Document Number:
Rev. 0.1 10/2021

1. General Introduction

The nRF Sniffer is a tool for debugging Bluetooth low energy (BLE) applications by detecting packets between a selected device and the device it is communicating with, even when the link is encrypted. When developing a BLE product, knowing what happens over-the-air between devices can help you isolate and solve any potential issues.

By default, the Sniffer lists nearby BLE devices that are advertising, providing the Bluetooth Address and Address type, complete or shortened name, and RSSI.

2. Required hardware

To set up the Sniffer you will need one of the following kits:

- nRF51 Development Kit (PCA10028) v1.0 or later and a micro USB cable
- nRF51 Dongle(PCA10031)
- nRF51822 Evaluation Kit (PCA10001) and a mini USB cable
- nRF51422 Evaluation Kit (PCA10003) v3.0.0 or later and a mini USB cable
- nRF51822 Development Kit dongle (PCA10000)
- nRF52 Development Kit (PCA10040) and a micro USB cable
- nRF52840 Development Kit (PCA10056) and a micro USB cable
- nRF52840 Dongle (PCA10059)

3. Required software

- Wireshark v3.2.4 or later available from official site (http://www.wireshark.org/) or use downloaded software on internal website.Wireshark is a free software tool that captures wireless traffic and reproduces it in a readable format.
- nRF Sniffer software v3.x or later available on the Sniffer product page under the downloads tab (https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le/) or download it through our website.
- An operating system that runs the required version of Wireshark
  - Windows 7 or later
  - 64 bit OS X/macOS 10.6 or later
  - Linux (check for version compatibility)

4. Install nRF Sniffer

The nRF Sniffer for Bluetooth LE software consists of firmware that is programmed onto a development board or dongle and a capture plugin for Wireshark that records and analyzes the detected data.Before you start setting up the nRF Sniffer, make sure that you have the following prerequisites installed on your computer:

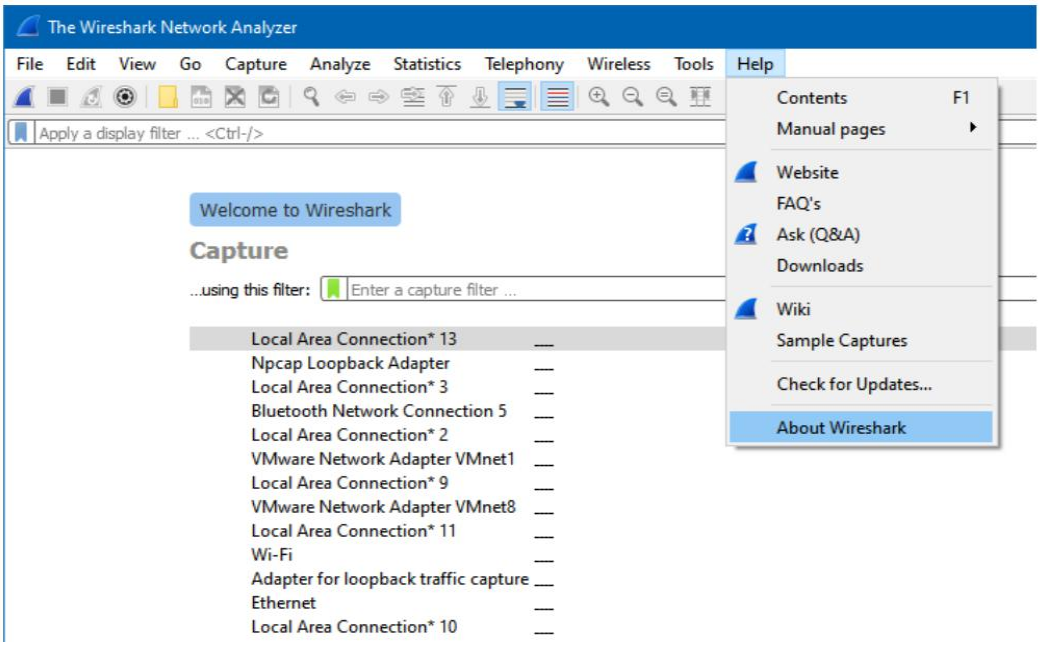
- Wireshark v3.2.4 or later (v3.0.7 or later recommended on Windows).
- Download nRF Sniffer for Bluetooth LE v3.x or later and extract the archive into a folder

Then install the nRF Sniffer capture tool, and add a Wireshark profile for the Sniffer as described in the following sections.

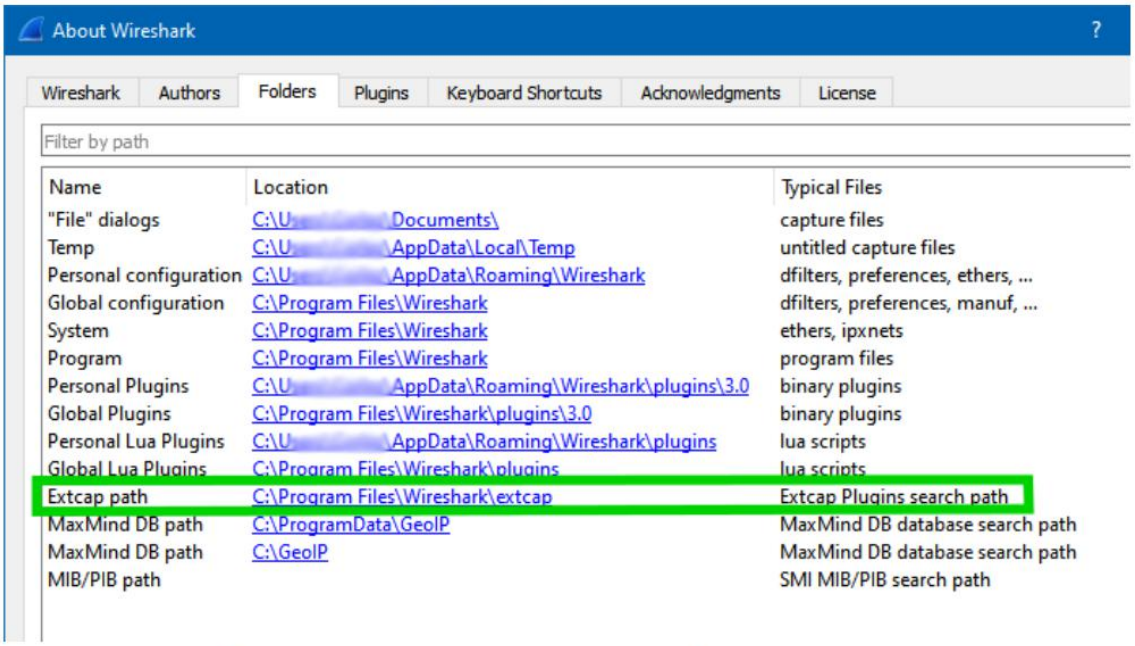
5. Installing the nRF Sniffer capture tool

The nRF Sniffer for Bluetooth LE software is installed as an external capture plugin in Wireshark. To install the nRF Sniffer capture tool, complete the following steps:

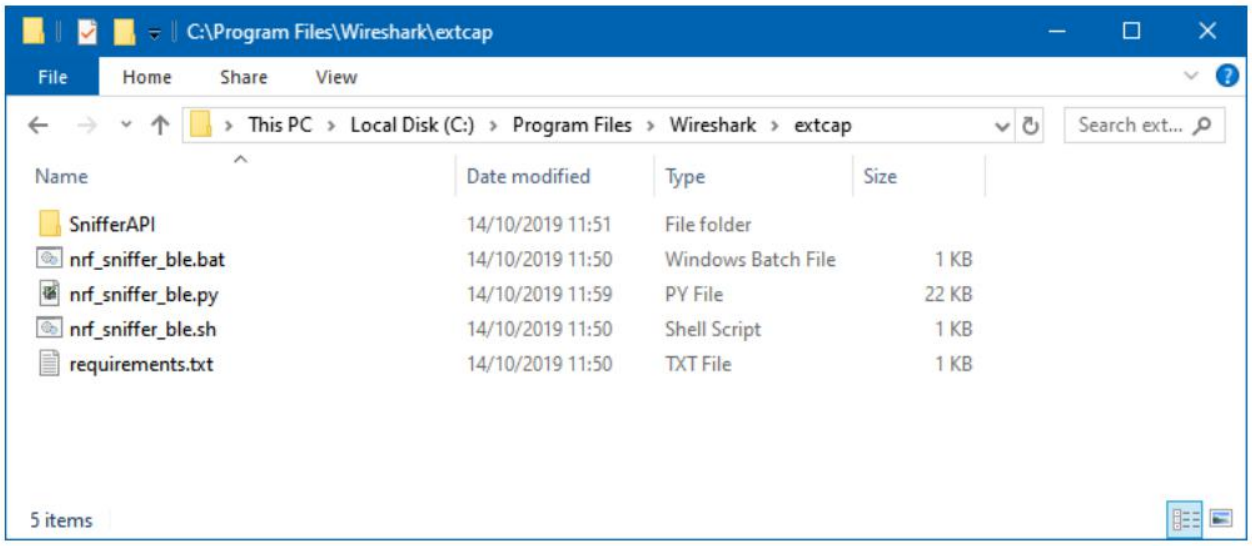
- Open Wireshark- Go to Help > About Wireshark.



- Select the Folders tab.
- Double-click the location for the Global Extcap path to open this folder.



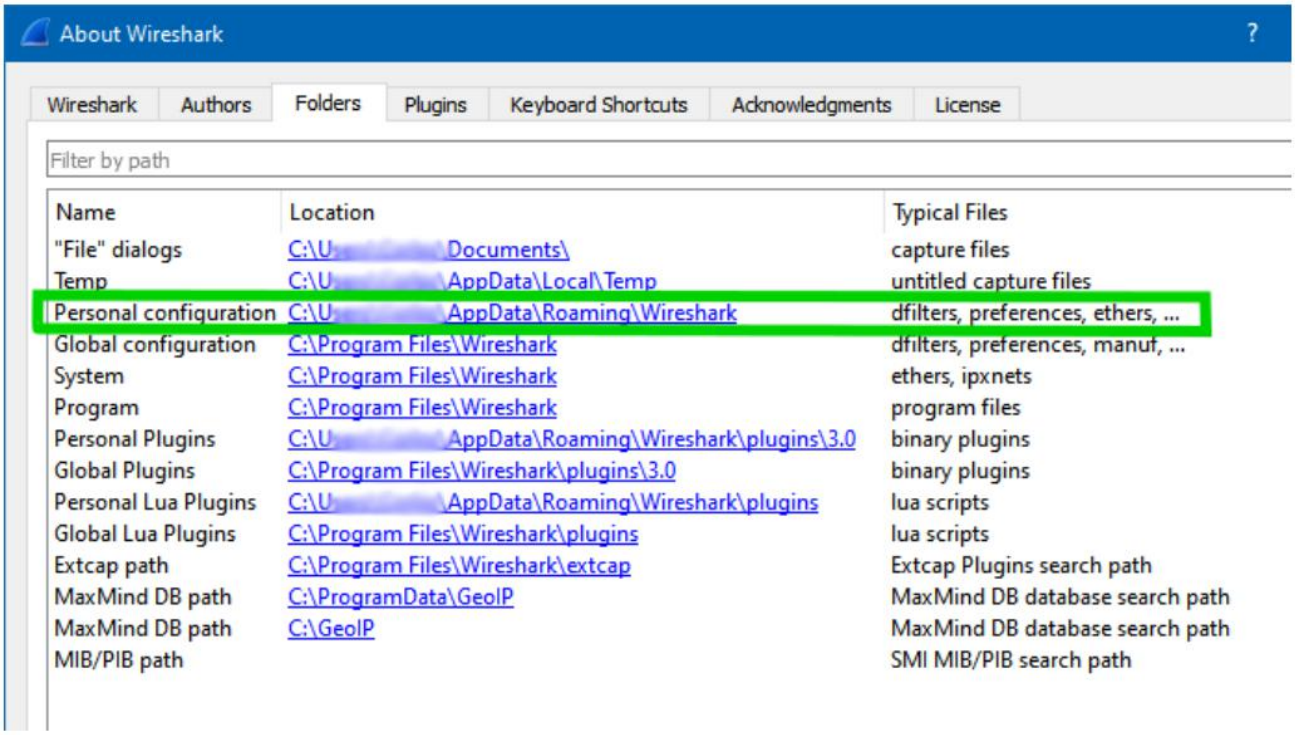
- Copy the contents of the nrf_sniffer_for_bluetooth_le_3.1.0_7cc811f /extcap/ folder into this folder.



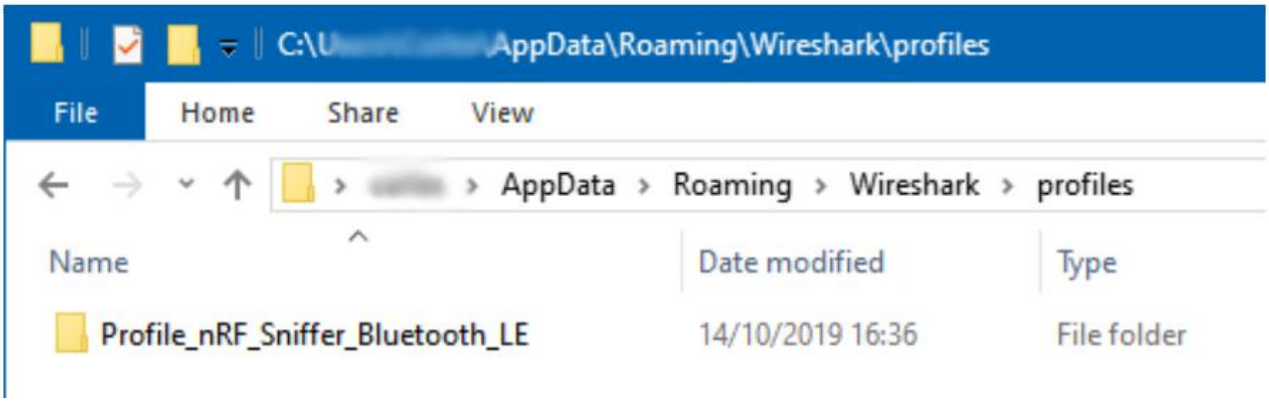
6. Adding a Wireshark profile for nRF Sniffer

You can add a profile in Wireshark for displaying the data recorded by the nRF Sniffer for Bluetooth LE in a convenient way. To add the nRF Sniffer profile in Wireshark, complete the following steps:

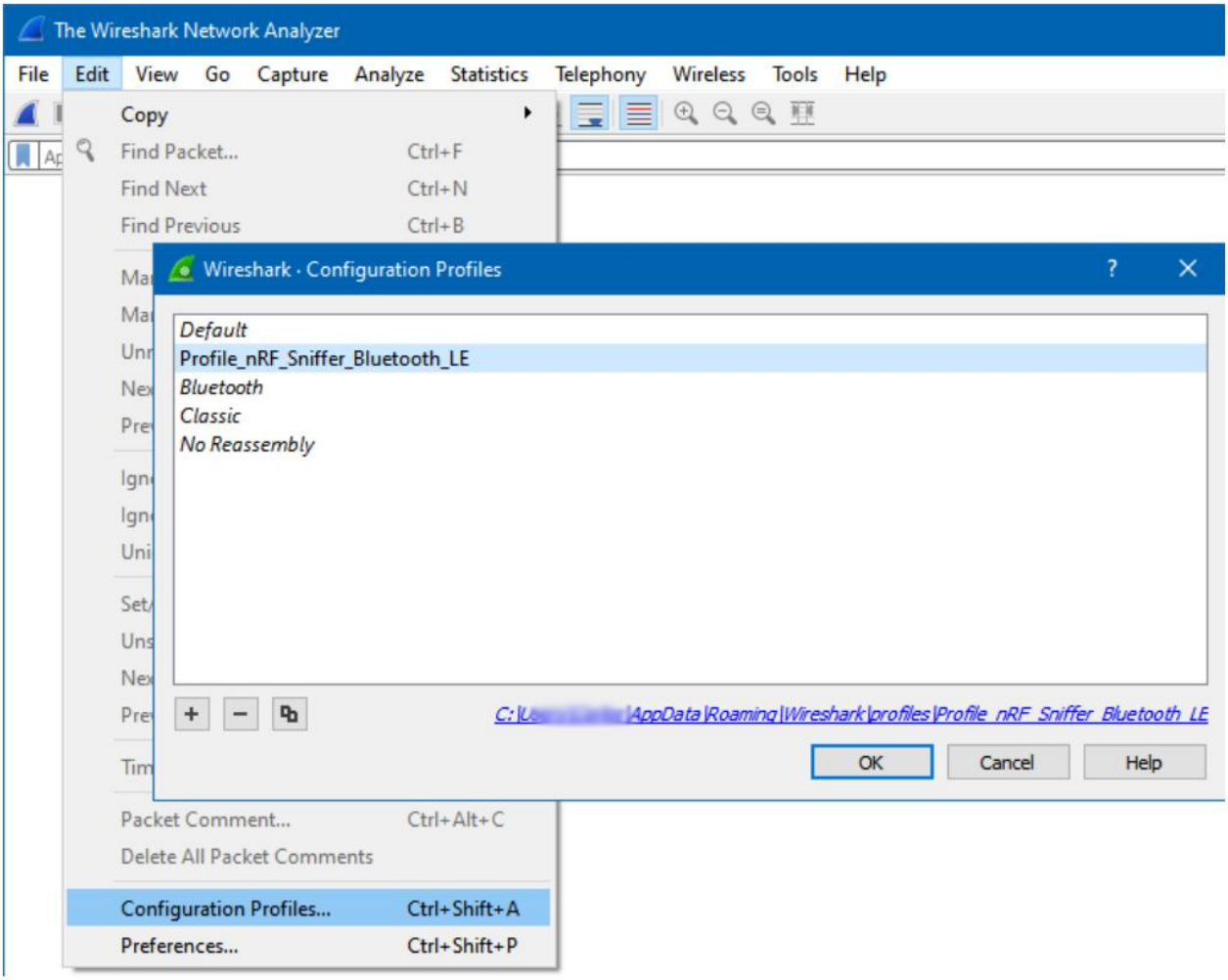
- Go to Help > About Wireshark .
- Select the Folders tab.
- Double-click the location for the Personal configuration to open this folder



- Copy the folder Profile_nRF_Sniffer_Bluetooth_LE, which is found in the nRF Sniffer v3 release ZIP file, to the profiles folder within the Personal Configuration folder.



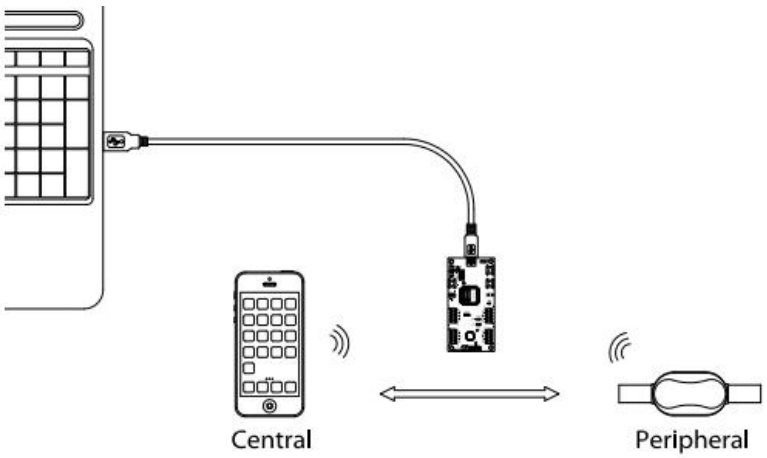
- In Wireshark, select Edit > Configuration Profiles.
- Select Profile_nRF_Sniffer_Bluetooth_LE and click OK.



7. Running nRF Sniffer

To start sniffing, place the board or dongle that runs the nRF Sniffer for Bluetooth LE firmware between the two devices that are communicating. Then open Wireshark and start recording packets.

Connect the development board or dongle to your computer and turn it on. Then place it between the Central and Peripheral device that you want to sniff.



When you open Wireshark, the Wireshark capture screen is displayed. It includes the Wireshark interface for managing packets that are captured, the nRF Sniffer toolbar, and the hardware interfaces connected to the nRF Sniffe.To start sniffing, double-click on the hardware interface (nRF Sniffer for Bluetooth LE COM18 in the following figure)

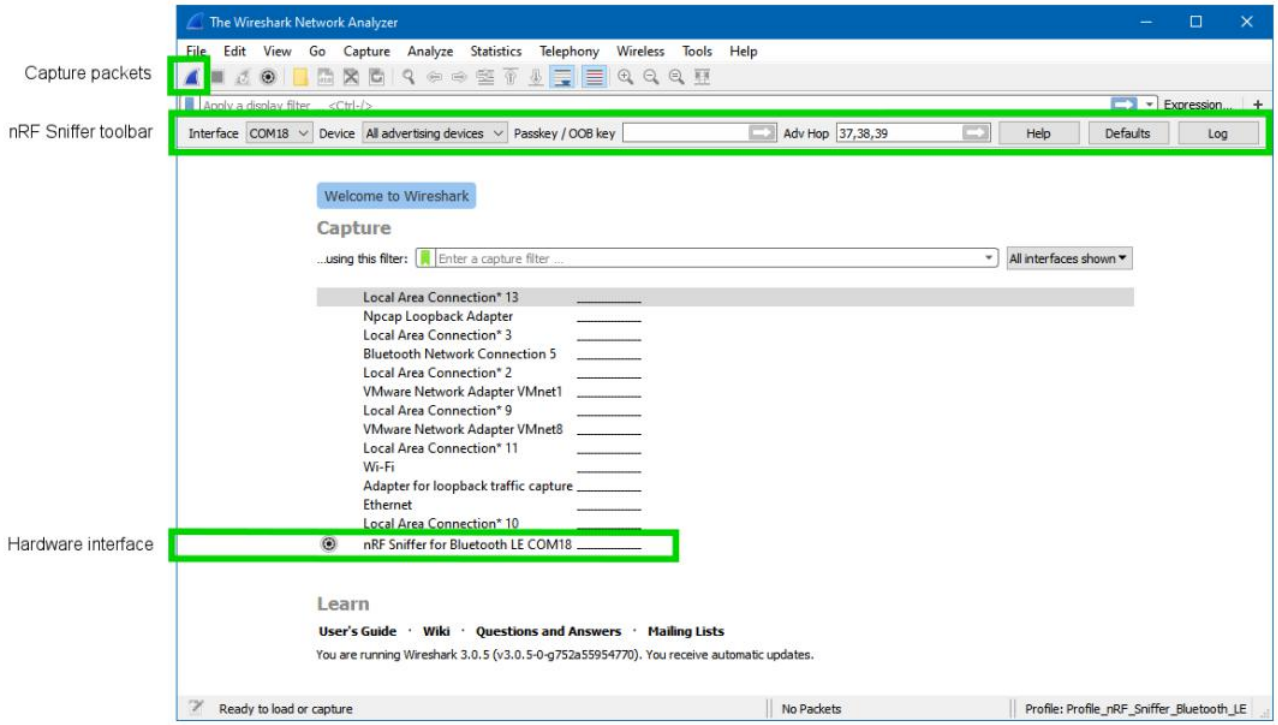


Figure 2: Wireshark capture screen

8. nRF Sniffer usage

Once the nRF Sniffer for Bluetooth LE is running, it reports advertisements and lists nearby devices in the Device List. The software interface has several commands for controlling the operating mode of the Sniffer.

The Sniffer has two modes of operation:

1. Listen on all advertising channels to pick up as many packets as possible from as many devices as possible. This is the default mode.

2. Follow one particular device and try to catch all packets sent to or from this particular device. This mode will catch all:

- Advertisements and Scan Responses sent from the device
- Scan Requests and Connect Requests sent to the device
- Packets in the connection sent between the two devices in the connection

The software interface provides commands and options that control the Sniffer operation：

- **Hardware interface**

This list shows the available hardware interfaces. If you have more than one board with the nRF Sniffer firmware connected, you can choose which one to control with the toolbar. To use several hardware interfaces at the same time, see Capturing from multiple hardware interfaces on page14.

- **Device list**

This list shows nearby devices that are advertising. When you start sniffing All advertising devices is selected. Choose a device from the list to sniff that specific device. When you select a different device while in a connection, the current connection is lost.

- **Passkey and OOB key**

If your device asks you to provide your passkey, type the 6-digit passkey in the passkey text field and press Enter. Then enter the passkey into the device. Passkey entry utilizes Just Works pairing.If you are asked to provide the 16-byte Out-of-band (OOB) key, provide it in hexadecimal format(starting with 0x, big endian). You must do this before the device enters encryption. If the entered key is shorter than 16 bytes, it will be padded with zeros in front. OOB entry uses Out of Band pairing.

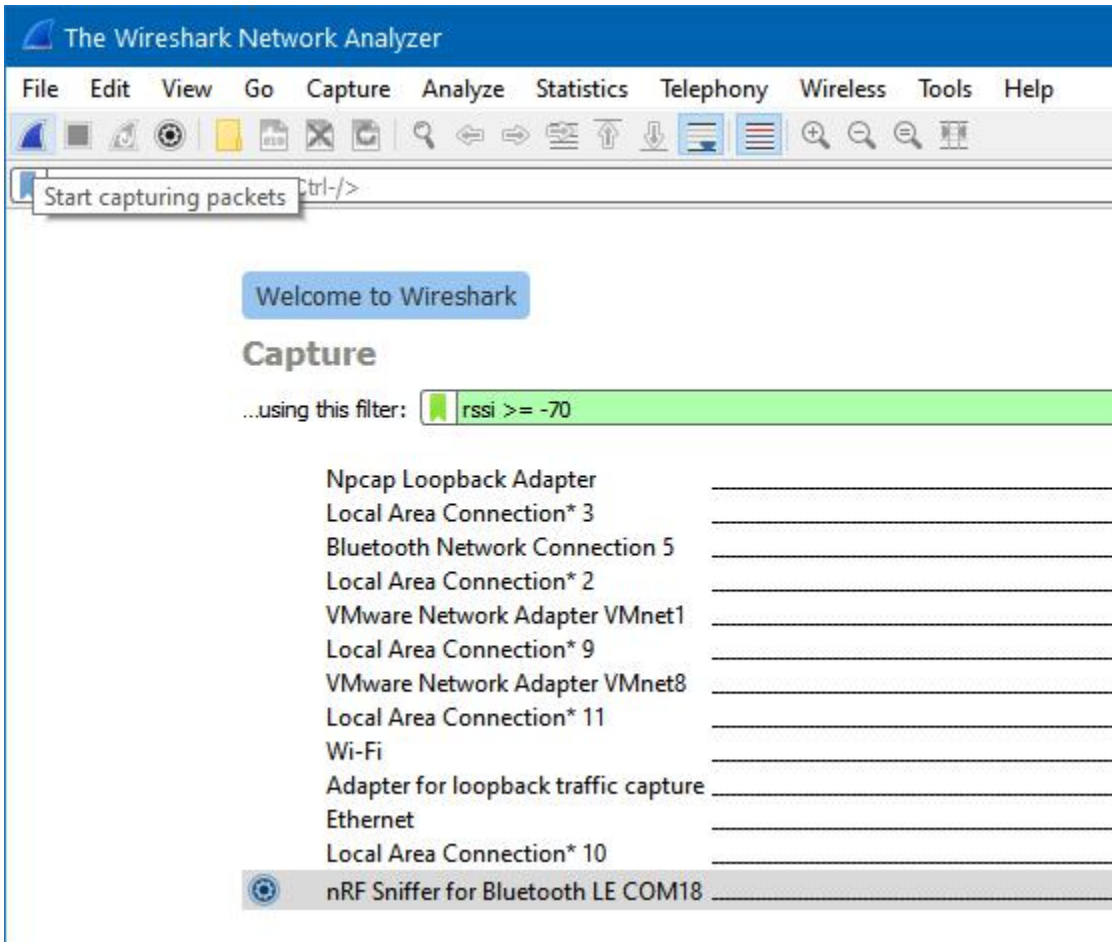
See Sniffing a connection between paired devices on page 18 for more information.

- **Advertising hop sequence**

You can change the order in which the Sniffer switches advertising channels when following a device.Define the order with comma-separated channel numbers, for example, 37,38,39. Press Enter when done.
With the default configuration, the Sniffer will wait for a packet on channel 37. After it receives a packet on channel 37, it will transition to sniffing on channel 38. When it receives a packet on channel 38, it will transition to sniffing on channel 39. When it receives a packet on channel 39, it will start sniffing on channel 37, and repeats the operation.

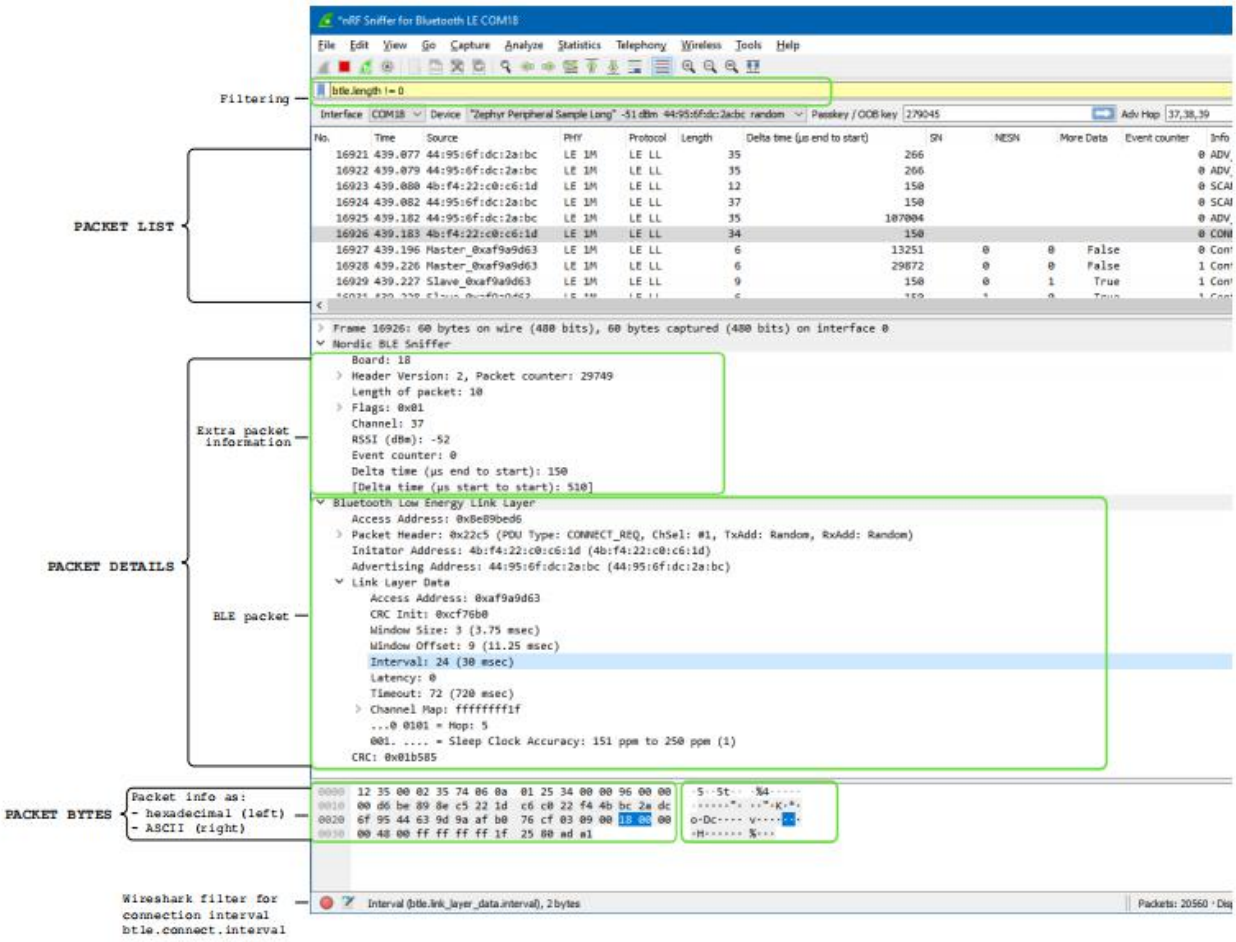
- **RSSI filter**

You can apply an RSSI filter on the packets that are being received. Only packets that match the filter are displayed.
You must set the capture filter in the capture screen in Wireshark. Use the keyword "rssi". For example, the filter rssi >= -70 will capture only packets that have an RSSI greater than or equal to -70 dBm.



9. Inspecting captured data

All Bluetooth Low Energy packets detected by the Sniffer for Bluetooth LE are passed to Wireshark, where they are wrapped in a header containing useful meta-information not present in the Bluetooth Low Energy packet itself. Wireshark dissects the packets and separates the actual packet from the meta-information.When you browse captured packets, select a packet in the packet list to show the breakdown of that packet in the packet details pane. The bytes of the packet are shown in the packet bytes pane. Click a value in the details to highlight it among the bytes, or click on the bytes to highlight it in the details.



Use display filters to display a chosen packet subset. Most filters are based on the values of the packets,such as length or access address. The filter expressions use Boolean operators (&& || == != !). To construct a filter, click Expression in the filtering bar. See the following table for some examples.

Display filter	Description
btle.length != 0	Filter that displays only packets where the length field of the Bluetooth Low Energy packet is not zero, meaning it hides empty data packets.
btle.advertising_address	Filter that displays only packets that have an advertising address (advertising packets).
btle	Protocol filter that displays all Bluetooth Low Energy packets.
btatt, btsmp, btl2cap	Protocol filters for ATT, SMP, and L2CAP packets, respectively.

The following tips can help when inspecting your data:

- Turn any field in the packet details pane into a column. To do so:

a) Right-click the value in the packet details.

b) Click Apply as Column.

- Apply a value as a filter to, for example, see only operations affecting a particular handle. To filter packets that have a specific value for some field:

a) Right-click the value in the packet details.

b) Click Apply as Filter.

c) Click Selected.

- Save a set of captured packets to be able to look at them later. To do so:

a) Click the Stop button to stop capturing packets.

b) Click File > Save As to save all packets, or click File > Export Specified Packets to save a selection of

packets.

- Clear the packet list and restart a capture by clicking the Restart button.

See the documentation on the Wireshark website for more information.