Práctica de laboratorio 11.5.6: Estudio de caso final: Análisis de datagrama con Wireshark

Objetivos de aprendizaje

Al completar este ejercicio, los estudiantes podrán demostrar lo siguiente:

- cómo se construye un segmento TCP y explicar los campos del segmento;
- cómo se construye un paquete IP y explicar los campos del paquete;
- cómo se construye una trama de Ethernet II y explicar los campos de la trama;
- los contenidos de una SOLICITUD DE ARP y de una RESPUESTA DE ARP.

Información básica

Esta práctica de laboratorio requiere dos archivos de paquetes capturados y Wireshark, un analizador de protocolos de red. Descargar los siguientes archivos de Eagle server e instalar Wireshark en su computadora si es que aún no se ha instalado:

- eagle1_web_client.pcap (ya mencionado)
- eagle1_web_server.pcap (sólo referencia)
- wireshark.exe

Escenario

Este ejercicio detalla la secuencia de datagramas que se crean y envían a través de una red entre un cliente Web, PC_Client, y un servidor Web, eagle1.example.com. Comprender el proceso que se utiliza para ubicar los paquetes en secuencia en la red permitirá al estudiante diagnosticar las fallas de red de manera lógica cuando se interrumpe la conectividad. Para una mayor rapidez y claridad, se ha omitido de las capturas el sonido de los paquetes de la red. Antes de ejecutar un analizador de protocolos de red en una red que no le pertenece, debe asegurarse de obtener el permiso (por escrito).

La Figura 1 muestra la topología de esta práctica de laboratorio.

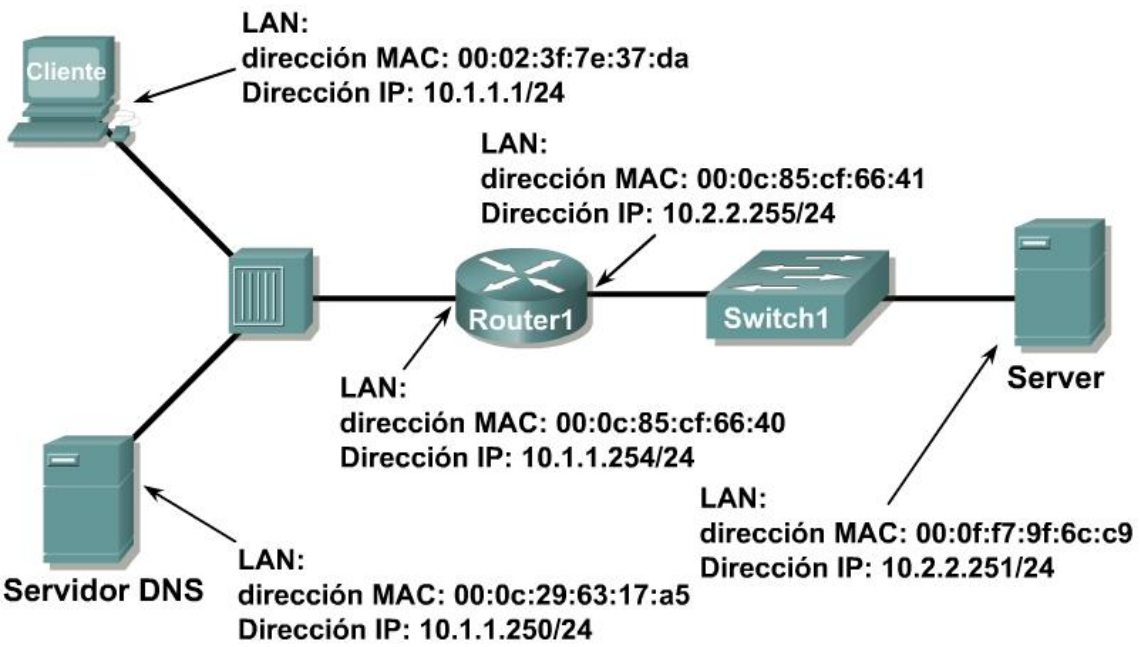

Figura 1. Topología de la red.

A través de las herramientas de la línea de comandos de Microsoft ®, se muestra la información de configuración IP y el contenido de la caché ARP. Consulte la Figura 2.

```
C: > ipconfig / all
Configuración IP de Windows
Conexión de área local del adaptador Ethernet:
     Sufijo de conexión específica DNS. :
     Descripción. . . . . . . . . . . . : Intel(R) PRO/1000 MT
                                          Conexión de red
     Dirección física . . . . . . . . . : 00:02:3f:7e:37:da
     Dhcp habilitado. . . . . . . . . . : No
     Dirección IP . . . . . . . . . . . : 10.1.1.1
     Máscara de subred. . . . . . . . . : 255.255.255.0
     Gateway por defecto. . . . . . . . : 10.1.1.254
     Servidores DNS . . . . . . . . . . : 10.1.1.250
C: > arp –a
No se encontraron entradas de ARP
C: >
```

Figura 2. Estado de red inicial de PC Client.

Se inicia un cliente Web y se ingresa el URL eagle1.example.com, como se observa en la Figura 3. Aquí comienza el proceso de comunicación con el servidor Web, que es donde comienzan los paquetes capturados.

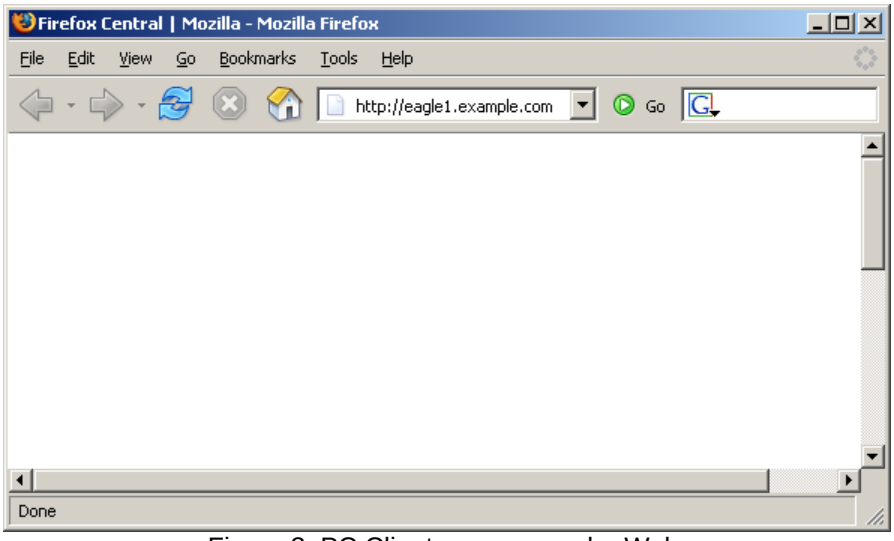

Figura 3. PC Client con navegador Web.

Tarea 1: Preparar el laboratorio.

Paso 1: Inicie Wireshark en el equipo.

Consulte la Figura 4 para realizar cambios en los resultados predeterminados. Desmarque `Barra de herramientas principal`, `Barra de herramientas de filtro` y ~~`Bytes del paquete`~~. Verifique que `Lista de paquetes` y `Detalles del paquete` estén marcados. Para asegurarse de que no haya traducción automática de las direcciones MAC, desmarque `Resolución de nombres` para `Capa de MAC` y `Capa de Transporte`.

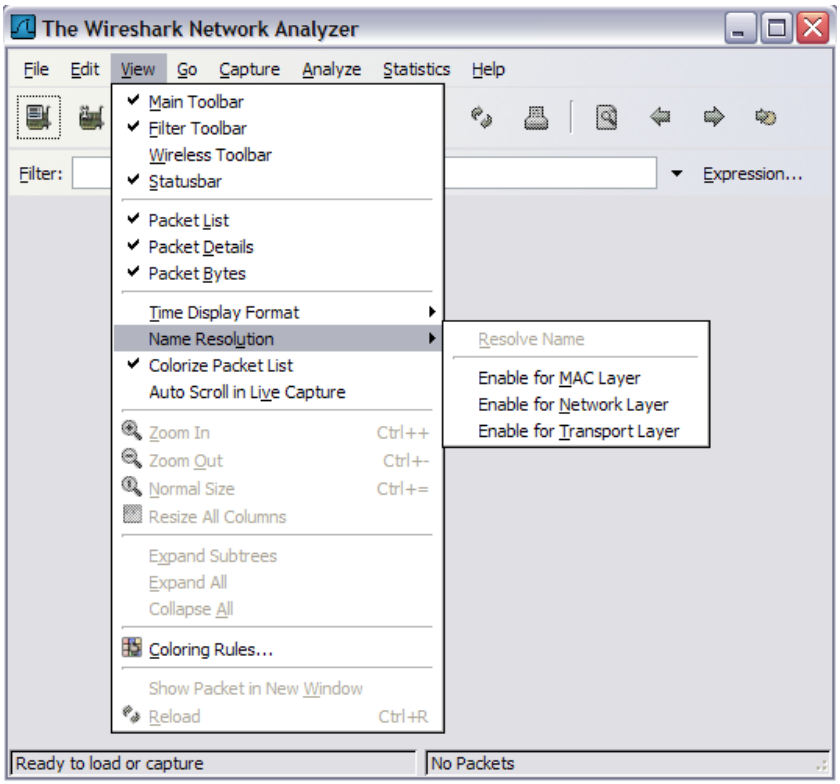

Figura 4. Cambios a la vista predeterminada de Wireshark.

Paso 2: Cargue la captura del cliente Web, `eagle1_web_client.pcap`.

Se muestra una pantalla similar a la de la Figura 5. Hay varios menús y submenús desplegables disponibles. También hay dos ventanas de datos separadas. La ventana Wireshark de arriba muestra todos los paquetes capturados. La ventana inferior contiene los detalles de los paquetes. En la ventana inferior, cada línea que contiene una casilla de verificación ☒ indica que hay información adicional disponible.

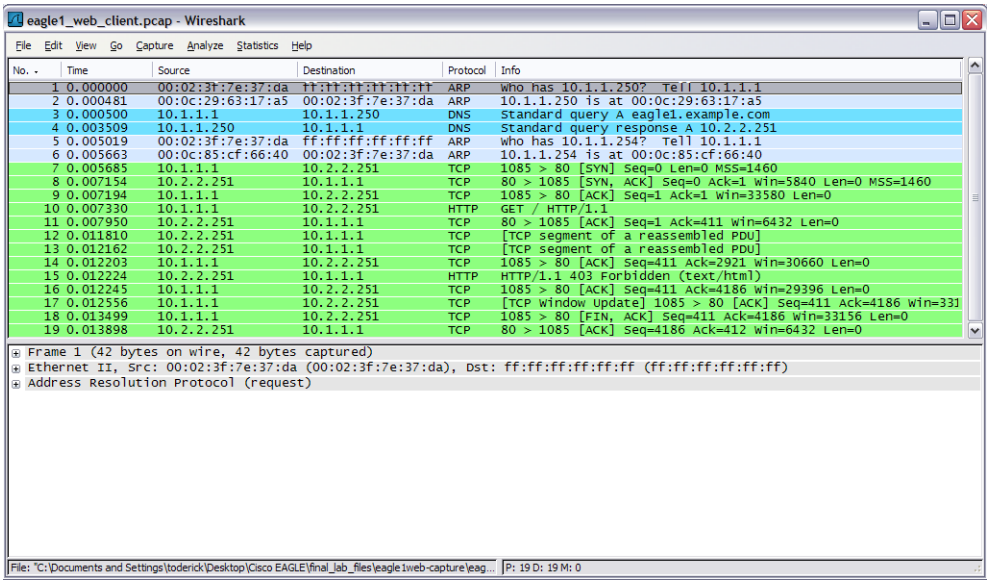

Figura 5. Wireshark con el archivo eagle1_web_client.pcap cargado.

Tarea 2: Revisar el proceso de flujo de datos a través de la red.

Paso 1: Revise el funcionamiento de la capa de Transporte.

Cuando PC_Client crea el datagrama para una conexión con eagle1.example.com, el datagrama viaja a través de las distintas capas de red. En cada capa se agrega la información de encabezado importante. Dado que esta comunicación es desde un cliente Web, el protocolo de la capa de Transporte será TCP. Vea el segmento TCP que se muestra en la Figura 6. PC_Client genera una dirección de puerto TCP interna, en esta conversación 1085, y reconoce la dirección de puerto del servidor Web conocida, 80. De la misma forma, se ha generado internamente un número de secuencia. Se incluye información suministrada por la capa de Aplicación. Habrá ciertos tipos de información que PC_Client no conocerá, y que por lo tanto deberán averiguarse utilizando otros protocolos red.

No hay número de acuse de recibo. Antes de que este segmento pueda pasar a la capa de Red, debe realizarse el protocolo de enlace de tres vías de TCP.

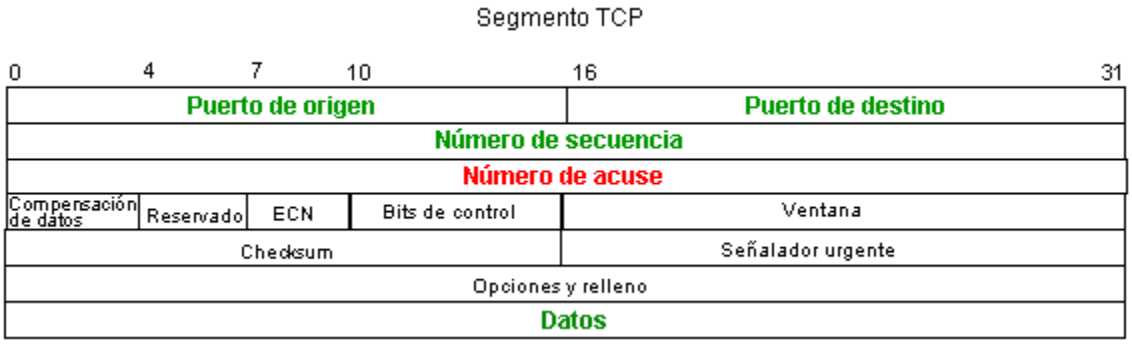

Figura 6. Campos del segmento TCP.

Paso 2: Revise el funcionamiento de la capa de Red.

En la capa de Red, el PAQUETE (IP) IPv4 tiene varios campos completados con información. Esto se ilustra en la Figura 7. Por ejemplo: se observa la Versión del paquete (IPv4), al igual que la dirección IP de origen.

El destino para este paquete es eagle1.example.com. La dirección IP correspondiente se debe averiguar a través del DNS (Sistema de nombres de dominio). ~~Los campos relacionados con los protocolos de la capa superior permanecen vacíos hasta que se recibe el datagrama de la capa superior~~.

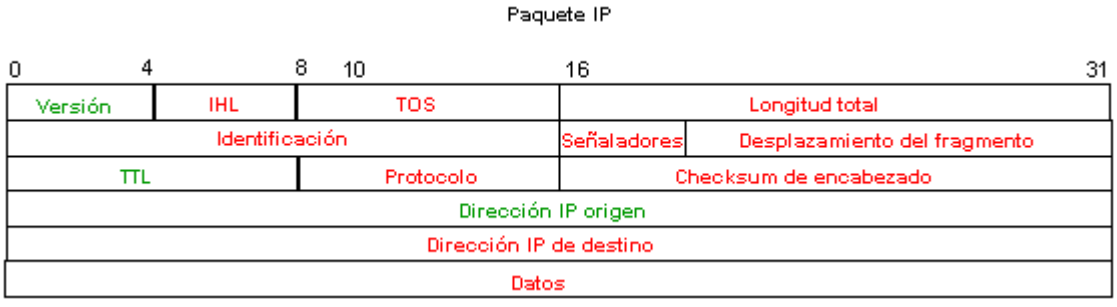

Figura 7. Campos del Paquete IP.

Paso 3: Revise el funcionamiento de la capa de Enlace de datos.

Antes de que el datagrama se coloque en el medio físico, debe encapsularse dentro de una trama. Esto se ilustra en la Figura 8. PC_Client conoce la dirección MAC de origen, pero debe averiguar la dirección MAC de destino.

Se debe averiguar la dirección MAC de destino.

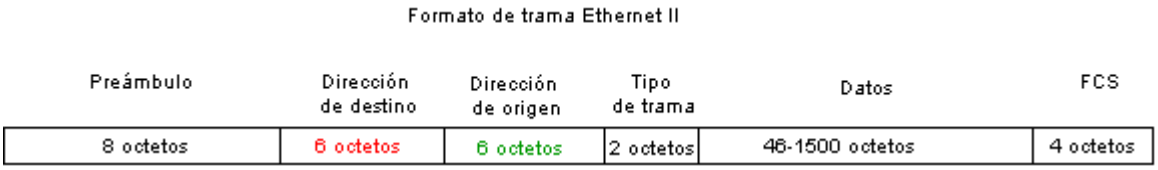

Figura 8. Campos de la trama de Ethernet II.

Tarea 3: Analizar los paquetes capturados.

Paso 1: Revise la secuencia del flujo de datos.

Revisar la información que falta es de utilidad en el seguimiento de la secuencia de los paquetes capturados:

a. ~~No se puede construir el segmento TCP porque el campo de acuse de recibo está en blanco~~. Primero debe completarse un protocolo de enlace de tres vías de TCP con eagle1.example.com.

b. El protocolo de enlace de tres vías de TCP no se puede aplicar porque PC_Client no conoce la dirección IP de eagle1.example.com. Esto se resuelve con una solicitud de DNS de PC_Client a servidor DNS.

c. No se puede consultar al servidor DNS porque se desconoce su dirección MAC. El protocolo ARP se emite en la LAN para averiguar la dirección MAC del servidor DNS.

d. No se conoce la dirección MAC para eagle1.example.com. El protocolo ARP se emite en la LAN para averiguar la dirección MAC de destino de eagle1.example.com.

Paso 2: Examine la solicitud de ARP.

Consulte el N.º 1 en la ventana Lista de paquetes de Wireshark. La trama capturada es una Solicitud de ARP (Address Resolution Protocol). Se puede consultar el contenido de la trama de Ethernet II haciendo clic en la casilla de verificación en la segunda línea de la ventana Detalles del paquete. Se puede ver el contenido de la Solicitud de ARP haciendo clic en la línea de Solicitud de ARP en la ventana Detalles del paquete.

1. ¿Cuál es la dirección MAC de origen para la Solicitud de ARP? _____
2. ¿Cuál es la dirección MAC de destino para la Solicitud de ARP? _____
3. ¿Cuál es la dirección IP desconocida en la Solicitud de ARP? _____
4. ¿Cuál es el tipo de trama de Ethernet II? _____

Paso 3: Examine la respuesta de ARP.

Consulte el N.º 2 en la ventana Lista de paquetes de Wireshark. El servidor DNS envió una Respuesta de ARP.

1. ¿Cuál es la dirección MAC de origen para la Respuesta de ARP? _____
2. ¿Cuál es la dirección MAC de destino para la Solicitud de ARP? _____
3. ¿Cuál es el tipo de trama de Ethernet II? _____
4. ¿Cuál es la dirección IP de destino en la Respuesta de ARP? _____
5. En base a la observación del protocolo ARP, ¿qué se puede inferir acerca de la dirección de destino de una Solicitud de ARP y de la dirección de destino de una Respuesta de ARP?
   _____
   _____
   _____
6. ¿Por qué el servidor DNS no tuvo que enviar una Solicitud de ARP para la dirección MAC de PC_Client? _____
   _____

Paso 4: Examine la consulta de DNS.

Consulte el N.º 3 en la ventana Lista de paquetes de Wireshark. PC_Client envió una consulta de DNS al servidor DNS. Utilizando la ventana Detalles del paquete, responda a las siguientes preguntas:

1. ¿Cuál es el tipo de trama de Ethernet II? _____
2. ¿Cuál es el protocolo de la capa de Transporte, y cuál es el número de puerto de destino?
   _____

Paso 5: Examine la respuesta a la consulta de DNS.

Consulte el N.º 4 en la ventana Lista de paquetes de Wireshark. El servidor DNS envió una respuesta a la consulta de DNS de PC_Client. Utilizando la ventana Detalles del paquete, responda a las siguientes preguntas:

1. ¿Cuál es el tipo de trama de Ethernet II? _____
2. ¿Cuál es el protocolo de la capa de Transporte, y cuál es el número de puerto de destino?
   _____
3. ¿Cuál es la dirección IP de eagle1.example.com? _____
4. Un colega es un administrador de firewall, y preguntó si conocía alguna razón por la que no debería bloquearse la entrada de todos los paquetes UDP a la red interna. ¿Cuál es su respuesta?
   _____
   _____
   _____
   _____

Paso 6: Examine la solicitud de ARP.

Consulte el N.º 5 y el N.º 6 de la ventana Lista de paquetes de Wireshark. PC_Client envió una Solicitud de ARP a la dirección IP 10.1.1.254.

1. ¿Esta dirección IP difiere de la dirección IP para eagle1.example.com? Explique.
   _____
   _____

Paso 7: Examine el protocolo de enlace de tres vías de TCP.

Consulte el N.º 7, el N.º 8 y el N.º 9 de la ventana Lista de paquetes de Wireshark. Estas capturas contienen el protocolo de enlace de tres vías de TCP entre PC_Client e eagle1.example.com. Inicialmente, sólo está configurado en el datagrama el señalizador TCP SYN enviado desde PC_Client, número de secuencia 0. eagle1.example.com responde con los señalizadores TCP ACK y SYN establecidos, junto con el acuse de recibo de 1 y la secuencia de 0. ~~En la ventana Lista de paquetes, figura un valor no descrito, **MSS=1460**. MSS significa tamaño máximo de segmento. Cuando se transporta un segmento TCP a través del IPv4, el MSS se calcula como el tamaño máximo de un datagrama IPv4 menos 40 bytes. Este valor se envía durante el comienzo de la conexión. Esto también sucede cuando se negocian las ventanas deslizantes de TCP~~.

1. Si el valor de secuencia inicial de TCP de PC_Client es 0, ¿por qué eagle1.example respondió con un acuse de recibo de 1?
   _____
   _____
2. En el N.º 8 de eagle1.example.com, ¿qué significa el valor de 0x04 del señalador IP?
   _____
3. Una vez que PC_Client completa el protocolo de enlace de 3 vías de TCP, N.º 9 de la Lista de paquetes de Wireshark, ¿cuáles son los estados del señalizador TCP que se devuelven a eagle1.example.com?
   _____

Tarea 4: Completar el análisis final.

Paso 1: Haga coincidir el resultado de Wireshark con el proceso.

Ha sido necesario el envío de un total de nueve datagramas entre PC_Client, el servidor DNS, el gateway e eagle1.example.com para que PC_Client tuviera la información suficiente para enviar la solicitud original del cliente Web a eagle1.example.com. Esto se muestra en el N.º 10 de la Lista de paquetes de Wireshark, donde PC_Client envió una solicitud GET del protocolo Web.

1. Complete con el número correcto de la Lista de paquetes de Wireshark correspondiente a cada una de las siguientes entradas que faltan:

   a. ~~No se puede construir el segmento TCP porque el campo de acuse de recibo está en blanco~~. Primero debe completarse un protocolo de enlace de tres vías de TCP con eagle1.example.com. _____

   b. El protocolo de enlace de tres vías de TCP no se puede aplicar porque PC_Client no conoce la dirección IP de eagle1.example.com. Esto se resuelve con una solicitud de DNS de PC_Client a servidor DNS. _____

   c. No se puede consultar al servidor DNS porque se desconoce su dirección MAC. El protocolo ARP se emite en la LAN para averiguar la dirección MAC del servidor DNS. _____

   d. Se desconoce la dirección MAC para que el gateway llegue a eagle1.example.com. El protocolo ARP se emite en la LAN para averiguar la dirección MAC de destino del gateway. _____

2. El N.º 11 de la Lista de paquetes de Wireshark es un acuse de recibo de eagle1.example.com para la solicitud GET de PC_Client, el N.º 10 de la Lista de paquetes Wireshark.

3. Los N.º 12, 13 y 15 de la Lista de paquetes de Wireshark son segmentos TCP de eagle1.example.com. Los N.º 14 y 16 de la Lista de paquetes de Wireshark son datagramas de ACK de PC_Client.

4. Para verificar el ACK, resalte el N.º 14 de la Lista de paquetes de Wireshark. Luego, desplácese hasta la parte inferior de la ventana de la lista de detalles, y amplíe la trama [SEQ/ACK analysis]. ¿A qué datagrama de eagle1.example.com responde el datagrama ACK para el N.º 14 de la Lista de paquetes de Wireshark? _____

5. El datagrama N.º 17 de la Lista de paquetes de Wireshark se envía desde PC_Client a eagle1.example.com. Revise la información que se encuentra dentro de la trama [SEQ/ACK analysis]. ¿Cuál es el propósito de este datagrama? _____

6. Cuando PC_Client finaliza, se envían los señalizadores TCP ACK y FIN, que se muestran en el N.º 18 de la Lista de paquetes de Wireshark. eagle1.example.com responde con un ACK de TCP, y se cierra la sesión TCP.

Paso 2: Use el flujo TCP de Wireshark.

Analizar el contenido de los paquetes puede ser una experiencia abrumadora, prolongada y con tendencia a los errores. Wireshark incluye una opción que construye el flujo TCP en otra ventana. Para usar esta función, seleccione primero un datagrama TCP de la Lista de paquetes de Wireshark. A continuación, en el menú de Wireshark, seleccione las opciones Analizar | Seguir flujo TCP. Se mostrará una ventana similar a la Figura 9.

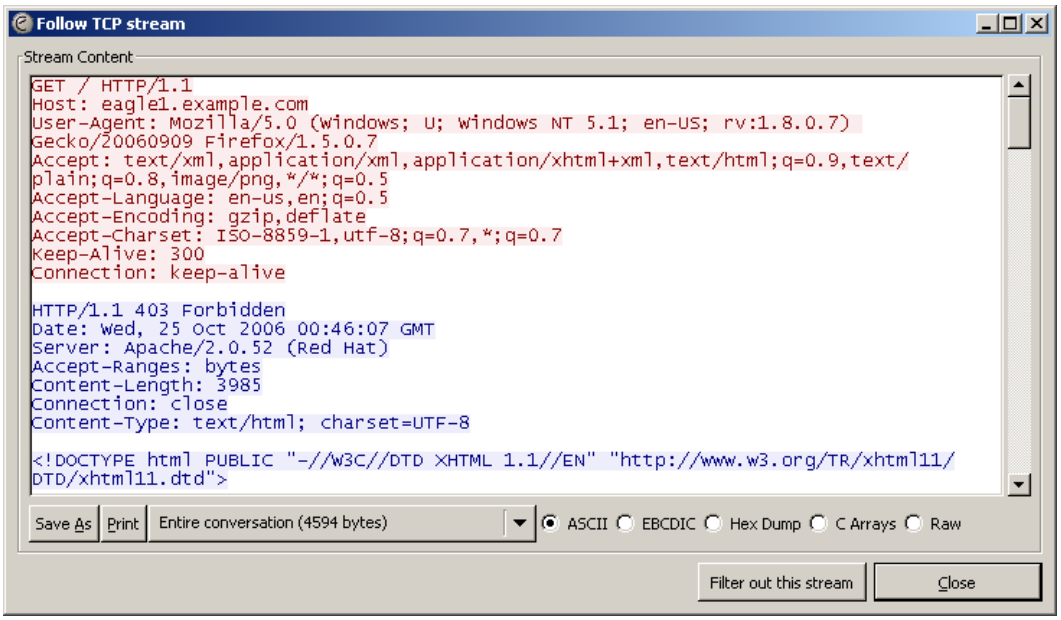

Figura 9. Resultado del flujo TCP.

Tarea 5: Conclusión

Usar un analizador de protocolos de red puede ser una herramienta de aprendizaje efectiva para comprender los elementos fundamentales de la comunicación en red. Una vez que el administrador de red se familiariza con los protocolos de comunicación, el mismo analizador de protocolos puede convertirse en una herramienta efectiva para la resolución de problemas cuando se producen fallas en la red. Por ejemplo, si un explorador Web no se pudo conectar a un servidor Web pueden existir diversas causas. Un analizador de protocolos muestra las solicitudes de ARP fallidas, las consultas de DNS fallidas y los paquetes sin acuse de recibo.

Tarea 6: Resumen

En este ejercicio el estudiante ha aprendido cómo se establece la comunicación entre en un cliente Web y un servidor Web. Los protocolos que no están a la vista, como DNS y ARP, se usan para completar las partes faltantes de los paquetes IP y de las tramas de Ethernet, respectivamente. Antes de poder iniciar una sesión TCP, el protocolo de enlace de tres vías de TCP debe establecer una ruta confiable y suministrar la información del encabezado TCP inicial a ambos sistemas finales que se comunican. Por ultimo, cuando el cliente envía un señalizador TCP FIN se elimina la sesión TCP de manera ordenada.