

# MacBookでの空中でのパケットキャプチャの収集

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[選択肢A.ワイヤレス診断を使用したPCAPの設定](#)

[選択肢B. AirtoolでPCAPを設定する](#)

[選択肢C. WiresharkでPCAPを設定する](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、ワイヤレスビヘイビアのトラブルシューティングと分析のために、ネイティブツールのワイヤレス診断とMacBookのAirtoolやWiresharkなどのサードパーティアプリケーションを使用して、Packet Captures(PCAP)Over the Air(OTA)を収集する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Wireless LAN Controller(WLC)AireOSまたはCisco IOS®-XE
- 802.11規格の基礎知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- MacOSバージョン10.14.X以降を搭載したApple MacBook
- Apple Wireless Diagnosticsツール
- Airtool 1.9以降
- Wireshark 3.X以降
- Cisco Access Point(AP)2802

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

考慮すべき事柄:

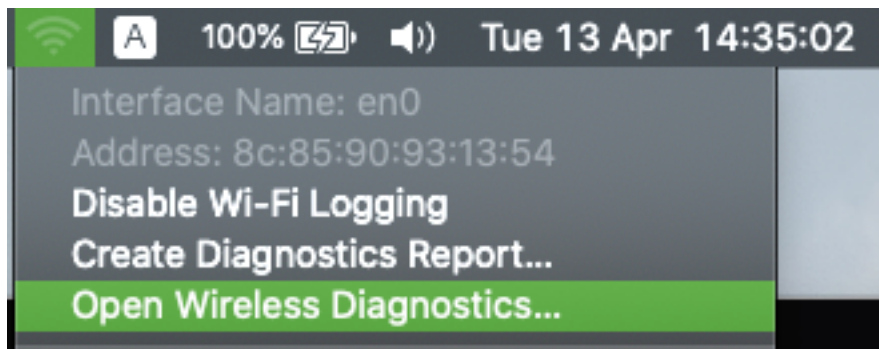
- ワイヤレススニファとして動作するMacbookをAPとターゲットデバイスの近くに配置することを推奨します。
- 使用する802.11チャンネルと幅、クライアントデバイス、およびAPを確認します。
- チャンネルと幅は次の場所にあります。Cisco IOS®-XE Web Graphical User Interface(GUI)の [Configuration] > [Wireless] > [5GHz or 2.4GHz] > [Select an AP] > [Channel and Width]の順に選択します。AireOS Web GUIの[Wireless] > [Access Points] > [802.11a/n/ac (5GHz)または [802.11 b/g/n (2.4GHz)] > [Select an AP] > [Channel and Width]

## 設定

### 選択肢A.ワイヤレス診断を使用したPCAPの設定

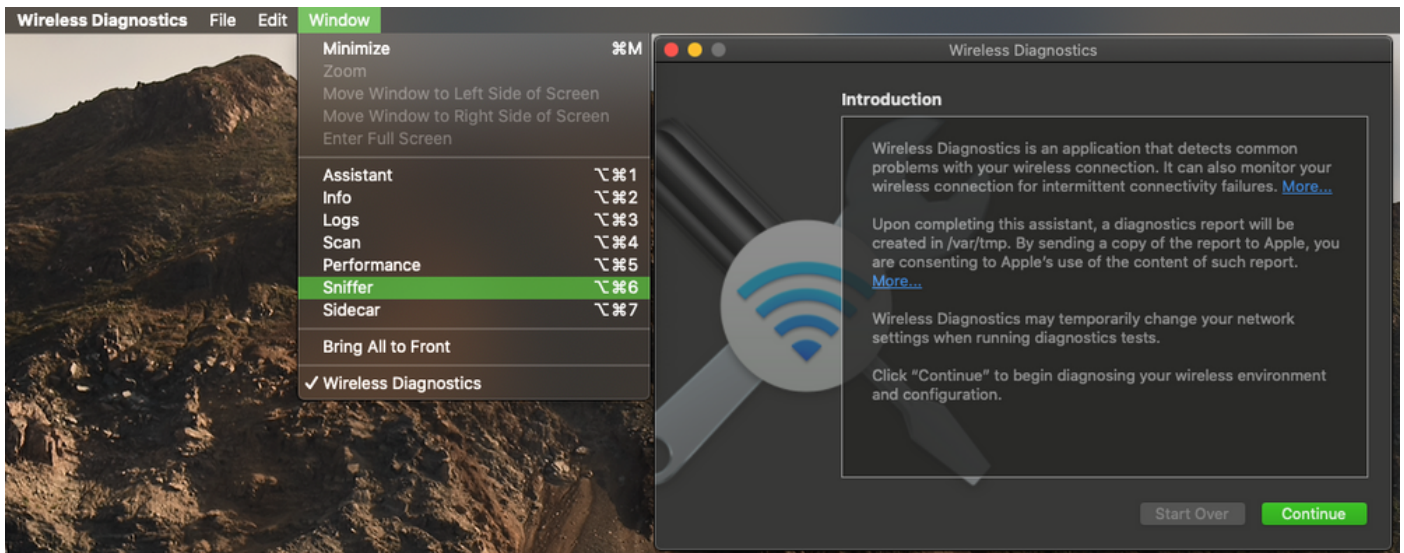
ステップ1：ワイヤレス診断ツールを起動します。

図に示すように、キーボードのAlt/Optionキーを押したまま、右上のWi-Fiアイコンをクリックします。



ステップ2：スニファツールを開きます。

Wireless Diagnostic ToolのメニューバーからWindowメニューを選択して、Snifferを選択するかまたはキーボードショートカットを使用して、Altキー+Commandキー+ 6キーを同時に押します（図を参照）。

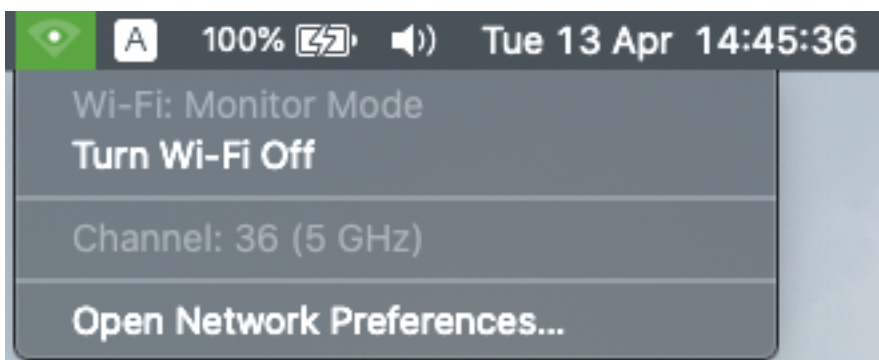


ステップ3：図に示すように、ターゲットデバイスとAPが使用するチャンネルと幅を選択します。



ステップ4:[Start]をクリックします。

この操作により、ワイヤレスアダプタがモニタモードになり、図に示すように、デバイスをワイヤレスLAN(WLAN)に接続するために使用することはできません。



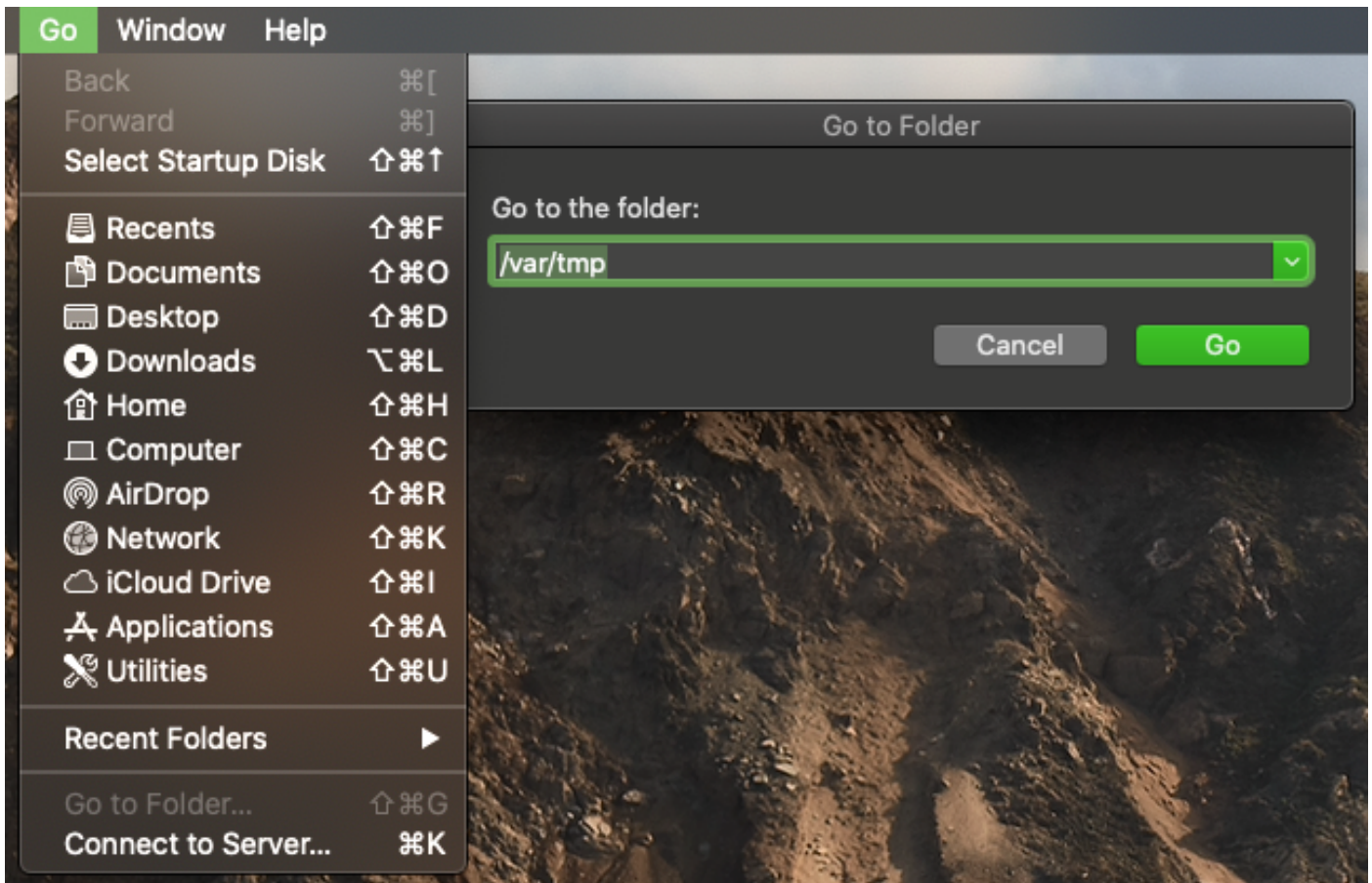
ステップ5：必要な情報を収集するまで待ち、[Stop]をクリックします。



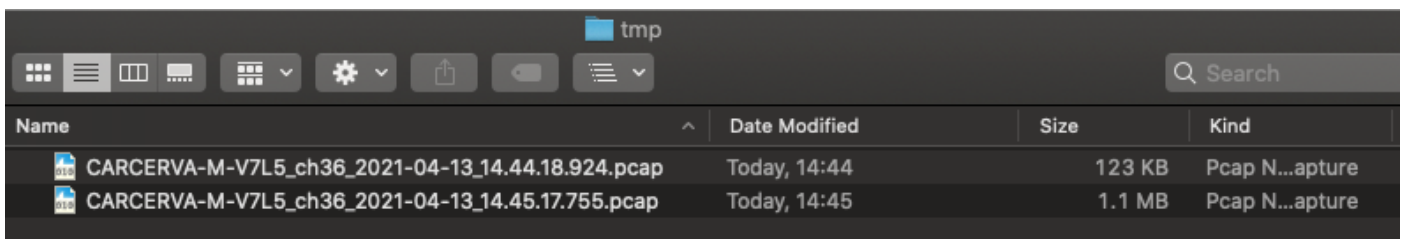
ヒント：WLANで事前共有キー(PSK)などの暗号化が使用されている場合は、APと目的のクライアント間の4ウェイハンドシェイクがキャプチャされることを確認します。これは、デバイスがWLANに関連付けられる前にOTA PCAPが起動する場合、またはキャプチャの実行中にクライアントの認証と再認証が解除された場合に実行できます。

ステップ6：ファイルはDesktopフォルダかパス/var/tmp/にあります(MacBookが実行しているmacOSのバージョンによって異なる場合があります)。

1. 図に示すように、MacBookでFinderアプリケーションを起動します。
2. Finderから[Go Menu]を選択します。
3. 「デスクトップフォルダ」または「フォルダに移動」を選択し、宛先パスを入力します。



宛先フォルダが表示されます。



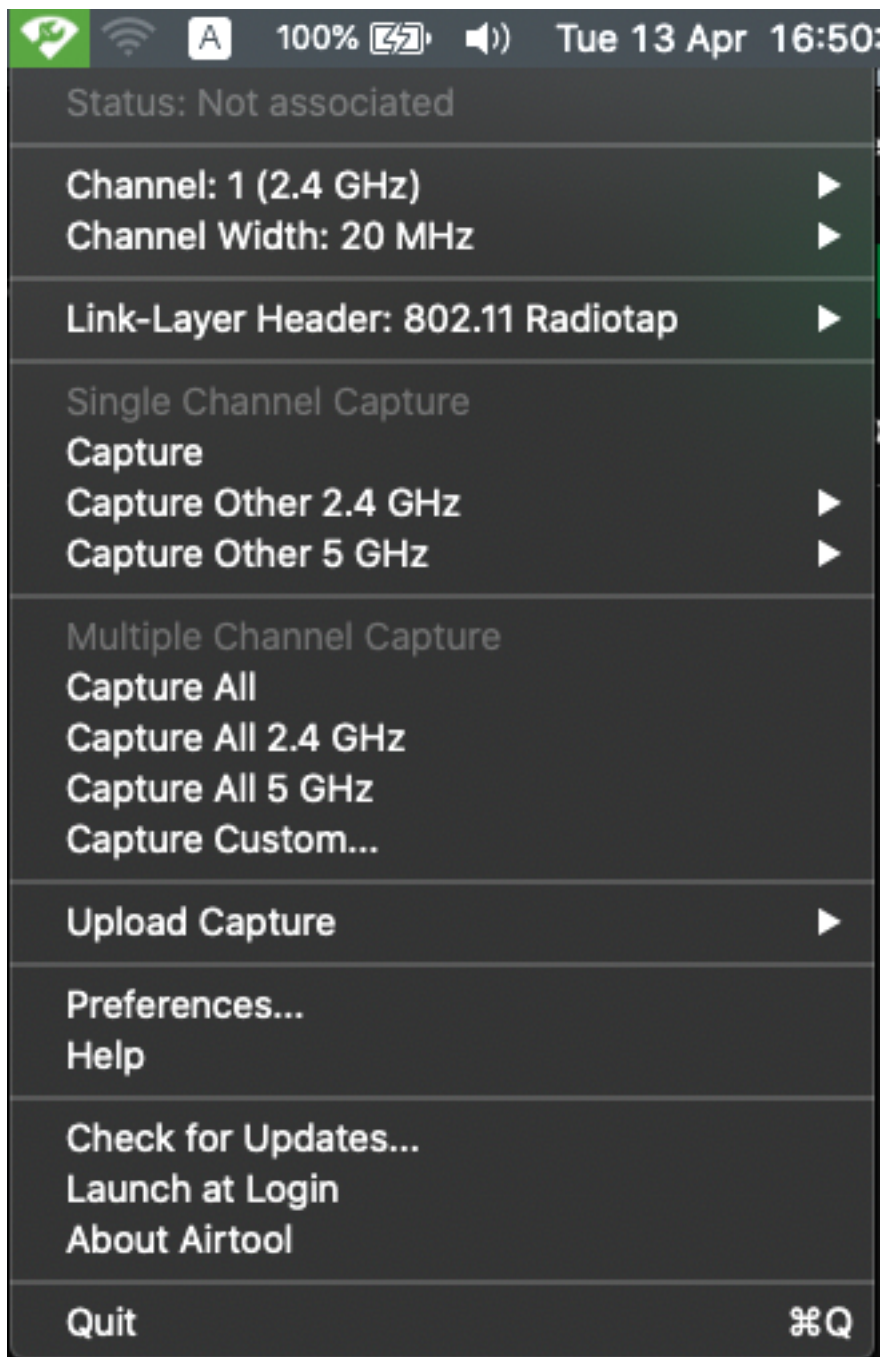
## 選択肢B. AirtoolでPCAPを設定する

ステップ1：サードパーティのAirtoolアプリケーションを[インストール](#)します。

ステップ2：ツールを起動します。

起動すると、図に示すように、AirtoolはmacOSメニューバーの右上に配置できます。

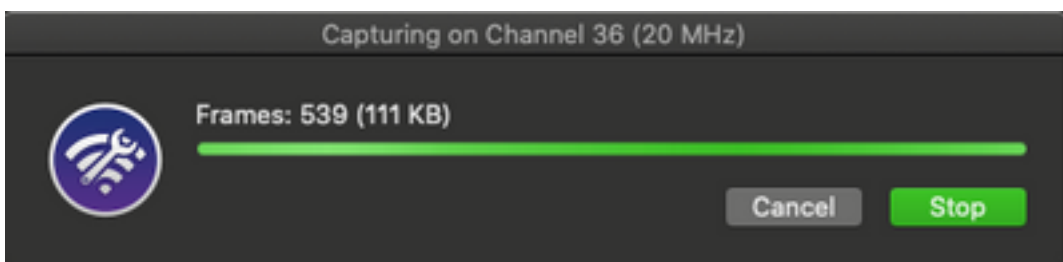




ステップ3 : 図に示すように、ターゲット・デバイスとAPが使用するチャンネルと幅 ( このアクションはPCAPを開始します ) を選択します。



ステップ4：必要な情報を収集するまで待ち、図に示すように[Stop]をクリックします。



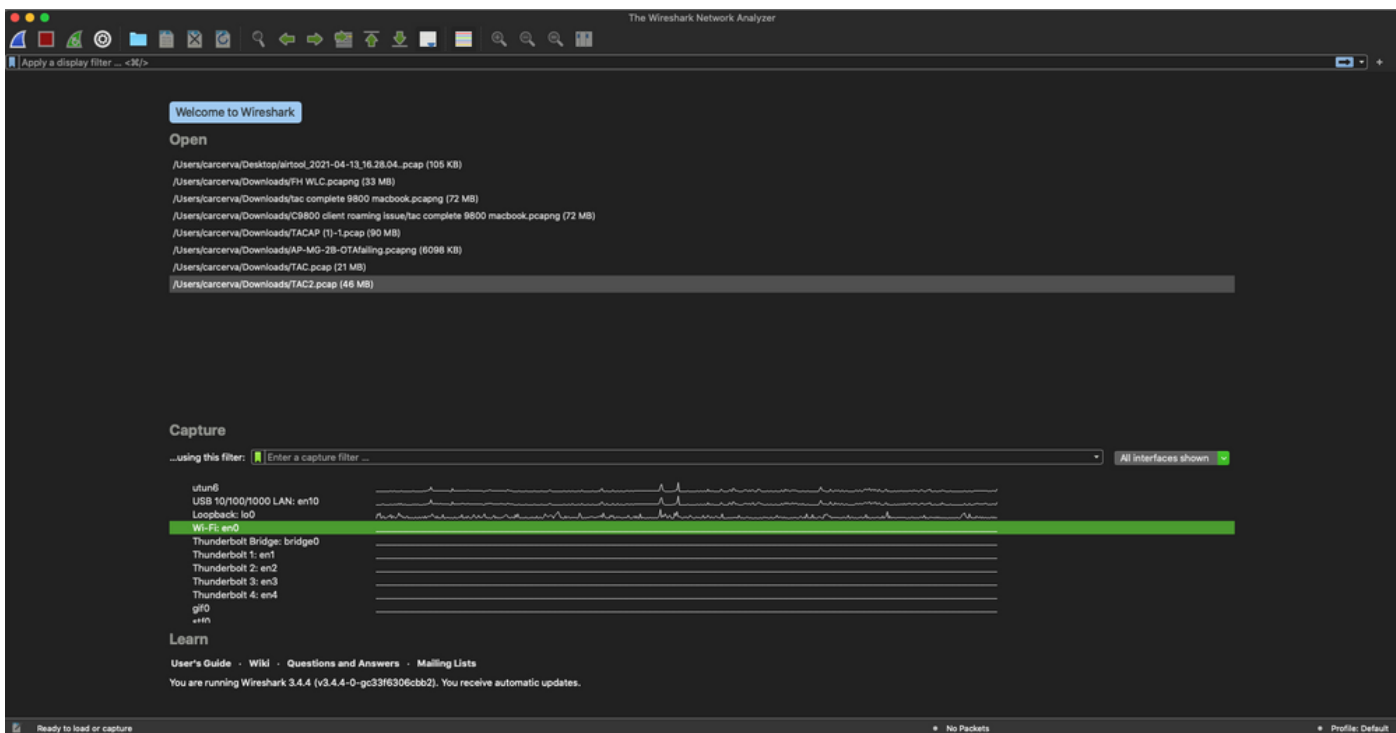
ヒント：WLANで事前共有キー(PSK)などの暗号化が使用されている場合は、APと目的のクライアント間の4ウェイハンドシェイクがキャプチャされることを確認します。これは、デバイスがWLANに関連付けられる前にOTA PCAPが起動する場合、またはキャプチャの実行中にクライアントの認証と再認証が解除された場合に実行できます。

ステップ5：ファイルはDesktopフォルダにあります。

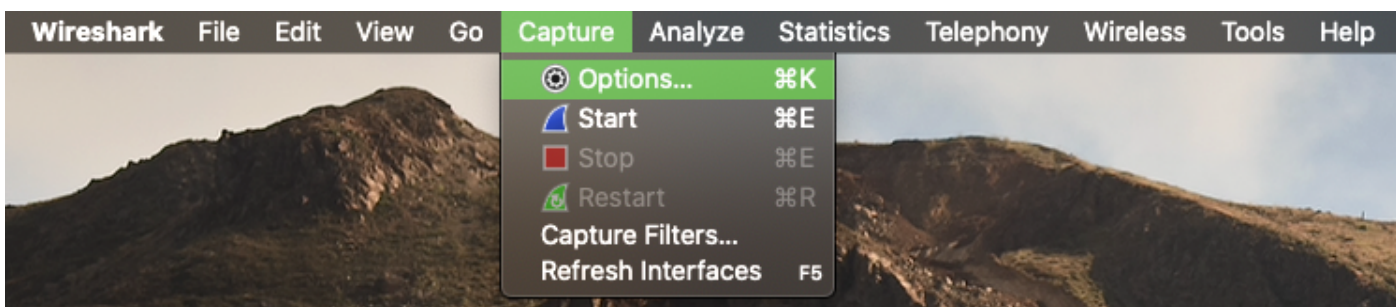
## 選択肢C. WiresharkでPCAPを設定する

ステップ1:Wiresharkをインストール[します。](#)

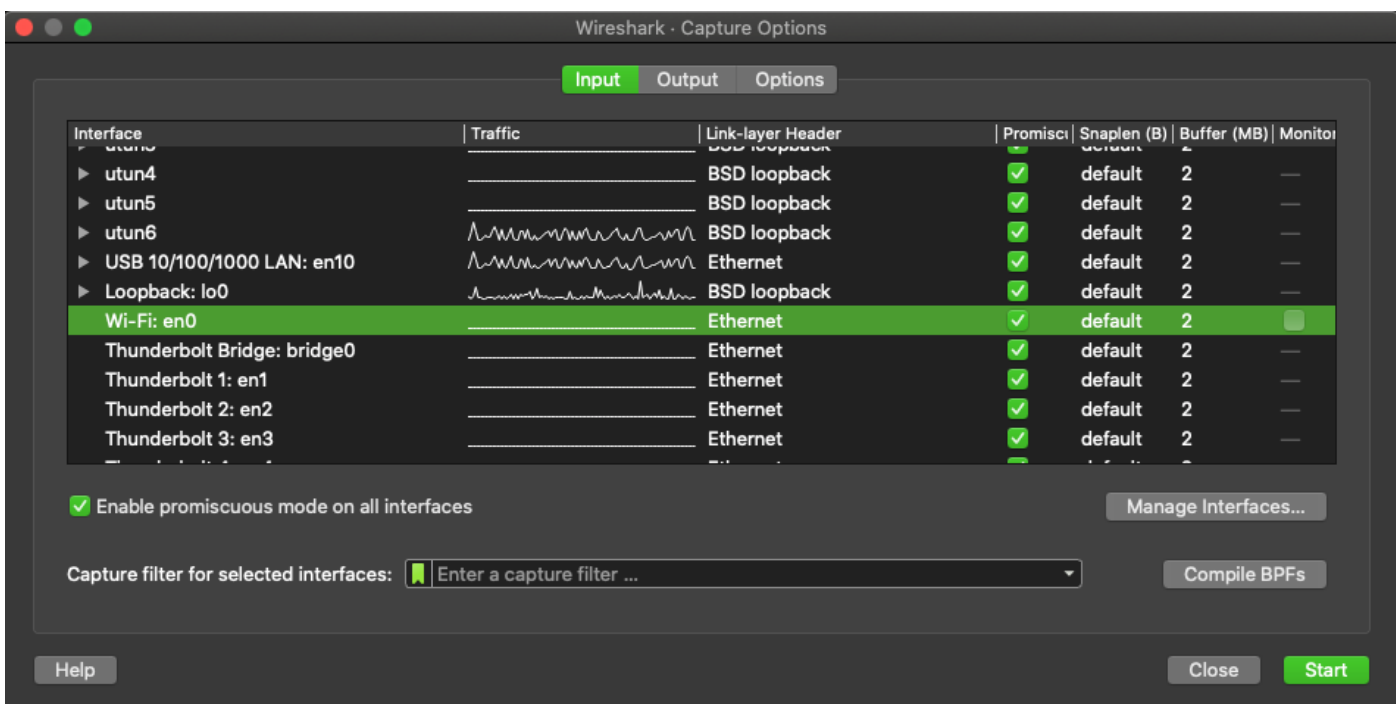
ステップ2：図に示すように、アプリケーションを起動します。



ステップ3 : 図に示すように、メニューバーから[Capture]メニューを選択し、[Options]を選択します。

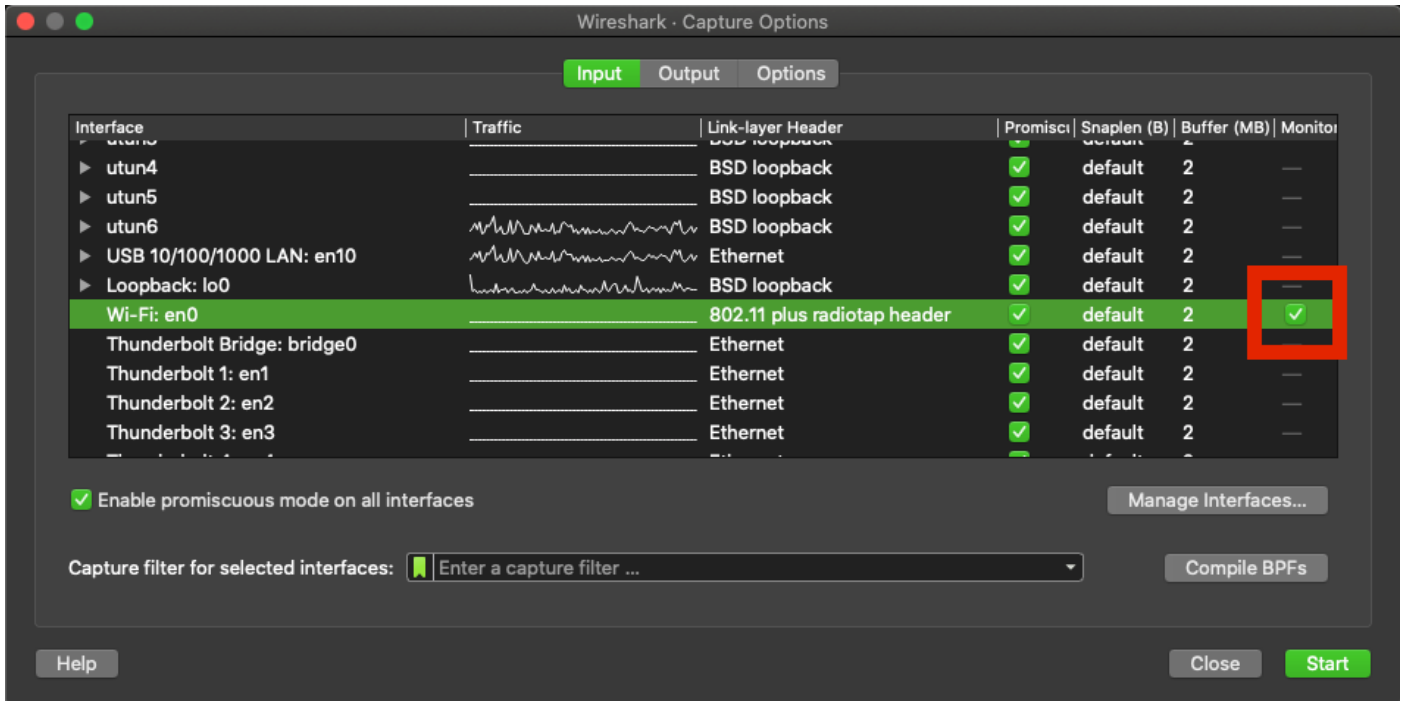


図に示すように、ポップアップウィンドウが開きます。





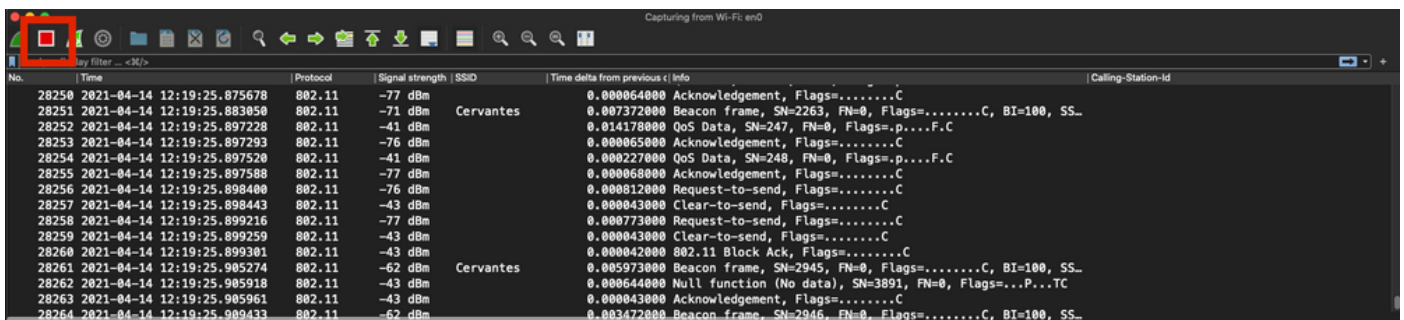
ステップ4:[Wi-Fi:en0(ワイヤレスアダプタ)]を選択し、図に示すように、インターフェースの右側にある[Monitor]オプションをオンにします。



注：この方法では、Wiresharkはスキャン対象のチャンネルと幅を選択できません。チャンネルと幅は、このドキュメントで説明するスニファツールで割り当てられます。変更するには、「オプションA：手順3」を参照してください。

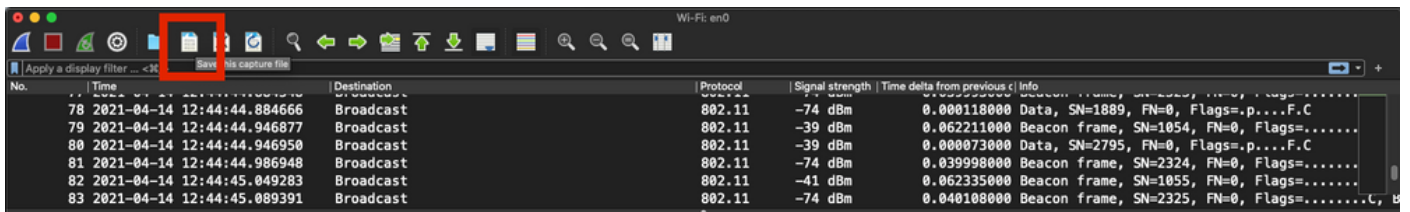
ステップ5：[Start] を選択します。

ステップ6：必要な情報を収集するまで待ち、図に示すように、Wiresharkから[Stop]ボタンを選択します。

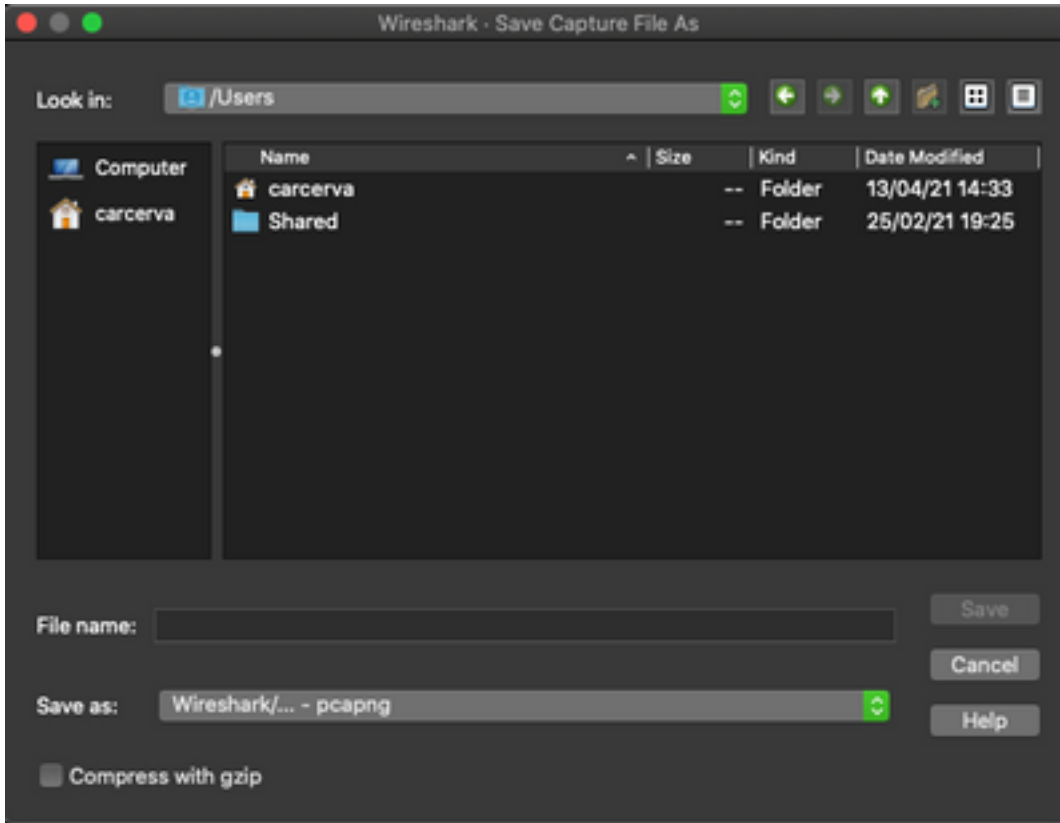


ヒント：WLANで事前共有キー(PSK)などの暗号化が使用されている場合は、APと目的のクライアント間の4ウェイハンドシェイクがキャプチャされることを確認します。これは、デバイスがWLANに関連付けられる前にOTA PCAPが起動する場合、またはキャプチャの実行中にクライアントの認証と再認証が解除された場合に実行できます。

ステップ7:PCAPファイルを保存します。図に示すように、Wiresharkから[Save]ボタンをクリックします。



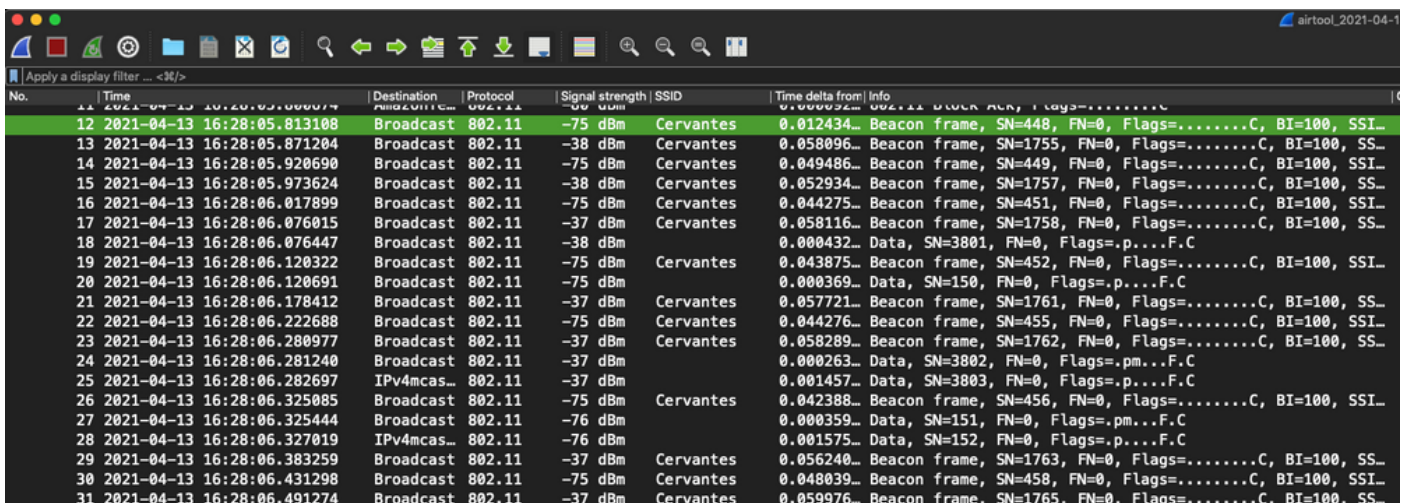
図に示すように、宛先フォルダを選択します。



## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

図に示すように、Wiresharkでキャプチャを開き、802.11フレームが表示されていることを確認します。



# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [802.11 ワイヤレス スニフィングの基礎](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)