

Práctica de laboratorio 8.3.2 Realización de una captura de red con Wireshark

Objetivos

- Realizar una captura del tráfico de la red con Wireshark para familiarizarse con el entorno y la interfaz de Wireshark.
- Analizar el tráfico que va hacia el servidor Web
- Crear un filtro para limitar la captura de red a los paquetes ICMP.
- Hacer ping en un host remoto para observar cómo funciona el filtro de paquete ICMP durante la captura de red.

Información básica / Preparación

En esta práctica de laboratorio instalará Wireshark, una conocida herramienta de monitoreo y analizador del protocolo de red. Wireshark captura todos los paquetes que envía y recibe la NIC de la computadora. Puede instalarse en el laboratorio o en una PC en su casa. Lo utilizará para rastrear y visualizar los distintos tipos de tráfico y protocolos de red. Wireshark antes se denominaba Ethereal.

El software Wireshark es freeware y se puede obtener de www.wireshark.org. El instalador del software, `wireshark-setup-0.99.5.exe`, debería estar en el servidor local Networking Academy.

Puede llevar a cabo esta práctica de laboratorio en forma individual, con un compañero o en equipo.

Se necesitan los siguientes recursos:

- Una PC con Windows XP, con red Ethernet y por lo menos dos hosts.
- Software Wireshark versión 0.99.5 (o la versión más reciente)
- Conectividad a Internet (opcional pero conveniente)
- Acceso al indicador de comando de la PC
- Acceso a la configuración TCP/IP de red de la PC

Paso 1: Instalar e iniciar Wireshark

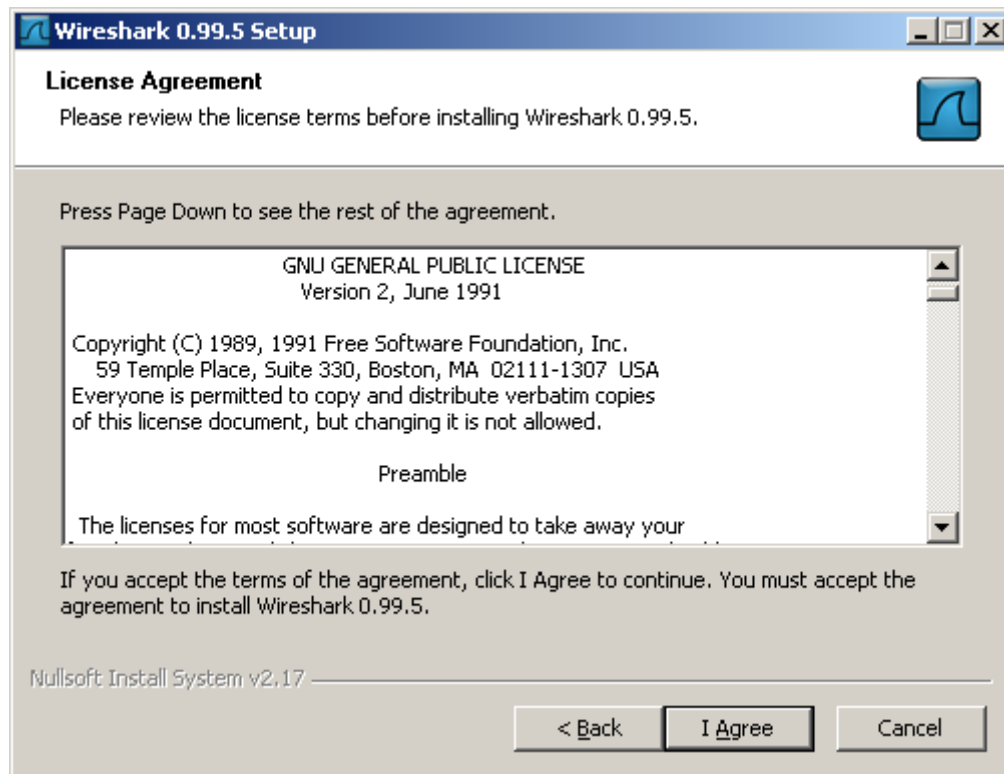
Si Wireshark se cargó previamente en la PC, vaya a la carpeta del programa Wireshark **Inicio > Todos los programas > Wireshark > Wireshark** y haga clic en el ícono de la aplicación.

Si Wireshark no se hubiese instalado, siga estos pasos:

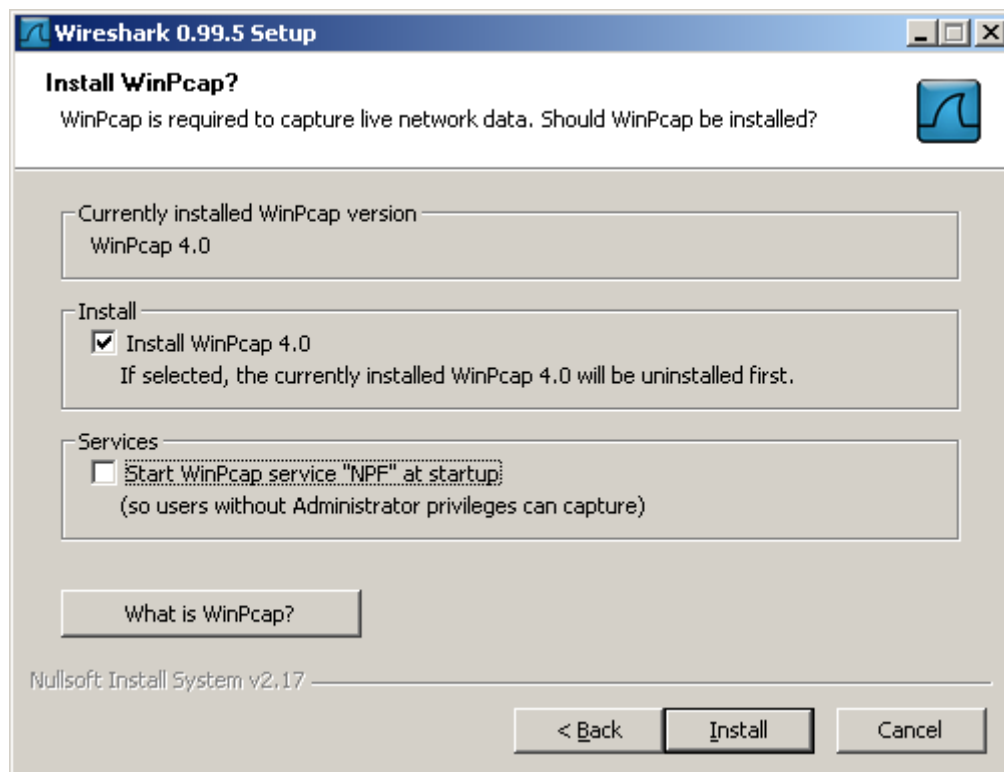
- Dada la ruta de red local hasta el instalador del software Wireshark, wireshark-setup-0.99.5.exe, descargue el instalador en el escritorio de la PC.
- Haga doble clic en el instalador, siga las indicaciones del instalador y acepte las configuraciones predeterminadas.



- 1) Haga clic en **I Agree (Acepto)**.



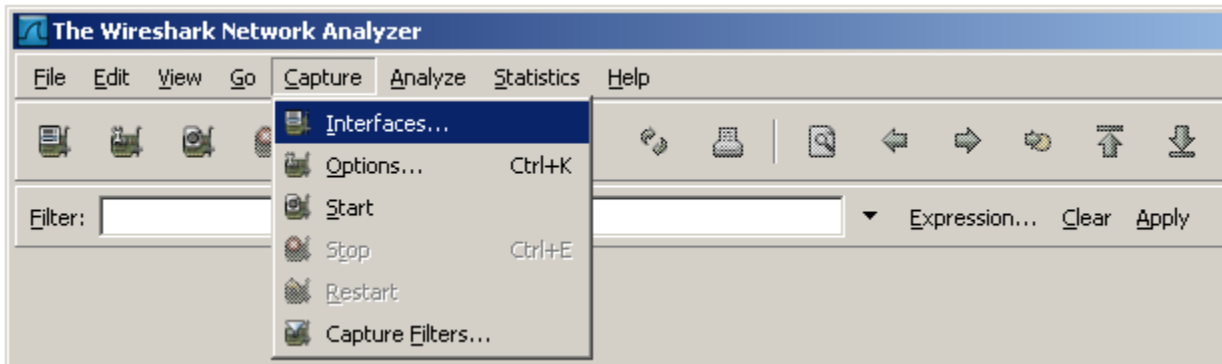
- 2) Asegúrese de instalar WinPcap en la PC. WinPcap incluye un controlador para admitir la captura de paquetes. Wireshark utiliza esta biblioteca para capturar datos de la red activa con Windows.



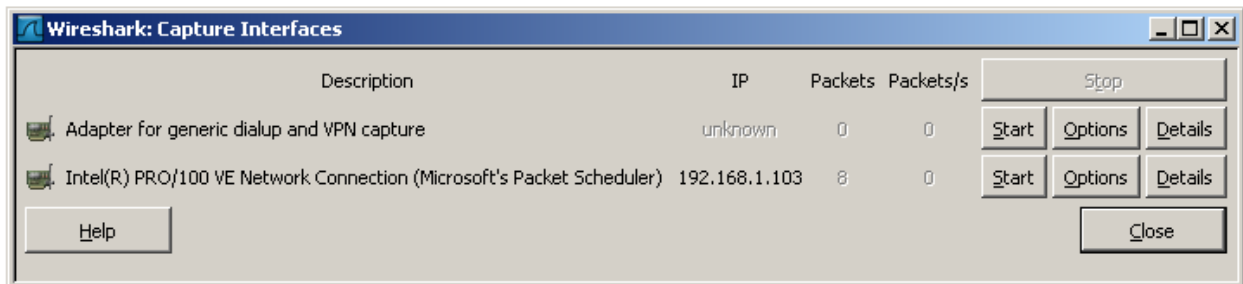
- c. Haga clic en **Install (Instalar)** y siga las indicaciones hasta finalizar el proceso de la instalación.
- d. Una vez instalado el software, haga clic en la casilla de verificación para iniciar Wireshark.

Paso 2: Seleccionar una interfaz para usar para la captura de paquetes

- a. Inicie la aplicación Wireshark.
- b. En el menú **Capture (Captura)**, haga clic en **Interfaces**.

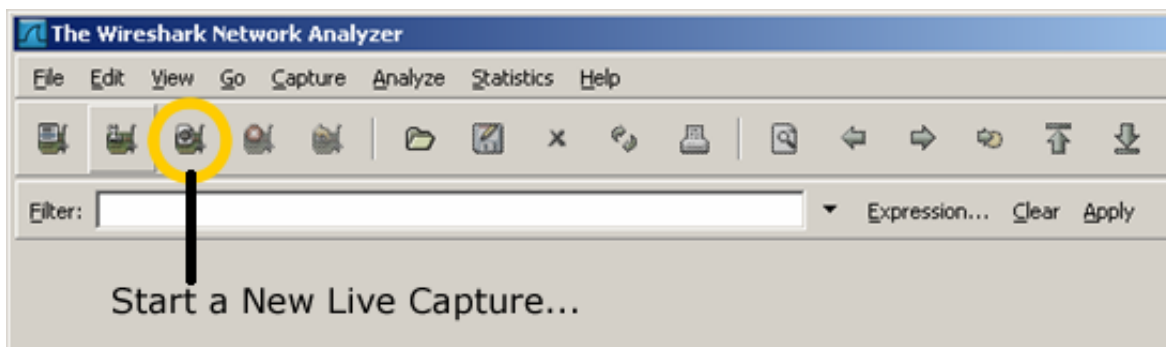


- 3) Haga clic en el botón **Start (Inicio)** para la interfaz Ethernet (NIC) que desea utilizar para capturar el tráfico de red.



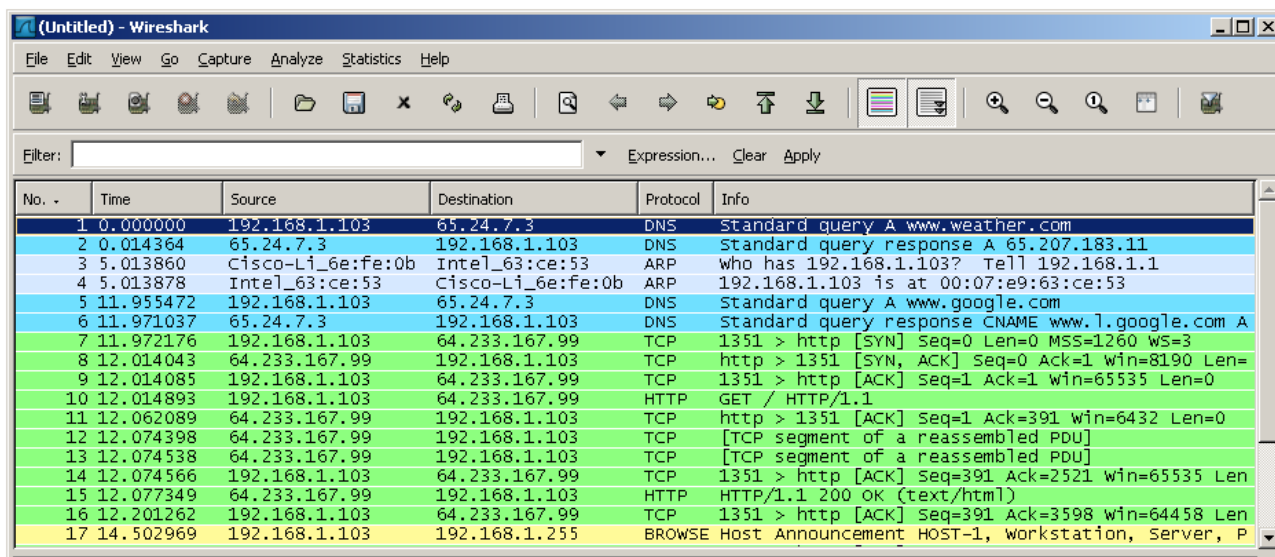
Paso 3: Iniciar una captura de red

- a. Desplácese a través de los menús y visualice la barra de herramientas de la interfaz para inicio de Wireshark.
- b. Haga clic en el botón **New Live Capture (Nueva captura en vivo)** y observe la información que reúne Wireshark. Permita que la captura continúe durante algunos minutos para que pueda ver los distintos tipos de tráfico en la red.



Paso 4: Analizar la información del tráfico Web (opcional)

- Si hubiera conectividad a Internet disponible, abra un explorador y vaya a www.google.com. Minimice la ventana de Google y vuelva a Wireshark. Debería ver el tráfico capturado de manera similar a la que se muestra a continuación. Localice las columnas **Source** (Origen), **Destination** (Destino) y **Protocol** (Protocolo) en la pantalla de Wireshark.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.103	65.24.7.3	DNS	Standard query A www.weather.com
2	0.014364	65.24.7.3	192.168.1.103	DNS	Standard query response A 65.207.183.11
3	5.013860	Cisco-Li_6e:fe:0b	Intel_63:ce:53	ARP	who has 192.168.1.103? Tell 192.168.1.1
4	5.013878	Intel_63:ce:53	Cisco-Li_6e:fe:0b	ARP	192.168.1.103 is at 00:07:e9:63:ce:53
5	11.955472	192.168.1.103	65.24.7.3	DNS	Standard query A www.google.com
6	11.971037	65.24.7.3	192.168.1.103	DNS	Standard query response CNAME www.l.google.com A
7	11.972176	192.168.1.103	64.233.167.99	TCP	1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
8	12.014043	64.233.167.99	192.168.1.103	TCP	http > 1351 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=
9	12.014085	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10	12.014893	192.168.1.103	64.233.167.99	HTTP	GET / HTTP/1.1
11	12.062089	64.233.167.99	192.168.1.103	TCP	http > 1351 [ACK] Seq=1 Ack=391 Win=6432 Len=0
12	12.074398	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
13	12.074538	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
14	12.074566	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=2521 Win=65535 Len=
15	12.077349	64.233.167.99	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
16	12.201262	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=3598 Win=64458 Len=
17	14.502969	192.168.1.103	192.168.1.255	BROWSE	Host Announcement HOST-1, Workstation, Server, P

- La conexión con el servidor Google comienza con una consulta para que el servidor DNS se fije en la dirección IP del servidor. La dirección IP del servidor de destino es muy probable que empiece con 64.x.x.x. ¿Cuál es el origen y el destino del primer paquete enviado al servidor Google?

- Abra otra ventana del explorador y vaya a la base de datos **ARIN Whois** en <http://www.arin.net/whois/> o utilice otra herramienta de búsqueda **whois** e ingrese la dirección IP del servidor destino. ¿A qué organización está asignada esta dirección IP?

_____ Debería ser Google.

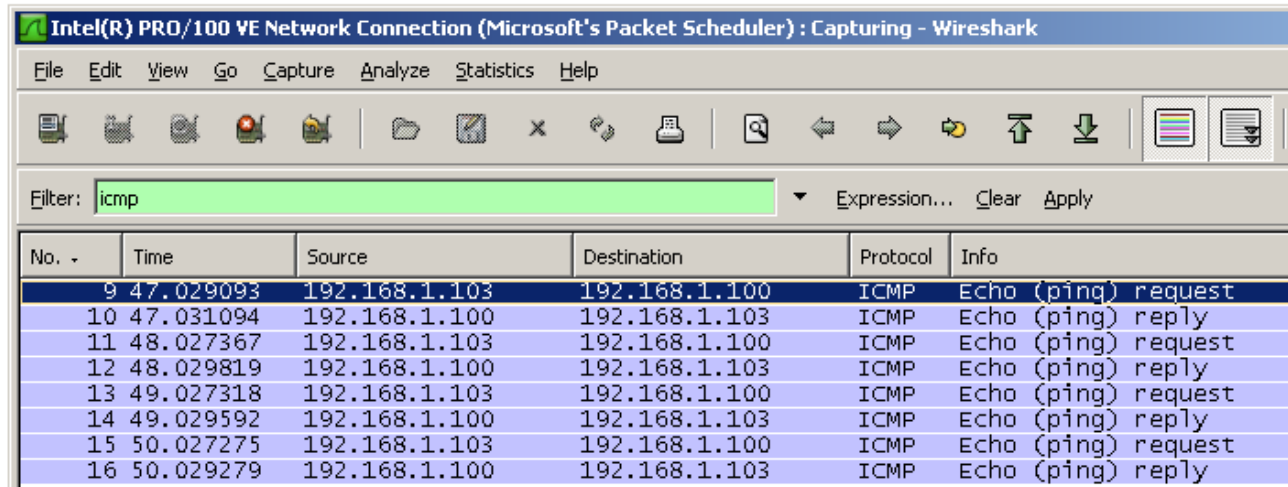
- ¿Cuáles son los protocolos que se utilizan para establecer la conexión con el servidor Web y entregar la página Web a su host local? _____ Protocolos TCP y HTTP.

- ¿Cuál es el color que se utiliza para resaltar el tráfico entre su host y el servidor Web de Google? _____ Puede variar pero en la pantalla anterior se muestra verde claro.

Paso 5: Filtrar una captura de red

- Abra una ventana del indicador de comandos al hacer clic en **Inicio > Todos los programas > Ejecutar** y al escribir **cmd**. Otra alternativa es hacer clic en **Inicio > Todos los programas > Accesorios** y seleccionar **Indicador de comandos**.
- Haga ping en la dirección IP del host de su red local y observe la ventana de captura de Wireshark. Desplácese hacia arriba y hacia abajo en la ventana en la que se muestra el tráfico. ¿Qué tipos de protocolos están en uso?

- c. En el cuadro de texto **Filter (Filtro)**, escriba **icmp** y haga clic en **Apply (Aplicar)**. El Protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol) es el protocolo que utiliza el **ping** para comprobar la conectividad de la red con otro host.



No. -	Time	Source	Destination	Protocol	Info
9	47.029093	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
10	47.031094	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply
11	48.027367	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
12	48.029819	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply
13	49.027318	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
14	49.029592	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply
15	50.027275	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
16	50.029279	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply

- d. Cuando en el cuadro de texto **Filter (Filtro)** se escribe icmp, ¿qué tipo de tráfico se muestra?
- _____
- e. Haga clic en el botón **Filter (Filtro)**: botón **Expression (Expresión)** en la ventana Wireshark. Desplácese hasta la lista y visualice ahí las posibilidades de filtrado. ¿Están TCP, HTTP, ARP y otros protocolos en la lista? _____

Paso 6: Reflexión

- a. Hay cientos de filtros que se incluyen en la opción Filter: Expression (Filtro: Expresión). Es posible que, en una red más grande, haya enormes cantidades y tipos diferentes de tráfico. ¿Qué tres filtros de esa larga lista cree usted que pueden serle de mayor utilidad a un administrador de red?
- _____
- b. ¿Es Wireshark una herramienta para el monitoreo de red fuera de banda o dentro de banda? _____ Dentro de banda. Justifique su respuesta.
- _____
- _____