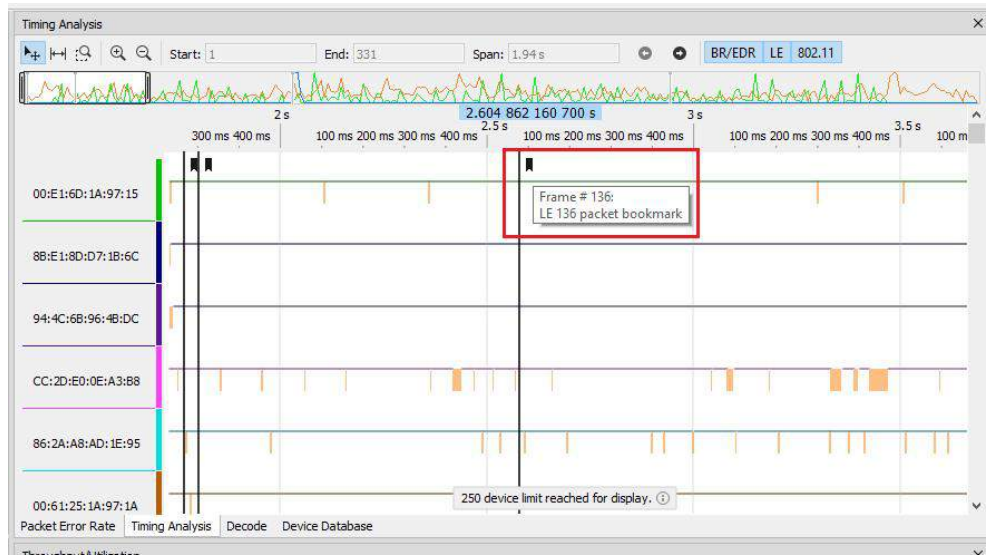


Figure 6.13 - Tooltip on Bookmark.



## Chapter 7 Saving and Importing Data

### 7.1 Saving Your Soder 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.


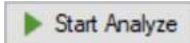

On the **Main windows** toolbar you can set up to capture a single file. [Click here to see those settings.](#)

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 to disk..](#)

#### 7.1.1 Saving the Capture File

Once your Soder capture and analysis is completed, you can save the captured file for future analysis. All data captured from start session (**Start Record**) to stop session (**Stop Record**) is saved.

Before saving the following conditions must be met:

1. Main Toolbar shows  .
2. Main Toolbar shows  .
3. In the Wireless Protocol Suite Application window, select **Save As f** from the File menu, or click on save icon  on the toolbar.

A **Save As** window will open. Select a location and enter a file name. Click on the **Save** button.

#### 7.1.2 Saving the Entire Capture File with Save Selection

1. Open the **Summary Pane** .
2. Right click in the data.
3. Select **All frames / Selected frames** and/or **All columns / Selected columns** from the right click menu.

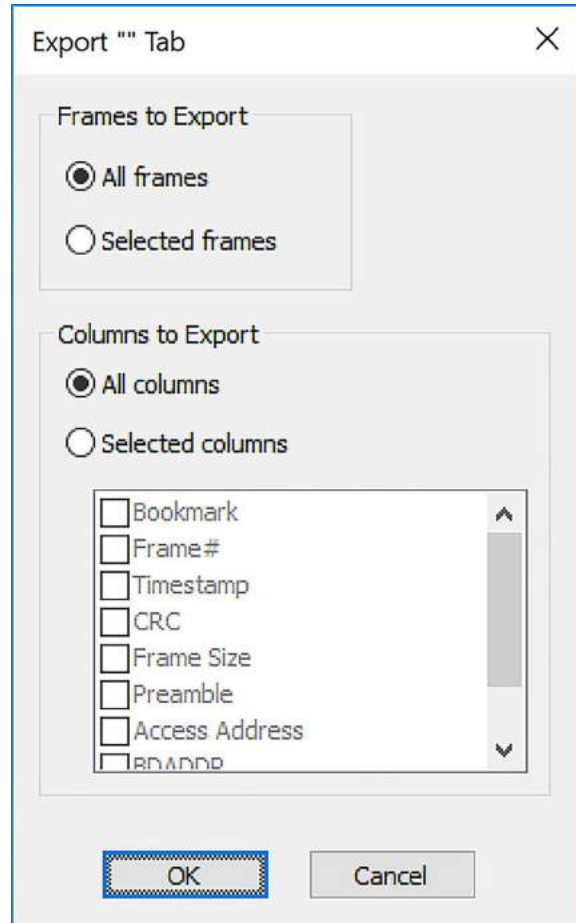


Figure 7.1 - Right Click -&gt; Export Dialog

4. Click on the radio button labeled **All frames** or **Selected frames**.
5. Click on the radio button labeled **All columns** or **Selected columns**
6. When you are finished, click **OK**.
7. If you select **All frames** and **All columns** the following dialog pops up to show you how long it will take to Save the file.

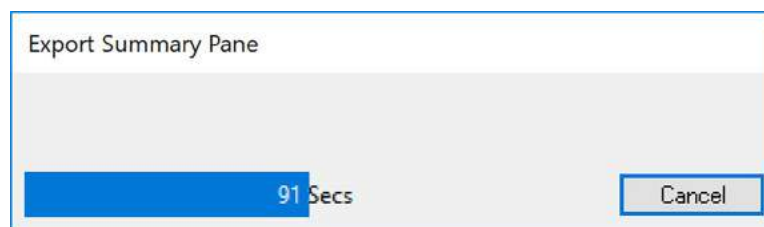
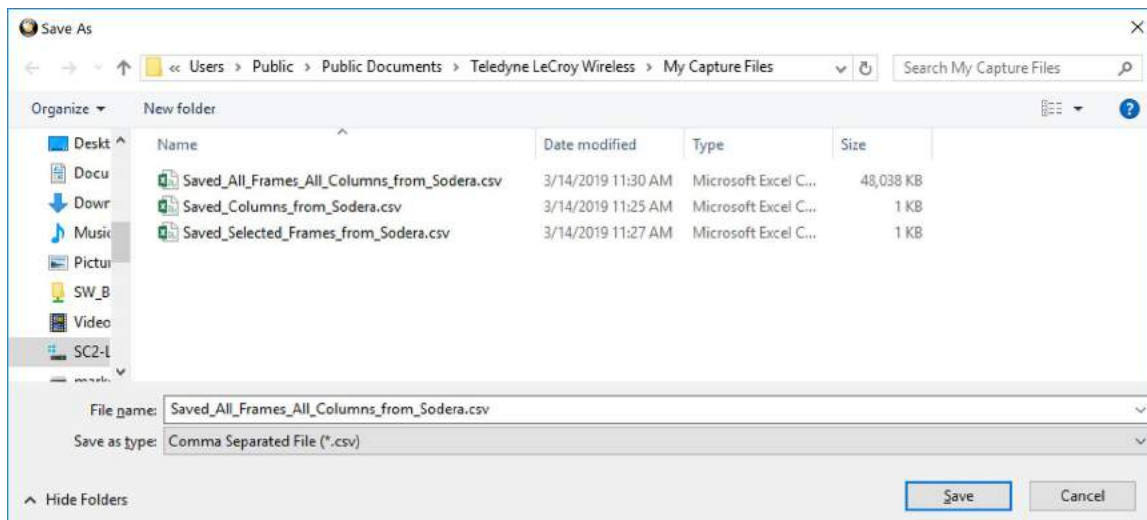


Figure 7.2 - Export Summary Pane

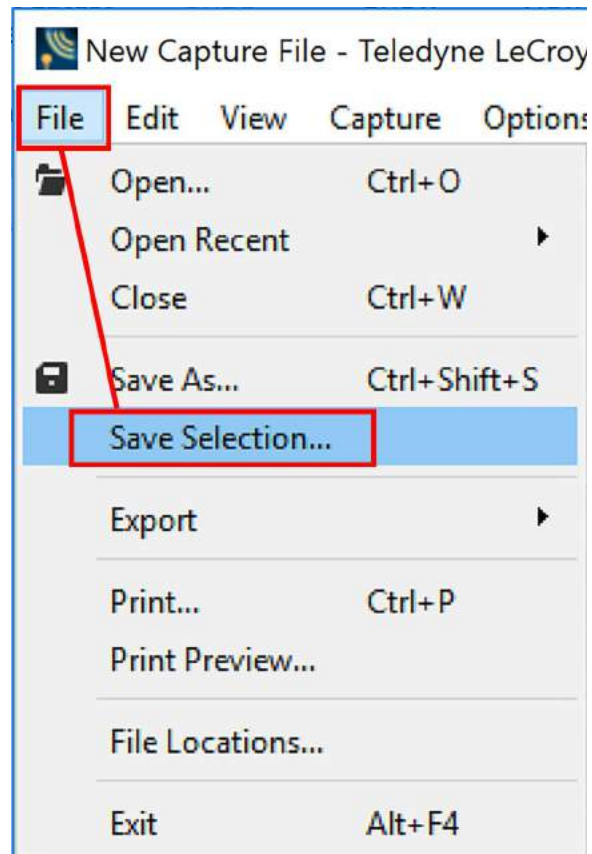
- When the export has been completed, a window with the path to the Save folder will be displayed.



- Type in the name of the file you want saved.
- Click on Save to store the file in the folder.

### 7.1.3 Save a Portion of Capture File with Save Selection

- Open the **Summary pane**.
- Select **File -> Save Selection**.



3. This will bring up the Save As dialog box.
4. 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 keyarrows or the navigation icons. If the range you want to save is too large to select, note the numbers of the first and last item in the range.

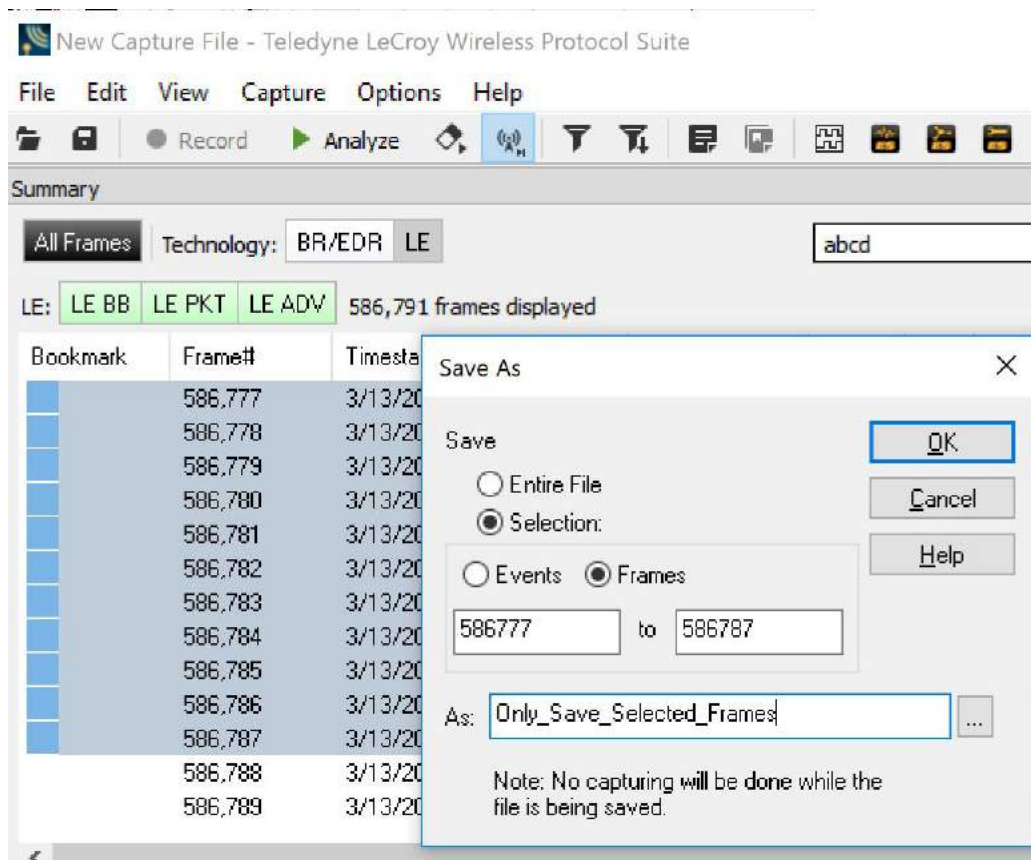
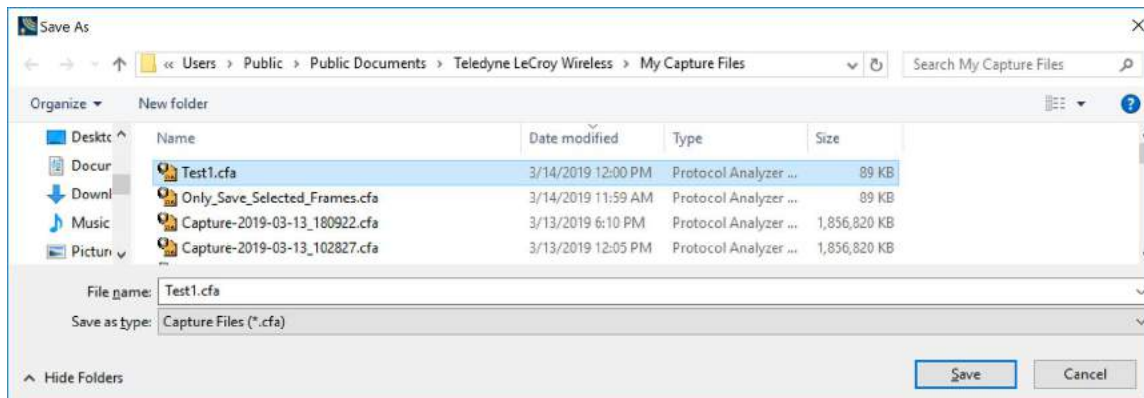


Figure 7.3 - Save As Dialog Box

5. In the Save As dialog box you can choose to save the entire file or select a range of events or frames to save.
6. You can also choose a file name for the frames you want to save.
7. Click on "OK" and a window will pop up showing you the path to the folder where you can save the file.



8. Type in a file name and click on Save.

## 7.2 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.)

1. Click the **Edit** tab in the toolbar, then select **Notes** option.

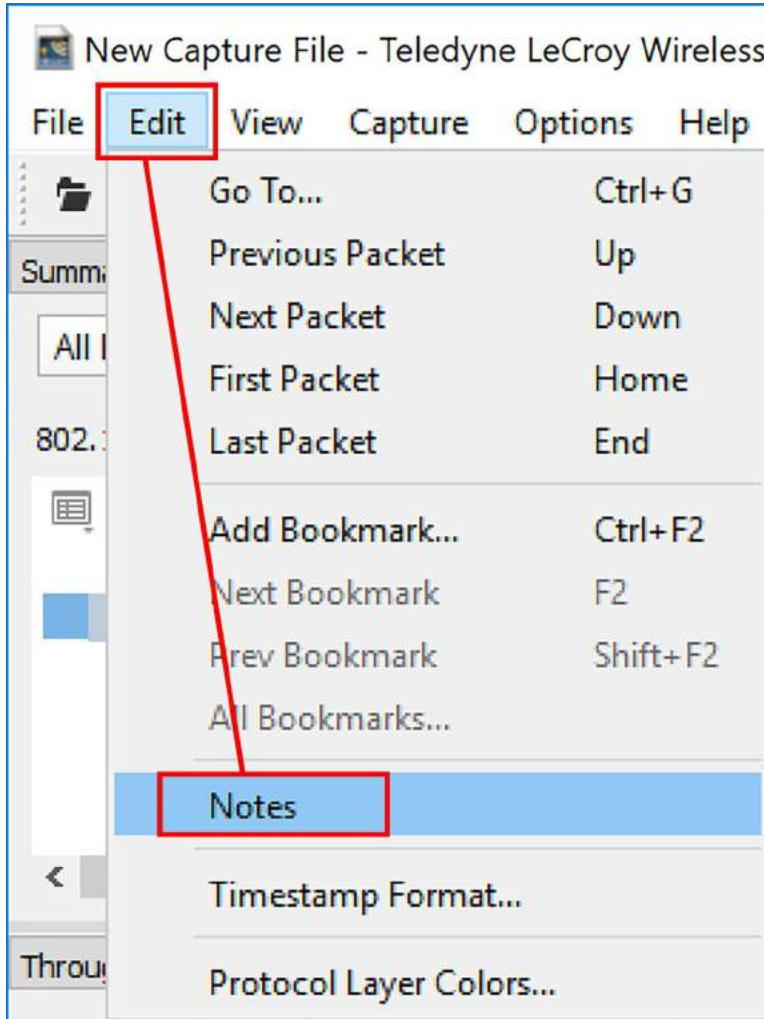
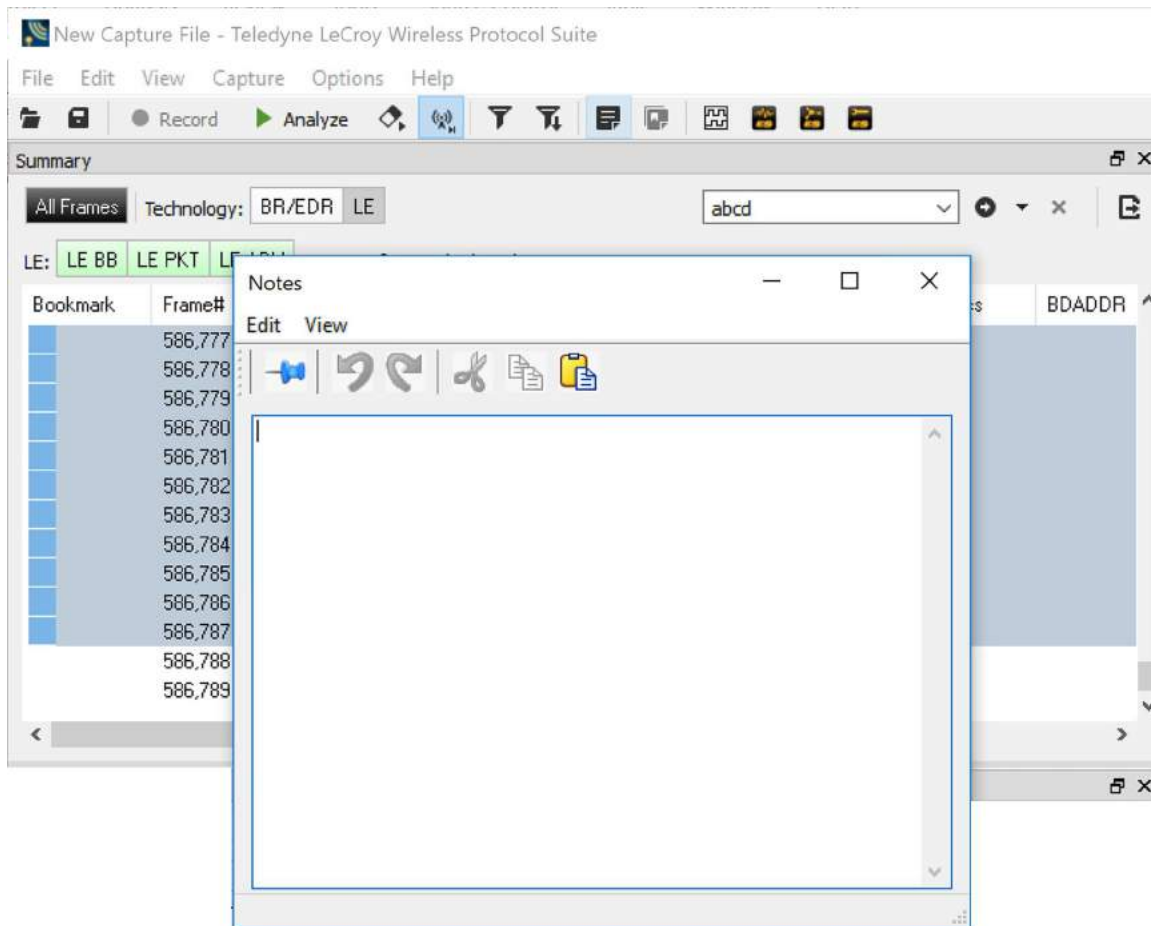





Figure 7.4 - Opening the Notes Feature

2. Another way to bring up the Notes Editor is to select the Notes icon in the toolbar and click on it.



3. 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.
4. Click the thumbtack icon  to keep the **Notes** window on top of any other windows.
5. When you're done adding comments, close the window.
6. 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.

### 7.3 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.

## 7.4 Loading and Importing a Capture File

### 7.4.1 Loading a Capture File

From the Main 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**.



## 7.4.2 Importing Capture Files

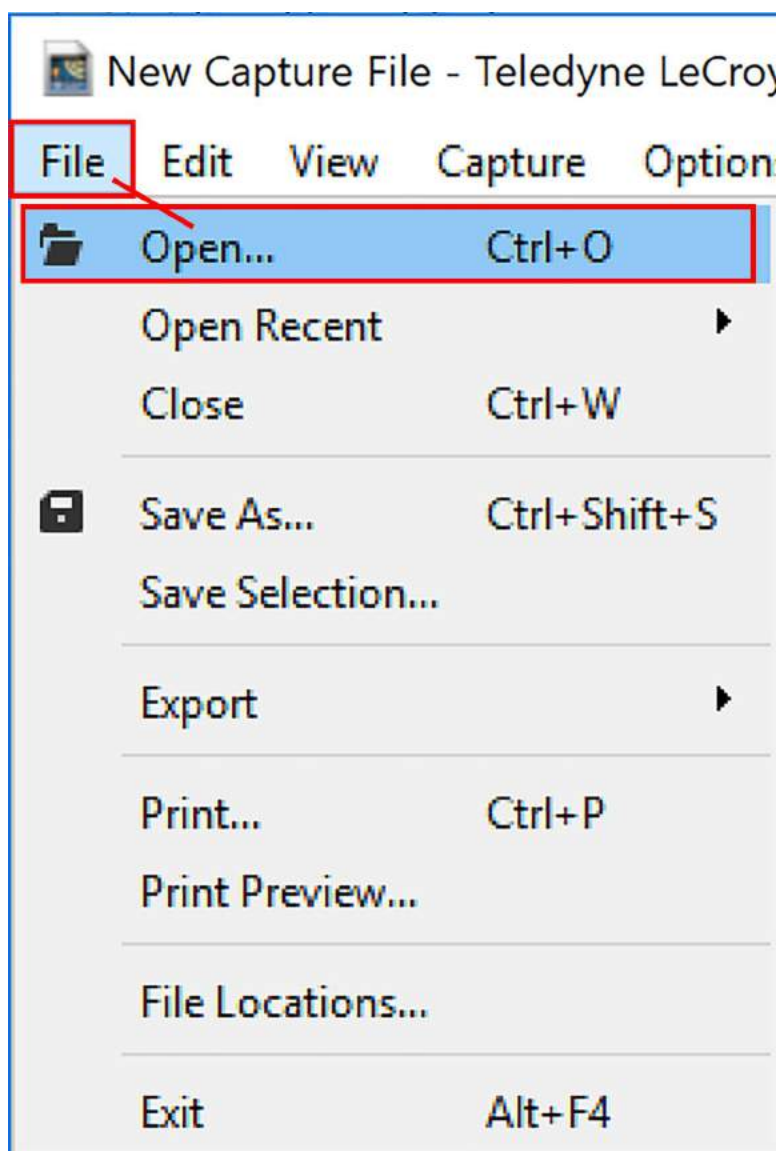


Figure 7.5 - Open a Capture File

1. Select **File** on the Toolbar then click on the **Open** option in the drop down menu..
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 Main window.

## 7.5 Printing

### 7.5.1 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.

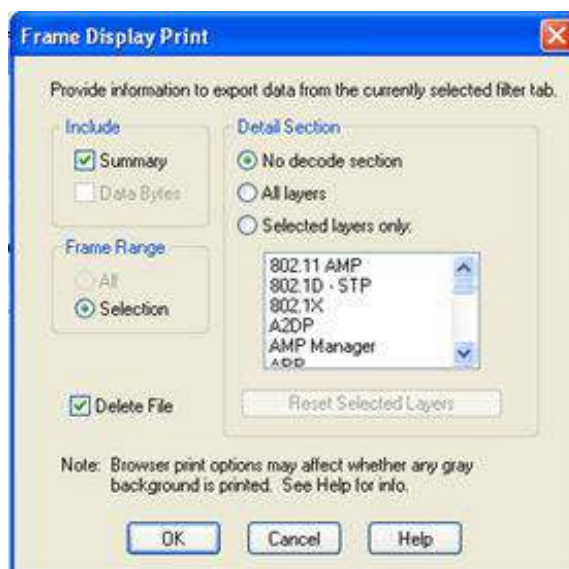


Figure 7.6 - Frame Display Print Dialog

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

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

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

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

### Frame Display Print Preview

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

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

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

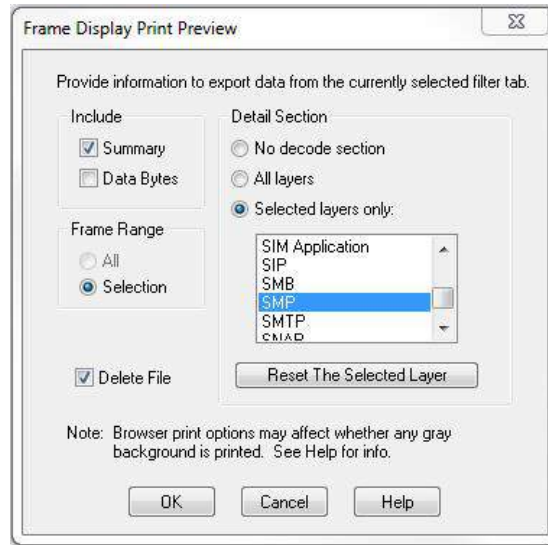


Figure 7.7 - Frame Display Print Preview Dialog

2. From this point the procedure is the same as steps 2 through 5 in "How to Print Frame Display Data" above.
3. Click the **OK** button, and after a brief wait a browser window will appear.

## 7.6 Exporting

### 7.6.1 Main windows - Byte Export

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

1. From the **File->Export** sub-menu select **Byte...** See figures below.

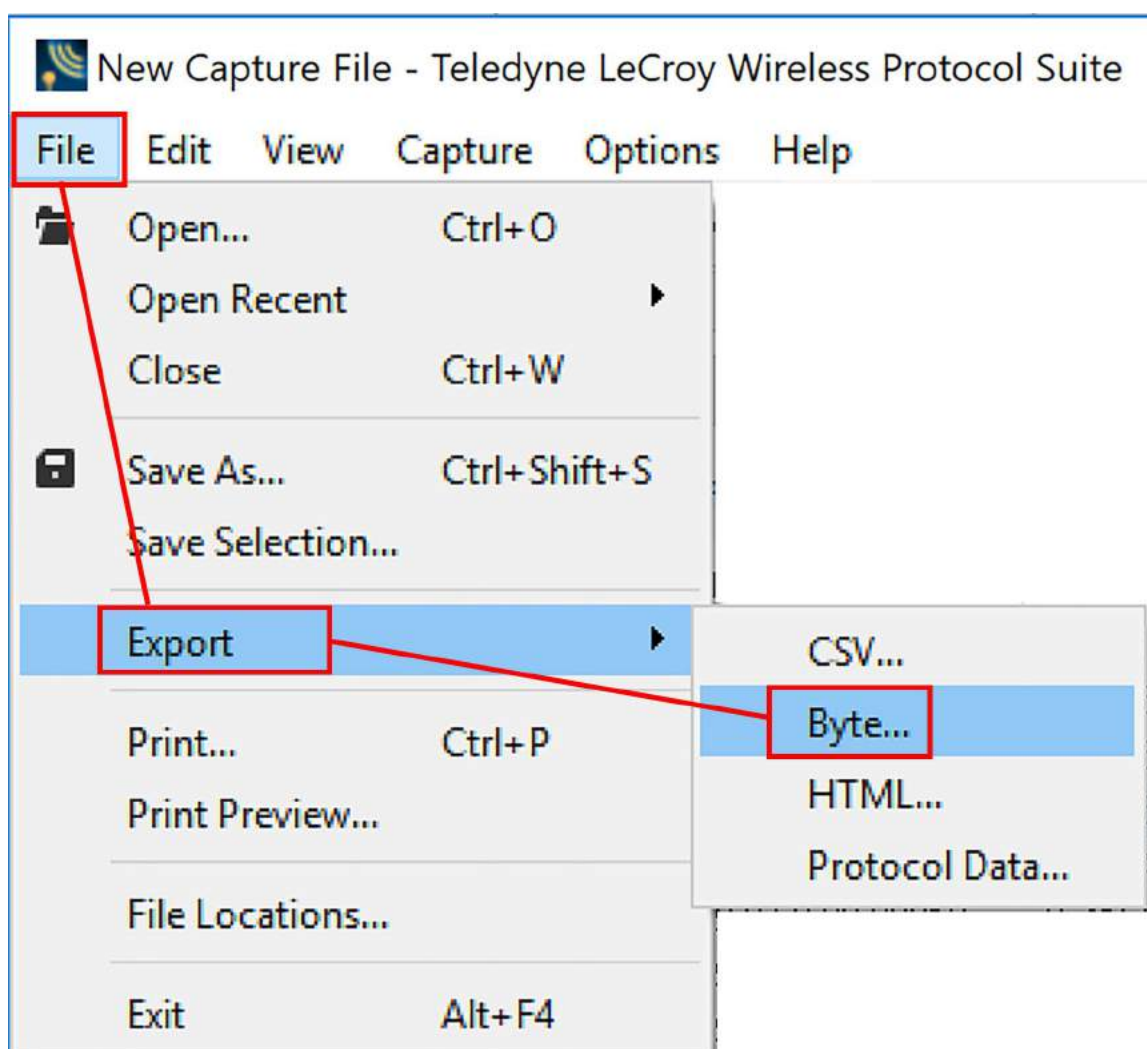


Figure 7.8 - Main windows File menu, Byte Export

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.

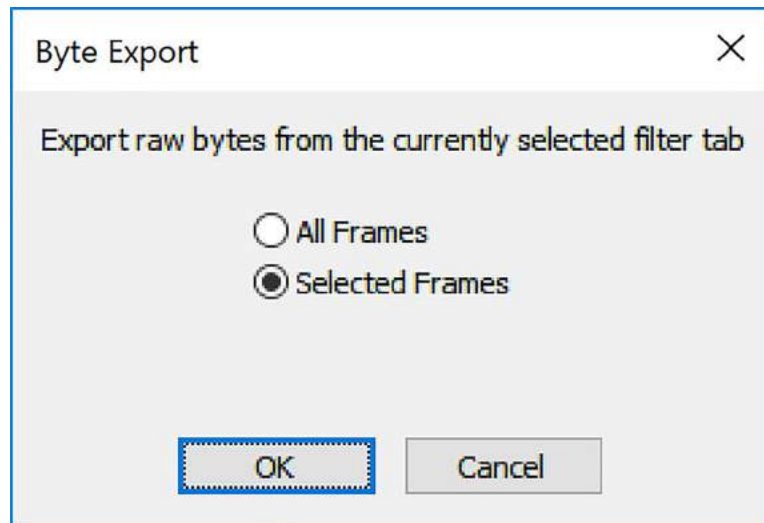


Figure 7.9 - Byte Export dialog

Click the **OK** button to save the export. Clicking the **Cancel** button will exit Byte Export.

3. The **Save As** dialog will open. Select a directory location and enter a file name for the exported frames file.

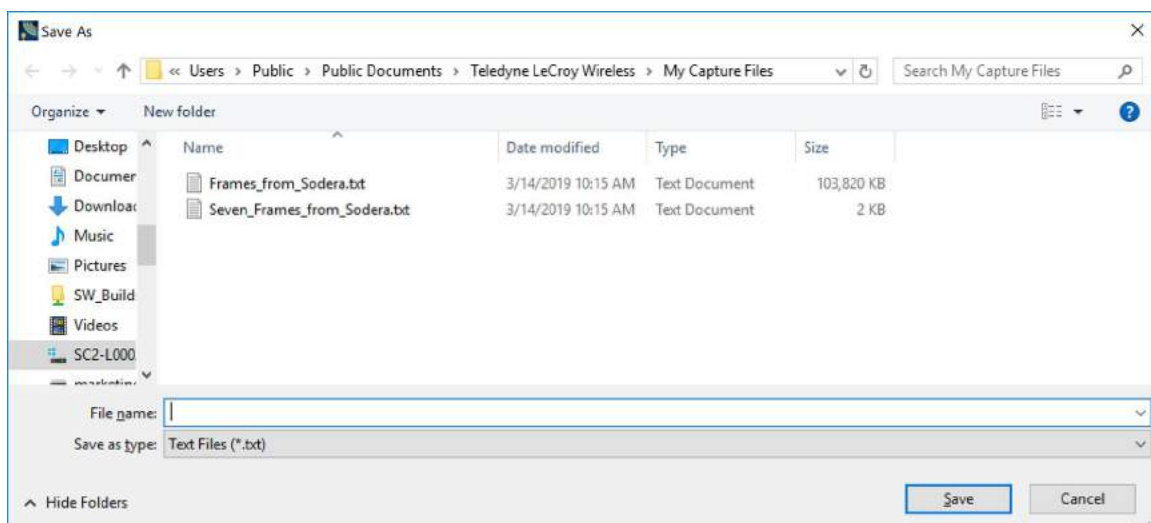
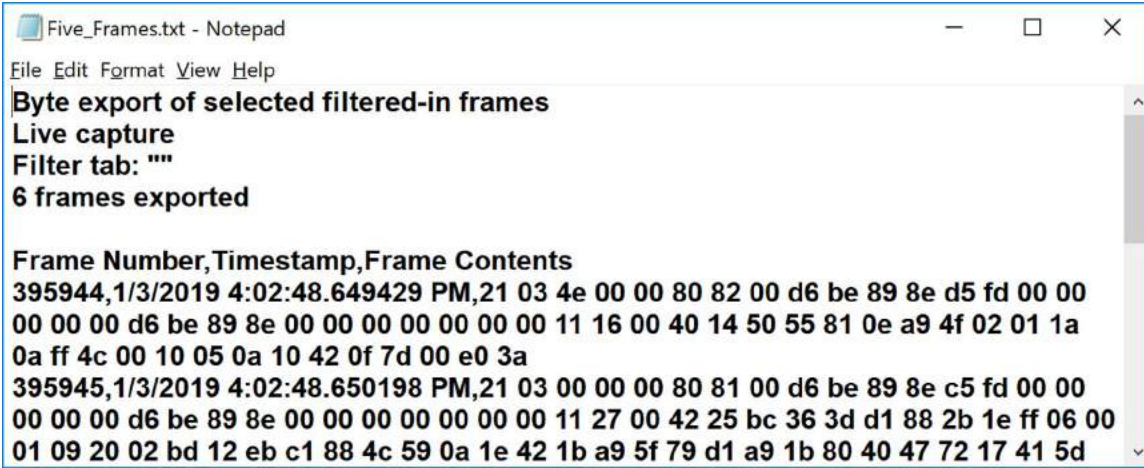


Figure 7.10 - Save As dialog

Click on the **Save** button.

The exported frames are in a text file that can be opened in any standard text editing application. The header shows the export type, the capture file name, the selected filter tab, and the number of frames. The body shows

the Frame Number, the Timestamp and Frame Contents in the same format shown in the **Summary** pane, and the frame contents as raw bytes.



```

Five_Frames.txt - Notepad
File Edit Format View Help
Byte export of selected filtered-in frames
Live capture
Filter tab: ""
6 frames exported

Frame Number, Timestamp, Frame Contents
395944,1/3/2019 4:02:48.649429 PM,21 03 4e 00 00 80 82 00 d6 be 89 8e d5 fd 00 00
00 00 00 d6 be 89 8e 00 00 00 00 00 00 00 11 16 00 40 14 50 55 81 0e a9 4f 02 01 1a
0a ff 4c 00 10 05 0a 10 42 0f 7d 00 e0 3a
395945,1/3/2019 4:02:48.650198 PM,21 03 00 00 00 80 81 00 d6 be 89 8e c5 fd 00 00
00 00 00 d6 be 89 8e 00 00 00 00 00 00 00 11 27 00 42 25 bc 36 3d d1 88 2b 1e ff 06 00
01 09 20 02 bd 12 eb c1 88 4c 59 0a 1e 42 1b a9 5f 79 d1 a9 1b 80 40 47 72 17 41 5d

```

Figure 7.11 - Sample Exported Frames Text File

## 7.6.2 Export

You can dump the contents of the **Summary** pane into a Comma Separated File (.csv). You have the option to select which frames and columns you would like to export from the currently displayed tab in Summary Pane.

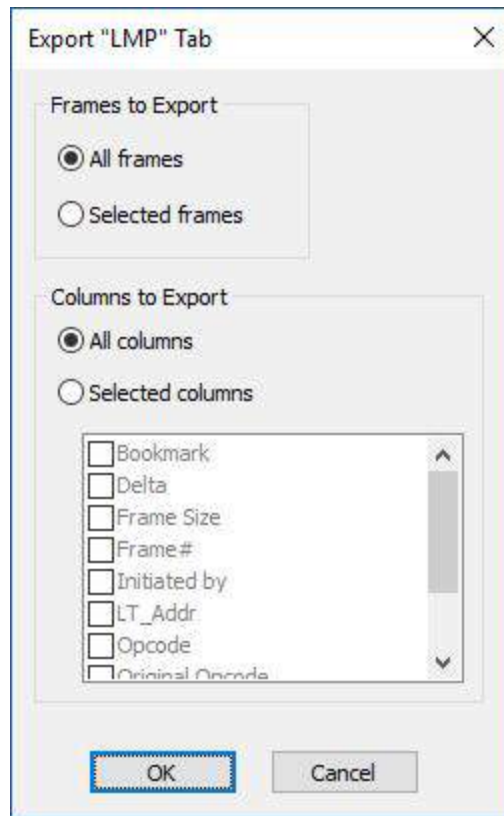


Figure 7.12 - Export Example

To access this feature:

1. Right click on the **Summary** pane or open the **File** menu.
2. Select the **Export...** menu item.
3. Select whether to export all frames or the frames currently selected.
4. Select whether to export all columns displayed or select the specific columns.
5. Select a storage location and enter a **File name**.
6. Select **Save**.

### 7.6.3 Export to pcapng Format

#### PCAPNG Export

The captured frames can be exported to a PCAPNG file.



1. From the **File** menu click **Export** then select **FPCAPNGI**.

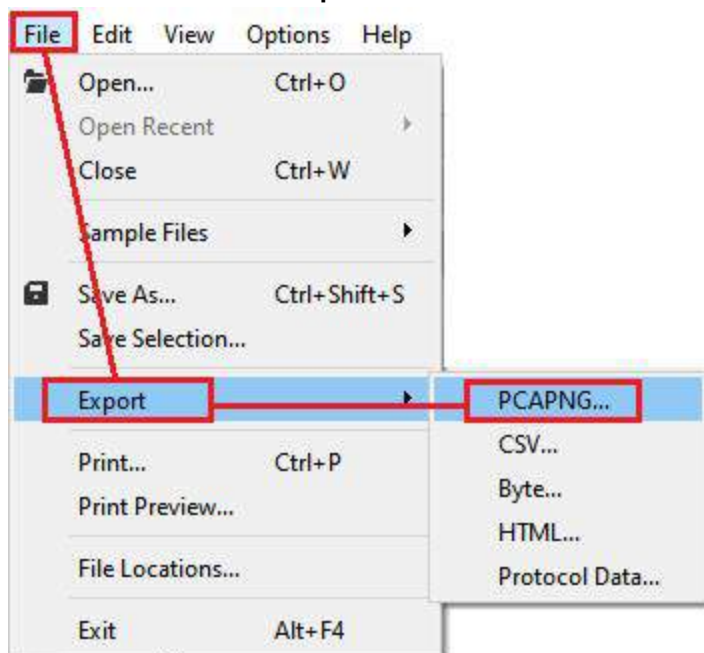


Figure 7.13 - File Menu, PCAPNG Export

2. From the **Export to PCAPNG** window specify the technologies to export. Currently only Bluetooth BR/EDR, LE, Wi-Fi and 802.15.4 packet conversion is supported.

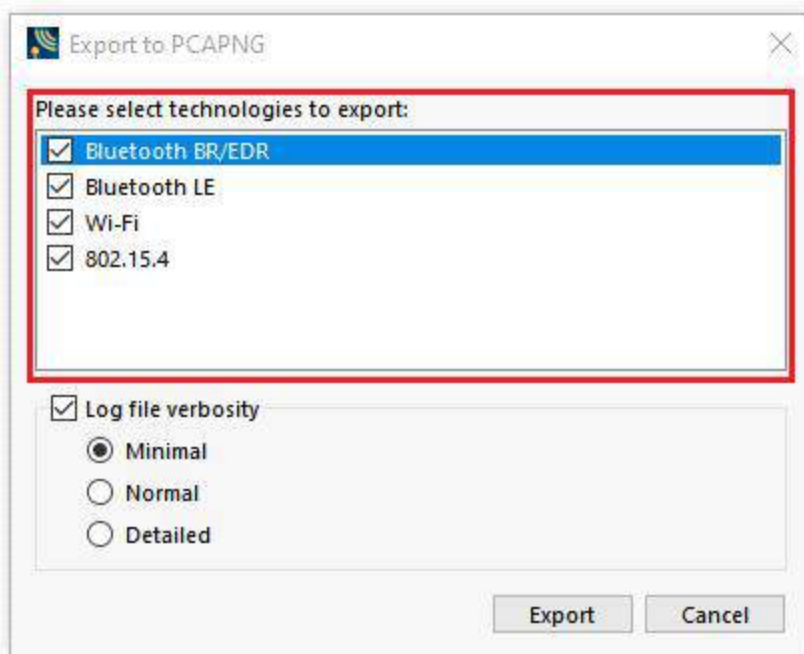


Figure 7.14 - Export to PCAPNG dialog, Available Technologies

3. From the **Export to PCAPNG** window specify the log verbosity. Possible options include Off, Minimal, Normal and Detailed. To disable logging, uncheck **Log file verbosity**.

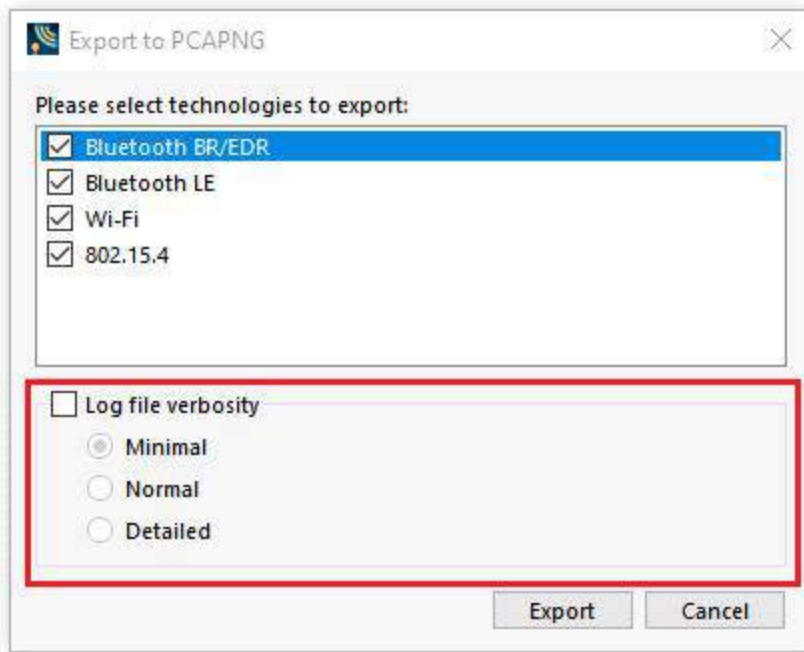


Figure 7.15 - Export to PCAPNG Dialog, Disable Logging

4. Click **Export** to confirm settings of the export or click **Cancel** to exit the Export to PCAPNG dialog.
5. The **Save As** dialog appears. Select a directory location and enter a file name.

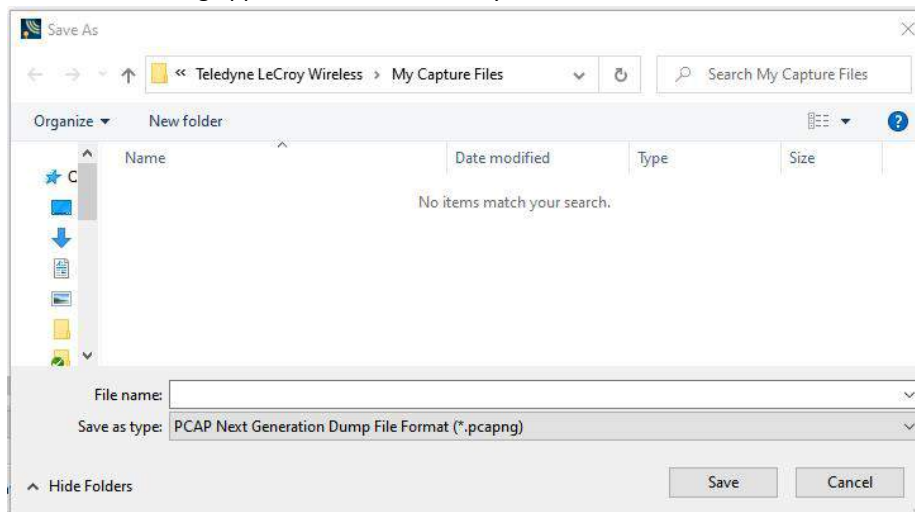


Figure 7.16 - Export to PCAPNG, Save As Dialog

6. Click **Save**.

## CfaToPcapNG Conversion Utility

### Description

CfaToPcapNG is Teledyne LeCroy command line utility that converts a .cfa capture file to Wireshark's .pcapng file. You can find the utility in the following location - C:\Program Files (x86)\Teledyne LeCroy Wireless\Wireless Protocol Suite 1.50\Executables\Core\CfaToPcapNG.exe.

The utility converts Cfa BR/EDR, LE baseband, Wi-Fi and 802.15.4 packets to .pcapng frames of the following link types:

CFA Packet	Corresponding pcapng link type
BR/EDR baseband	LINKTYPE_BLUETOOTH_BREDR_BB
LE baseband	LINKTYPE_BLUETOOTH_LE_LL_WITH_PHDR
Wi-Fi 802.11	LINKTYPE_IEEE802_11
Wi-Fi Radiotap	LINKTYPE_IEEE802_11_RADIOTAP
802.15.4	LINKTYPE_IEEE802_15_4_TAP

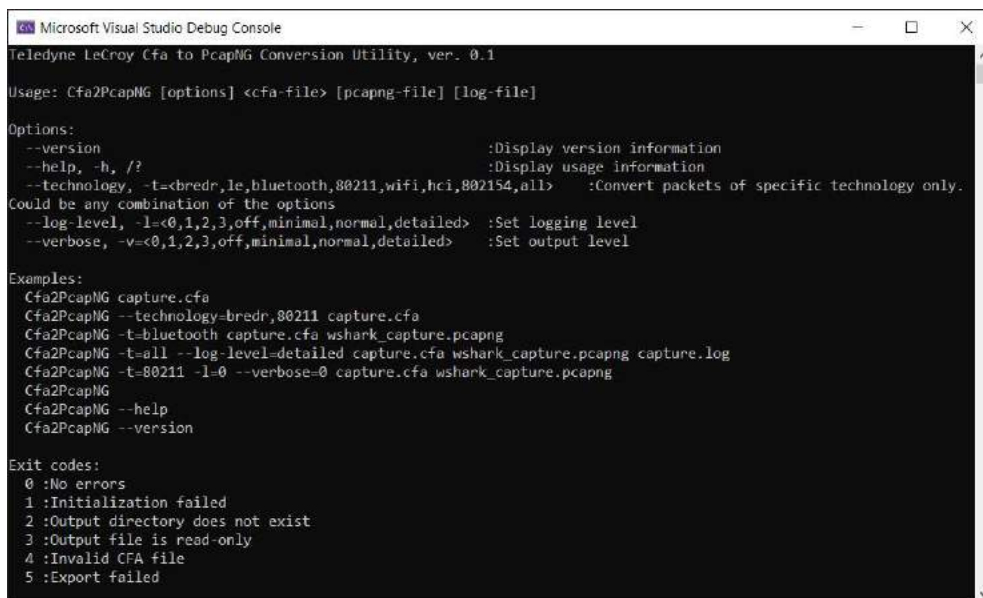
The utility accepts the following command line arguments :

- [cfa-file name] - input CFA file, optional
- [pcapng-file name] - output PcapNG file, optional
- [log-file name] - conversion log, optional
- [options] - additional parameters that control the conversion process, optional:

CLI options	Meaning
• --version	Displays application title with version information.
• --help, -help, -h, /?, no arguments	Displays full help with version info, usage options, usage samples, and exit codes.
• --technology, -t	Specifies the technologies to export from an input file. Possible options include: bredr, le, bluetooth, 80211, hci, 802154, all, as well as any combination of the above. NOTE: Only bredr, le, 80211 and 802154 options are supported in the current version of the utility.

CLI options	Meaning
<ul style="list-style-type: none"> <li>• --log-level, -ll</li> </ul>	<p>Sets conversion logging level. Possible options include:</p> <ul style="list-style-type: none"> <li>• 0 or <i>off</i> - no logging</li> <li>• 1 or <i>minimal</i> - will create a log with basic information about conversion progress, and conversion result</li> <li>• 2 or <i>normal</i> - will create a log with extended information about conversion progress, and summary of the results.</li> <li>• 3 or <i>detailed</i> - will create a log with information about conversion parameters, conversion progress, conversion summary, and conversion status for each packet. Also an internal diagnostic information will be logged.</li> </ul>
<ul style="list-style-type: none"> <li>• --verbose, -v</li> </ul>	<p>Sets console output level. Possible options include:</p> <ul style="list-style-type: none"> <li>• 0 or <i>off</i> - no console output</li> <li>• 1 or <i>minimal</i> - will output basic information about conversion progress, and conversion result</li> <li>• 2 or <i>normal</i> - will output extended information about conversion progress, and summary of the results.</li> <li>• 3 or <i>detailed</i> - will output an information about conversion parameters, conversion progress, conversion summary, and conversion status for each packet. Also an internal diagnostic information will be sent to the output.</li> </ul>

Below is help screen from the utility:



```
Microsoft Visual Studio Debug Console
Teledyne LeCroy Cfa to PcapNG Conversion Utility, ver. 0.1

Usage: Cfa2PcapNG [options] <cfa-file> [pcapng-file] [log-file]

Options:
--version                :Display version information
--help, -h, ??          :Display usage information
--technology, -t=<bredr,le,bluetooth,80211,wifi,hci,802154,all> :Convert packets of specific technology only.
Could be any combination of the options
--log-level, -l=<0,1,2,3,off,minimal,normal,detailed> :Set logging level
--verbose, -v=<0,1,2,3,off,minimal,normal,detailed> :Set output level

Examples:
Cfa2PcapNG capture.cfa
Cfa2PcapNG --technology=bredr,80211 capture.cfa
Cfa2PcapNG -t=bluetooth capture.cfa wshark_capture.pcapng
Cfa2PcapNG -t=all --log-level=detailed capture.cfa wshark_capture.pcapng capture.log
Cfa2PcapNG -t=80211 -l=0 --verbose=0 capture.cfa wshark_capture.pcapng
Cfa2PcapNG
Cfa2PcapNG -help
Cfa2PcapNG --version

Exit codes:
0 :No errors
1 :Initialization failed
2 :Output directory does not exist
3 :Output file is read-only
4 :Invalid CFA file
5 :Export failed
```

**Known issues and limitations:**

- The utility currently supports conversion of the Bluetooth BR/EDR, LE and Wi-Fi packets only.
- The timestamps of the converted packets as displayed in Wireshark do not match the timestamps displayed in the WPS. Wireshark internally applies local time as set in Windows, and displays the timestamps in local time instead of UTC.

## Chapter 8 General Information

### 8.1 System Settings and Program Options

#### 8.1.1 System Settings

Open the **Capture File Options** window by selecting **Capture -> Capture File Options** from the **Main Menu** on the **Wireless Protocol Suite Main window**.

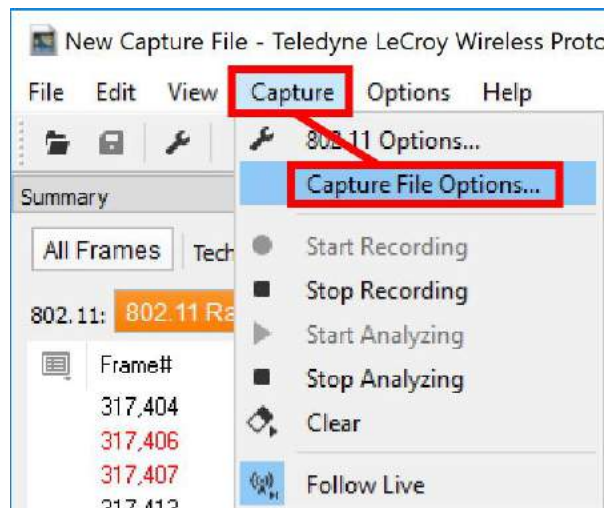


Figure 8.1 - Capture -> Capture File Options

To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.

## Single File

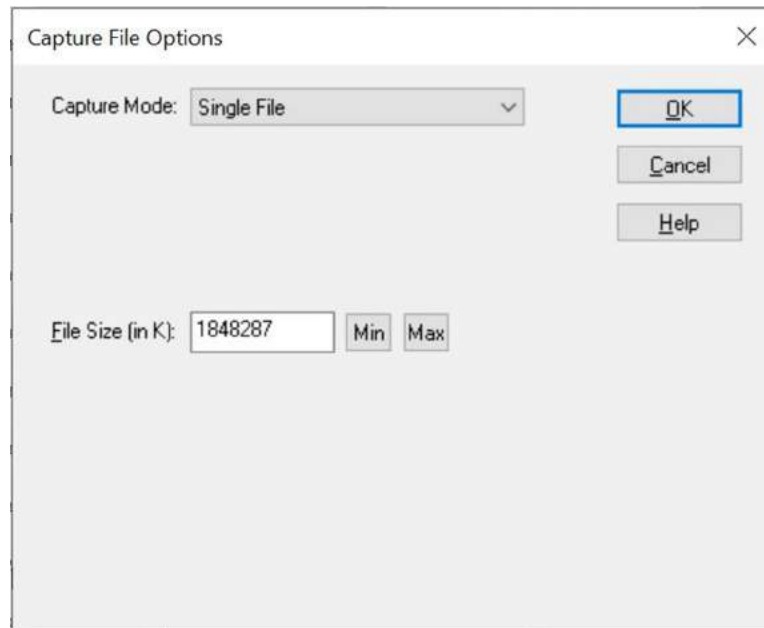


Figure 8.2 - System Settings Single File Mode

This option allows the analyzer to capture data to a file. Each time you capture the file you must provide a file name. The size of each file cannot be larger than the number given in File Size (in K).

- **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.

### 8.1.2 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. Select **File** -> **File Locations** from the main menu. See figure below.

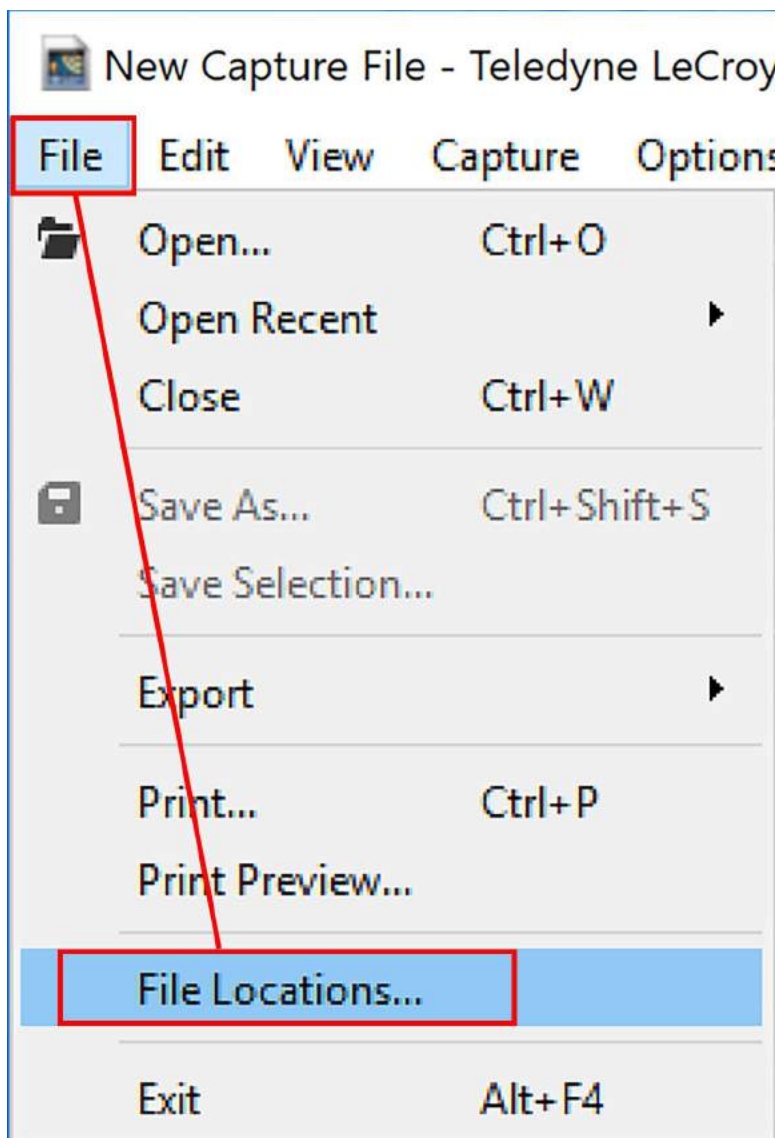


Figure 8.3 - File: File Locations

This will pop up a menu with all the locations of the Capture Files, Configurations, Decoders, Log files etc. See figure below.



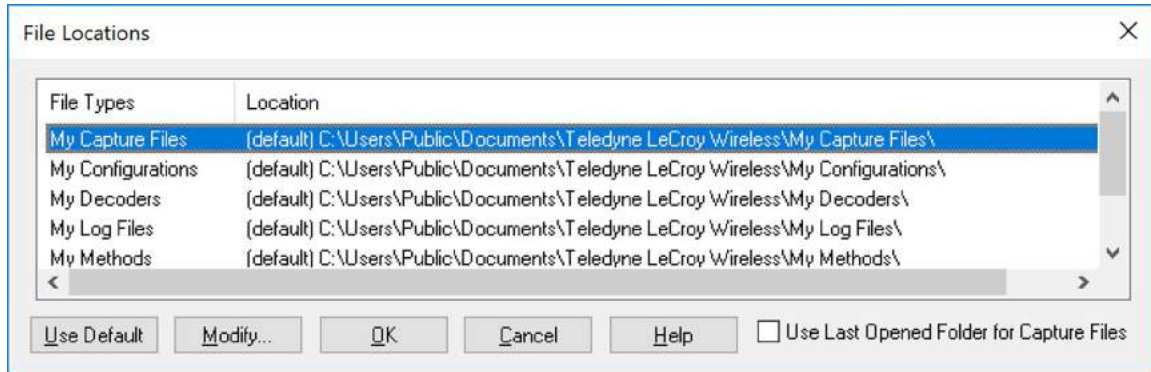


Figure 8.4 - File Locations dialog

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

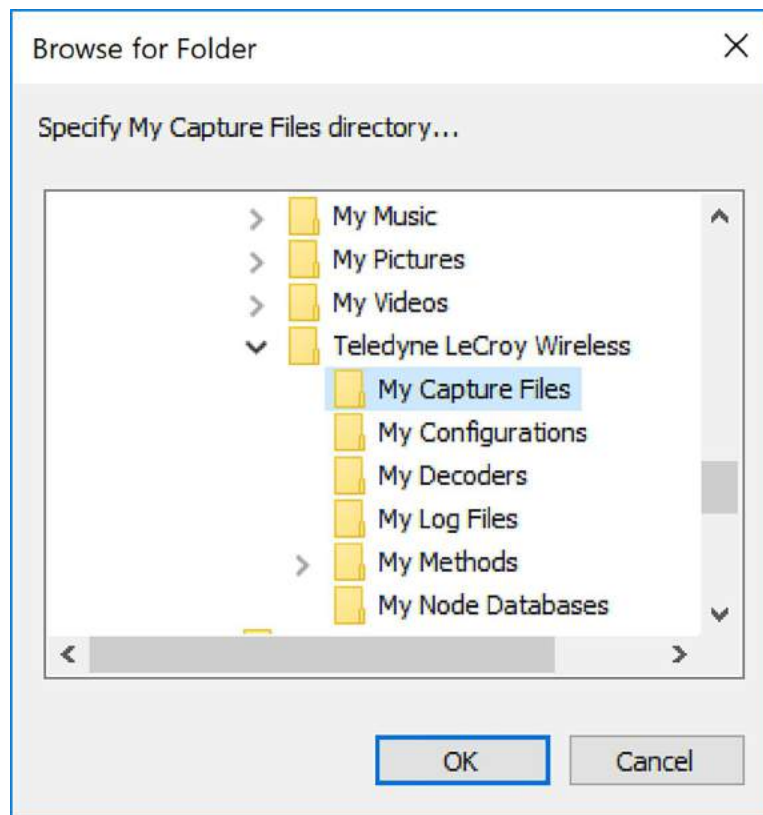


Figure 8.5 - File Locations Browse dialog

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

If a user sets the My Decoders directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch the **Wireless Protocol Suite**. For example, if an Frontline product is installed at C:\Users\Public\Public Documents\Teledyne LeCroy Wireless\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\Teledyne LeCroy Wireless\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. **Wireless Protocol Suite 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.

### 8.1.3 Timestamping

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

#### 8.1.3.1 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 Main windows.

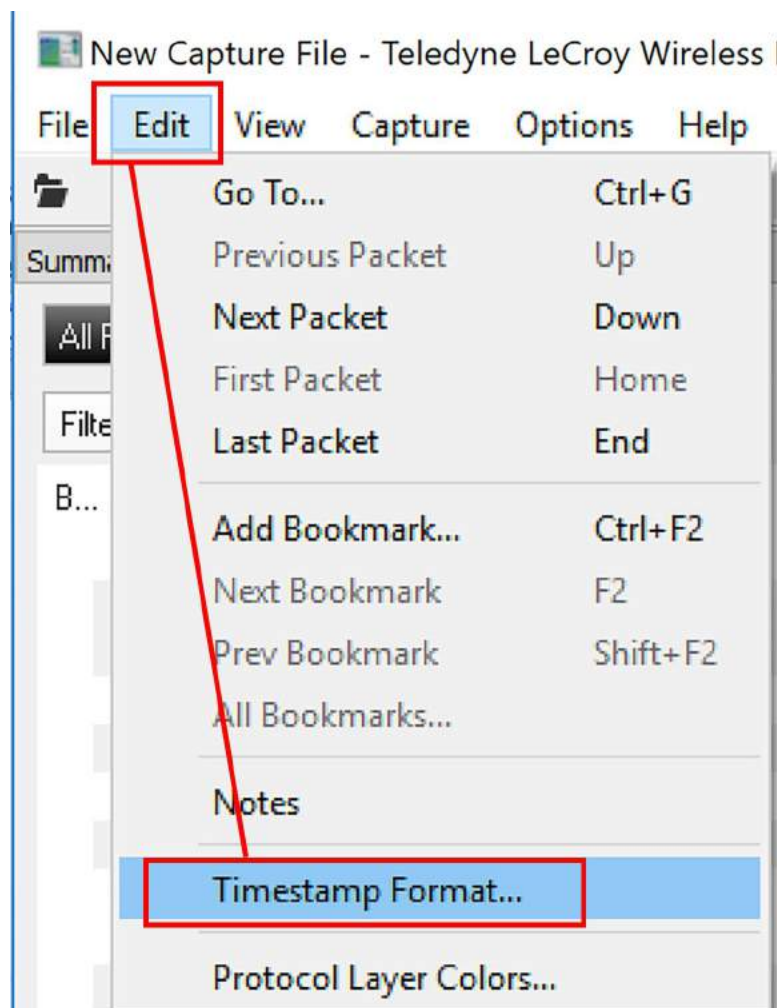


Figure 8.6 - Edit -> Timestamp Format

The Timestamping Options window will open.

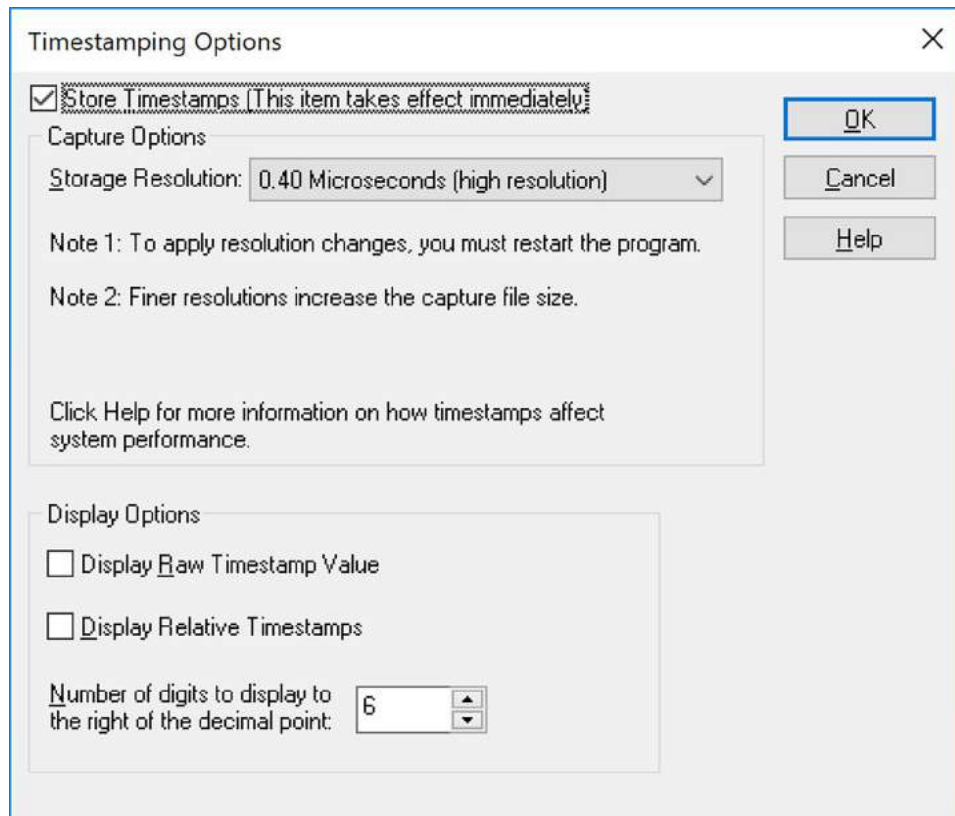


Figure 8.7 - Timestamping Options dialog

### Enabling/Disabling Timestamp

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

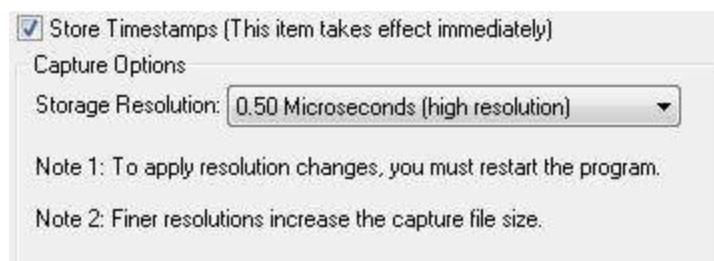
### Changing the Timestamp Resolution

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

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

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

1. Go to the **Capture Options** section of the window.
2. Change the resolution listed in the **Storage Resolution** box.



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

### Performance Issues with High Resolution Timestamp

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

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

You can increase the size of your capture file in the [System Settings](#).

### Switching Between Relative and Absolute Time

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

1. Choose **Set Timestamp Format...** from the **Options** menu on the Main windows.
2. Go to the **Display Options** section at the bottom of the window and find the **Display Relative Timestamps** checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

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

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

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

## Displaying Fractions of a Second

1. Choose **Set Timestamp Format...** from the **Options** menu on the Main windows. .
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.

## 8.2 Technical Information

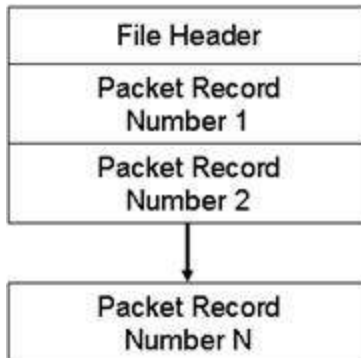
### 8.2.1 BTSnoop File Format

#### Overview

The BTSnoop file format is suitable for storing *Bluetooth*<sup>®</sup> HCI traffic. It closely resembles the snoop format, as documented in RFC 1761.

#### File Format

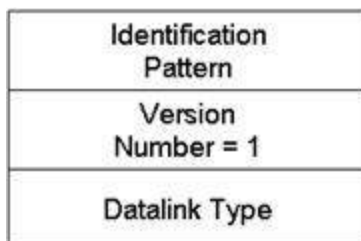
The snoop packet capture file is an array of octets structured as follows:



The File Header is a fixed-length field containing general information about the packet file and the format of the packet records it contains. One or more variable-length Packet Record fields follow the File Header field. Each Packet Record field holds the data of one captured packet.

#### File Header

The structure of the File Header is as follows:



#### Identification Pattern:

A 64-bit (8 octet) pattern used to identify the file as a snoop packet capture file. The Identification Pattern consists of the 8 hexadecimal octets:

62 74 73 6E 6F 6F 70 00

This is the ASCII string "btsnoop" followed by one null octets.

**Version Number:**

A 32-bit (4 octet) unsigned integer value representing the version of the packet capture file being used. This document describes version number 1.

**Datalink Type:**

A 32-bit (4 octet) field identifying the type of datalink header used in the packet records that follow. The datalink type codes are listed in the table below. Values 0 - 1000 are reserved, to maximize compatibility with the RFC1761 snoop version 2 format.

Table 8.1 - Datalink Codes

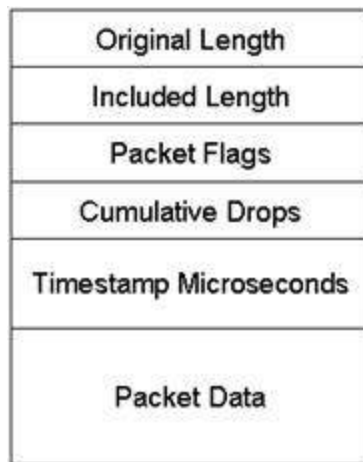
Datalink Type	Code
Reserved	0 - 1000
Un-encapsulated HCI (H1)	1001
HCI UART (H4)	1002
HCI BSCP	1003
HCI Serial (H5)	1004
Unassigned	1005 - 4294967295

**Packet Record Format**

Each packet record holds a partial or complete copy of one packet as well as some descriptive information about that packet. The packet may be truncated in order to limit the amount of data to be stored in the packet file.

Each packet record holds 24 octets of descriptive information about the packet, followed by the packet data, which is variable-length, and an optional pad field. The descriptive information is structured as six 32-bit (4-octet) integer values.

The structure of the packet record is as follows:



**Original Length**

A 32-bit unsigned integer representing the length in octets of the captured packet as received via a network.

**Included Length**

A 32-bit unsigned integer representing the length of the Packet Data field. This is the number of octets of the captured packet that are included in this packet record. If the received packet was truncated, the Included Length field is less than the Original Length field.

**Packet Flags**

Flags specific to this packet. Currently the following flags are defined:

Table 8.2 - Packet Flag Description

Bit No.	Definition
0	Direction flag 0 = Sent, 1 = Received
1	Command flag 0 = Data, 1 = Command/Event
2 - 31	Reserved

Bit 0 is the least significant bit of the 32-bit word.

Direction is relative to host / DTE. i.e. for Bluetooth controllers, Send is Host->Controller, Receive is Controller->Host.

Note: Some Datalink Types already encode some or all of this information within the Packet Data. With these Datalink Types, these flags should be treated as informational only, and the value in the Packet Data should take precedence.

**Cumulative Drops**

A 32-bit unsigned integer representing the number of packets that were lost by the system that created the packet file between the first packet record in the file and this one. Packets may be lost because of insufficient resources in the capturing system, or for other reasons.

Note: some implementations lack the ability to count dropped packets. Those implementations may set the cumulative drops value to zero.

**Timestamp Microseconds**

A 64-bit signed integer representing the time of packet arrival, in microseconds since midnight, January 1st, 0 AD nominal Gregorian.

In order to avoid leap-day ambiguity in calculations, note that an equivalent epoch may be used of midnight, January 1st 2000 AD, which is represented in this field as 0x00E03AB44A676000.

**Packet Data**

Variable-length field holding the packet that was captured, beginning with its datalink header. The Datalink Type field of the file header can be used to determine how to decode the datalink header. The length of the Packet Data field is given in the Included Length field.

Note that the length of this field is not necessarily rounded to any particular multi-octet boundary, as might otherwise be suggested by the diagram.

**Data Format**

All integer values are stored in "big-endian" order, with the high-order bits first.



## 8.2.2 Ring Indicator

The following information applies when operating the analyzer in **Spy** mode or **Source DTE, No FTS Cables** mode. When using the cables supplied with the analyzer to capture or source data, Ring Indicator (RI) is routed to a different pin which generates interrupts normally.

There is a special case involving Ring Indicator and computers with 8250 UARTs or UARTs from that family where the state of RI may not be captured accurately. Normally when a control signal changes state from high to low or low to high, an interrupt is generated by the UART, and the analyzer goes to see what has changed and record it. Ring Indicator works a little differently. An interrupt is generated when RI changes from high to low, but not when RI changes from low to high. If Ring Indicator changes from low to high, the analyzer does not know that RI has changed state until another event occurs that generates an interrupt. This is simply the way the UART works, and is not a deficiency in the analyzer software.

To minimize the chance of missing a Ring Indicator change, the analyzer polls the UART every millisecond to see if RI has changed. It is still possible for the analyzer to miss a Ring Indicator change if RI and only RI changes state more than once per millisecond.

UARTs in the 8250 family include 8250s, 16450s, 16550s and 16550 variants. If you have any questions about the behavior of your UART and Ring Indicator, please [contact technical support](#).

## 8.2.3 Useful Character Tables

### 8.2.3.1 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

### 8.2.3.2 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

### 8.2.3.3 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						

### 8.2.3.4 Communication Control Characters

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

Table 8.3 - Communications Control Characters

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

Table 8.3 - Communications Control Characters(continued)

Abbreviation	Control Character	Text
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit Separator
VT	VT	Vertical Tabulation

### 8.2.4 Bluetooth Low Energy ATT Decoder Handle Mapping

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

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

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

The solution to this problem is to

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

#### Creating handle-UUID mapping file

Create a file named "ATT\_Handle\_UUID\_Preload.ini" in the root directory of "C:\Users\Public\Public Documents\Teledyne LeCroy Wireless\My Decoders\", but the file can be located anywhere.

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

Create a section in the ini file called

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

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

Next add the following section.

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

A4 = 2a01  
A5 = 2803  
A6 = 2a04

A few things of note:

- In the code above, lines beginning with a semi-colon are comments.
- **If you want to change the base handle of the GAP service, change the "1" to some other number.**

### 8.3 Contacting Teledyne LeCroy Frontline 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](mailto:tech_support@fte.com)

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

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

#### Instructional Videos

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

## 8.4 License Manager

### 8.4.1 Introduction

The X240 Hardware requires a license in order to be used with the Wireless Protocol Suite software. All X240's will be shipped with a license file already installed. Updated license files can be applied by the user on their own using the **Manage License** dialog.

### 8.4.2 Manage License Dialog

Viewing the details of a currently installed license file or updating the X240 license file is done through a menu item accessed from the X240 Analyzer Toolbar. With hardware connected, from the Analyzer Information menu dropdown, select **Manage License....**

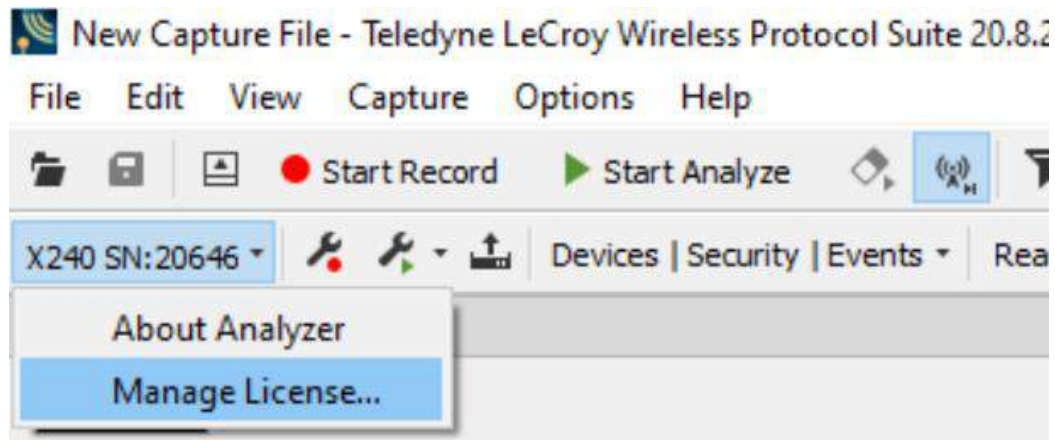


Figure 8.8 - Manage License Dialog

After selecting Manage License, the following window is presented:

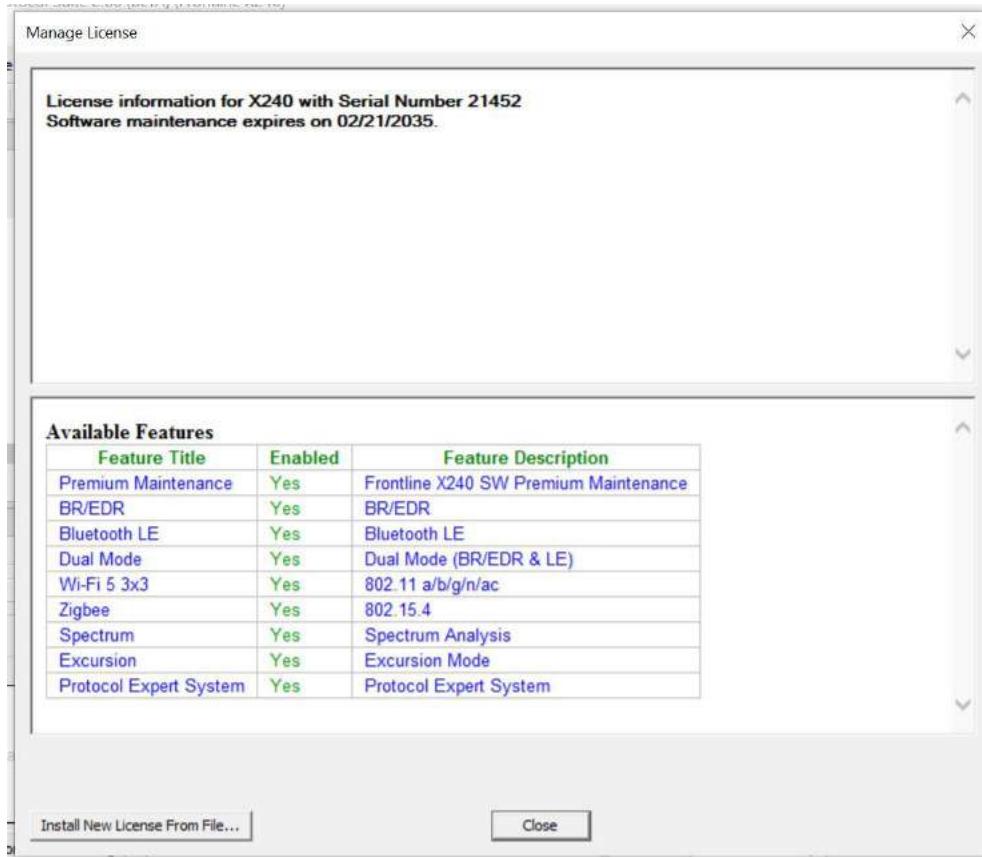


Figure 8.9 - License Manager (showing License Features)

On this window you will see the expiration of the currently loaded license at the top. Below this is a list of available features and whether or not they are included in your license.

To add or update your license, you will need to click on the “Install New License From File...” button on the Manage License window. This will open a Windows Explorer window. After selecting the license file you’d like to update to, click Open. The “Install New License” window will appear showing you the details of both your old and new license.

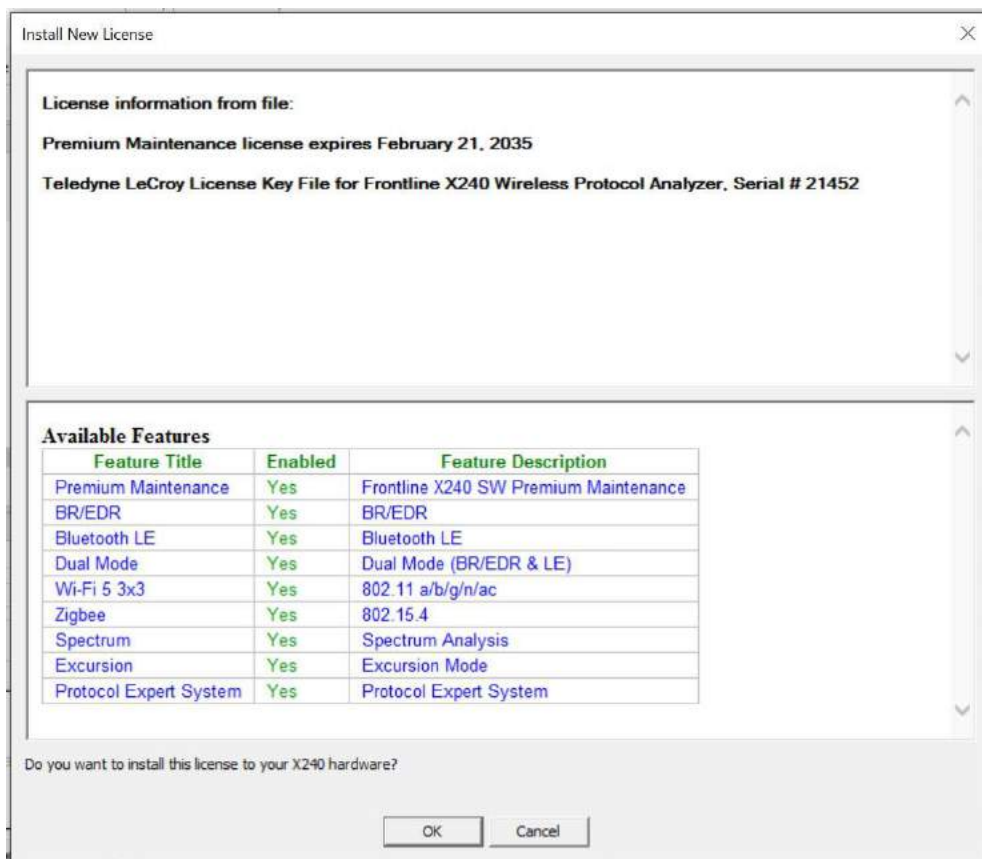


Figure 8.10 - Install New License

**Note:** The license file must be for the specific X240 hardware unit connected or you will see the following error:



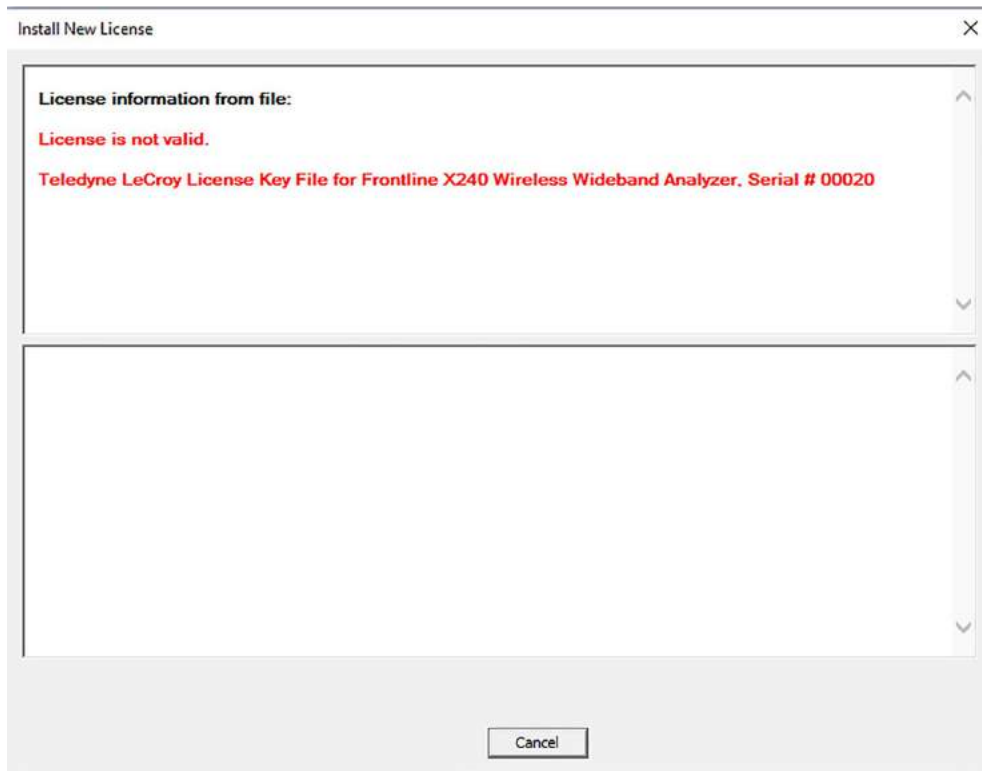


Figure 8.11 - License Not Valid Warning

With a valid license selected, clicking OK will present the following message:

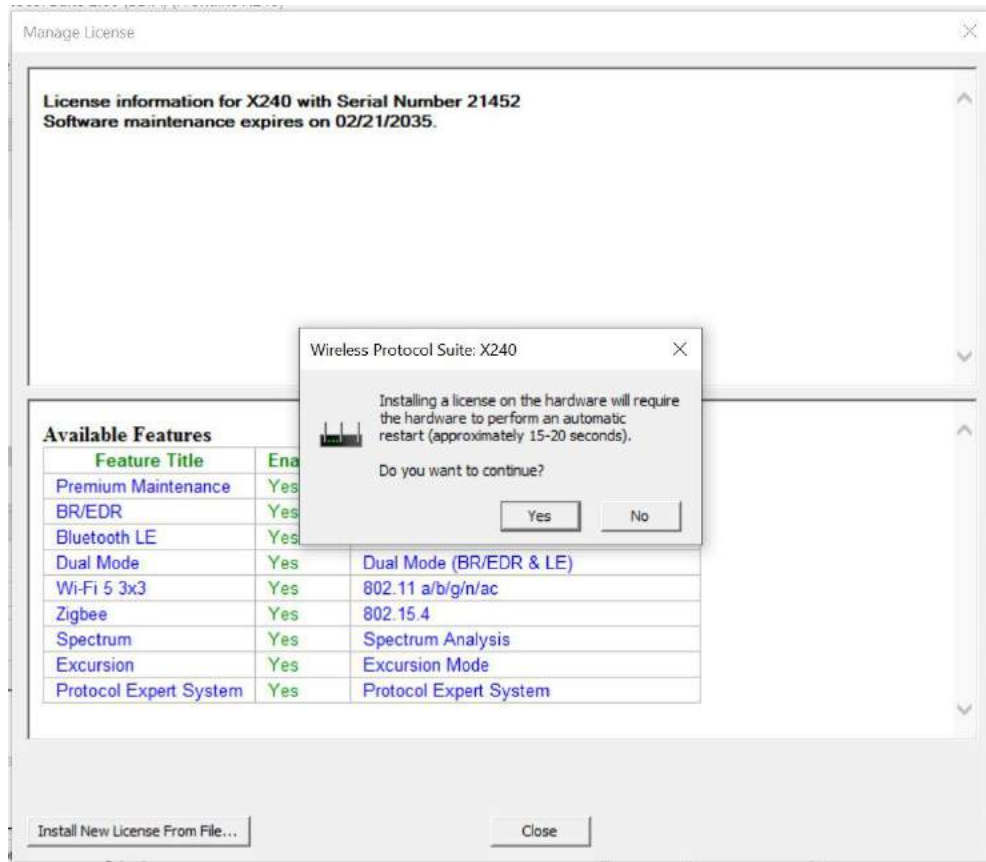


Figure 8.12 - Valid License

Clicking “Yes” will install the new license file and automatically restart your hardware. After the unit powers back up, the new license should be recognized, and the unit will be able to be used.

### 8.4.3 Trial Licenses

Your X240 may have a trial license with features available for a limited amount of time.

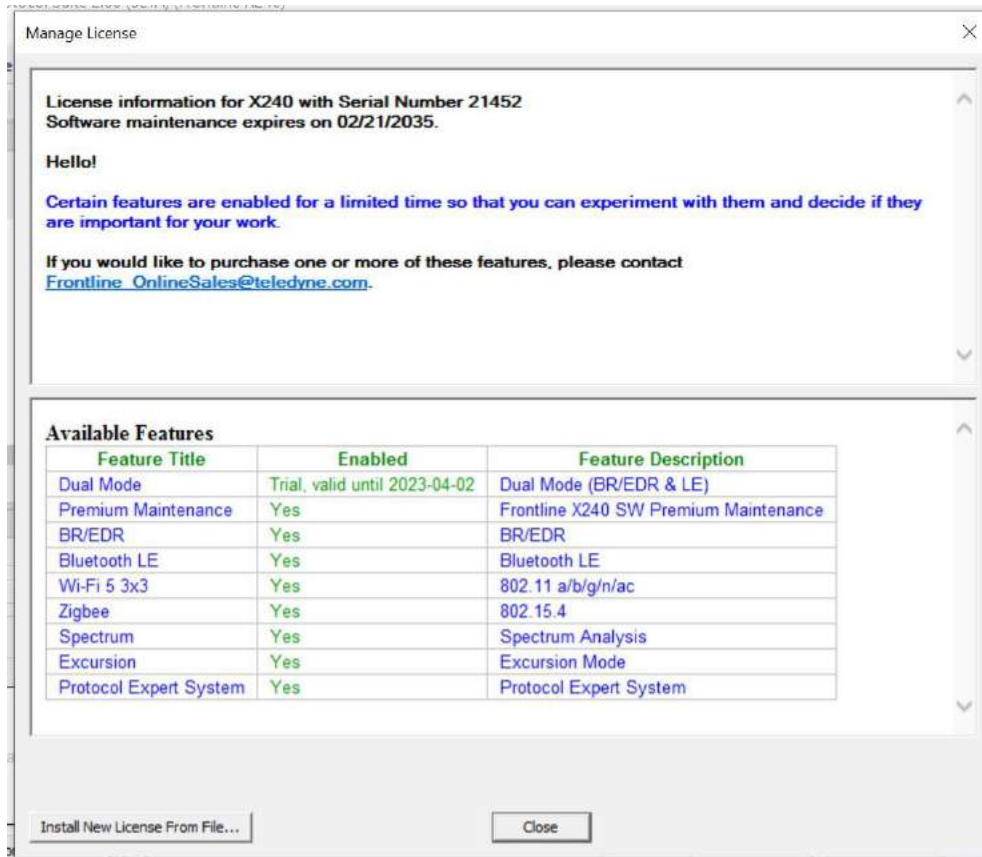


Figure 8.13 - Trial License

If your X240 has a trial license but it has not been activated for use, you may see an "Activate Trial" button.

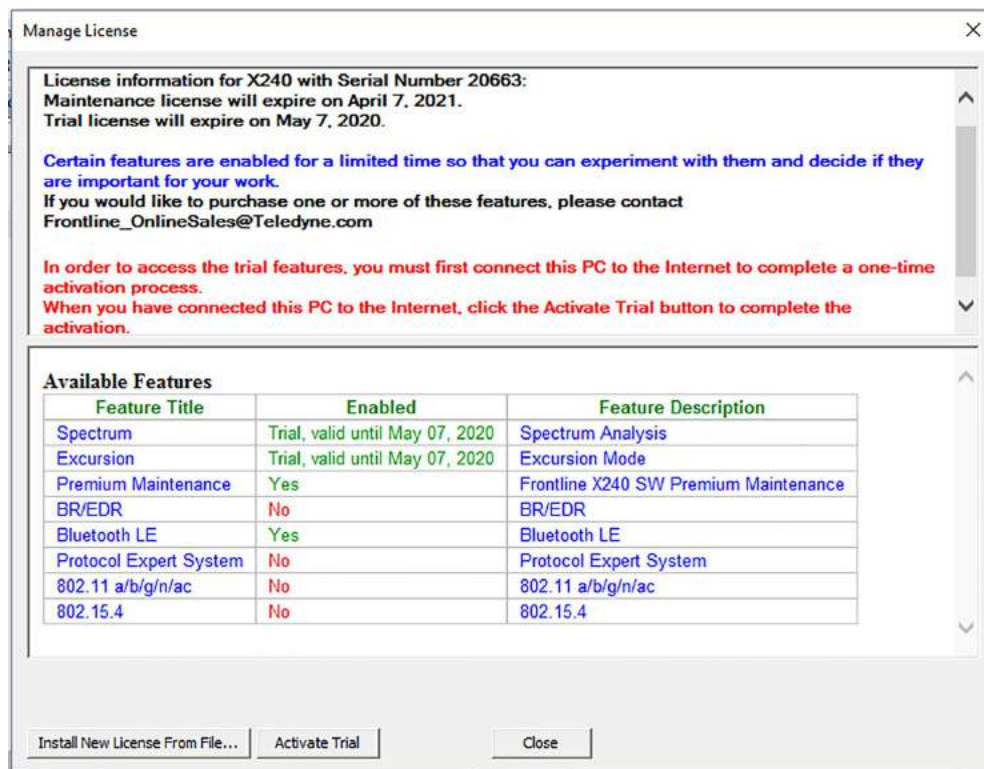


Figure 8.14 - Activate Trial License

To activate use of trial licenses, connect the PC to the internet and click the button. The trial license activation needs to only be done once and the button will not appear again.

## 8.5 What's New

Information about newly released features is shown in *Release notes & Welcome Tour*, located under the Help menu.



## Appendices

---

<b>Appendix A: X500 Technical Specifications/Service Information</b> .....	<b>450</b>
<b>Appendix B: X240 Technical Specifications/Service Information</b> .....	<b>451</b>
<b>Appendix C: Sodera Technical Specifications/Service Information</b> .....	<b>452</b>
<b>Appendix D: Sodera LE Technical Specifications/Service Information</b> .....	<b>453</b>
<b>Appendix E: File Extension Descriptions</b> .....	<b>453</b>
<b>Appendix F: Application Notes</b> .....	<b>454</b>
<b>Appendix G: ra X500 Wi-Fi 6E Frequencies</b> .....	<b>471</b>

### Appendix A: X500 Technical Specifications/Service Information

#### X500 Specifications

- Dimensions: 278 x 242 x 45 mm (11" x 9.5" x 1.77")
- Weight: 2.3 kg (5 lbs.)
- Humidity: Operating: 0% - 80% RH (non-condensing)
- Temperature Operating: 32° F to 122° F (0° C to 50° C)
- Input Voltage: 15 V
- Max Power: 90 W

#### X500 Battery Specifications

- Type: Rechargeable Smart Lithium Ion Battery Pack
- Assembly: External, user removable
- Dimensions: 310.39 x 241.3 x 56.39 mm (12.22" x 9.5" x 2.22")
- Weight: 1.36 kg (3 lbs.)
- Temperature Operating: 32° F to 113° F (0° C to 45° C) for charging and -4° F to 140° F (-20° C to 60° C) for discharging
- Power Capacity: 90 WAh
- Operating time: ~2 hours (varies based on RF activity)

#### Service Notes

The X500 hardware does not contain any user serviceable items. Any repairs and maintenance must be performed by a service technician that has been trained and approved by Teledyne LeCroy.

Before any service is performed on X500, all power sources must be removed. This includes disconnecting any power sources from the 15 VDC input power connector on X500. Typical power sources include external AC/DC power supplies, battery pack, or auxiliary power sources from a vehicle.

## **Appendix B: X240 Technical Specifications/Service Information**

- Dimensions: 7.5" wide X 4" deep X 1" tall (190.5 mm X 101.6 mm X 25.4 mm)
- Weight: 1.5 lbs
- Humidity: Operating: 0% - 90% RH (non-condensing)
- Temperature Operating: 32° F to 104° F (0° C to 40° C)
- Input Voltage: 5 V
- Max Power: 18 W

### **Service Notes**

The X240 hardware does not contain any user serviceable items. Any repairs and maintenance must be performed by a service technician that has been trained and approved by Teledyne LeCroy.

Before any service is performed on X240, all power sources must be removed. This includes disconnecting any power sources from the 5 VDC input power connector on X240. Typical power sources include external AC/DC power supplies or auxiliary power sources from a vehicle.

### **Internal Fuse Information**

- Manufacturer: Littlefuse
- Type: OmniBlok
- Current rating: 3A
- Speed rating: Very Fast Acting
- Voltage rating: 125V ac/dc

## Appendix C: Sodera Technical Specifications/Service Information

- Dimensions: 159 mm wide X 57 mm tall" X 165 mm deep" (6.3" X 2.3 " 6.5" X mm)
- Weight: 1.0 kg (2.2 lb)
- Humidity: Operating: 0% - 90% (0 °C – 35 °C)
- Temperature: -10 °C to +40 °C (14 °F to +104 °F)
- Power Input: 12 VDC (tip positive)
- Max Power: 25 W
- Battery: NB2037FQ31



**Caution:** There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of old batteries according to your local regulations.

### Service Notes

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

Before any service is performed on Sodera, all power sources must be removed. This includes removing the battery and disconnecting any power sources from the 12 VDC input power connector on Sodera. Typical power sources include external AC/DC power supplies or auxiliary power sources from a vehicle.

### Internal Fuse Information

- Manufacturer: Littlefuse
- Type: OmniBlok
- Current rating: 5A
- Speed rating: Very Fast Acting
- Voltage rating: 125V ac/dc



## Appendix D: Sodera LE Technical Specifications/Service Information

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

### Service Notes

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

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

## Appendix E: File Extension Descriptions

Wireless analyzer capture files generate several different files of various types. The following table describes their use and purpose:

File Type	Purpose
.cfa	This file includes all data with all context, decryption, user data (bookmarks, etc) for the recorded and analyze packets.
.scap	Allows access to the full unanalyzed and unfiltered capture. The presence of this file will allow a user to enter a different link key or analyze a different set of devices within the same capture.
.swsd	Wireless spectrum data.
.wcap	802.11 wireless data.
.frm	Companion file created upon decoding and filtering the capture. This allows for faster reopening of a capture. Companion files are recreated per WPS software version.
.fsc	Companion file created upon decoding and filtering the capture. This allows for faster reopening of a capture. Companion files are recreated per WPS software version.
.bes	Text file of various events and statistics

## Appendix F: Application Notes

---

<b>F.1 Audio Expert System: aptX 'hiccup' Detected</b> .....	<b>455</b>
<b>F.2 Getting the Android Link Key for Classic Decryption</b> .....	<b>460</b>
<b>F.3 Decrypting Encrypted Bluetooth® Low Energy</b> .....	<b>464</b>
<b>F.4 Table of Acronyms</b> .....	<b>470</b>

---

## F.1 Audio Expert System: aptX 'hiccup' Detected

This paper presents a case study in *Bluetooth*<sup>®</sup> audio debugging that highlights the importance of Frontline's Audio Expert System (AES) in the process. The actual case involves transmission of a high quality, stereo audio using the aptX codec from a smartphone to a *Bluetooth* headset. The transmission contained SBC encoded packets despite a successful negotiation of aptX encoding and decoding mechanism between the source and the sink devices. Frontline's AES software discovered this transmission error which most likely would not have been easily discovered by using traditional *Bluetooth* protocol and event analysis. Without the Audio Expert System a product may have been shipped that was not performing as expected by the manufacturer.

### F.1.1 Background

In *Bluetooth* technology, Audio/Video Distribution Transport Protocol (AVDTP) uses Advanced Audio Distribution Profile (A2DP) for streaming audio in stereo. The A2DP encompasses compression techniques to reduce the amount of radio frequency bandwidth required to transmit audio. In addition to A2DP, Audio/Video Remote Control Profile (AVRCP) controls certain functions of the sending device such as pause, play, next track, etc.

All *Bluetooth* products using A2DP are required to implement audio encoding and decoding using low complexity Sub Band Coding (SBC) that supports up to 345 kb per second bit rate for stereo audio. The SBC codec has some issues though. SBC coding and decoding produces some undesirable artifacts in the audio signal. In addition, the SBC encoding and decoding cycle introduces a time lag in the audio. To improve on SBC's artifacts and time lag issues, a CSR proprietary codec that is called aptX<sup>®</sup> is implemented on some *Bluetooth* products.

During the negotiation phase, both *Bluetooth* devices handshake and they automatically discover the best codec and the highest bit rate to use for audio. If both devices support aptX, it is used rather than the default SBC.

The AES software helps identify audio issues in *Bluetooth* protocol by highlighting information, warnings, and errors related to audio data, codec used, and *Bluetooth* protocol implementation. They are collectively called "events" in AES. The AES window shows audio data plotted as PCM samples versus time in the Wave Panel. The audio data, codec, and protocol events are also graphically displayed in the Wave Panel, and with a single click on an event, engineers and testers are brought directly to the exact packets or frames related to the event in the *Bluetooth* protocol trace in the Main windows. This helps users find issues quickly and easily. The events are shown time aligned with both the actual audio waveform and bit rate variances graph in the Wave Panel. The bit rate variance graph shows the average or actual amount of *Bluetooth* audio data sent over a period of time.

AES can operate in two modes: 1) referenced mode, and 2) non-referenced mode. In referenced mode a Frontline provided audio test file is streamed between the Devices Under Test (DUTs). The test file content and parameters are known to the AES software that performs a comparison for deviations. This process helps the software accurately detect anomalies created by the streaming process. In non-referenced mode DUTs stream audio of unknown content, limiting the types of detectable events. The software automatically determines the operation mode with no user input required.

### F.1.2 Test Setup

The following DUTs below were used in our test setup:

- DUT1 = smartphone with *Bluetooth* and aptX capability. The smartphone operating system was Android.
- DUT2 = Earphones with *Bluetooth* and aptX capability.

The protocol analyzer: Frontline Sodera, Sodera LE Dual Mode *Bluetooth* Protocol Analyzer with *Bluetooth* Audio Expert System activated. The Sodera, Sodera LE is connected to a personal computer (PC) that is running Wireless Protocol Suite software.

DUT1 was used as a source device. DUT1 was streaming an AES Reference file.

DUT2 was used as a sink device. After establishing a valid *Bluetooth* link, DUT2 played the AES Reference file.

The audio test file was played from the Bluetooth smart phone to the Bluetooth headphone. The data captured by the Frontline Sodera, Sodera LE hardware was sent to the analysis computer running Wireless Protocol Suite software with AES. As the data was captured, it was analyzed by the AES module and displayed live in the AES window. The AES software automatically detected the test ID tones in the captured audio and operated in the referenced mode. The figure 1 below shows the test setup.

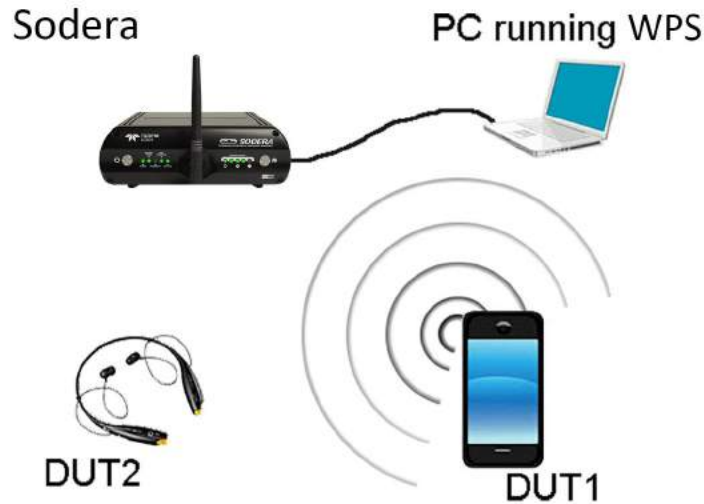


Figure 1 - The Test Setup.

### F.1.3 Discussion

The test began without any issue. DUT1 and DUT2 negotiated a Bluetooth connection suitable for transmitting the audio. When the Reference Audio was played there were no obvious audio distortions or anomalies heard by the tester.

The tester used a Frontline Sodera, Sodera LE configured for capturing Classic Bluetooth over a single connection.

In Main windows AVDTP Signaling tab we see the start of the negotiation between DUT1 and DUT2 to establish an audio connection, see Figure 2. At frames 554 and 602 the initiating or local device sends an AVDTP\_DISCOVER command. The remote device responds by identifying the ACP Stream Endpoint IDs. In this case the remote device identifies three audio media-type devices that are SNK (sink) devices currently not in use: SEPID (Stream Endpoint Identification) 1 through 10.

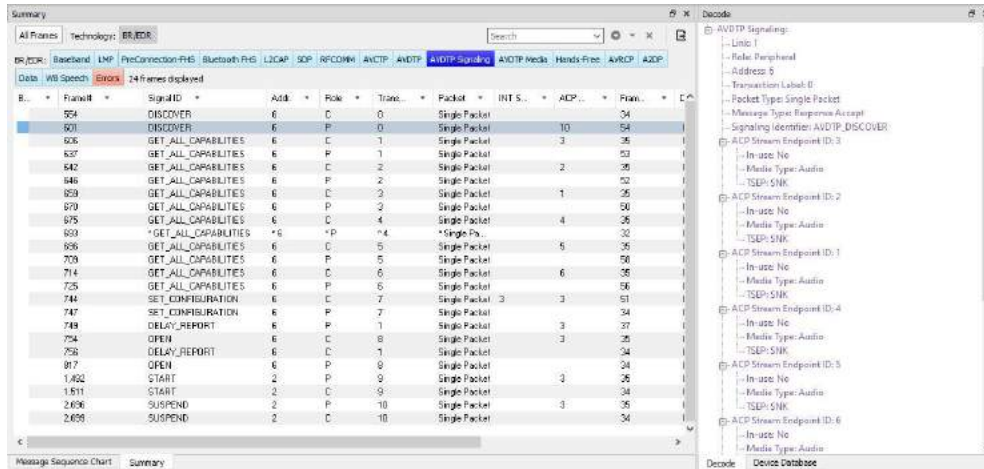


Figure 2 - Main windows for AVDTP Signaling Frame 601

**Note:** "ACP" is AVDTP terminology for the remote device.

The next step in the negotiation is to get the audio capabilities of each SEPID. For each SEPID there is an exchange of GET\_CAPABILITIES AVDTP signals.

Examination of the Main windows AVDTP Signaling protocol tab shows at frame 602 the peripheral device request SEP (Stream End Point) characteristics. From SEPID (SEP Identifier) 3. Details of the GET\_CAPABILITIES command are show in Figure 3.

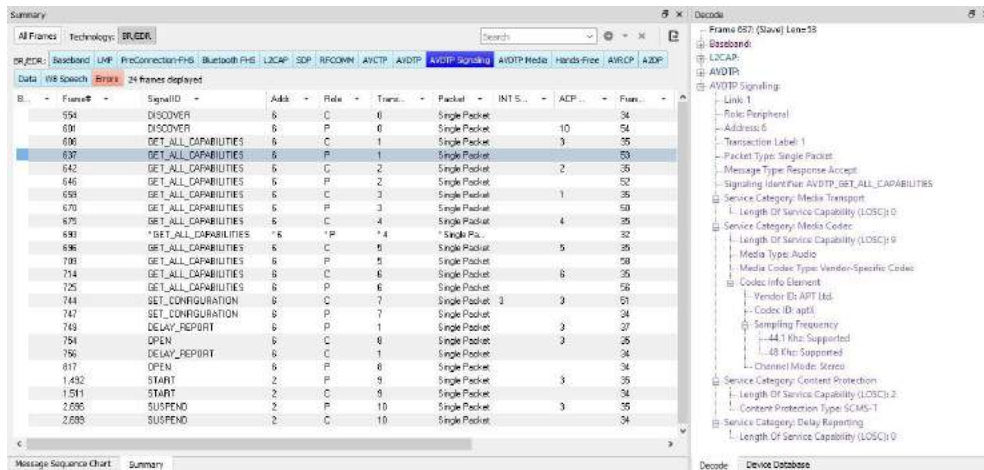


Figure 3 - Main windows for AVDTP Signaling Frame 637

At frame 774 the remote device responds to the GET\_CAPABILITIES for SEPID 3, reporting that this SEP codec is aptX with a Channel Mode of Stereo

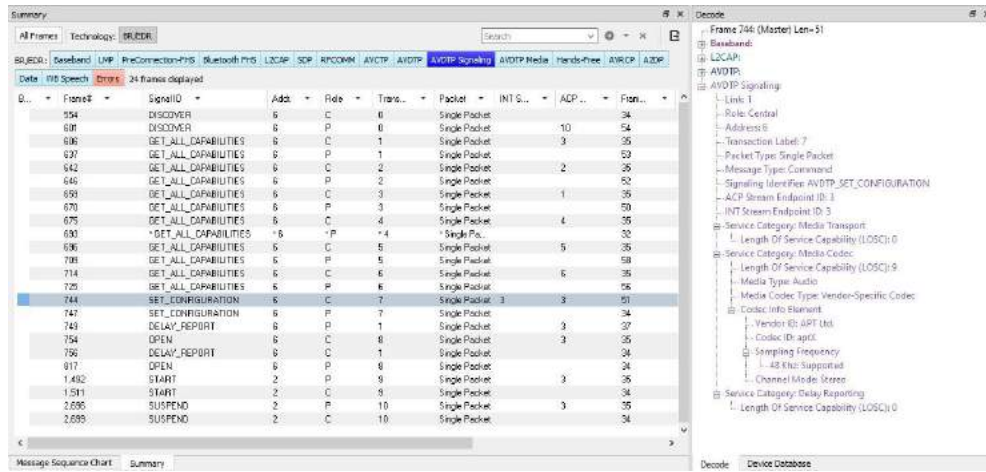


Figure 4 - Main windows for AVDTP Signaling Frame 774

In Figure 4, frames 606 through 725 perform the GET\_CAPABILITIES negotiation between the local and remote device for SEPIIDs 1 through 6.

Frames 744 and 747 set the specific details of the connection with the SET\_CONFIGURATION signal. The local device sets the remote endpoint to the aptX device (ACP Stream Endpoint ID: 3). The Codec, Sampling Frequency and Channel Mode are also configured.

Frames 754 and 817 are the local request and the remote response to OPEN the audio stream.



Frames 1,492 and 1,511 START the audio stream with the local request and remote response respectively.

So far the process of setting up an aptX audio connection between DUT1 and DUT2 appears normal, correct and error free. We now move from the AVDTP protocol to the A2DP protocol to observe the audio.

### Problem Discovery

In the Wireless Protocol Suite software, the audio data is shown in the A2DP tab in the Main windows, which is the first audio frame, is identified as being aptX encoded because of the successful codec negotiation. At this frame, the conventional audio data analysis methods do not show any issues. Assuming the data is aptX encoded, the AES software passes it to the AES aptX decoder. However, the data was not decoded correctly and is marked as a bad aptX frame. On further analysis, the AES software discovers that the frame is not aptX encoded but is actually SBC encoded. Frame 2839 begins with "0x9C", and all SBC audio frames begin with sync word "0x9c" as shown in F.1.3. The AES cannot solely rely on the sync word to determine if it is a SBC frame. To confirm the suspicion, the AES passed the data through its SBC decoder, and the data came out cleanly decoded.

The AES software not only showed that there is a problem in the audio data but also made it clear where the problem is.

The Error that is identified by Event 4, the Severity red circle , is a codec  event at Frame 2839 states "Unable to process AptX data as extracted. It appears that SBC encoded data is being sent over this stream."

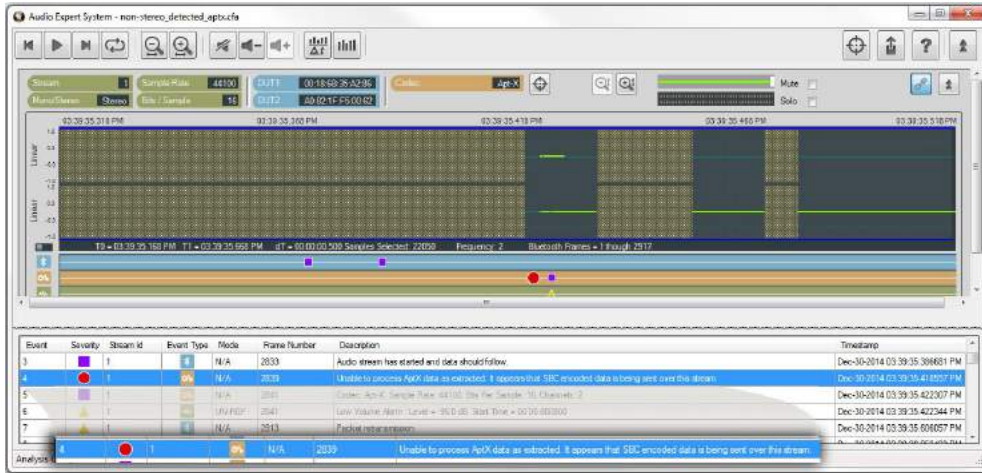


Figure 5 - Audio Expert System Error on Frame 2839: Data not aptX.

### F.1.4 Conclusions

This case shows the value of Frontline's Audio Expert System. An error in the transmission of an audio stream compressed using aptX was not easily detected in the protocol analysis using frames. While, in this situation with audio streaming between a smartphone and a *Bluetooth* headset, there was not a significant disruption of the audio, but in playback using other devices there may have been a more significant interruption of the audio streaming.

The smartphone manufacturer may wish to find out why aptX compressed audio contained SBC compressed data in the stream. We can speculate that there may be an underlying problem with clearing stacks or memory between streaming events. This investigation is beyond the scope of this paper.

---

Publish Date: 3/3/2023

## F.2 Getting the Android Link Key for Classic Decryption

---

*Bluetooth* devices on an encrypted link share a common "link key" used to exchange encrypted data. For a *Bluetooth* sniffer, such as the Frontline Soderia, Soderia LE, to be able to decrypt the encrypted data, it must also have this shared link key. For obvious security reasons, the link key is never sent over the air, so either the user must get the key out of one of the devices being sniffed and supply the key to the sniffer or the sniffer must create the key itself.

*Bluetooth* devices using the Android operating system have a "developer" option that will provide the link key for Classic *Bluetooth* decryption. This procedure will use the developer options to obtain the Android HCI (Host Controller Interface) log that contains the link keys for all active links..

### F.2.1 What You Need to Get the Android Link Key

The process applies to the Android 4.4 or later operating system.

- Android device with Bluetooth enabled and paired with another *Bluetooth* device.
- Wireless Protocol Suite software installed on your computer
- Android Debug Bridge (optional)

**Note:** Each Android device model can vary in screen organization, layout and format. The directions in this paper are based on known typical Android device. Refer to the manufacturer's manual, on-line help, or technical support for detailed information about your particular device.

### F.2.2 Activating Developer options

The Android HCI log will contain the link key for an active *Bluetooth* link.

1. On the Android device go to **Settings**,
2. Select **About**.
3. In the About screen tap on **Build number** eight times. At some point you will see a notice similar to "You are now a developer!".

**Note:** On some devices the build information may be under one or more sub-screens below the About screen. Also the number of taps may vary; in most cases the screen will provide status of your tap count.

4. Return to the **Settings** screen and you will see **Developer options**

### F.2.3 Retrieving the HCI Log

Now that **Developer options** have been activated on the Android device, you can retrieve the HCI log.

1. On the Android device go to **Settings**.
2. Select **Developer options**.



3. Click to enable **Bluetooth HCI snoop logging**.
4. Return to the **Settings** screen and select **Developer options**.
5. In the **Developer options** screen select **Enable Bluetooth HCI snoop log**. The log file is now enabled.

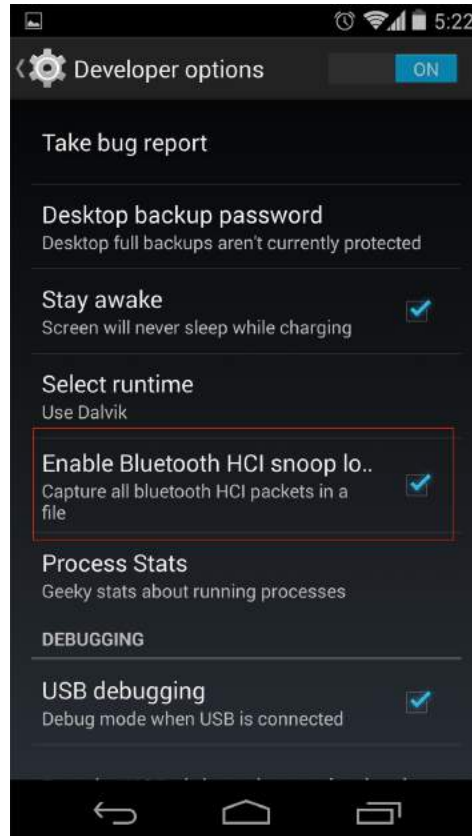


Figure 6 - Typical Android Developer options screen

6. On the Android device turn off *Bluetooth*.
7. Turn on *Bluetooth*.
8. Reboot the Android device.

The HCI log file is now being generated and is saved to `/sdcard/btsnoop_hci.log`.

**Note:** Samsung devices have a slightly different location for the btsnoop file.

There are two options for retrieving the HCI log from the Android device.

- a. Attach the Android device to your computer. The file `/sdcard/btsnoop_hci.log` is in the root of one of the mountable drives. Copy the file to directory `C:/Users/Public/Public Documents/Frontline Test Equipement/My Capture File/`.

b. The second option is to use the Android Debug Bridge (ADB) using the following steps. The debug bridge is included with Android Software Developer Kit.

(1). On the Android device **Development** screen, select **Android debugging** or **USB debugging**.

(2). Connect your computer and Android device with a USB cable.

(3). Open a terminal on your computer and run the following command.

```
adb devices.
```

(4). Your Android device should show up in this list confirming that ADB is working.

```
List of devices attached
XXXXXXXXXXXX device
```

(5). In the terminal enter the following command to copy the HCI Log to your computer.

```
adb pull /sdcard/btsnoop_hci.log
```

### F.2.4 Using the Wireless Protocol Suite software to Get the Link Key

You will load the HCI Log file *btsnoop\_HCI.log* into the Wireless Protocol Suite software on your computer as a capture file. Then you can use the **Main windows** to locate the link key.

1. Activate the Wireless Protocol Suite software. (Refer to the Frontline Sodera, Sodera LE User Manual on [fte.com](http://fte.com)).
2. From the main menu select **File, Open Capture File....**
3. When the **Open** window appears, set the file type to **BTSnoop Files (\*.log)**. If not already selected navigate to the *My Capture Files* directory and select *btsnoop\_hci.log*.

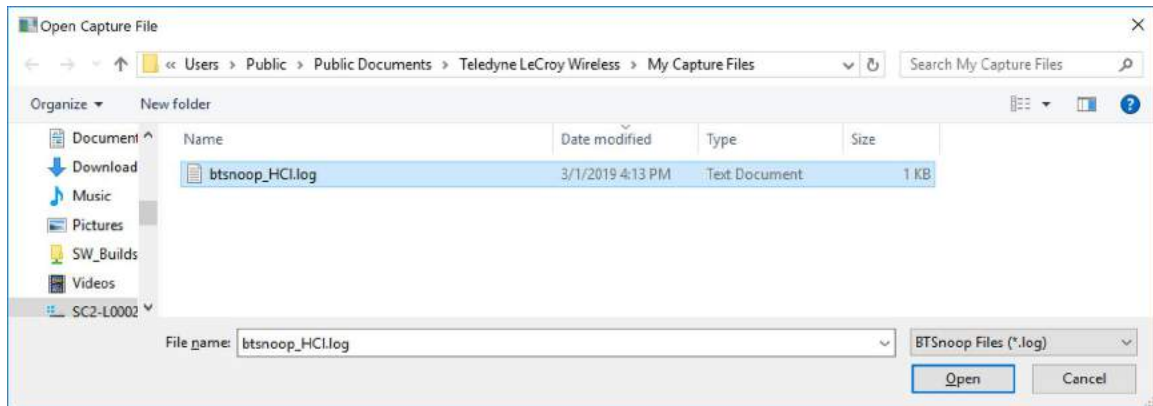


Figure 7 - Select Capture File

4. Open the **Main windows**
5. In the **Summary pane** protocol tabs select **HCI**. (See image below)
6. Using the Search box located in the Summary pane, search for an “HCI\_Link\_Key\_Notification” event in the capture. Note: If not found, the key may also be found searching for “HCI\_Link\_Key\_Request\_Reply”.

Frame#	Type	Opcodes	Opcode Group	Opcode Command	Event	Status	Handle	Credits	FBF	Length	Frame...	Delta
621	ACL Data						0x00b	24	29	00:00:00.0...		
622	ACL Data						0x00b	Available Hoofs...	Fast	34	39	00:00:00.0...
623	ACL Data						0x00b	Available Hoofs...	Fast	12	17	00:00:00.0...
624	ACL Data						0x00b	Available Hoofs...	Fast	12	17	00:00:00.0...
625	Event				HCI_Number_Of_Completed_Packets		0x00b	Available Hoofs...	Fast	5	8	00:00:00.0...
626	Event				HCI_ID_Capability_Response					9	12	00:00:00.2...
627	Event				HCI_User_Confirmation_Request					10	13	00:00:00.0...
628	Command	0x042c	Link Control	HCI_User_Confirmation_Request_Reply						6	10	00:00:00.0...
629	Event	0x042c	Link Control	HCI_User_Confirmation_Request_Reply	HCI_Command_Complete	Success				10	13	00:00:00.0...
630	Event				HCI_Simple_Pairing_Complete	Success				7	10	00:00:01.1...
631	Event				HCI_Link_Key_Notification					23	26	00:00:00.0...
632	Event				HCI_Authentication_Complete	Success	0x00b			3	6	00:00:00.0...
633	ACL Data						0x00b	Available Hoofs...	Fast	12	17	00:00:00.0...
634	ACL Data						0x00b	Available Hoofs...	Fast	16	21	00:00:00.0...
635	ACL Data						0x00b	Available Hoofs...	Fast	16	21	00:00:00.0...
636	ACL Data						0x00b	Available Hoofs...	Fast	16	21	00:00:00.0...
637	Event				HCI_Number_Of_Completed_Packets		0x00b	Available Hoofs...	Fast	5	8	00:00:00.0...
638	ACL Data						0x00b	Available Hoofs...	Fast	14	19	00:00:00.0...

Figure 8 - Find Link Key Notification

- 7. Once the event is found, look in the Decode pane under the “HCI” section for a field named “Link\_Key”. The value found is the Link Key, which can be copied and pasted in to the Security pane of the Sodera datasource window.

```
Decode
-----
Frame 631: (Controller) Len=26
+ HCI UART:
- HCI:
  Packet from: Controller
  HCI Event
    Event: HCI_Link_Key_Notification
    Total Length: 23
    + BD_ADDR: 0x00-24-1c-61-20-54
    Link_Key: 0x0d c5 21 c1 80 b7 3b 37 84 14 a1 c2 29 7a 3b fc
    Key_Type: Unauthenticated Combination Key
```

Figure 9 - Decode: Link Key Shown

Publish Date: 3/3/2023

## **F.3 Decrypting Encrypted *Bluetooth*® Low Energy**

---

### **F.3.1 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* central and central 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.



### F.3.2 Bluetooth® Low Energy Security

"Paris is quiet and the good citizens are content." Upon seizing power in 1799 Napoleon sent this message on Claude Chappe's optical telegraph. Chappe had invented a means of sending messages line-of-sight. The stations were placed approximately six miles apart and each station had a signaling device made of paddles on the ends of a rotating "regulator" arm whose positions represented code numbers. Each station was also outfitted with two telescopes for viewing the other stations in the link, and clocks were used to synchronize the stations. By 1803 a communications network extended from Paris across the countryside and into Belgium and Italy.



Figure 10 - Chappe's Optical Telegraph

Chappe developed several coding schemes through the next few years. The station operators only knew the codes, not what characters they represented. Not only was Chappe's telegraph system the first working network with protocols, synchronization of serial transmissions but it also used data encryption. Although cryptography has been around for millenniums—dating back to 2000 B.C. — Chappe, was the first to use it in a wide area network in the modern sense.



Figure 11 - Chappe's Telegraph Code

Of course anyone positioned between the telegraph stations that had Chappe's telegraph code in hand could decode the transmission. So securing the code was of paramount importance in Chappe's protocol.

**Modern wireless networks** such as *Bluetooth* Low Energy employ security measures to prevent similar potentially man-in-the-middle attacks that may have malicious intent.

*Bluetooth* Low Energy devices connected in a link can pass sensitive data by setting up a secure encrypted link. The process is similar to but not identical to *Bluetooth* BR/EDR Secure Simple Pairing. One difference is that in *Bluetooth* Low Energy the confidential payload includes a Message Identification Code (MIC) that is encrypted with the data. In *Bluetooth* BR/EDR only the data is encrypted. Also in *Bluetooth* Low Energy the secure link is more vulnerable to passive eavesdropping, however because of the short transmission periods this vulnerability is considered a low risk. The similarity to BR/EDR occurs with "shared secret key", a fundamental building block of modern wireless network security.

This paper describes the process of establishing a *Bluetooth* Low Energy secure link.

### F.3.3 Pairing

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

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

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

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

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

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

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

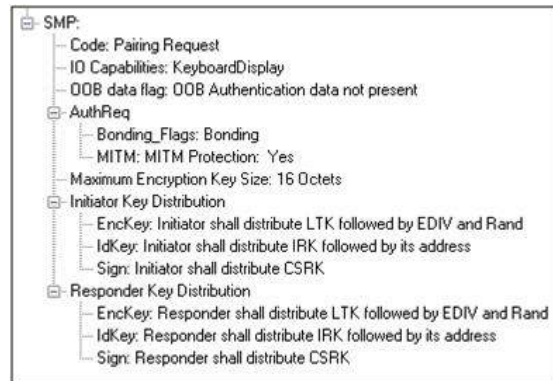


Figure 12 - Sample Initiator Pairing Request Decode (Wireless Protocol Suite software Main windows, Sodera, Sodera LE Low Energy capture)

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

### F.3.4 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**<sup>1</sup>. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

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

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



Figure 13 - Initiator Pairing Confirm Example (Wireless Protocol Suite software Main windows, Sodera, Sodera LE Low Energy capture)



Figure 14 - Responder Pairing Confirm Example (Wireless Protocol Suite software Main windows, Sodera, Sodera LE Low Energy capture)

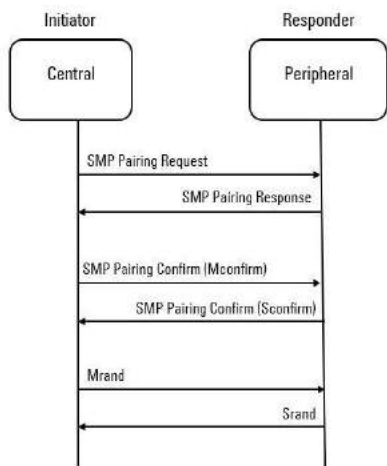


Figure 15 - Message Sequence Chart: SMP Pairing

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

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

<sup>1</sup>A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link.



### F.3.5 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**).

### F.3.6 Encryption Key Generation and Distribution

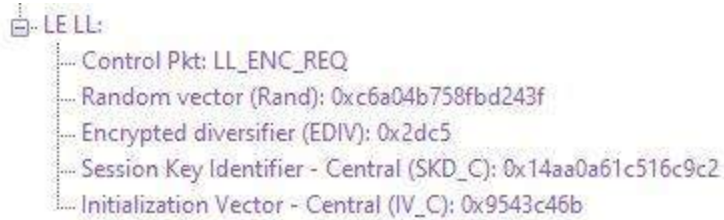


Figure 16 - Encryption Request from Central, Example (Wireless Protocol Suite software Main windows, Sodera, Sodera LE Low Energy capture)

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 central device will generate along with EDIV and Rand. Both the central and peripheral devices can distribute these numbers, but *Bluetooth* Low Energy is designed to conserve energy, so the central device is often resource constrained and does not have the database storage resources for holding LTKs. Therefore the central will

distribute LTK, EDIV, and Rand to the central device for storage. When a central begins a new encrypted session with a previously linked central device, it will request distribution of EDIV and Rand and will regenerate LTK.

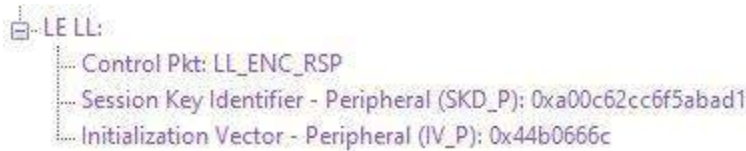


Figure 17 - Encryption Response from Peripheral, Example (Wireless Protocol Suite software Main windows, Sodera, Sodera LE Low Energy capture)

### F.3.7 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the central device to send Link Layer encryption request message (LL\_ENC\_REQ) that contains the SKD<sub>central</sub>. The SKD<sub>central</sub> is generated using the LTK. The central receives SKD<sub>central</sub>, generates SKD<sub>central</sub>, and generates SK by concatenating parts of SKD<sub>central</sub> and SKD<sub>central</sub>. The central device responds with an encryption response message (LL\_ENC\_RSP) that contains SKD<sub>central</sub>; the central will create the same SK.

Now that a SK has been calculated, the central and peripheral devices will now begin a handshake process. The central will transmit unencrypted LL\_START\_ENC\_REQ, but sets the central to receive encrypted data using the recently calculated SK. The central responds with encrypted LL\_START\_ENC\_RSP that uses the same SK just calculated and setting the central to receive encrypted data. Once the central receives the peripheral's encrypted LL\_START\_ENC\_RSP message and responds with an encrypted LL\_START\_ENC\_RSP message the *Bluetooth* Low Energy devices can now begin transmitting and receiving encrypted data.

### F.3.8 IRK and CSRK Revisited

Earlier in this paper it was stated that LTK would be the focus, however the IRK and CSRK were mentioned. We revisit these keys because they are used in situations that require a lesser level of security. First let us note that IRK and CSRK are passed in an encrypted link along with LTK and EDIV.

Use of the IRK and CSRK attempt to place an identity on devices operating in a piconet. The probability that two devices will have the same IRK and generate the same random number is low, but not absolute.

#### IRK and Bluetooth Low Energy Privacy Feature

*Bluetooth* Low Energy has a feature that reduces the ability of an attacker to track a device over a long period by frequently and randomly changing an advertising device's address. This is the privacy feature. This feature is not used in the discovery mode and procedures but is used in the connection mode and procedures.

If the advertising device was previously discovered and has returned to an advertising state, the device must be identifiable by trusted devices in future connections without going through discovery procedure again. The IRK stored in the trusted device will overcome the problem of maintaining privacy while saving discovery computational load and connection time. The advertising devices IRK was passed to the central device during initial bonding. The a central device will use the IRK to identify the advertiser as a trusted device.

#### CSRK and Signing for Authentication

*Bluetooth* Low Energy supports the ability to authenticate data sent over an unencrypted ATT bearer between two devices in a trust relationship. If authenticated pairing has occurred and encryption is not required (security mode 2) data signing is used if CSRK has been exchanged. The sending device attaches a digital signature after the data in the packet that includes a counter and a message authentication code (MAC). The key used to generate MAC is CSRK. Each peer device in a piconet will have a unique CSRK.

The receiving device will authenticate the message from the trusted sending device using the CSRK exchanged from the sending device. The counter is initialized to zero when the CSRK is generated and is incremented with each message signed with a given CSRK. The combination of the CSRK and counter mitigates replay attacks.

### F.4 Table of Acronyms

CSRK	Connection Signature Resolving Key
EDIV	Encrypted Diversifier
IO	Input and output
IRK	Identity Resolving Key
LTK	Long Term Key
Mconfirm	128-bit confirm value from initiator
MIC	Message Integrity Check
MITM	Man-in-the-middle
Mrand	128-bit random number used to generate Mconfirm
OOB	Out of Band
RAND	Random Number

Sconfirm	128-bit confirmation value from the responder
SK	Session key
SMP	Security Manager Protocol
Srand	128-bit random number used to generate Sconfirm
SSP	Secure Simple Pairing
STK	Short Term Key
TK	Temporary Key

## Appendix G: ra X500 Wi-Fi 6E Frequencies

Table A.1 - X500 Wi-Fi 6E Frequencies

Channel	Frequency (MHz)	Channel Width
1	2412	20, +40
2	2417	20, +40
3	2422	20, +40
4	2427	20, +40
5	2432	20, +40, -40
6	2437	20, +40, -40
7	2442	20, +40, -40
8	2447	20, +40, -40
9	2452	20, +40, -40
10	2457	20, -40
11	2462	20, -40
12	2467	20, -40
13	2472	20, -40
36	5180	20, 40, 80, 160
40	5200	20, 40, 80, 160
44	5220	20, 40, 80, 160
48	5240	20, 40, 80, 160
52	5260	20, 40, 80, 160
56	5280	20, 40, 80, 160
60	5300	20, 40, 80, 160

Table A.1 - X500 Wi-Fi 6E Frequencies (continued)

Channel	Frequency (MHz)	Channel Width
64	5320	20, 40, 80, 160
100	5500	20, 40, 80, 160
104	5520	20, 40, 80, 160
108	5540	20, 40, 80, 160
112	5560	20, 40, 80, 160
116	5580	20, 40, 80, 160
120	5600	20, 40, 80, 160
124	5620	20, 40, 80, 160
128	5640	20, 40, 80, 160
132	5660	20, 40, 80
136	5680	20, 40, 80
140	5700	20, 40, 80
144	5720	20, 40, 80
149	5745	20, 40, 80
153	5765	20, 40, 80
157	5785	20, 40, 80
161	5805	20, 40, 80
165	5825	20
169	5845	20
1	5955	20, 40, 80, 160
5	5975	20, 40, 80, 160
9	5995	20, 40, 80, 160
13	6015	20, 40, 80, 160
17	6035	20, 40, 80, 160
21	6055	20, 40, 80, 160
25	6075	20, 40, 80, 160
29	6095	20, 40, 80, 160
33	6115	20, 40, 80, 160
37	6135	20, 40, 80, 160

Table A.1 - X500 Wi-Fi 6E Frequencies (continued)

Channel	Frequency (MHz)	Channel Width
41	6155	20, 40, 80, 160
45	6175	20, 40, 80, 160
49	6195	20, 40, 80, 160
53	6215	20, 40, 80, 160
57	6235	20, 40, 80, 160
61	6255	20, 40, 80, 160
65	6275	20, 40, 80, 160
69	6295	20, 40, 80, 160
73	6315	20, 40, 80, 160
77	6335	20, 40, 80, 160
81	6355	20, 40, 80, 160
85	6375	20, 40, 80, 160
89	6395	20, 40, 80, 160
93	6415	20, 40, 80, 160
97	6435	20, 40, 80, 160
101	6455	20, 40, 80, 160
105	6475	20, 40, 80, 160
109	6495	20, 40, 80, 160
113	6515	20, 40, 80, 160
117	6535	20, 40, 80, 160
121	6555	20, 40, 80, 160
125	6575	20, 40, 80, 160
129	6595	20, 40, 80, 160
133	6615	20, 40, 80, 160
137	6635	20, 40, 80, 160
141	6655	20, 40, 80, 160
145	6675	20, 40, 80, 160
149	6695	20, 40, 80, 160
153	6715	20, 40, 80, 160

Table A.1 - X500 Wi-Fi 6E Frequencies (continued)

Channel	Frequency (MHz)	Channel Width
157	6735	20, 40, 80, 160
161	6755	20, 40, 80, 160
165	6775	20, 40, 80, 160
169	6795	20, 40, 80, 160
173	6815	20, 40, 80, 160
177	6835	20, 40, 80, 160
181	6855	20, 40, 80, 160
185	6875	20, 40, 80, 160
189	6895	20, 40, 80, 160
193	6915	20, 40, 80, 160
197	6935	20, 40, 80, 160
201	6955	20, 40, 80, 160
205	6975	20, 40, 80, 160
209	6995	20, 40, 80, 160
213	7015	20, 40, 80, 160
217	7035	20, 40, 80, 160
221	7055	20, 40, 80, 160

---

Publish Date: 3/3/2023

