# **BLE Sniffer抓包工具使用说明**



修改记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 版本号 | 修改人 | 备注 |
| 2019.03.22 | V1 | 韦东山 | 创建 |

[**BLE Sniffer抓包工具使用说明** 1](#_Toc4502867)

[第1章. 安装抓包硬件Sniffer的驱动 3](#_Toc4502868)

[1.1 自动安装 3](#_Toc4502869)

[1.2 手动安装 4](#_Toc4502870)

[第2章. 安装抓包软件Wireshark 5](#_Toc4502871)

[2.1 安装依赖软件python2.7x 5](#_Toc4502872)

[2.1.1 安装python 5](#_Toc4502873)

[2.1.2设置环境变量 5](#_Toc4502874)

[2.1.3验证 7](#_Toc4502875)

[2.2 安装依赖软件pyserial 7](#_Toc4502876)

[2.3 安装Wireshark 8](#_Toc4502877)

[2.4 关联Wireshark和Sniffer 8](#_Toc4502878)

[2.4.1确定2个目录 8](#_Toc4502879)

[2.4.2复制文件 9](#_Toc4502880)

[2.4.3验证 9](#_Toc4502881)

[第3章. Wireshark使用说明 10](#_Toc4502882)

[3.1 启动Wireshark 10](#_Toc4502883)

[3.2 打开接口工具栏 10](#_Toc4502884)

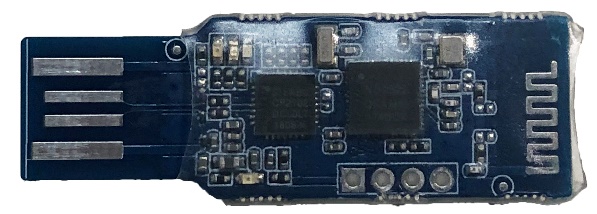
[3.3 接口工具栏介绍 10](#_Toc4502885)

[3.4 查看数据包 11](#_Toc4502886)

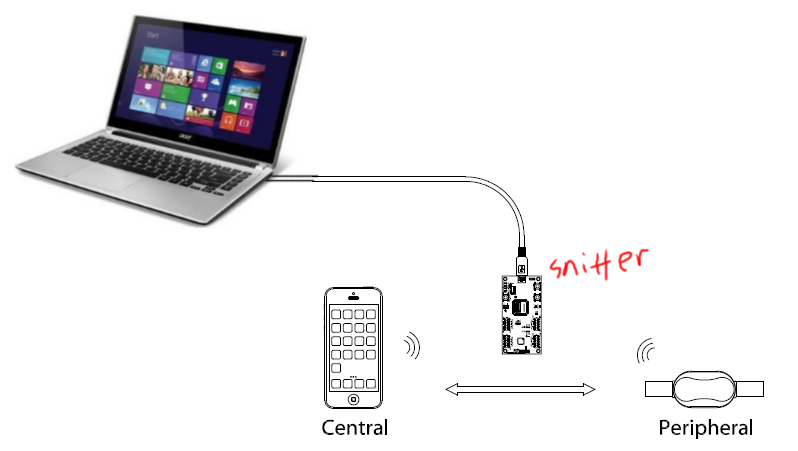
## 安装抓包硬件Sniffer的驱动

Sniffer的中文意思是嗅探器，在无线系统中它就是一个抓包的硬件工具。

nRF Sniffer是基于nordic公司的芯片及固件制作的BLE抓包工具，它是一个硬件。它的样子如下：

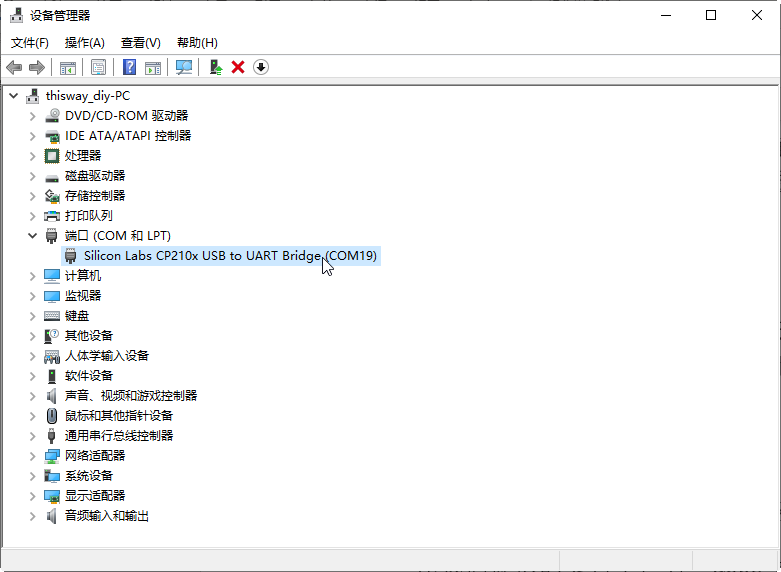


一个nRF Sniffer就可以抓取所有广播通道、数据通道的数据；相比较而言，需要3个TI Sniffer才能抓取所有广播通道的数据，并且它不能抓取数据通道的数据。



### 1.1 自动安装

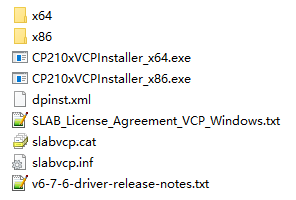
把Sniffer插到电脑上，一般来说就会自动安装驱动程序。如果成功，可以在设备管理器中看到如下信息(COM的编号可能与下图不同)。



### 1.2 手动安装

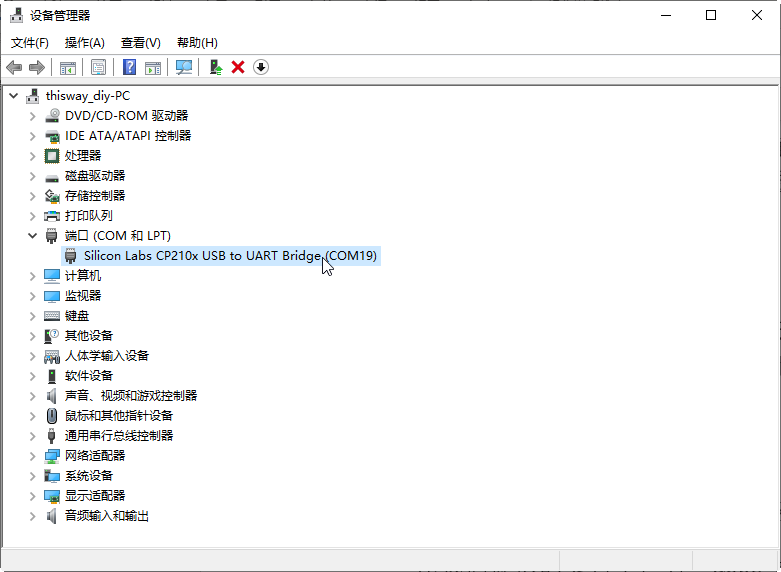
把Sniffer插到电脑上，如果驱动程序没能自动安装，可以手动安装。

在我们提供的资料中，有“apps\_and\_drivers\CP210x\_Windows\_Drivers.zip”，解压后可以看到如下文件。



1. 先从电脑上拔出Sniffer
2. 对于32位的电脑，请运行 CP210xVCPInstaller\_x86.exe
3. 对于4位的电脑，请运行 CP210xVCPInstaller\_x64.exe
4. 再插上Sniffer

如果成功驱动安装成功，可以在设备管理器中看到如下信息(COM的编号可能与下图不同)。



## 安装抓包软件Wireshark

Wireshark是一个强大的无线数据抓包及分析工具，它通过串口来访问Sniffer。要用到python版本的串口工具：pyserial。

所以我们需要先安装python，再安装pyserial，最后安装Wireshark。

本节内容来自nordic公司英文文档：nRF\_Sniffer\_User\_Guide\_v2.2.pdf，你可以从下面地址下载：<https://www.nordicsemi.com/DocLib?Product=nRF%20Tools>

本节内容是对上述英文文档的翻译，并添加了些许内容以方便理解。

### 2.1 安装依赖软件python2.7x

#### 2.1.1 安装python

在我们提供的资料中，在apps\_and\_drivers目录下，有2个文件：



对于32位Windows系统，请安装python-2.7.13.msi。

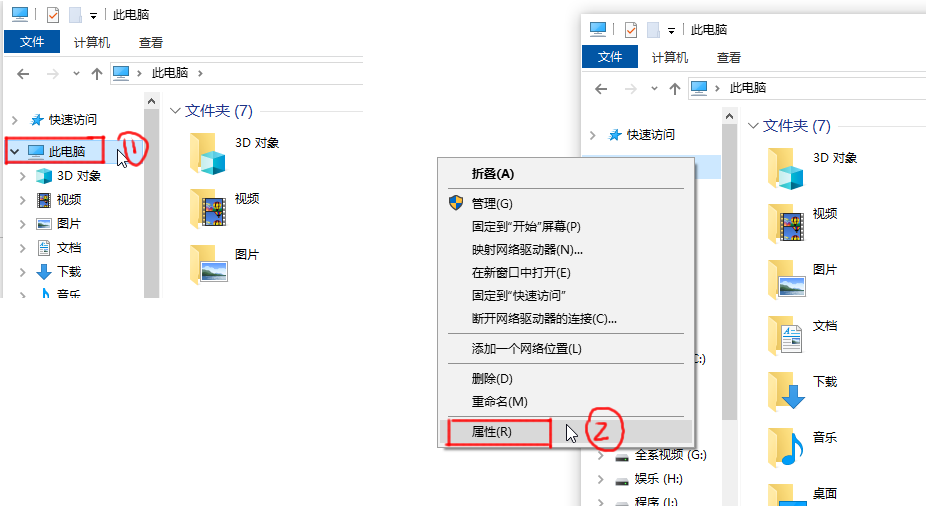
对于64位Windows系统，请安装python-2.7.13.amd64.msi。

这些安装软件，也可以去官网下载：<https://www.python.org/downloads/>

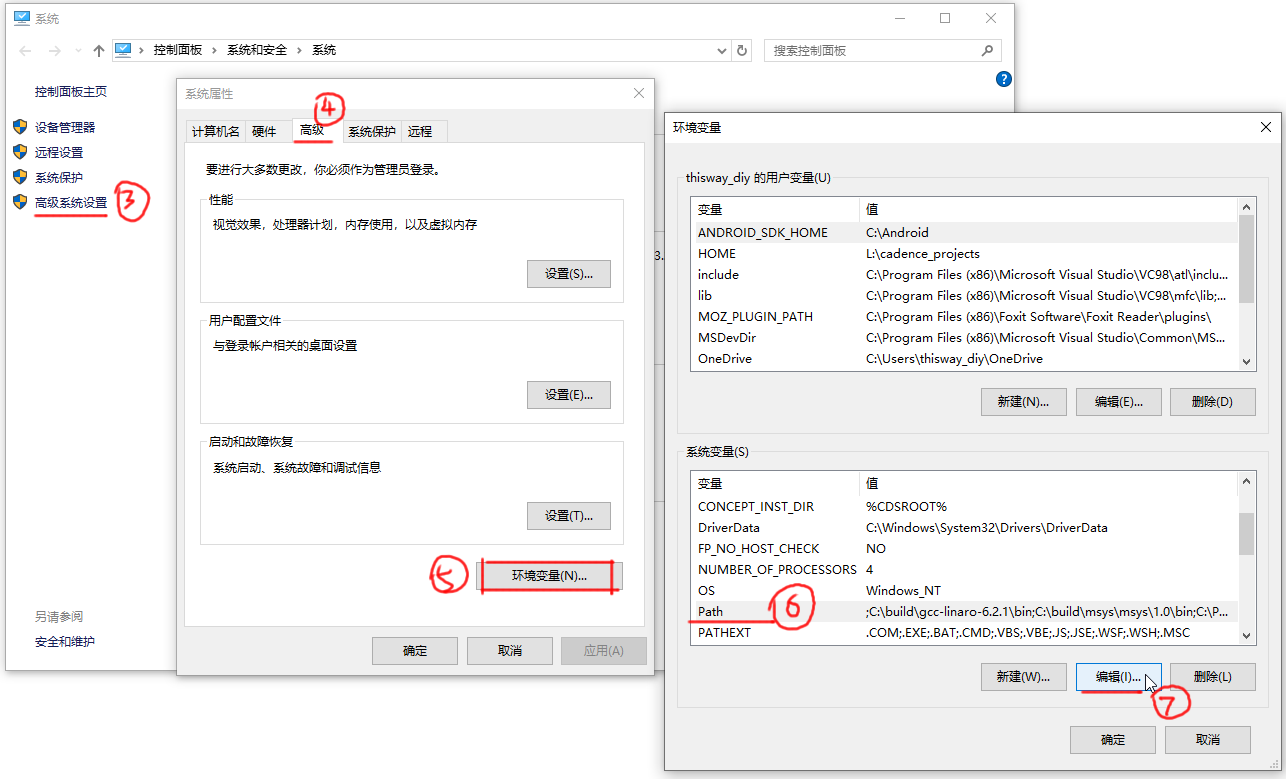
#### 2.1.2设置环境变量

假设安装目录为“C:\Python27”，安装完成之后，需要设置环境变量，把“C:\Python27”加入Path变量中。

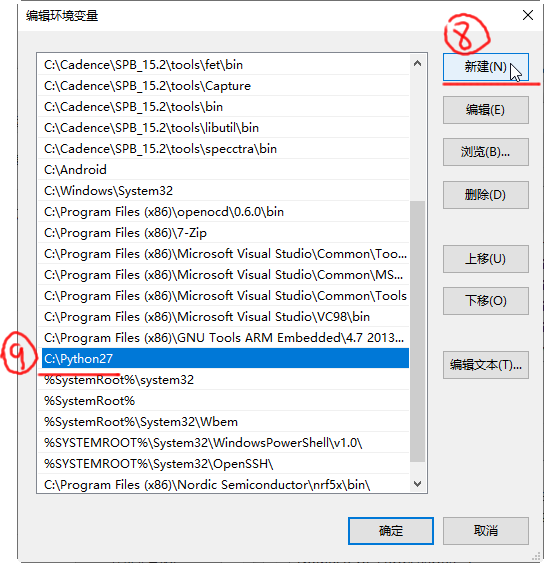
1. 在“此电脑 ”或“我的电脑”上，右键点击“属性”：



1. 按下图中的序号，一路点击：



1. 继续按下图点击，新建一个值“C:\Python27”：



#### 2.1.3验证

启动命令行，执行命令：python -V (**注意**：是大写字母V)

如果一切正常，可以得到如下图的版本号：



### 2.2 安装依赖软件pyserial

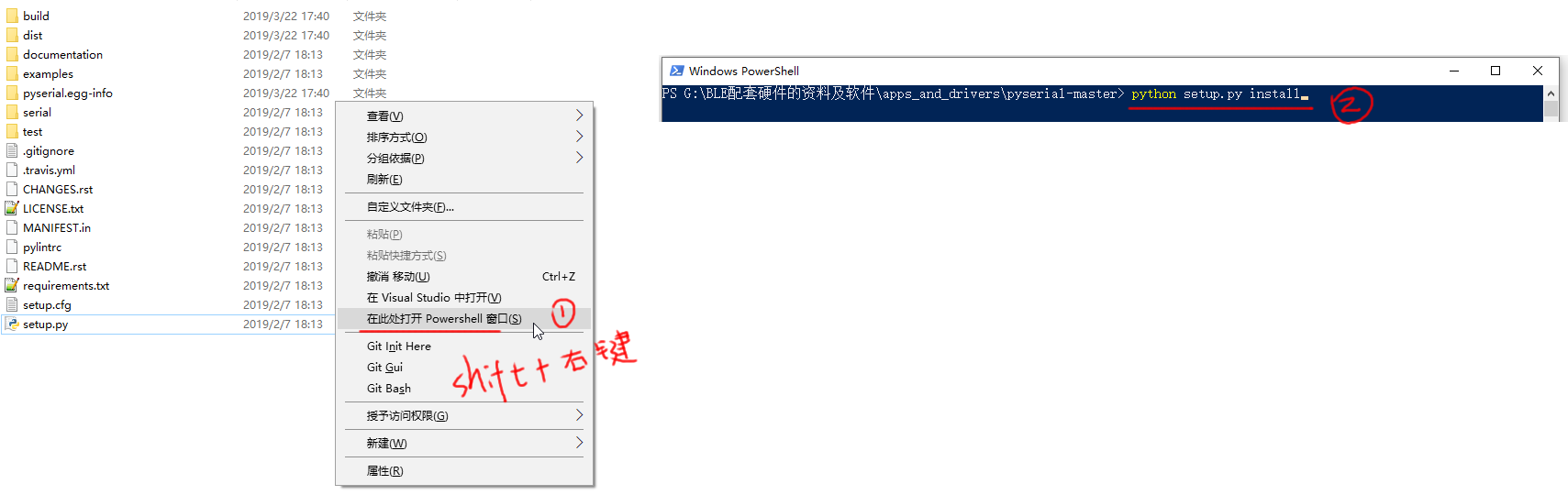
pyserial是一个使用python编写的串口工具。

在我们提供的资料中，在apps\_and\_drivers目录下有一个“pyserial-master”子目录。

进入pyserial-master目录：

1. 按住键盘shift键，同时在任意空白位置点击鼠标右键，在弹出的菜单中选择“在此处打开Powershell窗口” (在windows7中菜单显示的是“在此处打开命令窗口”)，启动命令行窗口
2. 在命令行窗口里，运行命令：python setup.py install，即可安装。

如下图：



### 2.3 安装Wireshark

在我们提供的资料中，在apps\_and\_drivers目录下有如下2个文件：



对于32位Windows系统，请安装Wireshark-win32-3.0.0.msi。

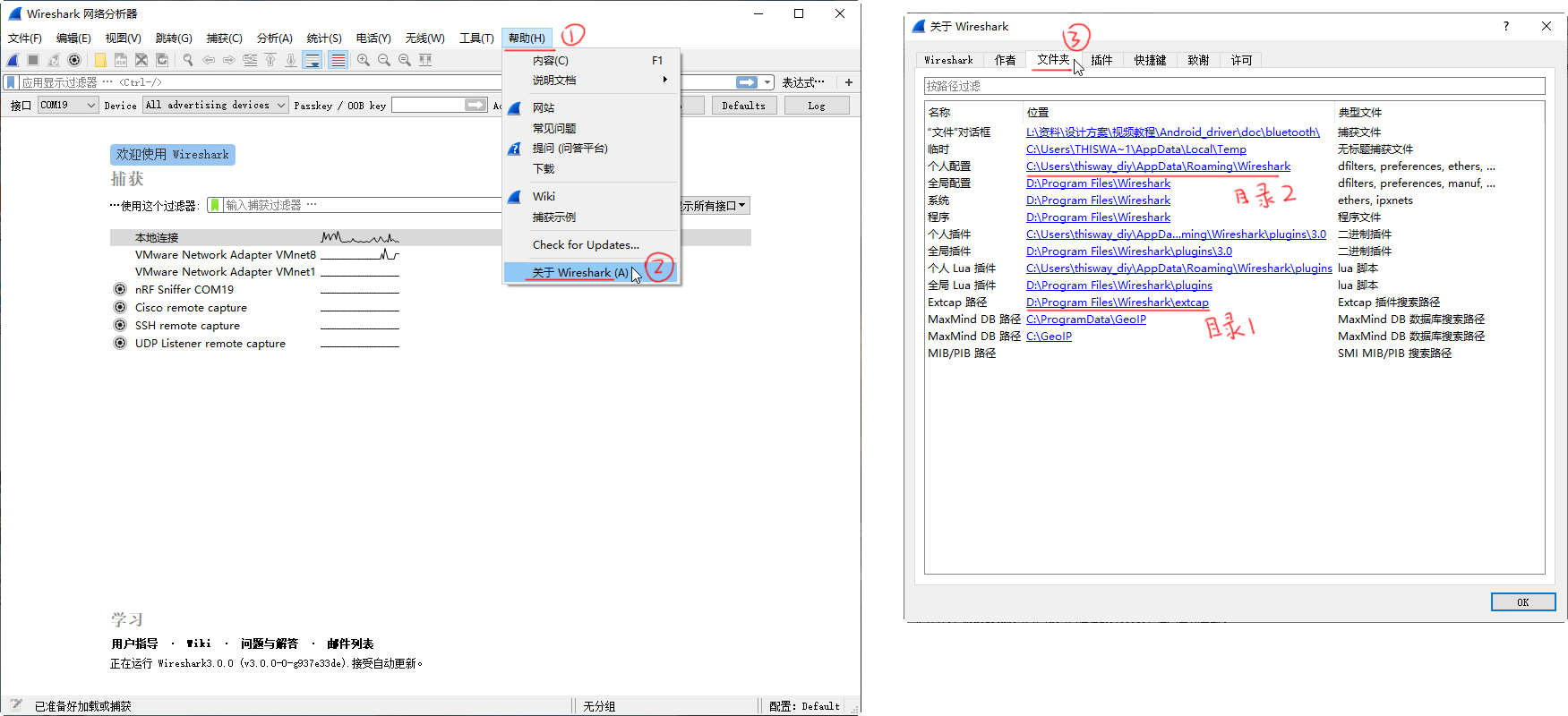
对于64位Windows系统，请安装Wireshark-win64-3.0.0.msi。

这些安装软件，也可以去官网下载：<https://www.wireshark.org/>

### 2.4 关联Wireshark和Sniffer

#### 2.4.1确定2个目录

运行Wireshark，点击“帮助 -> 关于Wireshark(A)”，如下图：



记住上图中的2个目录：“Extcap路径”，“个人配置”。这2个目录因人而已。

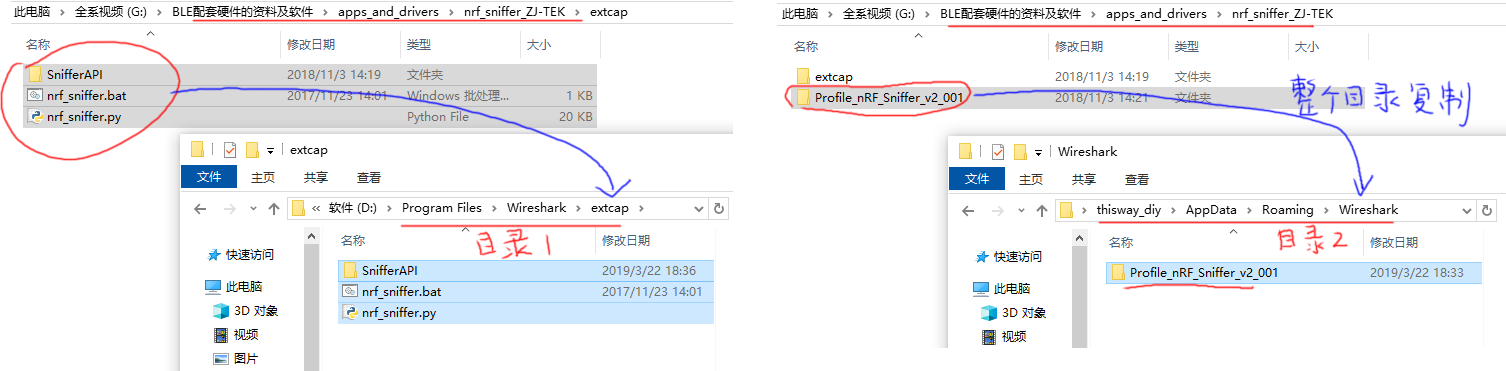
#### 2.4.2复制文件

在我们提供的资料中，在apps\_and\_drivers/ nrf\_sniffer\_ZJ-TEK中有2个子目录：

把extcap子目录下的所有内容，复制到上图中的目录1中；

把Profile\_nRF\_Sniffer\_v2\_001整个目录，复制到上图中的目录2中；

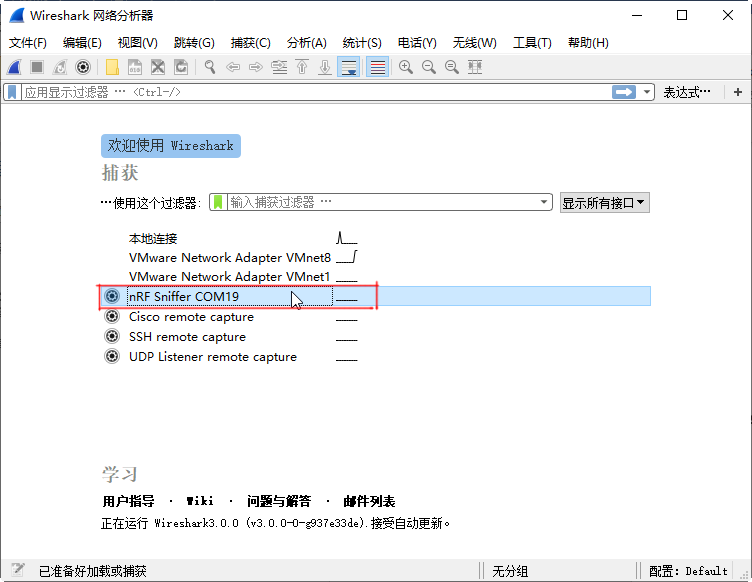
如下图所示：



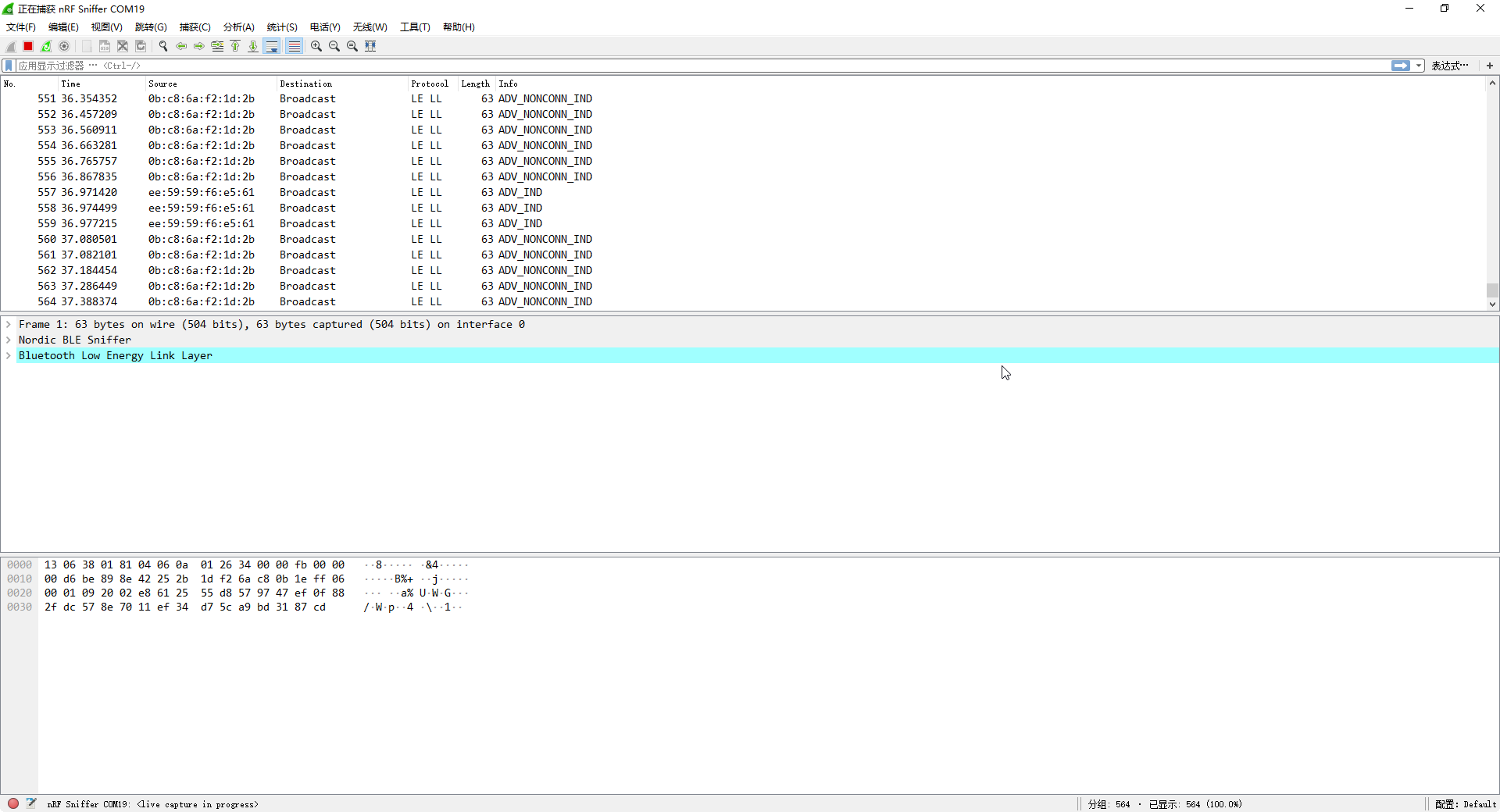
#### 2.4.3验证

在电脑上插入Sniffer，假设从设备管理器中看到它对应COM19(你的电脑上COM的编号可能不同)；

启动Wireshark，如果一切正常，在界面中可以看到COM19，如下图：



双击COM19即可开始抓包：



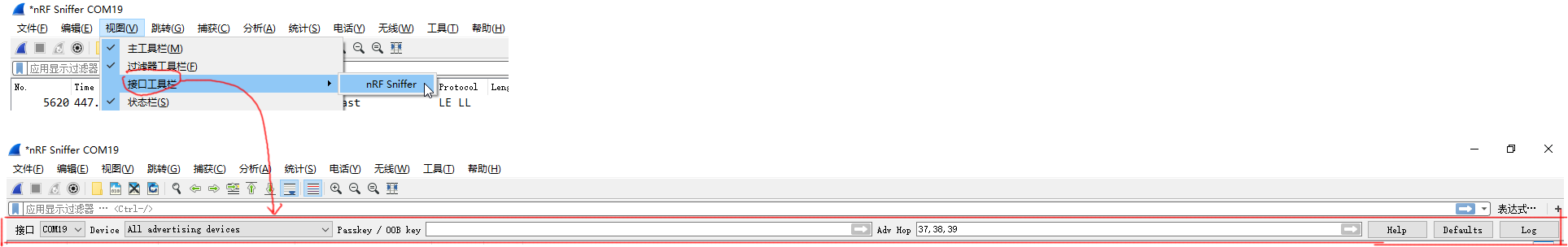
## Wireshark使用说明

### 3.1 启动Wireshark

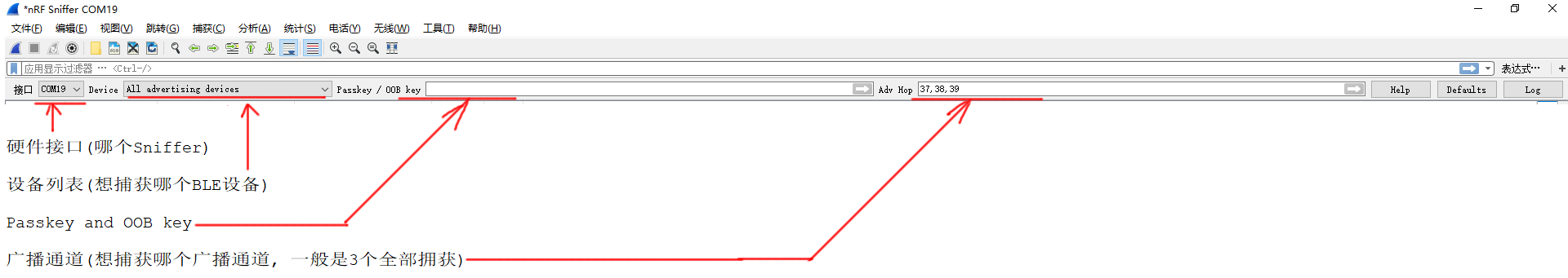
请参考《**2.4.3验证**》

### 3.2 打开接口工具栏

点击菜单“视图 -> 接口工具栏 -> nRF Sniffer”，如下图：

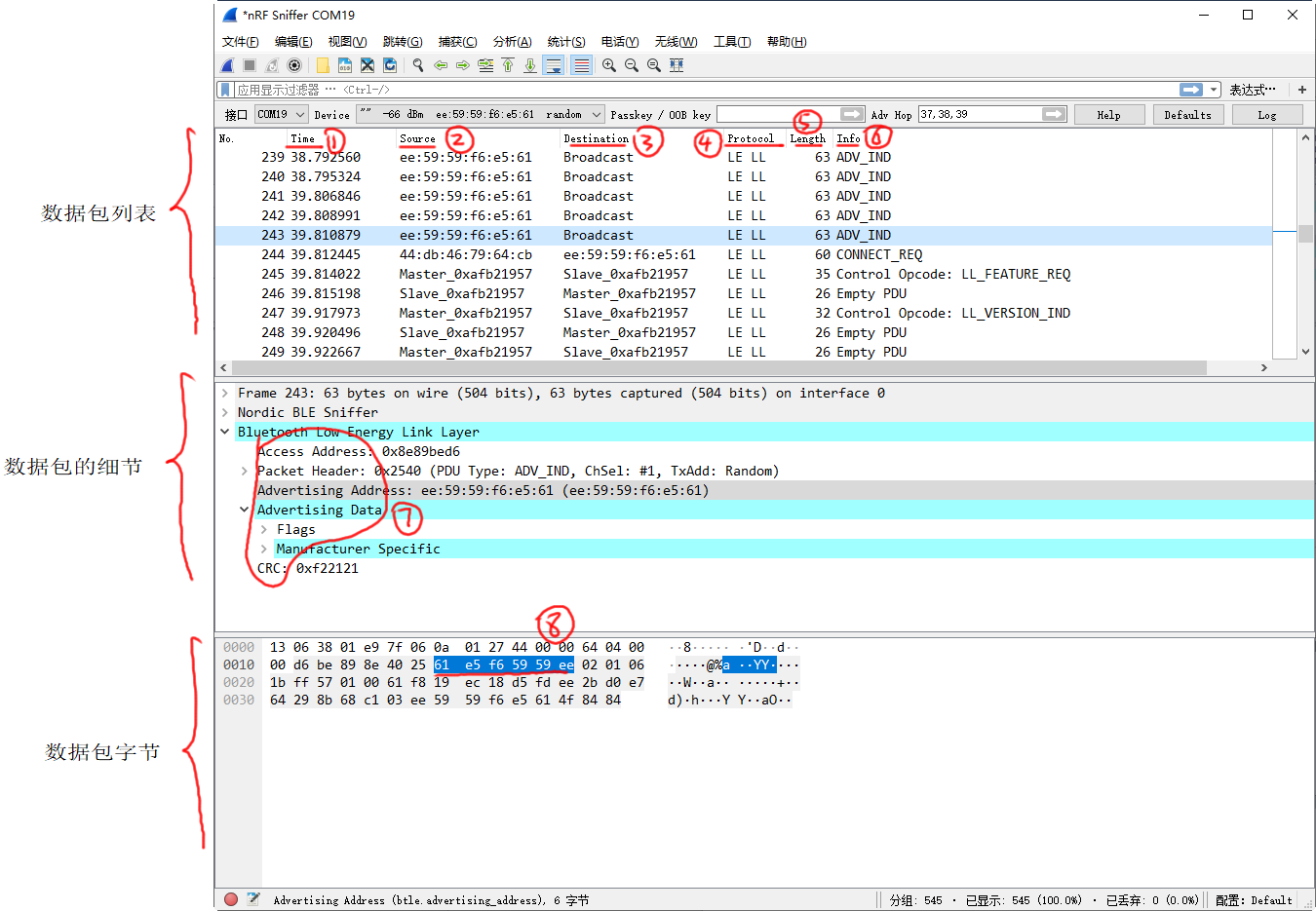


### 3.3 接口工具栏介绍



### 3.4 查看数据包

以下图为例来说明：



图中数据分为三栏：

数据包列表：每行表示捕获的一个数据包

数据包细节：点中“数据包列表”中的某行，会显示它的细节

数据包字节：原始数据

图中红色标号的含义：

1. 时间，捕获数据包的时间
2. 源：该数据包由谁发出，可以是源设备的MAC地址，也可以是某个连接的master或slave
3. 目的：该数据包发给谁，Broadcast表示这是广播包，否则是某个设备的MAC地址, 也可以是某个连接的master或slave
4. 协议：是哪层的数据
5. 长度
6. 包的信息
7. 数据包中的字段：点击前面的小箭头可以展开内部细节
8. 在⑦中点中某字段，会在⑧处把对应的数据反黑显示出来