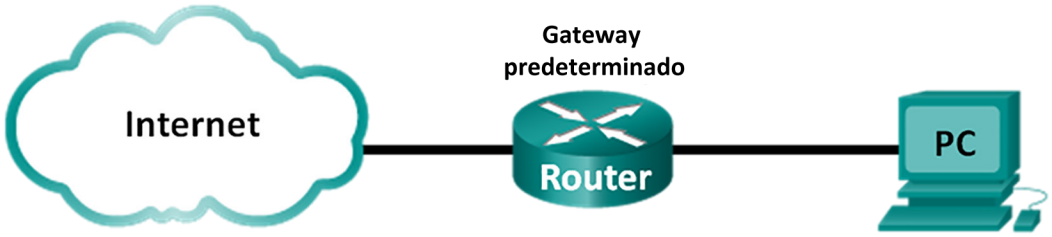
Práctica de laboratorio: Uso de Wireshark para observar la negociación en tres pasos de TCP

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.

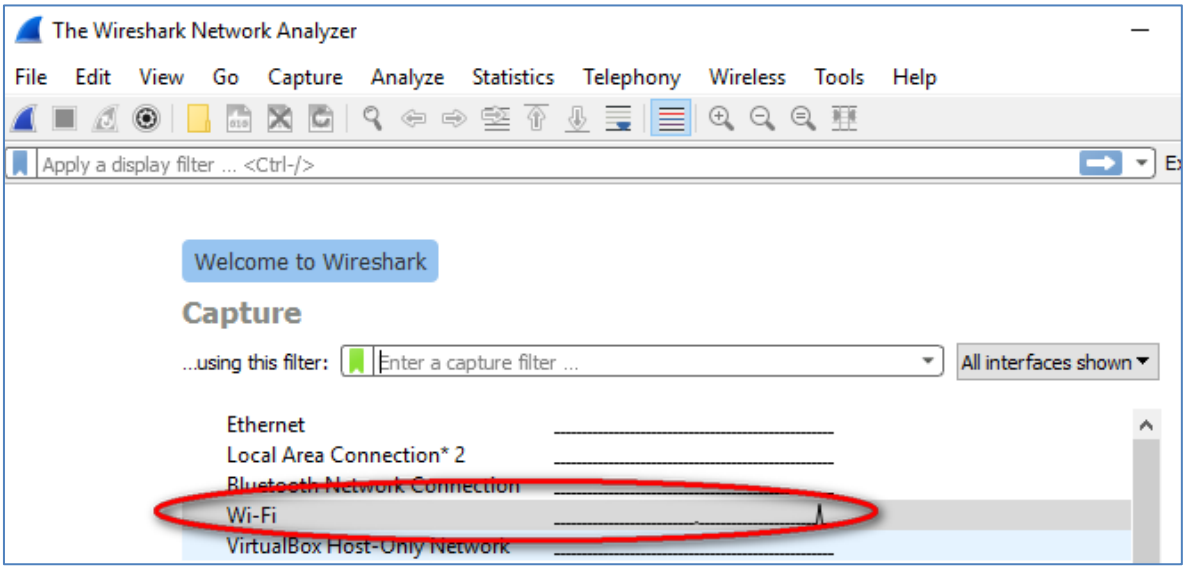
La dirección IP del host de la PC: 192.168.1.4

La dirección MAC del host de la PC: D4-6D-6D-25-E1-85

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**.

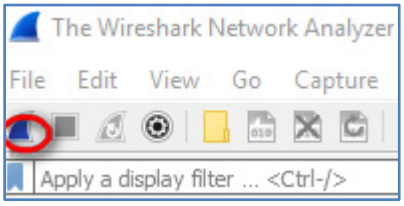
b. Después de que se inicie Wireshark, seleccione la interfaz activa para captura de datos. La interfaz activa muestra las actividades de tráfico.



Parte 2: Capturar, localizar y examinar paquetes

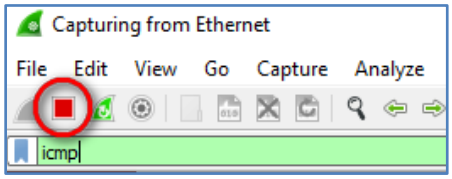
Paso 1: Capturar los datos

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



b. Abra un navegador web y escriba www.google.com.

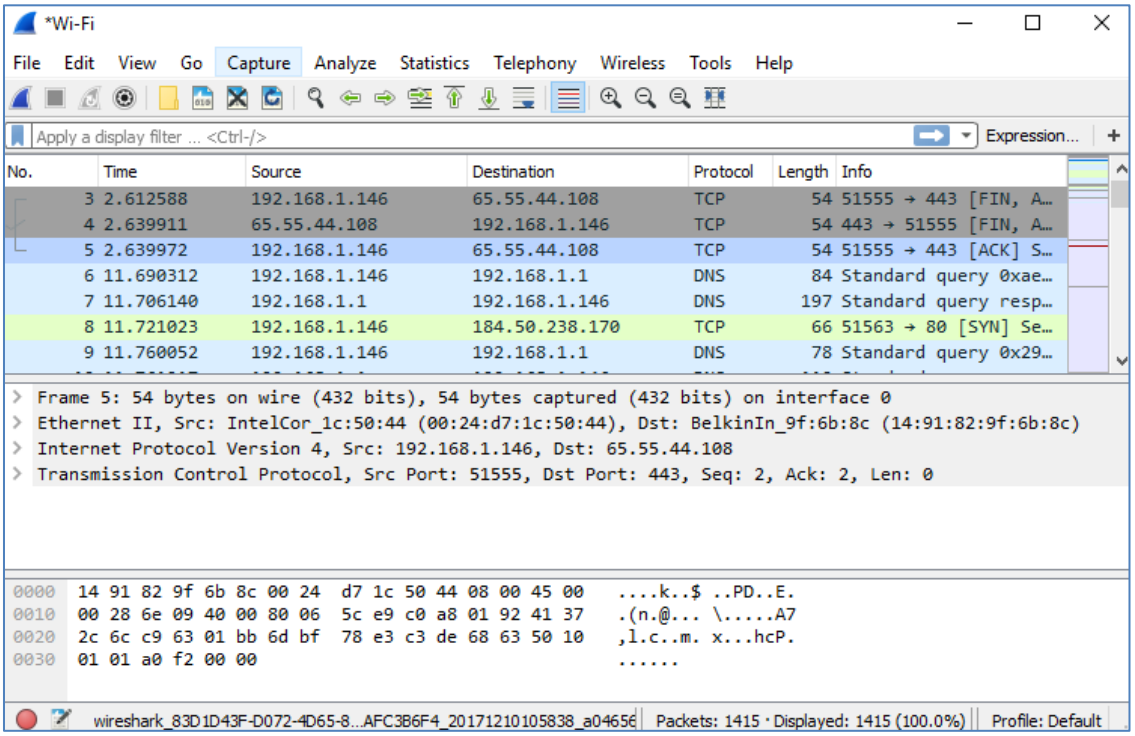
c. Minimice el navegador y regrese a Wireshark. Detenga la captura de datos.



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:

https://www.google.com/

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.

a. 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.

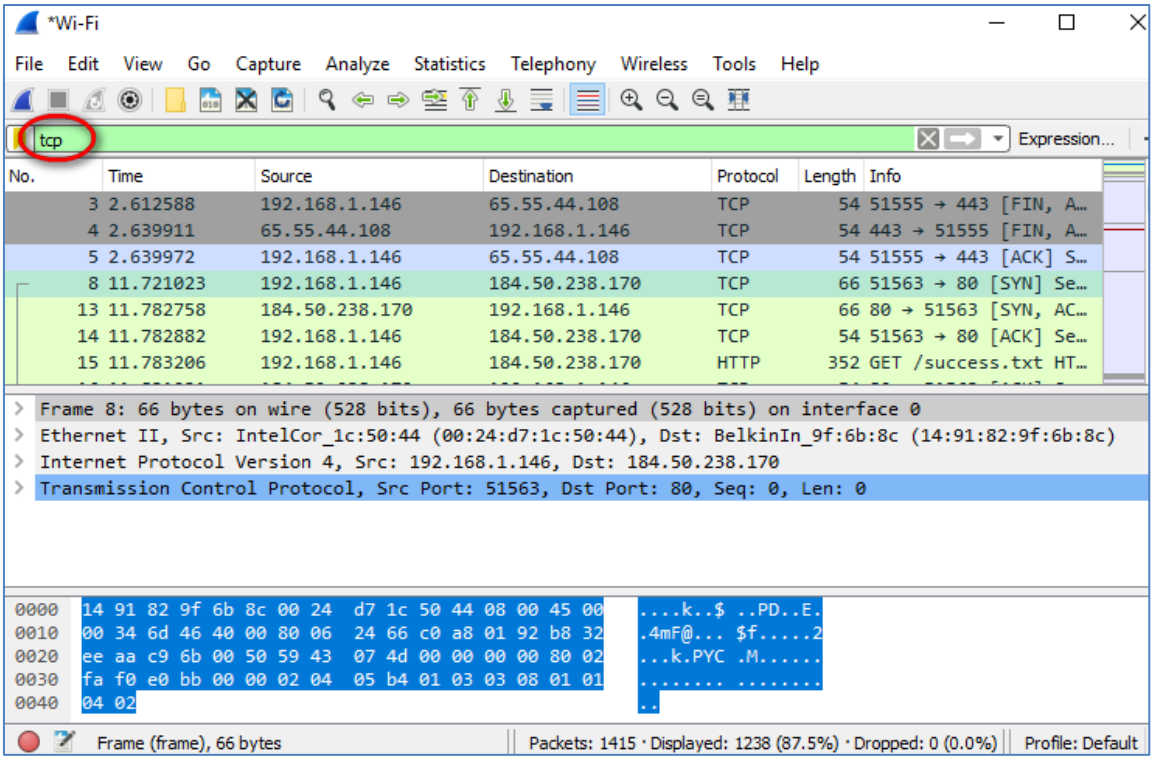
¿Cuál es la dirección IP del servidor DNS que consultó el equipo? 192.168.1.4

b. La trama 7 es la respuesta del servidor DNS. Contiene la dirección IP de www.google.com.

c. 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? 172.217.16.228

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).



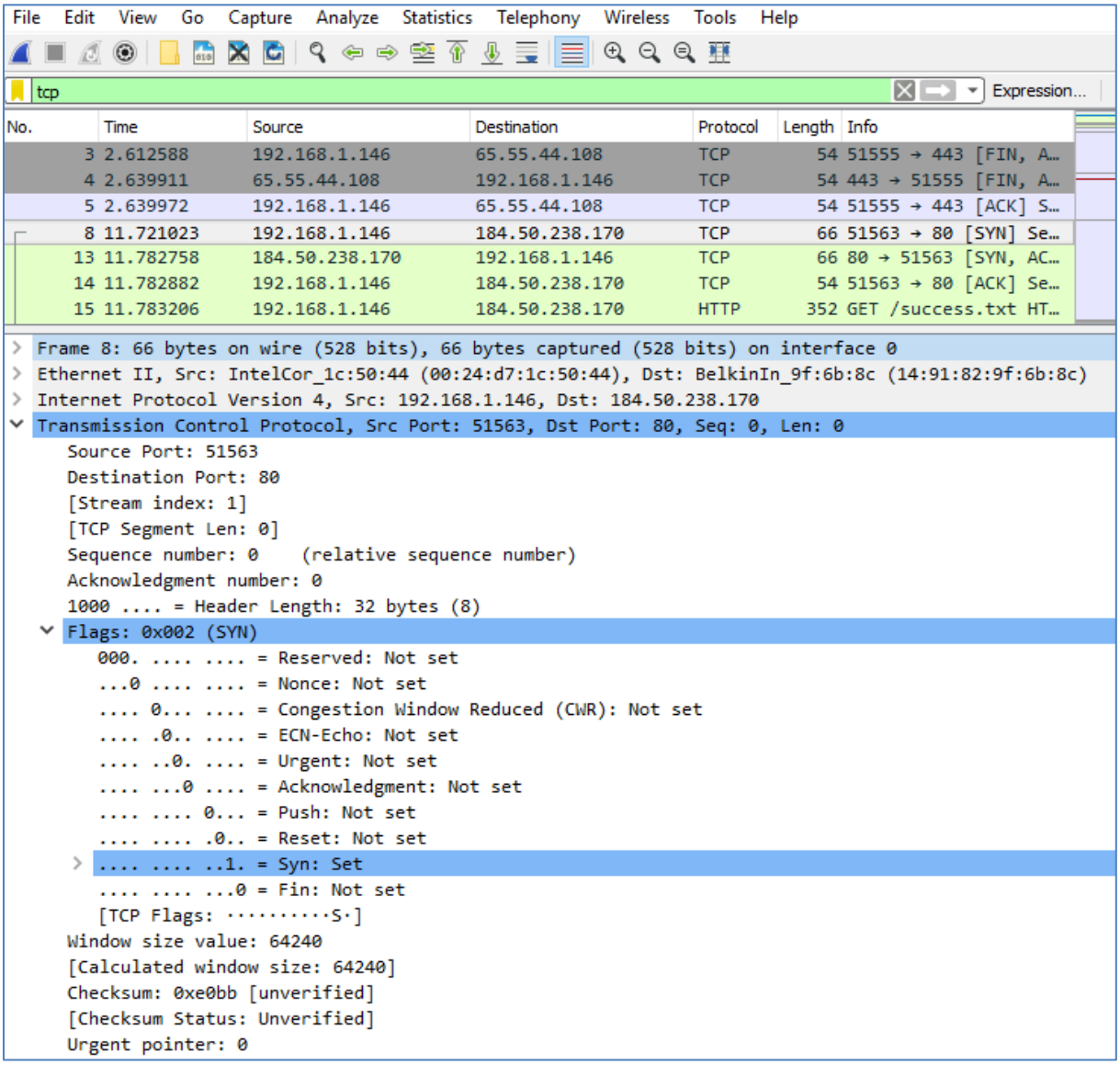
Paso 3: Examinar la información dentro de los paquetes, como las direcciones IP, los números de puerto TCP y los marcadores de control de TCP

a. 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).

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.

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.



¿Cuál es el número de puerto de origen de TCP? 443

¿Cómo clasificaría el puerto de origen? privado

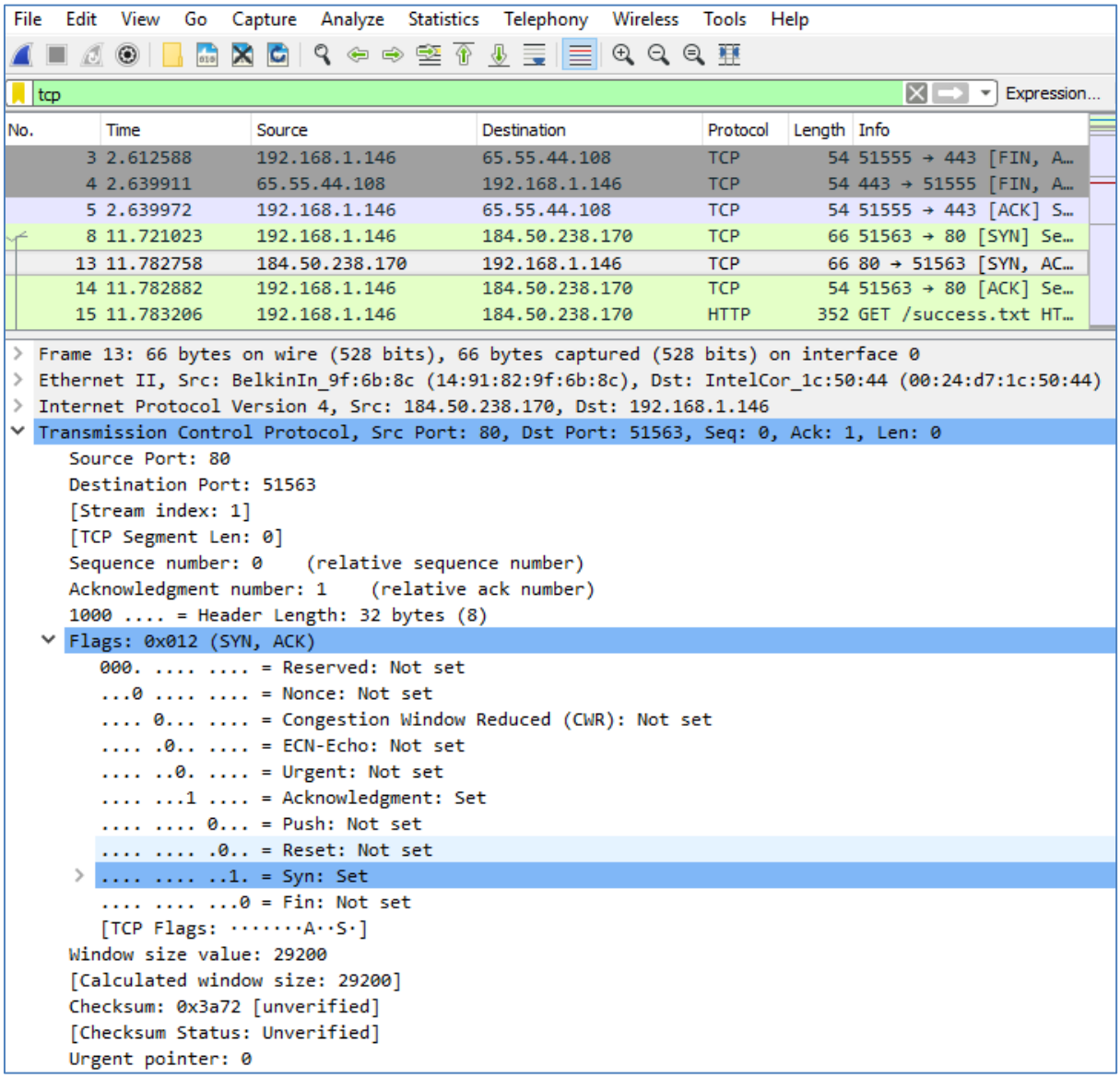
¿Cuál es el número de puerto de destino de TCP? 51867

¿Cómo clasificaría el puerto de destino? HTTP

¿Qué marcadores están establecidos? SYN

¿Qué número de secuencia relativo está establecido? 0

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.



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

origen de 443 y destino 51867

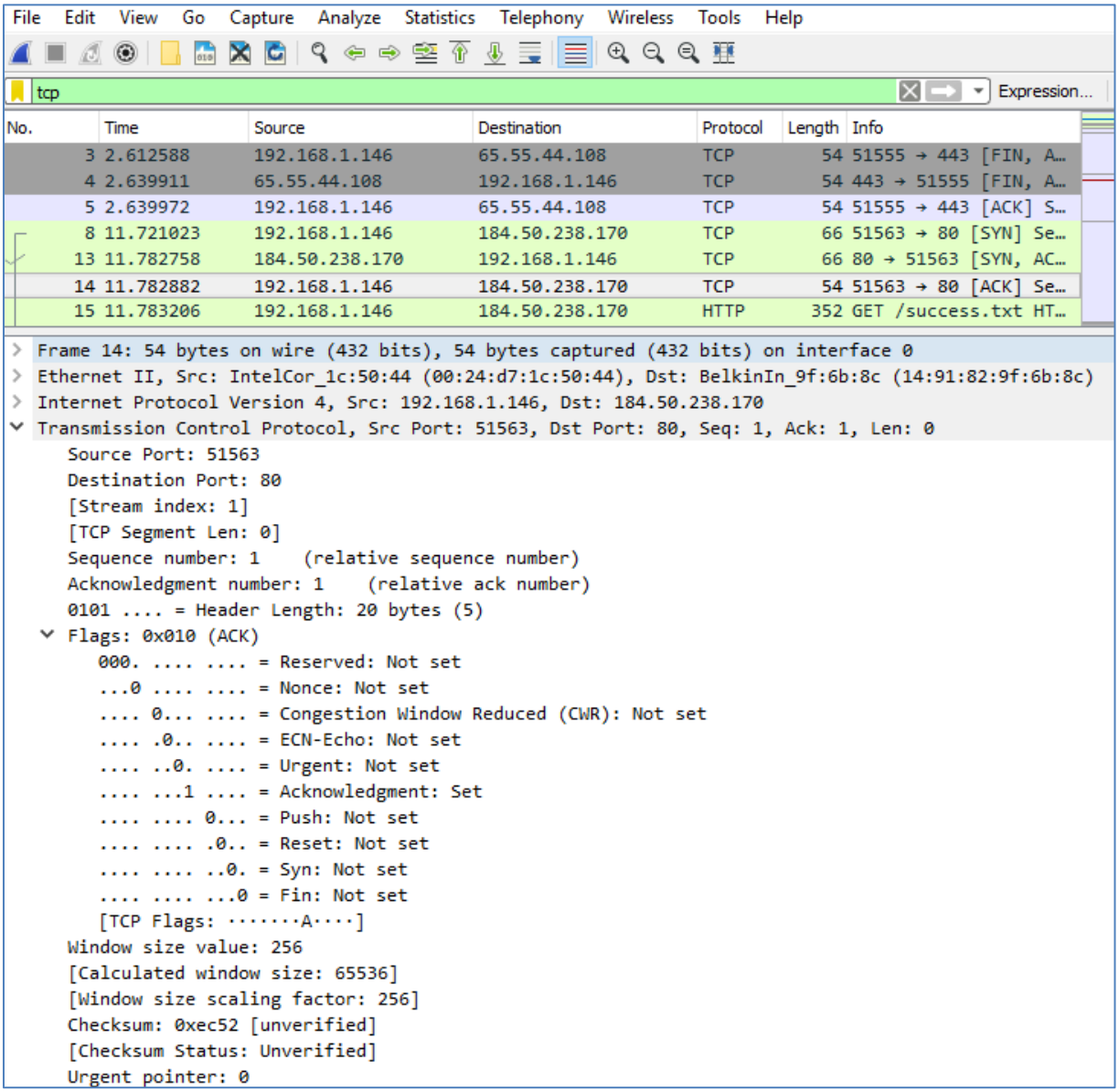
¿Qué marcadores están establecidos?

SYN

¿Qué números relativos de secuencia y reconocimiento están establecidos?

numero secuencia 0 y reconocimento 0

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:



Examine el tercer y último paquete de la negociación.

¿Qué marcadores están establecidos?

SYNC y ACK

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.

   TCP, DNS, IP

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

   Para la seguridad en redes.