

LABORATORIOS WIRESHARK

Morales Aguilar Miguel Ángel

Docente: Jiménez Sánchez Ismael

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

LABORATORIO 2

*Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

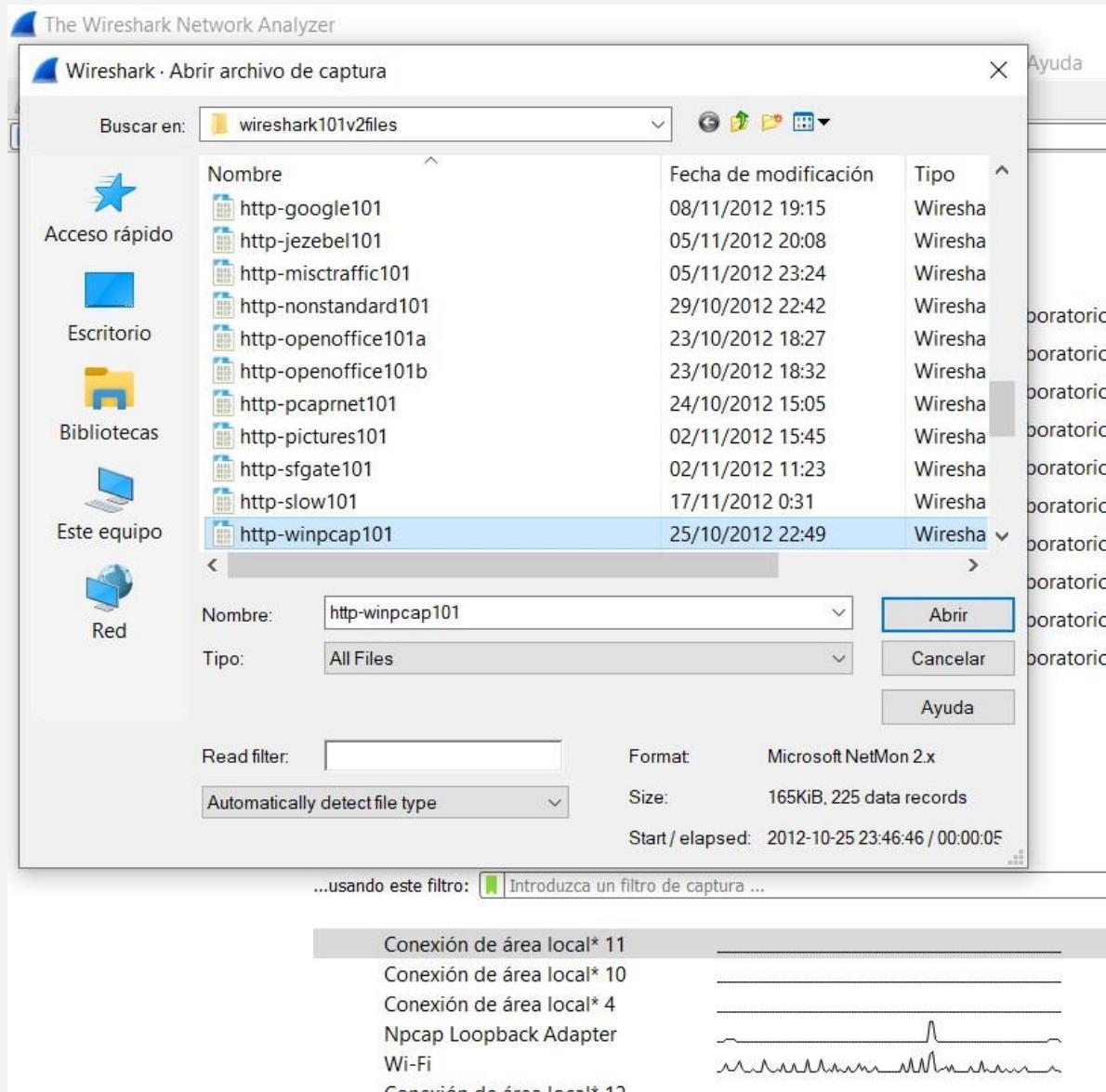
Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.8	31.13.89.53	TLSv1.2 Application Data	
2	0.063449	31.13.89.53	192.168.0.8	TCP	443 → 50023 [ACK] Seq=1 Ack=121 Win=493 Len=0
3	0.064996	31.13.89.53	192.168.0.8	TLSv1.2 Application Data	
4	0.043371	192.168.0.8	31.13.89.53	TCP	50023 → 443 [ACK] Seq=121 Ack=35 Win=260 Len=0
5	0.460290	31.13.89.53	192.168.0.8	TLSv1.2 Application Data	
6	0.050859	192.168.0.8	31.13.89.53	TCP	50023 → 443 [ACK] Seq=121 Ack=83 Win=260 Len=0
7	0.563670	192.168.0.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
8	0.204910	192.168.0.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
9	0.411444	192.168.0.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
10	1.701031	192.168.0.8	152.195.55.22	TCP	49975 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
11	0.054022	152.195.55.22	192.168.0.8	TCP	443 → 49975 [ACK] Seq=1 Ack=2 Win=135 Len=0 SLE=1 SRE=2
12	0.149795	192.168.0.8	10.223.234.2	DNS	Standard query 0x309f A grant.rewards.brave.com
13	0.000591	192.168.0.8	10.223.234.2	DNS	Standard query 0xfa0d A api.uphold.com
14	0.014629	10.223.234.2	192.168.0.8	DNS	Standard query response 0xfa0d A api.uphold.com A 104.16.79.80 A 104.16.80.80
15	0.000882	192.168.0.8	104.16.79.80	TCP	50043 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	0.046188	10.223.234.2	192.168.0.8	DNS	Standard query response 0x309f A grant.rewards.brave.com CNAME dualstack.j3.shared.global.fastly.net A 151.101.50.217
17	0.001051	192.168.0.8	151.101.50.217	TCP	50044 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	0.009080	104.16.79.80	192.168.0.8	TCP	443 → 50043 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
19	0.000244	192.168.0.8	104.16.79.80	TCP	50043 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
20	0.000633	192.168.0.8	104.16.79.80	TLSv1.3 Client Hello	
21	0.055543	104.16.79.80	192.168.0.8	TCP	443 → 50043 [ACK] Seq=1 Ack=547 Win=67584 Len=0
22	0.000606	104.16.79.80	192.168.0.8	TLSv1.3 Server Hello, Change Cipher Spec, Application Data	
23	0.000610	151.101.50.217	192.168.0.8	TCP	443 → 50044 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM=1 WS=512
24	0.000074	192.168.0.8	151.101.50.217	TCP	50044 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
25	0.000461	192.168.0.8	151.101.50.217	TLSv1.2 Client Hello	
26	0.009794	192.168.0.8	104.16.79.80	TLSv1.3 Change Cipher Spec, Application Data	
27	0.000316	192.168.0.8	104.16.79.80	TLSv1.3 Application Data	
28	0.000246	192.168.0.8	104.16.79.80	TLSv1.3 Application Data	

> Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{2A376F01-54A3-4463-A648-1F1978A118B4}, id 0
> Ethernet II, Src: IntelCor_86:dd:3c (50:eb:71:86:dd:3c), Dst: ARRISGro_f2:00:e6 (f8:8b:37:f2:00:e6)
> Internet Protocol Version 4, Src: 192.168.0.8, Dst: 31.13.89.53
> Transmission Control Protocol, Src Port: 50023, Dst Port: 443, Seq: 1, Ack: 1, Len: 120
> Transport Layer Security

0000	f8	8b	37	f2	00	e6	50	eb	71	86	dd	3c	08	00	45	00	..7..P.	q..<..E.
0010	00	a0	06	e7	40	00	80	06	00	00	c0	a8	00	08	1f	0d@...

LABORATORIO 3



LABORATORIO 4

http-disney101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

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
5723	0.000636	24.6.173.220	68.71.216.36	HTTP	weblogger01.data....	GET /?app=w88_dolwa_prod02&trckTp=trackpage&vendorLst=o%2Cc&lSwid=FB605814-055A-4D39-AD95-CEC0317E6054&pgVwId=1351116
5941	0.030253	24.6.173.220	66.235.138.59	HTTP	w88.go.com	GET /b/ss/wdgldoldhom,wgdgsec/1/H.23.3/s35316858611427?AQB=1&pccr=true&vidn=2844329A851490A5-600001A2C02AE96&&ndh=1&t
5730	0.000717	24.6.173.220	66.235.138.59	HTTP	w88.go.com	GET /b/ss/wdgldoldhom,wgdgsec/1/H.23.3/s35316858611427?AQB=1&ndh=1&t=24%2F9%2F2012%2015%3A1%3A35%203%20420&ns=dol&cdp=
1859	0.000394	24.6.173.220	68.71.209.50	HTTP	tredir.go.com	GET /capmon/GetDE/?set=j¶m=countryisocode¶m=state¶m=connection HTTP/1.1
3456	0.000216	24.6.173.220	199.181.131.249	HTTP	search.disney.com	GET /_xd/home/account/swid.js HTTP/1.1
4876	0.000346	24.6.173.220	74.217.240.83	HTTP	pix04.revsci.net	GET /A08723/b3/0/3/1008211/600426858.js?D=DM_LOC%3Dhttp%253A%252F%252Fdisney.com%252F%253F_rsiL%253D0%26DM_EOM%3D1&C=
3445	0.000399	24.6.173.220	74.217.240.83	HTTP	js.revsci.net	GET /gateway/gw.js?csid=A08723 HTTP/1.1
32	0.000373	24.6.173.220	199.181.132.249	HTTP	disney.com	GET / HTTP/1.1
5728	0.000233	24.6.173.220	198.105.199.137	HTTP	ctologger01.analy...	GET /cto/?app=w88_dolwa_prod03&trckTp=trackpage&vendorLst=o%2Cc&lSwid=FB605814-055A-4D39-AD95-CEC0317E6054&pgVwId=135
5583	0.000304	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/9da0f78de11590e89376c4da5943506f1cb1ce9a.jpg HTTP/1.1
5491	0.000492	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/85456a4db5f75eee152f2e90f8e054d1674b159a.jpg HTTP/1.1
5433	0.000001	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/147ac28b4a83a911c8597a0e2ef601691cdef8f6.jpg HTTP/1.1
5349	0.000467	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/85bf6fa6b4a5aafb414573f78f965a500330cb8f.jpg HTTP/1.1
5129	0.000524	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/08f0cdd111cede4a9a3a1376e08ea7f154b6f37d8.jpg HTTP/1.1
5014	0.000465	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/86cf2be448320070b71bed0c8680d878feb0e567.jpg HTTP/1.1
4952	0.000347	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/7d2549aec01fd225c7d9803b6a4128bae09dbc5.jpg HTTP/1.1
4875	0.000230	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/14226f6f9b22164825625a46ce8b48551d7421c3.jpg HTTP/1.1
4812	0.000358	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/f646b72e9c6c1602241ed6ddbfb224b1cffcb25.jpg HTTP/1.1
4793	0.000497	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/d33887e0a5d0e433ba4708afd2c399d406765733.jpg HTTP/1.1
4764	0.000396	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/9dc97a27a7dd906d07b5914c630fa29cb08a3af4.jpg HTTP/1.1

> 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]

 [GET / HTTP/1.1\r\n]

 [Severity level: Chat]

 [Group: Sequence]

 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

LABORATORIO 5

Wireshark

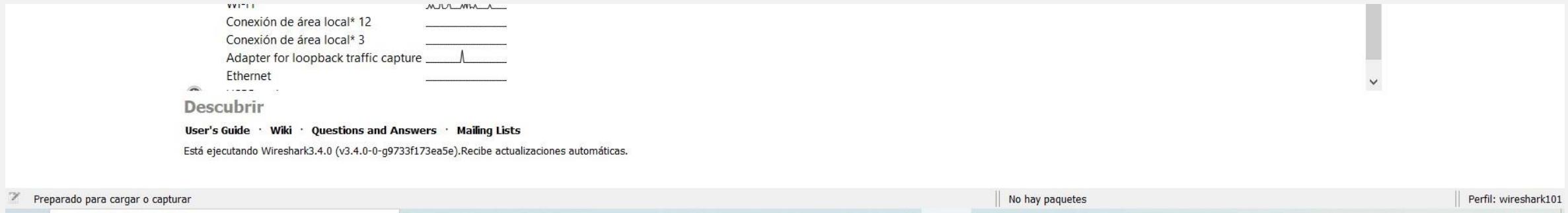
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Host	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS		Standard query 0xc3bf A www.pcapr.net
2	0.021485	75.75.75.75	24.6.173.220	DNS		Standard query response 0xc3bf A www.pcapr.net A 209.133.32.69
3	0.001630	24.6.173.220	75.75.75.75	DNS		Standard query 0x406e AAAA www.pcapr.net
4	0.025362	75.75.75.75	24.6.173.220	DNS		Standard query response 0x406e AAAA www.pcapr.net SOA pdns1.ultradns.net
5	0.002836	24.6.173.220	209.133.32.69	TCP		21213 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6	0.019083	209.133.32.69	24.6.173.220	TCP		80 → 21213 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=8
7	0.000198	24.6.173.220	209.133.32.69	TCP		21213 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	0.000778	24.6.173.220	209.133.32.69	HTTP	www.pcapr.net	GET / HTTP/1.1
9	0.017096	209.133.32.69	24.6.173.220	TCP		80 → 21213 [ACK] Seq=1 Ack=288 Win=6912 Len=0

[TCP Segment Len: 287]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1288438180
[Next Sequence Number: 288 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 82469421
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 16425
[Calculated window size: 65700]
[Window size scaling factor: 4]
Checksum: 0xb8e6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.019281000 seconds]
[Bytes in flight: 287]
[Bytes sent since last PSH flag: 287]
[Timestamps]
[Time since first frame in this TCP stream: 0.020059000 seconds]
[Time since previous frame in this TCP stream: 0.000778000 seconds]

LABORATORIO 6



LABORATORIO 8^a.

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Host	Info
354	118.195308	24.6.173.220	69.4.231.53	TCP		12609 → 80 [FIN, ACK] Seq=1971 Ack=151255 Win=65700 Len=0
210	29.006113	69.4.231.53	24.6.173.220	TCP		80 → 12609 [PSH, ACK] Seq=545 Ack=1300 Win=8704 Len=334 [TCP segment of a reassembled PDU]
16	18.096205	24.6.173.220	69.4.231.53	TCP		12607 → 80 [FIN, ACK] Seq=641 Ack=1 Win=65700 Len=0
23	17.965049	69.4.231.53	24.6.173.220	TCP		80 → 12608 [PSH, ACK] Seq=1 Ack=641 Win=7168 Len=335 [TCP segment of a reassembled PDU]
1098	14.745399	69.4.231.53	24.6.173.220	TCP		80 → 12621 [FIN, ACK] Seq=846303 Ack=672 Win=7680 Len=0
1100	14.381621	24.6.173.220	69.4.231.53	TCP		12621 → 80 [FIN, ACK] Seq=672 Ack=846304 Win=261340 Len=0
200	13.189802	24.6.173.220	69.4.231.53	HTTP	anonsvn.wireshark...	GET /viewvc/trunk-1.6/epan/ HTTP/1.1
206	10.916739	24.6.173.220	69.4.231.53	TCP		12608 → 80 [FIN, ACK] Seq=641 Ack=169491 Win=65700 Len=0
352	9.771177	24.6.173.220	69.4.231.53	HTTP	anonsvn.wireshark...	GET /viewvc/trunk-1.6/epan/dissectors/ HTTP/1.1
365	3.085901	69.4.231.53	24.6.173.220	TCP		80 → 12621 [PSH, ACK] Seq=1 Ack=672 Win=7680 Len=335 [TCP segment of a reassembled PDU]
361	2.411608	69.4.231.53	24.6.173.220	TCP		80 → 12609 [PSH, ACK] Seq=151255 Ack=1972 Win=10240 Len=334 [TCP segment of a reassembled PDU]
202	1.115240	69.4.231.53	24.6.173.220	TCP		80 → 12610 [FIN, ACK] Seq=767 Ack=627 Win=7168 Len=0
204	0.512248	69.4.231.53	24.6.173.220	TCP		80 → 12608 [FIN, ACK] Seq=169490 Ack=641 Win=7168 Len=0
227	0.120264	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=14043 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
219	0.105283	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=5283 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
18	0.100442	69.4.231.53	24.6.173.220	TCP		80 → 12608 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
250	0.099336	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=38863 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
7	0.095042	69.4.231.53	24.6.173.220	TCP		80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
353	0.093634	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=151255 Ack=1971 Win=10240 Len=0
201	0.090446	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=545 Ack=1300 Win=8704 Len=0
264	0.090432	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=54923 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
369	0.090323	69.4.231.53	24.6.173.220	TCP		80 → 12621 [ACK] Seq=360 Ack=672 Win=7680 Len=1460 [TCP segment of a reassembled PDU]
214	0.089760	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=903 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
356	0.089529	69.4.231.53	24.6.173.220	TCP		80 → 12621 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
208	0.089033	69.4.231.53	24.6.173.220	TCP		80 → 12610 [ACK] Seq=768 Ack=628 Win=7168 Len=0

> Frame 354: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface unknown, 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: 69.4.231.53
> Transmission Control Protocol, Src Port: 12609, Dst Port: 80, Seq: 1971, Ack: 151255, Len: 0

0000	00 01 5c 31 bb c1 d4 85	64 a7 bf a3 08 00 45 00	..1.... d....E.
0010	00 28 5a 3c 40 00 80 06	00 00 18 06 ad dc 45 04	(Z<@...E.
0020	e7 35 31 41 00 50 f0 1e	4a c2 07 ec 42 a2 50 11	.51A.P.. J...B.P.
0030	40 29 f2 36 00 00		@).6..

http-slow101.pcapng Paquetes: 1101 · Mostrado: 1101 (100.0%) Perfil: wireshark101

LABORATORIO 8B

http-slow101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	TCP DELTA	Source	Destination	Protocol	Host	Info
354	118.195308000	24.6.173.220	69.4.231.53	TCP			12609 → 80 [FIN, ACK] Seq=1971 Ack=151255 Win=65700 Len=0
210	29.006113	41.640641000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [PSH, ACK] Seq=545 Ack=1300 Win=8704 Len=334 [TCP segment of a reassembled PDU]
34	0.006965	36.357656000	69.4.231.53	24.6.173.220	TCP		80 → 12592 [PSH, ACK] Seq=1 Ack=2 Win=17 Len=334 [TCP segment of a reassembled PDU]
16	18.096205	18.096205000	24.6.173.220	69.4.231.53	TCP		12607 → 80 [FIN, ACK] Seq=641 Ack=1 Win=65700 Len=0
30	0.015479	18.052142000	69.4.231.53	24.6.173.220	TCP		80 → 12607 [PSH, ACK] Seq=1 Ack=642 Win=7168 Len=335 [TCP segment of a reassembled PDU]
23	17.965049	17.965049000	69.4.231.53	24.6.173.220	TCP		80 → 12608 [PSH, ACK] Seq=1 Ack=641 Win=7168 Len=335 [TCP segment of a reassembled PDU]
204	0.512248	14.907886000	69.4.231.53	24.6.173.220	TCP		80 → 12608 [FIN, ACK] Seq=169490 Ack=641 Win=7168 Len=0
202	1.115240	14.812617000	69.4.231.53	24.6.173.220	TCP		80 → 12610 [FIN, ACK] Seq=767 Ack=627 Win=7168 Len=0
1098	14.745399	14.745399000	69.4.231.53	24.6.173.220	TCP		80 → 12621 [FIN, ACK] Seq=846303 Ack=672 Win=7680 Len=0
1100	14.381621	14.381621000	24.6.173.220	69.4.231.53	TCP		12621 → 80 [FIN, ACK] Seq=672 Ack=846304 Win=261340 Len=0
200	13.189802	13.743938000	24.6.173.220	69.4.231.53	HTTP	anonsvn.wireshark...	GET /viewvc/trunk-1.6/epan/ HTTP/1.1
207	0.000126	11.429253000	24.6.173.220	69.4.231.53	TCP		12610 → 80 [FIN, ACK] Seq=627 Ack=768 Win=64932 Len=0
206	10.916739	10.916739000	24.6.173.220	69.4.231.53	TCP		12608 → 80 [FIN, ACK] Seq=641 Ack=169491 Win=65700 Len=0
352	9.771177	9.771177000	24.6.173.220	69.4.231.53	HTTP	anonsvn.wireshark...	GET /viewvc/trunk-1.6/epan/dissectors/ HTTP/1.1
365	3.085901	5.498980000	69.4.231.53	24.6.173.220	TCP		80 → 12621 [PSH, ACK] Seq=1 Ack=672 Win=7680 Len=335 [TCP segment of a reassembled PDU]
361	2.411608	2.474089000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [PSH, ACK] Seq=151255 Ack=1972 Win=10240 Len=334 [TCP segment of a reassembled PDU]
113	0.036049	0.198088000	24.6.173.220	69.4.231.53	TCP		12610 → 80 [ACK] Seq=627 Ack=767 Win=64932 Len=0
90	0.061081	0.195158000	24.6.173.220	69.4.231.53	TCP		12609 → 80 [ACK] Seq=645 Ack=545 Win=65156 Len=0
21	0.026921	0.136967000	69.4.231.53	24.6.173.220	TCP		80 → 12607 [ACK] Seq=1 Ack=642 Win=7168 Len=0
14	0.029099	0.130304000	69.4.231.53	24.6.173.220	TCP		80 → 12592 [ACK] Seq=1 Ack=2 Win=17 Len=0
359	0.026930	0.120314000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=151255 Ack=1972 Win=10240 Len=0
227	0.120264	0.120264000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=14043 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
219	0.105283	0.105283000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=5283 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
18	0.100442	0.100442000	69.4.231.53	24.6.173.220	TCP		80 → 12608 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
51	0.007838	0.099399000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
250	0.000226	0.000226000	69.4.231.53	24.6.173.220	TCP		80 → 12609 [ACK] Seq=12609 Ack=12609 Win=1460 Len=0 [TCP segment of a reassembled PDU]

Window size scaling factor: 4

Cheksum: 0xf236 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

▼ [Timestamps]

[Time since first frame in this TCP stream: 184.977107000 seconds]

[Time since previous frame in this TCP stream: 118.195308000 seconds]

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1... d....E.

0010 00 28 5a 3c 40 00 80 06 00 00 18 06 ad dc 45 04 -(Z@...E.

0020 e7 35 31 41 00 50 f0 1e 4a c2 07 ec 42 a2 50 11 .51A-P... J...B.P.

0030 40 29 f2 36 00 00 @)-6..

Time delta from previous frame in this TCP stream (tcp.time_delta)

Paquetes: 1101 · Mostrado: 1101 (100.0%)

Perfil: wireshark101

LABORATORIO 9

CaptureSet101_00004_20201129110730

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	TCP DELTA	Source	Destination	Protocol	Host	Info
1	0.000000	0.000000000 40.79.78.1	192.168.0.8	TCP	443 → 50162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
2	0.031696	ARRISGro_f2:00:e6	IntelCor_86:dd:3c	ARP	Who has 192.168.0.8? Tell 192.168.0.1		
3	0.000028	IntelCor_86:dd:3c	ARRISGro_f2:00:e6	ARP	192.168.0.8 is at 50:eb:71:86:dd:3c		
4	1.732198	0.000000000 192.168.0.8	172.217.8.78	TCP	50153 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]		
5	0.037023	0.037023000 172.217.8.78	192.168.0.8	TCP	443 → 50153 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2		

< >

CaptureSet101_00004_20201129110730 Paquetes: 5 · Mostrado: 5 (100.0%) · Perdido: 0 (0.0%) | Perfil: wireshark101

LABORATORIO II

CaptureSet101

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

icmp

No.	Source	Destination	Protocol	Host	Info
41	192.168.0.8	185.230.61.96	ICMP		Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 42)
42	185.230.61.96	192.168.0.8	ICMP		Echo (ping) reply id=0x0001, seq=9/2304, ttl=237 (request in 41)
466	192.168.0.8	185.230.61.96	ICMP		Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 848)
848	185.230.61.96	192.168.0.8	ICMP		Echo (ping) reply id=0x0001, seq=10/2560, ttl=237 (request in 466)
1500	192.168.0.8	185.230.61.96	ICMP		Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 1501)
1501	185.230.61.96	192.168.0.8	ICMP		Echo (ping) reply id=0x0001, seq=11/2816, ttl=237 (request in 1500)
1502	192.168.0.8	185.230.61.96	ICMP		Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 1503)
1503	185.230.61.96	192.168.0.8	ICMP		Echo (ping) reply id=0x0001, seq=12/3072, ttl=237 (request in 1502)

> Frame 41: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2A376F01-54A3-4463-A648-1F1978A118B4}, id 0
> Ethernet II, Src: IntelCor_86:dd:3c (50:eb:71:86:dd:3c), Dst: ARRISGro_f2:00:e6 (f8:8b:37:f2:00:e6)
> Internet Protocol Version 4, Src: 192.168.0.8, Dst: 185.230.61.96
> Internet Control Message Protocol

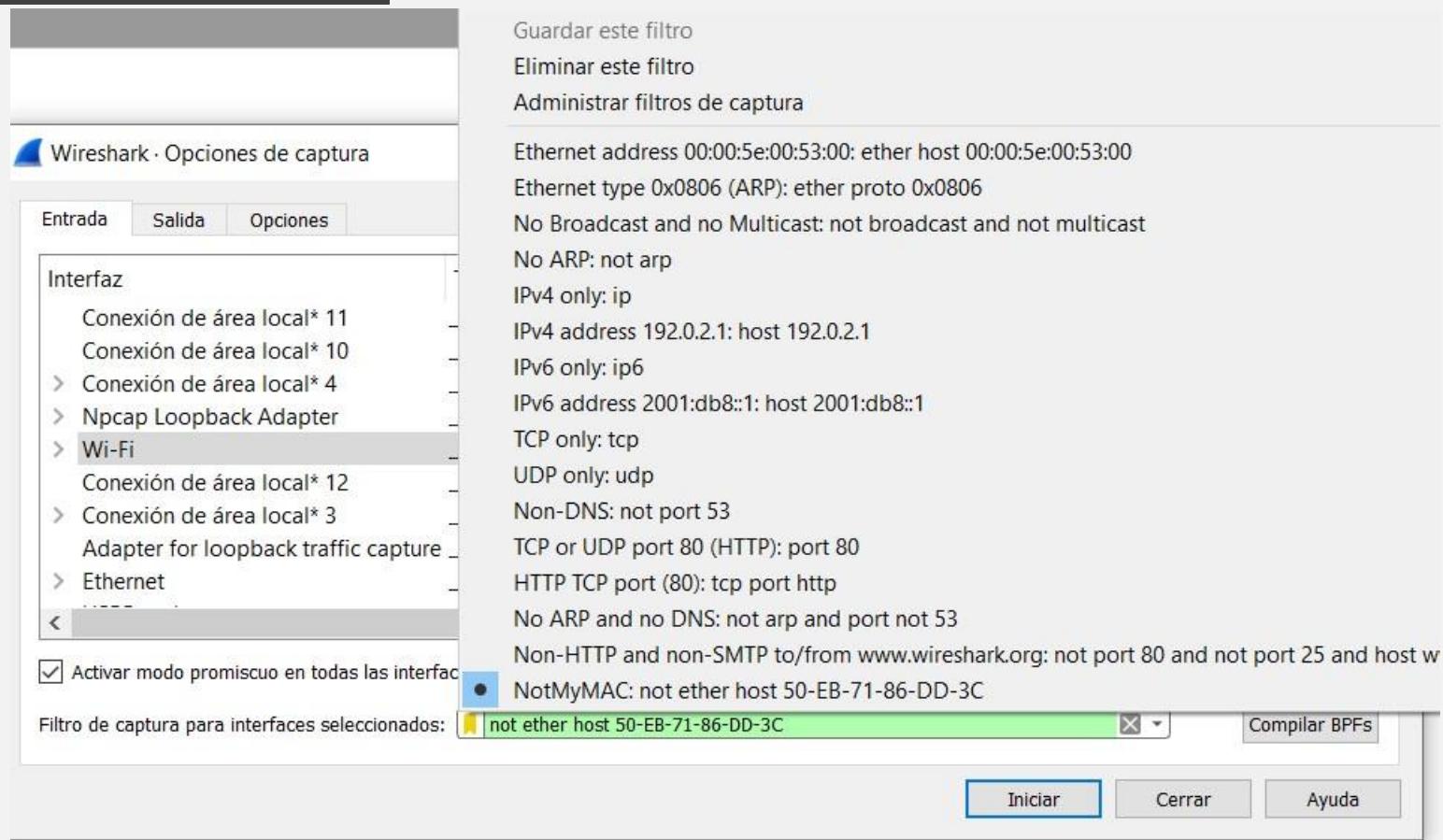
0000	f8	8b	37	f2	00	e6	50	eb	71	86	dd	3c	08	00	45	00	..7...P..q..<..E..
0010	00	3c	86	89	00	00	80	01	00	00	c0	a8	00	08	b9	e6	.<.....
0020	3d	60	08	00	4d	52	00	01	00	09	61	62	63	64	65	66	=`..MR.. ..abcdef
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn opqrstuv
0040	77	61	62	63	64	65	66	67	68	69	wabdefg	hi					

Internet Control Message Protocol: Protocol

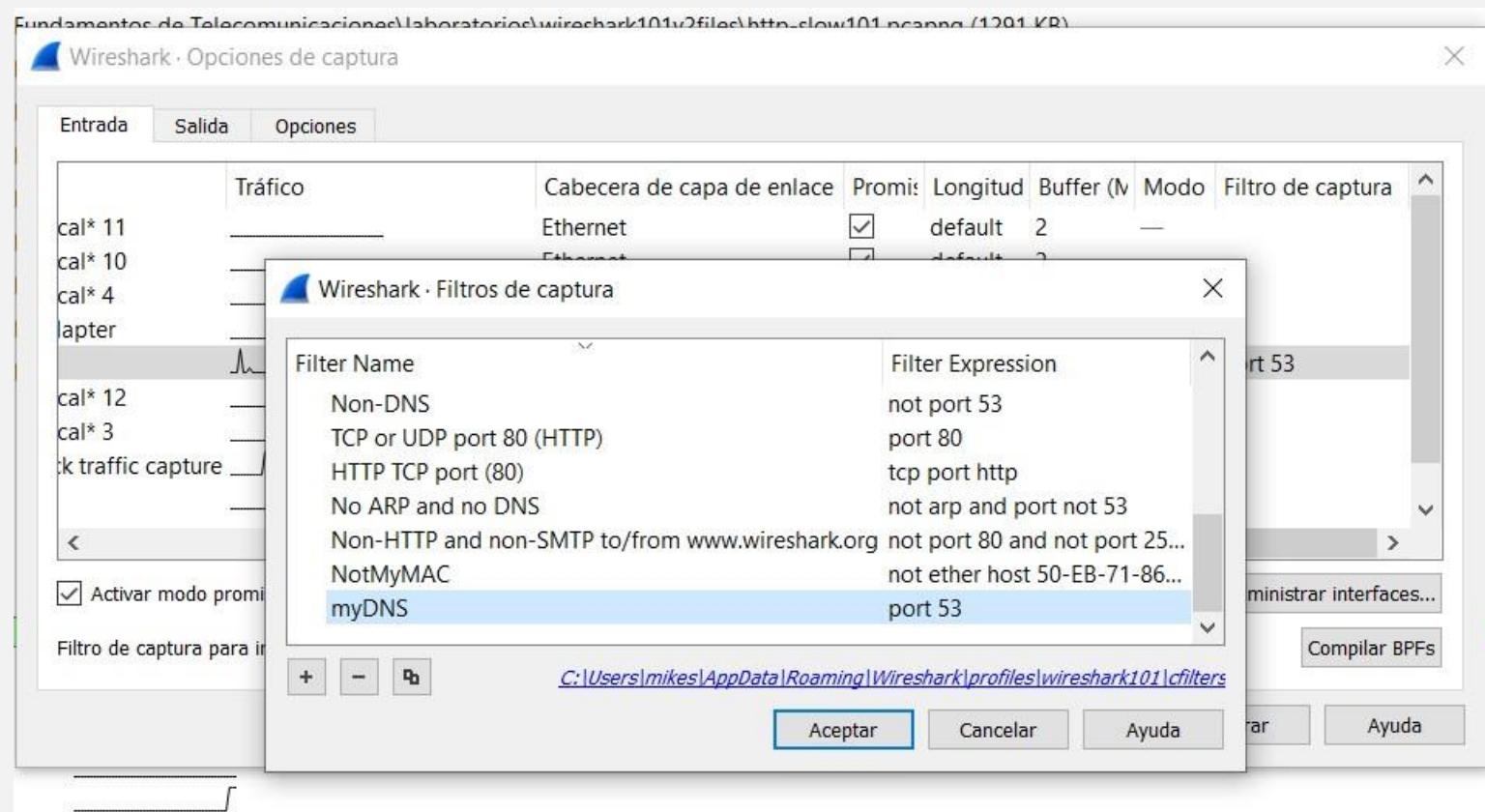
Paquetes: 1923 · Mostrado: 8 (0.4%) · Perdido: 0 (0.0%)

Perfil: wireshark101

LABORATORIO 12



LABORATORIO 13



LABORATORIO 13 B

mydns101_00002_20201117114520

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Source	Destination	Protocol	Host	Info
1	192.168.0.10	10.223.234.2	DNS		Standard query 0x01fb A api.uphold.com
2	192.168.0.10	10.223.234.2	DNS		Standard query 0x64e5 A api.rewards.brave.com
3	192.168.0.10	10.223.234.2	DNS		Standard query 0xeb6d A accounts.google.com
4	192.168.0.10	10.223.234.2	DNS		Standard query 0xb717 A grant.rewards.brave.com
5	10.223.234.2	192.168.0.10	DNS		Standard query response 0x01fb A api.uphold.com A 104.16.79.80 A 104.16.80.80
6	10.223.234.2	192.168.0.10	DNS		Standard query response 0xb717 A grant.rewards.brave.com CNAME dualstack.j3.shared.global.fastly.net A 151.101.50.217
7	10.223.234.2	192.168.0.10	DNS		Standard query response 0xeb6d A accounts.google.com A 172.217.2.77
8	10.223.234.2	192.168.0.10	DNS		Standard query response 0x64e5 A api.rewards.brave.com CNAME rewards-alb-734651130.us-west-2.elb.amazonaws.com A 44.230.228.94 A
9	192.168.0.10	10.223.234.2	DNS		Standard query 0x9d5a A web.whatsapp.com
10	10.223.234.2	192.168.0.10	DNS		Standard query response 0x9d5a A web.whatsapp.com CNAME mmx-ds.cdn.whatsapp.net A 31.13.89.53
11	192.168.0.10	10.223.234.2	DNS		Standard query 0xe679 A laptop-updates.brave.com
12	10.223.234.2	192.168.0.10	DNS		Standard query response 0xe679 A laptop-updates.brave.com CNAME dualstack.f4.shared.global.fastly.net A 151.101.50.110
13	192.168.0.10	10.223.234.2	DNS		Standard query 0xb107 A fonts.gstatic.com
14	10.223.234.2	192.168.0.10	DNS		Standard query response 0xb107 A fonts.gstatic.com CNAME gstaticadssl.1.google.com A 172.217.15.195
15	192.168.0.10	10.223.234.2	DNS		Standard query 0xf785 A s.w.org
16	192.168.0.10	10.223.234.2	DNS		Standard query 0x8aab A ajax.googleapis.com
17	192.168.0.10	10.223.234.2	DNS		Standard query 0x7a10 A cm.g.doubleclick.net
18	10.223.234.2	192.168.0.10	DNS		Standard query response 0xf785 A s.w.org A 192.0.77.48
19	10.223.234.2	192.168.0.10	DNS		Standard query response 0x8aab A ajax.googleapis.com A 142.250.64.202
20	10.223.234.2	192.168.0.10	DNS		Standard query response 0x7a10 A cm.g.doubleclick.net CNAME pagead.l.doubleclick.net A 142.250.64.162
21	192.168.0.10	10.223.234.2	DNS		Standard query 0x8bea A use.fontawesome.com
22	10.223.234.2	192.168.0.10	DNS		Standard query response 0x8bea A use.fontawesome.com CNAME fontawesome-cdn.iconfont.netdna-cdn.com A 23.111.9.35
23	192.168.0.10	10.223.234.2	DNS		Standard query 0xd4bc A www.youtube.com
24	10.223.234.2	192.168.0.10	DNS		Standard query response 0xd4bc A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.15.206 A 142.250.64.142 A 172.217.8.78
25	192.168.0.10	10.223.234.2	DNS		Standard query 0x975f A blog.desdelinux.net
26	10.223.234.2	192.168.0.10	DNS		Standard query 0x975f A blog.desdelinux.net

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{05DD3FF2-38D3-4EDB-8A00-5203D2B425A2}, id 0
> Ethernet II, Src: LCFCHefE_f3:b9:a1 (98:fa:9b:f3:b9:a1), Dst: ARRISGro_f2:00:e6 (f8:8b:37:f2:00:e6)
> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 10.223.234.2
> User Datagram Protocol, Src Port: 51239, Dst Port: 53
> Domain Name System (query)

Offset	Hex	Text
0000	f8 8b 37 f2 00 e6 98 fa	..7..... E-
0010	9b f3 b9 a1 08 00 45 00	<.....
0020	00 3c 07 b2 00 00 80 11	'5(.....
0030	00 00 c0 a8 00 0a dfa pi-uphol
0040	ea 02 c8 27 00 35 00 28	d.com... .
0050	b5 cd 01 fb 01 00 00 01	
0060	00 00 00 00 00 03 61	
0070	70 69 06 75 70 68 6f 6c	
0080	64 03 63 6f 6d 00 00 01	
0090	00 01	

Paquetes: 31 · Mostrado: 31 (100.0%) | Perfil: wireshark101

LABORATORIO 14

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Source	Destination	Protocol	Host	Info
8	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1
33	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/css/global.shared.2.8.4p3.19000.css HTTP/1.1
34	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/css/global.site.2.8.4p3.19000.css HTTP/1.1
37	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.header.2.8.4p3.19000.js HTTP/1.1
42	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /css/pages/sections/feedback.css HTTP/1.1
43	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.top.2.8.4p3.19000.js HTTP/1.1
65	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/css)
68	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/omniture/analyticsconfig.js HTTP/1.1
73	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK
74	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/css)
83	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/s_code.js HTTP/1.1
84	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
119	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)
124	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/ysmwrapper.js HTTP/1.1
126	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)
130	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)
136	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.bottom.2.8.4p3.19000.js HTTP/1.1
143	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
154	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)
156	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/brand.png HTTP/1.1
159	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1
176	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)
181	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1
185	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)
187	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
188	208.93.137.180	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)

Frame 8: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 208.93.137.180

Transmission Control Protocol, Src Port: 10615, Dst Port: 80, Seq: 1, Ack: 1, Len: 495

Hypertext Transfer Protocol

Hex	Text
0000 00 01 5c 31 bb c1 d4 85	..1.... d.....E-
0010 02 17 21 f4 40 00 80 06	..!@.... ..]
0020 00 00 18 06 ad dc d0 5d	..)w-P8 ..13...P-
0030 89 b4 29 77 00 50 38 ea	@!)...GE T /feedb
0040 eb 6c 33 fb ac 9d 50 18	ack/ HTT P/1.1-H

Hypertext Transfer Protocol: Protocol

Paquetes: 11678 · Mostrado: 948 (8.1%)

Perfil: wireshark101

LABORATORIO 14B

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda



No.	Source	Destination	Protocol	Host	Info
8	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1
33	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/css/global.shared.2.8.4p3.19000.css HTTP/1.1
34	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/css/global.site.2.8.4p3.19000.css HTTP/1.1
37	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.header.2.8.4p3.19000.js HTTP/1.1
42	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /css/pages/sections/feedback.css HTTP/1.1
43	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.top.2.8.4p3.19000.js HTTP/1.1
68	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/omniture/analyticsconfig.js HTTP/1.1
83	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/s_code.js HTTP/1.1
84	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
124	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/ysmwrapper.js HTTP/1.1
136	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.bottom.2.8.4p3.19000.js HTTP/1.1
143	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
156	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/brand.png HTTP/1.1
159	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1
181	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1
187	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
191	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/partners/target/target_weekly_ad_animated.gif HTTP/1.1
197	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/utils/rss_icon.png HTTP/1.1
201	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/slideshow/promo/wide/button-prev.gif HTTP/1.1
234	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/slideshow/promo/wide/button-next.gif HTTP/1.1
278	24.6.173.220	208.93.137.180	HTTP	ww2.hdnux.com	GET /photos/16/01/46/3676557/5/square_horiz_promo.jpg HTTP/1.1
290	24.6.173.220	208.93.137.180	HTTP	ww2.hdnux.com	GET /photos/16/02/37/3680253/3/blockstates2.jpg HTTP/1.1
301	24.6.173.220	208.93.137.180	HTTP	ww2.hdnux.com	GET /photos/16/01/41/3676237/5/blockstates2.jpg HTTP/1.1
302	24.6.173.220	208.93.137.180	HTTP	ww1.hdnux.com	GET /photos/16/02/34/3680004/3/square_horiz_promo.jpg HTTP/1.1
303	24.6.173.220	208.93.137.180	HTTP	ww1.hdnux.com	GET /photos/16/01/31/3675736/3/blockstates2.jpg HTTP/1.1
304	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1

> Frame 8: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 208.93.137.180
> Transmission Control Protocol, Src Port: 10615, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
> Hypertext Transfer Protocol

0000	00	01	5c	31	bb	c1	d4	85	64	a7	bf	a3	08	00	45	00	..\\1...	d.....E..
0010	02	17	21	f4	40	00	80	06	00	00	18	06	ad	dc	d0	5d	..!@...]
0020	89	b4	29	77	00	50	38	ea	eb	6c	33	fb	ac	9d	50	18	..)w-P8..	.l3...P..
0030	40	29	21	fe	00	00	47	45	54	20	2f	66	65	65	64	62	@)!...GE	T /feedb
0040	61	63	6b	2f	20	48	54	54	50	2f	31	2e	31	0d	0a	48	ack/	HTT P/1.1..H

LABORATORIO I4C

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.host

Destination	Protocol	Host	Info
208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /external/css/global.shared.2.8.4p3.19000.css HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /external/css/global.site.2.8.4p3.19000.css HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.header.2.8.4p3.19000.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /css/pages/sections/feedback.css HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.top.2.8.4p3.19000.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /js/omniture/analyticsconfig.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/s_code.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/ysmwrapper.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /external/js/global.bottom.2.8.4p3.19000.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/brand.png HTTP/1.1
208.93.137.180	HTTP	aps.hearstnlp.com	GET /Scripts/loadAds.js HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/partners/target/target_weekly_ad_animated.gif HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/utils/rss_icon.png HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/slideshow/promo/wide/button-prev.gif HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/slideshow/promo/wide/button-next.gif HTTP/1.1
208.93.137.180	HTTP	ww2.hdnux.com	GET /photos/16/01/46/3676557/5/square_horiz_promo.jpg HTTP/1.1
208.93.137.180	HTTP	ww2.hdnux.com	GET /photos/16/02/37/3680253/3/blockstates2.jpg HTTP/1.1
208.93.137.180	HTTP	ww2.hdnux.com	GET /photos/16/01/41/3676237/5/blockstates2.jpg HTTP/1.1
208.93.137.180	HTTP	ww1.hdnux.com	GET /photos/16/02/34/3680004/3/square_horiz_promo.jpg HTTP/1.1
208.93.137.180	HTTP	ww1.hdnux.com	GET /photos/16/01/31/3675736/3/blockstates2.jpg HTTP/1.1
208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1

> Frame 8: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 208.93.137.180
> Transmission Control Protocol, Src Port: 10615, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
▼ Hypertext Transfer Protocol
> GET /feedback/ HTTP/1.1\r\nHost: www.sfgate.com\r\n

0040 61 63 6b 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 ack/ HTT P/1.1..H
0050 6f 73 74 3a 20 77 77 77 2e 73 66 67 61 74 65 2e host: www .sfgate.
0060 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a com..Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 Mozilla /5.0 (Wi
0080 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f ndows NT 6.1; WO

HTTP Host (http.host), 22 byte(s)

Paquetes: 11678 · Mostrado: 464 (4.0%)

Perfil: wireshark101

LABORATORIO 14D

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.host contains "hearst"

No.	Source	Destination	Protocol	Host	Info
159	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1
388	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAdsMain.js HTTP/1.1
406	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /SRO/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/initDefineAds.js HTTP/1.1
586	24.6.173.220	216.155.207.26	HTTP	cm.npc-hearst.ove...	GET /js_1_0/?config=2130893885&type=news&cxtId=news&keywordCharEnc=utf8&source=npc_hearst_sanfranciscochronicle_t2_ctxt&adwd=728&adht
1071	24.6.173.220	23.23.99.162	HTTP	hearst.jump-time...	GET /sfgate.gif?url=http%3A//www.sfgate.com/feedback/&uuid=13ac1d11a80-16d57cc1dedb3d3a&proj=sfgate&sec=home&ss=home%3Asan%20francisco
10055	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmfThirdPartyFooter HTTP/1.1
10067	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /SRO/GetJS?url=extras.sfgate.com/sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1
10250	24.6.173.220	216.155.207.26	HTTP	cm.npc-hearst.ove...	GET /js_1_0/?config=2130893885&type=news&cxtId=news&keywordCharEnc=utf8&source=npc_hearst_sanfranciscochronicle_t2_ctxt&adwd=728&adht
10332	24.6.173.220	23.23.99.162	HTTP	hearst.jump-time...	GET /sfgate.gif?url=http%3A//www.sfgate.com/feedback/&uuid=13ac1d11a80-16d57cc1dedb3d3a&proj=sfgate&sec=home&ss=home%3Asan%20francisco

< >

> Frame 159: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 208.93.137.180

> Transmission Control Protocol, Src Port: 10625, Dst Port: 80, Seq: 1, Ack: 1, Len: 290

> Hypertext Transfer Protocol

> GET /Scripts/loadAds.js HTTP/1.1\r\nHost: aps.hearstnp.com\r\n

0050	54 50 2f 31 2e 31 0d 0a	48 6f 73 74 3a 20 61 70	TP/1.1..	Host: ap
0060	73 2e 68 65 61 72 73 74	6e 70 2e 63 6f 6d 0d 0a		s.hearst np.com
0070	55 73 65 72 2d 41 67 65	6e 74 3a 20 4d 6f 7a 69	User-Age nt:	Mozi
0080	6c 6c 61 2f 35 2e 30 20	28 57 69 6e 64 6f 77 73	l1a/5.0 (Windows	
0090	20 4e 54 20 36 2e 31 3b	20 57 4f 57 36 34 3b 20	NT 6.1;	WOW64;

HTTP Host (http.host), 24 byte(s)

Paquetes: 11678 · Mostrado: 10 (0.1%)

Perfil: wireshark101

LABORATORIO 14E

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

http.request.method=="POST"

No.	Source	Destination	Protocol	Host	Info
859	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
864	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
865	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
897	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
898	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
2043	24.6.173.220	67.192.92.227	HTTP	ad.auditude.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=50912&l=20121102085039&of=1.4&tm=15&g=1000002 H
3418	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
3419	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
3476	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)
+ 10022	24.6.173.220	208.93.137.180	HTTP	extras.sfgate.com	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1 (application/x-www-form-urlencoded)
10406	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
10578	24.6.173.220	67.192.92.227	HTTP	ad.auditude.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=50912&l=20121102085149&of=1.4&tm=15&g=1000002 H

> Frame 10022: 1595 bytes on wire (12760 bits), 1595 bytes captured (12760 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 208.93.137.180

> Transmission Control Protocol, Src Port: 10893, Dst Port: 80, Seq: 1, Ack: 1, Len: 1541

▼ Hypertext Transfer Protocol

> POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1\r\n

Host: extras.sfgate.com\r\n

03c0 5b 43 45 5d 3b 20 69 63 78 69 64 3d 31 33 35 31 [CE]; ic xid=1351

03d0 38 37 31 34 33 37 34 32 32 2d 36 37 30 39 38 32 87143742 2-670982

03e0 34 33 37 38 31 39 31 34 36 36 3b 20 5f 5f 67 61 43781914 66; __ga

03f0 64 73 3d 49 44 3d 38 64 62 30 64 61 37 61 64 65 ds=ID=8d b0da7ade

0400 31 33 35 31 37 61 3a 54 3d 31 33 35 31 38 37 31 13517a:T =1351871

0410 34 34 33 3a 53 3d 41 4c 4e 49 5f 4d 62 4b 62 36 443:S=AL NI_MbKb6

0420 75 42 50 69 41 34 78 39 39 5a 56 34 69 65 43 36 uBPiA4x9 9ZV4ieC6

0430 68 6b 46 45 73 47 4e 41 0d 0a 43 6f 6e 74 65 6e hkFEsGNA --Conten

0440 74 2d 54 79 70 65 3a 20 61 70 70 6e 69 63 61 74 t-Type: applicat

0450 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 ion/x-ww w-form-u

0460 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 rlencode d- Conte

0470 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 34 31 0d 0a nt-Lengt h: 441--

0480 0d 0a 66 65 65 64 62 61 63 6b 54 6f 70 69 63 3d .-feedba ckTopic=

0490 73 75 70 70 6f 72 74 2d 69 70 61 64 26 66 65 65 support- ipad&fee

04a0 64 62 61 63 6b 4e 61 6d 65 3d 53 63 6f 6f 74 65 dbackNam e=Scoote

04b0 72 26 66 72 6f 6d 41 64 64 72 3d 73 63 6f 6f 74 &fromAd dr=scoot

04c0 65 72 39 39 39 25 34 30 67 6d 61 69 6c 2e 63 6f er999%40 gmail.co

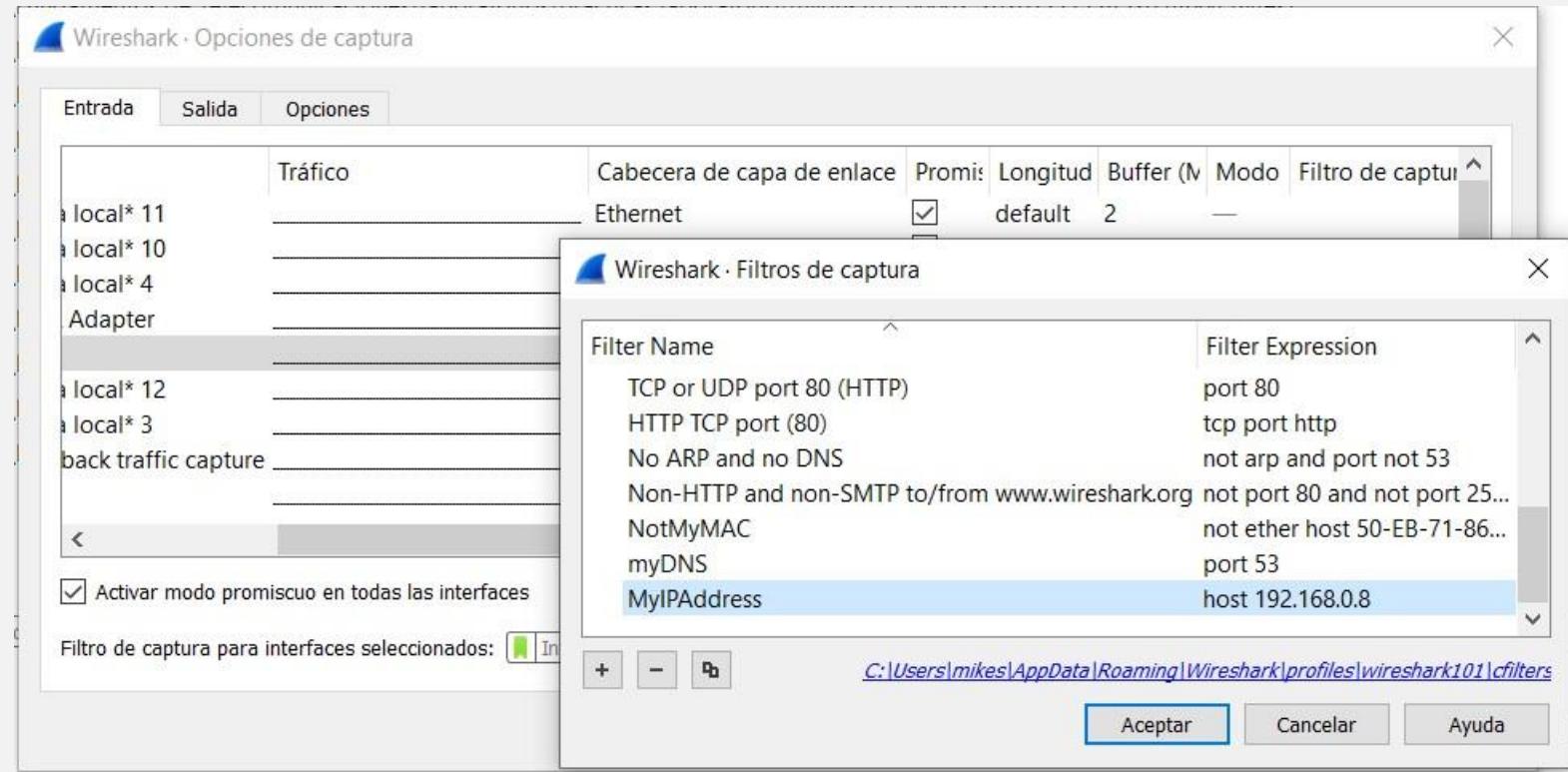
04d0 6d 26 66 65 65 64 62 61 63 6b 43 6f 6d 6d 65 6e m&feedba ckCommen

Bytes 1194-1200: Value (urlencoded-form.value)

Paquetes: 11678 · Mostrado: 12 (0.1%)

Perfil: wireshark101

LABORATORIO 15



LABORATORIO 16

http-disney101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Source	Destination	Protocol	Host	Info
15	24.6.173.220	199.181.132.249	HTTP	www.disney.com	GET / HTTP/1.1
16	199.181.132.249	24.6.173.220	HTTP		HTTP/1.1 301 Moved Permanently (text/html)
32	24.6.173.220	199.181.132.249	HTTP	disney.com	GET / HTTP/1.1
70	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/314da08c2cc0c65e47e899c1c092812dbffa8e6a6.jpg HTTP/1.1
77	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/9d31acc4393a7912869c8d837e51aba2065422c.jpg HTTP/1.1
78	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/69d7937a4e5ed43103011adb5a79af6e77a96d2.jpg HTTP/1.1
79	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/cbb81d69317f2a1c1b5f4d375b71997ea8d49a4b.jpg HTTP/1.1
82	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/7602bb2a242100e3fecaec7bbd7f82a554eb6145.png HTTP/1.1
93	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/525d4cdb4a32ae2cf6b4b220195893749ca271e7.jpg HTTP/1.1
97	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	199.181.132.249	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)
272	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/head-home-6b7ff11bc453.js HTTP/1.1
273	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /f/framework-1.0.2.min.css HTTP/1.1
274	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/application-8d98127cd6fd.css HTTP/1.1
278	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/goc/responsive-84c076723eef.css HTTP/1.1
279	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/goc/responsive-desktop-c543607e68a8.css HTTP/1.1
280	24.6.173.220	198.78.220.87	HTTP	a.dilcdn.com	GET /a/goc/responsive-mobile-8086c89bd3dd.css HTTP/1.1
323	208.111.148.6	24.6.173.220	HTTP		HTTP/1.1 200 OK (JPEG JFIF image)
324	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/bb6f095a6b9899f4f2add8712e77ecf205462eb3.jpg HTTP/1.1
352	208.111.148.6	24.6.173.220	HTTP		HTTP/1.1 200 OK (JPEG JFIF image)
355	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/a818139b961369dfde8137858981752cc8f9db05.jpg HTTP/1.1
414	208.111.148.6	24.6.173.220	HTTP		HTTP/1.1 200 OK (JPEG JFIF image)
416	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/6c969f60841b8bbdd84de3b2f960f4b82ddc8dd.jpg HTTP/1.1
424	208.111.148.6	24.6.173.220	HTTP		HTTP/1.1 200 OK (PNG)
429	24.6.173.220	208.111.148.6	HTTP	cdnvideo.dolimg.com	GET /cdn_assets/4de6a490eae4f1d55218436b0ce1d5b353ed789f.jpg HTTP/1.1
520	173.194.79.95	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/javascript)

> 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

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	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

Hypertext Transfer Protocol: Protocolo | Paquetes: 6143 · Mostrado: 205 (3.3%) | Perfil: wireshark101

LABORATORIO 16B

http-disney101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port==80

No.	Source	Destination	Protocol	Host	Info
12	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	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	24.6.173.220	199.181.132.249	TCP		35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	24.6.173.220	199.181.132.249	HTTP	www.disney.com	GET / HTTP/1.1
16	199.181.132.249	24.6.173.220	HTTP		HTTP/1.1 301 Moved Permanently (text/html)
21	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	24.6.173.220	199.181.132.249	TCP		35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
29	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	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	24.6.173.220	199.181.132.249	TCP		35520 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
32	24.6.173.220	199.181.132.249	HTTP	disney.com	GET / HTTP/1.1
34	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 PDU]
35	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 PDU]
36	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 PDU]
37	24.6.173.220	199.181.132.249	TCP		35520 → 80 [ACK] Seq=285 Ack=4369 Win=65700 Len=0
47	199.181.132.249	24.6.173.220	TCP		80 → 35520 [ACK] Seq=4369 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled PDU]
48	199.181.132.249	24.6.173.220	TCP		80 → 35520 [ACK] Seq=5829 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled PDU]
49	199.181.132.249	24.6.173.220	TCP		80 → 35520 [ACK] Seq=7289 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled PDU]
50	199.181.132.249	24.6.173.220	TCP		80 → 35520 [ACK] Seq=8749 Ack=285 Win=4664 Len=1460 [TCP segment of a reassembled PDU]
51	24.6.173.220	199.181.132.249	TCP		35520 → 80 [ACK] Seq=285 Ack=10209 Win=65700 Len=0
53	24.6.173.220	173.194.79.95	TCP		35521 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55	24.6.173.220	198.78.220.87	TCP		35522 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
56	24.6.173.220	198.78.220.87	TCP		35523 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
57	24.6.173.220	198.78.220.87	TCP		35524 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
58	24.6.173.220	198.78.220.87	TCP		35525 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
59	24.6.173.220	198.78.220.87	TCP		35526 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

> 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

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

HTTP Host (http.host), 22 byte(s)

Paquetes: 6143 · Mostrado: 5917 (96.3%)

Perfil: wireshark101

LABORATORIO 17

mybackground101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

dns

No.	Source	Destination	Protocol	Host	Info
28	24.6.173.220	75.75.75.75	DNS		Standard query 0x5183 A javadl-esd-secure.oracle.com
29	75.75.75.75	24.6.173.220	DNS		Standard query response 0x5183 A javadl-esd-secure.oracle.com CNAME javadl-esd-secure.oracle.com.edgekey.net CNAME e5486.g.akamaiedge.
30	24.6.173.220	75.75.75.75	DNS		Standard query 0x5ae1 AAAA javadl-esd-secure.oracle.com
31	75.75.75.75	24.6.173.220	DNS		Standard query response 0x5ae1 AAAA javadl-esd-secure.oracle.com CNAME javadl-esd-secure.oracle.com.edgekey.net CNAME e5486.g.akamaied
127	24.6.173.220	75.75.75.75	DNS		Standard query 0x4372 A api.memeo.info
128	75.75.75.75	24.6.173.220	DNS		Standard query response 0x4372 A api.memeo.info A 216.115.74.235
129	24.6.173.220	75.75.75.75	DNS		Standard query 0x027b AAAA api.memeo.info
130	75.75.75.75	24.6.173.220	DNS		Standard query response 0x027b AAAA api.memeo.info SOA a4.nstld.com
420	24.6.173.220	75.75.75.75	DNS		Standard query 0x81b6 A api.memeo.com
421	75.75.75.75	24.6.173.220	DNS		Standard query response 0x81b6 A api.memeo.com A 216.115.74.202
422	24.6.173.220	75.75.75.75	DNS		Standard query 0xe061 AAAA api.memeo.com
423	75.75.75.75	24.6.173.220	DNS		Standard query response 0xe061 AAAA api.memeo.com SOA a4.nstld.com
450	24.6.173.220	75.75.75.75	DNS		Standard query 0xaad8 A memeo.info
451	75.75.75.75	24.6.173.220	DNS		Standard query response 0xaad8 A memeo.info A 216.115.74.234
452	24.6.173.220	75.75.75.75	DNS		Standard query 0xb69b AAAA memeo.info
453	75.75.75.75	24.6.173.220	DNS		Standard query response 0xb69b AAAA memeo.info SOA a4.nstld.com

< >

> Frame 28: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 75.75.75.75
> User Datagram Protocol, Src Port: 58537, Dst Port: 53
> Domain Name System (query)

0000	00 01 5c 31 bb c1 d4 85	64 a7 bf a3 08 00 45 00	..\\1.....d.....E..
0010	00 4a 04 cd 00 00 80 11	00 00 18 06 ad dc 4b 4b	.J.....KK
0020	4b 4b e4 a9 00 35 00 36	5c c0 51 83 01 00 00 01	KK--5-6 \\Q.....
0030	00 00 00 00 00 11 6a	61 76 61 64 6c 2d 65 73j avadl-es
0040	64 2d 73 65 63 75 72 65	06 6f 72 61 63 6c 65 03	d-secure .oracle-
0050	63 6f 6d 00 00 01 00 01		com.....

mybackground101.pcapng | Paquetes: 514 · Mostrado: 16 (3.1%) | Perfil: wireshark101

LABORATORIO 17B

mybackground101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr==216.115.74.0/24

No.	Source	Destination	Protocol	Host	Info
118	24.6.173.220	216.115.74.235	TCP		1145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
119	216.115.74.235	24.6.173.220	TCP		80 → 1145 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
120	24.6.173.220	216.115.74.235	TCP		1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
121	24.6.173.220	216.115.74.235	HTTP	www.memeo.info	GET /php/updateMetric.php?product_key=MABPEME000-6E2P-2AC]-3KP3-JF0E-009F&locale=en-US&num_jobs=1&eseller_id=STR3685286259&unique
122	216.115.74.235	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)
123	24.6.173.220	216.115.74.235	TCP		1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0
131	24.6.173.220	216.115.74.235	TCP		1146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
132	216.115.74.235	24.6.173.220	TCP		80 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
133	24.6.173.220	216.115.74.235	TCP		1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
134	24.6.173.220	216.115.74.235	HTTP	api.memeo.info	GET /ClientSettings.php?buildtype=sgm&esellerid=STR3685286259&product=autobackuppro&productleveltype=PREMIUM HTTP/1.1
135	216.115.74.235	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)
136	216.115.74.235	24.6.173.220	TCP		80 → 1146 [FIN, ACK] Seq=247 Ack=163 Win=4062 Len=0
137	24.6.173.220	216.115.74.235	TCP		1146 → 80 [ACK] Seq=163 Ack=248 Win=66052 Len=0
138	24.6.173.220	216.115.74.235	TCP		1146 → 80 [FIN, ACK] Seq=163 Ack=248 Win=66052 Len=0
139	216.115.74.235	24.6.173.220	TCP		80 → 1146 [ACK] Seq=248 Ack=164 Win=4062 Len=0
424	24.6.173.220	216.115.74.202	TCP		1187 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
425	216.115.74.202	24.6.173.220	TCP		80 → 1187 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
426	24.6.173.220	216.115.74.202	TCP		1187 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
427	24.6.173.220	216.115.74.202	HTTP	api.memeo.com	GET /1.0/util/get_conf HTTP/1.1
428	216.115.74.202	24.6.173.220	TCP		80 → 1187 [ACK] Seq=1 Ack=168 Win=4067 Len=0
429	216.115.74.202	24.6.173.220	TCP		80 → 1187 [ACK] Seq=1 Ack=168 Win=4067 Len=1300 [TCP segment of a reassembled PDU]
430	216.115.74.202	24.6.173.220	TCP		80 → 1187 [PSH, ACK] Seq=1301 Ack=168 Win=4067 Len=160 [TCP segment of a reassembled PDU]
431	24.6.173.220	216.115.74.202	TCP		1187 → 80 [ACK] Seq=168 Ack=1461 Win=66300 Len=0
432	216.115.74.202	24.6.173.220	HTTP		HTTP/1.1 200 OK (application/x-javascript)
433	216.115.74.202	24.6.173.220	TCP		80 → 1187 [FIN, ACK] Seq=2300 Ack=168 Win=4067 Len=0
434	24.6.173.220	216.115.74.202	TCP		1187 → 80 [ACK] Seq=168 Ack=2301 Win=65460 Len=0

> Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFF300A9B9F}, 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: 216.115.74.235
> Transmission Control Protocol, Src Port: 1145, Dst Port: 80, Seq: 0, Len: 0

0000	00 01 5c 31 bb c1 d4 85	64 a7 bf a3 08 00 45 00	.. \1 .. d .. E ..
0010	00 34 04 fb 40 00 80 06	00 00 18 06 ad dc d8 73	.. 4 .. @ s ..
0020	4a eb 04 79 00 50 c8 f4	05 1d 00 00 00 00 80 02	J .. y .. P
0030	20 00 e9 67 00 00 02 04	05 b4 01 03 03 02 01 01	.. g
0040	04 02	

mybackground101.pcapng Paquetes: 514 · Mostrado: 51 (9.9%) Perfil: wireshark101

LABORATORIO 18

http-errors101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

[{dns.flags.code == 3} || (http.response.code == 404)]

No.	Source	Destination	Protocol	Host	Info
9	198.66.239.146	24.6.173.220	HTTP		HTTP/1.1 404 Not Found (text/html)
18	75.75.75.75	24.6.173.220	DNS		Standard query response 0x8e30 No such name A www.chappelluuu.com SOA a.gtld-servers.net
27	198.66.239.146	24.6.173.220	HTTP		HTTP/1.1 404 Not Found (text/html)

< >

> Frame 9: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFF300A9B9F}, id 0
> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
> Internet Protocol Version 4, Src: 198.66.239.146, Dst: 24.6.173.220
> Transmission Control Protocol, Src Port: 80, Dst Port: 14845, Seq: 1, Ack: 304, Len: 580
▼ Hypertext Transfer Protocol
 ▼ HTTP/1.1 404 Not Found\r\n > [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n] Response Version: HTTP/1.1 Status Code: 404 [Status Code Description: Not Found] Response Phrase: Not Found Date: Fri, 02 Nov 2012 19:23:43 GMT\r\n

0030	80 52 df bf 00 00 48 54 54 50 2f 31 2e 31 20 34 .R----HT TP/1.1 4
0040	30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 44 61 04 Not F ound..Da
0050	74 65 3a 20 46 72 69 2c 20 30 32 20 4e 76 20 te: Fri, 02 Nov
0060	32 30 31 32 20 31 39 3a 32 33 3a 34 33 20 47 4d 2012 19: 23:43 GM
0070	54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 T..Serve r: Apach
0080	65 2f 31 2e 33 2e 34 32 20 28 55 6e 69 78 29 20 e/1.3.42 (Unix)

Frame (634 bytes) De-chunked entity body (276 bytes)

HTTP Response Status Code (http.response.code), 3 byte(s)

Paquetes: 28 · Mostrado: 3 (10.7%)

Perfil: wireshark101

LABORATORIO 19

Wireshark · Conversations · gen-startupchatty101.pcapng

Ethernet · 13	IPv4 · 15	IPv6 · 12	TCP · 6	UDP · 52							
Address A	Port A	Address B	Port B	Packets	Bytes	Bytes A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.169.43	54693	50.17.223.168	443	2.886	2971k	955	58k	1.931	2913k 17.806716	117.4765	3968
24.6.169.43	54692	199.47.216.174	443	45	31k	18	1868	27	29k 11.194685	124.0885	120
24.6.169.43	54689	199.47.217.177	443	26	17k	10	3584	16	13k 0.192944	17.2411	1663
24.6.169.43	54694	24.6.173.220	17500	27	4948	14	2331	13	2617 23.797097	111.4851	167
24.6.169.43	54690	108.160.161.163	80	17	2318	8	1254	9	1064 0.207287	135.1267	74
24.6.169.43	54675	65.54.87.217	80	3	180	0	0	3	180 0.798543	128.0016	0

Resolución de nombre Limitar filtro de visualización Hora de inicio absoluta

Conversation Types ▾

Copiar ▾ Follow Stream... Graph... Cerrar Ayuda

LABORATORIO 19B

gen-startupchatty101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr==24.6.169.43 && tcp.port==54693 && ip.addr==50.17.223.168 && tcp.port==443

No.	Source	Destination	Protocol	Host	Info
311	24.6.169.43	50.17.223.168	TCP		54693 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
313	50.17.223.168	24.6.169.43	TCP		443 → 54693 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
314	24.6.169.43	50.17.223.168	TCP		54693 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
315	24.6.169.43	50.17.223.168	TLSv1		Client Hello
316	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=1 Ack=97 Win=5888 Len=0
317	50.17.223.168	24.6.169.43	TLSv1		Server Hello
318	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=1461 Ack=97 Win=5888 Len=1460 [TCP segment of a reassembled PDU]
319	50.17.223.168	24.6.169.43	TLSv1		Certificate, Server Key Exchange, Server Hello Done
320	24.6.169.43	50.17.223.168	TCP		54693 → 443 [ACK] Seq=97 Ack=2921 Win=65700 Len=0
321	24.6.169.43	50.17.223.168	TLSv1		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
322	50.17.223.168	24.6.169.43	TLSv1		New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
323	24.6.169.43	50.17.223.168	TLSv1		Application Data
326	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=4067 Ack=540 Win=8064 Len=0
327	24.6.169.43	50.17.223.168	TLSv1		Application Data
328	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=4067 Ack=993 Win=9088 Len=0
329	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=4067 Ack=993 Win=9088 Len=1460 [TCP segment of a reassembled PDU]
330	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=5527 Ack=993 Win=9088 Len=1460 [TCP segment of a reassembled PDU]
331	50.17.223.168	24.6.169.43	TCP		443 → 54693 [ACK] Seq=6987 Ack=993 Win=9088 Len=1460 [TCP segment of a reassembled PDU]
332	24.6.169.43	50.17.223.168	TCP		54693 → 443 [ACK] Seq=993 Ack=6987 Win=65700 Len=0

> Frame 311: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, id 0
> Ethernet II, Src: ASUSTekC_19:9e:19 (c8:60:00:19:9e:19), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.169.43, Dst: 50.17.223.168
> Transmission Control Protocol, Src Port: 54693, Dst Port: 443, Seq: 0, Len: 0

Offset	Hex	Dec	Text
0000	00 01 5c 31 bb c1 c8 60	256 1 92 49 199 192 204 96	..`1...`.....E-
0010	00 34 01 ff 40 00 80 06	204 52 1 255 64 0 128 6	-4..@....%....+2.
0020	25 da 18 06 a9 2b 32 11	40 182 28 6 177 43 50 17J@.....
0030	df a8 d5 a5 01 bb 4a 40	223 168 213 165 1 187 74 64	@.....
0040	19 a2 00 00 00 00 80 02	29 162 0 0 0 0 128 2	..
0040	04 02	4 2	

gen-startupchatty101.pcapng Paquetes: 3290 · Mostrado: 2886 (87.7%) Perfil: wireshark101

LABORATORIO 20

general101b.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

[tcp.flags == 0x002]

No.	Source	Destination	Protocol	Host	Info
1	24.6.173.220	216.115.212.254	TCP		16190 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	24.6.173.220	67.217.65.244	TCP		16191 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8	24.6.173.220	64.74.80.187	TCP		16192 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19	24.6.173.220	202.173.28.250	TCP		16193 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
38	24.6.173.220	216.115.212.254	TCP		16194 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
44	24.6.173.220	67.217.65.244	TCP		16195 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
45	24.6.173.220	64.74.80.187	TCP		16196 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
56	24.6.173.220	202.173.28.250	TCP		16197 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
65	24.6.173.220	216.115.212.254	TCP		16198 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
81	24.6.173.220	67.217.65.244	TCP		16199 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
82	24.6.173.220	64.74.80.187	TCP		16200 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
93	24.6.173.220	202.173.28.250	TCP		16201 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
140	24.6.169.43	199.47.217.177	TCP		54704 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
162	24.6.173.220	199.47.216.174	TCP		16202 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
164	24.6.169.43	199.47.219.159	TCP		54705 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
245	24.6.169.43	107.20.249.66	TCP		54706 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
248	24.6.169.43	107.20.249.54	TCP		54707 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
352	121.125.72.180	24.6.169.43	TCP		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
353	121.125.72.180	24.6.173.220	TCP		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

Transmission Control Protocol, Src Port: 16190, Dst Port: 443, Seq: 0, Len: 0

Source Port: 16190
Destination Port: 443
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 4069868883
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)

0000	00	01	5c	31	bb	c1	d4	85	64	a7	bf	a3	08	00	45	00	.. \1.... d.....E-
0010	00	34	01	c0	40	00	80	06	00	00	18	06	ad	dc	d8	73	.4...@..... .s
0020	d4	fe	3f	3e	01	bb	f2	95	45	53	00	00	00	00	80	02	.?>.... ES.....
0030	20	00	73	7b	00	00	02	04	05	b4	01	03	03	02	01	01	.s{....
0040	04	02															..

Flags (12 bits) (tcp.flags), 2 bytes(s)

Paquetes: 575 · Mostrado: 42 (7.3%)

Perfil: wireshark101

LABORATORIO 20B

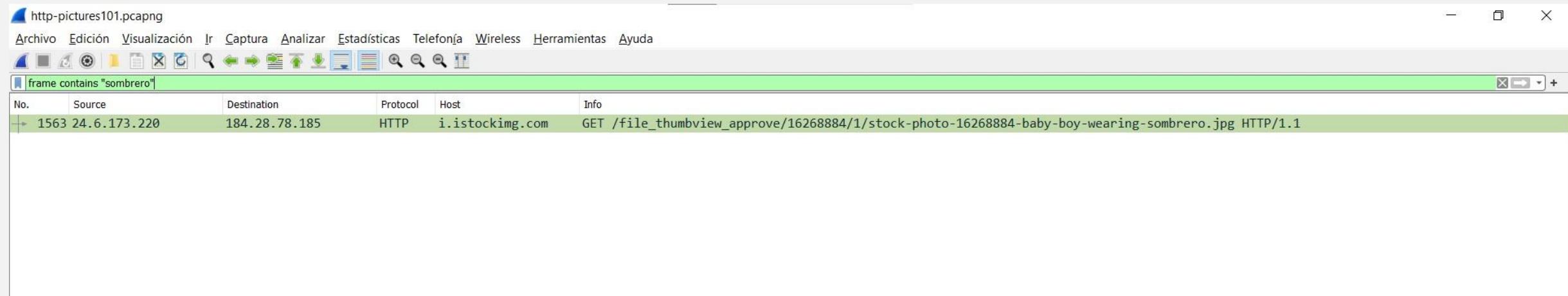
general101b.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

tcp.flags == 0x002 && ip.dst==24.6.0.0/16

No.	Source	Destination	Protocol	Host	Info
352	121.125.72.180	24.6.169.43	TCP		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
353	121.125.72.180	24.6.173.220	TCP		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
535	24.6.169.43	24.6.173.220	TCP		54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
537	24.6.169.43	24.6.173.220	TCP		[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
551	24.6.169.43	24.6.173.220	TCP		[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

LABORATORIO 21



LABORATORIO 2IB

http-pictures101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

frame matches "(?i)(sombrero|football)"

No.	Source	Destination	Protocol	Host	Info
1563	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/16268884/1/stock-photo-16268884-baby-boy-wearing-sombrero.jpg HTTP/1.1
3418	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/21968700/1/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1
3740	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/21968700/2/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1

Transmission Control Protocol, Src Port: 16652, Dst Port: 80, Seq: 9981, Ack: 245610, Len: 418

Source Port: 16652
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 418]
Sequence Number: 9981 (relative sequence number)
Sequence Number (raw): 1052593534
[Next Sequence Number: 10399 (relative sequence number)]
Acknowledgment Number: 245610 (relative ack number)
Acknowledgment number (raw): 2417661067
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)

0020	4e b9 41 0c 00 50 3e bd 4d 7e 90 1a 94 8b 50 18	N-A--P>.. M~....p.
0030	3f b8 ce 74 00 00 47 45 54 20 2f 66 69 6c 65 5f	?..t--GE T /file_
0040	74 68 75 6d 62 76 69 65 77 5f 61 70 72 6f 76	thumbvie w_approv
0050	65 2f 31 36 32 36 38 38 38 34 2f 31 2f 73 74 6f	e/162688 84/1/sto
0060	63 6b 2d 70 68 6f 74 6f 2d 31 36 32 36 38 38 38	ck-photo -1626888
0070	34 2d 62 61 62 79 2d 62 6f 79 2d 77 65 61 72 69	4-baby-b oy-weari
0080	6e 67 2d 73 6f 6d 62 72 65 72 6f 2e 6a 70 67 20	ng-sombr ero.jpg

Flags (12 bits) (tcp.flags), 2 byte(s)

Paquetes: 3823 · Mostrado: 3 (0.1%)

Perfil: wireshark101

LABORATORIO 22

http-pictures101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.request.uri matches "baby.{1,3}smiling"

No.	Source	Destination	Protocol	Host	Info
+ 427	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/16072653/1/stock-photo-16072653-mom-and-baby-smiling.jpg HTTP/1.1
749	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/16072653/2/stock-photo-16072653-mom-and-baby-smiling.jpg HTTP/1.1

Transmission Control Protocol, Src Port: 16649, Dst Port: 80, Seq: 2904, Ack: 72223, Len: 413

Source Port: 16649
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 413]
Sequence Number: 2904 (relative sequence number)
Sequence Number (raw): 2363155570
[Next Sequence Number: 3317 (relative sequence number)]
Acknowledgment Number: 72223 (relative ack number)
Acknowledgment number (raw): 5583658
0101 = Header length: 20 bytes (5)

LABORATORIO 22B

http-pictures101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

http.request.uri matches "baby.{1,20}smiling"

No.	Source	Destination	Protocol	Host	Info
404	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/10195917/1/stock-video-10195917-baby-on-belly-smiling.jpg HTTP/1.1
→ 427	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/16072653/1/stock-photo-16072653-mom-and-baby-smiling.jpg HTTP/1.1
749	24.6.173.220	184.28.78.185	HTTP	i.istockimg.com	GET /file_thumbview_approve/16072653/2/stock-photo-16072653-mom-and-baby-smiling.jpg HTTP/1.1

Transmission Control Protocol, Src Port: 16649, Dst Port: 80, Seq: 2904, Ack: 72223, Len: 413

Source Port: 16649
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 413]
Sequence Number: 2904 (relative sequence number)
Sequence Number (raw): 2363155570
[Next Sequence Number: 3317 (relative sequence number)]
Acknowledgment Number: 72223 (relative ack number)
Acknowledgment number (raw): 5583658
0101 = Header Length: 20 bytes (5)

LABORATORIO 25

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Source	Destination	Protocol	Host	Coloring Rule Name	Info
461	24.6.173.220	75.75.75.75	DNS		UDP	Standard query 0xbb69 AAAA www.googletagservices.com
462	208.93.137.180	24.6.173.220	TCP		HTTP	80 → 10625 [ACK] Seq=7112 Ack=1190 Win=10240 Len=0
463	208.93.137.180	24.6.173.220	HTTP		HTTP	HTTP/1.1 200 OK (application/x-javascript)
464	184.73.197.77	24.6.173.220	TCP		HTTP	80 → 10642 [ACK] Seq=4381 Ack=308 Win=6912 Len=1460 [TCP segment of a reassembled PDU]
465	184.73.197.77	24.6.173.220	HTTP		HTTP	HTTP/1.1 200 OK (text/javascript)
466	24.6.173.220	184.73.197.77	TCP		HTTP	10642 → 80 [ACK] Seq=308 Ack=6271 Win=65700 Len=0
467	24.6.173.220	208.93.137.180	TCP		HTTP	10618 → 80 [ACK] Seq=1275 Ack=40046 Win=65700 Len=0
468	75.75.75.75	24.6.173.220	DNS		UDP	Standard query response 0xbb69 AAAA www.googletagservices.com CNAME pagead46.l.doubleclick.net AAAA 2001:4860:4001:800::1
469	24.6.173.220	66.109.241.50	TCP		HTTP	10622 → 80 [ACK] Seq=320 Ack=450 Win=65788 Len=0
470	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=6901 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
471	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=8281 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
472	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=9661 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
473	24.6.173.220	66.109.241.50	TCP		HTTP	10623 → 80 [ACK] Seq=316 Ack=11041 Win=66240 Len=0
474	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=11041 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
475	66.109.241.50	24.6.173.220	TCP		Bad TCP	[TCP Dup ACK 410#1] 80 → 10623 [ACK] Seq=12421 Ack=316 Win=65220 Len=0
476	24.6.173.220	75.75.75.75	DNS		UDP	Standard query 0x7394 A partner.googleadservices.com
477	24.6.173.220	107.22.233.219	TCP		HTTP	10635 → 80 [ACK] Seq=380 Ack=308 Win=65392 Len=0
478	75.75.75.75	24.6.173.220	DNS		UDP	Standard query response 0x7394 A partner.googleadservices.com CNAME partnerad.1.doubleclick.net A 74.125.224.45 A 74.125
479	24.6.173.220	75.75.75.75	DNS		UDP	Standard query 0x6d20 AAAA partner.googleadservices.com
480	75.75.75.75	24.6.173.220	DNS		UDP	Standard query response 0x6d20 AAAA partner.googleadservices.com CNAME partnerad.1.doubleclick.net SOA ns1.google.com

[Time since reference or first frame: 0.696044000 seconds]

Frame Number: 472

Frame Length: 1434 bytes (11472 bits)

Capture Length: 1434 bytes (11472 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)

> Internet Protocol Version 4, Src: 66.109.241.50, Dst: 24.6.173.220

> Transmission Control Protocol, Src Port: 80, Dst Port: 10623, Seq: 9661, Ack: 316, Len: 1380

0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20 ..d..... \1....E
0010 05 8c 0b e0 40 00 6c 06 03 ea 42 6d f1 32 18 06@-1 ..Bm-2..
0020 ad dc 00 50 29 7f 74 5c cc 79 03 94 71 5f 50 10 ...P).+\\ .y..q_P.
0030 fe c4 00 37 00 00 20 20 20 20 69 66 20 28 4f ...7.. if (0
0040 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e bject.pr ototype.
0050 74 6f 53 74 72 69 6e 67 2e 61 70 70 6c 79 28 76 toString .apply(v
0060 61 6c 75 65 29 20 3d 3d 20 27 5b 6f 62 6a 65 alue) == = '[obje

The frame matched the coloring rule with this name (frame.coloring_rule.name)

Paquetes: 11678 · Mostrado: 11678 (100.0%)

Perfil: wireshark101

LABORATORIO 26

Source Destination Protocol Host Coloring Rule Name Info

Wireshark · Reglas de coloreado wireshark101

Nombre	Filtro
<input checked="" type="checkbox"/> S-FTP arguments	ftp.request.arg
<input type="checkbox"/> Nueva regla de coloreado	TCP DELTA
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3 icmpv6.type eq 4
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.4 && ip.ttl < 5 && !ipim && !ospf) (ip.dst == 224.0.0.24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp carp))
<input checked="" type="checkbox"/> Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.status=="Bad" mstp
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal sysdig

Doble clic para editar. Arrastrar para mover. Las reglas son procesadas en orden hasta que una coincidencia es encontrada.

+ -   Primer plano Fondo Aplicar como filtro

C:\Users\mikes\AppData\Roaming\Wireshark\profiles\wireshark101\colorfilters

Aceptar Copiar desde Cancelar Import... Export... Ayuda

LABORATORIO 26B

ftp-crack101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	TCP DELTA	Source	Destination	Protocol	Host	Coloring Rule Name	Info
1	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2217 [ACK] Seq=1 Ack=1 Win=49152 Len=0
2	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	21 → 2227 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
3	0.000117000	10.234.125.254	10.121.70.151	TCP		TCP	2227 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.012755000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 530 Login incorrect.
5	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP SYN/FIN	21 → 2228 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
6	0.000056000	10.234.125.254	10.121.70.151	TCP		TCP	2228 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
7	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2222 [ACK] Seq=1 Ack=1 Win=49152 Len=0
8	0.011870000	10.234.125.254	10.121.70.151	TCP		TCP SYN/FIN	2217 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0
9	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2220 [ACK] Seq=1 Ack=1 Win=49152 Len=0
10	0.012407000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
11	0.000473000	10.234.125.254	10.121.70.151	FTP		S-FTP argumento...	Request: PASS merlin
12	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2221 [ACK] Seq=1 Ack=1 Win=49152 Len=0
13	0.013168000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 530 Login incorrect.
14	0.001176000	10.234.125.254	10.121.70.151	TCP		TCP SYN/FIN	2220 → 21 [FIN, ACK] Seq=1 Ack=23 Win=17447 Len=0
15	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2224 [ACK] Seq=1 Ack=1 Win=49152 Len=0
16	0.016828000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.
17	0.001306000	10.234.125.254	10.121.70.151	FTP		S-FTP argumento...	Request: PASS mercury
18	0.00000000	10.121.70.151	10.234.125.254	TCP		TCP	21 → 2223 [ACK] Seq=1 Ack=1 Win=49152 Len=0
19	0.009972000	10.121.70.151	10.234.125.254	FTP		TCP	Response: 331 Password required for admin.

> Frame 11: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface unknown, id 0
> Ethernet II, Src: AmbitMic_aa:af:80 (00:0d:59:aa:af:80), Dst: Cisco_3c:3f:a8 (00:01:96:3c:3f:a8)
> Internet Protocol Version 4, Src: 10.234.125.254, Dst: 10.121.70.151
> Transmission Control Protocol, Src Port: 2222, Dst Port: 21, Seq: 1, Ack: 35, Len: 13
File Transfer Protocol (FTP)
PASS merlin\r\nRequest command: PASS
Request arg: merlin
[Current working directory:]

0000	00	01	96	3c	3f	a8	00	d0	59	aa	af	80	08	00	45	00	...<?...Y....E-
0010	00	35	36	44	40	00	80	06	ea	86	0a	ea	7d	fe	0a	79	.56D@...-...}...y
0020	46	97	08	ae	00	15	42	79	8f	49	4b	86	20	cd	50	18	F.....By .IK..P.
0030	44	3d	c4	c5	00	00	50	41	53	53	20	6d	65	72	6c	69	D=...PA SS merli
0040	6e	0d	0a														n..

Request arg (ftp.request.arg), 6 byte(s)

Paquetes: 19730 · Mostrado: 19730 (100.0%)

Perfil: wireshark101

LABORATORIO 27

http-browse101d.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	TCP DELTA	Source	Destination	Protocol	Host	Coloring Rule Name	Info
127	0.000007000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61608 [ACK] Seq=1849 Ack=323 Win=5504 Len=1460 [TCP segment of a reassembled
128	0.000004000	209.177.86.18	24.6.173.220	HTTP		HTTP	HTTP/1.0 200 OK (GIF89a)
129	0.002637000	209.177.86.18	24.6.173.220	HTTP		HTTP	HTTP/1.0 200 OK (GIF89a)
130	0.091574000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61605 [ACK] Seq=1 Ack=322 Win=5504 Len=0
131	0.000002000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61605 [PSH, ACK] Seq=1 Ack=322 Win=5504 Len=386 [TCP segment of a reassembled
132	0.001334000	24.6.173.220	209.177.86.18	HTTP	images.china.cn	HTTP	GET /images1/en/2011first/120626-sd.jpg HTTP/1.1
133	0.001335000	24.6.173.220	209.177.86.18	TCP		HTTP	61606 → 80 [ACK] Seq=322 Ack=535 Win=65164 Len=0
134	0.002135000	209.177.86.18	24.6.173.220	HTTP		HTTP	HTTP/1.0 200 OK (GIF89a)
135	0.000223000	24.6.173.220	209.177.86.18	TCP		HTTP	61605 → 80 [ACK] Seq=322 Ack=625 Win=65076 Len=0
136	0.001398000	24.6.173.220	209.177.86.18	HTTP	images.china.cn	HTTP	GET /images1/en/2011first/120622-qd.jpg HTTP/1.1
137	0.001288000	24.6.173.220	209.177.86.18	HTTP	images.china.cn	HTTP	GET /images1/en/2011first/121101-en.jpg HTTP/1.1
138	0.270454000	210.72.21.11	24.6.173.220	TCP		__conversation	80 → 61601 [ACK] Seq=2921 Ack=268 Win=6912 Len=1460 [TCP segment of a reassembled
139	0.002220000	210.72.21.11	24.6.173.220	HTTP		__conversation	HTTP/1.1 200 OK (text/javascript)
140	0.000125000	24.6.173.220	210.72.21.11	TCP		__conversation	61601 → 80 [ACK] Seq=268 Ack=4742 Win=65700 Len=0
141	0.140393000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61604 [ACK] Seq=7696 Ack=309 Win=5504 Len=1460 [TCP segment of a reassembled
142	0.001012000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61604 [ACK] Seq=9156 Ack=309 Win=5504 Len=1460 [TCP segment of a reassembled
143	0.000091000	24.6.173.220	209.177.86.18	TCP		HTTP	61604 → 80 [ACK] Seq=309 Ack=10616 Win=65700 Len=0
144	0.000752000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61604 [ACK] Seq=10616 Ack=309 Win=5504 Len=1460 [TCP segment of a reassembled
145	0.000865000	209.177.86.18	24.6.173.220	TCP		HTTP	80 → 61604 [ACK] Seq=12076 Ack=309 Win=5504 Len=1460 [TCP segment of a reassembled

LABORATORIO 28

Wireshark · Reglas de coloreado wireshark101

Nombre	Filtro
<input checked="" type="checkbox"/> T-retransmissions	tcp.analysis.retransmission
<input checked="" type="checkbox"/> S-FTP arguments	ftp.request.arg
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3 icmpv6.type eq 4
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.4 && ip.ttl < 5 && !ipim && !ospf) (ip.dst == 224.0.0.24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp carp))
<input checked="" type="checkbox"/> Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.status=="Bad" mstp.checksum.status=="Bad"
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal sysdig

Doble clic para editar. Arrastrar para mover. Las reglas son procesadas en orden hasta que una coincidencia es encontrada.

+ - Primer plano Fondo Aplicar como filtro

C:\Users\mikes\AppData\Roaming\Wireshark\profiles\wireshark101\colorfilters

Aceptar Copiar desde Cancelar Import... Export... Ayuda

LABORATORIO 28B

net-lost-route.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Source	Destination	Protocol	Host	Coloring Rule Name	Info
1	161.58.73.170	12.234.12.108	TCP		HTTP	80 → 1124 [PSH, ACK] Seq=1 Ack=1 Win=49152 Len=1305 [TCP segment of a reassembled PDU]
2	161.58.73.170	12.234.12.108	HTTP		HTTP	HTTP/1.0 401 Authorization Required (text/html)
3	12.234.12.108	161.58.73.170	TCP		HTTP	1124 → 80 [ACK] Seq=1 Ack=1307 Win=63207 Len=0
4	12.234.12.108	161.58.73.170	TCP		HTTP	1124 → 80 [FIN, ACK] Seq=1 Ack=1307 Win=63207 Len=0
5	12.234.12.108	161.58.73.170	TCP		HTTP	1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
6	161.58.73.170	12.234.12.108	TCP		HTTP	80 → 1124 [ACK] Seq=1307 Ack=2 Win=49152 Len=0
7	12.234.12.108	161.58.73.170	TCP		T-retransmiss...	[TCP Retransmission] 1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
8	12.234.12.108	161.58.73.170	TCP		T-retransmiss...	[TCP Retransmission] 1125 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
9	161.58.73.170	12.234.12.108	TCP		HTTP	80 → 1125 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
10	12.234.12.108	161.58.73.170	TCP		HTTP	1125 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0
11	12.234.12.108	161.58.73.170	HTTP	www.packet-level...	HTTP	GET /stats HTTP/1.1
12	161.58.73.170	12.234.12.108	TCP		HTTP	80 → 1125 [ACK] Seq=1 Ack=382 Win=49152 Len=0
13	161.58.73.170	12.234.12.108	TCP		HTTP	80 → 1125 [PSH, ACK] Seq=1 Ack=382 Win=49152 Len=507 [TCP segment of a reassembled PDU]
14	161.58.73.170	12.234.12.108	HTTP		HTTP	HTTP/1.0 301 Moved Permanently (text/html)
15	12.234.12.108	161.58.73.170	TCP		HTTP	1125 → 80 [ACK] Seq=382 Ack=509 Win=64005 Len=0
16	12.234.12.108	161.58.73.170	TCP		HTTP	1125 → 80 [FIN, ACK] Seq=382 Ack=509 Win=64005 Len=0
17	12.234.12.108	161.58.73.170	TCP		HTTP	1126 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
18	161.58.73.170	12.234.12.108	TCP		HTTP	80 → 1126 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SACK_PERM=1
19	12.234.12.108	161.58.73.170	TCP		HTTP	1126 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0

LABORATORIO 29

http-mistraffic101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.request.uri contains "exe"

No.	Source	Destination	Protocol	Host	Coloring Rule Name	Info
211	24.6.181.160	107.6.133.250	HTTP	downloads.metasploit...	HTTP	GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1

< >

> Frame 211: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface unknown, id 0
> Ethernet II, Src: Flextron_40:d6:91 (00:21:cc:40:d6:91), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.181.160, Dst: 107.6.133.250
> Transmission Control Protocol, Src Port: 1266, Dst Port: 80, Seq: 1, Ack: 1, Len: 701
▼ Hypertext Transfer Protocol
 > GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1\r\n Accept: text/html, application/xhtml+xml, */*\r\n Referer: http://www.metasploit.com/download/\r\n Accept-Language: en-US\r\n User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)\r\n Accept-Encoding: gzip, deflate\r\n Host: downloads.metasploit.com\r\n

0000 00 01 5c 31 bb c1 00 21 cc 40 d6 91 08 00 45 00 ..\r\n0010 02 e5 0f f6 40 00 80 06 29 76 18 06 b5 a0 6b 06 ..@..\r\n0020 85 fa 04 f2 00 50 97 7c eb 8a bc 0b 71 f6 50 18 ..P| ..q.P.\r\n0030 40 29 82 3f 00 00 47 45 54 20 2f 64 61 74 61 2f @) ?..GE T /data/\r\n0040 72 65 6c 61 73 65 73 2f 6d 65 74 61 73 70 6c releases /metasploit-latest-windows-installer.exe\r\n0050 6f 69 74 2d 6c 61 74 65 73 74 2d 77 69 6e 64 6f oit-late st-windo\r\n0060 77 73 2d 69 6e 73 74 61 6c 6c 65 72 2e 65 78 65 ws-installer.exe

Paquetes: 682 · Mostrado: 1 (0.1%)

Perfil: wireshark101

LABORATORIO 29B

http-mistraffic101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

(ip.addr eq 24.6.181.160 and ip.addr eq 107.6.133.250) and (tcp.port eq 1266 and tcp.port eq 80)

No.	Source	Destination	Protocol	Host	Coloring Rule Name	Info
208	24.6.181.160	107.6.133.250	TCP		HTTP	1266 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
209	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
210	24.6.181.160	107.6.133.250	TCP		HTTP	1266 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
211	24.6.181.160	107.6.133.250	HTTP	downloads.metasploit...	HTTP	GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1
212	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=1 Ack=702 Win=7296 Len=0
213	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=1 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
214	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=1461 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
215	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=2921 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
216	24.6.181.160	107.6.133.250	TCP		HTTP	1266 → 80 [ACK] Seq=702 Ack=4381 Win=65700 Len=0
217	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=4381 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
218	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=5841 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
219	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=7301 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
220	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=8761 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
221	24.6.181.160	107.6.133.250	TCP		HTTP	1266 → 80 [ACK] Seq=702 Ack=10221 Win=65700 Len=0
222	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=10221 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
223	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=11681 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
224	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=13141 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
225	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=14601 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
226	107.6.133.250	24.6.181.160	TCP		HTTP	80 → 1266 [ACK] Seq=16061 Ack=702 Win=7296 Len=1460 [TCP segment of a reassembled PDU]

> Frame 211: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface unknown, id 0
> Ethernet II, Src: Flextron_40:d6:91 (00:21:cc:40:d6:91), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.181.160, Dst: 107.6.133.250
> Transmission Control Protocol, Src Port: 1266, Dst Port: 80, Seq: 1, Ack: 1, Len: 701
✓ Hypertext Transfer Protocol
> GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1\r\nAccept: text/html, application/xhtml+xml, /*\r\nReferer: http://www.metasploit.com/download/\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0.)\r\nAccept-Encoding: gzip, deflate\r\n

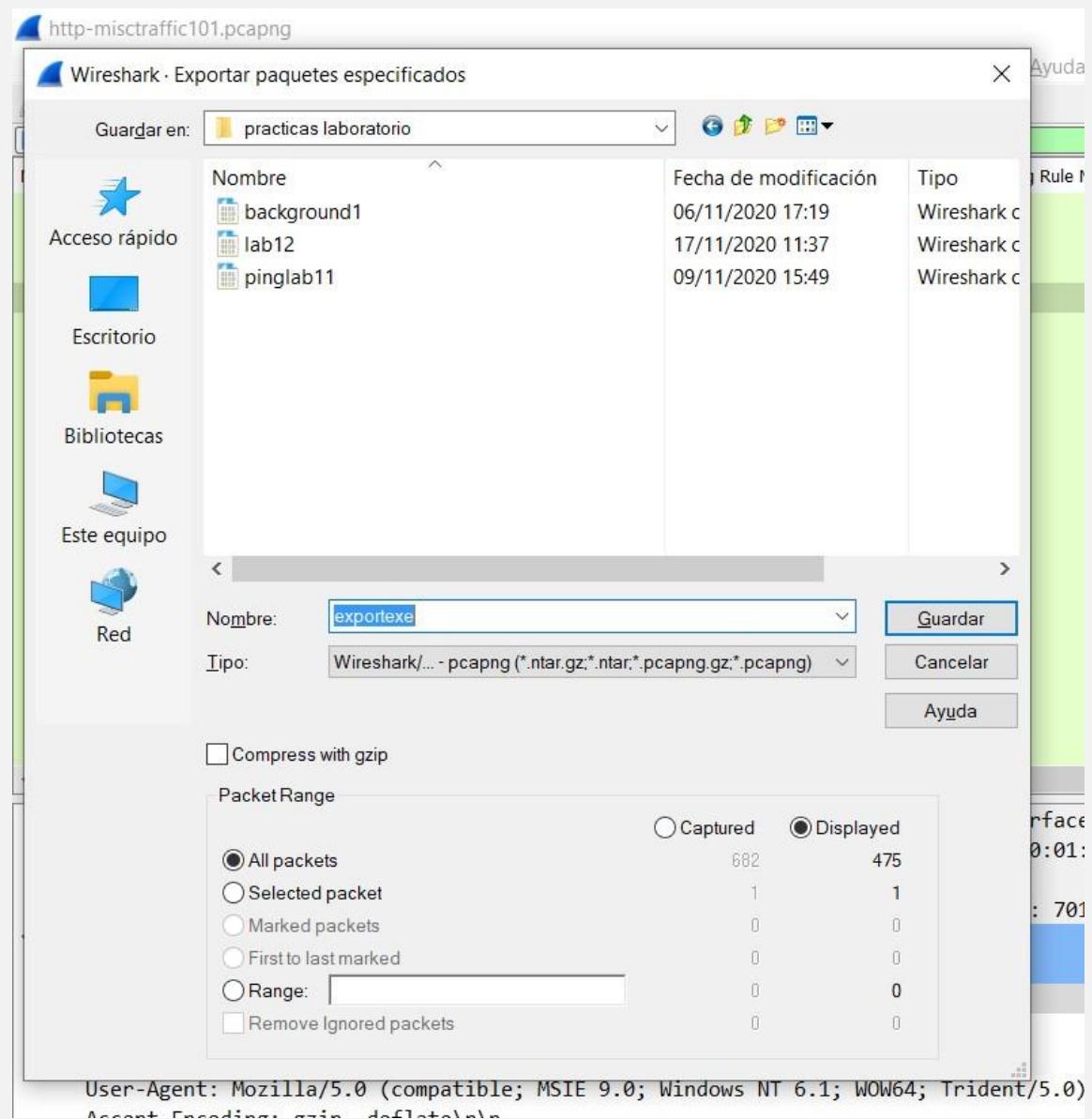
0070 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 HTTP/1.1..Accept
0080 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
0090 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
00a0 78 6d 6c 2c 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 xml, /* ..Refere
00b0 72 3a 20 68 74 74 70 3a 2f 77 77 2e 6d 65 r: http: //www.me
00c0 74 61 73 70 6c 6f 69 74 2e 63 6f 6d 2f 64 6f 77 taspoil.../dow
00d0 6e 6c 6f 61 64 2f 0d 0a 41 63 63 65 70 74 2d 4c nload/.. Accept-L

HTTP Accept (http.accept), 47 byte(s)

Paquetes: 682 · Mostrado: 475 (69.6%)

Perfil: wireshark101

LABORATORIO 29C



LABORATORIO 30

http.host

No.	Source	Destination	Protocol	Host	Coloring Rule Name	Info
8	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET / HTTP/1.1
11	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET /unique/track.js?referrer-about%3Abank HTTP/1.1
14	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET /?pagesection=body HTTP/1.1
18	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET /?pagesection=forsale HTTP/1.1
25	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET /common/fabulousdomains/skins/fab/images/banner/fabulous_sale_bottom.gif HTTP/1.1
26	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET /common/fabulousdomains/skins/fab/images/banner/sale_buynow.png HTTP/1.1
35	24.6.173.220	208.48.81.133	HTTP	www.freewebsites...	HTTP	GET /common/fabulousdomains/skins/fab/images/banner/sale_bg.png HTTP/1.1
39	24.6.173.220	50.57.118.49	HTTP	www.domainnames.c...	HTTP	GET / HTTP/1.1
53	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET / HTTP/1.1
78	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /style/style.css HTTP/1.1
79	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /style/dropdown.css HTTP/1.1
82	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/jquery-1.4.4.js HTTP/1.1
85	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/cufon-yui.js HTTP/1.1
88	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/Aller_400-Aller_700.font.js HTTP/1.1
90	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/Aller_Light_400.font.js HTTP/1.1
101	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/jquery.cycle.main.js HTTP/1.1
128	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/jquery.cycle.plugin.js HTTP/1.1
143	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/fancybox/jquery.mousewheel-3.0.4.pack.js HTTP/1.1
150	24.6.173.220	50.57.118.49	HTTP	domainnames.com.au	HTTP	GET /js/fancybox/jquery.fancybox-1.3.4.pack.js HTTP/1.1

> Frame 8: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, 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: 208.48.81.133
> Transmission Control Protocol, Src Port: 21180, Dst Port: 80, Seq: 1, Ack: 1, Len: 297

HyperText Transfer Protocol
> GET / HTTP/1.1\r\nHost: www.freewebsites.com.au\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n

Hex	Dec	Text
0000	00 01 5c 31 bb c1 d4 85	..`1.... d.....E.
0010	64 a7 bf a3 08 00 45 00	..Qb;@.....0
0020	01 51 62 3b 40 00 80 06	Q-R-P., `..;P.
0030	00 00 18 06 ad dc d0 30	@.....GE T / HTTP
0040	51 85 52 bc 00 50 14 2c	/1.1-Ho st: www.
0050	7c b7 60 ab 14 3b 50 18	freewebs ites.com
0060	54 20 2f 20 48 54 54 50	.au..Use r-Agent:
0070	2f 31 2e 31 0d 0a 48 6f	
0080	73 74 3a 20 77 77 77 2e	
0090	69 74 65 73 2e 63 6f 6d	
00a0	72 2d 41 67 65 6e 74 3a	

Host: Character string Paquetes: 854 · Mostrado: 63 (7.4%) Perfil: wireshark101