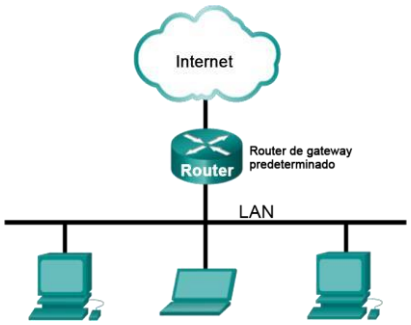
Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red Topología



Objetivos Parte 1: Descargar e instalar Wireshark 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** 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.

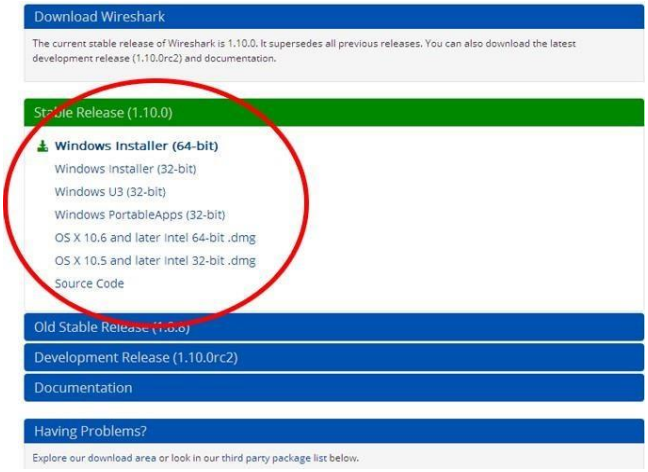
Wireshark es una herramienta útil para cualquier persona que trabaje con redes y se puede utilizar para tareas de **análisis de datos y resolución de problemas**. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark. Usará Wireshark para capturar direcciones IP del paquete de datos ICMP y direcciones MAC de la trama de Ethernet.

Parte 1: Descargar e instalar Wireshark

Wireshark se convirtió en el programa detector de paquetes estándar del sector. Este software de **código abierto** está disponible para **muchos sistemas operativos diferentes**, incluidos Windows, MAC y Linux. **Paso 1: Descargar Wireshark**

- Wireshark se puede descargar de www.wireshark.org.
- Haga clic en Download Wireshark (Descargar Wireshark).

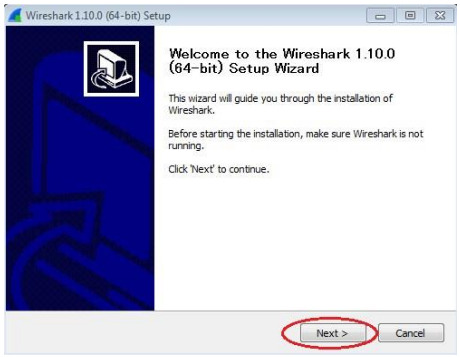
- Elija la versión de software que necesita según la arquitectura y el sistema operativo de la PC. Por ejemplo, si tiene una PC de 64 bits con Windows, seleccione Windows Installer (64-bit) (Instalador de Windows [64 bits]).



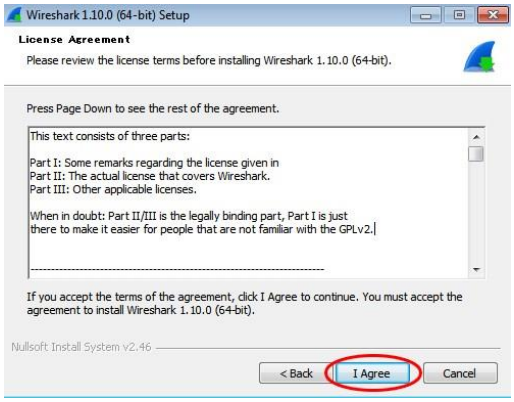
Después de realizar la selección, comienza la descarga. La ubicación del archivo descargado depende del explorador y del sistema operativo que utiliza.

Paso 2: Instalar Wireshark

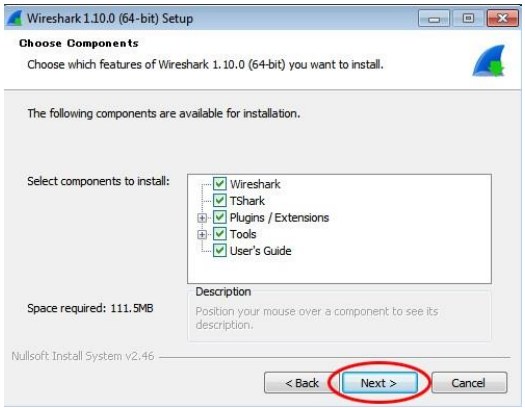
- El archivo descargado se denomina Wireshark-win64-x.x.x.exe, en el que x representa el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación.
- Responda los mensajes de seguridad que aparezcan en la pantalla.
- Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en Next



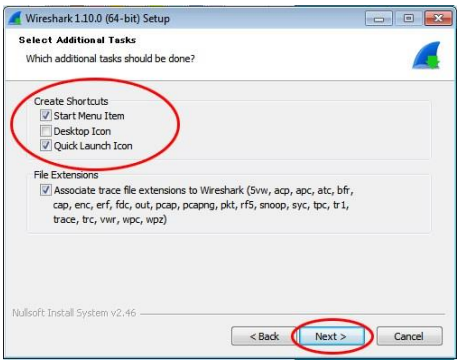
- Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana License Agreement, haga clic en I agree.



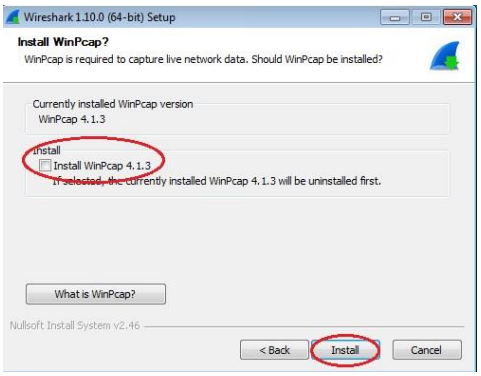
- Guarde la configuración predeterminada en la ventana Choose Components y haga clic en Next



Elija las opciones de método abreviado que desee y, a continuación, haga clic en Next

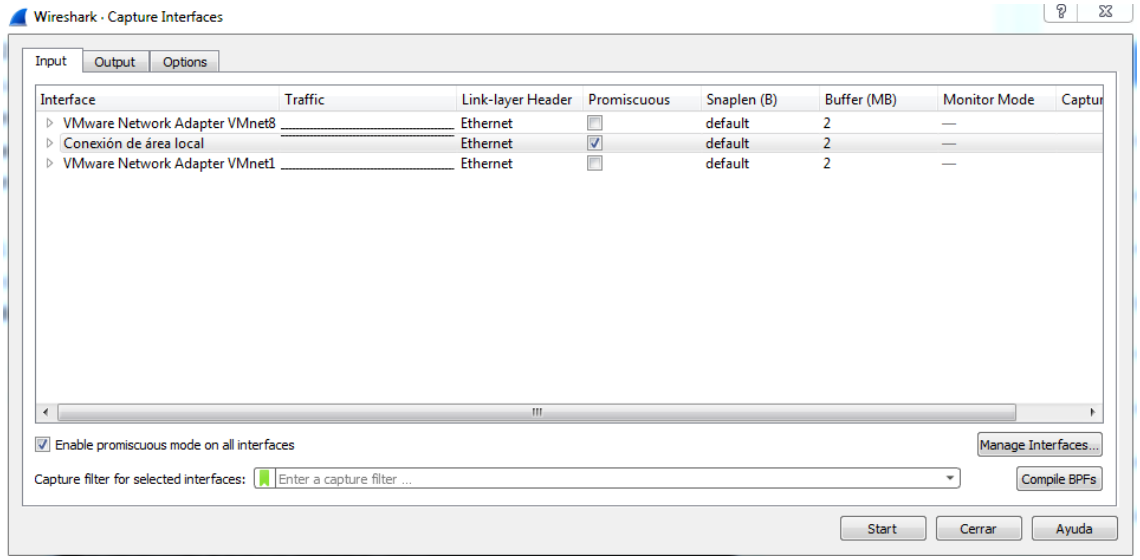


- Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.
- Para capturar datos de la red activa, WinPcap debe estar instalado en la PC.
- Finalice el asistente de instalación de WinPcap.



- Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en Next cuando la instalación esté completa.
- Haga clic en Finish para completar el proceso de instalación de Wireshark.

Parte 2: Capturar y analizar datos ICMP locales en Wireshark

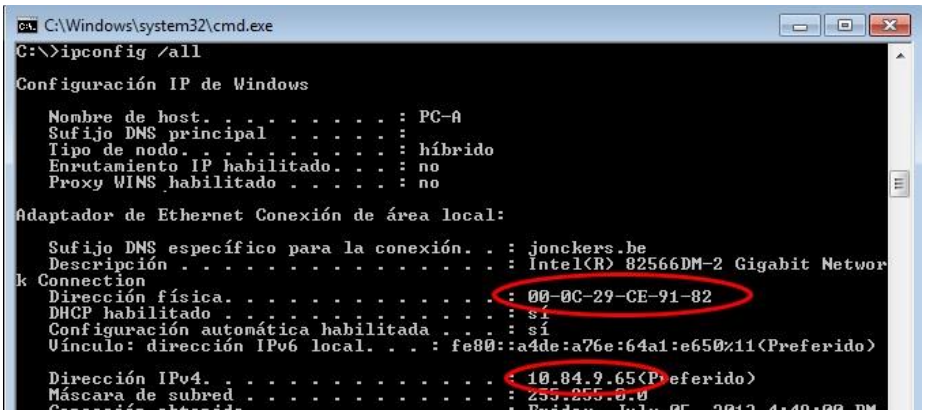


En la parte 2 de esta práctica, hará ping a otro PC en la LAN y **capturará solicitudes y respuestas ICMP en Wireshark**. También verá dentro de las tramas capturadas para **obtener información específica**. Este análisis debe ayudar a aclarar de **qué manera se utilizan los encabezados de paquetes para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

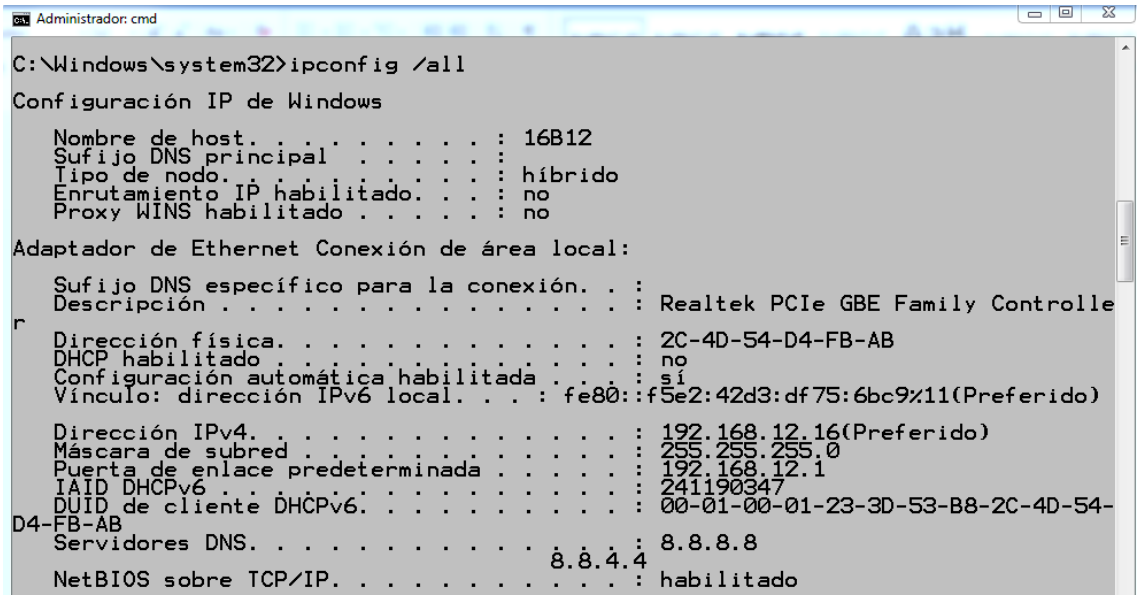
Paso 1: Recuperar las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá **obtener la dirección IP del PC y la dirección física de la tarjeta de interfaz de red (NIC) o "dirección MAC"**.

- Abra una ventana de comandos, escriba **ipconfig /all** y luego presione **Entrar**.
- Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC.



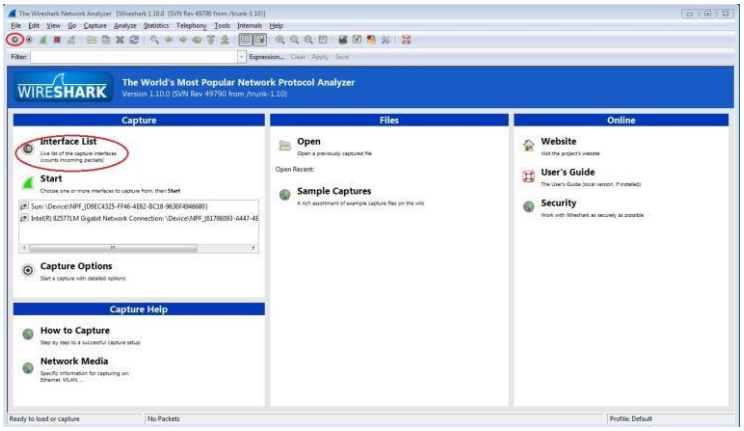
1“Muestra una captura de pantalla con tú tarjeta”



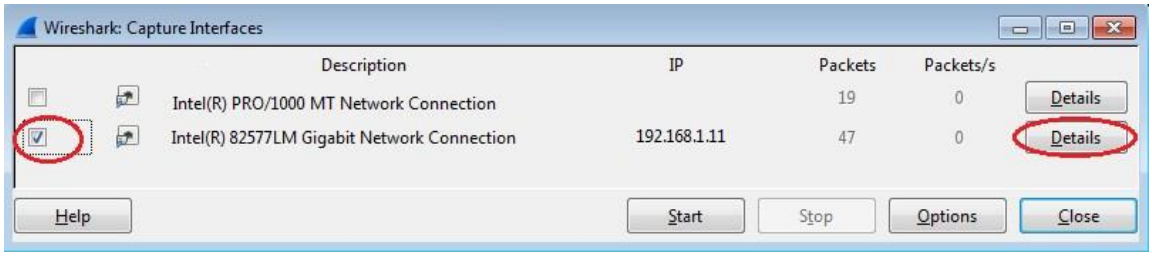
- Solicite a un compañero la dirección IP de su PC y proporciónele la suya. En esta instancia, no proporcione su dirección MAC.

Paso 2: Iniciar Wireshark y comenzar a capturar datos

- En el PC, haga doble clic en Wireshark.
- Una vez que se inicia Wireshark, haga clic en **Interface List**.

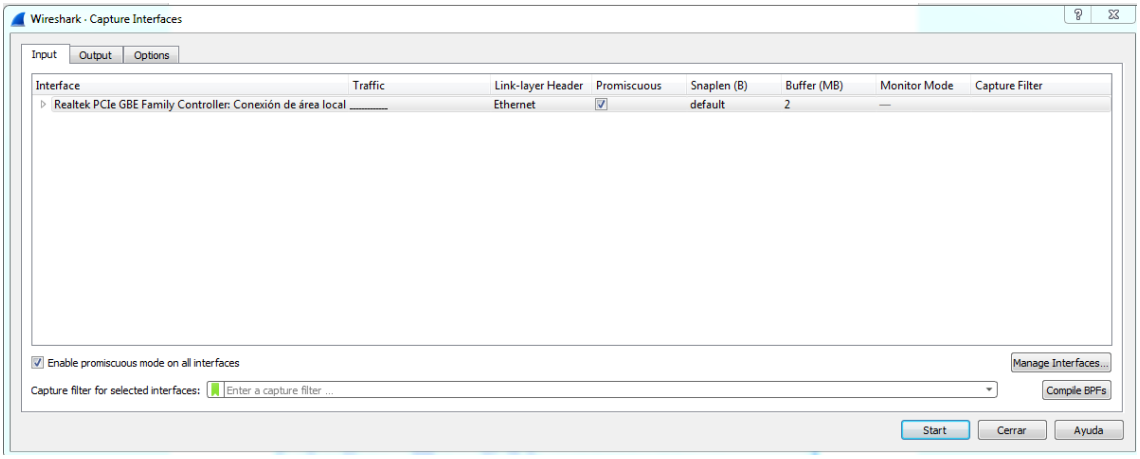


En la ventana Wireshark: Capture Interfaces, haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.

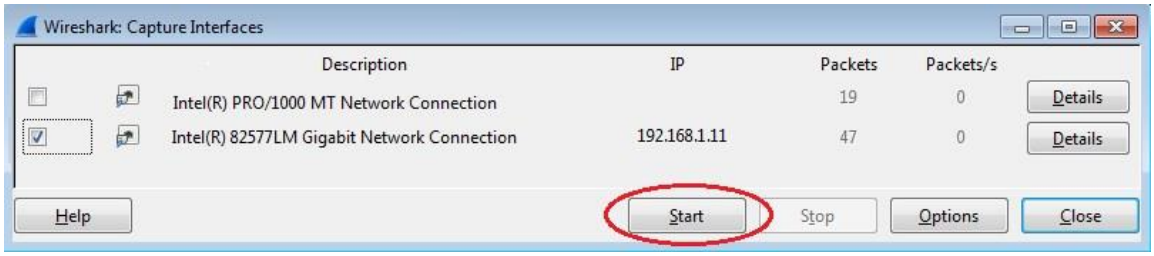


Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón **Details** (Detalles) y, a continuación, haga clic en la ficha **802.3 (Ethernet).** Verifique que la dirección MAC coincida con lo que observó en el paso anterior.

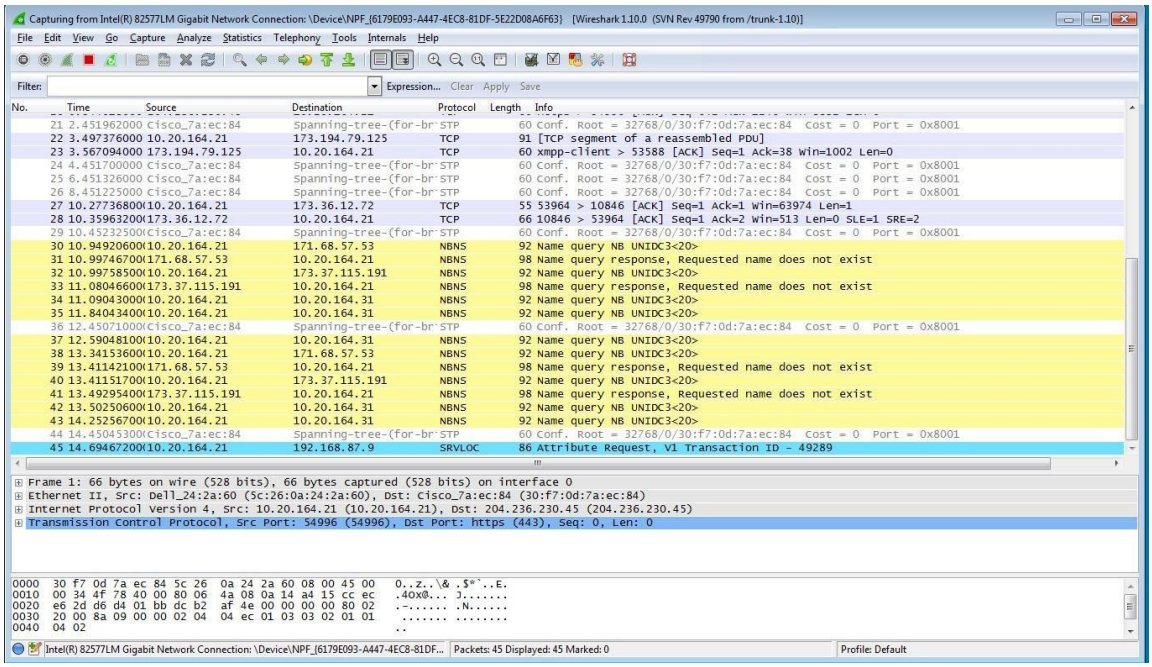
2"Muestra una captura de pantalla con tú tarjeta en WireShark"



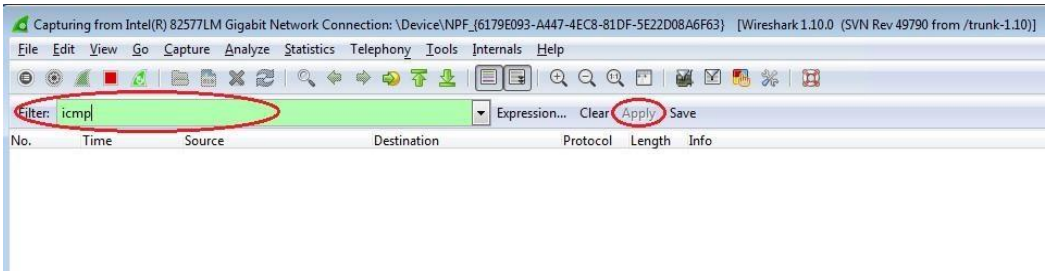
- Después de activar la interfaz correcta, haga clic en **Start** para comenzar la captura de datos.



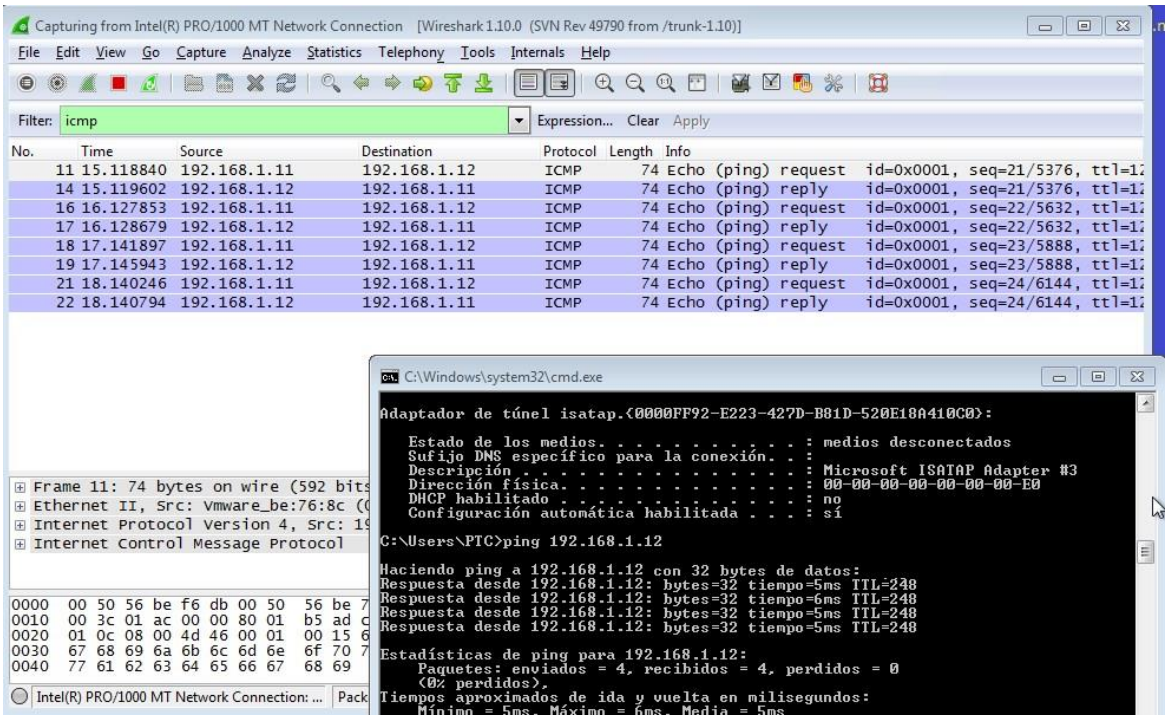
La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en **diferentes colores según el protocolo**.



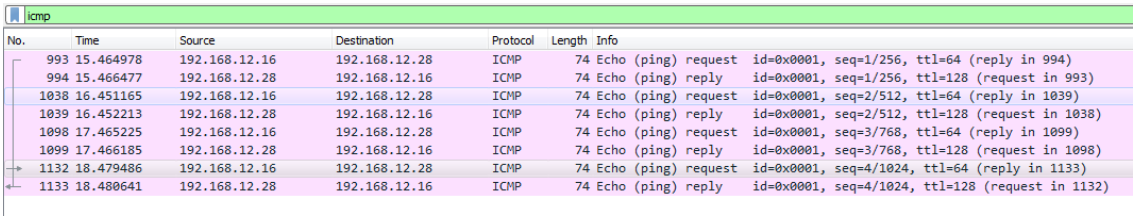
Se puede aplicar un **filtro** para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar **las PDU de ICMP** (ping). Escriba icmp en el cuadro Filter que se encuentra en la parte superior de Wireshark y presione Entrar o haga clic en el botón Apply para ver solamente PDU de ICMP (ping).



- 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.



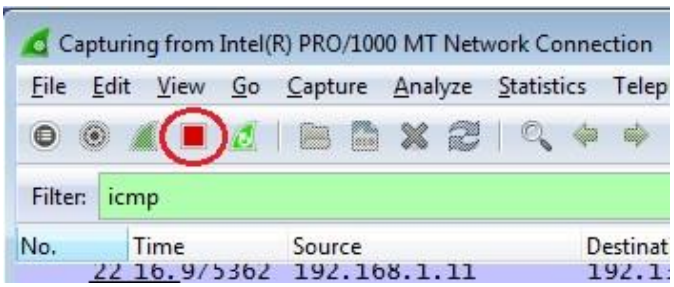
3"Muestra una captura de pantalla con la IP de tú compañero"



La ip de mi compañero es: 192.168.12.28, se muestra en la captura anterior.

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.

Detenga la captura de datos haciendo clic en el ícono **Stop** Capture



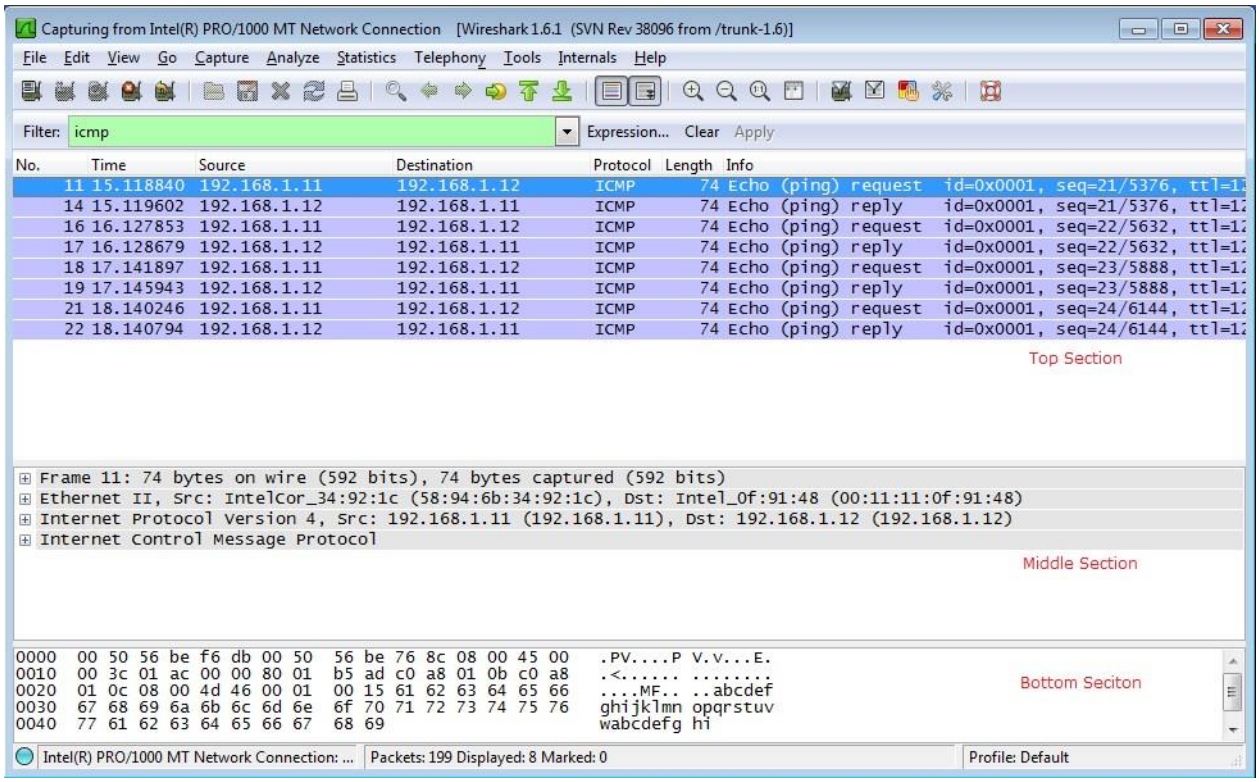
Paso 3: Examinar los datos capturados

Examine los datos que se generaron mediante las solicitudes de ping del PC del compañero. Los datos de Wireshark se muestran en tres secciones:

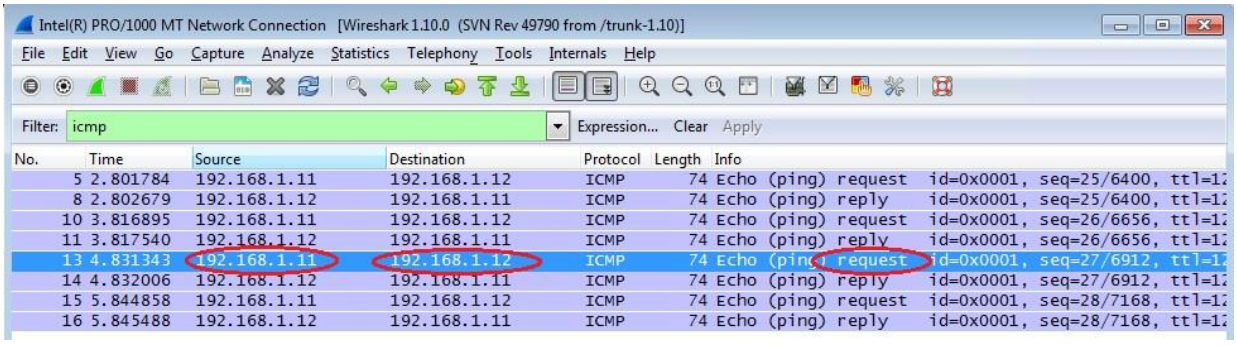
1) la sección **superior** muestra la lista de **tramas de PDU capturadas** con un resumen de la información de paquetes IP enumerada

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**

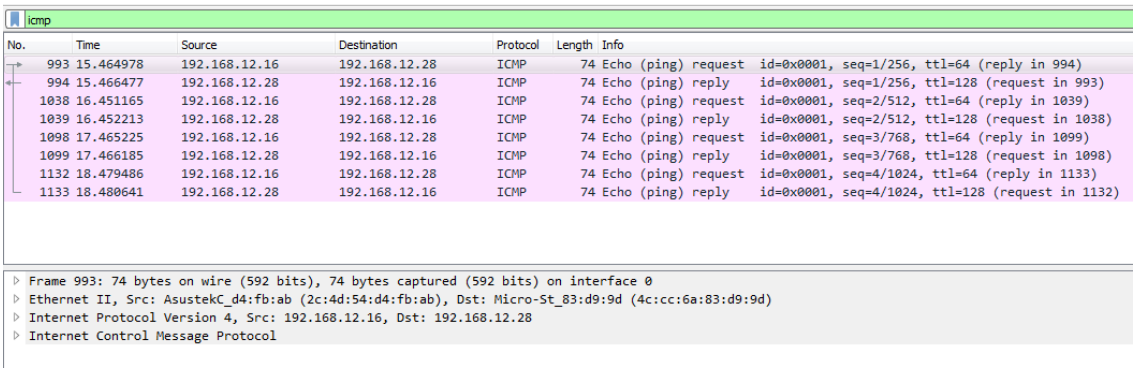
3) la sección **inferior** muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en **formatos hexadecimal y decimal**.



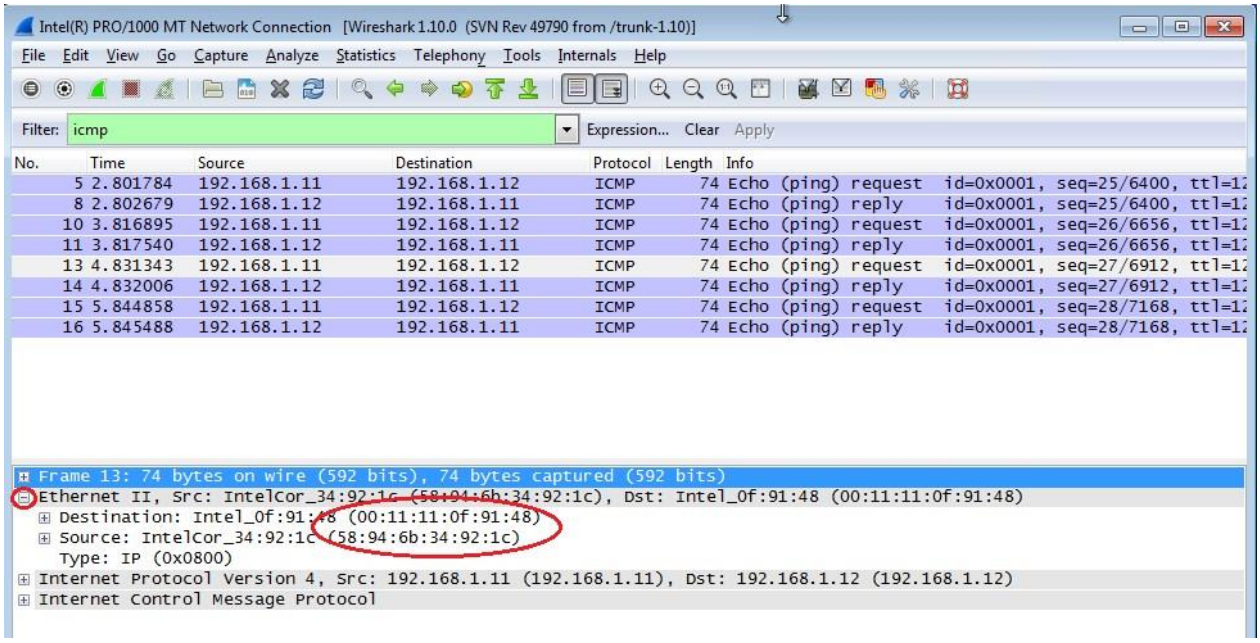
Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna Source (Origen) contiene la dirección IP de su PC y la columna Destination (Destino) contiene la dirección IP de la PC del compañero de equipo a la que hizo ping.



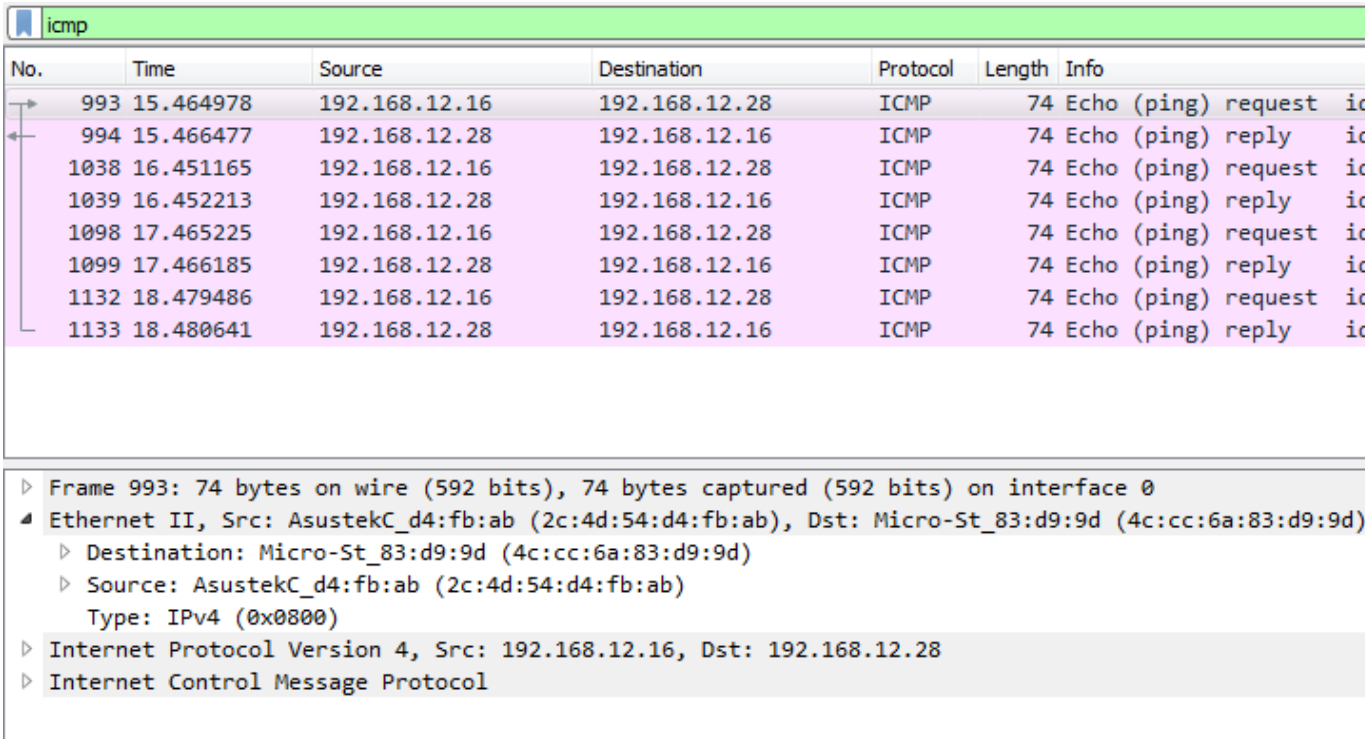
4“Muestra una captura de pantalla en Wireshark”



 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.



5"Muestra una captura de pantalla en WireShark"



6¿La dirección MAC de origen coincide con la interfaz de tú PC?

Si que coincide y es esta → 2c:4d:54:d4:fb:ab

7¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del compañero?

Si que coincide y es esta → 4c:cc:6a:83:d9:9d

8¿De qué manera tú PC obtiene la dirección MAC del PC del compañero al que hizo ping?

Consigo la ip de mi compañero mediante un ping y obtengo la dirección mac o física mediante arp.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

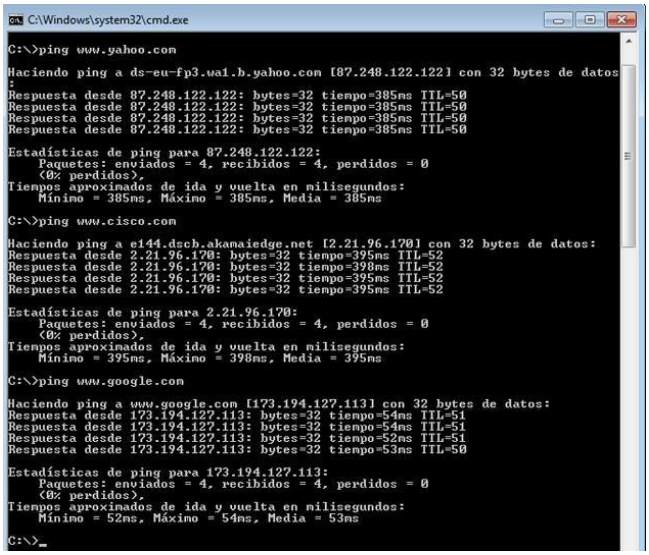
Hará ping a hosts remotos (hosts que no están en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la parte 2.

Paso 1: Comenzar a capturar datos en la interfaz

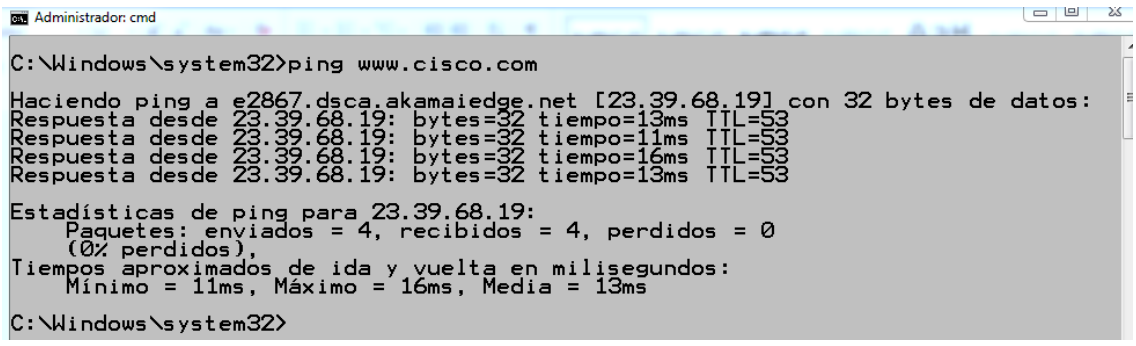
- Haga clic en el ícono Interface List para volver a abrir la lista de interfaces.
- Asegúrese de que la casilla de verificación junto a la interfaz LAN esté activada y, a continuación, haga clic en Start.
- Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en Continue without Saving (Continuar sin guardar).

- Con la captura activa, haga ping a un sitio Web:
  - www.cisco.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.



9"Muestra una captura de pantalla"



- Puede detener la captura de datos haciendo clic en el ícono Stop Capture.

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

- Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de la ubicación a la que hizo ping.

10Indique las direcciones IP y MAC de destino:

IP:23.39.68.19 ***MAC:*** 6c:3b:6b:32:44:f8

11¿Qué es importante sobre esta información?

Es importante saber que la mac que indico es la de nuestro router ya que a la mac de cisco me es imposible llegar.

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

En que cuando hago el ping en local si que obtengo la dirección mac de destino real ya que llego hasta la tarjeta de red de mi compañero, pero cuando hago el pingo a www.cisco.com solo llego hasta la mac de mi router y no hasta la mac de destino.