抓取ble包

实现抓包需要以下

1 usb嗅探器，最好三个

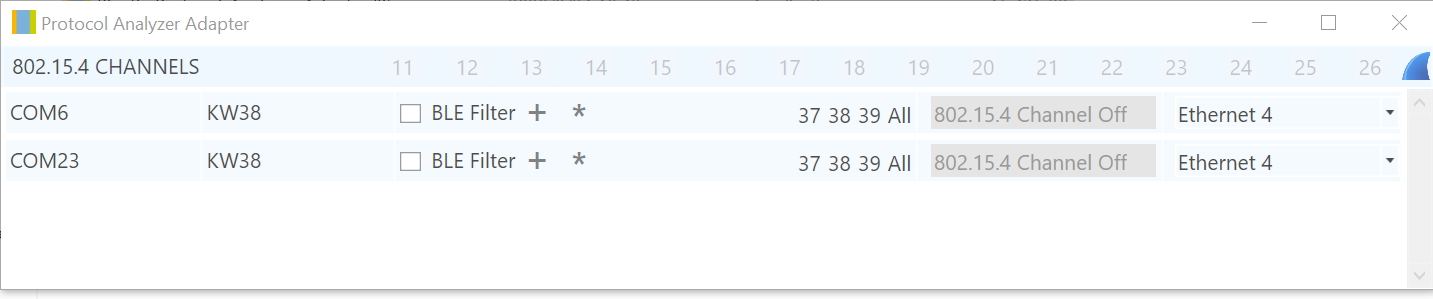
2 软件Kinetis\_Protocol\_Analyzer\_Adapter 2.0.2

3 wireshark，我用的是3.2.4

在安装Kinetis\_Protocol\_Analyzer\_Adapter会要求安装 TAP-Windows，给的链接失效了，自行安装tap。

一、基本用法

插入USB嗅探器，打开软件，会自动检测usb嗅探器

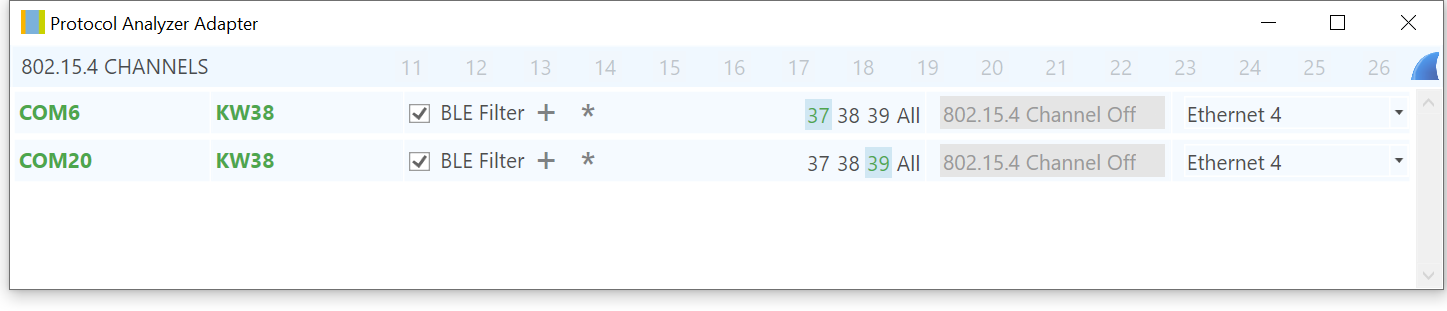


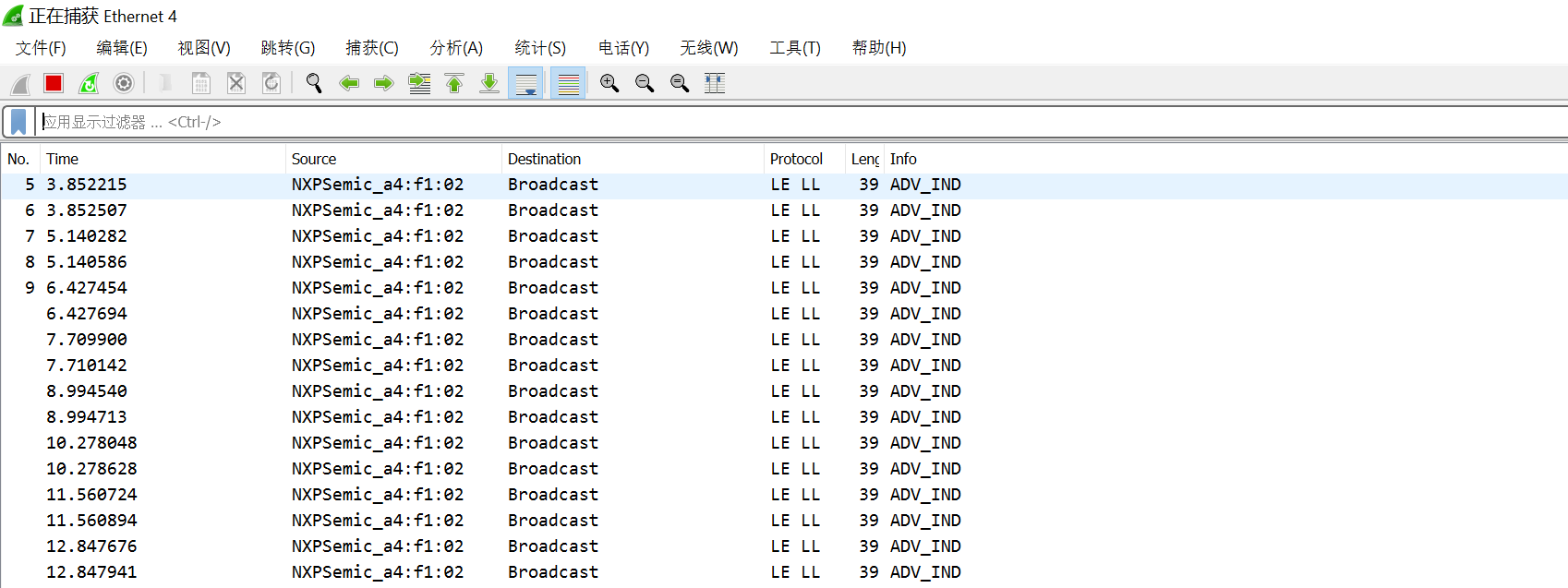
点击all，就可以检测37 38 39 三个通道,点击一个数字就检测一个通道，建议每个嗅探器检测一个通道。不要重复。这个工作原理是轮询每个广播通道获取数据，同时检测是否有连接事件，如果只用一个，万一连接事件发生在其他通道，就会错过连接事件，这样也就没法继续获得连接事件之后的数据。

点击右上角wireshark图标，就可以开始打开wireshark检测。

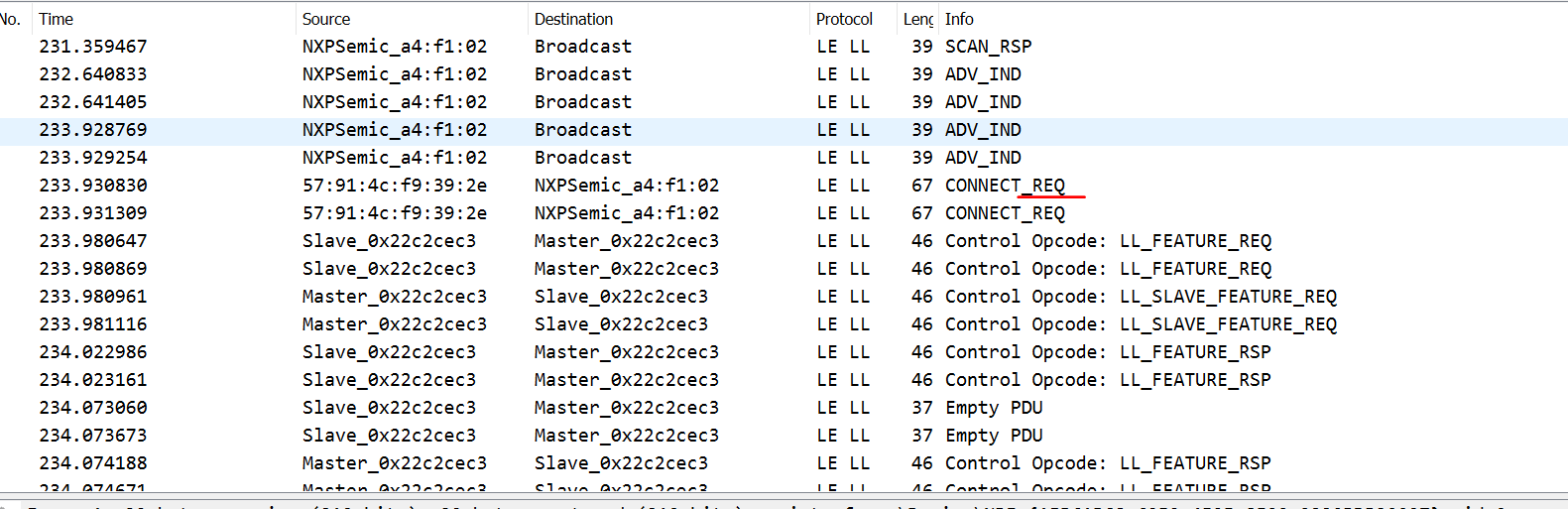
二、ble filter

用途在于专门检测某一个设备的地址，点击‘+’，再点击‘Add new address’，输入设备地址，再在ble filter前面点击，就会只接收这个地址的广播。我使用qn908x，知道他的地址是0xE05124A4F102。添加这个地址以后，只接收这个地址的数据。我使用了两个usb-kw38，分别检测37 和39两个通道。





此时如果连接设备就会出现如下包



三、wireshark的过滤

Ble的过滤的指令是btle\_ex，需要注意的是有ex，wireshark还有btle命令，这个命令是没法用来过滤数据的。

常用有btle\_ex.advertising\_address == E0:51:24:A4:F1:02过滤广播地址，结果同上图

btatt，获取所有ATT协议的数据

四、注意

usb-kw38预置的代码就是嗅探器的代码，如果要烧写其他代码，需要更新下jlink固件。如果这时候又想它作嗅探器，则参考这篇文章

<https://community.nxp.com/t5/Wireless-Connectivity-Knowledge/USB-KW41-Bluetooth-LE-Sniffer-Application-Update/ta-p/1100565>

所需要的bin文件在SDK\_2.6.5\_USB-KW38\tools\wireless\binaries。

注意是USB的sdk不是FRDM的sdk