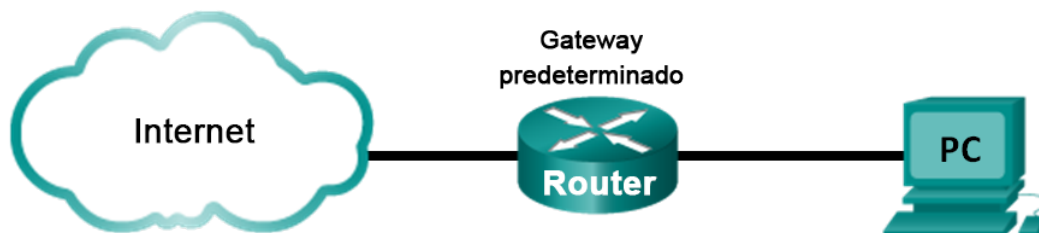


# Práctica de laboratorio: Uso de Wireshark para observar el protocolo TCP de enlace de tres vías

## 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.

## 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".

- 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
```

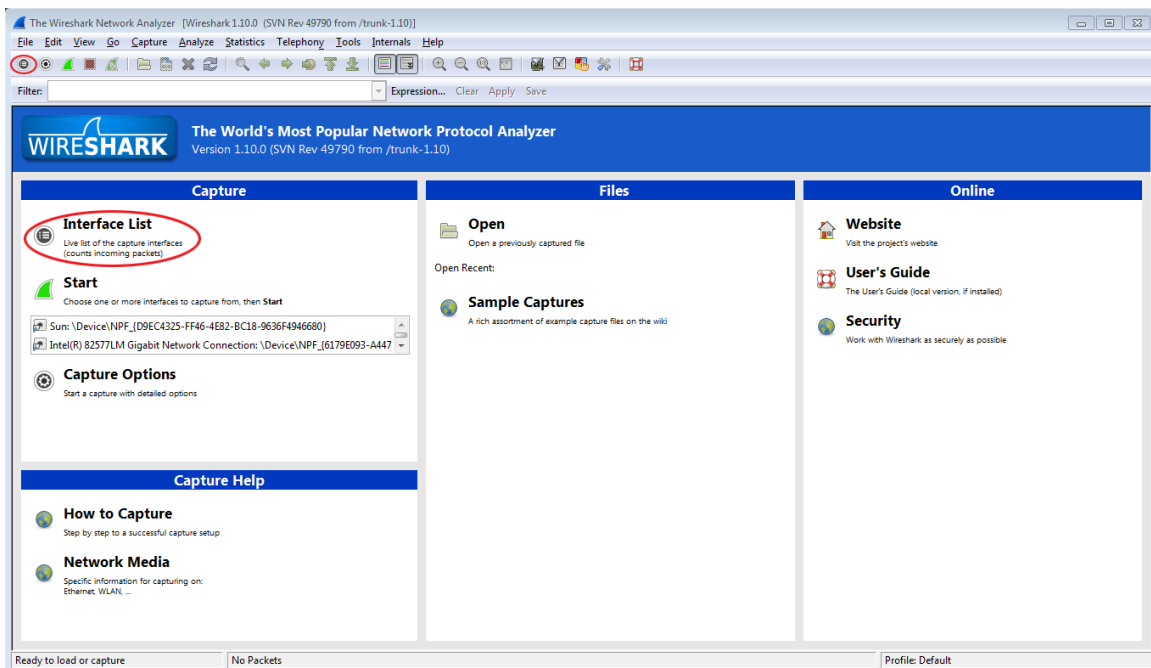
- b. Anote las direcciones IP y MAC asociadas al adaptador Ethernet seleccionado, ya que esa es la dirección de origen que debe buscar al examinar los paquetes capturados.

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

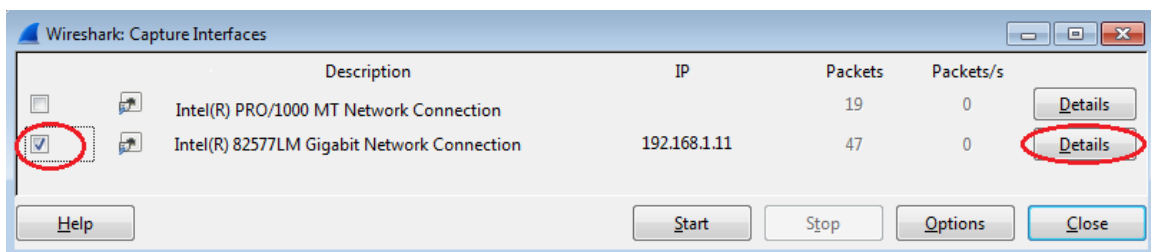
Dirección MAC del host de la PC: \_\_\_\_\_

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

- a. Haga clic en el botón **Inicio** de Windows 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).

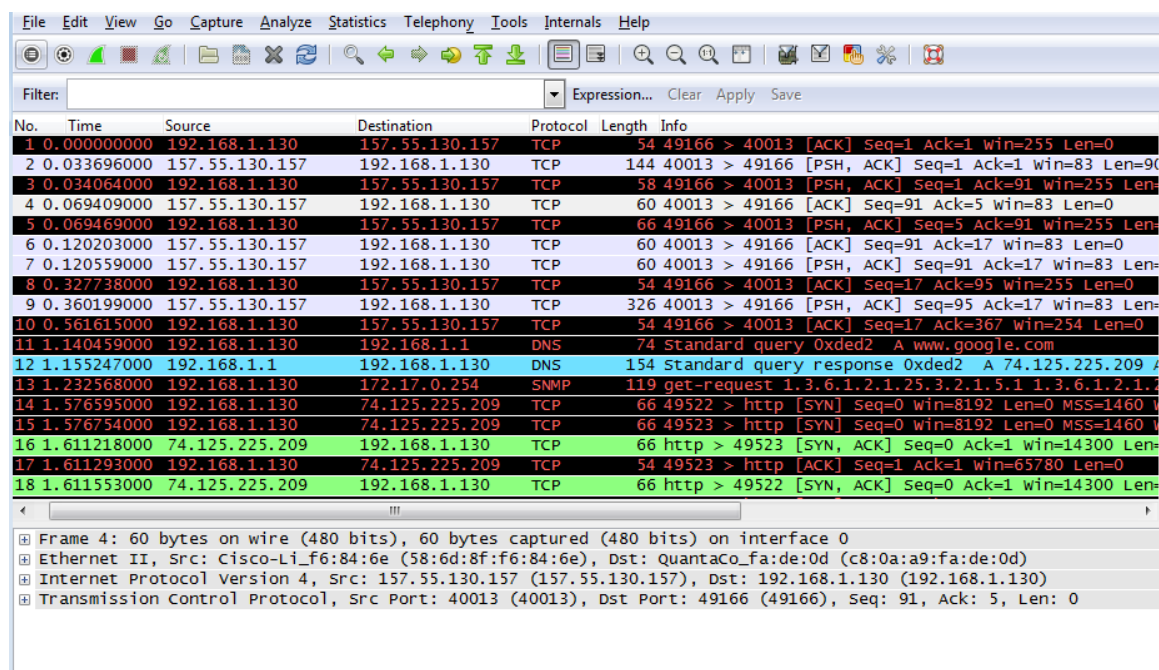
## Parte 2: Capturar, localizar y examinar paquetes

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

- 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:

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



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.130	157.55.130.157	TCP	54	49166 > 40013 [ACK] Seq=1 Ack=1 win=255 Len=0
2	0.033696000	157.55.130.157	192.168.1.130	TCP	144	40013 > 49166 [PSH, ACK] Seq=1 Ack=1 win=83 Len=90
3	0.034064000	192.168.1.130	157.55.130.157	TCP	58	49166 > 40013 [PSH, ACK] Seq=1 Ack=91 win=255 Len=0
4	0.069409000	157.55.130.157	192.168.1.130	TCP	60	40013 > 49166 [ACK] Seq=91 Ack=5 win=83 Len=0
5	0.069469000	192.168.1.130	157.55.130.157	TCP	66	49166 > 40013 [PSH, ACK] Seq=5 Ack=91 win=255 Len=0
6	0.120203000	157.55.130.157	192.168.1.130	TCP	60	40013 > 49166 [ACK] Seq=91 Ack=17 win=83 Len=0
7	0.120559000	157.55.130.157	192.168.1.130	TCP	60	40013 > 49166 [PSH, ACK] Seq=91 Ack=17 win=83 Len=0
8	0.327738000	192.168.1.130	157.55.130.157	TCP	54	49166 > 40013 [ACK] Seq=17 Ack=95 win=255 Len=0
9	0.360199000	157.55.130.157	192.168.1.130	TCP	326	40013 > 49166 [PSH, ACK] Seq=95 Ack=17 win=83 Len=0
10	0.561615000	192.168.1.130	157.55.130.157	TCP	54	49166 > 40013 [ACK] Seq=17 Ack=367 win=254 Len=0
11	1.140459000	192.168.1.130	192.168.1.1	DNS	74	Standard query 0xded2 A www.google.com
12	1.155247000	192.168.1.1	192.168.1.130	DNS	154	Standard query response 0xded2 A 74.125.225.209
13	1.232568000	192.168.1.130	172.17.0.254	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.4
14	1.576595000	192.168.1.130	74.125.225.209	TCP	66	49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460
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
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

Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: Cisco-Li\_f6:84:6e (58:6d:8f:f6:84:6e), Dst: Quantaco\_fa:de:0d (c8:0a:a9:fa:de:0d)  
 Internet Protocol Version 4, Src: 157.55.130.157 (157.55.130.157), Dst: 192.168.1.130 (192.168.1.130)  
 Transmission Control Protocol, Src Port: 40013 (40013), Dst Port: 49166 (49166), Seq: 91, Ack: 5, Len: 0

### 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.

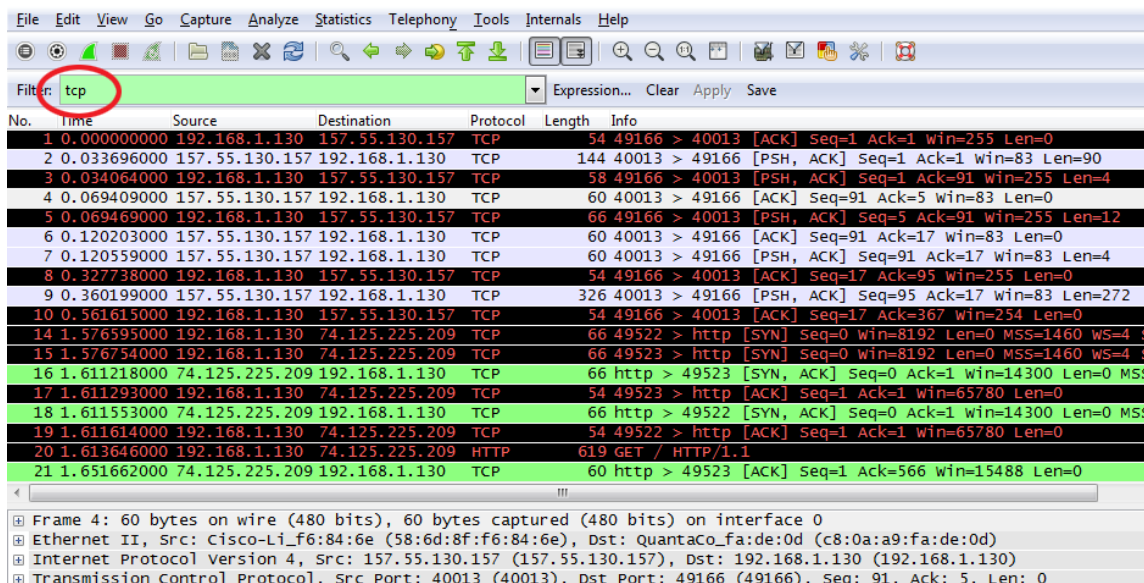
¿Cuál es la dirección IP del servidor DNS que consultó la PC? \_\_\_\_\_

- La trama 12 es la respuesta del servidor DNS con la dirección IP de [www.google.com](http://www.google.com).

- c. 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? \_\_\_\_\_

- d. 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.

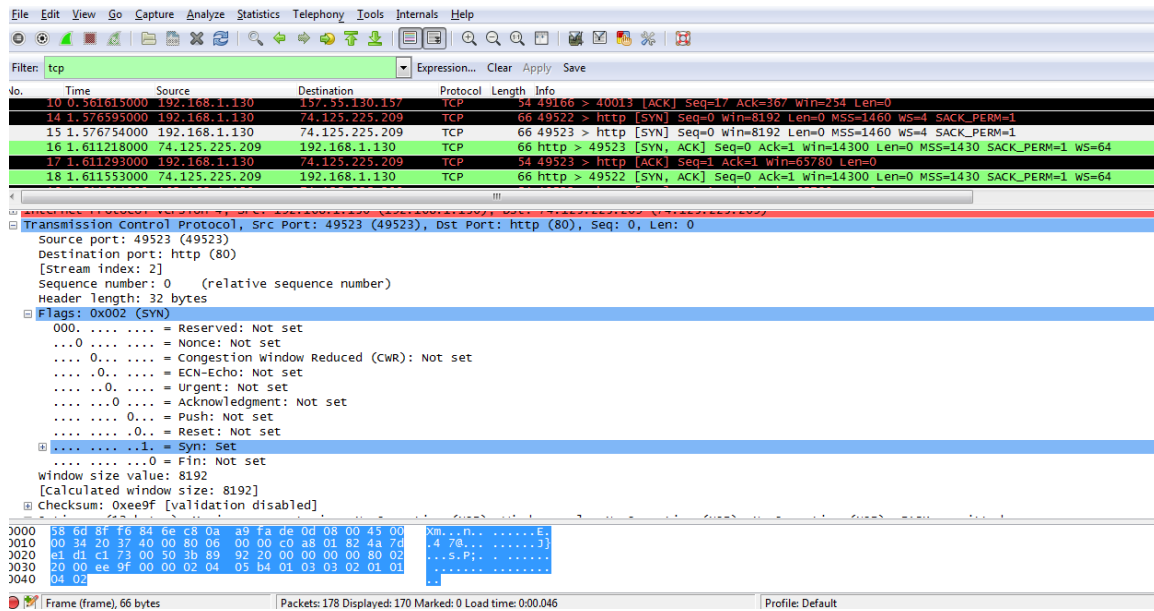


### Paso 3: Examinar la información de los paquetes, como direcciones IP, números de puerto TCP e indicadores de control TCP

- a. 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).
- b. 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.

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



¿Cuál es el número de puerto de origen TCP? \_\_\_\_\_

¿Cómo clasificaría el puerto de origen? \_\_\_\_\_

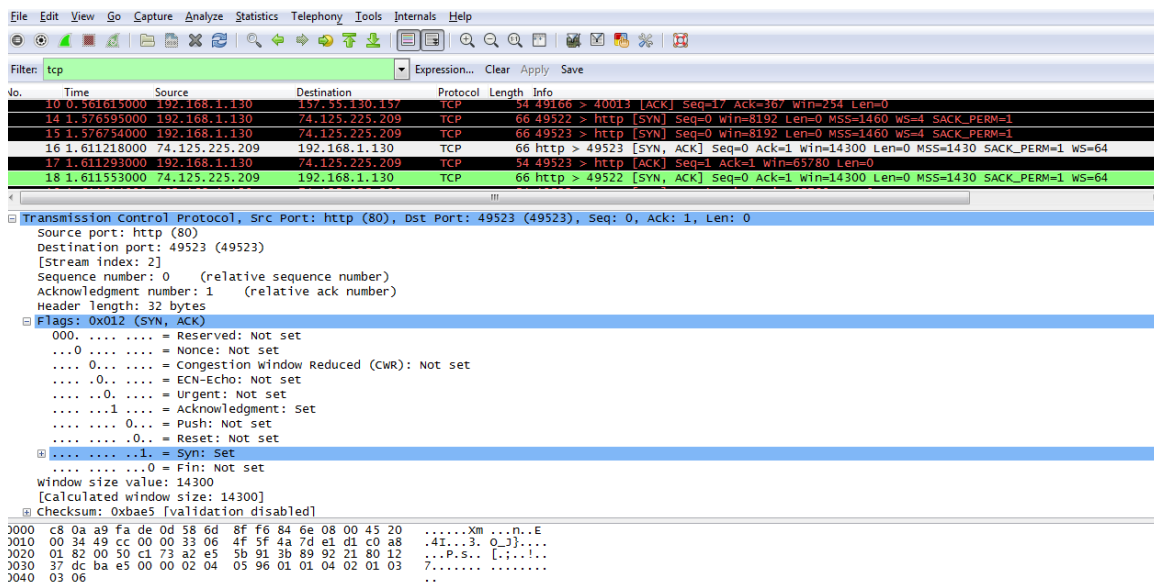
¿Cuál es el número de puerto de destino TCP? \_\_\_\_\_

¿Cómo clasificaría el puerto de destino? \_\_\_\_\_

¿Qué indicadores están establecidos? \_\_\_\_\_

¿Cuál es el número de secuencia relativa establecido? \_\_\_\_\_

- d. Para seleccionar la próxima trama en el 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.

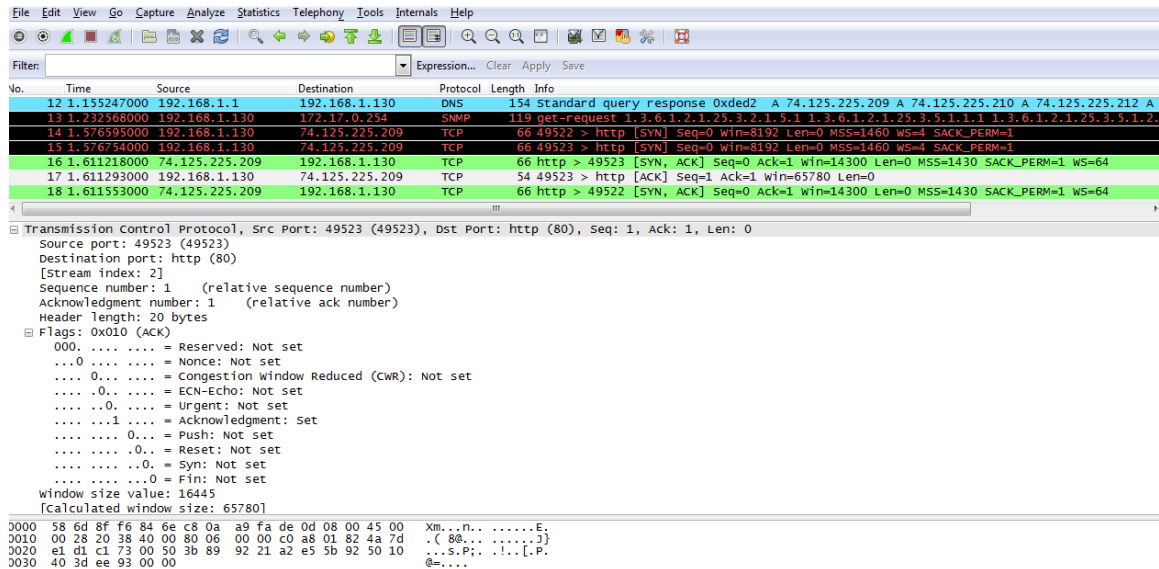


¿Cuáles son los valores de los puertos de origen y destino? \_\_\_\_\_

¿Qué indicadores están establecidos? \_\_\_\_\_

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

- 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:



Examine el tercer y último paquete del protocolo de enlace.

¿Qué indicadores están establecidos? \_\_\_\_\_

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

- 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?  
\_\_\_\_\_  
\_\_\_\_\_
- ¿De qué otras formas podría utilizarse Wireshark en una red de producción?  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_