Usando o Wireshark em um Cisco Business WAP para análise de pacotes: Carregar arquivo

Objetivo

Este artigo explica como usar o Cisco Business Wireless Access Point (WAP) e o Wireshark para executar, salvar e carregar uma captura de pacote.

Introduction

Alterações de configuração, monitoramento e solução de problemas são algo com que um administrador de rede precisa lidar com frequência. Ter uma ferramenta simples para usar é inestimável! O objetivo deste artigo é ficar mais confortável com os conceitos básicos de captura de pacotes, bem como como carregar um arquivo no Wireshark. Se você não está familiarizado com esse processo, responda a algumas perguntas que você talvez já tenha feito.

Primeiramente, o Wireshark é um analisador de pacotes gratuito para qualquer pessoa que deseje solucionar problemas de sua rede. O Wireshark fornece muitas opções para a captura, bem como para classificar o tráfego por vários parâmetros diferentes. Vá para o Wireshark para obter detalhes sobre esta opção de código aberto.

O que é uma captura de pacotes?

Uma captura de pacote, também conhecida como arquivo PCAP, é uma ferramenta que pode ser útil na solução de problemas. Ele pode registrar cada pacote enviado entre dispositivos na rede, em tempo real. A captura de pacotes permite que você descubra os detalhes do tráfego de rede, o que pode incluir tudo, desde descoberta de dispositivos, conversas de protocolo e autenticação com falha. Você pode ver o caminho do fluxo de tráfego específico e cada interação entre dispositivos em redes selecionadas. Esses pacotes podem ser salvos para análise adicional, conforme necessário. É como um raio-x do funcionamento interno da rede através da transferência de pacotes.

Que tipos de pacotes podem ser capturados?

O dispositivo WAP pode capturar os seguintes tipos de pacotes:

Pacotes 802.11 recebidos e transmitidos nas interfaces de rádio. Os pacotes capturados nas interfaces de rádio incluem o cabeçalho 802.11.

Pacotes 802.3 recebidos e transmitidos na interface Ethernet.

Pacotes 802.3 recebidos e transmitidos nas interfaces lógicas internas, como Pontos

de Acesso Virtuais (VAPs - Virtual Access Points) e Interfaces do Sistema de Distribuição Wireless (WDS - Wireless Distribution System).

Quais são as maneiras pelas quais uma captura de pacotes pode ser feita?

Há dois métodos disponíveis de captura de pacotes:

1. *Método de Captura Remota* - Os pacotes capturados são redirecionados em tempo real para um computador externo que executa o Wireshark. Você pode escolher *Stream to a Remote Host* para selecionar o método de captura remota. Se preferir o método de captura remota, confira Usando o Wireshark em um WAP para Análise de Pacotes: Transfira diretamente para o Wireshark.
2. *Método de Captura Local* - Os pacotes capturados são armazenados em um arquivo no dispositivo WAP. O dispositivo WAP pode transferir o arquivo para um servidor TFTP (Trivial File Transfer Protocol). O arquivo é formatado no formato PCAP e pode ser examinado usando o Wireshark. Você pode escolher *Salvar arquivo neste dispositivo* para selecionar o método de captura local.

O foco deste artigo é carregar um arquivo para o Wireshark com a interface gráfica do usuário (GUI) mais recente. Se preferir exibir um artigo que use a GUI mais antiga para o método de captura local, consulte Configurar Captura de Pacotes para Otimizar o Desempenho em um Ponto de Acesso Sem Fio.

O que eu faço com uma captura de pacote depois de ter o arquivo PCAP?

O recurso de captura de pacotes sem fio permite capturar e armazenar os pacotes recebidos e transmitidos pelo dispositivo WAP. Os pacotes capturados podem, então, ser analisados por um analisador de protocolo de rede para solução de problemas ou otimização de desempenho. Há muitos aplicativos de análise de pacotes de terceiros disponíveis on-line. Neste artigo, nos concentramos no Wireshark.

O Wireshark não é de propriedade da Cisco ou é compatível com ela. Para obter suporte, entre em contato com o Wireshark.

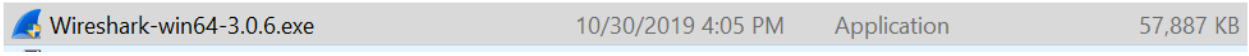
Dispositivos | Versão do software

- WAP125 |1.0.2.0
- WAP150 |1.1.1.0
- WAP121 |1.0.6.8
- WAP361 |1.1.1.0
- WAP581 |1.0.2.0
- WAP571 |1.1.0.4
- WAP571E |1.1.0.4

Download do Wireshark

Etapa 1. Vá para o site do Wireshark. Clique em **Download**. Selecione a versão apropriada para download. Você verá o progresso do download na parte inferior esquerda da tela.

Etapa 2. Vá para *Downloads* em seu computador e selecione o arquivo Wireshark para instalar seu aplicativo.



Faça login no WAP

No navegador da Web, insira o endereço IP do WAP. Digite suas credenciais. Se esta for a primeira vez que você acessa este dispositivo ou fez uma redefinição de fábrica, o nome de usuário e a senha padrão são *cisco*. Se precisar de instruções sobre como fazer login, siga as etapas do artigo Acesse o Utilitário baseado na Web do Ponto de acesso sem fio (WAP).

Salvar uma captura de pacote em um PC e carregar no Wireshark

Etapa 1. Navegue até **Troubleshoot > Packet Capture**.

Verifique se **Save File on this Device** está selecionado para o *Packet Capture Method*.

Configure estes parâmetros:

·*Interface* - Insira um tipo de interface de captura para a captura de pacotes:

·*Ethernet* - tráfego 802.3 na porta Ethernet.

·*Rádio 1 (5 GHz) / Rádio 2 (2,4 GHz)* - Tráfego 802.11 na interface de rádio.

·*Duration* - (Duração) Insira a duração em segundos para a captura. O intervalo é de 10 a 3600. O padrão é 60.

·*Tamanho máximo do arquivo* - Insira o tamanho máximo permitido para o arquivo de captura em kilobytes (KB). O intervalo é de 64 a 4096. O padrão é 1024.

Há dois modos para a captura de pacotes.

·*Todo o Tráfego Sem Fio* - Captura todos os pacotes sem fio.

·*Tráfego para/deste AP* - Captura os pacotes enviados do AP ou recebidos pelo AP.

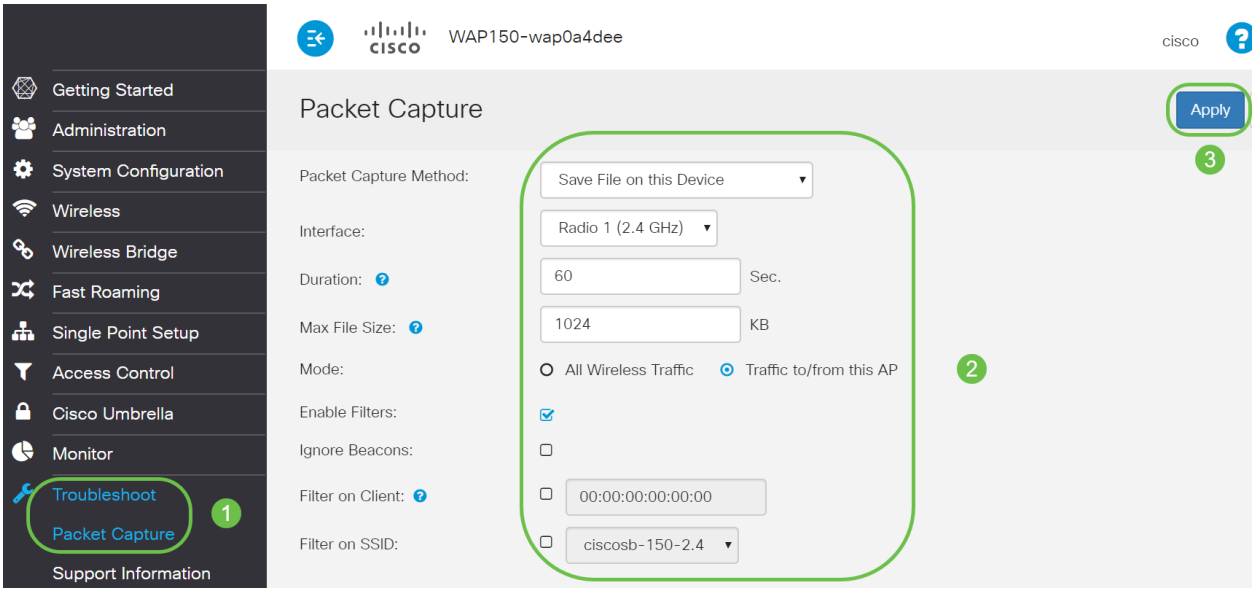
Clique em **Ativar filtros**. Há três caixas de seleção disponíveis: *Ignorar beacons, Filtrar no cliente* e *Filtrar no SSID*.

·*Ignorar Beacons* - Ative ou desative a captura de beacons 802.11 detectados ou transmitidos pelo rádio. Os quadros beacon são quadros de broadcast que transportam informações sobre uma rede. A finalidade de um beacon é anunciar a rede sem fio existente. Se você não estiver procurando esse tipo de tráfego, poderá selecionar Ignorar beacons.

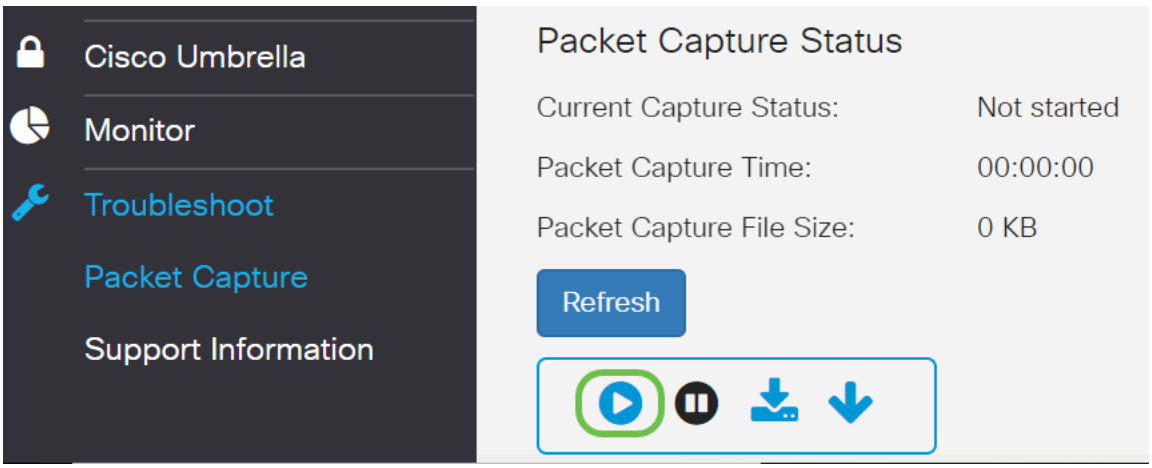
·*Filtro no Cliente* - Especifica o endereço MAC para o filtro do cliente WLAN. Observe que o filtro do cliente está ativo somente quando uma captura é executada em uma interface 802.11.

·*Filtro no SSID* - Selecione um nome SSID para a captura de pacotes.

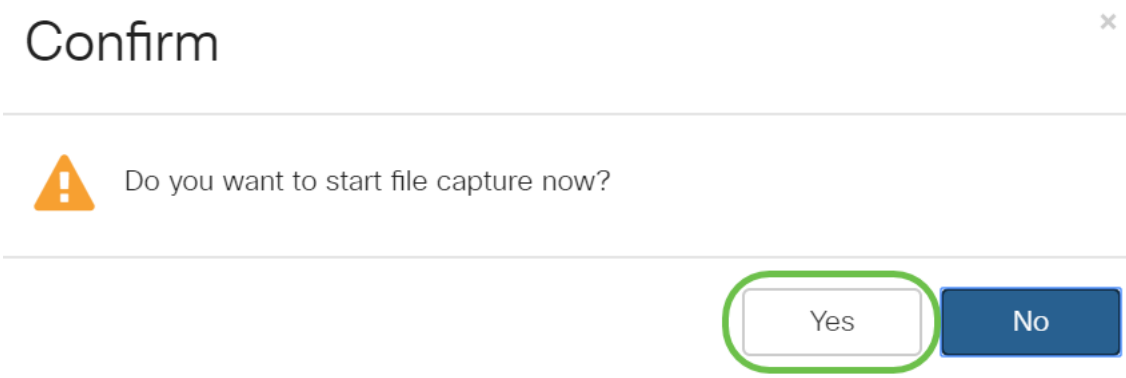
Clique em **Apply** para salvar na configuração de inicialização.



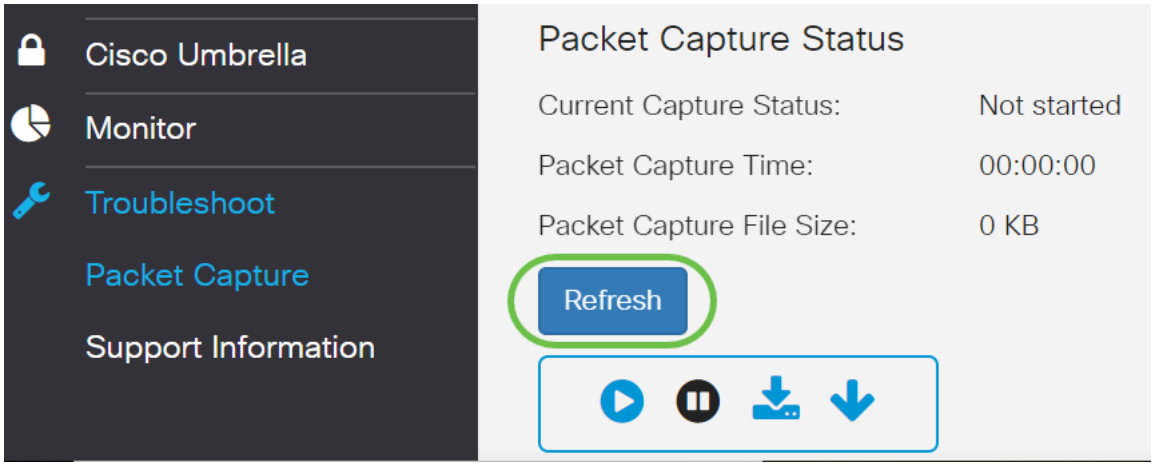
Etapa 2. Clique no ícone **Iniciar captura**.



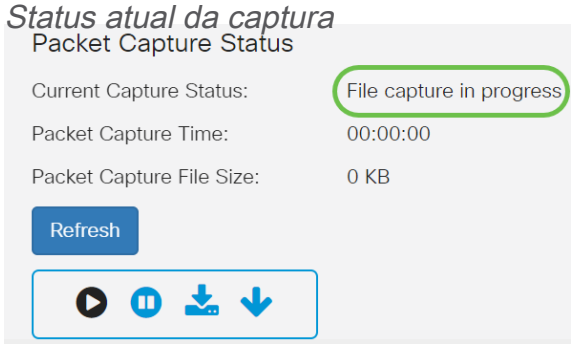
Etapa 3. Uma janela pop-up *Confirmar* abrirá para obter a confirmação para baixar o arquivo. Clique em **Sim** para iniciar o download do arquivo.



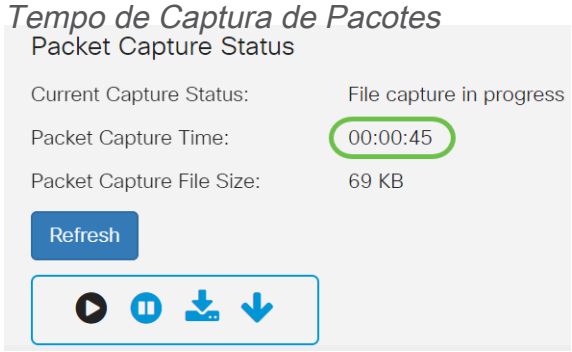
Etapa 4. Clique em **Atualizar** para obter o *Status de Captura de Pacotes* que contém os seguintes dados:



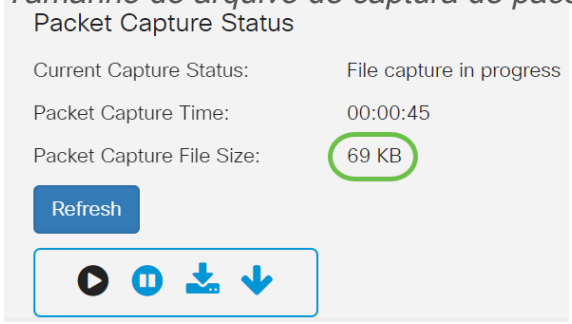
1. *Status atual da captura*



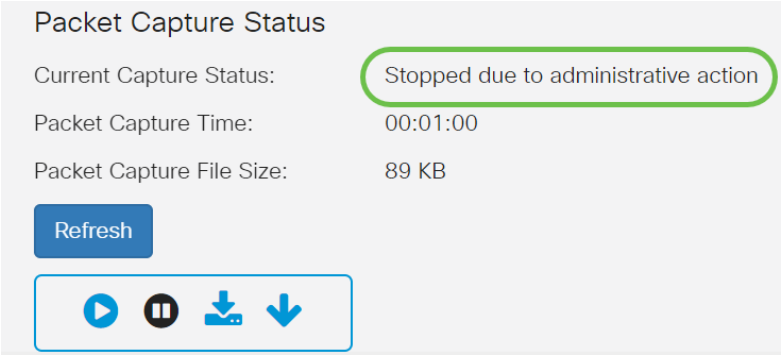
2. *Tempo de Captura de Pacotes*



3. *Tamanho do arquivo de captura de pacote*

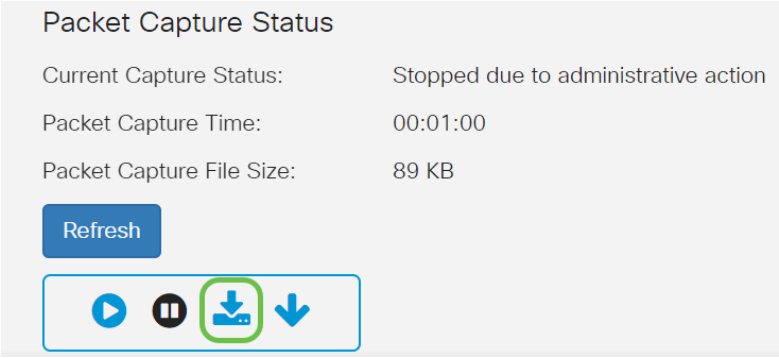


4. No modo *Packet File Capture*, o dispositivo WAP armazena os pacotes capturados no sistema de arquivos RAM (Random Access Memory). Após a ativação, a captura de pacote continua até que um destes eventos ocorra:
   O tempo de captura alcança a duração configurada.
   O arquivo de captura atinge seu tamanho máximo.
   O administrador para a captura.

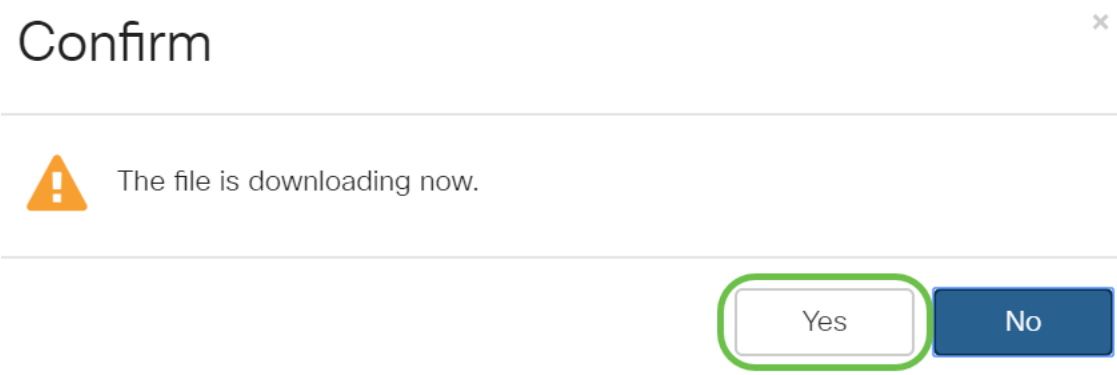


O arquivo de captura de pacote será armazenado no AP até que você reinicialize o AP.

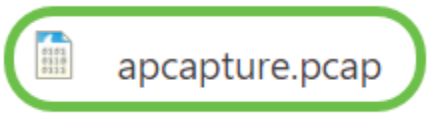
Etapa 5. Clique no ícone **Download para este dispositivo** para baixar o arquivo capturado recentemente.



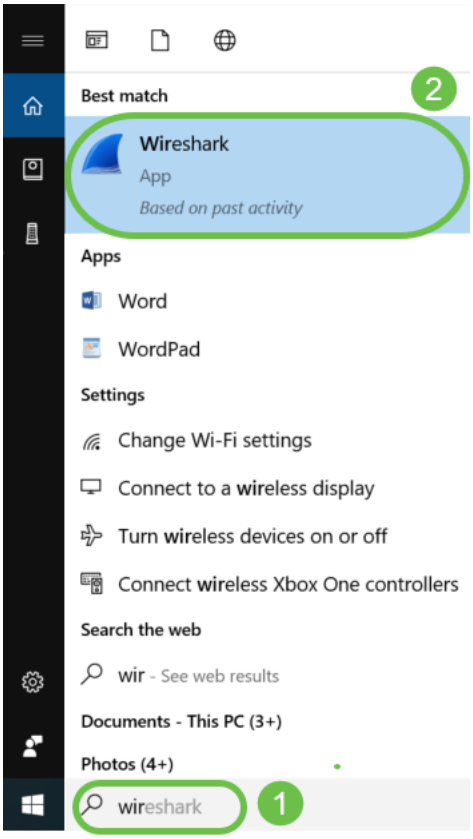
Etapa 6. Uma janela pop-up *Confirmar* abrirá para confirmar o download do arquivo e clique em **Sim**.



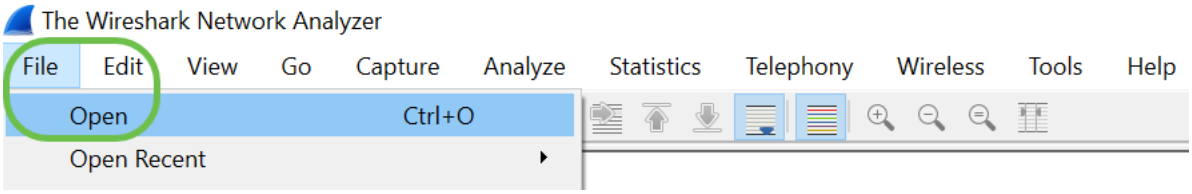
Passo 7. O arquivo de captura de pacote será baixado para o seu computador. Neste exemplo, *apcapture.pcap* é o nome do arquivo.



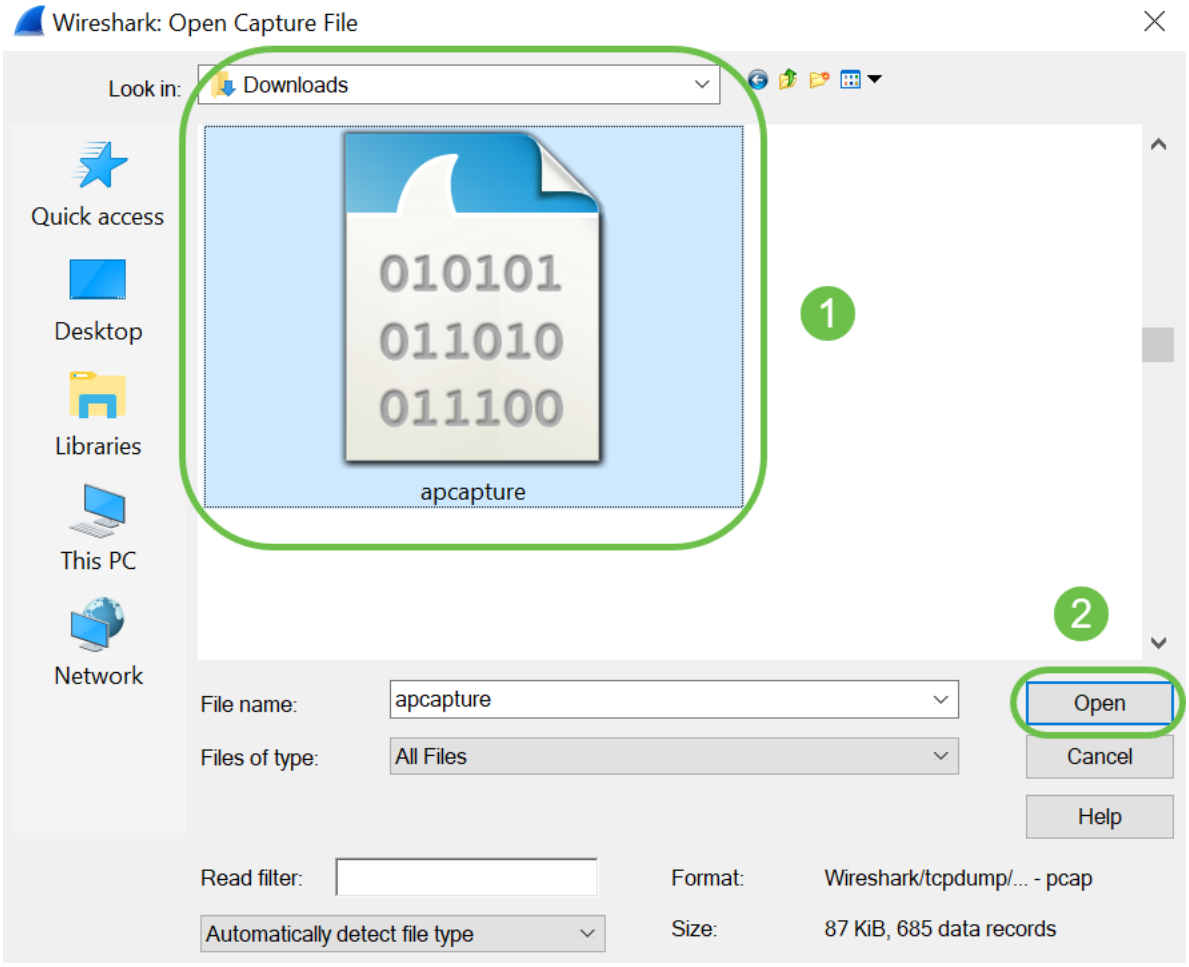
Etapa 8. Como o Wireshark já foi baixado, ele pode ser acessado digitando *Wireshark* na barra de pesquisa do Microsoft Windows e selecionando o aplicativo quando ele é uma opção.



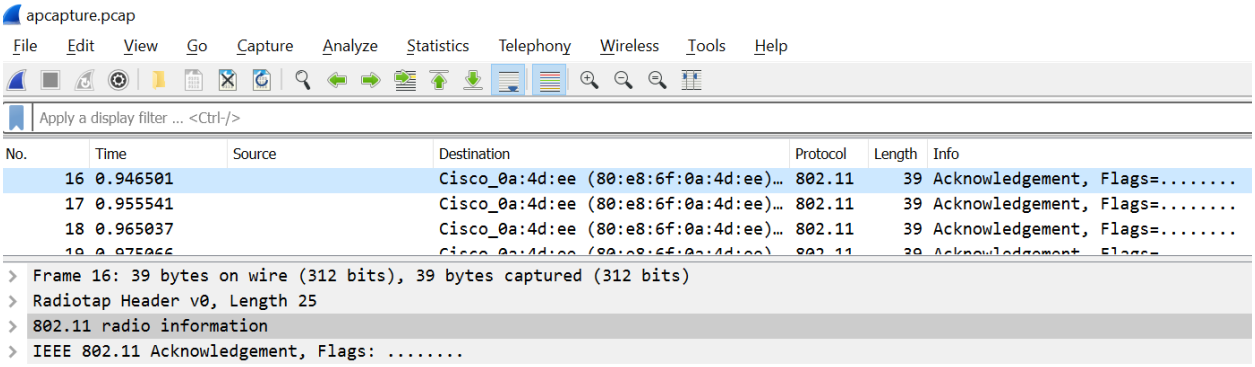
Etapa 9. Navegue até **Arquivo > Abrir**.



Etapa 10. Na nova janela pop-up, procure para localizar o arquivo, neste caso, *apcapture.pcap*. Clique em **Abrir**.



Etapa 11. O arquivo será aberto no aplicativo *Wireshark* e você poderá ver os detalhes dos pacotes.



Conclusão

Você tem seu pacote capturado e carregado no Wireshark, e agora você pode trabalhar analisando-o. Não sabe aonde ir daqui? Há muitos vídeos e artigos disponíveis online para explorar. O que você procura depende das necessidades da sua situação. Você tem isso!