- 冬 冬 说 无 线 -

无线空口抓包篇

H3C WLAN

热心网友：风凉瓜甜WiFi差，快乐失去十之八

神秘老王：无线偶感体验差，常用手段先排查

热心网友：重启重连还是卡，有线链路已排查

对方不在线中

对方不在线中

神秘老王：无线报文空口抓，方法如下共有俩

无线空口抓包篇

由于无线网络是电磁波，传输介质是在空气，没有实际存在的物理链路。经过初步排查后，如果怀疑问题出在AP到无线终端这一端，常常无法判断具体问题是出在无线客户端上还是在AP上。此时就需要采集无线空口的交互报文，再定位具体问题出在哪个节点。

此类问题一般涉及**无线空口丢包**，**无线终端接入异常**，**无线终端异常掉线**等接入层问题。

无线空口的交互总是令人扑朔迷离，终端和AP究竟都在空中传递什么信息呢？**空口抓包**让报文无所遁形~

第一弹 使用无线抓包网卡进行空口抓包

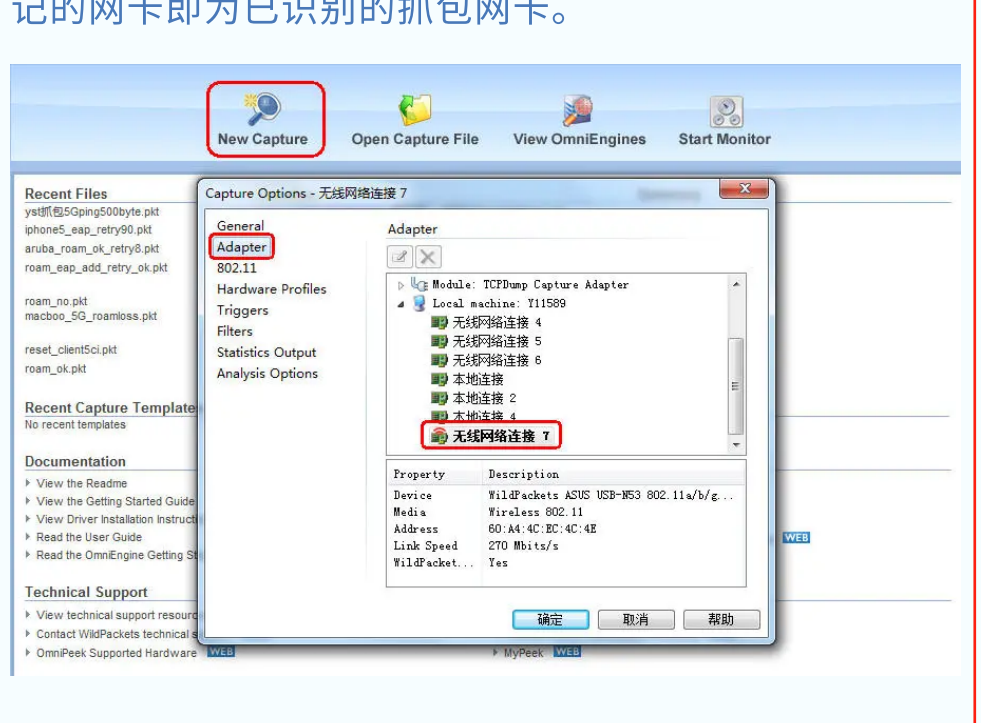
1、安装抓包网卡（以Netgear A6210为例）

将无线抓包网卡Netgear A6210接到PC上，使用Omnipeek空口抓包软件抓包。（无线抓包网卡的安装方式可移步知了社区查看：https://zhiliao.h3c.com/Theme/details/17144）

PS:相应的抓包网卡需要支持对应的802.11协议才能采集到空口的报文交互。网卡直接插上电脑为普通无线网卡接入模式，安装sniffer嗅探模式驱动才可用来抓包。

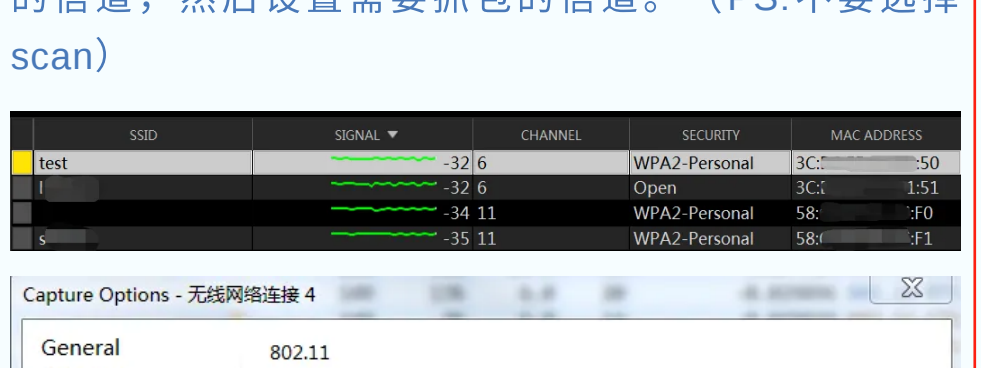
2、识别网卡驱动

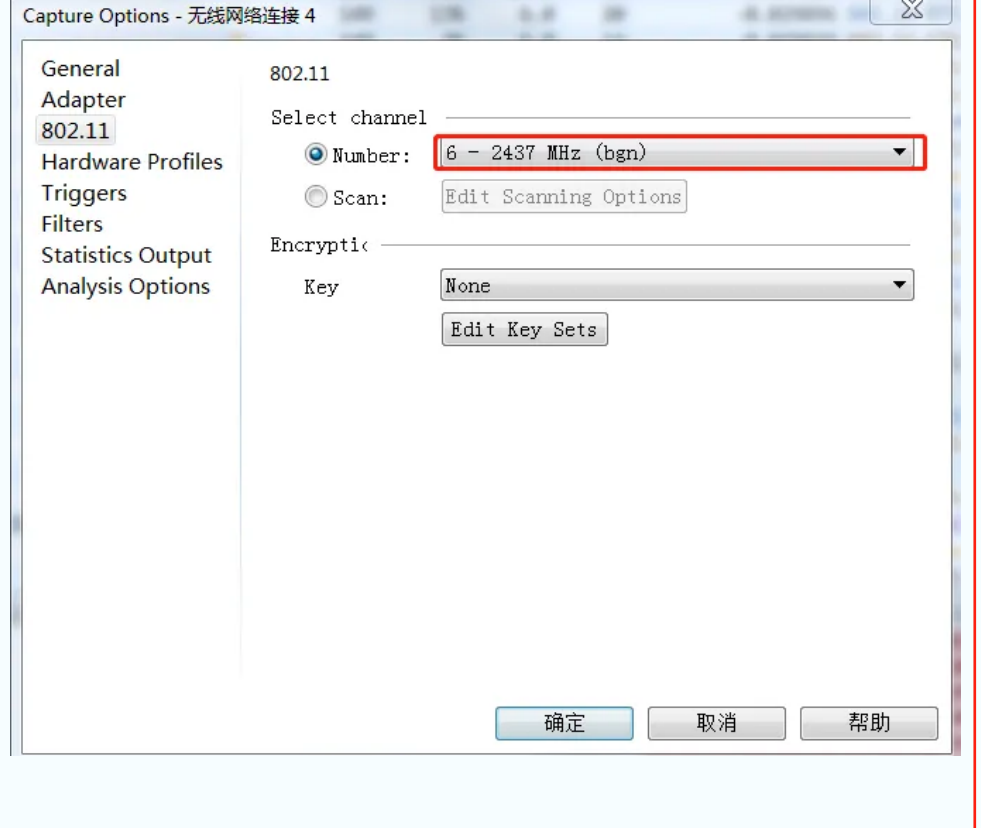
打开omnipeek 软件，选择"New Capture"弹出对话框，选择左侧"Adapter"查看抓包网卡是否已识别，有红色标记的网卡即为已识别的抓包网卡。



3、选择抓包信道

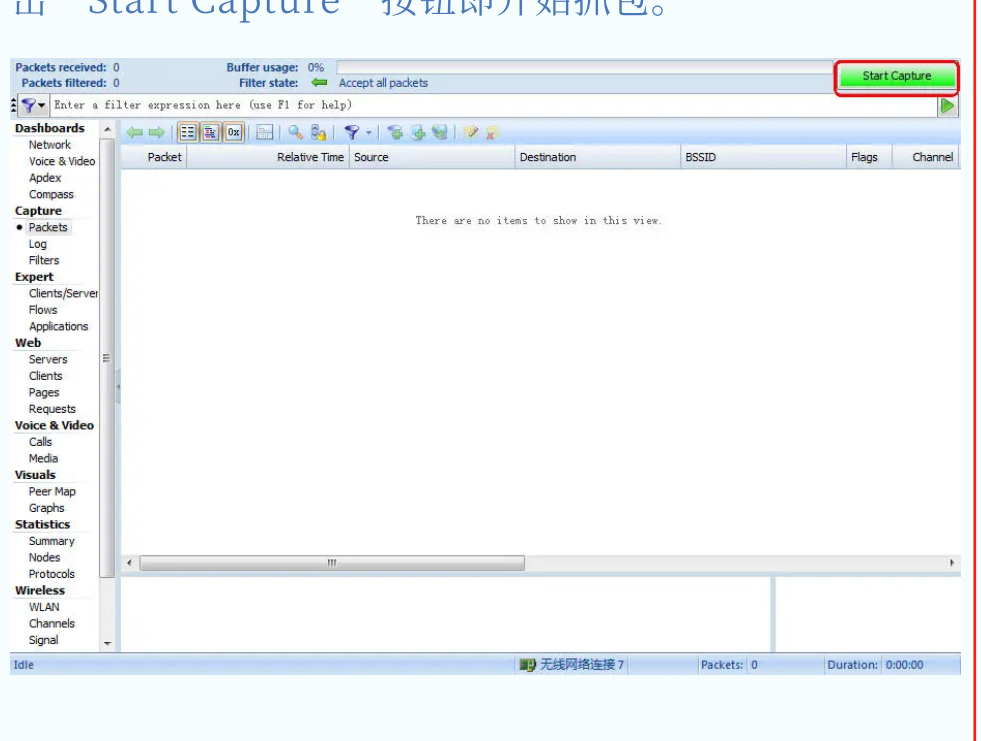
选择左侧"802.11"设置抓包的信道，在空口抓包过程中，网卡只能抓取指定信道的报文，因此需预先查看AP的信道，然后设置需要抓包的信道。（PS:不要选择scan）





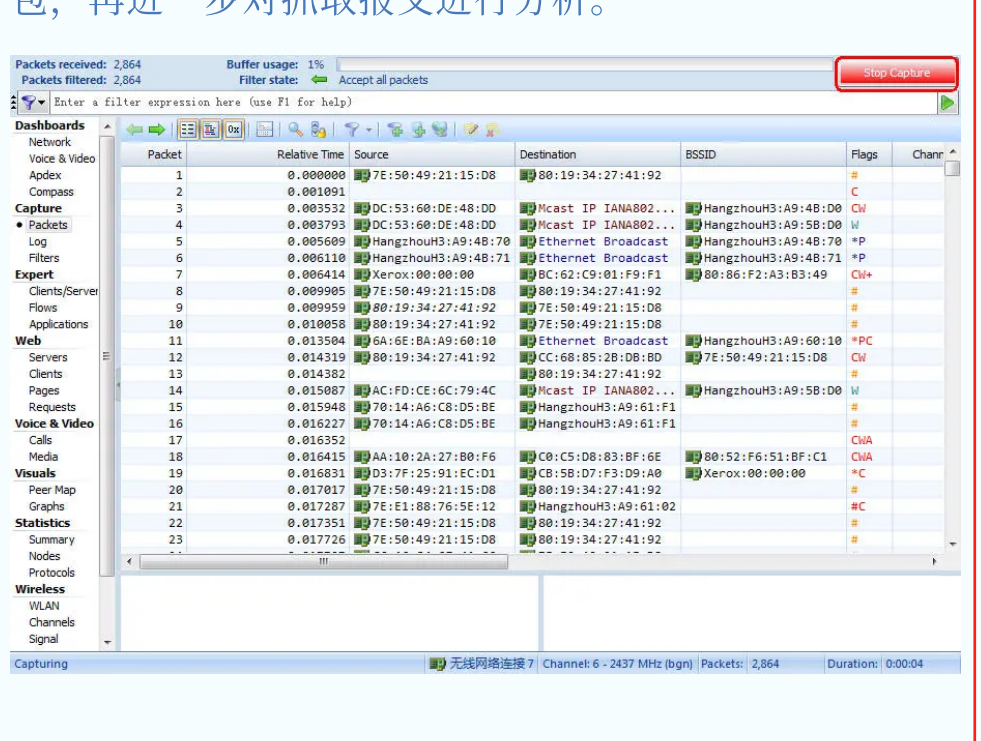
4、开始抓包

设置完成后，点击"确认"，即跳转到抓包界面，点击"Start Capture"按钮即开始抓包。



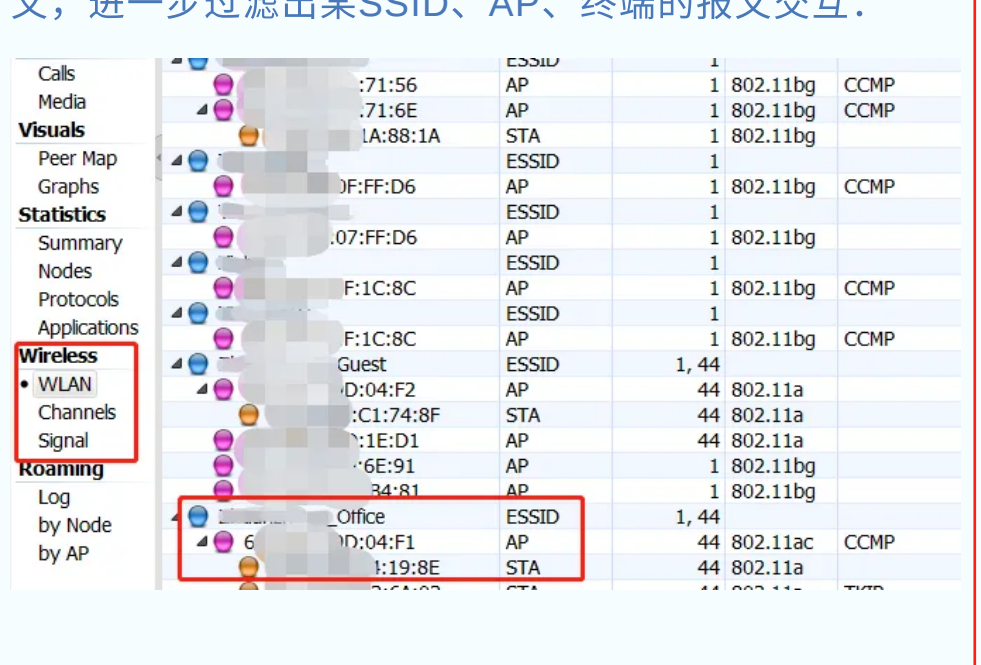
5、复现问题

点击开始抓包后就可以手动终端关联WiFi复现问题了，问题复现后停止抓包，点击"Stop Capture"停止抓包，再进一步对抓取报文进行分析。



6、筛选无线报文

通过点击左侧菜单栏"WLAN"，可以查看出无线的报文，进一步过滤出某SSID、AP、终端的报文交互：



第二弹使用Macbook进行空口抓包

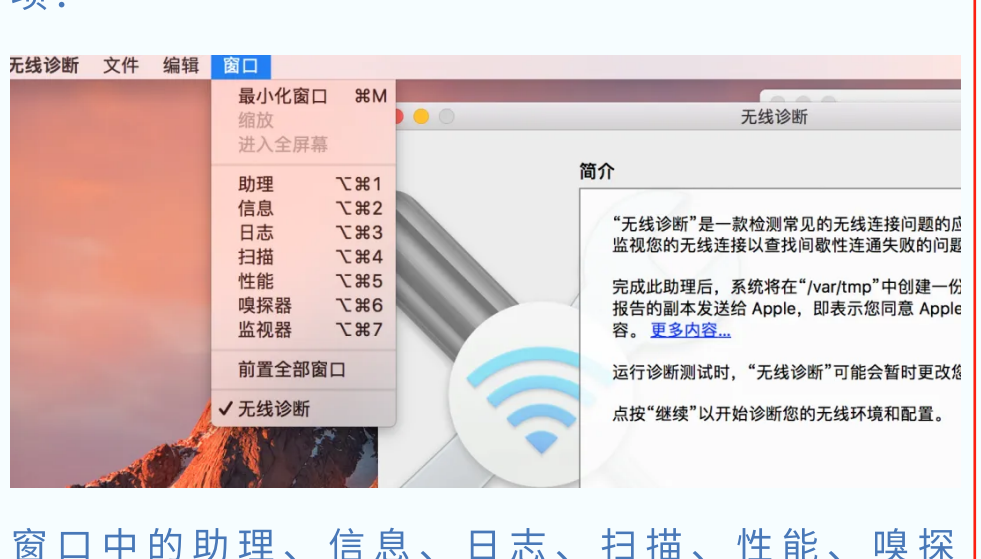
神秘老王：没有抓包网卡怎么办？如果你手边正有一台**苹果电脑**的话，一切问题迎刃而解~

1、打开无线诊断

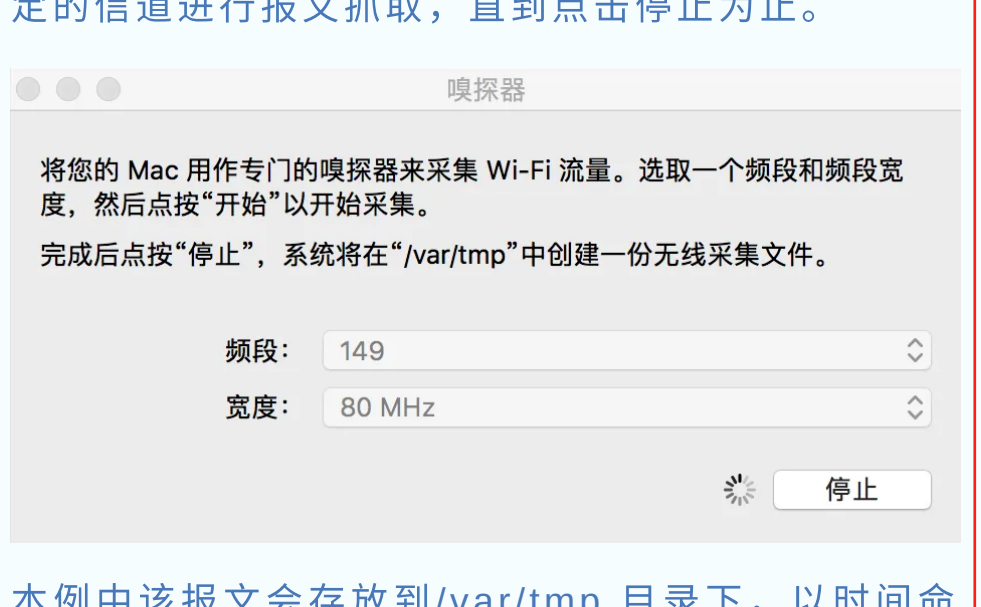
历史版本的macos都会在应用程序目录下的实用工具中直接存放无线诊断这个自带工具；但是在最新版本的10.12.x的版本中系统将该实用的自带工具隐藏了，第一次使用时需要通过如下方法进行获取：在搜索栏对整台Mac进行搜索 "无线诊断"，或者通过目录找寻：/System/Library/CoreServices/Applications

2、选择嗅探器

打开无线诊断工具后，可以在任务栏找到窗口选项：



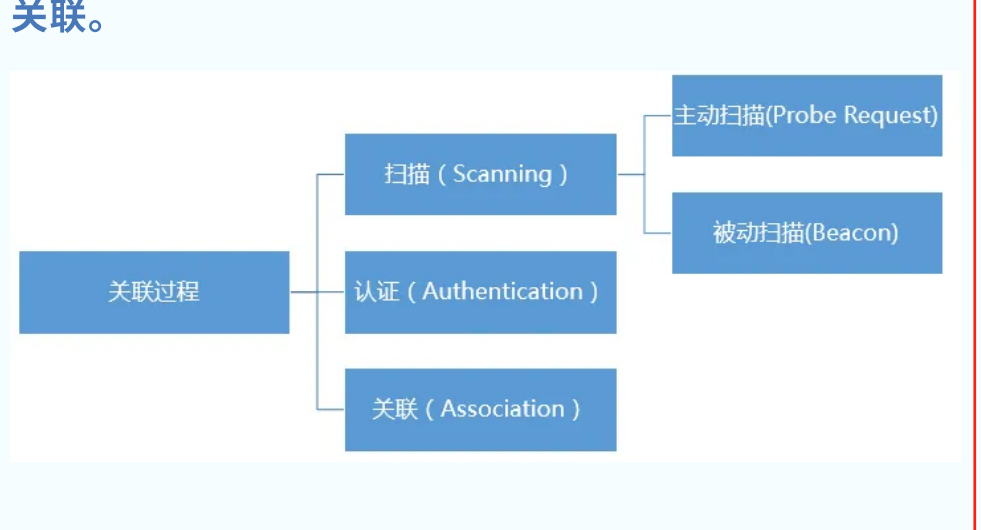
窗口中的助理、信息、日志、扫描、性能、嗅探器、监控器，都是工具中的不同小程序，都有各自的侧重功能，其中与无线抓包相关的是**嗅探器**，打开嗅探器可以选择信道（1～13、36～64 、149～161）和频宽（20、40、80），点击开始便会在指定的信道进行报文抓取，直到点击停止为止。



本例中该报文会存放到/var/tmp 目录下，以时间命名的文件，如：2020.11.17_22-22-47-GMT + 8 . wcap。

第三弹空口抓包报文解析

1、终端关联WiFi过程可以分为三部分：扫描、认证、关联。



- 主动扫描：终端主动在每个信道发送Probe Request广播，从AP回应的Probe Response中获取SSID的基本信息。
- 被动扫描：终端侦听AP定期发送的Beacon帧（PS:如果配置的为隐藏SSID，则AP发送的Beacon不携带SSID信息）

2、终端关联过程

3、终端解关联过程

如遇终端关联不上WiFi/异常下线等问题，可通过空口抓包查看是终端还是AP主动发了解关联请求，从而查看进一步的原因~

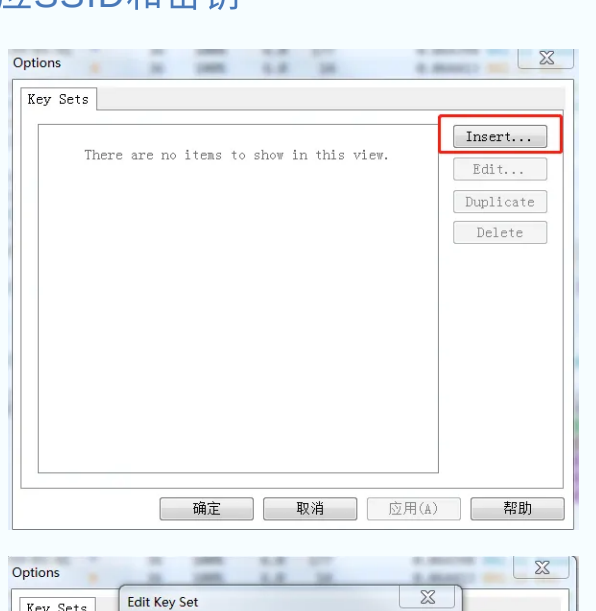
第四弹加密报文如何解密

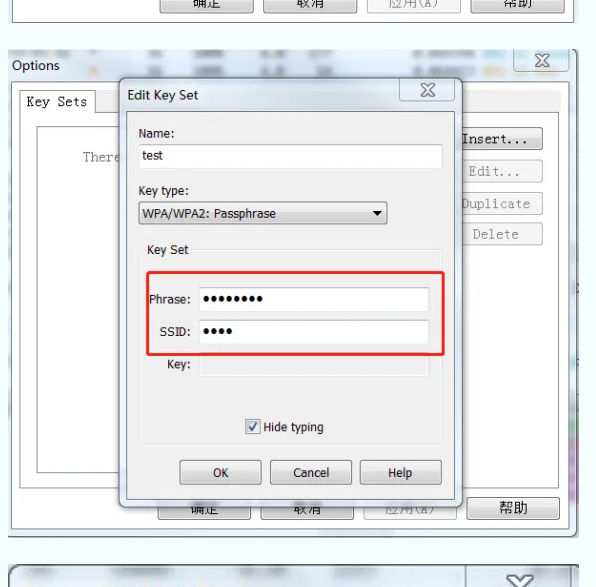
在加密的网络中，无线设备会跟终端先进行四次握手，生成密钥对，对无线数据报文进行加密传输。那么如何查看加密后的空口报文呢？

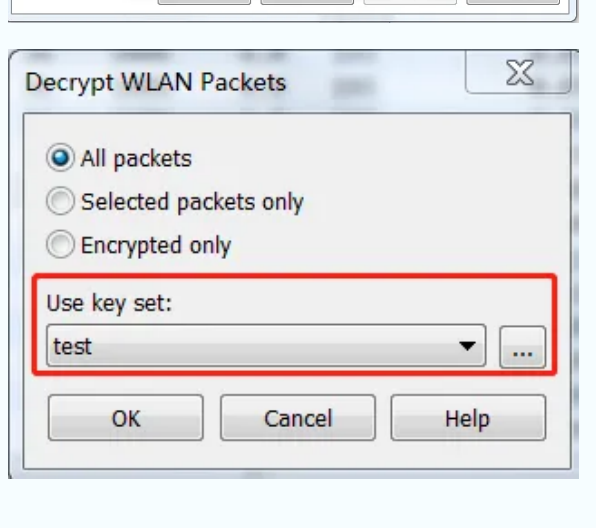
使用Omnipeek抓包后，可对报文进行解密处理：

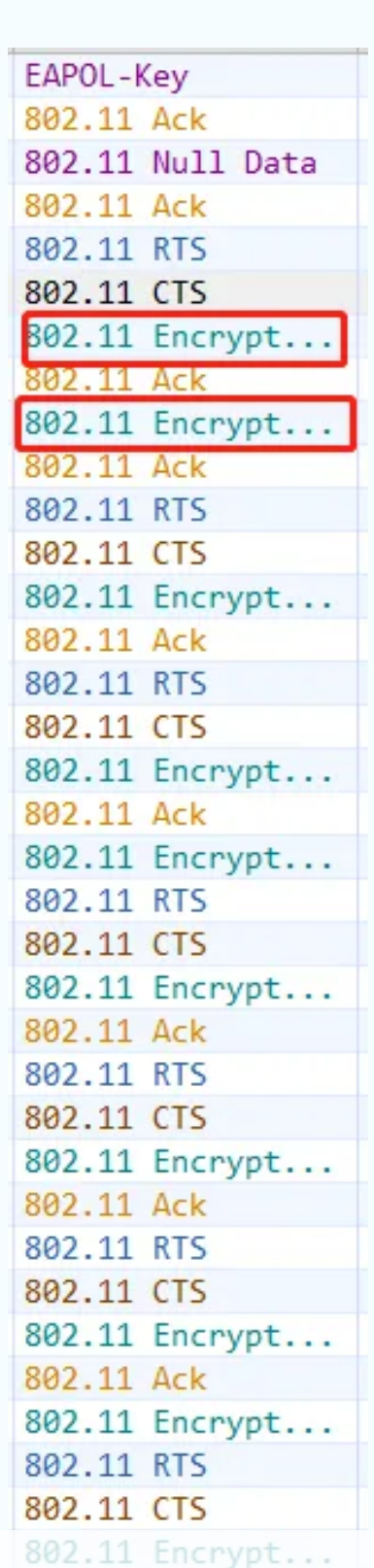
1、点击工具栏"Tools—Decrypt WLAN Packets"

2、输入对应SSID和密钥

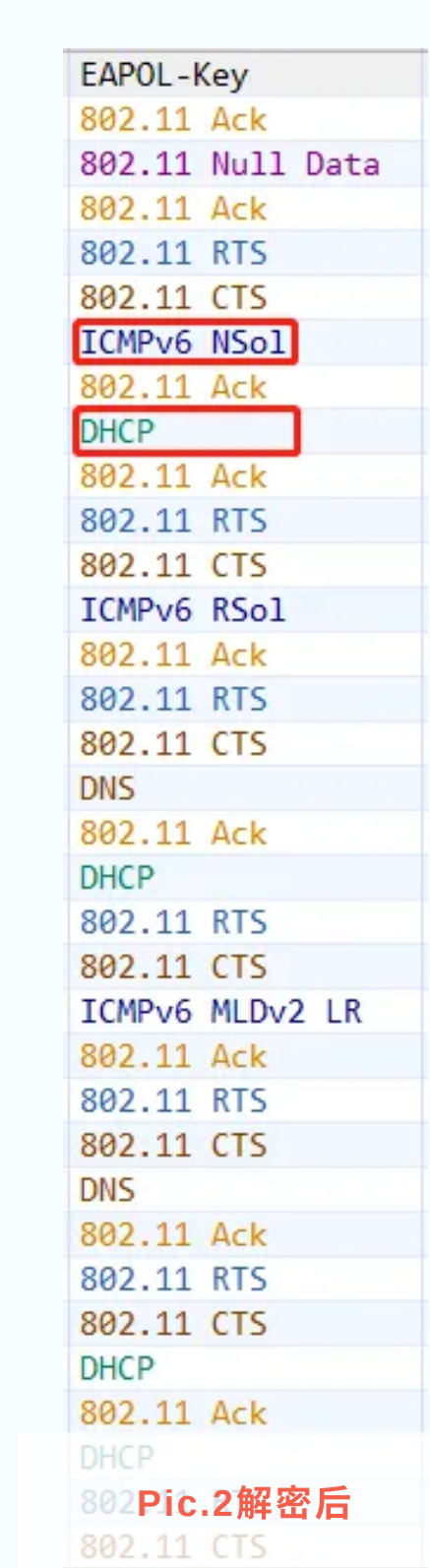








Pic.1 解密前



Pic.2解密后

神秘老王：以后你的WiFi不再是秘密~

<宠粉走起来>

更多感兴趣的无线专题 猛戳评论区留言给小编~

想了解更多无线知识可以复制下方链接或点击阅读全文，欢迎下载学习《无线V7一本通V2.0》，《小贝无线一本通V1.0》，无线维护的好帮手！

http://h3c.com/cn/Service/Document_Software/TechnicalInfo/PorductMaintanInfo/WLAN/DailyMainten/DailyMaintenGuide/

冬冬说无线 下期再见~！

PS：官方技术支持热线，请拨打400-810-0504

更多内容，请关注

H3C Service

球分享 球点赞 球在看