在MacBook上通过空中收集数据包捕获

目录

简介

本文档介绍如何在MacBook上使用本机工具无线诊断和第三方应用（如Airtool和Wireshark）收集空中数据包捕获(PCAP)，以排除和分析无线行为。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科无线局域网控制器(WLC)AireOS或Cisco IOS®-XE
- 802.11标准中的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Apple MacBook，带MacOS版本10.14.X或更高版本
- Apple无线诊断工具
- Airtool 1.9或更高版本
- Wireshark 3.X或更高版本
- 思科接入点(AP)2802

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

注意事项:

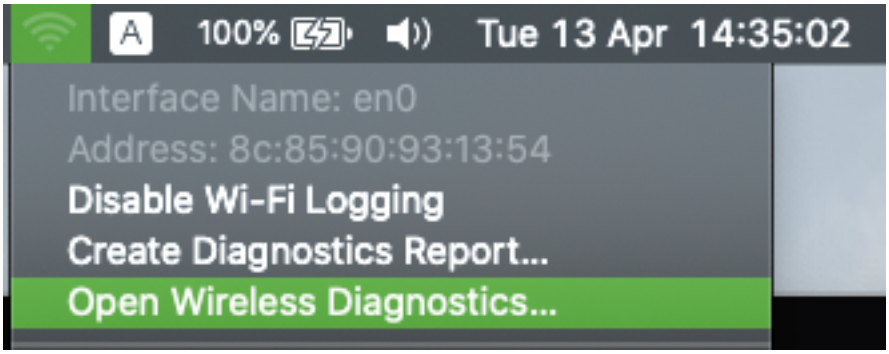
- 建议将Macbook用作无线嗅探器，使其靠近AP和目标设备。
- 确保您知道使用哪个802.11通道和宽度、客户端设备和AP。
- 信道和宽度可在以下位置找到： Cisco IOS®-XE Web图形用户界面(GUI)在**Configuration > Wireless > 5GHz or 2.4GHz > Select an AP > Channel and Width**下AireOS Web GUI在**Wireless > Access Points > 802.11a/n/ac(5GHz)或802.11 b/g/n(2.4GHz)> Select an AP > Channel and Width**

配置

选项A.使用无线诊断配置PCAP

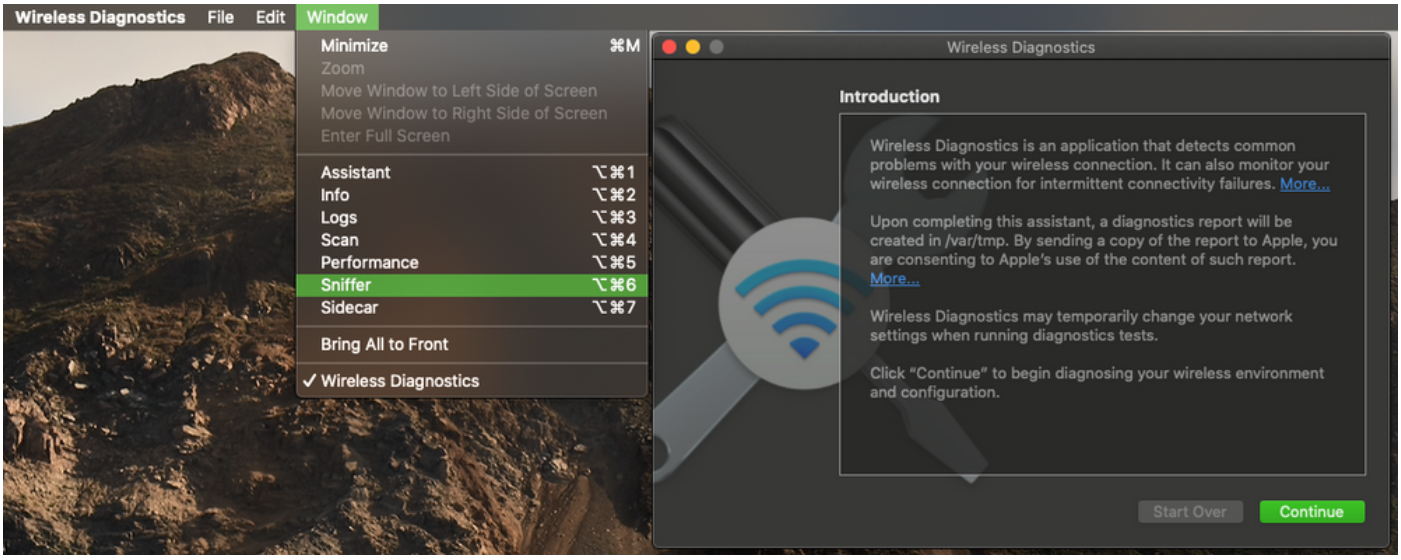
步骤1.启动无线**诊断**工具。

按住键盘**上的ALT/**Option键，然后单击右上**角的Wi-Fi**图标，如图所示。



步骤2.打开嗅探器工具。

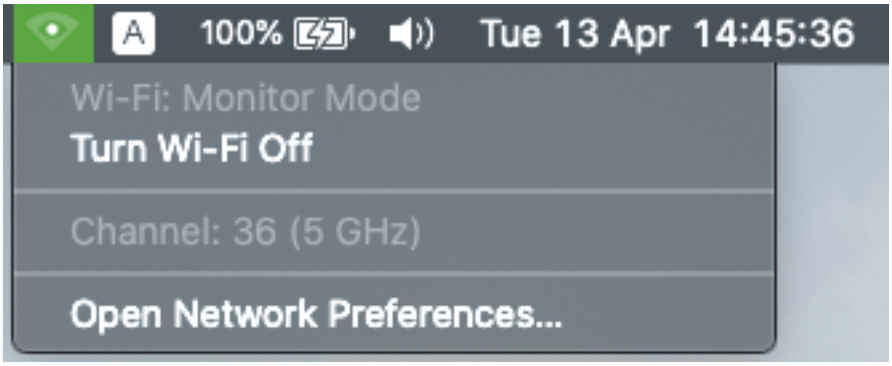
从菜单栏的**Wireless Diagnostic Tool中选**择“Window”菜单，然后选择**Sniffer**或使用键盘快捷键，同时按**ALT + Command + 6** Keys，如图所示。



步骤3.选择目标设备**和AP使用的通道**和宽度，如图所示。

步骤4.单击“开**始”。**

此操作将无线适配器置于监控模式，且无法将设备连接到无线局域网(WLAN)，如图所示。



步骤5.等待一段时间以收集所需信息，然后单击“停**止”。**

提示：如果WLAN使用加密(如预共享密钥(PSK))，请确保捕获捕获AP与所需客户端之间的四次握手。如果OTA PCAP在设备与WLAN关联之前启动，或者如果客户端在捕获运行期间取消

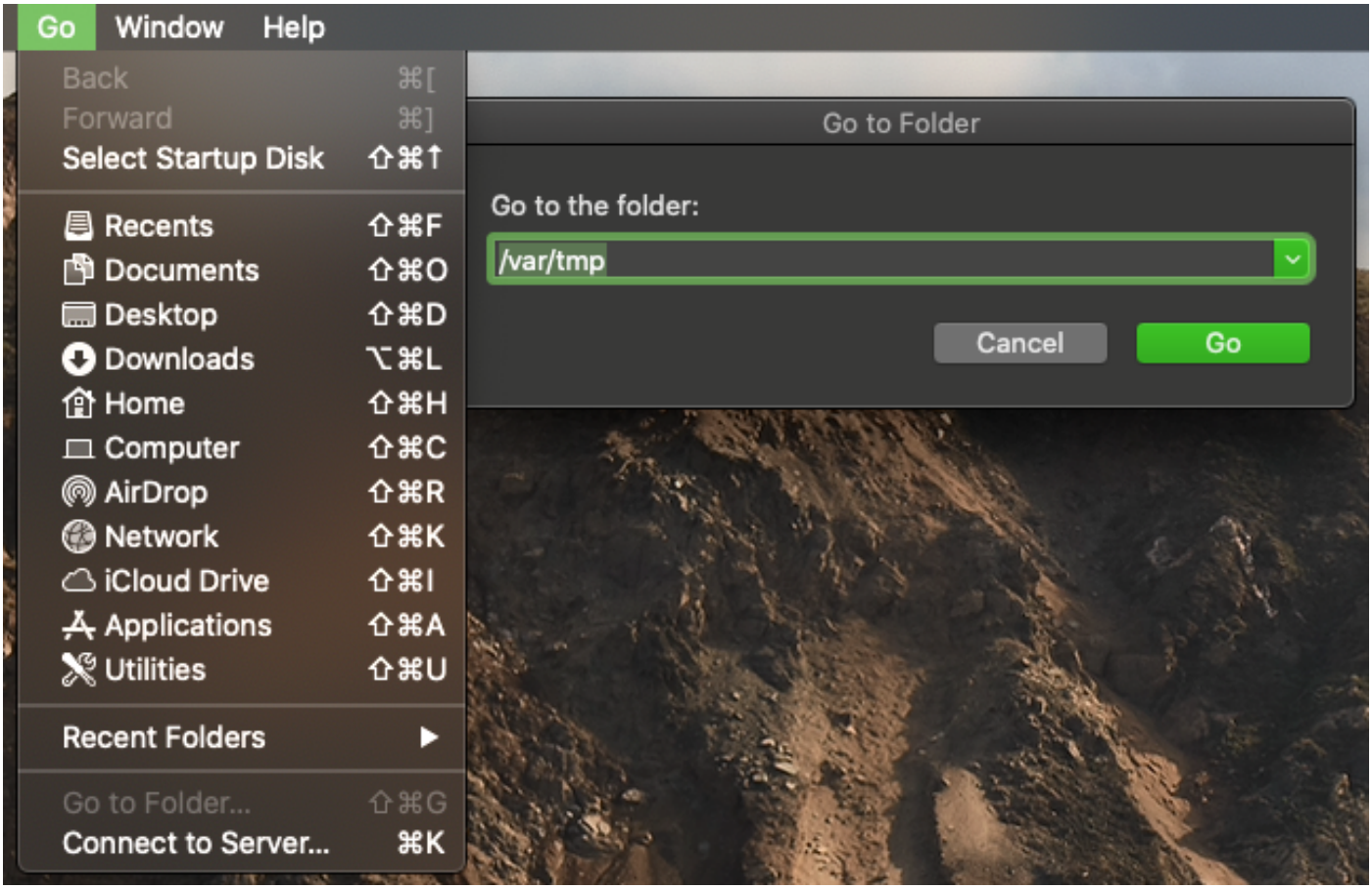
身份验证并重新进行身份验证，则可以执行此操作。

步骤6.该文件位于Desktop（桌面）文件夹或路径**/var/tmp/**（MacBook运行的macOS版本可能不同）。

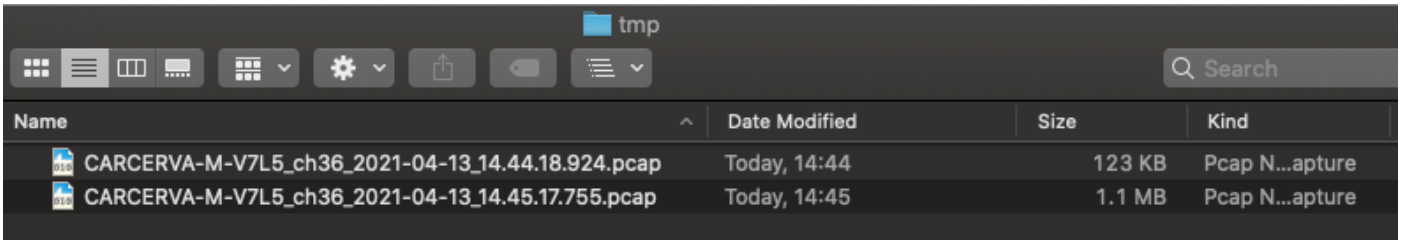
1.在MacBook上启动Finder应用程序，如图所示。

2.从Finder中选**择**"开始"菜单。

3.选择"**桌面文**件夹"**或"转到文**件夹"并键入目标路径。



显示目标文件夹。

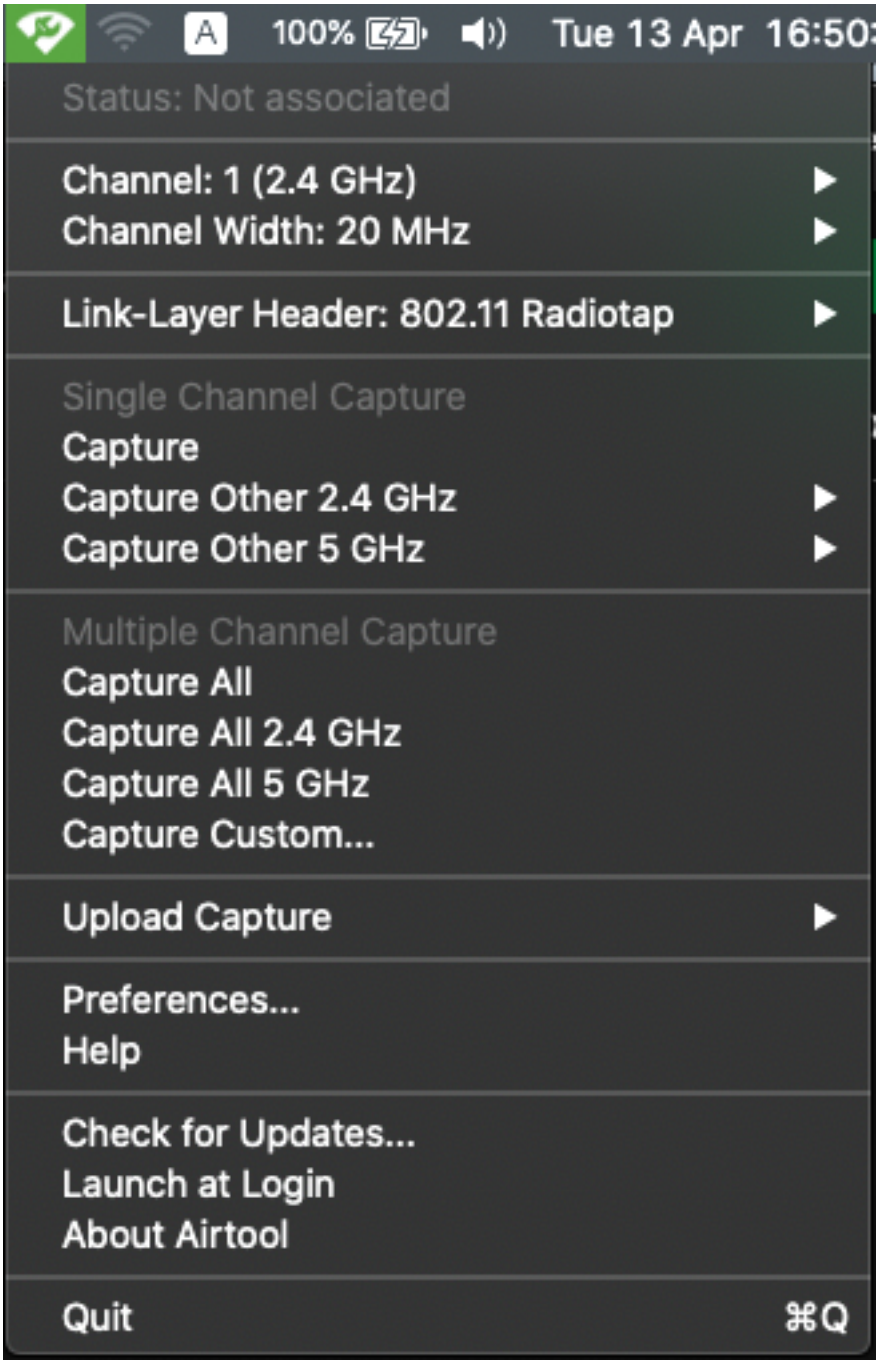


选项B.使用Airtool配置PCAP

步骤1.安装第三方Airtool应用程序。

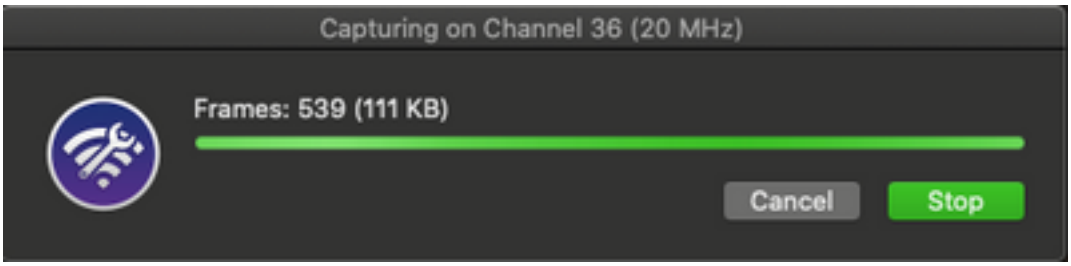
步骤2.启动工具。

启动后，Airtool可位于macOS菜单栏的右上角，如图所示。



步骤3.选择目标设备和AP使**用的**通道和**宽度**（此操作将启动PCAP），如图所示。

步骤4.等待一段时间收集所需信息，然后单击“停止”，如图所示。



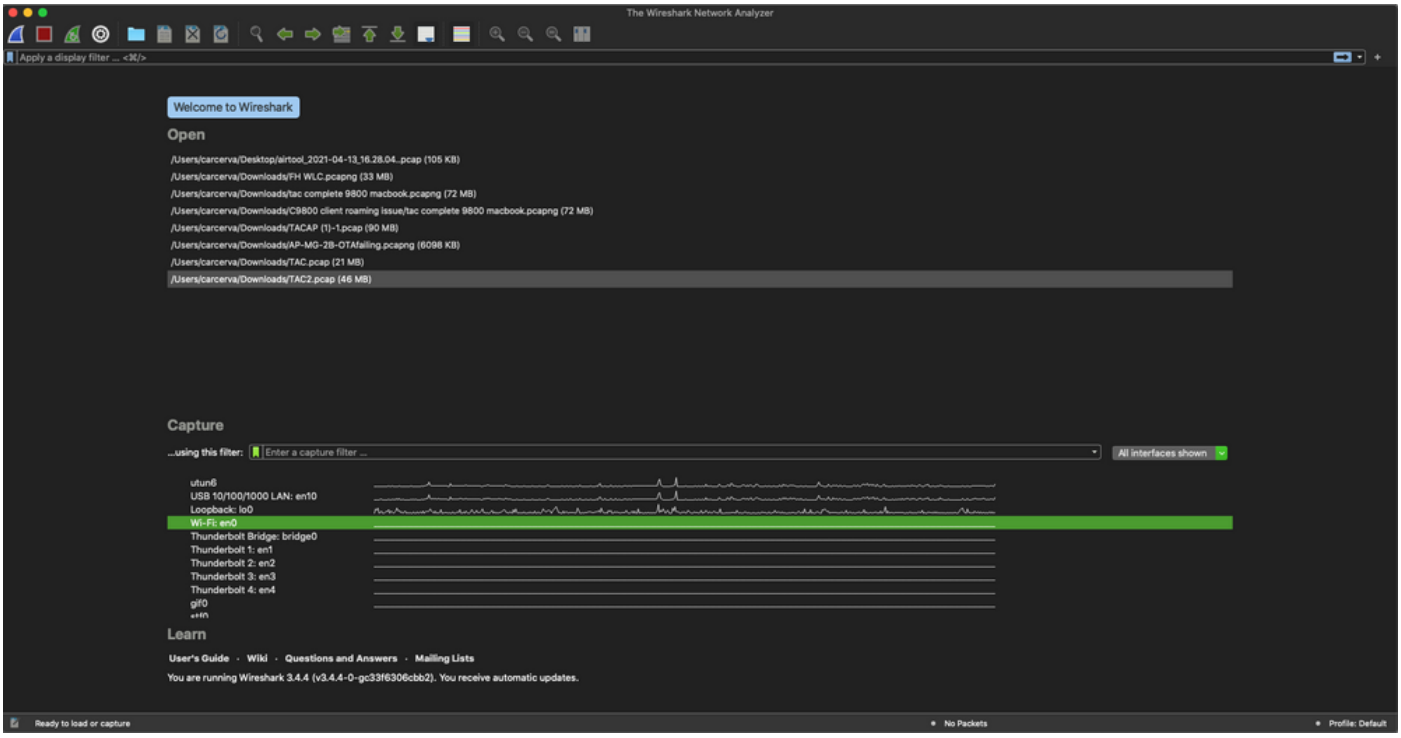
提示：如果WLAN使用加密(如预共享密钥(PSK))，请确保捕获捕获AP与所需客户端之间的四次握手。如果OTA PCAP在设备与WLAN关联之前启动，或者如果客户端在捕获运行期间取消身份验证并重新进行身份验证，则可以执行此操作。

步骤5.该文件位于Desktop（桌面）文件夹中。

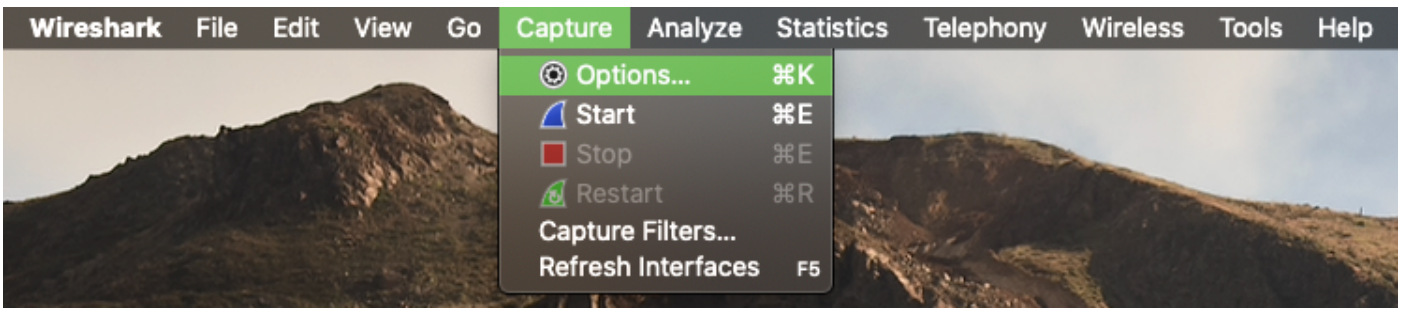
选项C.使用Wireshark配置PCAP

步骤1.安装Wireshark。

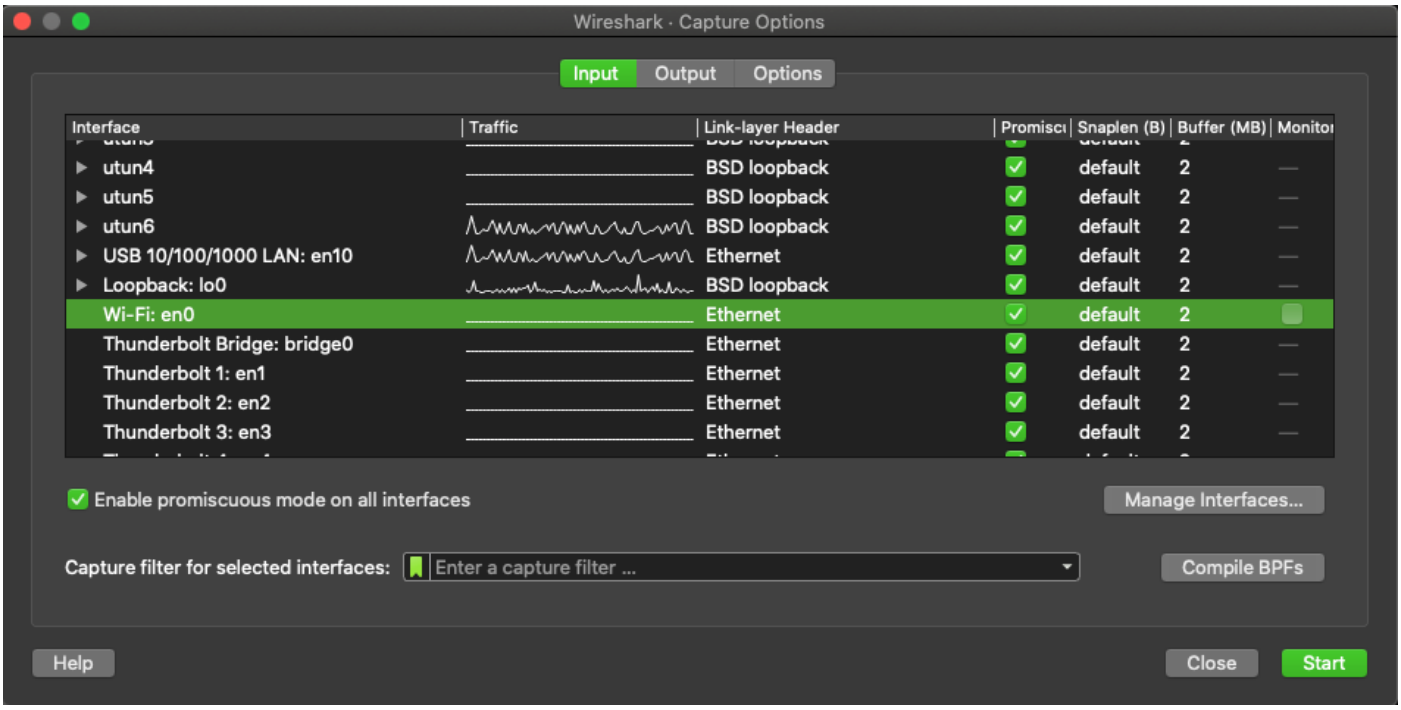
步骤2.启动应用程序，如图所示。



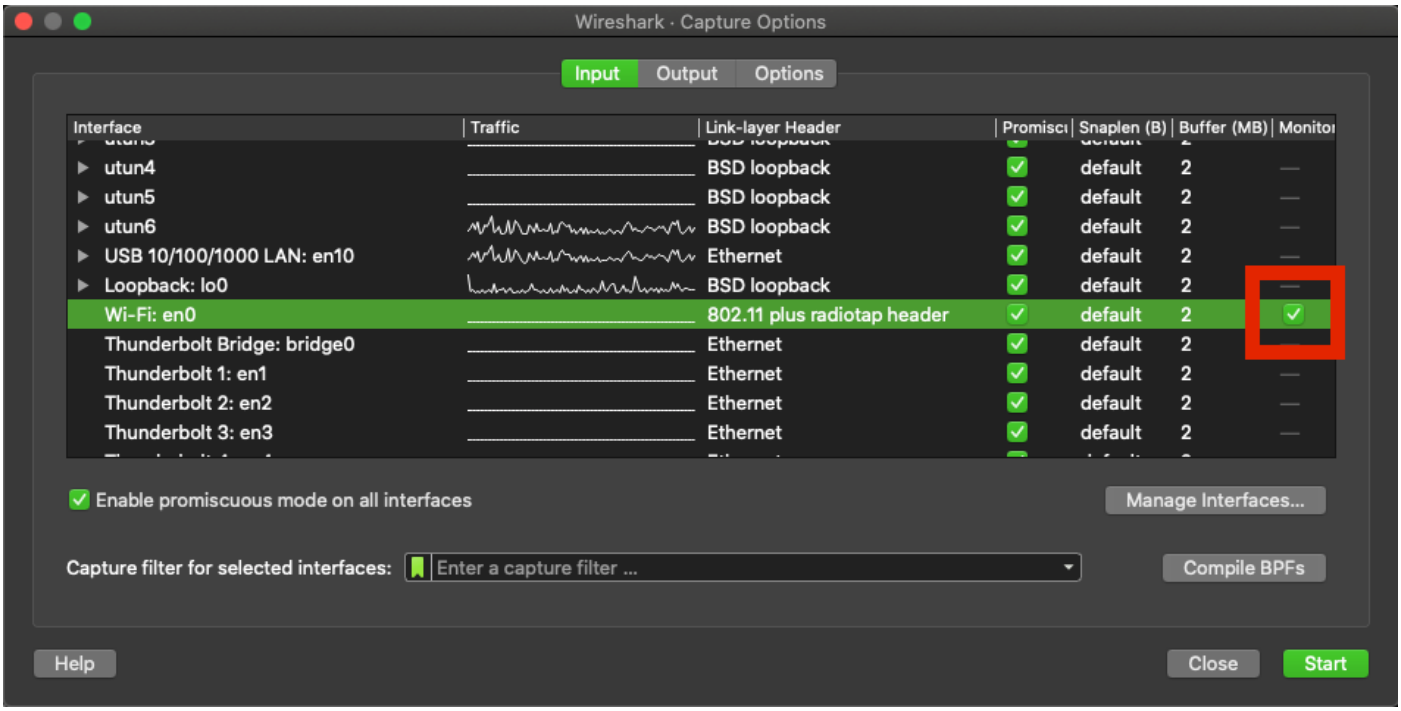
步骤3.从菜单栏中选择“捕获”菜单，然后选择“选项”，如图所示。



此操作将打开一个弹出窗口，如图所示。



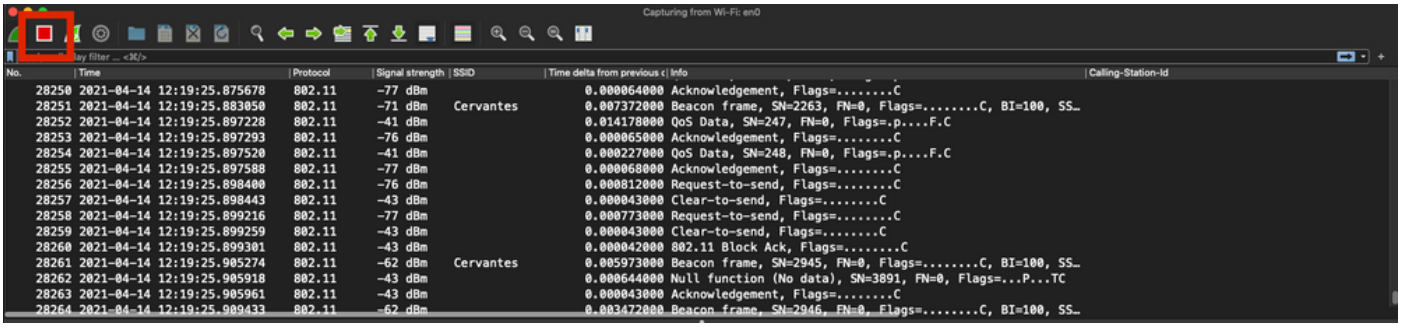
步骤4.选择**Wi-Fi:en0**（无线适配器），并勾选接口右侧的“Monitor（监控）”选项，如图所示。



注意：在此方法中，Wireshark无法选择要扫描的所需通道和宽度。“通道”和“宽度”是使用本文档中介绍的嗅探器工具分配的。请参阅选项A。步骤3以更改它们。

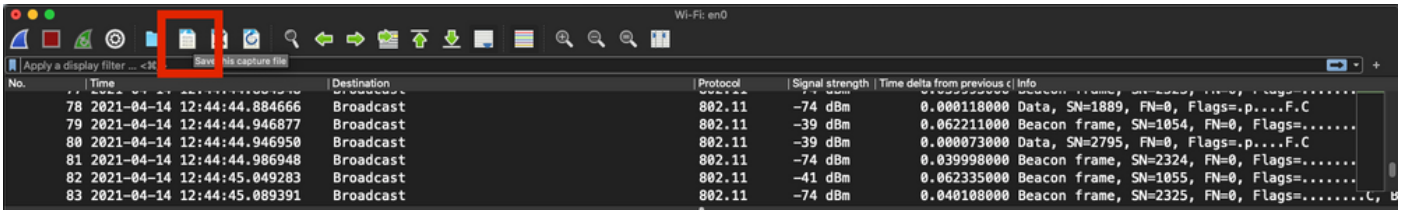
步骤5.选择“**开始”。**

步骤6.等待一段时间收集所需信息，然后从Wireshark中选择“停止”按钮，如图所示。

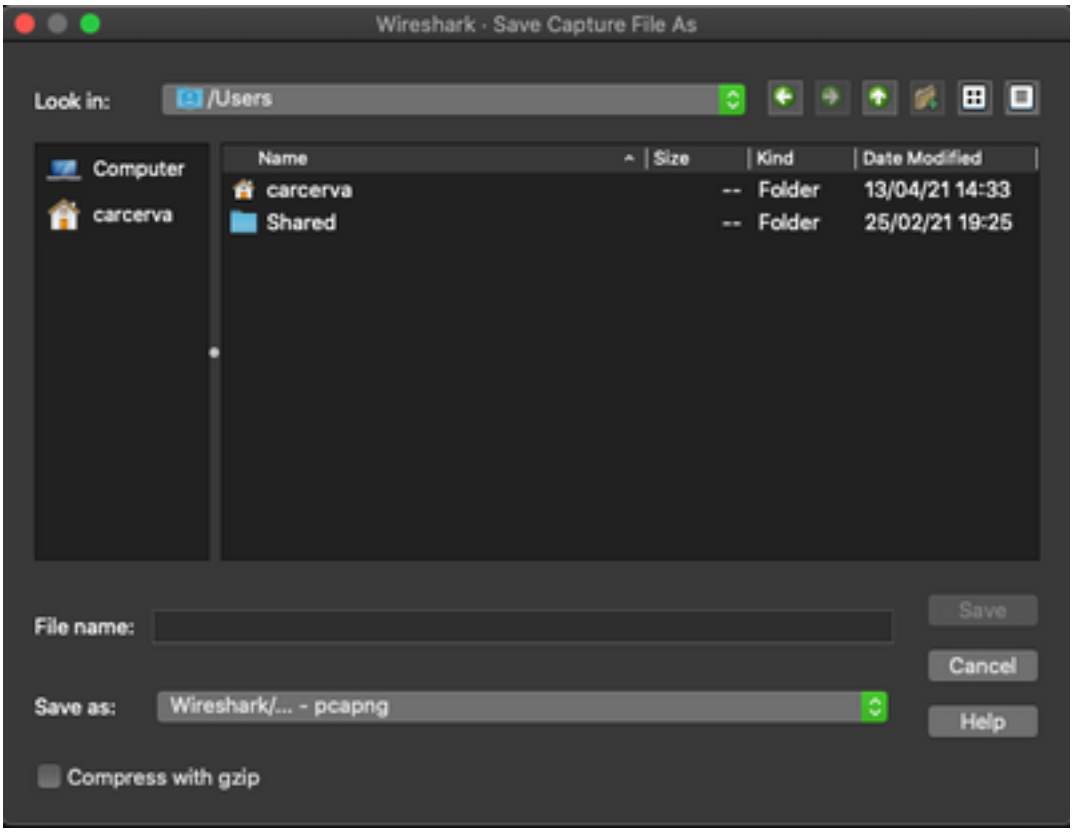


提示：如果WLAN使用加密(如预共享密钥(PSK))，请确保捕获捕获AP与所需客户端之间的四次握手。如果OTA PCAP在设备与WLAN关联之前启动，或者如果客户端在捕获运行期间取消身份验证并重新进行身份验证，则可以执行此操作。

步骤7.保存PCAP文件。单击Wireshark中**的Save**按钮，如图所示。



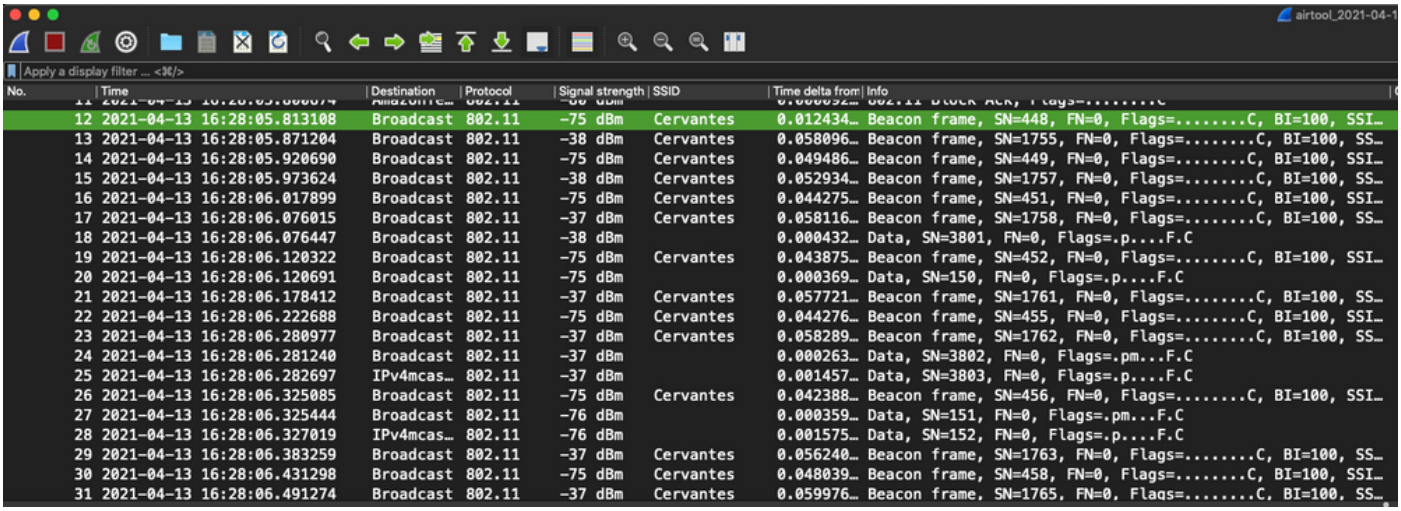
选择目标文件夹，如图所示。



验证

使用本部分可确认配置能否正常运行。

使用Wireshark打开捕获并验证802.11帧是否可见，如图所示。



故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 802.11无线嗅探的基础
- 技术支持和文档 - Cisco Systems