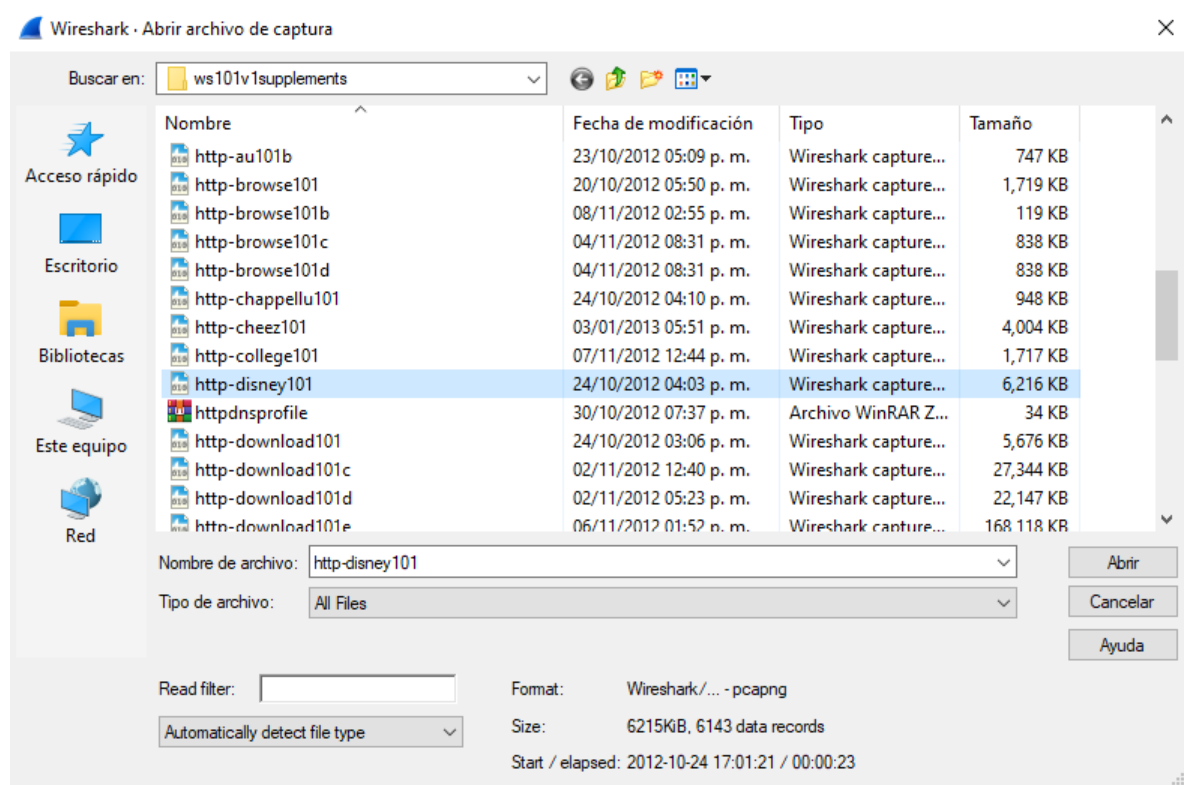
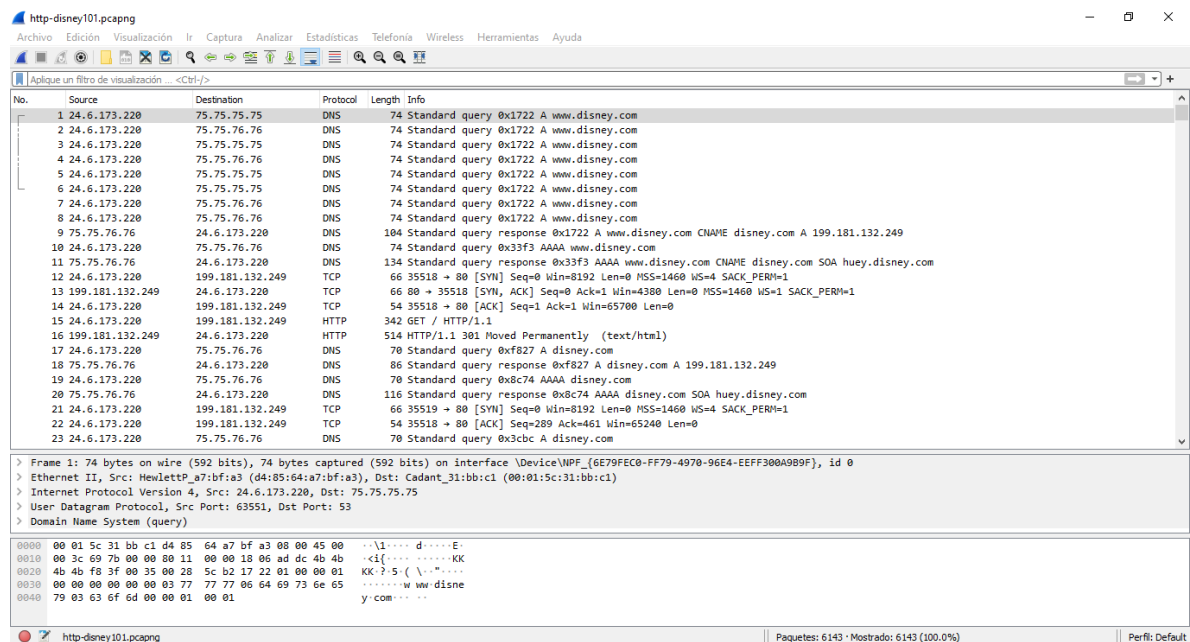


Lab 4

Step 1: Abriremos este archivo



Step 2



Step 3, 4

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	Info
13	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	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	24.6.173.220	199.181.132.249	HTTP	342	GET / HTTP/1.1
16	199.181.132.249	24.6.173.220	HTTP	514	HTTP/1.1 301 Moved Permanently (text/html)
17	24.6.173.220	75.75.76.76	DNS	70	Standard query response 0xf827 A disney.com
18	75.75.76.76	24.6.173.220	DNS	86	Standard query 0xf827 A disney.com A 199.181.132.249
19	24.6.173.220	75.75.76.76	DNS	70	Standard query 0x8c74 AAAA disney.com
20	75.75.76.76	24.6.173.220	DNS	116	Standard query response 0x8c74 AAAA disney.com SOA huey.disney.com
21	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	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0

> 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: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: 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

\r\n

[Full request URI: http://www.disney.com/]

[HTTP request 1/2]

[Response in frame: 16]

Step 5

Aplique un filtro de visualización: <Ctrl>->

No.	Source	Destination	Protocol	Length	Full request URI	Info
13	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	24.6.173.220	199.181.132.249	TCP	54		35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	24.6.173.220	199.181.132.249	HTTP	342	http://www.disney.com/	GET / HTTP/1.1
16	199.181.132.249	24.6.173.220	HTTP	514		HTTP/1.1 301 Moved Permanently (text/html)
17	24.6.173.220	75.75.76.76	DNS	70		Standard query response 0xf827 A disney.com
18	75.75.76.76	24.6.173.220	DNS	86		Standard query 0xf827 A disney.com A 199.181.132.249
19	24.6.173.220	75.75.76.76	DNS	70		Standard query 0x8c74 AAAA disney.com
20	75.75.76.76	24.6.173.220	DNS	116		Standard query response 0x8c74 AAAA disney.com SOA huey.disney.com
21	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	24.6.173.220	199.181.132.249	TCP	54		35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0

> 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: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: 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

\r\n

[Full request URI: http://www.disney.com/]

[HTTP request 1/2]

[Response in frame: 16]

Step 6, 7

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	Full request URI	Info
15	24.6.173.220	199.181.132.249	HTTP	342	http://www.disney.com/	GET / HTTP/1.1
5723	24.6.173.220	68.71.216.36	HTTP	1791	http://weblogger01.data.disney.com/?app=88_dolwa_prod02&trackTp=trackpage&vendorList=0%2Cc&1swid=FB605814-055A-4D39-AD95-CE	
5941	24.6.173.220	66.235.138.59	HTTP	1952	http://w88.go.com/b/ss/wdgdoldh... GET /b/ss/wdgdoldh...wdgsec/1/H.23.3/s35316858611427?AQ0=1&pccr=true&vid=2844329A851490A5-	
5730	24.6.173.220	66.235.138.59	HTTP	1579	http://w88.go.com/b/ss/wdgdoldh... GET /b/ss/wdgdoldh...wdgsec/1/H.23.3/s35316858611427?AQ0=1&ndh=1&t=24%2F9%2F2012%2015%3A1%3	
1859	24.6.173.220	68.71.209.50	HTTP	379	http://tredir.go.com/capmon/Get... GET /capmon/GetDE/?set=j¶m=countryIsoCode¶m=state¶m=connection HTTP/1.1	
3456	24.6.173.220	199.181.131.249	HTTP	338	http://search.disney.com/_xd/ho... GET /_xd/home/account/swid.js HTTP/1.1	
4876	24.6.173.220	74.217.240.83	HTTP	431	http://pix04.revsci.net/A08723/_... GET /A08723/b3/0/3/1008211/600426858.js?D=DM_L0C30http%253A%252F%252Fdisney.com%252F%253F_r	
3445	24.6.173.220	74.217.240.83	HTTP	335	http://js.revsci.net/gateway/gw... GET /gateway/gw.js?csid=A08723 HTTP/1.1	
32	24.6.173.220	199.181.132.249	HTTP	338	http://disney.com/	GET / HTTP/1.1
5728	24.6.173.220	198.105.199.137	HTTP	1735	http://ctologger01.analytics.go... GET /cto/?app=88_dolwa_prod03&trackTp=trackpage&vendorList=0%2Cc&1swid=FB605814-055A-4D39-AD9	
4160	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/fa5395db7ad080971f64d102a0c3630150bd162c.jpg HTTP/1.1	
4330	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/f9c270df91c61c1f2c183e3f4a329800eba3c0e.jpg HTTP/1.1	
570	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/f7c19c9cd079114a942b0334392e310d444be405.jpg HTTP/1.1	
4536	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/f758140f937e616d3d19b00cf85fd3ed1f4dc58.jpg HTTP/1.1	
4812	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/f646b7e9c6c1602241ed6ddbf224b1cfc25.jpg HTTP/1.1	
2839	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/eee2e3125f55defc647c1ebd7556e8f3f4678e4c.jpg HTTP/1.1	
1157	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/ec4f5867ea6925e4416d42d406bb4f68aa25035c.jpg HTTP/1.1	
1544	24.6.173.220	208.111.148.6	HTTP	401	http://cdnvideo.dolimg.com/cdn_... GET /cdn_assets/e57c5423a2dbf9f2326f9f9d4c1bf3214e1c6400.jpg HTTP/1.1	

Step 8

http-disney101.pcapng

Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización: <Ctrl-F>

No.	Source	Destination	Protocol	Length	Info
1	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
2	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
3	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
4	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
5	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
6	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x1722 A www.disney.com
7	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
8	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x1722 A www.disney.com
9	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	24.6.173.220	75.75.76.76	DNS	74	Standard query 0x33f3 AAAA www.disney.com
11	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	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	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	24.6.173.220	199.181.132.249	TCP	54	35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	24.6.173.220	199.181.132.249	HTTP	342	GET / HTTP/1.1
16	199.181.132.249	24.6.173.220	HTTP	514	HTTP/1.1 301 Moved Permanently (text/html)