



nRF Sniffer

User Guide v1.2

1 Overview

The nRF *Bluetooth*® Smart Sniffer is a tool for debugging *Bluetooth* low energy (BLE) applications, picking up (sniffs) every packet between a selected device and the device it is communicating with, even when the link is encrypted. When developing a BLE solution 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 pieces of hardware:

- nRF51822 Evaluation Kit (PCA10001) and a mini USB cable
- nRF51422 Evaluation Kit (PCA10003) v3.0.0 or later and a mini USB cable
- nRF51422 Development Kit (PCA10028) v1.0 or later and a mini USB cable
- nRF51822 Development Kit dongle (PCA10000)

1.2 Required software

- Windows 7 or later.
- nRFgo Studio.
- nRF tools downloaded from www.nordicsemi.com.
- **ble-sniffer-<os>-<version>.exe** and Sniffer plugins and firmware found in **ble-sniffer_<os>_<version>_Sniffer.zip** in the installer folder.
- Stable release of Wireshark v1.10.1 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.

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 Nordic *Bluetooth* Sniffer

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

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

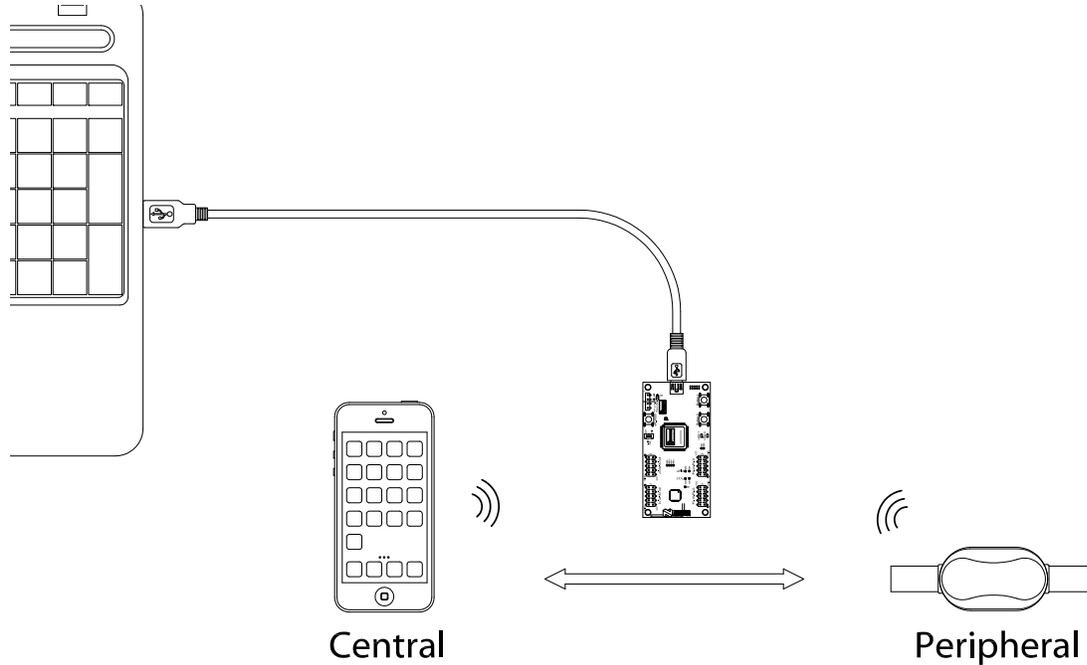


Figure 1 System overview

5. Download and install Wireshark to the default directory.
6. Unzip **ble-sniffer_<os>_<version>_Sniffer.zip**.
7. Open nRFgo Studio.
8. In the Device Manager pane on the left, select the hardware to use as a sniffer. It is identified by its SEGGER serial number.
9. Click **Erase all**.
10. Select the **Program Application** tab.
11. Click **Browse** and select **ble-sniffer_nRF51822_<xxx>_sniffer.hex** located in the **Firmware** folder.
12. Click **Program**.
13. Verify that the sniffer firmware is running correctly (PCA10001 and PCA10003 only) by checking that **LED1** toggles each time a packet is received. Make sure that at least one device is advertising for the sniffer to catch the advertisements.

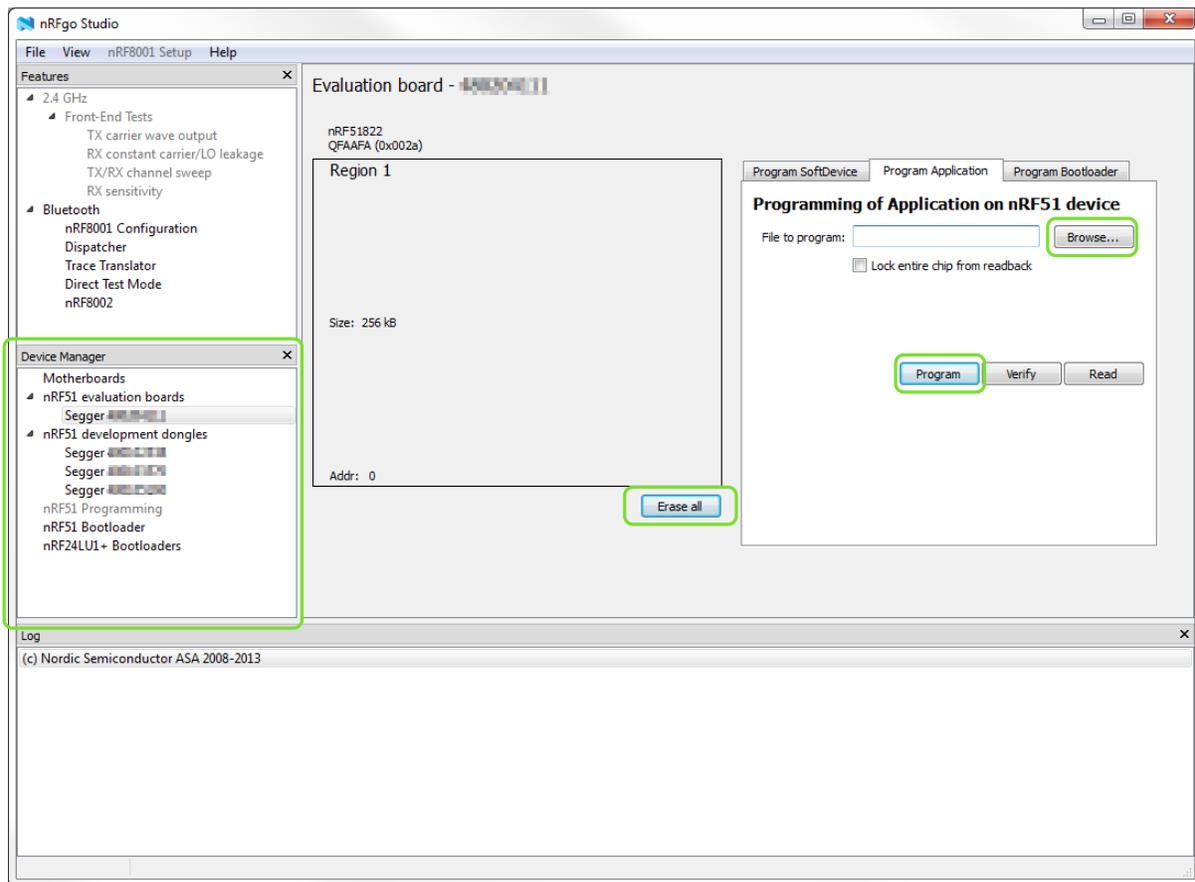


Figure 2 Programming the firmware

To upgrade the Sniffer to a new release of the Sniffer firmware, do the steps 7 to 12. Optionally you can use the Ctrl-R option in the Sniffer console to flash the new release of the Sniffer firmware.

2.1 Running the Sniffer

The Sniffer program reports advertisements and lists nearby devices.

Note: Do not remove **ble-sniffer-<os>-<version>.exe** from the sniffer folder. It does not run without the other files.

Once you have the Sniffer program running, the software should automatically find the hardware and start reporting advertisements and listing nearby devices. If things aren't working as they should, reset the hardware and refresh the device list by typing **l** or restart the Sniffer program.

Note: The Sniffer may not manage to pick up all connect requests and will not always pick up on a connection. In such cases, you need to reconnect.

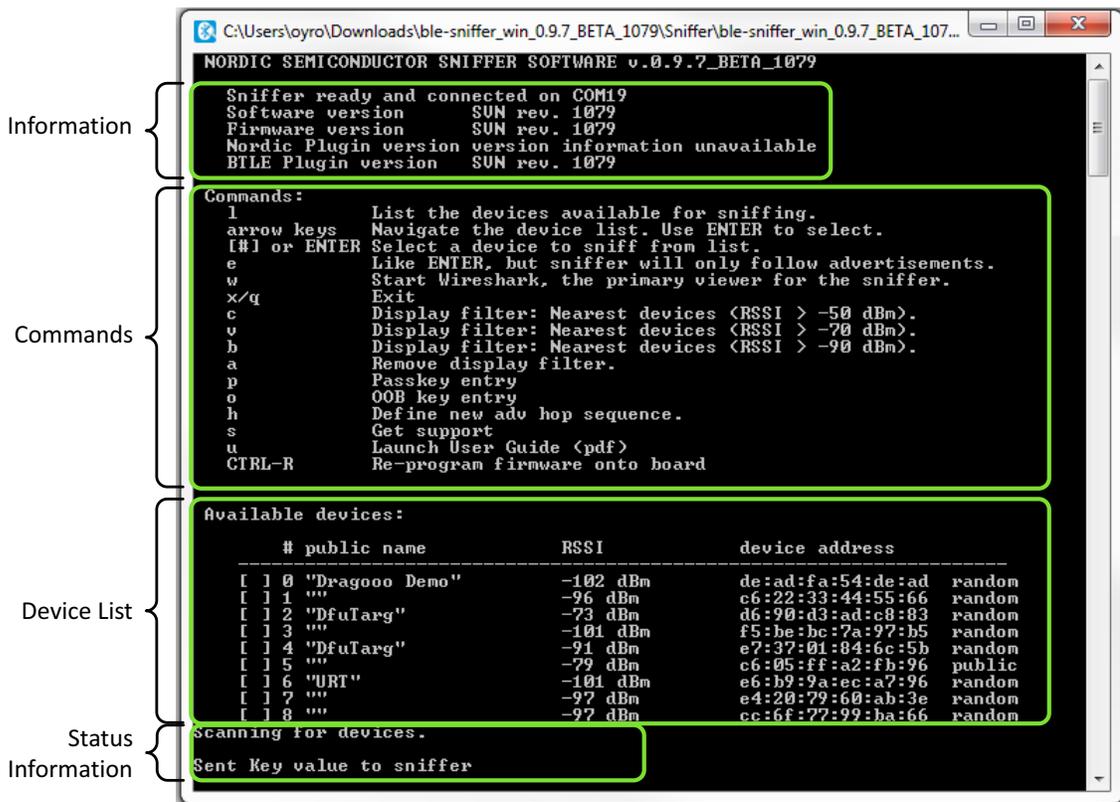


Figure 3 Sniffer commands

3 Using the Sniffer

The Sniffer has two modes of operation:

1. Listens on all advertising channels to try to pick up as many packets as possible from as many devices as possible.
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, and all packets in the Connection sent between the two devices in the Connection.

The Sniffer always starts in the first mode, showing information for all devices it receives packets from in the Device List, as shown in **Figure 3** on page 6. From this list, you can choose one particular device to sniff, and by that change the mode of the sniffer. As shown in **Table 1** on page 7, this is done by using either the arrow keys and pressing enter or pressing a number from 0-9. You can at any time return to mode 1 by pressing 1.

Keyboard commands

The keyboard commands listed in **Table 1** are used to control the sniffer.

Keyboard command	Description
1	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.
Arrow keys + Enter Numbers 0-9	Selects the device to sniff. While sniffing a device, the device list in the console application will not be updated.
e	Like ENTER, but the sniffer will not follow the device into a connection, it will only report advertisement packets.
w	Starts Wireshark with the settings necessary to immediately view incoming packets. If Wireshark is started manually, the correct capture interface must be chosen and filters need to be applied manually. Will copy the required plugins when run for the first time. Requires administrator rights when copying. Administrator rights will be automatically requested.
x/q	Exit.
c/v/b	Apply a RSSI filter on the device list. Show only devices with an RSSI greater than -50/-70/-90 dBm respectively.
a	Remove RSSI filter.
p	You are asked to provide your passkey. Type the 6 digit passkey followed by Enter .
o	You are asked to provide the 16 byte Out-of-band (OOB) key in hexadecimal, 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 zero-padded in front.
h	Change the order in which the sniffer switches advertising channels when following a device. Define the order by typing 7 for channel 37, 8 for 38 and 9 for 39. Press ENTER when done.
s	Opens online support with detailed help instructions. Here you can report a bug or a problem with the sniffer, or a problem seen on-air with a Nordic Semiconductor device.
u	Launch User Guide in pdf format.
CTRL-r	Re-program Sniffer firmware.

Table 1 Description of controls

4 Using Wireshark

Start Wireshark by pressing **w** inside the Sniffer application. At this point you will be prompted for administrator rights if this is the first time you run the **w** command on this version of the Sniffer. This is so the Sniffer can install the Wireshark plugins necessary to decode its packets.

Note: Wireshark must be started via the **w** command to view sniffed packets without manual setup.

All BLE packets detected by the Sniffer are passed to Wireshark and are wrapped in a header which contains 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 dissection 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.

The screenshot shows the Wireshark interface with the following components:

- Filtering:** Filter: `btle`
- PACKET LIST:** A table of captured packets. Packet 8350 is selected.

No.	Time	Source	SN	NESN	event counter	RSSI (dBm)
8346	173.923743000	40:34:b0:cf:93:4f				-46
8347	173.925761000	f9:01:14:e3:d9:a4				-68
8348	174.087206000	SY				-60
8349	174.114612000	SY				-67
8350	174.117430000	40:34:b0:cf:93:4f				-77
8351	174.123131000	Master	0	0	0x0000	-47
8352	174.129652000	Slave	0	1	0x0000	-67
8353	174.144080000	Master	1	1	0x0001	-47
8354	174.146607000	Slave	1	0	0x0001	-64
8355	174.174747000	Master	0	0	0x0002	-49
8356	174.176198000	Slave	0	1	0x0002	-67
8357	174.204135000	Master	1	1	0x0003	-47
8358	174.205537000	Slave	1	0	0x0003	-64
8359	174.234357000	Master	0	0	0x0004	-46
8360	174.236465000	Slave	0	1	0x0004	-70
8361	174.264316000	Master	1	1	0x0005	-49
- PACKET DETAILS:**
 - Extra packet information:**
 - Nordic BLE sniffer meta
 - uart packet counter: 970233
 - flags: 0x01
 -0.. = encrypted: No
 -0. = direction: slave -> Master
 -1 = CRC: OK
 - channel: 38
 - RSSI (dBm): -77
 - delta time (us end to start): 153
 - delta time (us start to start): 233
 - BLE packet:**
 - Bluetooth Low Energy
 - Access Address: 0x8e89bed6
 - Packet Header
 - Init Address: 40:34:b0:cf:93:4f (40:34:b0:cf:93:4f)
 - Advertising Address: f9:01:14:e3:d9:a4 (f9:01:14:e3:d9:a4)
 - Connection Request
 - Connection Access Address: 0xaf9a9bde
 - CRC Init: 0xc75cb2
 - Window size (ms): 3.75
 - Window offset (ms): 22.5
 - Interval (ms): 30**
 - Latency: 0
 - Timeout (ms): 720
 - Channel map: ffffffff1f
 - ...0 1010 = Hop interval: 10
 - 101. = Sleep Clock Accuracy: 31 ppm to 50 ppm (5)
 - CRC: 0x3f22c1
- PACKET BYTES:**
 - Packet info as:
 - hexadecimal (left)
 - ASCII (right)
 - 0000 be ef 06 f9 cd 0e 00 34 01 26 4d 00 00 99 00 004 .&M....
 - 0010 00 d6 be 89 8e c5 22 4f 93 cf b0 34 40 a4 d9 e3 "O" .4@...
 - 0020 14 01 f9 de 9b 9a af b2 5c c7 03 12 00 18 00 00 \..@. .
 - 0030 00 48 00 ff ff ff ff 1f aa 3f 22 c1 .H..... .?..
- Wireshark filter for connection interval:** `btle.connect.interval`

Figure 4 Wireshark interface

4.1 Display filtering

Display filters allow you to display a chosen subset of the packets. 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 2*.

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.adv_addr	Displays only packets that have an advertising address, that is, only advertising packets.
(btle.length != 0) && (!btle.adv_addr btle.connect)	A useful filter that will remove all empty data packets, and all advertisement packets except connect requests.
btle	A protocol filter that displays all <i>Bluetooth</i> low energy packets.
btatt, btsmp, btl2cap	Protocol filters for ATT, SMP, and L2CAP packets respectively.

Table 2 Display filtering

4.1.1 Wireshark Tips

More information can be found on Wireshark's [website](#) by clicking **Get Help** and selecting **Documentation**.

- To get help with constructing filters, click **Expression**.
- Any field in the Packet Details pane can be made into a column: Right click the value, and click **Apply as column**.

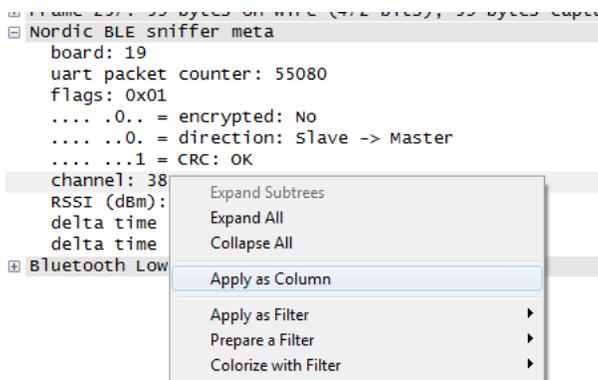


Figure 5 Apply as column

- 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.

- All captured packets are stored in **%APPDATA%\Nordic Semiconductor\Sniffer\logs\capture.pcap**.
 - **%APPDATA%** resolves to **C:\Users\[username]\AppData\Roaming**.
- Anytime a new filter is applied, the list is automatically scrolled to the packet that is selected.
- You can decide how packets are colored based on display filters. To change this go to **View** and select **Coloring Rules**.

5 Common sniffing actions

Sniffing advertisements from all nearby devices

To see advertisements from all nearby devices:

1. Start the Sniffer.
2. Press **w** to run Wireshark.

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. Press **w** to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device 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. Press **w** to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. 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. Press **w** to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Initiate pairing between the devices if it does not happen automatically. The Sniffer will automatically decrypt encrypted packets.

To sniff a connection between devices that are already paired, the Sniffer needs to have sniffed the pairing procedure. If the sniffer board is reset, stored pairing information will be lost.

Passkey - sniffing an encrypted connection

To sniff a connection encrypted with passkey:

1. Start the Sniffer if not already running.
2. Press **w** to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Initiate pairing between the devices if it does not happen automatically. A passkey will be displayed on either the Central or the Peripheral.
5. Enter the passkey into the Sniffer command by pressing **p** and typing the passkey digits as they are displayed.
6. Press **Enter**.
7. Enter the passkey into the other device after having entered it into the Sniffer command.

OOB - sniffing an encrypted connection

To sniff a connection encrypted with OOB:

1. Start the Sniffer if not already running.
2. Press **w** to run Wireshark if it's not already running.
3. In the Sniffer program, choose the device from the device list.
4. Enter the OOB key into the Sniffer command before the devices initiate pairing.
 - Press **o**.
 - Type the OOB key in big-endian, hexadecimal format. Leading zero-bytes may be omitted.
 - Press **Enter**.
5. Connect the Central to the Peripheral.
6. Initiate pairing between the devices if it does not happen automatically.

6 Troubleshooting

The Sniffer is connected to the computer and it says “Finding Sniffer Dongle” but it is taking a while to find the dongle.

1. Make sure that you have flashed the Sniffer firmware to the Sniffer hardware.
2. Make sure no other program is using the Sniffer serial port, including other instances of the Sniffer software.
3. Unplug the board and wait 5 seconds.
4. Plug it back in.

If it still can't find the Sniffer dongle you might have to specify the Sniffer's COM port number.

1. To find the COM port number in the Windows Device Manager, click **Start**, select **Run**, and then type **devmgmt.msc**.
2. The COM port number is located in the **Ports (COM & LPT)** menu.
3. Open the Sniffer folder and then open **sniffer.cfg** in a text editor like Notepad.
4. Set the **comPort** property to the COM port number used for the dongle. For example, **comPort=54** if the dongle is on COM54.

Wireshark does not recognize `btle` or `nordic_ble`, and the Sniffer program cannot find version information for the plugins.

Run the Sniffer as Administrator. This should install the plugin automatically.

If you are running the Sniffer program manually:

1. Copy **btle.dll** and **nordic_ble.dll** from the Sniffer directory to **<Wireshark installation>\plugins\<version>**.
2. Use the files in **...\plugins[Wireshark major version]\windows\x64** if your Wireshark version is 64 bit, or the files in **...\plugins[Wireshark major version]\windows\x86** if Wireshark is 32 bit.

Opening Wireshark with the `w` command does not work. How can I open Wireshark manually?

1. Run the Sniffer.
2. Open Wireshark.
3. Click **Interface List**, then click **Options, Manage Interfaces**, and select **New**.
4. In the **Pipe** field type **\\.\pipe\wireshark_nordic_ble**. Click **Save** and close the configuration windows.
5. Apply the filter **btle** and click **Start**.

Packets are not being picked up by the sniffer.

The Sniffer board should be placed between the Central and Peripheral.

Wireshark is not able to display the sniffed packets.

The Sniffer will generate a Wireshark capture file (**%APPDATA%\Nordic Semiconductor\capture.pcap**) which can be viewed afterwards even if real time viewing is not used. Press **S** to view the folder with the file.

The Sniffer starts showing “Malformed packets” after a while when sniffing an encrypted link.

This is a known limitation with the Sniffer, which will be improved in future releases. See the release notes for details.

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
July 2014	1.2	Updated content: <ul style="list-style-type: none">• <i>Section 1.1 "Required hardware"</i> on page 2• <i>Section 1.2 "Required software"</i> on page 3• <i>Chapter 2 "Setting up the Nordic Bluetooth Sniffer"</i> on page 4• <i>Section 2.1 "Running the Sniffer"</i> on page 6• <i>Chapter 3 "Using the Sniffer"</i> on page 7• <i>Chapter 4 "Using Wireshark"</i> on page 8• <i>Section 4.1.1 "Wireshark Tips"</i> on page 10• <i>Chapter 6 "Troubleshooting"</i> on page 14
April 2014	1.1	Updated firmware, now supports all versions of PCA10000 and PCA10001.
December 2013	1.0	First release.