nRF Sniffer for Bluetooth LE

v3.1.0

User Guide

v3.2

NORDIC® SEMICONDUCTOR

Contents

Revision history

Date	Version	Description
November 2020	3.2	• Updated Supported devices • Updated Programming the nRF Sniffer firmware on page 6 • Editorial changes
January 2020	3.1	Corrected Python requirements
December 2019	3.0	• Editorial changes to all sections • Updated to match nRF Sniffer for *Bluetooth*® LE v3.0.0
September 2018	2.2	Updated content: • Required software • Setting up the nRF Sniffer • Sniffer commands • Troubleshooting
January 2018	2.1	Updated content: • Required software • Setting up the nRF Sniffer
November 2017	2.0	• nRF Sniffer updated to work more closely with Wireshark • Updated software to support the nRF52 DK
April 2017	1.4	Updated content: • Removed reference to nRF52 Series in Required hardware • Required software • Setting up the nRF Sniffer
March 2017	1.3	Updated content: • Required hardware • Required software • Setting up the nRF Sniffer
July 2014	1.2	Updated content: • Required hardware • Required software • Setting up the nRF Sniffer • Running the Sniffer • Using the Sniffer • Using Wireshark • Wireshark Tips • Troubleshooting
April 2014	1.1	Updated firmware, now supports all versions of PCA10000 and PCA10001

Date	Version	Description
December 2013	1.0	First release

Previous versions

PDF files for relevant previous versions are available here:

- nRF Sniffer User Guide v3.1 (corresponds to nRF Sniffer v3.0.0)
- nRF Sniffer User Guide v2.2 (corresponds to nRF Sniffer v2.x)

1 Introduction

The nRF Sniffer for Bluetooth LE is a useful tool for learning about and debugging Bluetooth Low Energy applications. It provides a near real-time display of Bluetooth packets that are sent between a selected Bluetooth Low Energy device and the device it is communicating with, even when the link is encrypted.

When developing a Bluetooth Low Energy product, knowing what happens over-the-air between devices can help you identify and fix issues quickly.

On startup, the Sniffer lists all nearby Bluetooth Low Energy devices that are advertising, providing the Bluetooth address and address type, complete or shortened name, and RSSI.

Supported development kits and dongles

- nRF52840 DK (PCA10056)
- nRF52840 Dongle (PCA10059)
- nRF52 DK (PCA10040)
- nRF51 DK (PCA10028)
- nRF51 Dongle (PCA10031)

Supported operating systems

- Windows 7 or later
- 64-bit OS X/macOS 10.6 or later
- Linux (check the Wireshark prerequisites for version compatibility)

2 Installing nRF Sniffer

The nRF Sniffer for Bluetooth LE software consists of firmware that is programmed onto a development kit 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 v2.4.6 or later (v3.0.7 or later recommended on Windows). Wireshark is a free software tool that captures wireless traffic and reproduces it in a readable format.
- Python v3.6 or later.

Download nRF Sniffer for Bluetooth LE v3.x or later and extract the archive into a folder of your choice. In the following sections, we will refer to this folder as *Sniffer_Software*.

Then program the firmware to the development kit or dongle, install the nRF Sniffer capture tool, and add a Wireshark profile for the Sniffer as described in the following sections.

2.1 Programming the nRF Sniffer firmware

You must connect a development kit or dongle running the nRF Sniffer firmware to your computer to be able to use the nRF Sniffer for Bluetooth LE.

See Supported development kits and dongles for a list of development kits and dongles that can run the nRF Sniffer firmware.

There are various ways to program the nRF Sniffer firmware. The following instructions use nRF Connect Programmer, but you can also use the command-line tool **`nrfjprog`** (which is part of the nRF Command Line Tools).

To program your development kit or dongle, complete the following steps:

1. Install nRF Connect Programmer.

   See Installing the Programmer for instructions.
2. On macOS and Linux, install the SEGGER J-Link software.

   It is available from SEGGER J-Link Software.

   > **Note:** On Windows, the J-Link software is included in nRF Connect for Desktop, so you can skip this step.
3. Locate the firmware HEX file for your development kit or dongle.

   All firmware HEX files are located in `Sniffer_Software/hex/`. Use the suitable file for your development kit or dongle:

Development kit/dongle	Firmware file name
nRF52840 DK (PCA10056)	`sniffer_nrf52840dk_nrf52840_*.hex`
nRF52840 Dongle (PCA10059)	`sniffer_nrf52840dongle_nrf52840_*.hex`
nRF52 DK (PCA10040)	`sniffer_nrf52dk_nrf52832_*.hex`
nRF51 DK (PCA10028)	`sniffer_nrf51dk_nrf51422_*.hex`
nRF51 DK (PCA10031)	`sniffer_nrf51dongle_nrf51422_*.hex`

Table 1: Firmware file names

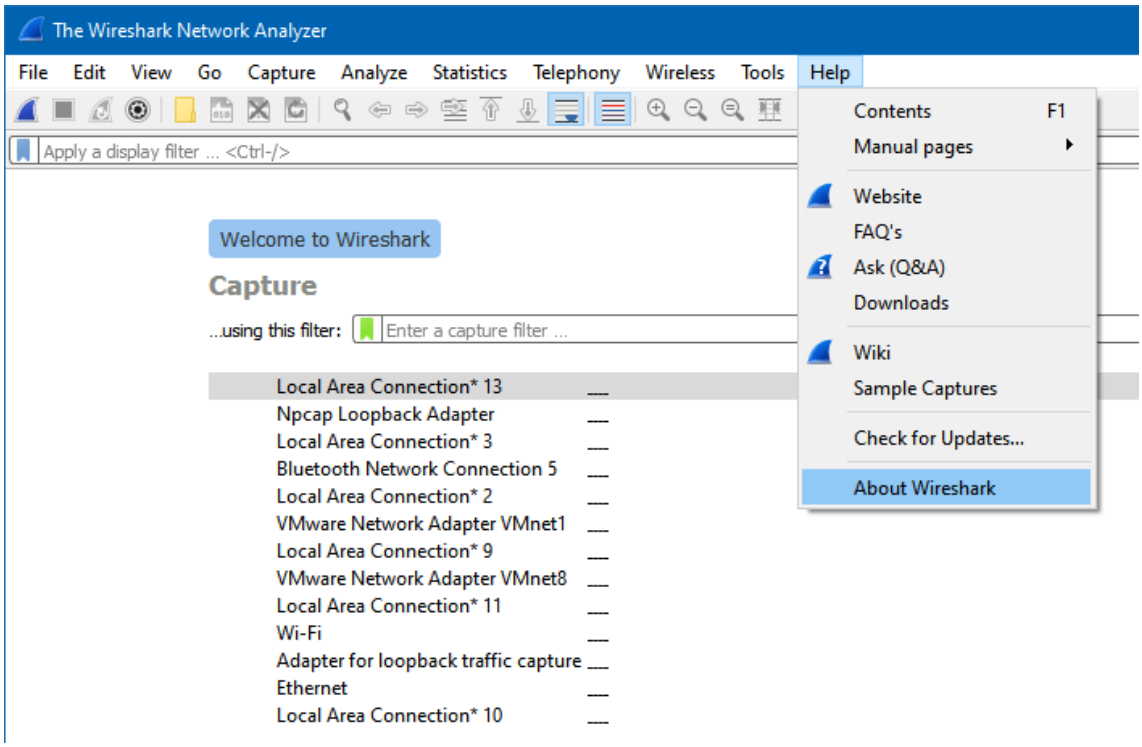
4. Follow the instructions in Programming a Development Kit or the nRF51 Dongle or Programming the nRF52840 Dongle to program the HEX file.

2.2 Installing the nRF Sniffer capture tool

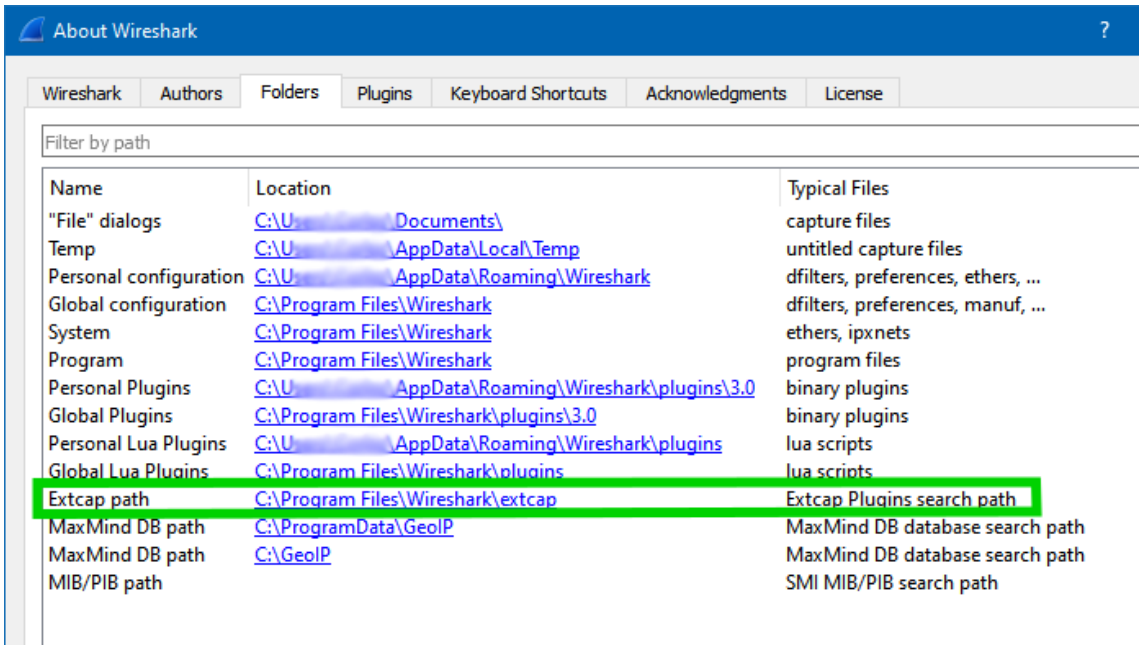
The nRF Sniffer for Bluetooth LE software is installed as an external capture plugin in Wireshark.

To install the nRF Sniffer capture tool, complete the following steps:

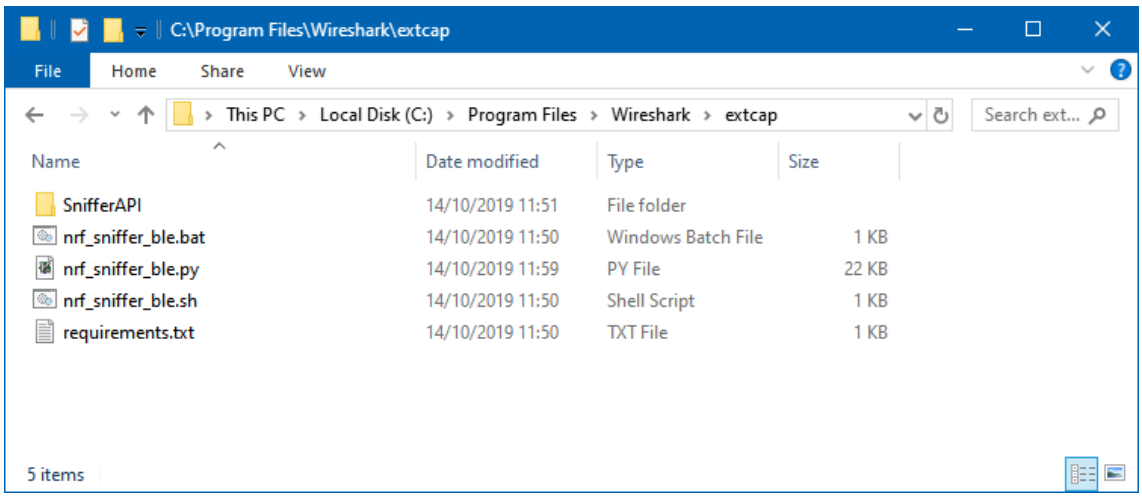
1. Install the Python requirements:
   a) Open a command window in the *`Sniffer_Software/extcap/`* folder.
   b) Type `pip3 install -r requirements.txt` to install the requirements.
   c) Close the command window.
2. Copy the Sniffer capture tool into Wireshark's folder for external capture plugins:
   a) Open Wireshark.
   b) Go to **Help** > **About Wireshark** (on Windows or Linux) or **Wireshark** > **About Wireshark** (on macOS).



   c) Select the **Folders** tab.
   d) Double-click the location for the **Extcap path** to open this folder.



e) Copy the contents of the *Sniffer_Software*/extcap/ folder into this folder.



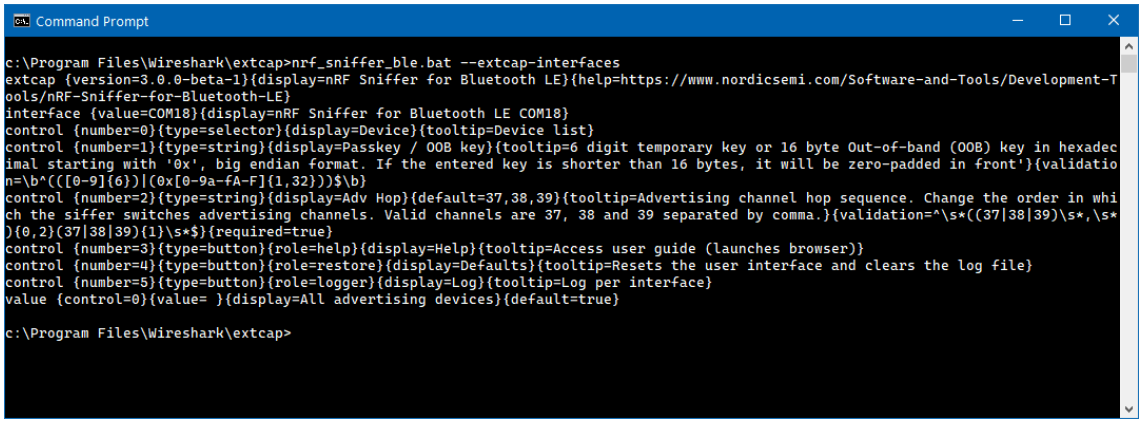
3. Make sure that the nRF Sniffer files can be run correctly:

a) Open a command window in Wireshark's folder for external capture plugins.

b) Run the Sniffer tool to list available interfaces.

On Windows, type `nrf_sniffer_ble.bat --extcap-interfaces`. On macOS or Linux, type `nrf_sniffer_ble.sh --extcap-interfaces`.

You should see a series of strings, similar to what is shown in the following screenshot.



c) If the previous step returned an error, verify that Python 3 is accessible.

On Windows, enter `python --version`. On macOS or Linux, enter `python3`. If the command cannot be found or the version is wrong, make sure that Python v3.6 or later is in your path and that it is the first Python version in the path.

d) For macOS or Linux: Verify that the `nrf_sniffer_ble.sh` file has the `x` permission.

If the `x` permission is missing, add it using `chmod +x nrf_sniffer_ble.sh`.

4. Enable the nRF Sniffer capture tool in Wireshark:

a) Refresh the interfaces in Wireshark by selecting **Capture** > **Refresh Interfaces** or pressing **F5**.

You should see that nRF Sniffer is displayed as one of the interfaces on the start page.

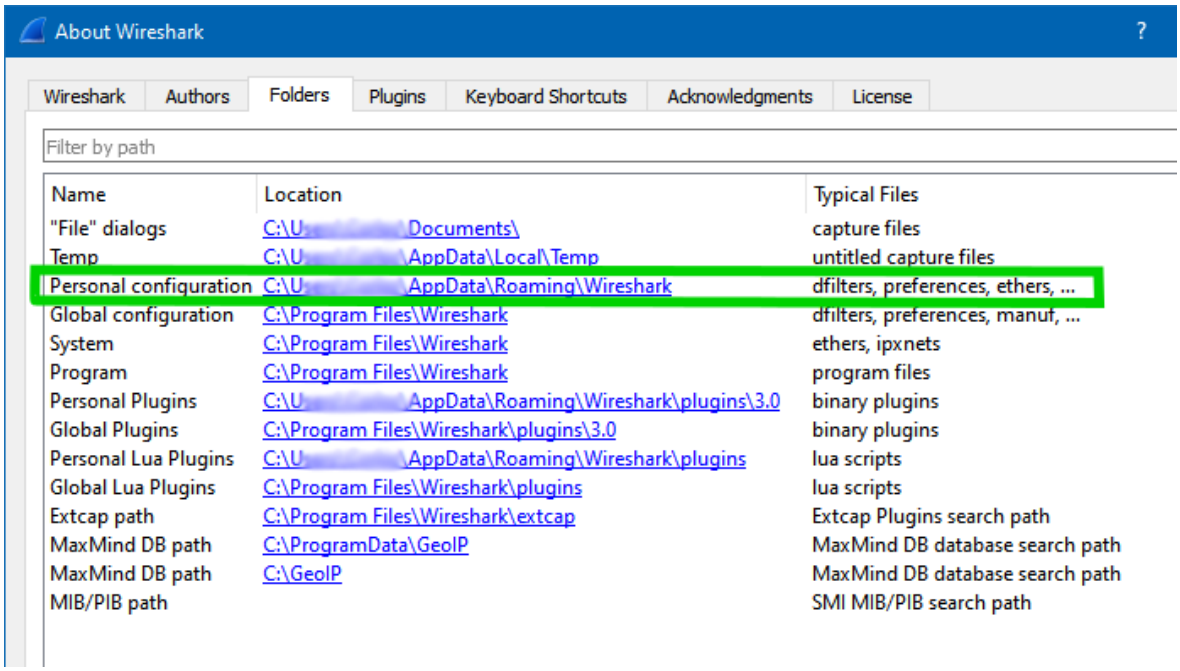
b) Select **View** > **Interface Toolbars** > **nRF Sniffer for Bluetooth LE** to enable the Sniffer interface.

2.3 Adding a Wireshark profile for nRF Sniffer

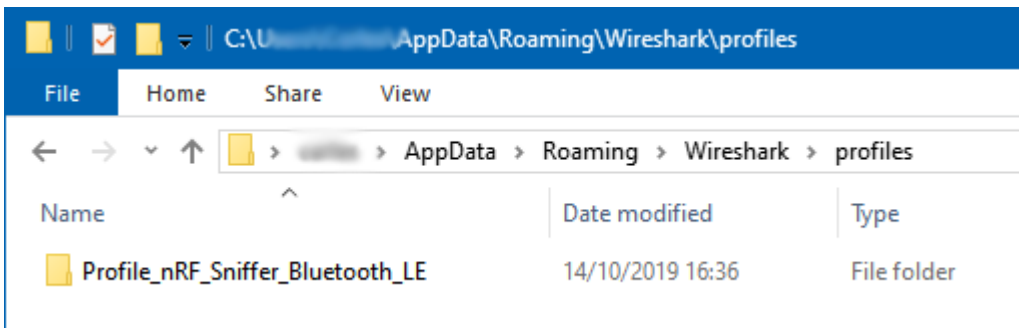
You can add a profile in Wireshark for displaying the data recorded by the nRF Sniffer for Bluetooth LE in a convenient way.

To add the nRF Sniffer profile in Wireshark, complete the following steps:

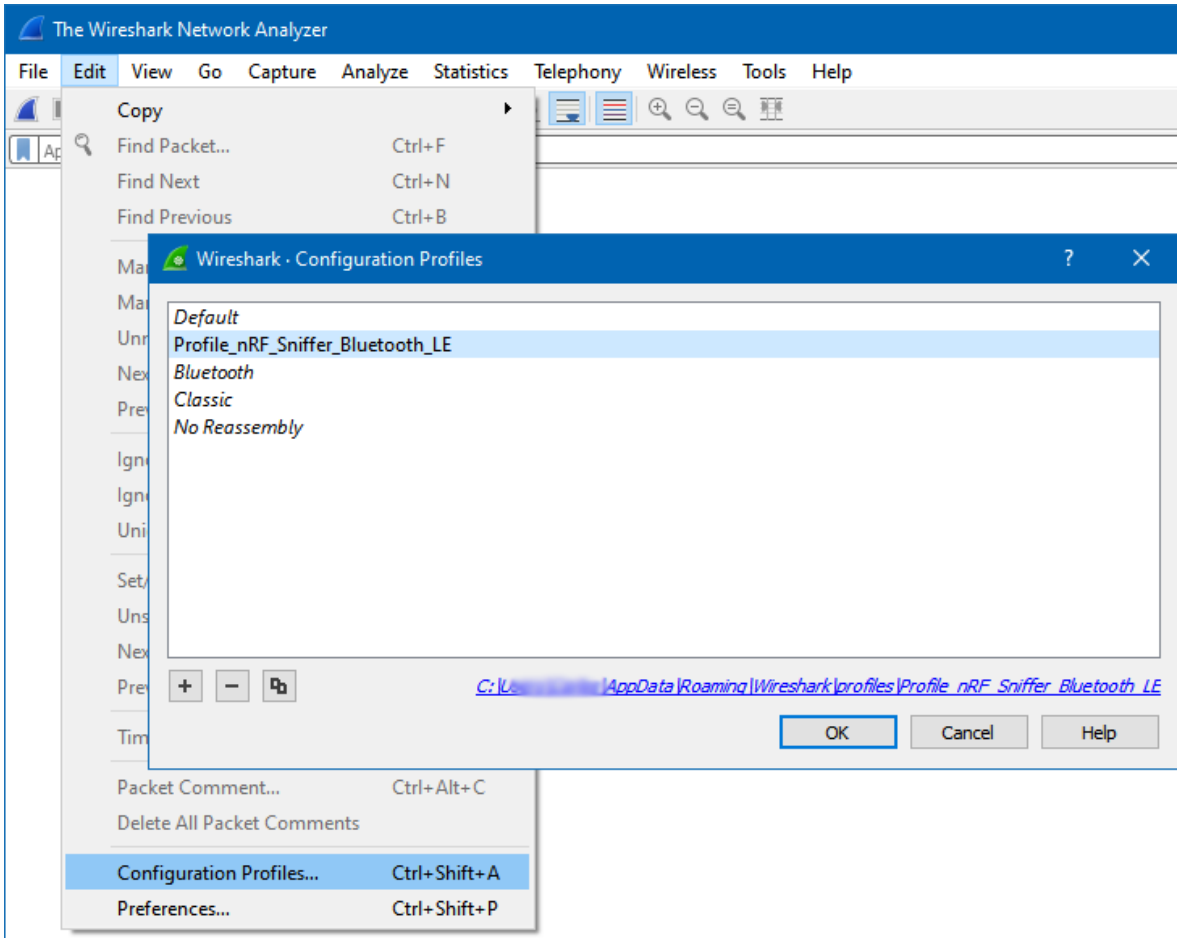
1. Go to **Help** > **About Wireshark** (on Windows or Linux) or **Wireshark** > **About Wireshark** (on macOS).
2. Select the **Folders** tab.
3. Double-click the location for the **Personal configuration** to open this folder.



4. Copy the profile folder *`Sniffer_Software`*`/Profile_nRF_Sniffer_Bluetooth_LE` into the `profiles` subfolder of this folder.



5. In Wireshark, select **Edit** > **Configuration Profiles**.
6. Select **Profile_nRF_Sniffer_Bluetooth_LE** and click **OK**.



3 Running nRF Sniffer

To start sniffing, place the development kit 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 kit or dongle to your computer and turn it on. Then place it between the Central and Peripheral device that you want to sniff.

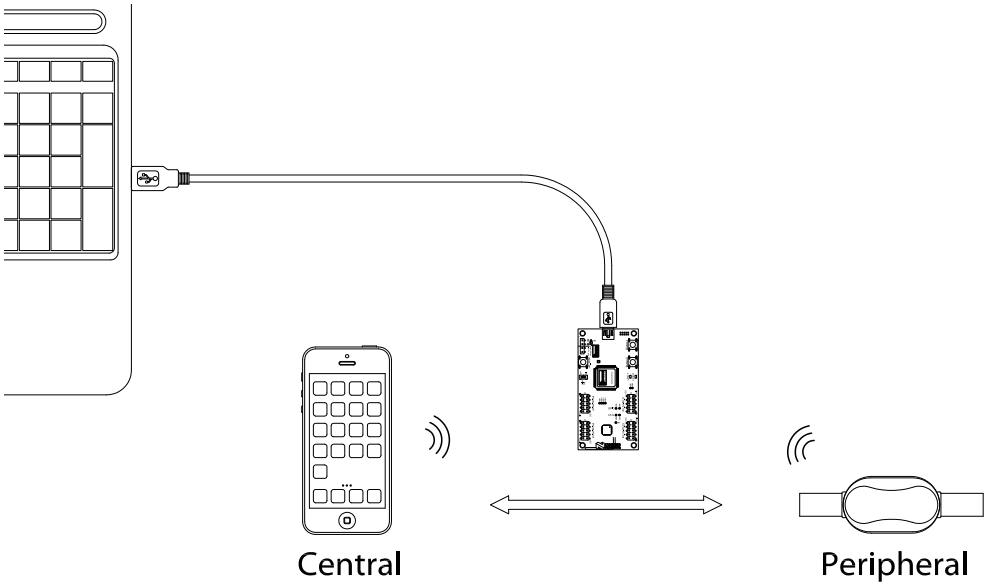


Figure 1: Hardware setup

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 Sniffer.

> **Note:** If the nRF Sniffer toolbar is not visible, select **View** > **Interface Toolbars** > **nRF Sniffer for Bluetooth LE**.

To start sniffing, double-click on the hardware interface (nRF Sniffer for Bluetooth LE COM18 in the following figure).

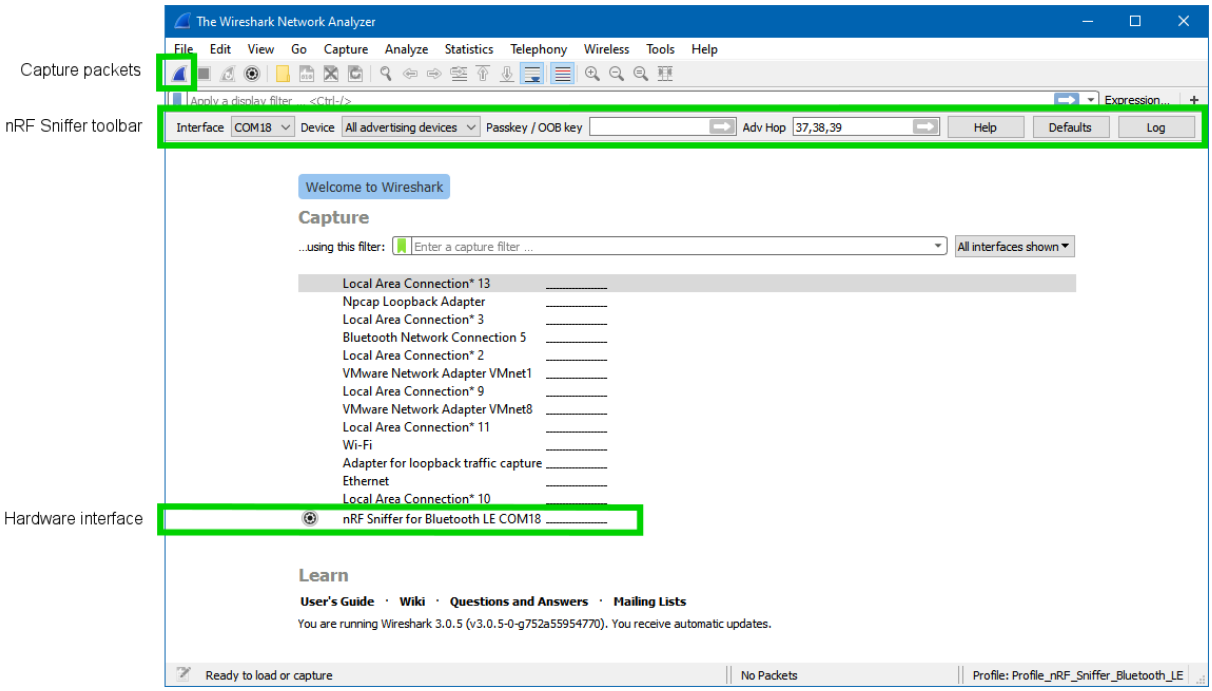


Figure 2: Wireshark capture screen

4 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.

> **Note:** The Sniffer may not pick up all connect requests and will not always pick up on a connection. In such cases, reconnect and try sniffing again. If you do not see any activity in your Wireshark console, see Troubleshooting on page 20.

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.

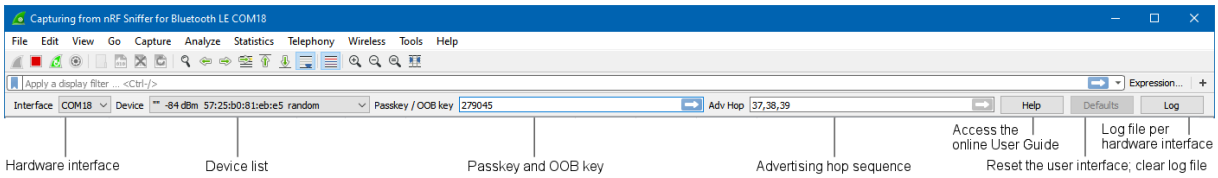


Figure 3: Sniffer software interface

Hardware interface

This list shows the available hardware interfaces. If you have more than one development kit or dongle 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 page 14.

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.

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.

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.

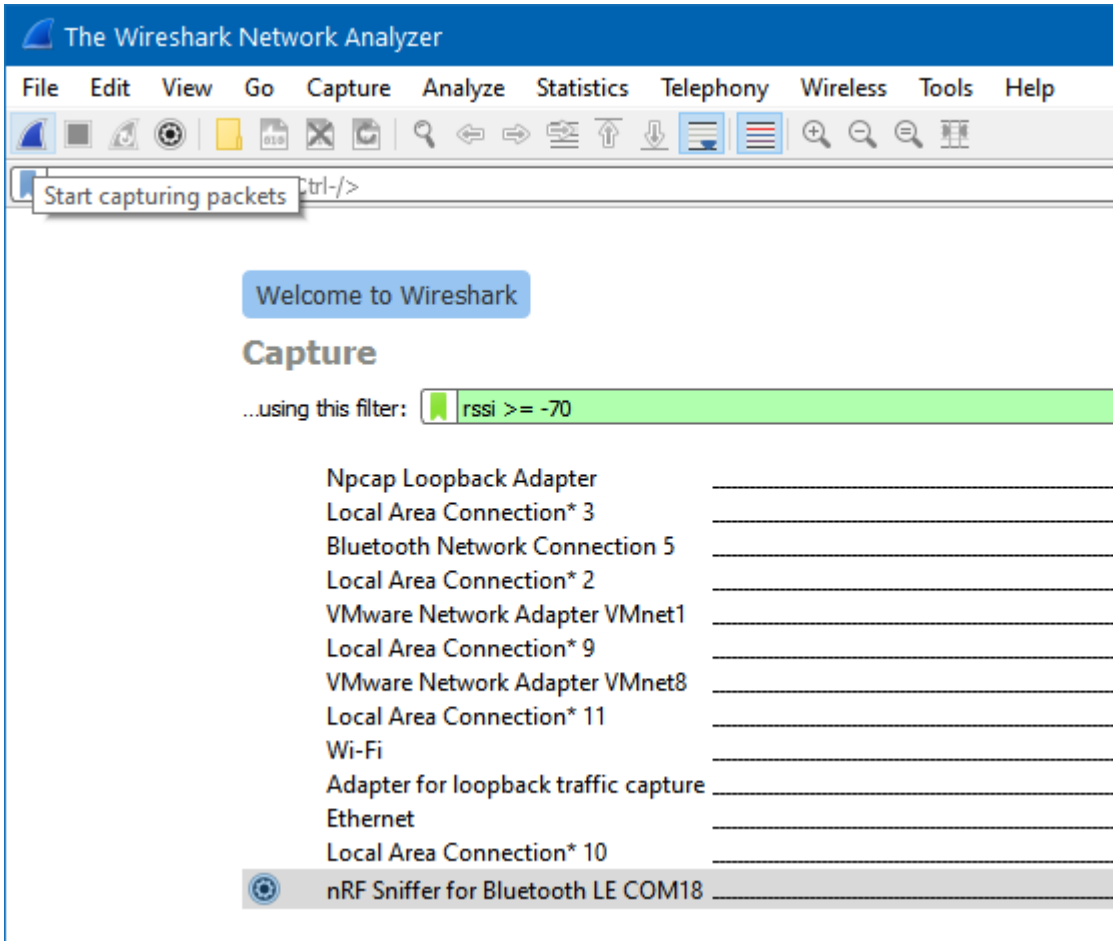


Figure 4: RSSI filter

4.1 Capturing from multiple hardware interfaces

You can capture packets from several hardware interfaces/devices simultaneously.

Note: On Windows, this feature is available in Wireshark v3.0.7 and v3.2.0 and later. If you are using an older version of Wireshark, you must run one instance of Wireshark for each Sniffer hardware attached to the computer. Select only one hardware interface in each of the Wireshark instances.

To capture from multiple hardware interface simultaneously, select the hardware interfaces in the capture screen and click **Start Capturing packets**.

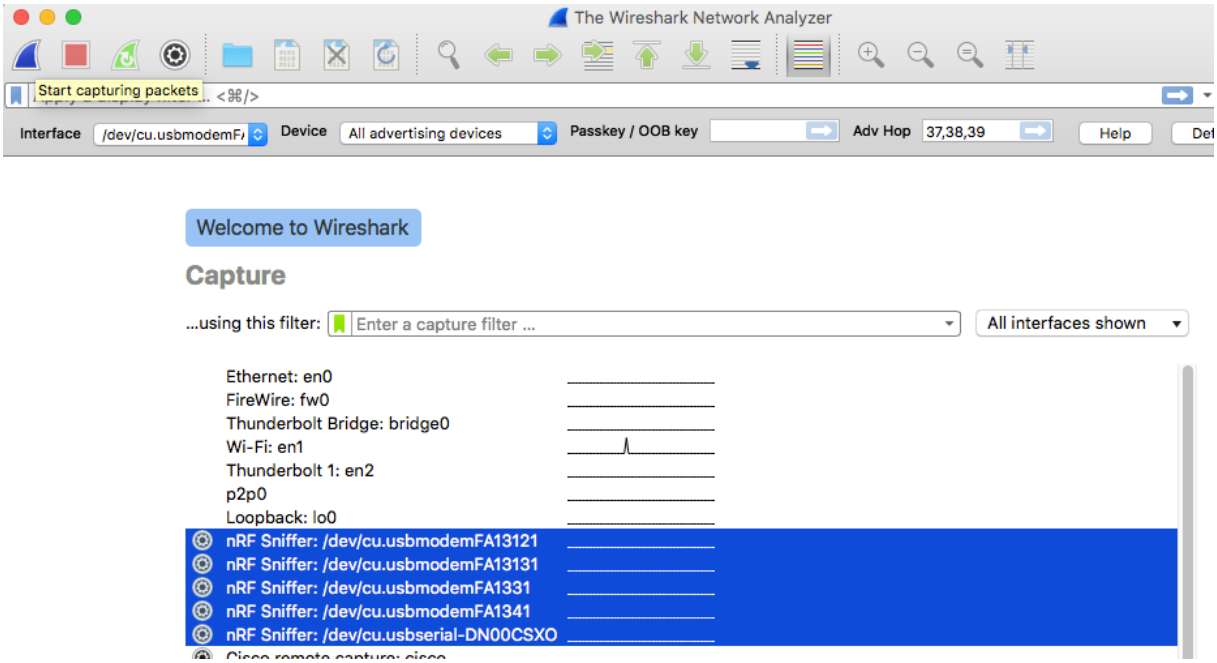


Figure 5: Select multiple hardware interfaces

The captured data contains the interface identifier used by Wireshark to identify the capture interface (frame.interface_id) and the hardware identifier for the development kit or dongle running the nRF Sniffer firmware (nordic_ble.board_id).

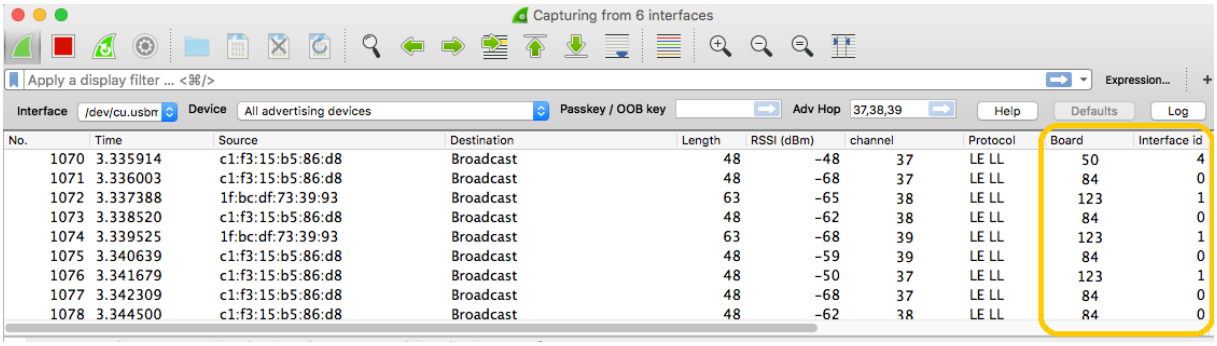


Figure 6: Data capture from multiple hardware interfaces

4.2 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.

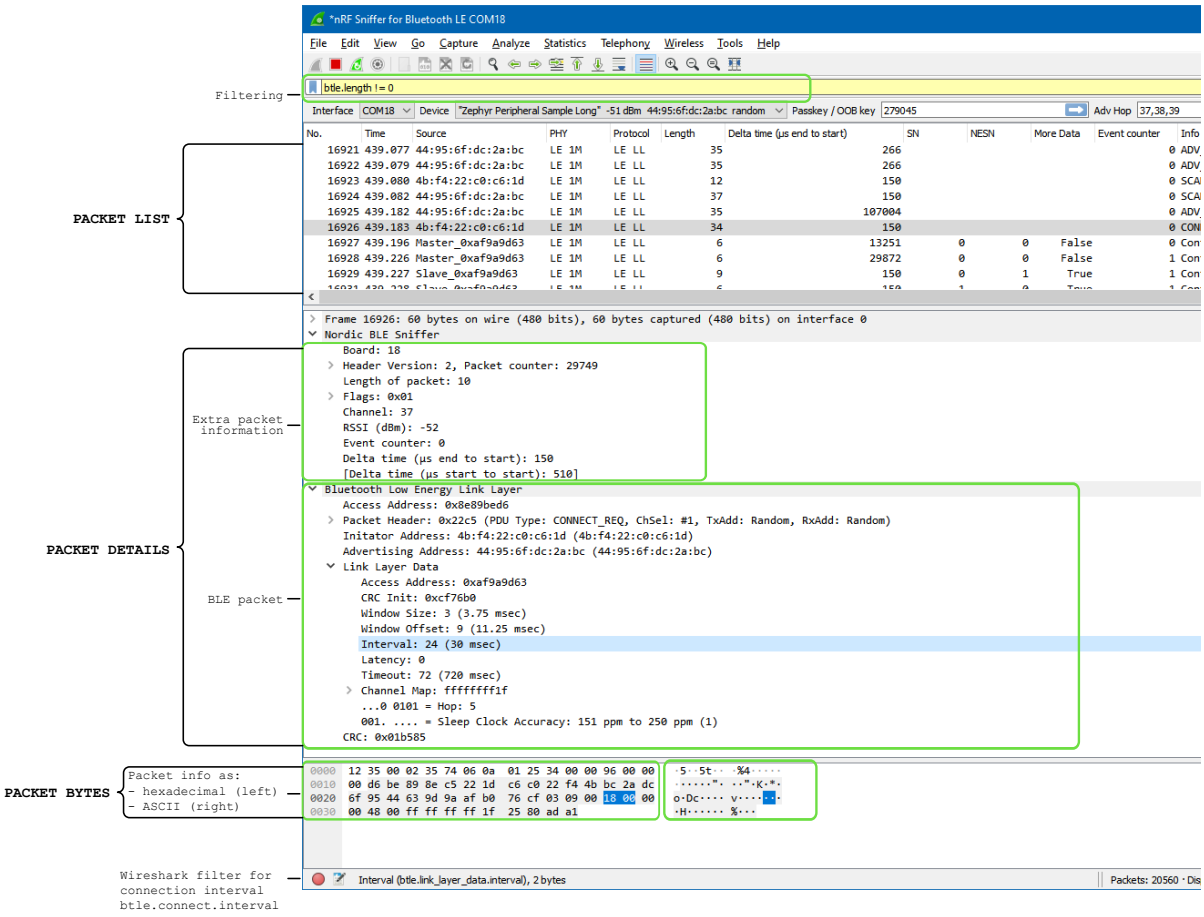


Figure 7: Wireshark interface

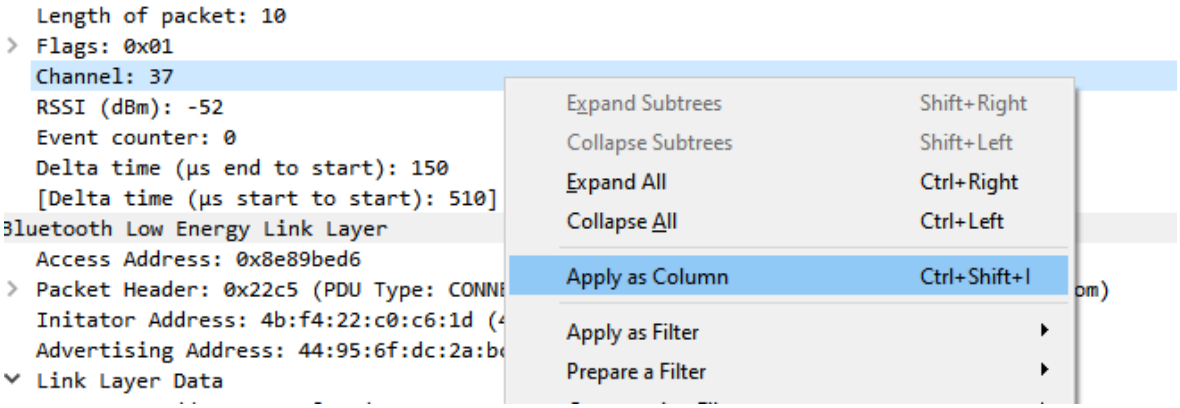
Use display filters to display a chosen packet subset. Most filters are based on the values of the packets, such as length or access address. The filter expressions use Boolean operators (`&&` `||` `==` `!=` `!`). To construct a filter, click **Expression** in the filtering bar. See the following table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

Table 2: Display filtering

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.

5 Common sniffing actions

The nRF Sniffer for Bluetooth LE can help you explore and debug Bluetooth Low Energy communication in a number of typical scenarios.

5.1 Sniffing advertisements from all nearby devices

Use nRF Sniffer for Bluetooth LE to see advertisements from all nearby devices.

1. Run nRF Sniffer (if not already running).
2. Ensure that **All advertising devices** is selected in the device list.

5.2 Sniffing advertisement packets involving a single slave device

Use nRF Sniffer for Bluetooth LE to see advertisement packets, scan requests, and scan responses to and from a single device.

1. Run nRF Sniffer (if not already running).
2. Select your device from the device list.

5.3 Sniffing a connection involving a single slave device

Use nRF Sniffer for Bluetooth LE to sniff a connection between a specific Peripheral device and a Central.

1. Run nRF Sniffer (if not already running).
2. Select your device from the device list.
3. Connect the Central to the Peripheral.

5.4 Sniffing a connection between paired devices

Use nRF Sniffer for Bluetooth to sniff a connection between devices that are already paired. The Sniffer must have sniffed the pairing procedure.

> **Note:** If the development kit or dongle running the nRF Sniffer firmware is reset, stored pairing information is lost.

1. Run nRF Sniffer (if not already running).
2. Select your device from the device list.
3. Enter the credentials for pairing. The procedure depends on the type of encryption.
   - For connections that use legacy pairing with Just Works:

     a. Initiate pairing between the devices if it does not happen automatically.

     No further action is required.
   - For connections that use legacy pairing with a passkey:

     a. Initiate pairing between the devices if it does not happen automatically.

   b. Type the 6-digit passkey that is displayed on either the Central or the Peripheral device into the **Passkey / OOB key** field in Wireshark.
   c. Press **Enter**.
   d. Enter the passkey into the other device.
- For connections that use legacy pairing with OOB:

   a. Before the devices initiate pairing, type the OOB key in big-endian, hexadecimal format with a leading "0x" into the **Passkey / OOB key** field in Wireshark.
   b. Press **Enter**.
   c. Connect the Central to the Peripheral device.
   d. Initiate pairing between the devices if it does not happen automatically.
- For connections that use LE Secure Connections:

   a. Enable Secure Connections debug mode on one or both of the devices.
   b. Initiate pairing between the devices if it does not happen automatically.

   In debug mode, the connection uses the debug keys specified in the Bluetooth Core Specification. The Sniffer uses the same keys to decrypt the encrypted packets.

6 Troubleshooting

If you have problems installing or using the nRF Sniffer for Bluetooth LE, see the following sections for troubleshooting information.

nRF Sniffer for Bluetooth LE is not listed in the Wireshark interface

Check that the hardware is set up correctly:

1. Ensure that the development kit or dongle has been enumerated on USB and that the drivers are loaded.
2. Ensure that the firmware HEX file has been programmed.
3. Reset the hardware by unplugging the hardware, waiting 5 seconds, and plugging it back in.

If these steps do not help, verify that you have installed the nRF Sniffer capture tool correctly and that the Python script located in the extcap folder can be run, as described in Installing the nRF Sniffer capture tool on page 7.

nRF Sniffer for Bluetooth LE does not show up as a toolbar

Make sure that you enabled the nRF Sniffer interface toolbar.

To do so, click **View** > **Interface Toolbars** > **nRF Sniffer for Bluetooth LE**.

nRF Sniffer for Bluetooth LE does not receive packets

When programming the Sniffer firmware, make sure to use the latest SEGGER J-Link software. If you used an older version, update your J-Link and program the firmware again.

nRF Sniffer for Bluetooth LE does not receive packets on Windows

On Windows, COM port numbers higher than 199 are not supported. If the COM port number is COM200 or higher, rename the COM port on Windows to a COM port number that is COM199 or lower. To do so, complete the following steps:

1. Open the Device Manager and click **Ports (COM & LPT)**.
2. Right-click on your COM port and click **Properties**.
3. In Properties, go to the **Port Settings** tab and click **Advanced**.
4. Change the COM port number by clicking the COM port number drop-down and selecting a COM port that is less than 200. Select a COM port number that is not in the list of devices currently attached to your computer. These are listed in the Device Manager under **Ports (COM & LPT)**.
5. Click **OK** and accept the changes when asked "Do you want to continue".

nRF Sniffer for Bluetooth LE occasionally works but appears unstable

Make sure that you are using the correct software versions as specified in the prerequisites and that you have installed the Python requirements.

When programming the Sniffer firmware, make sure to use the latest SEGGER J-Link software. If you used an older version, update your J-Link and program the firmware again.

If the problem persists, force J-Link to use flow control in the serial connection:

1. Open **`JLink.exe`** (Windows) or **`JLinkexe`** (macOS/Linux) in the installation folder of the required J-Link version.
2. Enter `sethwfc force`.
3. Exit the JLink software.

Packets are displayed incorrectly

Verify that the NORDIC_BLE protocol is enabled in Wireshark. To do so, click **Analyze** > **Enabled Protocols** and verify that the NORDIC_BLE protocol is selected.

Verify that a stable release of Wireshark is used. Development and user build versions are not supported. For example, v3.0.7 and v3.2.0 are stable versions of Wireshark, as indicated by the second number being an even number. Version 3.1.x is a development version of Wireshark, indicated by the second number being an odd number.

Legal notices

By using this documentation you agree to our terms and conditions of use. Nordic Semiconductor may change these terms and conditions at any time without notice.

Liability disclaimer

Nordic Semiconductor ASA reserves the right to make changes without further notice to the product to improve reliability, function, or design. Nordic Semiconductor ASA does not assume any liability arising out of the application or use of any product or circuits described herein.

Nordic Semiconductor ASA does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. If there are any discrepancies, ambiguities or conflicts in Nordic Semiconductor's documentation, the Product Specification prevails.

Nordic Semiconductor ASA reserves the right to make corrections, enhancements, and other changes to this document without notice.

Life support applications

Nordic Semiconductor products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury.

Nordic Semiconductor ASA customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nordic Semiconductor ASA for any damages resulting from such improper use or sale.

RoHS and REACH statement

Complete hazardous substance reports, material composition reports and latest version of Nordic's REACH statement can be found on our website www.nordicsemi.com.

Trademarks

All trademarks, service marks, trade names, product names, and logos appearing in this documentation are the property of their respective owners.

Copyright notice

COMPANY WITH
QUALITY SYSTEM
CERTIFIED BY DNV GL
= ISO 9001 =