使用Macbook进行无线报文捕获和分析

wlan接入 朱恺 2017-03-21 发表

在常见的无线网络问题处理中，我们往往会遇到抓捕无线空口802.11 mac层的报文进行分析来协助问题的处理。在windows pc上可以使用无线抓包网卡配合omnipeek软件来进行报文的获取和分析。但是实际上还存在一种更为便捷和可靠的无线报文捕获和分析的方式，这就是今天我们要讲述的使用macbook笔记本来进行报文的捕获。

本文以macbook pro为例，macbook的无线抓包分为2种方式：

1、macbook+wireshark进行报文的捕获；

2、直接使用macbook自带的无线诊断实用工具进行报文捕获。

Macbook with Wireshark方式：

首先确认你的macbook笔记本网卡时何种规格的，按照目前出厂情况，新款的macbook pro都已经支持802.11ac 3*3规格的无线环境，可以在macos系统中的 **关于本机→系统报告→网络→Wi-Fi**进行查看无线网卡的固件和软件版本，如图1：

图1

然后需要去获取wireshark软件macos版本，官方下载站点https://www.wireshark.org/download.html，如图2：

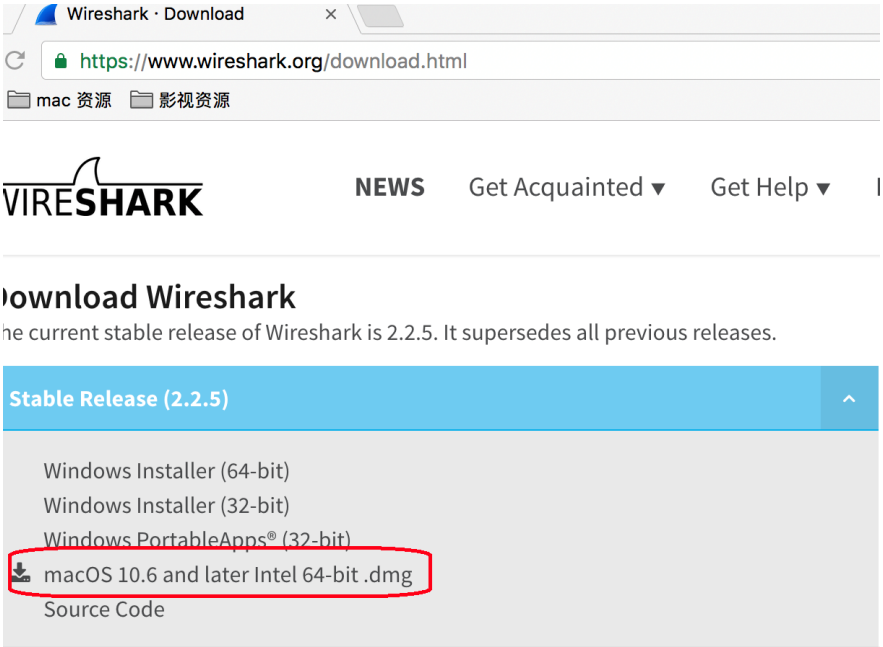

图2

按照正常macos软件安装的方式进行安装后，打开wireshark软件。最新版本的macos 10.12.3配合wireshark官方的v2.2.5版本集成度非常高，简便的安装完成之后，进入wireshark视图，选择 **捕获（**Capture）→ **选项（Option）**,可以看见默认的Wi-Fi接口就已经选择了混杂模式和监控模式，并且选择了802.11 plus radiotap header（若不想抓取802.11格式的无线报文，仅仅想看802.3以太报文可以将监控模式取消。）如图3:

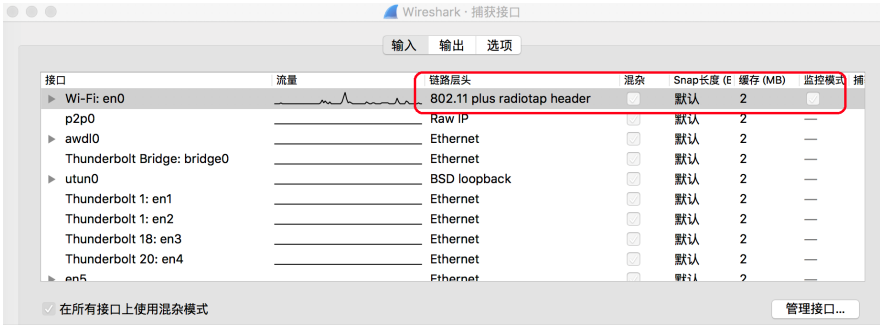

图3

此时抓取的报文就是当前macbook笔记本关联的BSSID所在信道的无线报文，若想知道当前macbook网卡所在的信道是哪一个，可以通过 **option键+鼠标点击**wifi扇形图标显示wifi链接的高级视图，在这个试图可以看到权限更高的wifi链接详情，如RSSI,当前协商速率，mcs等。如图4:

图4

上述便是macbook笔记本直接使用wireshark快速获取无线报文的方式，但是也存在一点局限性，比如想抓捕当前其他信道的无线报文，没有办法灵活的选择指定的信道和带宽模式去抓捕。因此我们介绍第二个抓捕方式：macbook自带的无线实用工具+wireshak。

Macbook自带的无线实用工具：

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 搜素 “无线诊断”，一般都能找到，可对其进行复制黏贴，存放到自己好获取的位置；或者通过目录找寻：/System/Library/CoreServices/Applications ； 图5：

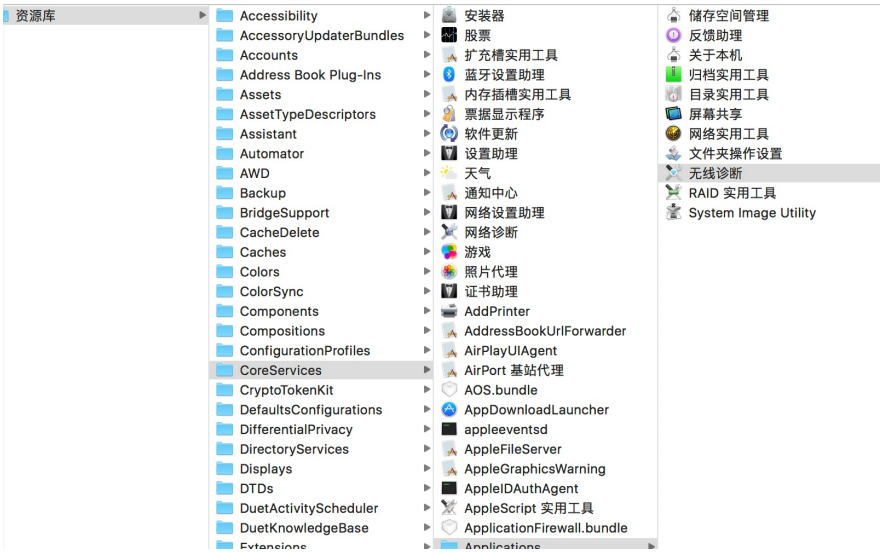

图5

打开无线诊断工具后，可以在任务栏找到窗口选项，如图6:

图6

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，如图7:

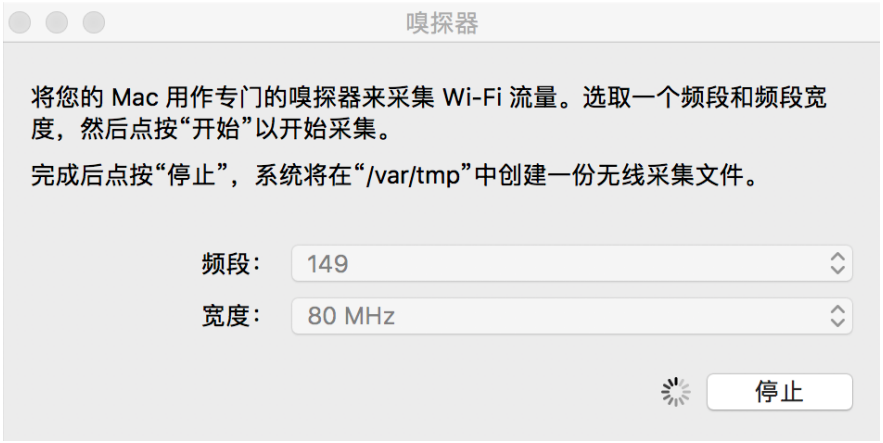

图7

本例中该报文会存放到/var/tmp 目录下，以时间命名的文件，如：2016.11.17_22-22-47-GMT+8.wcap该文件使用wireshark打开即可进行无线报文的分析。