INGENIERÍA DE TRÁFICO

PRACTICA DE LABORATORIO

TÍTULO: HISTOGRAMAS DE TRAZAS DE TRÁFICO

Profesor: Jhon Jairo Padilla Aguilar, PhD.

1. OBJETIVOS:

-Aprender a utilizar el programa Wireshark para realizar histogramas de ciertas variables como un paso inicial para el modelado matemático

2. REQUISITOS:

-Conocer los conceptos básicos de la organización de los protocolos de la arquitectura TCP/IP.

-Haber realizado la práctica de “Conceptos básicos de protocolos” para tener un conocimiento básico del programa “WireShark”.

3. MARCO TEÓRICO

3.1. DESCRIPCIÓN DEL PROTOCOLO HTTP

Los archivos extraídos de Internet son principalmente paginas HTML. Una página HTML que contiene imágenes es una combinación de múltiples objetos, lo que genera a su vez múltiples peticiones a un servidor. Como puede observarse en la figura 1, es importante entender que un simple “clic” dado por el cliente puede generar una serie de peticiones de archivos en el servidor.

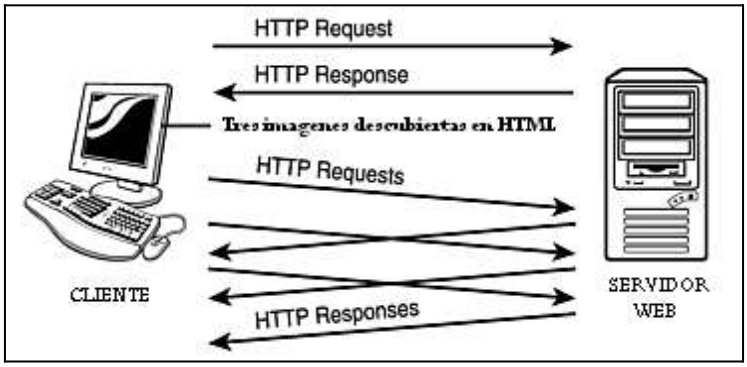


Figura 1. Página HTML con tres imágenes.

El software que principalmente interviene en los servidores Web, es el software que se encarga de gestionar el protocolo HTTP. Este es un protocolo de nivel de aplicación que es usado para comunicaciones entre clientes y servidores Web. Del lado del usuario, se utiliza un navegador tal como el Internet Explorer, el mozilla, etc.

3.1.1. Peticiones HTTP

HTTP define una simple interacción petición-respuesta, la cual puede ser vista como una transacción Web. Una petición HTTP incluye varias partes:

- *Método*: el cual especifica la acción legal a realizarse. Los tipos de métodos HTTP son: GET, POST, PUT, DELETE, HEAD, TRACE y OPTIONS. En la figura 2 se puede observar el Método GET en el mensaje de requerimiento, mientras que en la figura 3 se observa el Método PUT.
- *URL*: El cual identifica el nombre y la dirección de la información requerida como se observa en la figura 2.

- *Información Complementaria*: El tipo de documentos que se puede recibir, autenticación, aspectos de caching, etc. En la Figura 2 no se registra información complementaria en el mensaje requerido.

Como ejemplo se encuentra uno de los métodos más populares, el método GET, el cual se usa cuando se da un clic sobre un link o se digita un URL en la barra de un navegador, básicamente es una petición para recibir el contenido de la página Web solicitada como se observa en la figura 2.

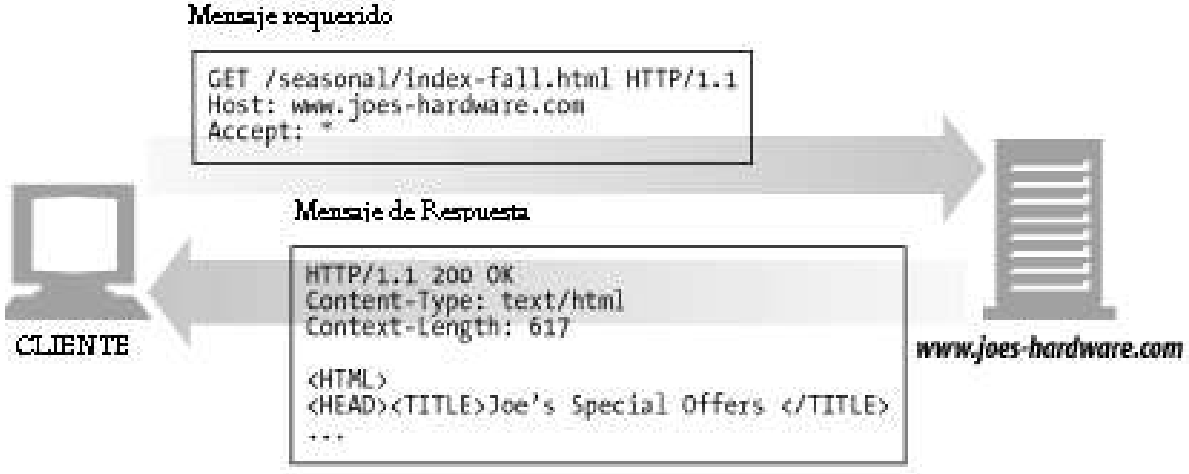


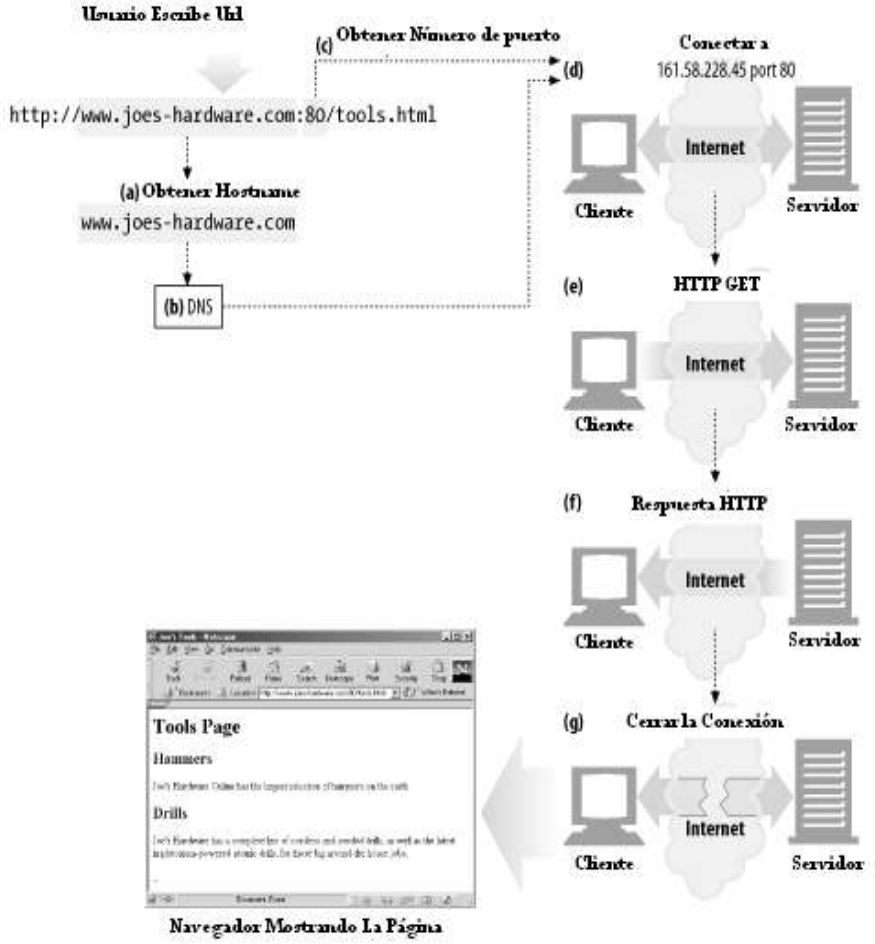
Figura 2: Ejemplo de Petición HTTP método GET.

3.1.2. Peticiones HTTP sobre Conexiones TCP

HTTP es considerado un protocolo sin estado debido a que no incluye el concepto de sesión o interacción mas allá de emitir documentos solicitados. Los principales pasos que intervienen en una interacción petición-respuesta en HTTP sobre TCP se observan en la figura 3.

En la versión original del protocolo HTTP 1.0, una conversación está restringida a la transferencia de un solo objeto (documento, imagen, etc.) a la vez, lo cual quiere decir que cada una es independiente de la otra como se muestra en la Figura 4 (a). Una página con texto y muchas imágenes pequeñas genera muchas conexiones por separado para el texto y para cada imagen. Ya que la mayoría de objetos en la Web son pequeños, una fracción alta de paquetes intercambiados entre clientes y servidores son simplemente paquetes de control TCP utilizados en la apertura y cierre de conexiones.

Por otra parte, en la versión HTTP 1.1, se usa la persistencia, que permite mantener la misma conexión TCP en todas peticiones HTTP de una misma página. Es decir se usa solo una conexión TCP para trasportar múltiples peticiones HTTP, eliminando el costo de varias aperturas y cierres de conexión como se observa en la figura 4 (b).



Navegador Mostrando La Página

Figura 3: HTTP sobre TCP.

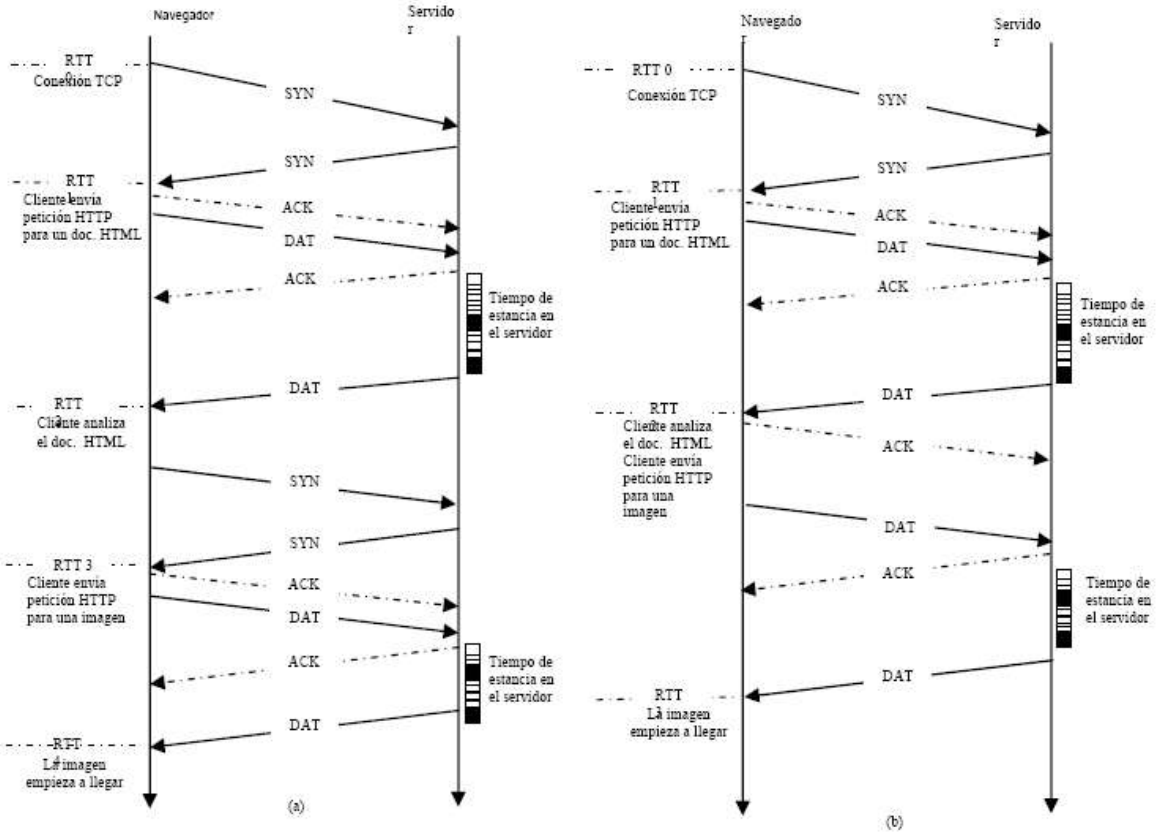


Figura 4: (a) Comunicación con HTTP 1.0, (b) Comunicación con HTTP 1.1.

4. PROCEDIMIENTO:

1. Active el modo de captura del WireShark usando la tarjeta de red que tenga su computador.
2. Ejecute el Browser de Internet y navegue en diferentes páginas durante 20 minutos mientras toma muestras de tráfico.
3. Con las muestras tomadas extraiga las comunicaciones que utilizan el protocolo HTTP (Hyper Text Transfer Protocol), usado para solicitar y transferir páginas Web (utilice la opción STATISTICS>CONVERSATIONS).
    a. En la ventana CONVERSATIONS, en la pestaña TCP, aparecerán las diferentes comunicaciones que ha habido con el protocolo TCP. Tales comunicaciones se identifican por la dirección IP origen, dirección IP destino, puerto origen y puerto destino.
    b. En la parte inferior hay una casilla con el título “Name Resolution”. Esta permite mostrar los datos de puertos en forma de nombres o en forma de números. Observe que hay comunicaciones entre diferentes puertos, uno de ellos lleva el nombre “http”.

c. Con esta herramienta, usted podrá saber cuántos paquetes y cuántos bytes se han transferido en cada sentido para cada comunicación HTTP y la duración de cada comunicación, además de la velocidad de transferencia en bps (bits por segundo). Anote esta información para cada sentido de la comunicación. Esta información también puede ser copiada haciendo clic en el botón COPY de la esquina inferior izquierda y pegando en un documento de Word o Excel (Los campos se separan por comas).
d. Utilice la información recolectada para hacer los siguientes histogramas:
    i. Duración de las conexiones
    ii. Tamaño en bytes de las descargas HTTP (sólo se toman los objetos o páginas web que recibió su computador).
    iii. Haga un análisis de estos histogramas.

4. TAREA: Realice un informe consignando el procedimiento seguido, las gráficas obtenidas y un análisis estadístico: media, varianza, máximo, mínimo de cada una de las variables.