Parte 1: Capturar y analizar datos ICMP locales en Wireshark

En la parte 1 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, 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

1. Una vez que se inicia Wireshark, haga clic en Interface List (Lista de nterfaces).

**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).

1. Después de activar la interfaz correcta, haga clic en Start (Comenzar) para comenzar la captura de datos.
2. 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, 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)
3. 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.

1. Detenga la captura de datos haciendo clic en el íconoStop Capture (Detener captura).