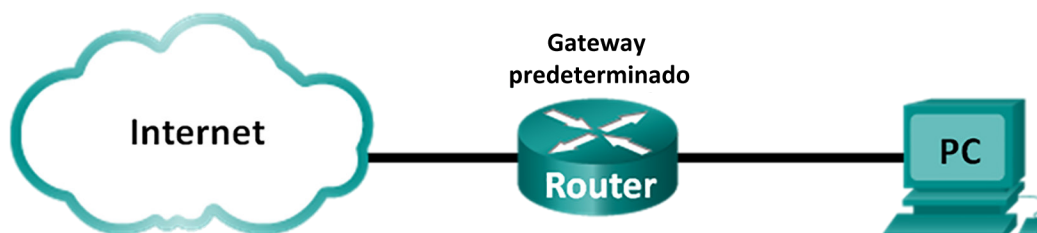


Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

Topología



Objetivos

Parte 1: Preparar Wireshark para capturar paquetes

Parte2: 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 FTP (protocolo de transferencia de archivos), 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, 8 o 10 con acceso a la petición de ingreso de comando, 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 Enter (Introducir).

```

Physical Address. . . . . : 00-24-D7-1C-50-44
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80dd:5657:ad20:f4b3%16(Preferred)
IPv4 Address. . . . . : 192.168.1.146(Preferred)
Subnet Mask . . . . . : 255.255.255.0
  
```

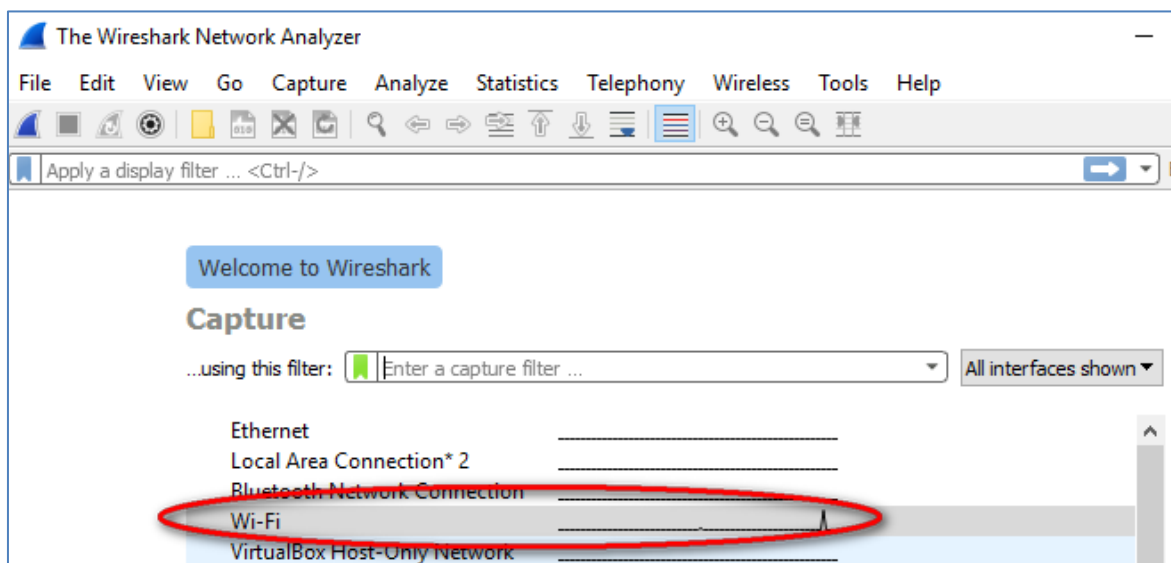
- b. Escriba las direcciones IP y MAC asociadas con el adaptador Ethernet seleccionado. Esa es la dirección de origen que debe buscar al examinar los paquetes capturados.

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

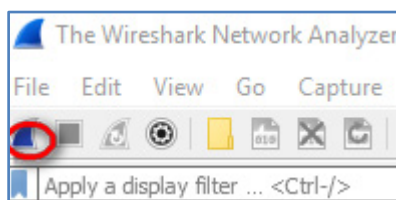
- a. Haga clic en el botón **Inicio** de Windows. En el menú emergente, haga doble clic en **Wireshark**.
- b. Después de que se inicie Wireshark, seleccione la interfaz activa para captura de datos. La interfaz activa muestra las actividades de tráfico.



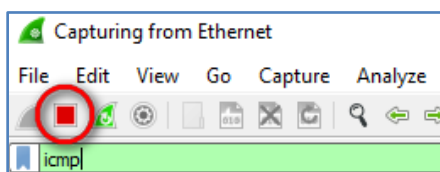
Parte 2: Capturar, localizar y examinar paquetes

Paso 1: Capturar los datos

- a. Haga clic en el botón **Start** (Comenzar) para iniciar la captura de datos.

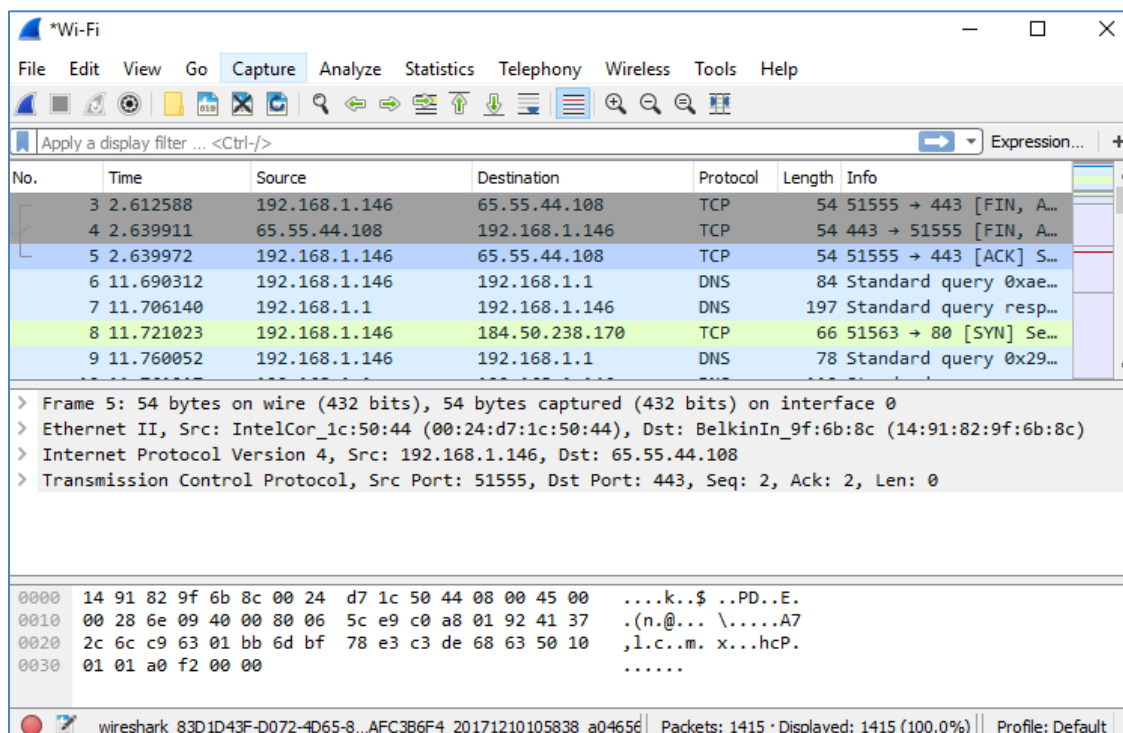


- b. Abra un navegador web y escriba www.google.com.
- c. Minimice el navegador y regrese a Wireshark. Detenga la captura de datos.



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).

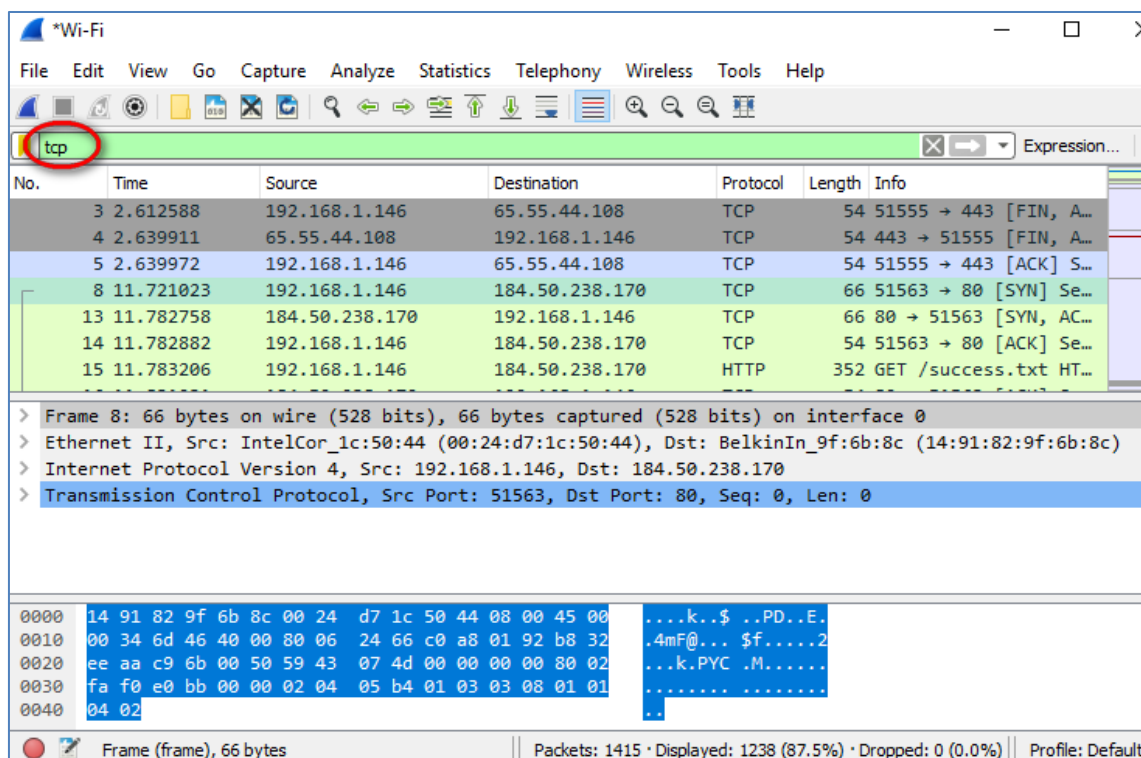


Paso 2: Localizar los paquetes correspondientes para la sesión web

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, como 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 ARP para el gateway predeterminado, se inició con la consulta DNS para resolver `www.google.com`.

- La trama 6 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 7 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 8 es el inicio de la negociación en tres pasos de TCP.
¿Cuál es la dirección IP del servidor web de Google? _____

- 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 **Enter** (Introducir).



Paso 3: Examinar la información dentro de los paquetes, como las direcciones IP, los números de puerto TCP y los marcadores de control de TCP

- En nuestro ejemplo, la trama 8 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).
- 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.
- 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.

The screenshot shows the Wireshark interface with a packet capture of a TCP SYN sequence. The packet list at the top shows frames 3 through 15. Frame 8 is selected, showing details of a SYN packet from 192.168.1.146 to 184.50.238.170.

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
Internet Protocol Version 4, Src: 192.168.1.146, Dst: 184.50.238.170
Transmission Control Protocol, Src Port: 51563, Dst Port: 80, Seq: 0, Len: 0
Source Port: 51563
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
1000 = Header Length: 32 bytes (8)
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
[TCP Flags:S.]
Window size value: 64240
[Calculated window size: 64240]
Checksum: 0xe0bb [unverified]
[Checksum Status: Unverified]
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? _____

- 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 13. 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:

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
Internet Protocol Version 4, Src: 184.50.238.170, Dst: 192.168.1.146
Transmission Control Protocol, Src Port: 80, Dst Port: 51563, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 51563
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
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: Set
...0... = Push: Not set
...0... = Reset: Not set
...0... = Syn: Set
...0... = Fin: Not set
[TCP Flags:A..S..]
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0x3a72 [unverified]
[Checksum Status: Unverified]
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?

- e. Finalmente, examine el tercer paquete de la negociación en tres pasos del ejemplo. Haga clic en la trama 14 en la ventana superior para mostrar la siguiente información en este ejemplo:

The screenshot shows the Wireshark interface with the packet list pane at the top and the packet details pane below it. The packet list pane shows a list of packets, with packet 14 selected. The packet details pane shows the details of packet 14, which is a TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)

Internet Protocol Version 4, Src: 192.168.1.146, Dst: 184.50.238.170

Transmission Control Protocol, Src Port: 51563, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 51563

Destination Port: 80

[Stream index: 1]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:A....]

Window size value: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

Checksum: 0xec52 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

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?
