KCon 2017 洞见未来

KCon

重现速8僵尸车队

蓝牙4.0 BLE协议的进攻

杨 晋
ThreatBook

曾任职于 Microsoft，COMODO，Qihoo360

邮箱：yangjin@threatbook.cn
Linkedin：Jin Yang

PART 01　BLE是什么？

PART 02　协议技术特点

PART 03　寻找身边的设备

PART 04　如何嗅探BLE协议数据

PART 05　协议分析与攻击方式

目录
CONTENTS

01

BLE是什么？

BLE是什么？

- Bluetooth 4.0 协议家族（2012）
- 经典蓝牙（Classic Bluetooth）
- 高速蓝牙
- 低功耗蓝牙（**Bluetooth Low Energy**）

BLE是什么？

- BLE VS 经典蓝牙

技术规范	BLE	经典蓝牙
频率	2.4GHz	2.4GHz
作用距离	100m	10m
响应延时	1-3ms	100ms
安全性	128-bit AES	64/128-bit
能耗	1-50%	100%
传输数据速率	1Mb/s	1-3Mb/s

BLE是什么？

- 哪些设备在使用BLE协议？

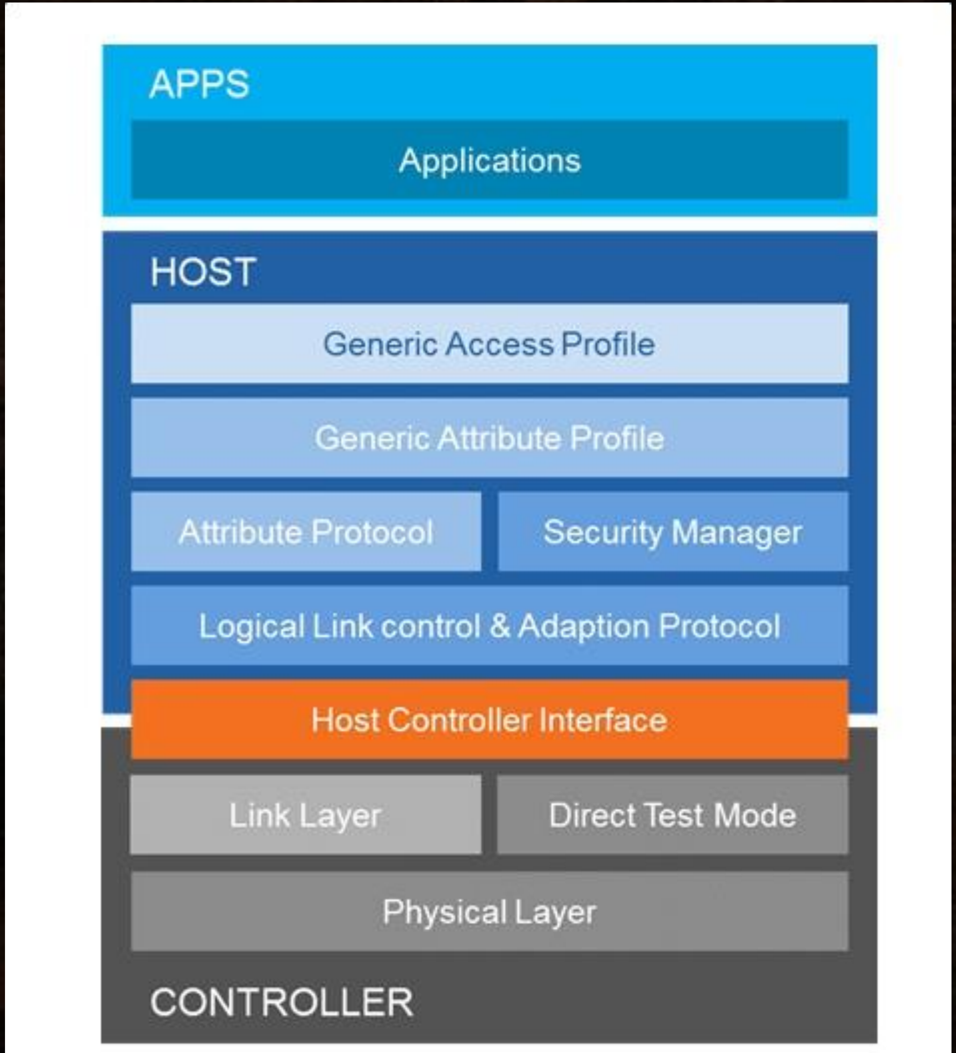
- 可穿戴设备：智能手表、手环、无线耳机、鼠标/键盘

- 家庭用智能设备：门锁、智能玩具、音箱

- 特种行业内设备：医疗器械、汽车、自动化

02 协议技术特点

协议技术特点



APPS

Applications

HOST

Generic Access Profile

Generic Attribute Profile

Attribute Protocol | Security Manager

Logical Link control & Adaption Protocol

Host Controller Interface

Link Layer | Direct Test Mode

Physical Layer

CONTROLLER

BLE协议栈

APP

HOST

CONTROLLER

协议技术特点

控制器部分 **（Controller）**
物理层 （Physical Layer）
链路层 （Link Layer）
主机控制接口层 （Host Controller Interface）

主机 **（Host）**
GATT 通用属性配置文件层 （Generic Attribute Profile）
GAP 通用访问配置文件层 （Generic Access Profile）
L2CAP 逻辑链路控制及自适应协议层 （Logical Link Control and Adaptation Protocol）
安全管理层（Security Manager）
ATT 属性协议层（Attribute Protocol）

协议技术特点

- 物理层特性：

- 免费的ISM频段：2.400 - 2.4835 GHz

- 分为40个频段：0 – 39 （每份的带宽为2MHz）

- 跳频通信 （Hopping）

协议技术特点

- 广播频段与数据频段
- 3 channels：37 38 39
- 37 channels：0 – 36
- 广播频段跳频与数据频段跳频

协议技术特点

频率	频段类型	数据频道编号	广播频道编号
2402MHz	广播		37
2404MHz	数据	0	
…	数据	…	
2424MHz	数据	10	
2426MHz	广播		38
2428MHz	数据	11	
…	数据	…	
2478MHz	数据	36	
2480MHz	广播		39

协议技术特点

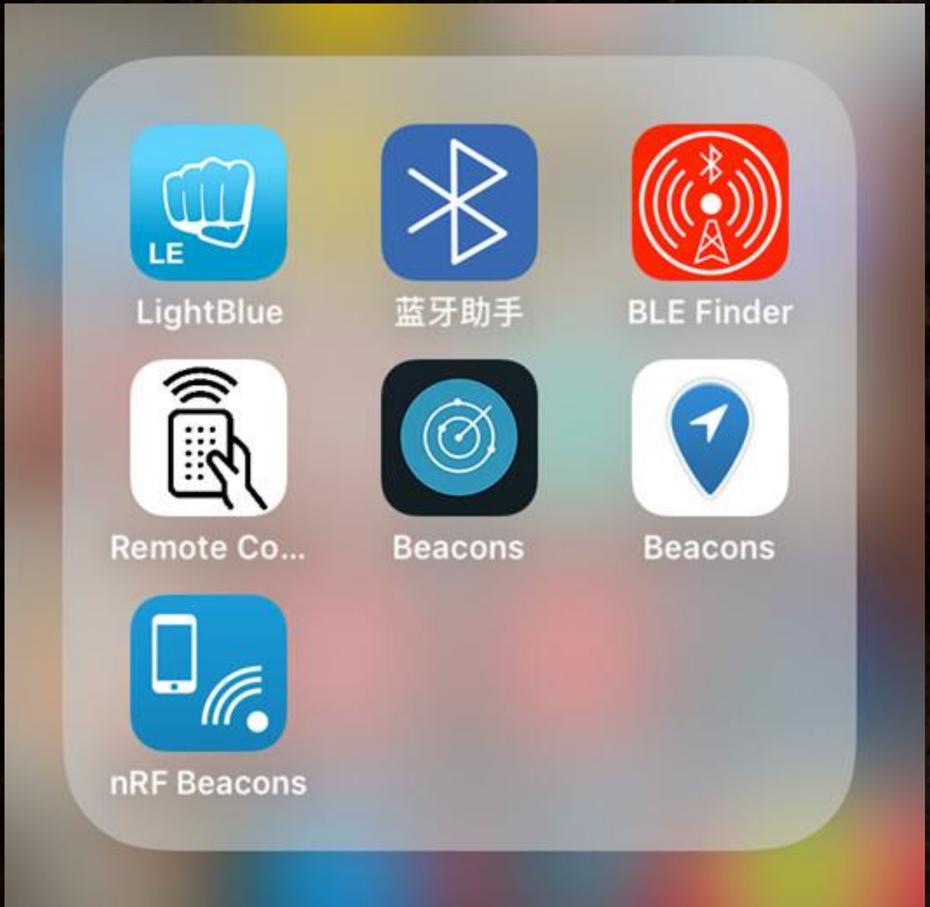
当发生ADV_CONNECT_REQ后，确定了 Hop Increment = 0x0C
Data Channel 12
Data Channel 24
Data Channel 36
Data Channel 11
Data Channel 23
Data Channel 35
Data Channel 10

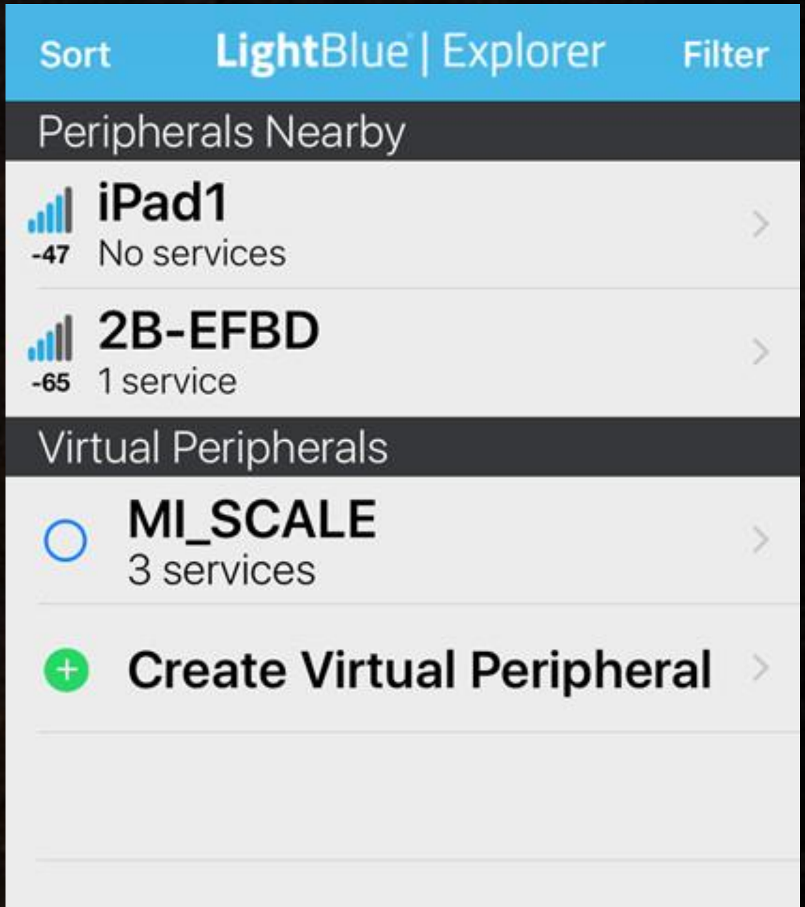
03

寻找身边的设备

寻找身边的设备

- 最简单的方法 iPhone （ LightBlue、BLE Finder ... ）





Peripherals Nearby

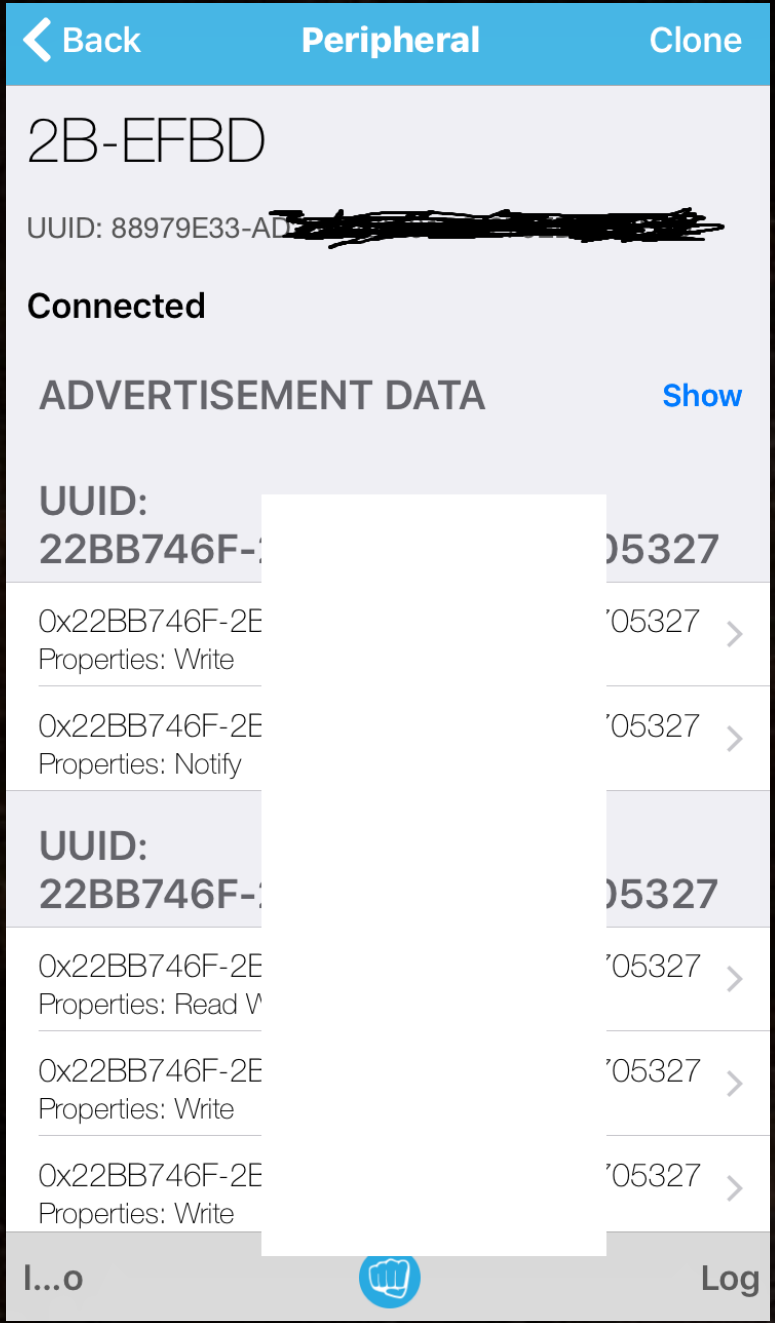
-47 iPad1
No services

-65 2B-EFBD
1 service

Virtual Peripherals

MI_SCALE
3 services

Create Virtual Peripheral



Back **Peripheral** Clone

2B-EFBD

UUID: 88979E33-AD[redacted]

Connected

ADVERTISEMENT DATA Show

UUID: 22BB746F-[redacted]05327

0x22BB746F-2E[redacted]'05327
Properties: Write

0x22BB746F-2E[redacted]'05327
Properties: Notify

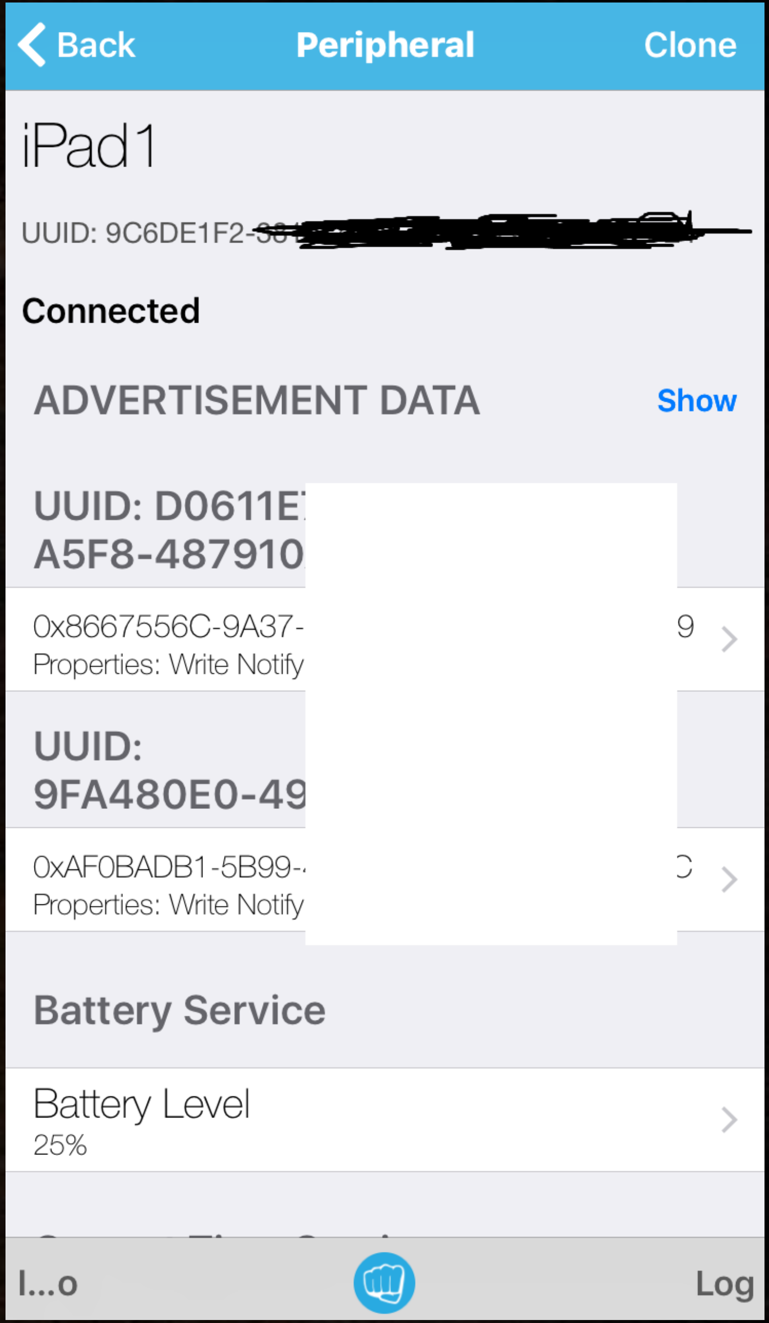
UUID: 22BB746F-[redacted]05327

0x22BB746F-2E[redacted]'05327
Properties: Read W[redacted]

0x22BB746F-2E[redacted]'05327
Properties: Write

0x22BB746F-2E[redacted]'05327
Properties: Write

I...o Log



Back **Peripheral** Clone

iPad1

UUID: 9C6DE1F2-[redacted]

Connected

ADVERTISEMENT DATA Show

**UUID: D0611E[redacted]
A5F8-487910[redacted]**

0x8667556C-9A37-[redacted]9
Properties: Write Notify

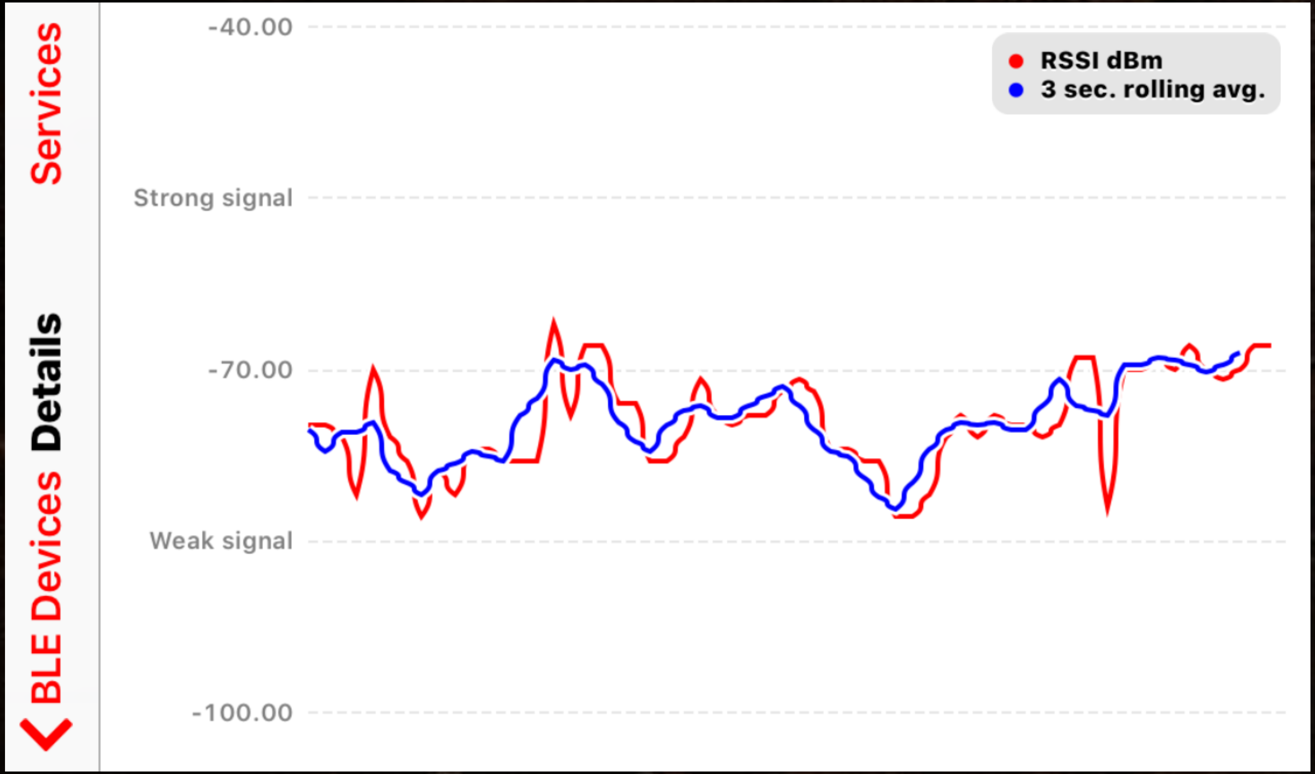
**UUID:
9FA480E0-49[redacted]**

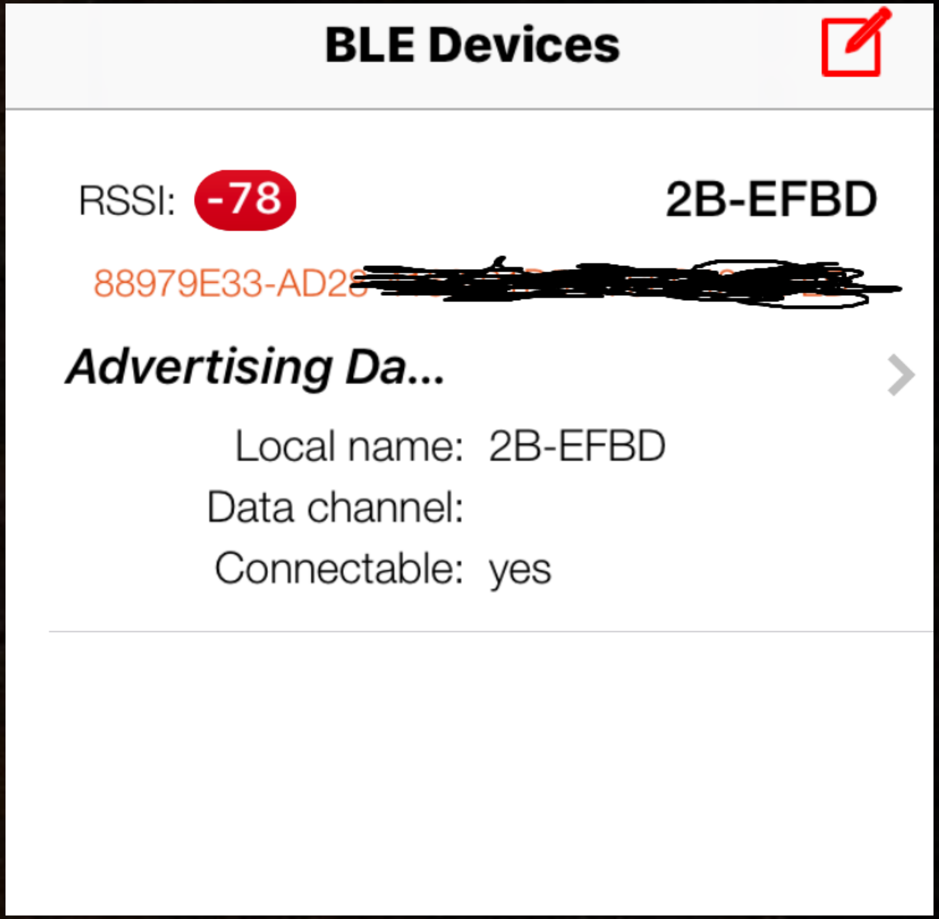
0xAF0BADB1-5B99-[redacted]C
Properties: Write Notify

Battery Service

Battery Level
25%

I...o Log





BLE Devices

RSSI: -78 2B-EFBD

88979E33-AD2[redacted]

Advertising Da...

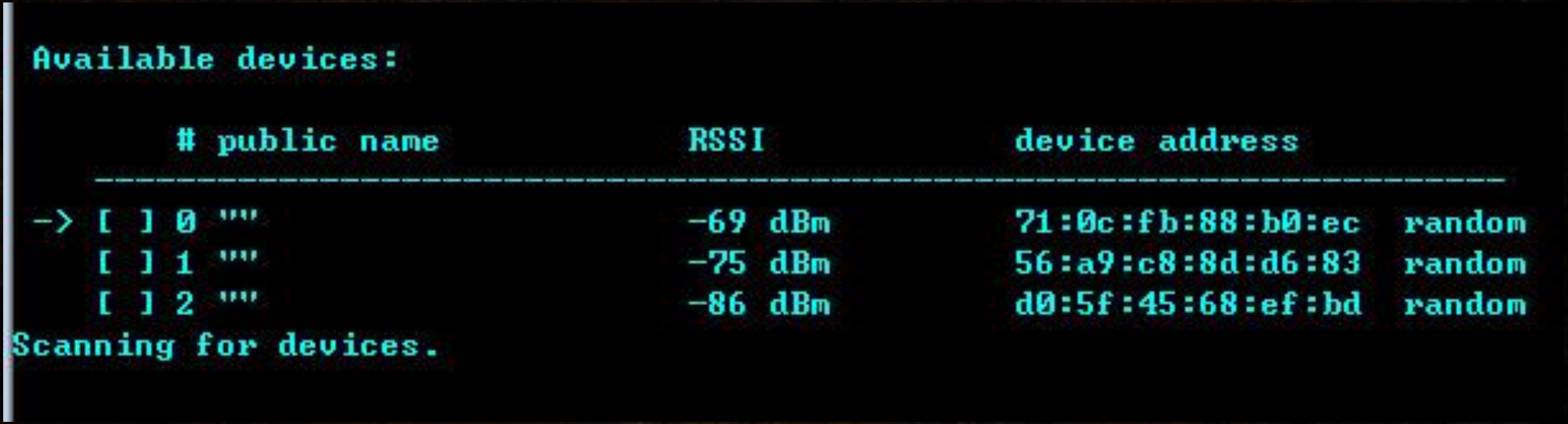
Local name: 2B-EFBD

Data channel:

Connectable: yes

寻找身边的设备

- 利用 nRF51822 芯片来寻找

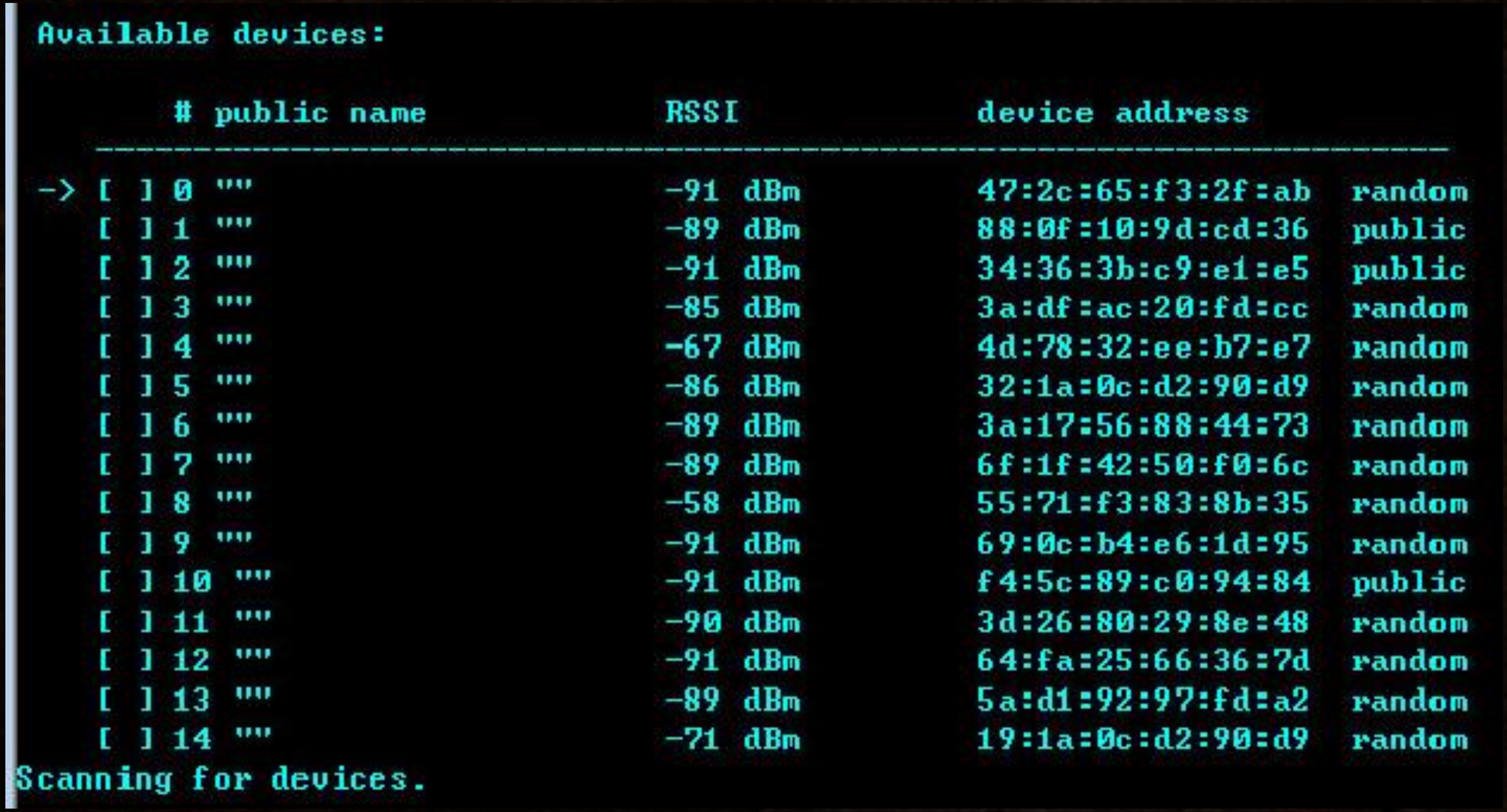


```
 Available devices:

       # public name                RSSI            device address
    ------------------------------------------------------------------------
 -> [ ] 0 ""                        -69 dBm         71:0c:fb:88:b0:ec  random
    [ ] 1 ""                        -75 dBm         56:a9:c8:8d:d6:83  random
    [ ] 2 ""                        -86 dBm         d0:5f:45:68:ef:bd  random
Scanning for devices.
```

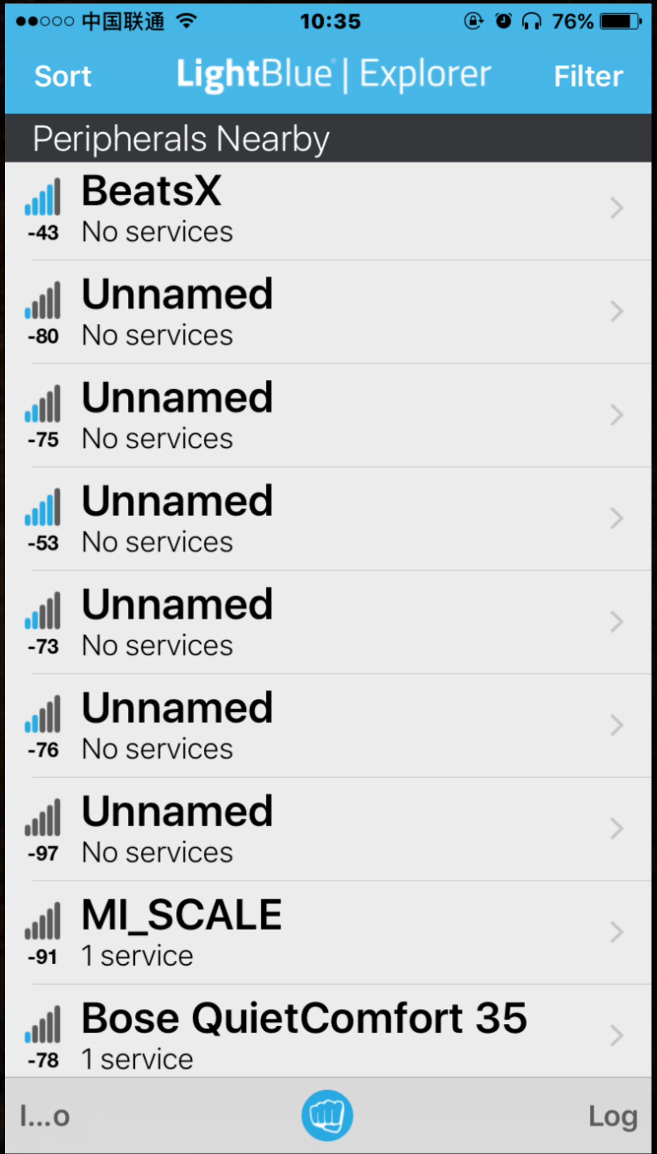
寻找身边的设备

- 大概判断一个设备的距离



```
Available devices:

      # public name              RSSI          device address
    ------------------------------------------------------------------
-> [ ] 0 ""                      -91 dBm       47:2c:65:f3:2f:ab  random
   [ ] 1 ""                      -89 dBm       88:0f:10:9d:cd:36  public
   [ ] 2 ""                      -91 dBm       34:36:3b:c9:e1:e5  public
   [ ] 3 ""                      -85 dBm       3a:df:ac:20:fd:cc  random
   [ ] 4 ""                      -67 dBm       4d:78:32:ee:b7:e7  random
   [ ] 5 ""                      -86 dBm       32:1a:0c:d2:90:d9  random
   [ ] 6 ""                      -89 dBm       3a:17:56:88:44:73  random
   [ ] 7 ""                      -89 dBm       6f:1f:42:50:f0:6c  random
   [ ] 8 ""                      -58 dBm       55:71:f3:83:8b:35  random
   [ ] 9 ""                      -91 dBm       69:0c:b4:e6:1d:95  random
   [ ] 10 ""                     -91 dBm       f4:5c:89:c0:94:84  public
   [ ] 11 ""                     -90 dBm       3d:26:80:29:8e:48  random
   [ ] 12 ""                     -91 dBm       64:fa:25:66:36:7d  random
   [ ] 13 ""                     -89 dBm       5a:d1:92:97:fd:a2  random
   [ ] 14 ""                     -71 dBm       19:1a:0c:d2:90:d9  random
Scanning for devices.
```



Peripherals Nearby

-43	BeatsX	No services
-80	Unnamed	No services
-75	Unnamed	No services
-53	Unnamed	No services
-73	Unnamed	No services
-76	Unnamed	No services
-97	Unnamed	No services
-91	MI_SCALE	1 service
-78	Bose QuietComfort 35	1 service

04 如何嗅探BLE协议数据

如何嗅探BLE协议数据

- 嗅探 广播频道数据

- 嗅探 数据频道数据

- 处理跳频

- 4种嗅探BLE协议数据的设备

如何嗅探BLE协议数据

- Ubertooth One （2011）

- Ubertooth 是著名无线硬件黑客 Michael Ossmann 研发的一个基于2.4GHz的开源无线蓝牙开发平台，共有两个版本分别是 Ubrtooth-One 和 Ubertooth-Zero ，而 Zero 版本已经停止开发，很多的最新功能以及平台已经无法支持 Zero

- Ubertooth + Wireshark + Kismet + Crackle

如何嗅探BLE协议数据

- Ubertooth 负责嗅探BLE协议数据并存储

- Wireshark + Kismet 分析BLE报文

- Crackle 在获取到一定数量的BLE报文之后，就可以用它来破解出 STK/LTK

  https://github.com/mikeryan/crackle

如何嗅探BLE协议数据

Ubertooth One

如何嗅探BLE协议数据

- HackRF SDR，8 bit

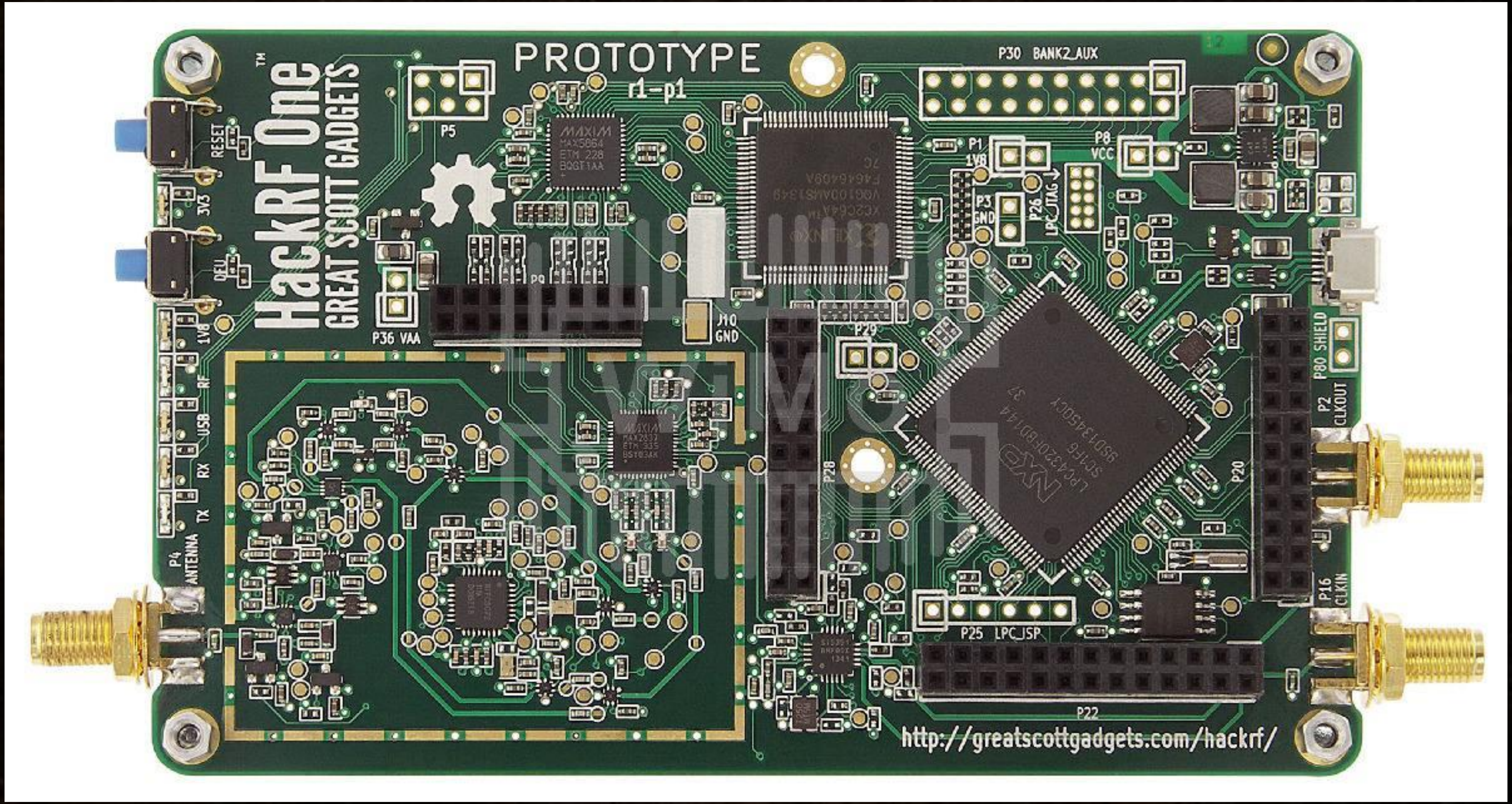
- Michael Ossmann 和 Jared Boone 一起研发的一款廉价且功能丰富的SDR硬件

- 支持GNURadio的全开源SDR，工作频率 10MHz - 6GHz

- USB 2.0

- btle_rx btle_tx (https://github.com/JiaoXianjun/BTLE)

如何嗅探BLE协议数据



如何嗅探BLE协议数据

- BladeRF SDR，12 bit
- 工作频率：300 MHz – 3.8 GHz
- 全双工的一款神器
- USB 3.0
- btle_rx btle_tx (https://github.com/JiaoXianjun/BTLE)

如何嗅探BLE协议数据

如何嗅探BLE协议数据

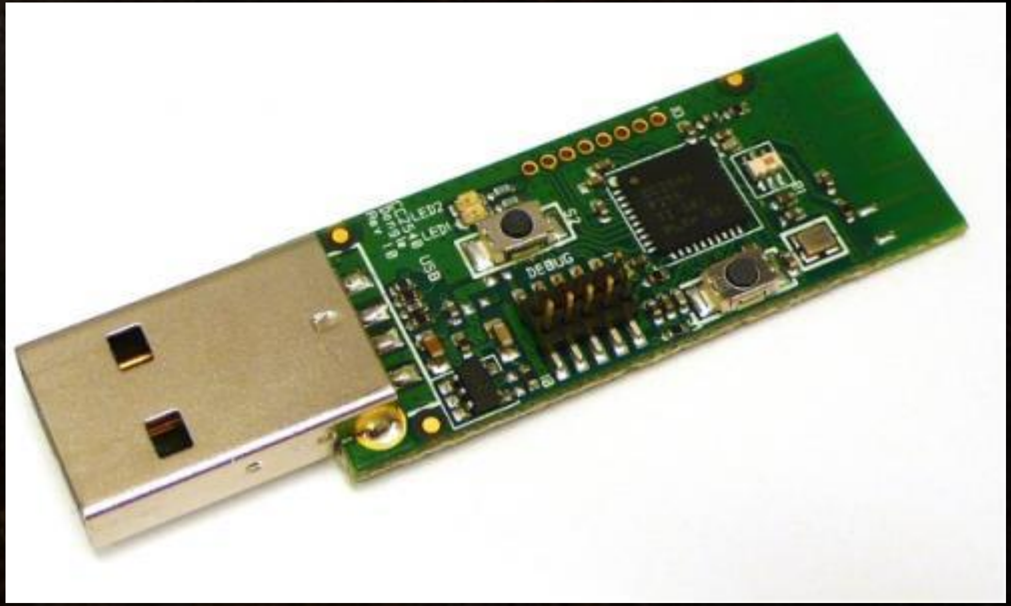
- nRF51822芯片 CC2540芯片

- 这些产品实际上是智能设备使用的芯片，但是也可以做 BLE Sniffer来使用

- 功能单一只支持蓝牙BLE协议

- 价格便宜

如何嗅探BLE协议数据



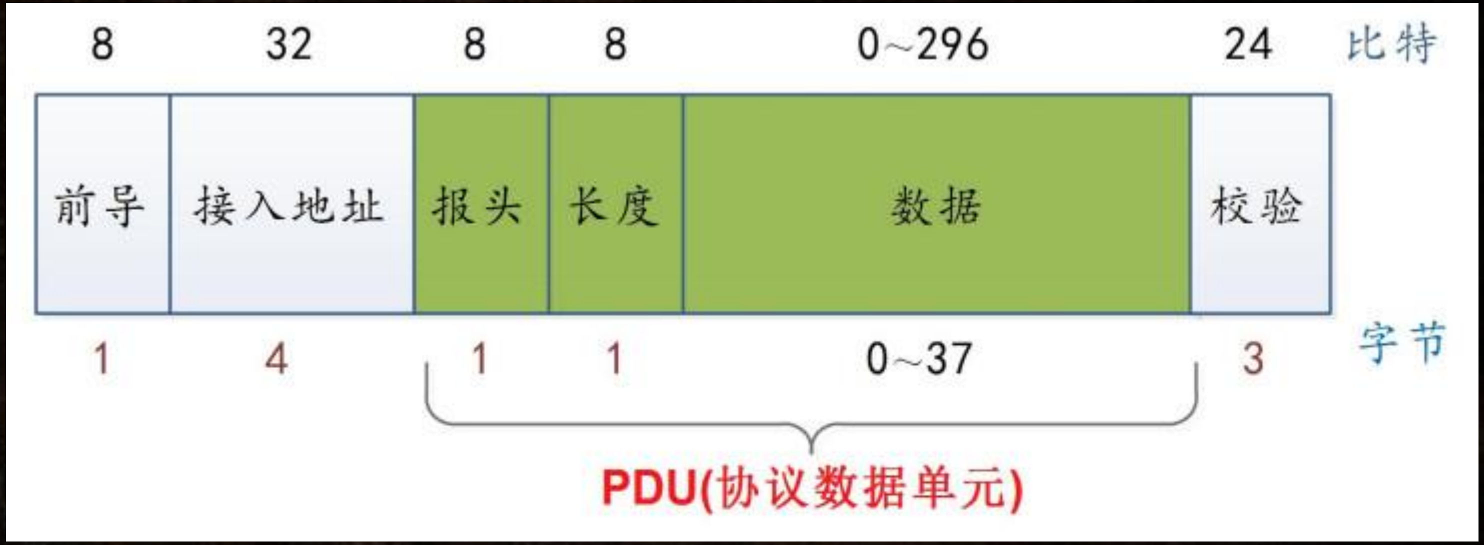
如何嗅探BLE协议数据

	Ubertooth	HackRF	BladeRF	nRF51822
工作频率	2.4G	10 MHz - 6GHz	300 MHz - 3.8GHz	BLE 2.4G
工作方式	半双工	半双工	全双工	半双工
接口	USB 2.0	USB 2.0	USB 3.0	USB 2.0
应用范围	蓝牙	SDR	SDR	蓝牙BLE
开源资源	全开源	全开源	部分	部分
价格	1000	2000	2800	100

05 协议分析与攻击方式

BLE协议分析

- BLE报文结构



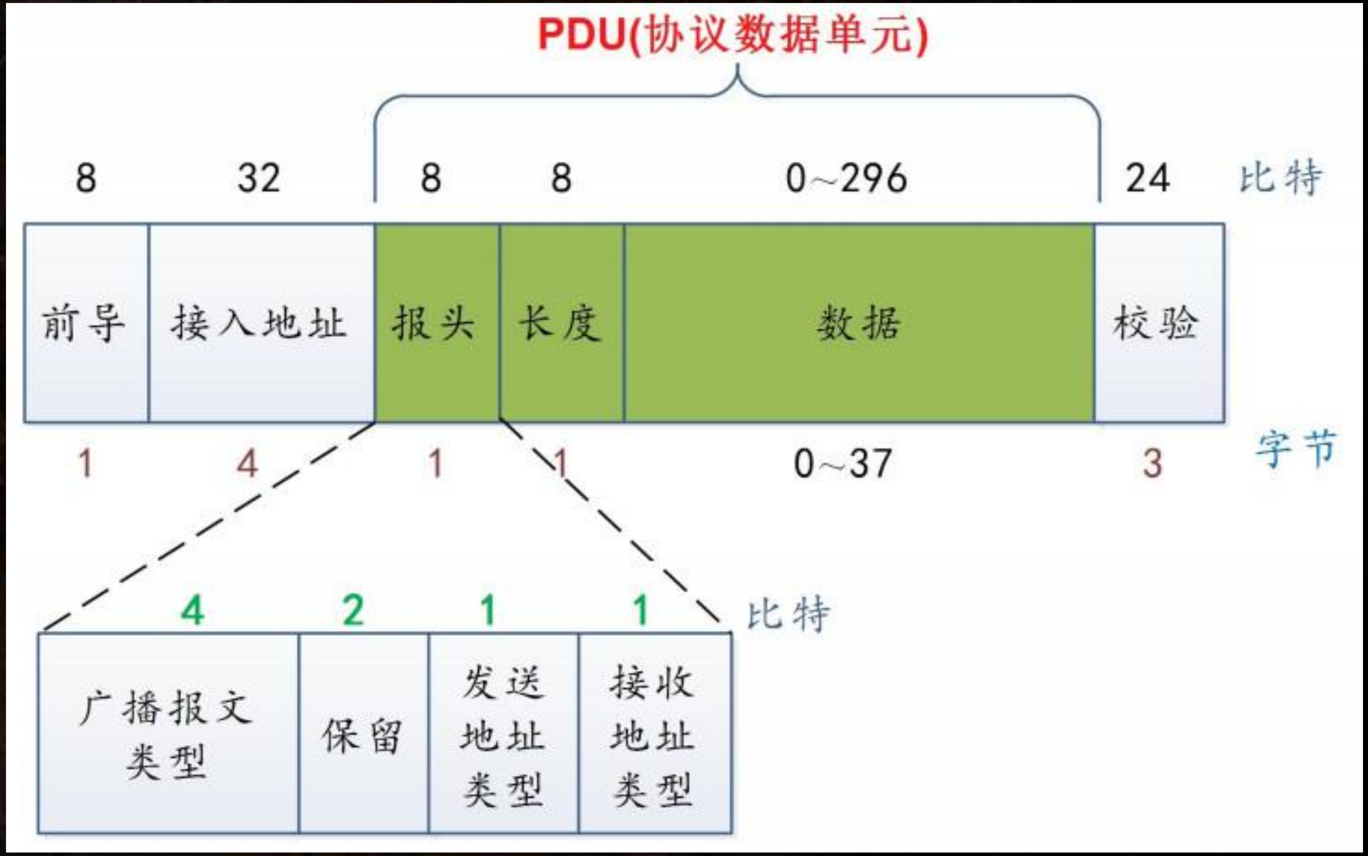
8	32	8	8	0~296	24	比特
前导	接入地址	报头	长度	数据	校验	
1	4	1	1	0~37	3	字节

PDU(协议数据单元)

- 字节序：大多数多字节域是从低字节开始传输的
- 比特序：各个字节传输时，每个字节都是从低位开始

BLE协议分析

- 报头包含4bit广播报文类型、2bit保留位、1bit发送地址类型和1bit接收地址类型



PDU(协议数据单元)

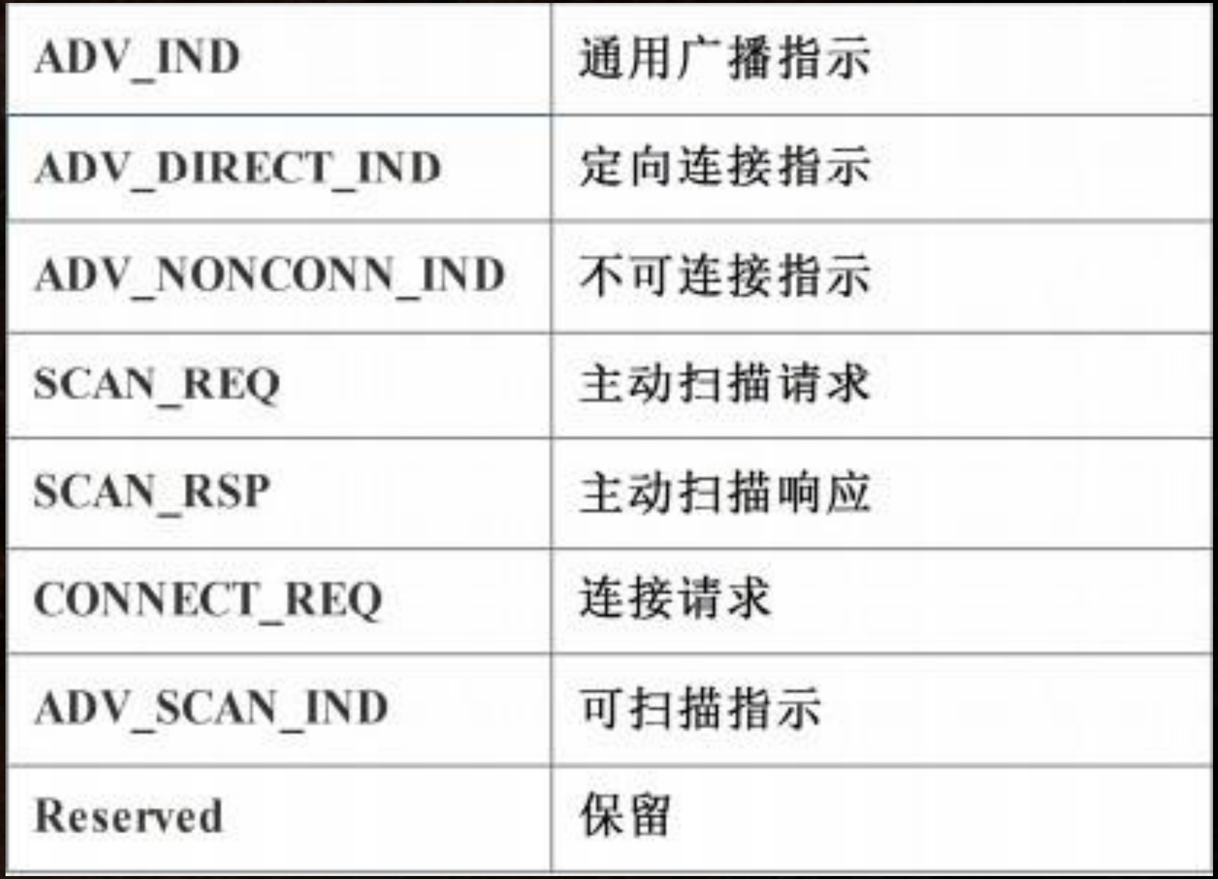
8	32	8	8	0~296	24	比特
前导	接入地址	报头	长度	数据	校验	
1	4	1	1	0~37	3	字节

4	2	1	1	比特
广播报文类型	保留	发送地址类型	接收地址类型	

BLE协议分析

- BLE广播报文7种类型

- ADV_IND
- SCAN_REQ
- SCAN_RSP
- CONNECT_REQ



ADV_IND	通用广播指示
ADV_DIRECT_IND	定向连接指示
ADV_NONCONN_IND	不可连接指示
SCAN_REQ	主动扫描请求
SCAN_RSP	主动扫描响应
CONNECT_REQ	连接请求
ADV_SCAN_IND	可扫描指示
Reserved	保留

BLE协议分析

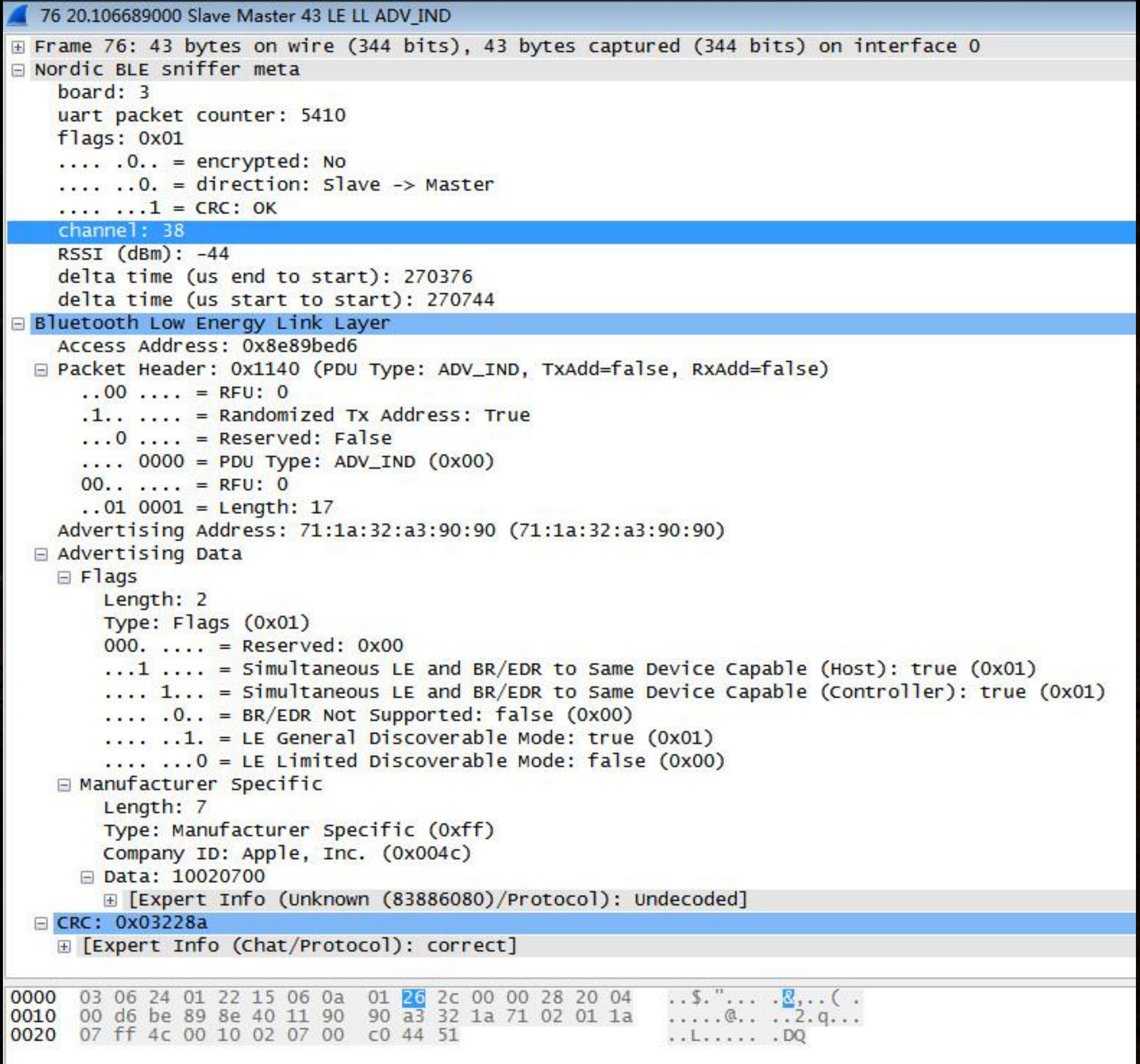
- BLE数据包的CRC验证公式

$$CRC = x^{24} + x^{10} + x^{9} + x^{6} + x^{4} + x^{3} + x^{1} + x^{0}$$

- 广播包最关键的：Access Address 0x8E89BED6

BLE协议连接/通信流程

- Slave 37>38>39> ADV_IND
- Master > SCAN_REQ
- Slave > SCAN_RSP
- Master > CONNECT_REQ
- Master >data> Slave (Hopping 0-36)
- Slave >data> Master (Hopping 0-36)
- Master >LL_Terminate_Ind or 异常断开



```
76 20.106689000 Slave Master 43 LE LL ADV_IND
⊞ Frame 76: 43 bytes on wire (344 bits), 43 bytes captured (344 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 5410
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 38
    RSSI (dBm): -44
    delta time (us end to start): 270376
    delta time (us start to start): 270744
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊟ Packet Header: 0x1140 (PDU Type: ADV_IND, TxAdd=false, RxAdd=false)
      ..00 .... = RFU: 0
      .1.. .... = Randomized Tx Address: True
      ...0 .... = Reserved: False
      .... 0000 = PDU Type: ADV_IND (0x00)
      00.. .... = RFU: 0
      ..01 0001 = Length: 17
    Advertising Address: 71:1a:32:a3:90:90 (71:1a:32:a3:90:90)
  ⊟ Advertising Data
    ⊟ Flags
        Length: 2
        Type: Flags (0x01)
        000. .... = Reserved: 0x00
        ...1 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): true (0x01)
        .... 1... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): true (0x01)
        .... .0.. = BR/EDR Not Supported: false (0x00)
        .... ..1. = LE General Discoverable Mode: true (0x01)
        .... ...0 = LE Limited Discoverable Mode: false (0x00)
    ⊟ Manufacturer Specific
        Length: 7
        Type: Manufacturer Specific (0xff)
        Company ID: Apple, Inc. (0x004c)
      ⊟ Data: 10020700
        ⊞ [Expert Info (Unknown (83886080)/Protocol): Undecoded]
  ⊟ CRC: 0x03228a
    ⊞ [Expert Info (Chat/Protocol): correct]

0000  03 06 24 01 22 15 06 0a  01 26 2c 00 00 28 20 04   ..$."... .&,..( .
0010  00 d6 be 89 8e 40 11 90  90 a3 32 1a 71 02 01 1a   .....@.. ..2.q...
0020  07 ff 4c 00 10 02 07 00  c0 44 51                  ..L..... .DQ
```

广播包

ADV_IND 38

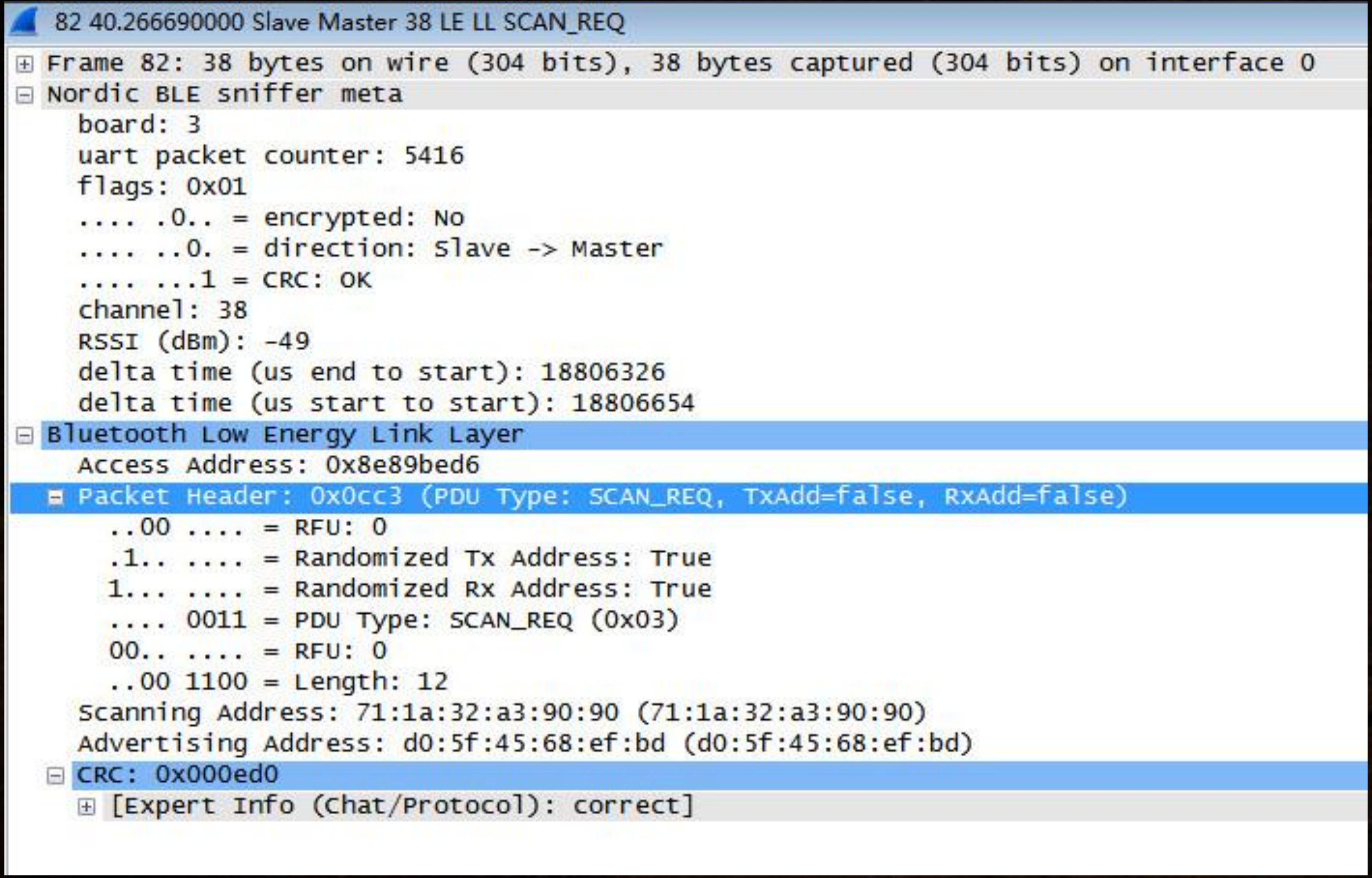
广播包固定的

Access Address

0x8e89bed6

广播设备地址

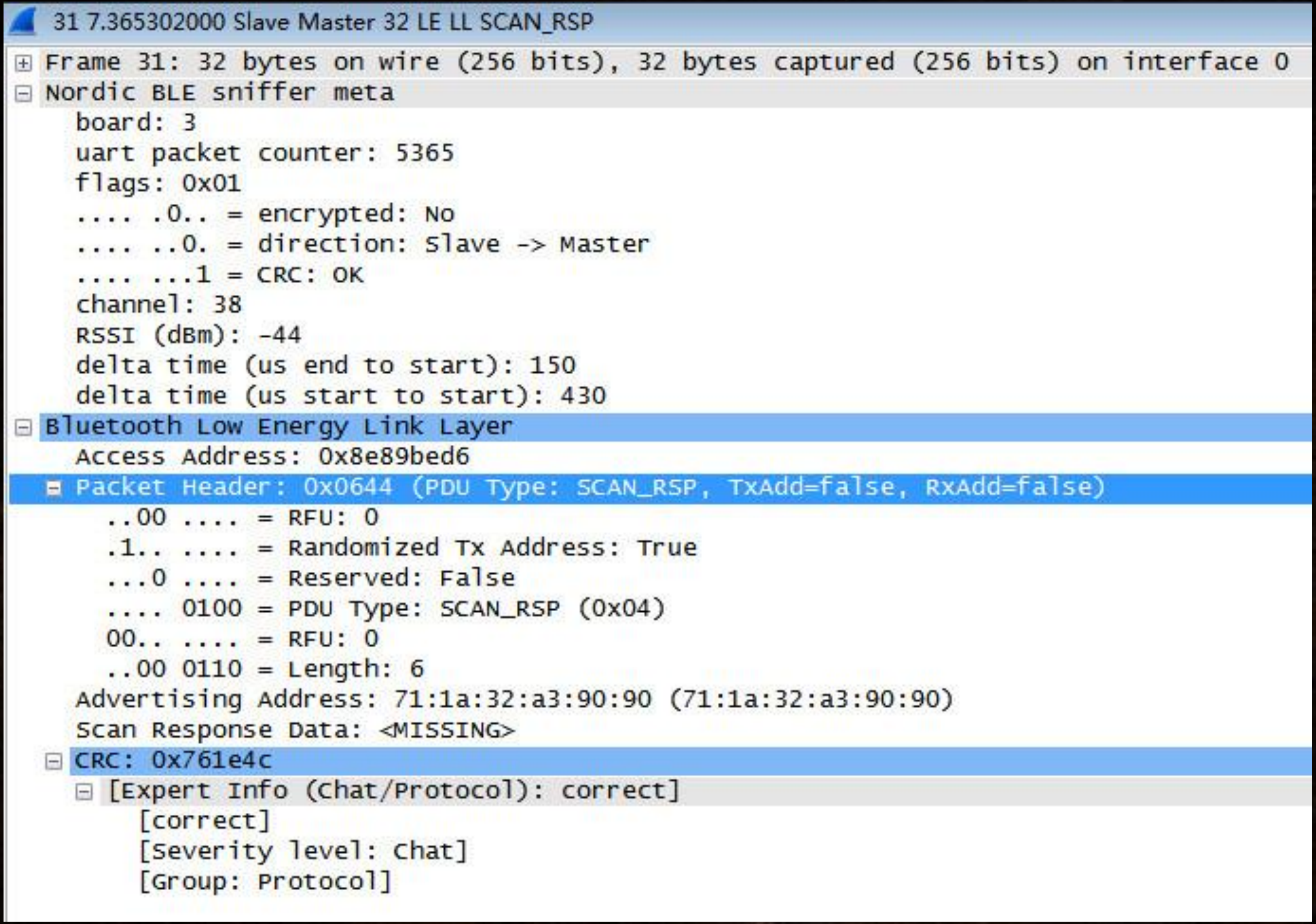
71:1a:32:a3:90:90



```
82 40.266690000 Slave Master 38 LE LL SCAN_REQ
⊞ Frame 82: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 5416
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 38
    RSSI (dBm): -49
    delta time (us end to start): 18806326
    delta time (us start to start): 18806654
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊟ Packet Header: 0x0cc3 (PDU Type: SCAN_REQ, TxAdd=false, RxAdd=false)
      ..00 .... = RFU: 0
      .1.. .... = Randomized Tx Address: True
      1... .... = Randomized Rx Address: True
      .... 0011 = PDU Type: SCAN_REQ (0x03)
      00.. .... = RFU: 0
      ..00 1100 = Length: 12
    Scanning Address: 71:1a:32:a3:90:90 (71:1a:32:a3:90:90)
    Advertising Address: d0:5f:45:68:ef:bd (d0:5f:45:68:ef:bd)
  ⊟ CRC: 0x000ed0
    ⊞ [Expert Info (Chat/Protocol): correct]
```

广播包含扫描请求
SCAN_REQ

扫描设备地址
71:1a:32:a3:90:90
广播设备地址
d0:5f:45:68:ef:bd
包长度 12



31 7.365302000 Slave Master 32 LE LL SCAN_RSP

```
⊞ Frame 31: 32 bytes on wire (256 bits), 32 bytes captured (256 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 5365
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 38
    RSSI (dBm): -44
    delta time (us end to start): 150
    delta time (us start to start): 430
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊟ Packet Header: 0x0644 (PDU Type: SCAN_RSP, TxAdd=false, RxAdd=false)
      ..00 .... = RFU: 0
      .1.. .... = Randomized Tx Address: True
      ...0 .... = Reserved: False
      .... 0100 = PDU Type: SCAN_RSP (0x04)
      00.. .... = RFU: 0
      ..00 0110 = Length: 6
    Advertising Address: 71:1a:32:a3:90:90 (71:1a:32:a3:90:90)
    Scan Response Data: <MISSING>
  ⊟ CRC: 0x761e4c
    ⊟ [Expert Info (Chat/Protocol): correct]
        [correct]
        [Severity level: Chat]
        [Group: Protocol]
```

扫描响应

SCAN_RSP

随机地址

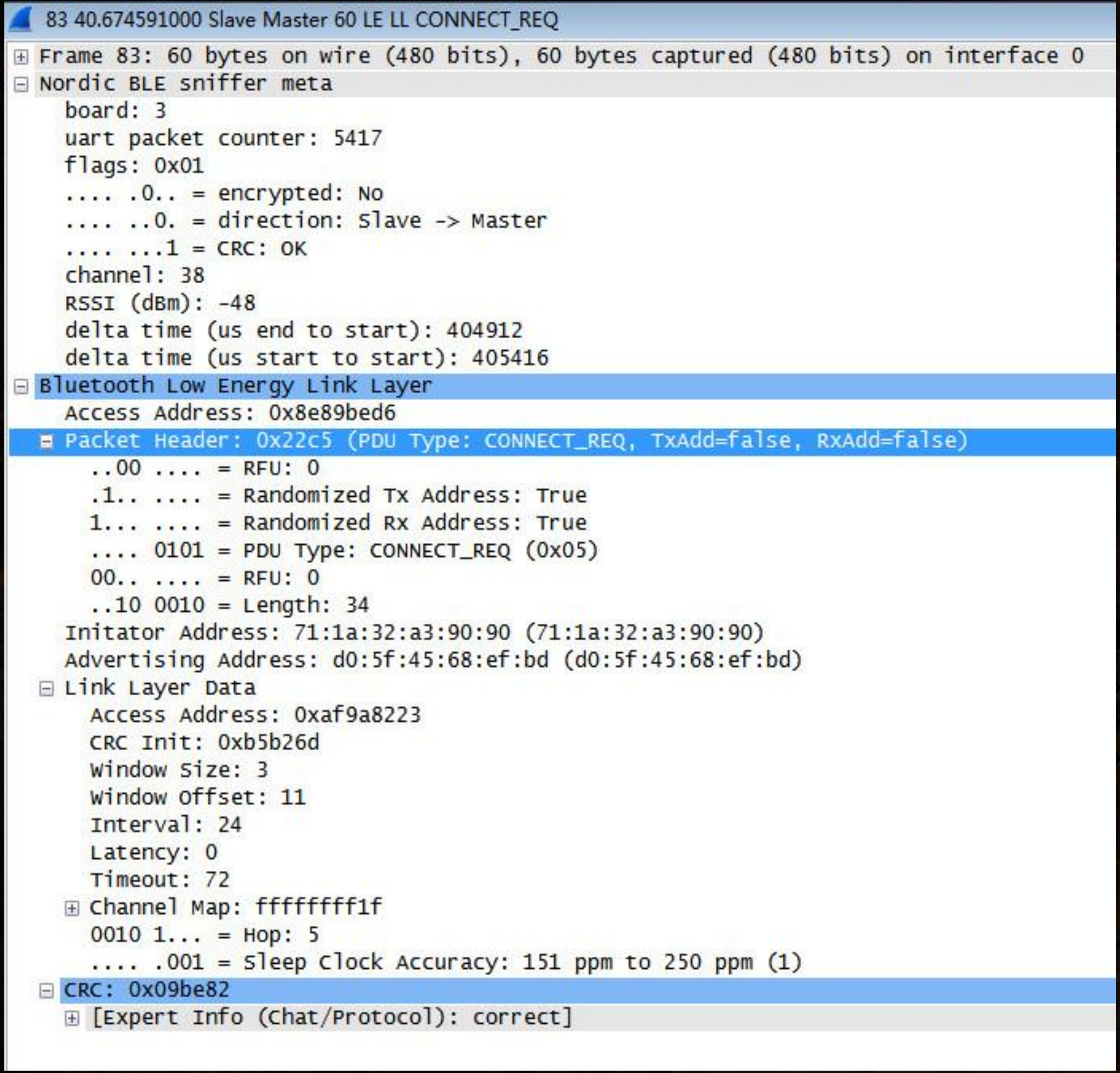
71:1a:32:a3:90:90

CONNECT_REQ

Hopping Interval

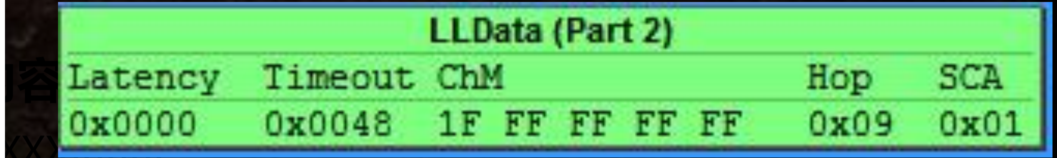
InitAddress

AdvAddress



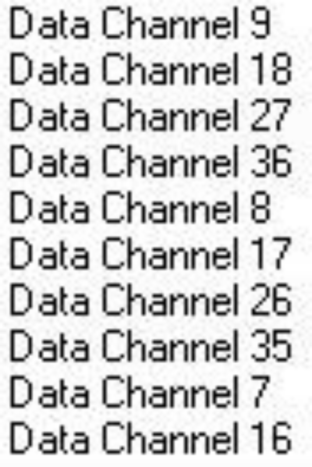
83 40.674591000 Slave Master 60 LE LL CONNECT_REQ

```
⊞ Frame 83: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 5417
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 38
    RSSI (dBm): -48
    delta time (us end to start): 404912
    delta time (us start to start): 405416
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊟ Packet Header: 0x22c5 (PDU Type: CONNECT_REQ, TxAdd=false, RxAdd=false)
      ..00 .... = RFU: 0
      .1.. .... = Randomized Tx Address: True
      1... .... = Randomized Rx Address: True
      .... 0101 = PDU Type: CONNECT_REQ (0x05)
      00.. .... = RFU: 0
      ..10 0010 = Length: 34
    Initator Address: 71:1a:32:a3:90:90 (71:1a:32:a3:90:90)
    Advertising Address: d0:5f:45:68:ef:bd (d0:5f:45:68:ef:bd)
  ⊟ Link Layer Data
      Access Address: 0xaf9a8223
      CRC Init: 0xb5b26d
      Window Size: 3
      Window Offset: 11
      Interval: 24
      Latency: 0
      Timeout: 72
    ⊞ Channel Map: ffffffff1f
      0010 1... = Hop: 5
      .... .001 = Sleep Clock Accuracy: 151 ppm to 250 ppm (1)
  ⊟ CRC: 0x09be82
    ⊞ [Expert Info (Chat/Protocol): correct]
```



LLData (Part 2)

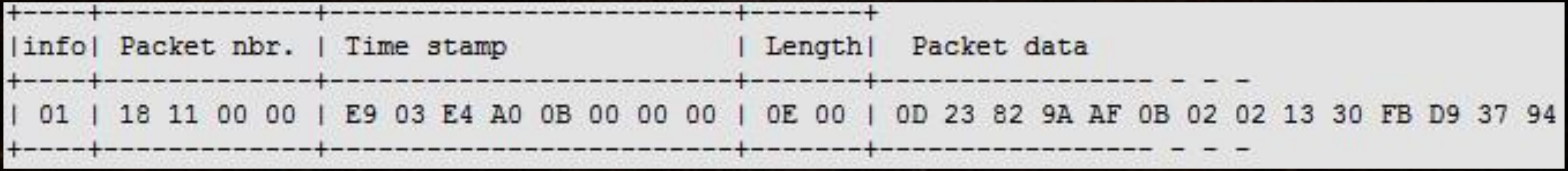
Latency	Timeout	ChM	Hop	SCA
0x0000	0x0048	1F FF FF FF FF	0x09	0x01



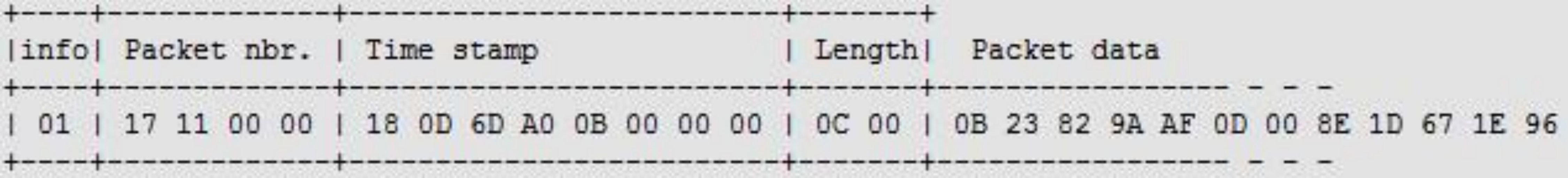
Data Channel 9
Data Channel 18
Data Channel 27
Data Channel 36
Data Channel 8
Data Channel 17
Data Channel 26
Data Channel 35
Data Channel 7
Data Channel 16

BLE协议分析

- 数据报文分析 Data Type: Empty PDU



```
+----+-------------+-------------------------+-------+
|info| Packet nbr. | Time stamp              | Length|  Packet data
+----+-------------+-------------------------+-------+----------------- - - -
| 01 | 18 11 00 00 | E9 03 E4 A0 0B 00 00 00 | 0E 00 | 0D 23 82 9A AF 0B 02 02 13 30 FB D9 37 94
+----+-------------+-------------------------+-------+----------------- - - -
```

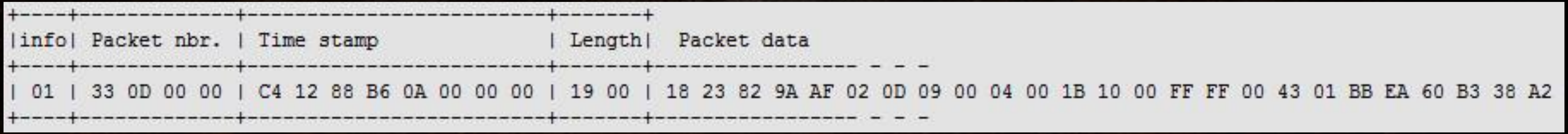


```
+----+-------------+-------------------------+-------+
|info| Packet nbr. | Time stamp              | Length|  Packet data
+----+-------------+-------------------------+-------+----------------- - - -
| 01 | 17 11 00 00 | 18 0D 6D A0 0B 00 00 00 | 0C 00 | 0B 23 82 9A AF 0D 00 8E 1D 67 1E 96
+----+-------------+-------------------------+-------+----------------- - - -
```

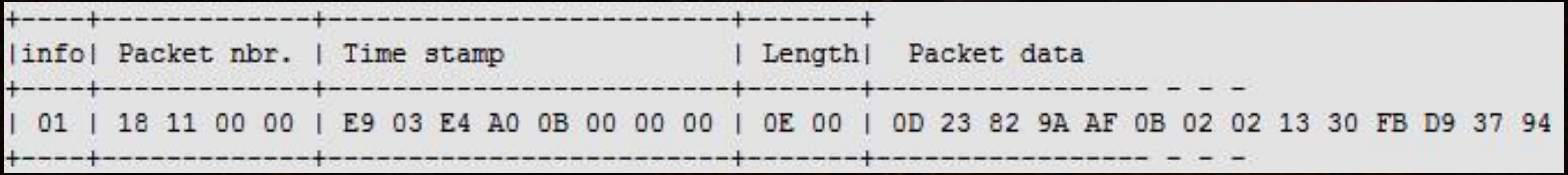
报文序号，长度，数据内容，CRC，信号增益

BLE协议分析

- 数据报文分析 Data Type: L2CAP



```
+----+-------------+-------------------------+-------+
|info| Packet nbr. | Time stamp              | Length|  Packet data
+----+-------------+-------------------------+-------+---------------- - - -
| 01 | 33 0D 00 00 | C4 12 88 B6 0A 00 00 00 | 19 00 | 18 23 82 9A AF 02 0D 09 00 04 00 1B 10 00 FF FF 00 43 01 BB EA 60 B3 38 A2
+----+-------------+-------------------------+-------+---------------- - - -
```



```
+----+-------------+-------------------------+-------+
|info| Packet nbr. | Time stamp              | Length|  Packet data
+----+-------------+-------------------------+-------+---------------- - - -
| 01 | 18 11 00 00 | E9 03 E4 A0 0B 00 00 00 | 0E 00 | 0D 23 82 9A AF 0B 02 02 13 30 FB D9 37 94
+----+-------------+-------------------------+-------+---------------- - - -
```

Logical Link Control and Adaptation Protocol
逻辑链路控制及自适应协议层协议

攻击方式

- 被动嗅探，窃取BLE协议内的数据

- 重放攻击，冒名顶替，未授权的访问

- 中间人攻击，跨越BLE的通信距离，篡改数据

中间人攻击

正常方式连接：Phone M<------>S BleCar

中间人攻击：Phone M<--->S1 代理 M1<--->S BleCar

代理端在中转数据的时候，可以修改其中的数据内容

演示 - 速度与激情8的僵尸车队

Thank you!

KCon洞见
2017未来