ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA
Departamento de Tecnología Electrónica

Redes de Computadores

Estudio Teórico Sesión Laboratorio 3: Nivel de Aplicación en Internet: DNS y HTTP.

2º Curso, Grado en Ingeniería en Informática
Departamento de Tecnología Electrónica
Universidad de Sevilla

Octubre 2019

Enunciado de la Sesión de Laboratorio 3: Nivel de Aplicación en Internet: DNS y HTTP.

Objetivos de la práctica

- Aplicar filtros Wireshark.
- Analizar tráfico DNS y HTTP con Wireshark.

Estudio previo

Además de estudiar toda la teoría de los temas 1 y 2, se deben resolver **de manera justificada y manuscrita** las siguientes cuestiones, antes de la sesión de laboratorio:

1. En un PC con dirección IP 193.1.3.116 se ha abierto un navegador, se ha borrado la caché de páginas y se ha escrito en la barra de direcciones el URL de la página /letras/omega.html, ubicada en un servidor web, del cual se ha descargado. Mientras se hacía esto se estaba capturando el tráfico de la red con Wireshark, para posteriormente exportar a un fichero todo el tráfico TCP de la red durante el tiempo que duró la descarga de la página. Al final de este documento, en la Figura 1, puede verse el aspecto de la pantalla de Wireshark mostrando el contenido del fichero de captura con un filtro de visualización que sólo deja ver las tramas que contienen PDUs del protocolo HTTP. Responda ***de manera razonada*** las siguientes cuestiones:
    - **a.** ¿Qué dirección IP tiene el servidor web?
    - **b.** Podrá observar que hay otro cliente distinto al 193.1.3.116, generando tráfico en la red. Indique la IP de este segundo cliente.
    - **c.** ¿El otro cliente se ha conectado al mismo servidor que nosotros?
    - **d.** ¿Cuál cree que es la URL completa que hemos escrito en el navegador del PC cuya IP es la 193.1.3.116?
    - **e.** Indique si está o no activada la opción "Resolve transport names" de Wireshark.
    - **f.** Indique si está o no activada la opción "Resolve network (IP) adresses" de Wireshark.
    - **g.** Indique qué columnas del listado de tramas se han añadido con respecto a las que aparecen por defecto en Wireshark y cuáles se han eliminado**.**
    - **h.** Indique cuántas conexiones TCP pueden verse en la Figura 1. Para cada conexión indique los cuatro parámetros que la identifican (socket del cliente y socket del servidor).
    - **i.** Indique en qué instante de tiempo se puede ver claramente que el equipo 193.1.3.116 está usando "en paralelo" sus conexiones TCP para pedir los objetos al servidor. Debe indicar el instante preciso en el que esté pidiendo "en paralelo" un número máximo de objetos e indicar cuáles son esos objetos. Nótese que con la expresión "pedir en paralelo" se quiere decir que hay varias peticiones "en vuelo", cada una por una conexión diferente, pendientes de ser respondidas por el servidor.
    - **j.** Fíjese en la HTTP_PDU mostrada en la trama 17 y diga si se trata de un "GET CONDICIONAL".
    - **k.** ¿Ha respondido el servidor al GET mostrado en la trama 17? Si es así, explique qué significa la respuesta del servidor.
    - **l.** ¿Se han pedido más objetos al servidor por la misma conexión TCP por la que se ha hecho el GET de la trama 17? Si es así indique cuáles han sido.
    - **m.** Explique si el GET mostrado en la trama 18 es un "GET CONDICIONAL".
    - **n.** Explique si el GET mostrado en la trama 27 es un "GET CONDICIONAL".
    - **o.** Indique cuántos objetos referenciados contiene la página web que se ha cargado en el navegador del PC cuya IP es 193.1.3.116.
    - **p.** Identifique la conexión TCP por la que se haya pedido al servidor web un número mayor de objetos e indique el nombre de dichos objetos.

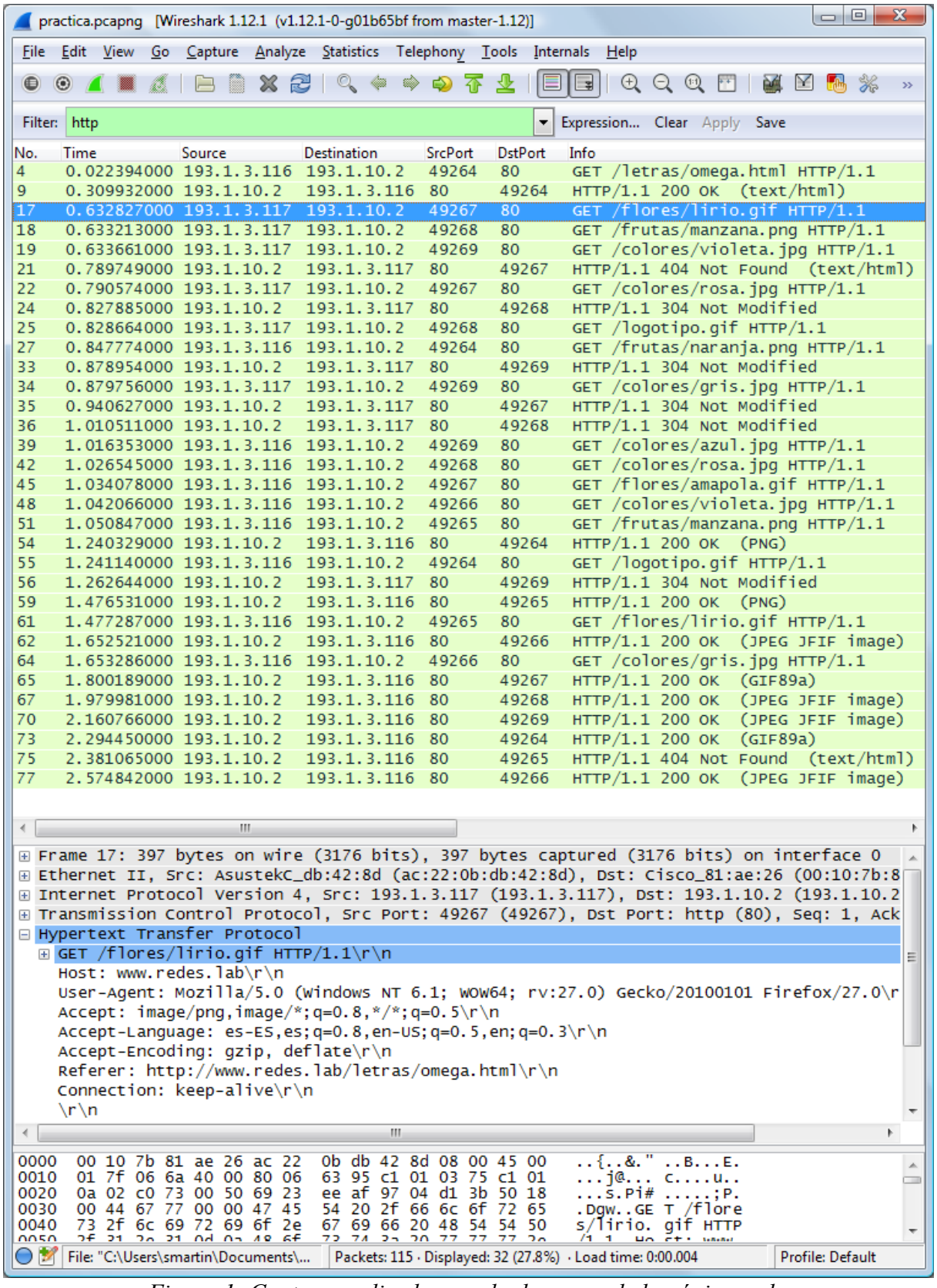

Figura 1: Captura realizada para la descarga de la página web.