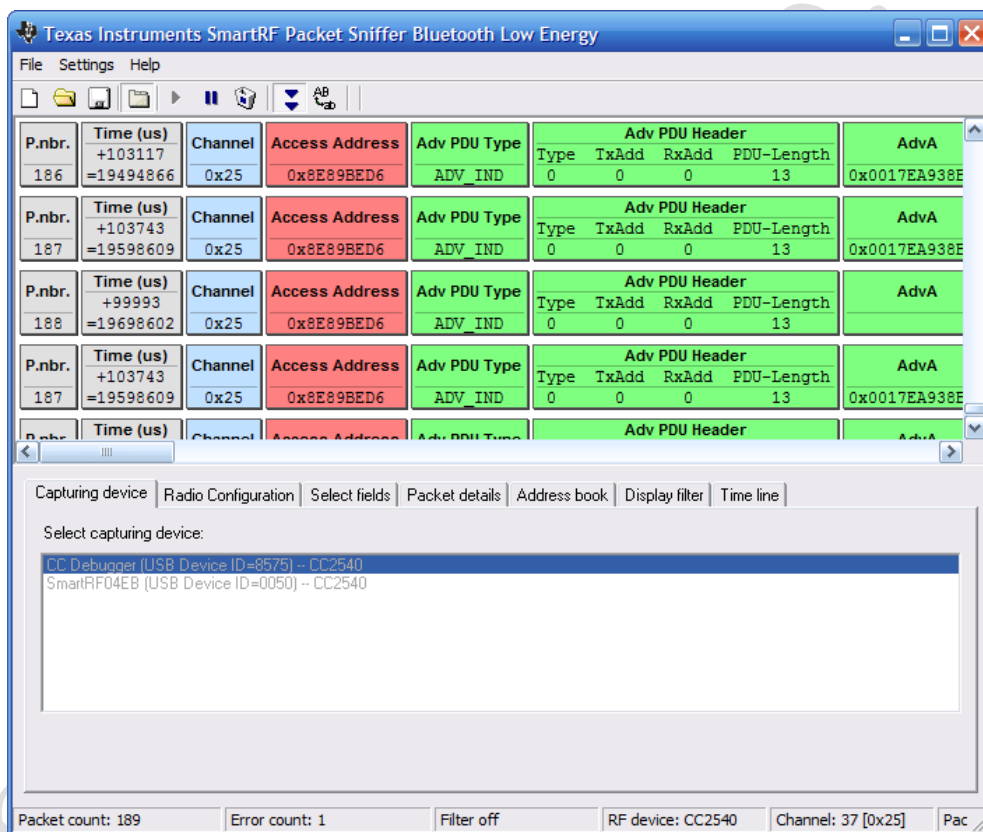




# 使用 CC-Debugger 实现 Packetsniffer 抓包功能



刘雨

15861666207

Ghostyu.taobao.com

2013-05



## 版本

V1.0	2013-05	初始版发布



## 目的

本文旨在指导用户使用 CC-Debugger 配合开发板实现 Packetsniffer 无线抓包功能。

阅读本文档前，请先阅读下列文档

Flash Programmer 使用指南



## 1 CC-Debugger

CC-Debugger 是 TI 新一代的 CC 系列芯片的仿真器，除了对芯片的仿真器调试外，还可作为 Packetsniffer 协议分析仪。



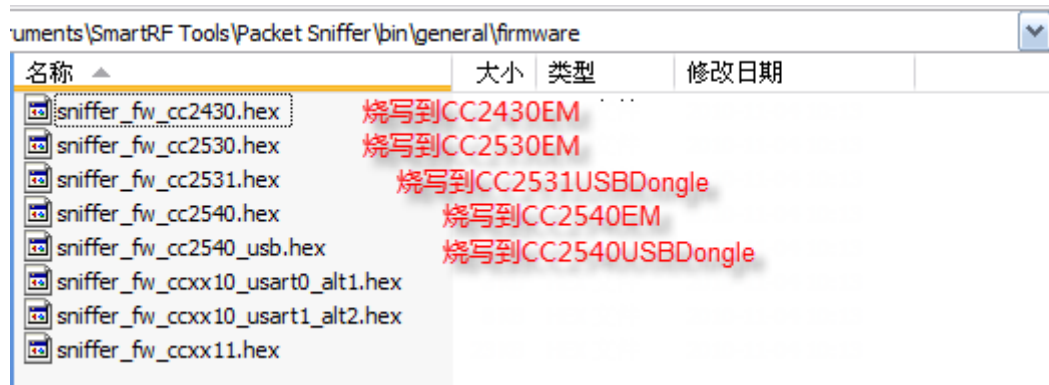
## 2 作为协议分析仪的条件

CC-Debugger 并不能像 usbdongle 那样独立的完成 packetsniffer 功能，需要连接相应的目标芯片，且连接的芯片需要烧写对应的 packetsniffer 固件。

也就是说 CC-Debugger+CCxxxx（烧写了 packetsniffer 固件），才相当于烧写了 packetsniffer 固件的 usbdongle。

Packetsniffer 固件位于 Packetsniffer 软件的安装目录，例如默认的目录如下：

C:\Program Files\Texas Instruments\SmartRF Tools\Packet Sniffer\bin\general\firmware





### 3 烧写 Packetsniffer 固件

使用 Flash Programmer 将上一节中介绍的 packetsniffer 固件烧写到开发板中。

Flash Programmer 使用方法参见《Flash Programmer 使用指南》

以 CC2540 为例。

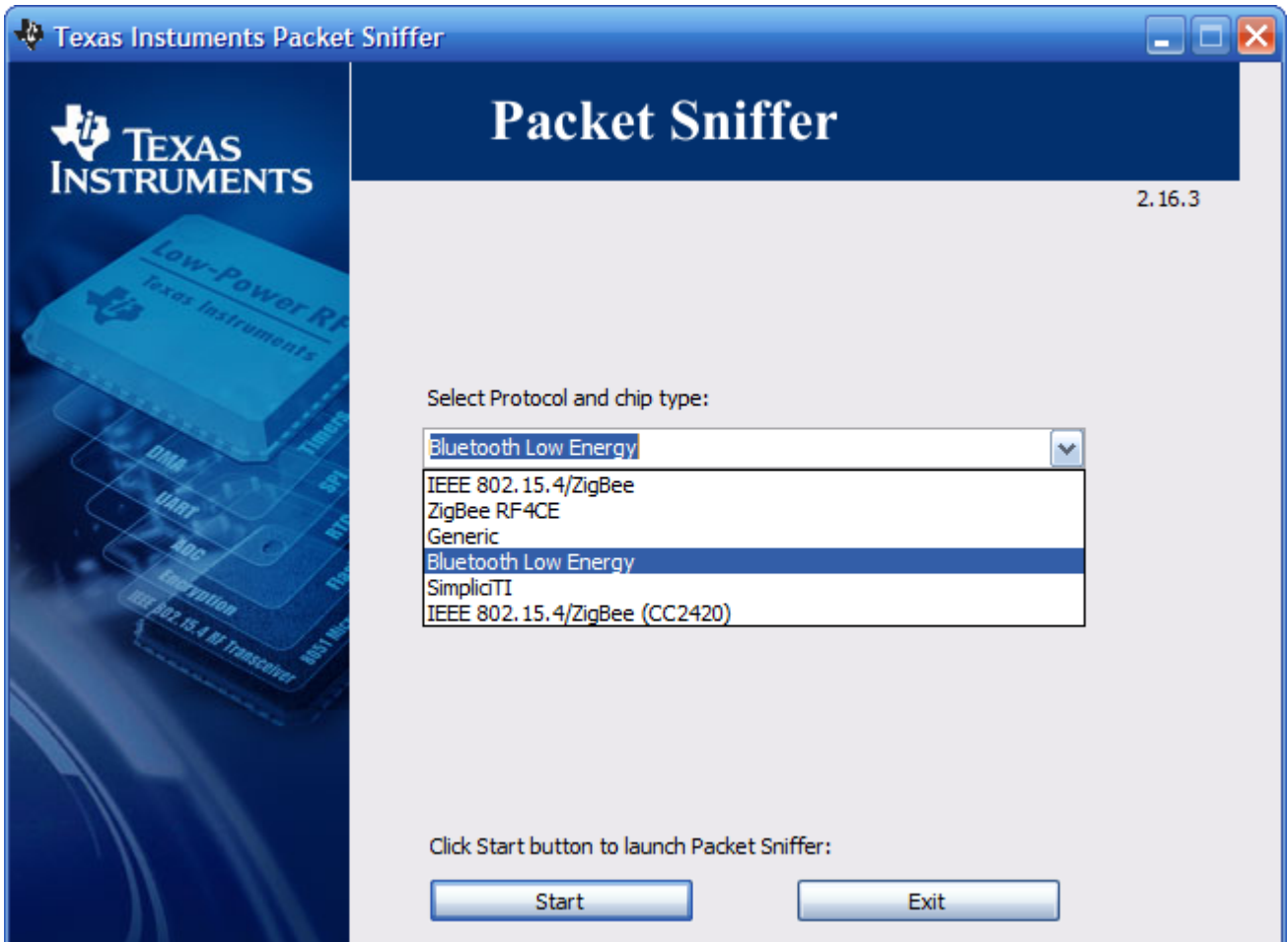
注意，这里描述有误，BB板debugger接口没有连接spi，无法做协议分析

- 1、将 CC-Debugger 连接到 BLE-SmartRF 开发板（或者 SmartRF-BB），并且给开发板上电。
- 2、将 sniffer\_fw\_cc2540.hex 通过 FlashProgrammer 烧写到 CC2540 中。



## 4 运行 PC 端 PacketSniffer 开始抓包

烧写完 PacketSniffer 固件后，保持 CC-Debugger 和开发板的连接，然后在电脑上打开 PacketSniffer 软件，并且选择 Bluetooth Low Energy 如下图：



IEEE 802.15.4/Zigbee 捕获 zigbee 数据包

Zigbee RF4CE 捕获 RF4CE 数据包

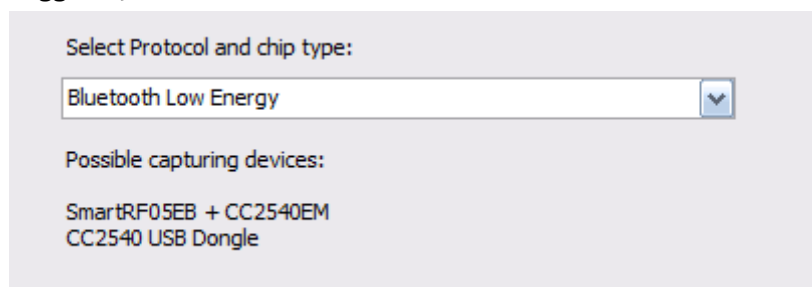
Generic 捕获一般的（无协议）数据包

Bluetooth Low Energy 捕获低功耗蓝牙的数据包

SimpliciTI 捕获 TI 的 SimpliciTI 协议数据包

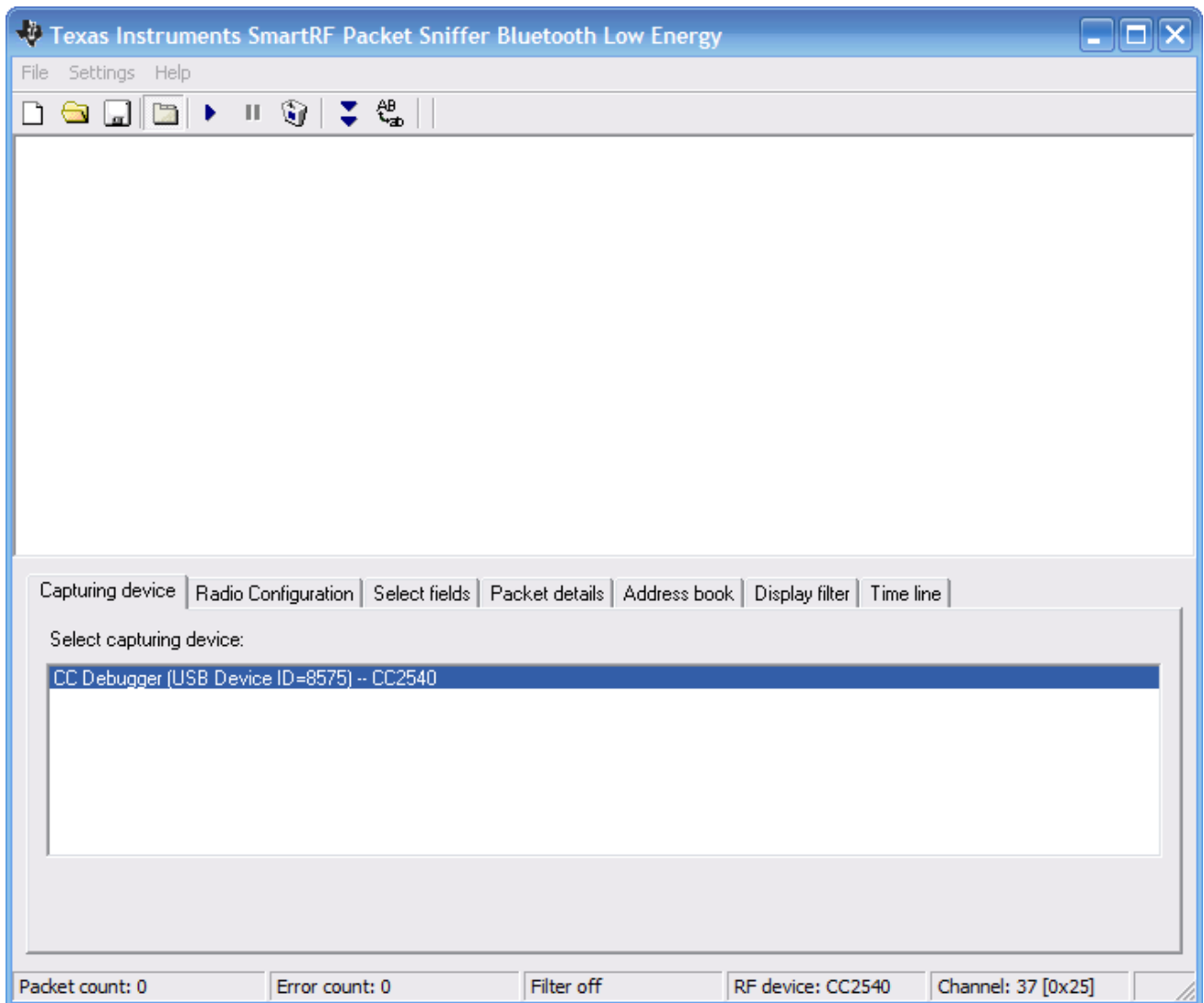
IEEE802.15.4/Zigbee(CC2420) 捕获 CC2420 的 zigbee 数据包

选择相应协议后，会在下方列出捕获该协议可以使用的抓包设备，例如 BLE，需要使用 CC2540USB Dongle，或者使用连接 CC-Debugger 的 SmartRF+CC2540EM

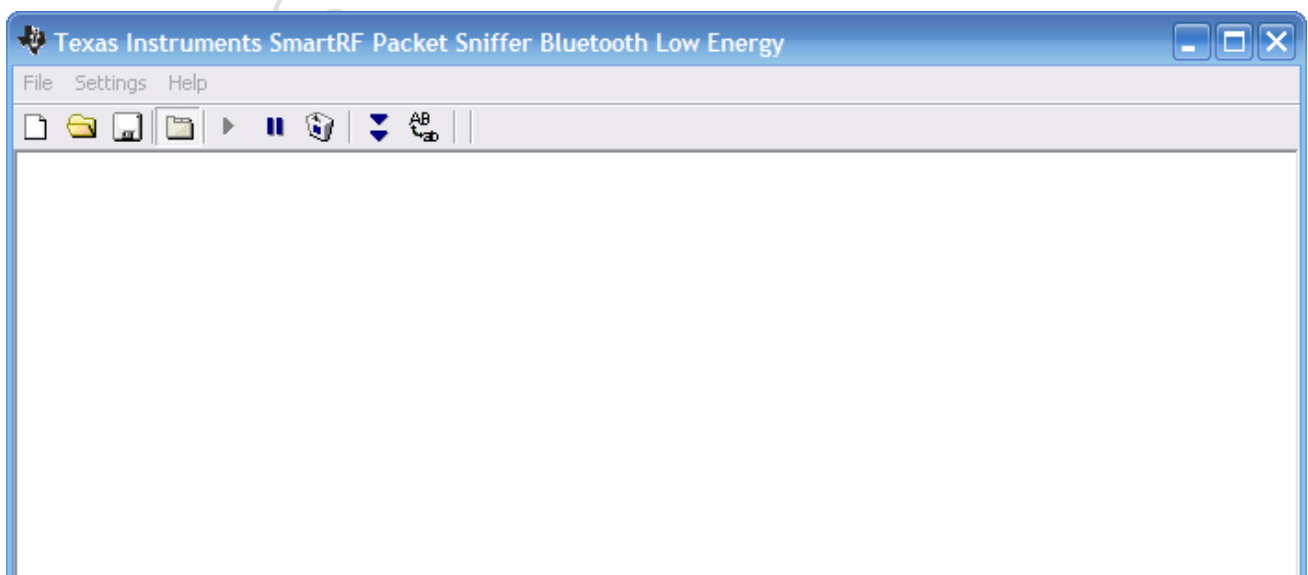




单击 Start 进入抓包界面，在下方的 Capturing device 中会出现可用的抓包工具，如下图，识别到的是 CC-Debugger+CC2540



然后单击蓝色小三角箭头，开始抓包，如下图：







没有任何数据？不要奇怪，这是因为空中没有符合条件的无线数据，不要认为 CC2540 已经在工作，就应该有蓝牙数据包，因为此时的 CC2540 是作为协议分析仪的一部分，并不会参数蓝牙的通信，如果使用该办法想捕获 CC2540 间的蓝牙数据包，则需要另外的两个运行 ble 协议栈的 CC2540 设备。

一旦有在广播的 ble 数据，就会出现在 PacketSniffer 的窗口中，如下图：

The screenshot displays the Texas Instruments SmartRF Packet Sniffer Bluetooth Low Energy application. The main window shows a list of captured packets with the following columns: P.nbr., Time (us), Channel, Access Address, Adv PDU Type, Adv PDU Header, and AdvA. The packets are filtered to show ADV\_IND types on channel 0x25.

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA
					Type TxAdd RxAdd PDU-Length	
390	+101868 =41678922	0x25	0x8E89BED6	ADV_IND	0 0 0 13	0x0017EA938E
391	+102492 =41781414	0x25	0x8E89BED6	ADV_IND	0 0 0 13	0x0017EA938E
392	+104993 =41886407	0x25	0x8E89BED6	ADV_IND	0 0 0 13	0x0017EA938E
393	+101243 =41987650	0x25	0x8E89BED6	ADV_IND	0 0 0 13	0x0017EA938E

Below the packet list, the 'Capturing device' tab is selected, showing a list of available devices. The device 'CC Debugger (USB Device ID=8575) - CC2540' is highlighted.

At the bottom, the status bar shows: Packet count: 393, Error count: 4, Filter off, RF device: CC2540, Channel: 37 [0x25].



## 5 PacketSniffer 中个字段的含义

当前请参考 TI 的 PacketSniffer 的软件帮助。

ghostyu.taobao.com



## 6 故障排查

如果确定各项连接 OK，并且有数据在广播，去无法捕获数据包，则请检查 Radio Configuration 中 channel 的设置是否与正在有数据交换的设备一致。如下图：

