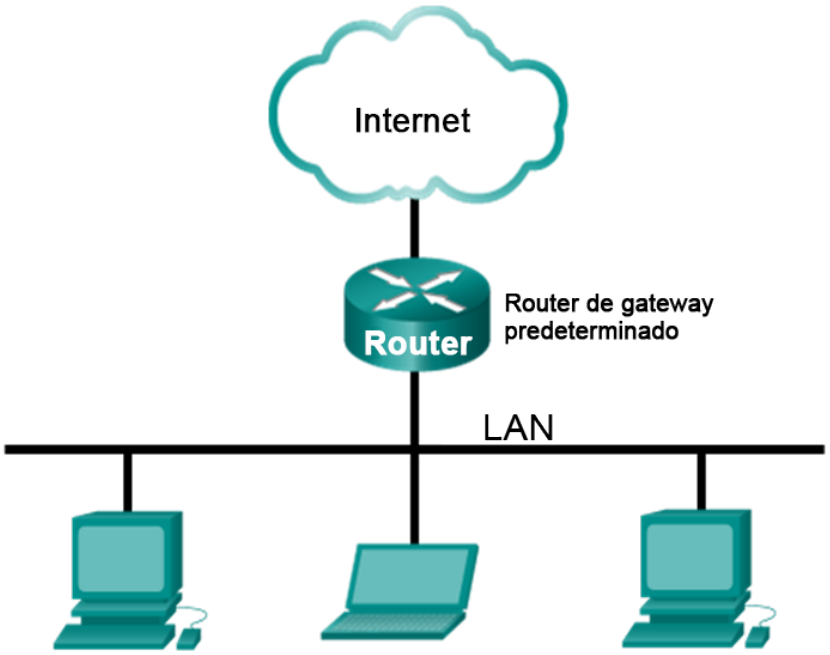
Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Descargar e instalar Wireshark (Optativo)

Parte 2: Capturar y analizar datos ICMP locales en Wireshark

- Inicie y detenga la captura de datos del tráfico de ping a los hosts locales.
- Ubicar la información de la dirección MAC y de la dirección IP en las PDU capturadas.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

- Inicie y detenga la captura de datos del tráfico de ping a los hosts remotos.
- Ubicar la información de la dirección MAC y de la dirección IP en las PDU capturadas.
- Explicar por qué las direcciones MAC para los hosts remotos son diferentes de las direcciones MAC para los hosts locales.

Información básica/Situación

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación. Mientras los streams de datos van y vienen por la red, el programa detector “captura” cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con la RFC correcta u otras especificaciones.

Wireshark es una herramienta útil para cualquier persona que trabaje con redes y se puede utilizar con la mayoría de las prácticas de laboratorio en los cursos de CCNA para tareas de análisis de datos y resolución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. En esta práctica de laboratorio, usará Wireshark para capturar direcciones IP del paquete de datos ICMP y direcciones MAC de la trama de Ethernet.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP, con acceso a Internet)
- Se utilizarán PC adicionales en una red de área local (LAN) para responder a las solicitudes de ping.

Nota para el instructor: esta práctica de laboratorio supone que el alumno utiliza una PC con acceso a Internet y puede hacer ping a otras PC en la red de área local. Si usa PC de la academia, el instructor puede preferir instalar previamente Wireshark en las PC y recomendar a los alumnos que lean la parte 1 y realicen las partes 2 y 3 de la práctica de laboratorio. El procedimiento de instalación de Wireshark y las capturas de pantalla pueden cambiar según la versión de Wireshark. En esta práctica de laboratorio, se utiliza Wireshark v1.8.3 para Windows 7 (64 bits).

El uso de un programa detector de paquetes como Wireshark se puede considerar una infracción de la política de seguridad del lugar de estudios. Se recomienda obtener permiso para realizar esta práctica de laboratorio antes de ejecutar Wireshark. Si el uso de un programa detector de paquetes como Wireshark constituye un problema, se sugiere que el instructor asigne la práctica de laboratorio como tarea para el hogar o realice una demostración explicativa.

Parte 1: Descargar e instalar Wireshark (optativo)

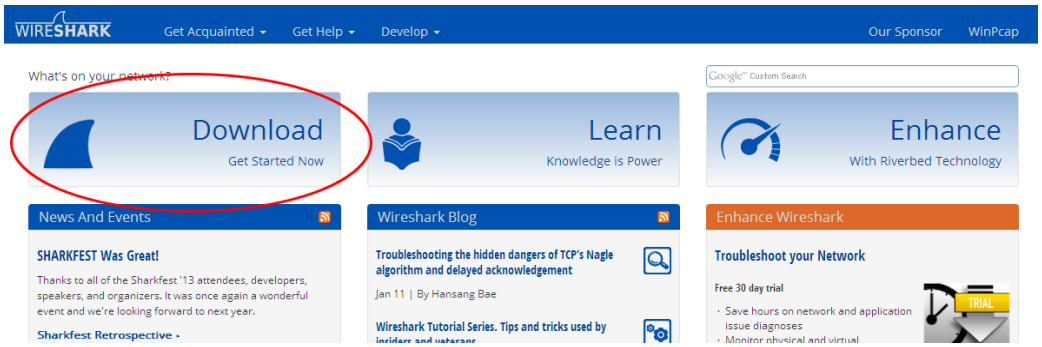
Wireshark se convirtió en el programa detector de paquetes estándar del sector que utilizan los ingenieros de redes. Este software de código abierto está disponible para muchos sistemas operativos diferentes, incluidos Windows, MAC y Linux. En la parte 1 de esta práctica de laboratorio, descargará e instalará el programa de software Wireshark en la PC.

Nota: si Wireshark ya está instalado en la PC, puede saltear la parte 1 e ir directamente a parte 2. Si Wireshark no está instalado en la PC, consulte con el instructor acerca de la política de descarga de software de la academia.

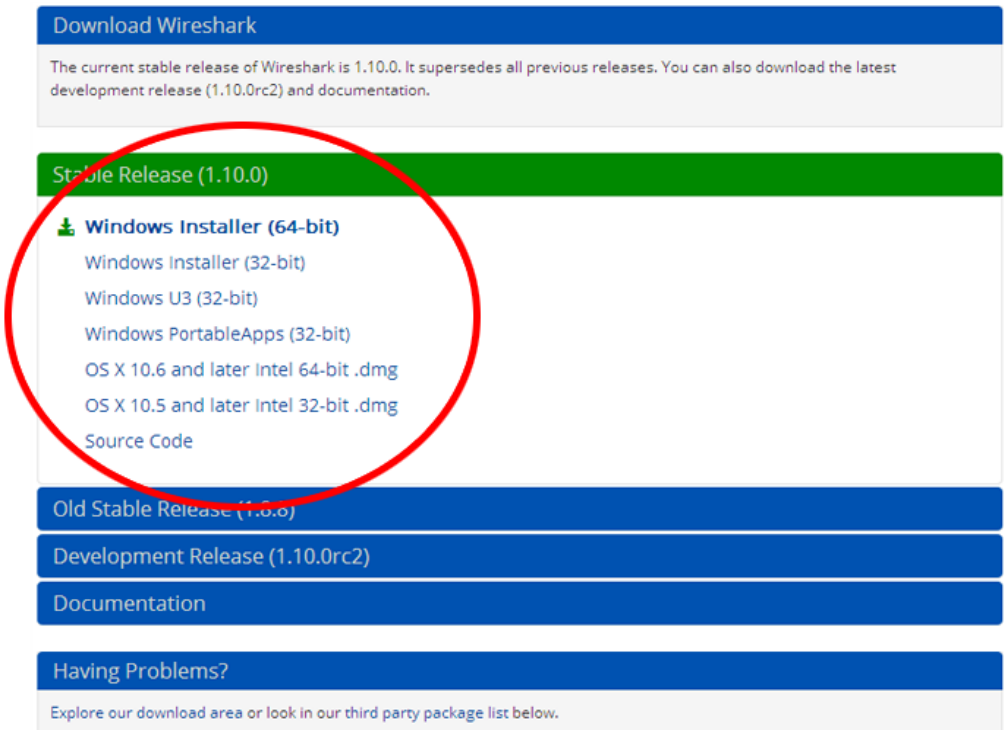
Paso 1: Descargar Wireshark

a. Wireshark se puede descargar de www.wireshark.org.

b. Haga clic en **Download Wireshark** (Descargar Wireshark).



c. Elija la versión de software que necesita según la arquitectura y el sistema operativo de la PC. Por ejemplo, si tiene una PC de 64 bits con Windows, seleccione **Windows Installer (64-bit)** (Instalador de Windows [64 bits]).

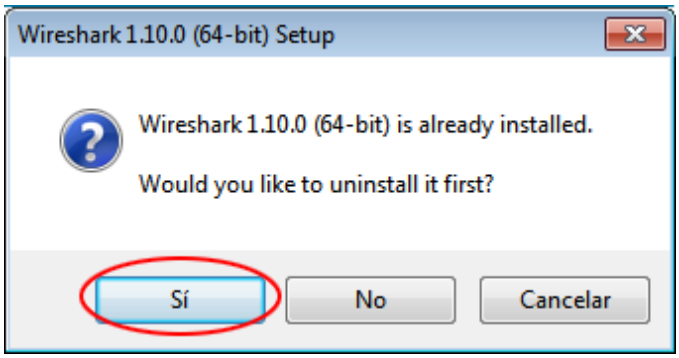


Después de realizar la selección, comienza la descarga. La ubicación del archivo descargado depende del explorador y del sistema operativo que utiliza. Para usuarios de Windows, la ubicación predeterminada es la carpeta **Descargas**.

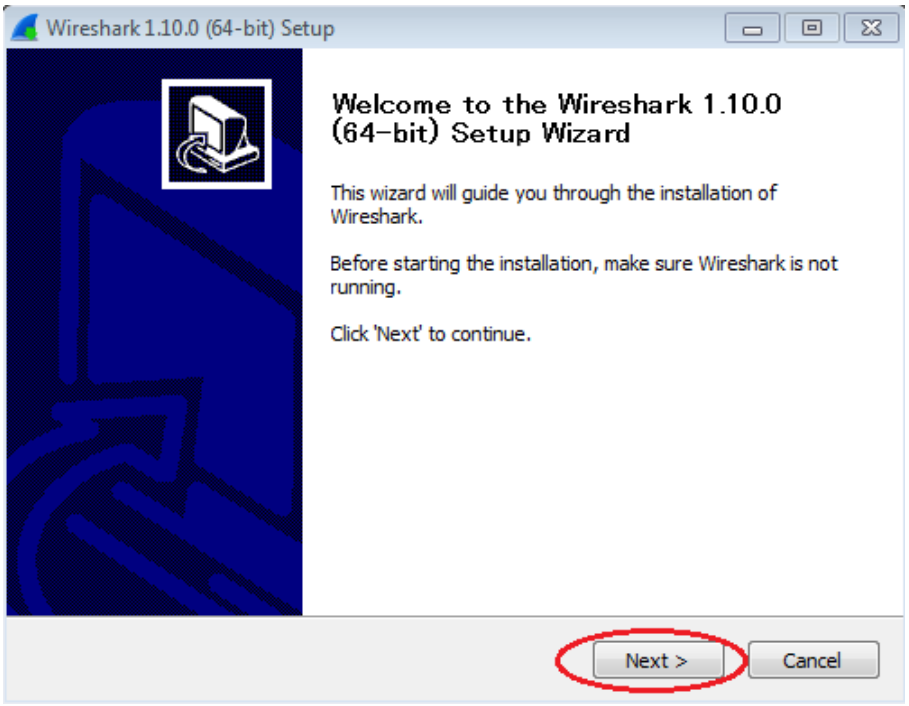
Paso 2: Instalar Wireshark

a. El archivo descargado se denomina **Wireshark-win64-x.x.x.exe**, en el que **x** representa el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación.

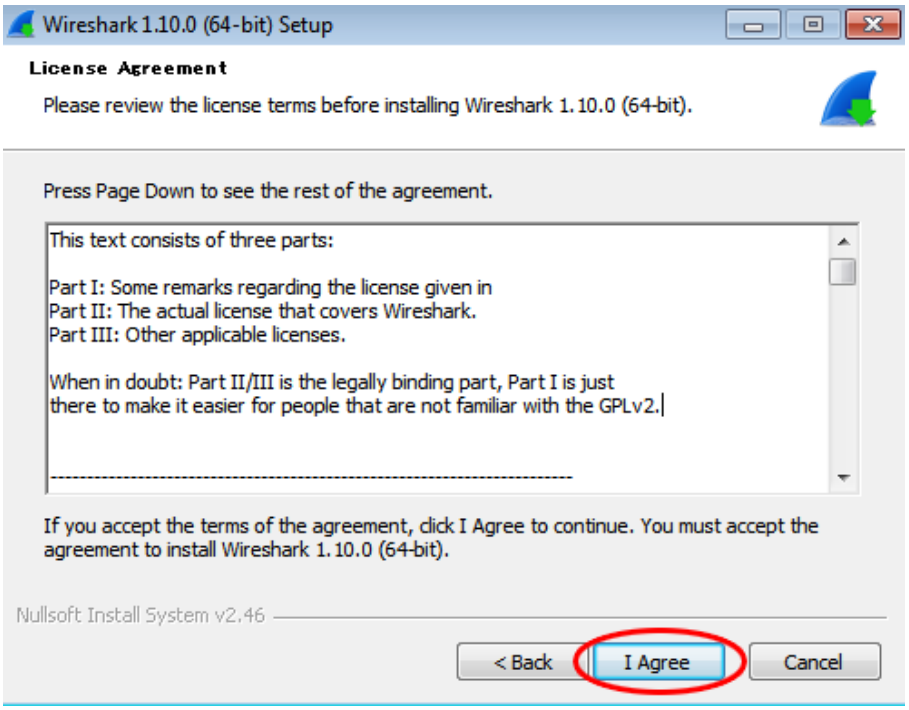
b. Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en la PC, se le solicitará desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Sí** para desinstalar la versión anterior de Wireshark.



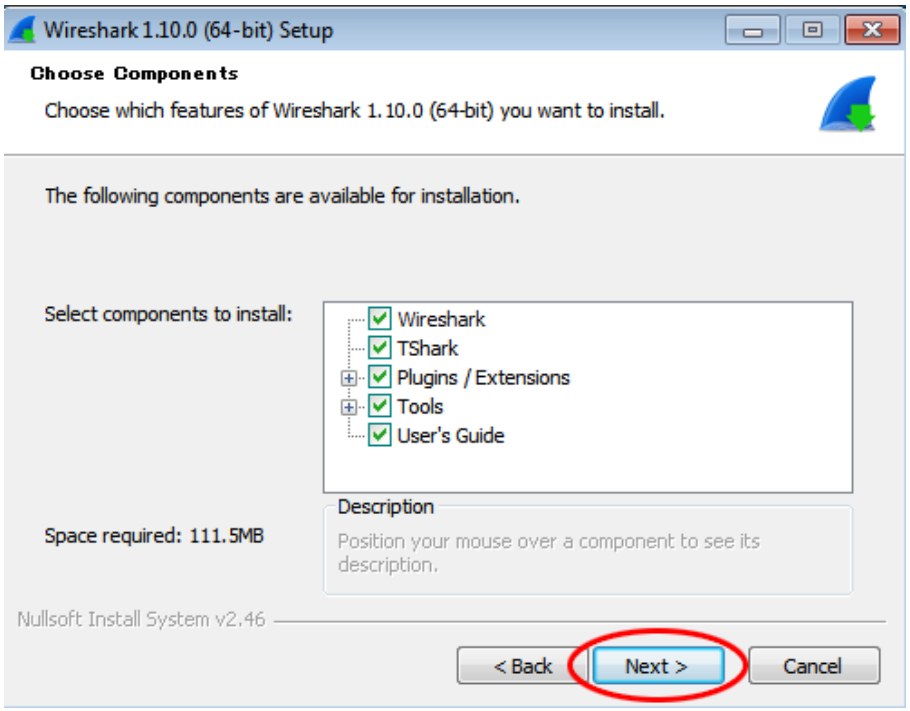
c. Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Next** (Siguiente).



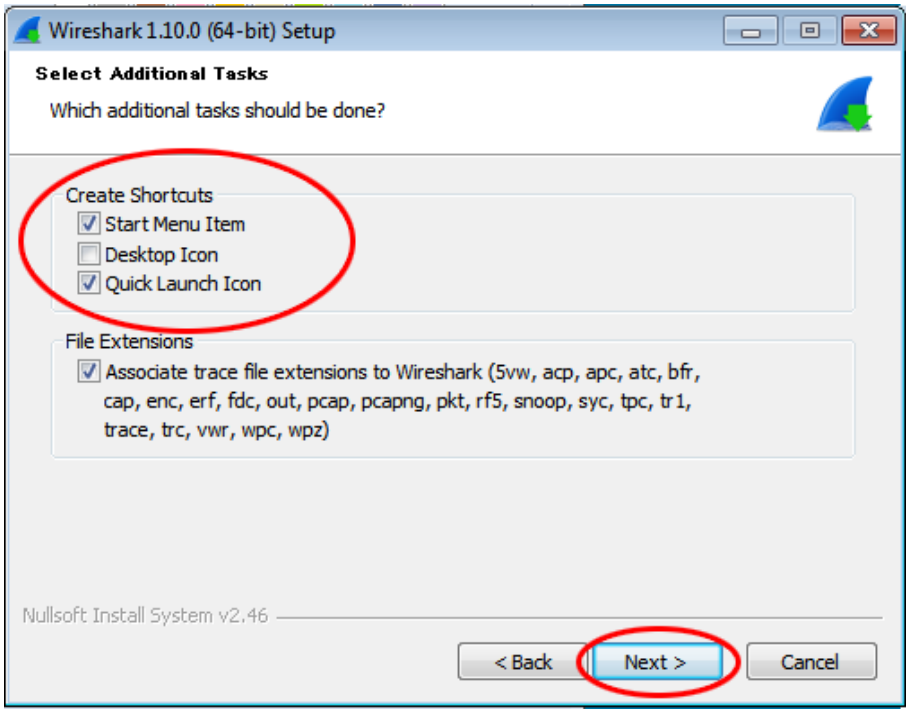
d. Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana License Agreement (Contrato de licencia), haga clic en **I agree** (Acepto).



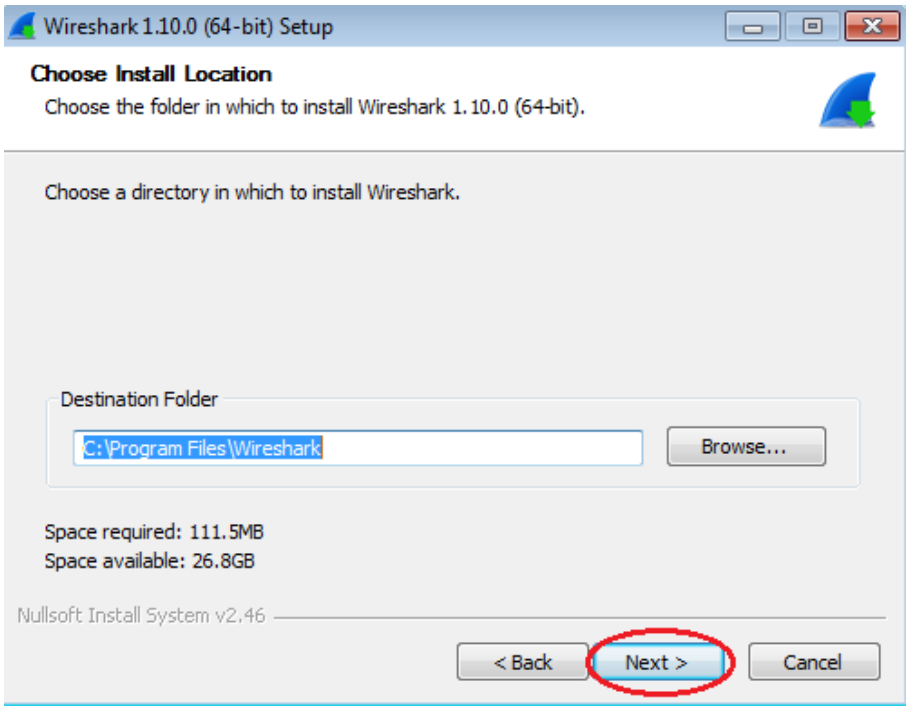
e. Guarde la configuración predeterminada en la ventana Choose Components (Elegir componentes) y haga clic en **Next** (Siguiente).



f. Elija las opciones de método abreviado que desee y, a continuación, haga clic en **Next** (Siguiente).

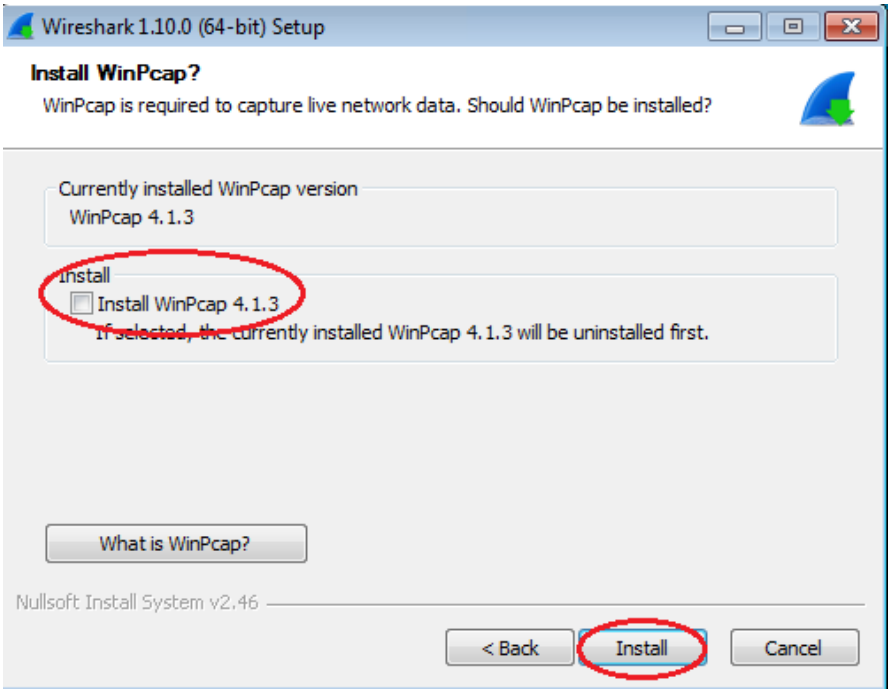


g. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.

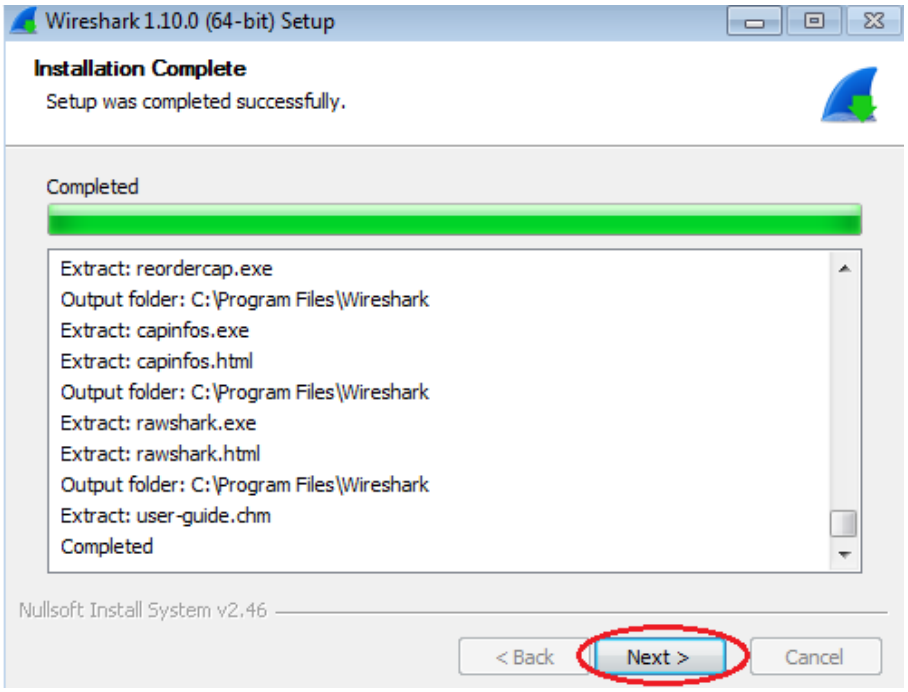


h. Para capturar datos de la red activa, WinPcap debe estar instalado en la PC. Si WinPcap ya está instalado en la PC, la casilla de verificación Install (Instalar) estará desactivada. Si la versión instalada de WinPcap es anterior a la versión que incluye Wireshark, se recomienda que permita que la versión más reciente se instale haciendo clic en la casilla de verificación **Install WinPcap x.x.x** (Instalar WinPcap [número de versión]).

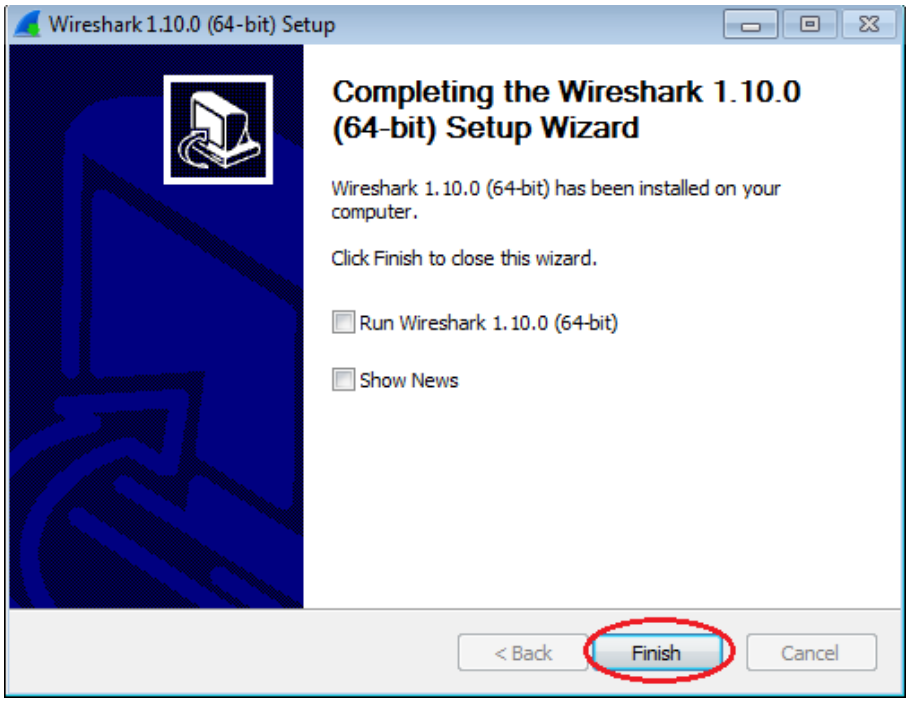
i. Finalice el asistente de instalación de WinPcap si instala WinPcap.



j. Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en **Next** (Siguiente) cuando la instalación esté completa.



k. Haga clic en **Finish** (Finalizar) para completar el proceso de instalación de Wireshark.



Parte 2: Capturar y analizar datos ICMP locales en Wireshark

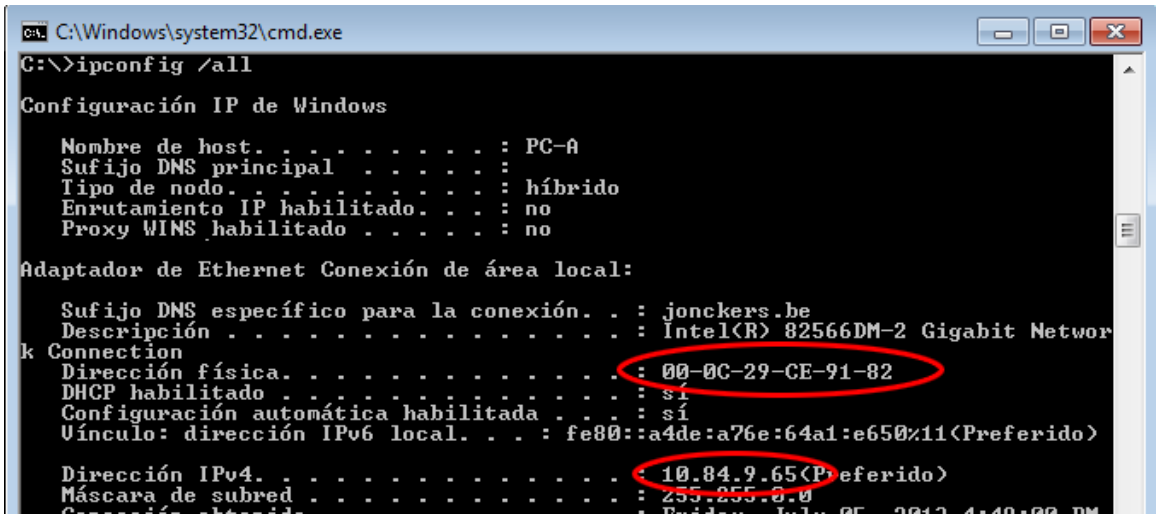
En la parte 2 de esta práctica de laboratorio, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Paso 1: Recuperar las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como “dirección MAC”.

a. Abra una ventana de comandos, escriba **ipconfig /all** y luego presione Entrar.

b. Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC.

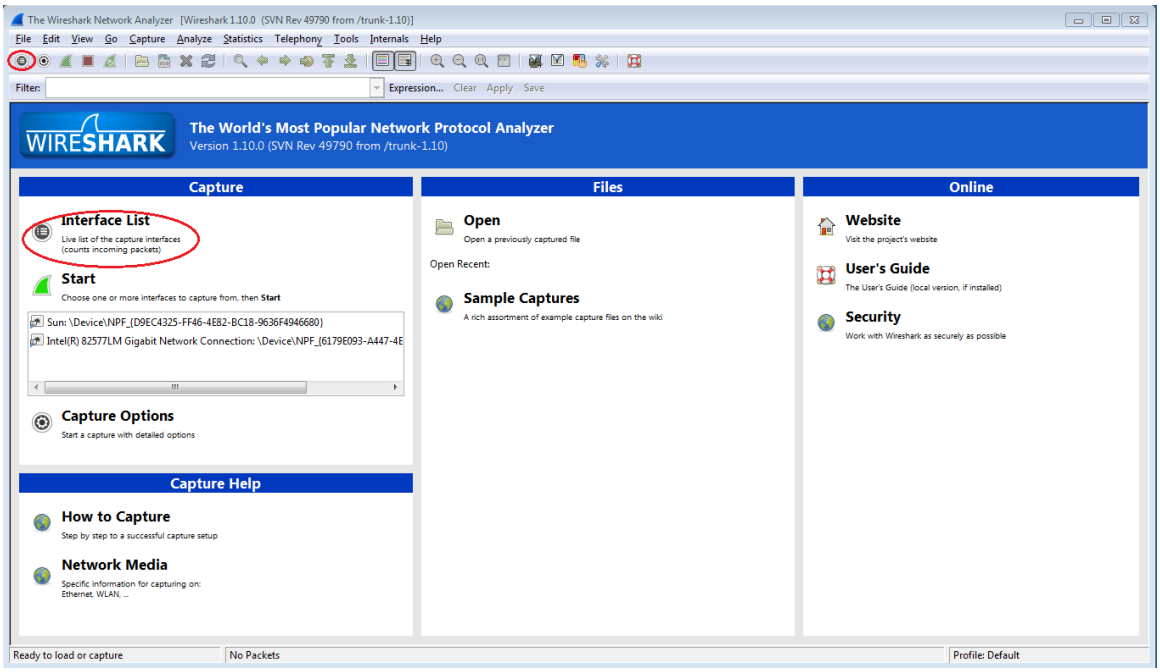


c. Solicite a un miembro del equipo la dirección IP de su PC y proporciónele la suya. En esta instancia, no proporcione su dirección MAC.

Paso 2: Iniciar Wireshark y comenzar a capturar datos

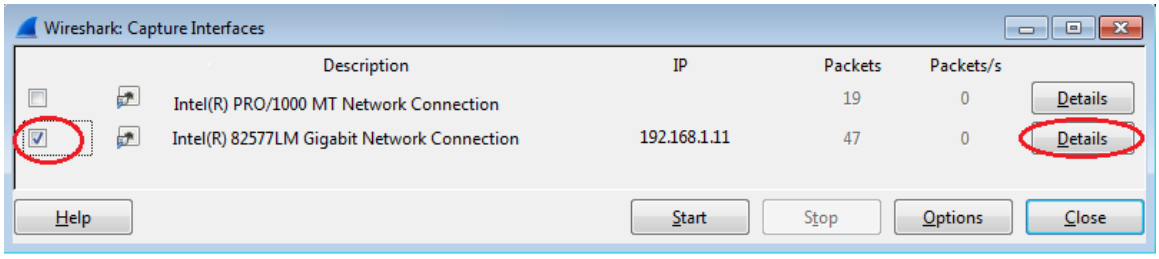
a. En la PC, haga clic en el botón **Inicio** de Windows para ver Wireshark como uno de los programas en el menú emergente. Haga doble clic en **Wireshark**.

b. Una vez que se inicia Wireshark, haga clic en **Interface List** (Lista de interfaces).

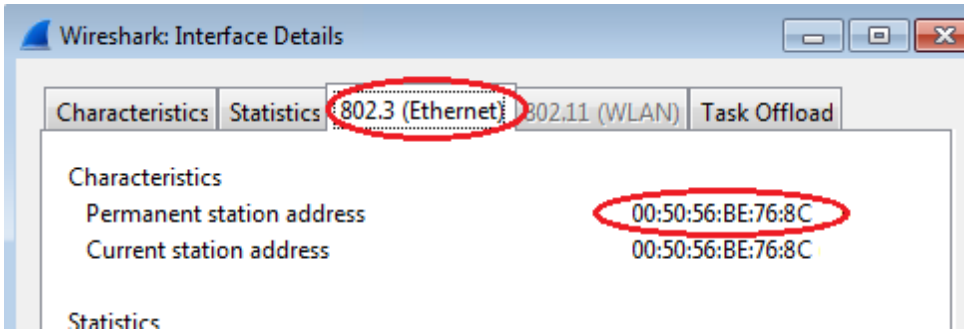


Nota: al hacer clic en el ícono de la primera interfaz de la fila de íconos, también se abre Interface List (Lista de interfaces).

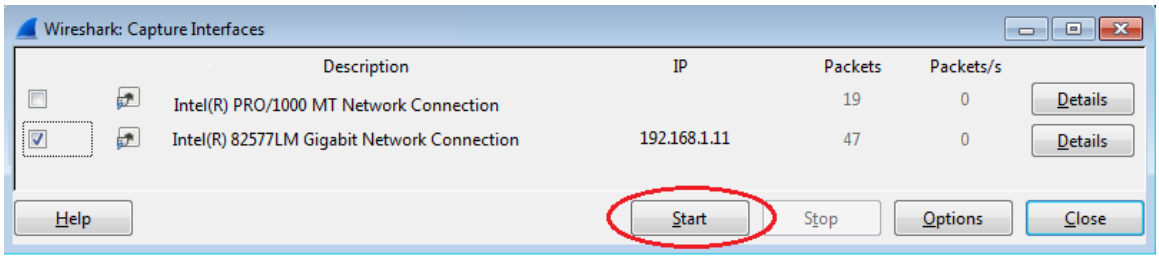
c. En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.



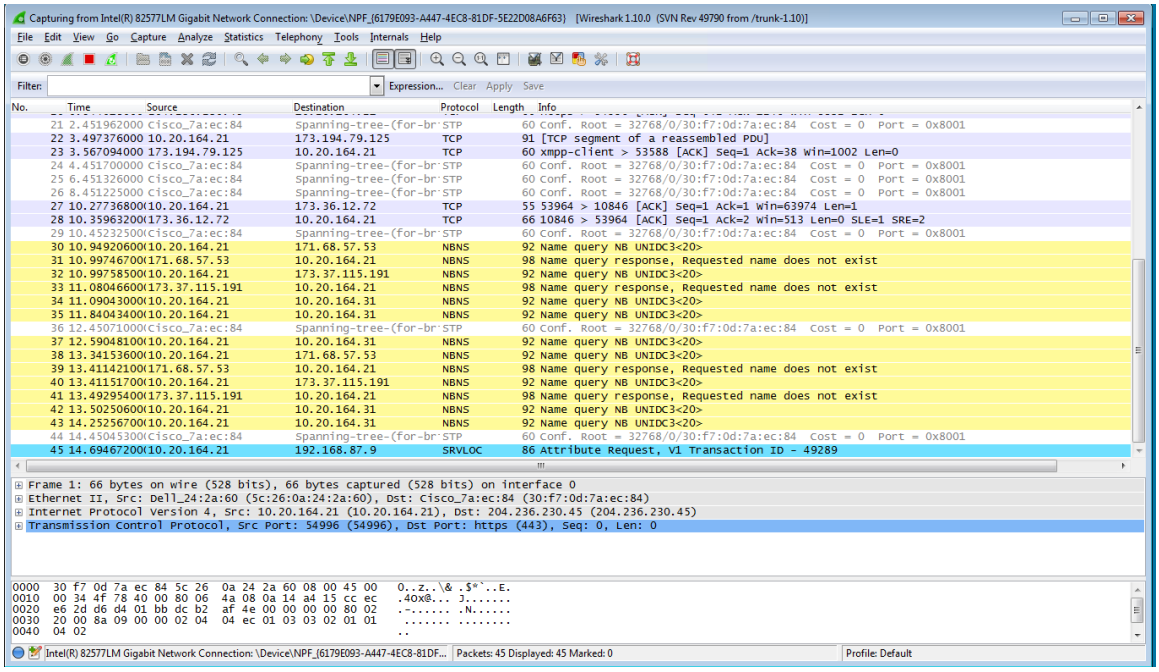
Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón **Details** (Detalles) y, a continuación, haga clic en la ficha **802.3 (Ethernet)**. Verifique que la dirección MAC coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre la ventana Interface Details (Detalles de la interfaz).



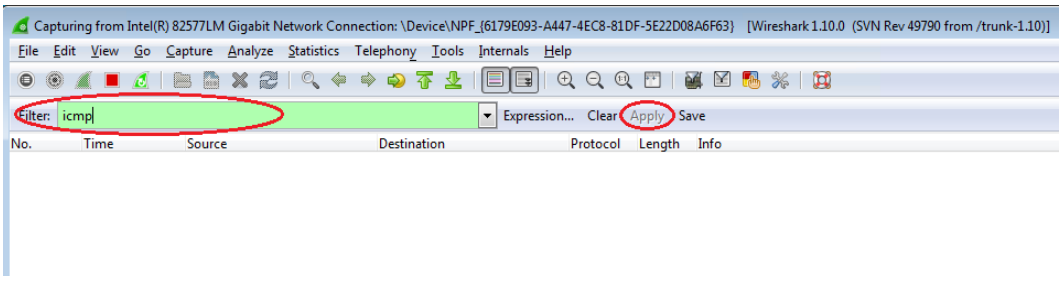
d. Después de activar la interfaz correcta, haga clic en **Start** (Comenzar) para comenzar la captura de datos.



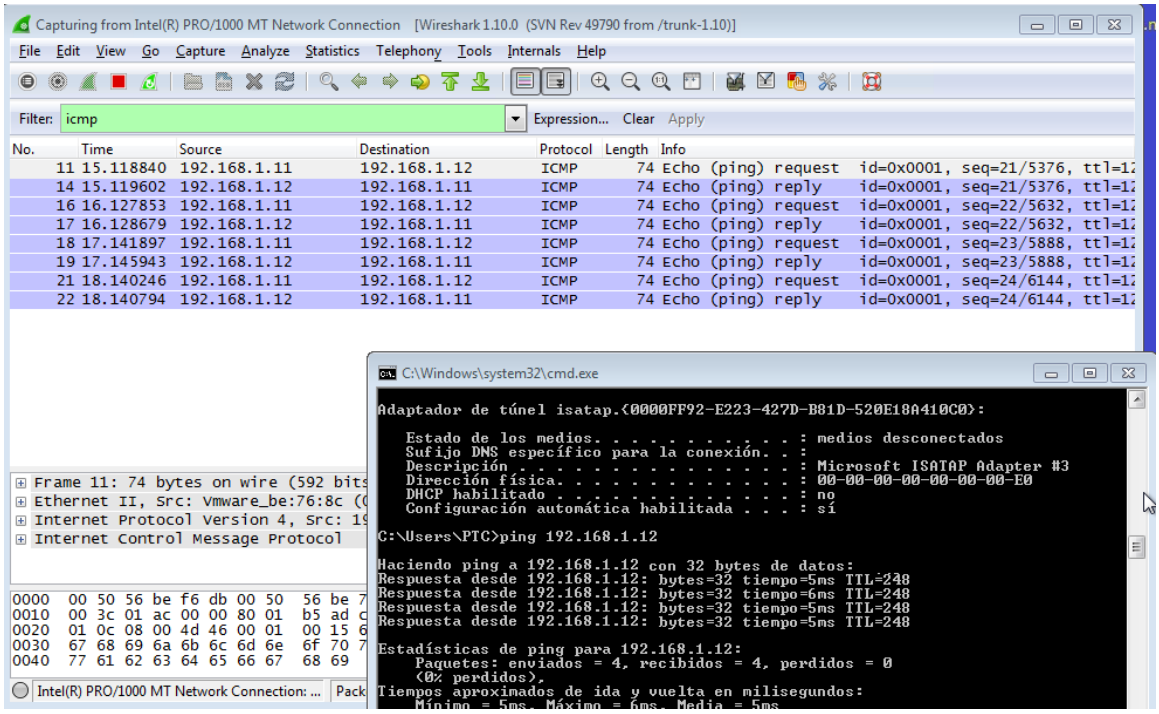
La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo.



e. Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** en el cuadro Filter (Filtro) que se encuentra en la parte superior de Wireshark y presione Entrar o haga clic en el botón **Apply** (Aplicar) para ver solamente PDU de ICMP (ping).

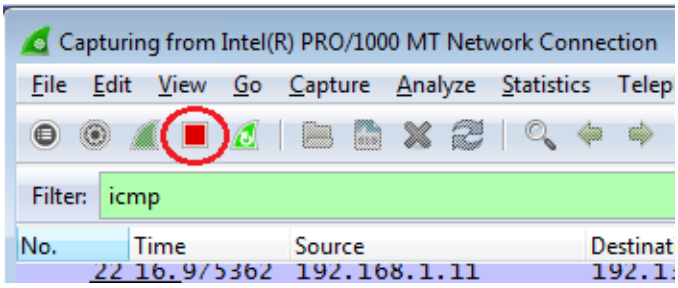


f. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.



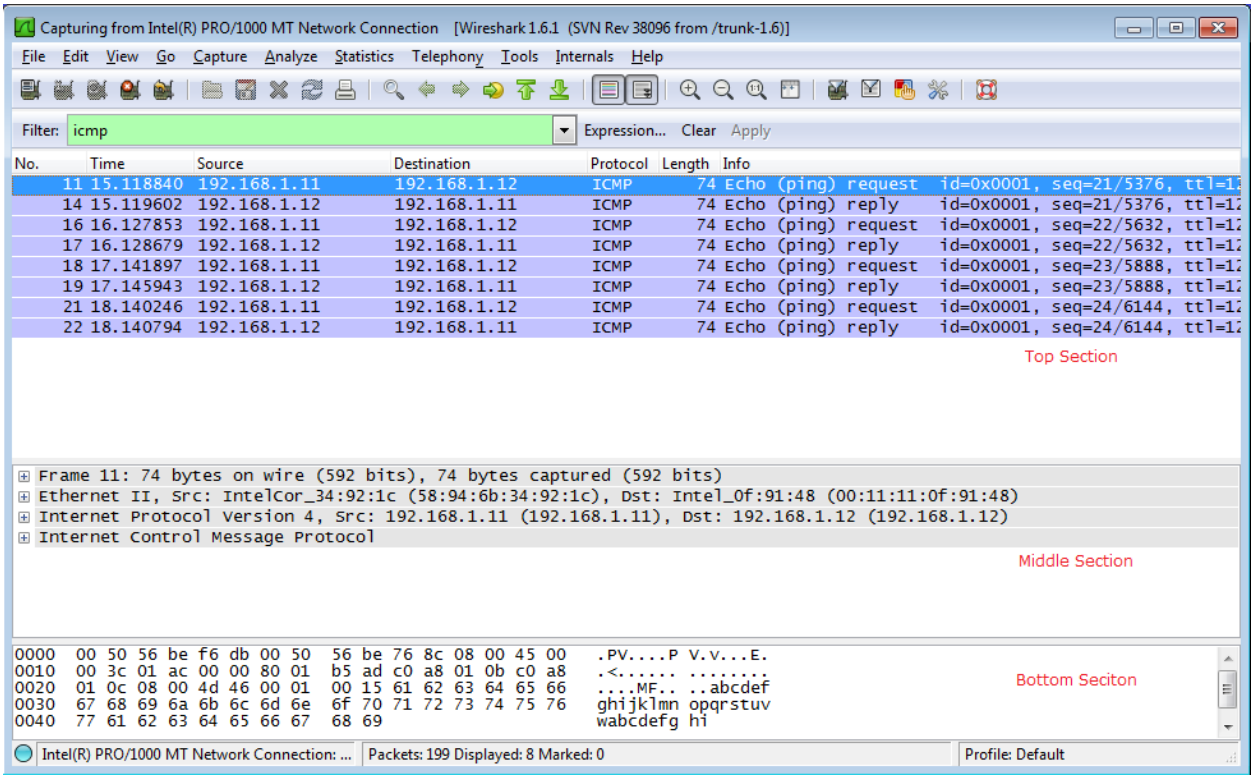
Nota: si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Consulte Apéndice A: Permitir el tráfico ICMP a través de un firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall con Windows 7.

g. Detenga la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).

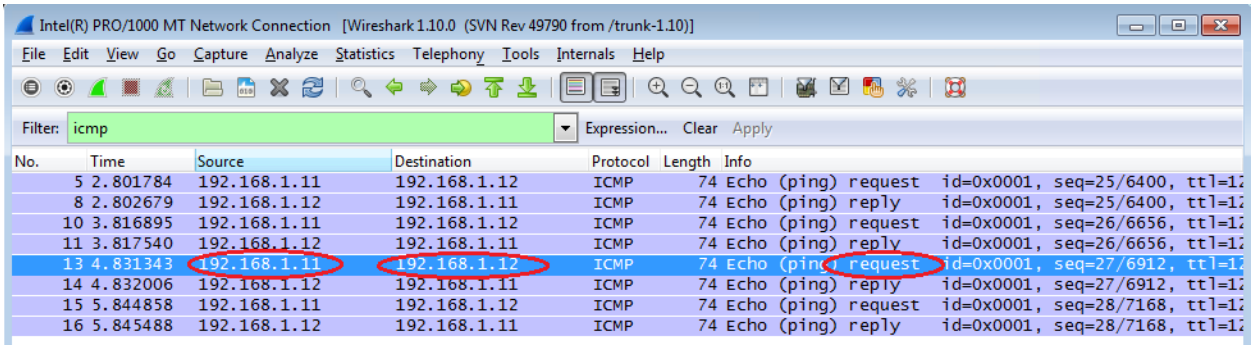


Paso 3: Examinar los datos capturados

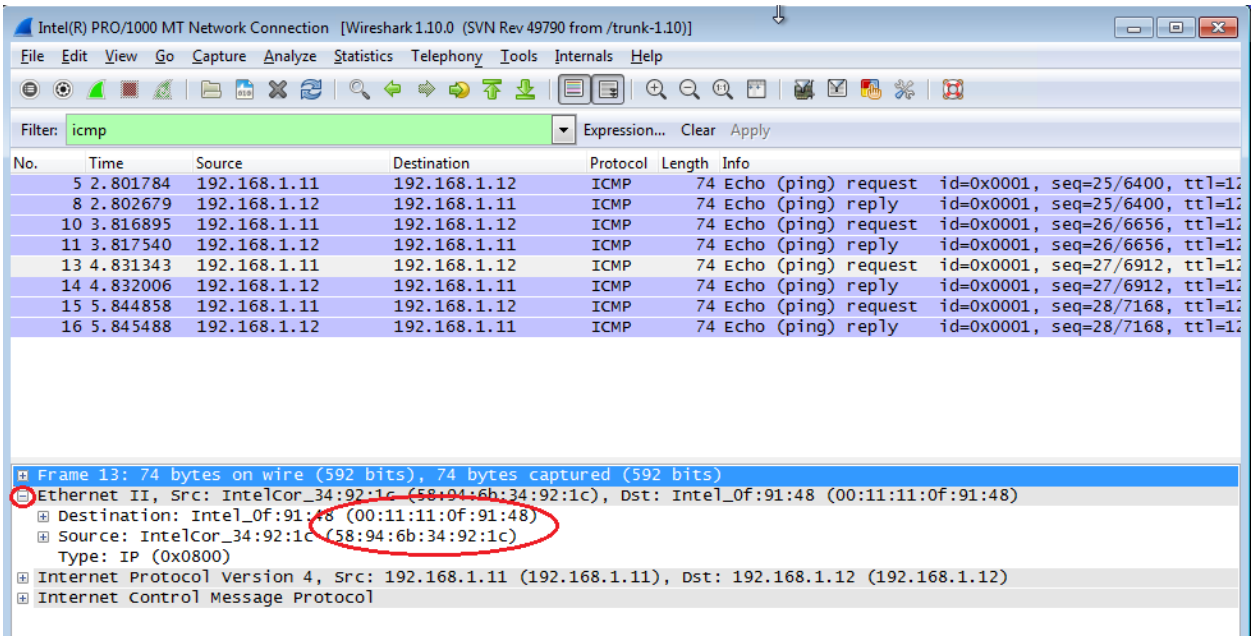
En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la sección media indica información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo, y 3) la sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal.



a. Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna Source (Origen) contiene la dirección IP de su PC y la columna Destination (Destino) contiene la dirección IP de la PC del compañero de equipo a la que hizo ping.



b. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino.



¿La dirección MAC de origen coincide con la interfaz de su PC? _____ Sí

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del miembro del equipo?

_____ Sí

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

_____

La dirección MAC se obtiene a través de una solicitud de ARP.

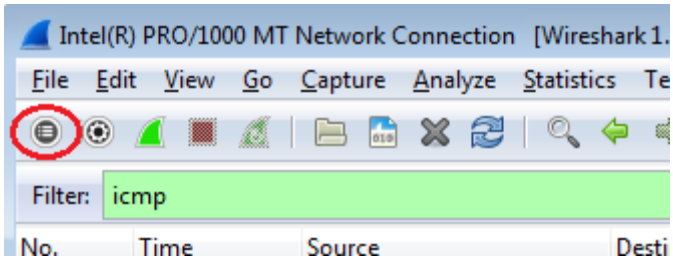
Nota: en el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encapsulan dentro de una PDU del paquete IPV4 (encabezado de IPv4), que luego se encapsula en una PDU de trama de Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

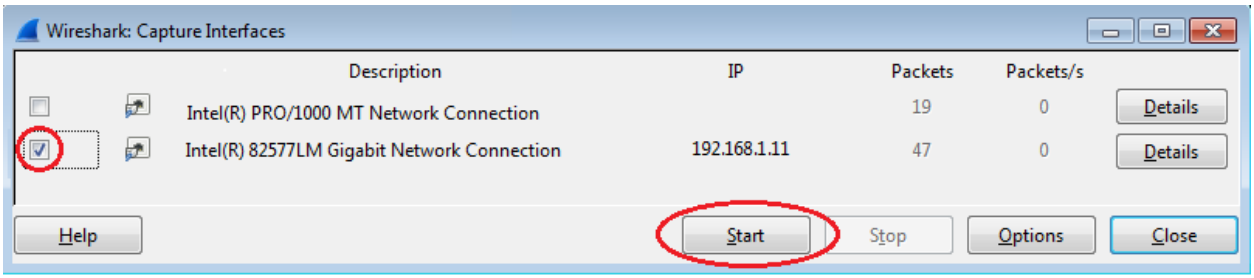
En la parte 3, hará ping a los hosts remotos (hosts que no están en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la parte 2.

Paso 1: Comenzar a capturar datos en la interfaz

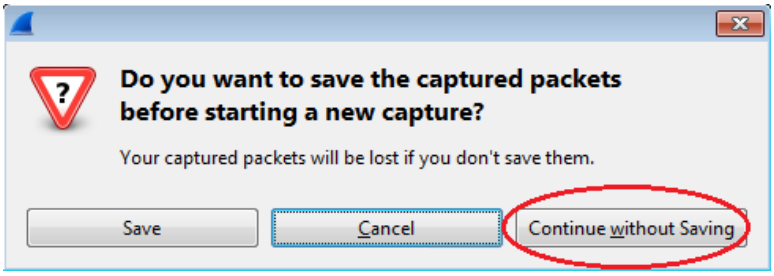
a. Haga clic en el ícono **Interface List** (Lista de interfaces) para volver a abrir la lista de interfaces de la PC.



b. Asegúrese de que la casilla de verificación junto a la interfaz LAN esté activada y, a continuación, haga clic en **Start** (Comenzar).

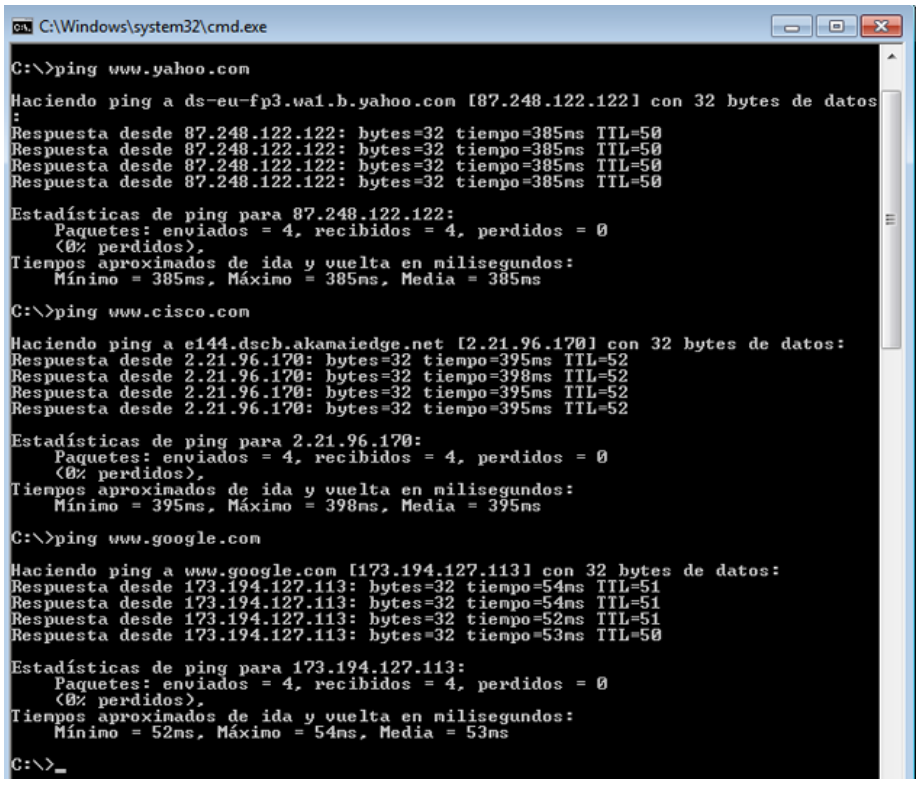


c. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving** (Continuar sin guardar).



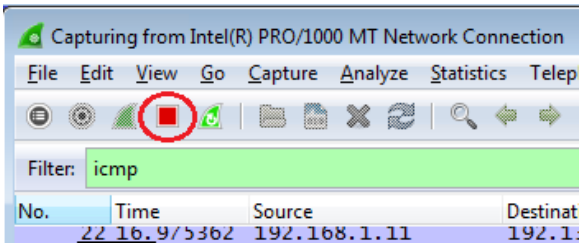
d. Con la captura activa, haga ping a los URL de los tres sitios Web siguientes:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



Nota: al hacer ping a los URL que se indican, observe que el servidor de nombres de dominio (DNS) traduce el URL a una dirección IP. Observe la dirección IP recibida para cada URL.

e. Puede detener la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).



Paso 2: Inspeccionar y analizar los datos de los hosts remotos

a. Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de las tres ubicaciones a las que hizo ping. Indique las direcciones IP y MAC de destino para las tres ubicaciones en el espacio proporcionado.

1.ª ubicación: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2.ª ubicación: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3.ª ubicación: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

Direcciones IP: 72.30.38.140, 192.133.219.25, 74.125.129.99 (estas direcciones IP pueden variar).

Dirección MAC: será la misma para las tres ubicaciones. Es la dirección física de la interfaz LAN del gateway predeterminado del router.

b. ¿Qué es importante sobre esta información?

_____

La dirección MAC para las tres ubicaciones es la misma.

c. ¿En qué se diferencia esta información de la información de ping local que recibió en la parte 2?

_____

_____

Un ping a un host local devuelve la dirección MAC de la NIC de la PC. Un ping a un host remoto devuelve la dirección MAC de la interfaz LAN del gateway predeterminado.

Reflexión

¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

_____

_____

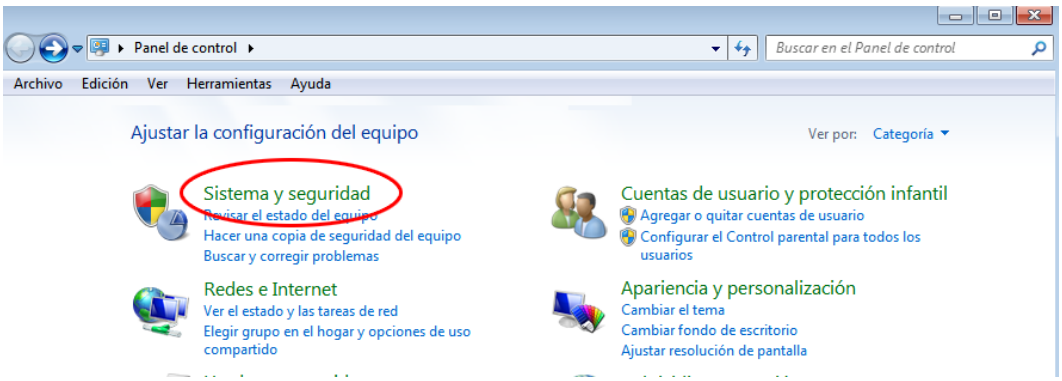
Las direcciones MAC de los hosts remotos no se conocen en la red local; por eso, se utiliza la dirección MAC del gateway predeterminado. Una vez que el paquete llega al router del gateway predeterminado, la información de la capa 2 se elimina del paquete y un nuevo encabezado de capa 2 se asocia a la dirección MAC de destino del router del salto siguiente.

Apéndice A: Permitir el tráfico ICMP a través de un firewall

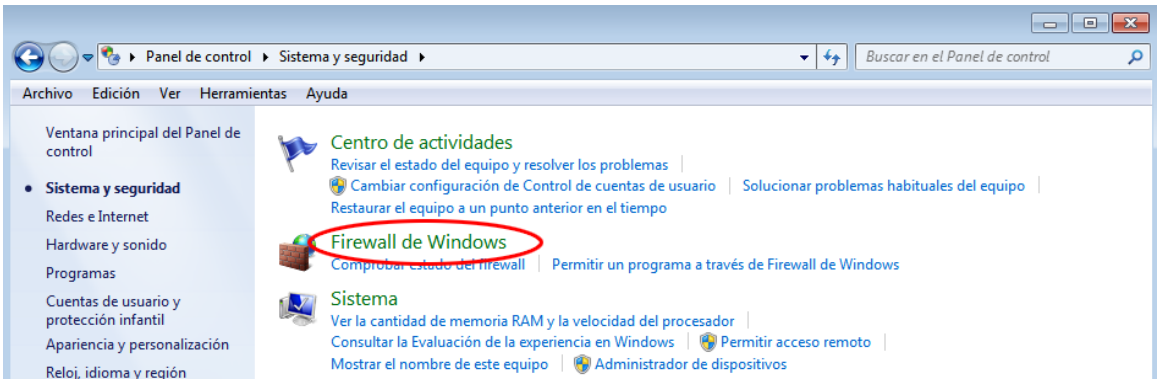
Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado la práctica de laboratorio.

Paso 1: Crear una nueva regla de entrada que permita el tráfico ICMP a través del firewall

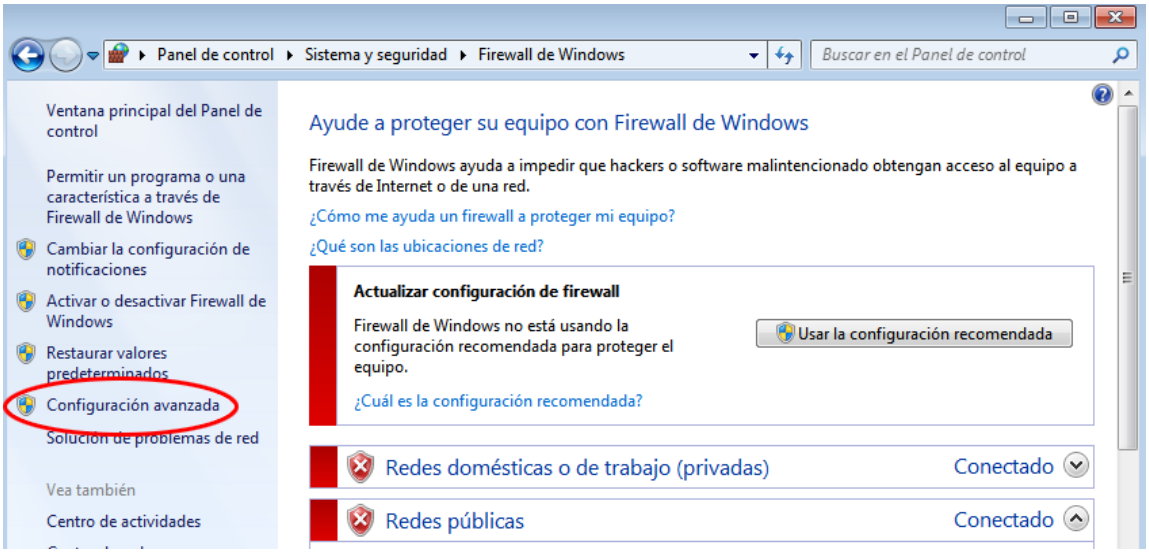
a. En el panel de control, haga clic en la opción **Sistema y seguridad**.



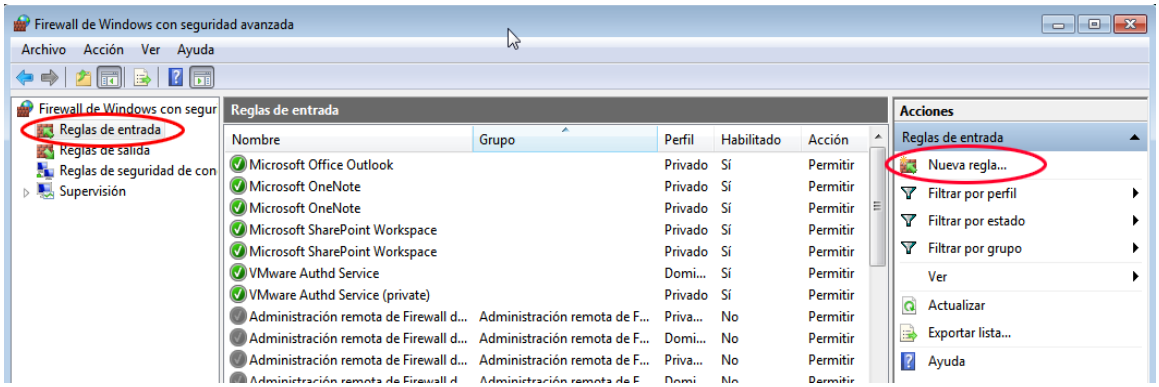
b. En la ventana Sistema y seguridad, haga clic en **Firewall de Windows**.



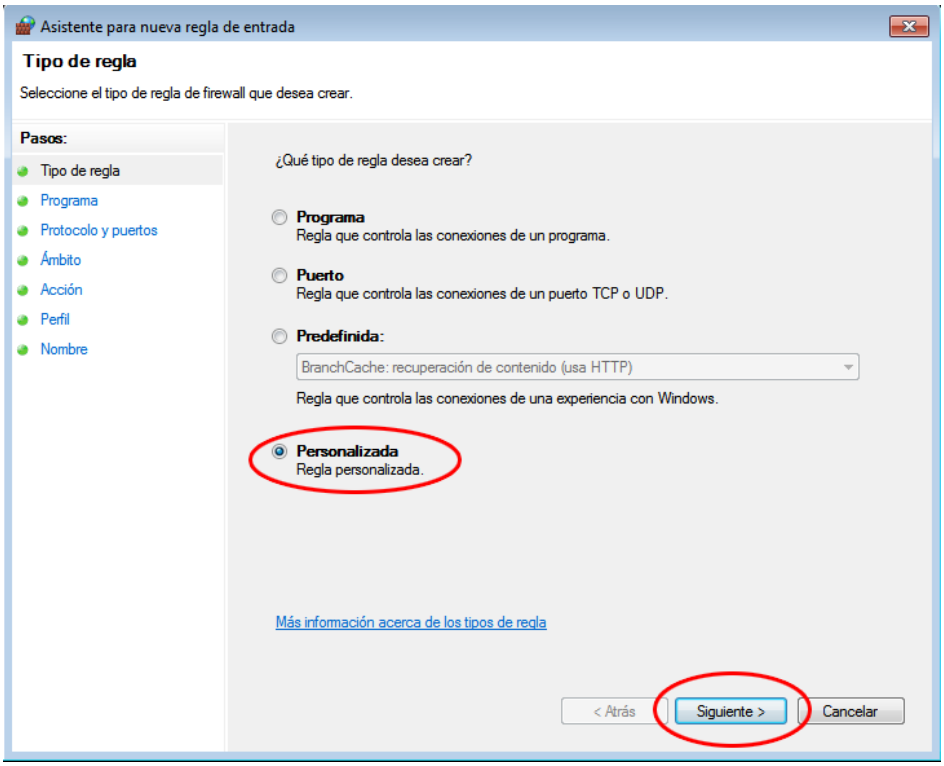
c. En el panel izquierdo de la ventana Firewall de Windows, haga clic en **Configuración avanzada**.



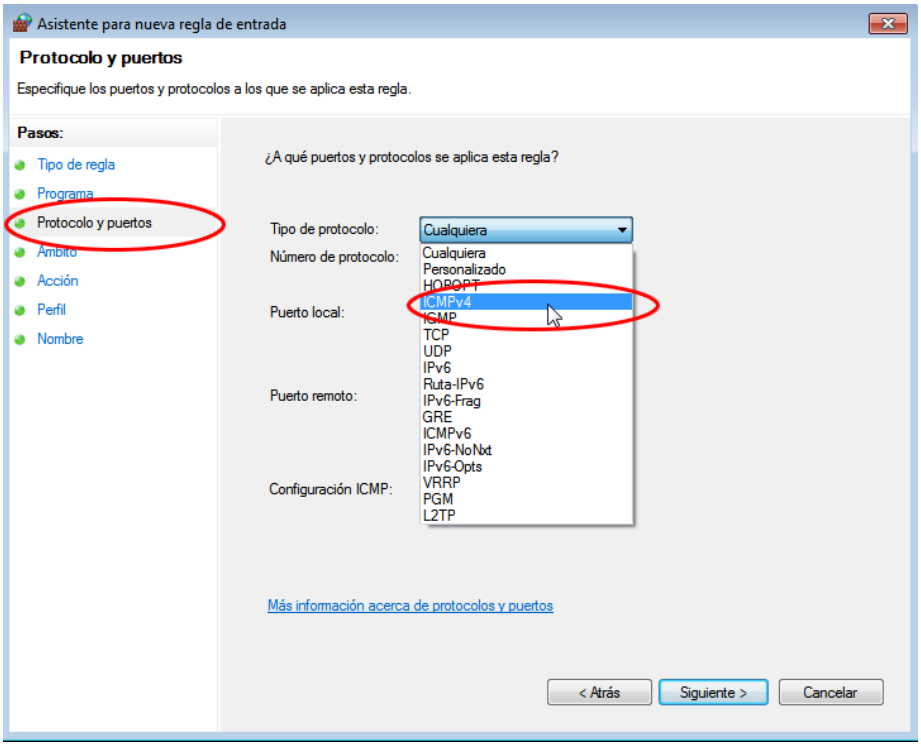
d. En la ventana Seguridad avanzada, seleccione la opción **Reglas de entrada** en la barra lateral izquierda y, a continuación, haga clic **Nueva regla** en la barra lateral derecha.



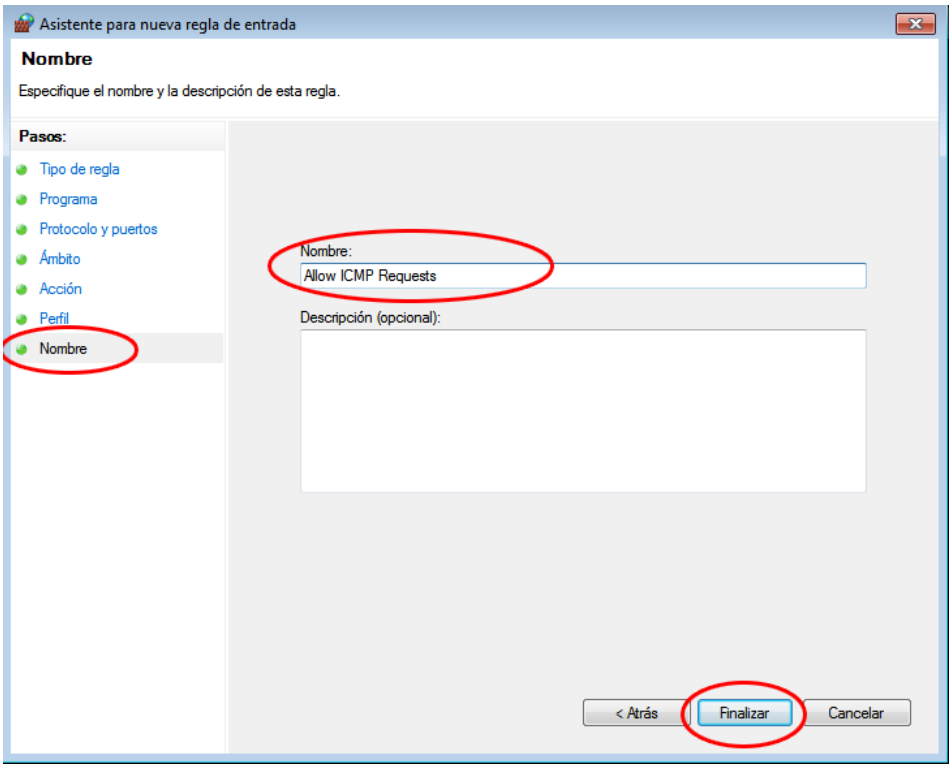
e. Se inicia el Asistente para nueva regla de entrada. En la pantalla Tipo de regla, haga clic en el botón de opción **Personalizada** y, a continuación, en **Siguiente.**



f. En el panel izquierdo, haga clic en la opción **Protocolo y puertos**, y en el menú desplegable Tipo de protocolo, seleccione **ICMPv4**; a continuación, haga clic en **Siguiente**.



g. En el panel izquierdo, haga clic en la opción **Nombre**, y en el campo Nombre, escriba **Allow ICMP Requests** (Permitir solicitudes ICMP). Haga clic en **Finish** (Finalizar).

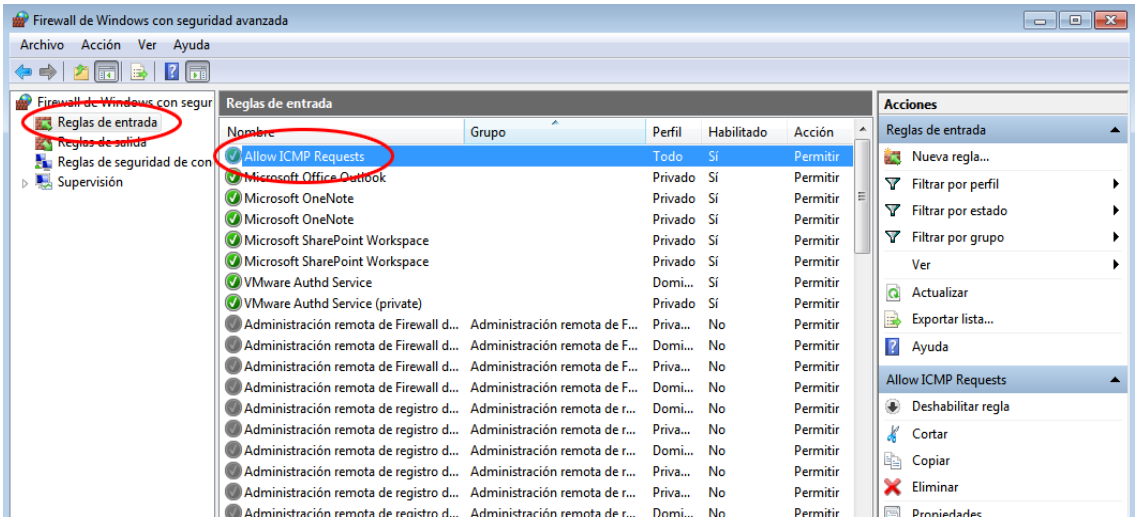


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

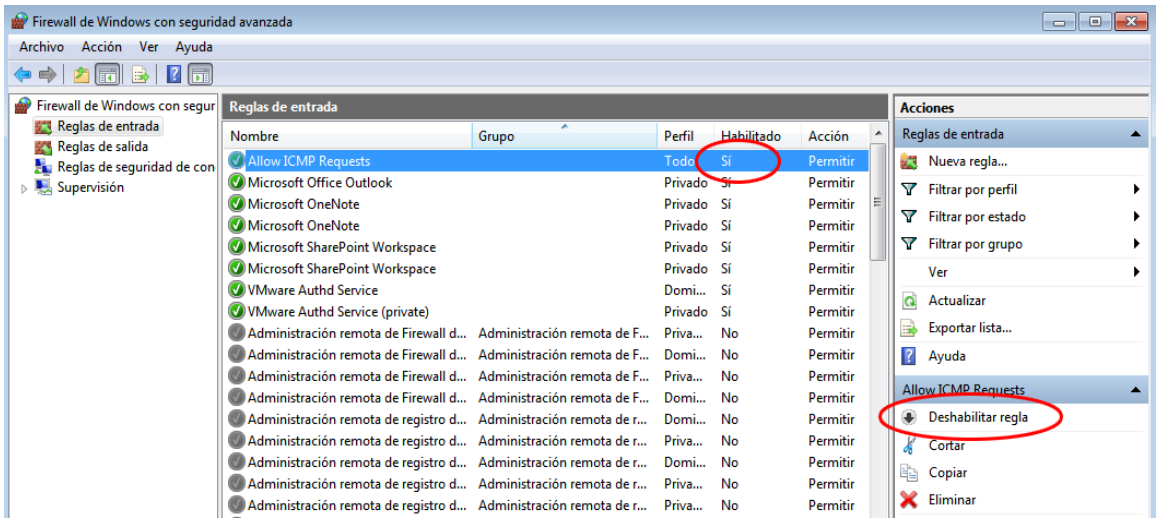
Paso 3: Deshabilitar o eliminar la nueva regla ICMP

Una vez completada la práctica de laboratorio, es posible que desee deshabilitar o incluso eliminar la nueva regla que creó en el paso 1. La opción **Deshabilitar regla** permite volver a habilitar la regla en una fecha posterior. Al eliminar la regla, esta se elimina permanentemente de la lista de Reglas de entrada.

a. En el panel izquierdo de la ventana Seguridad avanzada, haga clic en **Reglas de entrada** y, a continuación, ubique la regla que creó en el paso 1.



b. Para deshabilitar la regla, haga clic en la opción **Deshabilitar regla**. Al seleccionar esta opción, verá que esta cambia a **Habilitar regla**. Puede alternar entre deshabilitar y habilitar la regla; el estado de la regla también se muestra en la columna Habilitada de la lista Reglas de entrada.



c. Para eliminar permanentemente la regla ICMP, haga clic en **Eliminar**. Si elige esta opción, deberá volver a crear la regla para permitir las respuestas de ICMP.