TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

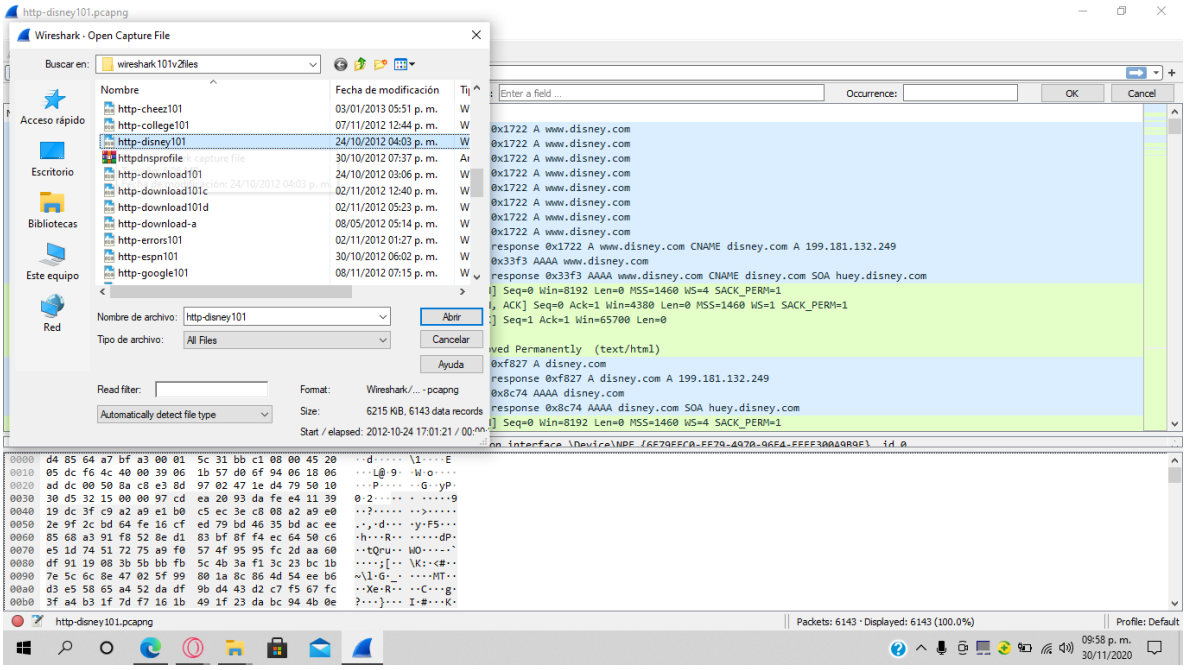
DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

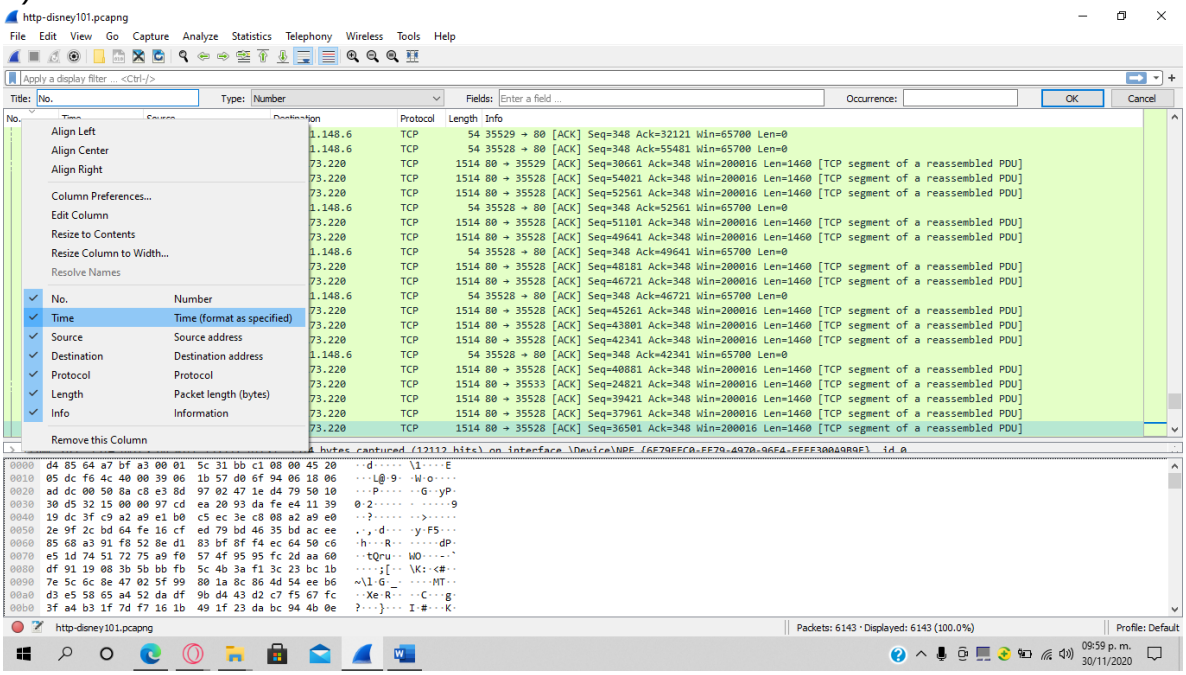
“LABORATORIO 2.1”

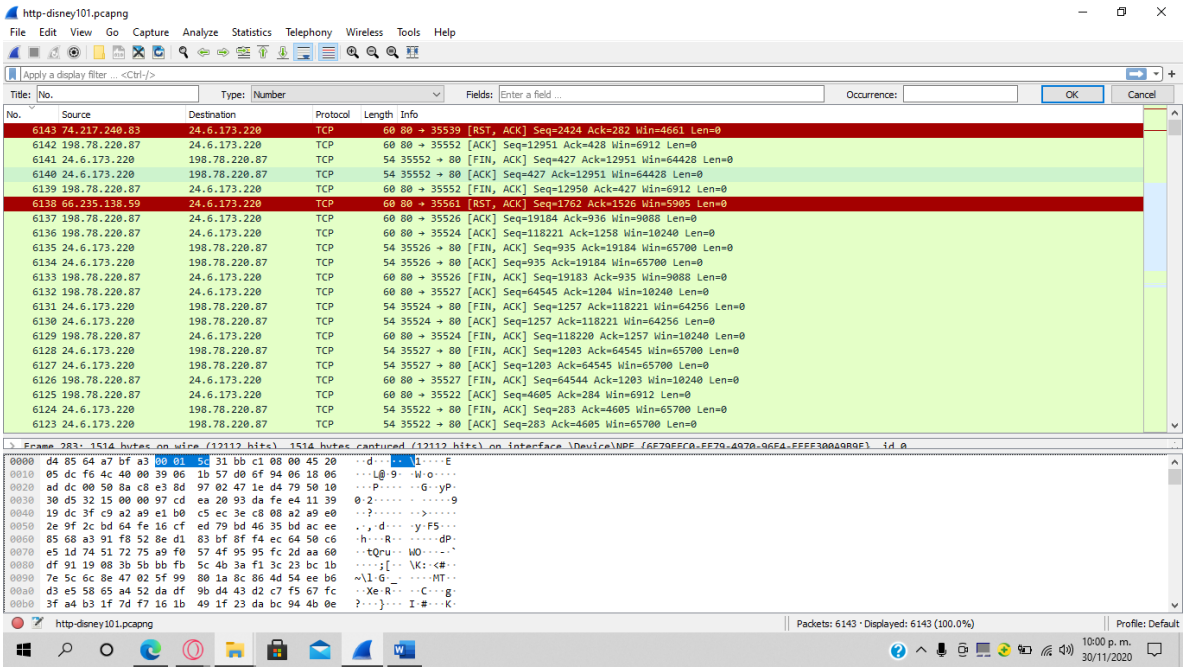
UNIDAD 3

1)

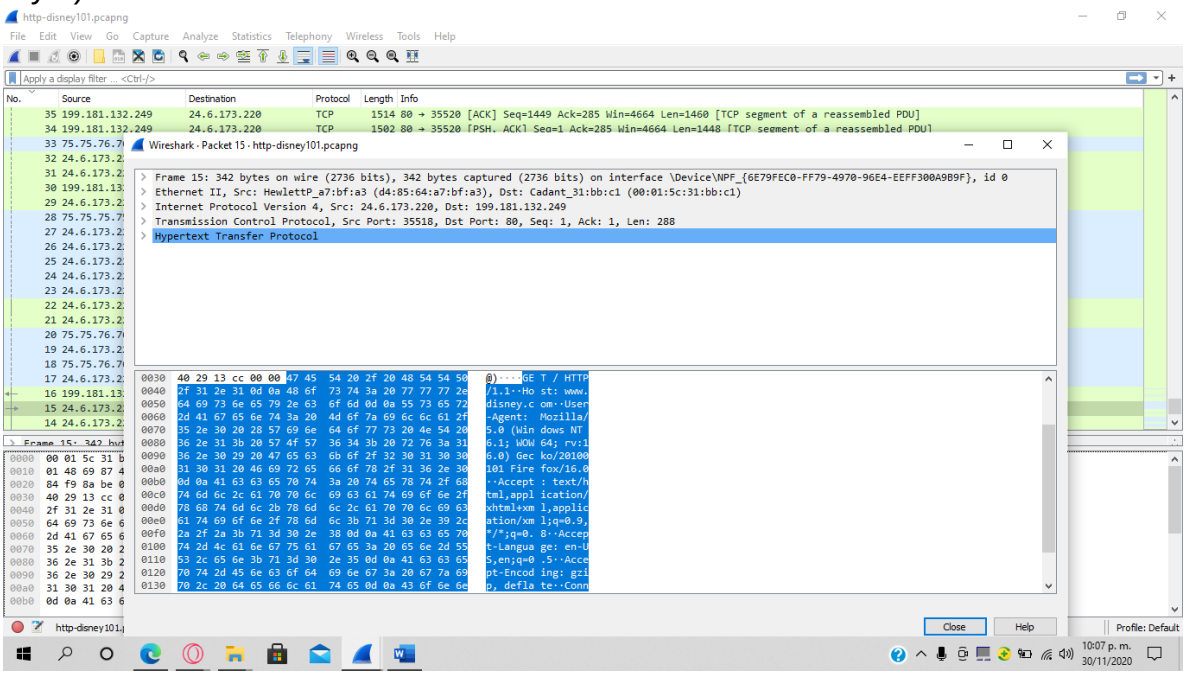

http-disney101.pcapng
Wireshark · Open Capture File
Buscar en:
wireshark101v2files
Nombre
Fecha de modificación
http-cheez101
http-college101
http-disney101
httpdnsprofile
http-download101
http-download101c
http-download101d
http-download-a
http-errors101
http-espn101
http-google101
Acceso rápido
Escritorio
Bibliotecas
Este equipo
Red
Nombre de archivo:
http-disney101
Tipo de archivo:
All Files
Abrir
Cancelar
Ayuda
Read filter:
Format:
Size:
6215 KiB, 6143 data records
Automatically detect file type
Enter a field ...
Occurrence:
OK
Cancel
http-disney101.pcapng
Packets: 6143 · Displayed: 6143 (100.0%)
Profile: Default
09:58 p. m.
30/11/2020

2)

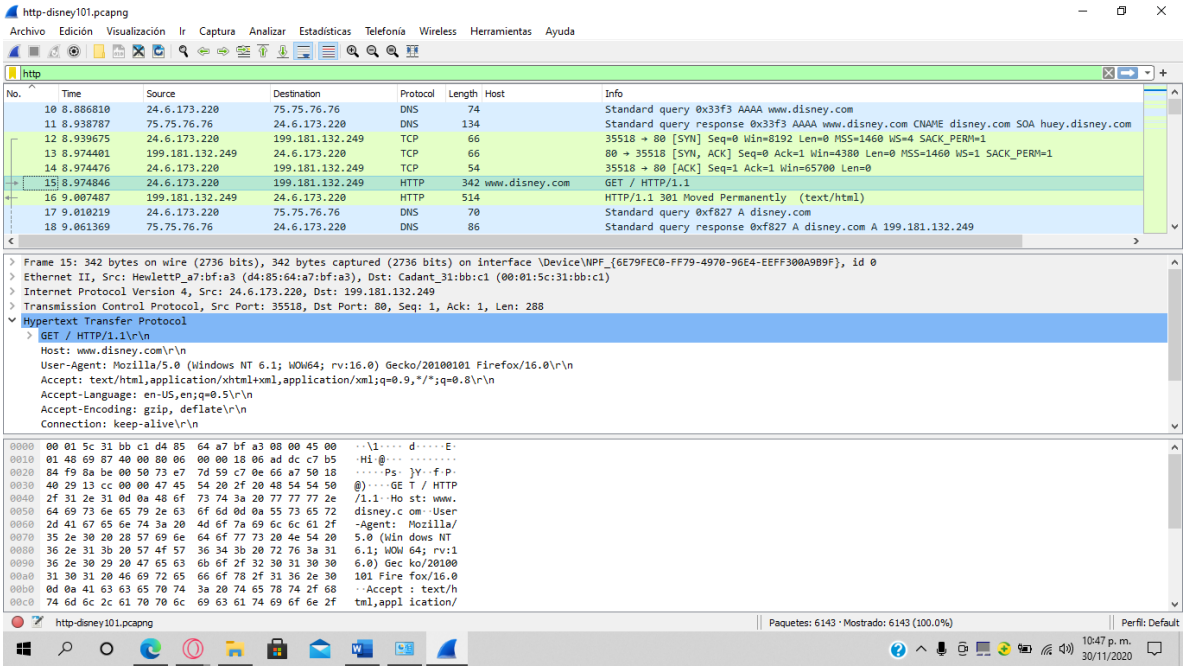

http-disney101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Title: No.
Type: Number
Fields: Enter a field ...
Occurrence:
OK
Cancel
Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize to Contents
Resize Column to Width...
Resolve Names
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
Remove this Column
Packets: 6143 · Displayed: 6143 (100.0%)
Profile: Default
09:59 p. m.
30/11/2020


http-disney101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Title: No.
Type: Number
Fields: Enter a field ...
Occurrence:
OK
Cancel
No. Source Destination Protocol Length Info
6143 74.217.240.83 24.6.173.220 TCP 60 80 → 35539 [RST, ACK] Seq=2424 Ack=282 Win=4661 Len=0
6142 198.78.220.87 24.6.173.220 TCP 60 80 → 35552 [ACK] Seq=12951 Ack=428 Win=6912 Len=0
6141 24.6.173.220 198.78.220.87 TCP 54 35552 → 80 [FIN, ACK] Seq=427 Ack=12951 Win=64428 Len=0
6140 24.6.173.220 198.78.220.87 TCP 54 35552 → 80 [ACK] Seq=427 Ack=12951 Win=64428 Len=0
6139 198.78.220.87 24.6.173.220 TCP 60 80 → 35552 [FIN, ACK] Seq=12950 Ack=427 Win=6912 Len=0
6138 66.235.138.59 24.6.173.220 TCP 60 80 → 35561 [RST, ACK] Seq=1762 Ack=1526 Win=5905 Len=0
6137 198.78.220.87 24.6.173.220 TCP 60 80 → 35526 [ACK] Seq=19184 Ack=936 Win=9088 Len=0
6136 198.78.220.87 24.6.173.220 TCP 60 80 → 35524 [ACK] Seq=118221 Ack=1258 Win=10240 Len=0
6135 24.6.173.220 198.78.220.87 TCP 54 35526 → 80 [FIN, ACK] Seq=935 Ack=19184 Win=65700 Len=0
6134 24.6.173.220 198.78.220.87 TCP 54 35526 → 80 [ACK] Seq=935 Ack=19184 Win=65700 Len=0
6133 198.78.220.87 24.6.173.220 TCP 60 80 → 35526 [FIN, ACK] Seq=19183 Ack=935 Win=9088 Len=0
6132 198.78.220.87 24.6.173.220 TCP 60 80 → 35527 [ACK] Seq=64545 Ack=1204 Win=10240 Len=0
6131 24.6.173.220 198.78.220.87 TCP 54 35524 → 80 [FIN, ACK] Seq=1257 Ack=118221 Win=64256 Len=0
6130 24.6.173.220 198.78.220.87 TCP 54 35524 → 80 [ACK] Seq=1257 Ack=118221 Win=64256 Len=0
6129 198.78.220.87 24.6.173.220 TCP 60 80 → 35524 [FIN, ACK] Seq=118220 Ack=1257 Win=10240 Len=0
6128 24.6.173.220 198.78.220.87 TCP 54 35527 → 80 [FIN, ACK] Seq=1203 Ack=64545 Win=65700 Len=0
6127 24.6.173.220 198.78.220.87 TCP 54 35527 → 80 [ACK] Seq=1203 Ack=64545 Win=65700 Len=0
6126 198.78.220.87 24.6.173.220 TCP 60 80 → 35527 [FIN, ACK] Seq=64544 Ack=1203 Win=10240 Len=0
6125 198.78.220.87 24.6.173.220 TCP 60 80 → 35522 [ACK] Seq=4605 Ack=284 Win=6912 Len=0
6124 24.6.173.220 198.78.220.87 TCP 54 35522 → 80 [FIN, ACK] Seq=283 Ack=4605 Win=65700 Len=0
6123 24.6.173.220 198.78.220.87 TCP 54 35522 → 80 [ACK] Seq=283 Ack=4605 Win=65700 Len=0
Packets: 6143 · Displayed: 6143 (100.0%)
Profile: Default
10:00 p. m.
30/11/2020

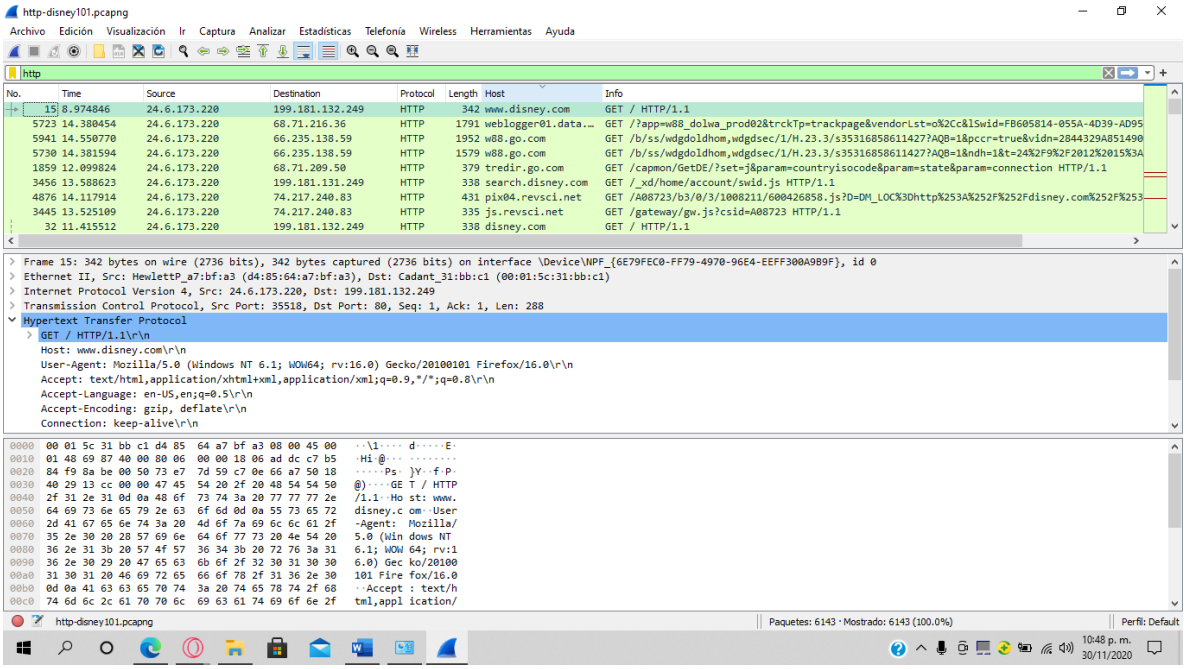
3 y 4)


http-disney101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Source Destination Protocol Length Info
35 199.181.132.249 24.6.173.220 TCP 1514 80 → 35520 [ACK] Seq=1449 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled PDU]
34 199.181.132.249 24.6.173.220 TCP 1502 80 → 35520 [PSH, ACK] Seq=1 Ack=285 Win=4664 Len=1448 [TCP segment of a reassembled PDU]
Wireshark · Packet 15 · http-disney101.pcapng
Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 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: 199.181.132.249
Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
Hypertext Transfer Protocol
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 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
Close Help
Profile: Default
10:07 p. m.
30/11/2020

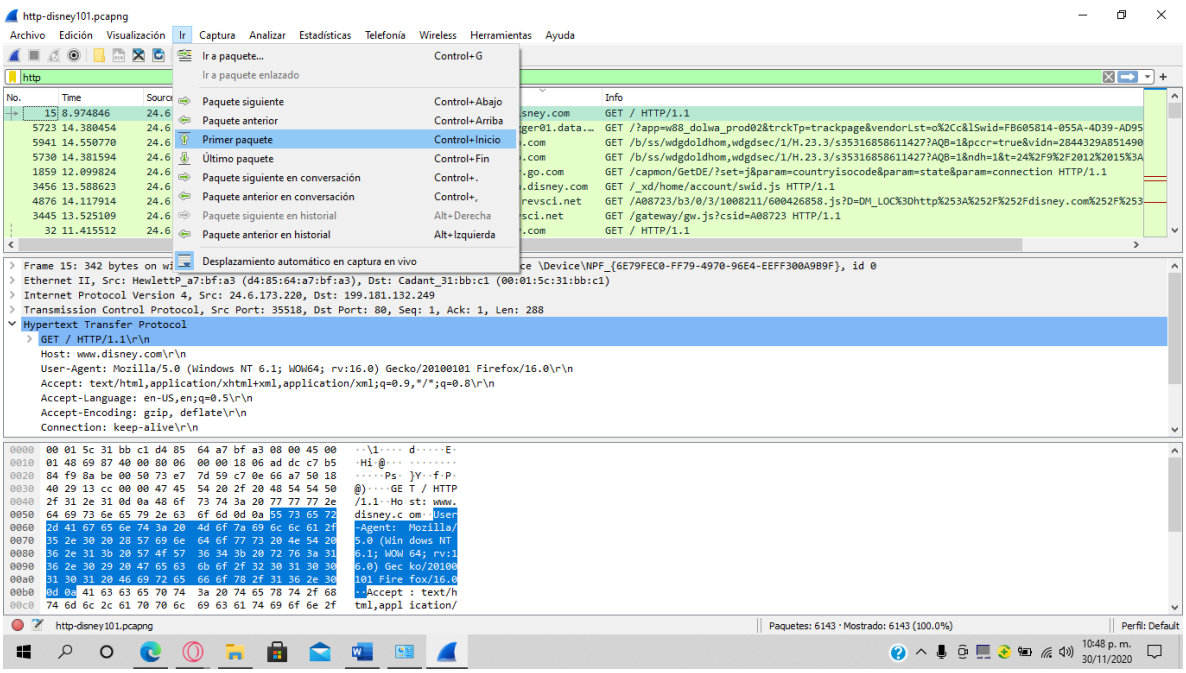
5)


http-disney101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
http
No. Time Source Destination Protocol Length Host Info
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 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
Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 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: 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
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
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 @)····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/
http-disney101.pcapng
Paquetes: 6143 · Mostrado: 6143 (100.0%)
Perfil: Default
10:47 p. m.
30/11/2020

6)


http-disney101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
http
No. Time Source Destination Protocol Length Host Info
15 8.974846 24.6.173.220 199.181.132.249 HTTP 342 www.disney.com GET / HTTP/1.1
5723 14.380454 24.6.173.220 68.71.216.36 HTTP 1791 weblogger01.data... GET /?app=w88_dolwa_prod02&trckTp=trackpage&vendorLst=o%2Cc&lSwid=FB605814-055A-4D39-AD95
5941 14.550770 24.6.173.220 66.235.138.59 HTTP 1952 w88.go.com GET /b/ss/wdgdoldhom,wdgdsec/1/H.23.3/s35316858611427?AQB=1&pccr=true&vidn=2844329A851490
5730 14.381594 24.6.173.220 66.235.138.59 HTTP 1579 w88.go.com GET /b/ss/wdgdoldhom,wdgdsec/1/H.23.3/s35316858611427?AQB=1&ndh=1&t=24%2F9%2F2012%2015%3A
1859 12.099824 24.6.173.220 68.71.209.50 HTTP 379 tredir.go.com GET /capmon/GetDE/?set=j&param=countryisocode&param=state&param=connection HTTP/1.1
3456 13.588623 24.6.173.220 199.181.131.249 HTTP 338 search.disney.com GET /_xd/home/account/swid.js HTTP/1.1
4876 14.117914 24.6.173.220 74.217.240.83 HTTP 431 pix04.revsci.net GET /A08723/b3/0/3/1008211/600426858.js?D=DM_LOC%3Dhttp%253A%252F%252Fdisney.com%252F%253
3445 13.525109 24.6.173.220 74.217.240.83 HTTP 335 js.revsci.net GET /gateway/gw.js?csid=A08723 HTTP/1.1
32 11.415512 24.6.173.220 199.181.132.249 HTTP 338 disney.com GET / HTTP/1.1
Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 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: 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
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
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 01 48 69 87 40 00 80 06 00 00 18 06 ad dc c7 b5
0020 84 f9 8a be 00 50 73 e7 7d 59 c7 0e 66 a7 50 18
0030 40 29 13 cc 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e
0050 64 69 73 6e 65 79 2e 63 6f 6d 0d 0a 55 73 65 72
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20
0080 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31
0090 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30
00a0 31 30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30
00b0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68
00c0 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f
http-disney101.pcapng
Paquetes: 6143 · Mostrado: 6143 (100.0%)
Perfil: Default
10:48 p. m.
30/11/2020

7)


http-disney101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Ir a paquete... Control+G
Ir a paquete enlazado
Paquete siguiente Control+Abajo
Paquete anterior Control+Arriba
Primer paquete Control+Inicio
Último paquete Control+Fin
Paquete siguiente en conversación Control+.
Paquete anterior en conversación Control+,
Paquete siguiente en historial Alt+Derecha
Paquete anterior en historial Alt+Izquierda
Desplazamiento automático en captura en vivo
http
No. Time Info
15 8.974846 GET / HTTP/1.1
5723 14.380454 GET /?app=w88_dolwa_prod02&trckTp=trackpage&vendorLst=o%2Cc&lSwid=FB605814-055A-4D39-AD95
5941 14.550770 GET /b/ss/wdgdoldhom,wdgdsec/1/H.23.3/s35316858611427?AQB=1&pccr=true&vidn=2844329A851490
5730 14.381594 GET /b/ss/wdgdoldhom,wdgdsec/1/H.23.3/s35316858611427?AQB=1&ndh=1&t=24%2F9%2F2012%2015%3A
1859 12.099824 GET /capmon/GetDE/?set=j&param=countryisocode&param=state&param=connection HTTP/1.1
3456 13.588623 GET /_xd/home/account/swid.js HTTP/1.1
4876 14.117914 GET /A08723/b3/0/3/1008211/600426858.js?D=DM_LOC%3Dhttp%253A%252F%252Fdisney.com%252F%253
3445 13.525109 GET /gateway/gw.js?csid=A08723 HTTP/1.1
32 11.415512 GET / HTTP/1.1
Frame 15: 342 bytes on wi ce \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: 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
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
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 01 48 69 87 40 00 80 06 00 00 18 06 ad dc c7 b5
0020 84 f9 8a be 00 50 73 e7 7d 59 c7 0e 66 a7 50 18
0030 40 29 13 cc 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e
0050 64 69 73 6e 65 79 2e 63 6f 6d 0d 0a 55 73 65 72
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20
0080 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31
0090 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30
00a0 31 30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30
00b0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68
00c0 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f
http-disney101.pcapng
Paquetes: 6143 · Mostrado: 6143 (100.0%)
Perfil: Default
10:48 p. m.
30/11/2020