

# INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 16

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

# Lab16- Filter on HTTP Traffic the Right Way

## Paso 1:

Wireshark · Open Capture File

Buscar en: wireshark 101v2files

Nombre	Fecha de modificación	Tipo	Tamaño
ftp-passwords101.pcapng	14/07/2016 22:17	Wireshark capture...	1.200 KB
general101.pcapng	25/10/2012 23:55	Wireshark capture...	92 KB
general101b.pcapng	02/11/2012 15:13	Wireshark capture...	182 KB
general101c.pcapng	06/11/2012 13:38	Wireshark capture...	449 KB
general101d.pcapng	06/11/2012 15:47	Wireshark capture...	34.807 KB
gen-startupchatty101.pcapng	02/11/2012 14:28	Wireshark capture...	3.240 KB
http-au101b.pcapng	23/10/2012 17:09	Wireshark capture...	747 KB
http-browse101.pcapng	20/10/2012 17:50	Wireshark capture...	1.719 KB
http-browse101b.pcapng	08/11/2012 14:55	Wireshark capture...	119 KB
http-browse101c.pcapng	04/11/2012 20:31	Wireshark capture...	838 KB
http-browse101d.pcapng	04/11/2012 20:31	Wireshark capture...	838 KB
http-chappellu101.pcapng	24/10/2012 16:10	Wireshark capture...	948 KB
http-chappellu101b.pcapng	24/01/2013 18:41	Wireshark capture...	615 KB
http-cheez101.pcapng	03/01/2013 17:51	Wireshark capture...	4.004 KB
http-college101.pcapng	07/11/2012 12:44	Wireshark capture...	1.717 KB
http-disney101.pcapng	24/10/2012 16:03	Wireshark capture...	6.216 KB
httpdnsprofile.zip	30/10/2012 19:37	Archivo WinRAR Z...	34 KB
http-download101.pcapng	24/10/2012 15:06	Wireshark capture...	5.676 KB
http-download101c.pcapng	02/11/2012 12:40	Wireshark capture...	27.344 KB
http-download101d.pcapng	02/11/2012 17:23	Wireshark capture...	22.147 KB
http-download-a.pcapng	08/05/2012 17:14	Wireshark capture...	168.118 KB

Nombre de archivo: http-disney101.pcapng

Tipo de archivo: All Files

Read filter:  Format: Wireshark/... - pcapng

Automatically detect file type

Size: 6215 KiB, 6143 data records

Start / elapsed: 2012-10-24 17:01:21 / 00:00:23

Buttons: Abrir, Cancelar, Ayuda

Packet list (Hypertext Transfer Protocol: Protocol):

No.	Time	Source	Destination	Protocol	Length	Info
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,			
00f0	2a 2f 2a 3b 71 3d 30 2e	38 0d 0a 41 63 63 65 70	*/*;q=0. 8..Accep			
0100	74 2d 4c 61 6e 67 75 61	67 65 3a 20 65 6e 2d 55	t-Langua ge: en-U			
0110	53 2c 65 6e 3b 71 3d 30	2e 35 0d 0a 41 63 63 65	S,en;q=0 .5..Acce			
0120	70 74 2d 45 6e 63 6f 64	69 6e 67 3a 20 67 7a 69	pt-Encod ing: gzi			
0130	70 2c 20 64 65 66 6c 61	74 65 0d 0a 43 6f 6e 6e	p, defla te..Conn			
0140	65 63 74 69 6f 6e 3a 20	6b 65 65 70 2d 61 6c 69	ection: keep-ali			
0150	76 65 0d 0a 0d 0a		ve....			

Summary: Packets: 6143 · Displayed: 4093 (66.6%) Profile: Default

## Paso 2:

The image shows a Wireshark packet capture window titled "http-disney101.pcapng". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a packet list pane. The packet list shows several HTTP packets, with packet 15 selected. The packet details pane displays the structure of the selected packet, showing it is an HTTP GET request to "http://www.disney.com". The packet bytes pane shows the raw data of the packet, with the first few bytes highlighted in blue. The status bar at the bottom indicates "HTTP Request Method (http.request.method), 3 byte(s)", "Packets: 6143 · Displayed: 4093 (66.6%)", and "Profile: Default".

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
15	0.000000	24.6.173.220	199.181.132.249	HTTP	342	GET / HTTP/1.1
16	0.032641	199.181.132.249	24.6.173.220	HTTP	514	HTTP/1.1 301 Moved Permanently (text/html)
32	2.408025	24.6.173.220	199.181.132.249	HTTP	338	GET / HTTP/1.1
34	0.034794	199.181.132.249	24.6.173.220	HTTP	1502	HTTP/1.1 200 OK (text/html)
35	0.001266	199.181.132.249	24.6.173.220	HTTP	1514	Continuation
36	0.000003	199.181.132.249	24.6.173.220	HTTP	1514	Continuation
47	0.034084	199.181.132.249	24.6.173.220	HTTP	1514	Continuation
48	0.001265	199.181.132.249	24.6.173.220	HTTP	1514	Continuation
49	0.000004	199.181.132.249	24.6.173.220	HTTP	1514	Continuation
50	0.000002	199.181.132.249	24.6.173.220	HTTP	1514	Continuation
70	0.028883	24.6.173.220	208.111.148.6	HTTP	401	GET /cdn_assets/314da08c2cc0c65e47e89c1c092812dbff
77	0.000854	24.6.173.220	208.111.148.6	HTTP	401	GET /cdn_assets/9d31acc4393a7912869c8d837e51aba20
78	0.000249	24.6.173.220	208.111.148.6	HTTP	401	GET /cdn_assets/69d7937a4e5ed43103011adb5a79afb6e7

Packet Details:

- Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{6E79FEC0-FF79-4970-96E4-EEFF300A9} 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\r\n
    - [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    - Request Method: GET
    - Request URI: /
    - Request Version: 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

Packet Bytes:

```
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 18 .....P...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 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,
00f0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 /*;q=0. 8..Accep
0100 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 t-Langua ge: en-U
0110 53 2c 65 6e 6b 71 3d 30 2e 35 0d 0a 41 63 63 65 S,en;q=0 .5..Acce
0120 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
0130 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e p, defla te..Conn
0140 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
0150 76 65 0d 0a 0d 0a ve....
```

### Paso 3:

The image shows a Wireshark packet capture of an HTTP GET request. The top pane displays a list of packets, with packet 15 selected. The middle pane shows the details of packet 15, highlighting the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
12	0.000000	24.6.173.220	199.181.132.249	TCP	66	35518 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
13	0.034726	199.181.132.249	24.6.173.220	TCP	66	80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 M
14	0.000075	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	0.000370	24.6.173.220	199.181.132.249	HTTP	342	GET / HTTP/1.1
16	0.032641	199.181.132.249	24.6.173.220	HTTP	514	HTTP/1.1 301 Moved Permanently (text/html)
21	0.108487	24.6.173.220	199.181.132.249	TCP	66	35519 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
22	0.091631	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
29	2.176632	24.6.173.220	199.181.132.249	TCP	66	35520 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
30	0.030767	199.181.132.249	24.6.173.220	TCP	66	80 → 35520 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 M
31	0.000135	24.6.173.220	199.181.132.249	TCP	54	35520 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
32	0.000373	24.6.173.220	199.181.132.249	HTTP	338	GET / HTTP/1.1
34	0.034794	199.181.132.249	24.6.173.220	HTTP	1502	HTTP/1.1 200 OK (text/html)
35	0.001266	199.181.132.249	24.6.173.220	HTTP	1514	Continuation

**Packet 15 Details:**

- Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{6E79FEC0-FF79-4970-96E4-EEFF300A9}
- 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\r\n
    - [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    - Request Method: GET
    - Request URI: /
    - Request Version: 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

**Raw Packet Data (Hex/ASCII):**

```
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 18  ....Ps..}Y..f.P.
0030 40 29 13 cc 00 00 47 45 54 20 2f 20 48 54 54 50  (@)....GET / HTTP
0040 2f 1.1..Ho st: www.  /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,
00f0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70  /*;q=0. 8..Accep
0100 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55  t-Langua ge: en-U
0110 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65  S,en;q=0 .5..Acce
0120 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69  pt-Encod ing: gzi
0130 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e  p, defla te..Conn
0140 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69  ection: keep-ali
0150 76 65 0d 0a 0d 0a  ve....
```

**Status Bar:** HTTP Request Method (http.request.method), 3 byte(s) | Packets: 6143 · Displayed: 5917 (96.3%) | Profile: Default