PANalyzr™ Protocol Analyzer User Guide for Windows

11/17/2022

Table of Contents

Spanalytics Contact Details

Technical Support: support@panalyzr.com
Technical Support Phone: 804-364-1050, option 6

Sales: sales@panalyzr.com

Other inquiries: support@panalyzr.com

Open-Source Utilities

The PANalyzr protocol analyzer software uses the open-source utility Wireshark to provide additional features to the system. The modified binary is included in this installation, and the modified source code is available upon request.

- □ Knob - The original Knob code can be found at https://github.com/francozappa/knob. The source code modifications made are included in this installation (located in the **C:\Program Files (x86)\Spanalytics\PANalyzr** directory after the installation completes)
- □ E0 – The original E0 code can be found at https://github.com/adelmas/e0. The source code modifications made for this installation are available upon request
- □ Brackle – The original crackle code can be found at https://github.com/mikeryan/crackle. The source code modifications made for this installation are available upon request
- □ KillerZee – The original code can be found at https://github.com/joswr1ght/killerzee. The source code modifications made for this installation are available upon request
- □ Z-Wave Wireshark plugin – The original code can be found at https://github.com/AFITWiSec/EZ-Wave. The source code modifications for this installation are available upon request
- □ Wireshark – The original Wireshark code can be found at https://www.wireshark.org/download.html. The source code modifications made for this installation are available upon request
- □ libpcap – The original libpcap code can be found at https://www.tcpdump.org/index.html#latest-releases

License Clauses

libpcap

Introduction

This procedure describes the steps necessary to run the PANalyzr protocol analyzer hardware and software on a Windows 10 machine.

Hardware

The PANalyzr software works with the following hardware:

- PANalyzr - (Bluetooth Low Energy, Bluetooth BR/EDR Classic, and IEEE 802.15.4 2.4GHz) wideband protocol analyzer
- USB GPS receiver - Purchased separately by the user. The PANalyzr software has been tested with the GlobalSat BU-353 USB GPS receiver. However, a similar serial/TTY device that adheres to the NMEA standard should work as well
- Optional hardware items - Purchased from Spanalytics at additional cost and requires additional software licensing in the PANalyzr software
    - Internet of Things (IoT) Expansion Pack (EP)
        - Rnode LoRa adapter
        - Exegin Q59 dongle for IEEE 802.15.4 2.4GHz and Sub-GHz packet capturing (non-production use only)
        - Silicon Labs ACC-UZB3-U for Z-Wave packet capturing
        - Panda N600 Dual Band (2.4GHz and 5.0GHz) Wireless N USB adapter for Wi-Fi packet capturing
        - Laird BT851 or Edimax BT8500 Bluetooth adapter for active Bluetooth device characterization
    - FindIT

Setup

- □ Make sure your machine is powered on, and you have logged in prior to attaching the applicable hardware listed above
- □ Be sure to use the cable provided for the PANalyzr protocol analyzer, and attach it to a USB 3.0 port on the host computer
- □ PANalyzr indicator lights:
    - Blue LED light – Hardware is in standby mode but not yet active. Will change to active mode when the PANalyzr software is started the first time.
    - Green LED light – Hardware is in active mode.
    - Red LED light – An error was detected. To resolve this, re-attach the PANalyzr protocol analyzer.
    - Purple LED light – An error was detected. To resolve this, re-attach the PANalyzr protocol analyzer.

Help Menu

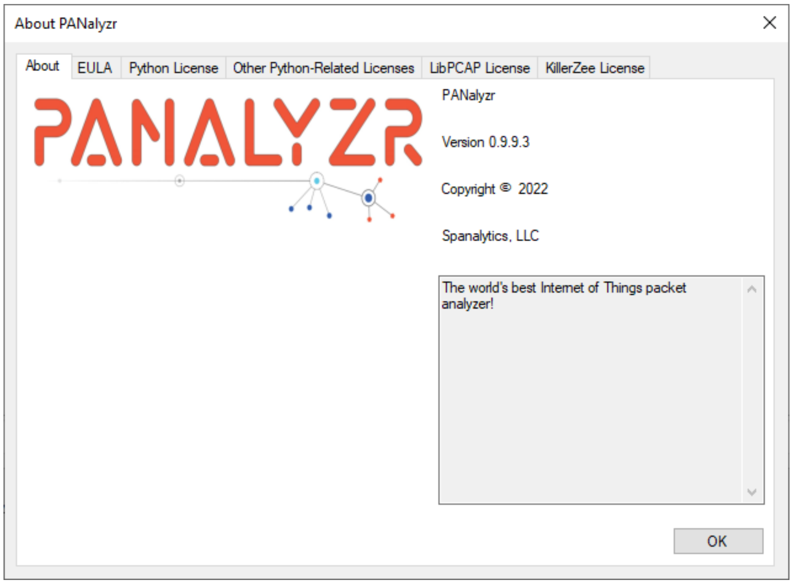
The Help menu provides general system and licensing information about the PANalyzr software.

License Manager

Displays information about the current software license, including which add-on features have been purchased and enabled (ex. IoT Expansion Pack, FindIT, etc.)

About

Displays the PANalyzr software version number, the Spanalytics EULA, and open-source software licensing information.



PANalyzr

Version 0.9.9.3

Copyright © 2022

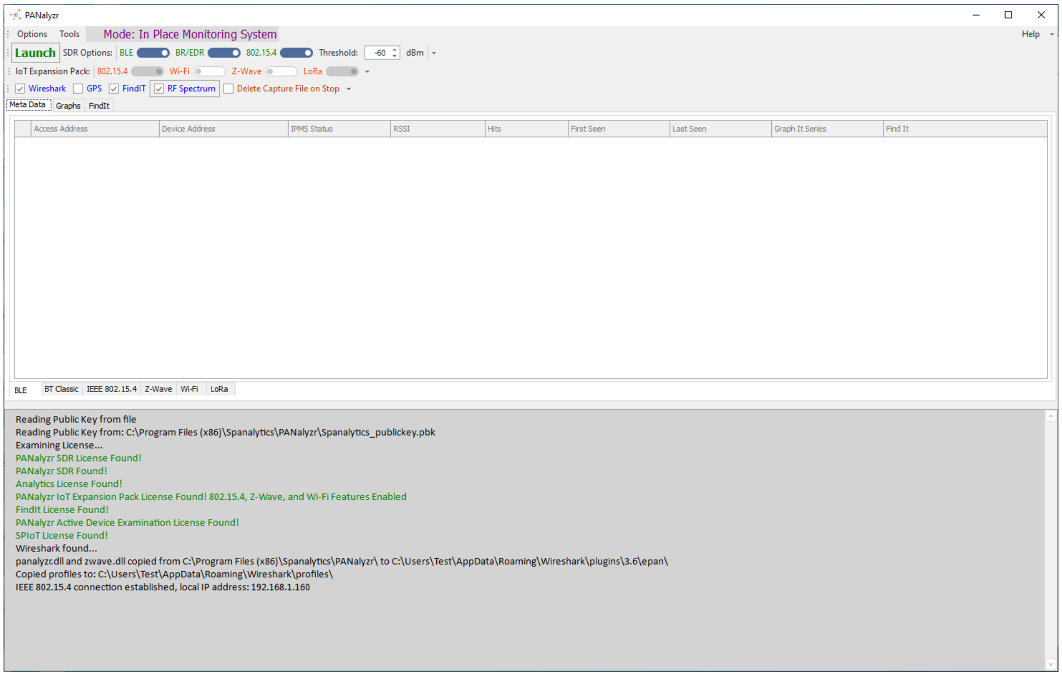
Spanalytics, LLC

The world's best Internet of Things packet analyzer!

PANalyzr Operation

- □ On the Desktop, double-click the **PANalyzr.exe** icon
- □ The PANalyzr main window will open

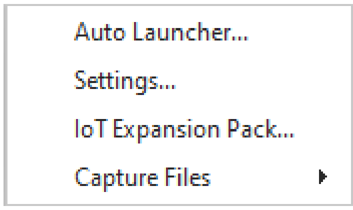
Capture Configuration & Settings



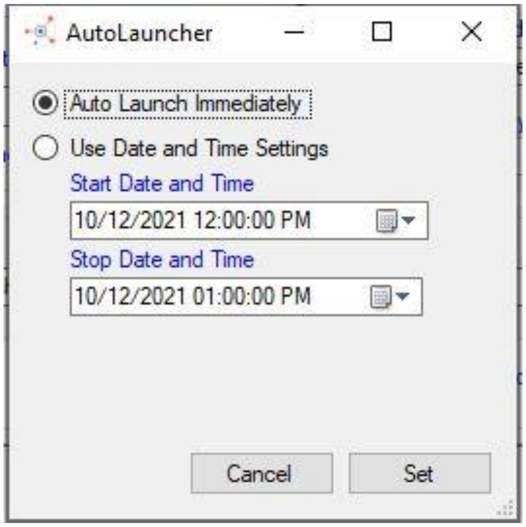
```
Reading Public Key from file
Reading Public Key from: C:\Program Files (x86)\Spanalytics\PANalyzr\Spanalytics_publickey.pbk
Examining License...
PANalyzr SDR License Found!
PANalyzr SDR Found!
Analytics License Found!
PANalyzr IoT Expansion Pack License Found! 802.15.4, Z-Wave, and Wi-Fi Features Enabled
FindIt License Found!
PANalyzr Active Device Examination License Found!
SPIoT License Found!
Wireshark found...
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to C:\Users\Test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\Test\AppData\Roaming\Wireshark\profiles\
IEEE 802.15.4 connection established, local IP address: 192.168.1.160
```

- □ Check the **Wireshark** checkbox to launch Wireshark during the capture. Uncheck the box to not launch Wireshark during the capture, and display meta data only
- □ Check the **GPS** checkbox to get GPS data during the capture. If a USB GPS receiver is connected to capture device location details, the software will automatically identify and connect to it
- □ Check the **FindIt** checkbox to utilize the FindIT hardware. If the hardware is connected, the software will automatically identify and connect to it
- □ Check the **Delete Capture File on Stop** checkbox to delete the current pcap file and close Wireshark when the **Stop** button is clicked
  - ▪ To delete a specific capture file navigate to the **Options** menu, select **Capture Files -> Pick Files to Delete…**
- □ **RF Spectrum –** Enables displaying of the graph that shows the forty Bluetooth Low Energy channels with 2 MHz spacing and detects the RSSI of the surrounding devices outputting on those channels
- □ **Graphs** – Enables displaying of the *RSSI over Time* and *RF Channel vs. Hits* graphs

- □ To set a timer, select the **Options** menu and choose **Auto Launcher**



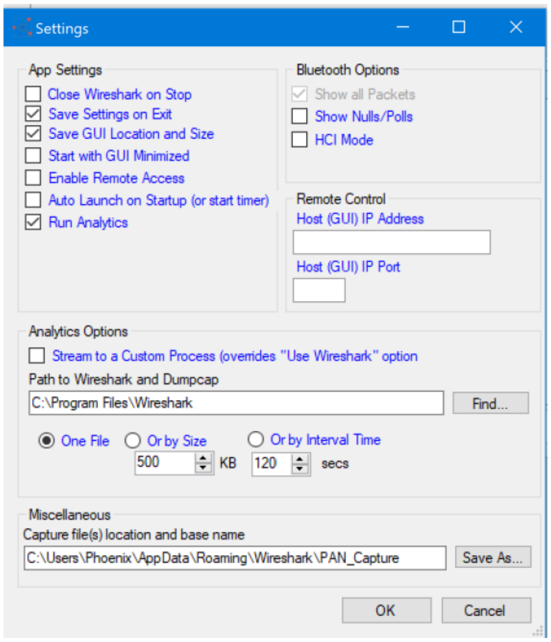
  - **Auto Launch Immediately** - Start Wireshark when PANalyzr software launches
  - **Use Date and Time Settings -** Set a Start and Stop Date and Time.



● Auto Launch Immediately
○ Use Date and Time Settings
Start Date and Time
10/12/2021 12:00:00 PM
Stop Date and Time
10/12/2021 01:00:00 PM

  - Delete

- □ In the **Options** menu, select **Settings**



App Settings
□ Close Wireshark on Stop
☑ Save Settings on Exit
☑ Save GUI Location and Size
□ Start with GUI Minimized
□ Enable Remote Access
□ Auto Launch on Startup (or start timer)
☑ Run Analytics

Bluetooth Options
☑ Show all Packets
□ Show Nulls/Polls
□ HCI Mode

Remote Control
Host (GUI) IP Address
Host (GUI) IP Port

Analytics Options
□ Stream to a Custom Process (ovemides "Use Wireshark" option
Path to Wireshark and Dumpcap
C:\Program Files\Wireshark
● One File ○ Or by Size ○ Or by Interval Time
500 KB 120 secs

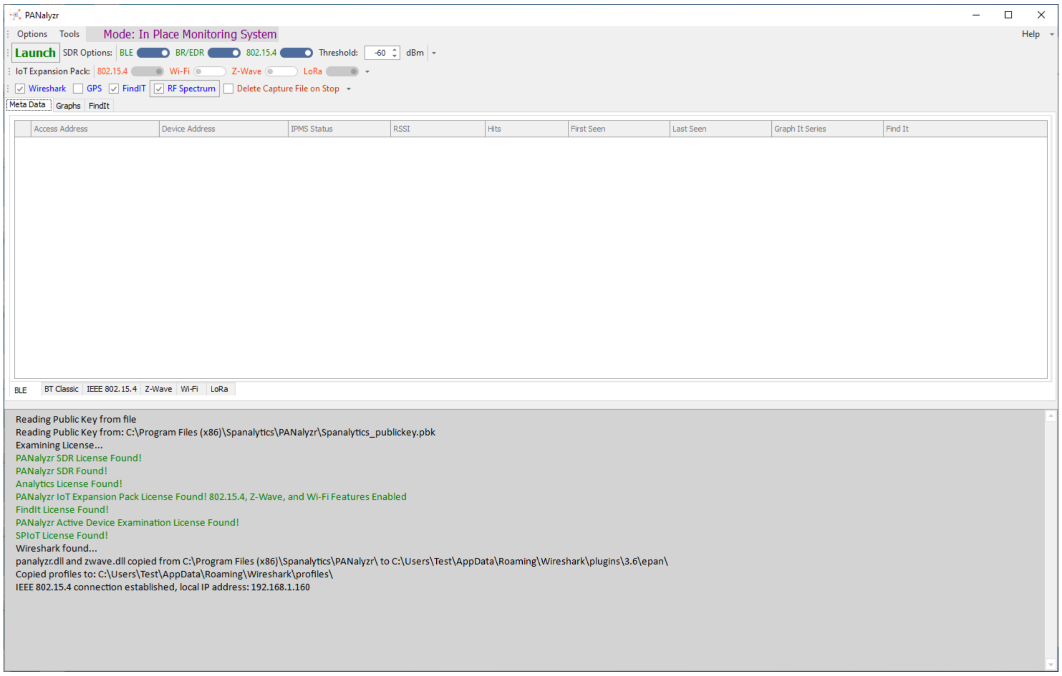
Miscellaneous
Capture file(s) location and base name
C:\Users\Phoenix\AppData\Roaming\Wireshark\PAN_Capture

- **Close Wireshark on Stop** - Automatically close Wireshark when the **Stop** button is clicked. (disabled by default)
- **Save Settings on Exit** - This option will save the PANalyzr settings for subsequent use (enabled by default)
- **Save GUI Location and Size** - This option will save the desired window size and location within the display for subsequent use (enabled by default)
- **Start with GUI minimized** - Launch the PANalyzr application with GUI minimized in the taskbar.
- **Enable Remote access** – Once the application has been restarted, PANalyzr will be configured to enable a server port. This allows a remote application to send the commands *Connect, Start, Stop, and Disconnect* (as a string) to control packet capturing over a TCP/IP socket. The IP address and port to connect to will be listed in the settings tab under *Host (GUI) IP Address* and *Host (GUI) Port*.
- **Auto launch on Startup (or start timer)** - Enables the Autolauncher described above.
- **Run Analytics** – Perform meta data analytics while a live capture is in progress. If this checkbox is unchecked, no meta data will be displayed for any protocols
- **Show Nulls/Polls -** Configures PANalyzr to display BR/EDR nulls and polls packets
- **HCI mode** - Can be used to capture Bluetooth Hardware Control Interface (HCI) packets in Wireshark. To use this mode, the computer must have:
    - on-board internal Bluetooth
    - or the Bluetooth adapter in the IoT Expansion Pack
    - or another Bluetooth adapter that works with the Windows Bluetooth device driver
- **Analytics Options** –
    - **Stream to a Custom Process (overrides "Use Wireshark" option)** - Pipes and interfaces will be created according to the SDR and IoT Expansion Pack options selected by the user, but no packet capturing utility will be launched when the main **Launch** button is clicked
- **Path to Wireshark and Dumpcap** – (Required) Specify where the Wireshark executables (Wireshark.exe, tshark.exe) are installed on the system by clicking the **Find…** button
- Options for saving capture files are as follows:
    - **One File:** PANalyzr will save the recent capture into one pcapng file upon stopping capture; this is selected by default
    - **Or by Size:** PANalyzr will create a capture file every time the user-specified size is reached. EX *1000KB*
    - **Or by Interval Time:** PANalyzr will create a capture file once the the user specified time is reached. EX *60 secs, 900 secs*
- **Capture file(s) location and base name** – (Required) A file path and base name must be specified for the capture files that PANalyzr creates. By default the path and the base name

is *"C:\Users\<username>\AppData\Roaming\Wireshark\PAN_capture"* and can be changed by clicking the **Save As…** button

- □ The **Status window** provides various system status updates, including licensing information (which will vary depending on purchased configurations), the software version, Wireshark application configuration, etc.

2.4GHz Packet Capturing (Bluetooth Low Energy, Bluetooth Classic, and/or 802.15.4)



Mode: In Place Monitoring System

SDR Options: BLE BR/EDR 802.15.4 Threshold: -60 dBm

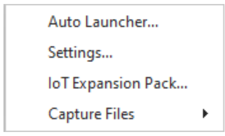
☑ Wireshark □ GPS ☑ FindIT ☑ RF Spectrum □ Delete Capture File on Stop

```
Reading Public Key from file
Reading Public Key from: C:\Program Files (x86)\Spanalytics\PANalyzr\Spanalytics_publickey.pbk
Examining License...
PANalyzr SDR License Found!
PANalyzr SDR Found!
Analytics License Found!
PANalyzr IoT Expansion Pack License Found! 802.15.4, Z-Wave, and Wi-Fi Features Enabled
FindIt License Found!
PANalyzr Active Device Examination License Found!
SPIoT License Found!
Wireshark found...
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to C:\Users\Test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\Test\AppData\Roaming\Wireshark\profiles\
IEEE 802.15.4 connection established, local IP address: 192.168.1.160
```

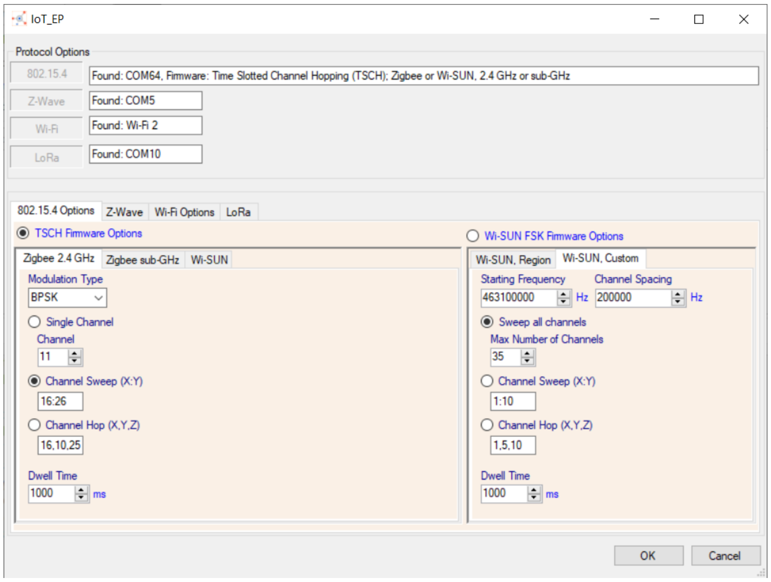
- □ Select one or more of the **SDR Options** for data capture: **BLE, BR/EDR,** or **802.15.4**
  - ▪ The user may also set a power level threshold for capturing transmitted data in the **Set Threshold** scroll box; the initial system default is -60 dBm (decibel-milliwatts)

IoT Expansion Packet Capturing

- ☐ Select one or more of the options listed in the IoT Expansion Pack bar: **802.15.4, Wi-Fi, Z-Wave** or **LoRa**
- ☐ Click **Options -> IoT Expansion Pack…** to view the settings menu for the IoT Expansion Pack



- ☐ In the **Protocol Options** window**,** if the protocol adapter has been detected the text “Found:” will be displayed along with interface information for the hardware



Protocol Options

802.15.4: Found: COM64, Firmware: Time Slotted Channel Hopping (TSCH); Zigbee or Wi-SUN, 2.4 GHz or sub-GHz

Z-Wave: Found: COM5

Wi-Fi: Found: Wi-Fi 2

LoRa: Found: COM10

● TSCH Firmware Options

Modulation Type: BPSK

○ Single Channel

Channel: 11

● Channel Sweep (X:Y): 16:26

○ Channel Hop (X,Y,Z): 16,10,25

Dwell Time: 1000 ms

○ Wi-SUN FSK Firmware Options

Starting Frequency: 463100000 Hz

Channel Spacing: 200000 Hz

● Sweep all channels

Max Number of Channels: 35

○ Channel Sweep (X:Y): 1:10

○ Channel Hop (X,Y,Z): 1,5,10

Dwell Time: 1000 ms

802.15.4 Options Tab

The 802.15.4 Option tab supports configuration for packet capturing of three 802.15.4 specifications: **Zigbee 2.4GHz, Zigbee sub-GHz,** and **Wi-SUN**

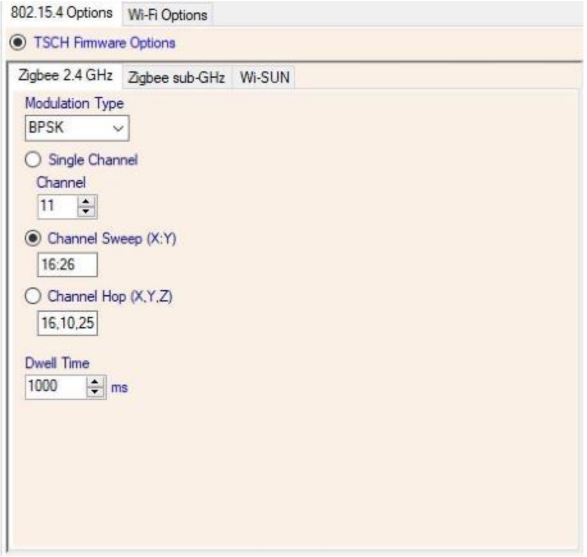
TSCH Firmware Option – Zigbee 2.4 GHz

Modulation Types: BPSK | ASK | O-QPSK

Dwell Options: Single Channel | Channel Sweep (separate channels by commas) | Channel Hop (separate channels by commas)

Channels: 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26

Dwell Time: 1000ms – 10000ms = 1 second – 10 seconds



● TSCH Firmware Options

Modulation Type: BPSK

○ Single Channel

Channel: 11

● Channel Sweep (X:Y): 16:26

○ Channel Hop (X,Y,Z): 16,10,25

Dwell Time: 1000 ms

TSCH Firmware Option – Zigbee sub-GHz

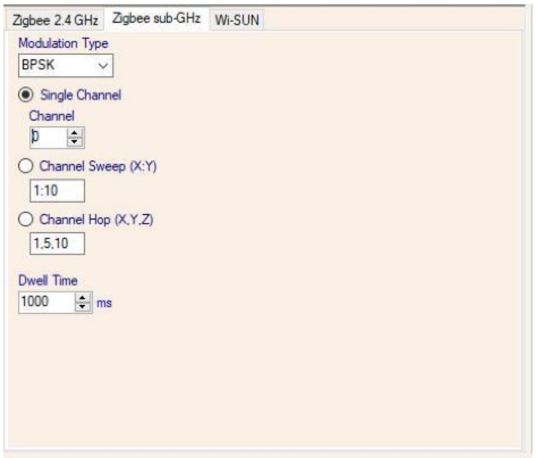
Options for **868MHz and 915MHz packet** capturing

Modulation Types: BPSK | O-QPSK

Dwell Options: Single Channel | Channel Sweep (separate channels by colons) | Channel Hop (separate channels by commas)

Channels: 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Dwell Time: 1000ms – 10000ms = 1 second – 10 seconds



Modulation Type: BPSK

● Single Channel

Channel: 0

○ Channel Sweep (X:Y): 1:10

○ Channel Hop (X,Y,Z): 1,5,10

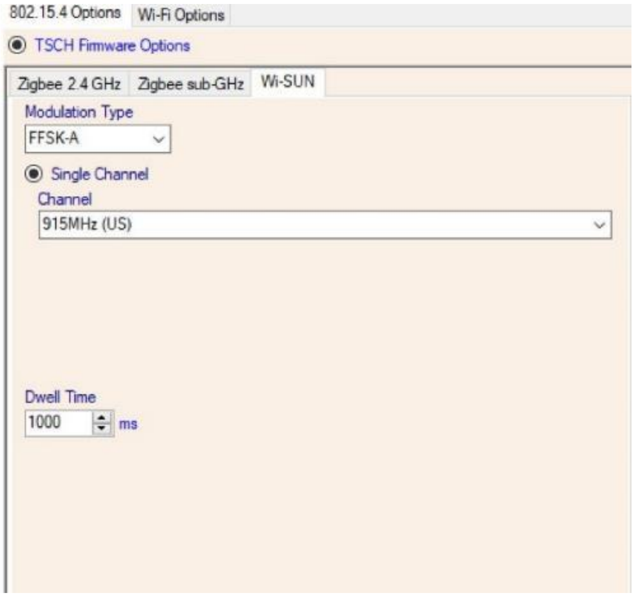
Dwell Time: 1000 ms

TSCH Firmware Option – Wi-Sun

Modulation Types: FFSK-A, FFSK-B | O-QPSK- A, O-QPSK-B, O-QPSK-C | OFDM-OPT1, OFDM-OPT2, OFDM-OPT3, OFDM-OPT4 | O-QPSK-Legacy | BPSK-Legacy

Channels: 169MHz | 433MHz | 450MHz | 470MHz | 780MHz | 863MHz | 866MHz | 868MHz | 896MHz | 901MHz | 915MHz | 917MHz | 919MHz | 920MHz | 928MHz | 950MHz | 1427MHz | 2380MHz | 2450MHz

Dwell Time: 1000ms – 10000ms = 1 second – 10 seconds



● TSCH Firmware Options

Modulation Type: FFSK-A

● Single Channel

Channel: 915MHz (US)

Dwell Time: 1000 ms

Wi-SUN FSK Firmware Option – Wi-SUN, Region

Channels: 0 | 1 | 2 | 3 | 4 | 5| 6 | 7| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60

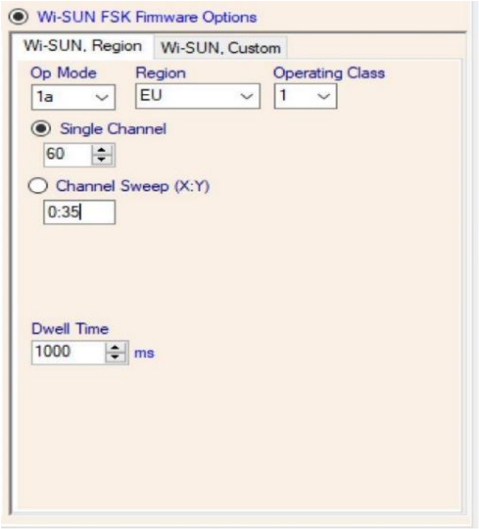
Region: WW = Worldwide | NA = North America | USA | Japan | EU = Europe | China | India | Mexico | Brazil | AUS | NZL | Korea | Philippines | Malaysia | Hong Kong | Singapore | Thailand | Vietnam

Operation Mode (Op Mode): 1a | 1b | 2a | 2b | 3 | 4a | 4b | 5

Operating Class: 1 | 2 | 3 | 4 | 5

Dwell Options: Single Channel | Channel Sweep (separate channels by commas)

Dwell Time: 1000ms – 10000ms = 1 second – 10 seconds



● Wi-SUN FSK Firmware Options

Wi-SUN, Region | Wi-SUN, Custom

Op Mode: 1a

Region: EU

Operating Class: 1

● Single Channel: 60

○ Channel Sweep (X:Y): 0:35

Dwell Time: 1000 ms

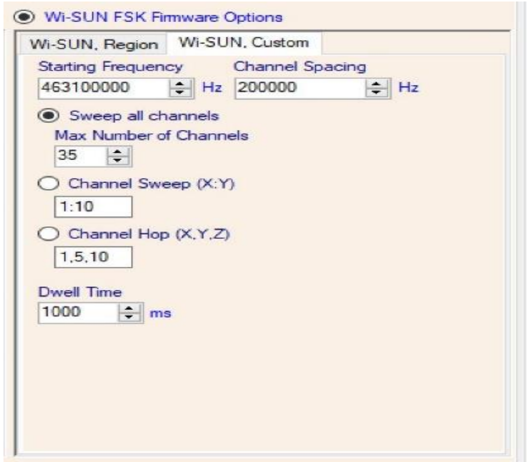
Wi-SUN FSK Firmware Option – Wi-SUN, Custom

Starting Frequency: Set the necessary hertz (1 – 1000000000Hz)

Channel Spacing: Set the necessary hertz (1 – 1000000000Hz)

Dwell Options: Sweep all channels, set a max number of channels |Channel Sweep (separate channels by commas) | Channel Hop (separate channels by commas)

Dwell Time: 1000ms – 10000ms = 1 second – 10 seconds



● Wi-SUN FSK Firmware Options

Wi-SUN, Region | Wi-SUN, Custom

Starting Frequency: 463100000 Hz

Channel Spacing: 200000 Hz

● Sweep all channels

Max Number of Channels: 35

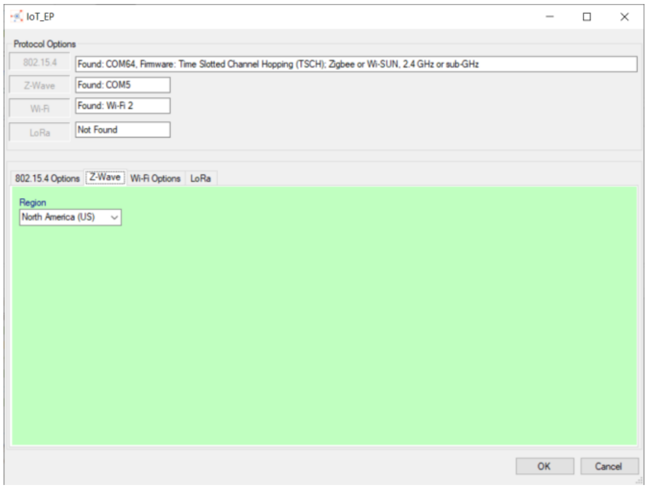
○ Channel Sweep (X:Y): 1:10

○ Channel Hop (X,Y,Z): 1,5,10

Dwell Time: 1000 ms

Z-Wave Tab

Regions: Europe | North American (US) | Australia | New Zealand | Hong Kong | Malaysia | India | Japan | Russia | Israel | Korea | China



802.15.4: Found: COM64, Firmware: Time Slotted Channel Hopping (TSCH); Zigbee or Wi-SUN, 2.4 GHz or sub-GHz

Z-Wave: Found: COM5

Wi-Fi: Found: Wi-Fi 2

LoRa: Not Found

Region: North America (US)

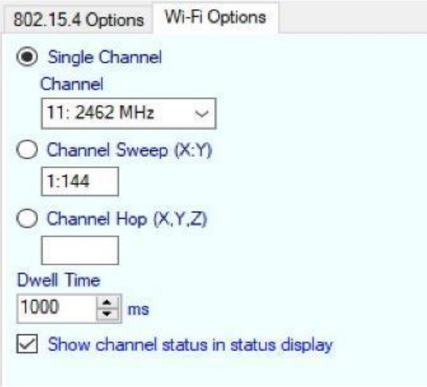
Wi-Fi Options Tab

Channels: 1: 2412 MHz | 2: 2417 MHz | 3: 2422 MHz | 4: 2427 MHz | 5: 2432 MHz | 6: 2437 MHz | 7: 2442 MHz | 8: 2447 MHz | 9: 2452 MHz | 10: 2457 MHz | 11: 2462 MHz | 12: 2467 MHz | 13: 2472 MHz |14: 2484 MHz | 32: 5160 MHz | 34: 5170 MHz | 36: 5180 MHz | 38: 5190 MHz | 40: 5200 MHz | 42: 5210 MHz | 44: 5220 MHz | 46: 5230 MHz | 48: 5240 MHz | 50: 5250 MHz | 52: 5260 MHz | 54: 5270 MHz | 56: 5280 MHz | 58: 5290 MHz | 60: 5300 MHz | 62: 5310 MHz | 64: 5320 MHz | 68: 5340 MHz | 96: 5480 MHz | 100: 5500 MHz | 102: 5510 MHz | 104: 5520 MHz | 106: 5530 MHz | 108: 5540 MHz | 110: 5550 MHz | 112: 5560 MHz | 114: 5570 MHz | 116: 5580 MHz | 118: 5590 MHz | 120: 5600 MHz | 122: 5610 MHz | 124: 5620 MHz | 126: 5630 MHz | 128: 5640 MHz | 132: 5660 MHz | 134: 5670 MHz | 136: 5680 MHz | 138: 5690 MHz | 140: 5700 MHz | 142: 5710 MHz | 144: 5720 MHz | 149: 5745 MHz | 151: 5755 MHz | 153: 5765 MHz | 155: 5775 MHz | 157: 5785 MHz | 159: 5795 MHz | 161: 5805 MHz | 163: 5815 MHz | 165: 5825 MHz | 167: 5835 MHz | 169: 5845 MHz | 171: 5855 MHz | 173: 5865 MHz | 175: 5875 MHz | 177: 5885 MHz

Dwell Options: Single Channel | Channel Sweep (separate channels by commas) | Channel Hop (separate channels by commas)

Dwell Time: 1000ms – 10000ms = 1 second – 10 seconds

Channel Status: Display the Wi-Fi channel(s) in the status window



● Single Channel

Channel: 11: 2462 MHz

○ Channel Sweep (X:Y): 1:144

○ Channel Hop (X,Y,Z):

Dwell Time: 1000 ms

☑ Show channel status in status display

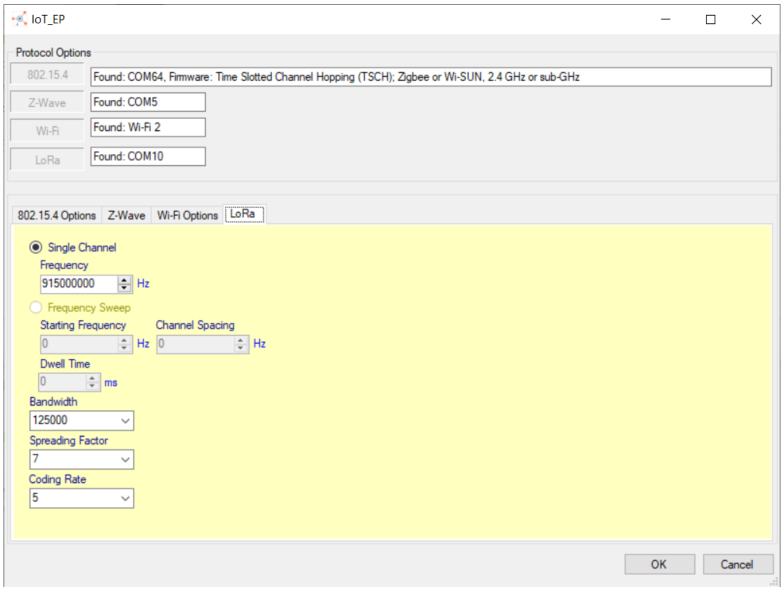
LoRa Tab

Dwell Options: Single Channel (frequency)

Bandwidth: 125000 | 250000

Spreading Factor: 7 | 8 | 9 | 10 | 11 | 12

Coding Rate: 5 | 6 | 7 | 8



Protocol Options

802.15.4: Found: COM64, Firmware: Time Slotted Channel Hopping (TSCH); Zigbee or Wi-SUN, 2.4 GHz or sub-GHz

Z-Wave: Found: COM5

Wi-Fi: Found: Wi-Fi 2

LoRa: Found: COM10

● Single Channel

Frequency: 915000000 Hz

○ Frequency Sweep

Starting Frequency: 0 Hz   Channel Spacing: 0 Hz

Dwell Time: 0 ms

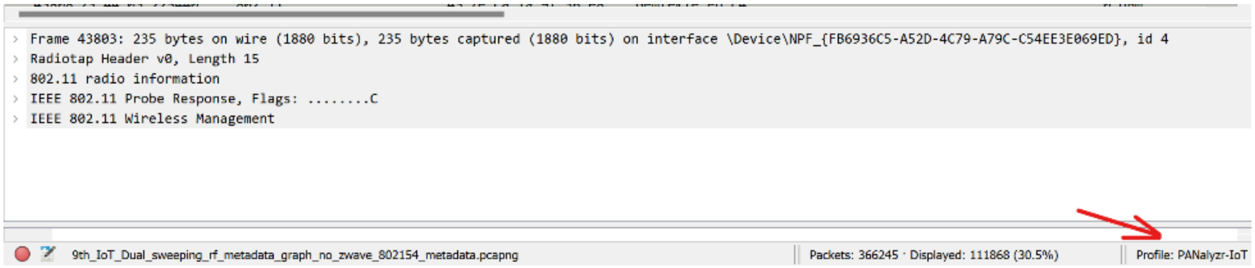
Bandwidth: 125000

Spreading Factor: 7

Coding Rate: 5

Identifying IoT Protocols in Wireshark

In Wireshark, change the Profile setting to **PANalyzr-IoT**, located at the bottom right of Wireshark, to quickly identify all Bluetooth, Z-Wave, 802.15.4, Wi-Fi and LoRa packets.



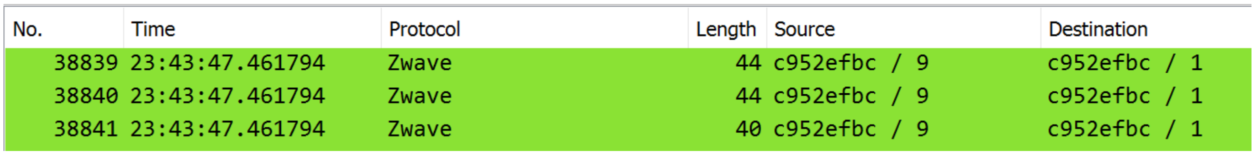
```
> Frame 43803: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on interface \Device\NPF_{FB6936C5-A52D-4C79-A79C-C54EE3E069ED}, id 4
> Radiotap Header v0, Length 15
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: ........C
> IEEE 802.11 Wireless Management
```

9th_IoT_Dual_sweeping_rf_metadata_graph_no_zwave_802154_metadata.pcapng | Packets: 366245 · Displayed: 111868 (30.5%) | Profile: PANalyzr-IoT

Z-Wave

If Z-Wave capturing is enabled, captured packets will be displayed with this coloring rule in Wireshark

Coloring: Green

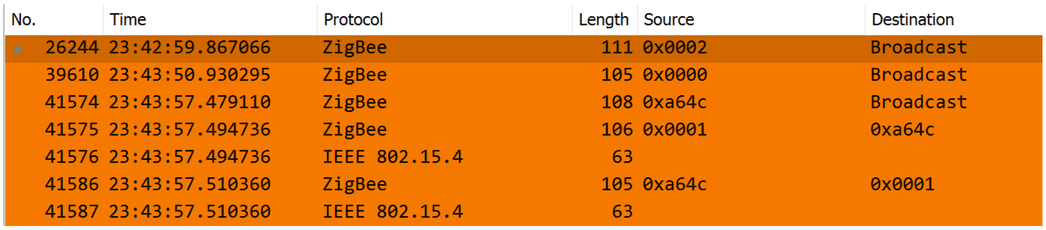


No.	Time	Protocol	Length	Source	Destination
38839	23:43:47.461794	Zwave	44	c952efbc / 9	c952efbc / 1
38840	23:43:47.461794	Zwave	44	c952efbc / 9	c952efbc / 1
38841	23:43:47.461794	Zwave	40	c952efbc / 9	c952efbc / 1

802.15.4

If 802.15.4 capturing is enabled, captured packets will be displayed with this coloring rule in Wireshark

Coloring: Orange

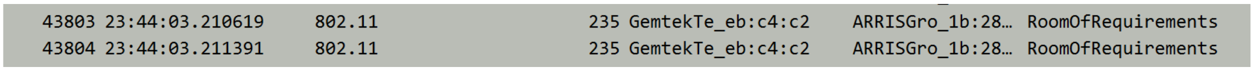


No.	Time	Protocol	Length	Source	Destination
26244	23:42:59.867066	ZigBee	111	0x0002	Broadcast
39610	23:43:50.930295	ZigBee	105	0x0000	Broadcast
41574	23:43:57.479110	ZigBee	108	0xa64c	Broadcast
41575	23:43:57.494736	ZigBee	106	0x0001	0xa64c
41576	23:43:57.494736	IEEE 802.15.4	63		
41586	23:43:57.510360	ZigBee	105	0xa64c	0x0001
41587	23:43:57.510360	IEEE 802.15.4	63		

Wi-Fi

If Wi-Fi capturing is enabled, captured packets will be displayed with this coloring rule in Wireshark

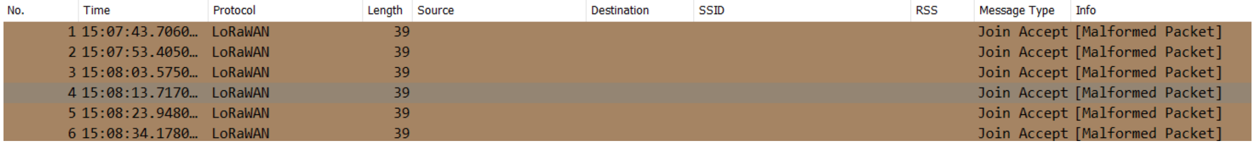
Coloring: Gray



43803	23:44:03.210619	802.11	235	GemtekTe_eb:c4:c2	ARRISGro_1b:28…	RoomOfRequirements
43804	23:44:03.211391	802.11	235	GemtekTe_eb:c4:c2	ARRISGro_1b:28…	RoomOfRequirements

LoRa

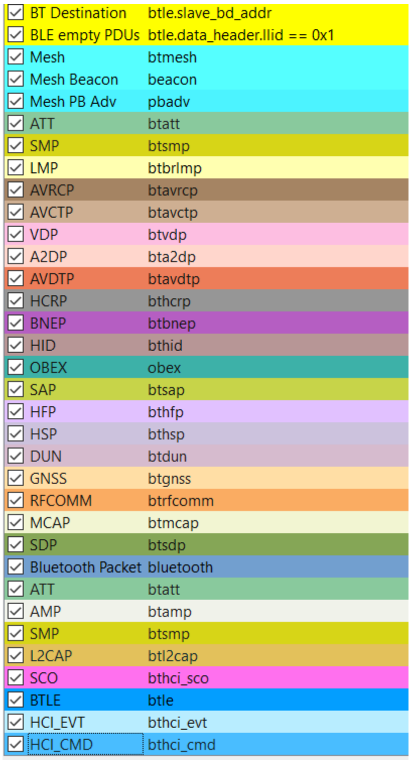
If LoRa capturing is enabled, captured packets will be displayed with this coloring rule in Wireshark



No.	Time	Protocol	Length	Source	Destination	SSID	RSS	Message Type	Info
1	15:07:43.7060…	LoRaWAN	39					Join Accept	[Malformed Packet]
2	15:07:53.4050…	LoRaWAN	39					Join Accept	[Malformed Packet]
3	15:08:03.5750…	LoRaWAN	39					Join Accept	[Malformed Packet]
4	15:08:13.7170…	LoRaWAN	39					Join Accept	[Malformed Packet]
5	15:08:23.9480…	LoRaWAN	39					Join Accept	[Malformed Packet]
6	15:08:34.1780…	LoRaWAN	39					Join Accept	[Malformed Packet]

Bluetooth

If Bluetooth capturing is enabled, packets will be displayed with multiple coloring rules in Wireshark:



☑ BT Destination	btle.slave_bd_addr
☑ BLE empty PDUs	btle.data_header.llid == 0x1
☑ Mesh	btmesh
☑ Mesh Beacon	beacon
☑ Mesh PB Adv	pbadv
☑ ATT	btatt
☑ SMP	btsmp
☑ LMP	btbrlmp
☑ AVRCP	btavrcp
☑ AVCTP	btavctp
☑ VDP	btvdp
☑ A2DP	bta2dp
☑ AVDTP	btavdtp
☑ HCRP	bthcrp
☑ BNEP	btbnep
☑ HID	bthid
☑ OBEX	obex
☑ SAP	btsap
☑ HFP	bthfp
☑ HSP	bthsp
☑ DUN	btdun
☑ GNSS	btgnss
☑ RFCOMM	btrfcomm
☑ MCAP	btmcap
☑ SDP	btsdp
☑ Bluetooth Packet	bluetooth
☑ ATT	btatt
☑ AMP	btamp
☑ SMP	btsmp
☑ L2CAP	btl2cap
☑ SCO	bthci_sco
☑ BTLE	btle
☑ HCI_EVT	bthci_evt
☑ HCI_CMD	bthci_cmd

Start a Capture

- □ Once the options and settings have been selected, click the green **Launch** button
- □ When the **Launch** button is clicked, the text changes to **Stop**. Clicking the **Stop** button will stop the in-progress capture and change the text of the button back to **Launch**

Stop a Capture

Depending on how the user chooses to use the software, there are a few ways to stop an in-progress capture:

- □ Close the open Wireshark window: the user may select the **File** menu, **Quit** option or select the '**X'** in the upper right window corner.
    - ○ Note: Because of the way Wireshark and dumpcap are launched, the file is automatically saved in the "Capture Files Location and Base Name" field directory and will have the selected base file name along with timestamp information appended to it
- □ Click the **Stop** button. Then the user can change options, if necessary, and start a new capture
- □ Close the PANalyzr window by selecting the '**X'** in the upper right window corner

When PANalyzr closes, the various capture and display settings will be saved and loaded the next time PANalyzr is launched.

Additional Wireshark Info

Display GPS Columns

If utilizing a GPS USB receiver with the PANalyzr software, the latitude and longitude values are provided in each BR/EDR and BLE packet. These values can be added as columns for easier viewing.

Add BLE GPS column

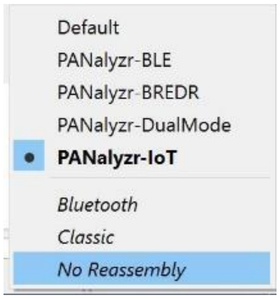
Select a BLE packet in the Packet List pane, next select the *Bluetooth Low Energy RF Info OTA* in the Packet Detail pane, and right-click on *Latitude* and 'Apply as Column.' Then, perform the same steps for the *Longitude* field*.*

Add BR/EDR GPS column

Select a BR/EDR packet in the packet list pane, next select the *Bluetooth Pseudoheader for BR/EDR OTA* in the packet detail pane, and right-click on *Latitude* and 'Apply as Column.' Then, perform the same steps for the *Longitude* field.

Profiles

Wireshark profiles for **Dual Mode**, **BR/EDR only**, **BLE only**, and **PANalyzr-IoT** capturing are included in the PANalyzr software. These profiles provide specific column settings, colorizations, preferences, and enabled protocols for improved packet capture analysis when in the different capturing modes. The profiles can be selected by clicking the *Profiles* menu option, located on the bottom right Wireshark toolstrip.



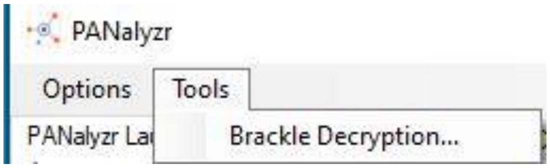
General Usage

Most of the standard Wireshark menu options function similarly to other protocols. However, PANalyzr does not currently support clicking the **Restart current capture** button or clicking the **Stop capturing packets** followed by the **Start capturing packets** button. To correctly restart PANalyzr, see the *To Stop* and *To Start* sections of this document.

Brackle Operation

To Start

- □ On the Desktop, double-click the **PANalyzr.exe** icon
- □ The PANalyzr main window will open
- □ On the Menu Bar, click on **Tools**
- □ Click on **Brackle Decryption**



Brackle Options

The brackle feature decrypts capture files that contain both BLE and BR/EDR encrypted packets. Decryption requires parameters provided by the user.

Input Capture File: Select an encrypted capture file

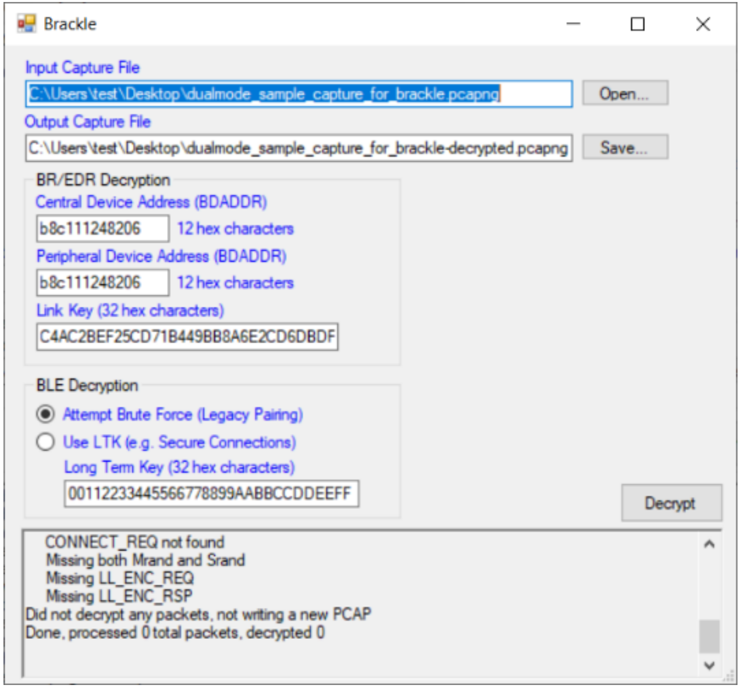
Output Capture File: display the path file of the decrypted captured file

BR/EDR Decryption: Central Device Address | Peripheral Device Address |Temporary Link Key

BLE Decryption: Attempt Brute Force (Legacy Pairing) | Semi-permanent Link Key (Secure Connection)

Decrypt button: Start decrypting the *input capture file*

Status Window: display and output brackle information



Input Capture File: C:\Users\test\Desktop\dualmode_sample_capture_for_brackle.pcapng

Output Capture File: C:\Users\test\Desktop\dualmode_sample_capture_for_brackle-decrypted.pcapng

BR/EDR Decryption

Central Device Address (BDADDR): b8c111248206 (12 hex characters)

Peripheral Device Address (BDADDR): b8c111248206 (12 hex characters)

Link Key (32 hex characters): C4AC2BEF25CD71B449BB8A6E2CD6DBDF

BLE Decryption

● Attempt Brute Force (Legacy Pairing)

○ Use LTK (e.g. Secure Connections)

Long Term Key (32 hex characters): 00112233445566778899AABBCCDDEEFF

```
    CONNECT_REQ not found
    Missing both Mrand and Srand
    Missing LL_ENC_REQ
    Missing LL_ENC_RSP
Did not decrypt any packets, not writing a new PCAP
Done, processed 0 total packets, decrypted 0
```

Brackle Sample Captures

Sample capture files are part of the PANalyzr install and can be found in the **C:\Program Files (x86)\Spanalytics\PANalyzr\Sample Capture Files** folder

Note: The output filename field will populate automatically based on the user-provided input file name. However, this output file name can be changed. Also, error messages will be generated if brackle is run on a capture file in a folder that the user does not have written permission (for example, Program Files (x86)). To run brackle on the sample captures provided in this installation, copy them to a folder the user has write permission to.

PANalyzr BREDR_Sample_Capture

- input_filename: PANalyzr_BREDR_Sample_Capture.pcapng
- output_filename: PANalyzr_BREDR_Sample_Capture-decrypted.pcapng
- Central Device Address: b8c111248206
- Peripheral Device Address: b8c111248206
- Link Key: C4AC2BEF25CD71B449BB8A6E2CD6DBDF

PANalyzr BLE Secure Connections Initial Sample Capture

- input_filename: PANalyzr_BLE_Secure_Connections_Initial_Sample_Capture.pcapng
- output_filename: PANalyzr_BLE_Secure_Connections_Initial_Sample_Capture-decrypted.pcapng
- Link Key: 08592E625C21F5954564731D980245A5 (e.g., Secure Connections)

PANalyzr BLE Legacy Pairing Initial Sample Capture

- input_filename: PANalyzr_BLE_Legacy_Pairing_Initial_Sample_Capture.pcapng
- output_filename: PANalyzr_BLE_Legacy_Pairing_Initial_Sample_Capture-decrypted.pcapng
- Attempt Brute Force (Legacy Pairing)

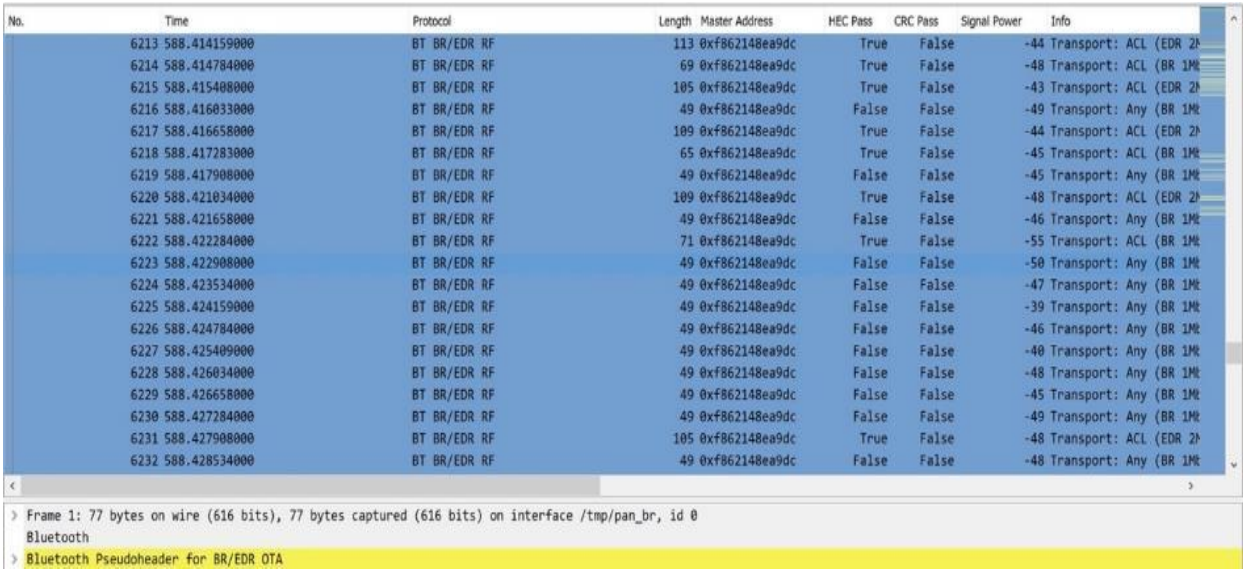
PANalyzr BLE Legacy Pairing Reconnect Sample Capture

- input_filename: PANalyzr_BLE_Legacy_Pairing_Reconnect_Sample_Capture.pcapng
- output_filename: PANalyzr_BLE_Legacy_Pairing_Reconnect_Sample_Capture-decrypted.pcapng
- Use LTK (e.g Secure Connections)
- Long Term Key: e869f960d17b19048a9c9235c970f06f

Brackle Encrypted / Decrypted Comparison

Below is an example of sample BR/EDR packets encrypted and decrypted.

Encrypted Capture File

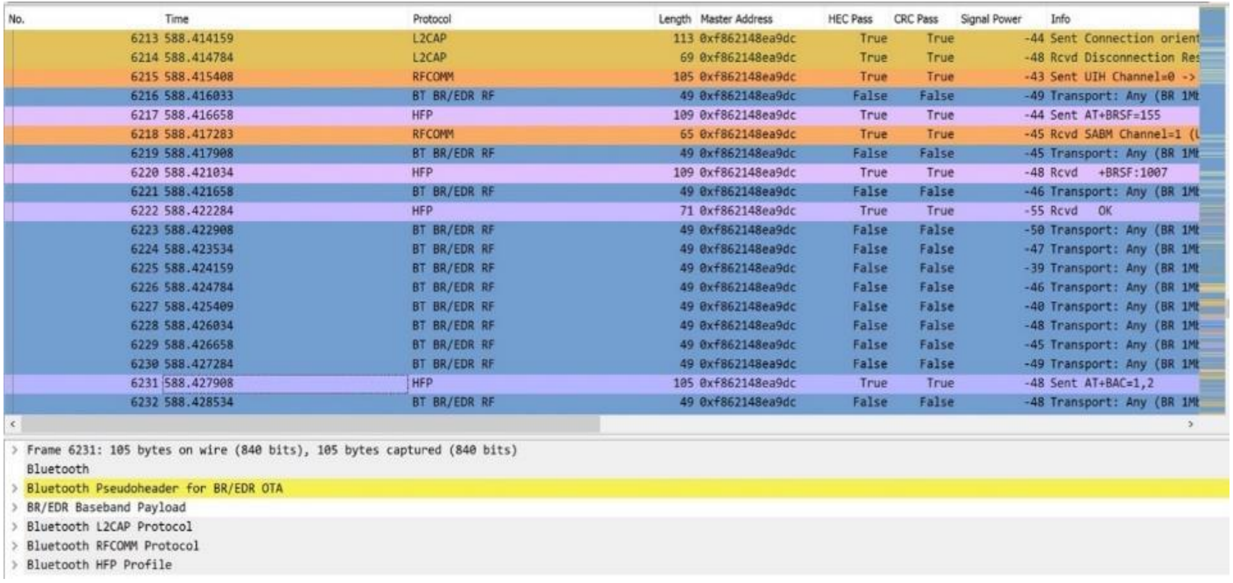


No.	Time	Protocol	Length	Master Address	HEC Pass	CRC Pass	Signal Power	Info
6213	588.414159000	BT BR/EDR RF	113	0xf862148ea9dc	True	False	-44	Transport: ACL (EDR 2M
6214	588.414784000	BT BR/EDR RF	69	0xf862148ea9dc	True	False	-48	Transport: ACL (BR 1M
6215	588.415408000	BT BR/EDR RF	105	0xf862148ea9dc	True	False	-43	Transport: ACL (EDR 2M
6216	588.416033000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-49	Transport: Any (BR 1M
6217	588.416658000	BT BR/EDR RF	109	0xf862148ea9dc	True	False	-44	Transport: ACL (EDR 2M
6218	588.417283000	BT BR/EDR RF	65	0xf862148ea9dc	True	False	-45	Transport: ACL (BR 1M
6219	588.417908000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-45	Transport: Any (BR 1M
6220	588.421034000	BT BR/EDR RF	109	0xf862148ea9dc	True	False	-48	Transport: ACL (EDR 2M
6221	588.421658000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-46	Transport: Any (BR 1M
6222	588.422284000	BT BR/EDR RF	71	0xf862148ea9dc	True	False	-55	Transport: ACL (BR 1M
6223	588.422908000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-50	Transport: Any (BR 1M
6224	588.423534000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-47	Transport: Any (BR 1M
6225	588.424159000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-39	Transport: Any (BR 1M
6226	588.424784000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-46	Transport: Any (BR 1M
6227	588.425409000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-40	Transport: Any (BR 1M
6228	588.426034000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-48	Transport: Any (BR 1M
6229	588.426658000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-45	Transport: Any (BR 1M
6230	588.427284000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-49	Transport: Any (BR 1M
6231	588.427908000	BT BR/EDR RF	105	0xf862148ea9dc	True	False	-48	Transport: ACL (EDR 2M
6232	588.428534000	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-48	Transport: Any (BR 1M

```
> Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface /tmp/pan_br, id 0
  Bluetooth
> Bluetooth Pseudoheader for BR/EDR OTA
```

Decrypted Capture File

Packets 6213-6215, 6217, 6218, 6220, 6222, 6231 are decrypted as L2CAP RFCOMM, and HFP profiles.

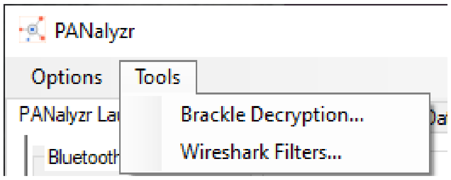


No.	Time	Protocol	Length	Master Address	HEC Pass	CRC Pass	Signal Power	Info
6213	588.414159	L2CAP	113	0xf862148ea9dc	True	True	-44	Sent Connection orient
6214	588.414784	L2CAP	69	0xf862148ea9dc	True	True	-48	Rcvd Disconnection Res
6215	588.415408	RFCOMM	105	0xf862148ea9dc	True	True	-43	Sent UIH Channel=0 ->
6216	588.416033	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-49	Transport: Any (BR 1M
6217	588.416658	HFP	109	0xf862148ea9dc	True	True	-44	Sent AT+BRSF=155
6218	588.417283	RFCOMM	65	0xf862148ea9dc	True	True	-45	Rcvd SABM Channel=1 (U
6219	588.417908	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-45	Transport: Any (BR 1M
6220	588.421034	HFP	109	0xf862148ea9dc	True	True	-48	Rcvd +BRSF:1007
6221	588.421658	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-46	Transport: Any (BR 1M
6222	588.422284	HFP	71	0xf862148ea9dc	True	True	-55	Rcvd OK
6223	588.422908	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-50	Transport: Any (BR 1M
6224	588.423534	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-47	Transport: Any (BR 1M
6225	588.424159	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-39	Transport: Any (BR 1M
6226	588.424784	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-46	Transport: Any (BR 1M
6227	588.425409	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-40	Transport: Any (BR 1M
6228	588.426034	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-48	Transport: Any (BR 1M
6229	588.426658	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-45	Transport: Any (BR 1M
6230	588.427284	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-49	Transport: Any (BR 1M
6231	588.427908	HFP	105	0xf862148ea9dc	True	True	-48	Sent AT+BAC=1,2
6232	588.428534	BT BR/EDR RF	49	0xf862148ea9dc	False	False	-48	Transport: Any (BR 1M

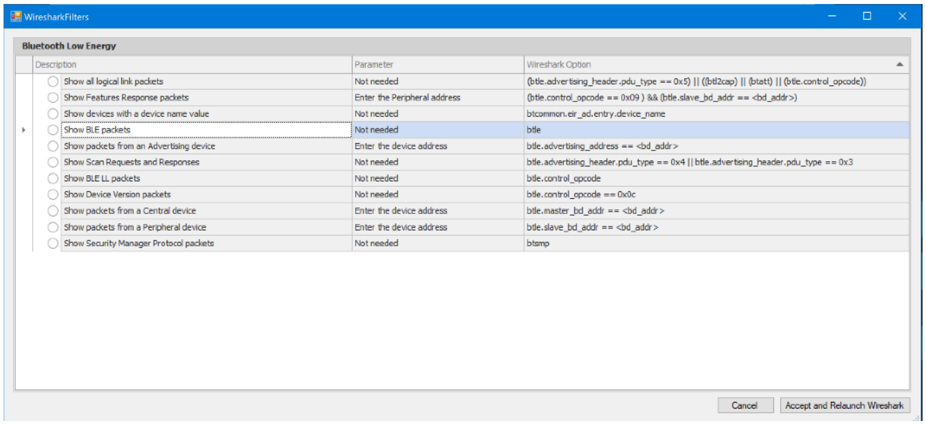
```
> Frame 6231: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
  Bluetooth
> Bluetooth Pseudoheader for BR/EDR OTA
> BR/EDR Baseband Payload
> Bluetooth L2CAP Protocol
> Bluetooth RFCOMM Protocol
> Bluetooth HFP Profile
```

Wireshark Filters

The Wireshark filter allows a user to set the filter parameters prior to launching a capture.

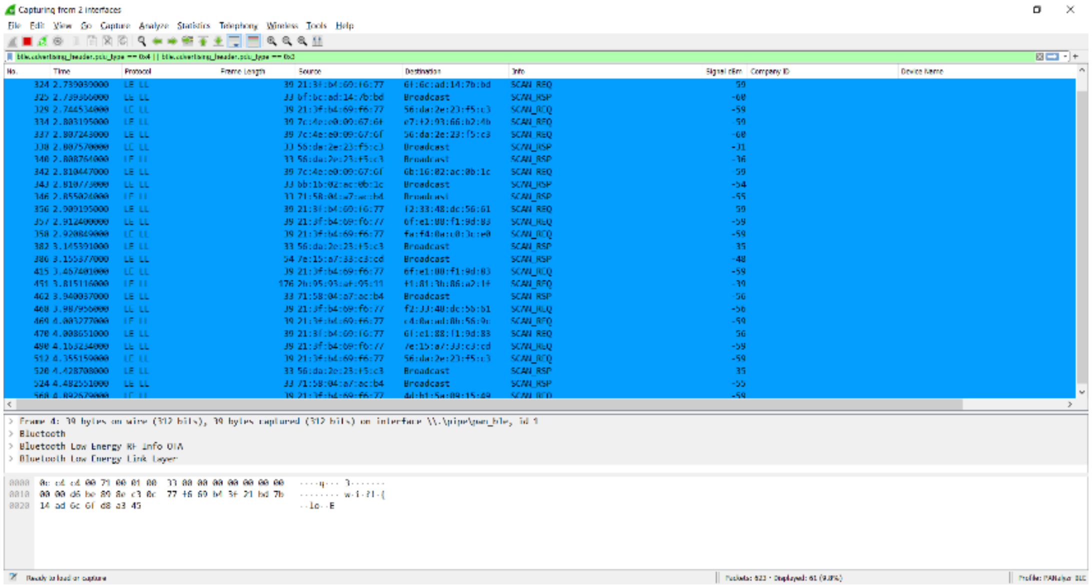


To utilize this feature, first select the radio button of the desired filter in the **Description** column. Then enter the *device address* in the **Parameters** field (if applicable) and click the **Accept and Relaunch Wireshark** button



Description	Parameter	Wireshark Option
○ Show all logical link packets	Not needed	(btle.advertising_header.pdu_type == 0x5) || ((btl2cap) || (btatt) || (btle.control_opcode))
○ Show Features Response packets	Enter the Peripheral address	(btle.control_opcode == 0x09) && (btle.slave_bd_addr == <bd_addr>)
○ Show devices with a device name value	Not needed	btcommon.eir_ad.entry.device_name
○ Show BLE packets	Not needed	btle
○ Show packets from an Advertising device	Enter the device address	btle.advertising_address == <bd_addr>
○ Show Scan Requests and Responses	Not needed	btle.advertising_header.pdu_type == 0x4 || btle.advertising_header.pdu_type == 0x3
○ Show BLE LL packets	Not needed	btle.control_opcode
○ Show Device Version packets	Not needed	btle.control_opcode == 0x0c
○ Show packets from a Central device	Enter the device address	btle.master_bd_addr == <bd_addr>
○ Show packets from a Peripheral device	Enter the device address	btle.slave_bd_addr == <bd_addr>
○ Show Security Manager Protocol packets	Not needed	btsmp

When Wireshark launches, the selected filter will be applied in the Filter field, and the packets will be filtered automatically accordingly


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
btle.advertising_header.pdu_type == 0x4 || btle.advertising_header.pdu_type == 0x3
```

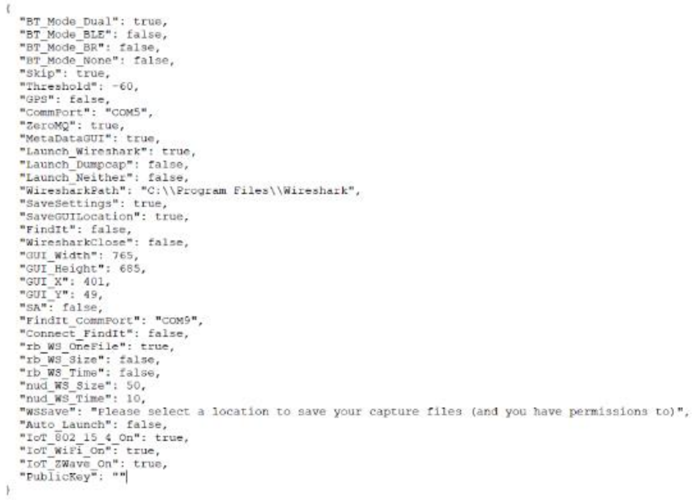
```
No.   Time         Protocol  Frame Length  Source             Destination        Info      Signal dBm  Company ID  Device Name
  324 2.739039000  LE LL     39 21:3f:b4:69:f6:77  6f:6c:ad:14:7b:bd  SCAN_REQ   59
  325 2.739366000  LE LL     33 bf:bc:ad:14:7b:bd  Broadcast          SCAN_RSP  -60
  329 2.744534000  LE LL     39 21:3f:b4:69:f6:77  56:da:2e:23:f5:c3  SCAN_REQ  -59
  334 2.803195000  LE LL     39 7c:4e:e0:09:67:6f  e7:f2:93:66:b2:4b  SCAN_REQ  -59
  337 2.807243000  LE LL     39 7c:4e:e0:09:67:6f  56:da:2e:23:f5:c3  SCAN_REQ  -60
  338 2.807570000  LE LL     33 56:da:2e:23:f5:c3  Broadcast          SCAN_RSP  -31
  340 2.808764000  LE LL     33 56:da:2e:23:f5:c3  Broadcast          SCAN_RSP  -36
  342 2.810447000  LE LL     39 7c:4e:e0:09:67:6f  6b:16:82:ac:0b:1c  SCAN_REQ  -59
  343 2.810773000  LE LL     33 bb:16:82:ac:0b:1c  Broadcast          SCAN_RSP  -54
  346 2.855024000  LE LL     33 71:58:04:a7:ac:b4  Broadcast          SCAN_RSP  -55
  356 2.909195000  LE LL     39 21:3f:b4:69:f6:77  12:33:48:dc:56:61  SCAN_REQ   59
  357 2.912400000  LE LL     39 21:3f:b4:69:f6:77  6f:e1:88:f1:9d:83  SCAN_REQ  -59
  358 2.920849000  LE LL     39 21:3f:b4:69:f6:77  fa:f4:0a:c0:3c:e0  SCAN_REQ  -59
  382 3.145391000  LE LL     33 56:da:2e:23:f5:c3  Broadcast          SCAN_RSP   35
  386 3.155377000  LE LL     54 7e:15:a7:33:c3:cd  Broadcast          SCAN_RSP  -48
  415 3.467401000  LE LL     39 21:3f:b4:69:f6:77  6f:e1:88:f1:9d:83  SCAN_REQ  -59
  451 3.815116000  LE LL    176 2b:95:93:af:95:11  f1:81:3b:86:a2:1f  SCAN_REQ  -39
  462 3.940037000  LE LL     33 71:58:04:a7:ac:b4  Broadcast          SCAN_RSP  -56
  468 3.987956000  LE LL     39 21:3f:b4:69:f6:77  f2:33:40:dc:5b:b1  SCAN_REQ  -56
  469 4.003277000  LE LL     39 21:3f:b4:69:f6:77  c4:0a:ad:0b:56:9c  SCAN_REQ  -59
  470 4.008651000  LE LL     39 21:3f:b4:69:f6:77  6f:e1:88:f1:9d:83  SCAN_REQ   56
  490 4.153234000  LE LL     39 21:3f:b4:69:f6:77  7e:15:a7:33:c3:cd  SCAN_REQ  -59
  512 4.355159000  LE LL     39 21:3f:b4:69:f6:77  56:da:2e:23:f5:c3  SCAN_REQ  -59
  520 4.428708000  LE LL     33 56:da:2e:23:f5:c3  Broadcast          SCAN_RSP   35
  524 4.482551000  LE LL     33 71:58:04:a7:ac:b4  Broadcast          SCAN_RSP  -55
  560 4.892679000  LE LL     39 21:3f:b4:69:f6:77  4d:b1:5a:09:15:49  SCAN_REQ  -59

> Frame 4: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on interface \\.\pipe\gen_ble, id 1
> Bluetooth
> Bluetooth Low Energy RF Info OIA
> Bluetooth Low Energy Link Layer

0000  0c c4 c4 00 71 00 01 00  33 00 00 00 00 00 00 00   ····q··· 3·······
0010  00 00 d6 be 89 8e c3 0c  77 f6 69 b4 3f 21 bd 7b   ········ w·i·?!·{
0020  14 ad 6c 6f d8 a3 45                               ··lo··E

Ready to load or capture | Packets: 623 · Displayed: 61 (9.8%) | Profile: PANalyzr BLE
```

Configuration file (.json)

The Panalyzr configuration file can be accessed and edited at:

C:\User\<username>\AppData\Roaming or enter "*%appdata%*" in the **File Explorer** app

Open the ***PANalyzr_Config.json*** file with a text editing application to edit it.



```
{
  "BT_Mode_Dual": true,
  "BT_Mode_BLE": false,
  "BT_Mode_BR": false,
  "BT_Mode_None": false,
  "Skip": true,
  "Threshold": -60,
  "GPS": false,
  "CommPort": "COM5",
  "ZeroMQ": true,
  "MetaDataGUI": true,
  "Launch_Wireshark": true,
  "Launch_Dumpcap": false,
  "Launch_Neither": false,
  "WiresharkPath": "C:\\Program Files\\Wireshark",
  "SaveSettings": true,
  "SaveGUILocation": true,
  "FindIt": false,
  "WiresharkClose": false,
  "GUI_Width": 765,
  "GUI_Height": 685,
  "GUI_X": 401,
  "GUI_Y": 49,
  "SA": false,
  "FindIt_CommPort": "COM9",
  "Connect_FindIt": false,
  "rb_WS_OneFile": true,
  "rb_WS_Size": false,
  "rb_WS_Time": false,
  "nud_WS_Size": 50,
  "nud_WS_Time": 10,
  "WSSave": "Please select a location to save your capture files (and you have permissions to)",
  "Auto_Launch": false,
  "IoT_802_15_4_On": true,
  "IoT_WiFi_On": true,
  "IoT_ZWave_On": true,
  "PublicKey": ""
}
```

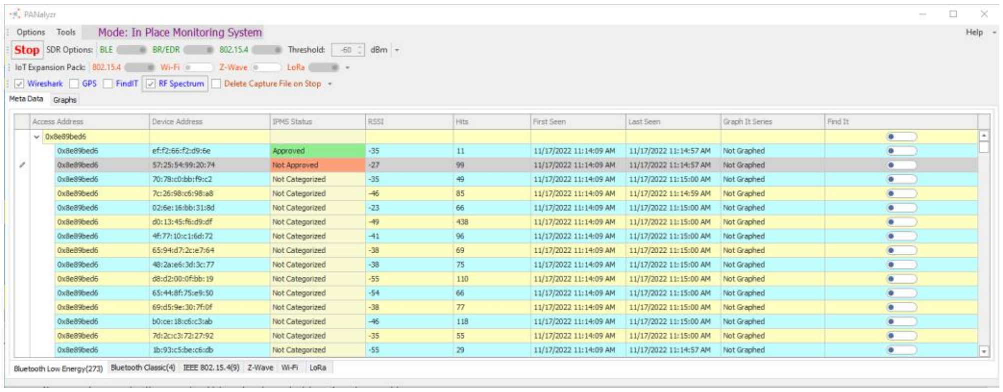
JSON	GUI Feature	Value	Example
BT_Mode_Dual	Dual Mode	true or false	"BT_Mode_Dual": false,
BT_Mode_BLE	BLE Only	true or false	"BT_Mode_BLE": false,
BT_Mode_BR	BR/EDR Only	true or false	"BT_Mode_BR": false,
Skip	Skip Short Packets	true or false	"Skip": true,
Threshold	Set Threshold dBm	integers	"Threshold": -65,
GPS	Set GPS Mode	true or false	"GPS": false,
CommPort	Set GPS Serial Port	COM#	"CommPort": COM4,
ZeroMQ	Start ZeroMQ Server	true or false	"ZeroMQ": true,
MetaDataGUI	Show Meta Data	true or false	"MetaDataGUI": true,
Launch_Wireshark	Launch Wireshark GUI	true or false	"Launch_Wireshark": true
Launch_Dumpcap	Launch dumpcap only	true or false	"Launch_Dumpcap": false
Launch_Neither	Do not launch Wireshark or dumpcap	true or false	"Launch_Neither": false
WiresharkPath	Set file path to Wireshark	File path	“WiresharkPath”: “C:\\Program Files\\Wireshark”,
SaveSettings	Save Setting on Exit	true or false	"SaveSetting": true,
SaveGUILocation	Save GUI Location and Size	true or false	"SaveGUILocation": true,
FindIt		N/A	N/A

WiresharkClose	Close Wireshark when the user click the "Stop" button	true or false	"WiresharkClose": false,
GUI_Width	Panalyzr GUI Width	integers	"GUI_Width": 586,
GUI_Height	Panalyzr GUI Height	integers	"GUI_Height": 758,
GUI_X	Location of the GUI on the X-axis of user's Desktop	integers	"GUI_X": 585,
GUI_Y	Location of the GUI on the Y-axis of user's Desktop	integers	"GUI_Y": 458,
SA	Show RF Spectrum	true or false	"SA": false,
FindIt_CommPort	FindIT Com Port number	N/A	N/A
Connect_FindIt	Connect to FindIT on the selected Com port	N/A	N/A
rb_WS_OneFile	Save Wireshark capture in on file	true or false	"rb_WS_OneFile": true,
rb_WS_Size	Save Wireshark capture by file size	true or false	"rb_WS_Size": true,
rb_WS_Time	Save Wireshark capture by time intervals	true or false	"rb_WS_Time": true,
nud_WS_Size	Set Wireshark capture by file size	Integers	“nud_WS_Size”: 1000,
nud_WS_Time	Set Wireshark capture by time intervals	Integers	“nud_WS_Time”: 30,
WSSave	Set capture file location	file-path	“C:\\Users\\Tester\\AppData\\Roaming\\Wireshark\\PAN_Capture”,
Auto_Launch	Launch Wireshark or Dumpcap on startup	true or false	"Auto_Launch": false
Public_Key	Key provided to the user to enable features	String	See license key file for details

Meta Data Display

PANalyzr provides the ability to display and graph metadata received from the SDR and IoT Expansion pack hardware.

On the Meta Data tab, there is a tab to display the captured meta data for each protocol (Bluetooth Low Energy, Bluetooth Classic, IEEE 802.15.4, Z-Wave, Wi-Fi and LoRa)



Mode: In Place Monitoring System

Threshold: -60 dBm

☑ Wireshark ☐ GPS ☐ FindIT ☑ RF Spectrum ☐ Delete Capture File on Stop

Access Address	Device Address	IPMS Status	RSSI	Hits	First Seen	Last Seen	Graph It Series	Find It
0x8e89bed6								
0x8e89bed6	ef:f2:66:f2:d9:6e	Approved	-35	11	11/17/2022 11:14:09 AM	11/17/2022 11:14:57 AM	Not Graphed	
0x8e89bed6	57:25:54:99:20:74	Not Approved	-27	99	11/17/2022 11:14:09 AM	11/17/2022 11:14:57 AM	Not Graphed	
0x8e89bed6	70:78:c0:bb:f9:c2	Not Categorized	-35	49	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	7c:26:98:c6:98:a8	Not Categorized	-46	85	11/17/2022 11:14:09 AM	11/17/2022 11:14:59 AM	Not Graphed	
0x8e89bed6	02:6e:16:bb:31:8d	Not Categorized	-23	66	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	d0:13:45:f6:d9:df	Not Categorized	-49	438	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	4f:77:10:c1:6d:72	Not Categorized	-41	96	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	65:94:d7:2c:e7:64	Not Categorized	-38	69	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	48:2a:e6:3d:3c:77	Not Categorized	-38	75	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	d8:d2:00:0f:bb:19	Not Categorized	-55	110	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	65:44:8f:75:e9:50	Not Categorized	-54	66	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	69:d5:9e:30:7f:0f	Not Categorized	-38	77	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	b0:ce:18:c6:c3:ab	Not Categorized	-46	118	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	7d:2c:c3:72:27:92	Not Categorized	-35	55	11/17/2022 11:14:09 AM	11/17/2022 11:15:00 AM	Not Graphed	
0x8e89bed6	1b:93:c5:be:c6:db	Not Categorized	-55	29	11/17/2022 11:14:09 AM	11/17/2022 11:14:57 AM	Not Graphed	

Details Metadata

Bluetooth Low Energy: Access Address | Device Address | IPMS Status | RSSI | Hits | First Seen | Last Seen | Graph It Series | FindIt

Bluetooth Classic (BR/EDR): Address | RSSI | Hits | Graph It Series | FindIt

802.15.4: Destination PAN | Destination Address | Source Address| RSSI | Hits | Graph It Series | FindIt

Z-Wave: Home ID | Source Node| RSSI | Hits | Graph It Series

Wi-Fi: Tx Address | Rx Address | Primary Channel | Hits

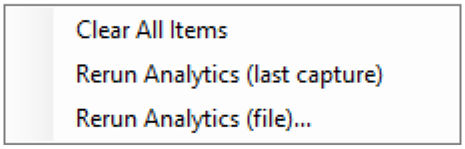
LoRa: Tx Address | Frequency | Spreading Factor | Bandwidth | Hits

Note: Currently, Wi-Fi and LoRa data cannot be graphed

Meta Data Grid Controls

There are two ways to get to the Meta Data grid controls:

- □ Right-click in the blank space area of the Meta Data grid
- □ Right-click in the upper left-hand corner of the grid table header



Clear All

- □ Clears Metadata screen

Rerun Analytics (Last Capture)

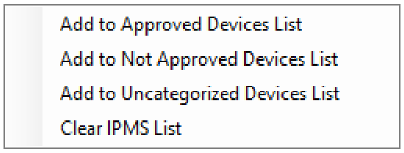
- □ Retrieve metadata from the current capture file

Rerun Analytics (file)

- □ Select a stored capture file to retrieve and display metadata

Meta Data In-Place Monitoring System Device Controls

*This feature only works in Bluetooth Low Energy


Add to Approved Devices List
Add to Not Approved Devices List
Add to Uncategorized Devices List
Clear IPMS List

When the **Add to Approved Devices List** option is selected, the following behavior should be seen:

- The IPMS Status for the device should change to "Approved"
- The cell in the meta data tab should be highlighted green

When the **Add to Not Approved Devices List** option is selected, the following behavior should be seen:

- The IPMS Status for the device should change to "Not Approved"
- The cell in the meta data tab should be highlighted orange/red

When the **Add to Uncategorized Devices List** option is selected, the following behavior should be seen:

- The IPMS Status for the device should change to "Not Categorized"
- The cell in the meta data tab should be highlighted yellow (default color)

When the **Clear IPMS List** option is selected, the following behavior should be seen:

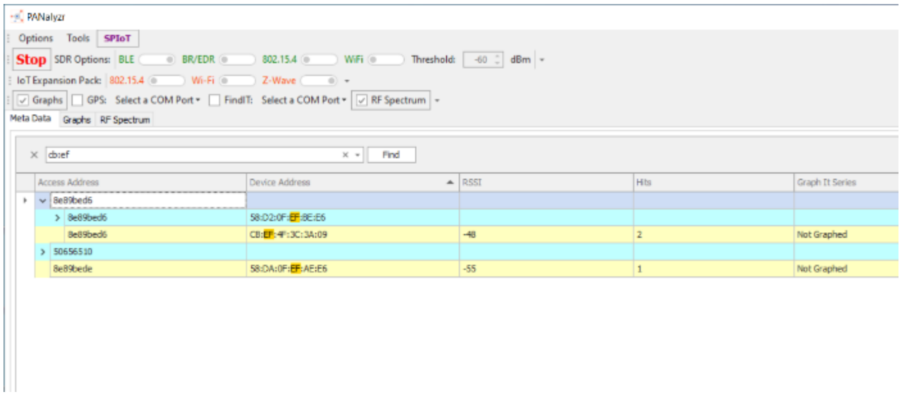
- The dialog "Delete File?" should be displayed. If the user selects OK, the file *<userpath>\AppData\Roaming\WIDS_List.wids* will be deleted
- The IPMS Status for any devices will **not** change from what it was before

Find

☐ Right-click on a column heading and select **Show Find Panel**

☐ In the Find panel, type any text to search for, then click the Find button

☐ The Meta Data list should be updated, and filtered to only include items that include the search values

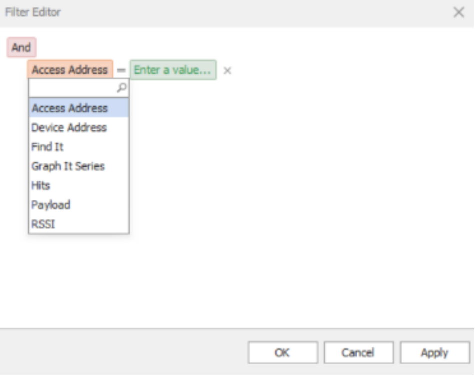


Access Address	Device Address	RSSI	Hits	Graph It Series
8e89bed6				
8e89bed6	58:D2:0F:EF:8E:E6			
8e89bed6	CB:EF:4F:3C:3A:09	-48	2	Not Graphed
50656510				
8e89bede	58:DA:0F:EF:AE:E6	-55	1	Not Graphed

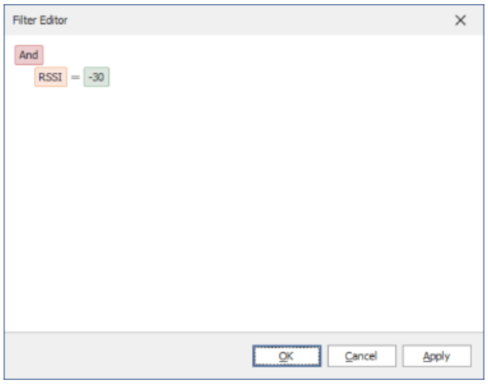
Filter Editor (simple)

☐ Right-click on a column heading and select **Filter Editor**

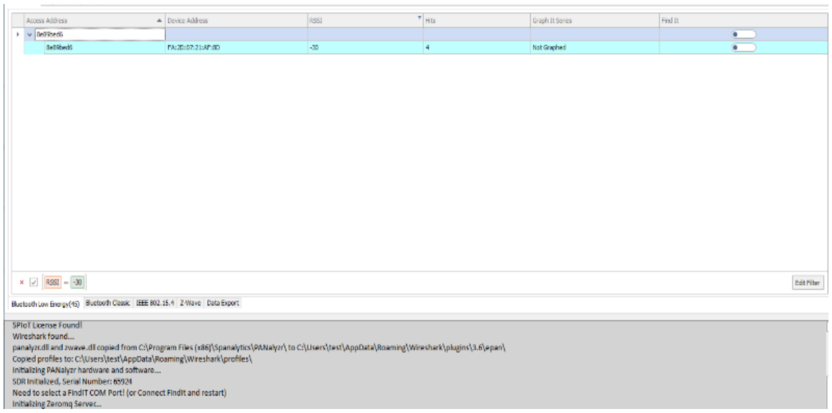
☐ In the Filter Editor window, click on the value on the left side of the filter equation and select a field



☐ On the right side of the filter equation, enter a value to filter on, then click the **OK** button



☐ The Meta Data list should be updated with the filter applied

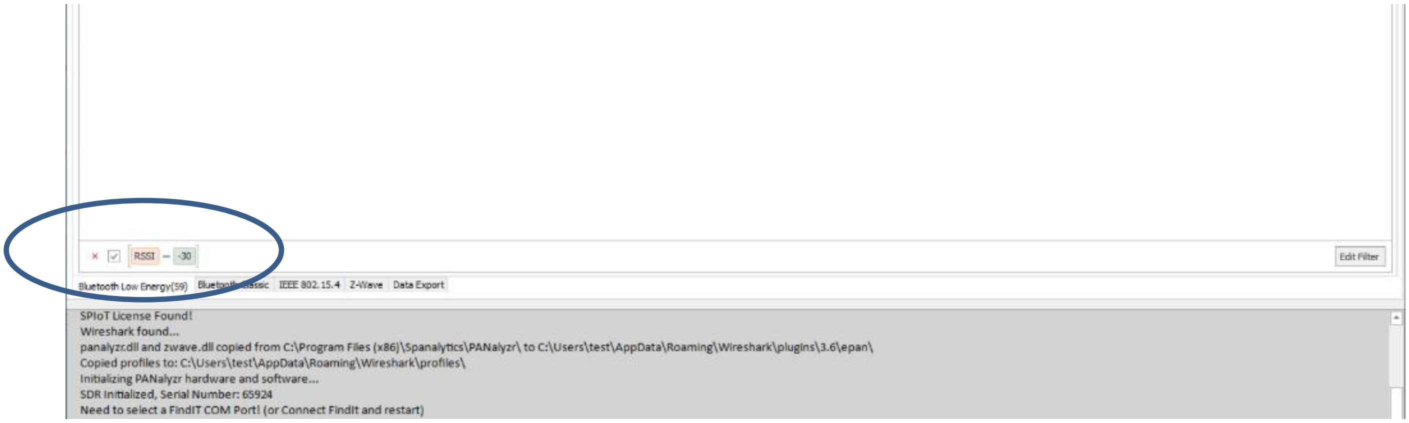


Access Address	Device Address	RSSI	Hits	Graph It Series	Find It
0e89bed6					
0e89bed6	FA:2D:07:21:AF:8D	-30	4	Not Graphed	

```
SPIoT License Found!
Wireshark found...
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to C:\Users\test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\test\AppData\Roaming\Wireshark\profiles\
Initializing PANalyzr hardware and software...
SDR Initialized, Serial Number: 65924
Need to select a FindIT COM Port! (or Connect FindIt and restart)
Initializing Zeromq Server...
```

Remove a filter

☐ Click the Red X on the filter listed at the bottom of the Meta Data grid

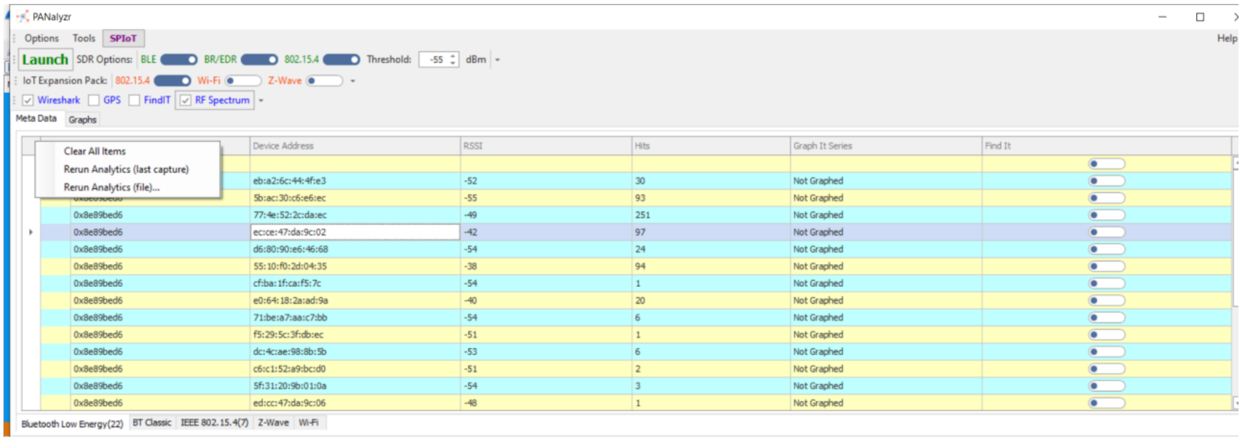


```
SPIoT License Found!
Wireshark found...
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to C:\Users\test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\test\AppData\Roaming\Wireshark\profiles\
Initializing PANalyzr hardware and software...
SDR Initialized, Serial Number: 65924
Need to select a FindIT COM Port! (or Connect FindIt and restart)
```

Rerun Analytics

Once the user stops a capture, they can run post-capture analytics by right-clicking either in a blank area of the Meta Data grid or in the upper left corner in the table header, and selecting **Rerun Analytics (last capture)**. The Analytics Running progress bar will be displayed while the analytics are processed.

When this is complete, all packet data from the capture will be added to the Meta Data grid list



SDR Options: BLE BR/EDR 802.15.4 Threshold: -55 dBm

IoT Expansion Pack: 802.15.4 Wi-Fi Z-Wave

☑ Wireshark □ GPS □ FindIT ☑ RF Spectrum

	Device Address	RSSI	Hits	Graph It Series	Find It
					○
	eb:a2:6c:44:4f:e3	-52	30	Not Graphed	○
	5b:ac:30:c6:e6:ec	-55	93	Not Graphed	○
0x8e89bed6	77:4e:52:2c:da:ec	-49	251	Not Graphed	○
0x8e89bed6	ec:ce:47:da:9c:02	-42	97	Not Graphed	○
0x8e89bed6	d6:80:90:e6:46:68	-54	24	Not Graphed	○
0x8e89bed6	55:10:f0:2d:04:35	-38	94	Not Graphed	○
0x8e89bed6	cf:ba:1f:ca:f5:7c	-54	1	Not Graphed	○
0x8e89bed6	e0:64:18:2a:ad:9a	-40	20	Not Graphed	○
0x8e89bed6	71:be:a7:aa:c7:bb	-54	6	Not Graphed	○
0x8e89bed6	f5:29:5c:3f:db:ec	-51	1	Not Graphed	○
0x8e89bed6	dc:4c:ae:98:8b:5b	-53	6	Not Graphed	○
0x8e89bed6	c6:c1:52:a9:bc:d0	-51	2	Not Graphed	○
0x8e89bed6	5f:31:20:9b:01:0a	-54	3	Not Graphed	○
0x8e89bed6	ed:cc:47:da:9c:06	-48	1	Not Graphed	○

Note: Depending on the total number of packets captured, the rerun analytics function can take seconds to minutes to complete. The GUI will not be responsive during this time

Graph Display

Graphing during live capture

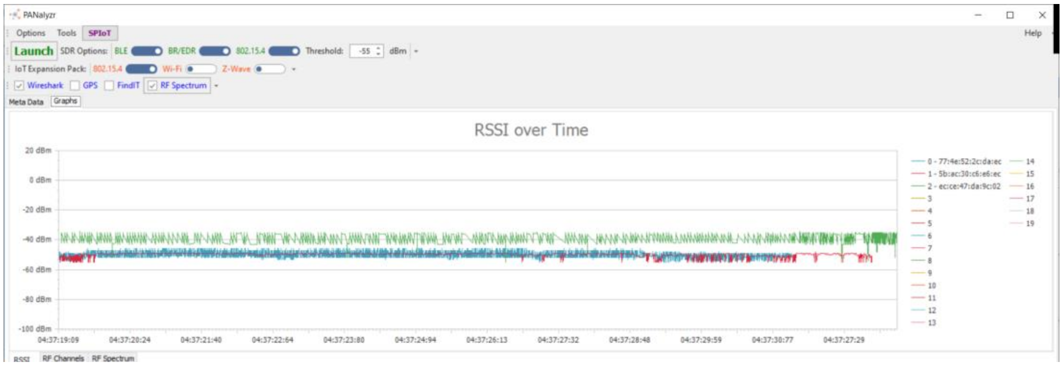
Go to the **Meta Data** tab during a capture, double-click a device row and select a Series number from the **Graph It Series** drop-down menu. Then click the **Update** button. Click on the **Graphs** tab to see the data graphed as RSSI over hits and RF Channel over hits (from that point on)

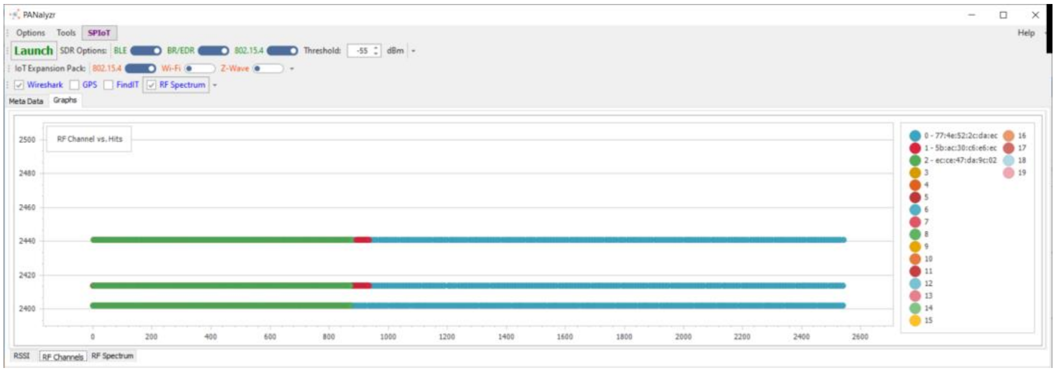
Graphing post-capture

Once a capture has stopped, go to the **Meta Data** tab and double-click a device row. Select a Series number from the **Graph It Series** drop-down menu, then click the **Update** button.

Then right-click anywhere in the Meta Data grid list and select **Rerun Analytics (last capture)**. A progress bar will be displayed as the data is re-analyzed. When this completes, click on the **Graphs** tab to see the different graphing displays: *RSSI over Time* and *RF Channel vs. Hits*

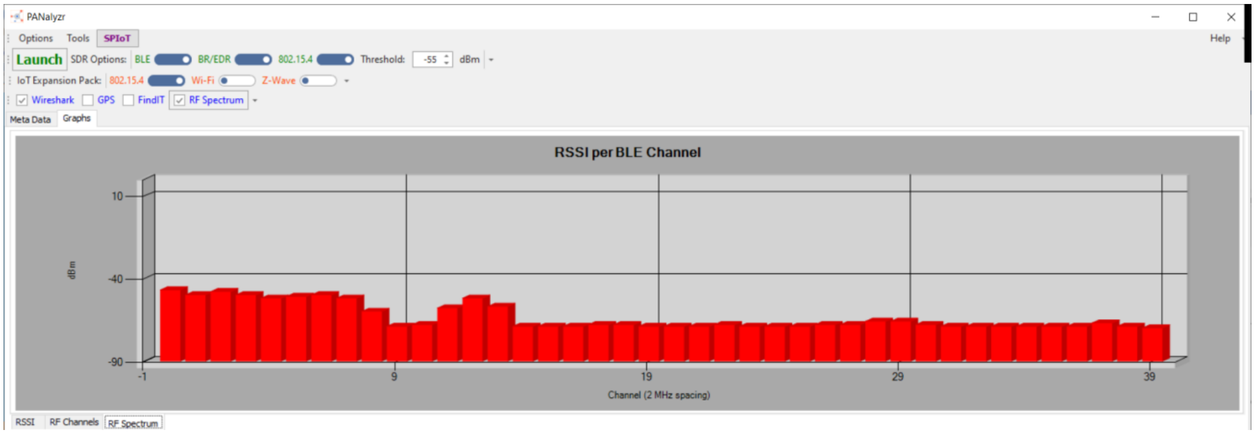
Note: Multiple devices can be selected to graph before running Rerun Analytics





RF Spectrum

The data on this tab shows the 40 Bluetooth Low Energy channels with 2 MHz spacing and detects the RSSI of the surrounding devices outputting on those channels.

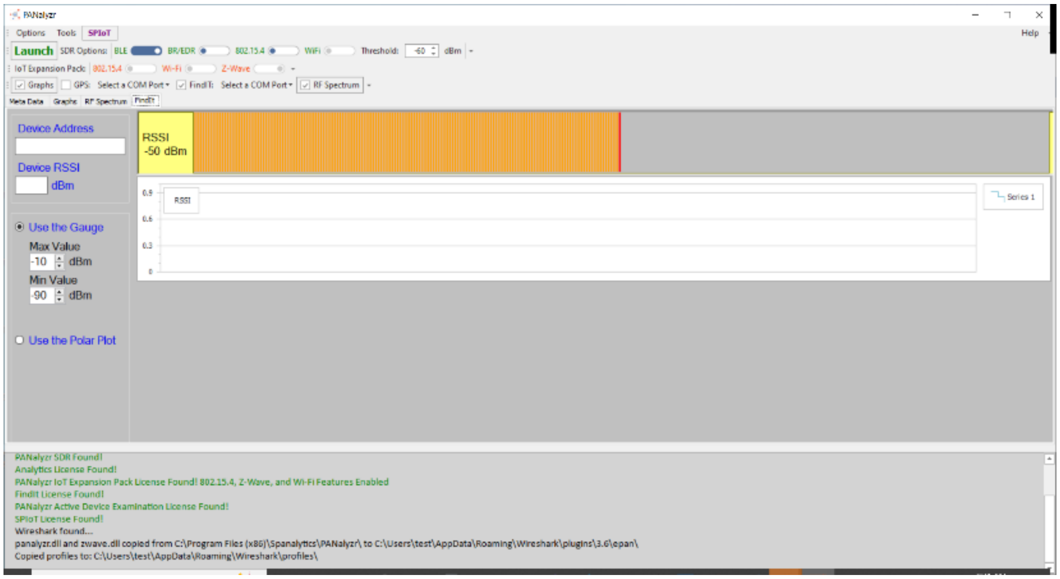


Threshold: -55 dBm

☑ Wireshark □ GPS □ FindIT ☑ RF Spectrum

FindIT

Approximates a device's location via RSSI and true north calculation



Threshold: -60 dBm

☑ Graphs □ GPS: Select a COM Port ☑ FindIT: Select a COM Port ☑ RF Spectrum

RSSI -50 dBm

● Use the Gauge

Max Value -10 dBm

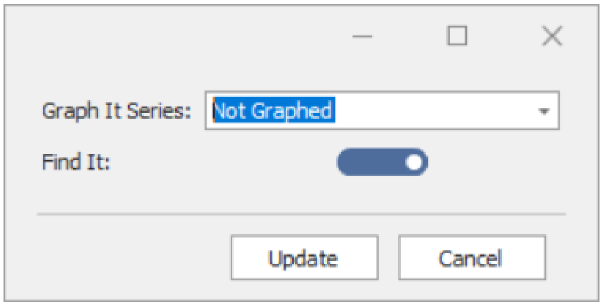
Min Value -90 dBm

○ Use the Polar Plot

```
PANalyzr SDR Found!
Analytics License Found!
PANalyzr IoT Expansion Pack License Found! 802.15.4, Z-Wave, and Wi-Fi Features Enabled
FindIt License Found!
PANalyzr Active Device Examination License Found!
SPIoT License Found!
Wireshark found....
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to C:\Users\test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\test\AppData\Roaming\Wireshark\profiles\
```

To begin, connect the FindIT hardware to the SDR and computer, then start the PANalyzr software. Check the **FindIT** checkbox, and validate that a COM port value was auto-detected for the FindIT.

Click the **Launch** button, allow Wireshark to start capturing packets, navigate to the **Meta Data** tab and double-click the desired device row**.** Check the **Find It** radio button, then click the **Update** button


Graph It Series: Not Graphed

Find It: ●

Click on the **FindIt** tab

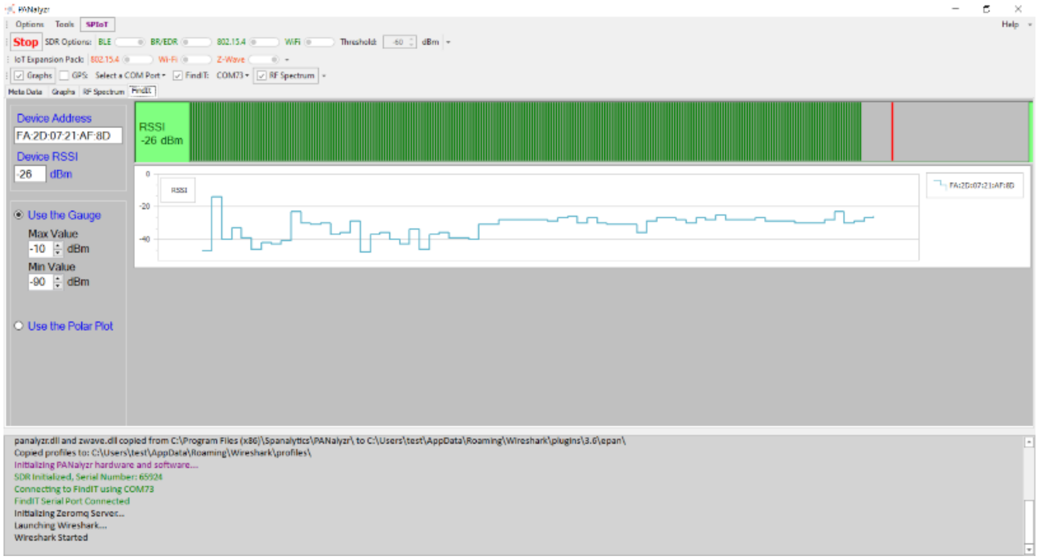
Device Address: The address selected from the metadata view

Device RSSI: The current RSSI value from the selected device

Use the Gauge: Displays the RSSI gauge and RSSI values over time. The RSSI gauge will turn red when the RSSI value is in a range of -20dBm of the Min Value. The RSSI gauge will turn green when the RSSI value is in a range of -20dBm of the Max Value.

Max Value: Max RSSI value

Min Value: Minimum RSSI value



Threshold: -60 dBm

☑ Graphs □ GPS: Select a COM Port ☑ FindIT: COM73 ☑ RF Spectrum

Device Address: FA:2D:07:21:AF:8D

Device RSSI: -26 dBm

RSSI -26 dBm

● Use the Gauge

Max Value: -10 dBm

Min Value: -90 dBm

○ Use the Polar Plot

```
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to C:\Users\test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\test\AppData\Roaming\Wireshark\profiles\
Initializing PANalyzr hardware and software....
SDR Initialized, Serial Number: 65924
Connecting to FindIT using COM73
FindIT Serial Port Connected
Initializing Zeromq Server...
Launching Wireshark....
Wireshark Started
```

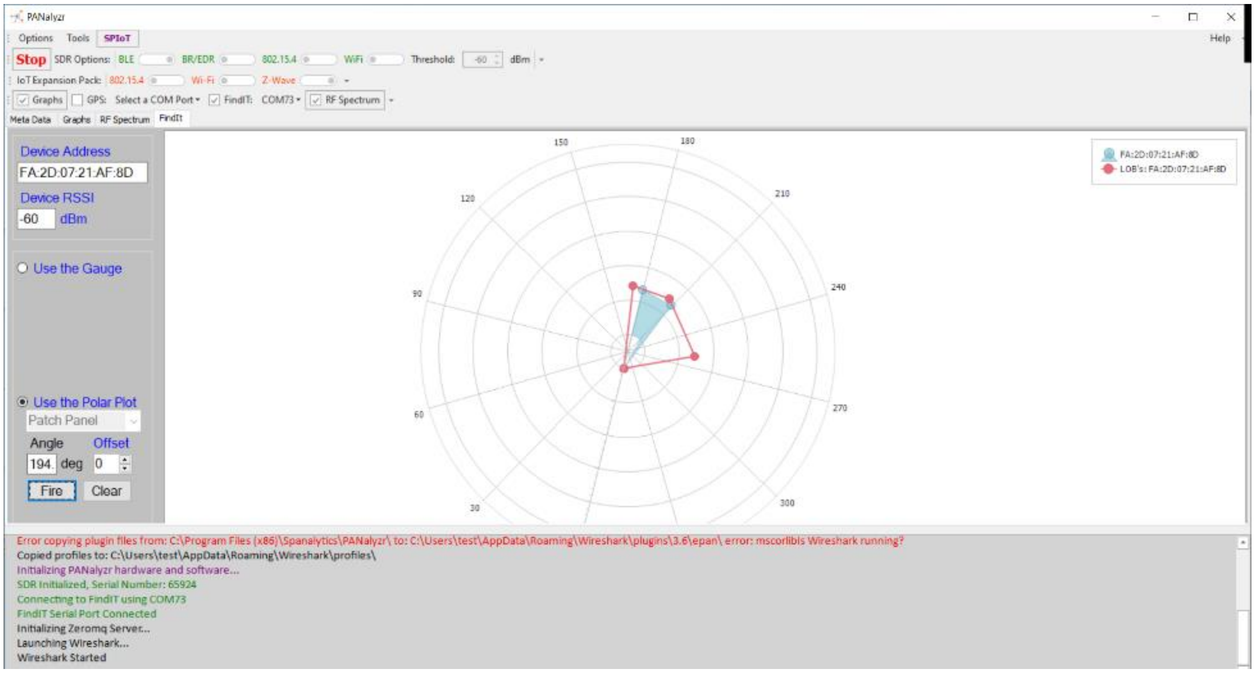
Use the Polar Plot: Displays a rotating polar plot graph with a rotating cone indicating antenna direction and RSSI. Select an antenna type from the drop-down menu.

Angle: The FindIT hardware arc of degree, offset by the offset input value.

Offset: Input the computer’s arc of degree in relation to true north

Fire: Shoots a line of bearing from the position marker in the direction of the FindIT angle, which is offset by the offset value.

Clear: Clears the polar plot of any Lines of bearing



Threshold: -60 dBm

☑ Graphs ☐ GPS: Select a COM Port ☑ FindIT: COM73 ☑ RF Spectrum

Device Address: FA:2D:07:21:AF:8D

Device RSSI: -60 dBm

Patch Panel

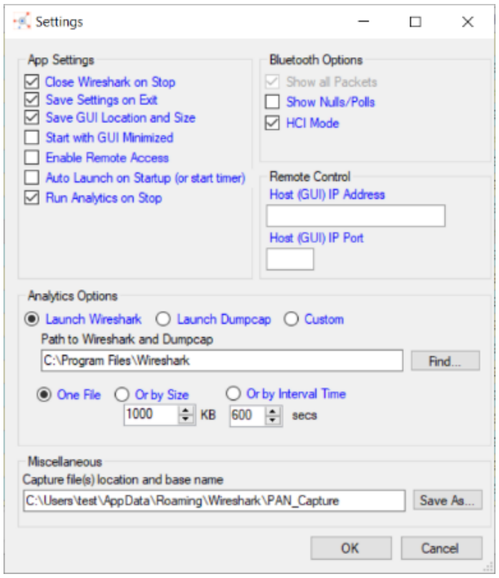
Angle: 194 deg Offset: 0

```
Error copying plugin files from: C:\Program Files (x86)\Spanalytics\PANalyzr\ to: C:\Users\test\AppData\Roaming\Wireshark\plugins\3.6\epan\ error: mscorlibIs Wireshark running?
Copied profiles to: C:\Users\test\AppData\Roaming\Wireshark\profiles\
Initializing PANalyzr hardware and software...
SDR Initialized, Serial Number: 65924
Connecting to FindIT using COM73
FindIT Serial Port Connected
Initializing Zeromq Server...
Launching Wireshark...
Wireshark Started
```

HCI Mode

The user can select the option to capture and display Bluetooth HCI packets in Wireshark. To use this function, the computer must either have an on-board Bluetooth radio or an external Bluetooth USB adapter (such as the one included in the IoT Expansion Pack) attached.

To capture HCI packets, select **Options -> Settings….** Check the **HCI Mode** checkbox, then click the **OK** button



Settings

App Settings
- ☑ Close Wireshark on Stop
- ☑ Save Settings on Exit
- ☑ Save GUI Location and Size
- □ Start with GUI Minimized
- □ Enable Remote Access
- □ Auto Launch on Startup (or start timer)
- ☑ Run Analytics on Stop

Bluetooth Options
- ☑ Show all Packets
- □ Show Nulls/Polls
- ☑ HCI Mode

Remote Control
Host (GUI) IP Address:
Host (GUI) IP Port:

Analytics Options
● Launch Wireshark ○ Launch Dumpcap ○ Custom
Path to Wireshark and Dumpcap: C:\Program Files\Wireshark

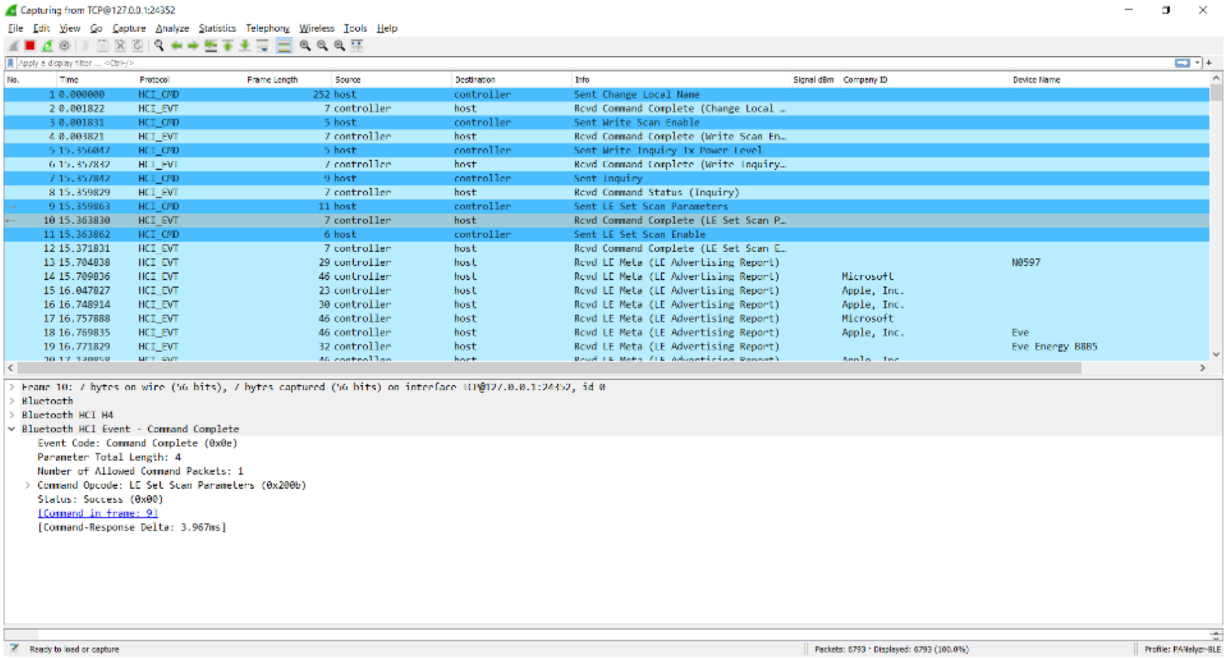
● One File ○ Or by Size 1000 KB ○ Or by Interval Time 600 secs

Miscellaneous
Capture file(s) location and base name: C:\Users\test\AppData\Roaming\Wireshark\PAN_Capture

Click the main **Launch** button, then the **Yes** button in the Account Control window.

Use the standard Windows Bluetooth device manager to find and connect to an in-range Bluetooth device

The HCI commands and events sent and received from the Bluetooth radio/adapter will be displayed in the Wireshark window



Capturing from TCP@127.0.0.1:24352

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Protocol  Frame Length  Source      Destination  Info                                    Signal dBm  Company ID    Device Name
  1 0.000000    HCI_CMD            252  host        controller   Sent Change Local Name
  2 0.001822    HCI_EVT              7  controller  host         Rcvd Command Complete (Change Local …
  3 0.001831    HCI_CMD              5  host        controller   Sent Write Scan Enable
  4 0.003821    HCI_EVT              7  controller  host         Rcvd Command Complete (Write Scan En…
  5 15.356047   HCI_CMD              5  host        controller   Sent Write Inquiry Tx Power Level
  6 15.357842   HCI_EVT              7  controller  host         Rcvd Command Complete (Write Inquiry…
  7 15.357842   HCI_CMD              9  host        controller   Sent Inquiry
  8 15.359829   HCI_EVT              7  controller  host         Rcvd Command Status (Inquiry)
  9 15.359863   HCI_CMD             11  host        controller   Sent LE Set Scan Parameters
 10 15.363830   HCI_EVT              7  controller  host         Rcvd Command Complete (LE Set Scan P…
 11 15.363862   HCI_CMD              6  host        controller   Sent LE Set Scan Enable
 12 15.371831   HCI_EVT              7  controller  host         Rcvd Command Complete (LE Set Scan E…
 13 15.704838   HCI_EVT             29  controller  host         Rcvd LE Meta (LE Advertising Report)                              N0597
 14 15.709036   HCI_EVT             46  controller  host         Rcvd LE Meta (LE Advertising Report)                Microsoft
 15 16.047827   HCI_EVT             23  controller  host         Rcvd LE Meta (LE Advertising Report)                Apple, Inc.
 16 16.748914   HCI_EVT             30  controller  host         Rcvd LE Meta (LE Advertising Report)                Apple, Inc.
 17 16.757888   HCI_EVT             46  controller  host         Rcvd LE Meta (LE Advertising Report)                Microsoft
 18 16.769835   HCI_EVT             46  controller  host         Rcvd LE Meta (LE Advertising Report)                Apple, Inc.   Eve
 19 16.771829   HCI_EVT             32  controller  host         Rcvd LE Meta (LE Advertising Report)                              Eve Energy B8B5
 20 17.130858   HCI_EVT             46  controller  host         Rcvd LE Meta (LE Advertising Report)                Apple, Inc.
```

```
> Frame 10: 7 bytes on wire (56 bits), 7 bytes captured (56 bits) on interface TCP@127.0.0.1:24352, id 0
> Bluetooth
> Bluetooth HCI H4
v Bluetooth HCI Event - Command Complete
    Event Code: Command Complete (0x0e)
    Parameter Total Length: 4
    Number of Allowed Command Packets: 1
  > Command Opcode: LE Set Scan Parameters (0x200b)
    Status: Success (0x00)
    [Command in frame: 9]
    [Command-Response Delta: 3.967ms]
```

Ready to load or capture | Packets: 6793 · Displayed: 6793 (100.0%) | Profile: PANalyzr-BLE

To switch back to using the SDR for packet capturing, do the following:

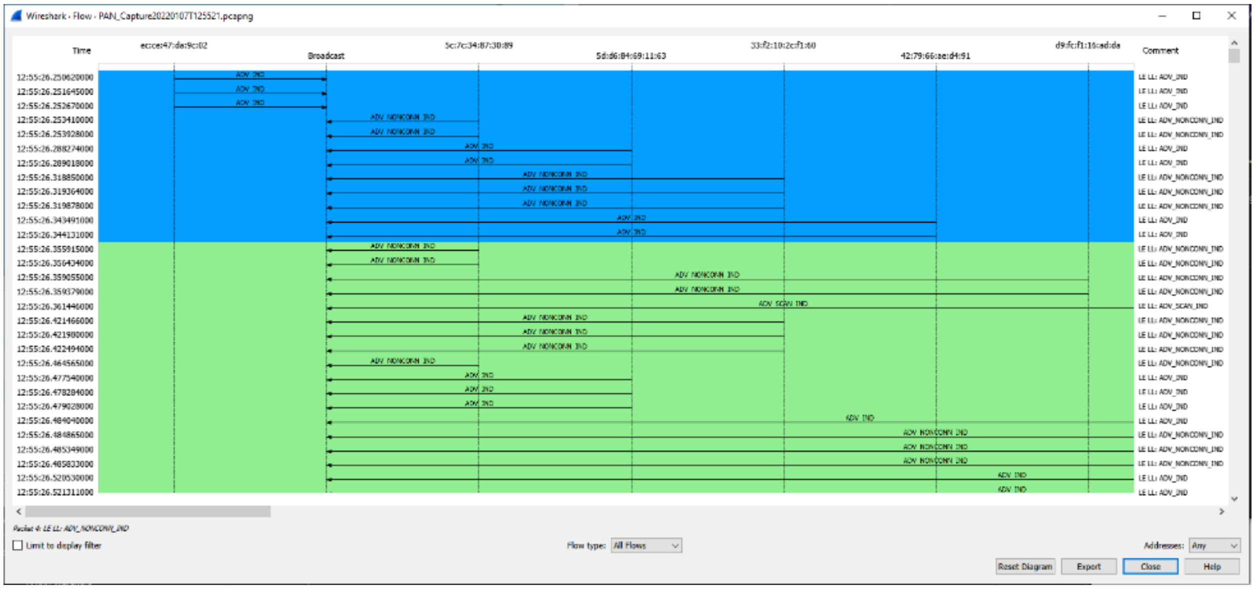
- Select **Options -> Settings…**
- Uncheck the **HCI Mode** checkbox, then click the **OK** button
- Close PANalyzr
- Restart PANalyzr

Wireshark Flow Graph

During a capture, navigate to the **Statistics** -> **Flow Graph**

This will display the message sequences in the capture.

To narrow down specific devices in the flow graph, filter them in Wireshark and select *Limit to display filter*



```
Time                 Comment
12:55:26.250620000   LE LL: ADV_IND
12:55:26.251645000   LE LL: ADV_IND
12:55:26.252670000   LE LL: ADV_IND
12:55:26.253410000   LE LL: ADV_NONCONN_IND
12:55:26.253928000   LE LL: ADV_NONCONN_IND
12:55:26.288274000   LE LL: ADV_IND
12:55:26.289018000   LE LL: ADV_IND
12:55:26.318850000   LE LL: ADV_NONCONN_IND
12:55:26.319364000   LE LL: ADV_NONCONN_IND
12:55:26.319878000   LE LL: ADV_NONCONN_IND
12:55:26.343491000   LE LL: ADV_IND
12:55:26.344131000   LE LL: ADV_IND
12:55:26.355915000   LE LL: ADV_NONCONN_IND
12:55:26.356434000   LE LL: ADV_NONCONN_IND
12:55:26.359055000   LE LL: ADV_NONCONN_IND
12:55:26.359379000   LE LL: ADV_NONCONN_IND
12:55:26.361446000   LE LL: ADV_SCAN_IND
12:55:26.421466000   LE LL: ADV_NONCONN_IND
12:55:26.421980000   LE LL: ADV_NONCONN_IND
12:55:26.422494000   LE LL: ADV_NONCONN_IND
12:55:26.464565000   LE LL: ADV_NONCONN_IND
12:55:26.477540000   LE LL: ADV_IND
12:55:26.478284000   LE LL: ADV_IND
12:55:26.479028000   LE LL: ADV_IND
12:55:26.484040000   LE LL: ADV_IND
12:55:26.484865000   LE LL: ADV_NONCONN_IND
12:55:26.485349000   LE LL: ADV_NONCONN_IND
12:55:26.485833000   LE LL: ADV_NONCONN_IND
12:55:26.520530000   LE LL: ADV_IND
12:55:26.521311000   LE LL: ADV_IND
```

Packet 4: LE LL: ADV_NONCONN_IND

☐ Limit to display filter   Flow type: All Flows   Addresses: Any

Command Line Interface

Using PANalyzr Command Line Interface (CLI) commands, a capture file can be started and stopped (no GUI interaction required). A regular Windows command prompt is required, but elevated permissions or Powershell are **not** required. The command line parameters include:

PANalyzr.exe Mode=<mode> Path=<"path"> Convention=<convention> File=<filename> State=<state>

[Upper or Lower case accepted for options]
Mode="Start" or "Stop", no quotes. Start will auto launch PANalyzr. Stop will kill the running PANalyzr.

Path="path to use for capture files", in quotes

Convention="Time", "Fixed", or "Random", no quotes. Capture file names will have a fixed name (specified by the "File" parameter), time code or a random set of 8 characters.

State="Silent", or "Normal", no quotes. Silent = minimized.

File=filename to be used, use quotes. Do **not** include file extension (example: File="file1")

To use the PANalyzr CLI, run the following steps:

- □ Open a Windows command prompt window
- □ At the command prompt type: **cd <PANalyzr Install Directory>**
  - □ If the default install configuration was used, this path would **C:\Program Files (x86)\Spanalytics\PANalyzr**
    Ex. **cd C:\Program Files (x86)\Spanalytics\PANalyzr**

Start PANalyzr with a fixed capture filename, a specified path for the capture file and with the GUI minimized

PANalyzr.exe Mode=Start Path="D:\MyCaptureFiles\\" Convention=Fixed File="file1" State=Silent

Note: The double "\\" is currently required at the end of the path string

Note: Using the Path parameter changes the "Capture file(s) location and base name" field in the PANalyzr settings. All future capture files will be stored in this folder until changed

Start PANalyzr with a timestamp-based capture filename, a specified path, with the GUI maximized and a capture threshold -55

PANalyzr.exe mode=start path="C:\Users\test\AppData\Roaming\Wireshark\\" convention=Time state=Normal threshold=-55

Stop PANalyzr

PANalyzr.exe Mode=Stop

Note: The PANalyzr software must be manually stopped (by clicking the "stop" button in the GUI) or by using the ***PANalyzr.exe Mode=Stop*** *CLI command before launching the PANalyzr software again. Otherwise, the SDR can get into a bad state and require a reset.*

Remote Control Access

The PANalyzr software can be configured to be controlled remotely to start a capture and stop a capture. To use the Remote Control access function, select **Options -> Settings….** In the Settings dialog box, check the **Enable Remote Access** checkbox then click the **OK** button. Close the PANalyzr software, and restart it. Select **Options -> Settings….** again and note the **Host (GUI) IP Address** and **Host (GUI) IP Port** fields are now populated.

The PANalyzr software has now been configured to accept a standard socket connection via the displayed IP address and IP port, and must continue to run for the duration of the remote control usage. The following strings are accepted by that socket connection:

Connect
Send this string to establish an initial socket connection to the PANalyzr server (required)

Start
Send this string to start a capture (with the current capture settings)

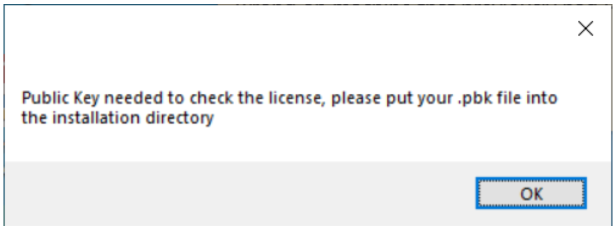
Stop
Send this string to stop the capture (GUI and Wireshark windows remain open)

Disconnect
Send this string to disconnect from the PANalyzr server
For additional assistance with this utility, contact Spanalytics customer support.

PANalyzr Troubleshooting

Licensing error message is displayed

The correct license files were not found if the following message is displayed when the PANalyzr software is launched.



Public Key needed to check the license, please put your .pbk file into the installation directory

To resolve this:

- □ Copy the provided .pbk and .lic files to the selected PANalyzr software installation folder (the default installation path is C:\Program Files (x86)\Spanalytics\PANalyzr)
- □ If no .pbk or .lic file is available, contact Spanalytics Technical Support

PANalyzr “hangs” during Rerun Analytics

The Rerun Analytics function can take various amounts of time to run depending on the number of packets captured during the capture. It can take a few seconds to a few minutes, during which the GUI will not be responsive to user interaction. Once the function completes, the GUI will become responsive as normal. If this occurs, we recommend waiting several minutes for the function to complete and the meta data and graphs in the GUI. This will be improved in future releases.

PANalyzr SDR fails on restart

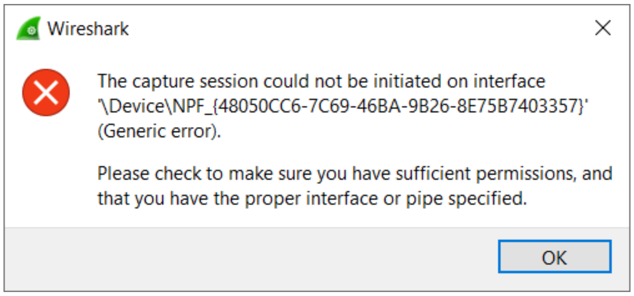
The SDR does not fully reset after the PANalyzr software has been launched and the computer has been restarted. In this scenario, when the PANalyzr software is launched after the computer restart, the LED on the SDR will change to purple and the error message “`Error Initializing SDR, please connect/reconnect!`” will be displayed in the GUI status window. To resolve this, close the PANalyzr software, detach the PANalyzr hardware, wait 10 seconds then re-attach it to the computer.

Command Line Interface Path File

If a user uses the command line interface path option, the file path must exist prior to using path options or the application will not work as intended. If the user runs for example ‘PANalyzr.exe Mode=Start Path=C:\Tester\Captures” and the file path C:\Tester\Captures does not exist, PANalyzr will not properly launch.

Wi-Fi error

If npcap is not installed correctly, the following error message is displayed when Wireshark is launched with the option to use the Panda Wi-Fi adapter.



The capture session could not be initiated on interface '\Device\NPF_{48050CC6-7C69-46BA-9B26-8E75B7403357}' (Generic error).

Please check to make sure you have sufficient permissions, and that you have the proper interface or pipe specified.

Error Initializing SDR

If the following messages are displayed in the status window, detach the PANalyzr hardware, wait 10 seconds then re-attach it to the computer

```
Failed Invalid response
Error Initializing SDR, please connect/reconnect!

Failed Connection error
Error Initializing SDR, please connect/reconnect!
```

802.15.4 Toggle is Disabled

If a user launches PANalyzr and has the Q59 dongle attached, but the **802.15.4 toggle switch is disabled**, they need to verify that the correct driver installed for the Q59 dongle. To resolve this:

- ☐ Open **Device Manager -> Ports (COM & LPT)**
- ☐ Unplug and re-insert the Q59 dongle to observe which COM device driver is applied to the dongle. If it does not show up as "**USB Serial Device (COMX)**", it won't be detected and selectable in PANalyzr. Right-click the device in the COM ports list and select **Uninstall device** from the menu
- ☐ Once the device driver uninstall completes, select the **Scan for hardware changes** button on the Device Manager menu.

This should install the correct serial device driver for the Q59 adapter

BR/EDR Dissection is not complete

If the dissection for BR/EDR packets listed in the Packet View does not look complete, apply the profile ***PANalyzr-BREDR*** to add columns and refresh the view.

PANalyzr gets stuck / No packets in the Wireshark window

If there are no Bluetooth packets in the Wireshark window, attempt to generate the traffic again.

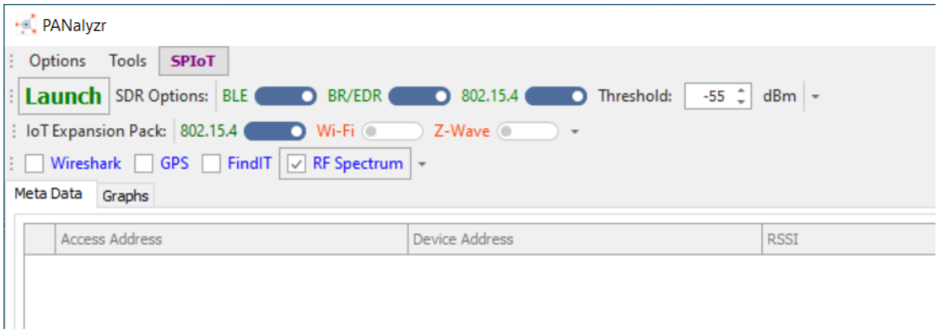
If packets are still not displayed in the Wireshark window, this could indicate the detection threshold is too high or low.

If the LED on the PANalyzr Protocol Analyzer has changed to a flashing Red or solid Blue color, then perform the following steps to resolve the issue:

- □ Close the PANalyzr software
- □ Detach the PANalyzr hardware
- □ Re-attach the PANalyzr hardware to the computer
- □ Restart the PANalyzr software

Longevity Usage Recommendations

- □ Launch with the **Wireshark** checkbox unchecked



- □ Disable Windows update and power settings (in accordance with your company IT policy)

Antivirus

Some antivirus software may quarantine the **panalyzr_win_gui.exe** executable. If this occurs:

1. Restore the panalyzr_win_gui.exe file if it's been quarantined
2. Add the executable to the allowed list of your antivirus software

“Error occurred: tshark: Syntax Error” Message Displayed in brackle status window

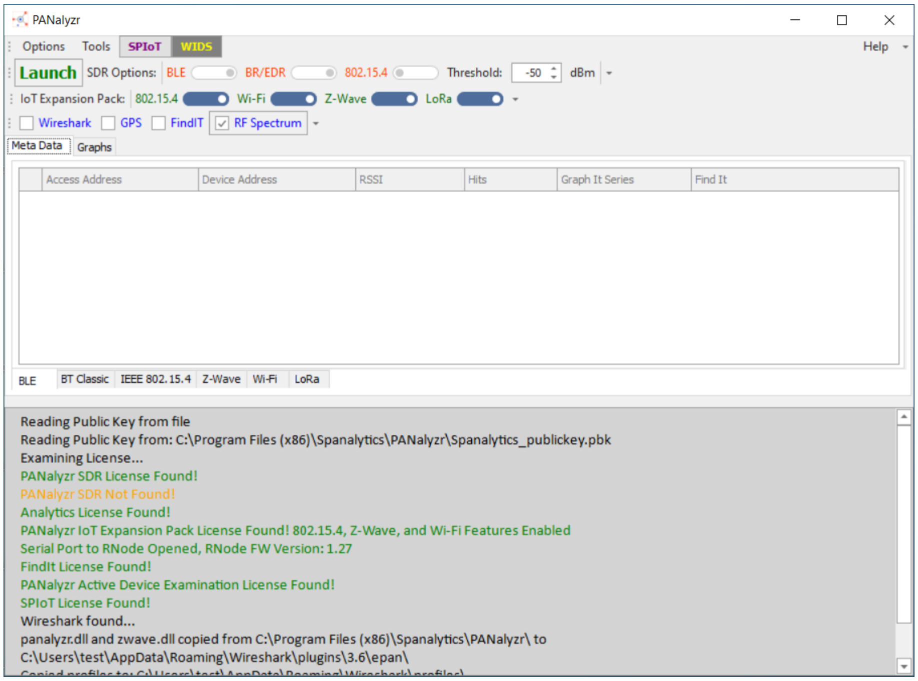
If the following error messages are displayed in the brackle status window, it means the user has tried to run brackle on files in a folder they don’t have permission in:

```
Calling Tshark to create capture file with only btle_rf1 type packets...
Error occurred: tshark: Syntax error.
Unable to process this capture file. See the User Guide for troubleshooting recommendations
Calling Tshark to create capture file with only btbredr_rf1 type packets...
Error occurred: tshark: Syntax error.
Unable to process this capture file. See the User Guide for troubleshooting recommendations
```

To resolve this, move or copy the capture files to a folder the user does have permission (e.g., Documents, Desktop, etc.)

SDR options are disabled (greyed out)

If the BLE, BR/EDR and 802.15.4 SDR options are all disabled (greyed out), this means that the SDR was not detected on startup. Additionally, the message “PANalyzr SDR Not Found!” will be displayed in the status window:



Threshold: -50 dBm

```
Reading Public Key from file
Reading Public Key from: C:\Program Files (x86)\Spanalytics\PANalyzr\Spanalytics_publickey.pbk
Examining License...
PANalyzr SDR License Found!
PANalyzr SDR Not Found!
Analytics License Found!
PANalyzr IoT Expansion Pack License Found! 802.15.4, Z-Wave, and Wi-Fi Features Enabled
Serial Port to RNode Opened, RNode FW Version: 1.27
FindIt License Found!
PANalyzr Active Device Examination License Found!
SPIoT License Found!
Wireshark found...
panalyzr.dll and zwave.dll copied from C:\Program Files (x86)\Spanalytics\PANalyzr\ to
C:\Users\test\AppData\Roaming\Wireshark\plugins\3.6\epan\
Copied profiles to: C:\Users\test\AppData\Roaming\Wireshark\profiles\
```

To resolve this, detach and re-attach the PANalyzr SDR to the computer, then restart the PANalyzr software. The options should then be selectable