# Capture y analice el tráfico de red con Wireshark para diagnósticos

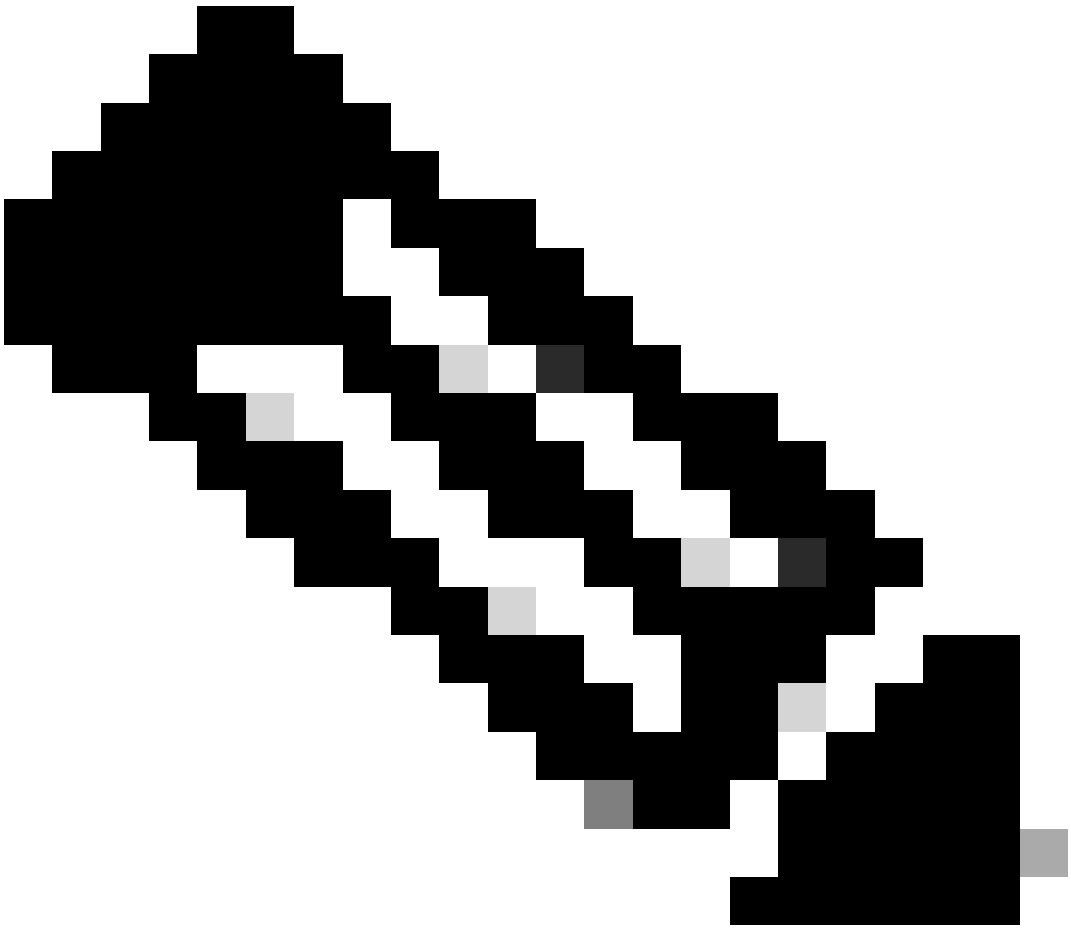
## Contenido

## Introducción

Este documento describe cómo utilizar Wireshark para capturar y analizar el tráfico de red con fines de diagnóstico.

## Overview

Wireshark es una aplicación gratuita que puede utilizar para leer y analizar capturas de paquetes (también llamada "volcados TCP"). Las capturas de paquetes revelan todas las comunicaciones a través de un adaptador de red en el nivel de paquete, lo que permite ver DNS, HTTP, ping y otros tipos de tráfico. Las capturas de paquetes son especialmente valiosas como paso de diagnóstico para la resolución de problemas en profundidad y, con la introducción de SIG, ahora son una parte fundamental del proceso de diagnóstico.



> Nota: Wireshark captura todo el tráfico del adaptador seleccionado. Debido a que las capturas de paquetes a menudo contienen información personalmente identificable (PII), utilice siempre un método seguro, como un enlace de cuadro, para compartir archivos de captura con asistencia.

## Obtener Wireshark

Puede descargar Wireshark para Windows, macOS o Linux en: https://www.wireshark.org/

## Recopilación de una captura de paquetes

1. Elija el adaptador de red conectado a Internet e inicie la captura en Wireshark.
2. Durante la captura, reproduzca el problema que desea diagnosticar.
3. Detenga la captura cuando haya terminado y guarde el archivo como a `.pcap`.

# Puertos y protocolos básicos

- La mayoría de los paquetes se comunican en los protocolos de capa de transporte TCP o UDP
  - Por ejemplo, "DNS" se ejecuta "sobre" UDP de forma predeterminada. Cambia a UDP si falla TCP.
- HTTP y DNS son protocolos comunes que se ejecutan en una combinación de protocolo de transporte + puertos.

| Protocolo de capa de transporte | Puerto | Nombre de protocolo | Uso |
|---|---|---|---|
| TCP | 22 | SSH | Acceso remoto a VA |
| TCP | 25 | SMTP | Supervisión VA |
| IP | 50 | ESP (carga útil de seguridad de encapsulación) | Confidencialidad, integridad de los datos, autenticación de origen |
| IP | 51 | AH (Encabezado de autenticación) | Integridad de datos, autenticación de origen |
| UDP | 53 | DNS | DNS predeterminado |
| TCP | 53 | DNS | Fail-Over de DNS |
| TCP | 80 | HTTP | Tráfico web (sin cifrar), API |
| UDP | 123 | NTP | VA Time Sync |
| TCP | 443 | HTTPS | Tráfico web cifrado, API, conectores AD a VA |
| UDP | 443 | HTTPS | Consultas de DNS cifrado RC |
| UDP | 500 | IKE | Negociaciones de túnel IPsec |
| UDP | 4500 | NAT-T | NAT traversal para túneles IPsec |
| TCP | 8080 | HTTP | Conectores AD para comunicaciones VA |

Conocer los nombres de protocolo, los puertos y sus usos le ayuda a identificar y analizar el tráfico relevante en Wireshark.

# Operadores básicos

Al crear cadenas de filtros en Wireshark, utilice estos operadores:

- `==`: Igual a (Ejemplo:`ip.dst==1.2.3.4`)
- `!=`: Distinto de (Ejemplo:`ip.dst!=1.2.3.4`)
- `&&`: Y (Ejemplo:`ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`: O (Ejemplo:`ip.dst==1.2.3.4 || ip.dst==1.2.3.5`)

Para ver las opciones de filtro avanzadas, consulte la documentación de Wireshark: 6.4. Creación

de expresiones de filtro de visualización

## Filtros

Las capturas de paquetes pueden contener miles de paquetes. Los filtros le ayudan a centrarse en tipos de tráfico específicos:

- Por protocolo:
  - `dns`: muestra solo el tráfico DNS
  - `http || dns`: muestra el tráfico HTTP o DNS
- Por dirección IP:
  - `ip.addr==<IP>`: todo el tráfico hacia/desde`<IP>`
  - `ip.src==<IP>`: todo el tráfico de`<IP>`
  - `ip.dst==<IP>`: todo el tráfico a`<IP>`
- Miscelánea:
  - `tcp.flags.reset==1`: comprobar si se restablece TCP (tiempos de espera)
  - `dns.qry.name contiene "[dominio]"`: consultas DNS que coinciden con un dominio
  - `tcp.port==80 || udp.port==80`: tráfico TCP o UDP en el puerto 80

## Visualización y análisis de paquetes

Después de localizar un paquete, expanda los segmentos dentro de Wireshark para analizar los detalles. La familiaridad con la estructura del protocolo le ayuda a interpretar estos detalles e incluso a reconstruir los datos si es necesario.

## Seguimiento de un flujo de datos

Utilice la lista de paquetes para localizar pares de solicitud y respuesta. Haga clic con el botón derecho del ratón en un paquete y seleccione Seguir > Transmisión TCP, Transmisión UDP, Transmisión TLS o Transmisión HTTP para ver la solicitud relacionada y la secuencia de respuesta.

- Esto resulta más útil con protocolos que tienen varios intercambios (por ejemplo, HTTP) que con protocolos de solicitud única (por ejemplo, DNS).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).