RF-DG-32B Bluetooth 5.0 Low Energy nRF52832 USB Dongle Sniffer User Guide

Version 1.2

Shenzhen RF-star Technology Co., Ltd.

May 26th, 2023

Table of Contents

1 Description

1. This Sniffer packet capture tool RF-DG-32B can be used to capture 1M bps data under the BLE5.0 protocol.
2. It is backward compatible with BLE 4.2 and can fully capture BLE4.2 data packets.
3. This tool supports capturing broadcast packets and data packets of our Nordic solutions nRF52810, nRF52832, nRF52840 and TI solutions CC2640R2F, CC2642R, CC2652R and other series BLE5.0 modules. The new series from Nordic need to be checked.

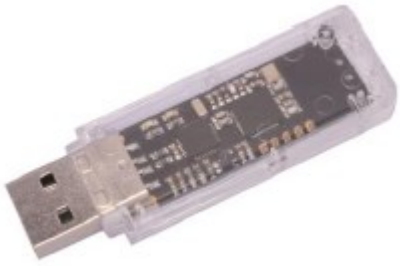
Bluetooth Protocol		Support or Not	Description
BLE4.2		Yes	RF-star Sniffer is backward compatible with BLE4.2
BLE5.0	1 Mbps	Yes	
	2 Mbps	No	If the user needs to work at 2 Mbps, adjust to 1 Mbps first for data capture test. The 2 Mbps data cannot be captured.
	Long range	No	nRF52832 chip does not support long range mode.
	Extend packet	No	Nordic official firmware supports to capture the packet of ADV_EXT_IND. But the Wireshark cannot recognize the extend packets, the users need to parse the data by themselves.

For the official reply about not being able to capture the extend packet, please check the following link:

https://devzone.nordicsemi.com/f/nordic-q-a/53885/rookie-seeking-help-to-receive-extended-adverts/217939#217939

2 Preparation before Use

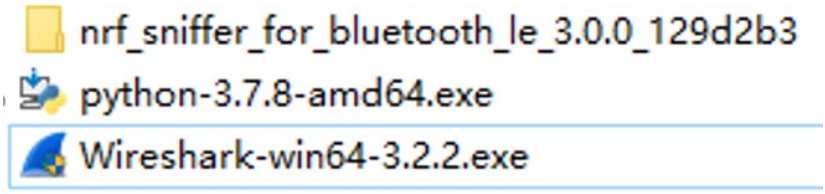
1. Prepare an RF-DG-32B and a Bluetooth slave device with data to be captured.



2. Download the Wireshark software to install and configure the environment.
   Wireshark download address: https://www.wireshark.org/#download
3. Install the Python v3.7.x environment.
   Python v3.7.x environment download address: https://www.Python.org/downloads/release/Python-378/
4. Download nRF Sniffer for Bluetooth LE v3.x.x environment.
   Download address: https://www.nordicsemi.com/Software-and-tools/Development-Tools/nRF-Sniffer-for-Bluetooth-LE/Download#infotabs
5. Download CP2102 driver.
   Download link: https://www.szrfstar.com/downloadnda/712-cn.html

3 Preparation for Development Environment

Download the above three APPs.

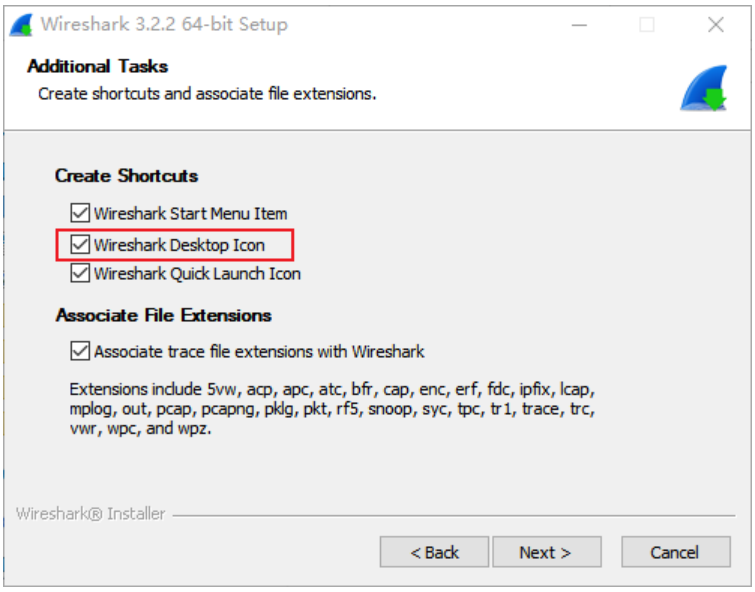


The compressed package file nrf_Sniffer_for_bluetooth_le_3.0.0_129d2b3 (hereinafter collectively referred to as the zip) is decompressed as shown in the following figure:

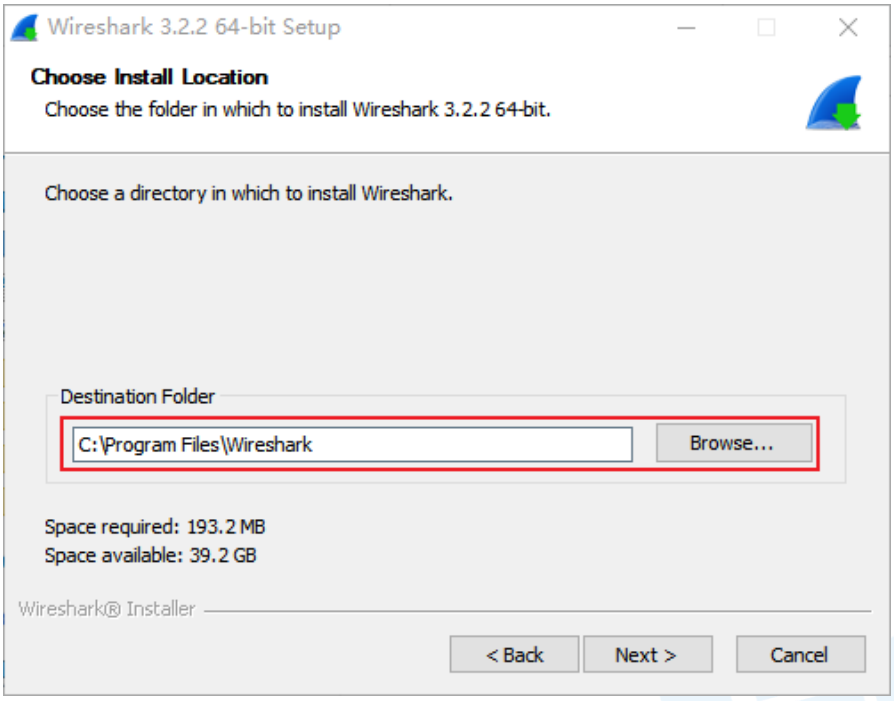
Note: Do not change the installation steps, otherwise the installation may fail.

3.1 Install Wireshark

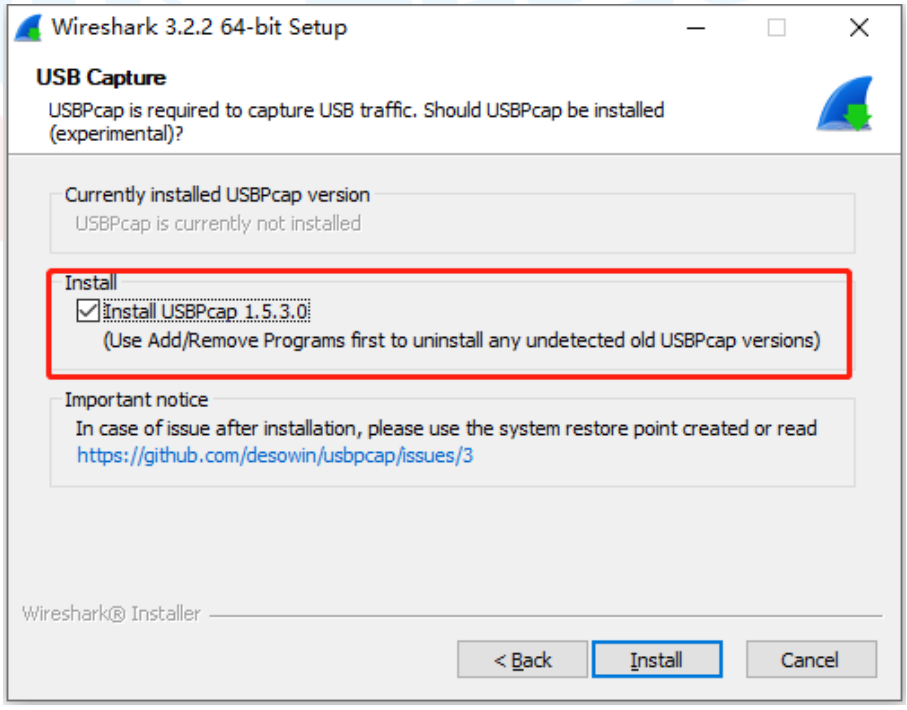
1. Double-click Wireshark-win64-3.2.2.exe to install, choose “next” all the way, and select the Wireshark Desktop Icon to create a shortcut:



2. As shown below, choose the install location:



3. As shown below, select USB Capture and install it:

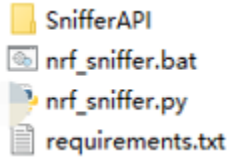


4. The remaining steps just need to click next and yes until the installation is complete, and then restart the computer.

3.2 Configure Wireshark Environment

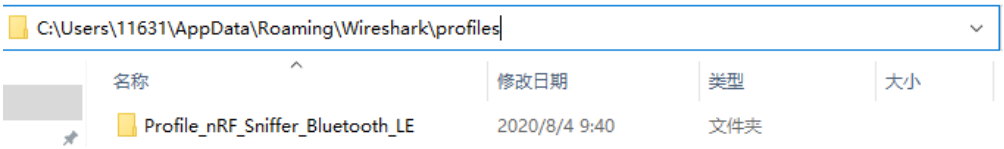
1. Open Wireshark -> help -> about Wireshark -> folder -> double-click to open Extcap path, as shown in the figure below:

2. Unzip the zip file and copy the four files in the extcap folder to the Wireshark extcap path just opened. Take the global path as an example. The following figure shows the copied effect:



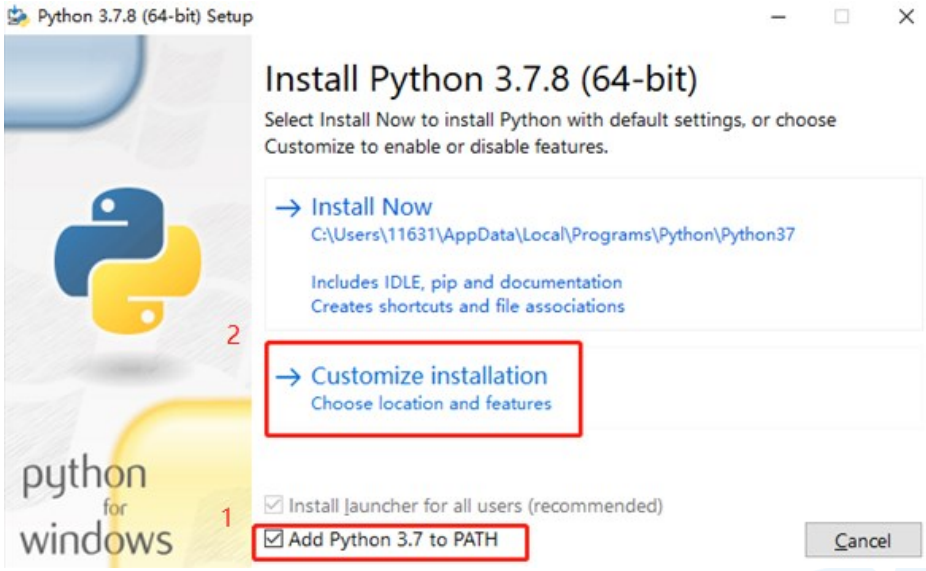
3. Then double-click the personally configured websites in Wireshark, as shown below:

4. Open the profiles folder under the pop-up folder.
5. Then copy the Profile_nRF_Sniffer_Bluetooth_LE folder in the decompressed zip file to the profiles folder, as shown below is the effect of the copy:

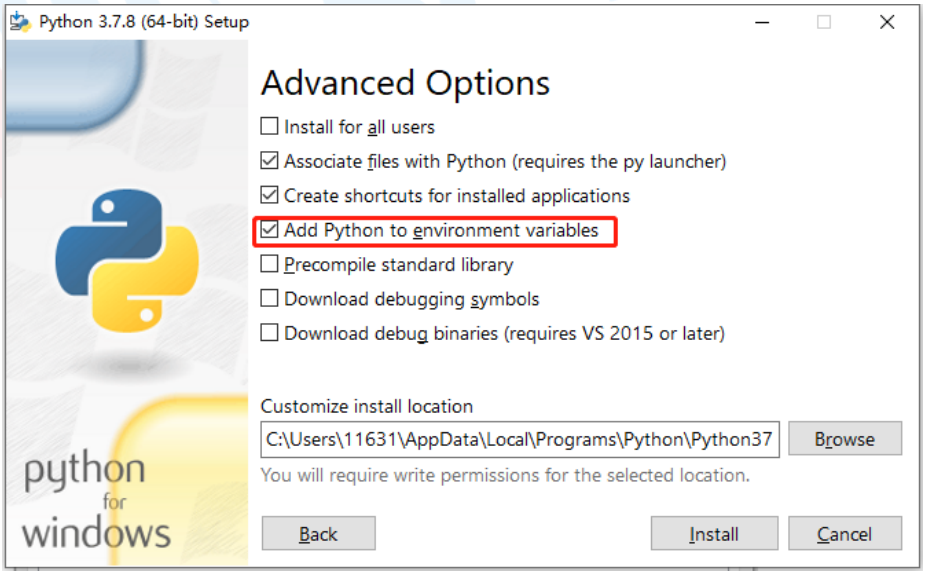


3.3 Install Python

1. Double-click Python-3.7.8.exe to install and keep clicking “next” until the following interface:



2. Here you need to select the option in the red box, that is, add an environment variable, and then click “next” until the installation is completed.



3.4 Install Pyserial v3.4

1. Press the Windows key and R key to bring up the run, then enter cmd and press Enter to enter the command line interface (note that running cmd as an administrator, the computer used for the demonstration is the administrator by default. If not, please google "How to Run cmd as administrator "), enter" pip --version "command in the cmd window to query the pip version of Python, as shown in the figure below, it means that pip has been started normally and the version number is 20.1.1.

```
C:\WINDOWS\system32>pip --version
pip 20.1.1 from c:\users\11631\appdata\local\programs\python\python37\lib\site-packages\pip (python 3.7)
```

2. Enter “Python -m pip install --upgrade pip” command to update pip, as shown below, the update is successful (pls note the number of “-“ in the code).

```
C:\WINDOWS\system32>python -m pip install --upgrade pip
Collecting pip
  Downloading pip-20.2-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 9.9 kB/s
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 20.1.1
    Uninstalling pip-20.1.1:
      Successfully uninstalled pip-20.1.1
Successfully installed pip-20.2
```

Note: If failed, the following will be shown:

```
WARNING: You are using pip version 20.1.1; however, version 20.2.2 is available.
You should consider upgrading via the 'C:\Users\81208\AppData\Local\Programs\Python\Python37\python.exe -m pip install --upgrade pip' command.
```

Then, pls enter “Python -m pip install -U pip” command, update the pip, then successfully installed.

```
C:\WINDOWS\system32>python -m pip install -U pip
Collecting pip
  Downloading pip-20.2.2-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 29 kB/s
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 20.1.1
    Uninstalling pip-20.1.1:
      Successfully uninstalled pip-20.1.1
Successfully installed pip-20.2.2
```

3. Enter the "cd C:\Program Files\Wireshark\extcap" command to locate the cmd interface to the "C:\Program Files\Wireshark\extcap" directory, if you use the global path before. Note that at this time, the extcap directory of the Wireshark installation directory is just our Where you copy the five files here, the Wireshark installation directory is different, this path may be different, please adjust it by yourself, as shown below after switching:

```
C:\WINDOWS\system32>cd C:\Program Files\Wireshark\extcap
```

4. After adjusting the directory, enter the command “pip install -r requirements.txt”, then the installation of pyserial v3.4 will start.

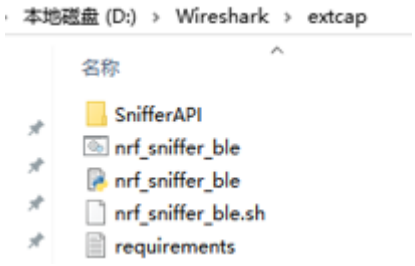
```
C:\Program Files\Wireshark\extcap>pip install -r requirements.txt
```

5. The following figure shows the success:

```
Collecting pyserial>=3.4
  Using cached pyserial-3.4-py2.py3-none-any.whl (193 kB)
Installing collected packages: pyserial
Successfully installed pyserial-3.4
```

Note:

To execute this command, the cmd operation interface must be located under the corresponding path selected in chapter 3.2 (global path extcap or personal path extcap ", that is, under the current operating directory, there must be a text file containing "requirements.txt", etc. Files, as shown below:



3.5 Parts of Solutions When Install in Windows 7

In the Window 7 environment, when using Python 3.7.x and Sniffer 2.0 provided by the current official website, it is easy to encounter the situation that Python cannot be upgraded during the installation process or the Sniffer port cannot be recognized by Wireshark after the installation environment. According to the installation environment provided by the installation manual, some problems that may occur during the installation process are explained as follows:

1. The Windows 10 system uses the latest configuration environment Python 3.7.x and Sniffer 2.0, and it is recommended to use the combination of Python 2.7.16, Wireshark 3.0.13, and Sniffer 2.0 for Window 7 to build a packet capture environment. Sniffer cannot be used mainly in three aspects: the failure to upgrade the pip version in the Python environment, the failure to install the pyserial v3.4 script, and the problem of driver installation.
2. After installing Python on Windows 7, the upgrade of Python often fails. First, run the CMD terminal with administrator privileges, and execute "pip --version" to query the current version of pip in Python.

   pip update issue:

   To update pip to the latest version, use the command:

   python –m pip install —upgrade pip

   Note: There are two consecutive "-" before the upgrade command upgrade.

   If the update fails at this step, try switching the update command:

   python -m pip install -U pip

   python -m pip install -U --force-reinstall pip

3. Pyserial v3.4 installation problem:

   On the premise of configuring the Wireshark file, the terminal interface executes the following command in the command directory to install Pyserial v3.4:

   pip install -r requirements.txt

   Note: The script file installation failure is mostly due to network problems.

4. Before using Sniffer, ensure that the relevant drivers are installed successfully

   Serial port driver CP2102: If the driver is not installed successfully, it will directly cause Wireshark to not recognize the Sniffer port. When the Sniffer is plugged into the computer, you can check whether there is a CP2102 port in the port column of the device manager in the Windows system as shown below:

   Note: If the above port can be successfully identified, it means that the Sniffer computer-side serial port driver has been successfully installed.

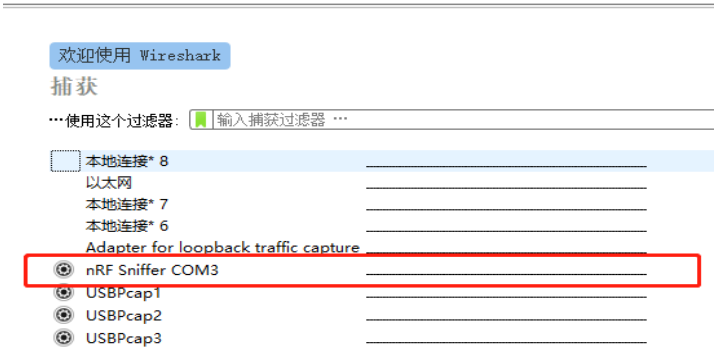
   USBPCAP packet capture tool: This tool appears in the Wireshark software installation process, although its installation does not directly affect the Wireshark software to identify Sniffer, that is, whether there is a Sniffer port, it will affect the subsequent packet capture, you need to follow the manual step by step Install the plugin tool.

   Note: Npcap and wincap are also used as packet capture plug-ins. Npcap is an upgraded version of wincap. In the Window 7 environment, if the previous Python environment and pyserial v3.4 are installed correctly, some ports cannot be recognized. You can try to install winpcap to solve it.

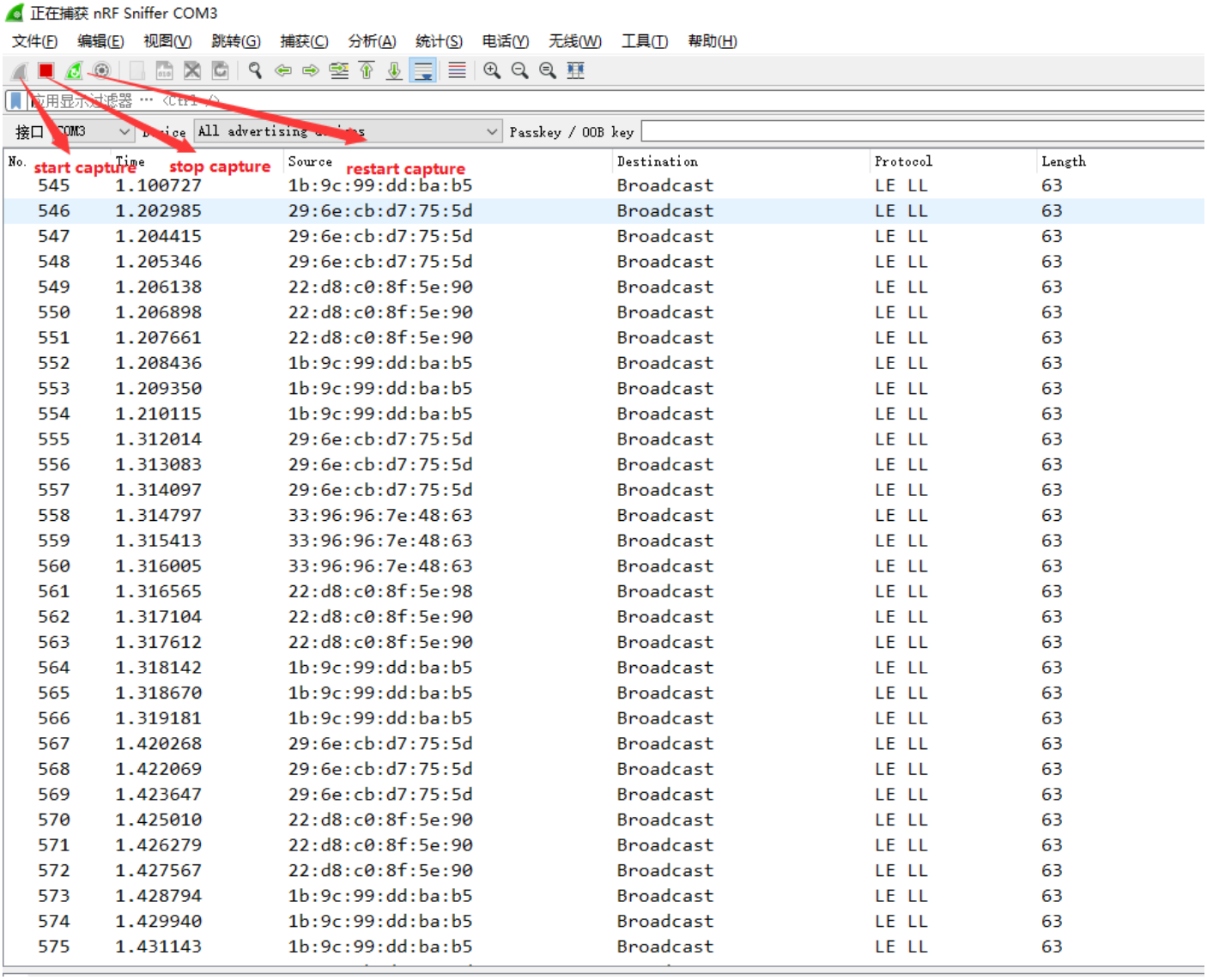
   If the above methods cannot solve the problem, you can try to uninstall all previous installations and rebuild the configuration environment.

4 Instruction for Use

1. After the software is successfully installed, connect the RF-DG-32B to the PC via USB, open Wireshark, and select nRF Sniffer COMx.



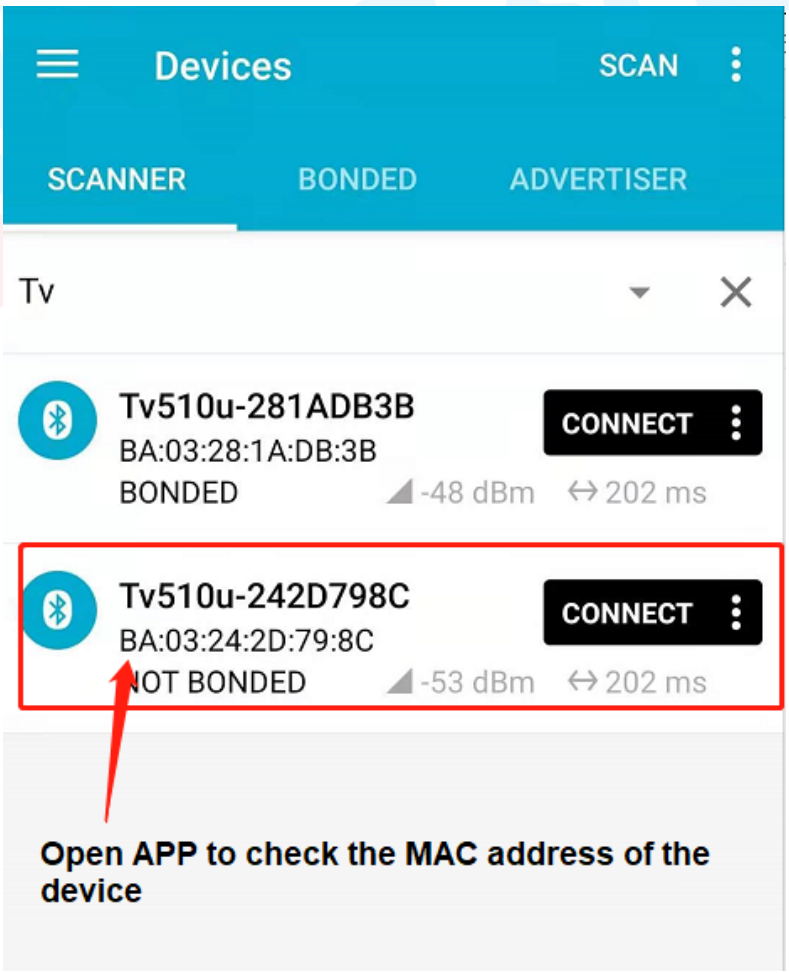
2. Select -> View -> Interface Toolbar -> nRF Sniffer in the toolbar, the following interface will appear (by default, all BLE broadcast signals are captured).



3. Select any RF-star BLE slave development board to power on for broadcasting.

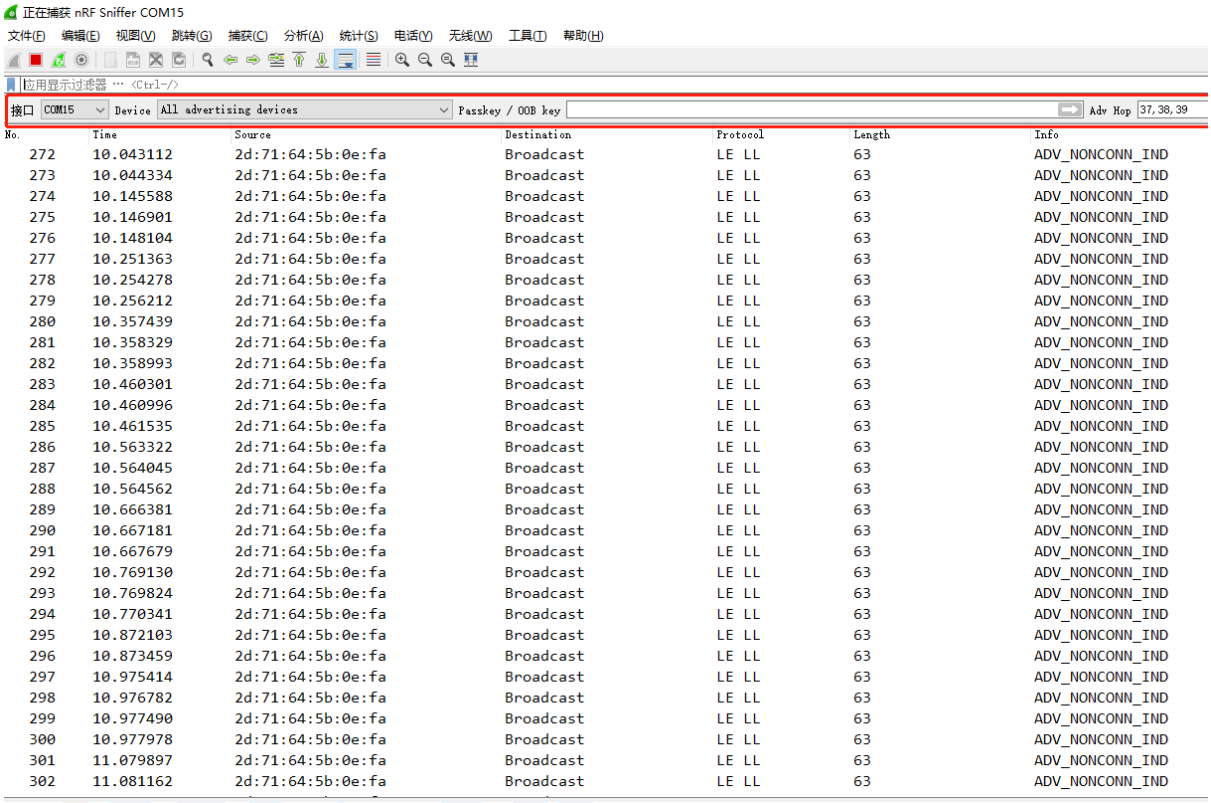
4. Capture the data packets of the specified MAC address device.

   You can check the device's MAC address through the APP, as shown below:



   As shown in the red box in the figure below, click the device filter drop-down box to select the device with the

corresponding MAC address. After selecting the fixed device, only the data packets related to the device will be captured.



No.	Time	Source	Destination	Protocol	Length	Info
272	10.043112	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
273	10.044334	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
274	10.145588	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
275	10.146901	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
276	10.148104	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
277	10.251363	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
278	10.254278	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
279	10.256212	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
280	10.357439	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
281	10.358329	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
282	10.358993	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
283	10.460301	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
284	10.460996	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
285	10.461535	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
286	10.563322	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
287	10.564045	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
288	10.564562	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
289	10.666381	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
290	10.667181	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
291	10.667679	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
292	10.769130	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
293	10.769824	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
294	10.770341	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
295	10.872103	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
296	10.873459	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
297	10.975414	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
298	10.976782	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
299	10.977490	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
300	10.977978	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
301	11.079897	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND
302	11.081162	2d:71:64:5b:0e:fa	Broadcast	LE LL	63	ADV_NONCONN_IND

5. After Wireshark selects the MAC address device, the broadcast packet, scan request packet and scan response packet of the device will be captured.

No.	Time	Source	Destination	Protocol	Length	Info
10094	458.592234	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10095	458.593469	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10096	458.795753	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10097	458.797325	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10098	458.798505	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10099	459.000875	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10100	459.002667	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10101	459.003979	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10102	459.206072	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10103	459.207238	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10104	459.208045	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10105	459.208734	46:1c:9d:dd:3b:58	ba:03:24:2d:79:8c	LE LL	38	SCAN_REQ
10106	459.209447	ba:03:24:2d:79:8c	Broadcast	LE LL	58	SCAN_RSP
10107	459.411627	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10108	459.413303	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10109	459.414699	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10110	459.617545	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10111	459.618539	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10112	459.619232	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10113	459.821226	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10114	459.822962	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10115	459.824387	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10116	460.026561	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10117	460.028202	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10118	460.029887	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10119	460.231604	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10120	460.232516	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10121	460.233123	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10122	460.434175	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND
10123	460.435742	ba:03:24:2d:79:8c	Broadcast	LE LL	59	ADV_IND

Scan request packet

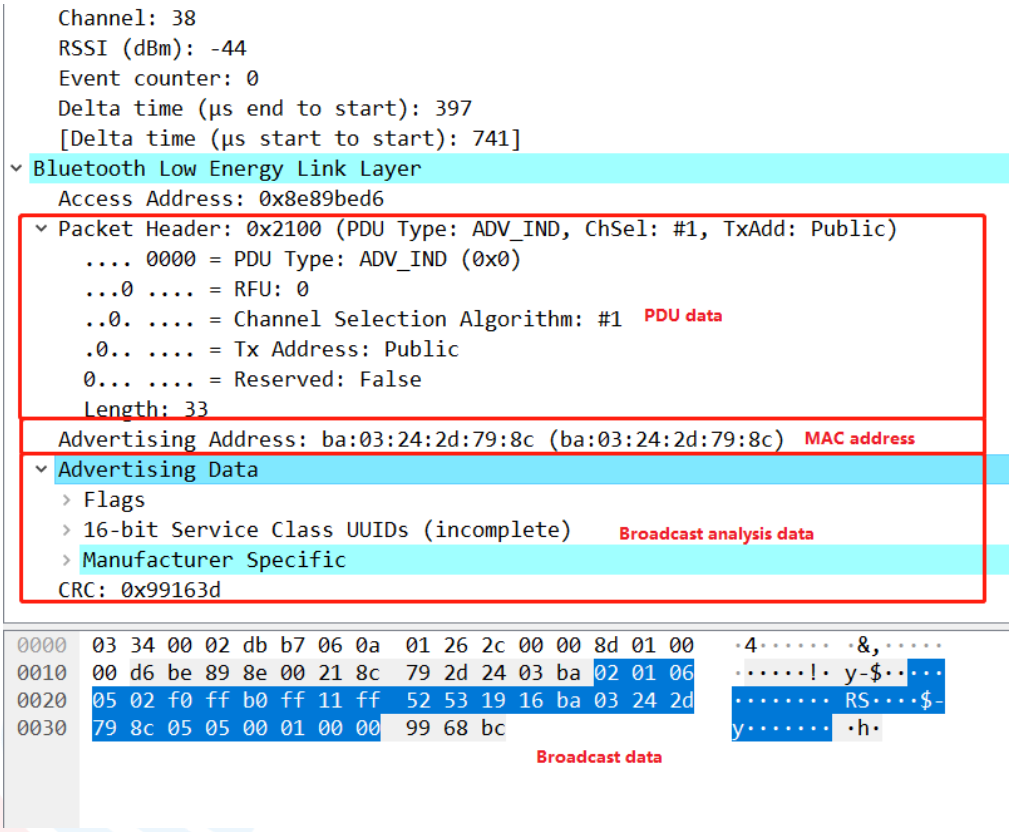
Scan Response packet

Broadcast packet

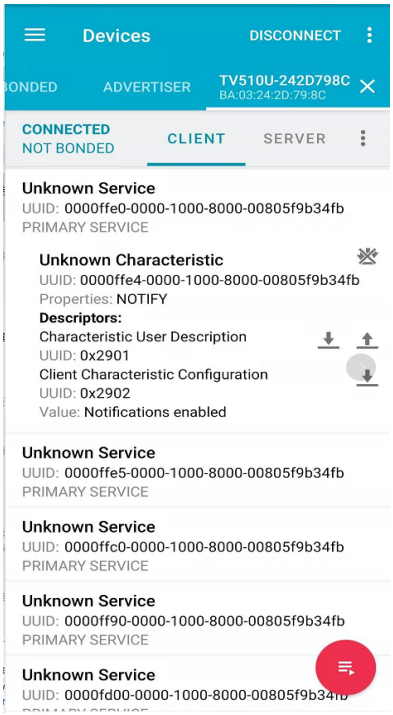
6. The data packets that the device communicates with any master can be captured, including the connection

process and the data packets after the connection.

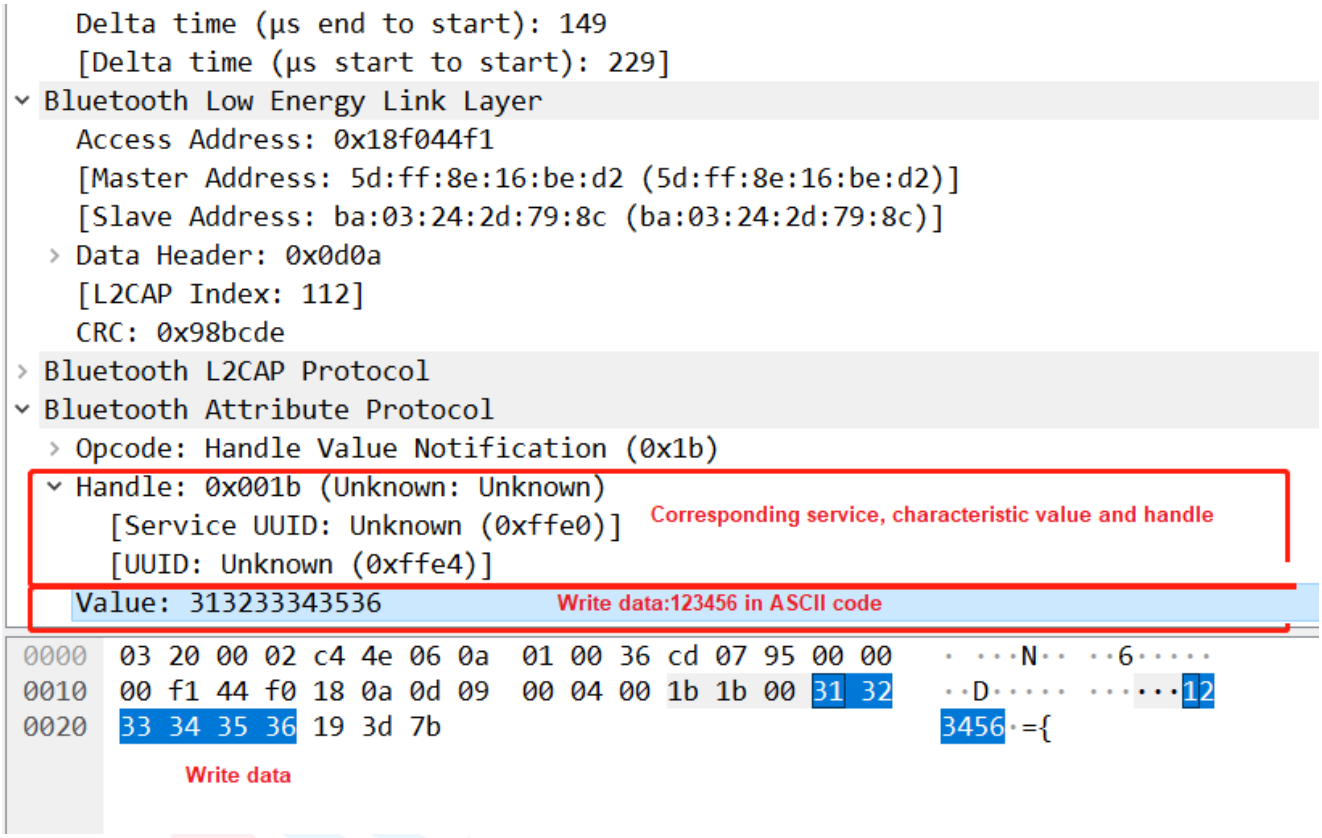
Double-click any packet to view the specific content. For example, the device captures the broadcast packet as follows:



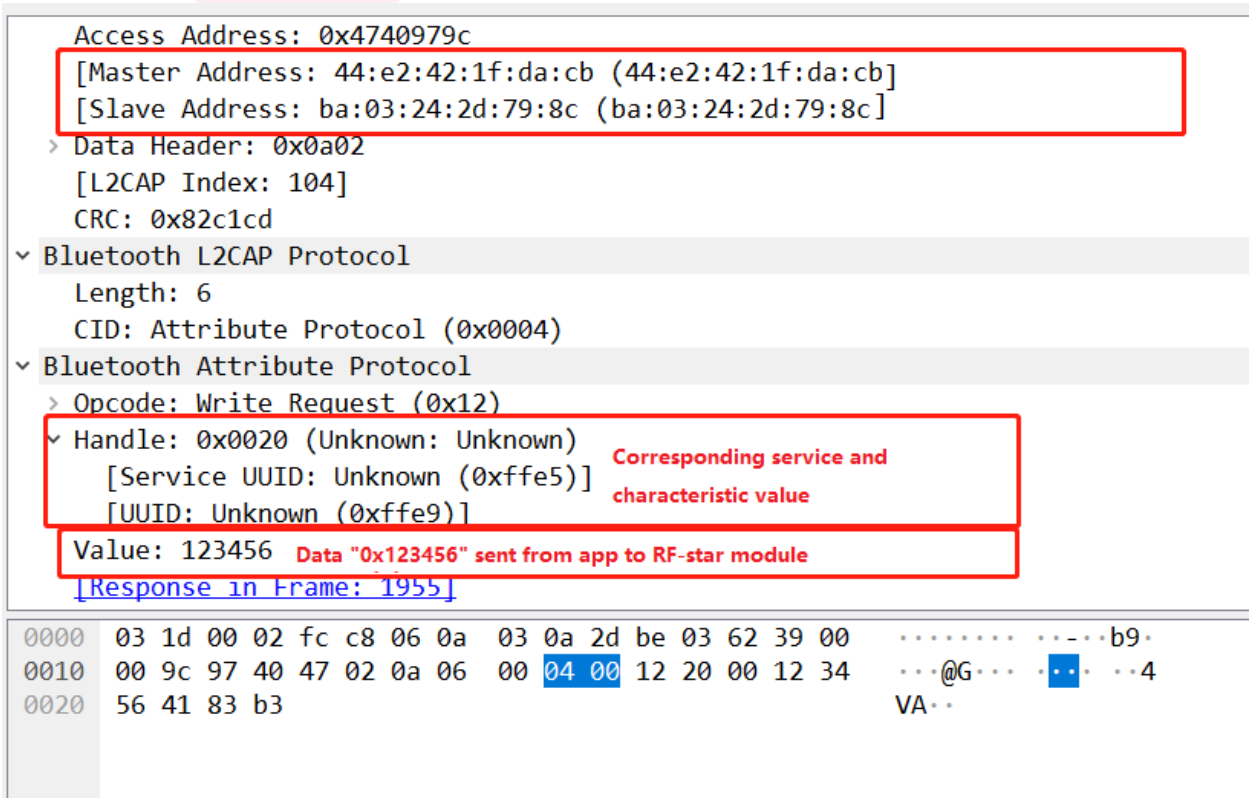
7. When a connection event occurs, all data communication processes of the connection process can be captured. After connecting the device, the APP interface is displayed as follows:



Use the serial assistant to send the ASCII code “123456” to the BLE transparent transmission module. After receiving, the BLE module will forward the data to the APP. The data captured by Sniffer is the data sent by BLE to the APP, as shown in the following figure:



Similarly, we can capture the data packets sent by the APP to the BLE module. The data captured by Sniffer after sending “0x123456” to the RF-Star transparent transmission module using APP is shown in the figure below.



5 Electrostatics Discharge Warnings

The module will be damaged by the discharge of static. RF-star suggests that all modules should follow the 3 precautions below:

1. According to the anti-static measures, bare hands are not allowed to touch modules.
2. Modules must be placed in anti-static areas.
3. Take the anti-static circuitry (when inputting HV or VHF) into consideration in product design.
   Static may result in the degradation in performance of the module, even causing the failure.

6 Revision History

Date	Version No.	Description
2020.03.26	V1.0	The initial version is released.
2020.08.14	V1.0	Update the environment version.
2020.11.27	V1.1	Add the chapter of Parts of Solutions When Install in Windows 7.
2021.08.02	V1.2	Update some screenshots.
2023.05.26	V1.0	Update MSL level. Update the Shenzhen office address.

Note:

1. The document will be optimized and updated from time to time. Before using this document, please make sure it is the latest version.
2. To obtain the latest document, please download it from the official website: www.rfstariot.com and www.szrfstar.com.

7 Contact Us

SHENZHEN RF-STAR TECHNOLOGY CO., LTD.

Shenzhen HQ:

Add.: Room 502, Podium Building No. 12, Shenzhen Bay Science and Technology Ecological Park, Nanshan District, Shenzhen, Guangdong, China, 518063

Tel.: 86-755-8632 9829

Chengdu Branch:

Add.: N2-1604, Global Center, North No. 1700, Tianfu Avenue, Hi-Tech District, Chengdu, Sichuan, China, 610095

Tel.: 86-28-8692 5399

Email: sunny@szrfstar.com, sales@szrfstar.com

Web.: www.rfstariot.com, www.szrfstar.com