Collecter des captures de paquets en vol sur un MacBook

Contenu

Introduction

Ce document décrit comment collecter des captures de paquets (PCAP) sur l'air (OTA) avec l'outil natif Wireless Diagnostics et des applications tierces telles que Airtool et Wireshark sur un MacBook afin de dépanner et d'analyser les comportements sans fil.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs LAN sans fil Cisco (WLC) AireOS ou Cisco IOS®-XE
- Connaissances de base dans la norme 802.11

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Apple MacBook avec macOS version 10.14.X ou ultérieure
- Outil Apple Wireless Diagnostics
- Airtool 1.9 ou supérieur
- Wireshark 3.X ou supérieur
- Point d'accès Cisco 2802

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Points à considérer :

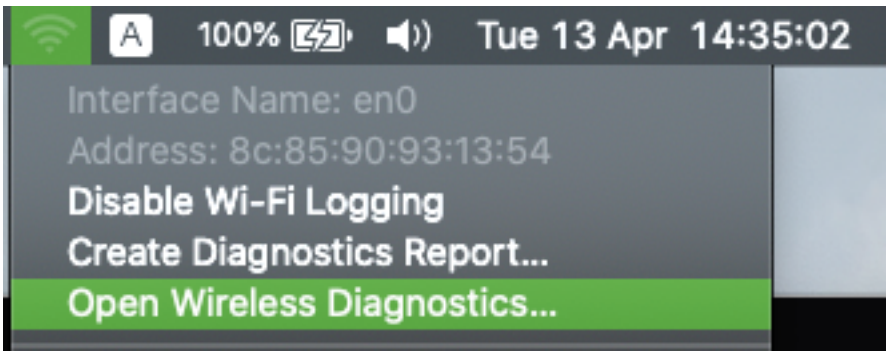
- Il est recommandé que le Macbook agisse comme un analyseur sans fil près du point d'accès et du périphérique cible.
- Assurez-vous de connaître le canal et la largeur 802.11, le périphérique client et le point d'accès utilisés.
- Le canal et la largeur se trouvent sur : Interface utilisateur graphique Web (GUI) de Cisco IOS®-XE sous **Configuration > Wireless > 5GHz or 2.4GHz > Select an AP > Channel and Width**Interface utilisateur graphique Web AireOS sous **Wireless > Access Points > 802.11a/n/ac (5 GHz) ou 802.11 b/g/n (2,4 GHz) > Select an AP > Channel and Width**

Configuration

Option A. Configuration de PCAP avec les diagnostics sans fil

Étape 1. Lancez l'outil de **diagnostic sans fil**.

Appuyez sur la touche **ALT/Option** et maintenez-la enfoncée à partir du clavier, puis cliquez sur l'**icône Wi-Fi** en haut à droite, comme illustré dans l'image.



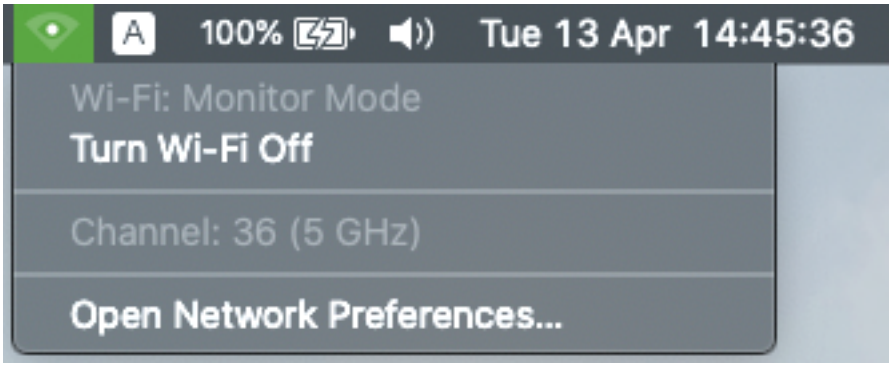
Étape 2. Ouvrez l'outil de renifleur.

Sélectionnez le menu **Fenêtre** de l'Outil de diagnostic sans fil dans la barre de menus et sélectionnez **Renifleur** ou utilisez le raccourci clavier, appuyez simultanément sur **ALT + Commande + 6** touches, comme illustré dans l'image.

Étape 3. Choisissez le **canal** et la **largeur** que le périphérique cible et le point d'accès utilisent, comme illustré dans l'image.

Étape 4. Cliquez sur **Démarrer.**

Cette action place la carte sans fil en mode de surveillance et ne peut pas être utilisée pour connecter le périphérique à un réseau local sans fil (WLAN), comme l'illustre l'image.



Étape 5. Attendez un certain temps pour recueillir les informations requises et cliquez sur **Arrêter.**

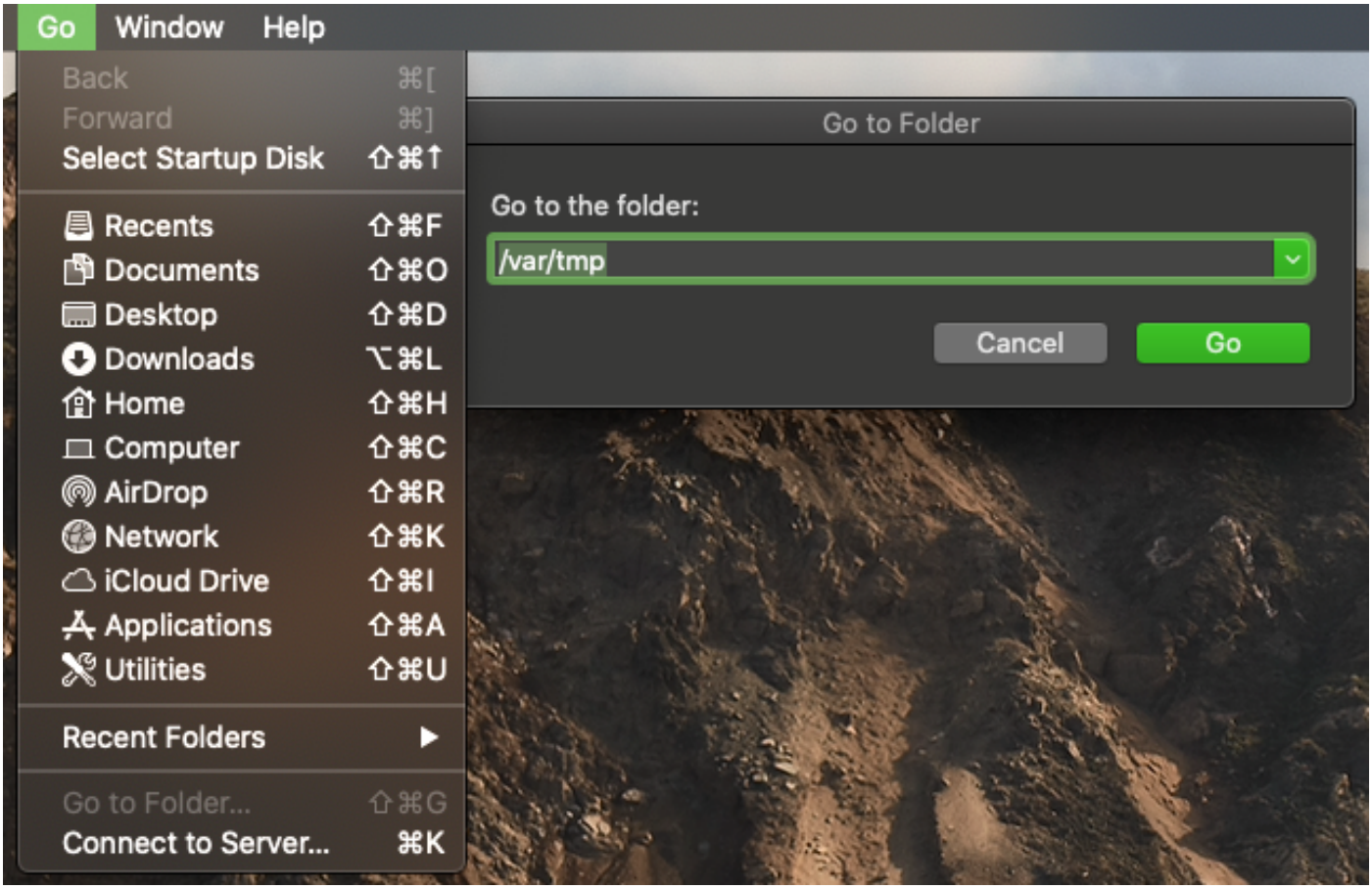
> **Astuce** : Si le WLAN utilise un chiffrement tel que la clé prépartagée (PSK), assurez-vous que la capture intercepte la connexion en quatre étapes entre le point d'accès et le client souhaité. Cela peut être fait si le PCAP OTA démarre avant que le périphérique ne soit associé au WLAN ou si le client est déauthentifié et réauthentifié pendant l'exécution de la capture.

Étape 6. Le fichier se trouve dans le dossier Desktop ou dans le chemin d'accès **/var/tmp/** (il peut varier sur la version macOS exécutée par MacBook).

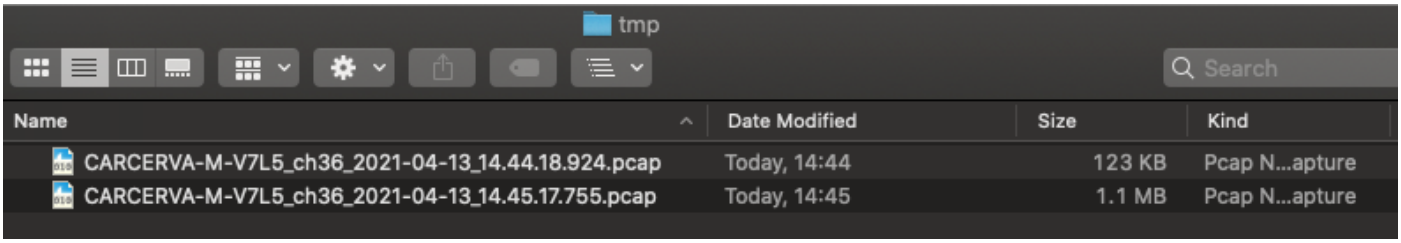
1. Lancez l'application Finder sur le MacBook, comme l'illustre l'image.

2. Sélectionnez le menu **Go** dans Finder.

3. Choisissez **Desktop** Folder ou **Go to Folder** et tapez le chemin d'accès de destination.



Le dossier de destination s'affiche.

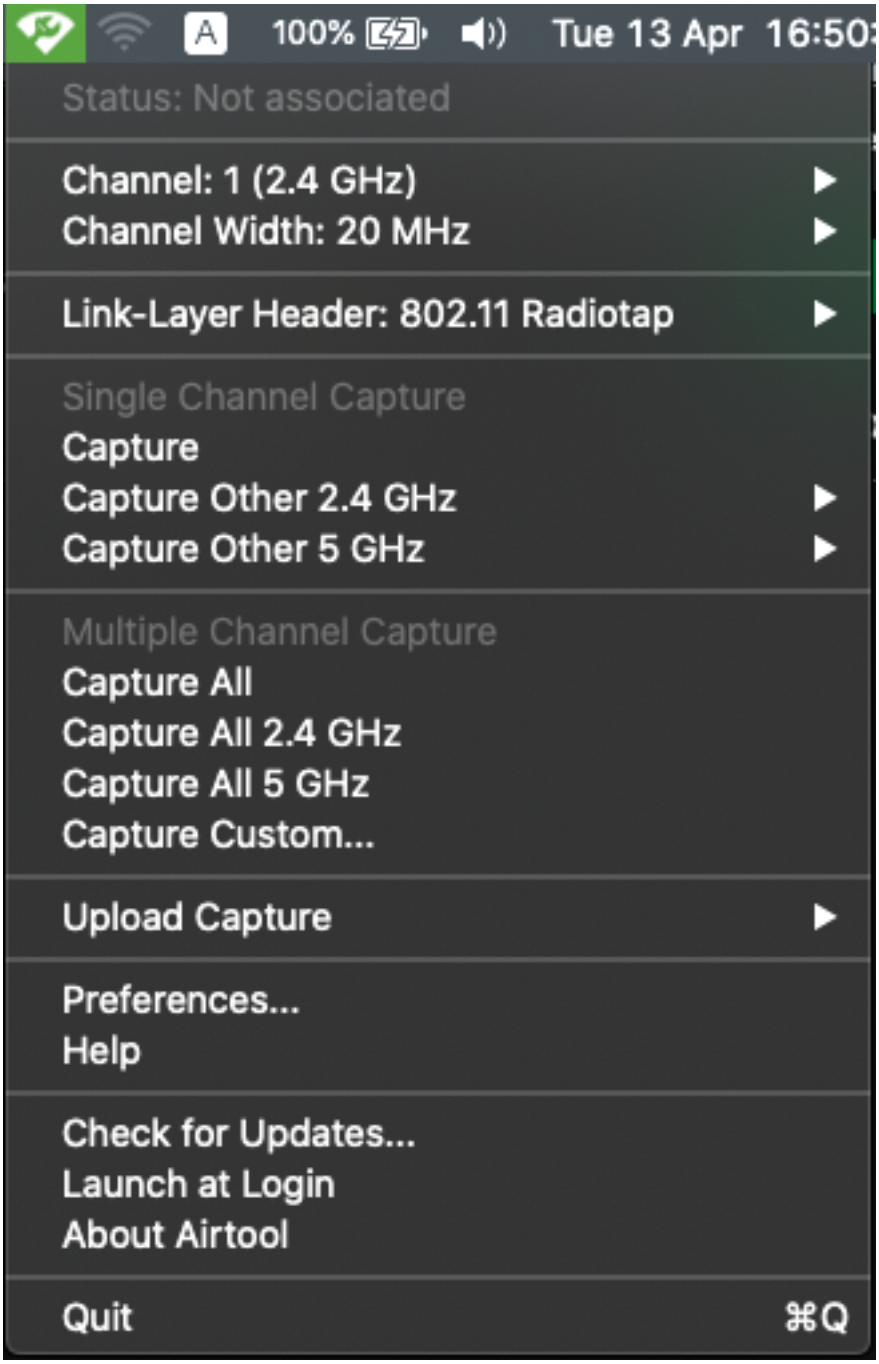


Option B. Configurer PCAP avec Airtool

Étape 1. Installez l'application Airtool tierce.

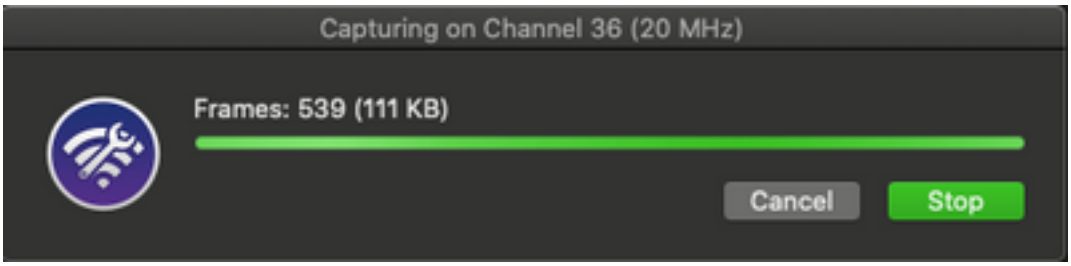
Étape 2. Lancez l'outil.

Une fois lancé, l'Airtool peut être situé en haut à droite de la barre de menus de macOS, comme l'illustre l'image.



Étape 3. Sélectionnez le **canal** et la **largeur** que le périphérique cible et le point d'accès utilisent (cette action démarre le PCAP), comme indiqué dans l'image.

Étape 4. Attendez un certain temps pour collecter les informations requises et cliquez sur **Arrêter,** comme indiqué dans l'image.



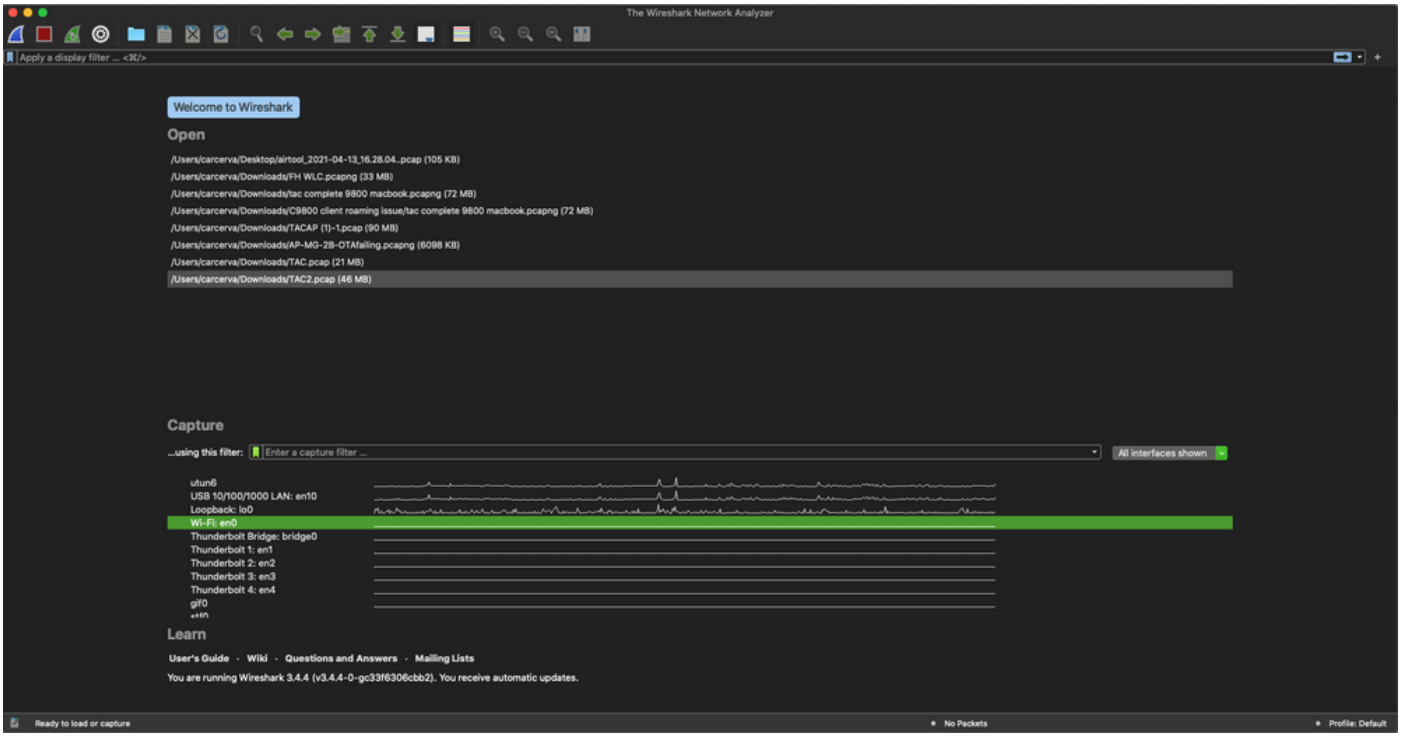
> **Astuce** : Si le WLAN utilise un chiffrement tel que la clé prépartagée (PSK), assurez-vous que la capture intercepte la connexion en quatre étapes entre le point d'accès et le client souhaité. Cela peut être fait si le PCAP OTA démarre avant que le périphérique ne soit associé au WLAN ou si le client est déauthentifié et réauthentifié pendant l'exécution de la capture.

Étape 5. Le fichier se trouve dans le dossier Bureau.

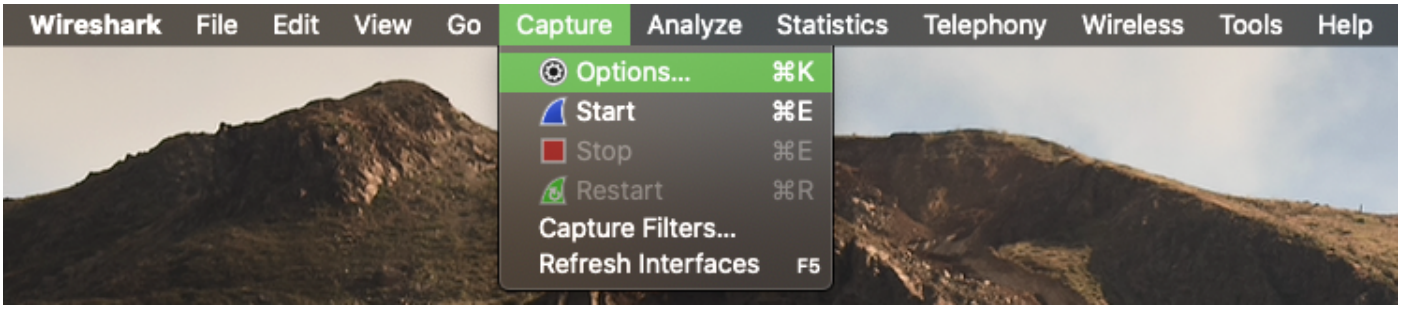
Option C. Configuration de PCAP avec Wireshark

Étape 1. Installez Wireshark.

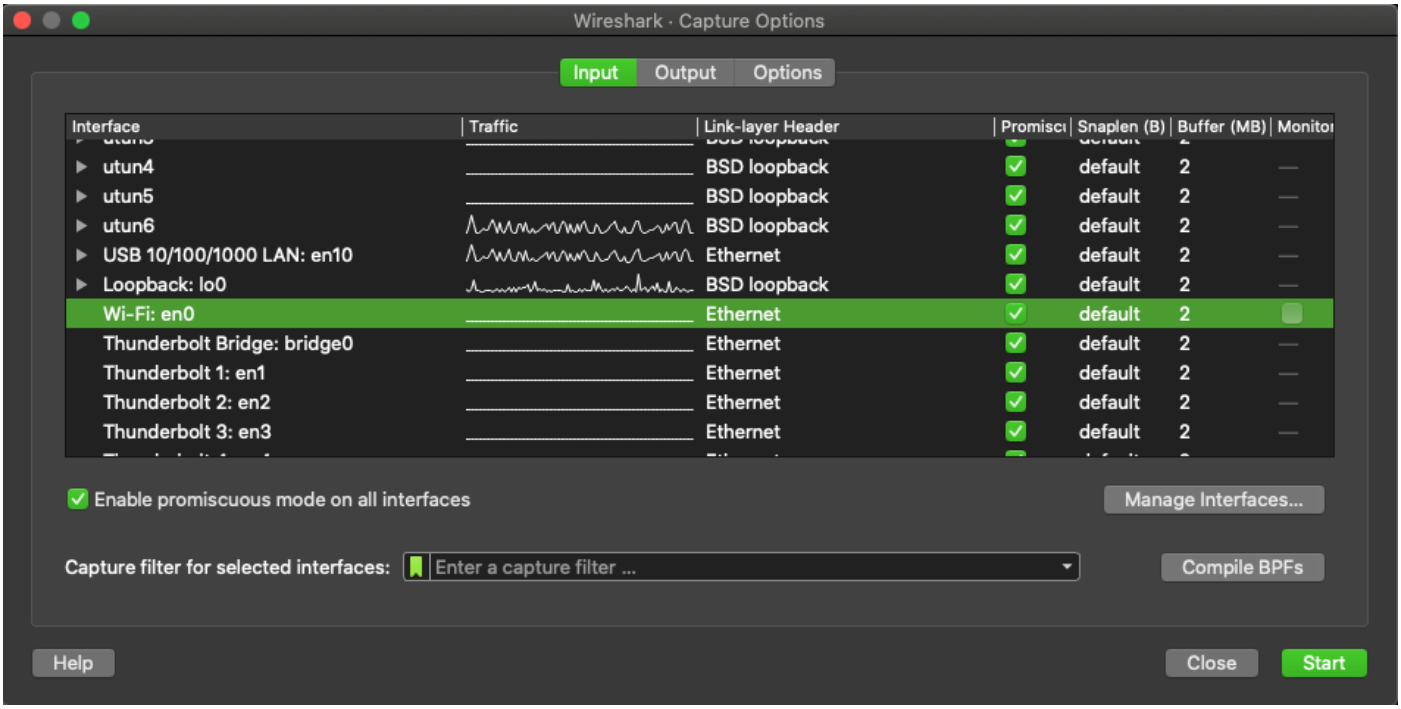
Étape 2. Lancez l'application, comme l'illustre l'image.



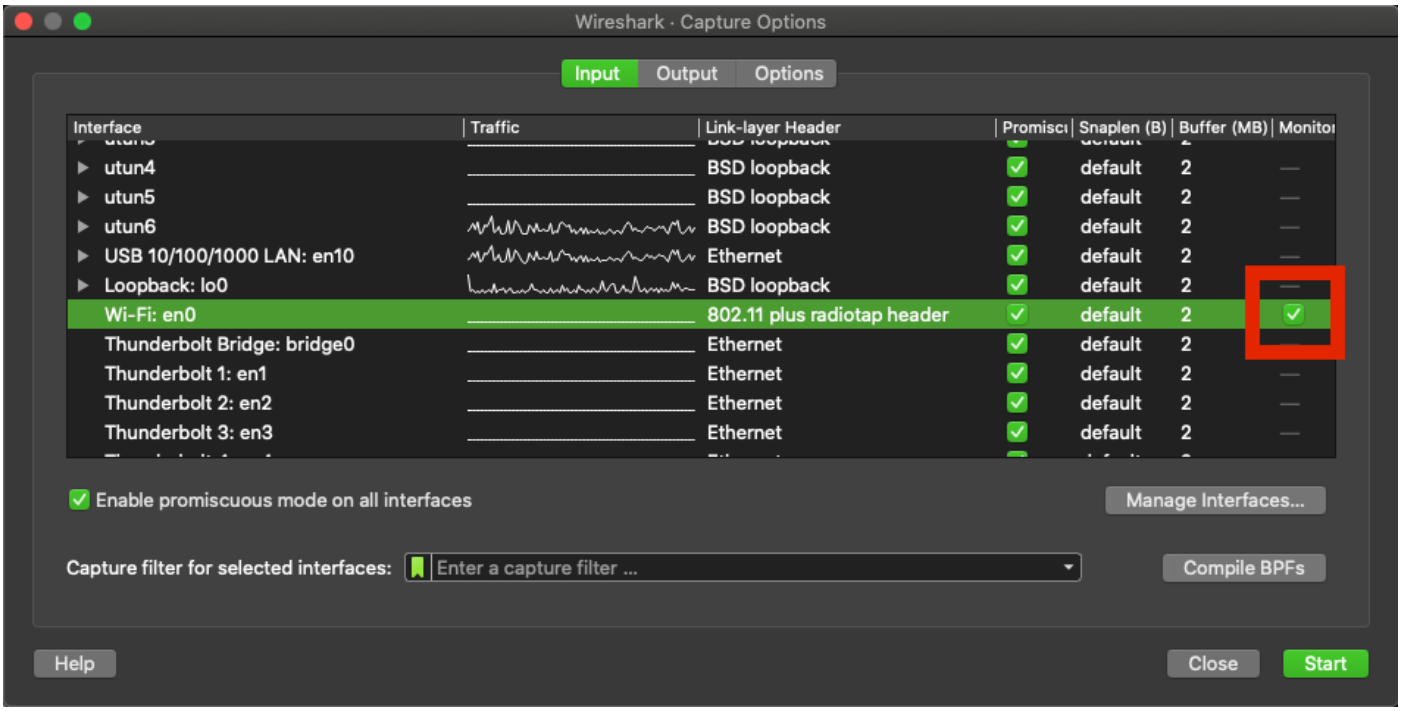
Étape 3. Sélectionnez le menu **Capture** dans la barre de menus et sélectionnez **Options**, comme illustré dans l'image.



Cette action ouvre une fenêtre contextuelle, comme le montre l'image.



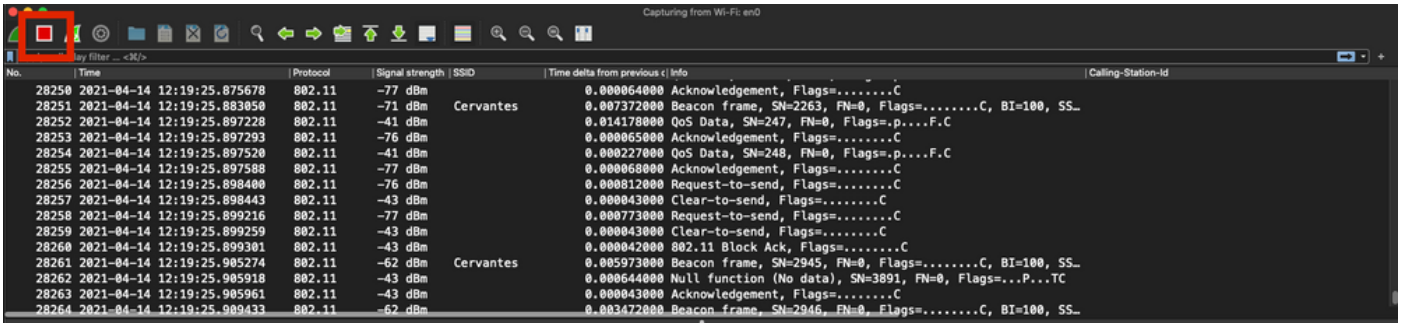
Étape 4. Sélectionnez le **Wi-Fi : en0** (adaptateur sans fil) et cochez l'option **Monitor** qui se trouve à droite de l'interface comme indiqué dans l'image.



Note: Dans cette méthode, Wireshark ne peut pas sélectionner le canal et la largeur souhaités pour l'analyse. Le canal et la largeur sont attribués avec l'outil de renifleur expliqué dans ce document. Reportez-vous à l'option A. Étape 3 afin de les modifier.

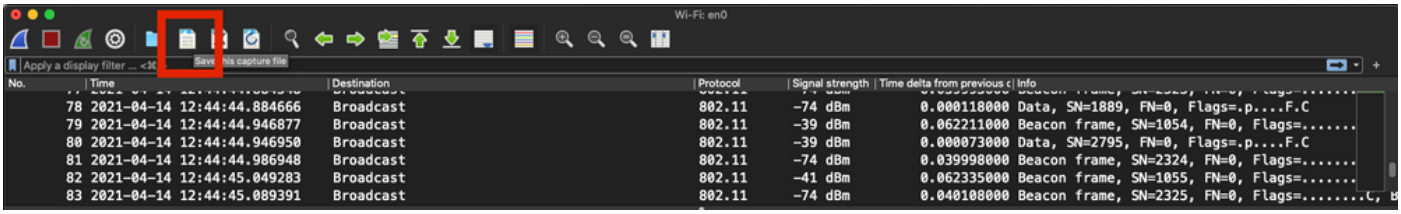
Étape 5. Sélectionnez **Démarrer.**

Étape 6. Attendez un certain temps pour recueillir les informations requises et sélectionnez le bouton **Arrêter** de Wireshark, comme l'illustre l'image.

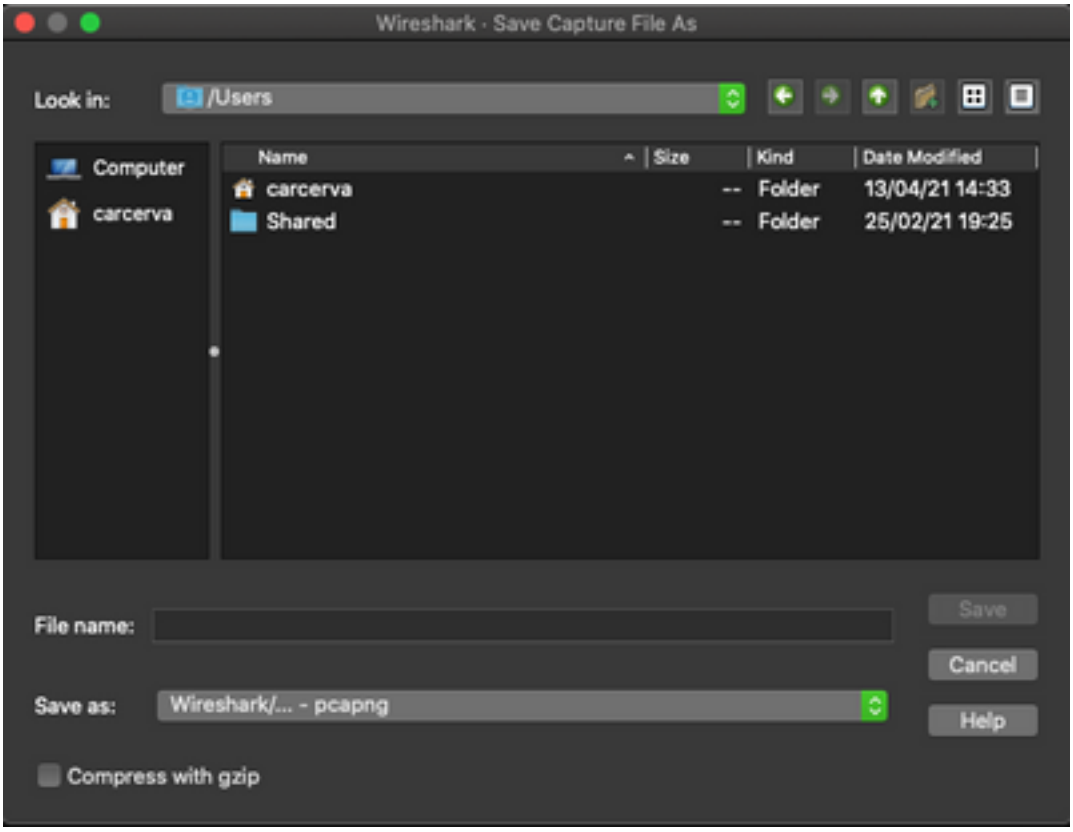


Astuce : Si le WLAN utilise un chiffrement tel que la clé prépartagée (PSK), assurez-vous que la capture intercepte la connexion en quatre étapes entre le point d'accès et le client souhaité. Cela peut être fait si le PCAP OTA démarre avant que le périphérique ne soit associé au WLAN ou si le client est déauthentifié et réauthentifié pendant l'exécution de la capture.

Étape 7. Enregistrez le fichier PCAP. Cliquez sur le bouton **Enregistrer** de Wireshark, comme illustré dans l'image.



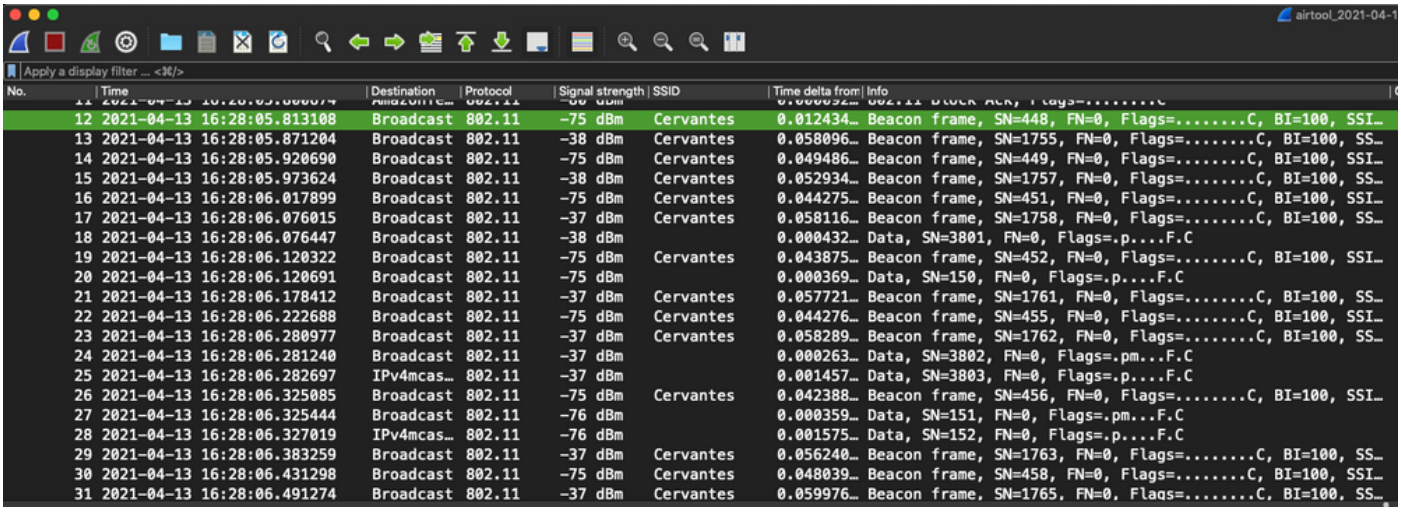
Sélectionnez le dossier de destination, comme illustré dans l'image.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Ouvrez la capture avec Wireshark et vérifiez que les trames 802.11 sont visibles, comme le montre l'image.



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Notions de base de la norme sans fil 802.11
- Support et documentation techniques - Cisco Systems