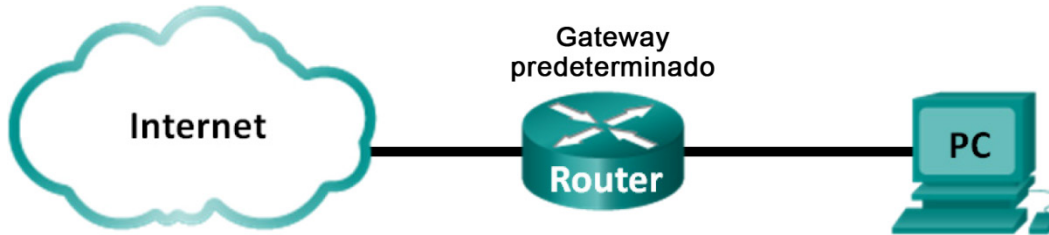


Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

Topología



Objetivos

Parte 1: Preparar Wireshark para capturar paquetes

Parte 2: Capturar, localizar y examinar paquetes

Aspectos básicos/situación

En este laboratorio, utilizará Wireshark para capturar y examinar los paquetes generados entre el navegador de PC utilizando el protocolo de transferencia de hipertexto (HTTP) y un servidor web, como www.google.com. Cuando una aplicación, como HTTP o el protocolo de transferencia de archivos (FTP), se inicia en un host, TCP utiliza la negociación en tres pasos para establecer una sesión de TCP confiable entre los dos hosts. Por ejemplo, cuando una PC utiliza un navegador web para navegar por Internet, se inicia una negociación en tres pasos y se establece una sesión entre el host de la PC y el servidor web. Una PC puede tener varias sesiones de TCP activas simultáneas con varios sitios web.

Nota: Esta práctica de laboratorio no se puede realizar con Netlab. Para esta práctica de laboratorio, se asume que usted tiene acceso a Internet.

Recursos necesarios

1 PC (Windows 7 u 8 con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

Parte 1: Preparar Wireshark para capturar paquetes

En la parte 1, debe iniciar el programa Wireshark y seleccionar la interfaz apropiada para comenzar a capturar paquetes.

Paso 1: Recuperar las direcciones de interfaz de la PC.

Para esta práctica de laboratorio, debe 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 símbolo del sistema, escriba `ipconfig /all` y luego presione Intro.

```
Physical Address. . . . . : 00-1A-73-EA-63-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%14(Preferred)
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

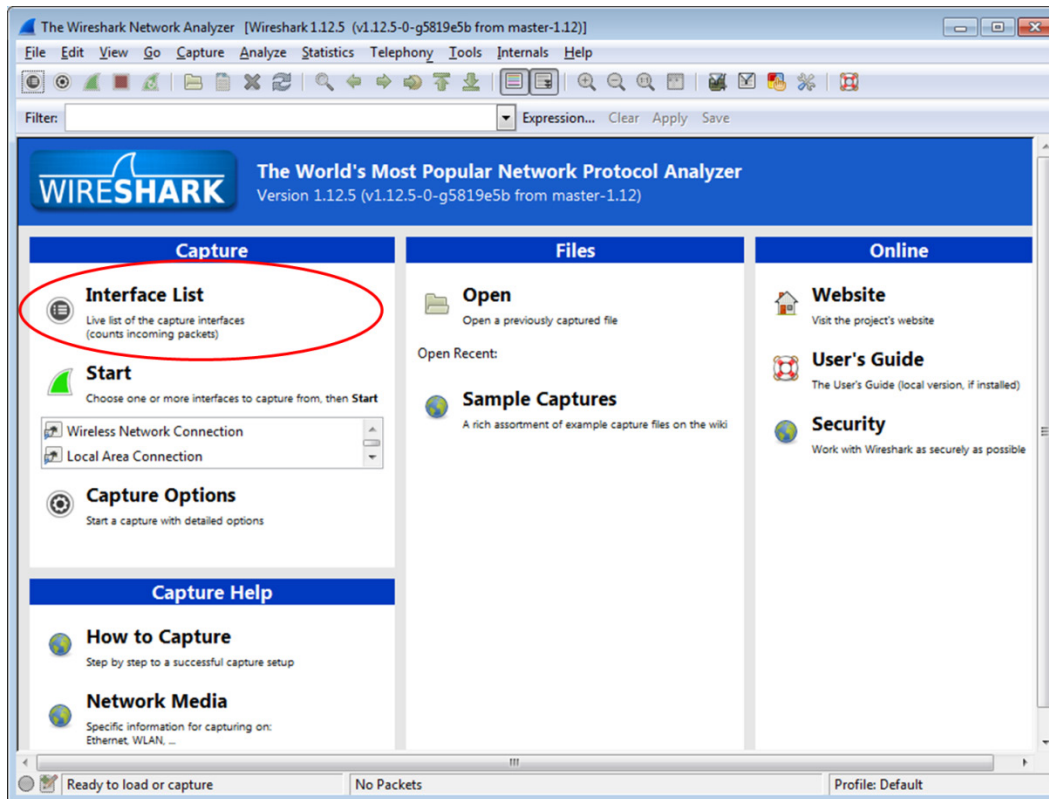
- b. Escriba las direcciones IP y MAC asociadas con el adaptador Ethernet seleccionado. Esa es la dirección de origen que debe buscar al examinar los paquetes capturados.

La dirección IP del host de la PC: _____

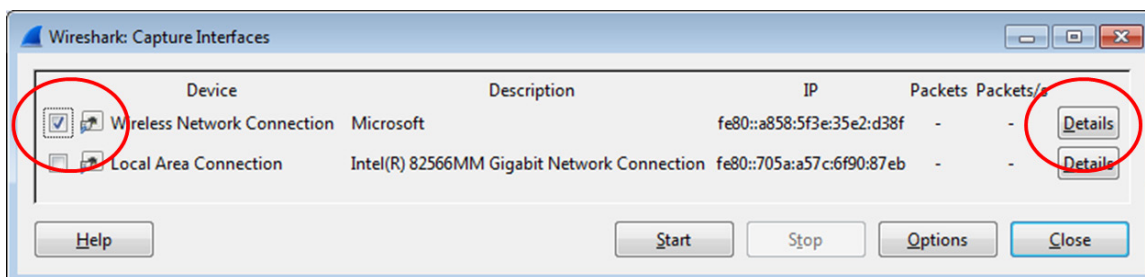
La dirección MAC del host de la PC: _____

Paso 2: Iniciar Wireshark y seleccionar la interfaz apropiada.

- a. Haga clic en el botón **Inicio** de Windows. En el menú emergente, haga doble clic en **Wireshark**.
b. Luego de que se inicia Wireshark, haga clic en la **Lista de interfaces**.



- c. En la ventana **Wireshark: Capture Interfaces** (Wireshark: Interfaces de captura), haga clic en la casilla de verificación junto a la interfaz que está conectada a su LAN.



Nota: Si aparecen varias interfaces y no está seguro de cuál interfaz debe seleccionar, haga clic en **Details** (Detalles). Haga clic en la ficha **802.3 (Ethernet)** y compruebe que la dirección MAC coincida con la que se introdujo en el paso 1b. Cierre la ventana Interface Details (Detalles de la interfaz) después de la verificación.

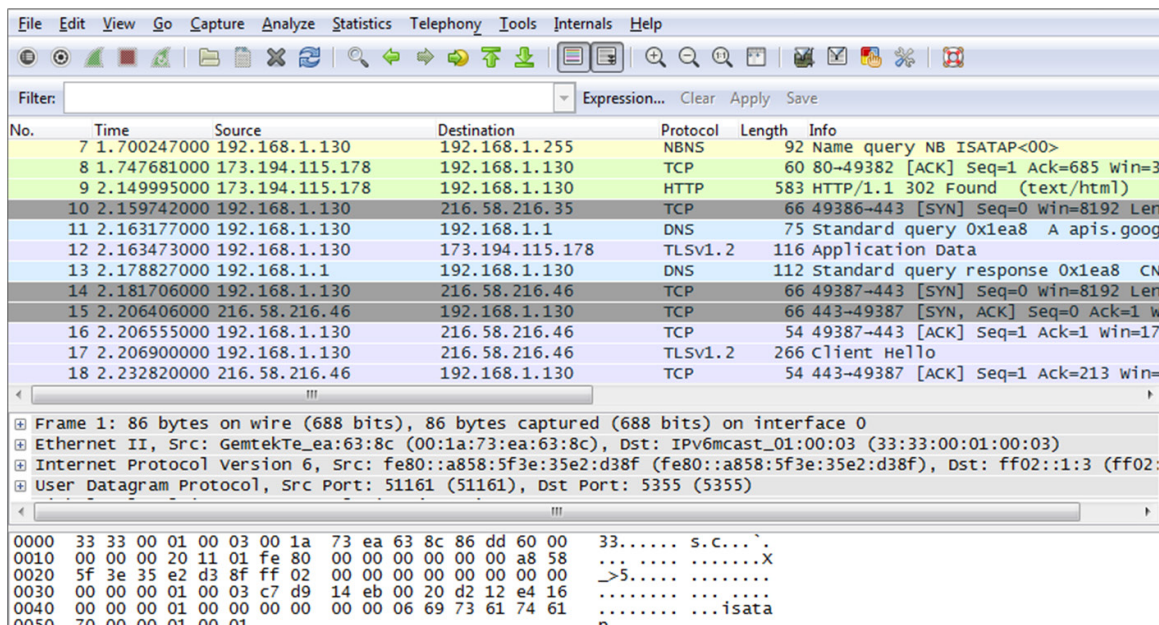
Parte 2: Capturar, localizar y examinar paquetes

Paso 1: Capturar los datos.

- Haga clic en el botón **Start** (Comenzar) para iniciar la captura de datos.
- Ingrese a www.google.com. Minimice el navegador y regrese a Wireshark. Detenga la captura de datos.

Nota: Es posible que su instructor le proporcione un sitio web diferente. Si es así, escriba el nombre o la dirección del sitio web aquí:

La ventana de captura ahora está activa. Localice las columnas **Source** (Origen), **Destination** (Destino) y **Protocol** (Protocolo).



Paso 2: Localizar los paquetes correspondientes para la sesión web.

Si el equipo se inició hace poco y no hubo ninguna actividad de acceso a Internet, podrá ver todo el proceso en el resultado capturado, incluido el protocolo de resolución de direcciones (ARP), el sistema de nombres de dominio (DNS) y la negociación en tres pasos de TCP. Si el equipo ya tenía una entrada de ARP para el gateway predeterminado, se inició con la consulta DNS para resolver www.google.com.

- La trama 11 muestra la consulta DNS de la PC al servidor DNS, que está intentando resolver el nombre de dominio www.google.com a la dirección IP del servidor web. La PC debe tener la dirección IP para poder enviar el primer paquete al servidor web.

¿Cuál es la dirección IP del servidor DNS que consultó el equipo? _____

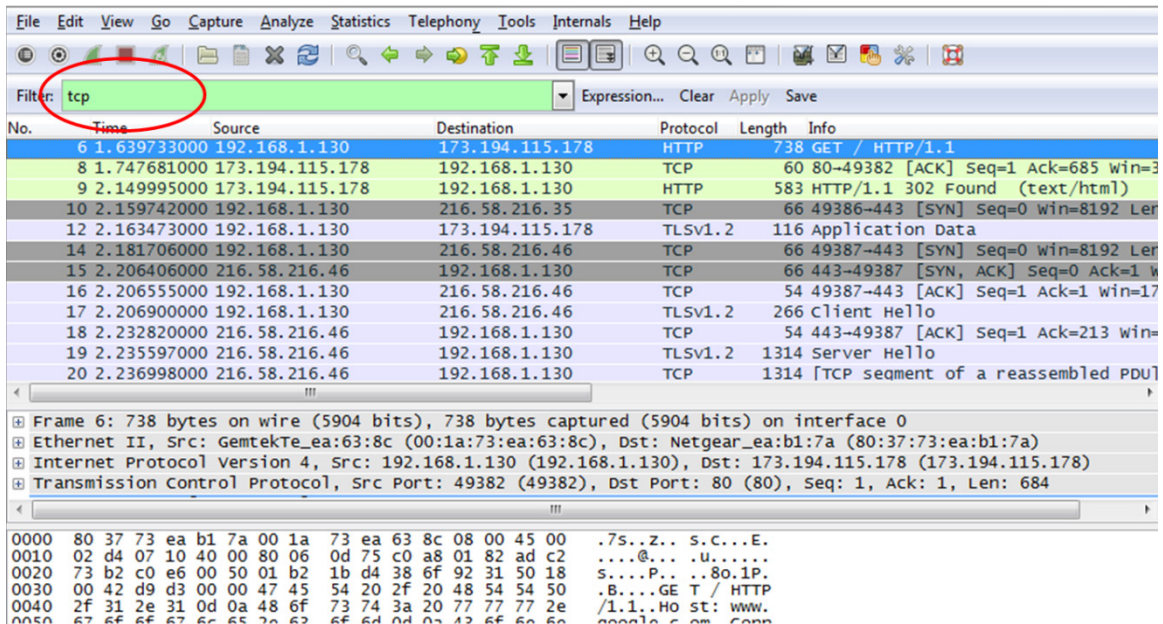
- La trama 13 es la respuesta del servidor DNS. Contiene la dirección IP de www.google.com.

- Encuentre el paquete correspondiente para iniciar la negociación en tres pasos. En el ejemplo, la trama 14 es el inicio de la negociación en tres pasos de TCP.

¿Cuál es la dirección IP del servidor web de Google? _____

Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

- d. Si tiene muchos paquetes que no están relacionados con la conexión de TCP, puede ser necesario utilizar la herramienta de filtro de Wireshark. Escriba **tcp** en el área de entrada del filtro dentro de Wireshark y presione **Intro**.



Paso 3: Examine la información dentro de los paquetes, incluidas las direcciones IP, los números de puerto TCP y los marcadores de control de TCP.

- a. En nuestro ejemplo, la trama 14 es el inicio de la negociación en tres pasos entre la PC y el servidor web de Google. En el panel de la lista de paquetes (sección superior de la ventana principal), seleccione la trama. De esta forma, se selecciona la línea y se muestra la información decodificada de ese paquete en los dos paneles inferiores. Examine la información de TCP en el panel de detalles del paquete (sección media de la ventana principal).
- b. Haga clic en el ícono + a la izquierda del protocolo de control de transmisión en el panel de detalles del paquete para ampliar la vista de la información de TCP.

Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

- c. Haga clic en el ícono + a la izquierda de los marcadores. Busque los puertos de origen y destino y los marcadores establecidos.

Nota: Es posible que deba ajustar los tamaños de las ventanas superior y media dentro de Wireshark para mostrar la información necesaria.

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
8	1.747681000	173.194.115.178	192.168.1.130	TCP	60	80-49382 [ACK] Seq=1 Ack=685 win=:
9	2.149995000	173.194.115.178	192.168.1.130	HTTP	583	HTTP/1.1 302 Found (text/html)
10	2.159742000	192.168.1.130	216.58.216.35	TCP	66	49386-443 [SYN] Seq=0 win=8192 Len:
12	2.163473000	192.168.1.130	173.194.115.178	TLSv1.2	116	Application Data
14	2.181706000	192.168.1.130	216.58.216.46	TCP	66	49387-443 [SYN] Seq=0 win=8192 Len:
15	2.206406000	216.58.216.46	192.168.1.130	TCP	66	443-49387 [SYN, ACK] Seq=0 Ack=1 V
16	2.206555000	192.168.1.130	216.58.216.46	TCP	54	49387-443 [ACK] Seq=1 Ack=1 win=17
17	2.206600000	192.168.1.130	216.58.216.46	TCP	266	Client Hello

Frame 14: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

- Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
- Internet Protocol Version 4, Src: 192.168.1.130 (192.168.1.130), Dst: 216.58.216.46 (216.58.216.46)
- Transmission Control Protocol, Src Port: 49387 (49387), Dst Port: 443 (443), Seq: 0, Len: 0
 - Source Port: 49387 (49387)
 - Destination Port: 443 (443)
 - [Stream index: 3]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - Acknowledgment number: 0
 - Header Length: 32 bytes
 - ... 0000 0000 0010 = Flags: 0x002 (SYN)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - ... 0... = Congestion window Reduced (cwr): Not set
 - 0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -0 = Acknowledgment: Not set
 - 0.. = Push: Not set
 - 0.. = Reset: Not set
 -1. = Syn: Set
 -0 = Fin: Not set
 - Window size value: 8192
 - [Calculated window size: 8192]
 - Checksum: 0x5c37 [validation disabled]
 - Urgent pointer: 0

¿Cuál es el número de puerto de origen de TCP? _____

¿Cómo clasificaría el puerto de origen? _____

¿Cuál es el número de puerto de destino de TCP? _____

¿Cómo clasificaría el puerto de destino? _____

¿Qué marcadores están establecidos? _____

¿Qué número de secuencia relativo está establecido? _____

Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

- d. Para seleccionar la próxima trama en la negociación en tres pasos, seleccione **Go** (Ir) en el menú de Wireshark y seleccione **Next Packet In Conversation** (Siguiente paquete en la conversación). En este ejemplo, es la trama 15. Esta es la respuesta del servidor web de Google a la solicitud inicial para iniciar una sesión.

The screenshot shows the Wireshark interface with the following details for packet 15:

- Packet List:** Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0. Protocol: TCP. Length: 66. Info: 443-49387 [SYN, ACK] Seq=0 Ack=1 win=17.
- Packet Details:**
 - Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)
 - Internet Protocol Version 4, Src: 216.58.216.46 (216.58.216.46), Dst: 192.168.1.130 (192.168.1.130)
 - Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49387 (49387), Seq: 0, Ack: 1, Len: 0
 - Source Port: 443 (443)
 - Destination Port: 49387 (49387)
 - [Stream index: 3]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - Header Length: 32 bytes
 - Flags: 0x012 (SYN, ACK)
 - Reserved: Not set
 - Nonce: Not set
 - Congestion window Reduced (CWR): Not set
 - ECN-Echo: Not set
 - Urgent: Not set
 - Acknowledgment: Set
 - Push: Not set
 - Reset: Not set
 - Syn: Set
 - Fin: Not set
 - Window size value: 42900
 - [Calculated window size: 42900]
 - Checksum: 0xf159 [validation disabled]
 - Urgent pointer: 0

¿Cuáles son los valores de los puertos de origen y destino? _____

¿Qué marcadores están establecidos? _____

¿Qué números relativos de secuencia y reconocimiento están establecidos? _____

Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

- e. Finalmente, examine el tercer paquete de la negociación en tres pasos del ejemplo. Haga clic en la trama 16 en la ventana superior para mostrar la siguiente información en este ejemplo:

The screenshot shows the Wireshark interface with the following details:

- Filter:** tcp
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
12	2.163473000	192.168.1.130	173.194.115.178	TLSv1.2	116	Application Data
14	2.181706000	192.168.1.130	216.58.216.46	TCP	66	49387→443 [SYN] Seq=0 Win=8192 Len=0
15	2.206406000	216.58.216.46	192.168.1.130	TCP	66	443→49387 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
16	2.206555000	192.168.1.130	216.58.216.46	TCP	54	49387→443 [ACK] Seq=1 Ack=1 Win=17408 Len=0
17	2.206900000	192.168.1.130	216.58.216.46	TLSv1.2	266	Client Hello
18	2.232820000	216.58.216.46	192.168.1.130	TCP	54	443→49387 [ACK] Seq=1 Ack=213 Win=0 Len=0
19	2.235597000	216.58.216.46	192.168.1.130	TLSv1.2	1314	Server Hello
- Packet 16 Details:**
 - Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 - Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Internet Protocol Version 4, Src: 192.168.1.130 (192.168.1.130), Dst: 216.58.216.46 (216.58.216.46)
 - Transmission Control Protocol, Src Port: 49387 (49387), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 0
 - Source Port: 49387 (49387)
 - Destination Port: 443 (443)
 - [Stream index: 3]
 - [TCP Segment Len: 0]
 - Sequence number: 1 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - Header Length: 20 bytes
 - Flags: 0x010 (ACK)
 - Reserved: Not set
 - Nonce: Not set
 - Congestion window Reduced (CWR): Not set
 - ECN-Echo: Not set
 - Urgent: Not set
 - Acknowledgment: Set
 - Push: Not set
 - Reset: Not set
 - Syn: Not set
 - Fin: Not set
 - Window size value: 68
 - [Calculated window size: 17408]
 - [Window size scaling factor: 256]
 - Checksum: 0xd95e [validation disabled]

Examine el tercer y último paquete de la negociación.

¿Qué marcadores están establecidos?

Los números relativos de secuencia y reconocimiento están establecidos en 1 como punto de inicio. La conexión TCP está establecida, y la comunicación entre el equipo de origen y el servidor web puede comenzar.

- f. Cierre el programa Wireshark.

Reflexión

1. Hay cientos de filtros disponibles en Wireshark. Una red grande podría tener numerosos filtros y muchos tipos diferentes de tráfico. Mencione tres filtros que podrían ser útiles para un administrador de redes.

2. ¿De qué otras maneras podría utilizarse Wireshark en una red de producción?