Sniffer 制作

基于 ZigBee 开发板的 BRD4151 Kit

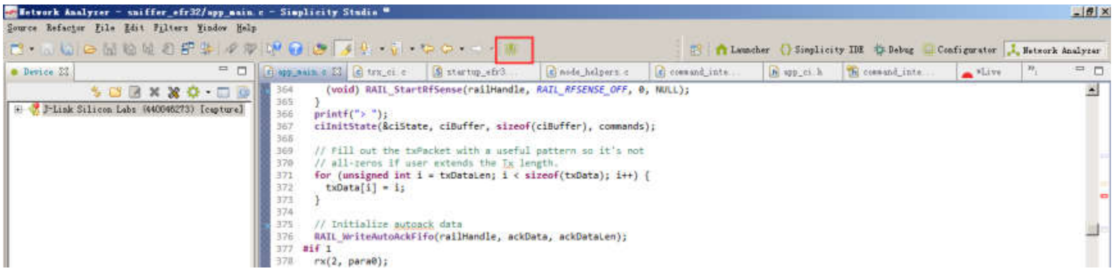
1. 烧写 Firmware 文件 sniffer_efr32.hex【制作过程见附录 A】

A. 命令行方式【有 Simplicity Commander 软件情况下】，进入 Dos 目录，输入下面的命令行即可

```
"D:\SiliconLabs\SimplicityStudio\v4\Simplicity Commander\commander" device masserase
"D:\SiliconLabs\SimplicityStudio\v4\Simplicity Commander\commander"   flash   sniffer_efr32.hex
```

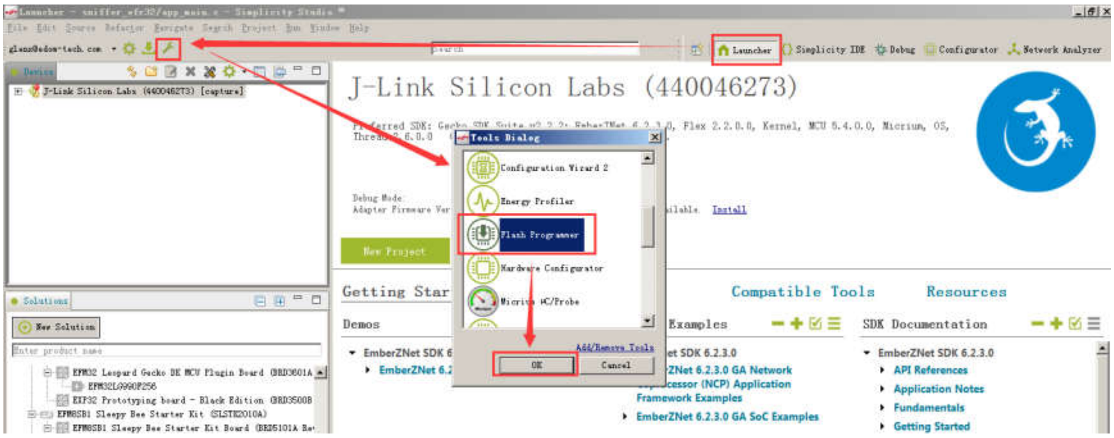
B. Simplicity Commander 的 Flash Program 烧写

点击工具栏按钮



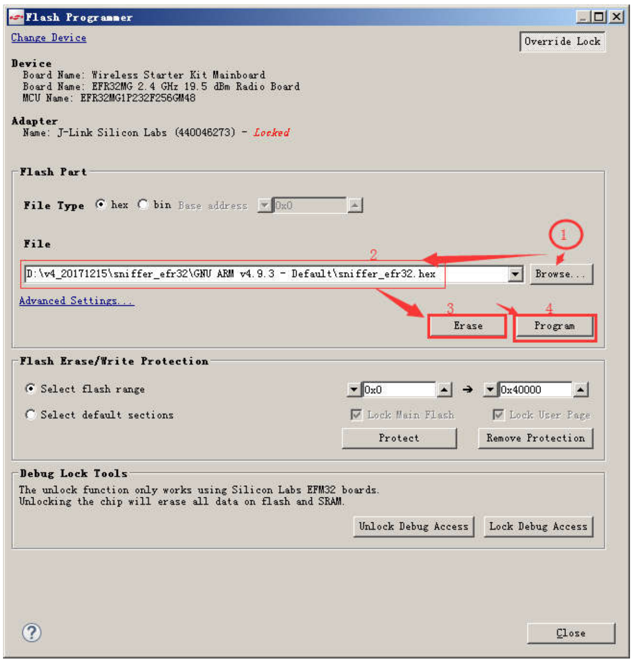
```
    (void) RAIL_StartRfSense(railHandle, RAIL_RFSENSE_OFF, 0, NULL);
  }
  printf("> ");
  ciInitState(&ciState, ciBuffer, sizeof(ciBuffer), commands);

  // Fill out the txPacket with a useful pattern so it's not
  // all-zeros if user extends the Tx length.
  for (unsigned int i = txDataLen; i < sizeof(txData); i++) {
    txData[i] = i;
  }

  // Initialize autoack data
  RAIL_WriteAutoAckFifo(railHandle, ackData, ackDataLen);
#if 1
  rx(2, param0);
```

或者



Preferred SDK: Gecko SDK Suite v2.2.2: EmberZNet 6.2.3.0, Flex 2.2.0.0, Kernel, MCU 5.4.0.0, Micrium, OS, Thread 2.6.0.0

然后如下烧写即可



Flash Programmer

Change Device

Override Lock

Device
  Board Name: Wireless Starter Kit Mainboard
  Board Name: EFR32MG 2.4 GHz 19.5 dBm Radio Board
  MCU Name: EFR32MG1P232F256GM48

Adapter
  Name: J-Link Silicon Labs (440046273) - *Locked*

Flash Part

File Type ● hex ○ bin Base address 0x0

File

D:\v4_20171215\sniffer_efr32\GNU ARM v4.9.3 - Default\sniffer_efr32.hex

Browse...

Advanced Settings...

Erase   Program

Flash Erase/Write Protection

● Select flash range   0x0 → 0x40000

○ Select default sections   ☑ Lock Main Flash   ☑ Lock User Page

Protect   Remove Protection

Debug Lock Tools

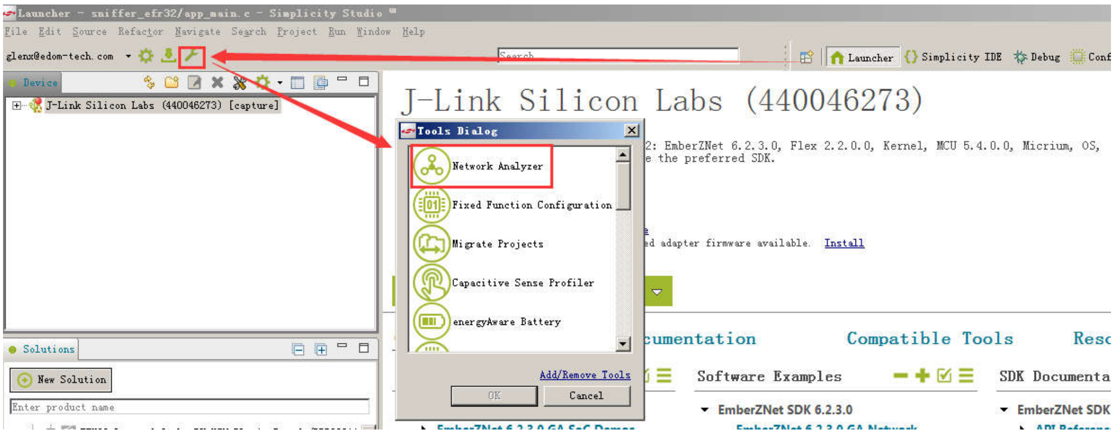
The unlock function only works using Silicon Labs EFM32 boards.
Unlocking the chip will erase all data on flash and SRAM.

Unlock Debug Access   Lock Debug Access

Close

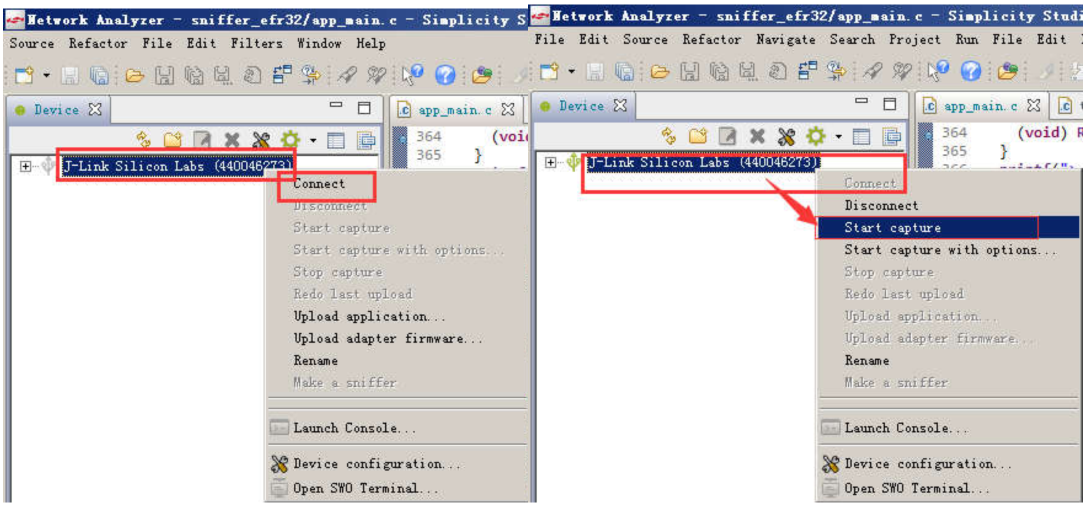
2. 抓包

工具栏打开 Network Analyzer【如果工具栏没有按照如下打开】

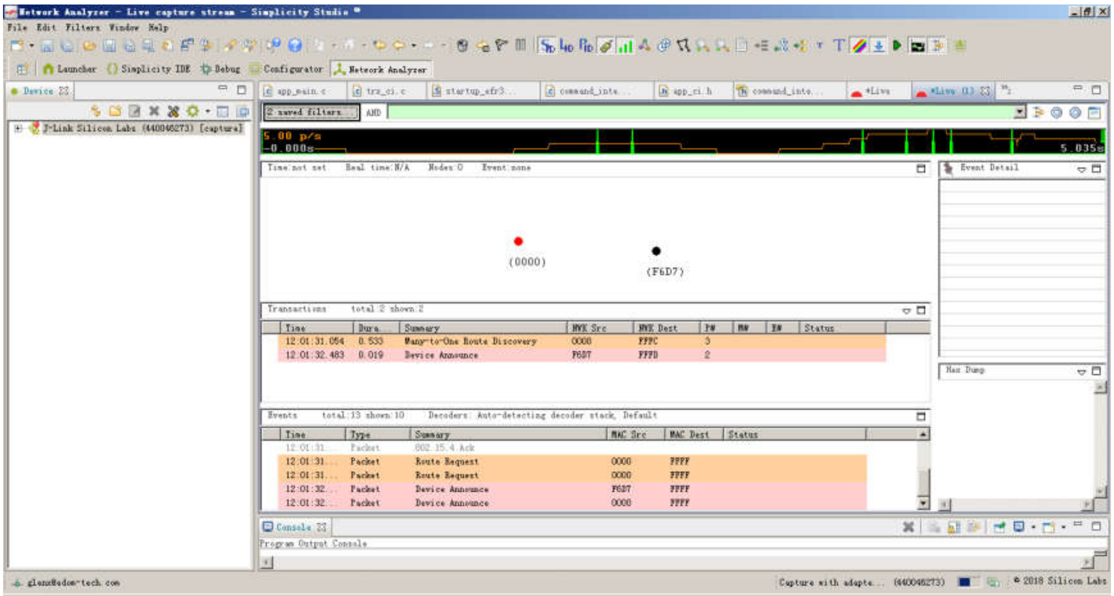


Launcher - sniffer_efr32/app_main.c - Simplicity Studio
File Edit Source Refactor Navigate Search Project Run Window Help
glenx@edom-tech.com
Search
Launcher
Simplicity IDE
Debug
Device
J-Link Silicon Labs (440046273) [capture]
J-Link Silicon Labs (440046273)
Tools Dialog
Network Analyzer
Fixed Function Configuration
Migrate Projects
Capacitive Sense Profiler
energyAware Battery
Add/Remove Tools
OK
Cancel
2: EmberZNet 6.2.3.0, Flex 2.2.0.0, Kernel, MCU 5.4.0.0, Micrium, OS,
e the preferred SDK.
ed adapter firmware available. Install
Solutions
New Solution
Enter product name
cumentation
Compatible Tools
Software Examples
SDK Documenta
EmberZNet SDK 6.2.3.0
EmberZNet SDK

然后连接设备，开始抓包



Network Analyzer - sniffer_efr32/app_main.c - Simplicity S
Source Refactor File Edit Filters Window Help
Device
app_main.c
364 (voi
365 }
J-Link Silicon Labs (440046273)
Connect
Disconnect
Start capture
Start capture with options...
Stop capture
Redo last upload
Upload application...
Upload adapter firmware...
Rename
Make a sniffer
Launch Console...
Device configuration...
Open SWO Terminal...
Network Analyzer - sniffer_efr32/app_main.c - Simplicity Studi
File Edit Source Refactor Navigate Search Project Run File Edit
Device
app_main.c
364 (void)
365 }
J-Link Silicon Labs (440046273)
Connect
Disconnect
Start capture
Start capture with options...
Stop capture
Redo last upload
Upload application...
Upload adapter firmware...
Rename
Make a sniffer
Launch Console...
Device configuration...
Open SWO Terminal...



Transactions total 2 shown 2

Time	Dura...	Summary	NWK Src	NWK Dest	PW	MW	EW	Status
12:01:31.054	0.533	Many-to-One Route Discovery	0000	FFFC	3			
12:01:32.483	0.019	Device Announce	F6D7	FFFD	2			

Events total 13 shown 10 Decoders: Auto-detecting decoder stack, Default

Time	Type	Summary	MAC Src	MAC Dest	Status
12:01:31...	Packet	802.15.4 Ack			
12:01:31...	Packet	Route Request	0000	FFFF	
12:01:31...	Packet	Route Request	0000	FFFF	
12:01:32...	Packet	Device Announce	F6D7	FFFF	
12:01:32...	Packet	Device Announce	0000	FFFF	

3. 常用串口命令

可以用 EVB 板的串口控制抓包命令，常用命令如下：

更改抓包的通道：**setChannel <Channel No>,** 例如抓 **11** 通道，

命令为： **setChannel 11** 【默认为 **11** 通道】

停止抓包命令： **rx 0**

开始抓包命令： **rx 1** 【默认状态为抓包状态】

4. 附录 A

1. Sniffer firmware

   按照 Silabs 论坛用 Flex SDK 制作 Sniffer 软件，链接地址

   https://www.silabs.com/community/wireless/zigbee-and-thread/knowledge-base.entry.html/2017/11/09/turning_any_efr32in-cbAD

2. 为了便于操作，把论坛中的初始化 Sniffer 命令行，写入了代码中，更改 app_main.c，主要是更改如下地方，红色部分

```
char paraInfo0[][32]={"rx","0"};
char paraInfo1[][32]={"config2p4GHz802154"};
char paraInfo2[][32]={"enable802154","rx","100","192","864"};
char paraInfo3[][32]={"setPromiscuousMode","1"};
char paraInfo4[][32]={"setChannel","11"};
char paraInfo5[][32]={"rx","1"};
char *para0[2]={paraInfo0[0], paraInfo0[1]};
char *para1[1]={paraInfo1[0]};
char *para2[5]={paraInfo2[0], paraInfo2[1], paraInfo2[2], paraInfo2[3],
paraInfo2[4]};
char *para3[2]={paraInfo3[0], paraInfo3[1]};
char *para4[2]={paraInfo4[0], paraInfo4[1]};
char *para5[2]={paraInfo5[0], paraInfo5[1]};

int main(void)
```

```
  // Initialize autoack data
  RAIL_WriteAutoAckFifo(railHandle, ackData, ackDataLen);
#if 1
  rx(2, para0);
  //config2p4Ghz802154(NULL, NULL);
  config2p4Ghz802154(1, para1);
  ieee802154Enable(5, para2);
  ieee802154SetPromiscuousMode(2, para3);
  setChannel(2, para4);
  rx(2, para5);
#endif
  //RAIL_StartRx(railHandle, channel, NULL); // Start in receive mode
  receiveModeEnabled = true;
  while (1) {
```