启明星辰

无线通讯协议安全分析

VFSec－宋希峰

Contents

Part
ONE
第一部分

无线安全概述

无线 ≠ 无线Wi-Fi

无线安全 ≠ 移动安全

无线安全攻击手段

报文监听

使用频率相同的监听设备对目标无线报文进行收集分析和解密。

重放攻击

对无时间戳或无随机性的无线信号进行重放操作

劫持攻击

一般通过拒绝服务或者其他干扰方式，将其劫持到一个虚假或者可控制的信号中。

欺骗攻击

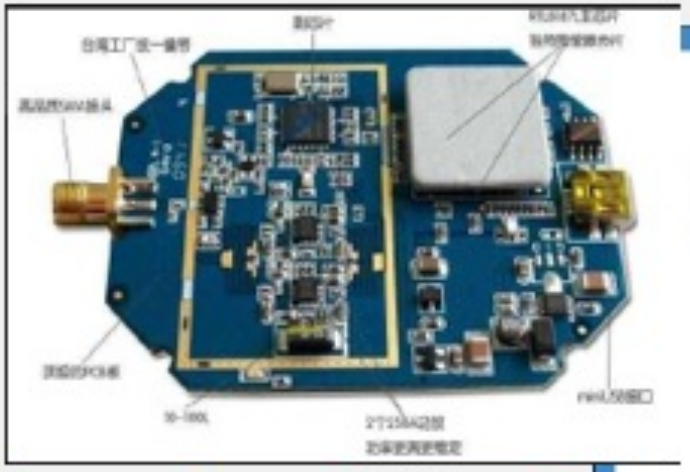
结合无线监听及解密，直接构造合法的可通过认证的报文进行欺骗攻击

Part
Two
第二部分

无线Wi-Fi安全

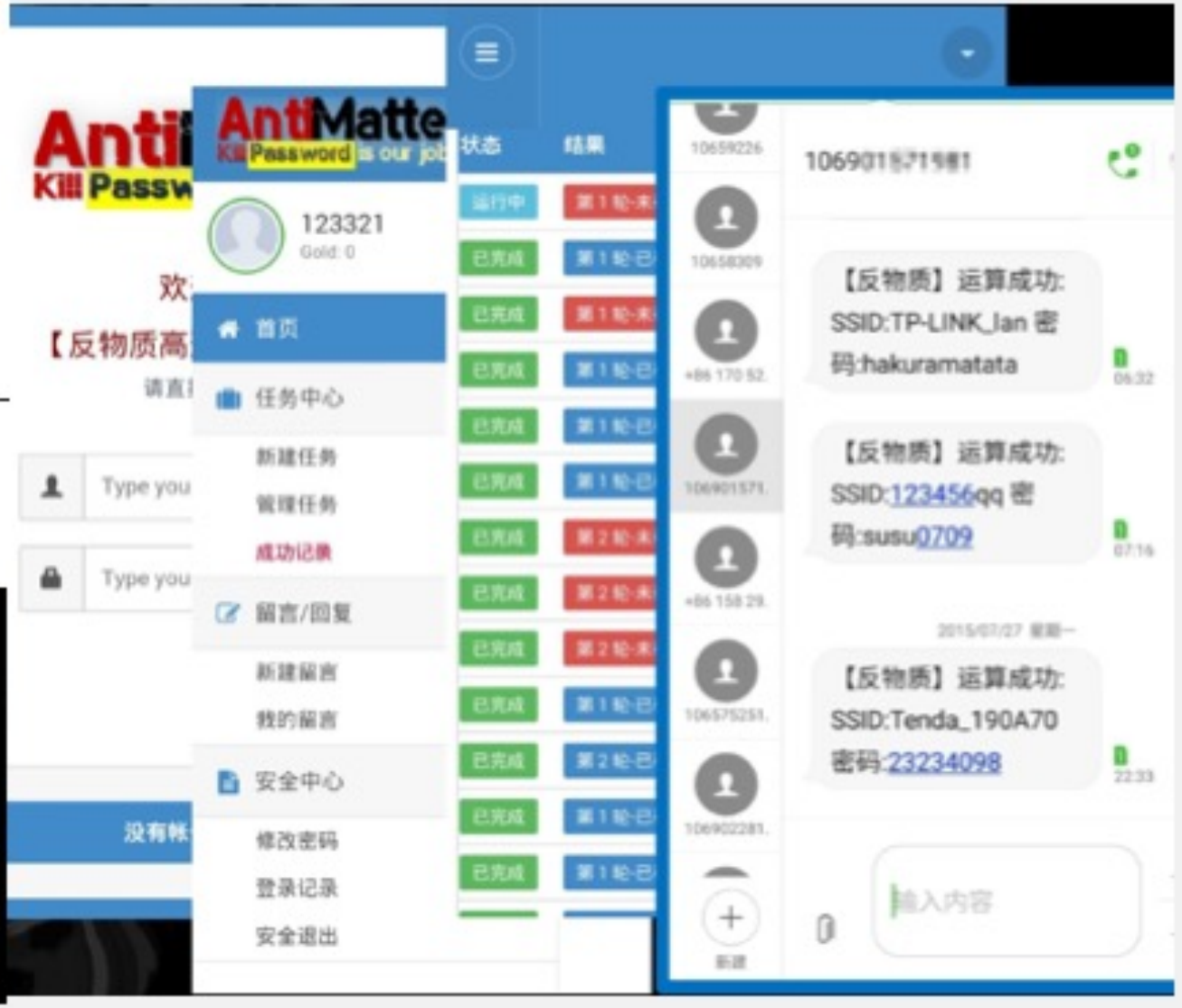
Part Two

无线Wi-Fi安全



06-07年

08-09年



Part Two
无线Wi-Fi安全

评估类	评估项	检测内容
密码安全	* 弱口令密码测试	检测wifi密码是否为弱密码可轻易猜解
	* 暴力破解	检测wifi密码是否可被暴力破解
	* 路由管理系统弱口令测试	检测路由管理系统是否存在默认账户
路由系统测试	* 欺骗性攻击测试	检测是否可搭建相同软AP欺骗用户访问链接
	* 路由安全漏洞测试	检测已有路由器存在的一些已知的安全风险
中间人攻击	* 信息篡改测试	篡改通讯数据并重新发送
	* 信息窃取测试	截取通讯数据获取账户、密码等敏感数据
	* DNS欺骗测试	冒充DNS服务器，实现控制用户访问
	* 会话劫持	介于两台机器中间实现通讯数据控制
	* ARP欺骗测试	对局域网内交互数据进行嗅探
WEB端管理测试	* sql注入测试	检测参数是否可以进行sql注入攻击
	* 信息泄漏测试	检测是否含有敏感信息的url
	* 跨站脚本攻击	检测是否可以进行xss攻击
	* 用户越权操作	检测是否可以非法越权操作
	* 登录接口绕过	检测是否可以绕过登录接口
	* 端口开放情况	检测服务端各设备、服务器端口开放情况。
无线网络	* 接入点端口开放情况	检测是否有任何不必要的端口打开
	* DDOS攻击测试	检测AP能否承受模拟的802.11 DoS攻击
	* AP默认账号密码测试	检测AP是否更改默认管理账号密码
	* 身份验证测试	检测是否开启更强身份验证措施如：私钥
	* AP加密测试	检测AP采用加密方式，如果为WEP测试破解时长等
	* AP信道测试	检测AP是否使用正确的ESSID和信道

Demonstration based on the paper

K s:

Forc PA2

ww m

扫一扫，直接在手机上打开

Part
Three

第三部分

RFID安全

Part Three
RFID安全

启明星辰

RFID与NFC的关系

频段

频段差异：
NFC仅限于13.56MHz高频段，不像RFID有较多频段可选

距离

通讯距离差异：
NFC大多在10厘米以内，而RFID可能扩展到几十米；

模式

工作模式差异：
NFC可被当作射频卡、阅读器或者点对点模式来使用，RFID需要阅读器和标签组成

场景

应用场景差异：
RFID往往运用于生产、物流、资产管理等企业场景，而NFC则更多运用在公交、门禁、手机支付上，更适合普通用户

	低频(LF)	高频(HF)	超高频(UHF)	微波(Microwave)
頻率	100~500KHz	10~15MHz	433~950MHz	1GHz以上
常見頻段	125KHz 135KHz			
系統型態	被動式			
全球接受頻率	是			
通訊距離	50cm以內			
傳輸功率	72dBμA/m			
成熟度	成熟			
讀取方式	電磁感應			

	低频(LF)	高频(HF)	超高频(UHF)	微波(Microwave)
價格	低	中	高	高
環境影響	X	金屬	潮濕	潮濕
資料傳輸率	低	高	較高	最高
記憶體(Bytes)	64~1K	256~512K	64~512	16~64
ISO對應標準	ISO18000-2 Two Type 被動式	ISO18000-3 Two Mode 被動式	ISO18000-6 Two Type 被動/半主動式	ISO18000-4 Two Mode 被動式/半主動式
應用	門禁系統 動物識別 存貨控制 晶片防盜鎖	智慧卡 圖書館管理 商品管理	鐵路車廂監控 倉存管理	道路收費系統

Part Three
RFID安全

目前RFID攻击方法主要表现在对ID、IC卡本身的攻击。

测试工具：ACR122U、Proxmark3等

对RFID攻击方法总结分为以下5种：

1、卡数据窃取

2、卡校验绕过(模拟卡)

3、卡复制

4、卡数据破解与篡改

5、终端攻击

IC卡

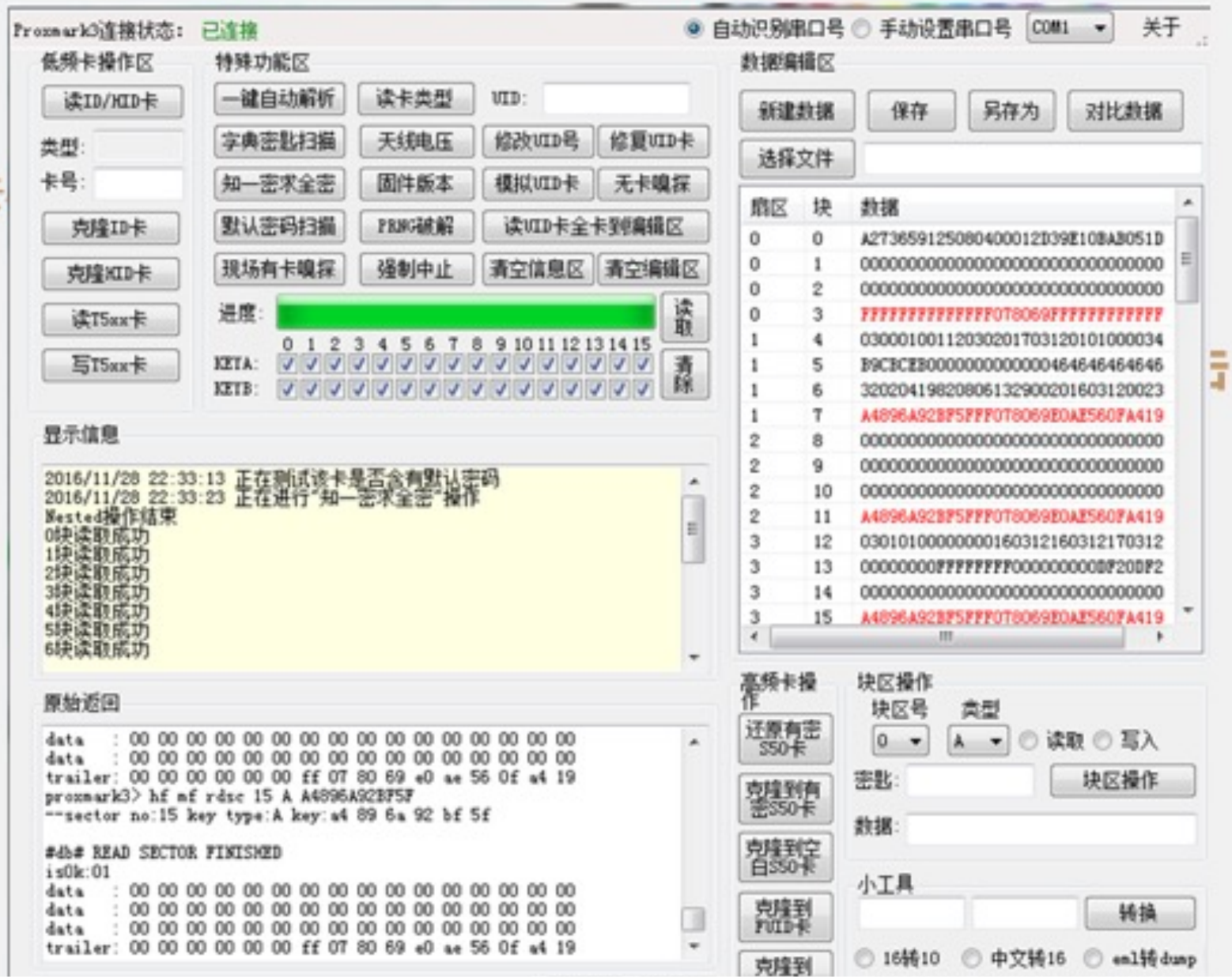
1）

2）

3）

4）

5）


Proxmark3连接状态: 已连接
自动识别串口号
手动设置串口号
COM1
关于
低频卡操作区
读ID/HID卡
类型:
卡号:
克隆ID卡
克隆HID卡
读T5xx卡
写T5xx卡
特殊功能区
一键自动解析
读卡类型
UID:
字典密匙扫描
天线电压
修改UID号
修复UID卡
知一密求全密
固件版本
模拟UID卡
无卡嗅探
默认密码扫描
PRNG破解
读UID卡全卡到编辑区
现场有卡嗅探
强制中止
清空信息区
清空编辑区
进度:
读取
清除
KEYA:
KEYB:
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
显示信息
2016/11/28 22:33:13 正在测试该卡是否含有默认密码
2016/11/28 22:33:23 正在进行"知一密求全密"操作
Nested操作结束
0块读取成功
1块读取成功
2块读取成功
3块读取成功
4块读取成功
5块读取成功
6块读取成功
原始返回
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
trailer: 00 00 00 00 00 00 ff 07 80 69 e0 ae 56 0f a4 19
proxmark3> hf mf rdsc 15 A A4896A92BF5F
--sector no:15 key type:A key:a4 89 6a 92 bf 5f
#db# READ SECTOR FINISHED
isOk:01
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
trailer: 00 00 00 00 00 00 ff 07 80 69 e0 ae 56 0f a4 19
数据编辑区
新建数据
保存
另存为
对比数据
选择文件
扇区 块 数据
0 0 A27365912508040001 2D39E108AB051D
0 1 00000000000000000000000000000000
0 2 00000000000000000000000000000000
0 3 FFFFFFFFFFFF0780690FFFFFFFFFFF
1 4 03000100112030201703120101000034
1 5 B9CBCEB000000000000046464646464 6
1 6 32020419820806132900201603120023
1 7 A4896A92BF5FFF0780690EDAE560FA419
2 8 00000000000000000000000000000000
2 9 00000000000000000000000000000000
2 10 00000000000000000000000000000000
2 11 A4896A92BF5FFF0780690EDAE560FA419
3 12 03010100000000160312160312170312
3 13 00000000FFFFFFFF000000000F20DF2
3 14 00000000000000000000000000000000
3 15 A4896A92BF5FFF0780690EDAE560FA419
高频卡操作
还原有密S50卡
克隆到有密S50卡
克隆到空白S50卡
克隆到FUID卡
克隆到
块区操作
块区号
类型
0
A
读取
写入
密匙:
块区操作
数据:
小工具
转换
16转10
中文转16
eml转dump

卡数据破解与篡改

一些M1卡很早之就已经被破解出来，但目前使用仍是很广泛，很多公司、学校的门禁、餐卡、一卡通都仍在使用这类芯片卡。

下面是某食堂餐卡被破解后获取到的数据，只有第1扇区存在数据。通过多次充值、消费等数据的对比，得到以下结果：

Part Three
RFID安全

启明星辰

1、余[redacted]其计
算单位[redacted]0元；
充值后[redacted]

2、检[redacted]发现在
充值后[redacted]修改
下方余[redacted]日期，
省去分[redacted]

比如我[redacted]以直接
将上面[redacted]


```
0040h: 1A 5A 80 99 01 64 00 03 23 AE 01 FF
0050h: 1A 5A 80 99 01 00 0A 03 23 AE 01 FF
```

Part Four

第四部分

蓝牙安全

BLE(Bluetooh Low Energy)协议栈

Part Four
蓝牙安全

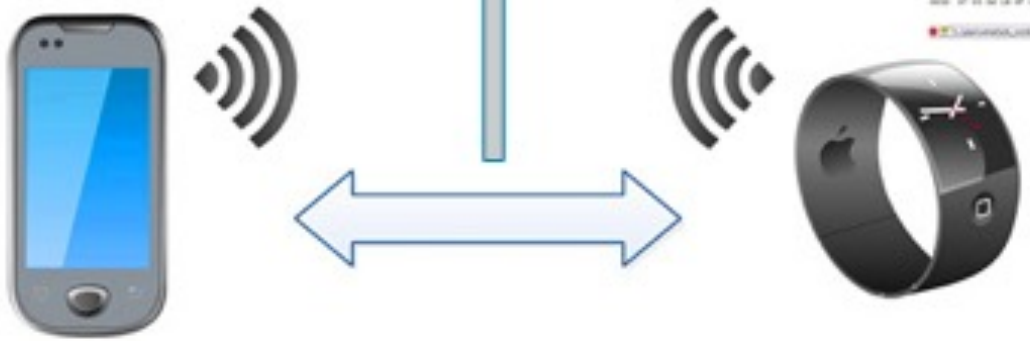
硬件

CSR4.0蓝牙适配器(接收器)
NRF51822开发板（适合开发 价格适中）
CC2540 USB Dongle （仅支持BLE 价格便宜)
Ubertooth（价格贵）

工具

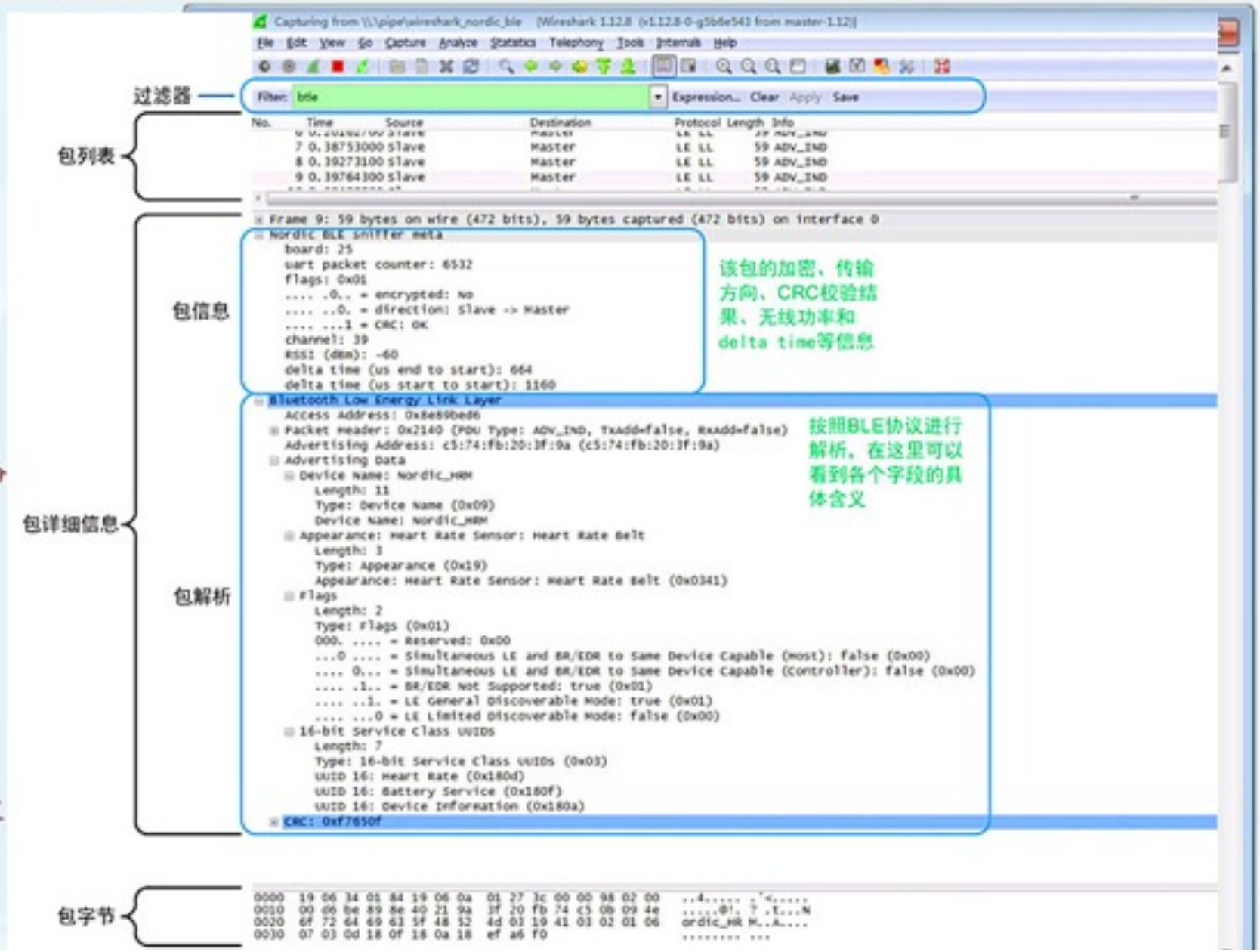
bluez bluez-utils
lightblue、ble scanner
pygatt

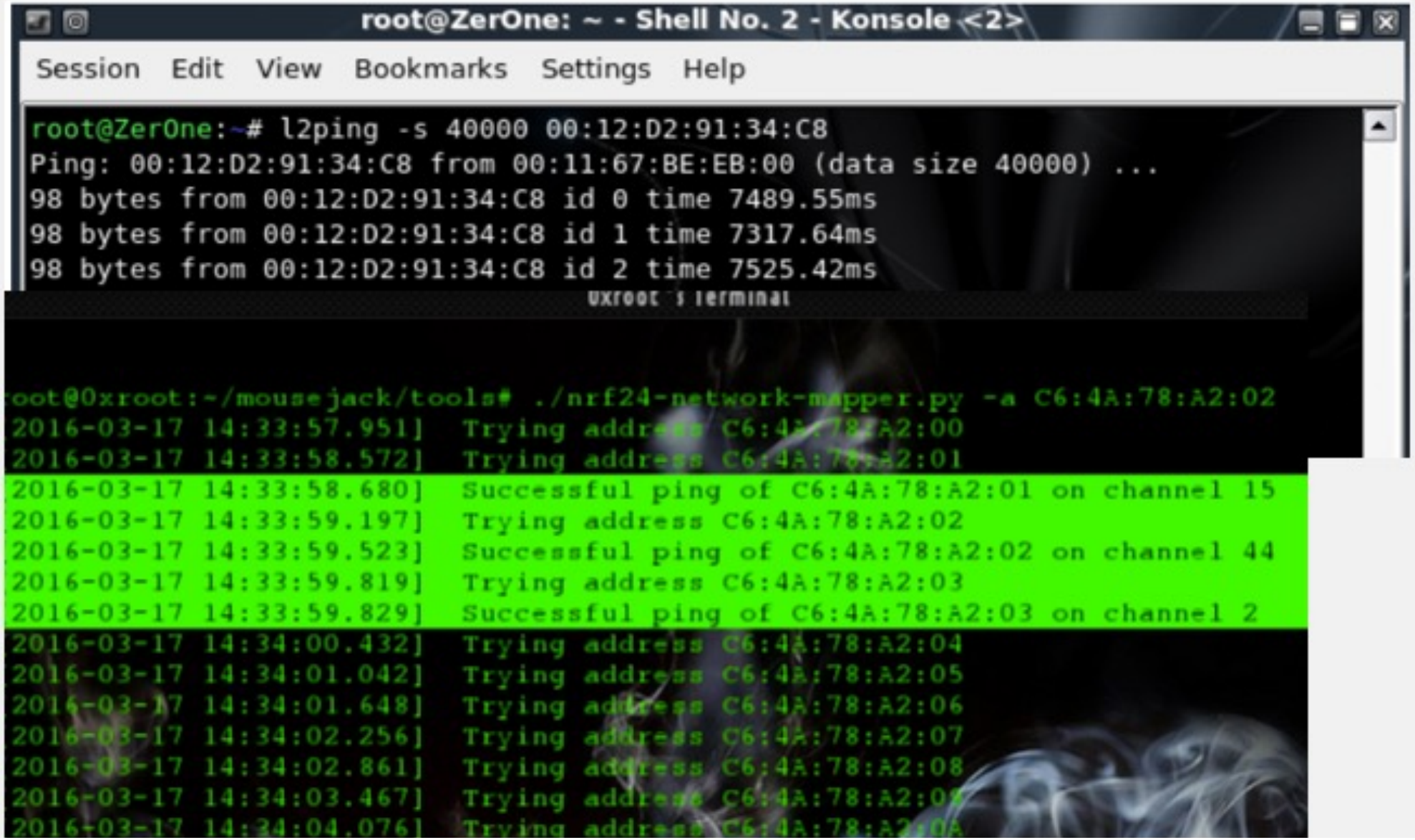
将Dongle连接到计算机的USB接口上
打开Sniffer软件进行抓包和协议分析



Central

Peripherel


过滤器
包列表
包信息
包详细信息
包解析
包字节
该包的加密、传输方向、CRC校验结果、无线功率和delta time等信息
按照BLE协议进行解析，在这里可以看到各个字段的具体含义
Capturing from \\.\pipe\wireshark_nordic_ble (Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12))
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: btle
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
7 0.38753000 Slave Master LE LL 59 ADV_IND
8 0.39273100 Slave Master LE LL 59 ADV_IND
9 0.39764300 Slave Master LE LL 59 ADV_IND
Frame 9: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
Nordic BLE sniffer meta
board: 25
uart packet counter: 6532
flags: 0x01
.... .0.. = encrypted: No
.... ..0. = direction: Slave -> Master
....1 = CRC: OK
channel: 39
RSSI (dBm): -60
delta time (us end to start): 664
delta time (us start to start): 1160
Bluetooth Low Energy Link Layer
Access Address: 0x8e89bed6
Packet Header: 0x2140 (PDU Type: ADV_IND, TxAdd=false, RxAdd=false)
Advertising Address: c5:74:fb:20:3f:9a (c5:74:fb:20:3f:9a)
Advertising Data
Device Name: Nordic_HRM
Length: 11
Type: Device Name (0x09)
Device Name: Nordic_HRM
Appearance: Heart Rate Sensor: Heart Rate Belt
Length: 3
Type: Appearance (0x19)
Appearance: Heart Rate Sensor: Heart Rate Belt (0x0341)
Flags
Length: 2
Type: Flags (0x01)
000. .... = Reserved: 0x00
...0 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x00)
.... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x00)
.... .1.. = BR/EDR Not Supported: true (0x01)
.... ..1. = LE General Discoverable Mode: true (0x01)
....0 = LE Limited Discoverable Mode: false (0x00)
16-bit Service Class UUIDs
Length: 7
Type: 16-bit Service Class UUIDs (0x03)
UUID 16: Heart Rate (0x180d)
UUID 16: Battery Service (0x180f)
UUID 16: Device Information (0x180a)
CRC: 0xf7650f
0000 19 06 34 01 84 19 06 0a 01 27 3c 00 00 98 02 00 ..4..... .'<.....
0010 00 d6 be 89 8e 40 21 9a 3f 20 fb 74 c5 0b 09 4e .....@!. ? .t...N
0020 6f 72 64 69 63 5f 48 52 4d 03 19 41 03 02 01 06 ordic_HR M..A....
0030 07 03 0d 18 0f 18 0a 18 ef a6 f0 ....


root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne:~# l2ping -s 40000 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:11:67:BE:EB:00 (data size 40000) ...
98 bytes from 00:12:D2:91:34:C8 id 0 time 7489.55ms
98 bytes from 00:12:D2:91:34:C8 id 1 time 7317.64ms
98 bytes from 00:12:D2:91:34:C8 id 2 time 7525.42ms
0xroot's Terminal
oot@0xroot:~/mousejack/tools# ./nrf24-network-mapper.py -a C6:4A:78:A2:02
2016-03-17 14:33:57.951] Trying address C6:4A:78:A2:00
2016-03-17 14:33:58.572] Trying address C6:4A:78:A2:01
2016-03-17 14:33:58.680] Successful ping of C6:4A:78:A2:01 on channel 15
2016-03-17 14:33:59.197] Trying address C6:4A:78:A2:02
2016-03-17 14:33:59.523] Successful ping of C6:4A:78:A2:02 on channel 44
2016-03-17 14:33:59.819] Trying address C6:4A:78:A2:03
2016-03-17 14:33:59.829] Successful ping of C6:4A:78:A2:03 on channel 2
2016-03-17 14:34:00.432] Trying address C6:4A:78:A2:04
2016-03-17 14:34:01.042] Trying address C6:4A:78:A2:05
2016-03-17 14:34:01.648] Trying address C6:4A:78:A2:06
2016-03-17 14:34:02.256] Trying address C6:4A:78:A2:07
2016-03-17 14:34:02.861] Trying address C6:4A:78:A2:08
2016-03-17 14:34:03.467] Trying address C6:4A:78:A2:09
2016-03-17 14:34:04.076] Trying address C6:4A:78:A2:0A

Part
Five

第五部分

其他无线协议

	频段	制式
调频广播	87MHz－108MHz	WFM
中波广播	526.5kHz－1606.5kHz	AM
短波广播	3MHz－30MHz	AM
机场塔台	118MHz－135.975MHz	AM
民用对讲机	VHF：136MHz－174MHz UHF：400MHz－470MHz	NFM
超短波电台	50－54MHz，144－148MHz， 430-440MHz	NFM

搭建ADS-B

硬件

RTL2832U R820T (电视棒)

RTL.SDR全波段接收器(100KHz-1766MHz)

工具

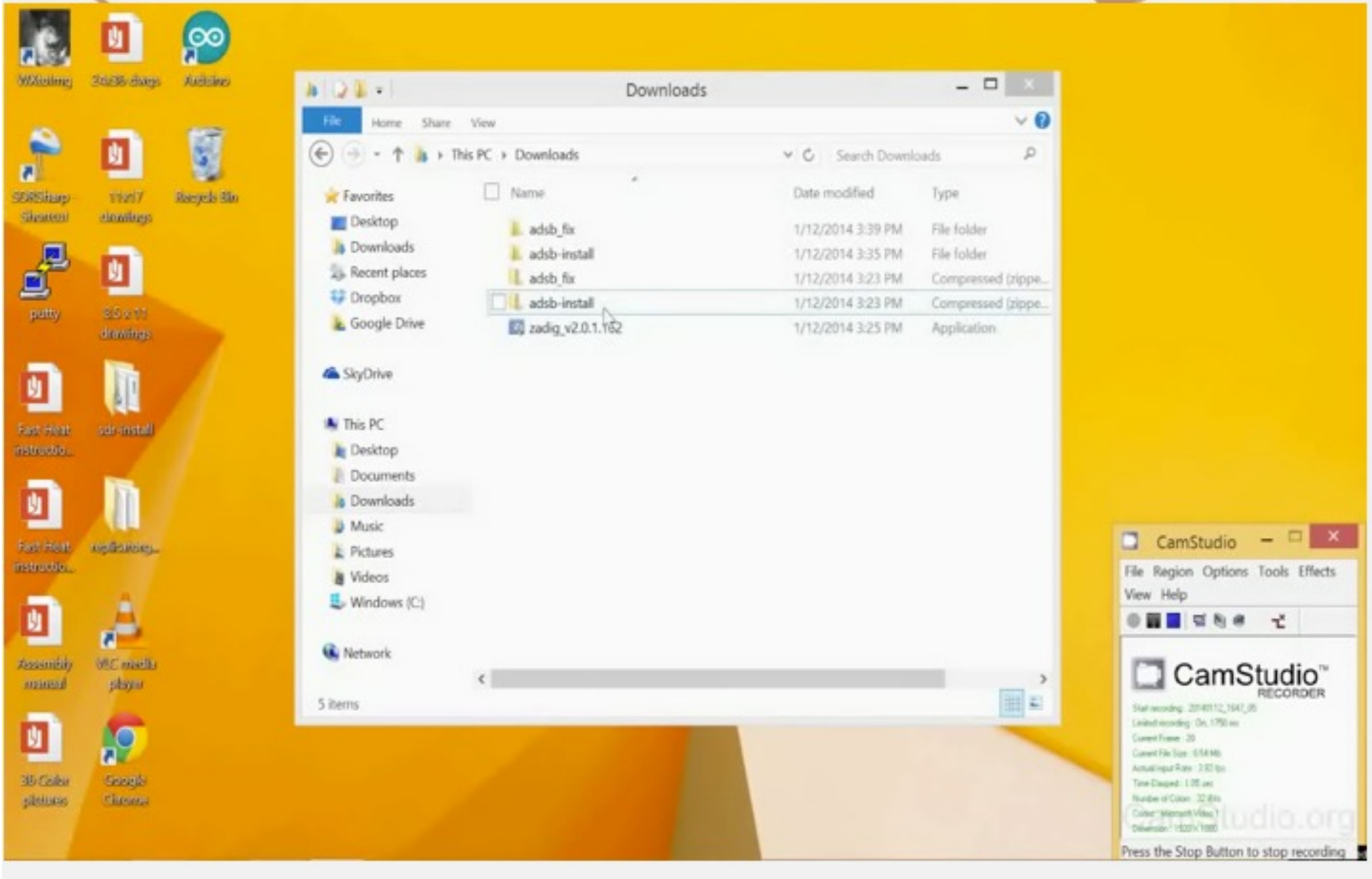
Dump1090 (Linux)

Zadig 驱动

SDRSharp

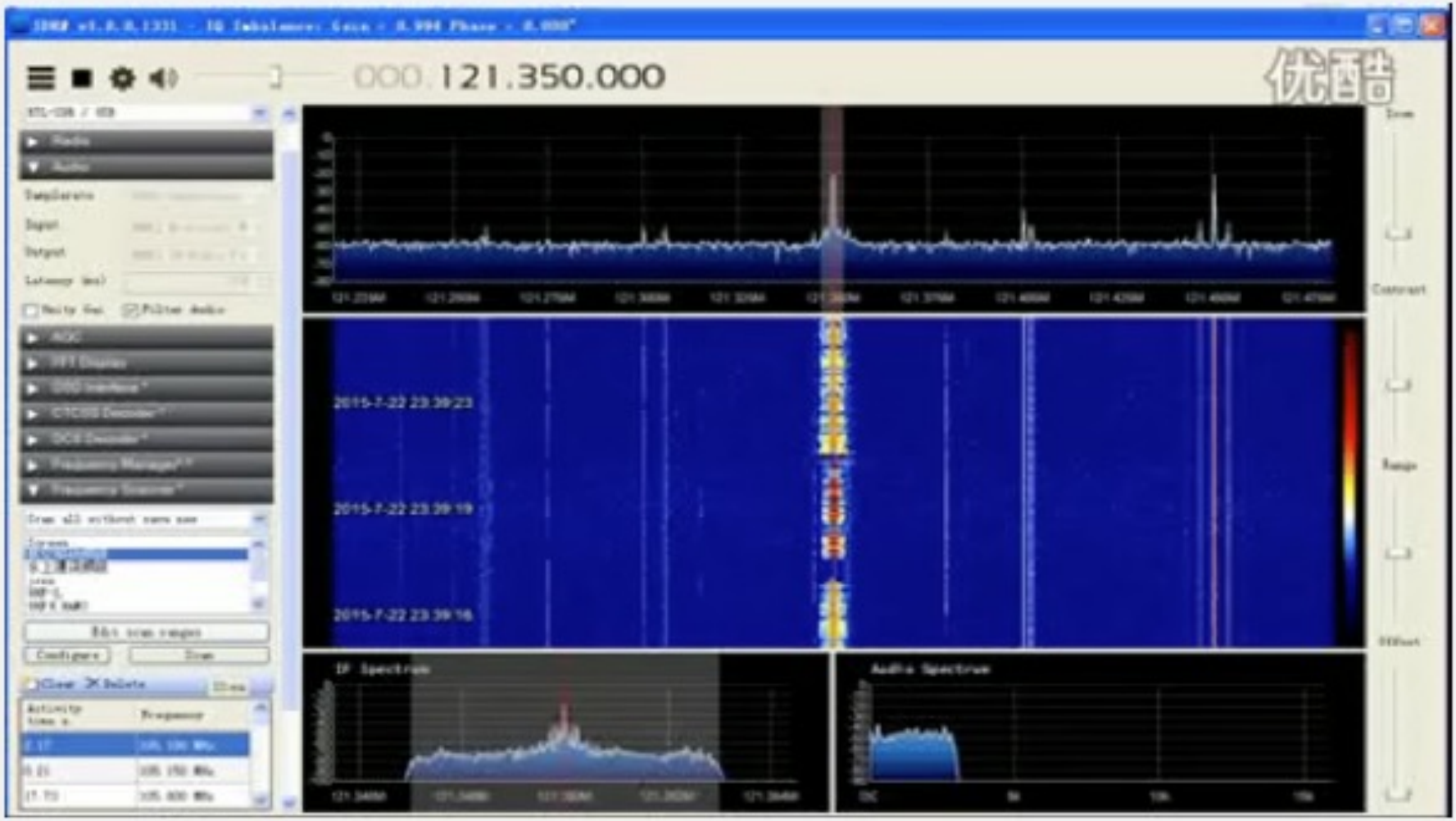
RTL1090

VirtualRadar


Downloads
File
Home
Share
View
This PC
Downloads
Search Downloads
Favorites
Desktop
Downloads
Recent places
Dropbox
Google Drive
SkyDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Network
Name
Date modified
Type
adsb_fix
1/12/2014 3:39 PM
File folder
adsb-install
1/12/2014 3:35 PM
File folder
adsb_fix
1/12/2014 3:23 PM
Compressed (zippe...
adsb-install
1/12/2014 3:23 PM
Compressed (zippe...
zadig_v2.0.1.162
1/12/2014 3:25 PM
Application
5 items
CamStudio
File Region Options Tools Effects
View Help
CamStudio™
RECORDER
Press the Stop Button to stop recording

Part Five

其他无线协议



ZigBee安全

ZigBee(紫蜂协议)基于IEEE802.15.4标准，作为一种低成本、低功耗、近距离的无线组网通讯技术。

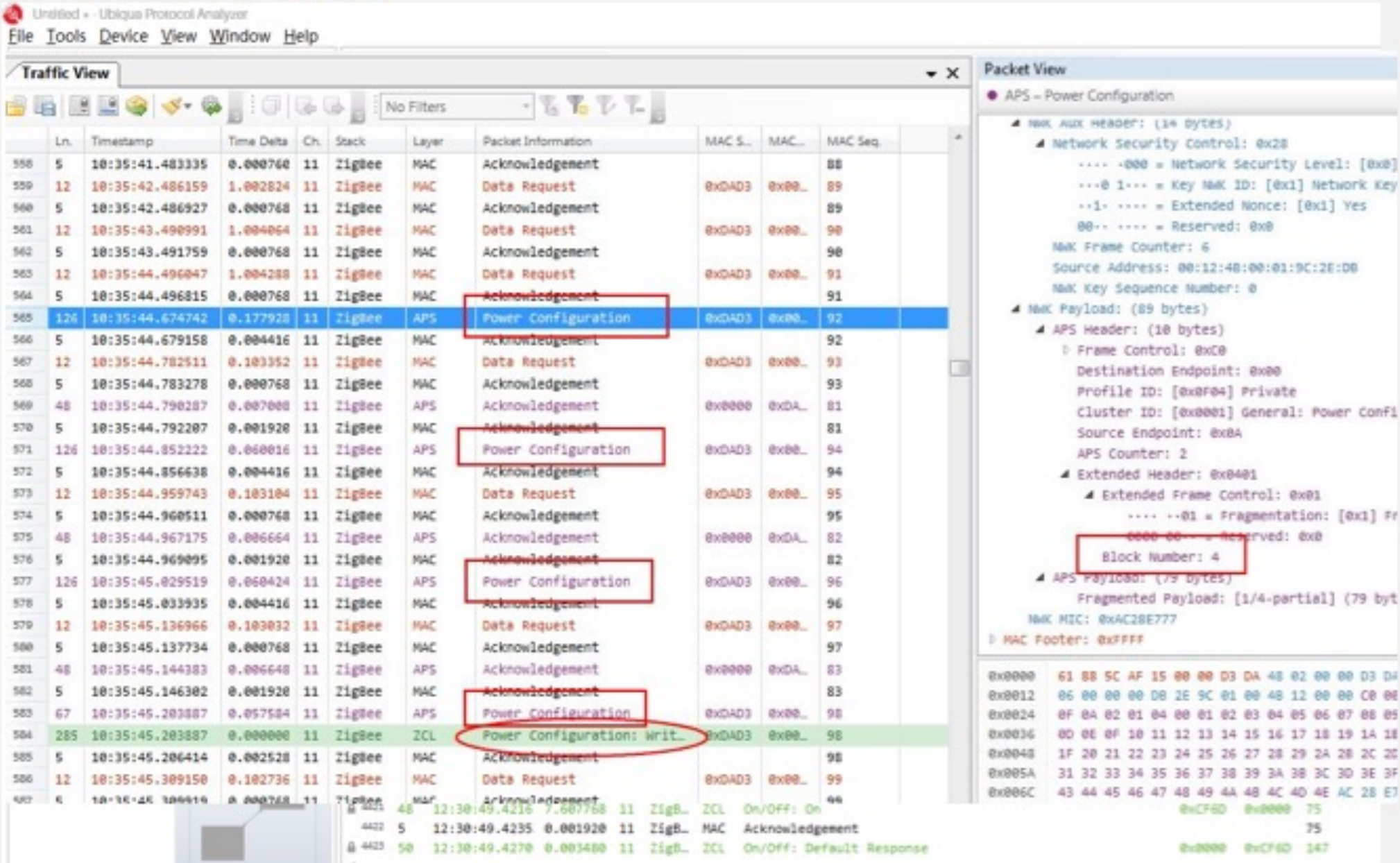
Zigbee是一个比较安全无线协议，它采用AES加密

抓包硬件设备：CC2530或CC2531 USB Dongle

协议分析软件：
Ubiqua Protocol Analyzer、Perytons Protocol Analyzer
TI Packet Sinffer等

Part Five

其他无线协议



SDR
WiFi
RFID
GSM
BLUETOOTH
ZigBee
Vo-LTE
HackRF
OpenBTS
SECRET
AGPS
移动互联网
LTE-FDD
LTE-HDD
Wireless
运营商
无线电
轨道交通
物联网
车联网
教育行业
电力行业
有源RFID
卫星通信
医疗
能源
交通
铁路
干扰
民航
GPS
GSM-R
NFC
Infrared
INTERNET
SPEED
TALENT
NEWS
EDUCATION
TELEVISION
APPLICATION
DEVELOPMENT
RESOURCE
SOCIAL
PHONE
KNOWLEDGE
INFORMATION
ADVERT
CLOCK
BLOG
DIGITAL
IOT
NO
YES

Venustech

THANKS!

谢 谢 观 看

金融 - VFSEC - 阿峰