How to do BLE Packet Sniffing using nRF Sniffer for Bluetooth LE

(2020.04.03)

Version 1.1.2

해당 문서는 **MasterLock**의 원활한 기술 지원을 위해 INSEM에서 제공하는 문서이므로
MasterLock 이외의 다른 용도로 사용이 금지 됩니다

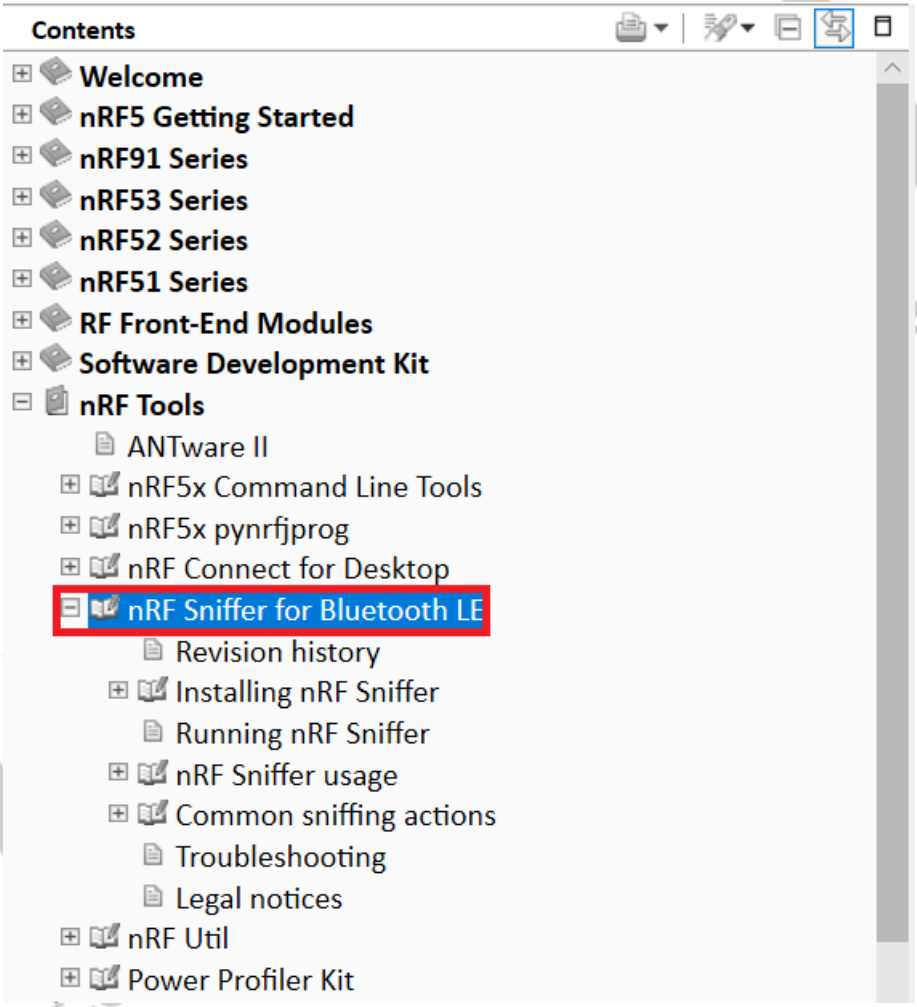
Contents

1. Inroduction

이 문서는 nRF Sniffer 를 이용하여 BLE packet sniffing 을 테스트 하기 위한 brief guide 문서입니다.

nRF Sniffer for Bluetooth LE 에 대한 자세한 설명은 Nordic inforcenter 에서 아래 부분을 참조 부탁드립니다.

https://infocenter.nordicsemi.com/topic/ug_sniffer_ble/UG/sniffer_ble/intro.html



2. Prerequisites

Software Development Environment : Segger Embedded Studio
Software Development Kit : nRF5 SDK v16.0.0
Tested EVK: nRF52840 DK, nRF52 DK
Example Project : ble_app_hrs(peripheral)
App : nRF Toolbox
PC GUI : nRF Connect on Desktop or laptop

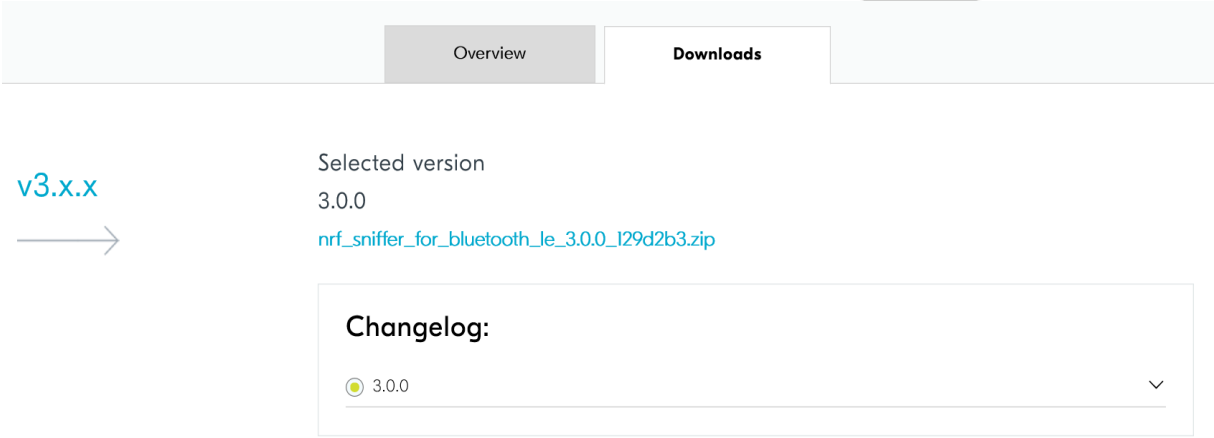
2 개의 EVK 가 필요합니다.
1 개의 EVK 는 PC 에 설치될 Wireshark PC program 에서 BLE packet sniffing 으로 사용하며 다른 1 개는 BLE peripheral 장치로 사용합니다.

nRF Toolbox Smatphone App 과 BLE peripheral 장치 간의 advertising 혹은 connection 전후의 BLE packet sniffing 을 테스트 진행 합니다.

3. How to do BLE packet sniffing using nRF Sniffer for Bluetooth LE

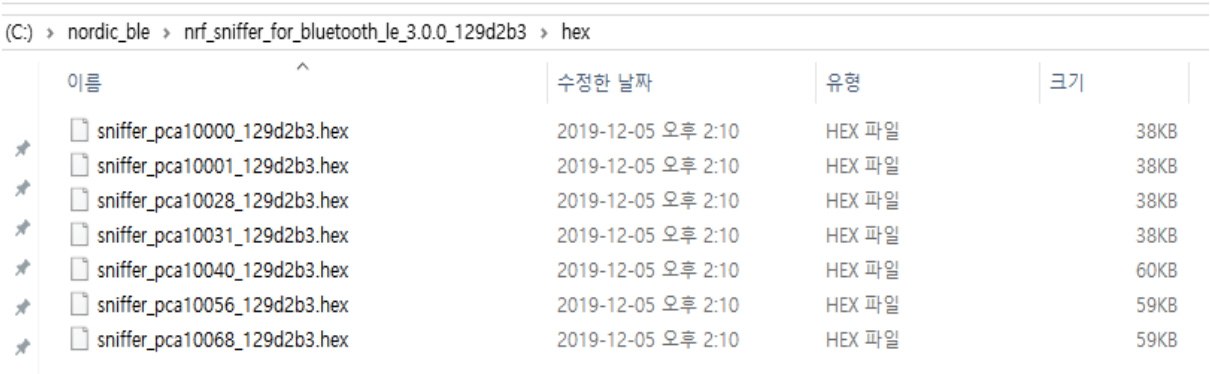
BLE Packet Sniffing 사용하기 위해서는 EVK 에 program 되어야 하는 firmware 와 WireShark 라는 detected data analyzing PC GUI 가 필요합니다. 우선 노르딕 홈페이지에서 nRF Sniffer for Bluetooth LE 를 download 받습니다.

https://www.nordicsemi.com/Software-and-tools/Development-Tools/nRF-Sniffer-for-Bluetooth-LE/Download#infotabs

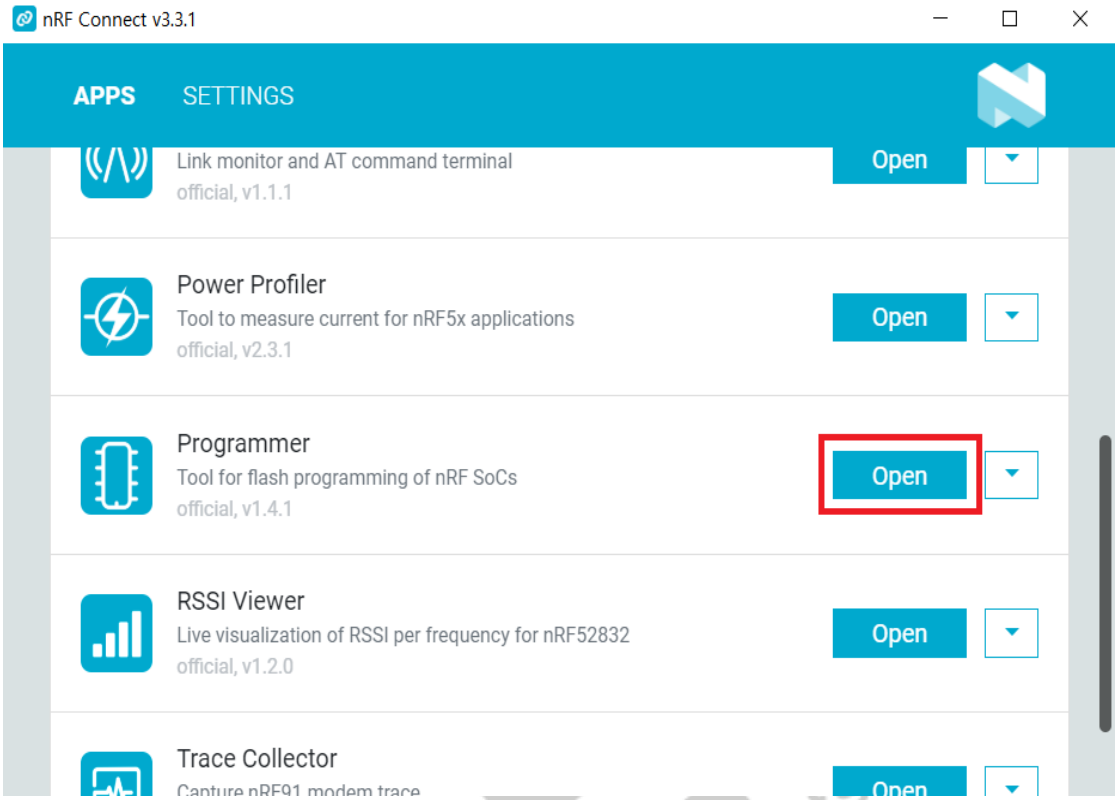


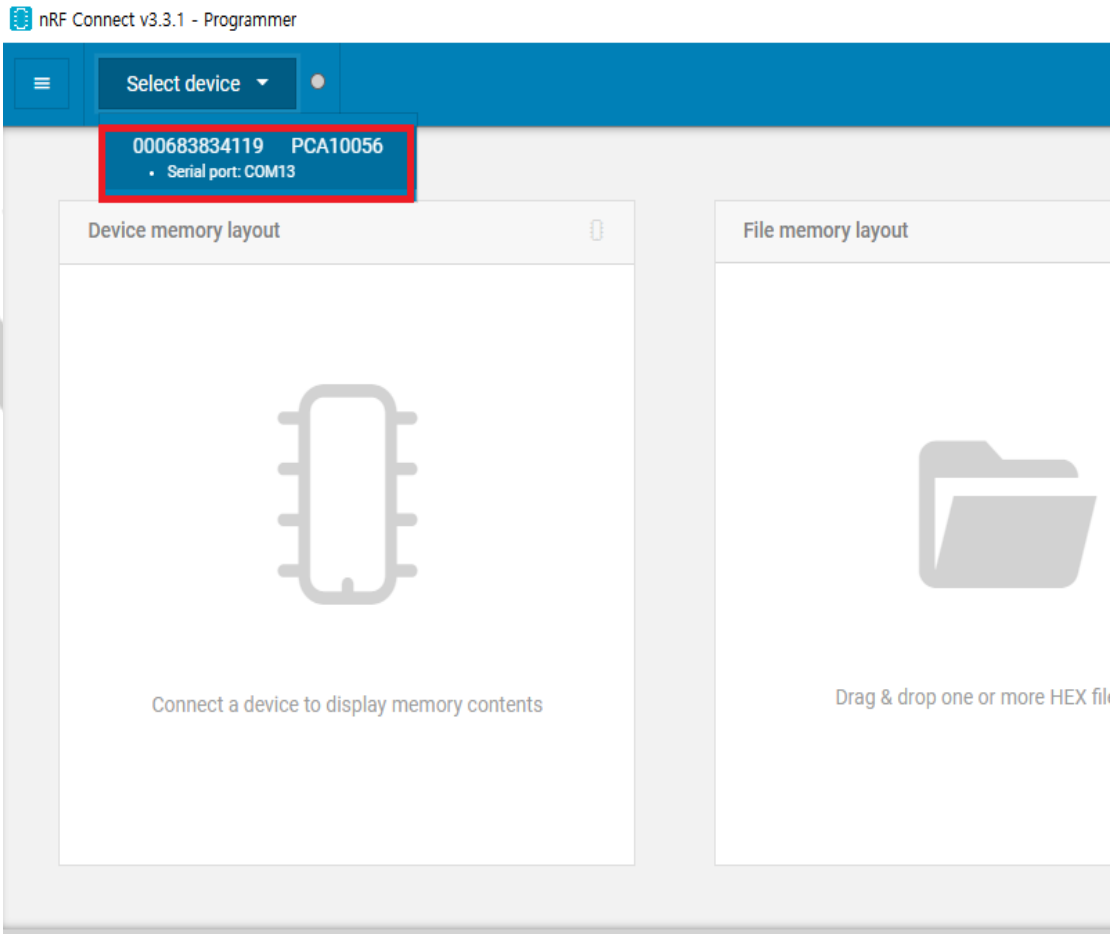
위에서 download 받은 nRF Sniffer for Bluetooth LE 파일을 압축해제 하시면 아래의 폴더 구조를 확인할 수 있습니다.

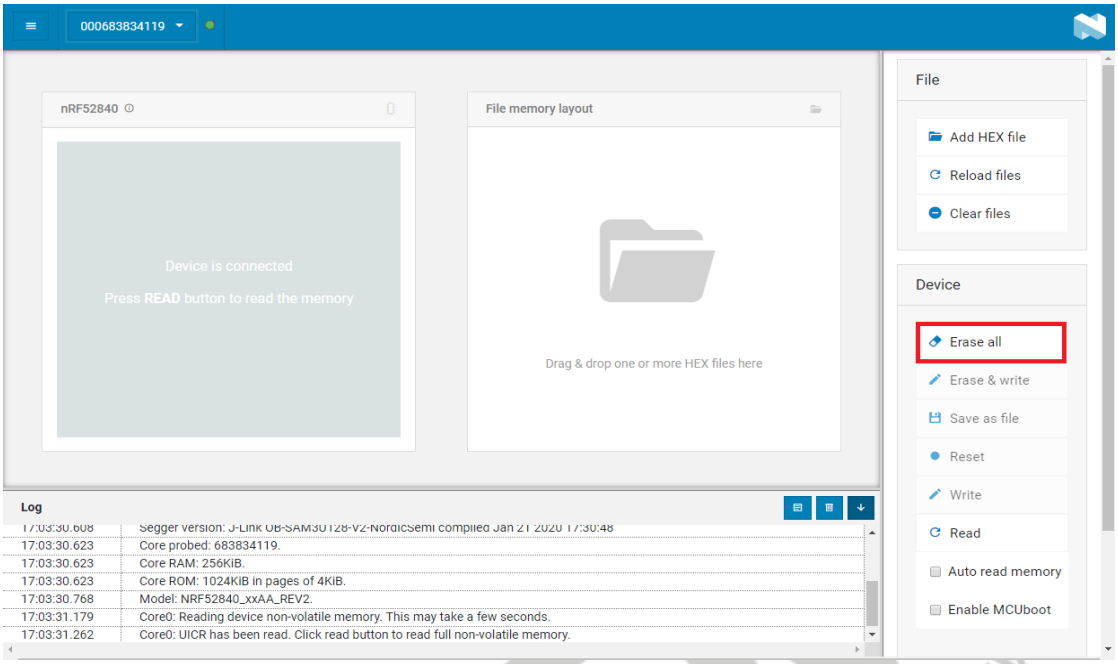
<Unzip Folder>\hex\

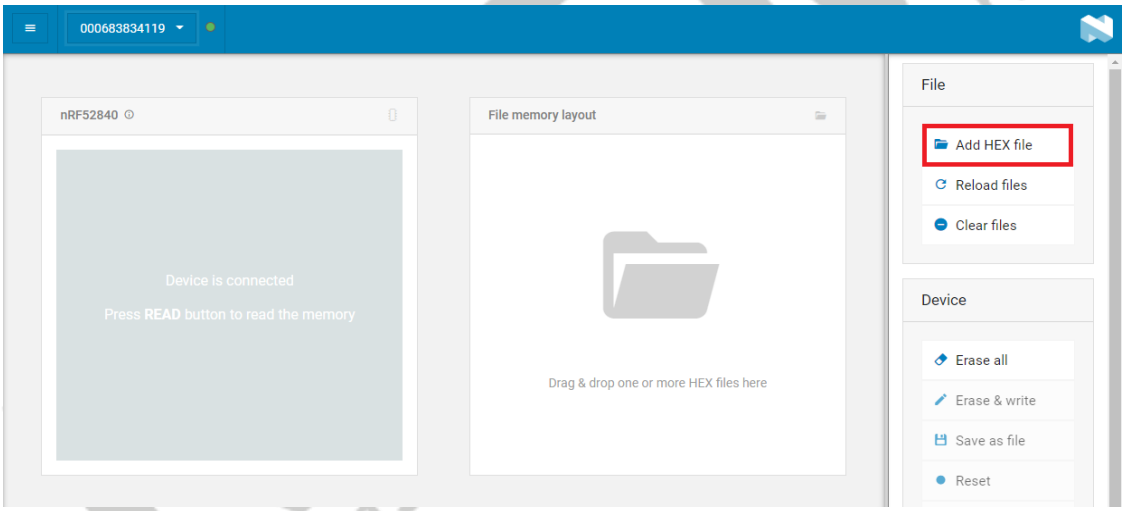


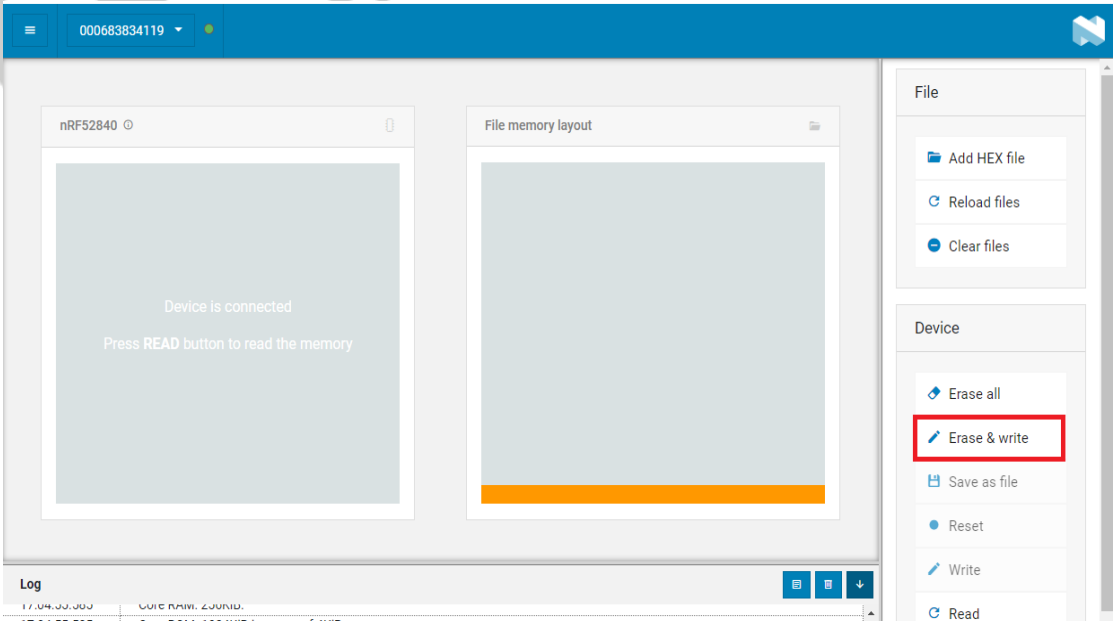
준비된 EVK 중에서 nRF52840 DK 를 Snffing 용도로 사용하려고 합니다. nRF Connect PC GUI 를 이용하여 erase 및 write 를 진행합니다.(sniffer_pca10056_129d2b3.hex)


nRF Connect v3.3.1
APPS
SETTINGS
Link monitor and AT command terminal
official, v1.1.1
Open
Power Profiler
Tool to measure current for nRF5x applications
official, v2.3.1
Open
Programmer
Tool for flash programming of nRF SoCs
official, v1.4.1
Open
RSSI Viewer
Live visualization of RSSI per frequency for nRF52832
official, v1.2.0
Open
Trace Collector
Open


nRF Connect v3.3.1 - Programmer
Select device
000683834119 PCA10056
Serial port: COM13
Device memory layout
File memory layout
Connect a device to display memory contents
Drag & drop one or more HEX fil







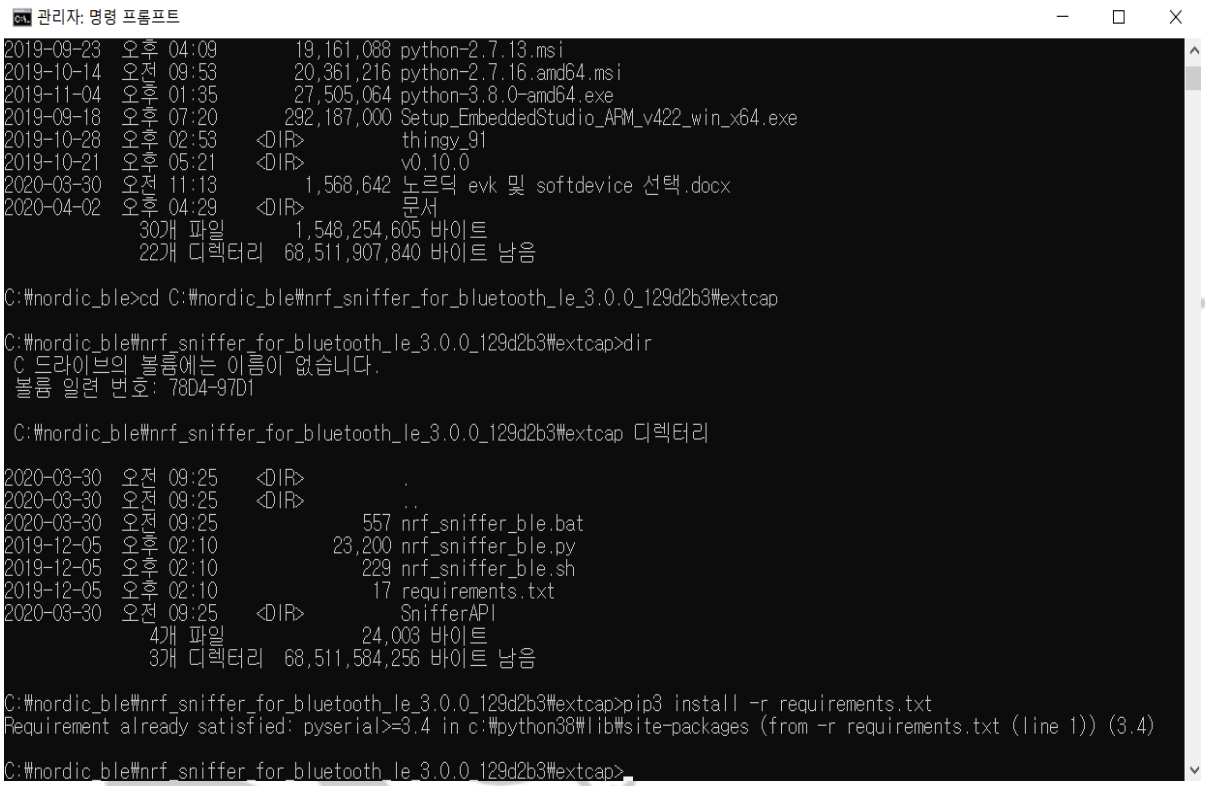
위의 작업을 수행 하신후 python requirements 를 install 합니다.

먼저 노르딕 홈페이지에서 download 받은 nRF Sniffer for Bluetooth LE 내의 subfolder 를 보면 아래 folder 를 확인하실 수 있습니다.

<Unzip Folder>\extcap\

Windows cmd 창을 활성화 시키신 후 위 폴더에서 다음의 python 명령을 수행합니다.

pip3 install –r requirements.txt

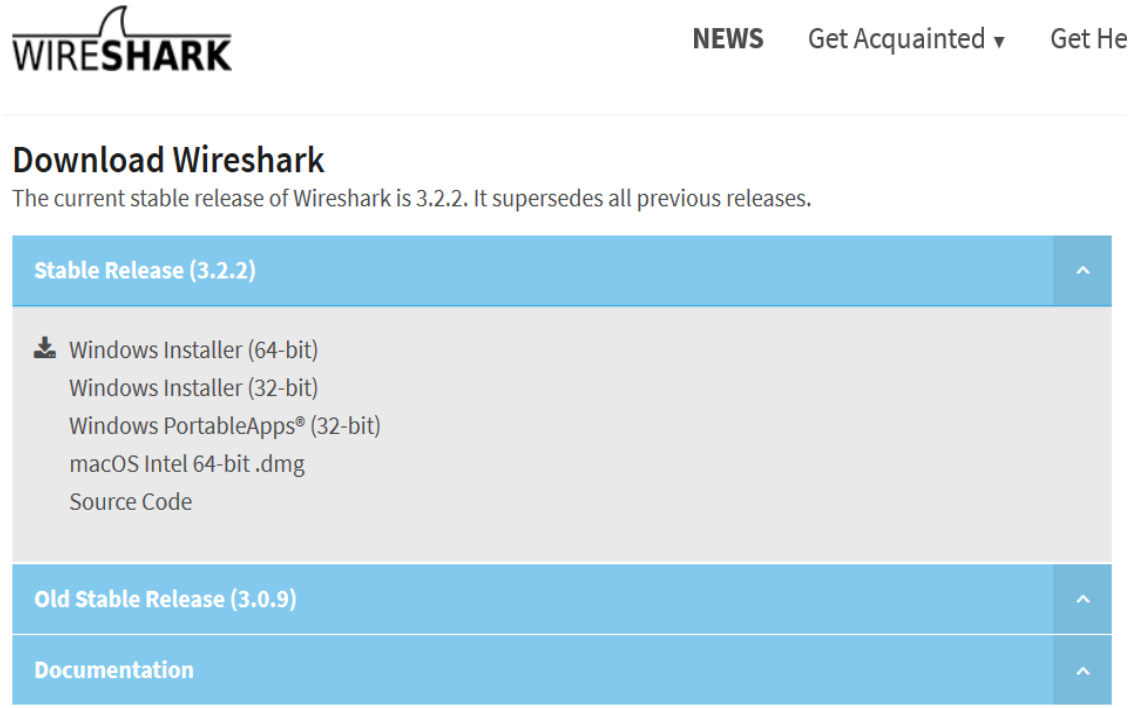


python 을 설치하지 않으신 경우에는 python 3.6 이상을 PC 에 설치 부탁드립니다.

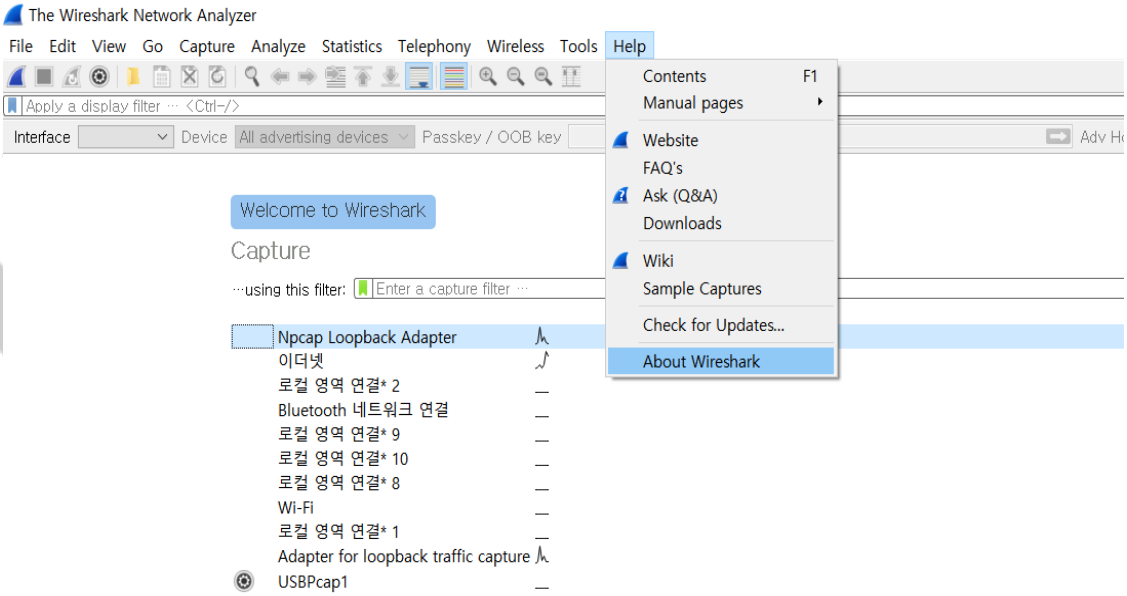
https://www.python.org/downloads/

다음은 WireShark 프로그램 설치 후 setup 과정을 진행합니다.

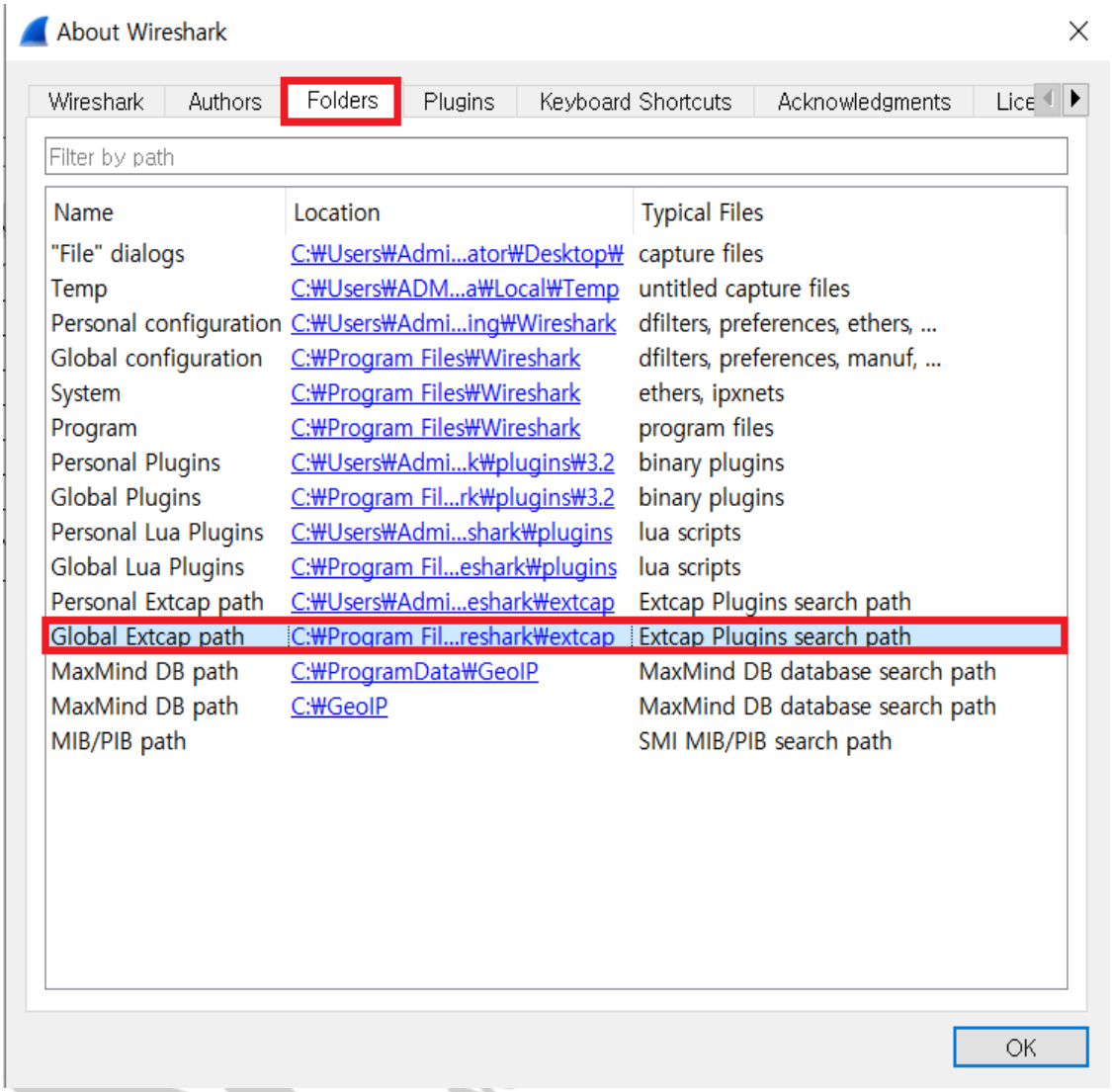
https://www.wireshark.org/download.html



설치 완료 후 WireShark 를 실행합니다. 화면 상단의 Help>About WireShark 를 선택합니다.

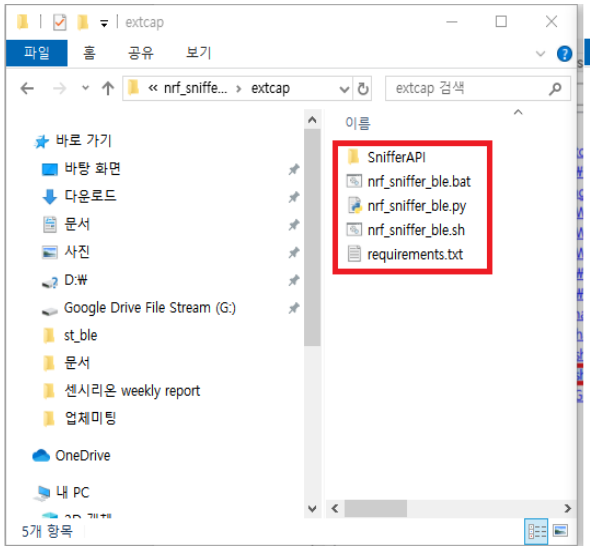


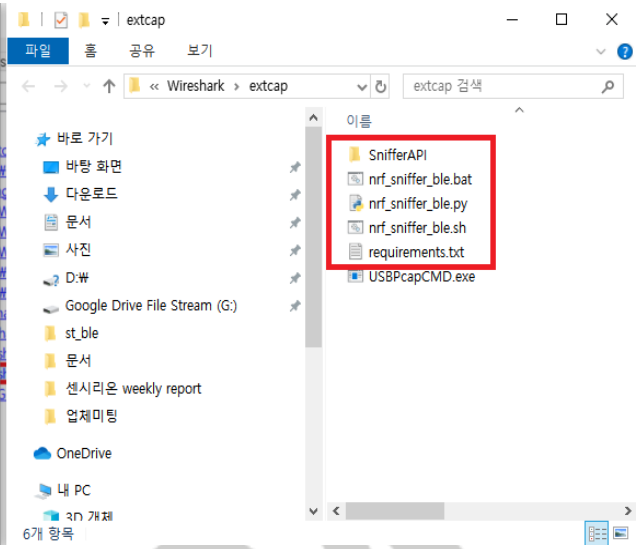
Folders 를 선택하신 후 Global Extcap path 를 double click 합니다.



Double click 후 창에 나오는 folder 에 download 받았었던 nRF Sniffer for Bluetooth LE 의 아래 폴더의 파일들을 copy 해서 위치 시킵니다.

<Unzip Folder>\extcap\





위에서 copy 한 sniffer 파일들이 정상적으로 동작할 수 있는지 확인을 해줘야 합니다. Windows cmd 창을 이용하여 아래 명령어를 실행시킵니다.

nrf_sniffer_ble.bat --extcap-interfaces

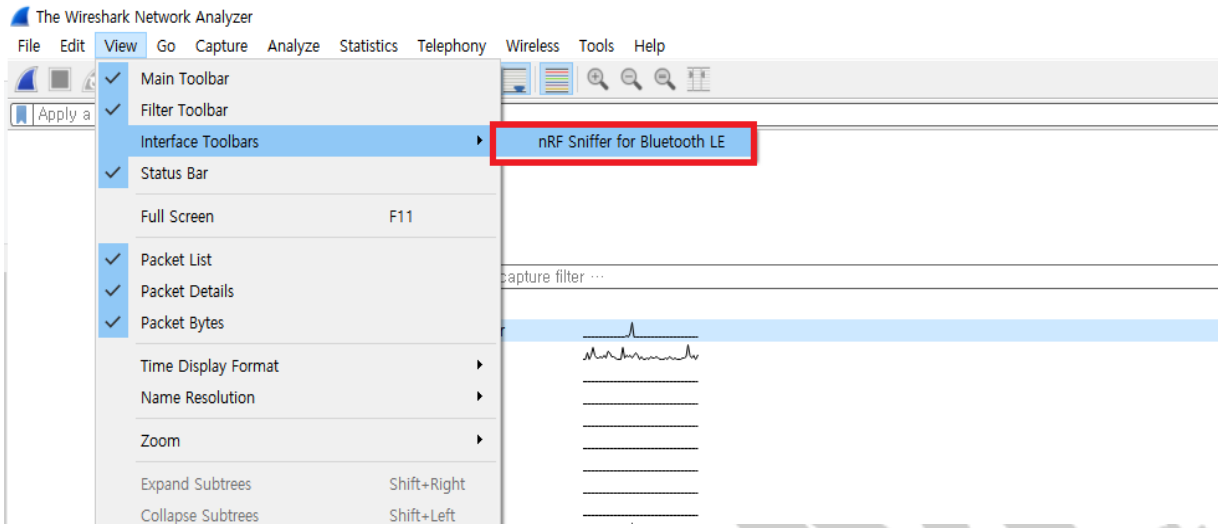
아래 폴더로 이동하셔서 진행합니다.

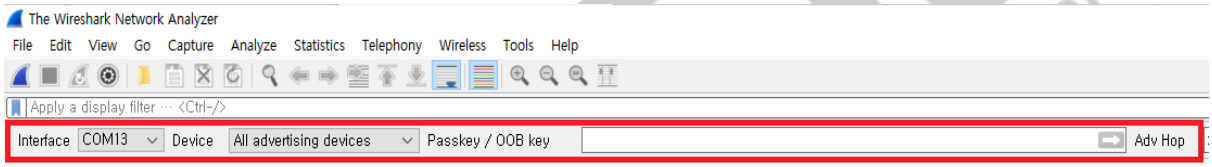
C:\Program Files\Wireshark\extcap

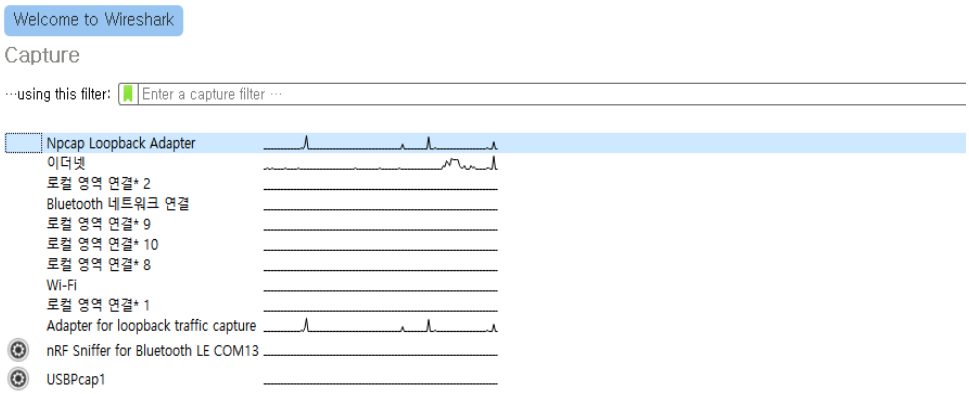
관리자: 명령 프롬프트

```
C:₩Program Files₩Wireshark₩extcap>nrf_sniffer_ble.bat --extcap-interfaces
extcap {version=3.0.0}{display=nRF Sniffer for Bluetooth LE}{help=https://www.nordicsemi.co
t-Tools/nRF-Sniffer-for-Bluetooth-LE}
control {number=0}{type=selector}{display=Device}{tooltip=Device list}
control {number=1}{type=string}{display=Passkey / OOB key}{tooltip=6 digit temporary key or
in hexadecimal starting with '0x', big endian format. If the entered key is shorter than 16
in front'}{validation=₩b^(([0-9]{6})|(0x[0-9a-fA-F]{1,32}))$₩b}
control {number=2}{type=string}{display=Adv Hop}{default=37,38,39}{tooltip=Advertising chan
der in which the siffer switches advertising channels. Valid channels are 37, 38 and 39 sep
s*((37|38|39)₩s*,₩s*){0,2}(37|38|39){1}₩s*$}{required=true}
control {number=3}{type=button}{role=help}{display=Help}{tooltip=Access user guide (launche
control {number=4}{type=button}{role=restore}{display=Defaults}{tooltip=Resets the user int

control {number=5}{type=button}{role=logger}{display=Log}{tooltip=Log per interface}
value {control=0}{value= }{display=All advertising devices}{default=true}

C:₩Program Files₩Wireshark₩extcap>
```

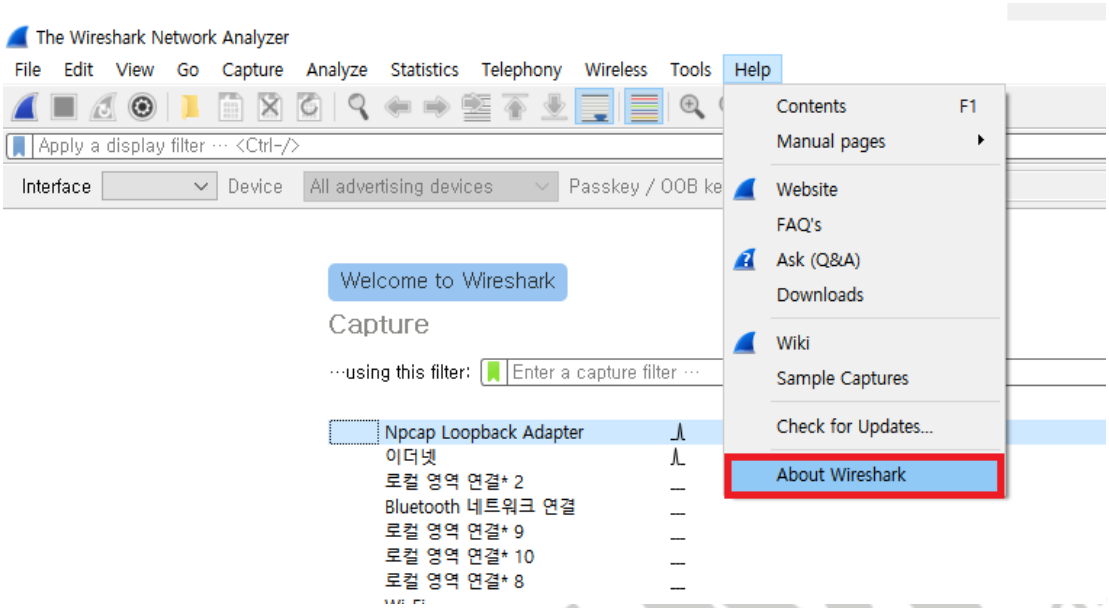
다음은 WireShark 에서 Sniffer interface 를 enable 합니다.



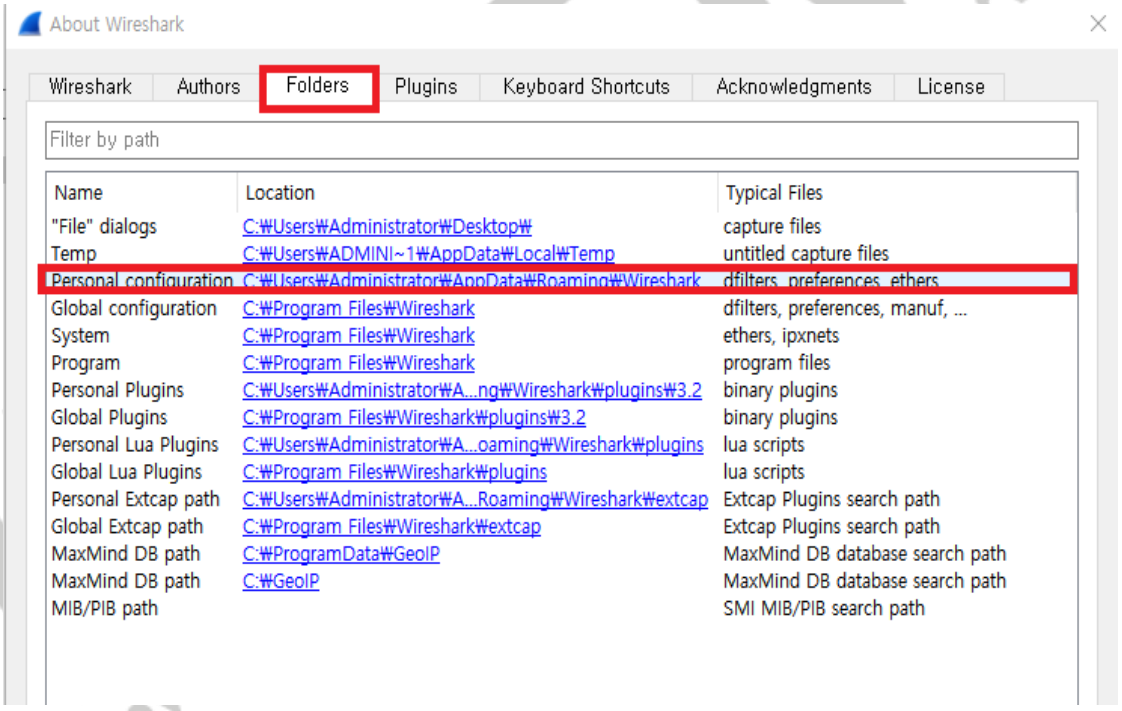




다음은 WireShark profile for nRF sniffer 를 추가 합니다.



Personal configuration 항목을 double click 합니다.

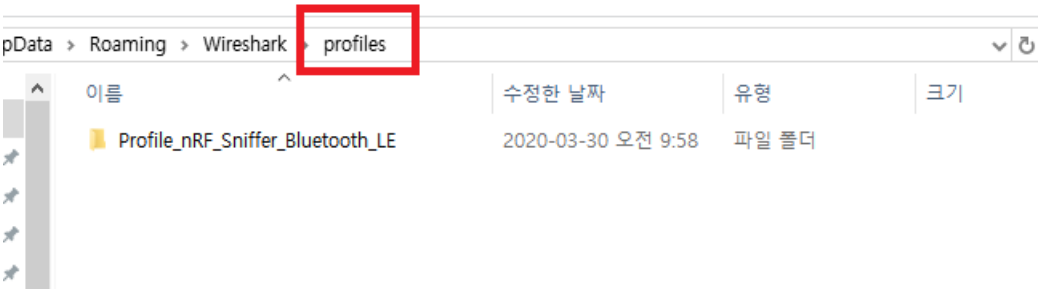


창에 나오는 folder 의 subfolder 에 download 받았었던 nRF Sniffer for Bluetooth LE 의 아래 폴더를 copy 해서 위치 시킵니다.

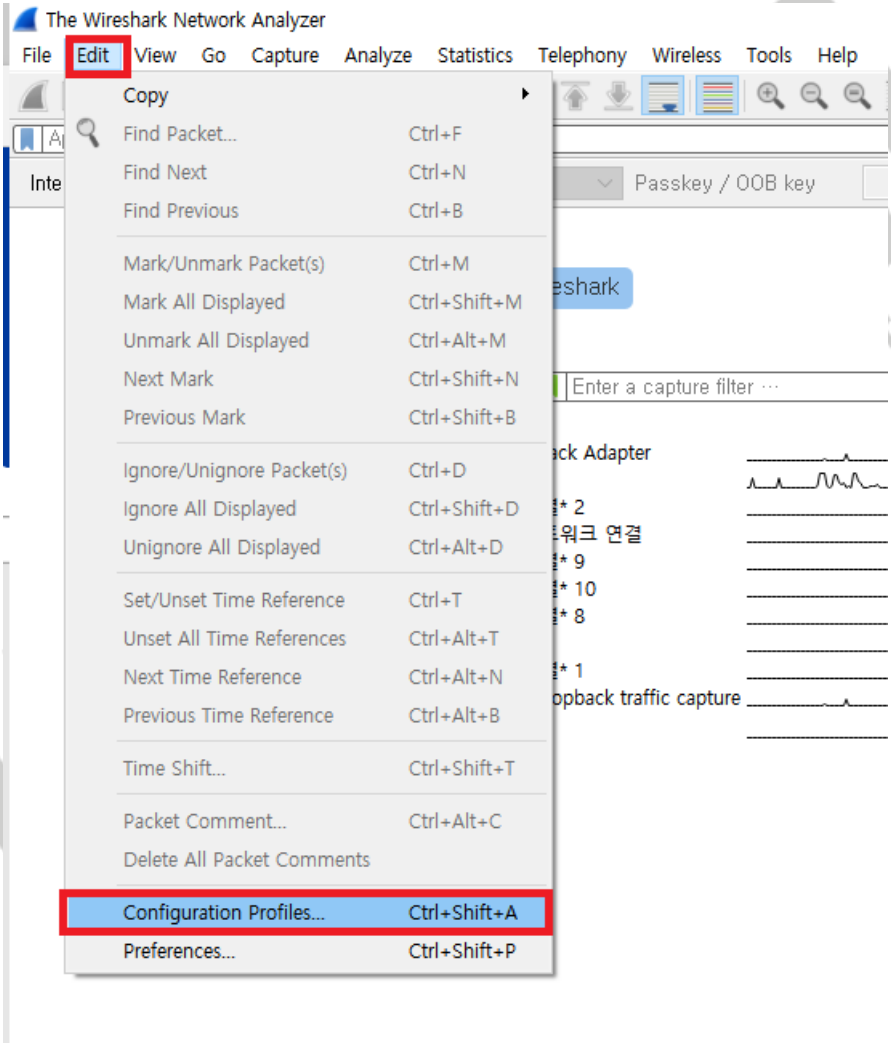
<Unzip Folder>\ Profile_nRF_Sniffer_Bluetooth_LE

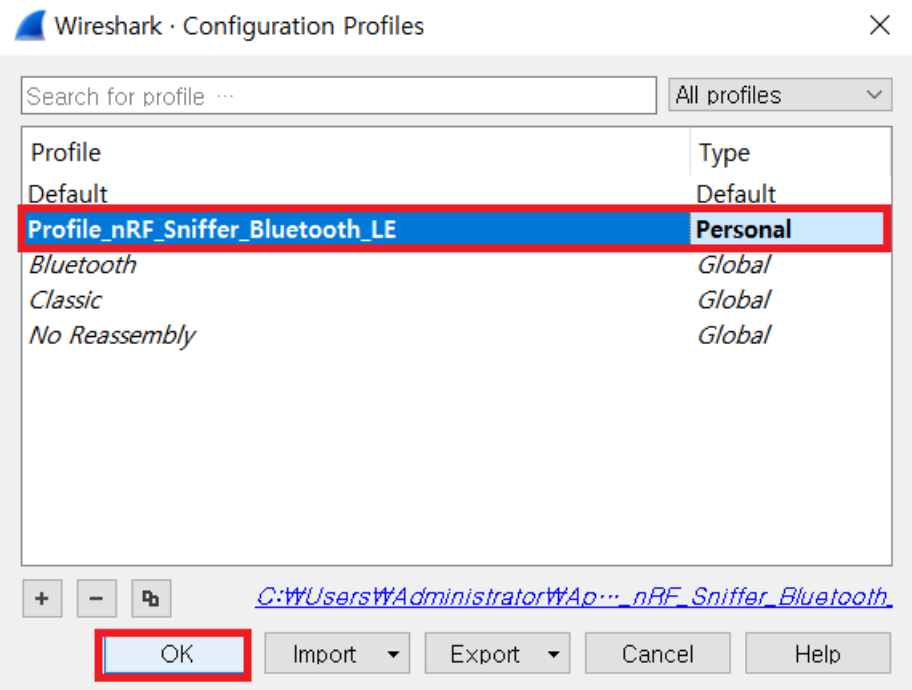
폴더는 아래와 같습니다.

..\profiles\ Profile_nRF_Sniffer_Bluetooth_LE



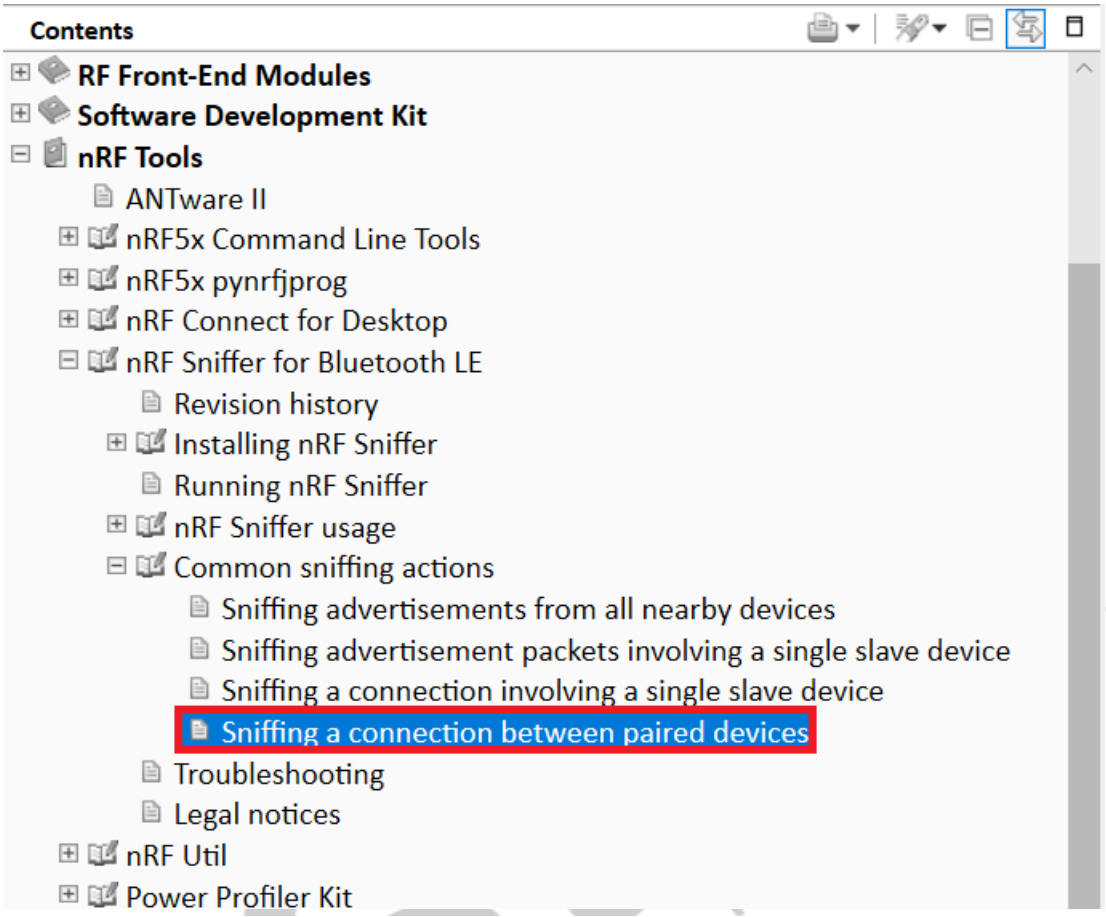
다음은 WireShark 에서 profile 을 선택합니다.





Wireshark 설정까지 끝났기 때문에 BLE packet sniffing 을 위한 BLE peripheral 장치를 준비해야 합니다. 준비한 다른 1 개의 EVK 에 ble_hrs_app 를 program 합니다.
이 부분은 개발자 분들이 노르딕 EVK 으로 program / run 하시는 방법을 아실 것이라는 판단에 skip 하도록 하겠습니다.

Tip:BLE peripheral, Nordic nRF Toolbox 간의 connection 이 발생한 후의 data packet 도 sniffing 하기 위해서는 반드시 확인해야 할 부분이 있습니다. 아래 링크에서 관련내용을 참조 부탁드립니다.



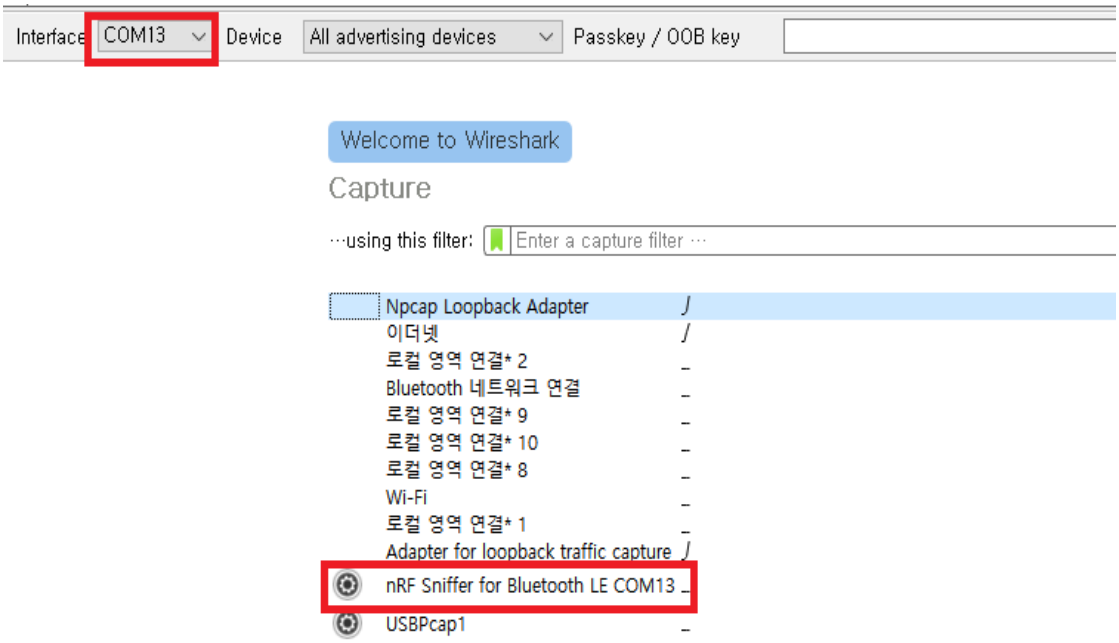
1. Run nRF Sniffer (if not already running).
2. Select your device from the device list.
3. Enter the credentials for pairing. The procedure depends on the type of encryption.
   - For connections that use legacy pairing with Just Works:
     a. Initiate pairing between the devices if it does not happen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

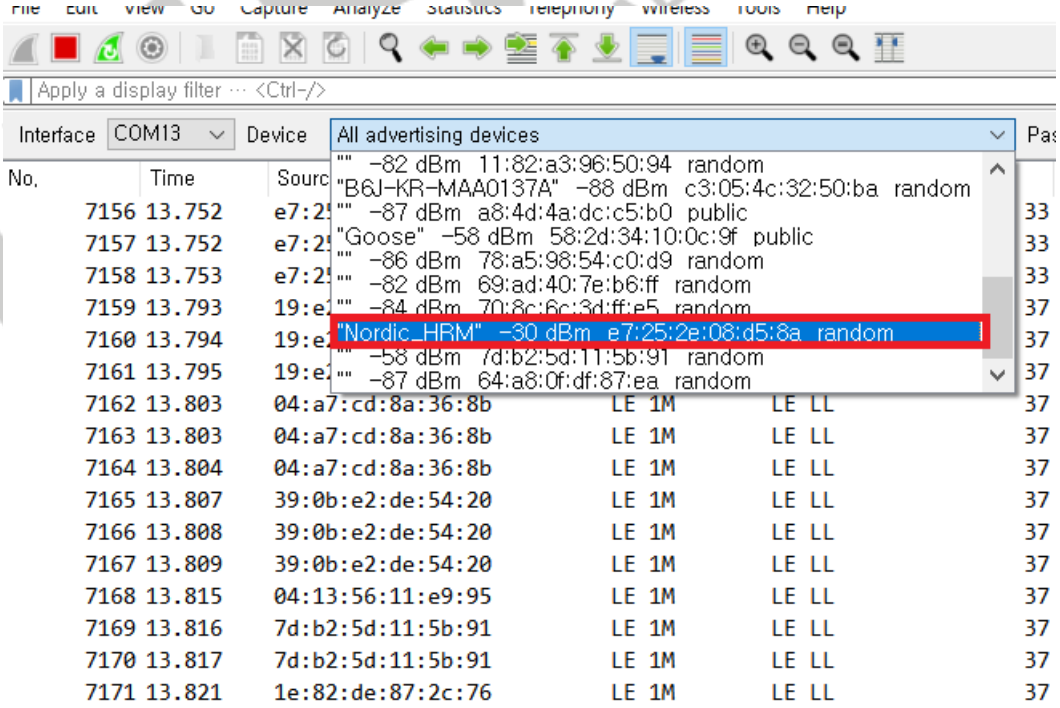
WireShark 설정이 완료되었으므로 실제 WireShark 를 이용한 advertising packet, data packet sniffing 을 테스트 하도록 하겠습니다.

WireShark 를 다시 실행하면 아래 항목을 확인하실 수 있습니다.



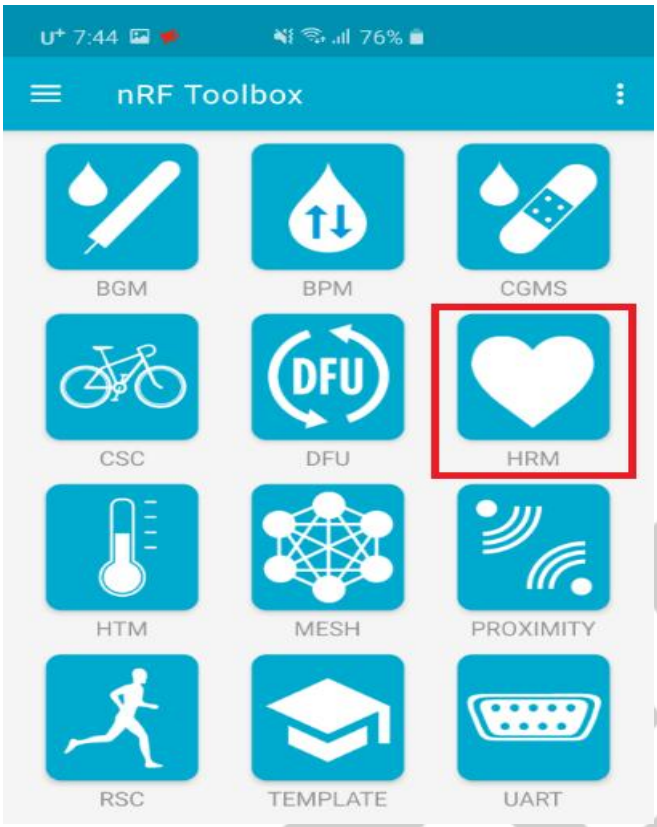
PC 의 COM port 로 sniffing 동작을 수행하는 EVK 이 연결된 경우 위처럼 화면에 표시되며 nRF Sniffer for Bluetooth LE 를 double click 합니다.

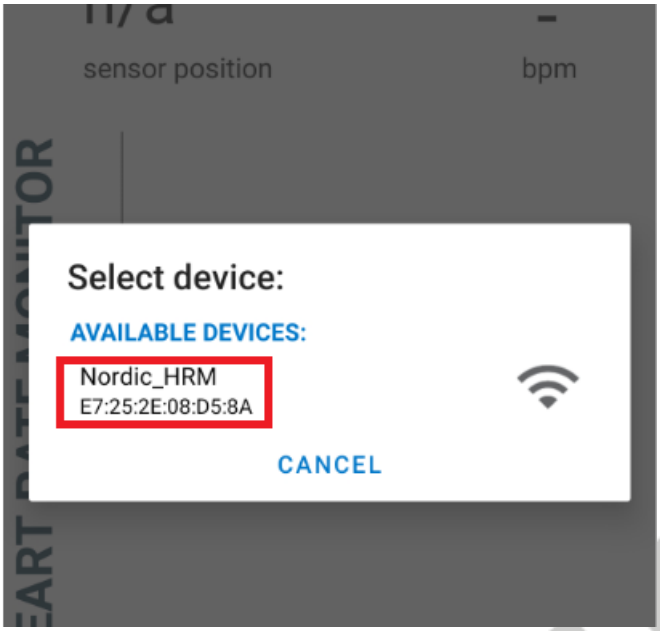
주변의 BLE advertising data 를 모두 sniffing 하기 때문에 sniffing 을 진행하고자 하는 device 를 선택합니다.

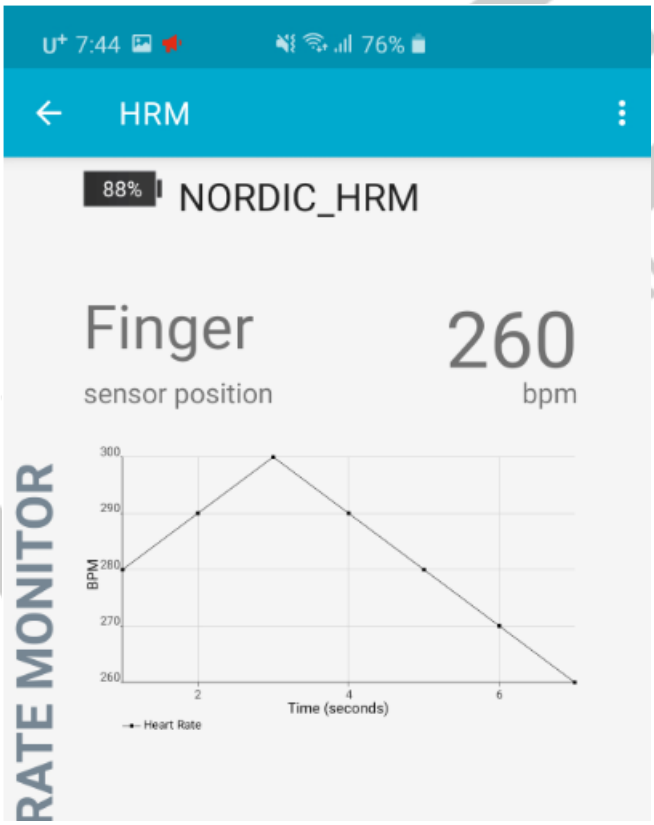


위와 같이 선택하면 선택한 device 에 대한 BLE advertising packet 및 connection 된 후의 BLE data packet 을 sniffing 할 수 있습니다.

Advertising pacekt 을 확인 할 수 있으니 connection 후의 data packet 을 확인하시려면 nRF ToolBox app 으로 device 를 connection 진행하시면 됩니다.







<Appendix>

1. BLE Packet types

WireShark tool 을 이용하여 packet sniffing 을 진행한 후 packet 에 대한 분석이 필요하여 관련 packet 에 대한 information 을 간략하게 추가합니다.

>>BLE Packet 구성

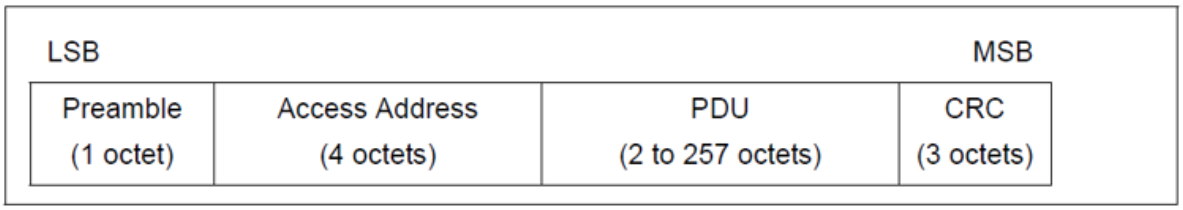
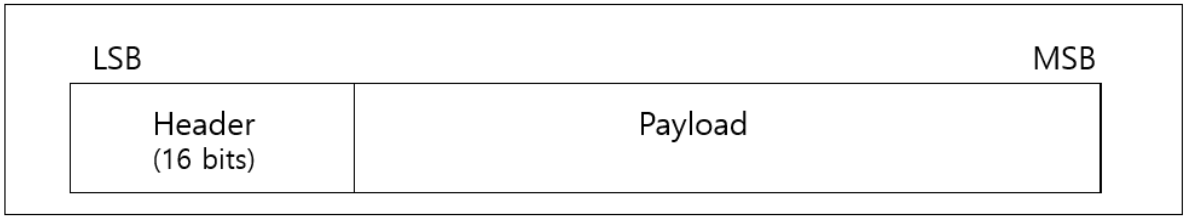


Figure 2.1: Link Layer packet format

>>PDU (Advertising Channel)



>>PDU (Data Channel)

Figure 2.12: Data Channel PDU

Data Channel PDU 는 MIC(message integrity check)를 Payload 에 포함합니다.

위의 PDU SIZE 는 BLE 4.2 specification 기준입니다.
header, payload 포함 2~39bytes <- advertising channel PDU
header, payload 포함 2~257bytes <- data channel PDU

BLE 4.0, 4.1 의 경우 PDU 의 size 는 header, payload 포함 2~39bytes 입니다.

먼저 **Advertising Channel PDU types** 에 대해서 살펴 보겠습니다.

Advertising PDUs

- **ADV_IND**, ADV_DIRECT_IND, ADV_NONCONN_IND, ADV_SCAN_IND

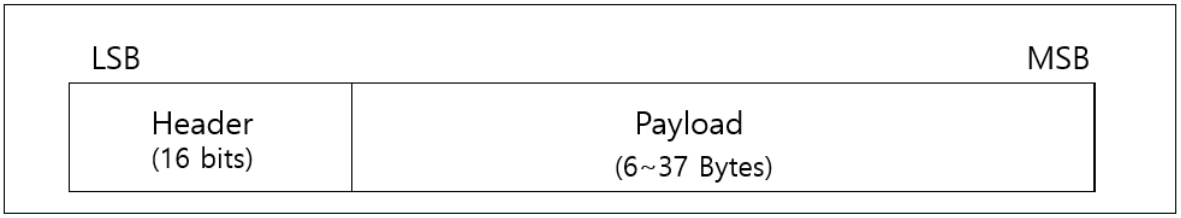
Scanning PDUs

- SCAN_REQ, SCAN_RSP

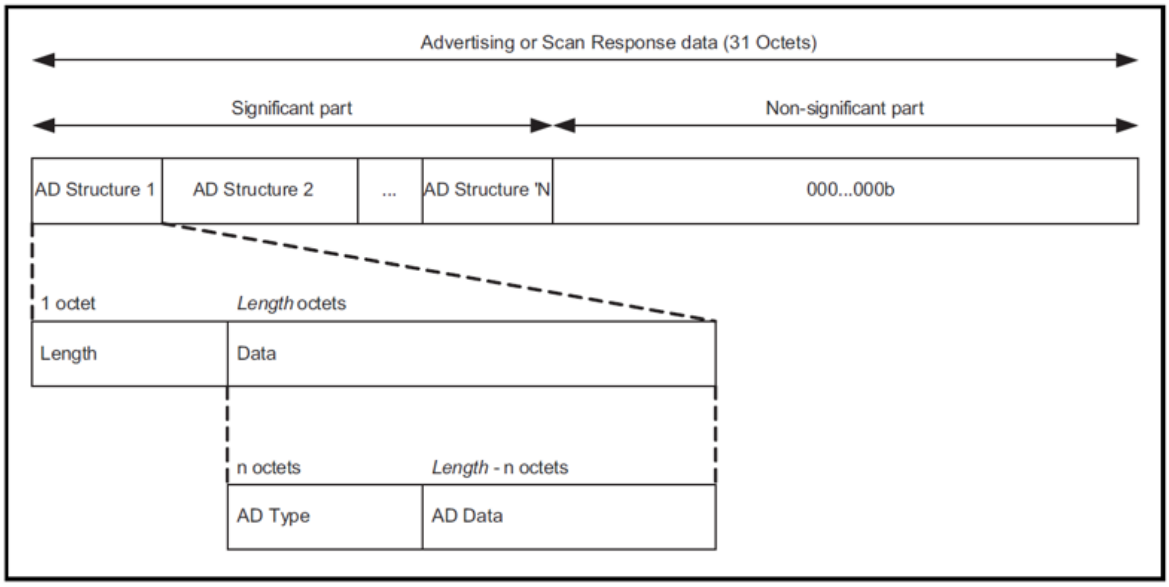
Initiating PDUs

- CONNECT_REQ

위 중에서 가장 일반적으로 사용되는 ADV_IND Packet 의 경우 아래와 같이 구성 됩니다.



위의 Payload 는 ADV Address(BLE Device address, 6bytes) 와 아래 그림처럼 AD structures 를 포함하여 구성됩니다.



AD Structure 1~N 내부 구성은 아래와 같이 구성됩니다.

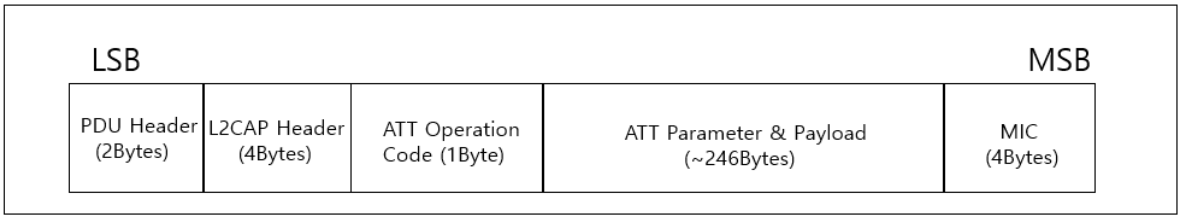
➔ AD Length(1byte)

➔ AD Type(1byte)

➔ AD Data(~29bytes)

Data channel PDU 는 Central 장치와 peripheral 장치간의 connection 후 사용됩니다.

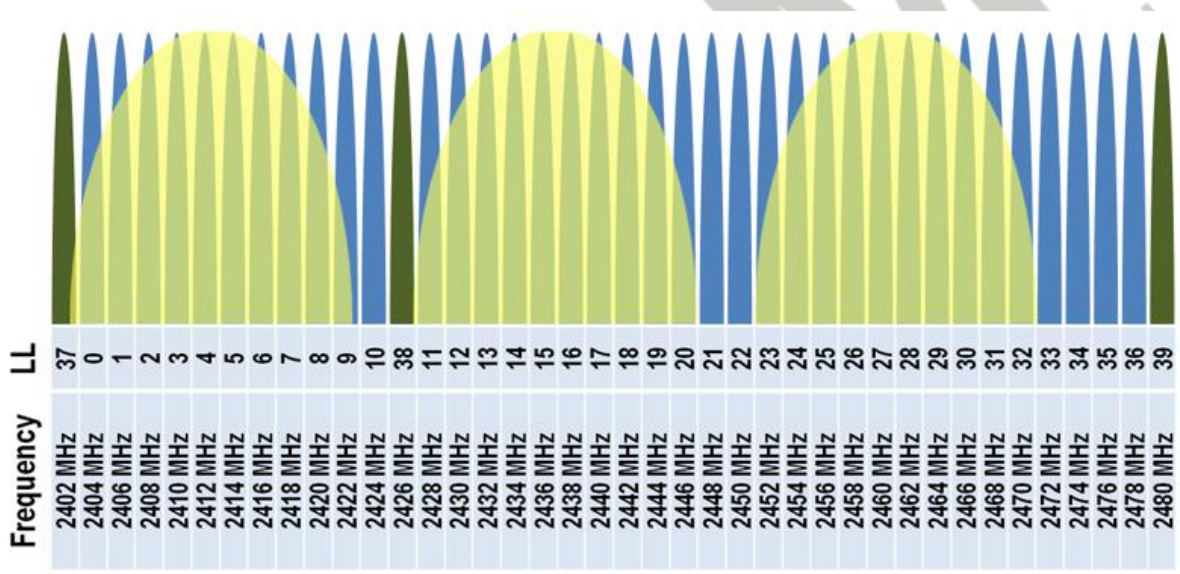
아래는 **Data Channel PDU** 구성에 대한 설명입니다.



1) **Advertising Process**

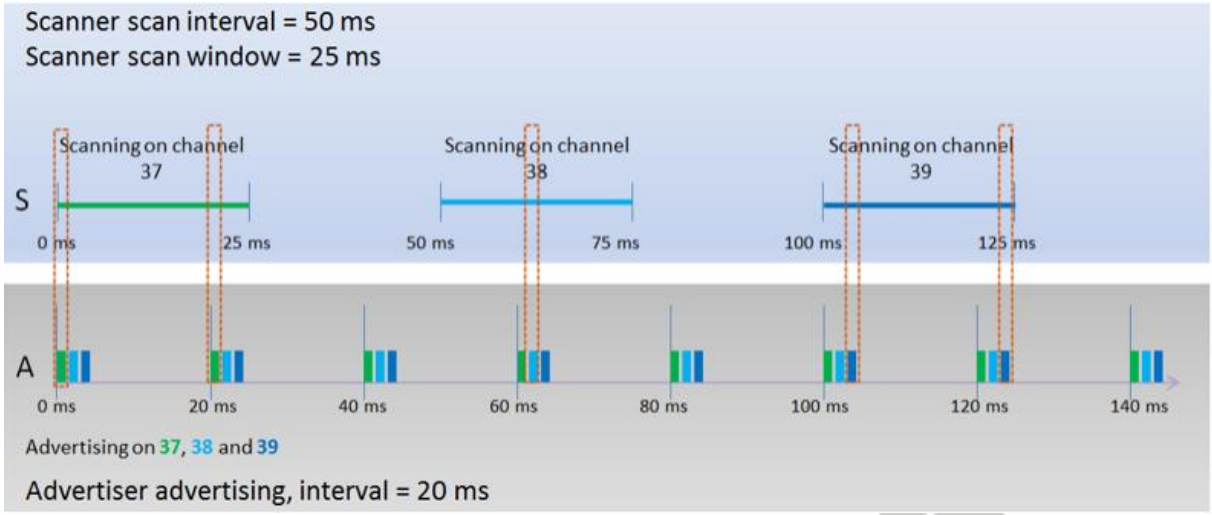
Peripheral 장치의 경우 정해진 advertising interval 마다 3 개의 advertising channel 에 같은 같은 packet 을 전송합니다.

BLE 는 2.4Ghz 의 frequency 대역을 40 개의 channel 로 구분해서 사용합니다.



위의 37, 38, 39 번 channel 이 advertising channel 이며 이 channel 을 통해서 advertising packet 을 전송합니다.

아래는 BLE Central 장치의 scanning 동작, 같은 시간대에서의 BLE Peripheral 장치의 adverting 동작에 대한 sequence 를 간략하게 설명한 그림입니다. 아래와 같이 동작함으로써 Central 장치는 advertising 동작중인 BLE 장치의 advertinsig packet 을 확인하게 됩니다.



BLE 5.0 LE advertising extensions 은 BLE 4.2 의 advertising PDU 와 차이점이 있습니다.

BLE 5.0 에서는 아래 advertising PDU types 가 추가 되었습니다.

- ADV_EXT_IND, AUX_ADV_IND, AUX_CHAIN_IND, AUX_SYNC_IND

PDU name	Components				
	where	when	what	version	how
ADV_IND		ADV			IND
ADV_DIRECT_IND		ADV	DIRECT		IND
ADV_EXT_IND		ADV		EXT	IND
AUX_ADV_IND	AUX	ADV			IND
AUX_CHAIN_IND	AUX	CHAIN			IND
SCAN_REQ		SCAN			REQ
AUX_SYNC_IND	AUX	SYNC			IND
LL_PHY_UPDATE_IND		LL	PHY_UPDATE		IND
LL_LENGTH_REQ		LL	LENGTH		REQ
LL_LENGTH_RSP		LL	LENGTH		RSP
LL_REJECT_IND		LL	REJECT		IND
LL_REJECT_EXT_IND		LL	REJECT	EXT	IND
BIG_CHANNEL_-MAP_IND		BIG	CHANNEL_-MAP		IND

Table 3.6: Examples

Payload			
Extended Header Length (6 bits)	AdvMode (2 bits)	Extended Header (0 - 63 octets)	AdvData (0 - 254 octets)

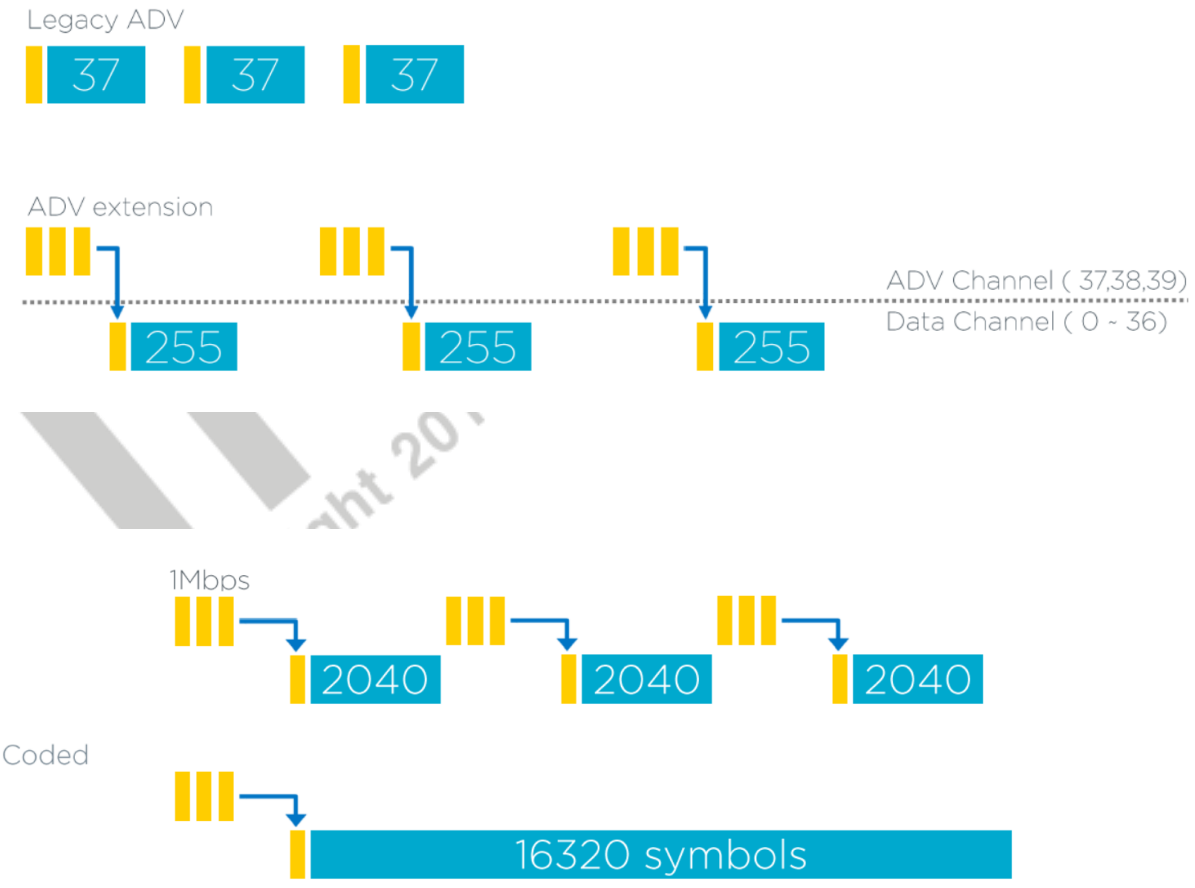
Figure 2.14: Common Extended Advertising Payload Format

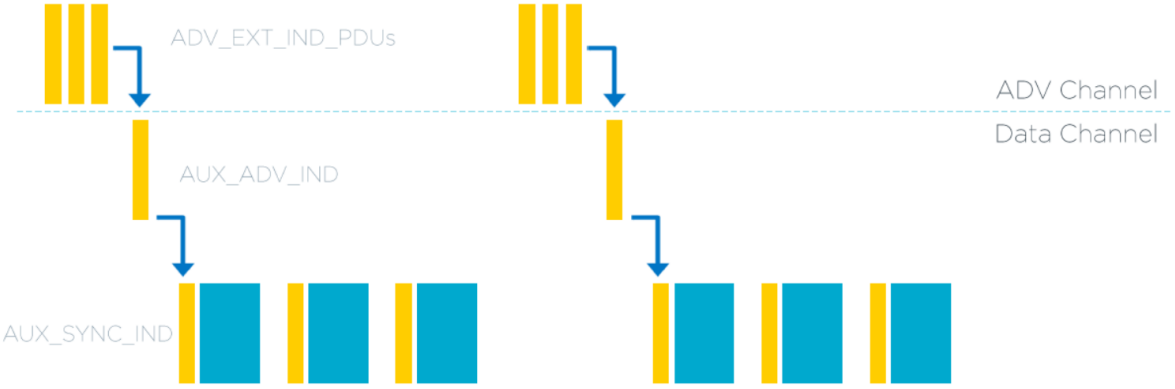
Extended Header								
Extended Header Flags (1 octet)	AdvA (6 octets)	TargetA (6 octets)	CTEInfo (1 octet)	AdvData Info (ADI) (2 octets)	AuxPtr (3 octets)	SyncInfo (18 octets)	TxPower (1 octet)	ACAD (varies)

Figure 2.15: Extended Header

위의 내용에 대한 자세한 사항은 Bluetooth Core Specification 자료를 참조 부탁드립니다.

아래는 위에서 설명드린 LE advertising extensions 에 대한 그림 설명입니다.





2) **Active Scanning Process**

Central 장치는 SCAN_REQ 를 Peripheral 장치에 보냄으로써 ADV_IND 에 포함된 advertising packet 외 추가적인 data 들을 확인할 수 있습니다. BLE Peripheral 장치는 SCAN_REQ 에서 대한 응답으로 SCAN_RSP 를 return 합니다.

Value	Meaning
IND	An indication that doesn't expect a reply
REQ	A request that expects a response
RSP	A response to a request

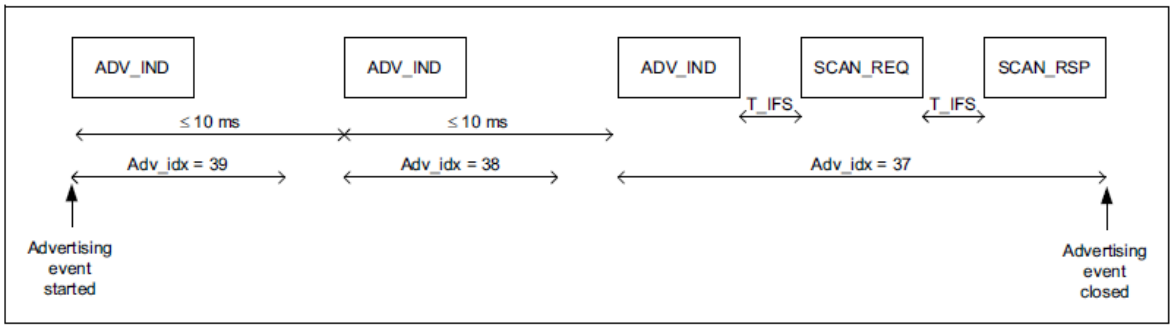
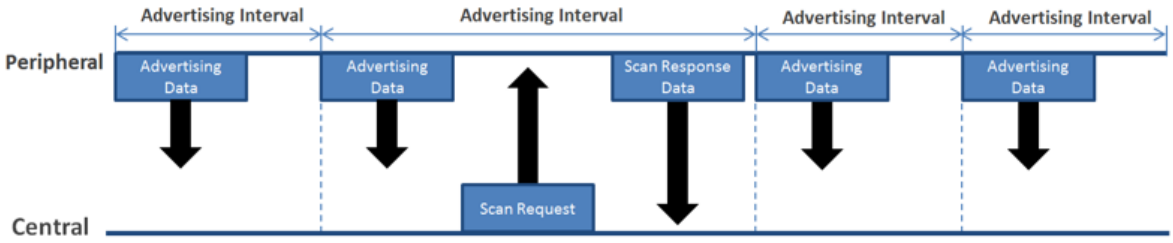


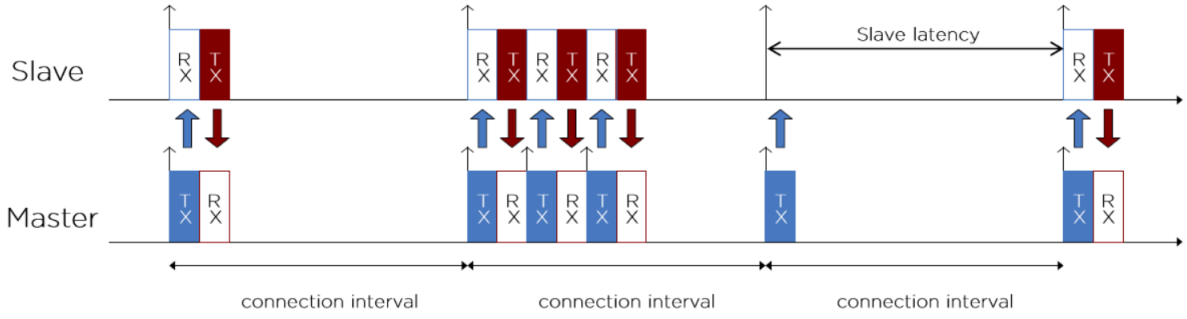
Figure 4.11: Connectable and scannable undirected advertising event with SCAN_REQ and SCAN_RSP PDUs at the end of an advertising event



3) Device Connection

BLE Central, peripheral 장치간의 Connection 후 BLE 동작에서 사용되는 용어에 대한 설명을 아래 추가 하였습니다. 참조 부탁드립니다.

- **Connection Interval**
  - Time between two connection events.
- **Slave Latency**
  - Number of consecutive connection events that a slave is *not* required to listen for the Master (events are skipped only if it doesn't have data to send).
- **Supervision Timeout**
  - Maximum time between two received valid data packets before a connection is considered "lost".



4) **Frequency Hopping**

Central 장치와 Peripheral 장치간의 connection 후 data packet 전송은 여러 data channel 을 순환하면서 data packet PDU 를 전송합니다. 아래는 frequency hopping 에 대한 개략적인 그림 설명입니다.