

## Práctica de laboratorio 9.1.3 Uso de Wireshark para observar el protocolo de enlace de tres vías del TCP

### Objetivos

- Uso de Wireshark para monitorear una interfaz Ethernet para registrar los flujos de paquetes
- Generación de una conexión TCP utilizando un explorador Web
- Observación del protocolo de enlace de tres vías de TCP/IP

### Información básica / Preparación

En esta práctica de laboratorio, usted utilizará el analizador de paquetes de red Wireshark (también conocido como detector de paquetes) para visualizar los paquetes de TCP/IP generados por el protocolo de enlace de tres vías de TCP. Cuando una aplicación que usa el TCP inicia primero en un host, el protocolo utiliza el protocolo de enlace de tres vías para establecer una conexión TCP confiable entre dos hosts. El usuario podrá observar los paquetes iniciales del flujo de TCP: el paquete SYN, luego el paquete SYN ACK y finalmente el paquete ACK.

**Precaución:** La instalación o el uso de una aplicación para detectar paquetes se pueden considerar como violación a la política de seguridad de una organización, teniendo así serias consecuencias legales y financieras. Se recomienda obtener permiso antes de descargar, instalar o ejecutar una aplicación para detectar paquetes.

**Nota:** El término “paquete” se utiliza en este laboratorio. En realidad, Wireshark captura las tramas de Ethernet que contienen paquetes IP. La aplicación Wireshark utiliza el término “trama” cuando analiza capturas. Por lo general, los dos términos se utilizan de forma indistinta, pero recuerde que una trama es un paquete de encapsulación de la Capa 2 de enlace de datos y un paquete es una encapsulación de la Capa 3 de red.

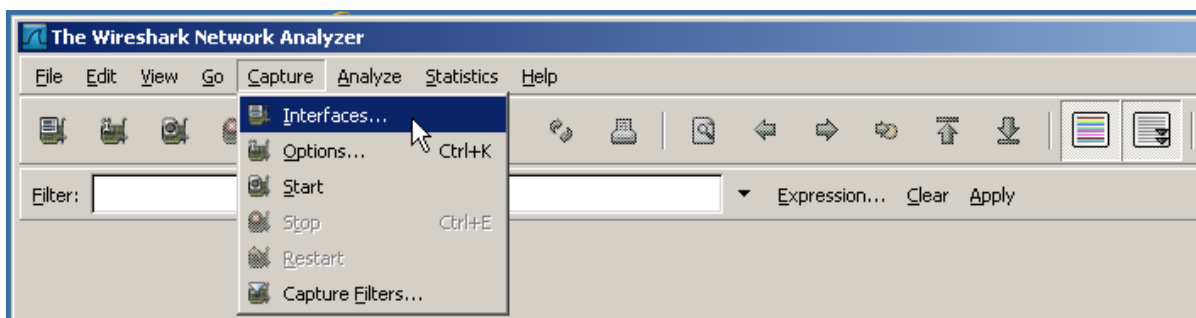
### Tarea 1: Preparación de Wireshark para capturar paquetes

#### Paso 1: Inicie Wireshark.

Haga doble clic en el icono de Wireshark que se encuentra en el escritorio.

#### Paso 2: Seleccione una interfaz para usar para la captura de paquetes.

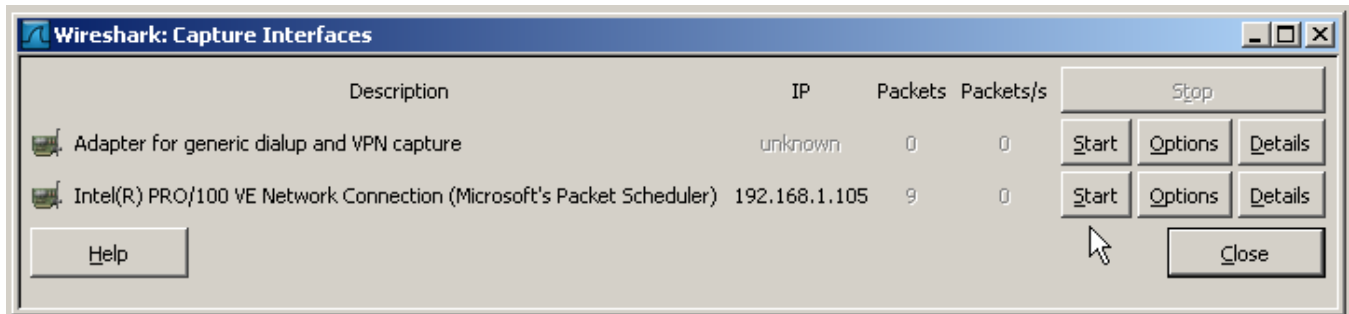
- En el menú Capture (Capturar), haga clic en **Interfaces**.



### Paso 3: Inicie una captura de red.

- Elija el adaptador de la interfaz Ethernet de la red local para capturar tráfico de la red. Haga clic en el botón **Start (Iniciar)** de la interfaz elegida.
- Anote la dirección IP relacionada con el adaptador de Ethernet seleccionado, dado que esa es la única dirección IP de origen que va a buscar al examinar los paquetes capturados.

Dirección IP del host: \_\_\_\_\_



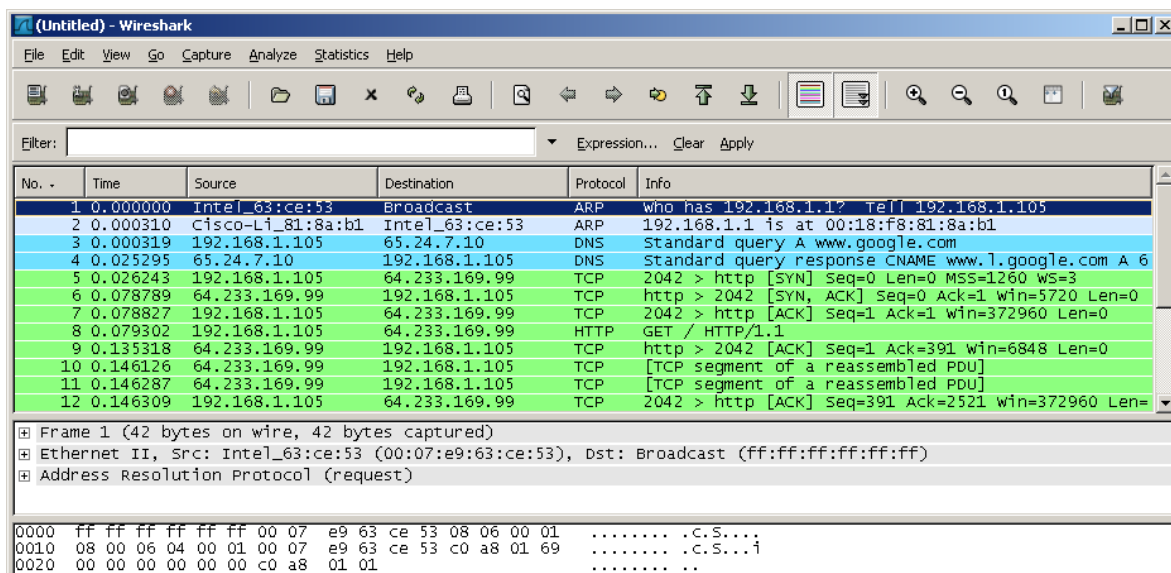
## Tarea 2: Generación y análisis de los paquetes capturados

### Paso 1: Abra un explorador y acceda a un sitio Web.

- Vaya a [www.google.com](http://www.google.com). Minimice la ventana de Google y vuelva a Wireshark. Debería ver el tráfico capturado de manera similar a la que se muestra a continuación.

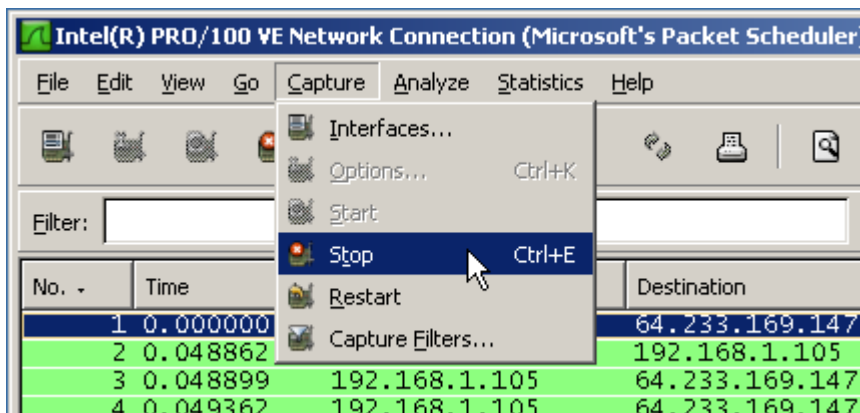
**Nota:** Es posible que su instructor le proporcione un sitio Web diferente. En ese caso, ingrese aquí el nombre o la dirección del sitio Web:

- Las ventanas de captura ahora están activas. Localice las columnas Source (Origen), Destination (Destino) y Protocol (Protocolo) en la pantalla de Wireshark. Los datos de HTTP que portan texto y gráficos de la página Web utilizan el TCP en cuanto a fiabilidad.



## Paso 2: Detenga la captura.

En el menú Capture de Wireshark, haga clic en **Stop (Detener)**.



## Paso 3: Analice el resultado capturado.

Si la computadora se inició recientemente y no ha habido actividad para acceder a Internet, podrá ver todo el proceso en los resultados capturados, incluidos ARP, DNS y el protocolo de enlace de tres vías.

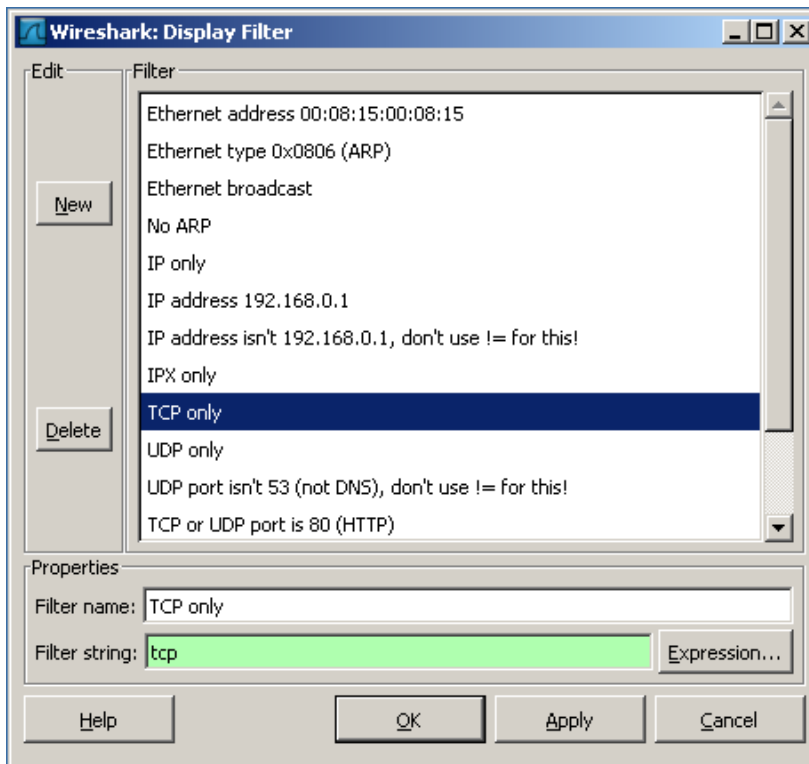
La pantalla de captura en la Tarea 2, Paso 1 muestra todos los paquetes que necesita la computadora para llegar a un sitio Web, comenzando con el ARP inicial para la dirección MAC de la interfaz del router predeterminado. (Su captura de pantalla puede variar.)

- En la captura de pantalla, el proceso inicia con la trama 1, que es un broadcast de ARP desde la computadora de origen para determinar la dirección MAC del gateway predeterminado del router. El gateway es la interfaz Fast Ethernet de la LAN local en el router. La computadora necesita resolver la dirección IP del gateway predeterminado a la dirección MAC de la interfaz antes de que pueda enviar la primera trama o paquete al router.  
¿Cuál es la dirección IP del gateway predeterminado del router? \_\_\_\_\_
- La segunda trama es la respuesta del router informándole a la computadora la dirección MAC de su interfaz Fast Ethernet.  
¿Cuál es la dirección MAC? \_\_\_\_\_
- La tercera trama es una consulta de DNS desde la computadora al servidor DNS configurado, intentando resolver el nombre de dominio [www.google.com](http://www.google.com) a la dirección IP del servidor Web. La computadora debe tener la dirección IP antes de que pueda enviar la primera trama al servidor Web.  
¿Cuál es la dirección IP del servidor DNS que consultó la computadora? \_\_\_\_\_
- La cuarta trama es la respuesta del servidor DNS con la dirección IP de [www.google.com](http://www.google.com). Es necesario que se desplace hacia la derecha para ver la dirección IP del servidor de Google en la respuesta de DNS, pero puede verla en la siguiente trama.
- La quinta trama es el inicio del protocolo de enlace de tres vías de TCP [SYN].  
¿Cuál es la dirección IP del servidor Web de Google? \_\_\_\_\_

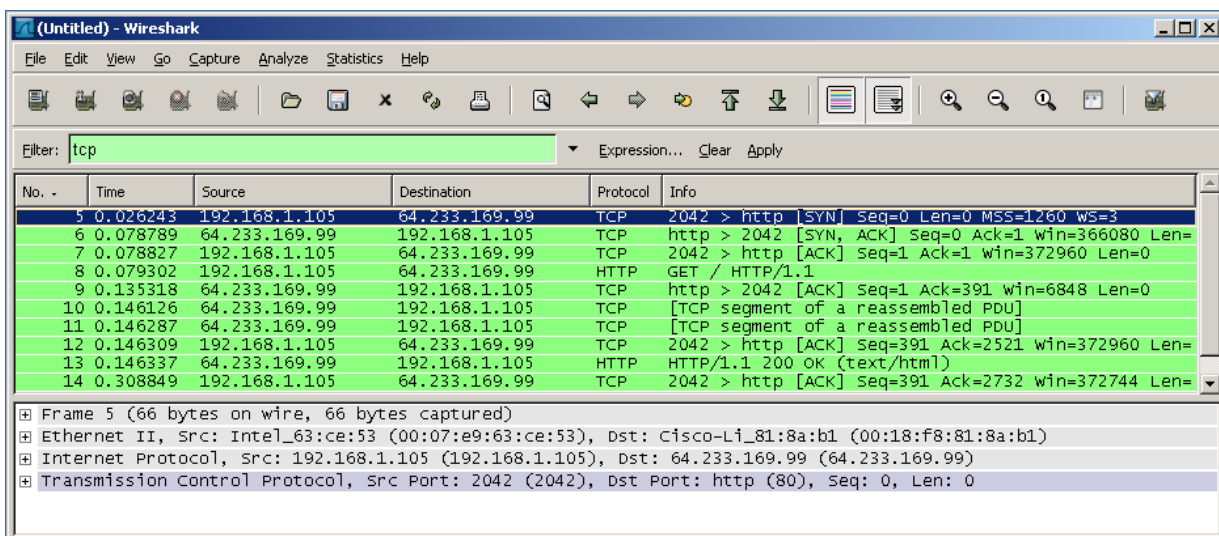
#### Paso 4: Filtre la captura para visualizar solamente los paquetes de TCP.

Si tiene muchos paquetes no relacionados con la conexión TCP, quizá sea necesario utilizar la capacidad de filtrado de Wireshark.

- Para usar un filtro previamente configurado, haga clic en la opción del menú **Analyze (Analizar)** y luego haga clic en **Display Filters (Mostrar Filtros)**.
- En la ventana **Display Filter (Mostrar filtro)**, haga clic en **TCP only (Sólo TCP)** y luego haga clic en **OK (Aceptar)**.



- En la ventana de Wireshark, desplácese al primer paquete de TCP capturado. Éste debe ser el primer paquete en el flujo.



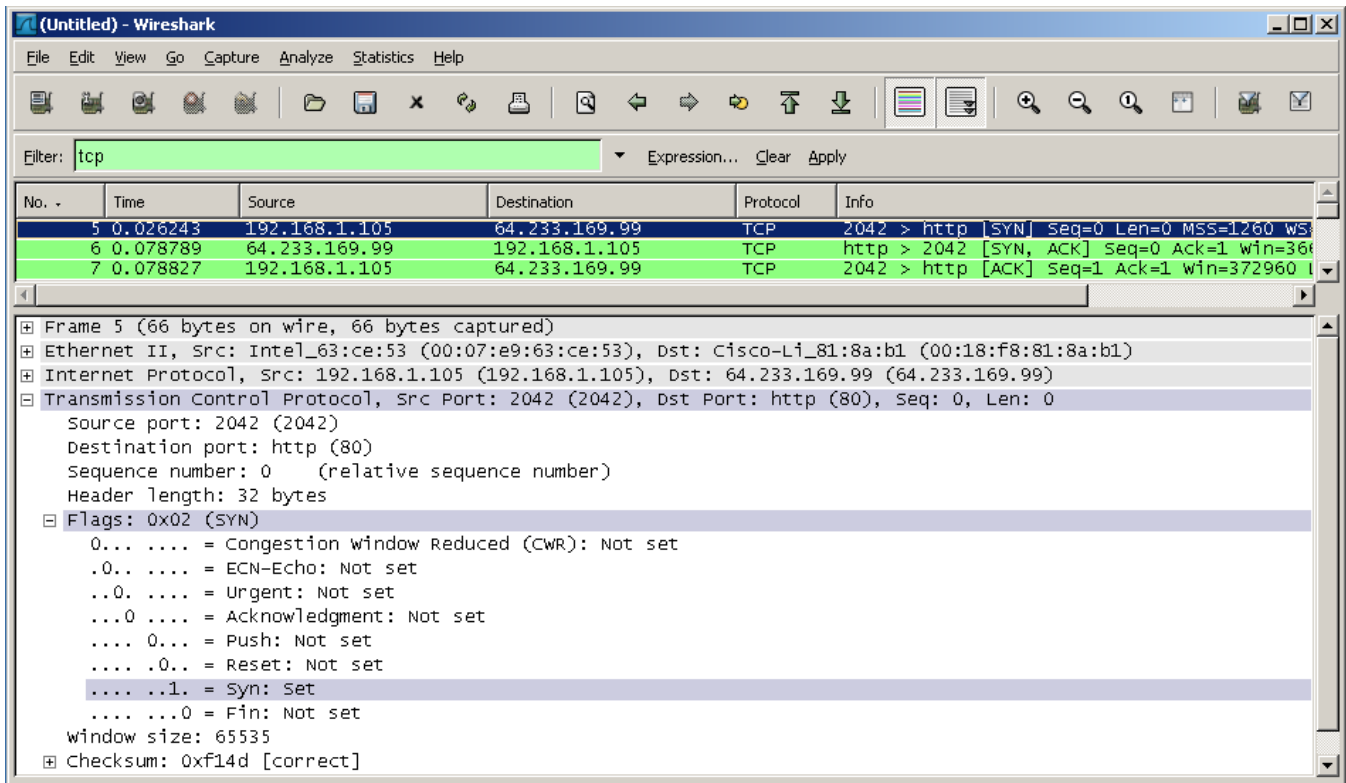
- d. En la columna **Info**, busque tres paquetes similares a los tres primeros que se muestran en la ventana de arriba. El primer paquete de TCP es el paquete [SYN] de la computadora de inicio. El segundo es la respuesta [SYN, ACK] del servidor Web. El tercer paquete es el [ACK] de la computadora de origen, que completa el enlace de tres vías.

### Paso 5: Inspeccione la secuencia de inicialización de TCP

- a. En la ventana superior de Wireshark, haga clic en la línea que contiene el primer paquete identificado en el Paso 4. Esto resalta la línea y muestra la información decodificada de ese paquete en el relleno de las dos ventanas inferiores.

**Nota:** Las ventanas de Wireshark que se encuentran a continuación fueron ajustadas para visualizar la información de forma compacta. La ventana intermedia contiene la decodificación detallada del paquete.

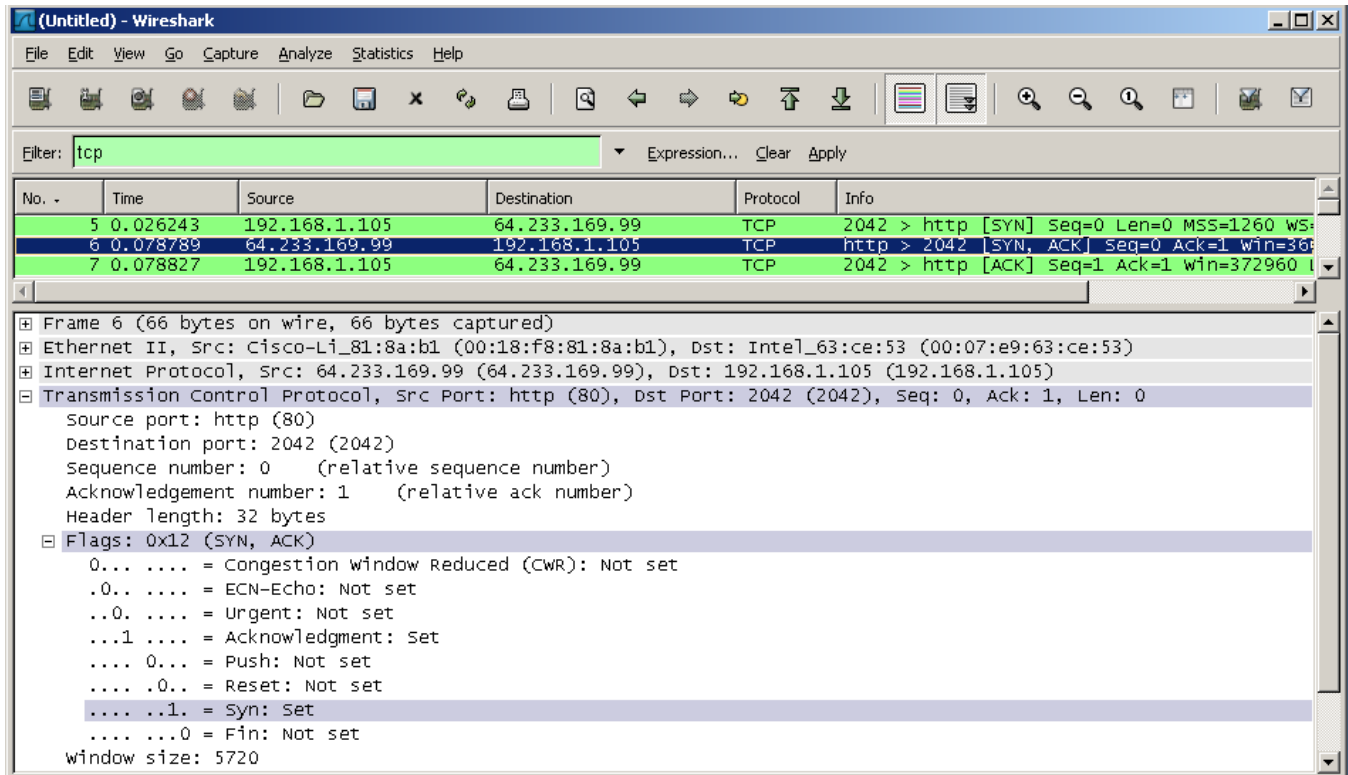
- b. Haga clic en el icono + para ampliar la vista de la información de TCP. Para contraer la vista, haga clic en el icono –.
- c. Observe que en el primer paquete TCP el número de secuencia relativa se estableció en 0 y el bit SYN se estableció en 1 en el campo Flags (Señaladores).



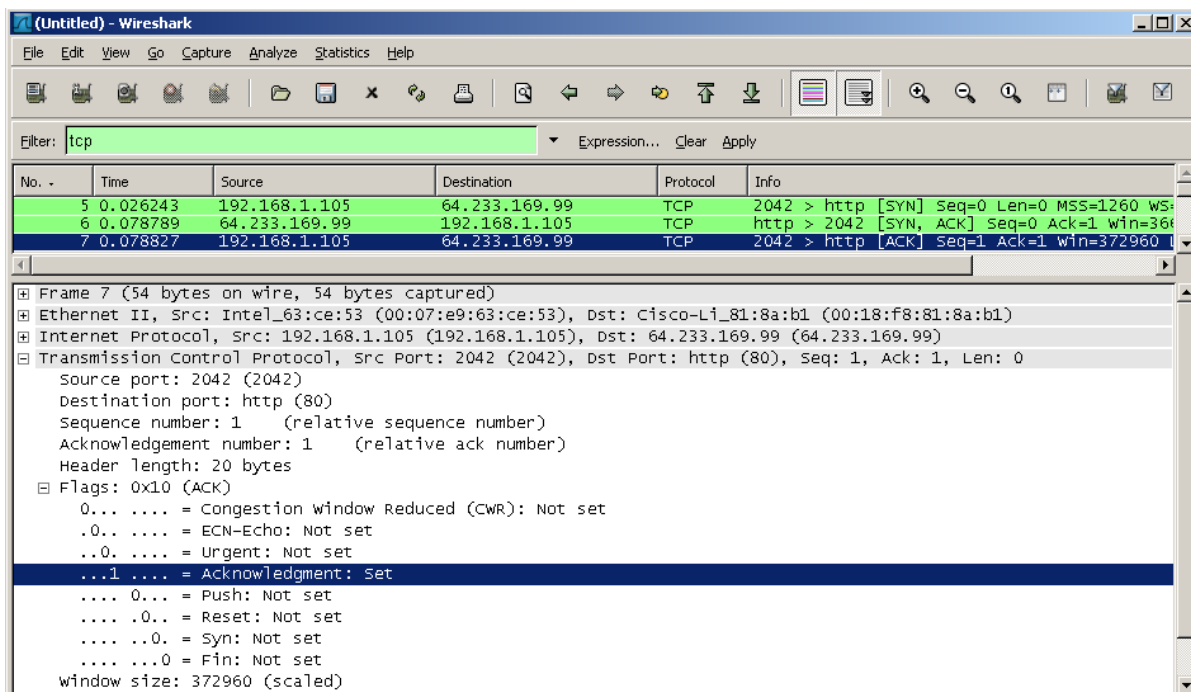
- d. Observe que en el segundo paquete TCP del enlace de tres vías, el número de secuencia relativa se estableció en 0 y el bit SYN y el bit ACK se establecieron en 1 en el campo Flags (Señaladores).

## CCNA Discovery

### Trabajar en una pequeña o mediana empresa o ISP



- e. En la tercera y última trama del enlace de tres vías, sólo se estableció el bit ACK y el número de secuencia se estableció en el punto de partida de 1. El número de acuse de recibo también se estableció en 1 como punto de partida. La conexión TCP se está estableciendo y la comunicación entre la computadora de origen y el servidor Web puede comenzar.



- f. Cierre Wireshark.

### Tarea 3: Reflexión

- a. Existen cientos de filtros disponibles en Wireshark. Una red grande podría tener varios filtros y muchos tipos de tráfico diferentes. ¿Qué tres filtros en la lista podrían serle de mayor utilidad a un administrador de red?

---

- b. ¿Es Wireshark una herramienta para el monitoreo de red fuera de banda o dentro de banda?

---

Justifique su respuesta.

---

---