

# Coletar capturas de pacote sobre o ar em um MacBook

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Opção A. Configurar PCAP com diagnóstico sem fio](#)

[Opção B. Configurar PCAP com Airtool](#)

[Opção C. Configure o PCAP com o Wireshark](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como coletar PCAPs (Packet Captures, Capturas de Pacotes) Sobre o Ar (OTA) com a ferramenta nativa Wireless Diagnostics e aplicativos de terceiros, como Airtool e Wireshark em um MacBook, para solucionar problemas e analisar comportamentos sem fio.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Wireless LAN Controllers (WLCs) AireOS ou Cisco IOS®-XE
- Conhecimento básico no padrão 802.11

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Apple MacBook com macOS versão 10.14.X ou superior
- ferramenta de Diagnóstico sem fio da Apple
- Airtool 1.9 ou superior
- Wireshark 3.X ou superior
- Access Point (AP) 2802 da Cisco

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. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Pontos a serem considerados:

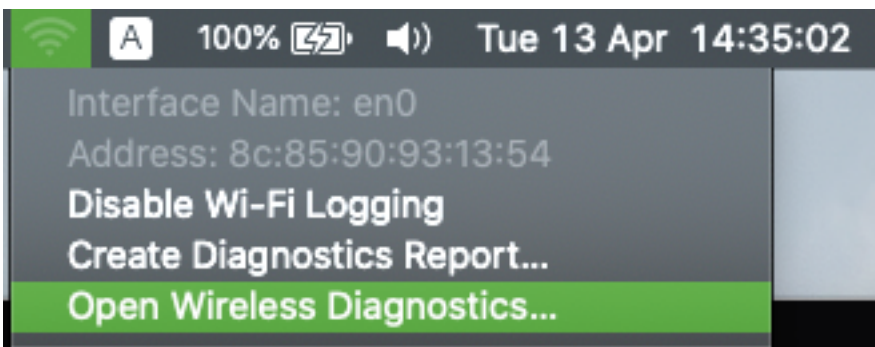
- Recomenda-se que o Macbook atue como um sniffer sem fio perto do AP e do dispositivo de destino.
- Certifique-se de saber qual canal e largura 802.11, o dispositivo cliente e o AP usam.
- O canal e a largura podem ser encontrados em: Interface gráfica do usuário (GUI) do Cisco IOS®-XE na Web em **Configuração > Sem fio > 5 GHz ou 2,4 GHz > Selecionar um AP > Canal e Largura** GUI da Web do AireOS em **Wireless > Access Points > 802.11a/n/ac (5 GHz) ou 802.11 b/g/n (2,4 GHz) > Selecione um AP > Canal e Largura**

## Configurar

### Opção A. Configurar PCAP com diagnóstico sem fio

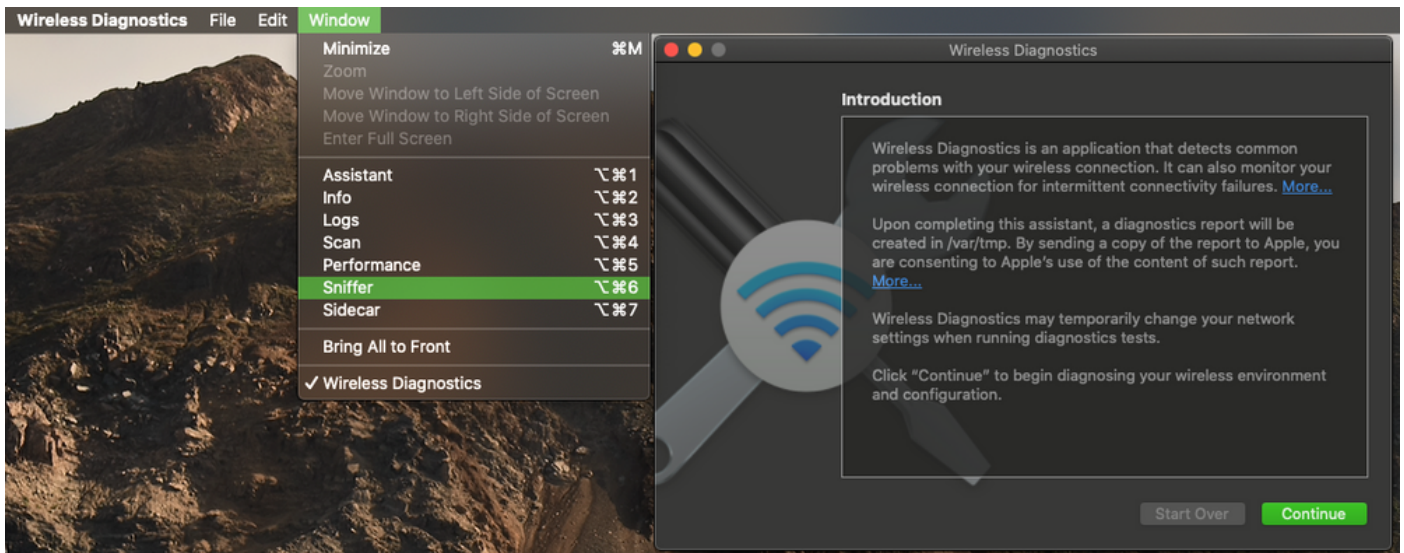
Etapa 1. Inicie a Ferramenta de diagnóstico sem fio.

Mantenha pressionada a tecla **ALT/Option** no teclado e clique no ícone **Wi-Fi** superior direito, como mostrado na imagem.



Etapa 2. Abra a ferramenta Sniffer.

Selecione o menu **Window** na Wireless Diagnostic Tool (Ferramenta de diagnóstico sem fio) na barra de menus e selecione **Sniffer** ou use o atalho do teclado; pressione ao mesmo tempo **ALT + Command + 6** Teclas, como mostrado na imagem.

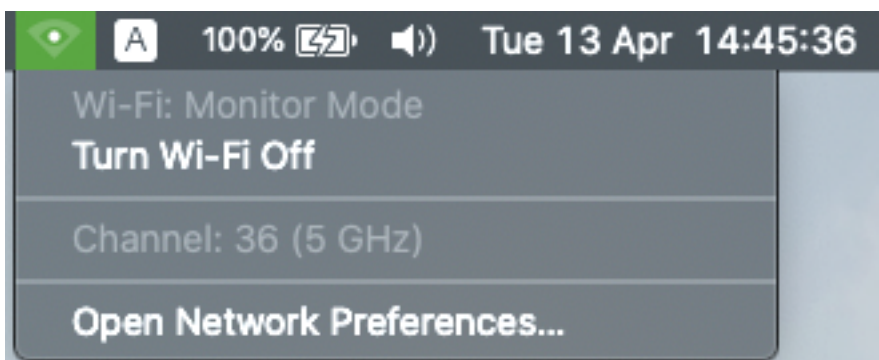


Etapa 3. Escolha o **Canal** e a **Largura** que o dispositivo de destino e o AP usam, como mostrado na imagem.



Etapa 4. Clique em Iniciar.

Esta ação coloca o adaptador sem fio no modo de monitor e ele não pode ser usado para conectar o dispositivo a uma LAN sem fio (WLAN), como mostrado na imagem.



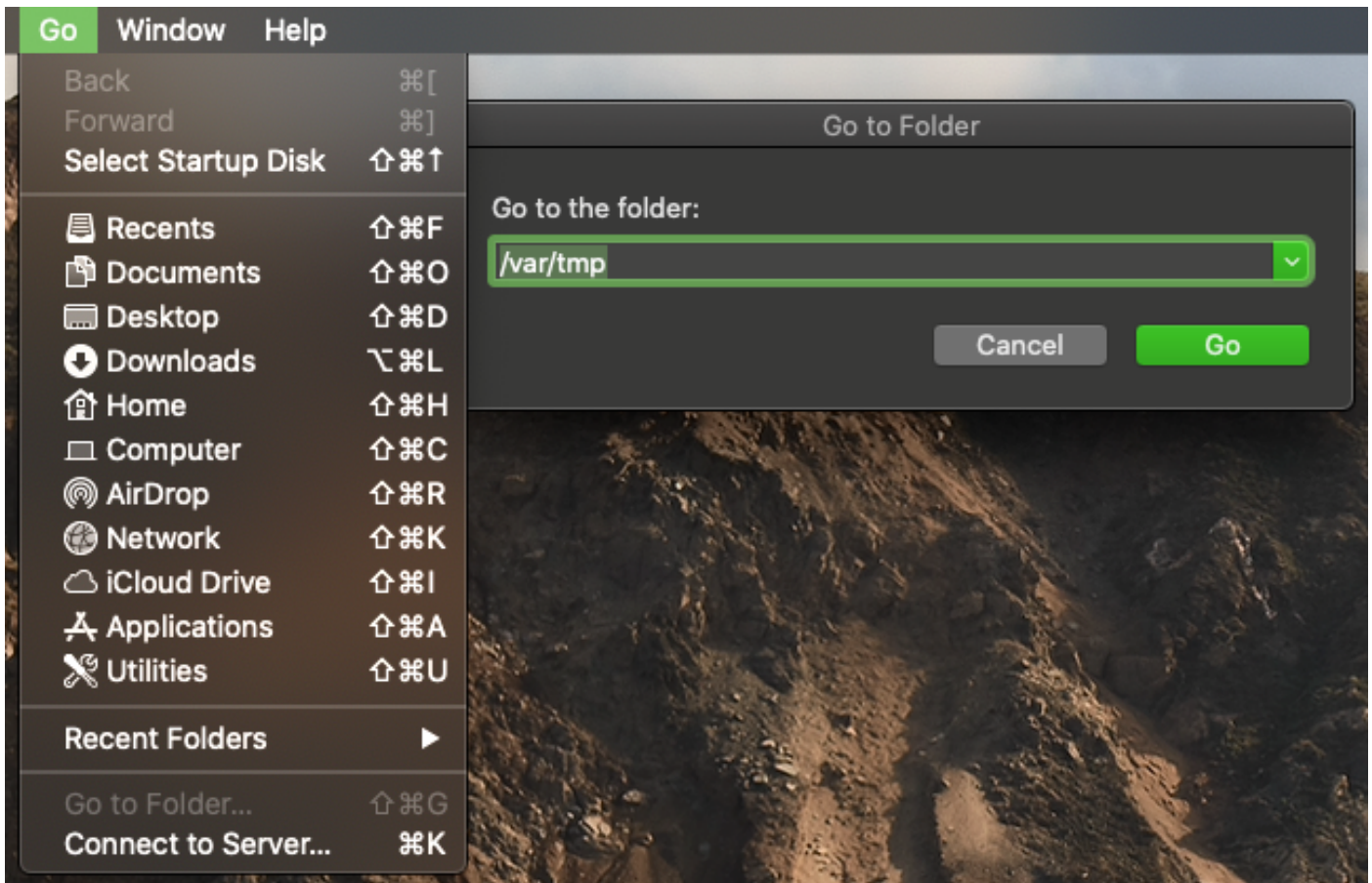
Etapa 5. Aguarde algum tempo para coletar as informações necessárias e clique em **Parar**.



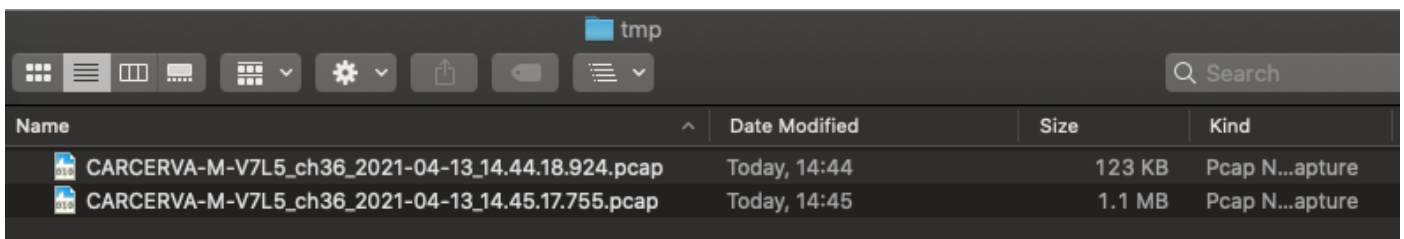
**Tip:** Se a WLAN usar criptografia como chave pré-compartilhada (PSK), assegure-se de que a captura capture o handshake de quatro vias entre o AP e o cliente desejado. Isso pode ser feito se o PCAP OTA for iniciado antes do dispositivo ser associado à WLAN ou se o cliente for desautenticado e reautenticado enquanto a captura é executada.

Etapa 6. O arquivo está localizado na pasta Desktop ou no caminho `/var/tmp/` (pode variar na versão macOS executada pelo MacBook).

1. Inicie o aplicativo Finder no MacBook, como mostrado na imagem.
2. Selecione o menu **Ir** no Finder.
3. Escolha **Desktop** Folder ou **Ir para Pasta** e digite o caminho de destino.



A pasta de destino é exibida.



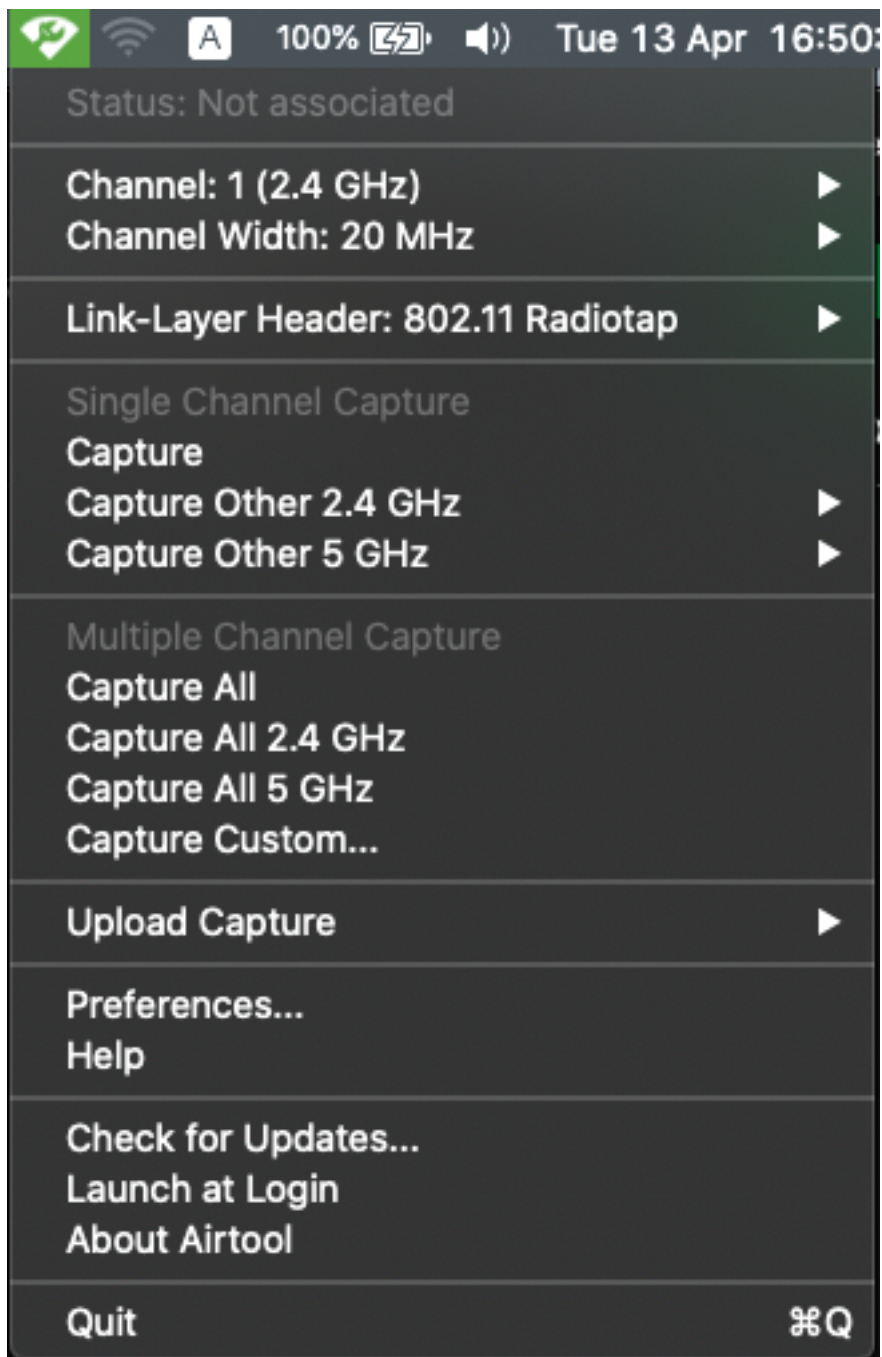
## Opção B. Configurar PCAP com Airtool

Etapa 1. Instale o aplicativo [Airtool](#) de terceiros.

Etapa 2. Inicie a ferramenta.

Uma vez iniciada, a Airtool pode estar localizada na parte superior direita da barra de menus macOS, como mostrado na imagem.

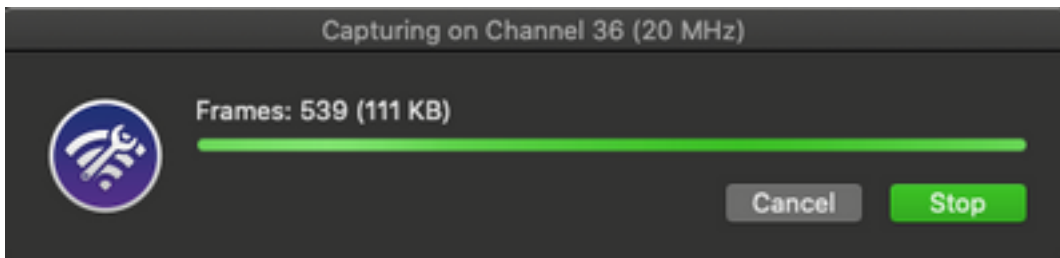




Etapa 3. Selecione o **Canal** e a **Largura** que o dispositivo de destino e o AP usam (esta ação inicia o PCAP), como mostrado na imagem.



Etapa 4. Aguarde algum tempo para coletar as informações necessárias e clique em **Parar**, como mostrado na imagem.



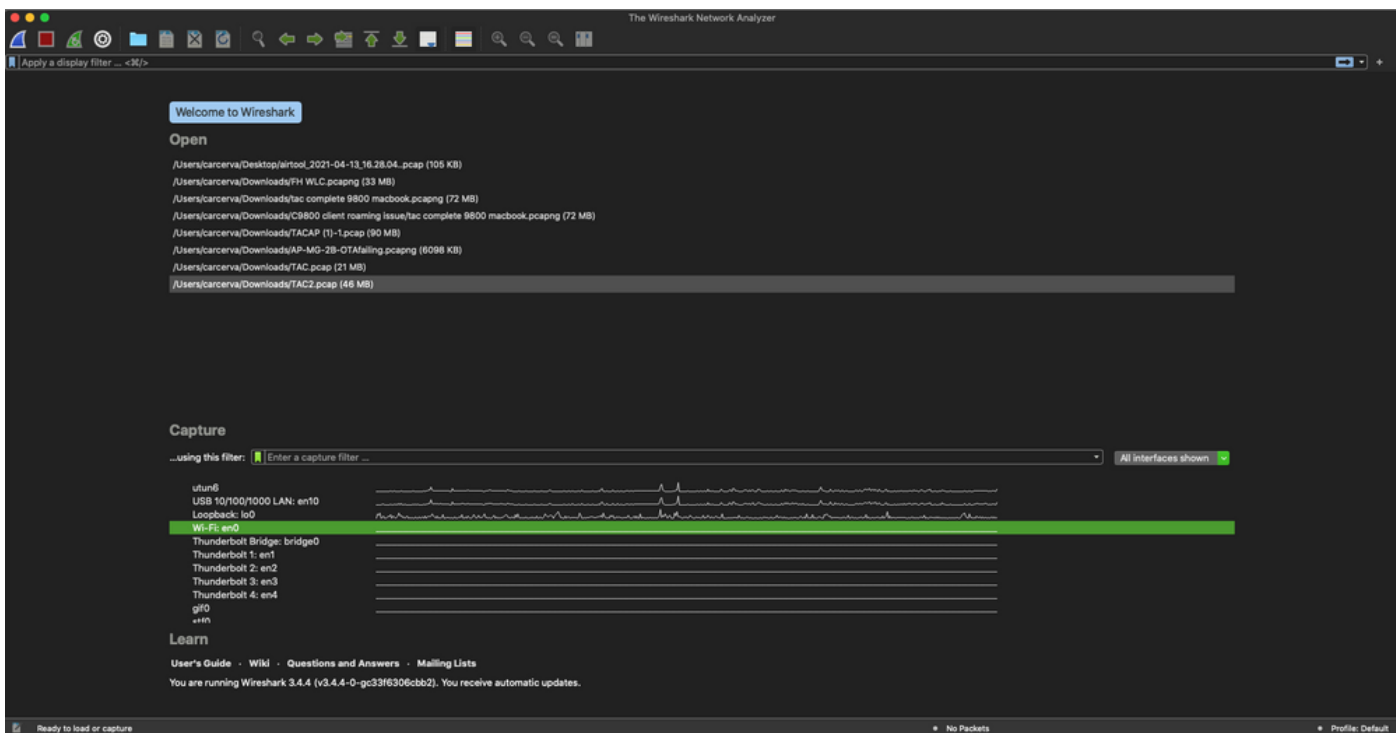
**Tip:** Se a WLAN usar criptografia como chave pré-compartilhada (PSK), assegure-se de que a captura capture o handshake de quatro vias entre o AP e o cliente desejado. Isso pode ser feito se o PCAP OTA for iniciado antes do dispositivo ser associado à WLAN ou se o cliente for desautenticado e reautenticado enquanto a captura é executada.

Etapa 5. O arquivo está localizado na pasta Área de Trabalho.

## Opção C. Configure o PCAP com o Wireshark

Etapa 1. Instale o [Wireshark](#).

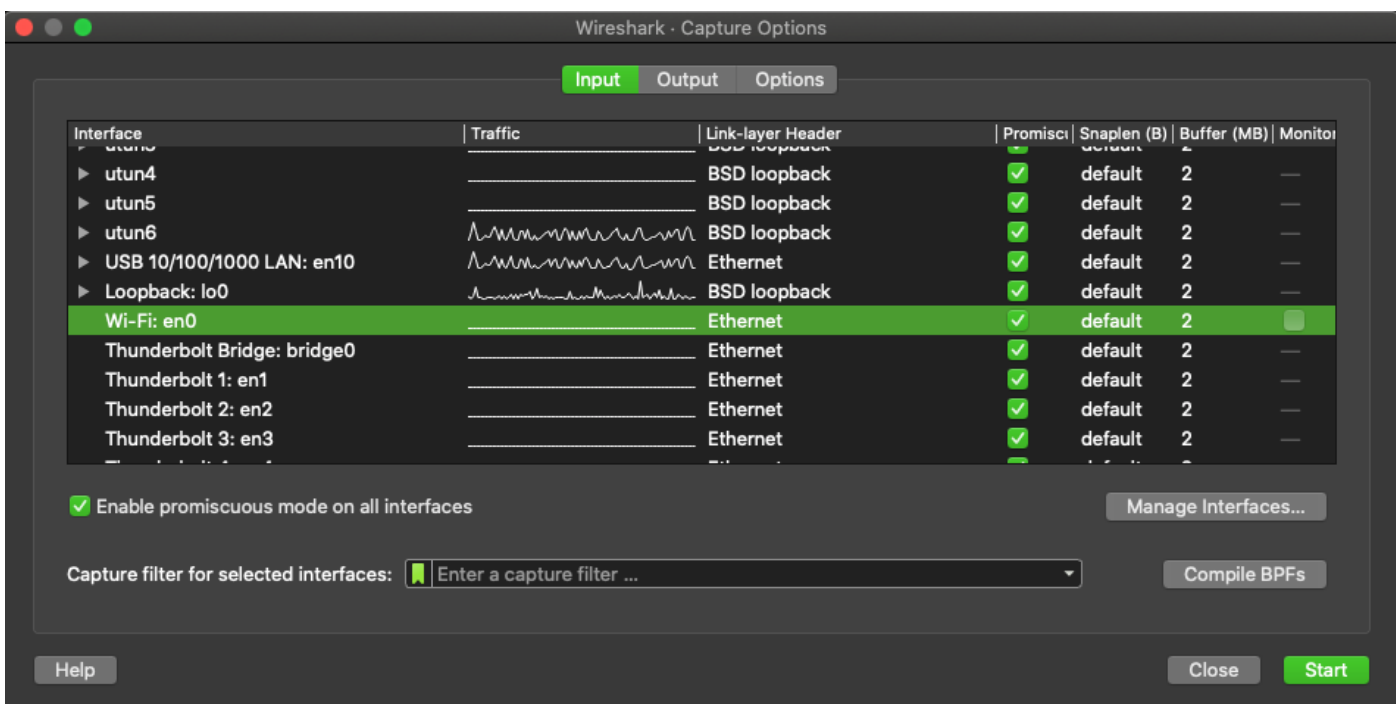
Etapa 2. Inicie o aplicativo, como mostrado na imagem.



Etapa 3. Selecione o menu **Capturar** na barra de menus e selecione **Opções**, como mostrado na imagem.

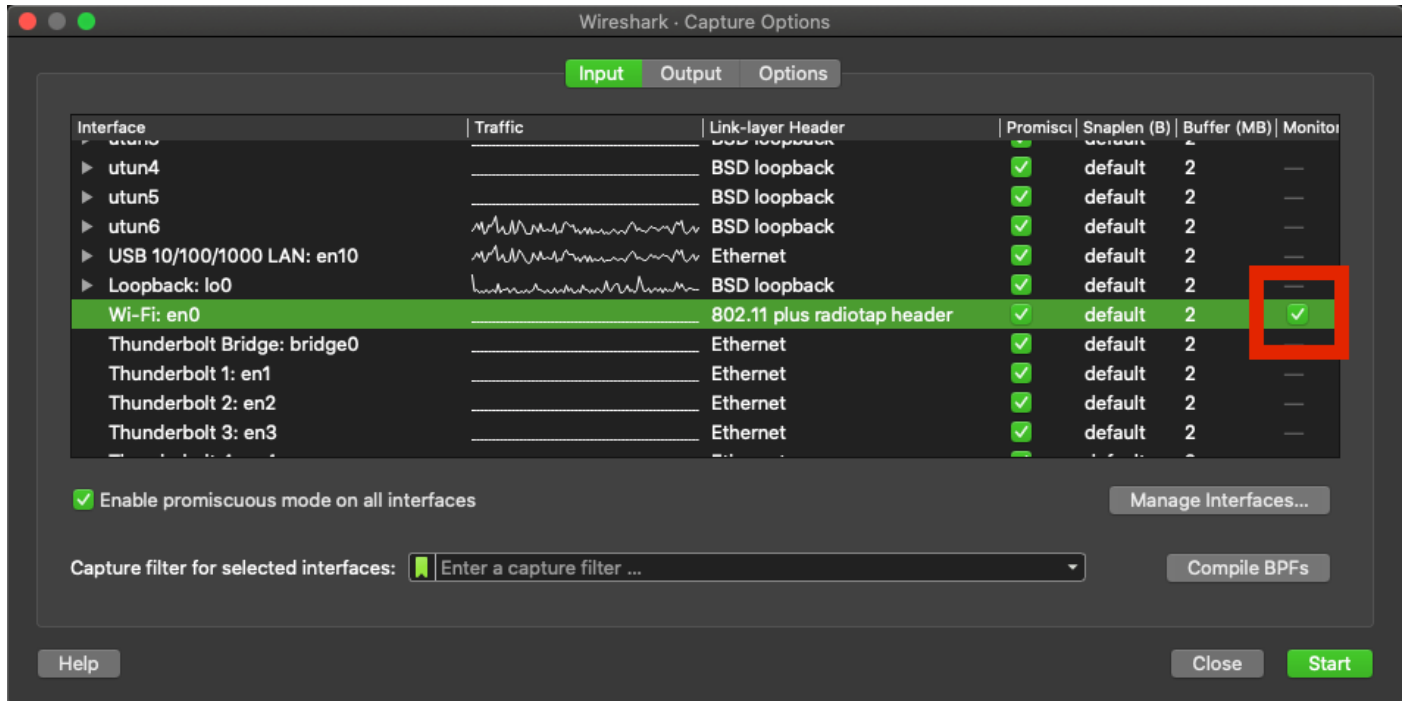


Essa ação abre uma janela pop-up, como mostrado na imagem.





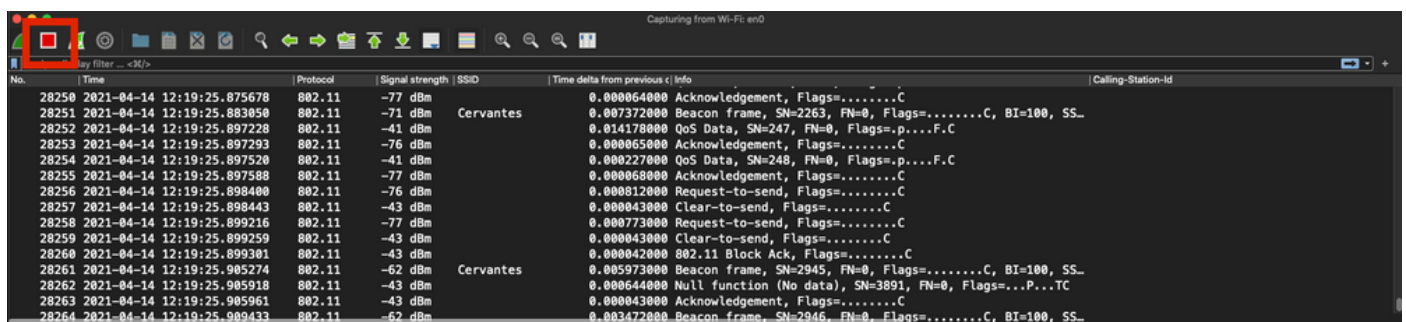
Etapa 4. Selecione o **Wi-Fi: en0** (Adaptador sem fio) e marque a opção **Monitor** à direita da interface, como mostrado na imagem.



**Note:** Neste método, o Wireshark não consegue selecionar o canal e a largura desejados para digitalização. O canal e a largura são atribuídos com a ferramenta de farejador explicada neste documento. Consulte a Opção A. Etapa 3 para alterá-los.

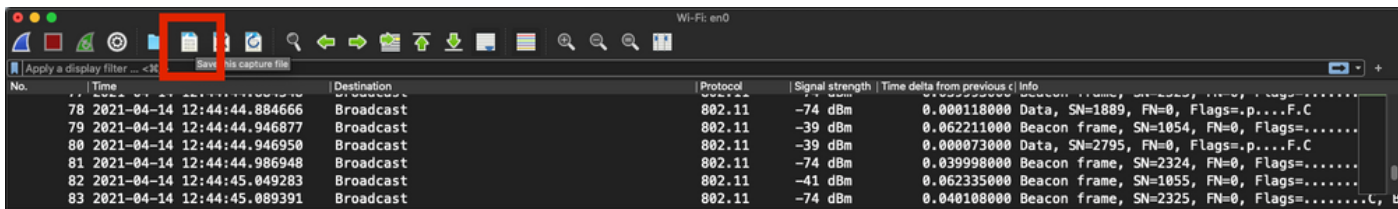
Etapa 5. Selecione **Iniciar**.

Etapa 6. Aguarde algum tempo para coletar as informações necessárias e selecione o botão **Parar** no Wireshark, como mostrado na imagem.

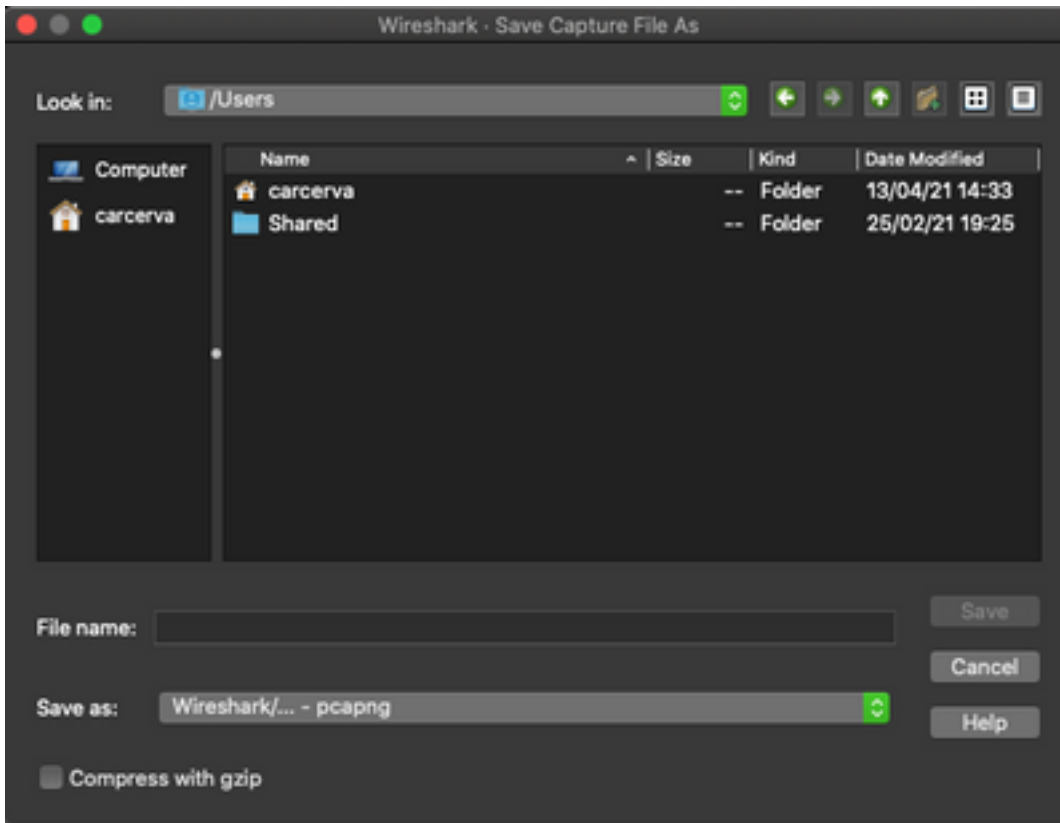


**Tip:** Se a WLAN usar criptografia como chave pré-compartilhada (PSK), assegure-se de que a captura capture o handshake de quatro vias entre o AP e o cliente desejado. Isso pode ser feito se o PCAP OTA for iniciado antes do dispositivo ser associado à WLAN ou se o cliente for desautenticado e reautenticado enquanto a captura é executada.

Passo 7. Salve o arquivo PCAP. Clique no botão **Salvar** do Wireshark, como mostrado na imagem.



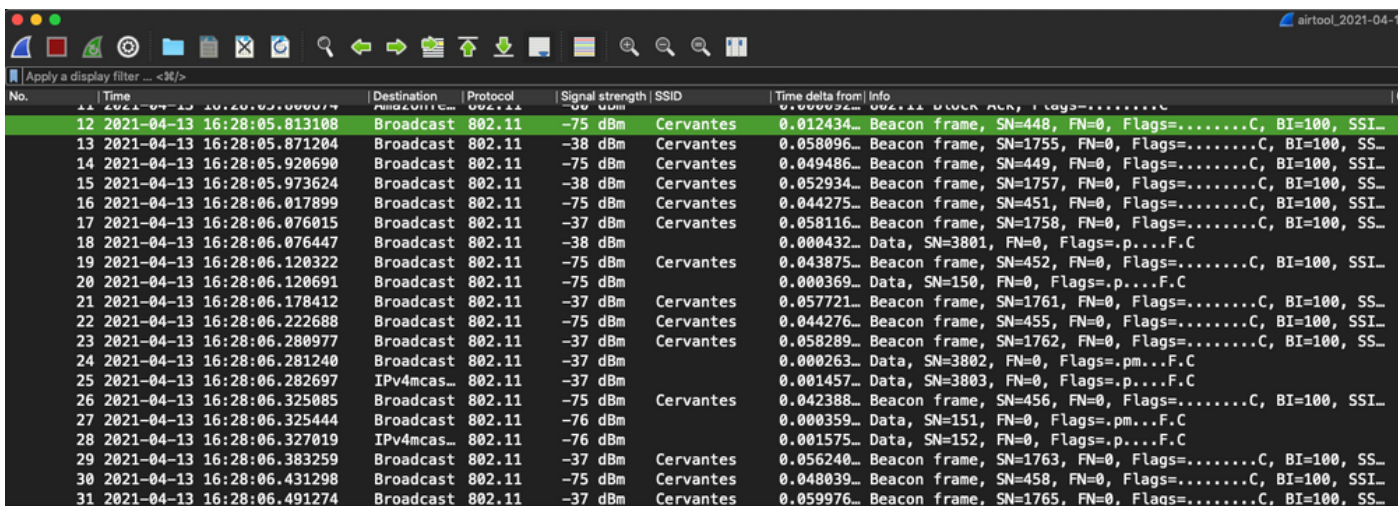
Selecione a pasta de destino, como mostrado na imagem.



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Abra a captura com o Wireshark e verifique se os quadros 802.11 estão visíveis, como mostrado na imagem.



# Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Fundamentos do 802.11 Wireless Sniffing](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)