

Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

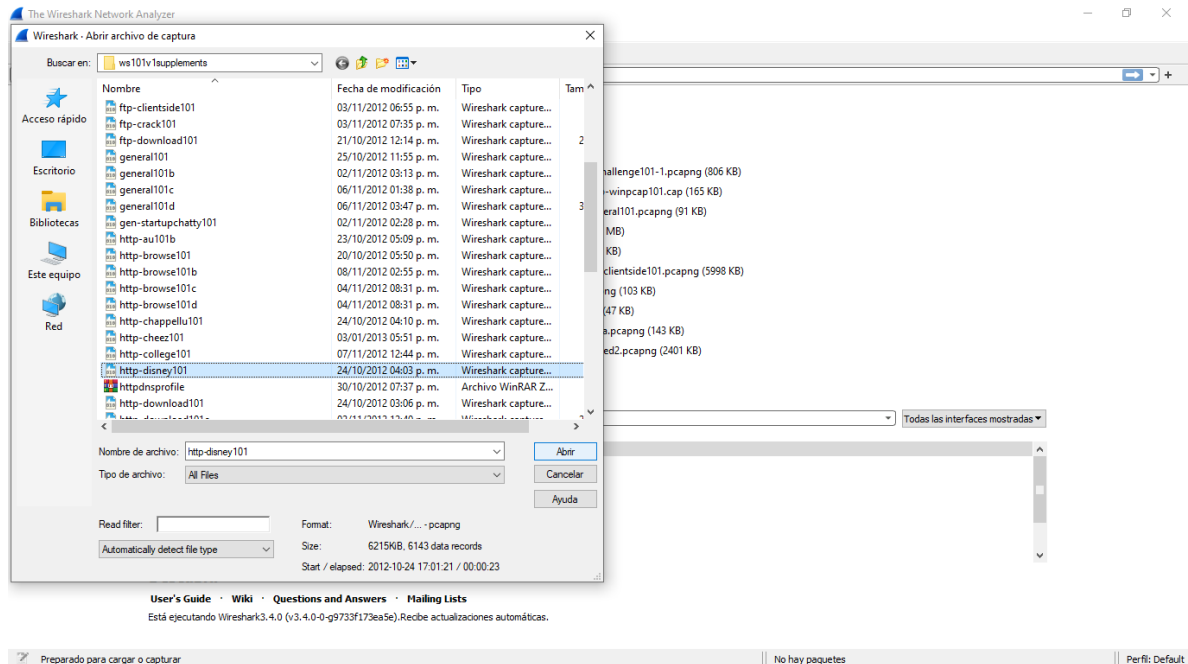
**Laboratorio 4: Agregar el Campo de
Host HTTP como una Columna**

Prof. Ismael Jiménez Sánchez

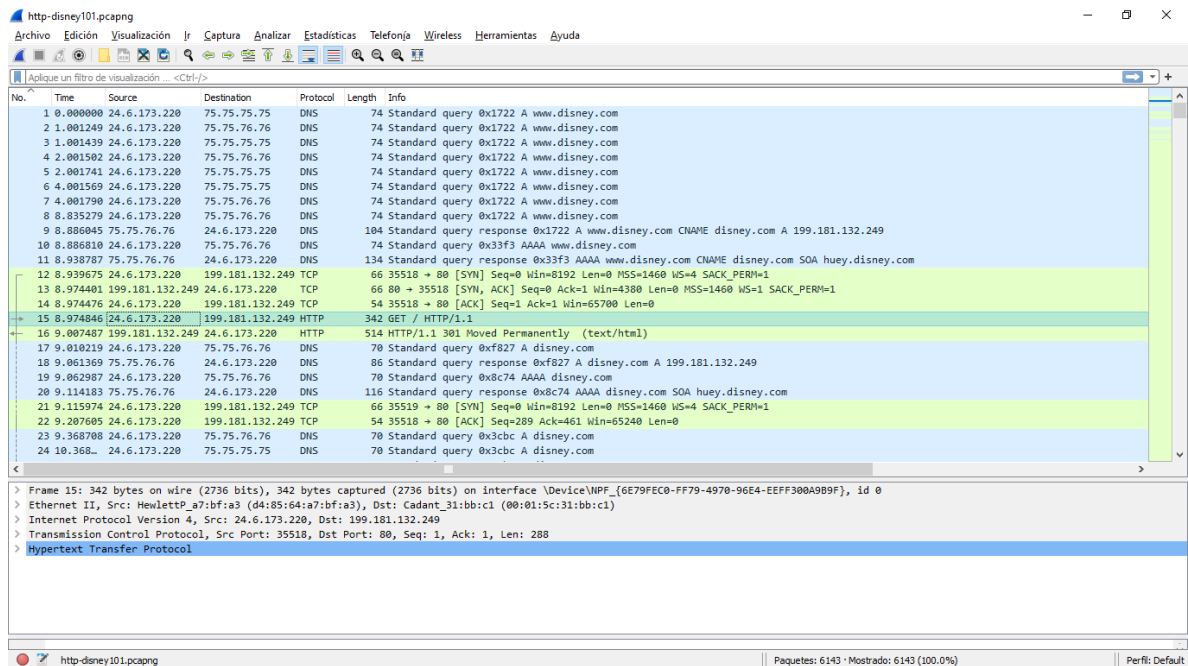
**Alumno(a). Laury del Rosario Mex
Martin**

Ciclo 2020-B

Paso 1: Haga clic en abrir archivo en la barra principal de herramientas y abrir http-disney101.pcapng



Paso 2: Desplazar hacia abajo en el panel Lista de paquetes y seleccione frame 15.



Paso 3: El panel de detalles muestra el contenido del frame 5. Hacemos clic en front of Hypertext Transfer Protocol de esta sección del frame

Wireshark capture of traffic to www.disney.com. The packet list shows a GET request in frame 15. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the request line and headers.

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 disney.com A 199.181.132.249
10	8.886810	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x33f3 AAAA www.disney.com
11	8.938787	75.75.76.76	24.6.173.220	DNS	134	Standard query response 0x33f3 AAAA www.disney.com CNAME disney.com SOA huey.disney.com
12	8.939675	24.6.173.220	199.181.132.249	TCP	66	35518 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	8.974401	199.181.132.249	24.6.173.220	TCP	66	80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
14	8.974476	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	8.974846	24.6.173.220	199.181.132.249	HTTP	342	GET / HTTP/1.1
16	9.007487	199.181.132.249	24.6.173.220	HTTP	514	HTTP/1.1 301 Moved Permanently (text/html)
17	9.010219	24.6.173.220	75.75.76.76	DNS	70	Standard query 0xf827 A disney.com
18	9.061369	75.75.76.76	24.6.173.220	DNS	86	Standard query response 0xf827 A disney.com A 199.181.132.249
19	9.062987	24.6.173.220	75.75.76.76	DNS	70	Standard query 0x8c74 AAAA disney.com
20	9.114183	75.75.76.76	24.6.173.220	DNS	116	Standard query response 0x8c74 AAAA disney.com SOA huey.disney.com
21	9.115974	24.6.173.220	199.181.132.249	TCP	66	35519 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	9.207605	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
23	9.368708	24.6.173.220	75.75.76.76	DNS	70	Standard query 0x3cbc A disney.com
24	10.368...	24.6.173.220	75.75.75.75	DNS	70	Standard query 0x3cbc A disney.com

Packet 15 details:

- 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: 199.181.132.249
- Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
- Hypertext Transfer Protocol
 - GET / HTTP/1.1
 - Host: www.disney.com
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate

Paso 4: Hacemos clic en el botón derecho en línea de host (que contiene www.disney.com/) y seleccione aplicar como columna. La nueva columna aparece del lado izquierdo de la columna de información.

Wireshark capture of traffic to www.disney.com. The packet list shows a GET request in frame 15. The packet details pane shows the Hypertext Transfer Protocol section expanded. A right-click context menu is open over the host 'www.disney.com', with 'Aplicar como columna' 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 disney.com A 199.181.132.249
10	8.886810	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x33f3 AAAA www.disney.com
11	8.938787	75.75.76.76	24.6.173.220	DNS	134	Standard query response 0x33f3 AAAA www.disney.com CNAME disney.com SOA huey.disney.com
12	8.939675	24.6.173.220	199.181.132.249	TCP	66	35518 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	8.974401	199.181.132.249	24.6.173.220	TCP	66	80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
14	8.974476	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	8.974846	24.6.173.220	199.181.132.249	HTTP	342	GET / HTTP/1.1
16	9.007487	199.181.132.249	24.6.173.220	HTTP	514	HTTP/1.1 301 Moved Permanently (text/html)
17	9.010219	24.6.173.220	75.75.76.76	DNS	70	Standard query 0xf827 A disney.com
18	9.061369	75.75.76.76	24.6.173.220	DNS	86	Standard query response 0xf827 A disney.com A 199.181.132.249
19	9.062987	24.6.173.220	75.75.76.76	DNS	70	Standard query 0x8c74 AAAA disney.com
20	9.114183	75.75.76.76	24.6.173.220	DNS	116	Standard query response 0x8c74 AAAA disney.com SOA huey.disney.com
21	9.115974	24.6.173.220	199.181.132.249	TCP	66	35519 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	9.207605	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
23	9.368708	24.6.173.220	75.75.76.76	DNS	70	Standard query 0x3cbc A disney.com
24	10.368...	24.6.173.220	75.75.75.75	DNS	70	Standard query 0x3cbc A disney.com

Packet 15 details:

- 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: 199.181.132.249
- Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
- Hypertext Transfer Protocol
 - GET / HTTP/1.1
 - Host: www.disney.com
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate

Right-click context menu options:

- Expand Subtrees
- Contrair subárboles
- Expandir todo
- Contrair todo
- Aplicar como columna (Control+Mayúsculas+I)
- Aplicar como filtro
- Prepare as Filter
- Filtro de conversación
- Colorize with Filter
- Seguir
- Copiar
- Mostrar bytes de paquete... (Control+Mayúsculas+O)
- Exportar bytes de paquete... (Control+Mayúsculas+X)
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decodificar como... (Control+Mayúsculas+U)
- Ir a paquete enlazado
- Show Linked Packet in New Window

http-disney101.pcapng

Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Host	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	4.001798	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 disney.com A 199.181.132.249
10	8.886810	24.6.173.220	75.75.76.76	DNS	74		Standard query 0x33f3 AAAA www.disney.com
11	8.938787	75.75.76.76	24.6.173.220	DNS	134		Standard query response 0x33f3 AAAA www.disney.com CNAME disney.com SOA huey.disney.com
12	8.939675	24.6.173.220	199.181.132.249	TCP	66		35518 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	8.974401	199.181.132.249	24.6.173.220	TCP	66		80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
14	8.974476	24.6.173.220	199.181.132.249	TCP	54		35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	8.974846	24.6.173.220	199.181.132.249	HTTP	342	www.disney.com	GET / HTTP/1.1
16	9.007487	199.181.132.249	24.6.173.220	HTTP	514		HTTP/1.1 301 Moved Permanently (text/html)
17	9.010219	24.6.173.220	75.75.76.76	DNS	70		Standard query 0xF027 A disney.com
18	9.051369	75.75.76.76	24.6.173.220	DNS	86		Standard query response 0xF027 A disney.com A 199.181.132.249
19	9.062987	24.6.173.220	75.75.76.76	DNS	70		Standard query 0x8c74 AAAA disney.com
20	9.114183	75.75.76.76	24.6.173.220	DNS	116		Standard query response 0x8c74 AAAA disney.com SOA huey.disney.com
21	9.115974	24.6.173.220	199.181.132.249	TCP	66		35519 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	9.207605	24.6.173.220	199.181.132.249	TCP	54		35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
23	9.368708	24.6.173.220	75.75.76.76	DNS	70		Standard query 0x33bc A disney.com
24	10.368...	24.6.173.220	75.75.75.75	DNS	70		Standard query 0x33bc A disney.com

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
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 \r\n
 [Full request URI: http://www.disney.com/]
 [HTTP request 1/2]
 [Response in frame: 16]

http-disney101.pcapng Paquetes: 6143 · Mostrado: 6143 (100.0%) Perfil: Default

Paso 5: Hacemos clic en el encabezado de host 2 veces para ordenar de mayor a menor

http-disney101.pcapng

Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Host	Info
45...	14.014...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/f758140f937e616d3d19b00cf85fd3ed1f4dc58.jpg HTTP/1.1
46...	14.053...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/d35e73955fd29e34bc75c6eb836a60d83b5bd60e.jpg HTTP/1.1
46...	14.056...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/a83e4e43db65bdb67078179115479dceadd6367.jpg HTTP/1.1
47...	14.085...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/9dc97a27a7d906d07b5914c630fa29cb08a3af4.jpg HTTP/1.1
47...	14.093...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/d33887e0a5d0e433ba4708afd2c399d406765733.jpg HTTP/1.1
48...	14.099...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/f646b72e9c6c1602241ed6ddbfbf224b1cfcc25.jpg HTTP/1.1
48...	14.117...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/14226f6f9b22164825625a46ce8b48551d7421c3.jpg HTTP/1.1
49...	14.137...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/7a2549aec01f0225c7d9803b6a4128bae090bcb05.jpg HTTP/1.1
50...	14.156...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/06cf7be448320070b71bed0c8060878f6be567.jpg HTTP/1.1
51...	14.193...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/08f6cd011cde4a9a3a1376e08ea7f15ab6f37d8.jpg HTTP/1.1
53...	14.262...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/85bf6fa6b4a5aaf4145737f8f965a500330cb0f.jpg HTTP/1.1
54...	14.290...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/147ac28b4a83a911c8597a0e2ef601691cdef8f6.jpg HTTP/1.1
54...	14.309...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/85456a4db5f75ee152f2e90f8e954d1674b159a.jpg HTTP/1.1
55...	14.337...	24.6.173.220	208.111.148.6	HTTP	401	cdnvideo.doling.com	GET /cdn_assets/9da0f78de11590e89376c4da5943506f1c1b1ce9a.jpg HTTP/1.1
57...	14.380...	24.6.173.220	198.105.199.137	HTTP	1735	ctologger01.analy...	GET /cto/?app=w88_dolwa_prod038trckTp=trackpage&vendorLst=0x2Cc&Swid=F8605814-055A-4D39-AD95-CEC0317E6054
32	11.415...	24.6.173.220	199.181.132.249	HTTP	338	disney.com	GET / HTTP/1.1
34...	13.525...	24.6.173.220	74.217.240.83	HTTP	335	js.revsci.net	GET /gateway/gw.js?csid=A08723 HTTP/1.1
48...	14.117...	24.6.173.220	74.217.240.83	HTTP	431	pix04.revsci.net	GET /A08723/b3/0/3/1008211/600426858.js?D=DM_LOCK3Dhttp%253A%252F%252Fdisney.com%252F%253F_rsl%2530%260M
34...	13.588...	24.6.173.220	199.181.131.249	HTTP	338	search.disney.com	GET /_xd/home/account/swid.js HTTP/1.1
18...	12.099...	24.6.173.220	68.71.209.50	HTTP	379	wredir.go.com	GET /capmon/GetDe/?set=j¶m=countrysIcode¶m=state¶m=connection HTTP/1.1
57...	14.381...	24.6.173.220	66.235.130.59	HTTP	1579	w08.go.com	GET /b/ss/wdg0ldidom.wdg0sec/1/H.23.3/5353168586114277AQ0=18dm=18t=2452f982f2012K015K3a1K3A3S%203%204200
59...	14.550...	24.6.173.220	66.235.130.59	HTTP	1952	w08.go.com	GET /b/ss/wdg0ldidom.wdg0sec/1/H.23.3/5353168586114277AQ0=18pcr=true&vidn=2044329A051490A5-600001A2C02AE8
57...	14.380...	24.6.173.220	68.71.216.36	HTTP	1791	weblogger01.data...	GET /?app=w88_dolwa_prod028trckTp=trackpage&vendorLst=0x2Cc&Swid=F8605814-055A-4D39-AD95-CEC0317E6054&pgV
15	8.974846	24.6.173.220	199.181.132.249	HTTP	342	www.disney.com	GET / HTTP/1.1

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
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 \r\n
 [Full request URI: http://www.disney.com/]
 [HTTP request 1/2]
 [Response in frame: 16]

http-disney101.pcapng Paquetes: 6143 · Mostrado: 6143 (100.0%) Perfil: Default

Paso 6: Hacemos clic en el botón de Go to up para saltar al inicio del archivo del seguimiento ordenado y se puede ver todo el host al que el cliente envió la solicitud

The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'http-disney101.pcapng'. The menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The toolbar contains various icons for file operations, capture, analysis, and display. The main window is divided into three panes:

- Packet List:** Displays a list of 25 captured packets. The first packet (No. 1) is a DNS standard query for 'www.disney.com' from source 24.6.173.220 to destination 75.75.75.75. The packet length is 74 bytes.
- Packet Details:** Shows the hierarchical structure of the selected packet (Frame 1). It includes:
 - 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:bfa3 (d4:85:64:a7:bfa3), 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)
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

The status bar at the bottom indicates 'Paquetes: 6143 · Mostrado: 6143 (100.0%)' and 'Perfil: Default'.