



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) addresses" 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.

practica.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	SrcPort	DstPort	Info
4	0.022394000	193.1.3.116	193.1.10.2	49264	80	GET /letras/omega.html HTTP/1.1
9	0.309932000	193.1.10.2	193.1.3.116	80	49264	HTTP/1.1 200 OK (text/html)
17	0.632827000	193.1.3.117	193.1.10.2	49267	80	GET /flores/lirio.gif HTTP/1.1
18	0.633213000	193.1.3.117	193.1.10.2	49268	80	GET /frutas/manzana.png HTTP/1.1
19	0.633661000	193.1.3.117	193.1.10.2	49269	80	GET /colores/violeta.jpg HTTP/1.1
21	0.789749000	193.1.10.2	193.1.3.117	80	49267	HTTP/1.1 404 Not Found (text/html)
22	0.790574000	193.1.3.117	193.1.10.2	49267	80	GET /colores/rosa.jpg HTTP/1.1
24	0.827885000	193.1.10.2	193.1.3.117	80	49268	HTTP/1.1 304 Not Modified
25	0.828664000	193.1.3.117	193.1.10.2	49268	80	GET /logotipo.gif HTTP/1.1
27	0.847774000	193.1.3.116	193.1.10.2	49264	80	GET /frutas/naranja.png HTTP/1.1
33	0.878954000	193.1.10.2	193.1.3.117	80	49269	HTTP/1.1 304 Not Modified
34	0.879756000	193.1.3.117	193.1.10.2	49269	80	GET /colores/gris.jpg HTTP/1.1
35	0.940627000	193.1.10.2	193.1.3.117	80	49267	HTTP/1.1 304 Not Modified
36	1.010511000	193.1.10.2	193.1.3.117	80	49268	HTTP/1.1 304 Not Modified
39	1.016353000	193.1.3.116	193.1.10.2	49269	80	GET /colores/azul.jpg HTTP/1.1
42	1.026545000	193.1.3.116	193.1.10.2	49268	80	GET /colores/rosa.jpg HTTP/1.1
45	1.034078000	193.1.3.116	193.1.10.2	49267	80	GET /flores/amapola.gif HTTP/1.1
48	1.042066000	193.1.3.116	193.1.10.2	49266	80	GET /colores/violeta.jpg HTTP/1.1
51	1.050847000	193.1.3.116	193.1.10.2	49265	80	GET /frutas/manzana.png HTTP/1.1
54	1.240329000	193.1.10.2	193.1.3.116	80	49264	HTTP/1.1 200 OK (PNG)
55	1.241140000	193.1.3.116	193.1.10.2	49264	80	GET /logotipo.gif HTTP/1.1
56	1.262644000	193.1.10.2	193.1.3.117	80	49269	HTTP/1.1 304 Not Modified
59	1.476531000	193.1.10.2	193.1.3.116	80	49265	HTTP/1.1 200 OK (PNG)
61	1.477287000	193.1.3.116	193.1.10.2	49265	80	GET /flores/lirio.gif HTTP/1.1
62	1.652521000	193.1.10.2	193.1.3.116	80	49266	HTTP/1.1 200 OK (JPEG JFIF image)
64	1.653286000	193.1.3.116	193.1.10.2	49266	80	GET /colores/gris.jpg HTTP/1.1
65	1.800189000	193.1.10.2	193.1.3.116	80	49267	HTTP/1.1 200 OK (GIF89a)
67	1.979981000	193.1.10.2	193.1.3.116	80	49268	HTTP/1.1 200 OK (JPEG JFIF image)
70	2.160766000	193.1.10.2	193.1.3.116	80	49269	HTTP/1.1 200 OK (JPEG JFIF image)
73	2.294450000	193.1.10.2	193.1.3.116	80	49264	HTTP/1.1 200 OK (GIF89a)
75	2.381065000	193.1.10.2	193.1.3.116	80	49265	HTTP/1.1 404 Not Found (text/html)
77	2.574842000	193.1.10.2	193.1.3.116	80	49266	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 17: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface 0

- Ethernet II, Src: AsustekC_db:42:8d (ac:22:0b:db:42:8d), Dst: Cisco_81:ae:26 (00:10:7b:8
- Internet Protocol Version 4, Src: 193.1.3.117 (193.1.3.117), Dst: 193.1.10.2 (193.1.10.2
- Transmission Control Protocol, Src Port: 49267 (49267), Dst Port: http (80), Seq: 1, Ack
- Hypertext Transfer Protocol
 - GET /flores/lirio.gif HTTP/1.1\r\n
 - Host: www.redes.lab\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0\r
 - Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n
 - Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Referer: http://www.redes.lab/letras/omega.html\r\n
 - Connection: keep-alive\r\n
 - \r\n

0000 00 10 7b 81 ae 26 ac 22 0b db 42 8d 08 00 45 00 ..{.&." ..B...E.
 0010 01 7f 06 6a 40 00 80 06 63 95 c1 01 03 75 c1 01 ...j@... C....u..
 0020 0a 02 c0 73 00 50 69 23 ee af 97 04 d1 3b 50 18 ...s.Pi#;P.
 0030 00 44 67 77 00 00 47 45 54 20 2f 66 6c 6f 72 65 .Dgw..GE T /flore
 0040 73 2f 6c 69 72 69 6f 2e 67 69 66 20 48 54 54 50 s/lirio. gif HTTP
 0050 2f 21 2a 21 0d 02 48 6f 72 74 2a 20 77 77 72 2a /1.1

File: "C:\Users\smartin\Documents\... Packets: 115 · Displayed: 32 (27.8%) · Load time: 0:00.004 Profile: Default

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