nRF Sniffer

User Guide v2.0

1 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.

1.1 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)
- nRF52 Development Kit (PCA10040) and a micro USB cable

1.2 Required software

- nRF Sniffer software v2.x or later available on the Sniffer product page under the downloads tab
- Wireshark v2.4.2 or later available from http://www.wireshark.org/.
  Wireshark is a free software tool that captures wireless traffic and reproduces it in a readable format.
- An operating system that runs Wireshark v2.4.2 or later
  - Windows 7 or later
  - 64 bit OS X 10.6 or later
  - Linux (check for version compatibility)
- Segger J-Link v6.16c (which comes bundled with the nRF Sniffer v2.x software) available from https://www.segger.com
- python v2.7.x available from https://www.python.org/downloads/
- pyserial v3.4 or later available from https://github.com/pyserial/pyserial

1.3 Writing conventions

This user guide follows a set of typographic rules that makes the document consistent and easy to read. The following writing conventions are used:

- Commands are written in `Lucida Console`.
- Pin names are written in **`Consolas`.**
- File names and User Interface components are written in **bold**.
- Internal cross references are italicized and written in ***semi-bold.***

2 Setting up the nRF Sniffer

Set up the Sniffer for the first time by performing the following steps:

1. Install the software listed in ***Section 1.2 "Required software"*** on page 2 before plugging in the hardware.
2. Connect the hardware to a USB port.
3. For Windows - Wait for the hardware drivers to be loaded before continuing. You can also click **Skip obtaining driver software from Windows Update** to speed up the driver installation process.
4. Place the hardware between the Peripheral and Central device. Now you're ready to set up the software.

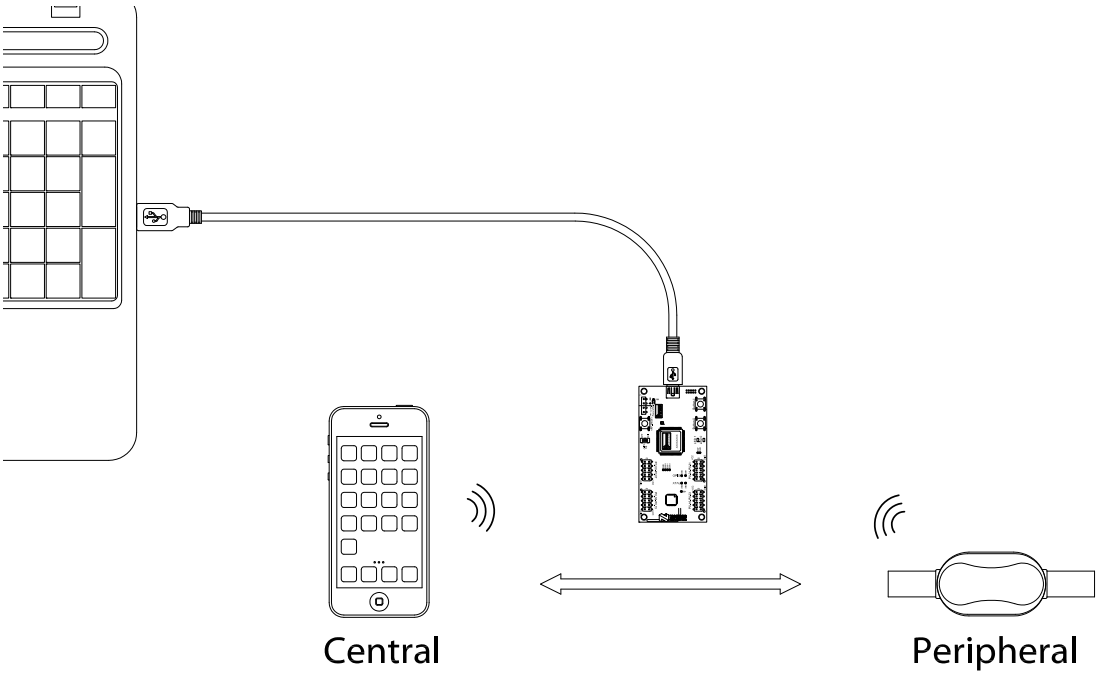
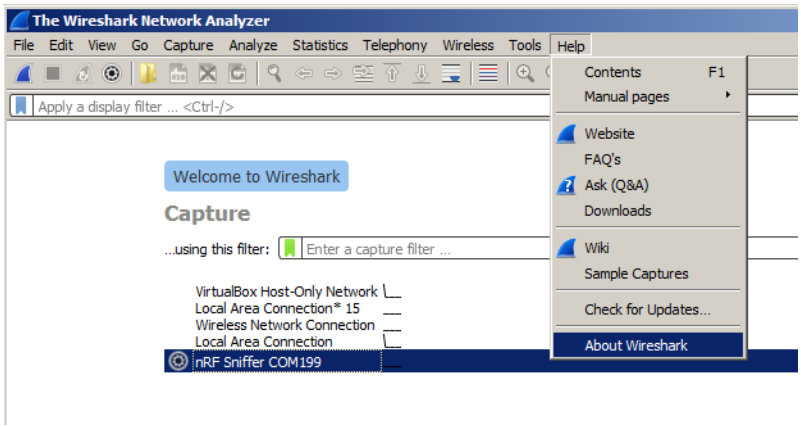


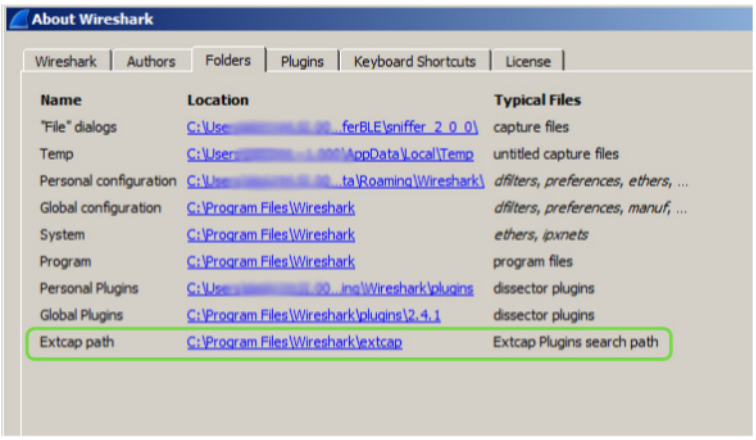
Figure 1 *System overview*

Install nRF Sniffer

1. For Windows - Go to **Help > About Wireshark**.



2. Click on the **Folders** tab.
3. Click on the location for **Extcap path**.
4. Find and copy the **nrf_sniffer_<version>_<hash>** ZIP file to the folder associated with "Extcap path".



5. Unzip the ZIP's extcap content to the Wireshark Extcap path found in "About Wireshark" (shown here as **C:\Program Files\Wireshark\extcap**).
6. For Windows - Verify that python is callable from the command line.

```
==
    C:>python --version
    Python 2.7.x
==
```

7. For OS X and Linux - Verify that the **nrf_sniffer.py** file has the "x" permission. If the "x" permission is missing add it using `chmod +x nrf_sniffer.py`.
8. Close Wireshark.

Install firmware with SEGGER J-Link.

1. Locate the J-Link software.
   - Windows - Use the **jlink.exe** program, usually in **C:\Program Files (x86)\SEGGER**.
   - OS X and Linux - Use the **jlinkexe** program.
2. Remove all hardware attached to the USB. Plug in one of the hardware boards and wait for the drivers to install.
3. Open a command window.
4. In the command window, type **jlink.exe** (for Windows) or **jlinkexe** (for OS X and Linux) and hit **Enter** to run the program.
5. Erase the contents by performing the following steps. Press **Enter** after each command.
   a. Type **erase**.
   b. Depending on the board you are using, type **nRF51422_XXAC** (for the nRF 51DK and Dongle) or **nRF52832_XXAA** (for the nRF52 DK).
   c. Type **s** to specify the SWD interface.
   d. For Speed, type **1000**.
   e. Type **loadfile** then **<Path to Wireshark>\extcap\nrf_sniffer_<version>_<hash>\hex\sniffer_<board name>_<hash>.hex**
   f. Type **r** to reset the board.
   g. Type **g** to run the board firmware.

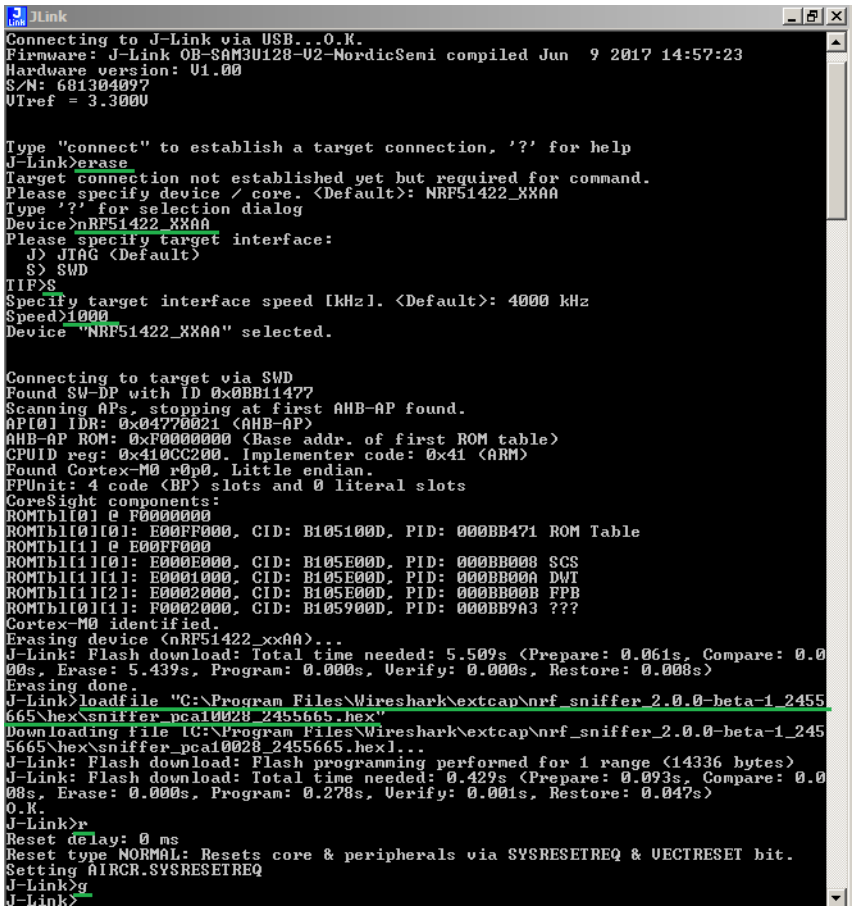
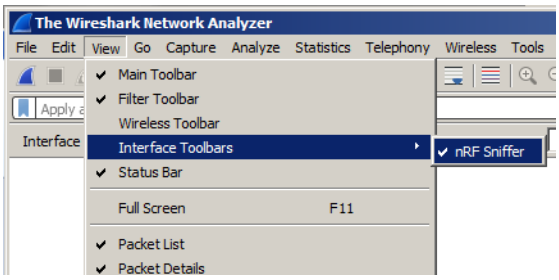


Figure 2 *J-Link erase*

Finalize the set up

1. Verify that the Sniffer firmware is running correctly by checking that **LED1** toggles each time a packet is received. At least one device must be advertising for the Sniffer to detect the advertisements.
2. Open Wireshark. You should see "nRF Sniffer on xxxxx" as one of the interfaces.
3. Click **View>Interface Toolbars>nRF Sniffer** to enable the Sniffer interface.



4. Click on the board to select it and then click the Wireshark icon to start capturing packets.

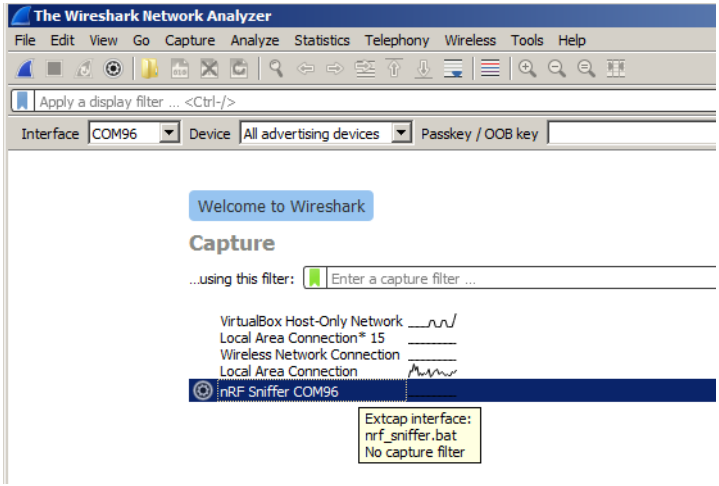


Figure 3 *Initial view - successful installation*

3 Using the Sniffer

The Wireshark capture screen is displayed when Wireshark is first launched. It includes the Wireshark interface for managing packets that are captured, the nRF Sniffer toolbar, and the hardware interfaces connected to the nRF Sniffer.

To make the nRF Sniffer toolbar visible, click **View>Interface Toolbars>nRF Sniffer**.

There are two ways to start sniffing:

- Double click on the hardware interface (nRF Sniffer COM54 in ***Figure 4***).
- Select the hardware interface by clicking on it and then click the Wireshark icon on the top left to start sniffing.

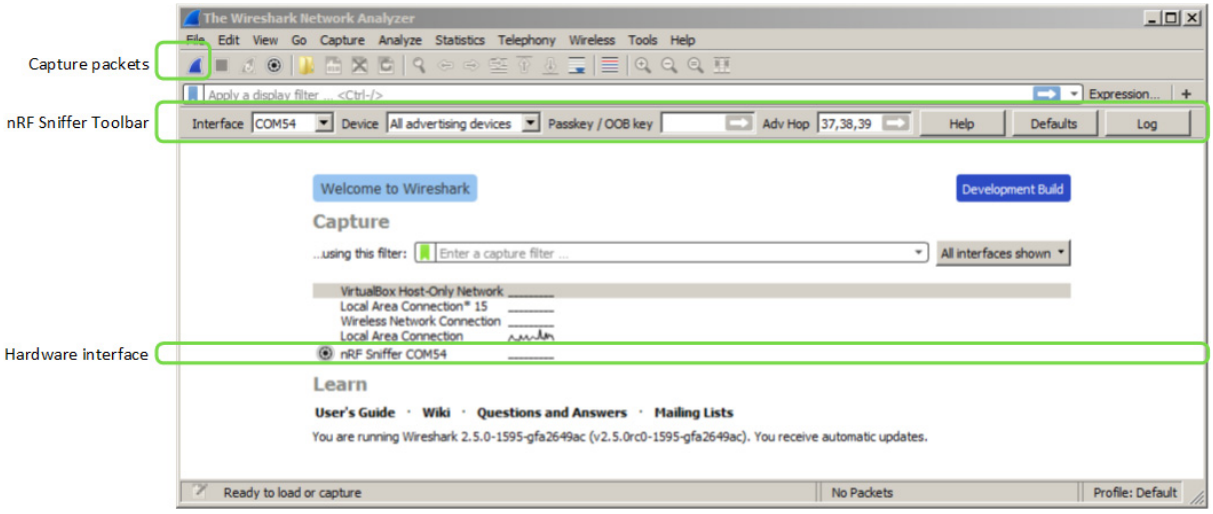


Figure 4 *Wireshark capture screen*

Once the Sniffer is running, it reports advertisements and lists nearby devices in the Device List. The Sniffer may not pick up all connect requests and will not always pick up on a connection. In such cases, you need to reconnect and try sniffing again. If you aren't seeing any activity in your Wireshark console, see ***Section 6 "Troubleshooting"*** on page 15.

The Sniffer has two modes of operation:

1. Listens on all advertising channels to pick up as many packets as possible from as many devices as possible. This is the default mode.
2. Follows one particular device and tries 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

3.1 Sniffer commands

The software interface has several commands to for controlling the Sniffer. Below you will find a list of commands and their description, along with some examples.

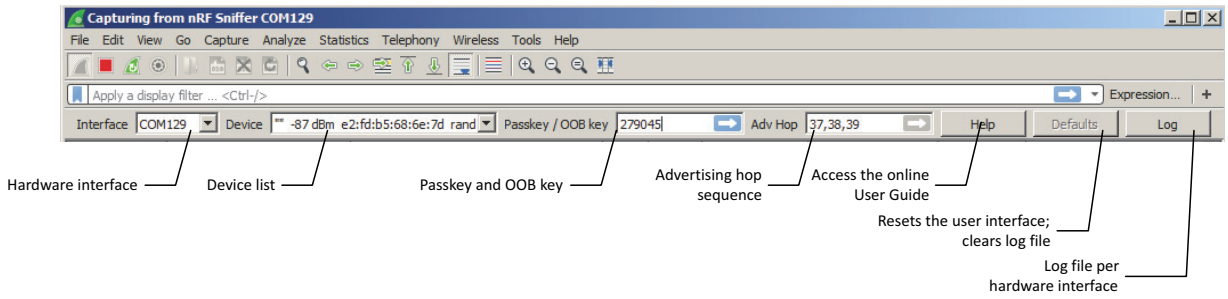


Figure 5 *Sniffer interface*

All advertising devices

Lists nearby devices. If this command is used while sniffing a device, it will stop sniffing that device. This means if the device is in a connection, the sniffer will lose that connection. To enable this option, click the **Device** list drop-down and select **All advertising devices**.

Passkey

Your device asks you to provide your passkey. Type the 6 digit passkey in the passkey text field from Wireshark, followed by **Enter**. Then enter the passkey into the device. Passkey entry utilizes Just Works pairing, which is described in detail in ***"Just Works - sniffing an encrypted connection"*** on page 13.

Out of band key exchange (OOB)

You are asked to provide the 16 byte Out-of-band (OOB) key in hexadecimal (starting with 0x, big endian format). This must be carried out 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, which is described in detail in ***"Sniffing a connection between devices that are already paired"*** on page 14.

Advertising hop sequence

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.

This will sniff waiting 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

Applies an RSSI filter on the packets being received. Only packets that match the filter are displayed. To set the capture filter in the Capture screen in Wireshark use the keyword "rssi".

Example: rssi > -70. This will only display packets that have an RSSI greater than -70 dBm.

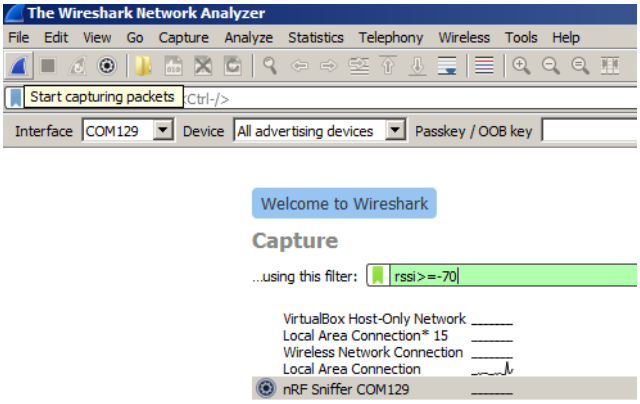


Figure 6 *RSSI filter*

Capturing from multiple hardware interfaces/boards

Select all hardware interfaces in the Capture Screen in Wireshark and click **Start Capturing Packets**.

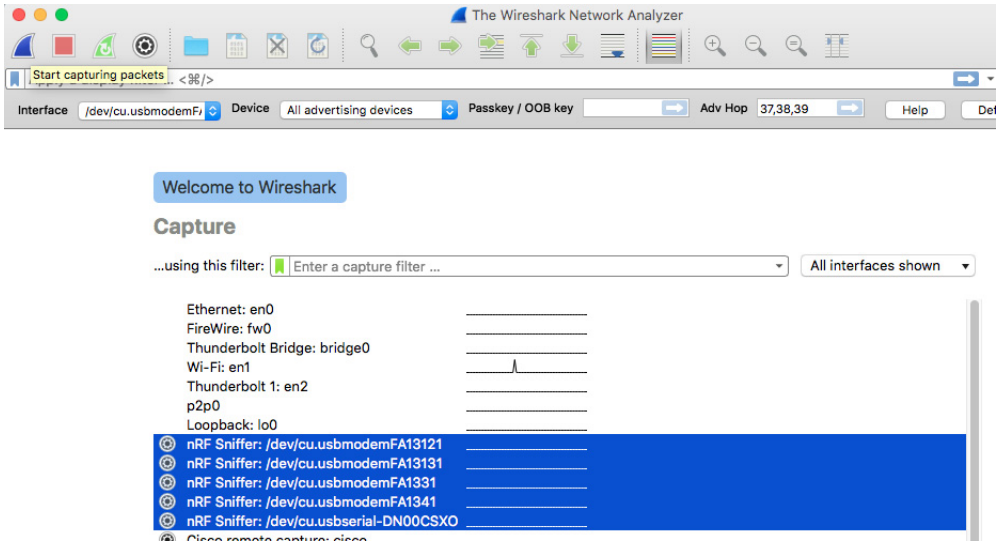


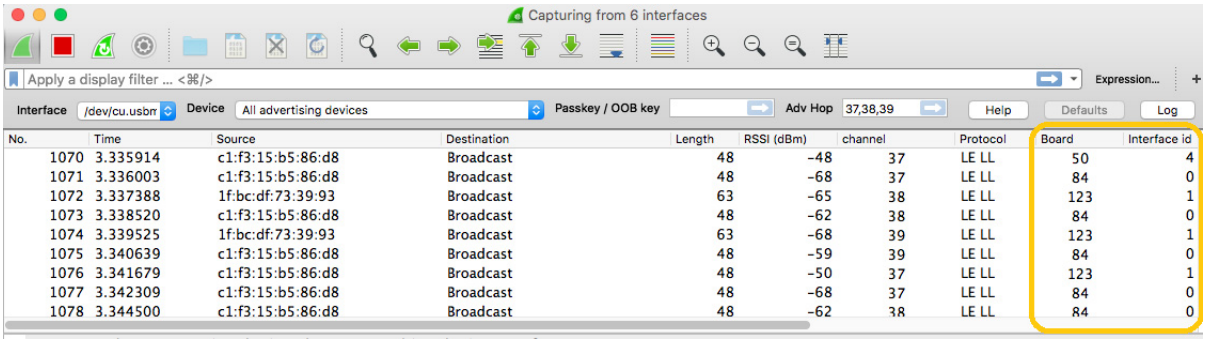
Figure 7 *Select multiple hardware interfaces*

Interface ID

Interface Identifier used by Wireshark to identify the capture interfaces (frame.interface_id)

Board

Hardware identifier for the board running the nRF Sniffer firmware (nordic_ble.board_id)



No.	Time	Source	Destination	Length	RSSI (dBm)	channel	Protocol	Board	Interface id
1070	3.335914	c1:f3:15:b5:86:d8	Broadcast	48	-48	37	LE LL	50	4
1071	3.336003	c1:f3:15:b5:86:d8	Broadcast	48	-68	37	LE LL	84	0
1072	3.337388	1f:bc:df:73:39:93	Broadcast	63	-65	38	LE LL	123	1
1073	3.338520	c1:f3:15:b5:86:d8	Broadcast	48	-62	38	LE LL	84	0
1074	3.339525	1f:bc:df:73:39:93	Broadcast	63	-68	39	LE LL	123	1
1075	3.340639	c1:f3:15:b5:86:d8	Broadcast	48	-59	39	LE LL	84	0
1076	3.341679	c1:f3:15:b5:86:d8	Broadcast	48	-50	37	LE LL	123	1
1077	3.342309	c1:f3:15:b5:86:d8	Broadcast	48	-68	37	LE LL	84	0
1078	3.344500	c1:f3:15:b5:86:d8	Broadcast	48	-62	38	LE LL	84	0

Figure 8 *Data capture from multiple hardware interfaces*

4 Using Wireshark

All BLE packets detected by the Sniffer are passed to Wireshark where they are wrapped in a header containing useful meta-information not present in the BLE packet itself. Wireshark dissects the packets and separates the actual packet from the meta-information.

Packet browsing

When a packet is selected in the Packet List, the Details pane shows the breakdown of that packet. The bytes of the packet are shown in the Bytes pane. Click a value in Details to highlight it among the bytes, or click on the bytes to highlight it in the Details.

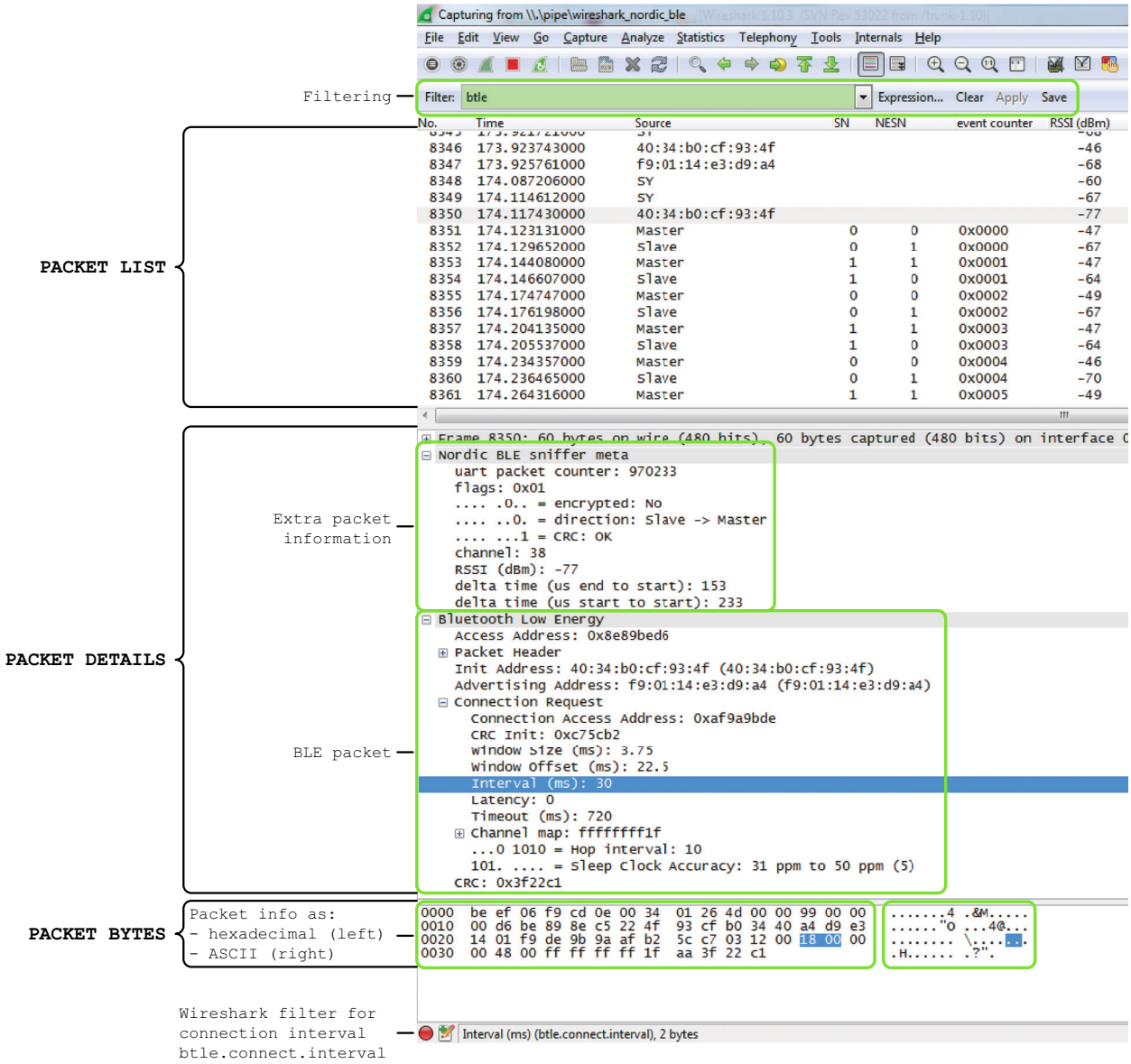


Figure 9 *Wireshark interface*

4.1 Display filtering

Display filters allow you 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 (&& || == != !). Some examples are given in ***Table 1***.

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

Table 1 *Display filtering*

4.1.1 Wireshark Tips

More information can be found in the documentation on Wireshark's website.

- For help with constructing filters, click **Expression**.
- Any field in the Packet Details pane can be made into a column by right clicking the value, and click **Apply as column**.

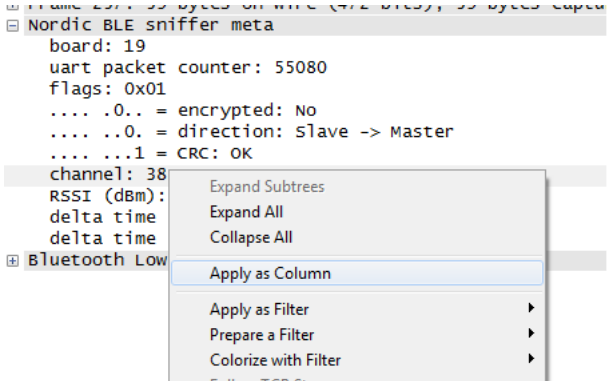


Figure 10 *Apply as column*

- You can apply a value as a filter. This can be useful if you want to see only operations affecting a particular handle, for example. To filter packets either having a specific value for some field, do as follows:
  - Right click the value in the packet details, click **Apply as Filter**, and click **Selected**.
- Saving a set of captured packets is useful if they need to be looked at later. To save a set of captured packets do the following:
  - Click the **Stop** button to quit capturing packets.
  - Click **File** and select **Save as** to save all packets. Click **File** and select **Export Specified Packets** to save a selection of packets.
- The Restart button is used to restart a capture and to clear the packet list.

5 Common sniffing actions

Sniffing advertisements from all nearby devices

To see advertisements from all nearby devices:

1. Start the nRF Sniffer.
2. Ensure "All advertising devices" is selected in the Device drop-down.

Sniffing advertisement packets involving a single slave device

To see advertisement packets, scan requests, and scan responses to and from a single device:

1. Start the Sniffer if not already running.
2. In the Sniffer, choose the device from the Device drop-down list.

Sniffing a connection involving a single slave device

To sniff a connection between a specific Peripheral device and a Central:

1. Start the Sniffer if not already running.
2. In the Sniffer, choose the device from the Device drop-down list.
3. Connect the Central to the Peripheral.

Just Works - sniffing an encrypted connection

To sniff a connection encrypted with Just Works:

1. Start the Sniffer if not already running.
2. In the Sniffer, choose the device from the Device drop-down list.
3. Initiate pairing between the devices if it does not happen automatically.The Sniffer will automatically decrypt encrypted packets.

Sniffing a connection between devices that are already paired

The Sniffer needs to have sniffed the pairing procedure if the devices are already paired. If the sniffer board is reset, stored pairing information will be lost.

To sniff a connection encrypted with passkey:

1. Start the Sniffer if not already running.
2. In the Sniffer, choose the device from the Device drop-down list.
3. Initiate pairing between the devices if it does not happen automatically. A passkey will be displayed on either the Central or the Peripheral device.
4. Type the 6 digit passkey from the passkey text field in Wireshark.
5. Press **Enter**.
6. Enter the passkey into the other device after entering it into the Sniffer.

To sniff a connection encrypted with OOB:

1. Start the Sniffer if not already running.
2. In the Sniffer, choose the device from the Device drop-down list.
3. Enter the OOB key into the Sniffer before the devices initiate pairing.
    - Type the OOB key in big-endian, hexadecimal format with a leading "0x".
    - Press **Enter**.
4. Connect the Central to the Peripheral device.
5. Initiate pairing between the devices if it does not happen automatically.

6 Troubleshooting

The nRF sniffer is not listed in the Wireshark interface.

1. See if the hardware has been enumerated on USB and the drivers are loaded.
2. Check that the HEX file for the hardware has been flashed.
3. Reset the hardware by unplugging the hardware, waiting 5 seconds, and plugging it back in.

If it still doesn't appear, verify the python script located in the extcap folder is able to run.

For Windows:

1. Run `nrf_sniffer.bat --extcap-interfaces` to list the interface.
2. If this exits with a python error, verify that **python.exe** can be run from the command line `c:>python.exe --version`, where the Python version is the same as ***Section 1.2 "Required software"*** on page 2.

For OS X and Linux:

1. Verify that the execute permission is present for the nrf_sniffer.py file.
   - `ls -l nrf_sniffer.py`
2. If the "x" permission is missing:
   - `chmod +x nrf_sniffer.py`
3. Run `nrf_sniffer.py --extcap-interfaces` to list the interface.

I cannot see the extcap folder in Wireshark.

1. Create the extcap folder as described in ***"Install nRF Sniffer"*** on page 4.

nRF Sniffer occasionally works and appears unstable.

Make sure you are using the correct software versions as stated in ***Section 1.2 "Required software"*** on page 2.

Verify that the J-Link emulator version on the hardware is as stated in ***Section 1.2 "Required software"*** on page 2. To verify:

1. Open the JLinkConfig.exe in the install folder of the required J-Link version.
2. The host firmware and the emulator firmware should have the same date.

Upgrade the J-Link emulator version on the hardware.

1. Download the J-Link software as mentioned in ***Section 1.2 "Required software"*** on page 2.
2. Unplug the hardware, wait 5 seconds.
3. Plug in the hardware.
4. For Windows:
   - Run **jlink.exe** from the folder where the J-Link software was installed.
   - A popup appears "A new firmware version is available.....Do you want to upgrade ...?"
   - Click **yes**.
5. OS X/Linux
   - Type "jlinkexe". The J-Link firmware updates automatically.

Downgrade the J-Link emulator version on the hardware.

For Windows:

1. Ensure only one J-Link is connected to your computer.
2. Run **jlink.exe** from the folder where the J-Link version was installed.
3. In jlink type “exec invalidatefw”.
4. Click **yes** when prompted.
5. In jlink type “exit” to exit jlink.exe.
6. Run **jlink.exe** from the folder where the J-Link version was installed (it is necessary to run it a second time).
7. Click **yes** to upgrade your firmware.
8. You have now successfully downgraded the J-Link version on the emulator.

For OS X and Linux:

1. Ensure only one J-Link is connected to your computer.
2. Run **jlink.exe** from the folder where the J-Link version was installed. (Install the older version of J-Link if required.)
3. Run jlinkexe.
4. In jlinkexe type "exec invalidatefw".
5. In jlinkexe type "exit" to exit the jlinkexe.
6. Run jlinkexe (this is required to be run for the second time). The J-Link firmware will be updated automatically to the installed version of J-Link.

“nRF Sniffer on xxxxx” doesn’t show up as one of the interfaces when I open Wireshark.

1. Click **View** in the Wireshark toolbar.
2. Select **Interface Toolbars** then click **nRF Sniffer**.

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.

Life support applications

Nordic Semiconductor's 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.

Contact details

For your nearest distributor, please visit http://www.nordicsemi.com.
Information regarding product updates, downloads, and technical support can be accessed through your My Page account on our homepage.

Main office:
Otto Nielsens veg 12
7052 Trondheim
Norway
Phone: +47 72 89 89 00
Fax: +47 72 89 89 89

Mailing address:
Nordic Semiconductor
P.O. Box 2336
7004 Trondheim
Norway

Revision History

Date	Version	Description
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 the ***Section 1.1 "Required hardware"*** on page 2 • ***Section 1.2 "Required software"*** on page 2 • ***Section 2 "Setting up the nRF Sniffer"*** on page 3
March 2017	1.3	**Updated content:** • ***Section 1.1 "Required hardware"*** on page 2 • ***Section 1.2 "Required software"*** on page 2 • ***Chapter 2 "Setting up the nRF Sniffer"*** on page 3
July 2014	1.2	**Updated content:** • ***Section 1.1 "Required hardware"*** on page 2 • ***Section 1.2 "Required software"*** on page 2 • ***Chapter 2 "Setting up the nRF Sniffer"*** on page 3 • ***Section 2.1 "Running the Sniffer"*** on page 6 • ***Chapter 3 "Using the Sniffer"*** on page 7 • ***Chapter 4 "Using Wireshark"*** on page 11 • ***Section 4.1.1 "Wireshark Tips"*** on page 12 • ***Chapter 6 "Troubleshooting"*** on page 15
April 2014	1.1	Updated firmware, now supports all versions of PCA10000 and PCA10001.
December 2013	1.0	First release.