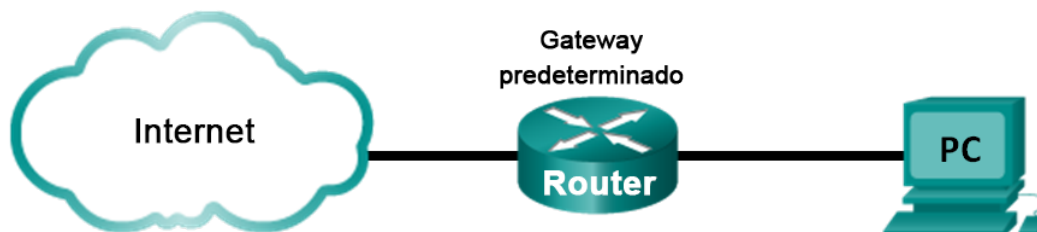


# Práctica de laboratorio: Uso de Wireshark para observar el protocolo TCP de enlace de tres vías (versión para el instructor)

**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: Preparar Wireshark para la captura de paquetes

- Seleccionar una interfaz NIC apropiada para capturar paquetes.

### Parte 2: Capturar, localizar y examinar paquetes

- Capturar una sesión Web para [www.google.com](http://www.google.com).
- Localizar paquetes apropiados para una sesión Web.
- Examinar la información de los paquetes, como direcciones IP, números de puerto TCP e indicadores de control TCP.

## Información básica/Situación

En esta práctica de laboratorio, utilizará Wireshark para capturar y examinar paquetes que se generan entre el explorador de la PC mediante el protocolo de transferencia de hipertexto (HTTP) y un servidor Web, como [www.google.com](http://www.google.com). Cuando una aplicación, como HTTP o el protocolo de transferencia de archivos (FTP), se inicia primero en un host, TCP utiliza el protocolo de enlace de tres vías para establecer una sesión TCP confiable entre los dos hosts. Por ejemplo, cuando una PC utiliza un explorador Web para navegar por Internet, se inicia un protocolo de enlace de tres vías y se establece una sesión entre el host de la PC y el servidor Web. Una PC puede tener varias sesiones TCP simultáneas activas con diversos sitios Web.

**Nota:** esta práctica de laboratorio no se puede realizar utilizando Netlab. Para la realización de esta práctica de laboratorio, se da por sentado que tiene acceso a Internet.

**Nota para el instructor:** 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.

## Recursos necesarios

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

## Parte 1: Preparar Wireshark para capturar paquetes

En la parte 1, inicia el programa Wireshark y selecciona la interfaz apropiada para comenzar a capturar paquetes.

### Paso 1: Recuperar las direcciones de la 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 del símbolo del sistema, escriba **ipconfig /all** y luego presione Entrar.

```
Physical Address. . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 01, 2012 1:43:35 PM
Lease Expires . . . . . : Sunday, December 02, 2012 1:43:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

- b. Anote las direcciones IP y MAC asociadas al adaptador Ethernet seleccionado, ya que esa es la dirección de origen que debe buscar al examinar los paquetes capturados.

Dirección IP del host de la PC: \_\_\_\_\_

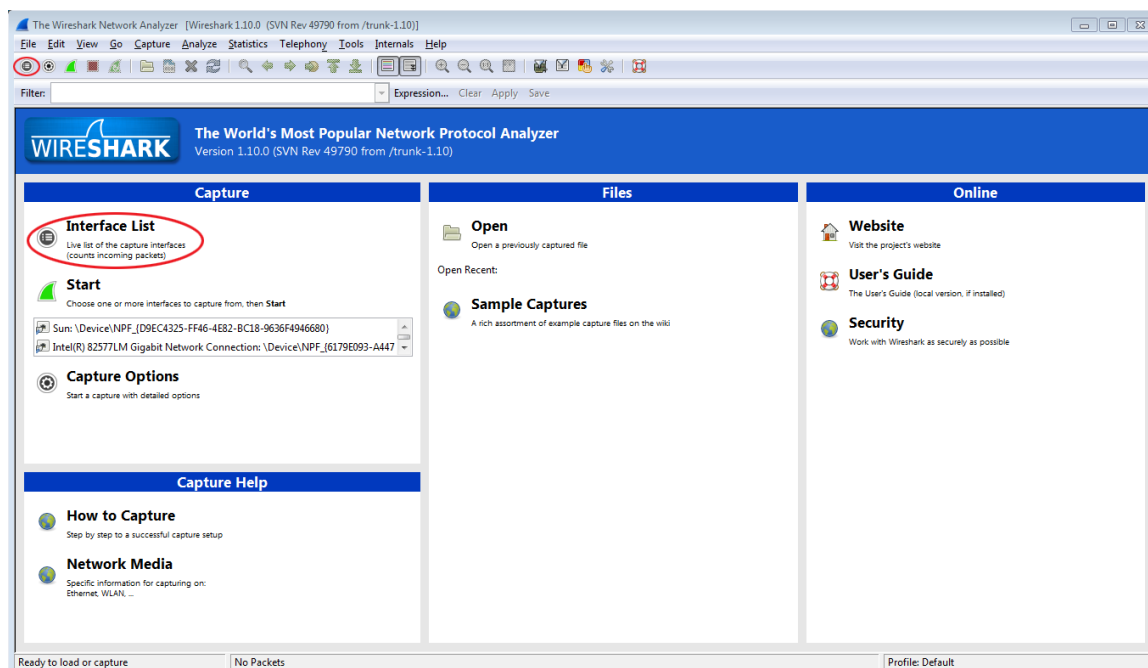
Las respuestas pueden variar. En este caso, 192.168.1.130.

Dirección MAC del host de la PC: \_\_\_\_\_

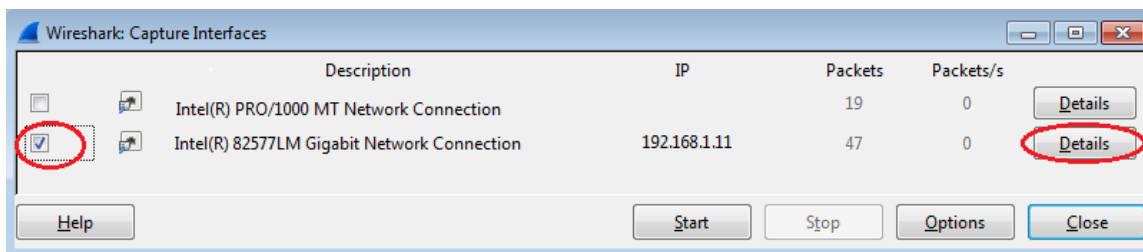
Las respuestas pueden variar. En este caso, C8:0A:A9:FA:DE:0D.

### Paso 2: Iniciar Wireshark y seleccionar la interfaz apropiada

- a. Haga clic en el botón **Inicio** de Windows y, en el menú emergente, haga doble clic en **Wireshark**.
- b. Una vez que se inicia Wireshark, haga clic en **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 **Details** (Detalles). Haga clic en la ficha **802.3 (Ethernet)** y verifique que la dirección MAC coincida con la que anotó en el paso 1b. Después de realizar esta verificación, cierre la ventana Interface Details (Detalles de la interfaz).

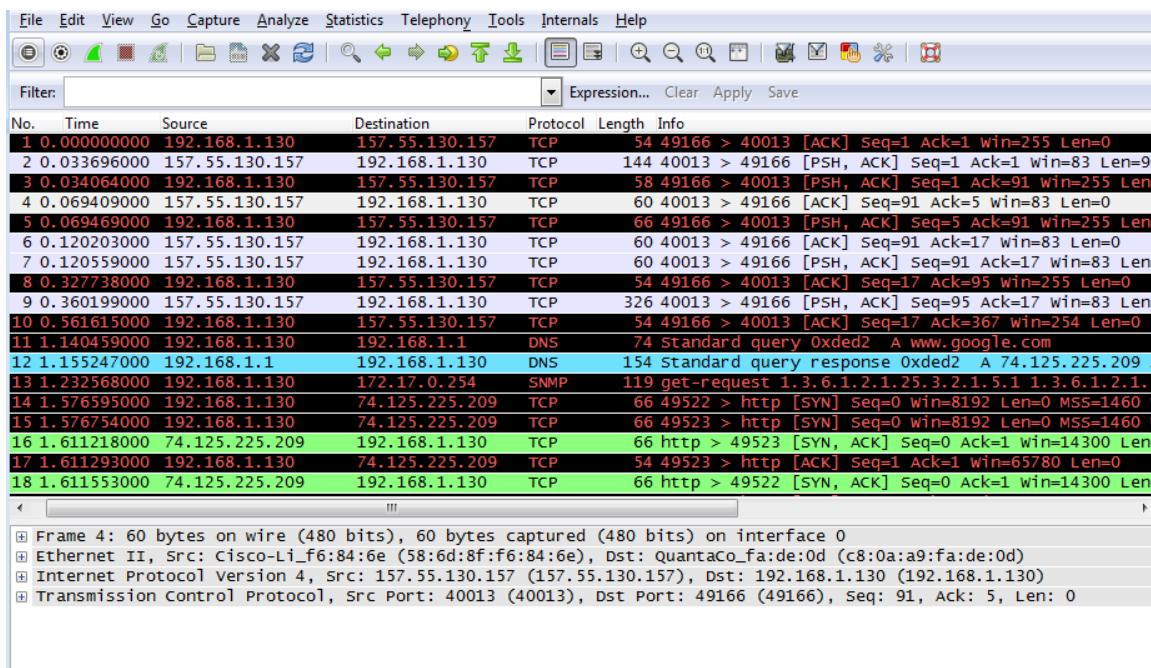
## Parte 2: Capturar, localizar y examinar paquetes

### Paso 1: Hacer clic en el botón Start (Comenzar) para iniciar la captura de datos

- a. Acceda a [www.google.com](http://www.google.com). Minimice la ventana de Google y vuelva a Wireshark. Detenga la captura de datos. Debería ver tráfico capturado similar al que se muestra a continuación, en el paso b.

**Nota:** es posible que el instructor le proporcione un sitio Web diferente. En ese caso, introduzca el nombre del sitio Web o la dirección aquí:

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



## Paso 2: Localizar paquetes adecuados para la sesión Web

Si la PC se inició recientemente y no hubo actividad al acceder a Internet, puede ver todo el proceso en el resultado de la captura, incluido el protocolo de resolución de direcciones (ARP), el sistema de nombres de dominios (DNS) y el protocolo TCP de enlace de tres vías. La captura de pantalla de la parte 2, paso 1, muestra todos los paquetes que la PC debe obtener para [www.google.com](http://www.google.com). En este caso, la PC ya tenía una entrada de ARP para el gateway predeterminado; por lo tanto, comenzó con la consulta DNS para resolver [www.google.com](http://www.google.com).

- En la trama 11, se muestra la consulta DNS de la PC al servidor DNS, mediante la que se intenta resolver el nombre de dominio, [www.google.com](http://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 la PC? \_\_\_\_\_

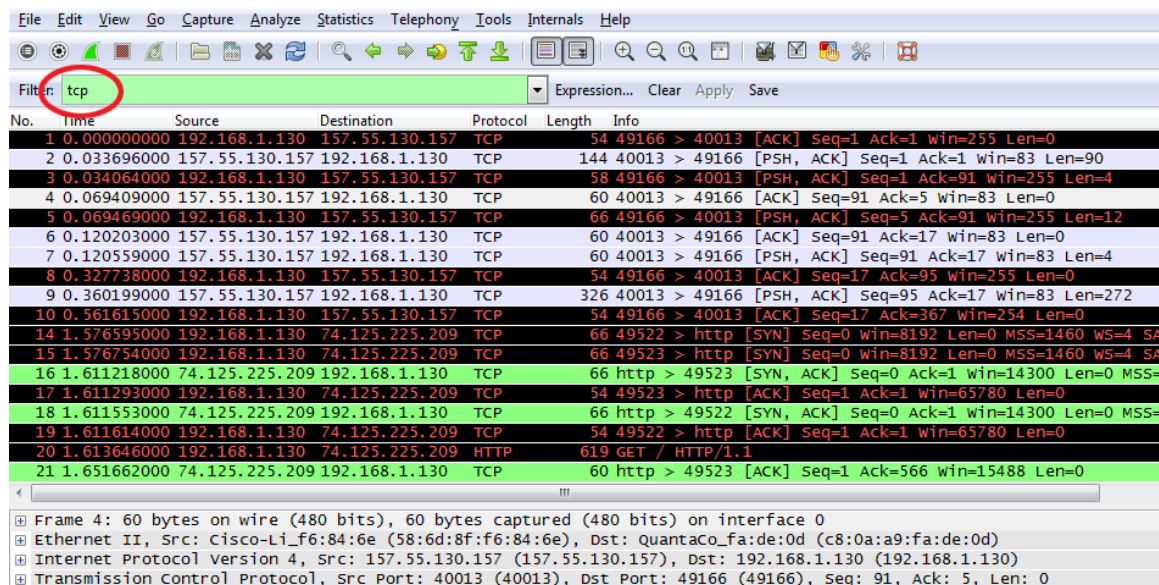
192.168.1.1

- La trama 12 es la respuesta del servidor DNS con la dirección IP de [www.google.com](http://www.google.com).
- Busque el paquete apropiado para iniciar el protocolo de enlace de tres vías. En este ejemplo, la trama 15 es el inicio del protocolo TCP de enlace de tres vías.

¿Cuál es la dirección IP del servidor Web de Google? \_\_\_\_\_

En este ejemplo, 74.125.225.209.

- Si tiene muchos paquetes que no están relacionados con la conexión TCP, es posible que sea necesario usar la capacidad de filtro de Wireshark. Escriba **tcp** en el área de entrada de filtro de Wireshark y presione Entrar.

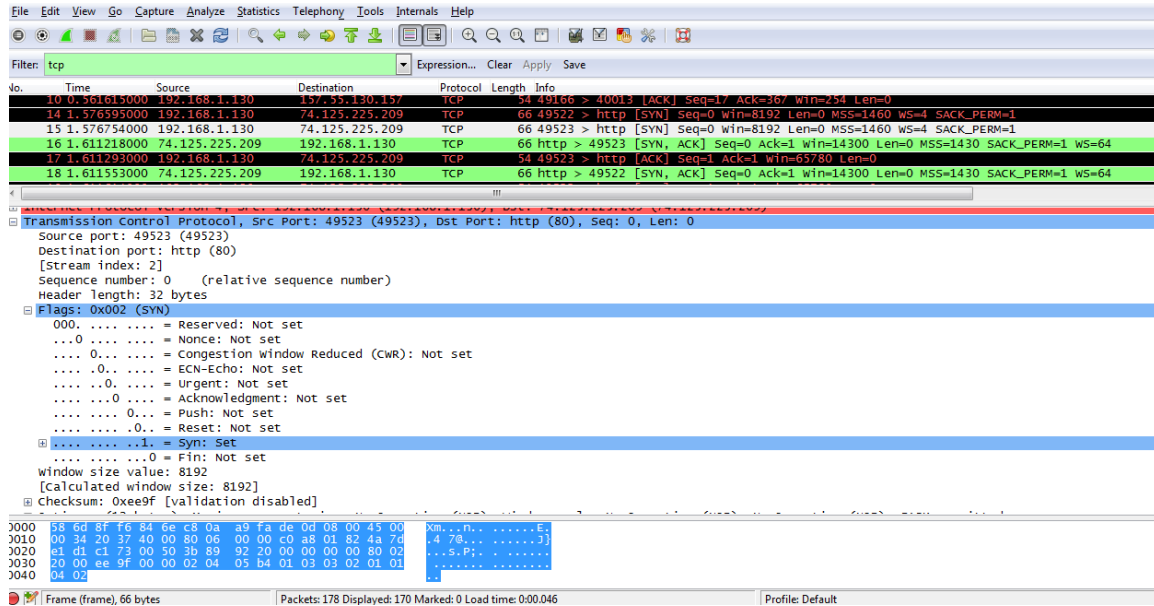


## Paso 3: Examinar la información de los paquetes, como direcciones IP, números de puerto TCP e indicadores de control TCP

- En el ejemplo, la trama 15 es el inicio del protocolo de enlace de tres vías entre la PC y el servidor Web de Google. En el panel de la lista de paquetes (en la sección superior de la ventana principal), seleccione la trama. La línea se resalta, y en los dos paneles inferiores se muestra la información decodificada proveniente de ese paquete. Examine la información de TCP en el panel de detalles del paquete (sección media de la ventana principal).
- Haga clic en el ícono + que se encuentra a la izquierda del protocolo de control de transmisión (TCP) del panel de detalles del paquete para ampliar la vista de la información de TCP.

- c. Haga clic en el ícono **+** que está a la izquierda de los indicadores. Observe los puertos de origen y destino y los indicadores que están establecidos.

**Nota:** es posible que tenga que ajustar los tamaños de las ventanas superior y media de Wireshark para visualizar la información necesaria.



¿Cuál es el número de puerto de origen TCP? 49523 En este ejemplo, el puerto de origen es 49523. Las respuestas varían

¿Cómo clasificaría el puerto de origen? Dinámico o privado

¿Cuál es el número de puerto de destino TCP? 80

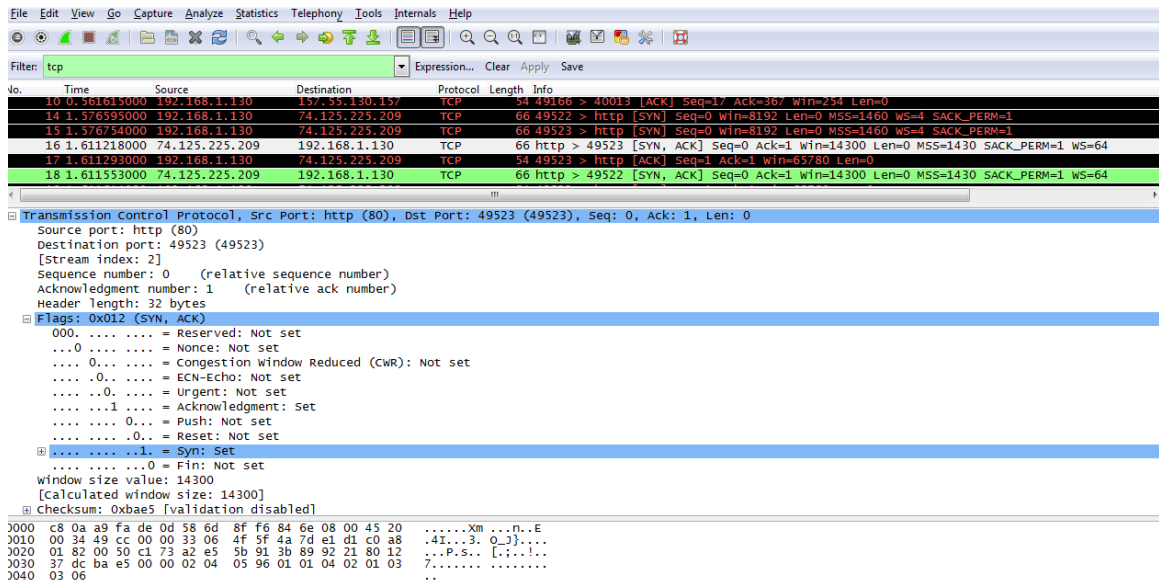
¿Cómo clasificaría el puerto de destino? Conocido, registrado (HTTP o protocolo Web)

¿Qué indicadores están establecidos? Indicador SYN

¿Cuál es el número de secuencia relativa establecido? 0

- d. Para seleccionar la próxima trama en le protocolo de enlace de tres vías, seleccione **Go** (Ir) en la barra de menús de Wireshark y, luego, **Next Packet in Conversation** (Siguiente paquete de la conversación). En este ejemplo, es la trama 16. Esta es la respuesta del servidor Web de Google a la solicitud inicial para iniciar una sesión.

## Práctica de laboratorio: Uso de Wireshark para observar el protocolo TCP de enlace de tres vías



No.	Time	Source	Destination	Protocol	Length	Info
10	0.261615000	192.168.1.130	192.168.1.130	ICMP	24	19166 > 40013 [ACK] Seq=17 Ack=367 Win=254 Len=0
14	1.576595000	192.168.1.130	74.125.225.209	TCP	66	49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	1.611218000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17	1.611293000	192.168.1.130	74.125.225.209	TCP	54	49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18	1.611553000	74.125.225.209	192.168.1.130	TCP	66	http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64

Transmission Control Protocol, Src Port: http (80), Dst Port: 49523 (49523), Seq: 0, Ack: 1, Len: 0

Source port: http (80)  
Destination port: 49523 (49523)  
[Stream index: 2]  
Sequence number: 0 (relative sequence number)  
Acknowledgment number: 1 (relative ack number)  
Header length: 32 bytes

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  
.... ..1... = Acknowledgment: Set  
.... .... 0... = Push: Not set  
.... .... 0.. = Reset: Not set  
...1... ..1. = Syn: set  
.... .... 0 = Fin: Not set  
Window size value: 14300  
[calculated window size: 14300]  
Checksum: 0xbae5 [validation disabled]

3000 c8 0a a9 fa de 0d 58 6d 8f f6 84 6e 08 00 45 20 .....Xm...n...E  
3010 00 34 49 cc 00 00 33 06 4f 5f 4a 7d e1 d1 c0 a8 ...4I...3. 0\_J}...  
3020 01 82 00 50 c1 73 33 e5 3b 91 3b 89 92 21 80 12 ...P.s..[...!..  
3030 37 dc ba e5 00 00 02 04 05 96 01 01 04 02 01 03 .....  
3040 03 06 ..

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

El puerto de origen ahora es 80 y el puerto de destino ahora es 49523.

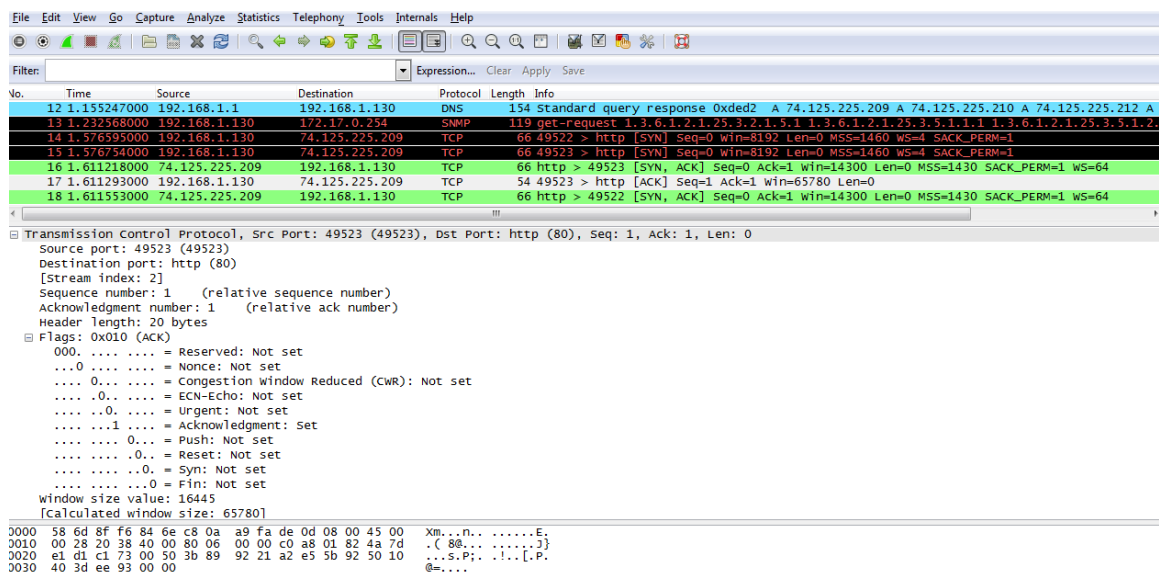
¿Qué indicadores están establecidos?

El indicador de acuse de recibo (ACK) y el indicador de sincronización (SYN).

¿Cuáles son los números de acuse de recibo y de secuencia relativa establecidos?

El número de secuencia relativa es 0 y el número de acuse de recibo es 1.

- e. Por último, examine el tercer paquete del protocolo de enlace de tres vías en el ejemplo. Al hacer clic en la trama 17 en la ventana superior, aparece la siguiente información en este ejemplo:



No.	Time	Source	Destination	Protocol	Length	Info
12	1.155247000	192.168.1.1	192.168.1.130	DNS	154	standard query response Oxded2 A 74.125.225.210 A 74.125.225.212 A
13	1.232968000	192.168.1.130	172.17.0.254	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.3.1.1.1 1.3.6.1.2.1.25.3.5.1.2
14	1.576595000	192.168.1.130	74.125.225.209	TCP	66	49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	1.611218000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17	1.611293000	192.168.1.130	74.125.225.209	TCP	54	49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18	1.611553000	74.125.225.209	192.168.1.130	TCP	66	http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64

Transmission Control Protocol, Src Port: 49523 (49523), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Source port: 49523 (49523)  
Destination port: http (80)  
[Stream index: 2]  
Sequence number: 1 (relative sequence number)  
Acknowledgment number: 1 (relative ack number)  
Header length: 20 bytes

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  
Window size value: 16445  
[calculated window size: 65780]

3000 58 6d 8f f6 84 6e c8 0a a9 fa de 0d 08 00 45 00 Xm...n...E;  
3010 00 28 20 38 40 00 80 06 00 00 c0 a8 01 82 43 00 { @8...c0...3  
3020 e1 d1 c1 73 00 50 3b 89 92 21 a2 e5 5b 92 50 10 ...s.P;...!...[P.  
3030 40 3d ee 93 00 00 @=....

Examine el tercer y último paquete del protocolo de enlace.

¿Qué indicadores están establecidos?

---

Indicador de acuse de recibo (ACK)

Los números de acuse de recibo y de secuencia relativa están establecidos en 1 como punto de inicio. La conexión TCP ahora está establecida, y la comunicación entre la PC 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 puede tener numerosos filtros y muchos tipos de tráfico diferentes. ¿Cuáles son los tres filtros de la lista que podrían ser los más útiles para un administrador de red?

---

Las respuestas varían, pero podrían incluir TCP, direcciones IP específicas (de origen o destino) y protocolos como HTTP.

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

---

Wireshark suele utilizarse con fines de seguridad, para el análisis posterior del tráfico normal o después de un ataque de red. Es posible que se deban capturar nuevos protocolos o servicios para determinar qué puerto o puertos se utilizan.