

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

**Lab16 - Filter on HTTP Traffic the Right
Way**

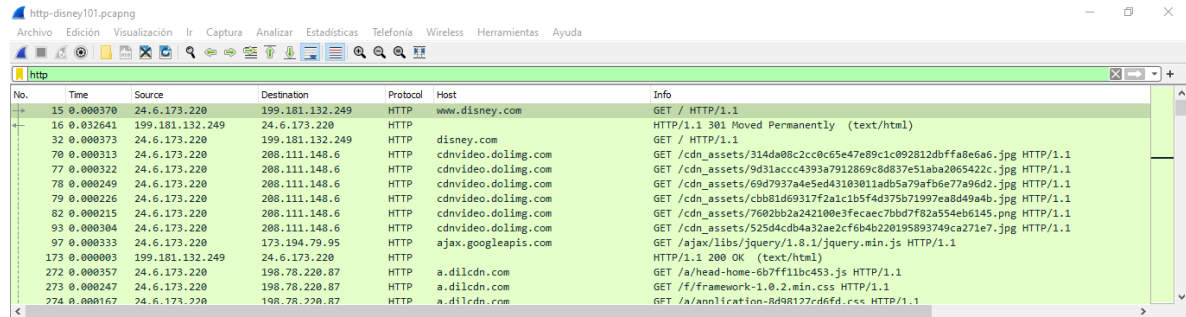
Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab16 - Filter on HTTP Traffic the Right Way

1 Abrimos el archivo http-disney101.pcapng.

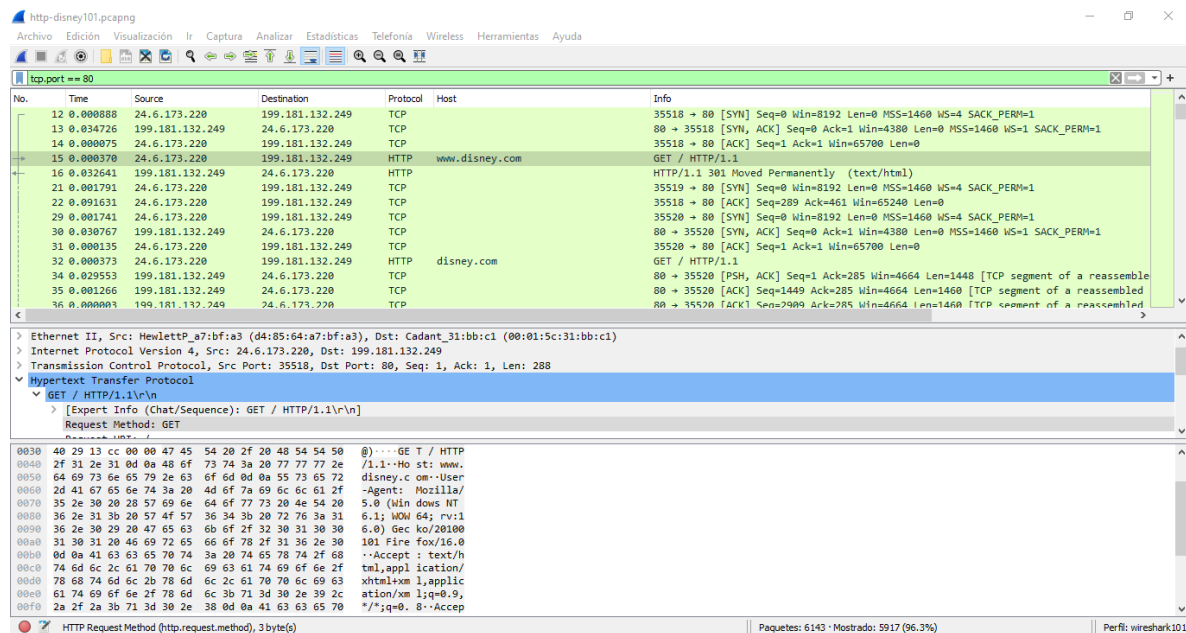
2 Aplicamos el filtro HTTP



The screenshot shows the Wireshark interface with the file 'http-disney101.pcapng' open. The filter bar at the top contains the filter 'http'. The packet list pane shows 274 packets, all of which are HTTP requests. The packet details pane shows the selected packet (No. 15) as a GET request to 'http://www.disney.com'.

No.	Time	Source	Destination	Protocol	Host	Info
15	0.000370	24.6.173.220	199.181.132.249	HTTP	www.disney.com	GET / HTTP/1.1
16	0.032641	199.181.132.249	24.6.173.220	HTTP		HTTP/1.1 301 Moved Permanently (text/html)
32	0.000373	24.6.173.220	199.181.132.249	HTTP	disney.com	GET / HTTP/1.1
70	0.000313	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/314da08c2cc0c65e47e89c1c092812dbffa8e6a6.jpg HTTP/1.1
77	0.000322	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/9d31acc4393a7912869c8d837e51aba2065422c.jpg HTTP/1.1
78	0.000249	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/69d7937a4e5ed43103011adb5a79af6e77a96d2.jpg HTTP/1.1
79	0.000226	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/cbb81d69317f2a1c1b5f4d375b71997ea8d49a4b.jpg HTTP/1.1
82	0.000215	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/7682bb2a24100e3fecae7bbd7f82a554eb6145.png HTTP/1.1
93	0.000304	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/525d4cbb4a32ae2cf6b4b220195893749ca271e7.jpg HTTP/1.1
97	0.000333	24.6.173.220	173.194.79.95	HTTP	ajax.googleapis.com	GET /ajax/libs/jquery/1.8.1/jquery.min.js HTTP/1.1
173	0.000003	199.181.132.249	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)
272	0.000357	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/head-home-0b7ff1b0c453.js HTTP/1.1
273	0.000247	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /f/framework-1.0.2.min.css HTTP/1.1
274	0.000167	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/animation-Bd9R122cd6fd.css HTTP/1.1

3. Cambiamos el filtro de HTTP por tcp.port == 80



The screenshot shows the Wireshark interface with the filter 'tcp.port == 80' applied. The packet list pane shows 36 packets, all of which are TCP segments. The packet details pane shows the selected packet (No. 15) as a GET request to 'http://www.disney.com'.

No.	Time	Source	Destination	Protocol	Host	Info
12	0.000088	24.6.173.220	199.181.132.249	TCP		35518 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	0.034726	199.181.132.249	24.6.173.220	TCP		80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
14	0.000075	24.6.173.220	199.181.132.249	TCP		35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	0.000370	24.6.173.220	199.181.132.249	HTTP	www.disney.com	GET / HTTP/1.1
16	0.032641	199.181.132.249	24.6.173.220	HTTP		HTTP/1.1 301 Moved Permanently (text/html)
21	0.001791	24.6.173.220	199.181.132.249	TCP		35519 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	0.091631	24.6.173.220	199.181.132.249	TCP		35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
29	0.001741	24.6.173.220	199.181.132.249	TCP		35520 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
30	0.030767	199.181.132.249	24.6.173.220	TCP		80 → 35520 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
31	0.000135	24.6.173.220	199.181.132.249	TCP		35520 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
32	0.000373	24.6.173.220	199.181.132.249	HTTP	disney.com	GET / HTTP/1.1
34	0.029553	199.181.132.249	24.6.173.220	TCP		80 → 35520 [PSH, ACK] Seq=1 Ack=285 Win=4664 Len=1448 [TCP segment of a reassembled
35	0.001266	199.181.132.249	24.6.173.220	TCP		80 → 35520 [ACK] Seq=1449 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled
36	0.000003	199.181.132.249	24.6.173.220	TCP		80 → 35520 [ACK] Seq=2909 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled

The packet details pane shows the selected packet (No. 15) as a GET request to 'http://www.disney.com'. The packet bytes pane shows the raw data of the packet, including the GET request line and the application/javascript content type.

Como podemos observar hay 5917 paquetes proyectados.

Paquetes: 6143 · Mostrado: 5917 (96.3%)