

在MacBook上收集無線資料包捕獲

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[選項A：使用無線診斷配置PCAP](#)

[選項B：使用Airtool配置PCAP](#)

[選項C.使用Wireshark配置PCAP](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何在MacBook上使用本機工具Wireless Diagnostics和第三方應用程式（例如Airtool和Wireshark）收集無線資料包捕獲(PCAP)，以便進行故障排除和分析。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco無線LAN控制器(WLC)AireOS或Cisco IOS®-XE
- 802.11標準中的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Apple MacBook，帶macOS版本10.14.X或更高版本
- Apple無線診斷工具
- Airtool 1.9或更高版本
- Wireshark 3.X或更高版本
- 思科存取點(AP)2802

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

需要考慮的事項：

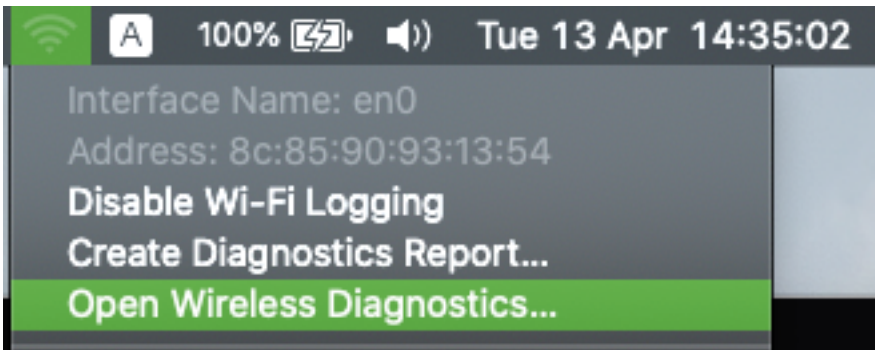
- 建議將Macbook用作無線嗅探器以靠近AP和目標裝置。
- 確保您知道哪個802.11通道和寬度、客戶端裝置和AP使用。
- 可以在以下位置找到通道和寬度：Cisco IOS®-XE Web圖形使用者介面(GUI)在**Configuration > Wireless > 5GHz or 2.4GHz > Select an AP > Channel and Width**AireOS Web GUI(在**Wireless > Access Points > 802.11a/n/ac(5GHz)或802.11 b/g/n(2.4GHz)**>選擇一個AP >通道和寬度

設定

選項A：使用無線診斷配置PCAP

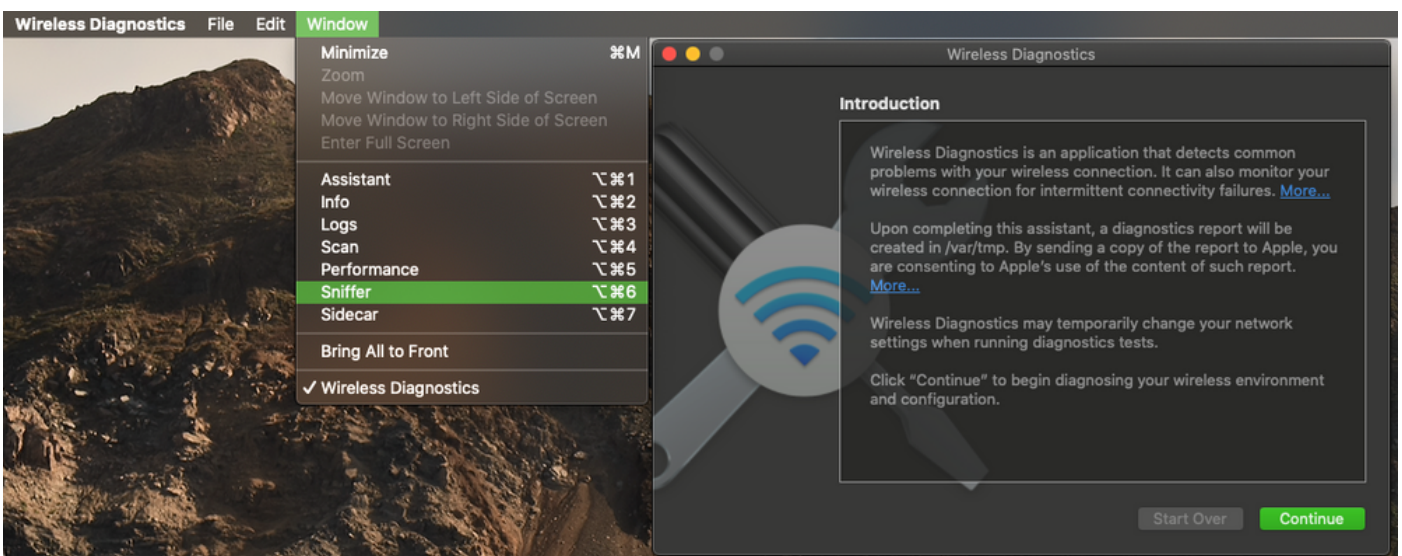
步驟1.啟動Wireless Diagnostics Tool。

按住鍵盤上的ALT/Option鍵，然後按一下右上角的Wi-Fi圖示，如下圖所示。



步驟2.開啟監聽器工具。

從選單欄上的「Wireless Diagnostic Tool (無線診斷工具)」中選擇「Window」選單，然後選擇「Sniffer」或使用鍵盤快捷鍵，同時按ALT + Command + 6 鍵，如下圖所示。

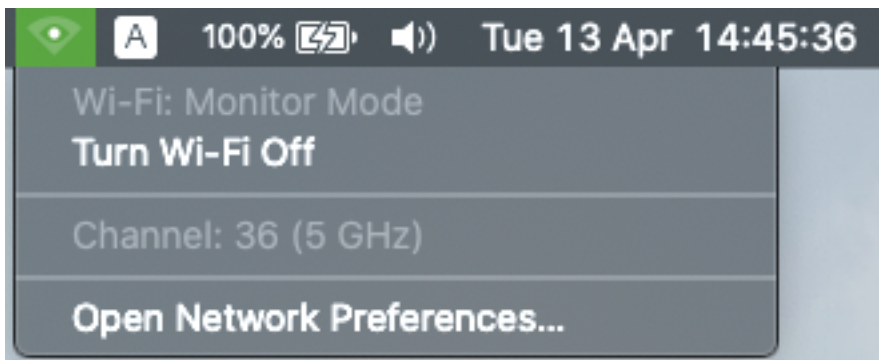


步驟3.選擇目標裝置和AP使用的Channel和Width，如下圖所示。



步驟4.按一下「Start」。

此操作將無線介面卡置於監控模式，它不能用於將裝置連線到無線LAN(WLAN)，如下圖所示。



步驟5.等待一段時間以收集所需的資訊，然後按一下停止。

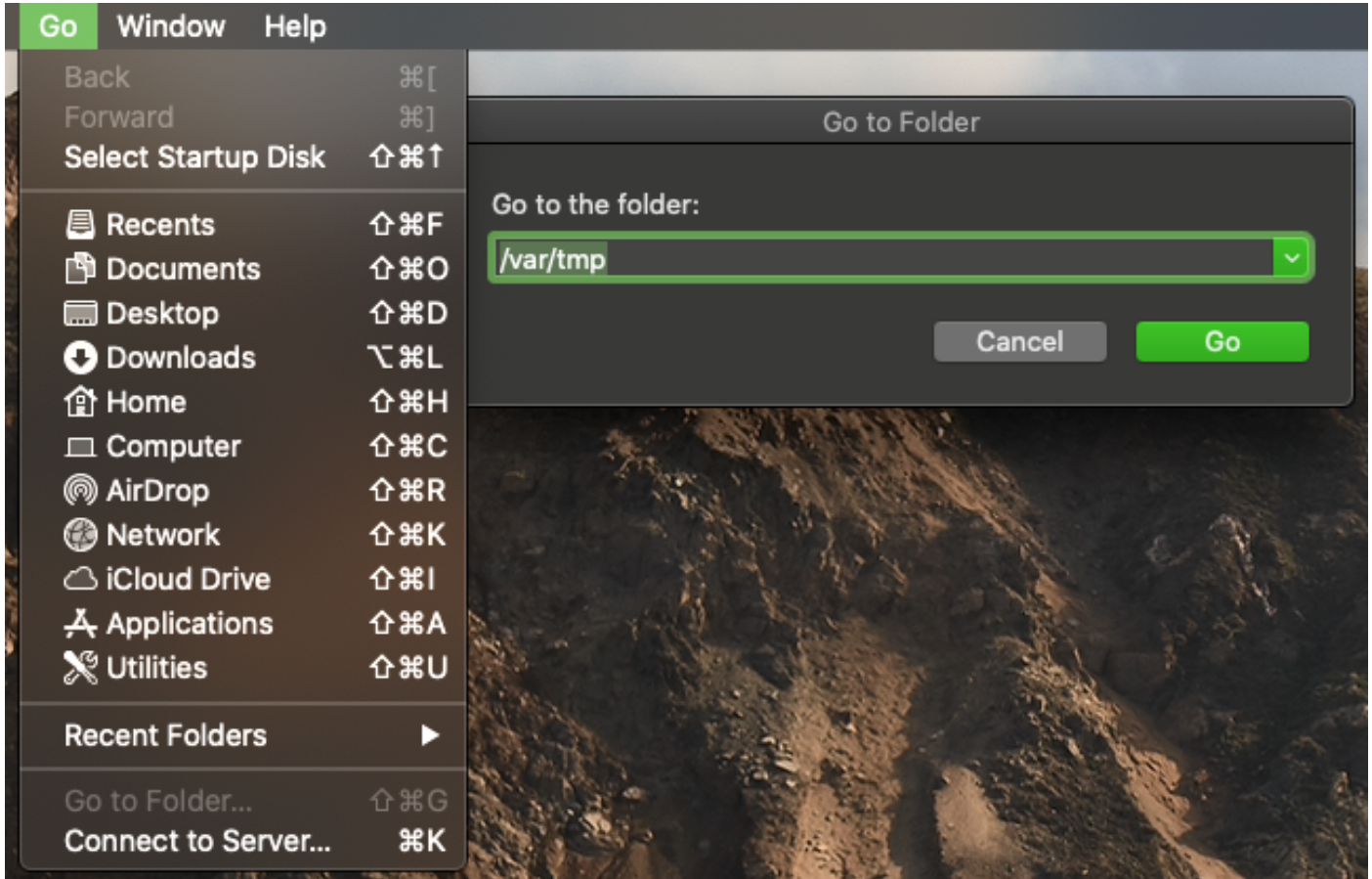


提示：如果WLAN使用加密(例如預共用金鑰(PSK))，請確保擷取會擷取AP和所需使用者端之間的四次握手。如果OTA PCAP在裝置與WLAN關聯之前啟動，或者如果客戶端在捕獲運行時

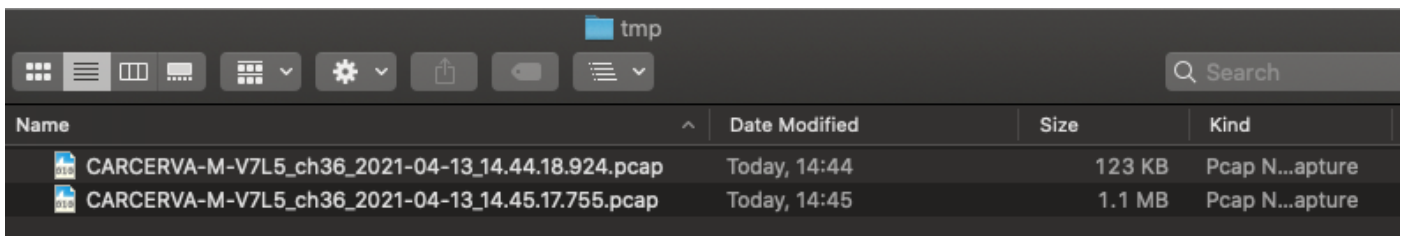
被取消身份驗證並重新身份驗證，則可以完成此操作。

步驟6.檔案位於Desktop資料夾或路徑/var/tmp/（可能因MacBook運行的macOS版本而異）。

- 1.在MacBook上啟動Finder應用程式，如下圖所示。
- 2.從Finder中選擇「轉到」選單。
- 3.選擇Desktop Folder或Go to Folder，然後鍵入目標路徑。



將顯示目標資料夾。

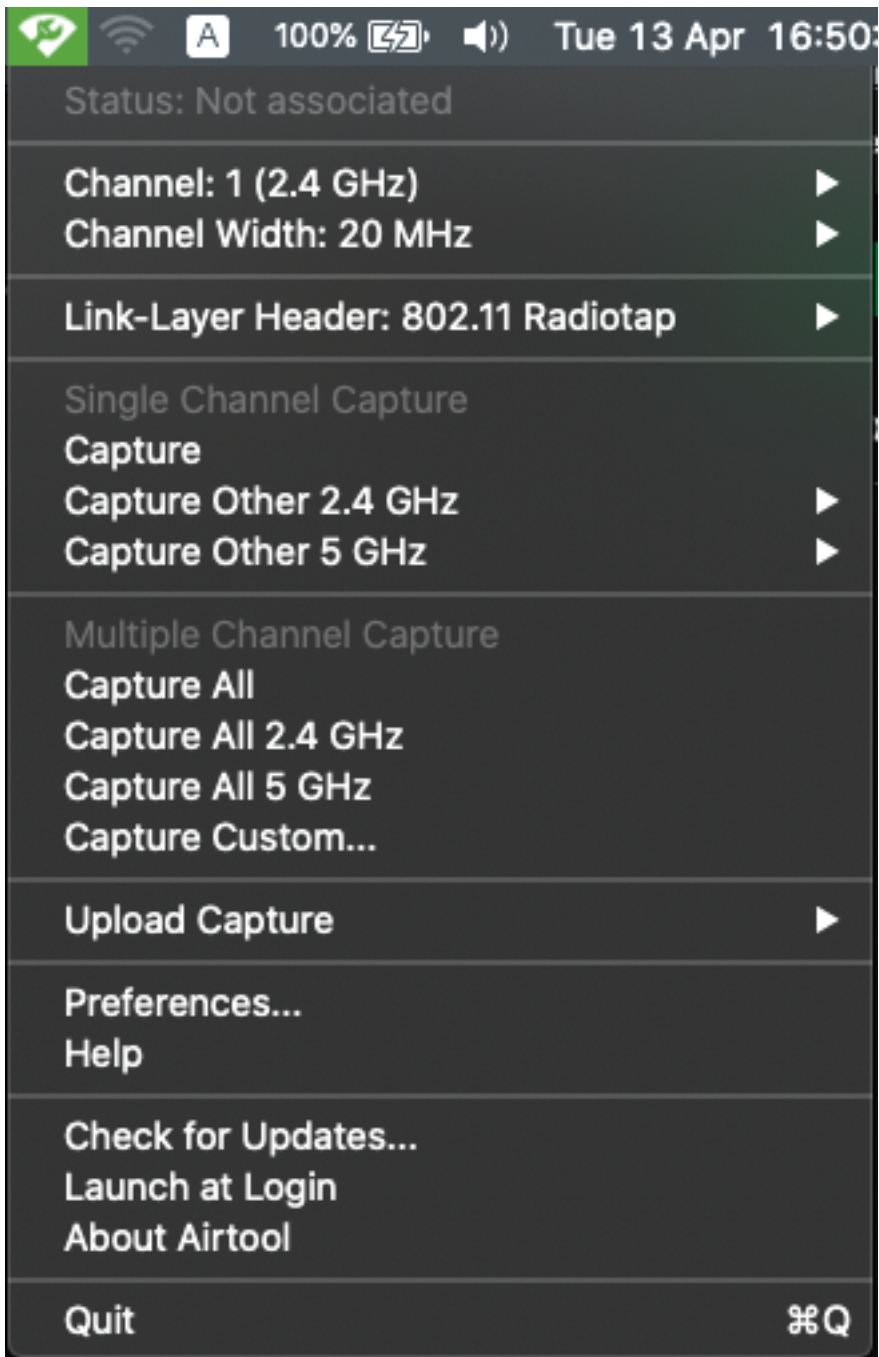


選項B：使用Airtool配置PCAP

步驟1.安裝第三方Airtool[應用](#)程式。

步驟2.啟動工具。

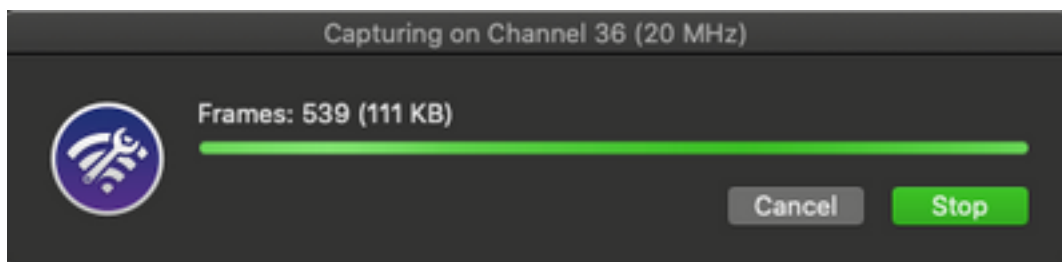
啟動後，Airtool可在macOS選單欄中位於右上角，如下圖所示。



步驟3.選擇目標裝置和AP使用的Channel和Width（此操作將啟動PCAP），如下圖所示。



步驟4.等待一段時間以收集所需的資訊，然後按一下「Stop」，如下圖所示。



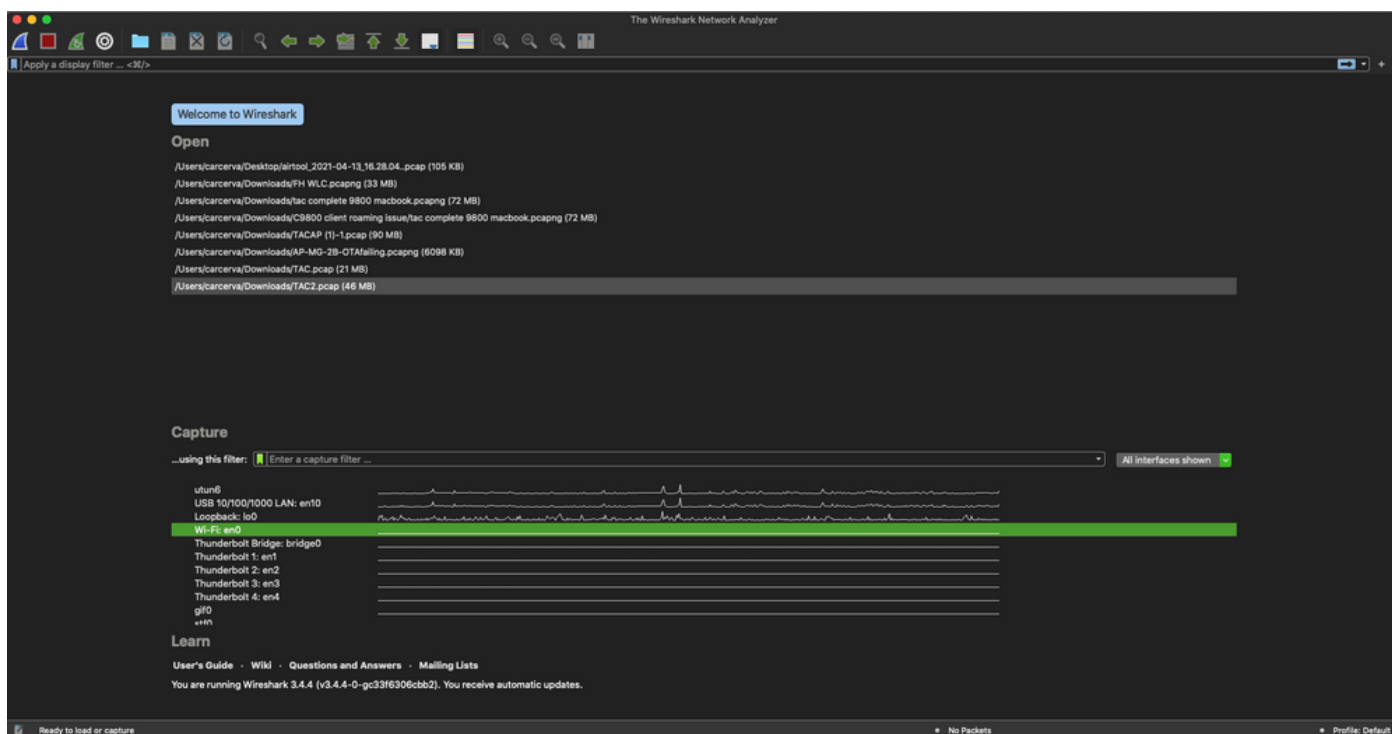
提示：如果WLAN使用加密(例如預共用金鑰(PSK))，請確保擷取會擷取AP和所需使用者端之間的四次握手。如果OTA PCAP在裝置與WLAN關聯之前啟動，或者如果客戶端在捕獲運行時被取消身份驗證並重新身份驗證，則可以完成此操作。

步驟5.檔案位於Desktop資料夾中。

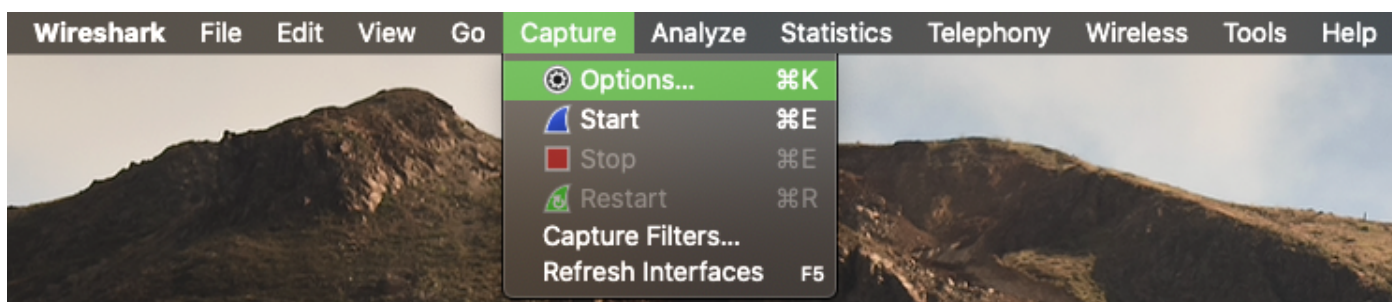
選項C.使用Wireshark配置PCAP

步驟1.安裝[Wireshark](#)。

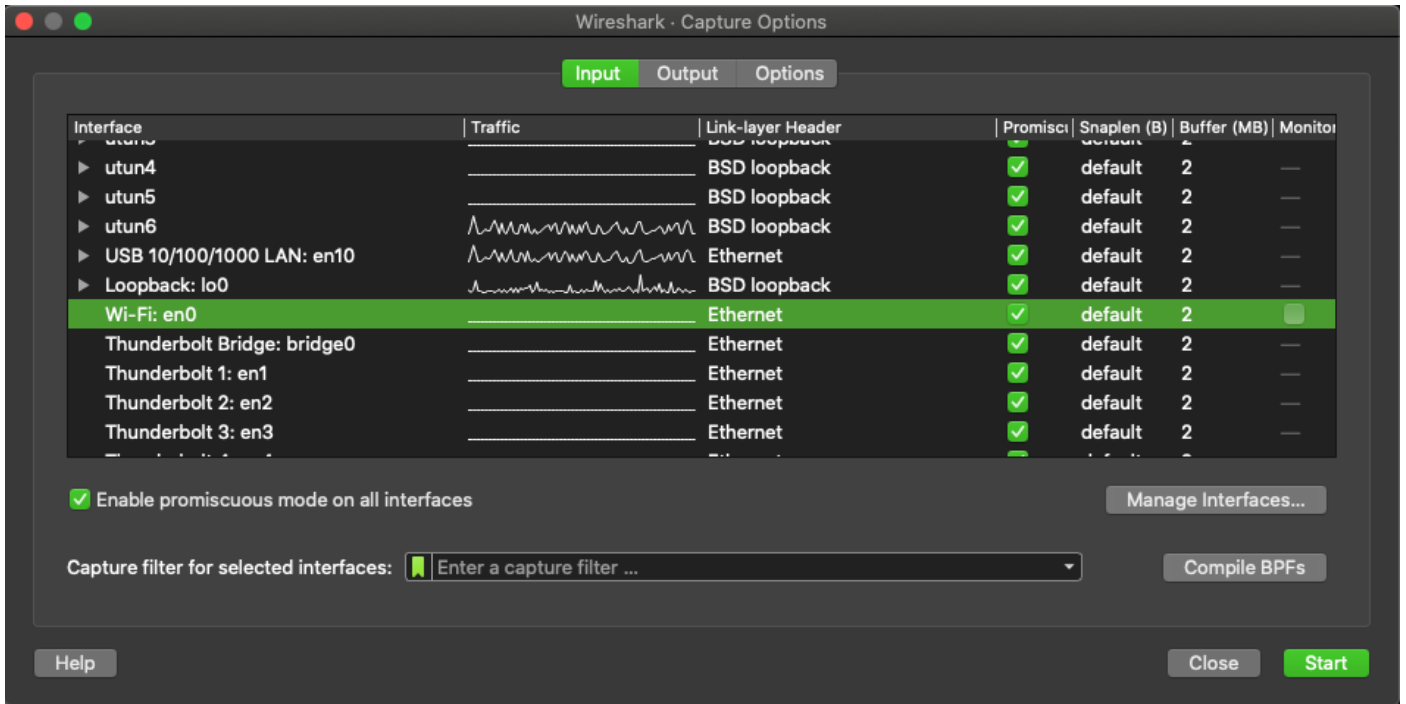
步驟2.啟動應用程式，如下圖所示。



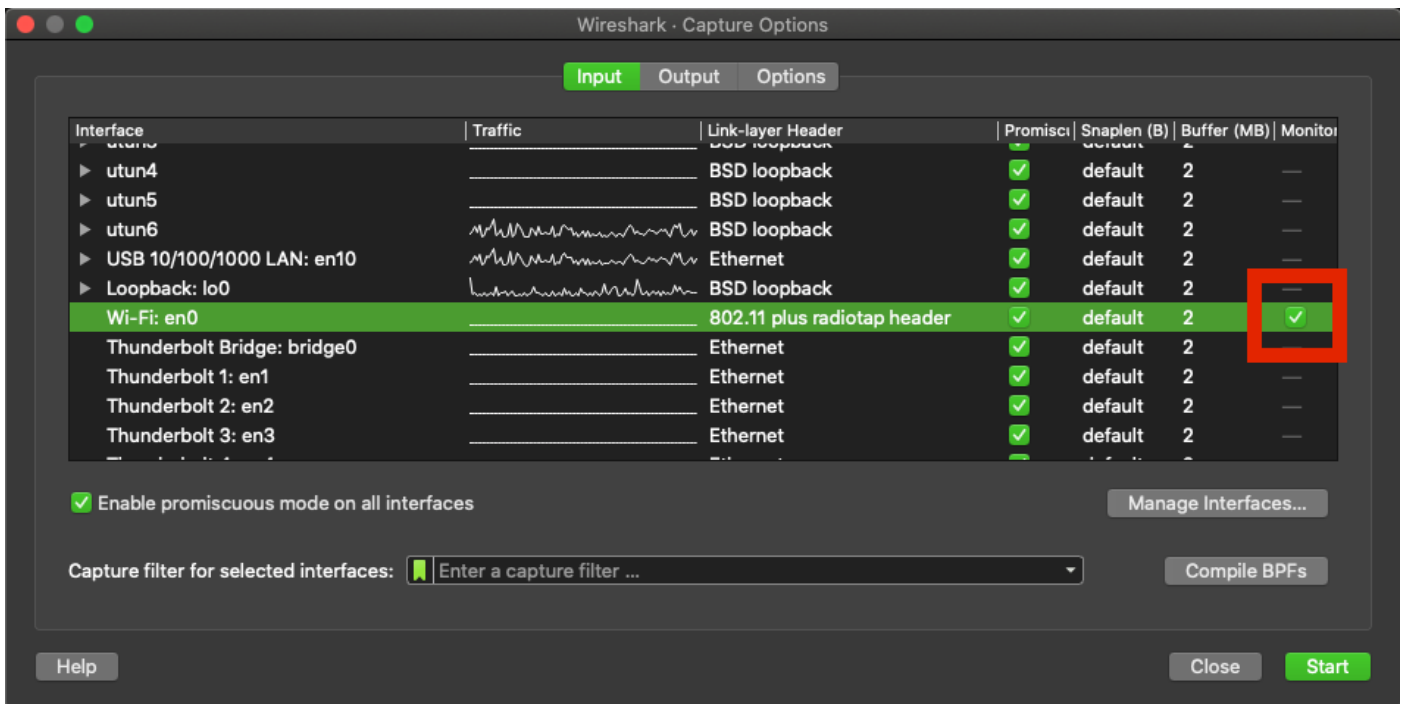
步驟3.從選單欄中選擇Capture選單，然後選擇Options，如下圖所示。



此操作將開啟一個彈出視窗，如下圖所示。



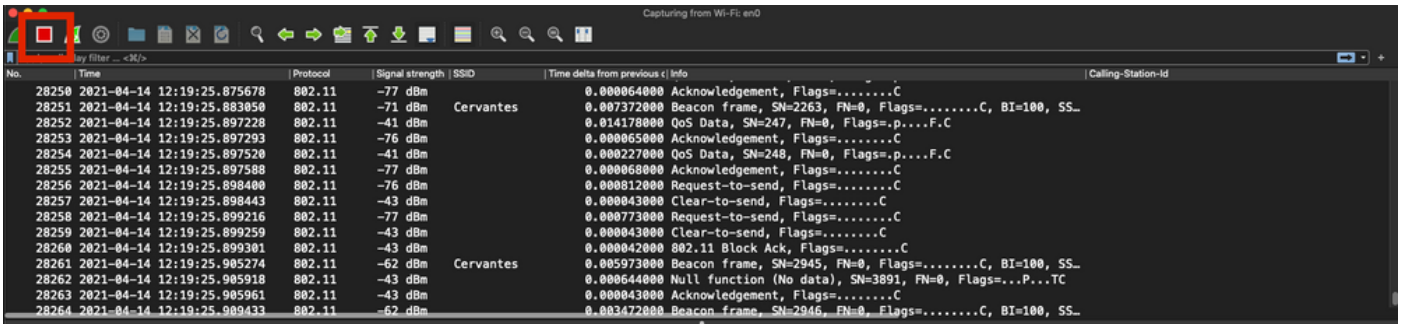
步驟4.選擇Wi-Fi:en0(無線介面卡)並勾選介面右側的Monitor選項，如下圖所示。



附註：在此方法中，Wireshark無法選擇要掃描的所需通道和寬度。通道和寬度是用監聽器工具指定的，如本文檔所述。請參閱選項A。步驟3以變更它們。

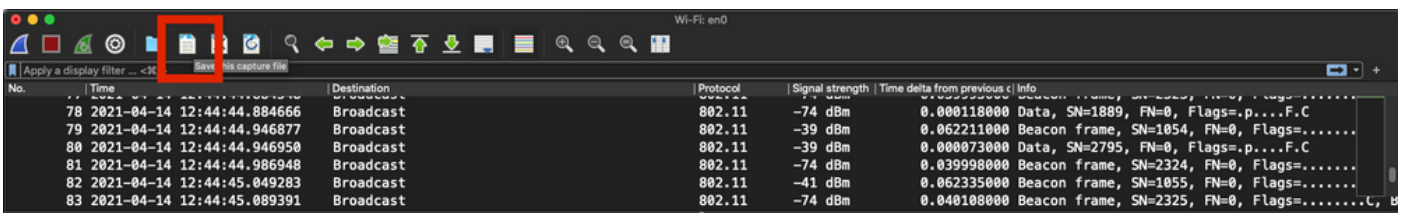
步驟5.選擇開始。

步驟6.等待一段時間以收集所需的資訊，然後從Wireshark中選擇Stop按鈕，如下圖所示。

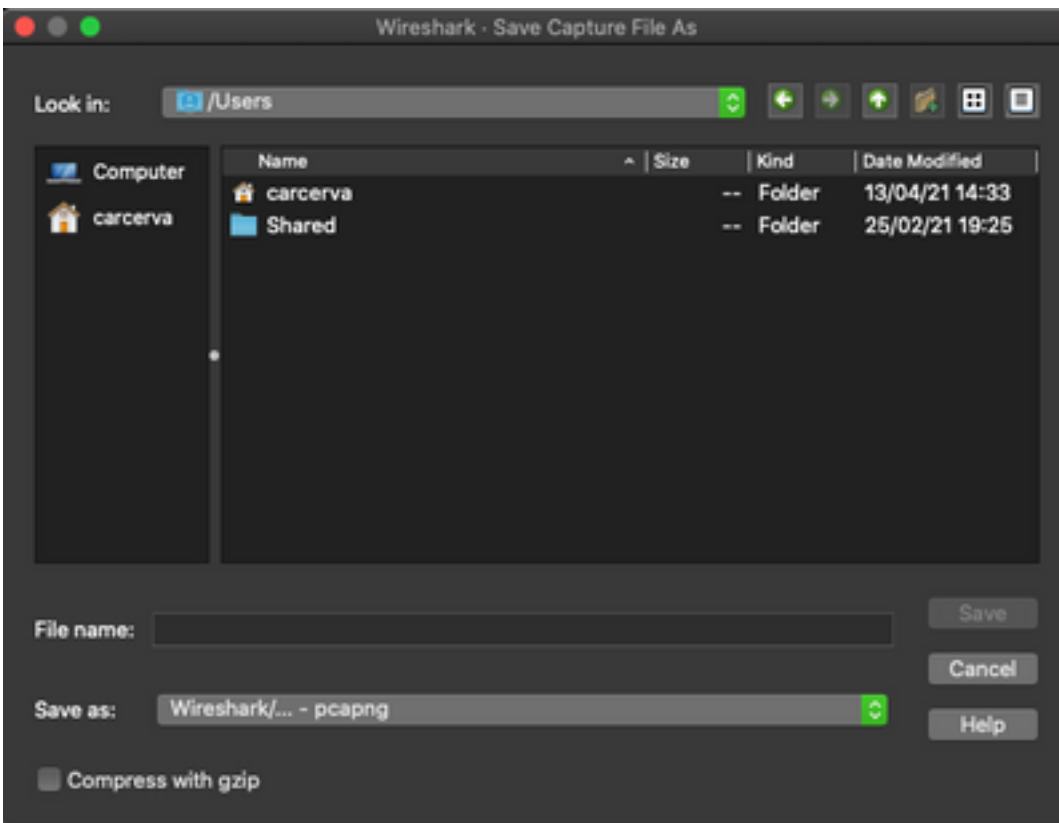


提示：如果WLAN使用加密(例如預共用金鑰(PSK))，請確保擷取會擷取AP和所需使用者端之間的四次握手。如果OTA PCAP在裝置與WLAN關聯之前啟動，或者如果客戶端在捕獲運行時被取消身份驗證並重新身份驗證，則可以完成此操作。

步驟7.儲存PCAP檔案。在Wireshark中按一下**Save**按鈕，如下圖所示。



選擇目標資料夾，如下圖所示。



驗證

使用本節內容，確認您的組態是否正常運作。

使用Wireshark開啟捕獲並驗證802.11幀是否可見，如圖所示。

No.	Time	Destination	Protocol	Signal strength	SSID	Time delta from	Info
12	2021-04-13 16:28:05.813108	Broadcast	802.11	-75 dBm	Cervantes	0.012434...	Beacon frame, SN=448, FN=0, Flags=.....C, BI=100, SSI...
13	2021-04-13 16:28:05.871204	Broadcast	802.11	-38 dBm	Cervantes	0.058096...	Beacon frame, SN=1755, FN=0, Flags=.....C, BI=100, SS...
14	2021-04-13 16:28:05.920690	Broadcast	802.11	-75 dBm	Cervantes	0.049486...	Beacon frame, SN=449, FN=0, Flags=.....C, BI=100, SSI...
15	2021-04-13 16:28:05.973624	Broadcast	802.11	-38 dBm	Cervantes	0.052934...	Beacon frame, SN=1757, FN=0, Flags=.....C, BI=100, SS...
16	2021-04-13 16:28:06.017899	Broadcast	802.11	-75 dBm	Cervantes	0.044275...	Beacon frame, SN=451, FN=0, Flags=.....C, BI=100, SSI...
17	2021-04-13 16:28:06.076015	Broadcast	802.11	-37 dBm	Cervantes	0.058116...	Beacon frame, SN=1758, FN=0, Flags=.....C, BI=100, SS...
18	2021-04-13 16:28:06.076447	Broadcast	802.11	-38 dBm	Cervantes	0.000432...	Data, SN=3801, FN=0, Flags=.p...F.C
19	2021-04-13 16:28:06.120322	Broadcast	802.11	-75 dBm	Cervantes	0.043875...	Beacon frame, SN=452, FN=0, Flags=.....C, BI=100, SSI...
20	2021-04-13 16:28:06.120691	Broadcast	802.11	-75 dBm	Cervantes	0.000369...	Data, SN=150, FN=0, Flags=.p...F.C
21	2021-04-13 16:28:06.178412	Broadcast	802.11	-37 dBm	Cervantes	0.057721...	Beacon frame, SN=1761, FN=0, Flags=.....C, BI=100, SS...
22	2021-04-13 16:28:06.222688	Broadcast	802.11	-75 dBm	Cervantes	0.044276...	Beacon frame, SN=455, FN=0, Flags=.....C, BI=100, SSI...
23	2021-04-13 16:28:06.280977	Broadcast	802.11	-37 dBm	Cervantes	0.058289...	Beacon frame, SN=1762, FN=0, Flags=.....C, BI=100, SS...
24	2021-04-13 16:28:06.281240	Broadcast	802.11	-37 dBm	Cervantes	0.000263...	Data, SN=3802, FN=0, Flags=.pm...F.C
25	2021-04-13 16:28:06.282697	IPv4mcas...	802.11	-37 dBm	Cervantes	0.001457...	Data, SN=3803, FN=0, Flags=.p...F.C
26	2021-04-13 16:28:06.325085	Broadcast	802.11	-75 dBm	Cervantes	0.042388...	Beacon frame, SN=456, FN=0, Flags=.....C, BI=100, SSI...
27	2021-04-13 16:28:06.325444	Broadcast	802.11	-76 dBm	Cervantes	0.000359...	Data, SN=151, FN=0, Flags=.pm...F.C
28	2021-04-13 16:28:06.327019	IPv4mcas...	802.11	-76 dBm	Cervantes	0.001575...	Data, SN=152, FN=0, Flags=.p...F.C
29	2021-04-13 16:28:06.383259	Broadcast	802.11	-37 dBm	Cervantes	0.056240...	Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SS...
30	2021-04-13 16:28:06.431298	Broadcast	802.11	-75 dBm	Cervantes	0.048039...	Beacon frame, SN=458, FN=0, Flags=.....C, BI=100, SSI...
31	2021-04-13 16:28:06.491274	Broadcast	802.11	-37 dBm	Cervantes	0.059976...	Beacon frame, SN=1765, FN=0, Flaqs=.....C, BI=100, SS...

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [802.11 無線監聽的基礎知識](#)
- [技術支援與文件 - Cisco Systems](#)