

Unisoc Confidential

WIFI空口包抓包方法

Wifi空口包抓包方法

一、准备条件：

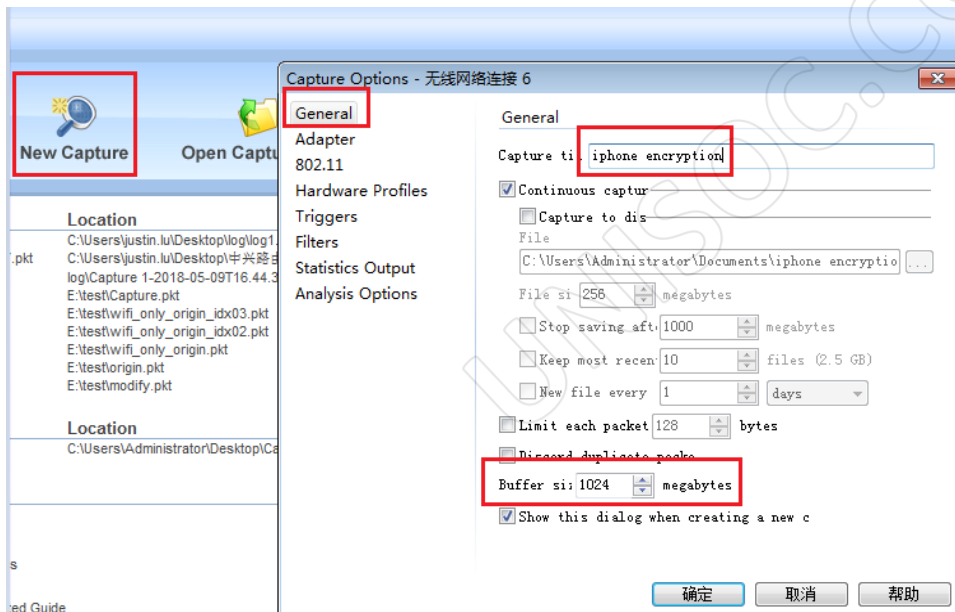
1. 笔记本
2. 抓包软件（安装在笔记本上），如：omnipeek
3. 无线网卡（如D-link DWA-125、ASUS USB-AC55 1300M 等，如右图
<https://item.jd.com/2175267.html>）
4. 另外一个android手机上安装一个wifi分析仪



Wifi空口包抓包方法

二、操作步骤：

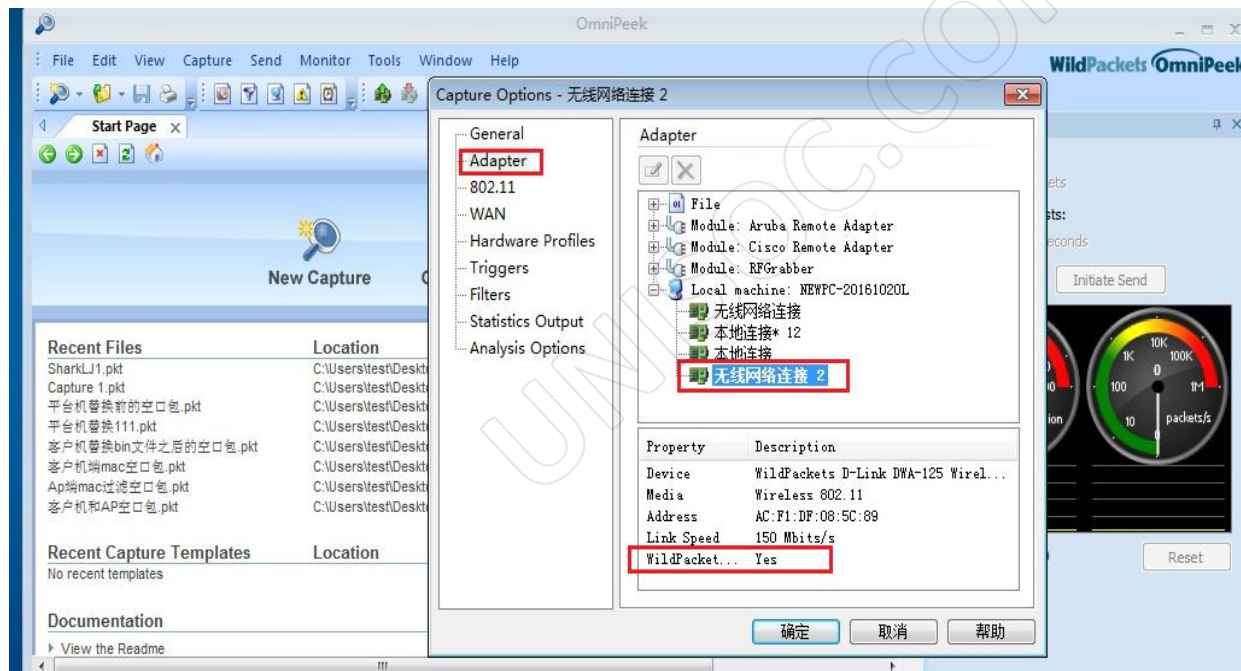
1. 打开omnipeek软件→new capture→取个名字；（建议将buffersize设置大一些，否则抓满了则后续log无法抓取到，如设置成1024）



Wifi空口包抓包方法

二、操作步骤：

2. 查看无线网卡是否连接成功，注意如下图3个地方(显示Yes才可以正常抓包)



Wifi空口包抓包方法

二、操作步骤：

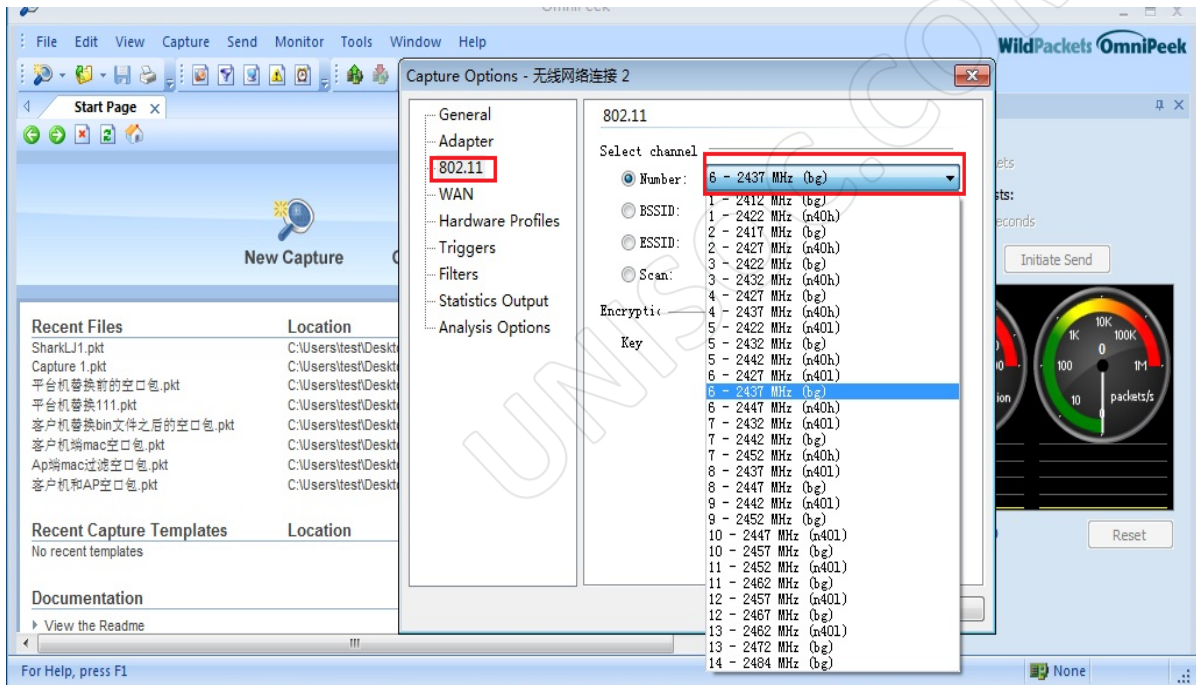
3. 查看手机wifi分析仪上手机连接的ap的**信道**、及ap的**mac**地址、**加密方式**等信息，如下图红色框内



Wifi空口包抓包方法

二、操作步骤：

4. 根据上步的信道信息，选择对应的信道（注意：需要选择 bg或者bgn）



Wifi空口包抓包方法

二、操作步骤：

5. 解密

解密空口包的两个必要条件：

1、抓到wifi连接的过程

2、如果加密ap需要导入key（请优先使用ap非加密模式进行log抓取）

如果是加密ap需要先输入ap的ssid和密码，会自动生成key，这样才能看到解密的数据包；

注意：ssid（ap的名字）不能包含中文，包含中文无法正常解析。

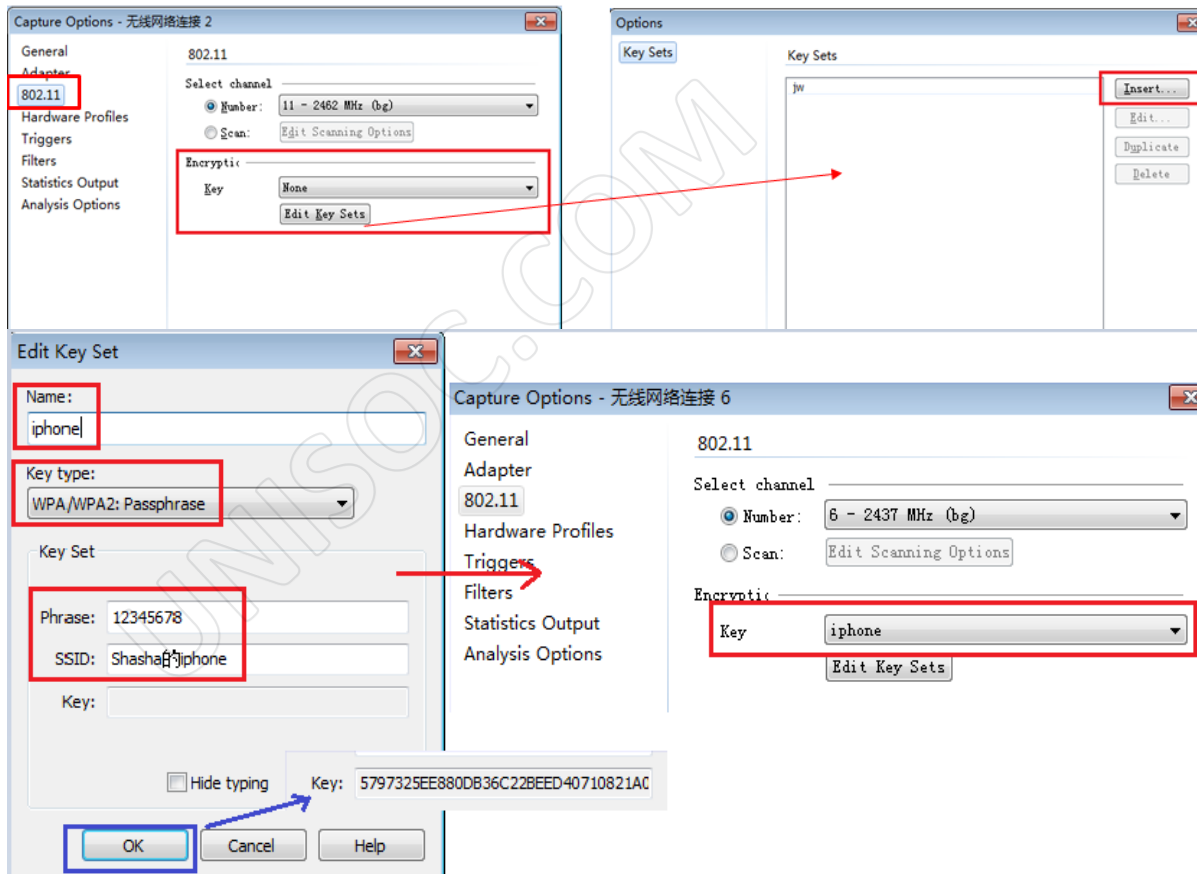
操作步骤：

802.11→Encryption→Edit Key Sets→Insert→Name：取个名字→Key type：选择对应ap的加密方式→Key Set→Phrase：AP密码→SSID：AP名称，需要完全一致→点击ok后会自动生成key→选择设置的key→确定

Wifi空口包抓包方法

二、操作步骤：

5. 解密

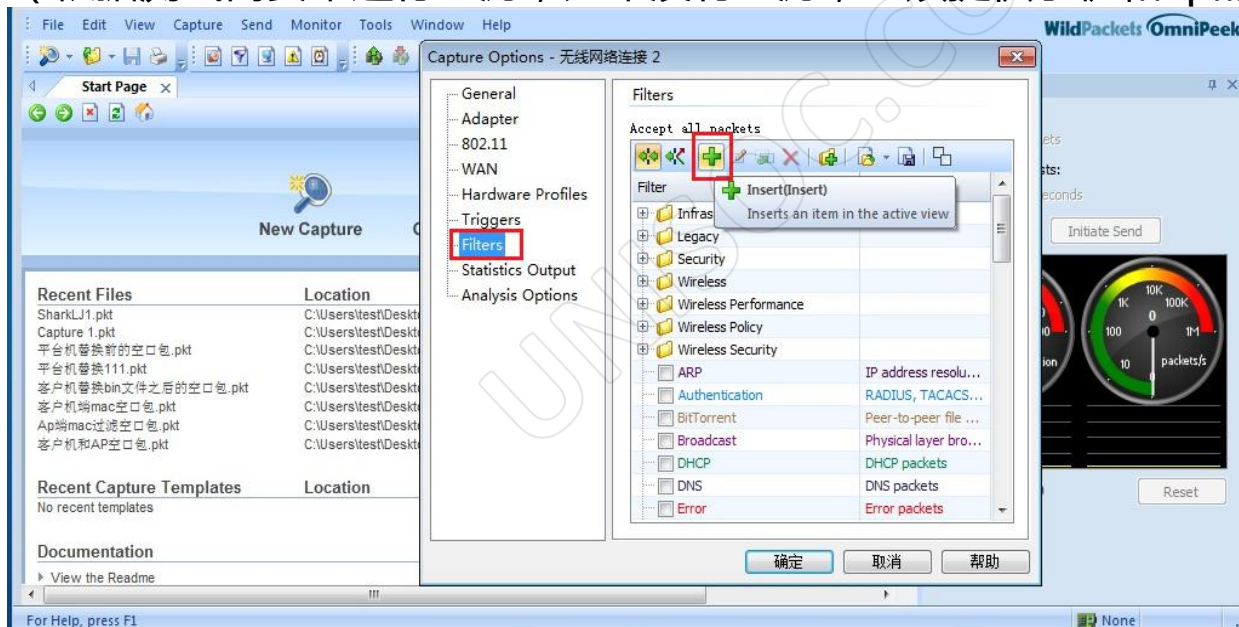


Wifi空口包抓包方法

二、操作步骤：

6. Mac地址过滤

(根据测试需要来进行过滤，如果没有过滤，必须提供手机和ap的mac地址)



Wifi空口包抓包方法

二、操作步骤：

6. Mac地址过滤

红色框内填写过滤条件的新起的名称，

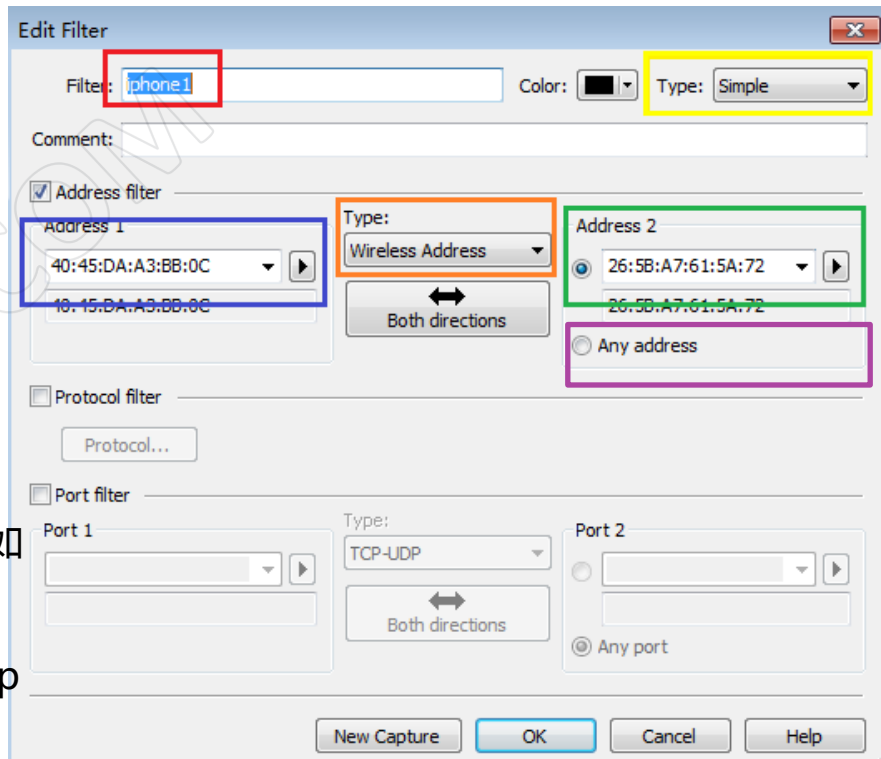
蓝色框是手机的mac地址，

绿色框是ap的mac地址

说明：

- 1、mac地址的过滤条件可根据自己的需求进行筛选，如果不筛选会抓到所有的空口信息，
- 2、如果右侧选择any，会抓到和左侧手机交互的所有ap的空口包)

注意type需要选对 **wireless address**

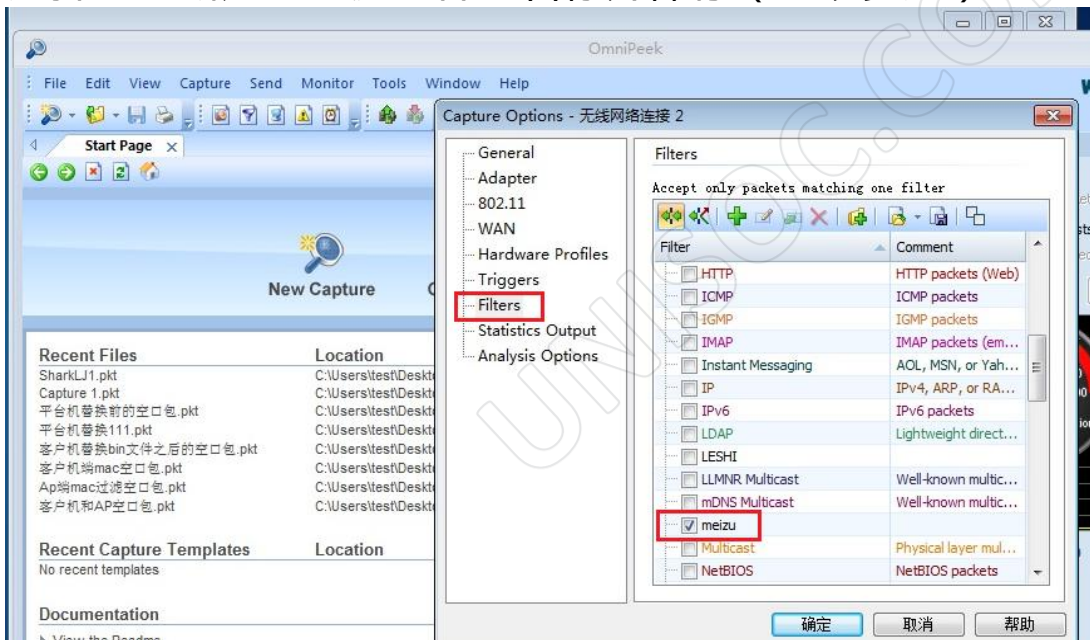


Wifi空口包抓包方法

二、操作步骤：

6. Mac地址过滤

选择刚才新建的过滤条件的名称并保存（可以多选）



Wifi空口包抓包方法

二、操作步骤：

7. 开始抓空口包

点击开始抓包按钮，Capture—packets可以看到空口包在抓（开始抓包后再测试）
需要从wifi搜索开始抓，必须要抓到连接过程才能解密空口包

空口包解密的两个条件：

- 1、ap open模式或加密模式已经导入key
- 2、空口包从连接过程开始抓

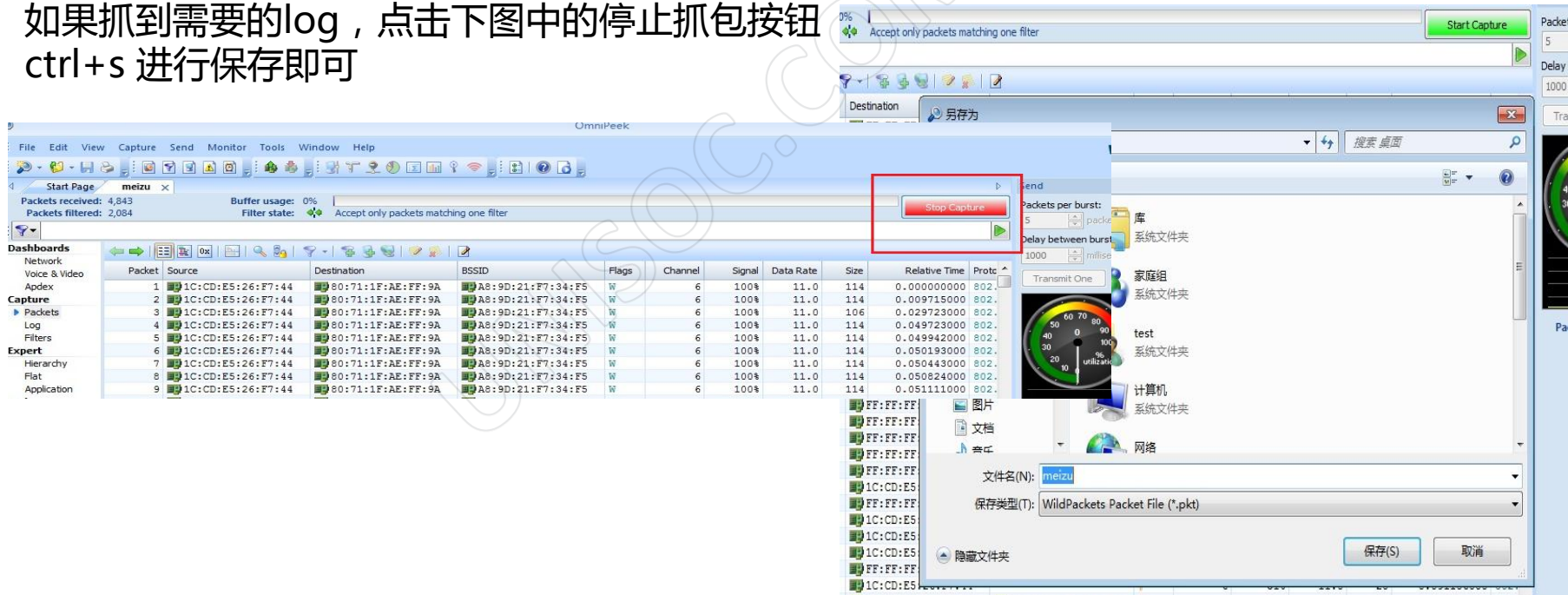


Wifi空口包抓包方法

二、操作步骤：

7. 开始抓空口包

如果抓到需要的log，点击下图中的停止抓包按钮
ctrl+s 进行保存即可



Wifi空口包抓包方法

三、空口Log确认：

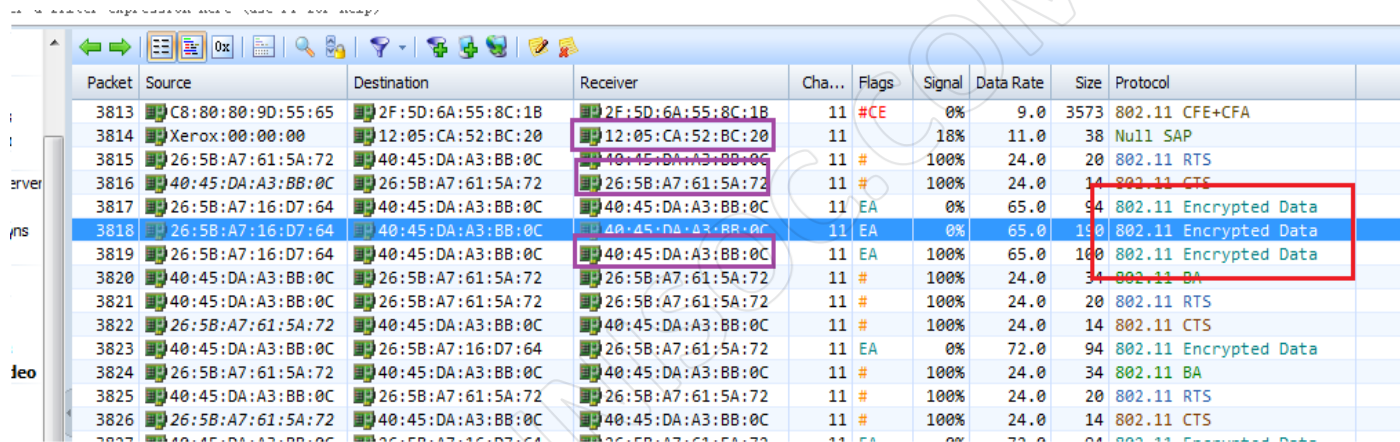
如何确认包是否有过滤和解密成功：

- 1、紫色区域可以看到是否只有要过滤的Mac地址
- 2、红色区域是已被解密的数据包（http、https等），如果是未解密的则会看到802.11 Encrypted Data
- 3、绿色区域是log抓取的系统时间

Packet	Source	Destination	Receiver	Ch...	Flags	Signal	Data Rate	Size	Protocol	Absolute Time
6127	192.168.43.163	112.65.203.49	04:4F:4C:2C:C9:F5	11	E	0%	72.0	857	HTTPS	18:56:19.796129
6128	04:4F:4C:2C:C9:F5	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	34	802.11 BA	18:56:19.796131
6129	112.65.203.49	192.168.43.163	40:45:DA:A3:BB:0C	11	E	100%	57.5	78	HTTPS	18:56:19.796797
6130	112.65.203.49	192.168.43.163	40:45:DA:A3:BB:0C	11	E	100%	57.5	78	HTTPS	18:56:19.796802
6131	112.65.203.49	192.168.43.163	40:45:DA:A3:BB:0C	11	E	100%	57.5	418	HTTPS	18:56:19.797248
6132	112.65.203.49	192.168.43.163	40:45:DA:A3:BB:0C	11	E	100%	57.5	103	HTTPS	18:56:19.797254
6133	112.65.203.49	192.168.43.163	40:45:DA:A3:BB:0C	11	E	100%	57.5	418	HTTPS	18:56:19.797793
6134	112.65.203.49	192.168.43.163	40:45:DA:A3:BB:0C	11	E	100%	57.5	103	HTTPS	18:56:19.797796
6135	04:4F:4C:2C:C9:F5	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	20	802.11 RTS	18:56:19.797798
6136	112.65.203.35	192.168.43.163	40:45:DA:A3:BB:0C	11	E	0%	57.5	1418	HTTP	18:56:19.798008
6137	112.65.203.35	192.168.43.163	40:45:DA:A3:BB:0C	11	EA	100%	57.5	1418	HTTP	18:56:19.798318
6138	40:45:DA:A3:BB:0C	04:4F:4C:2C:C9:F5	04:4F:4C:2C:C9:F5	11	#	100%	24.0	34	802.11 BA	18:56:19.798320
6139	04:4F:4C:2C:C9:F5	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	20	802.11 RTS	18:56:19.798539
6140	112.65.203.35	192.168.43.163	40:45:DA:A3:BB:0C	11	EA	100%	57.5	1418	HTTP	18:56:19.799191
6141	40:45:DA:A3:BB:0C	04:4F:4C:2C:C9:F5	04:4F:4C:2C:C9:F5	11	#	100%	24.0	34	802.11 BA	18:56:19.799193
6142	04:4F:4C:2C:C9:F5	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	E	100%	57.5	227	802.11 WEP Data	18:56:19.799194
6143	40:45:DA:A3:BB:0C	04:4F:4C:2C:C9:F5	04:4F:4C:2C:C9:F5	11	#	100%	24.0	20	802.11 RTS	18:56:19.799800
6144	192.168.43.163	112.65.203.49	04:4F:4C:2C:C9:F5	11	EA	0%	72.0	78	HTTPS	18:56:19.799802
6145	192.168.43.163	112.65.203.49	04:4F:4C:2C:C9:F5	11	EA	0%	72.0	78	HTTPS	18:56:19.799804
6146	192.168.43.163	112.65.203.35	04:4F:4C:2C:C9:F5	11	EA	0%	72.0	90	HTTP	18:56:19.799805

Wifi空口包抓包方法

三、空口Log确认：



Packet	Source	Destination	Receiver	Cha...	Flags	Signal	Data Rate	Size	Protocol
3813	C8:80:80:9D:55:65	2F:5D:6A:55:8C:1B	2F:5D:6A:55:8C:1B	11	#CE	0%	9.0	3573	802.11 CFE+CFA
3814	Xerox:00:00:00	12:05:CA:52:BC:20	12:05:CA:52:BC:20	11	#	18%	11.0	38	Null SAP
3815	26:5B:A7:61:5A:72	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	20	802.11 RTS
3816	40:45:DA:A3:BB:0C	26:5B:A7:61:5A:72	26:5B:A7:61:5A:72	11	#	100%	24.0	14	802.11 CTS
3817	26:5B:A7:16:D7:64	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	EA	0%	65.0	94	802.11 Encrypted Data
3818	26:5B:A7:16:D7:64	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	EA	0%	65.0	130	802.11 Encrypted Data
3819	26:5B:A7:16:D7:64	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	EA	100%	65.0	100	802.11 Encrypted Data
3820	40:45:DA:A3:BB:0C	26:5B:A7:61:5A:72	26:5B:A7:61:5A:72	11	#	100%	24.0	34	802.11 BA
3821	40:45:DA:A3:BB:0C	26:5B:A7:61:5A:72	26:5B:A7:61:5A:72	11	#	100%	24.0	20	802.11 RTS
3822	26:5B:A7:61:5A:72	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	14	802.11 CTS
3823	40:45:DA:A3:BB:0C	26:5B:A7:16:D7:64	26:5B:A7:61:5A:72	11	EA	0%	72.0	94	802.11 Encrypted Data
3824	26:5B:A7:61:5A:72	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	34	802.11 BA
3825	40:45:DA:A3:BB:0C	26:5B:A7:61:5A:72	26:5B:A7:61:5A:72	11	#	100%	24.0	20	802.11 RTS
3826	26:5B:A7:61:5A:72	40:45:DA:A3:BB:0C	40:45:DA:A3:BB:0C	11	#	100%	24.0	14	802.11 CTS
3827	40:45:DA:A3:BB:0C	26:5B:A7:16:D7:64	26:5B:A7:61:5A:72	11	EA	0%	72.0	94	802.11 Encrypted Data

未过滤会有多个Mac

加密的数据包



谢谢！

本文件所含数据和信息都属于紫光展锐机密及紫光展锐财产，紫光展锐保留所有相关权利。当您接受这份文件时，即表示您同意此份文件内含机密信息，且同意在未获得紫光展锐同意前，不使用或复制、整个或部分文件。紫光展锐有权在未经事先通知的情况下，对本文件做任何修改。紫光展锐对本文件所含数据和信息不做任何保证，在任何情况下，紫光展锐均不负责任何与文件相关的直接或间接的、任何伤害或损失。