



“Secretaría De La Educación Superior”
“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#4 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 1/Diciembre/2020

Horario: 5:00 pm – 6:00 pm

Laboratio N#4 – Agregue el campo de host HTTP como una columna.

Debemos de buscar y abrir el archivo http-disney101.pcapng.

Y esto es lo que nos debe de abrir el archivo en wireshark.

The screenshot shows the Wireshark interface with the file 'http-disney101.pcapng' open. The packet list pane displays a list of packets, with the first packet selected:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
2	1.001249	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
3	1.001439	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
4	2.001502	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
5	2.001741	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
6	4.001569	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
7	4.001790	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
8	8.835279	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
9	8.886045	75.75.76.76	24.6.173.220	DNS	104	Standard query response 0x1722 A www.disney.com CNAME

The packet details pane for the selected packet shows the following structure:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
- Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
- User Datagram Protocol, Src Port: 63551, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00  ..\1... d...E.
0010 00 3c 69 7b 00 00 80 11 00 00 18 06 ad dc 4b 4b  <i{.....KK
0020 4b 4b f8 3f 00 35 00 28 5c b2 17 22 01 00 00 01  KK.?5( \..."
0030 00 00 00 00 00 00 03 77 77 77 06 64 69 73 6e 65  ....www-disne
0040 79 03 63 6f 6d 00 00 01 00 01                    y.com... ..
```

The status bar at the bottom indicates: Bytes 12-13: Type (eth.type) | Paquetes: 6143 · Mostrado: 6143 (100.0%) | Perfil: Default

En este paso debemos de ocultar la columna Time, dándole clic derecho para que nos muestre todas las opciones y así poderla desactivar.

Ademas que debemos de desplazar la barra para acomodarlos.

The screenshot shows a Windows desktop environment. In the background, a Microsoft Word document titled "Laboratorio3 - Word" is open, displaying a "Navegación" (Navigation) pane on the left. In the foreground, the Wireshark network protocol analyzer is open, displaying a packet capture file named "http-disney101.pcapng". The main pane shows a list of DNS packets. A right-click context menu is open over the "Time" column header, and the option "Time (format as specified)" is selected. The taskbar at the bottom shows the Windows Start button, task view, search, and several application icons. The system clock in the bottom right corner indicates the time is 10:01 p.m. on 30/11/2020.

No.	Source	Destination	Protocol	Length	Info
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
74	Standard query 0x1722 A www.disney.com		DNS	74	Standard query 0x1722 A www.disney.com
104	Standard query response 0x1722 A www.disney.com CNAME disney.com		DNS	104	Standard query response 0x1722 A www.disney.com CNAME disney.com

Aquí debemos de buscar el Numero #15 en los detalles del paquete y ampliar nuestra selección del marco.

Debemos de darle clic derecho a la parte del Host (www.disney.com) y la aplicamos justamente en esa columna de host en la información.

The screenshot displays a Windows desktop environment. In the background, a Microsoft Word document titled 'Laboratorio3 - Word' is open, showing a blank page with a ribbon menu. Overlaid on top of the Word document is a packet capture analysis window titled 'http-disney101.pcapng'. The window has a menu bar with options like 'Archivo', 'Edición', 'Visualización', 'Ir', 'Captura', 'Analizar', 'Estadísticas', 'Telefonía', 'Wireless', 'Herramientas', and 'Ayuda'. Below the menu bar is a search bar with the text 'Aplicar un filtro de visualización... <Ctrl-F>'. The main area of the window is divided into two panes. The top pane is a table with columns: 'No.', 'Source', 'Destination', 'Protocol', 'Length', 'Hypertext Transfer Protocol', 'Host', and 'Info'. The table contains several rows of network traffic data. Row 15 is highlighted in green and shows an HTTP GET request to 'www.disney.com'. The bottom pane shows the details of the selected packet (No. 15), including the 'Transmission Control Protocol' and 'Hypertext Transfer Protocol' sections. The 'Hypertext Transfer Protocol' section shows the request details: 'GET / HTTP/1.1\r\n', 'Host: www.disney.com\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n', and 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n'. The bottom status bar of the packet capture window shows 'HTTP Host (http.host), 22 byte(s)' and 'Paquetes: 6143 · Mostrado: 6143 (100.0%)'. The Windows taskbar at the bottom shows the Start button, search icon, and several application icons, including Word, Chrome, and File Explorer. The system clock in the bottom right corner shows '10:43 p. m.' and '30/11/2020'.

No.	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
10	24.6.173.220	75.75.76.76	DNS	74			Standard query 0x33f3
11	75.75.76.76	24.6.173.220	DNS	134			Standard query respon
12	24.6.173.220	199.181.132.249	TCP	66			35518 → 80 [SYN] Seq=
13	199.181.132.249	24.6.173.220	TCP	66			80 → 35518 [SYN, ACK]
14	24.6.173.220	199.181.132.249	TCP	54			35518 → 80 [ACK] Seq=
15	24.6.173.220	199.181.132.249	HTTP	342	✓	www.disney.com	GET / HTTP/1.1
16	199.181.132.249	24.6.173.220	HTTP	514	✓		HTTP/1.1 301 Moved Pe
17	24.6.173.220	75.75.76.76	DNS	70			Standard query 0xf827
18	75.75.76.76	24.6.173.220	DNS	86			Standard query respon

```
> Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
> Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
Host: www.disney.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
```

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0050 64 69 73 6e 65 79 2e 63 6f 6d 0d 0a 55 73 65 72 disney.c om..User
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT
0080 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 6.1; WOW 64; rv:1
0090 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 6.0) Gec ko/20100
00a0 31 30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30 101 Fire fox/16.0
00b0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 ..Accept : text/h
00c0 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f tml,appl ication/
00d0 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 xhtml+xm l,applic
00e0 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c ation/xm l;q=0.9,

Hacemos clic en la parte de host dos veces para que esta se acomode mayor a menor como muestra en la captura de pantalla.

Labotario3 - Word

Herramientas de imagen

JAVIER JESUS VARGAS RODRIGUEZ

Archivo Inicio Insertar Diseño Disposición Referencias Correspondencia Revisar Vista Ayuda Formato

¿Qué desea hacer?

Compartir

Cortar Copiar Copiar formato

Portapapeles

Fuente

Arial 14

N K S abc X2 X2

Navegación

Buscar en documento

Titulos Páginas Resultados

Cree un esquema interactivo de su documento.

Es una buena manera de saber dónde se encuentra o moverse rápidamente por el contenido.

Para comenzar, vaya a la pestaña Inicio y aplique estilos de título a los títulos de su documento.

http-disney101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
3445	24.6.173.220	74.217.240.83	HTTP	335	✓	js.revsci.net	GET /gateway/gw.js?cs
4876	24.6.173.220	74.217.240.83	HTTP	431	✓	pix04.revsci.net	GET /A08723/b3/0/3/10
3456	24.6.173.220	199.181.131.249	HTTP	338	✓	search.disney.com	GET /_xd/home/account
1859	24.6.173.220	68.71.209.50	HTTP	379	✓	tredir.go.com	GET /capmon/GetDE/?se
5730	24.6.173.220	66.235.138.59	HTTP	1579	✓	w88.go.com	GET /b/ss/wdgdoldhom,
5941	24.6.173.220	66.235.138.59	HTTP	1952	✓	w88.go.com	GET /b/ss/wdgdoldhom,
5723	24.6.173.220	68.71.216.36	HTTP	1791	✓	weblogger01.data...	GET /?app=w88_dolwa_p
15	24.6.173.220	199.181.132.249	HTTP	342	✓	www.disney.com	GET / HTTP/1.1

< >

Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288

✓ Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: www.disney.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

< >

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1... d....E.

0010 01 48 69 87 40 00 80 06 00 00 18 06 ad dc c7 b5 .Hi.

0020 84 f9 8a be 00 50 73 e7 7d 59 c7 0e 66 a7 50 18Ps. }Y..f.p.

0030 40 29 13 cc 00 00 47 45 54 20 2f 20 48 54 54 50 @)....GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 72 e /1.1..Ho st: www.

0050 64 69 73 6e 65 79 2e 63 6f 6d 0d 0a 55 73 65 72 disney.c om..User

0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/

0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT

0080 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 6.1; WOW 64; rv:1

0090 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 6.0) Gec ko/20100

http-disney101.pcapng

Paquetes: 6143 · Mostrado: 6143 (100.0%) Perfil: Default

Página 4 de 4 41 palabras

10:56 p. m. 30/11/2020