Uso de Wireshark en un WAP empresarial de Cisco para el análisis de paquetes: Cargar archivo

Objetivo

En este artículo se explica cómo utilizar un punto de acceso inalámbrico (WAP) y un Wireshark empresarial de Cisco para realizar, guardar y cargar una captura de paquetes.

Introducción

Los cambios de configuración, la supervisión y la resolución de problemas son algo que el administrador de red debe tratar a menudo. Disponer de una herramienta sencilla es muy valioso. El objetivo de este artículo es sentirse más cómodo con los fundamentos de las capturas de paquetes, así como de cómo cargar un archivo en Wireshark. Si no está familiarizado con este proceso, conteste a algunas preguntas que podría haber hecho ya.

En primer lugar, Wireshark es un analizador de paquetes gratuito para cualquier persona que desee solucionar problemas en su red. Wireshark proporciona muchas opciones para la captura, así como para ordenar el tráfico mediante varios parámetros diferentes. Diríjase a Wireshark para obtener detalles sobre esta opción de código abierto.

¿Qué es una captura de paquetes?

Una captura de paquetes, también conocida como un archivo PCAP, es una herramienta que puede ser útil en la resolución de problemas. Puede registrar cada paquete enviado entre dispositivos de la red, en tiempo real. La captura de paquetes le permite profundizar en los detalles del tráfico de red, que puede incluir desde la detección de dispositivos, conversaciones de protocolo y autenticación fallida. Puede ver la ruta del flujo de tráfico específico y cada interacción entre los dispositivos en las redes seleccionadas. Estos paquetes se pueden guardar para un análisis adicional según sea necesario. Es como una radiografía del funcionamiento interno de la red a través de la transferencia de paquetes.

¿Qué tipos de paquetes se pueden capturar?

El dispositivo WAP puede capturar los siguientes tipos de paquetes:

·paquetes 802.11 recibidos y transmitidos en las interfaces de radio. Los paquetes capturados en las interfaces de radio incluyen el encabezado 802.11.

·paquetes 802.3 recibidos y transmitidos en la interfaz Ethernet.

·paquetes 802.3 recibidos y transmitidos en las interfaces lógicas internas, como las interfaces Virtual Access Points (VAP) y Wireless Distribution System (WDS).

¿Cuáles son las maneras en que se puede realizar una captura de paquetes?

Hay dos métodos de captura de paquetes disponibles:

1. *Método de captura remota*: los paquetes capturados se redirigen en tiempo real a un equipo externo que ejecuta Wireshark. Puede elegir *Stream to a Remote Host* para seleccionar el método de captura remota. Si prefiere el método de captura remota, desprotéjase Usando Wireshark en un WAP para el Análisis de Paquetes: Transfiera directamente a Wireshark.
2. *Método de captura local*: los paquetes capturados se almacenan en un archivo en el dispositivo WAP. El dispositivo WAP puede transferir el archivo a un servidor de protocolo de transferencia de archivos trivial (TFTP). El archivo tiene formato PCAP y se puede examinar mediante Wireshark. Puede elegir *Guardar archivo en este dispositivo* para seleccionar el método de captura local.

El objetivo de este artículo es cargar un archivo en Wireshark con la última interfaz gráfica de usuario (GUI). Si prefiere ver un artículo que utiliza la GUI más antigua para el método de captura local, consulte Configurar captura de paquetes para optimizar el rendimiento en un punto de acceso inalámbrico.

¿Qué hago con una captura de paquetes una vez que tengo el archivo PCAP?

La función de captura de paquetes inalámbricos permite capturar y almacenar los paquetes recibidos y transmitidos por el dispositivo WAP. Los paquetes capturados pueden entonces ser analizados por un analizador de protocolo de red para la resolución de problemas o la optimización del rendimiento. Hay muchas aplicaciones de analizador de paquetes de terceros disponibles en línea. En este artículo, nos centramos en Wireshark.

Wireshark no es propiedad de Cisco ni cuenta con el apoyo de Cisco. Para obtener ayuda, póngase en contacto con Wireshark.

Dispositivos | Versión de software

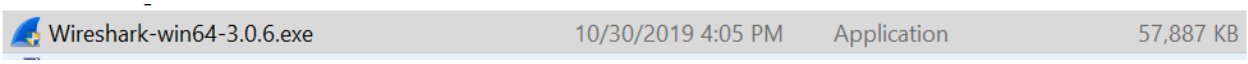
- WAP125 |1.0.2.0
- WAP150 |1.1.1.0
- WAP121 |1.0.6.8
- WAP361 |1.1.1.0
- WAP581 |1.0.2.0
- WAP571 |1.1.0.4

- WAP571E |1.1.0.4

Descargar Wireshark

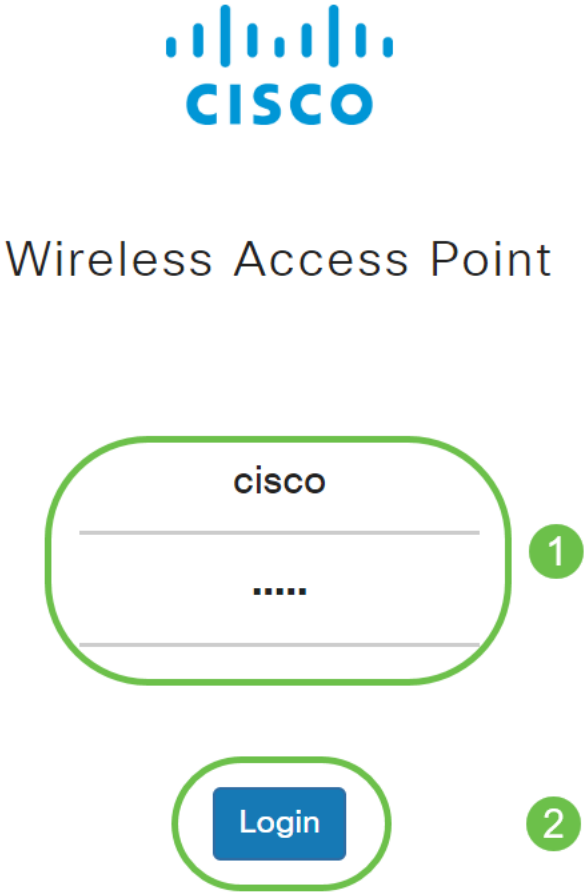
Paso 1. Vaya al sitio web de Wireshark. Haga clic en **Descarga**. Seleccione la versión adecuada para descargar. Verá el progreso de la descarga en la parte inferior izquierda de la pantalla.

Paso 2. Vaya a *Descargas* en su equipo y seleccione el archivo Wireshark para instalar su aplicación.



Inicie sesión en WAP

En el explorador Web, introduzca la dirección IP del WAP. Introduzca sus credenciales. Si es la primera vez que accede a este dispositivo o ha realizado un restablecimiento de fábrica, el nombre de usuario y la contraseña predeterminados son *cisco*. Si necesita instrucciones sobre cómo iniciar sesión, puede seguir los pasos del artículo Acceso a la utilidad basada en Web del punto de acceso inalámbrico (WAP).



Guardar una captura de paquetes en un PC y cargarla en

Wireshark

Paso 1. Vaya a **Solución de problemas > Captura de paquetes**.

Asegúrese de que **Save File on this Device** esté seleccionado para el *Método de captura de paquetes*.

Configure estos parámetros:

·*Interface*: Introduzca un tipo de interfaz de captura para la captura de paquetes:

·*Ethernet*: tráfico 802.3 en el puerto Ethernet.

·*Radio 1 (5 GHz) / Radio 2 (2,4 GHz)* - Tráfico 802.11 en la interfaz de radio.

Duración: introduzca la duración en segundos de la captura. El intervalo es de 10 a 3600. El valor predeterminado es 60.

Tamaño máximo de archivo: introduzca el tamaño máximo permitido para el archivo de captura en kilobytes (KB). El rango va de 64 a 4096. El valor predeterminado es 1024.

Hay dos modos para la captura de paquetes.

·*Todo el tráfico inalámbrico*: captura todos los paquetes inalámbricos.

·*Tráfico hacia/desde este AP* - Captura los paquetes enviados desde el AP o recibidos por el AP.

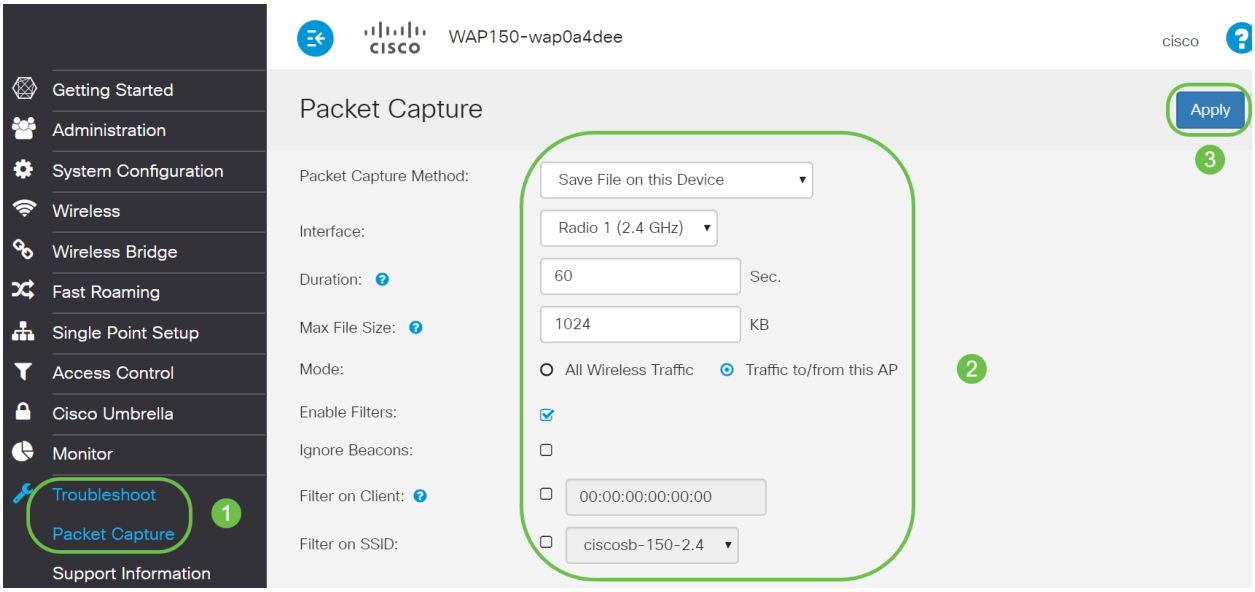
Haga clic en **Activar filtros**. Hay tres casillas de verificación disponibles, *Ignorar balizas, Filtrar en cliente* y *Filtrar en SSID*.

·*Ignore Beacons* - Habilite o deshabilite la captura de balizas 802.11 detectadas o transmitidas por la radio. Las tramas de baliza son tramas de broadcast que llevan información relativa a una red. El propósito de una baliza es anunciar la red inalámbrica existente. Si no busca este tipo de tráfico, puede seleccionar Ignorar balizas.

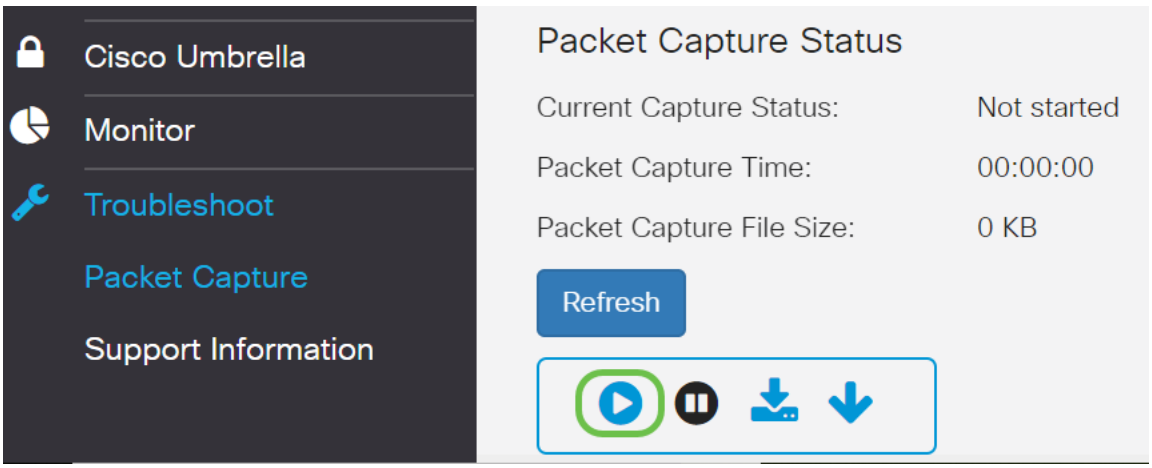
·*Filter on Client*: especifica la dirección MAC para el filtro de cliente WLAN. Tenga en cuenta que el filtro Cliente sólo está activo cuando se realiza una captura en una interfaz 802.11.

·*Filter on SSID*: seleccione un nombre SSID para la captura de paquetes.

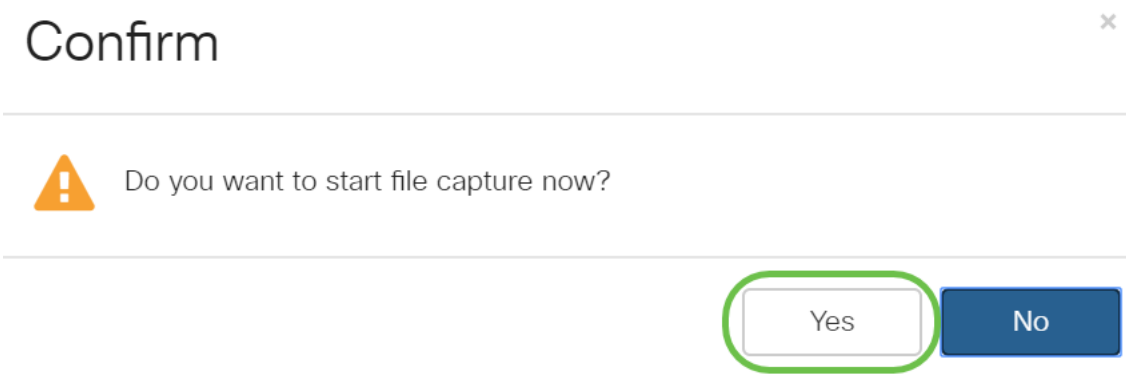
Haga clic en **Aplicar** para guardar en la configuración de inicio.



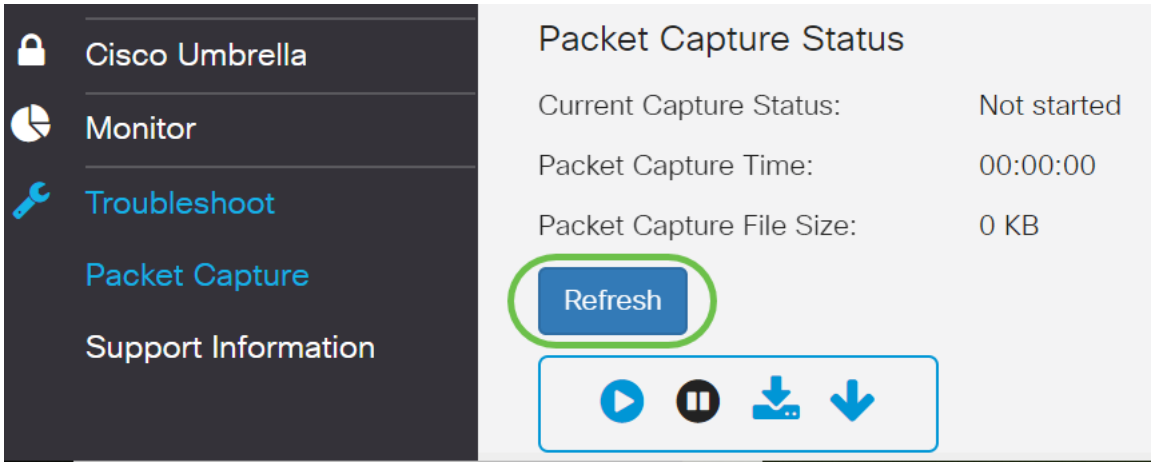
Paso 2. Haga clic en el icono **Iniciar captura**.



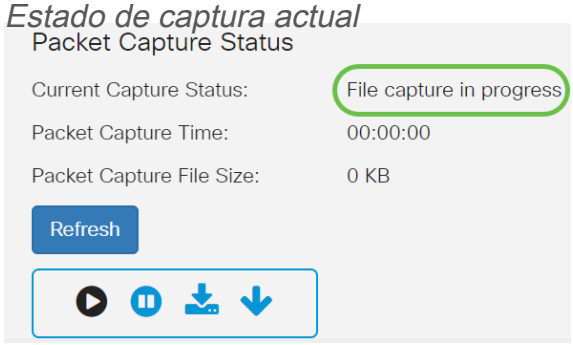
Paso 3. Se abrirá una ventana emergente *Confirm* para obtener la confirmación de descargar el archivo, haga clic en **Yes** para iniciar la descarga del archivo.



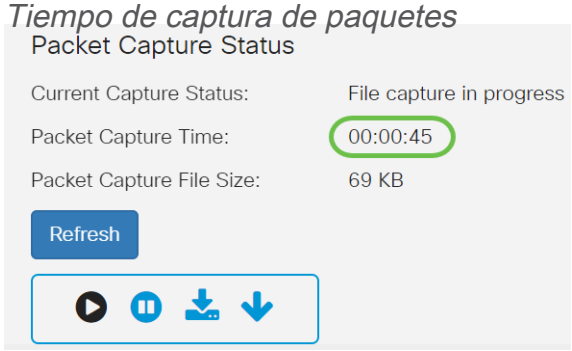
Paso 4. Haga clic en **Actualizar** para obtener el *Estado de captura de paquetes* que contiene los siguientes datos:



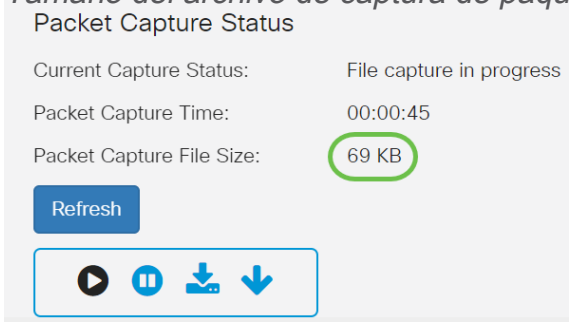
1. *Estado de captura actual*



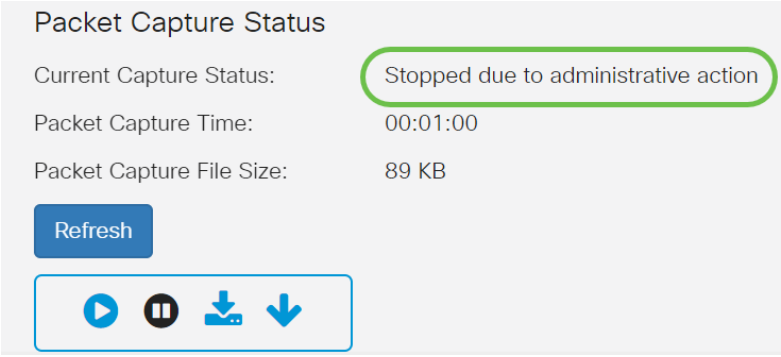
2. *Tiempo de captura de paquetes*



3. *Tamaño del archivo de captura de paquetes*

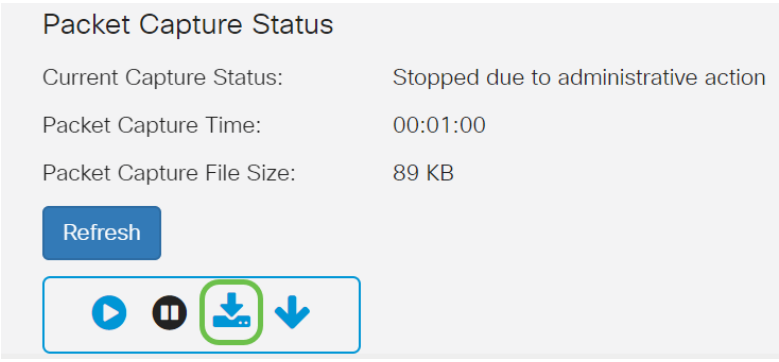


4. En el modo *Captura de archivos de paquetes*, el dispositivo WAP almacena los paquetes capturados en el sistema de archivos de memoria de acceso aleatorio (RAM). Después de la activación, la captura de paquetes continúa hasta que ocurre uno de estos eventos:
   ·El tiempo de captura alcanza la duración configurada.
   ·El archivo de captura alcanza su tamaño máximo.
   ·El administrador detiene la captura.

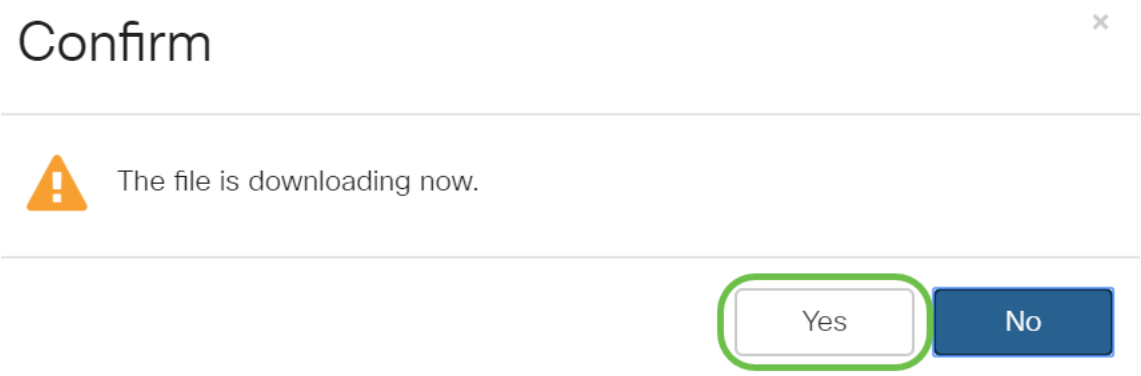


El archivo de captura de paquetes se guardará en el AP hasta que reinicie el AP.

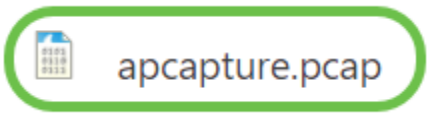
Paso 5. Haga clic en el icono **Descargar a este dispositivo** para descargar el archivo capturado recientemente.



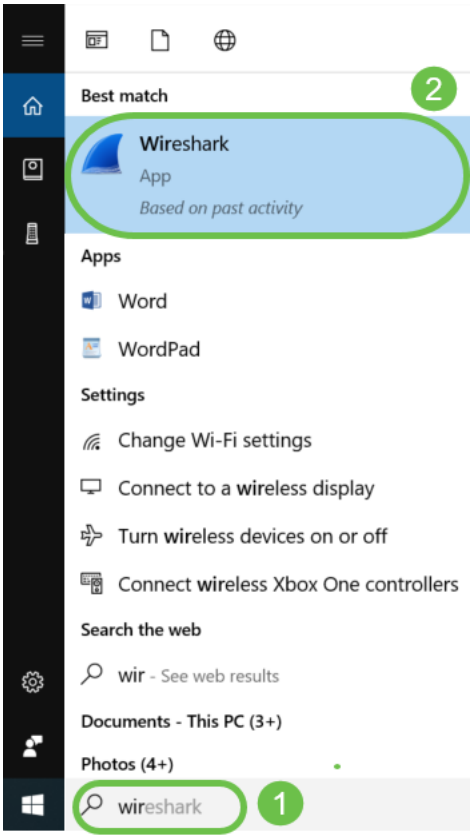
Paso 6. Se abrirá una ventana emergente *Confirm* para confirmar la descarga del archivo, haga clic en **Yes**.



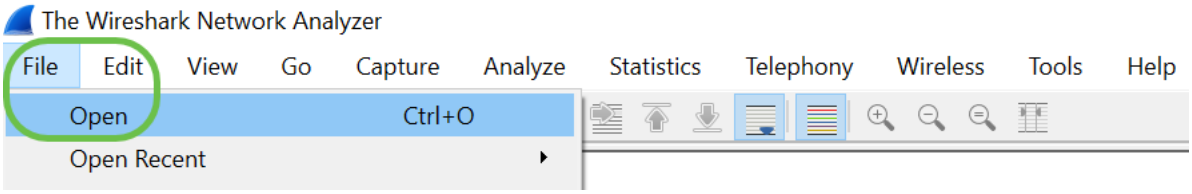
Paso 7. El archivo de captura de paquetes se descargará en el ordenador. En este ejemplo, *apcapture.pcap* es el nombre del archivo.



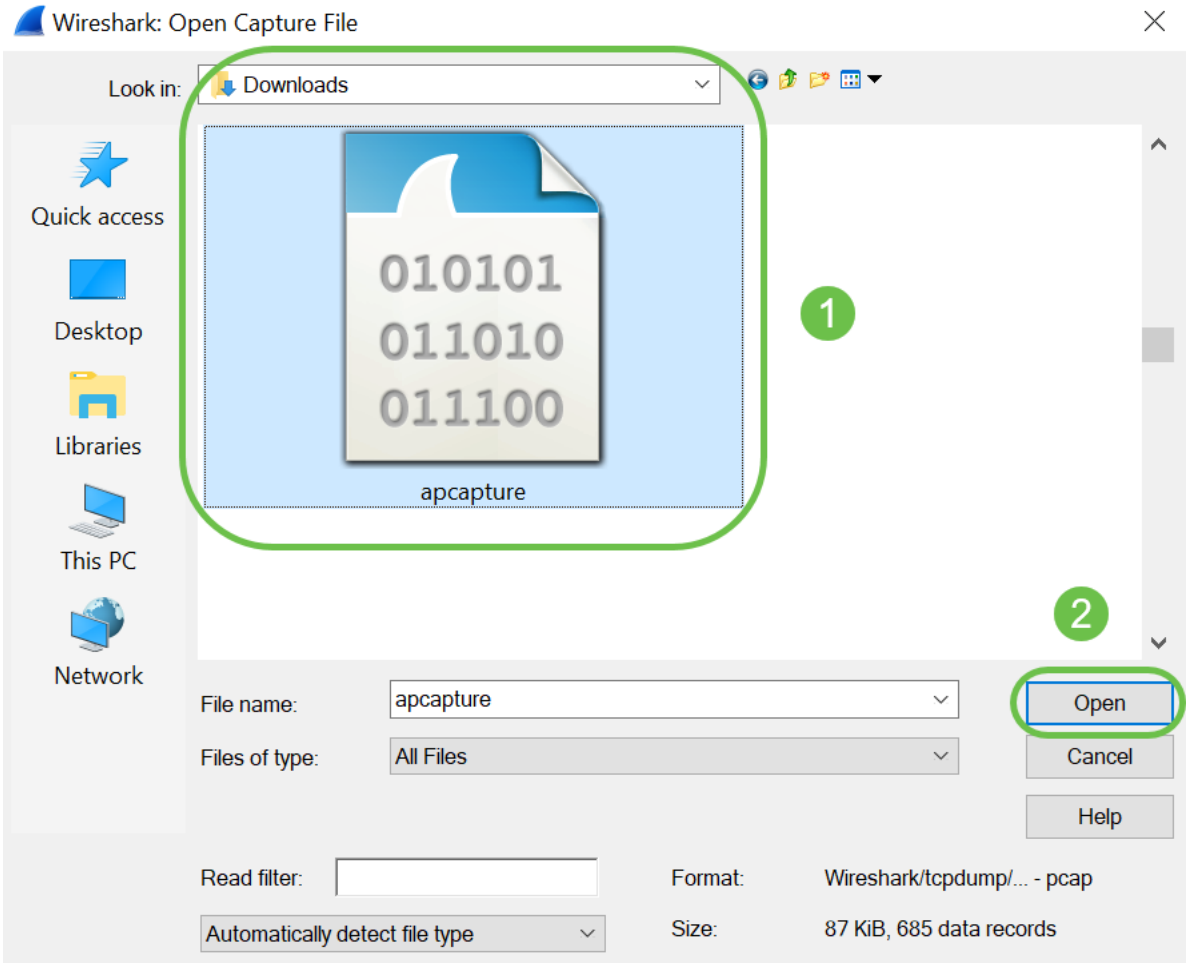
Paso 8. Dado que Wireshark ya se ha descargado, se puede acceder a él escribiendo *Wireshark* en la barra de búsqueda de Microsoft Windows y seleccionando la aplicación cuando se trata de una opción.



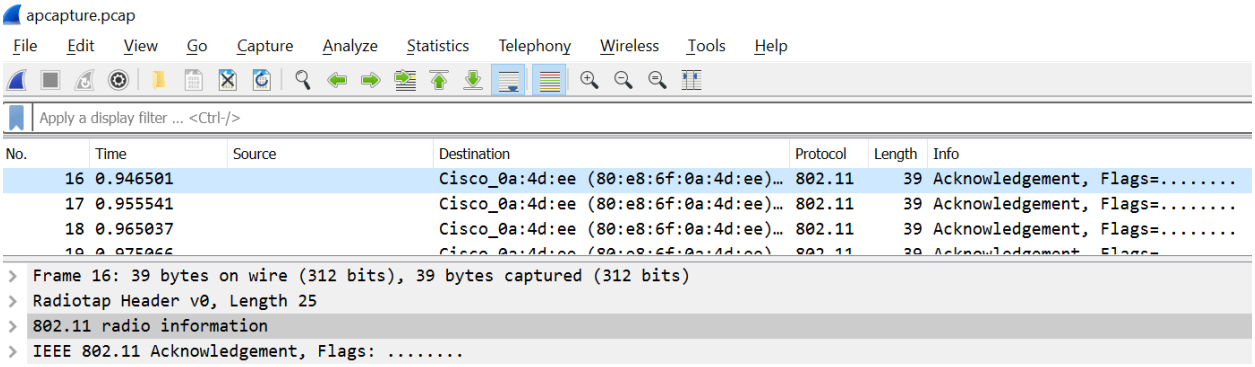
Paso 9. Vaya a **Archivo > Abrir**.



Paso 10. En la nueva ventana emergente, busque el archivo, en este caso, *apcapture.pcap*. Haga clic en **Abrir**.



Paso 11. El archivo se abrirá en la aplicación *Wireshark* y podrá ver los detalles de los paquetes.



Conclusión

Ha capturado y cargado el paquete en Wireshark, ahora puede trabajar analizándolo. ¿No está seguro de dónde ir desde aquí? Hay muchos videos y artículos disponibles en línea para explorar. Lo que busca depende de las necesidades de su situación. ¡Lo tienes!