How to use Raytac’s MDBT50Q-CX-40 dongle as a BLE sniffer?

Introduction

Uncertainties in Bluetooth Application Development

Bluetooth’s growing popularity comes with challenges during development. Common issues include hardware instability, software incompatibilities, and environmental interference.
Accurate issue identification and resolution are keys to successful development.

Common Uncertainties

Unstable Connections: Disruptions from wireless signals or physical obstacles.
Pairing Failures: Devices unable to establish connections.
Data Errors: Packet loss or corruption during transmission.
Compatibility Problems: Protocol version mismatches affecting interoperability.

Efficient Bluetooth Issue Analysis

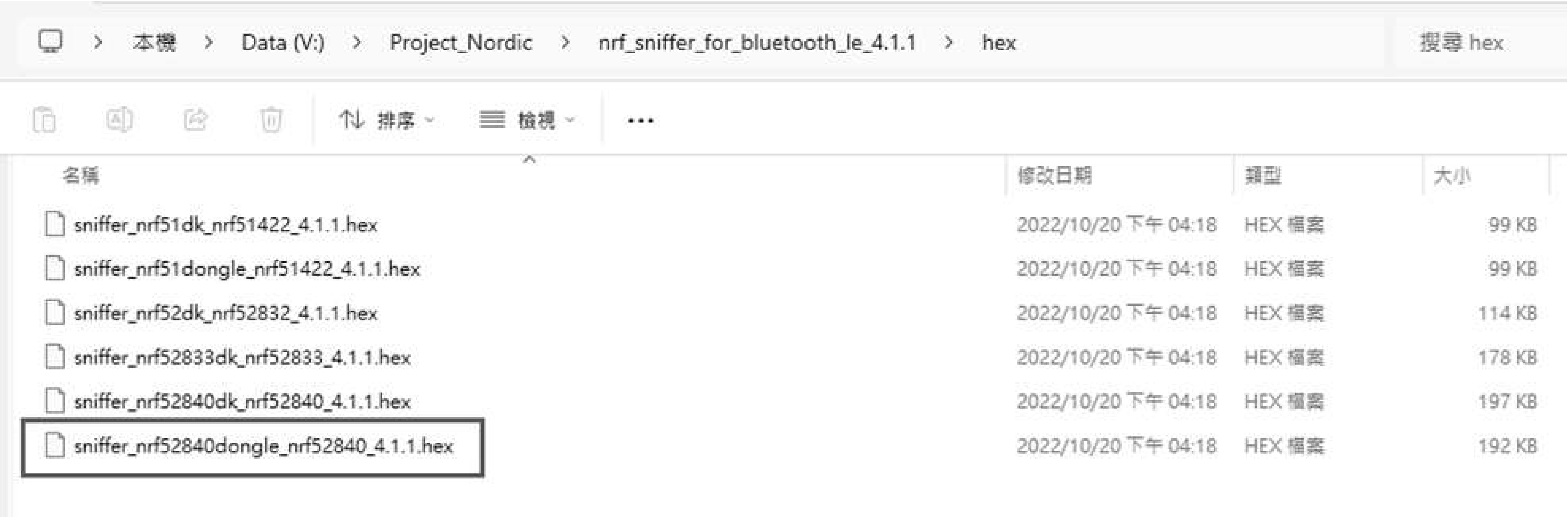
Challenges like transmission speed limitations, data loss, connection failures, or protocol violations can arise. As Bluetooth signals travel wirelessly, precise analysis requires specialized tools.
Nordic offers firmware integrated with Wireshark, flashable onto the Raytac MDBT50Q-CX-40 Dongle (https://www.raytac.com/product/ins.php?index_id=156), enabling engineers to capture and analyze Bluetooth broadcast signals via USB.
This setup streamlines issue identification and resolution.
Below’s how to configure the Dongle for Wireshark reception.

Flashing Firmware into MDBT50Q-CX-40

Step 1: Download and extract the **nRF Sniffer for Bluetooth LE** from Nordic:
https://www.nordicsemi.com/Products/Development-tools/nRF-Sniffer-for-Bluetooth-LE

(https://www.nordicsemi.com/Products/Development-tools/nRF-Sniffer-for-Bluetooth-LE)

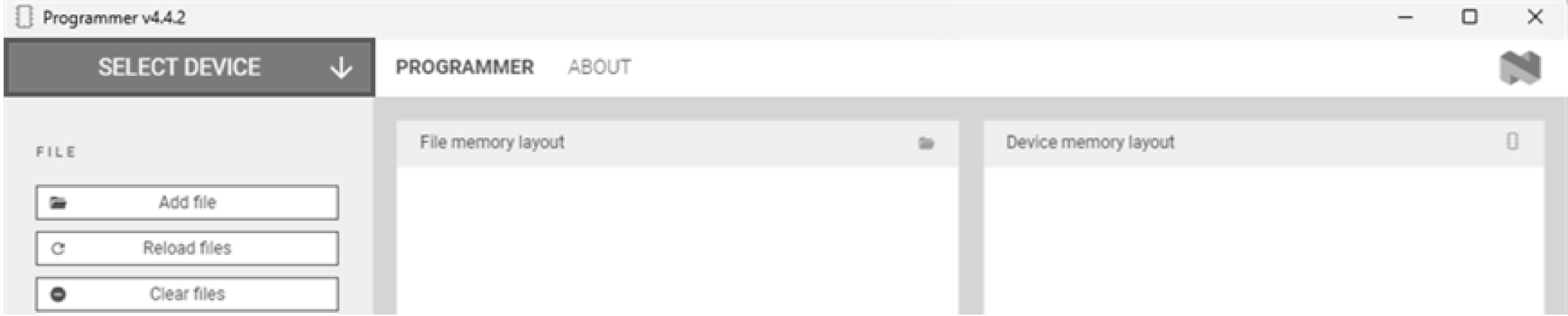
Step 2: Locate the file: *sniffer_nrf52840dongle_nrf52840_4.1.1.hex*
This is the firmware to flash into MDBT50Q-CX-40.


本機 > Data (V:) > Project_Nordic > nrf_sniffer_for_bluetooth_le_4.1.1 > hex
搜尋 hex
排序
檢視
...

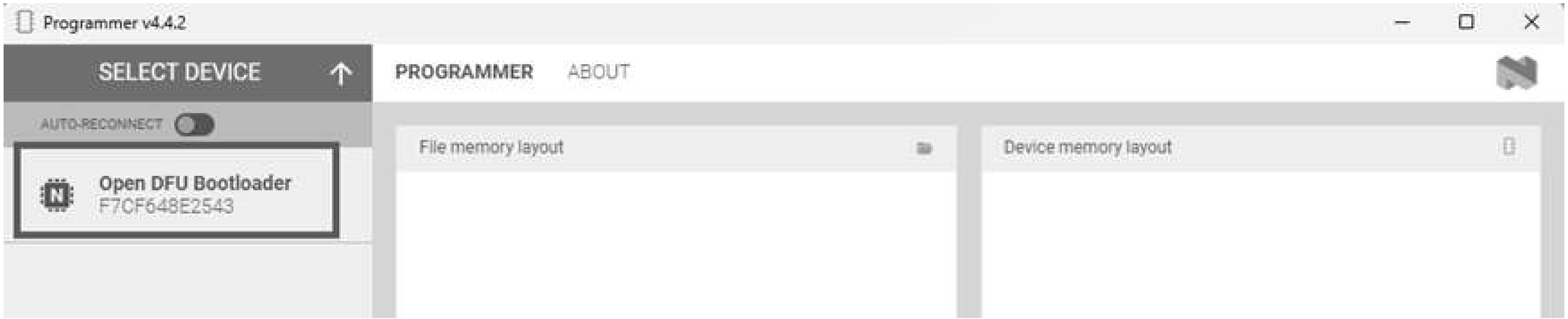
名稱	修改日期	類型	大小
sniffer_nrf51dk_nrf51422_4.1.1.hex	2022/10/20 下午 04:18	HEX 檔案	99 KB
sniffer_nrf51dongle_nrf51422_4.1.1.hex	2022/10/20 下午 04:18	HEX 檔案	99 KB
sniffer_nrf52dk_nrf52832_4.1.1.hex	2022/10/20 下午 04:18	HEX 檔案	114 KB
sniffer_nrf52833dk_nrf52833_4.1.1.hex	2022/10/20 下午 04:18	HEX 檔案	178 KB
sniffer_nrf52840dk_nrf52840_4.1.1.hex	2022/10/20 下午 04:18	HEX 檔案	197 KB
sniffer_nrf52840dongle_nrf52840_4.1.1.hex	2022/10/20 下午 04:18	HEX 檔案	192 KB

Step 3: Press and hold the button on MDBT50Q-CX-40 and plug it into a PC USB port.
Bootloader mode will be activated after the LED light is turned on.
Then flash the firmware using **nRF Programmer**.

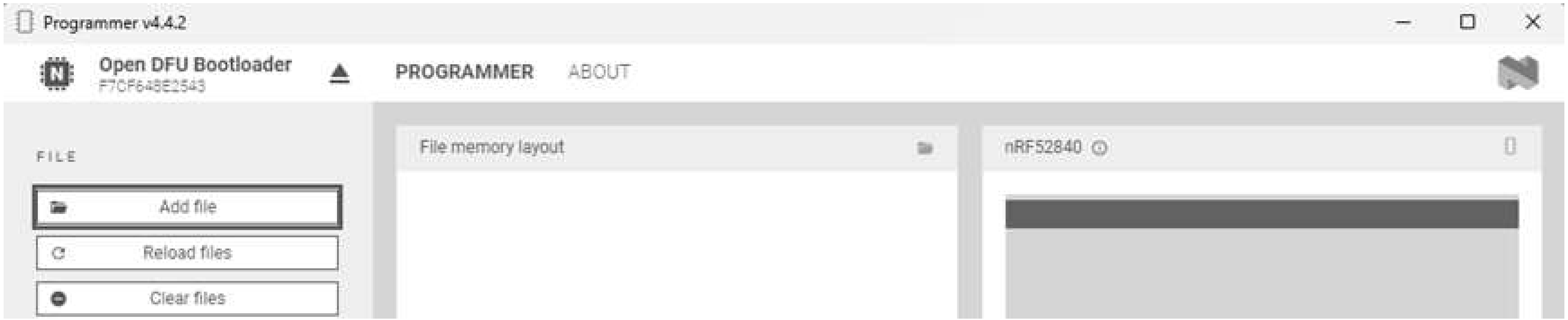
Step 4: Open the nRF Programmer and follow the below steps:
Select the Device:



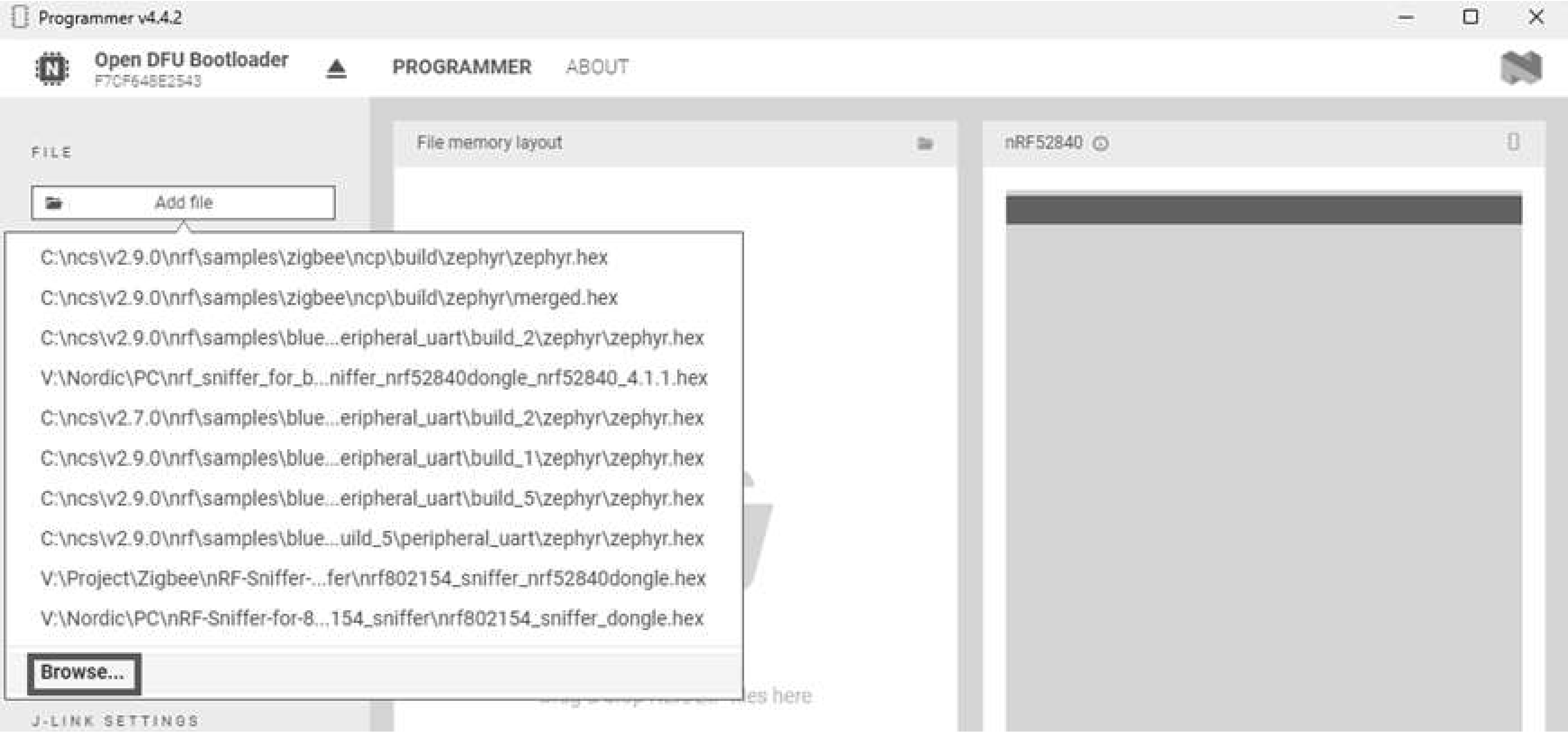
The device will appear as the name shown in below:



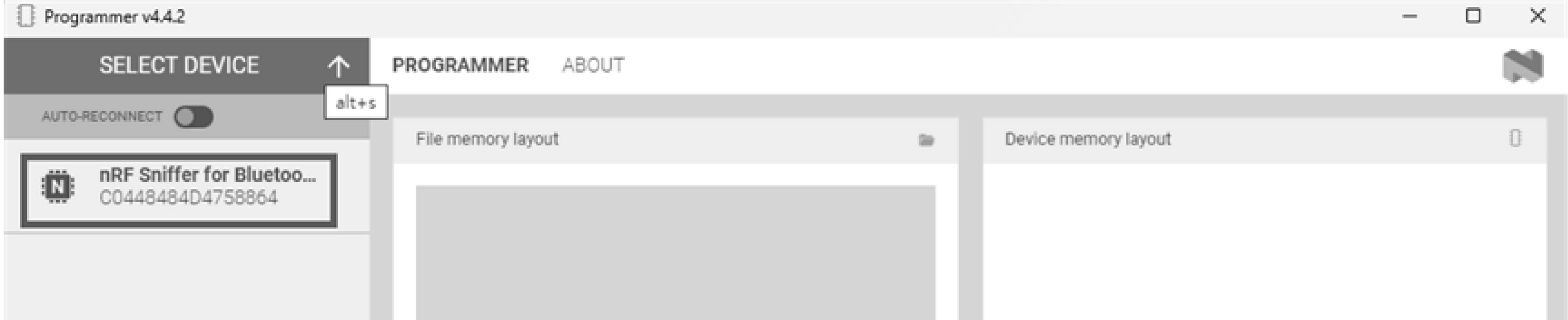
Add Firmware File:



Load *sniffer_nrf52840dongle_nrf52840_4.1.1.hex* into the Programmer:


Programmer v4.4.2
Open DFU Bootloader
F7CF648E2543
PROGRAMMER
ABOUT
FILE
Add file
File memory layout
nRF52840
C:\ncs\v2.9.0\nrf\samples\zigbee\ncp\build\zephyr\zephyr.hex
C:\ncs\v2.9.0\nrf\samples\zigbee\ncp\build\zephyr\merged.hex
C:\ncs\v2.9.0\nrf\samples\blue...eripheral_uart\build_2\zephyr\zephyr.hex
V:\Nordic\PC\nrf_sniffer_for_b...niffer_nrf52840dongle_nrf52840_4.1.1.hex
C:\ncs\v2.7.0\nrf\samples\blue...eripheral_uart\build_2\zephyr\zephyr.hex
C:\ncs\v2.9.0\nrf\samples\blue...eripheral_uart\build_1\zephyr\zephyr.hex
C:\ncs\v2.9.0\nrf\samples\blue...eripheral_uart\build_5\zephyr\zephyr.hex
C:\ncs\v2.9.0\nrf\samples\blue...uild_5\peripheral_uart\zephyr\zephyr.hex
V:\Project\Zigbee\nRF-Sniffer-...fer\nrf802154_sniffer_nrf52840dongle.hex
V:\Nordic\PC\nRF-Sniffer-for-8...154_sniffer\nrf802154_sniffer_dongle.hex
Browse...
...es here
J-LINK SETTINGS

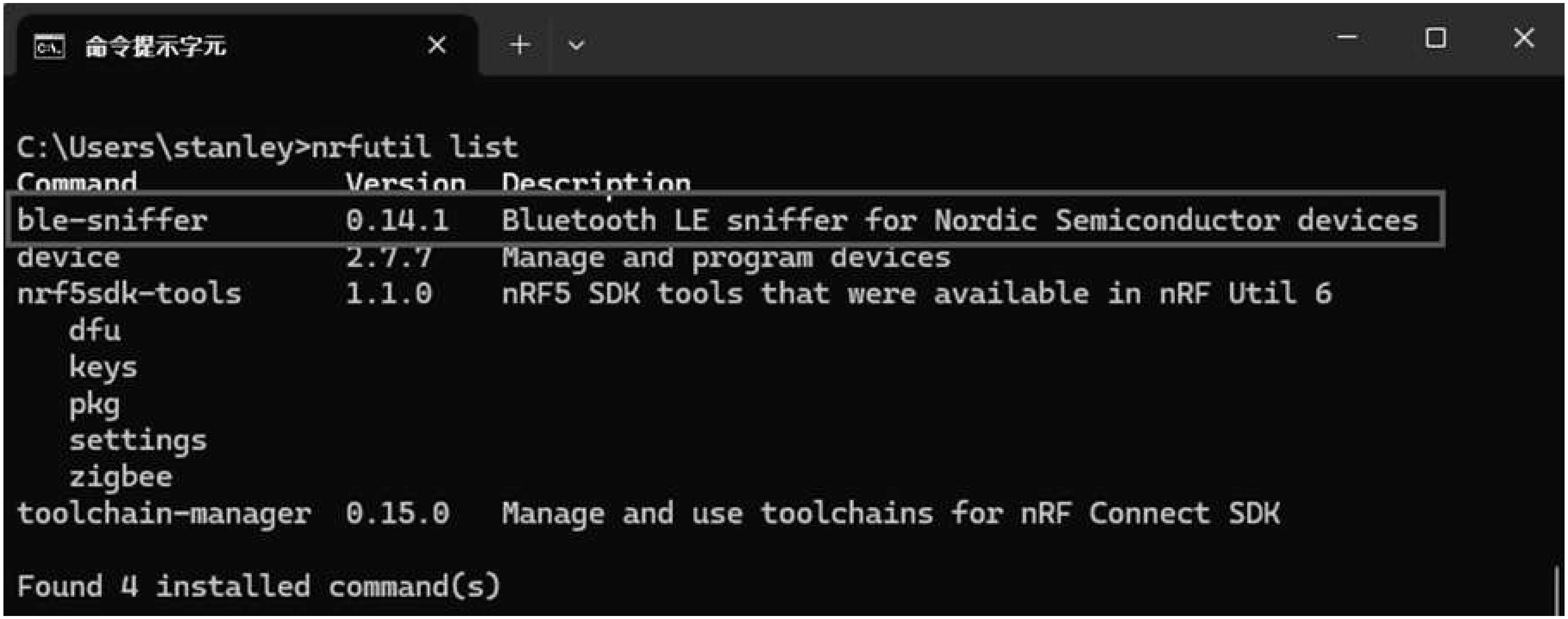
Press “Write" to flash the firmware.
After flashing, press “Select Device" again.
If the Device name appears as **nRF Sniffer for Bluetooth**, the flashing is successful.



Set Up Wireshark Software Environment

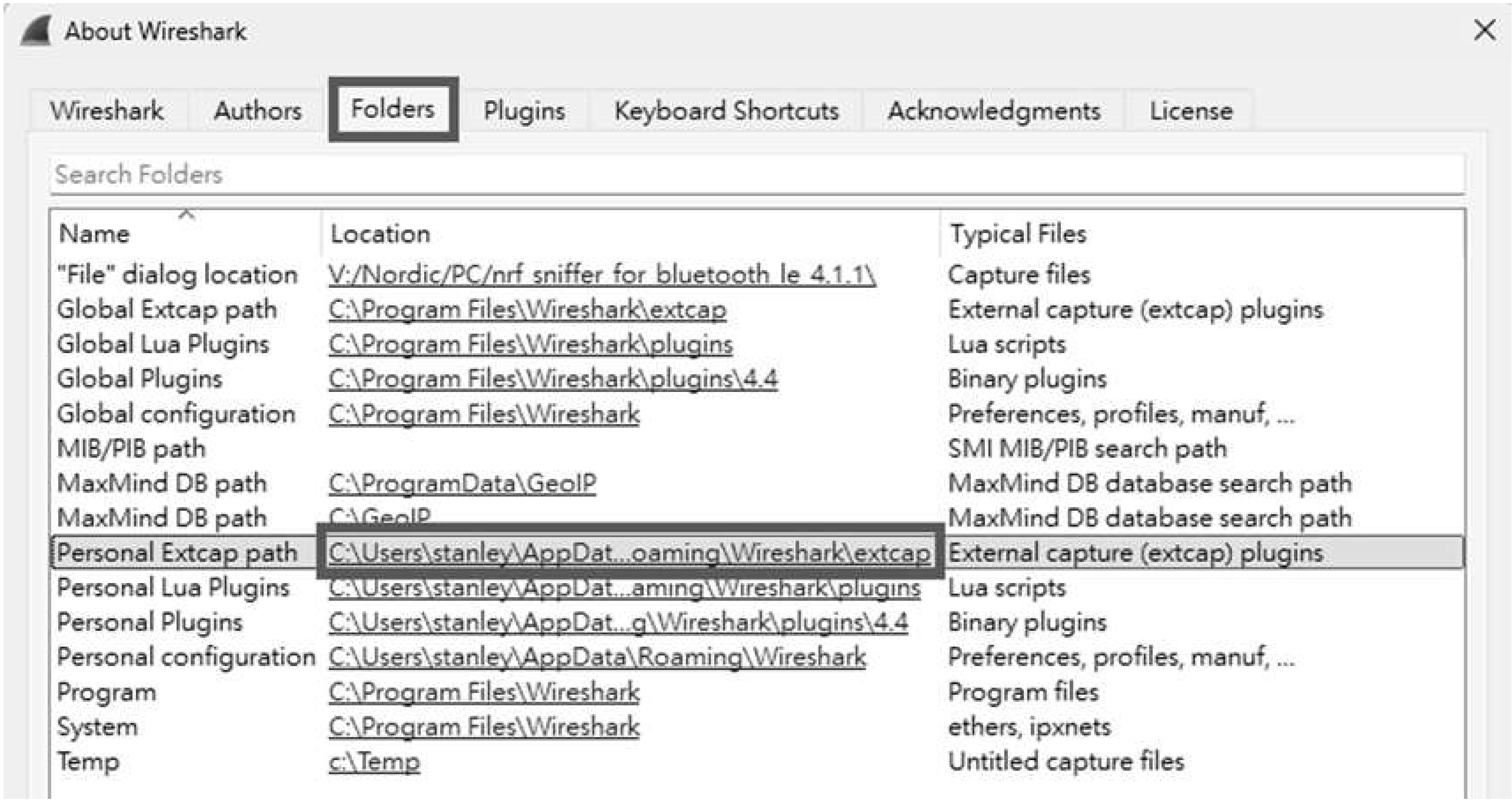
Step 1: Download & install nRF-Util: https://www.nordicsemi.com/Products/Development-tools/nRF-Util (https://www.nordicsemi.com/Products/Development-tools/nRF-Util)

Step 2: Open MS-DOS and use the command `nrfutil list` to check if the `ble-sniffer` item is available. If not, install it using `nrfutil install ble-sniffer` .



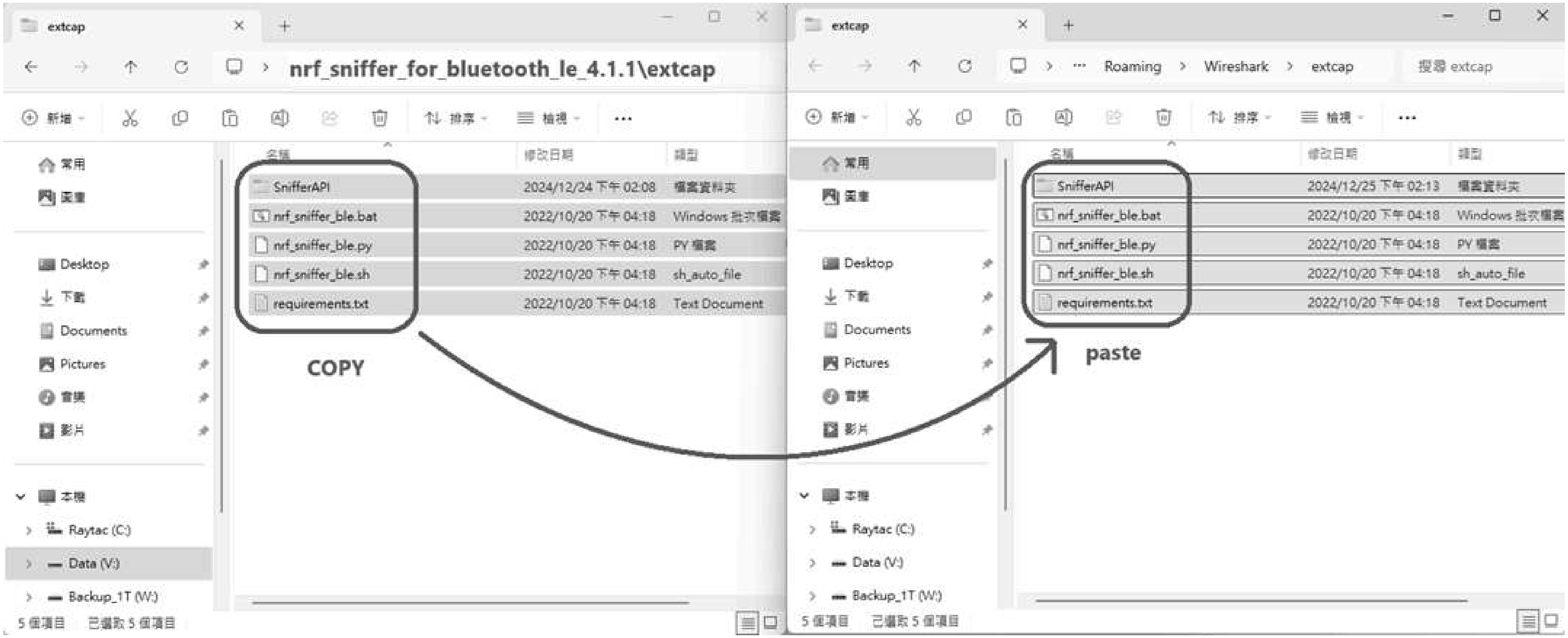
```
C:\Users\stanley>nrfutil list
Command            Version  Description
ble-sniffer        0.14.1   Bluetooth LE sniffer for Nordic Semiconductor devices
device             2.7.7    Manage and program devices
nrf5sdk-tools      1.1.0    nRF5 SDK tools that were available in nRF Util 6
   dfu
   keys
   pkg
   settings
   zigbee
toolchain-manager  0.15.0   Manage and use toolchains for nRF Connect SDK

Found 4 installed command(s)
```

Step 3: Download and Install Wireshark: https://www.wireshark.org/download.html (https://www.wireshark.org/download.html).
Step 4: Open Wireshark and navigate to: ***Help → About Wireshark → Folders***.
Step 5: Locate the string under **Personal Extcap Path** for the extcap directory, which will be an empty folder.



Name	Location	Typical Files
"File" dialog location	V:/Nordic/PC/nrf_sniffer_for_bluetooth_le_4.1.1\	Capture files
Global Extcap path	C:\Program Files\Wireshark\extcap	External capture (extcap) plugins
Global Lua Plugins	C:\Program Files\Wireshark\plugins	Lua scripts
Global Plugins	C:\Program Files\Wireshark\plugins\4.4	Binary plugins
Global configuration	C:\Program Files\Wireshark	Preferences, profiles, manuf, ...
MIB/PIB path		SMI MIB/PIB search path
MaxMind DB path	C:\ProgramData\GeoIP	MaxMind DB database search path
MaxMind DB path	C:\GeoIP	MaxMind DB database search path
Personal Extcap path	C:\Users\stanley\AppDat...oaming\Wireshark\extcap	External capture (extcap) plugins
Personal Lua Plugins	C:\Users\stanley\AppDat...aming\Wireshark\plugins	Lua scripts
Personal Plugins	C:\Users\stanley\AppDat...g\Wireshark\plugins\4.4	Binary plugins
Personal configuration	C:\Users\stanley\AppData\Roaming\Wireshark	Preferences, profiles, manuf, ...
Program	C:\Program Files\Wireshark	Program files
System	C:\Program Files\Wireshark	ethers, ipxnets
Temp	c:\Temp	Untitled capture files

Step 6: Copy the files from `nrf_sniffer_for_bluetooth_le_4.1.1\extcap` (downloaded earlier) into `Wireshark\extcap` directory.



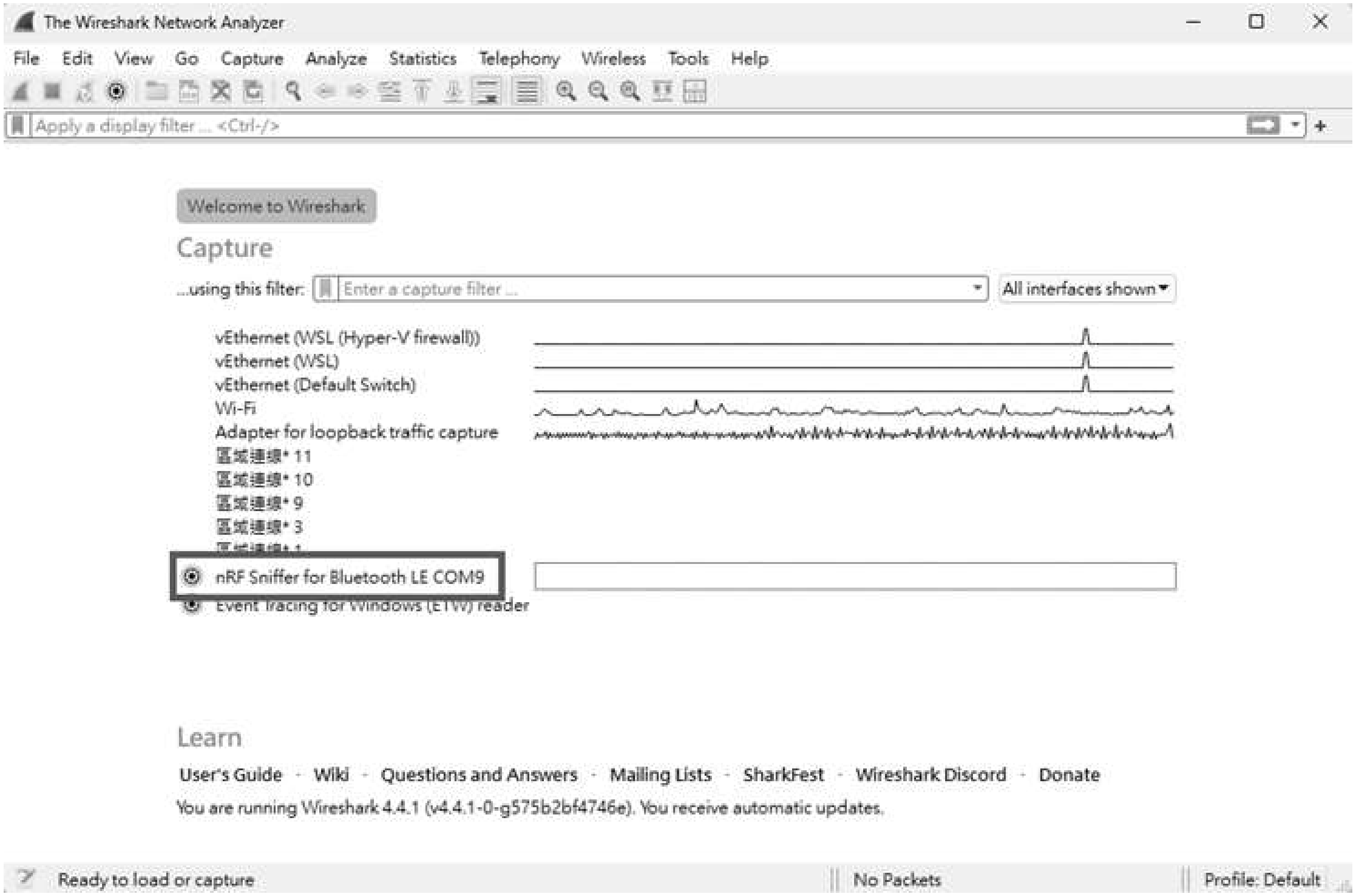
nrf_sniffer_for_bluetooth_le_4.1.1\extcap

名稱	修改日期	類型
SnifferAPI	2024/12/24 下午 02:08	檔案資料夾
nrf_sniffer_ble.bat	2022/10/20 下午 04:18	Windows 批次檔案
nrf_sniffer_ble.py	2022/10/20 下午 04:18	PY 檔案
nrf_sniffer_ble.sh	2022/10/20 下午 04:18	sh_auto_file
requirements.txt	2022/10/20 下午 04:18	Text Document

Roaming › Wireshark › extcap

名稱	修改日期	類型
SnifferAPI	2024/12/25 下午 02:13	檔案資料夾
nrf_sniffer_ble.bat	2022/10/20 下午 04:18	Windows 批次檔案
nrf_sniffer_ble.py	2022/10/20 下午 04:18	PY 檔案
nrf_sniffer_ble.sh	2022/10/20 下午 04:18	sh_auto_file
requirements.txt	2022/10/20 下午 04:18	Text Document

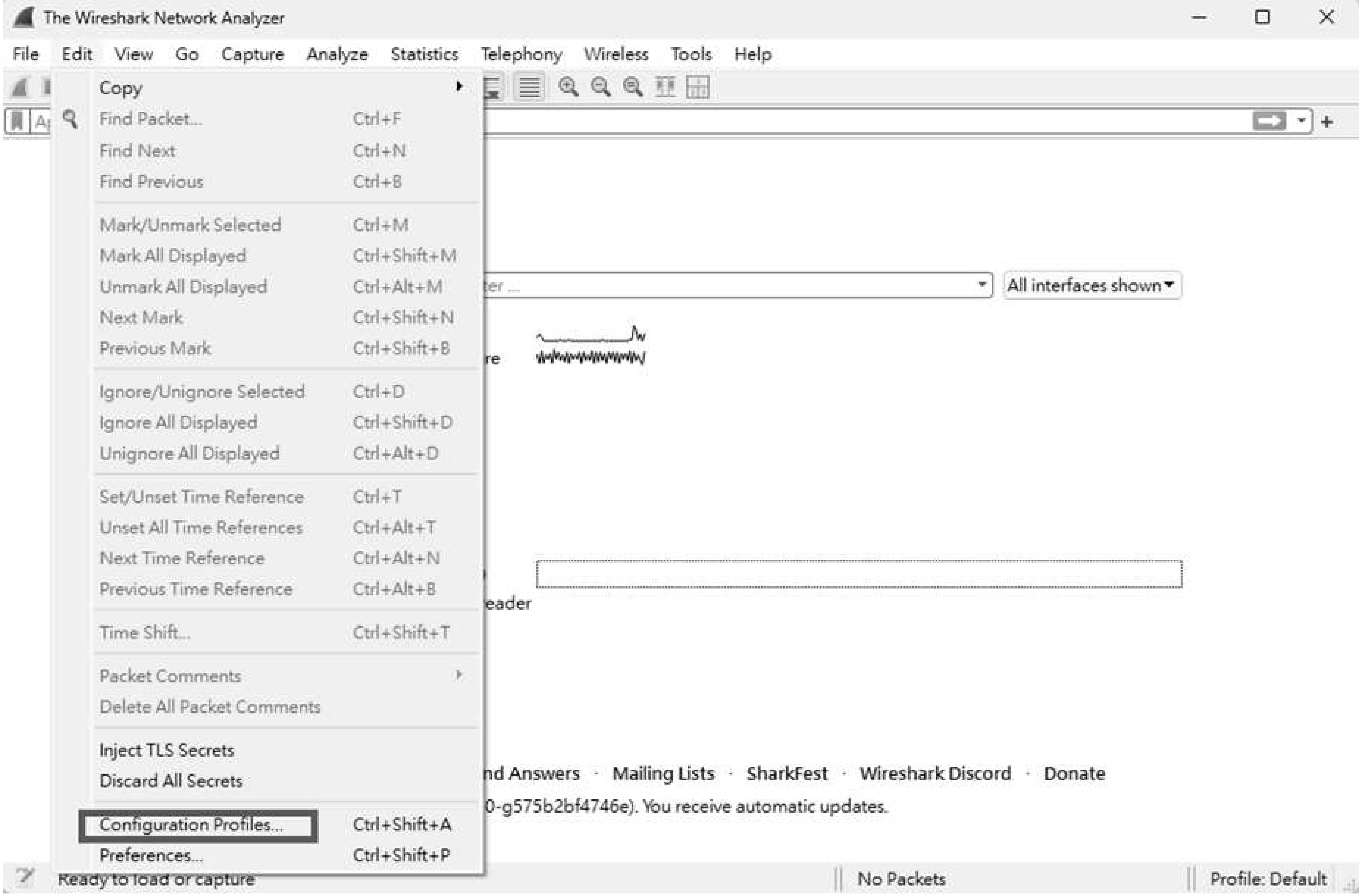
Step 7: After reopening, you should see an interface with a configurable icon next to the dongle.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter …
All interfaces shown
vEthernet (WSL (Hyper-V firewall))
vEthernet (WSL)
vEthernet (Default Switch)
Wi-Fi
Adapter for loopback traffic capture
區域連線* 11
區域連線* 10
區域連線* 9
區域連線* 3
nRF Sniffer for Bluetooth LE COM9
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
No Packets
Profile: Default

You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automatic updates.

Ready to load or capture

Step 8: Edit → Configuration Profiles → Import → From Directory → Navigate to the directory `nrf_sniffer_for_bluetooth_le_4.1.1\Profile_nRF_Sniffer_Bluetooth_LE` and click “Select Folder".

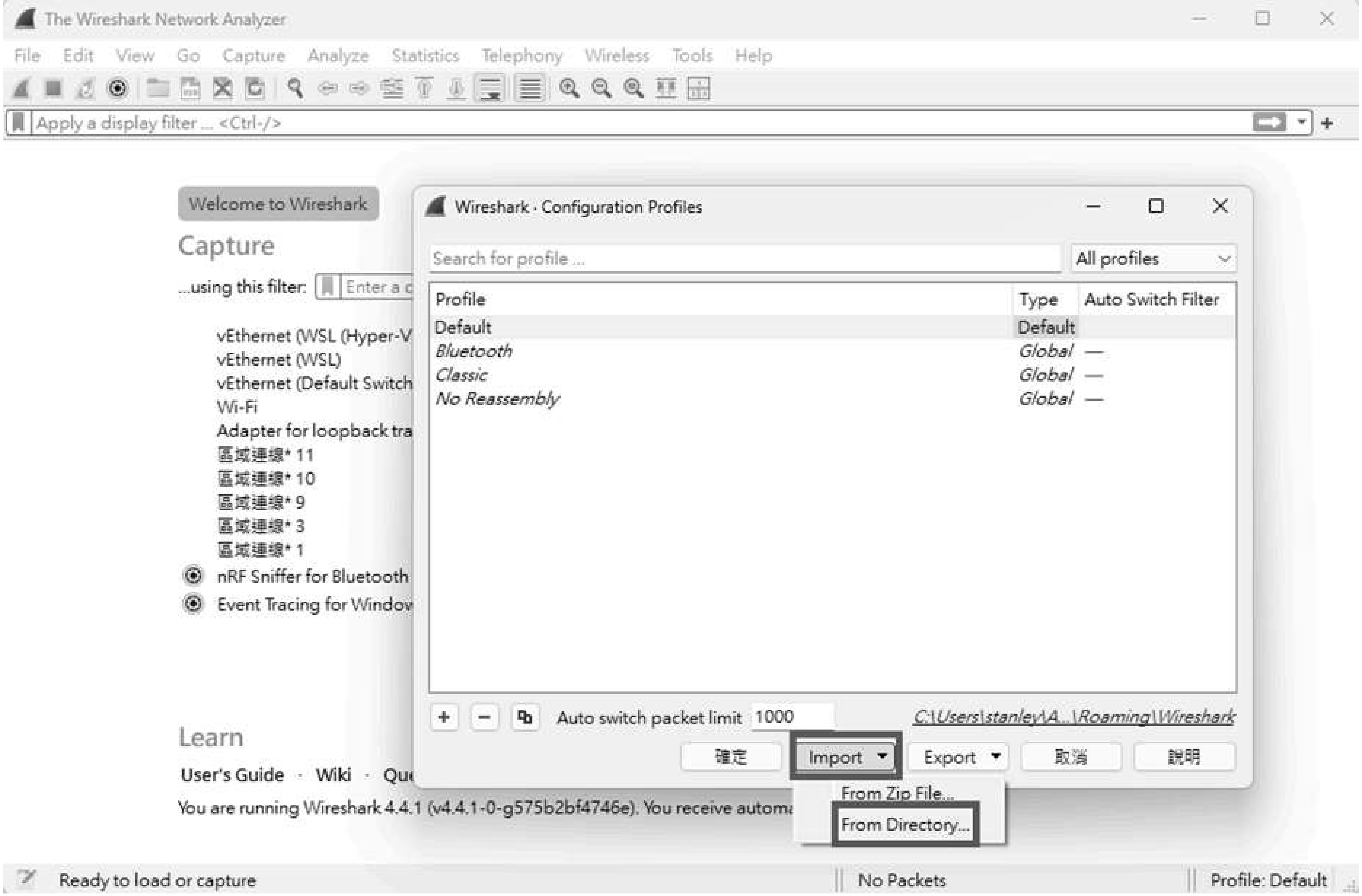

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Selected Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Selected Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comments
Delete All Packet Comments
Inject TLS Secrets
Discard All Secrets
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
ter ...
All interfaces shown
re
eader
nd Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

0-g575b2bf4746e). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default



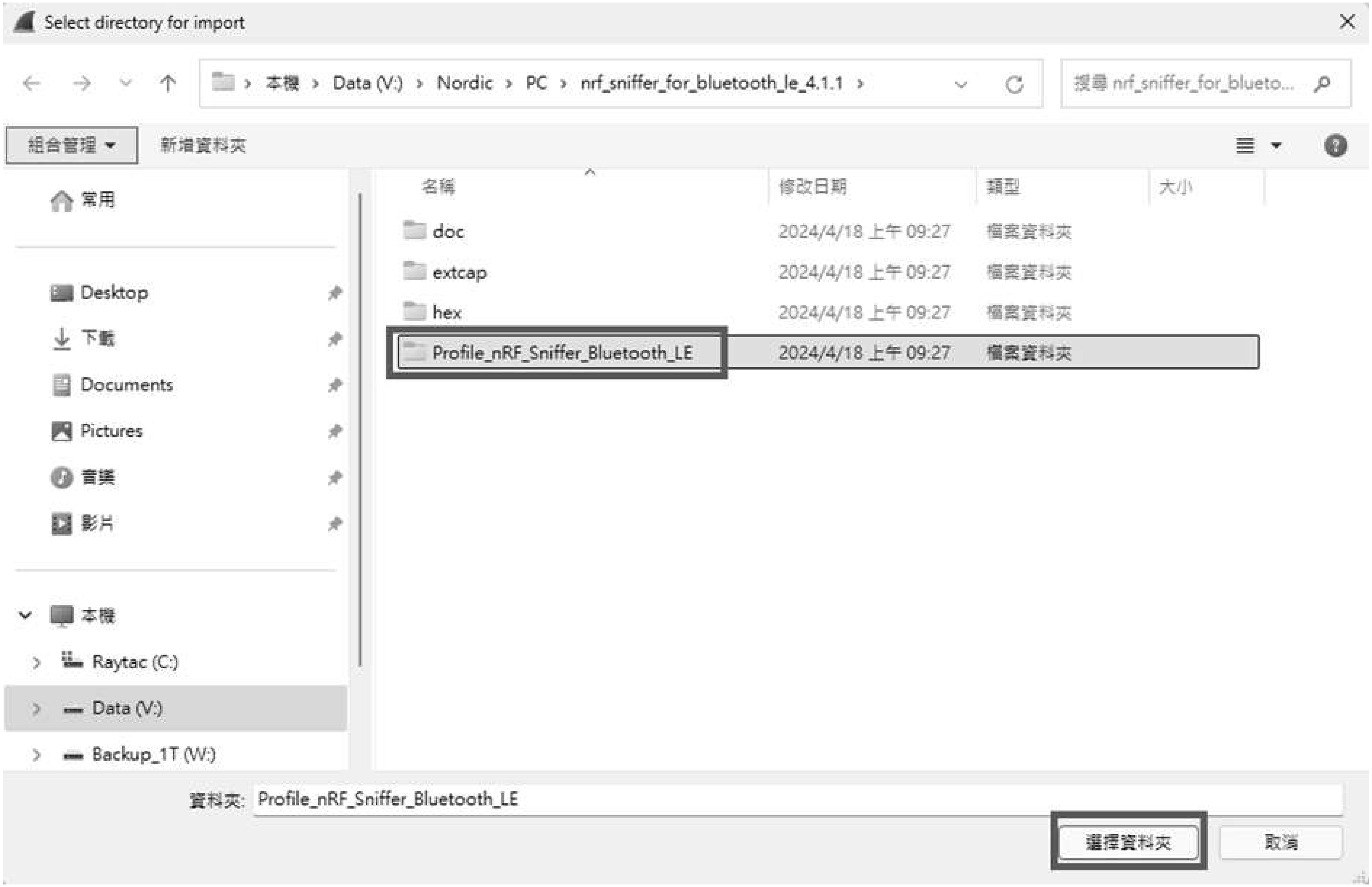
Profile	Type	Auto Switch Filter
Default	Default	
Bluetooth	*Global*	—
Classic	*Global*	—
No Reassembly	*Global*	—

Auto switch packet limit 1000

C:\Users\stanley\A...\Roaming\Wireshark

You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automa

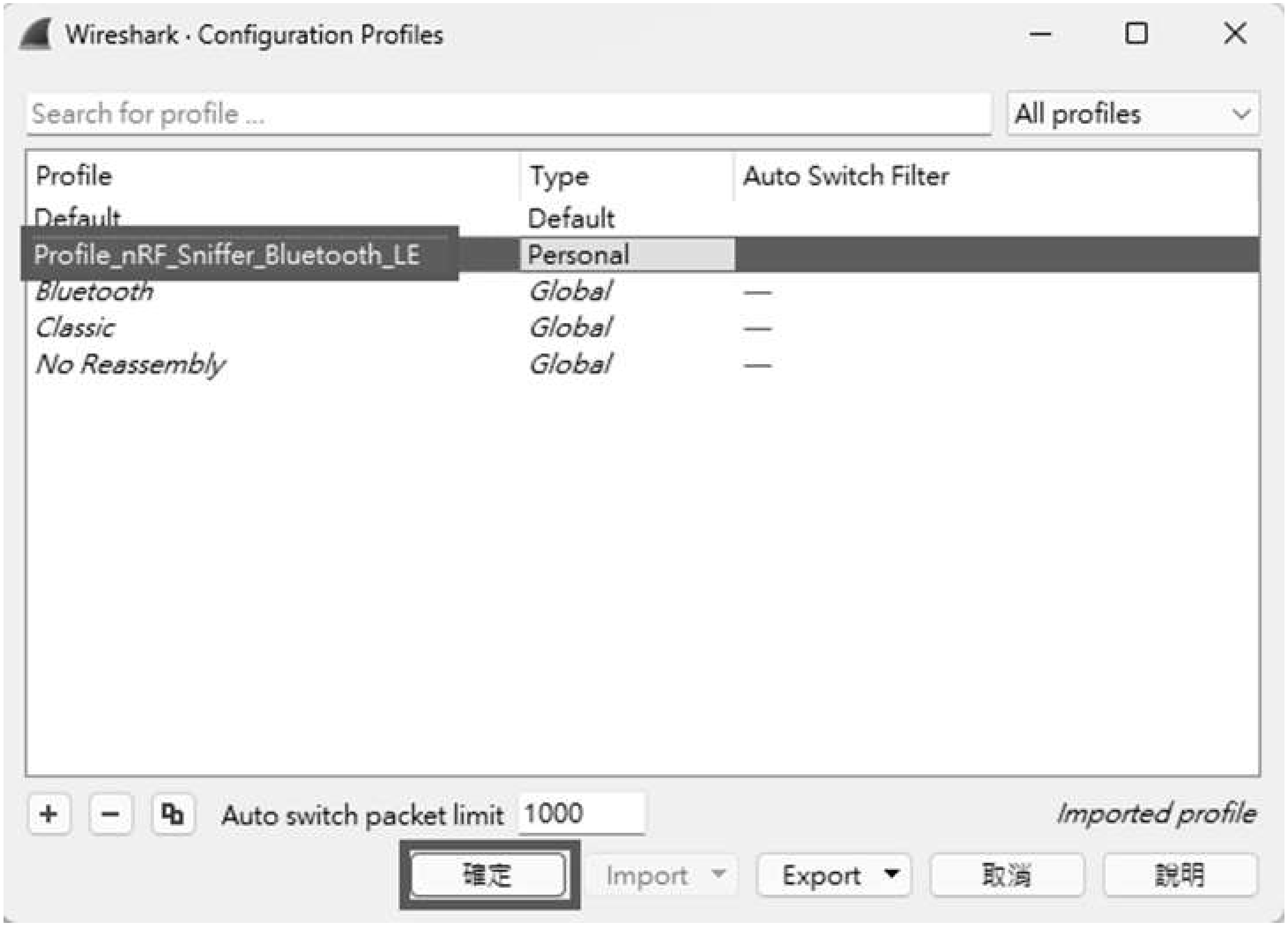
Ready to load or capture | No Packets | Profile: Default


Select directory for import
本機 › Data (V:) › Nordic › PC › nrf_sniffer_for_bluetooth_le_4.1.1 ›
搜尋 nrf_sniffer_for_blueto...
組合管理 ▾
新增資料夾
常用
Desktop
下載
Documents
Pictures
音樂
影片
本機
Raytac (C:)
Data (V:)
Backup_1T (W:)
選擇資料夾
取消

名稱	修改日期	類型	大小
doc	2024/4/18 上午 09:27	檔案資料夾	
extcap	2024/4/18 上午 09:27	檔案資料夾	
hex	2024/4/18 上午 09:27	檔案資料夾	
Profile_nRF_Sniffer_Bluetooth_LE	2024/4/18 上午 09:27	檔案資料夾	

資料夾: Profile_nRF_Sniffer_Bluetooth_LE

Step 9: The profile will be imported. Click **OK** to confirm.



Wireshark · Configuration Profiles

Search for profile ...

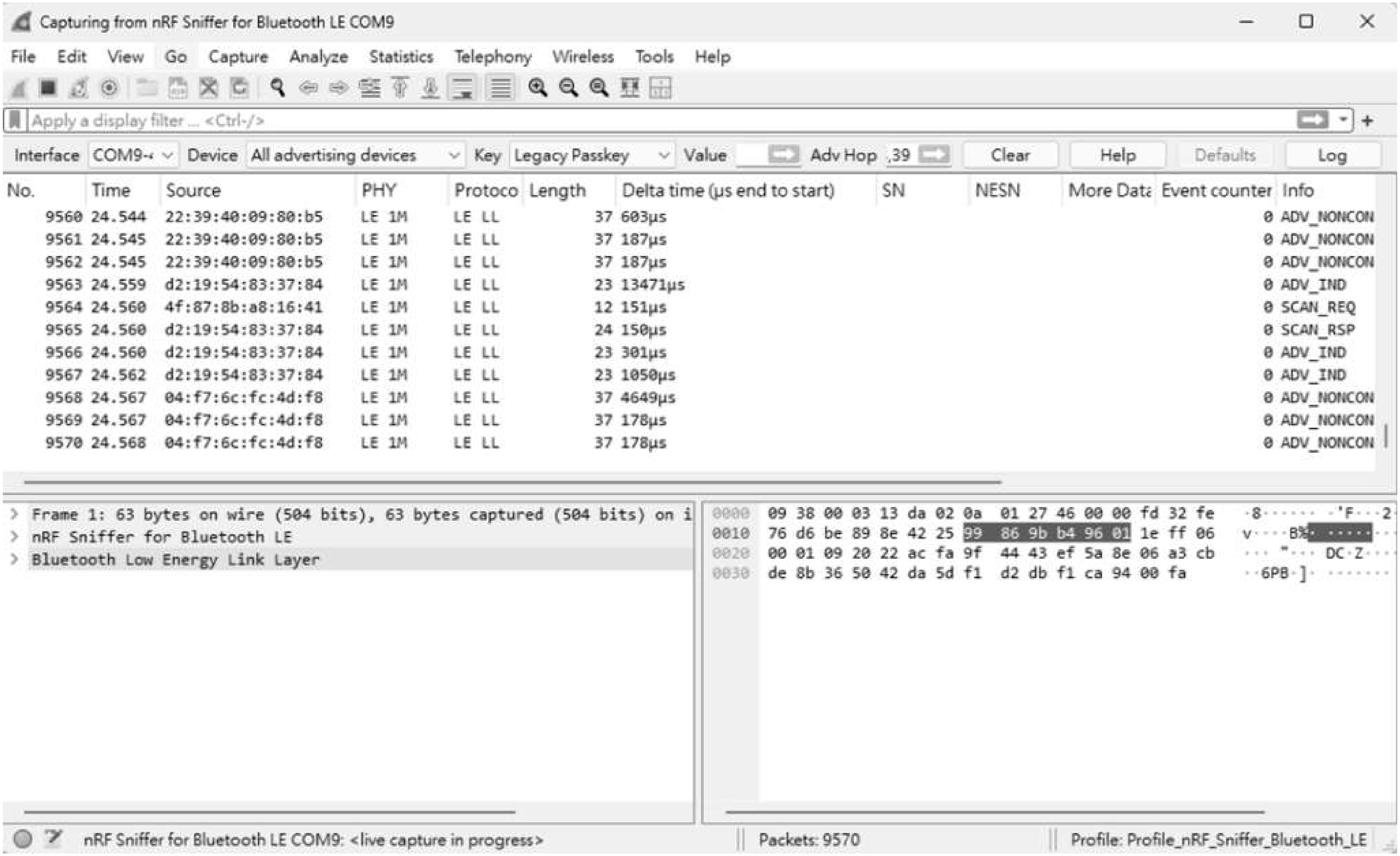
All profiles

Profile	Type	Auto Switch Filter
Default	Default	
Profile_nRF_Sniffer_Bluetooth_LE	Personal	
Bluetooth	*Global*	—
Classic	*Global*	—
No Reassembly	*Global*	—

Auto switch packet limit 1000

Imported profile

After all the above is done, the setup shall be completed.



Capturing from nRF Sniffer for Bluetooth LE COM9
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Clear
Help
Defaults
Log

Interface COM9-‹ Device All advertising devices Key Legacy Passkey Value Adv Hop ,39

```
No.     Time    Source              PHY     Protoco Length Delta time (µs end to start) SN NESN More Data Event counter Info
   9560 24.544  22:39:40:09:80:b5   LE 1M   LE LL       37 603µs                                                    0 ADV_NONCON
   9561 24.545  22:39:40:09:80:b5   LE 1M   LE LL       37 187µs                                                    0 ADV_NONCON
   9562 24.545  22:39:40:09:80:b5   LE 1M   LE LL       37 187µs                                                    0 ADV_NONCON
   9563 24.559  d2:19:54:83:37:84   LE 1M   LE LL       23 13471µs                                                  0 ADV_IND
   9564 24.560  4f:87:8b:a8:16:41   LE 1M   LE LL       12 151µs                                                    0 SCAN_REQ
   9565 24.560  d2:19:54:83:37:84   LE 1M   LE LL       24 150µs                                                    0 SCAN_RSP
   9566 24.560  d2:19:54:83:37:84   LE 1M   LE LL       23 301µs                                                    0 ADV_IND
   9567 24.562  d2:19:54:83:37:84   LE 1M   LE LL       23 1050µs                                                   0 ADV_IND
   9568 24.567  04:f7:6c:fc:4d:f8   LE 1M   LE LL       37 4649µs                                                   0 ADV_NONCON
   9569 24.567  04:f7:6c:fc:4d:f8   LE 1M   LE LL       37 178µs                                                    0 ADV_NONCON
   9570 24.568  04:f7:6c:fc:4d:f8   LE 1M   LE LL       37 178µs                                                    0 ADV_NONCON
```

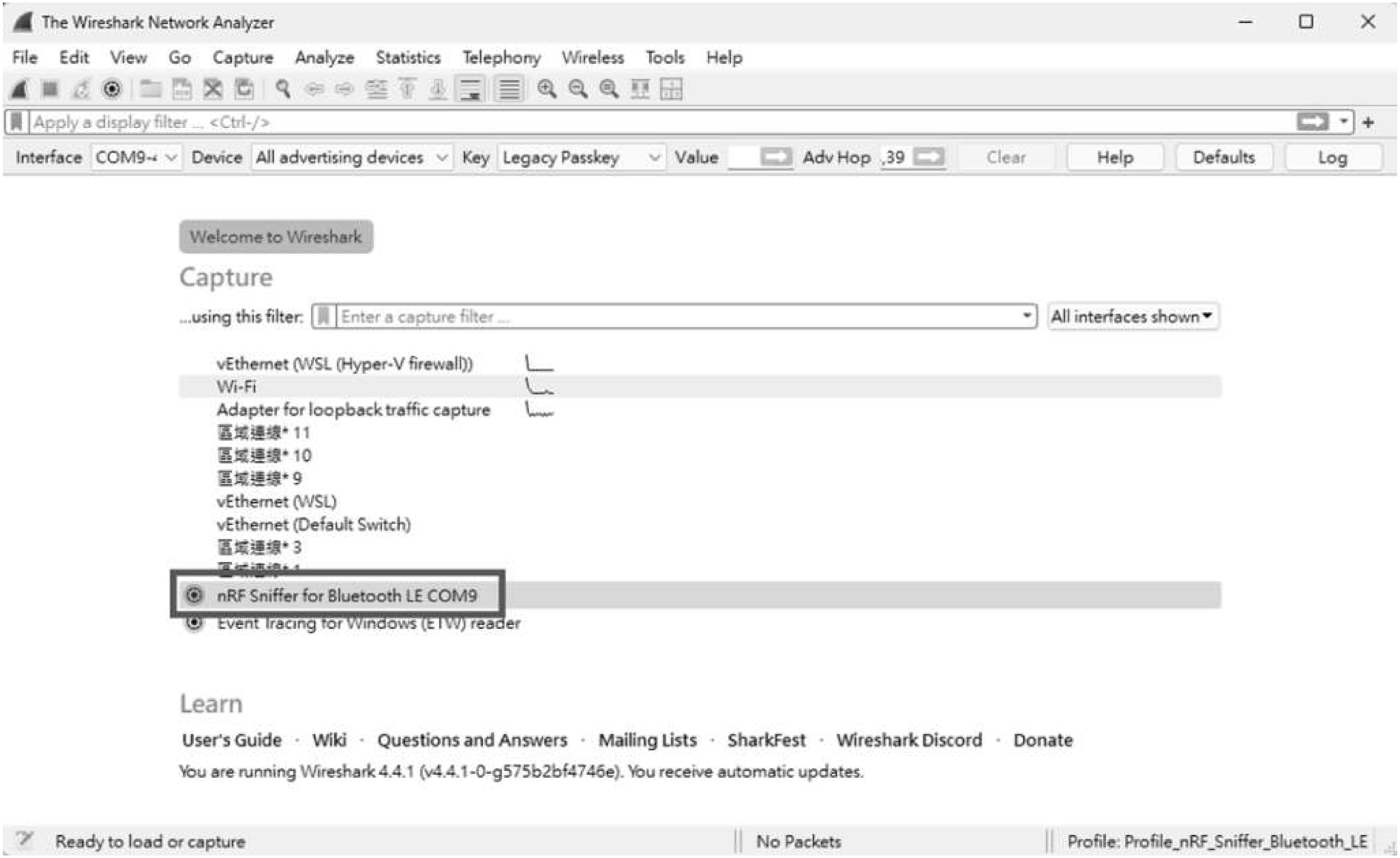
```
> Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on i
> nRF Sniffer for Bluetooth LE
> Bluetooth Low Energy Link Layer
```

```
0000  09 38 00 03 13 da 02 0a  01 27 46 00 00 fd 32 fe   ·8······ ·'F···2·
0010  76 d6 be 89 8e 42 25 99  86 9b b4 96 01 1e ff 06   v····B%· ········
0020  00 01 09 20 22 ac fa 9f  44 43 ef 5a 8e 06 a3 cb   ··· "··· DC·Z····
0030  de 8b 36 50 42 da 5d f1  d2 db f1 ca 94 00 fa      ··6PB·]· ·······
```

nRF Sniffer for Bluetooth LE COM9: <live capture in progress>   Packets: 9570   Profile: Profile_nRF_Sniffer_Bluetooth_LE

Capturing and analyzing Bluetooth packets

After launching the program, you can see the following devices and Dongle settings.
Double-click to start the packet capture process:


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>
Clear
Help
Defaults
Log
Welcome to Wireshark
Capture
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

Interface COM9-‹ Device All advertising devices Key Legacy Passkey Value Adv Hop ,39

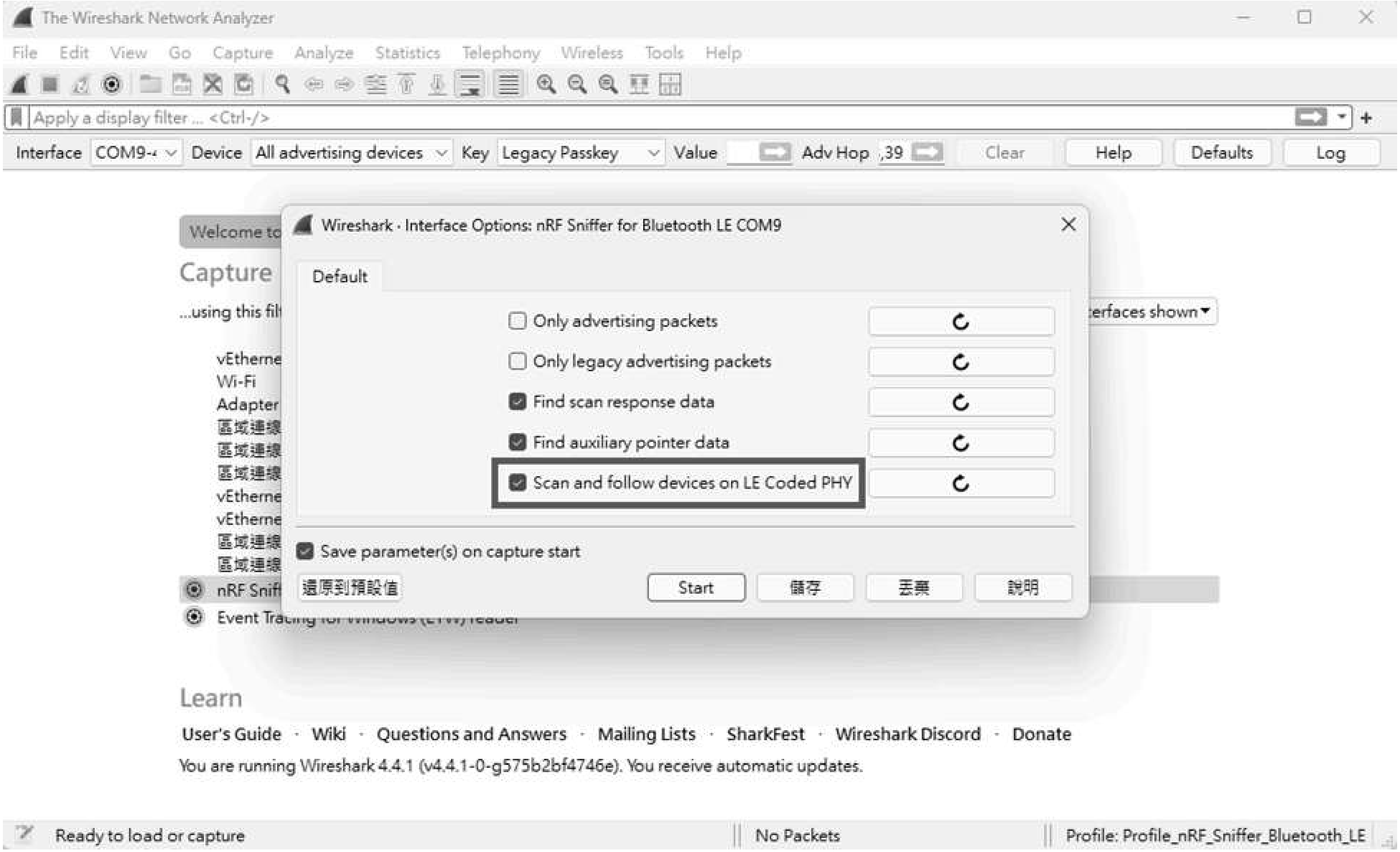
…using this filter:

vEthernet (WSL (Hyper-V firewall))
Wi-Fi
Adapter for loopback traffic capture
區域連線* 11
區域連線* 10
區域連線* 9
vEthernet (WSL)
vEthernet (Default Switch)
區域連線* 3
區域連線* 1
nRF Sniffer for Bluetooth LE COM9
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Profile_nRF_Sniffer_Bluetooth_LE

If you want to capture packets with PHY=125K, you can use the following settings:



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Interface COM9-
Device All advertising devices
Key Legacy Passkey
Value
Adv Hop ,39
Clear
Help
Defaults
Log
Welcome to
Capture
...using this fil
terfaces shown
vEtherne
Wi-Fi
Adapter
區域連線
區域連線
區域連線
vEtherne
vEtherne
區域連線
區域連線
nRF Snif
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Profile_nRF_Sniffer_Bluetooth_LE

Wireshark · Interface Options: nRF Sniffer for Bluetooth LE COM9

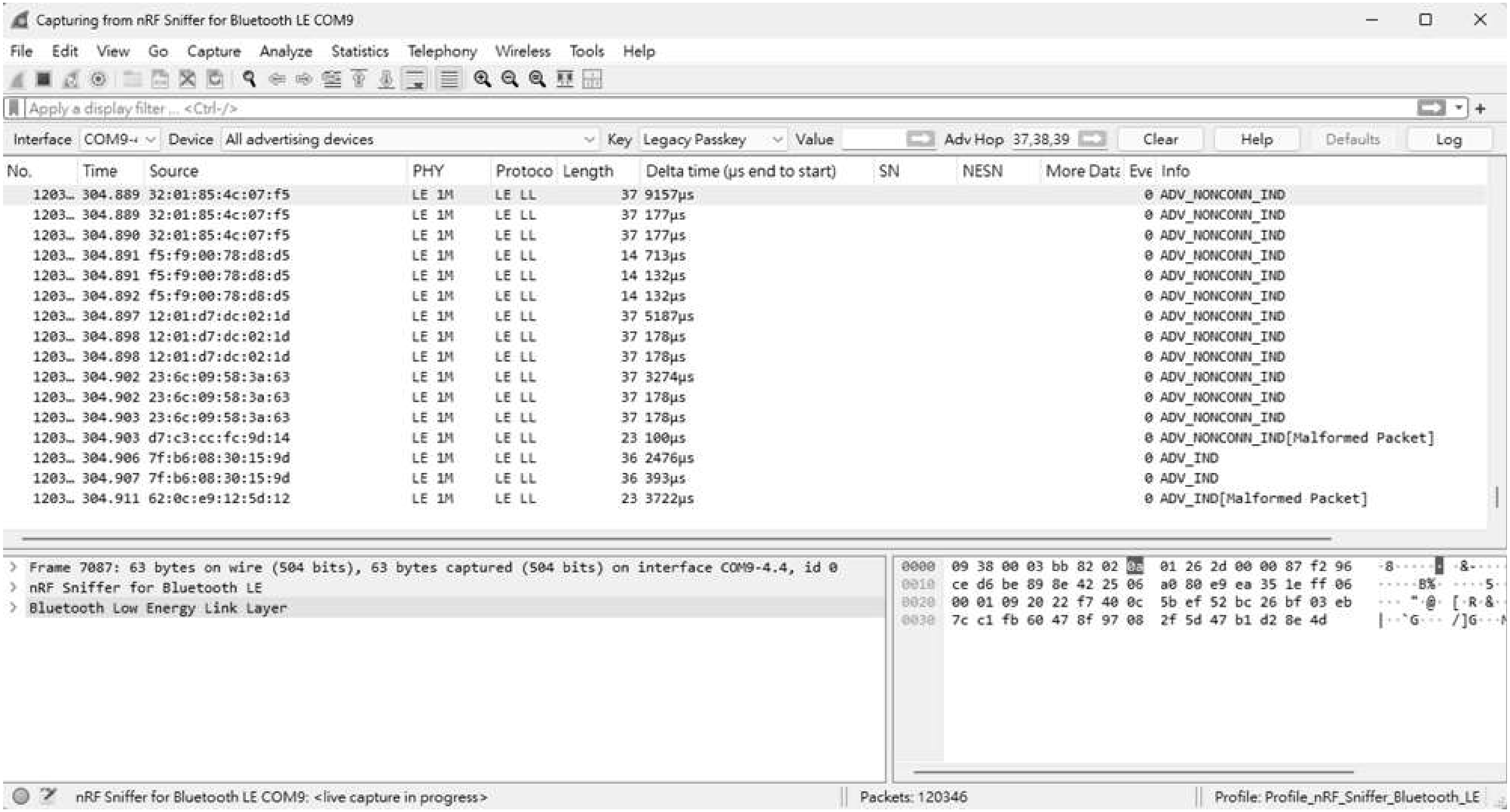
Default

- ☐ Only advertising packets
- ☐ Only legacy advertising packets
- ☑ Find scan response data
- ☑ Find auxiliary pointer data
- ☑ Scan and follow devices on LE Coded PHY

☑ Save parameter(s) on capture start

還原到預設值 | Start | 儲存 | 丟棄 | 說明

You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automatic updates.



Interface COM9-4 Device All advertising devices Key Legacy Passkey Adv Hop 37,38,39

```
No.       Time     Source                PHY     Protoco Length Delta time (µs end to start) SN  NESN  More Data Eve Info
  1203… 304.889 32:01:85:4c:07:f5     LE 1M   LE LL       37 9157µs                                       0 ADV_NONCONN_IND
  1203… 304.889 32:01:85:4c:07:f5     LE 1M   LE LL       37 177µs                                        0 ADV_NONCONN_IND
  1203… 304.890 32:01:85:4c:07:f5     LE 1M   LE LL       37 177µs                                        0 ADV_NONCONN_IND
  1203… 304.891 f5:f9:00:78:d8:d5     LE 1M   LE LL       14 713µs                                        0 ADV_NONCONN_IND
  1203… 304.891 f5:f9:00:78:d8:d5     LE 1M   LE LL       14 132µs                                        0 ADV_NONCONN_IND
  1203… 304.892 f5:f9:00:78:d8:d5     LE 1M   LE LL       14 132µs                                        0 ADV_NONCONN_IND
  1203… 304.897 12:01:d7:dc:02:1d     LE 1M   LE LL       37 5187µs                                       0 ADV_NONCONN_IND
  1203… 304.898 12:01:d7:dc:02:1d     LE 1M   LE LL       37 178µs                                        0 ADV_NONCONN_IND
  1203… 304.898 12:01:d7:dc:02:1d     LE 1M   LE LL       37 178µs                                        0 ADV_NONCONN_IND
  1203… 304.902 23:6c:09:58:3a:63     LE 1M   LE LL       37 3274µs                                       0 ADV_NONCONN_IND
  1203… 304.902 23:6c:09:58:3a:63     LE 1M   LE LL       37 178µs                                        0 ADV_NONCONN_IND
  1203… 304.903 23:6c:09:58:3a:63     LE 1M   LE LL       37 178µs                                        0 ADV_NONCONN_IND
  1203… 304.903 d7:c3:cc:fc:9d:14     LE 1M   LE LL       23 100µs                                        0 ADV_NONCONN_IND[Malformed Packet]
  1203… 304.906 7f:b6:08:30:15:9d     LE 1M   LE LL       36 2476µs                                       0 ADV_IND
  1203… 304.907 7f:b6:08:30:15:9d     LE 1M   LE LL       36 393µs                                        0 ADV_IND
  1203… 304.911 62:0c:e9:12:5d:12     LE 1M   LE LL       23 3722µs                                       0 ADV_IND[Malformed Packet]
```

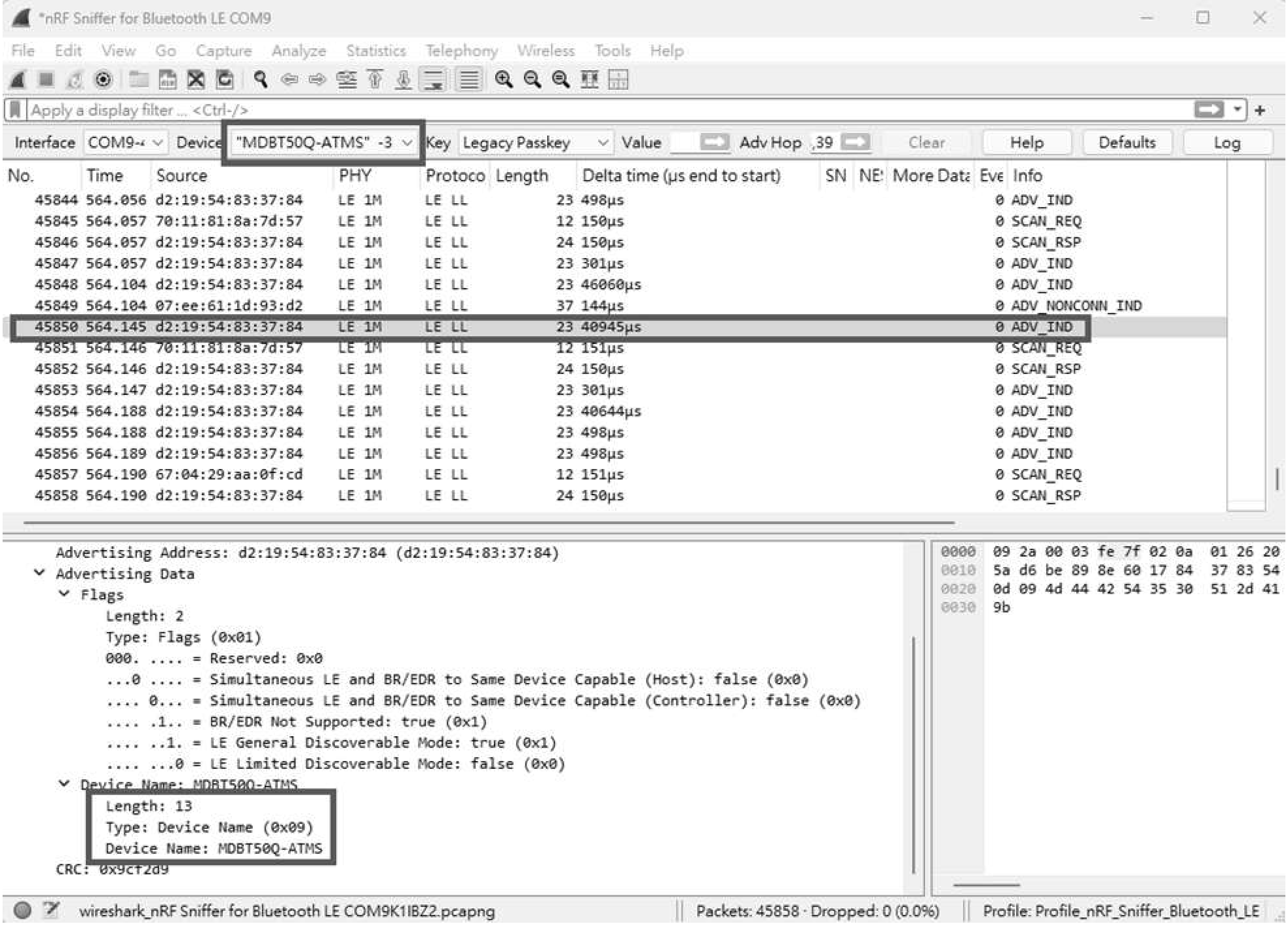
```
> Frame 7087: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface COM9-4.4, id 0
> nRF Sniffer for Bluetooth LE
> Bluetooth Low Energy Link Layer
```

```
0000  09 38 00 03 bb 82 02 0e  01 26 2d 00 00 87 f2 96   ·8·····▪ ·&-·····
0010  ce d6 be 89 8e 42 25 06  a0 80 e9 ea 35 1e ff 06   ·····B%· ····5··
0020  00 01 09 20 22 f7 40 0c  5b ef 52 bc 26 bf 03 eb   ··· "·@· [·R·&···
0030  7c c1 fb 60 47 8f 97 08  2f 5d 47 b1 d2 8e 4d      |··`G··· /]G···M
```

nRF Sniffer for Bluetooth LE COM9: <live capture in progress> Packets: 120346 Profile: Profile_nRF_Sniffer_Bluetooth_LE

Packet Analysis Method

In Wireshark, select the device from the “Device" menu to capture and analyze broadcast packets.



*nRF Sniffer for Bluetooth LE COM9
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Clear
Help
Defaults
Log

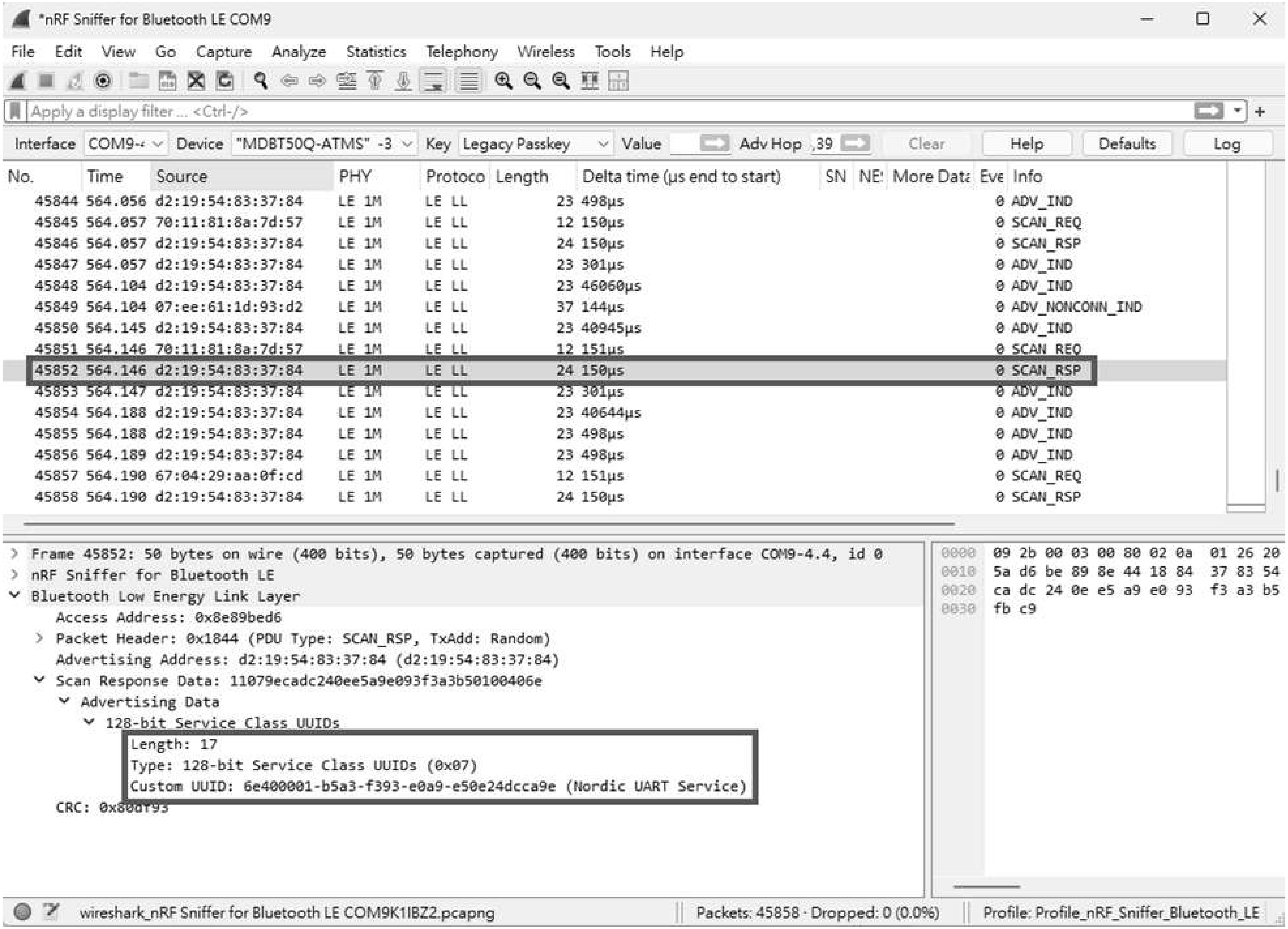
Interface COM9-‹ Device "MDBT50Q-ATMS" -3 Key Legacy Passkey Value Adv Hop ,39

```
No.      Time    Source             PHY     Protoco Length  Delta time (µs end to start)  SN  NE! More Data Eve Info
   45844 564.056 d2:19:54:83:37:84  LE 1M   LE LL       23 498µs                                              0 ADV_IND
   45845 564.057 70:11:81:8a:7d:57  LE 1M   LE LL       12 150µs                                              0 SCAN_REQ
   45846 564.057 d2:19:54:83:37:84  LE 1M   LE LL       24 150µs                                              0 SCAN_RSP
   45847 564.057 d2:19:54:83:37:84  LE 1M   LE LL       23 301µs                                              0 ADV_IND
   45848 564.104 d2:19:54:83:37:84  LE 1M   LE LL       23 46060µs                                            0 ADV_IND
   45849 564.104 07:ee:61:1d:93:d2  LE 1M   LE LL       37 144µs                                              0 ADV_NONCONN_IND
   45850 564.145 d2:19:54:83:37:84  LE 1M   LE LL       23 40945µs                                            0 ADV_IND
   45851 564.146 70:11:81:8a:7d:57  LE 1M   LE LL       12 151µs                                              0 SCAN_REQ
   45852 564.146 d2:19:54:83:37:84  LE 1M   LE LL       24 150µs                                              0 SCAN_RSP
   45853 564.147 d2:19:54:83:37:84  LE 1M   LE LL       23 301µs                                              0 ADV_IND
   45854 564.188 d2:19:54:83:37:84  LE 1M   LE LL       23 40644µs                                            0 ADV_IND
   45855 564.188 d2:19:54:83:37:84  LE 1M   LE LL       23 498µs                                              0 ADV_IND
   45856 564.189 d2:19:54:83:37:84  LE 1M   LE LL       23 498µs                                              0 ADV_IND
   45857 564.190 67:04:29:aa:0f:cd  LE 1M   LE LL       12 151µs                                              0 SCAN_REQ
   45858 564.190 d2:19:54:83:37:84  LE 1M   LE LL       24 150µs                                              0 SCAN_RSP
```

```
    Advertising Address: d2:19:54:83:37:84 (d2:19:54:83:37:84)
  ˅ Advertising Data
    ˅ Flags
        Length: 2
        Type: Flags (0x01)
        000. .... = Reserved: 0x0
        ...0 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x0)
        .... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x0)
        .... .1.. = BR/EDR Not Supported: true (0x1)
        .... ..1. = LE General Discoverable Mode: true (0x1)
        .... ...0 = LE Limited Discoverable Mode: false (0x0)
    ˅ Device Name: MDBT50Q-ATMS
        Length: 13
        Type: Device Name (0x09)
        Device Name: MDBT50Q-ATMS
    CRC: 0x9cf2d9
```

```
0000  09 2a 00 03 fe 7f 02 0a  01 26 20
0010  5a d6 be 89 8e 60 17 84  37 83 54
0020  0d 09 4d 44 42 54 35 30  51 2d 41
0030  9b
```

wireshark_nRF Sniffer for Bluetooth LE COM9K1IBZ2.pcapng || Packets: 45858 · Dropped: 0 (0.0%) || Profile: Profile_nRF_Sniffer_Bluetooth_LE


*nRF Sniffer for Bluetooth LE COM9
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Clear
Help
Defaults
Log

Interface COM9-4 Device "MDBT50Q-ATMS" -3 Key Legacy Passkey Value Adv Hop ,39

```
No.   Time    Source             PHY    Protoco Length Delta time (µs end to start) SN NE: More Data Eve Info
45844 564.056 d2:19:54:83:37:84  LE 1M  LE LL      23 498µs                                       0 ADV_IND
45845 564.057 70:11:81:8a:7d:57  LE 1M  LE LL      12 150µs                                       0 SCAN_REQ
45846 564.057 d2:19:54:83:37:84  LE 1M  LE LL      24 150µs                                       0 SCAN_RSP
45847 564.057 d2:19:54:83:37:84  LE 1M  LE LL      23 301µs                                       0 ADV_IND
45848 564.104 d2:19:54:83:37:84  LE 1M  LE LL      23 46060µs                                     0 ADV_IND
45849 564.104 07:ee:61:1d:93:d2  LE 1M  LE LL      37 144µs                                       0 ADV_NONCONN_IND
45850 564.145 d2:19:54:83:37:84  LE 1M  LE LL      23 40945µs                                     0 ADV_IND
45851 564.146 70:11:81:8a:7d:57  LE 1M  LE LL      12 151µs                                       0 SCAN_REQ
45852 564.146 d2:19:54:83:37:84  LE 1M  LE LL      24 150µs                                       0 SCAN_RSP
45853 564.147 d2:19:54:83:37:84  LE 1M  LE LL      23 301µs                                       0 ADV_IND
45854 564.188 d2:19:54:83:37:84  LE 1M  LE LL      23 40644µs                                     0 ADV_IND
45855 564.188 d2:19:54:83:37:84  LE 1M  LE LL      23 498µs                                       0 ADV_IND
45856 564.189 d2:19:54:83:37:84  LE 1M  LE LL      23 498µs                                       0 ADV_IND
45857 564.190 67:04:29:aa:0f:cd  LE 1M  LE LL      12 151µs                                       0 SCAN_REQ
45858 564.190 d2:19:54:83:37:84  LE 1M  LE LL      24 150µs                                       0 SCAN_RSP
```

```
> Frame 45852: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface COM9-4.4, id 0
> nRF Sniffer for Bluetooth LE
v Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  > Packet Header: 0x1844 (PDU Type: SCAN_RSP, TxAdd: Random)
    Advertising Address: d2:19:54:83:37:84 (d2:19:54:83:37:84)
  v Scan Response Data: 11079ecadc240ee5a9e093f3a3b50100406e
    v Advertising Data
      v 128-bit Service Class UUIDs
            Length: 17
            Type: 128-bit Service Class UUIDs (0x07)
            Custom UUID: 6e400001-b5a3-f393-e0a9-e50e24dcca9e (Nordic UART Service)
    CRC: 0x80df93
```

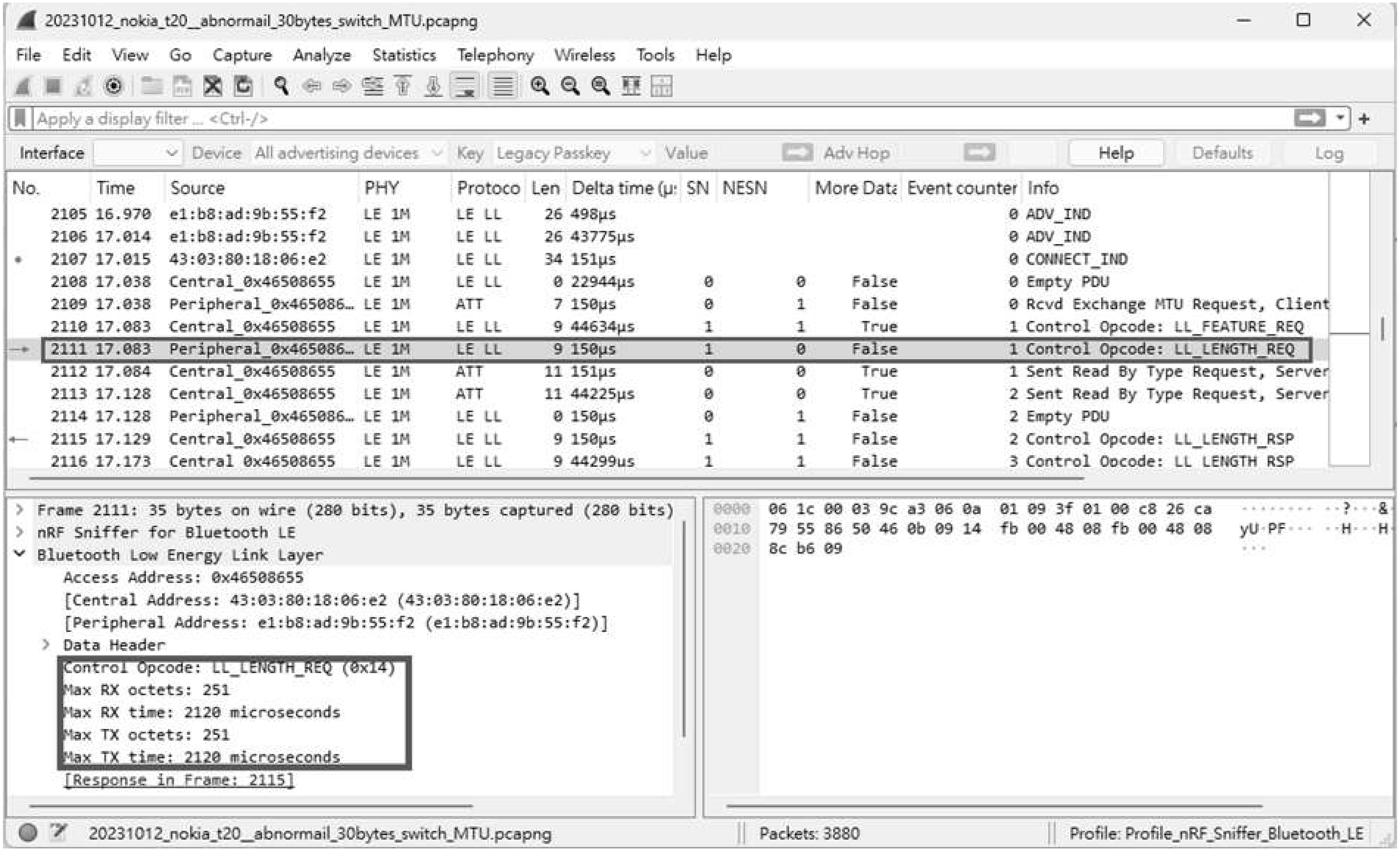
```
0000  09 2b 00 03 00 80 02 0a  01 26 20
0010  5a d6 be 89 8e 44 18 84  37 83 54
0020  ca dc 24 0e e5 a9 e0 93  f3 a3 b5
0030  fb c9
```

wireshark_nRF Sniffer for Bluetooth LE COM9K1IBZ2.pcapng | Packets: 45858 · Dropped: 0 (0.0%) | Profile: Profile_nRF_Sniffer_Bluetooth_LE

User Cases – What sniffer can offer

1. Disconnection when transmitting over 20 bytes between Tablet and Raytac's AT-Command Module:

Through sniffer analysis, it was discovered that Raytac's module requested a packet length of 251 bytes, but the tablet's TX setting was limited to 27 bytes.

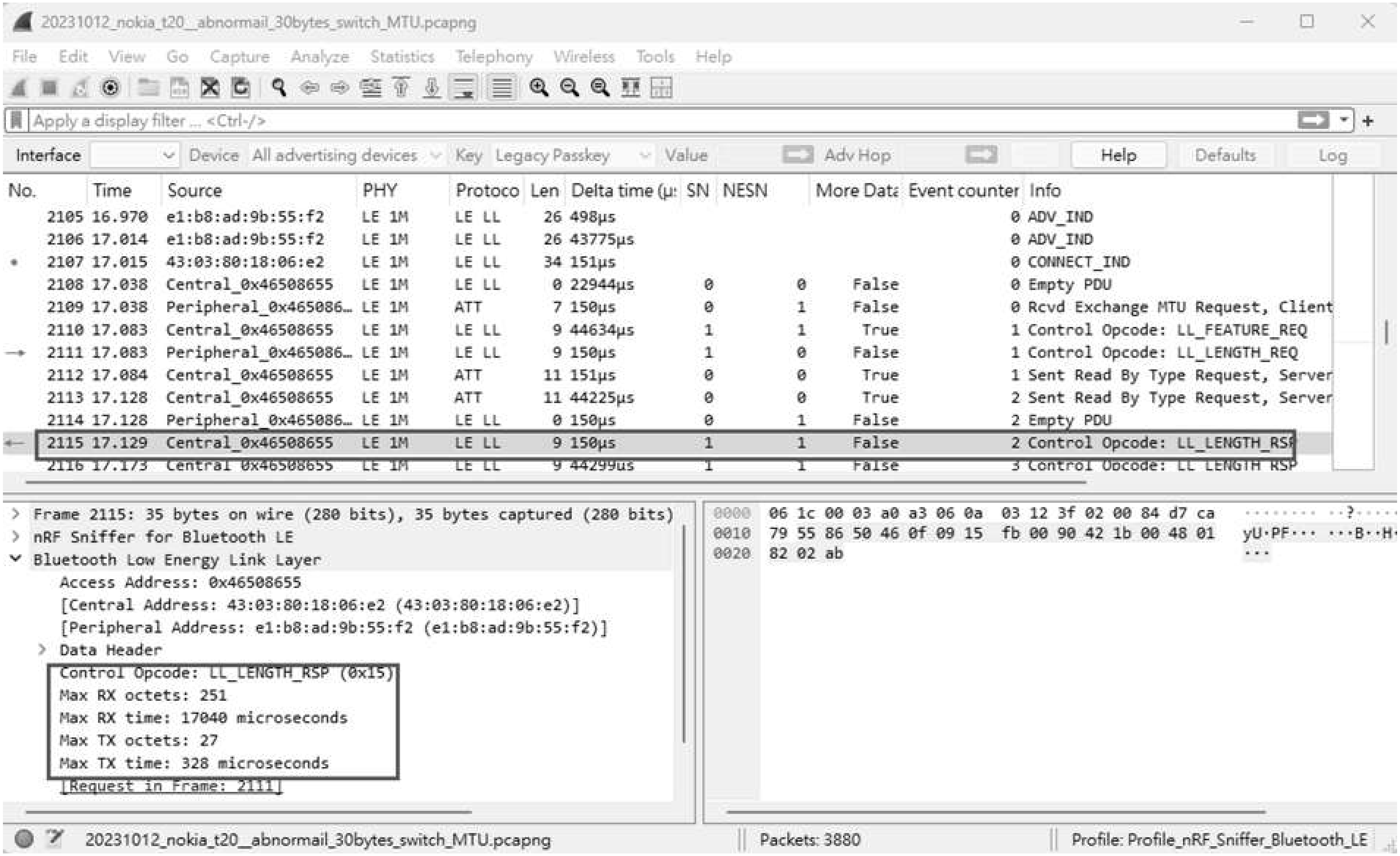


```
No.   Time   Source                 PHY    Protoco Len Delta time (µ: SN  NESN  More Data Event counter Info
 2105 16.970 e1:b8:ad:9b:55:f2      LE 1M  LE LL   26  498µs                                       0 ADV_IND
 2106 17.014 e1:b8:ad:9b:55:f2      LE 1M  LE LL   26  43775µs                                     0 ADV_IND
 2107 17.015 43:03:80:18:06:e2      LE 1M  LE LL   34  151µs                                       0 CONNECT_IND
 2108 17.038 Central_0x46508655     LE 1M  LE LL    0  22944µs      0     0  False                 0 Empty PDU
 2109 17.038 Peripheral_0x465086…   LE 1M  ATT      7  150µs        0     1  False                 0 Rcvd Exchange MTU Request, Client
 2110 17.083 Central_0x46508655     LE 1M  LE LL    9  44634µs      1     1  True                  1 Control Opcode: LL_FEATURE_REQ
 2111 17.083 Peripheral_0x465086…   LE 1M  LE LL    9  150µs        1     0  False                 1 Control Opcode: LL_LENGTH_REQ
 2112 17.084 Central_0x46508655     LE 1M  ATT     11  151µs        0     0  True                  1 Sent Read By Type Request, Server
 2113 17.128 Central_0x46508655     LE 1M  ATT     11  44225µs      0     0  True                  2 Sent Read By Type Request, Server
 2114 17.128 Peripheral_0x465086…   LE 1M  LE LL    0  150µs        0     1  False                 2 Empty PDU
 2115 17.129 Central_0x46508655     LE 1M  LE LL    9  150µs        1     1  False                 2 Control Opcode: LL_LENGTH_RSP
 2116 17.173 Central_0x46508655     LE 1M  LE LL    9  44299µs      1     1  False                 3 Control Opcode: LL_LENGTH_RSP
```

```
> Frame 2111: 35 bytes on wire (280 bits), 35 bytes captured (280 bits)
> nRF Sniffer for Bluetooth LE
v Bluetooth Low Energy Link Layer
     Access Address: 0x46508655
     [Central Address: 43:03:80:18:06:e2 (43:03:80:18:06:e2)]
     [Peripheral Address: e1:b8:ad:9b:55:f2 (e1:b8:ad:9b:55:f2)]
   > Data Header
     Control Opcode: LL_LENGTH_REQ (0x14)
     Max RX octets: 251
     Max RX time: 2120 microseconds
     Max TX octets: 251
     Max TX time: 2120 microseconds
     [Response in Frame: 2115]
```

```
0000  06 1c 00 03 9c a3 06 0a  01 09 3f 01 00 c8 26 ca   ········ ··?···&·
0010  79 55 86 50 46 0b 09 14  fb 00 48 08 fb 00 48 08   yU·PF··· ··H···H·
0020  8c b6 09                                           ···
```

20231012_nokia_t20__abnormail_30bytes_switch_MTU.pcapng
Packets: 3880
Profile: Profile_nRF_Sniffer_Bluetooth_LE


20231012_nokia_t20__abnormail_30bytes_switch_MTU.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Interface Device All advertising devices Key Legacy Passkey Value Adv Hop Help Defaults Log

```
No.  Time   Source                PHY    Protoco Len Delta time (µ: SN NESN More Data Event counter Info
2105 16.970 e1:b8:ad:9b:55:f2      LE 1M  LE LL   26 498µs                                      0 ADV_IND
2106 17.014 e1:b8:ad:9b:55:f2      LE 1M  LE LL   26 43775µs                                    0 ADV_IND
2107 17.015 43:03:80:18:06:e2      LE 1M  LE LL   34 151µs                                      0 CONNECT_IND
2108 17.038 Central_0x46508655     LE 1M  LE LL    0 22944µs    0     0   False                  0 Empty PDU
2109 17.038 Peripheral_0x465086…   LE 1M  ATT      7 150µs      0     1   False                  0 Rcvd Exchange MTU Request, Client
2110 17.083 Central_0x46508655     LE 1M  LE LL    9 44634µs    1     1    True                  1 Control Opcode: LL_FEATURE_REQ
2111 17.083 Peripheral_0x465086…   LE 1M  LE LL    9 150µs      1     0   False                  1 Control Opcode: LL_LENGTH_REQ
2112 17.084 Central_0x46508655     LE 1M  ATT     11 151µs      0     0    True                  1 Sent Read By Type Request, Server
2113 17.128 Central_0x46508655     LE 1M  ATT     11 44225µs    0     0    True                  2 Sent Read By Type Request, Server
2114 17.128 Peripheral_0x465086…   LE 1M  LE LL    0 150µs      0     1   False                  2 Empty PDU
2115 17.129 Central_0x46508655     LE 1M  LE LL    9 150µs      1     1   False                  2 Control Opcode: LL_LENGTH_RSP
2116 17.173 Central_0x46508655     LE 1M  LE LL    9 44299µs    1     1   False                  3 Control Opcode: LL_LENGTH_RSP
```

```
> Frame 2115: 35 bytes on wire (280 bits), 35 bytes captured (280 bits)
> nRF Sniffer for Bluetooth LE
v Bluetooth Low Energy Link Layer
    Access Address: 0x46508655
    [Central Address: 43:03:80:18:06:e2 (43:03:80:18:06:e2)]
    [Peripheral Address: e1:b8:ad:9b:55:f2 (e1:b8:ad:9b:55:f2)]
  > Data Header
    Control Opcode: LL_LENGTH_RSP (0x15)
    Max RX octets: 251
    Max RX time: 17040 microseconds
    Max TX octets: 27
    Max TX time: 328 microseconds
    [Request in Frame: 2111]
```

```
0000  06 1c 00 03 a0 a3 06 0a  03 12 3f 02 00 84 d7 ca   ········ ··?·····
0010  79 55 86 50 46 0f 09 15  fb 00 90 42 1b 00 48 01   yU·PF··· ···B··H·
0020  82 02 ab                                           ···
```

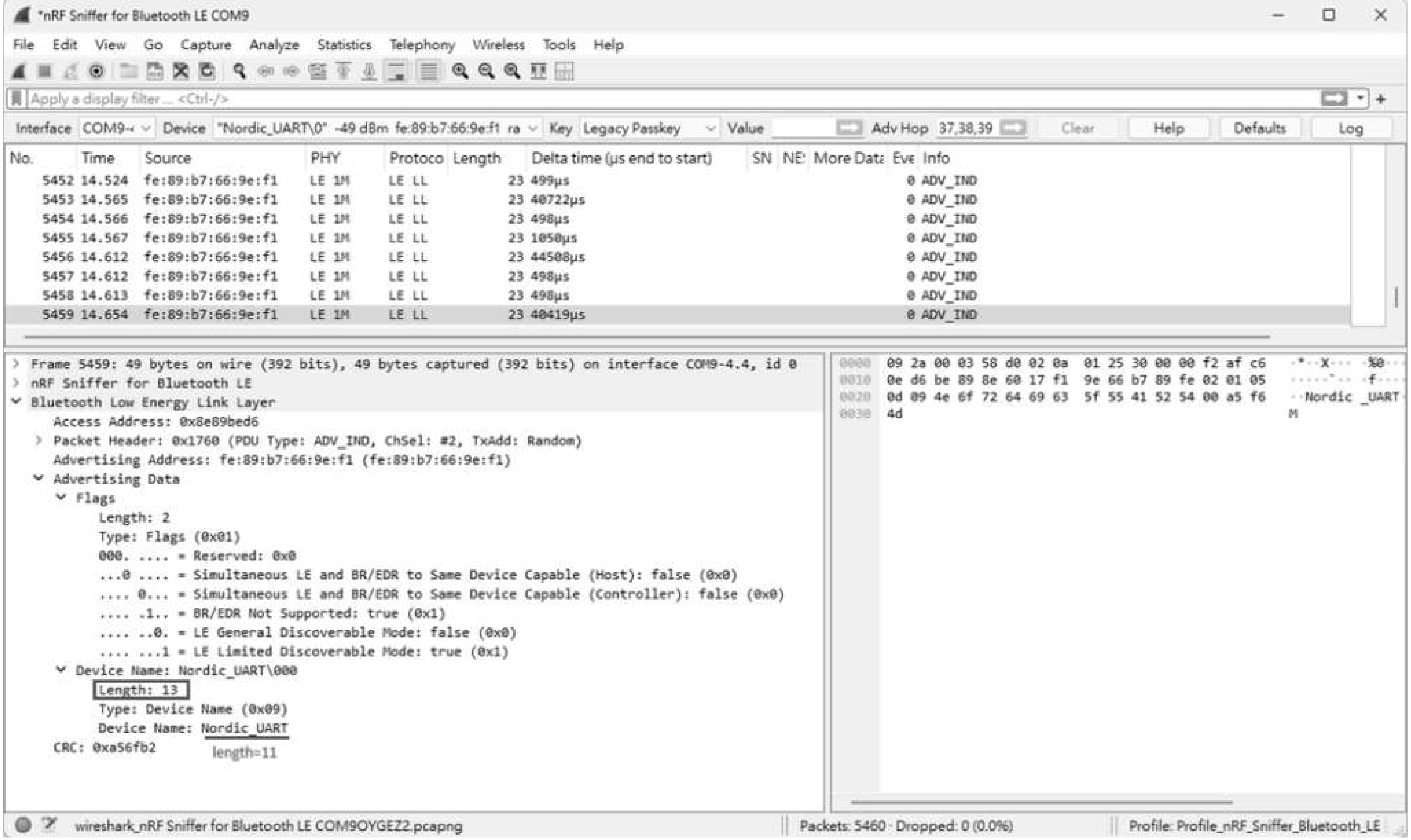
20231012_nokia_t20__abnormail_30bytes_switch_MTU.pcapng
Packets: 3880
Profile: Profile_nRF_Sniffer_Bluetooth_LE

2. Broadcast Device Name containing invisible characters:

The device could connect using a mobile app but failed to connect using Central's code.

From the sniffer interface shown below, the device name length is 11, but the Length field shows 13.

The actual data length (Type length + Device Name) = 1 + 11 = 12, indicating an issue with the program's broadcast name length.



Interface COM9-4 Device "Nordic_UART\0" -49 dBm fe:89:b7:66:9e:f1 ra Key Legacy Passkey Value Adv Hop 37,38,39

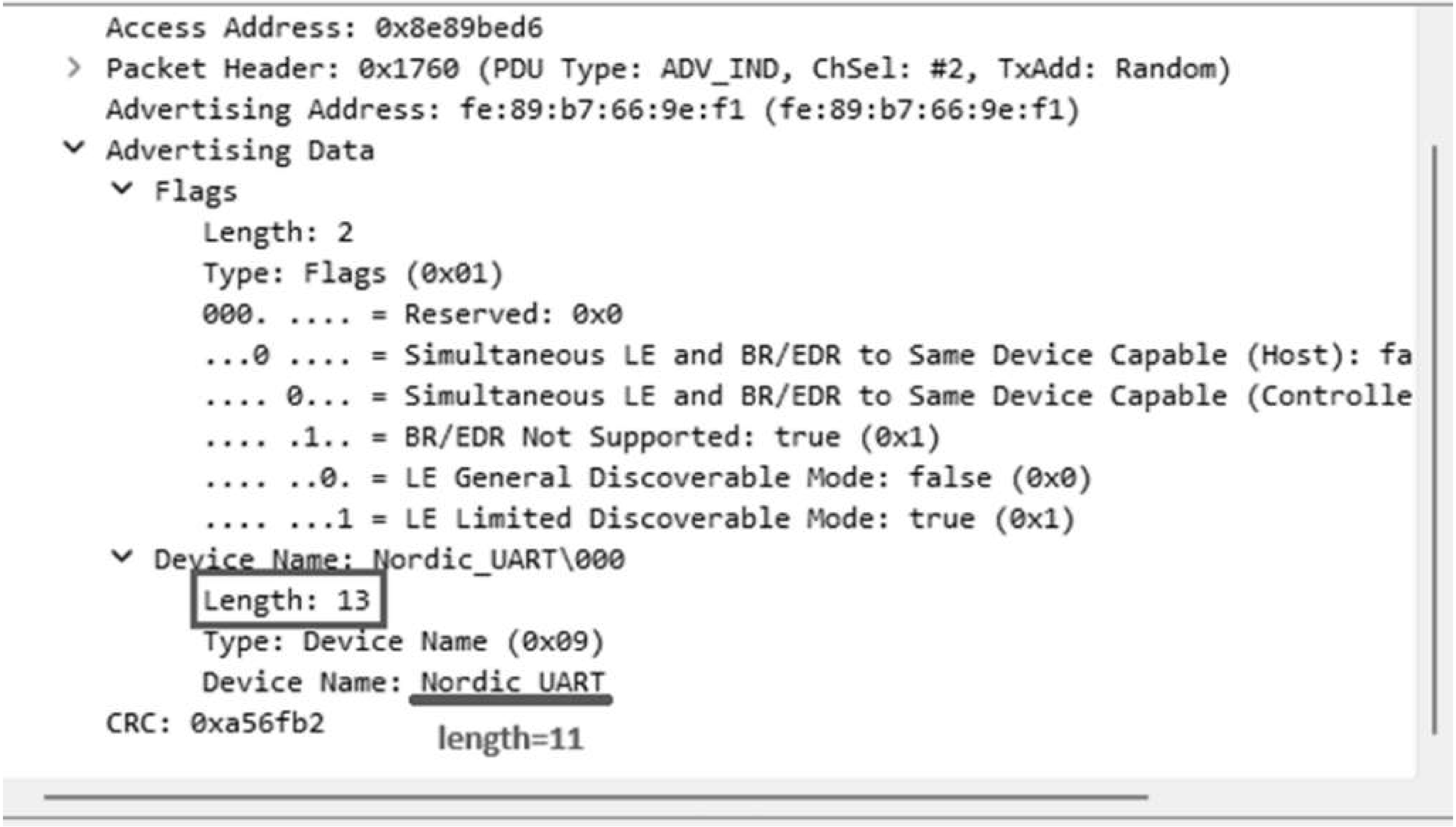
No.	Time	Source	PHY	Protoco	Length	Delta time (µs end to start)	SN	NE:	More Data	Eve	Info
5452	14.524	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	499µs				0	ADV_IND
5453	14.565	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	40722µs				0	ADV_IND
5454	14.566	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	498µs				0	ADV_IND
5455	14.567	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	1050µs				0	ADV_IND
5456	14.612	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	44508µs				0	ADV_IND
5457	14.612	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	498µs				0	ADV_IND
5458	14.613	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	498µs				0	ADV_IND
5459	14.654	fe:89:b7:66:9e:f1	LE 1M	LE LL	23	40419µs				0	ADV_IND

```
> Frame 5459: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface COM9-4.4, id 0
> nRF Sniffer for Bluetooth LE
v Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  > Packet Header: 0x1760 (PDU Type: ADV_IND, ChSel: #2, TxAdd: Random)
    Advertising Address: fe:89:b7:66:9e:f1 (fe:89:b7:66:9e:f1)
  v Advertising Data
    v Flags
        Length: 2
        Type: Flags (0x01)
        000. .... = Reserved: 0x0
        ...0 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x0)
        .... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x0)
        .... .1.. = BR/EDR Not Supported: true (0x1)
        .... ..0. = LE General Discoverable Mode: false (0x0)
        .... ...1 = LE Limited Discoverable Mode: true (0x1)
    v Device Name: Nordic_UART\000
        Length: 13
        Type: Device Name (0x09)
        Device Name: Nordic_UART
    CRC: 0xa56fb2
```

length=11

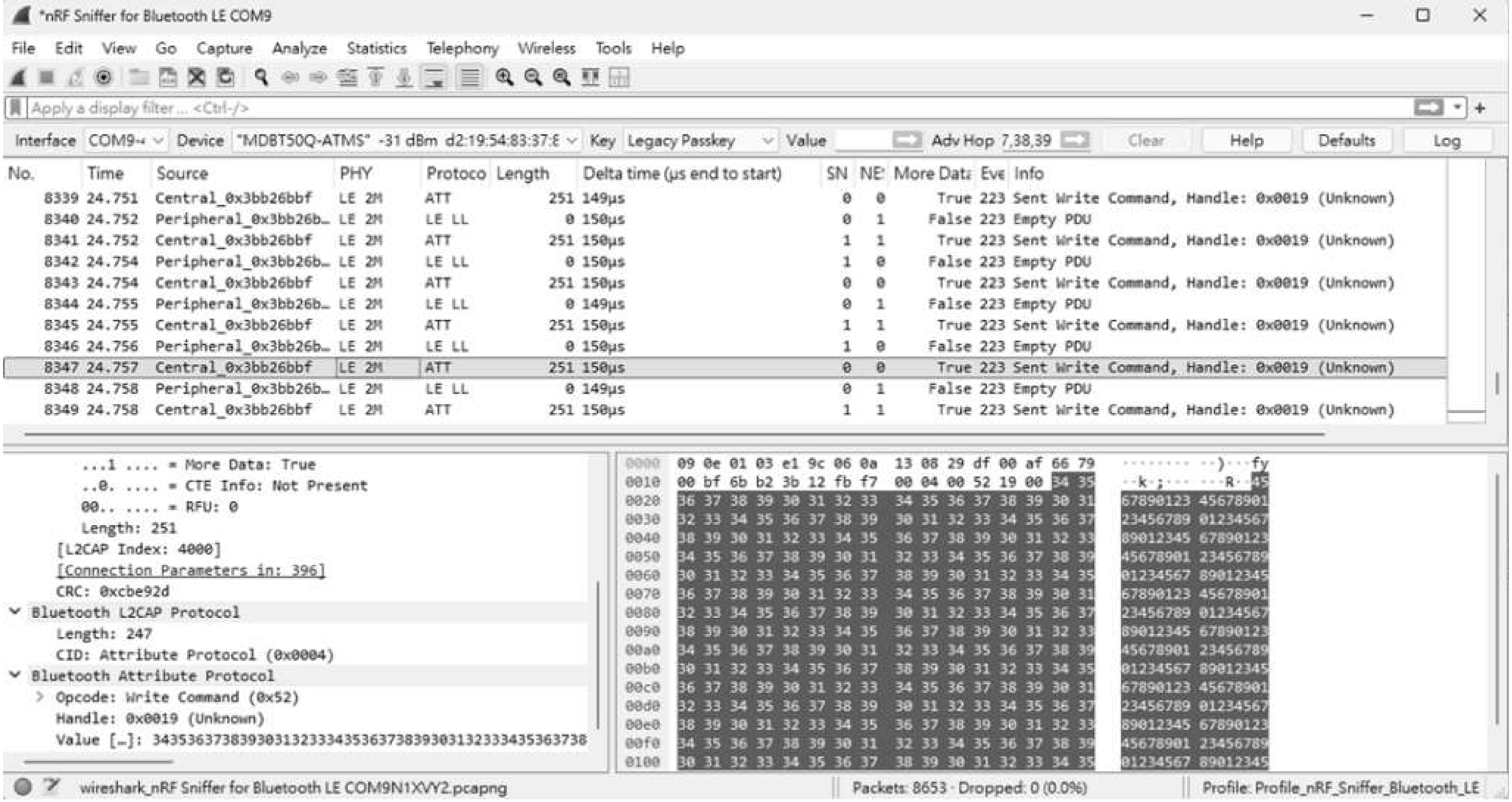
```
0000  09 2a 00 03 58 d0 02 0a  01 25 30 00 00 f2 af c6   ·*··X···  ·%0···
0010  0e d6 be 89 8e 60 17 f1  9e 66 b7 89 fe 02 01 05   ·····`··  ·f····
0020  0d 09 4e 6f 72 64 69 63  5f 55 41 52 54 00 a5 f6   ··Nordic _UART··
0030  4d                                                 M
```

wireshark_nRF Sniffer for Bluetooth LE COM9OYGEZ2.pcapng || Packets: 5460 · Dropped: 0 (0.0%) || Profile: Profile_nRF_Sniffer_Bluetooth_LE



```
    Access Address: 0x8e89bed6
  > Packet Header: 0x1760 (PDU Type: ADV_IND, ChSel: #2, TxAdd: Random)
    Advertising Address: fe:89:b7:66:9e:f1 (fe:89:b7:66:9e:f1)
  v Advertising Data
    v Flags
          Length: 2
          Type: Flags (0x01)
          000. .... = Reserved: 0x0
          ...0 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): fa
          .... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controlle
          .... .1.. = BR/EDR Not Supported: true (0x1)
          .... ..0. = LE General Discoverable Mode: false (0x0)
          .... ...1 = LE Limited Discoverable Mode: true (0x1)
    v Device Name: Nordic_UART\000
          Length: 13
          Type: Device Name (0x09)
          Device Name: Nordic UART
    CRC: 0xa56fb2
```

3. Incorrect parameter settings causing issues with throughput or packet reception:
Improper settings can lead to reduced throughput, incorrect data reception, or disconnections.
The diagram below shows a correct setup with high-volume data transmission. The Protocol Length is 251, and the data transmission intervals are consistent, achieving optimal throughput.


*nRF Sniffer for Bluetooth LE COM9
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Clear
Help
Defaults
Log

Interface COM9-- Device "MDBT50Q-ATMS" -31 dBm d2:19:54:83:37:E Key Legacy Passkey Value Adv Hop 7,38,39

```
No.  Time    Source                 PHY    Protoco Length Delta time (µs end to start)  SN NE: More Data Eve Info
8339 24.751  Central_0x3bb26bbf     LE 2M  ATT       251 149µs                          0  0   True 223 Sent Write Command, Handle: 0x0019 (Unknown)
8340 24.752  Peripheral_0x3bb26b…   LE 2M  LE LL       0 150µs                          0  1  False 223 Empty PDU
8341 24.752  Central_0x3bb26bbf     LE 2M  ATT       251 150µs                          1  1   True 223 Sent Write Command, Handle: 0x0019 (Unknown)
8342 24.754  Peripheral_0x3bb26b…   LE 2M  LE LL       0 150µs                          1  0  False 223 Empty PDU
8343 24.754  Central_0x3bb26bbf     LE 2M  ATT       251 150µs                          0  0   True 223 Sent Write Command, Handle: 0x0019 (Unknown)
8344 24.755  Peripheral_0x3bb26b…   LE 2M  LE LL       0 149µs                          0  1  False 223 Empty PDU
8345 24.755  Central_0x3bb26bbf     LE 2M  ATT       251 150µs                          1  1   True 223 Sent Write Command, Handle: 0x0019 (Unknown)
8346 24.756  Peripheral_0x3bb26b…   LE 2M  LE LL       0 150µs                          1  0  False 223 Empty PDU
8347 24.757  Central_0x3bb26bbf     LE 2M  ATT       251 150µs                          0  0   True 223 Sent Write Command, Handle: 0x0019 (Unknown)
8348 24.758  Peripheral_0x3bb26b…   LE 2M  LE LL       0 149µs                          0  1  False 223 Empty PDU
8349 24.758  Central_0x3bb26bbf     LE 2M  ATT       251 150µs                          1  1   True 223 Sent Write Command, Handle: 0x0019 (Unknown)
```

```
        ...1 .... = More Data: True
        ..0. .... = CTE Info: Not Present
        00.. .... = RFU: 0
        Length: 251
    [L2CAP Index: 4000]
    [Connection Parameters in: 396]
    CRC: 0xcbe92d
˅ Bluetooth L2CAP Protocol
    Length: 247
    CID: Attribute Protocol (0x0004)
˅ Bluetooth Attribute Protocol
  > Opcode: Write Command (0x52)
    Handle: 0x0019 (Unknown)
    Value […]: 34353637383930313233343536373839303132333435363738
```

```
0000  09 0e 01 03 e1 9c 06 0a  13 08 29 df 00 af 66 79   ·········  ··)···fy
0010  00 bf 6b b2 3b 12 fb f7  00 04 00 52 19 00 34 35   ··k·;··· ···R··45
0020  36 37 38 39 30 31 32 33  34 35 36 37 38 39 30 31   67890123 45678901
0030  32 33 34 35 36 37 38 39  30 31 32 33 34 35 36 37   23456789 01234567
0040  38 39 30 31 32 33 34 35  36 37 38 39 30 31 32 33   89012345 67890123
0050  34 35 36 37 38 39 30 31  32 33 34 35 36 37 38 39   45678901 23456789
0060  30 31 32 33 34 35 36 37  38 39 30 31 32 33 34 35   01234567 89012345
0070  36 37 38 39 30 31 32 33  34 35 36 37 38 39 30 31   67890123 45678901
0080  32 33 34 35 36 37 38 39  30 31 32 33 34 35 36 37   23456789 01234567
0090  38 39 30 31 32 33 34 35  36 37 38 39 30 31 32 33   89012345 67890123
00a0  34 35 36 37 38 39 30 31  32 33 34 35 36 37 38 39   45678901 23456789
00b0  30 31 32 33 34 35 36 37  38 39 30 31 32 33 34 35   01234567 89012345
00c0  36 37 38 39 30 31 32 33  34 35 36 37 38 39 30 31   67890123 45678901
00d0  32 33 34 35 36 37 38 39  30 31 32 33 34 35 36 37   23456789 01234567
00e0  38 39 30 31 32 33 34 35  36 37 38 39 30 31 32 33   89012345 67890123
00f0  34 35 36 37 38 39 30 31  32 33 34 35 36 37 38 39   45678901 23456789
0100  30 31 32 33 34 35 36 37  38 39 30 31 32 33 34 35   01234567 89012345
```

wireshark_nRF Sniffer for Bluetooth LE COM9N1XVY2.pcapng | Packets: 8653 · Dropped: 0 (0.0%) | Profile: Profile_nRF_Sniffer_Bluetooth_LE

Summary

Mastering hardware and software setups and effectively using packet analysis tools can boost development efficiency and enable high-performance Bluetooth applications.

Resources:
https://www.nordicsemi.com/Products/Development-tools/nRF-Sniffer-for-Bluetooth-LE
(https://www.nordicsemi.com/Products/Development-tools/nRF-Sniffer-for-Bluetooth-LE)
https://docs.nordicsemi.com/bundle/nrfutil_ble_sniffer_pdf/resource/nRF_Sniffer_BLE_UG_v4.0.0.pdf

(https://docs.nordicsemi.com/bundle/nrfutil_ble_sniffer_pdf/resource/nRF_Sniffer_BLE_UG_v4.0.0.pdf)
https://www.wireshark.org/download.html (https://www.wireshark.org/download.html)

User manual:
https://raytac.blog/2024/07/10/firmware-coding-dfu-onto-mdbt50q-rxuser-manual-of-mdbt50q-cx-nrf52840-usb-c-dongle/
(https://raytac.blog/2024/07/10/firmware-coding-dfu-onto-mdbt50q-rxuser-manual-of-mdbt50q-cx-nrf52840-usb-c-dongle/)

Edited by Business Development Manager: Mr. Tony Yin
Technical guidance provided by R&D Manager: Mr. Stanley Huang

Raytac Corporation 勁達國際電子股份有限公司
A Bluetooth, Wi-Fi, and LoRa Module Maker based on
Nordic nRF54; nRF53: nRF52; nRF51; nRF7002
Semtech Specification: SX1262

Bluetooth Specification: BT6.0 ; BT5.4 ; BT5.3 ; BT5.2.
Wi-Fi Specification: Wi-Fi 6
LoRa Specification: LoRaWAN

All products are FCC/IC/CE/Telec/KC/RCM/SRRC/NCC/WPC Pre-Certified.
http://www.raytac.com (http://www.raytac.com/)
email: sales@raytac.com (mailto:sales@raytac.com)
Tel: +886-2-3234-0208