Laboratorios wireshark

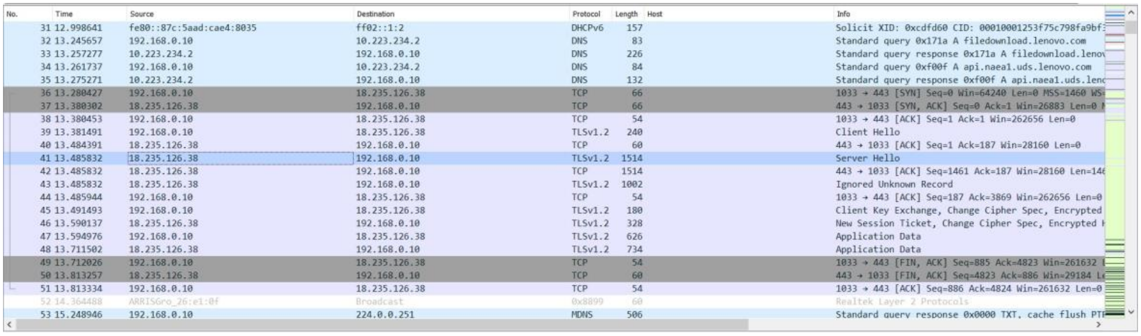
Kanxoc Ek Félix Gerardo

Profesor: Jiménez Sánchez Ismael

Instituto Tecnológico de Cancún

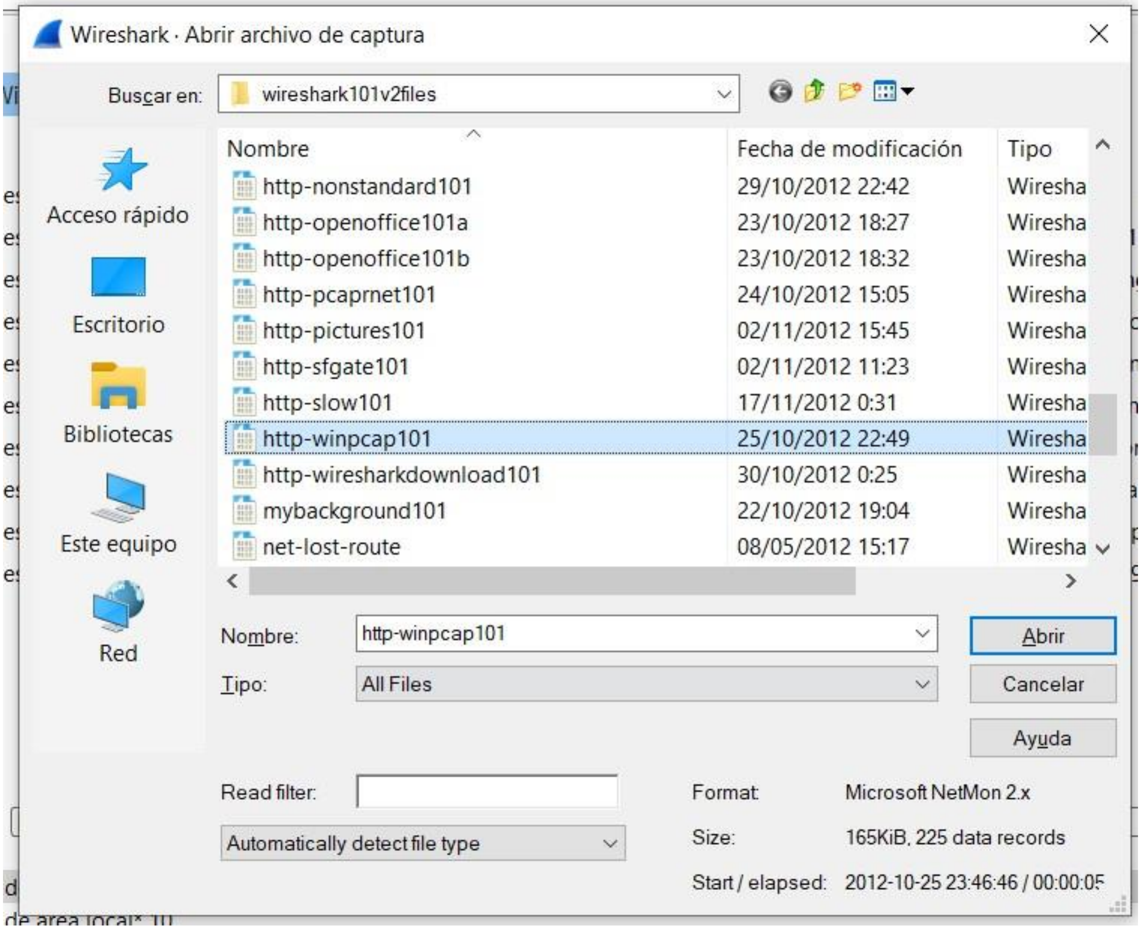
Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones



No.	Time	Source	Destination	Protocol	Length	Host	Info
31	12.998641	fe80::87c:5aad:cae4:8035	ff02::1:2	DHCPv6	157		Solicit XID: 0xcdfd60 CID: 00010001253f75c798fa9bf
32	13.245657	192.168.0.10	10.223.234.2	DNS	83		Standard query 0x171a A filedownload.lenovo.com
33	13.257277	10.223.234.2	192.168.0.10	DNS	226		Standard query response 0x171a A filedownload.leno
34	13.261737	192.168.0.10	10.223.234.2	DNS	84		Standard query 0xf00f A api.naea1.uds.lenovo.com
35	13.275271	10.223.234.2	192.168.0.10	DNS	132		Standard query response 0xf00f A api.naea1.uds.len
36	13.280427	192.168.0.10	18.235.126.38	TCP	66		1033 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
37	13.380302	18.235.126.38	192.168.0.10	TCP	66		443 → 1033 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0
38	13.380453	192.168.0.10	18.235.126.38	TCP	54		1033 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
39	13.381491	192.168.0.10	18.235.126.38	TLSv1.2	240		Client Hello
40	13.484391	18.235.126.38	192.168.0.10	TCP	60		443 → 1033 [ACK] Seq=1 Ack=187 Win=28160 Len=0
41	13.485832	18.235.126.38	192.168.0.10	TLSv1.2	1514		Server Hello
42	13.485832	18.235.126.38	192.168.0.10	TCP	1514		443 → 1033 [ACK] Seq=1461 Ack=187 Win=28160 Len=14
43	13.485832	18.235.126.38	192.168.0.10	TLSv1.2	1002		Ignored Unknown Record
44	13.485944	192.168.0.10	18.235.126.38	TCP	54		1033 → 443 [ACK] Seq=187 Ack=3869 Win=262656 Len=0
45	13.491493	192.168.0.10	18.235.126.38	TLSv1.2	180		Client Key Exchange, Change Cipher Spec, Encrypted
46	13.590137	18.235.126.38	192.168.0.10	TLSv1.2	328		New Session Ticket, Change Cipher Spec, Encrypted
47	13.594976	192.168.0.10	18.235.126.38	TLSv1.2	626		Application Data
48	13.711502	18.235.126.38	192.168.0.10	TLSv1.2	734		Application Data
49	13.712026	192.168.0.10	18.235.126.38	TCP	54		1033 → 443 [FIN, ACK] Seq=885 Ack=4823 Win=261632
50	13.813257	18.235.126.38	192.168.0.10	TCP	60		443 → 1033 [FIN, ACK] Seq=4823 Ack=886 Win=29184 L
51	13.813334	192.168.0.10	18.235.126.38	TCP	54		1033 → 443 [ACK] Seq=886 Ack=4824 Win=261632 Len=0
52	14.364488	ARRISGro_26:e1:0f	Broadcast	0x8899	60		Realtek Layer 2 Protocols
53	15.248946	192.168.0.10	224.0.0.251	MDNS	506		Standard query response 0x0000 TXT, cache flush PT

Ilustración 1 Laboratorio2



Buscar en: wireshark101v2files

Nombre	Fecha de modificación	Tipo
http-nonstandard101	29/10/2012 22:42	Wiresha
http-openoffice101a	23/10/2012 18:27	Wiresha
http-openoffice101b	23/10/2012 18:32	Wiresha
http-pcaprnet101	24/10/2012 15:05	Wiresha
http-pictures101	02/11/2012 15:45	Wiresha
http-sfgate101	02/11/2012 11:23	Wiresha
http-slow101	17/11/2012 0:31	Wiresha
http-winpcap101	25/10/2012 22:49	Wiresha
http-wiresharkdownload101	30/10/2012 0:25	Wiresha
mybackground101	22/10/2012 19:04	Wiresha
net-lost-route	08/05/2012 15:17	Wiresha

Nombre: http-winpcap101

Tipo: All Files

Read filter:

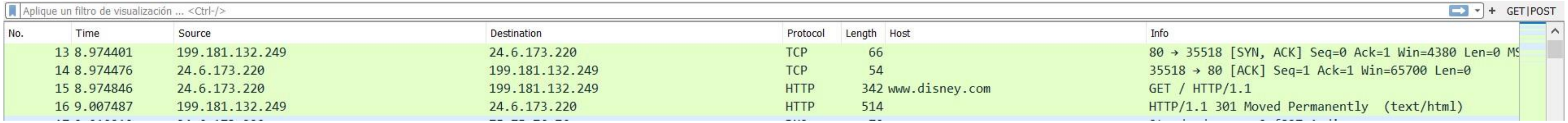
Automatically detect file type

Format: Microsoft NetMon 2.x

Size: 165KiB, 225 data records

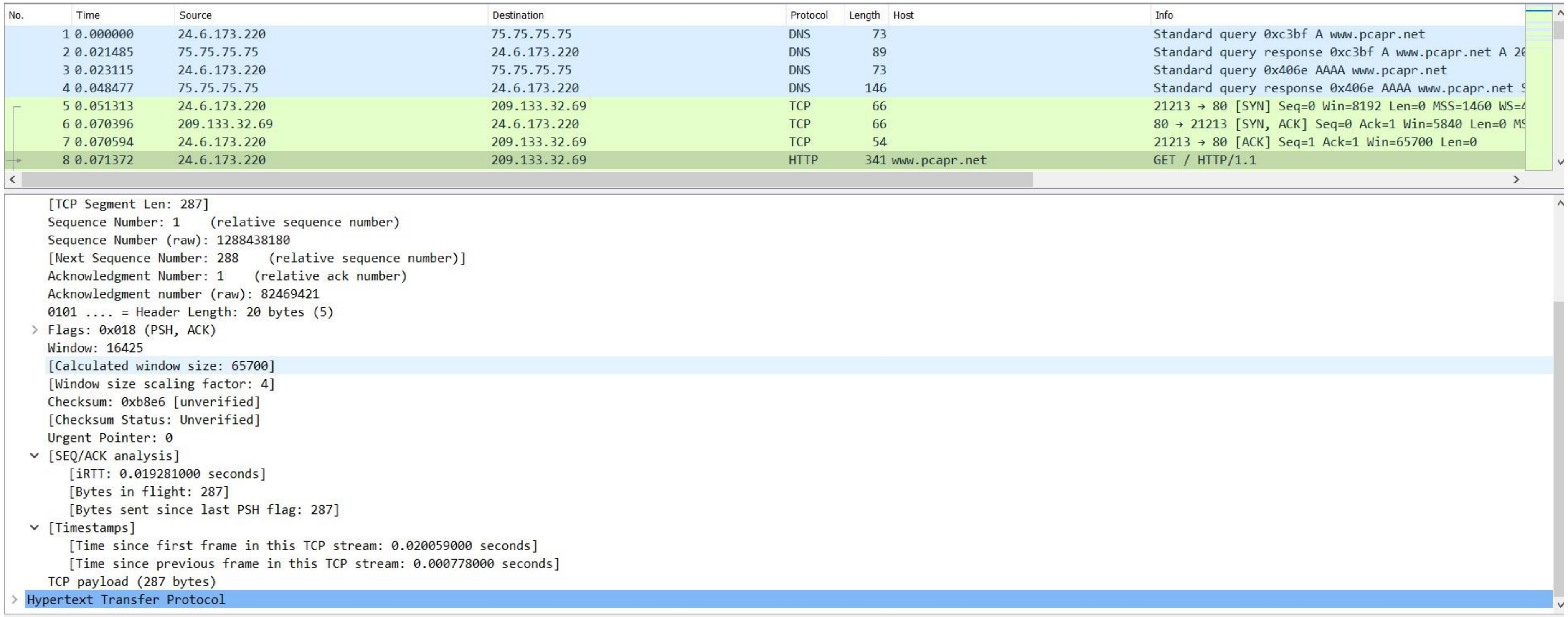
Start / elapsed: 2012-10-25 23:46:46 / 00:00:05

Ilustración 2 Laboratorio3



```
No.   Time      Source            Destination       Protocol  Length  Host            Info
   13 8.974401  199.181.132.249   24.6.173.220      TCP         66                    80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MS
   14 8.974476  24.6.173.220      199.181.132.249   TCP         54                    35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   15 8.974846  24.6.173.220      199.181.132.249   HTTP       342  www.disney.com    GET / HTTP/1.1
   16 9.007487  199.181.132.249   24.6.173.220      HTTP       514                    HTTP/1.1 301 Moved Permanently  (text/html)
```

Ilustración 3 Laboratorio4



```
No.   Time      Source          Destination     Protocol  Length  Host           Info
    1 0.000000  24.6.173.220    75.75.75.75     DNS         73                   Standard query 0xc3bf A www.pcapr.net
    2 0.021485  75.75.75.75     24.6.173.220    DNS         89                   Standard query response 0xc3bf A www.pcapr.net A 20
    3 0.023115  24.6.173.220    75.75.75.75     DNS         73                   Standard query 0x406e AAAA www.pcapr.net
    4 0.048477  75.75.75.75     24.6.173.220    DNS        146                   Standard query response 0x406e AAAA www.pcapr.net S
    5 0.051313  24.6.173.220    209.133.32.69   TCP         66                   21213 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
    6 0.070396  209.133.32.69   24.6.173.220    TCP         66                   80 → 21213 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS
    7 0.070594  24.6.173.220    209.133.32.69   TCP         54                   21213 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
    8 0.071372  24.6.173.220    209.133.32.69   HTTP       341  www.pcapr.net    GET / HTTP/1.1
```

```
    [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]
    TCP payload (287 bytes)
> Hypertext Transfer Protocol
```

Ilustración 4 Laboratorio5

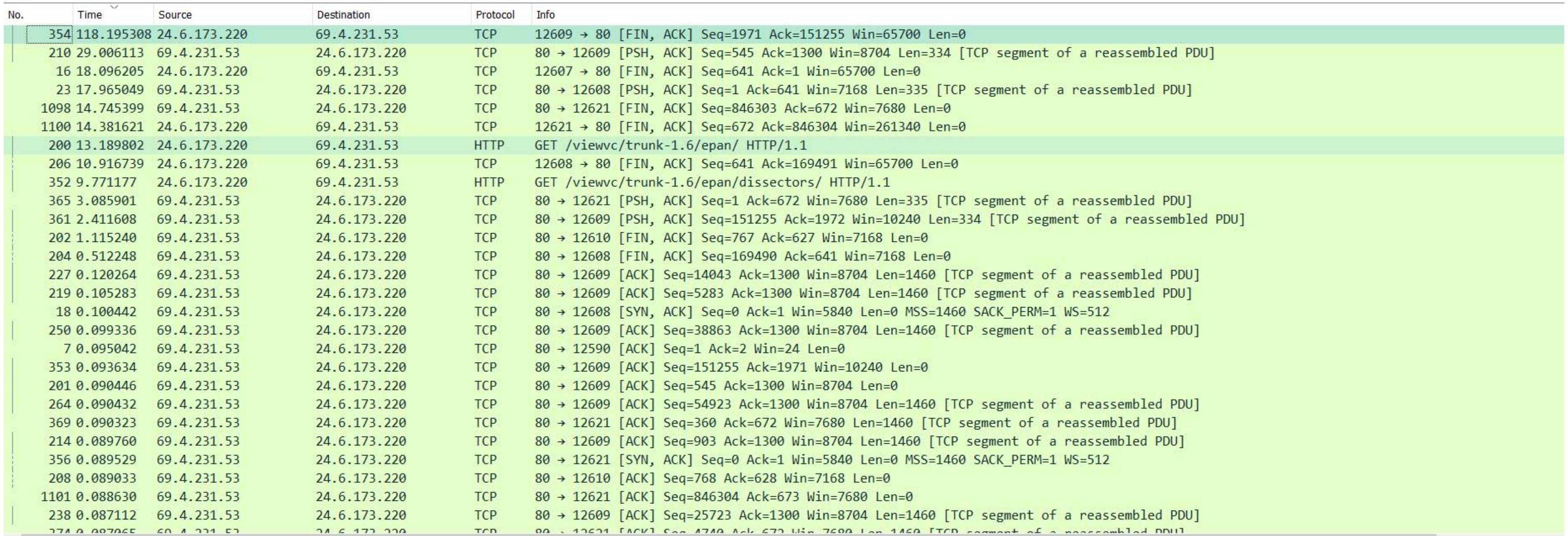
Descubrir

User's Guide · Wiki · Questions and Answers · Mailing Lists

Está ejecutando Wireshark3.4.0 (v3.4.0-0-g9733f173ea5e).Recibe actualizaciones automáticas.

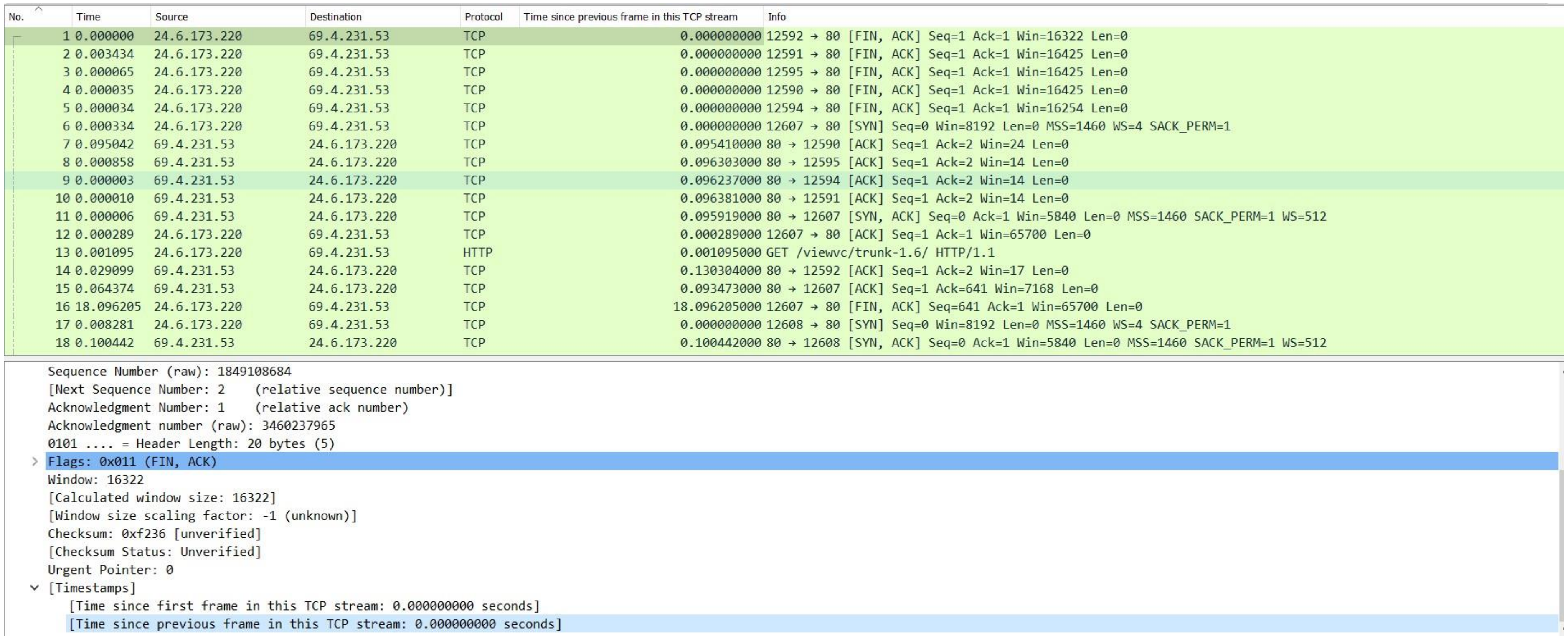
Preparado para cargar o capturar | No hay paquetes | Perfil: wireshark101

Ilustración 5 Laboratorio6



```
No.   Time       Source        Destination   Protocol 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     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     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
1101 0.088630   69.4.231.53   24.6.173.220  TCP      80 → 12621 [ACK] Seq=846304 Ack=673 Win=7680 Len=0
 238 0.087112   69.4.231.53   24.6.173.220  TCP      80 → 12609 [ACK] Seq=25723 Ack=1300 Win=8704 Len=1460 [TCP segment of a reassembled PDU]
 374 0.087065   69.4.231.53   24.6.173.220  TCP      80 → 12621 [ACK] Seq=4740 Ack=672 Win=7680 Len=1460 [TCP segment of a reassembled PDU]
```

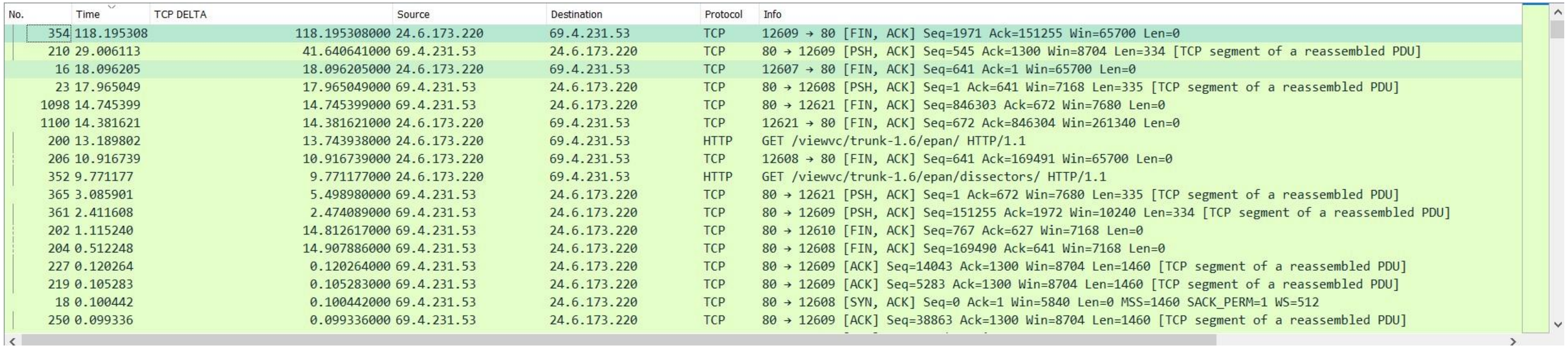
Ilustración 6 Laboratorio8



No.	Time	Source	Destination	Protocol	Time since previous frame in this TCP stream	Info
1	0.000000	24.6.173.220	69.4.231.53	TCP	0.000000000	12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
2	0.003434	24.6.173.220	69.4.231.53	TCP	0.000000000	12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
3	0.000065	24.6.173.220	69.4.231.53	TCP	0.000000000	12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
4	0.000035	24.6.173.220	69.4.231.53	TCP	0.000000000	12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
5	0.000034	24.6.173.220	69.4.231.53	TCP	0.000000000	12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
6	0.000334	24.6.173.220	69.4.231.53	TCP	0.000000000	12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	0.095042	69.4.231.53	24.6.173.220	TCP	0.095410000	80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
8	0.000858	69.4.231.53	24.6.173.220	TCP	0.096303000	80 → 12595 [ACK] Seq=1 Ack=2 Win=14 Len=0
9	0.000003	69.4.231.53	24.6.173.220	TCP	0.096237000	80 → 12594 [ACK] Seq=1 Ack=2 Win=14 Len=0
10	0.000010	69.4.231.53	24.6.173.220	TCP	0.096381000	80 → 12591 [ACK] Seq=1 Ack=2 Win=14 Len=0
11	0.000006	69.4.231.53	24.6.173.220	TCP	0.095919000	80 → 12607 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
12	0.000289	24.6.173.220	69.4.231.53	TCP	0.000289000	12607 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
13	0.001095	24.6.173.220	69.4.231.53	HTTP	0.001095000	GET /viewvc/trunk-1.6/ HTTP/1.1
14	0.029099	69.4.231.53	24.6.173.220	TCP	0.130304000	80 → 12592 [ACK] Seq=1 Ack=2 Win=17 Len=0
15	0.064374	69.4.231.53	24.6.173.220	TCP	0.093473000	80 → 12607 [ACK] Seq=1 Ack=641 Win=7168 Len=0
16	18.096205	24.6.173.220	69.4.231.53	TCP	18.096205000	12607 → 80 [FIN, ACK] Seq=641 Ack=1 Win=65700 Len=0
17	0.008281	24.6.173.220	69.4.231.53	TCP	0.000000000	12608 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
18	0.100442	69.4.231.53	24.6.173.220	TCP	0.100442000	80 → 12608 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512

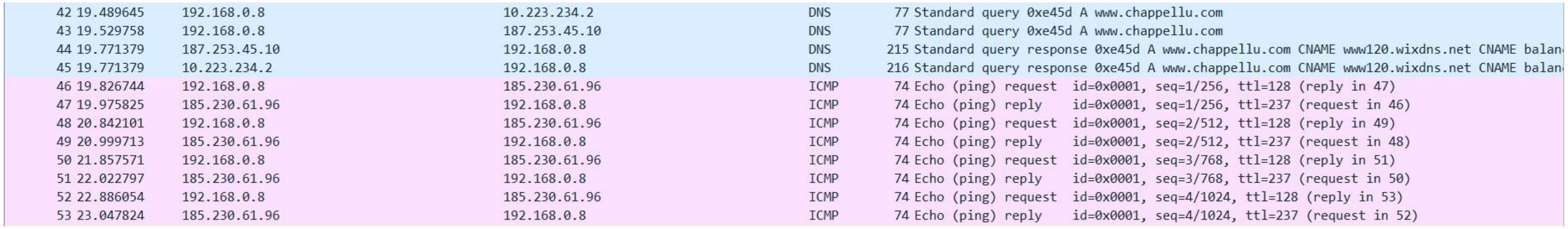
```
  Sequence Number (raw): 1849108684
  [Next Sequence Number: 2    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 3460237965
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x011 (FIN, ACK)
  Window: 16322
  [Calculated window size: 16322]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xf236 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
v [Timestamps]
     [Time since first frame in this TCP stream: 0.000000000 seconds]
     [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

Ilustración 7 Laboratorio8b



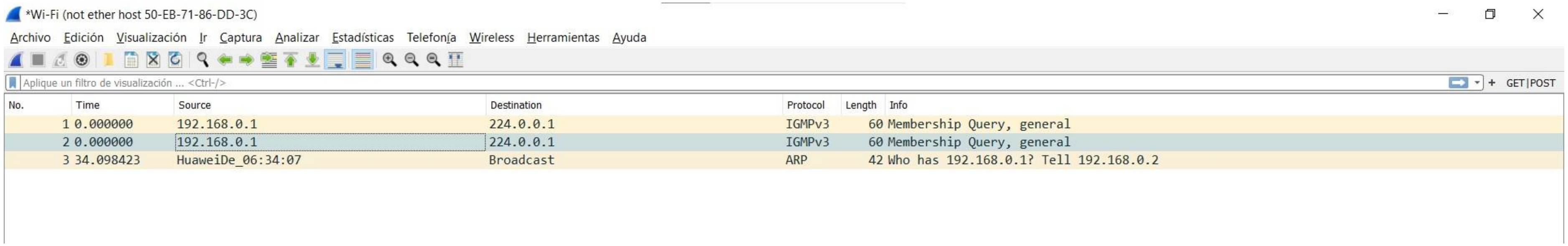
```
No.   Time        TCP DELTA          Source         Destination    Protocol  Info
 354 118.195308       118.195308000 24.6.173.220   69.4.231.53    TCP       12609 → 80 [FIN, ACK] Seq=1971 Ack=151255 Win=65700 Len=0
 210 29.006113         41.640641000 69.4.231.53    24.6.173.220   TCP       80 → 12609 [PSH, ACK] Seq=545 Ack=1300 Win=8704 Len=334 [TCP segment of a reassembled PDU]
  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
  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]
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      GET /viewvc/trunk-1.6/epan/ HTTP/1.1
 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      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]
 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
 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
 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
 250 0.099336           0.099336000 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]
```

Ilustración 8 Laboratorio8c



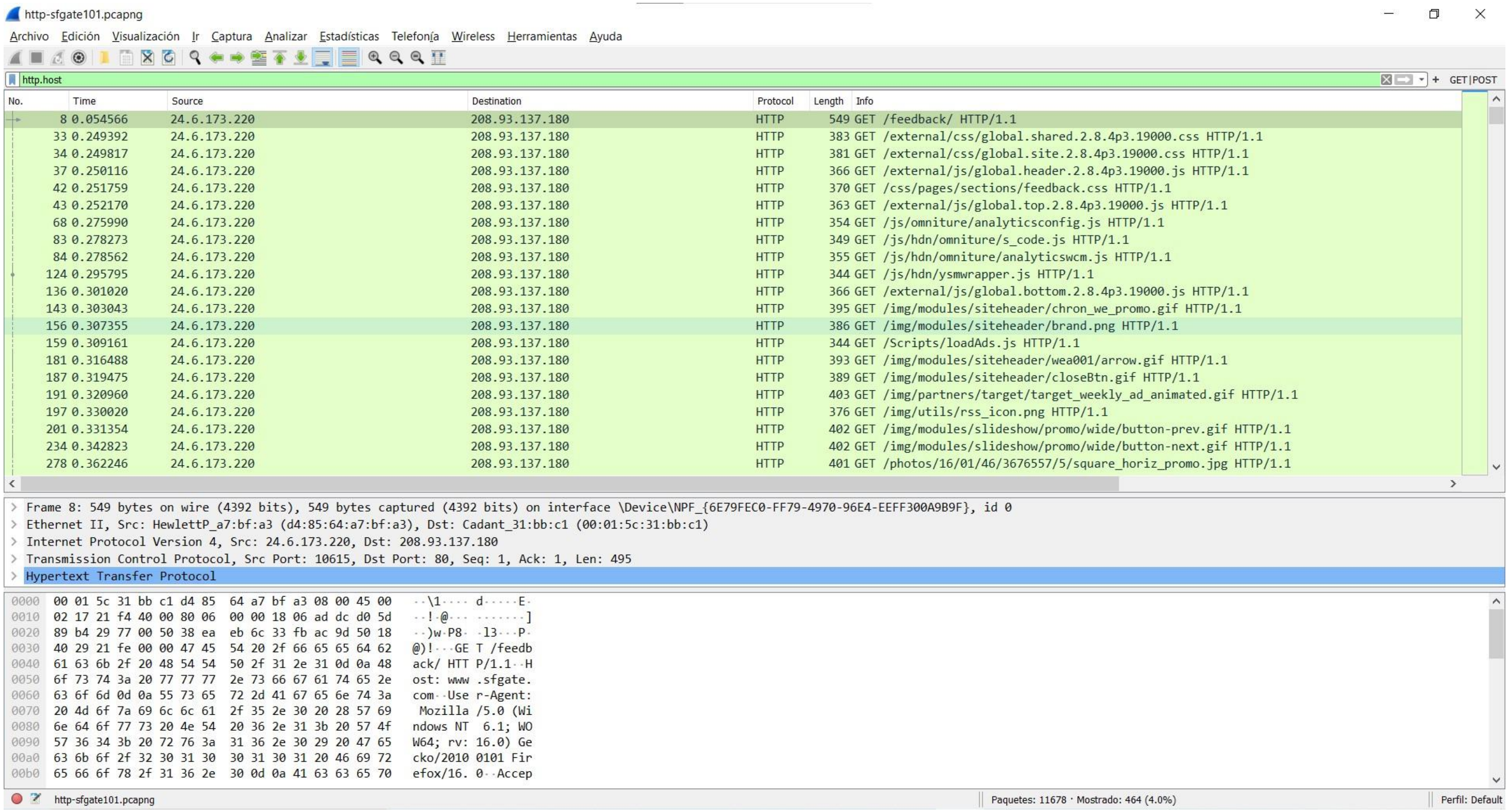
```
42 19.489645   192.168.0.8      10.223.234.2     DNS    77 Standard query 0xe45d A www.chappellu.com
43 19.529758   192.168.0.8      187.253.45.10    DNS    77 Standard query 0xe45d A www.chappellu.com
44 19.771379   187.253.45.10    192.168.0.8      DNS   215 Standard query response 0xe45d A www.chappellu.com CNAME www120.wixdns.net CNAME balan
45 19.771379   10.223.234.2     192.168.0.8      DNS   216 Standard query response 0xe45d A www.chappellu.com CNAME www120.wixdns.net CNAME balan
46 19.826744   192.168.0.8      185.230.61.96    ICMP   74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 47)
47 19.975825   185.230.61.96    192.168.0.8      ICMP   74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=237 (request in 46)
48 20.842101   192.168.0.8      185.230.61.96    ICMP   74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 49)
49 20.999713   185.230.61.96    192.168.0.8      ICMP   74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=237 (request in 48)
50 21.857571   192.168.0.8      185.230.61.96    ICMP   74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 51)
51 22.022797   185.230.61.96    192.168.0.8      ICMP   74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=237 (request in 50)
52 22.886054   192.168.0.8      185.230.61.96    ICMP   74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 53)
53 23.047824   185.230.61.96    192.168.0.8      ICMP   74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=237 (request in 52)
```

Ilustración 9 Laboratorio11


*Wi-Fi (not ether host 50-EB-71-86-DD-3C)
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
GET|POST

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
2	0.000000	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
3	34.098423	HuaweiDe_06:34:07	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2

Ilustración 10 Laboratorio12



```
http.host
```

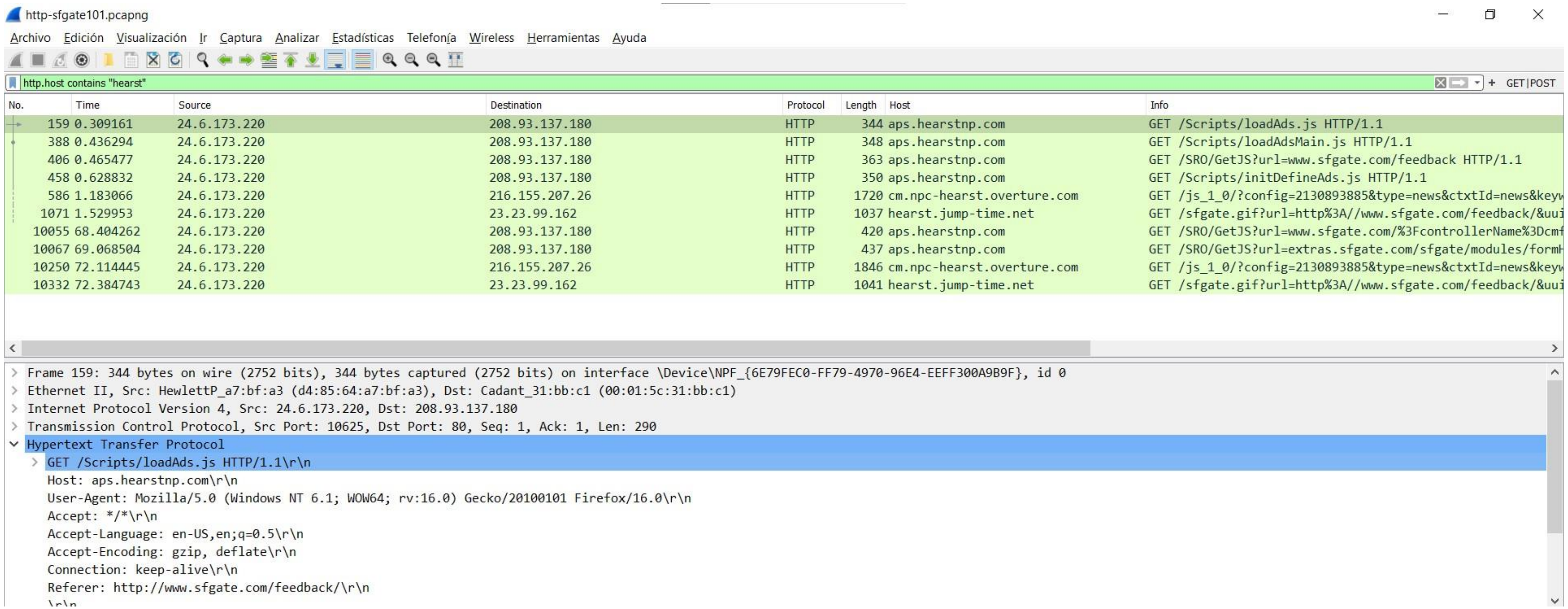
```
No.   Time      Source         Destination      Protocol  Length Info
    8 0.054566  24.6.173.220   208.93.137.180   HTTP      549 GET /feedback/ HTTP/1.1
   33 0.249392  24.6.173.220   208.93.137.180   HTTP      383 GET /external/css/global.shared.2.8.4p3.19000.css HTTP/1.1
   34 0.249817  24.6.173.220   208.93.137.180   HTTP      381 GET /external/css/global.site.2.8.4p3.19000.css HTTP/1.1
   37 0.250116  24.6.173.220   208.93.137.180   HTTP      366 GET /external/js/global.header.2.8.4p3.19000.js HTTP/1.1
   42 0.251759  24.6.173.220   208.93.137.180   HTTP      370 GET /css/pages/sections/feedback.css HTTP/1.1
   43 0.252170  24.6.173.220   208.93.137.180   HTTP      363 GET /external/js/global.top.2.8.4p3.19000.js HTTP/1.1
   68 0.275990  24.6.173.220   208.93.137.180   HTTP      354 GET /js/omniture/analyticsconfig.js HTTP/1.1
   83 0.278273  24.6.173.220   208.93.137.180   HTTP      349 GET /js/hdn/omniture/s_code.js HTTP/1.1
   84 0.278562  24.6.173.220   208.93.137.180   HTTP      355 GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
  124 0.295795  24.6.173.220   208.93.137.180   HTTP      344 GET /js/hdn/ysmwrapper.js HTTP/1.1
  136 0.301020  24.6.173.220   208.93.137.180   HTTP      366 GET /external/js/global.bottom.2.8.4p3.19000.js HTTP/1.1
  143 0.303043  24.6.173.220   208.93.137.180   HTTP      395 GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
  156 0.307355  24.6.173.220   208.93.137.180   HTTP      386 GET /img/modules/siteheader/brand.png HTTP/1.1
  159 0.309161  24.6.173.220   208.93.137.180   HTTP      344 GET /Scripts/loadAds.js HTTP/1.1
  181 0.316488  24.6.173.220   208.93.137.180   HTTP      393 GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1
  187 0.319475  24.6.173.220   208.93.137.180   HTTP      389 GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
  191 0.320960  24.6.173.220   208.93.137.180   HTTP      403 GET /img/partners/target/target_weekly_ad_animated.gif HTTP/1.1
  197 0.330020  24.6.173.220   208.93.137.180   HTTP      376 GET /img/utils/rss_icon.png HTTP/1.1
  201 0.331354  24.6.173.220   208.93.137.180   HTTP      402 GET /img/modules/slideshow/promo/wide/button-prev.gif HTTP/1.1
  234 0.342823  24.6.173.220   208.93.137.180   HTTP      402 GET /img/modules/slideshow/promo/wide/button-next.gif HTTP/1.1
  278 0.362246  24.6.173.220   208.93.137.180   HTTP      401 GET /photos/16/01/46/3676557/5/square_horiz_promo.jpg HTTP/1.1
```

```
> Frame 8: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 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
0050  6f 73 74 3a 20 77 77 77  2e 73 66 67 61 74 65 2e   ost: 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
0090  57 36 34 3b 20 72 76 3a  31 36 2e 30 29 20 47 65   W64; rv: 16.0) Ge
00a0  63 6b 6f 2f 32 30 31 30  30 31 30 31 20 46 69 72   cko/2010 0101 Fir
00b0  65 66 6f 78 2f 31 36 2e  30 0d 0a 41 63 63 65 70   efox/16. 0··Accep
```

```
http-sfgate101.pcapng    Paquetes: 11678 · Mostrado: 464 (4.0%)    Perfil: Default
```

Ilustración 11 Laboratorio14

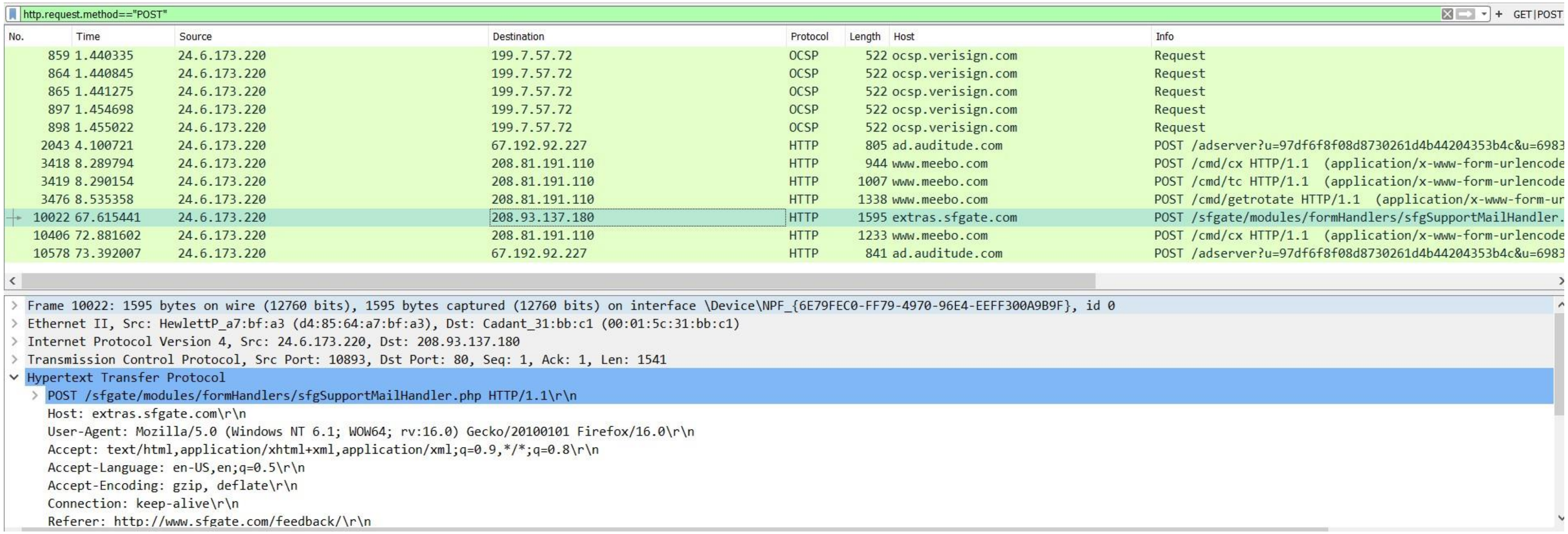

http-sfgate101.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
GET|POST

http.host contains "hearst"

No.	Time	Source	Destination	Protocol	Length	Host	Info
159	0.309161	24.6.173.220	208.93.137.180	HTTP	344	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1
388	0.436294	24.6.173.220	208.93.137.180	HTTP	348	aps.hearstnp.com	GET /Scripts/loadAdsMain.js HTTP/1.1
406	0.465477	24.6.173.220	208.93.137.180	HTTP	363	aps.hearstnp.com	GET /SRO/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458	0.628832	24.6.173.220	208.93.137.180	HTTP	350	aps.hearstnp.com	GET /Scripts/initDefineAds.js HTTP/1.1
586	1.183066	24.6.173.220	216.155.207.26	HTTP	1720	cm.npc-hearst.overture.com	GET /js_1_0/?config=2130893885&type=news&ctxtId=news&keyw
1071	1.529953	24.6.173.220	23.23.99.162	HTTP	1037	hearst.jump-time.net	GET /sfgate.gif?url=http%3A//www.sfgate.com/feedback/&uui
10055	68.404262	24.6.173.220	208.93.137.180	HTTP	420	aps.hearstnp.com	GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3Dcmf
10067	69.068504	24.6.173.220	208.93.137.180	HTTP	437	aps.hearstnp.com	GET /SRO/GetJS?url=extras.sfgate.com/sfgate/modules/formH
10250	72.114445	24.6.173.220	216.155.207.26	HTTP	1846	cm.npc-hearst.overture.com	GET /js_1_0/?config=2130893885&type=news&ctxtId=news&keyw
10332	72.384743	24.6.173.220	23.23.99.162	HTTP	1041	hearst.jump-time.net	GET /sfgate.gif?url=http%3A//www.sfgate.com/feedback/&uui

```
> Frame 159: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.93.137.180
> Transmission Control Protocol, Src Port: 10625, Dst Port: 80, Seq: 1, Ack: 1, Len: 290
v Hypertext Transfer Protocol
  > GET /Scripts/loadAds.js HTTP/1.1\r\n
    Host: aps.hearstnp.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.sfgate.com/feedback/\r\n
    \r\n
```

Ilustración 12 Laboratorio14b

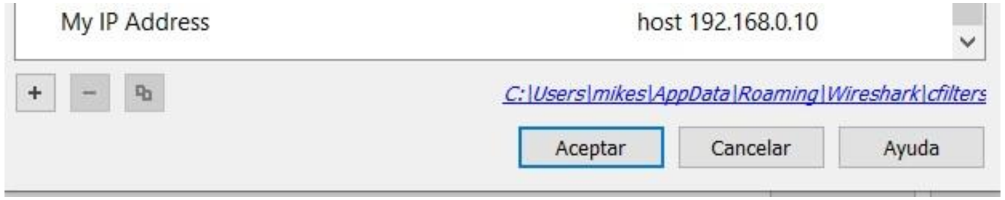


```
http.request.method=="POST"

No.    Time       Source          Destination      Protocol  Length Host               Info
  859  1.440335   24.6.173.220    199.7.57.72      OCSP       522   ocsp.verisign.com  Request
  864  1.440845   24.6.173.220    199.7.57.72      OCSP       522   ocsp.verisign.com  Request
  865  1.441275   24.6.173.220    199.7.57.72      OCSP       522   ocsp.verisign.com  Request
  897  1.454698   24.6.173.220    199.7.57.72      OCSP       522   ocsp.verisign.com  Request
  898  1.455022   24.6.173.220    199.7.57.72      OCSP       522   ocsp.verisign.com  Request
 2043  4.100721   24.6.173.220    67.192.92.227    HTTP       805   ad.auditude.com    POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=6983
 3418  8.289794   24.6.173.220    208.81.191.110   HTTP       944   www.meebo.com      POST /cmd/cx HTTP/1.1  (application/x-www-form-urlencode
 3419  8.290154   24.6.173.220    208.81.191.110   HTTP      1007   www.meebo.com      POST /cmd/tc HTTP/1.1  (application/x-www-form-urlencode
 3476  8.535358   24.6.173.220    208.81.191.110   HTTP      1338   www.meebo.com      POST /cmd/getrotate HTTP/1.1  (application/x-www-form-ur
10022 67.615441   24.6.173.220    208.93.137.180   HTTP      1595   extras.sfgate.com  POST /sfgate/modules/formHandlers/sfgSupportMailHandler.
10406 72.881602   24.6.173.220    208.81.191.110   HTTP      1233   www.meebo.com      POST /cmd/cx HTTP/1.1  (application/x-www-form-urlencode
10578 73.392007   24.6.173.220    67.192.92.227    HTTP       841   ad.auditude.com    POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=6983

> Frame 10022: 1595 bytes on wire (12760 bits), 1595 bytes captured (12760 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.93.137.180
> Transmission Control Protocol, Src Port: 10893, Dst Port: 80, Seq: 1, Ack: 1, Len: 1541
v Hypertext Transfer Protocol
  > POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1\r\n
    Host: extras.sfgate.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.sfgate.com/feedback/\r\n
```

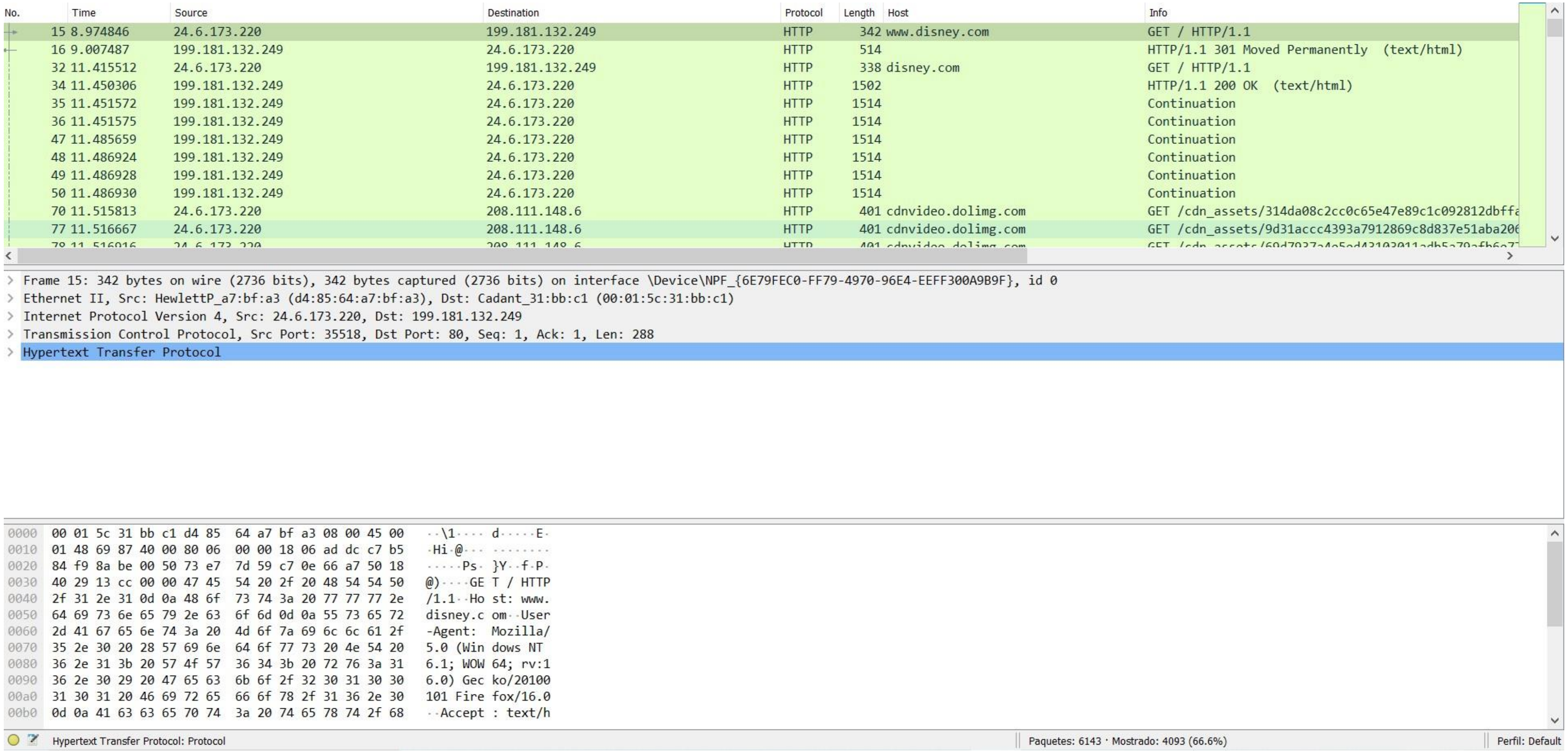
Ilustración 13 Laboratorio14c



My IP Address	host 192.168.0.10

C:\Users\mikes\AppData\Roaming\Wireshark\cfilters

Ilustración 14 Laboratorio15



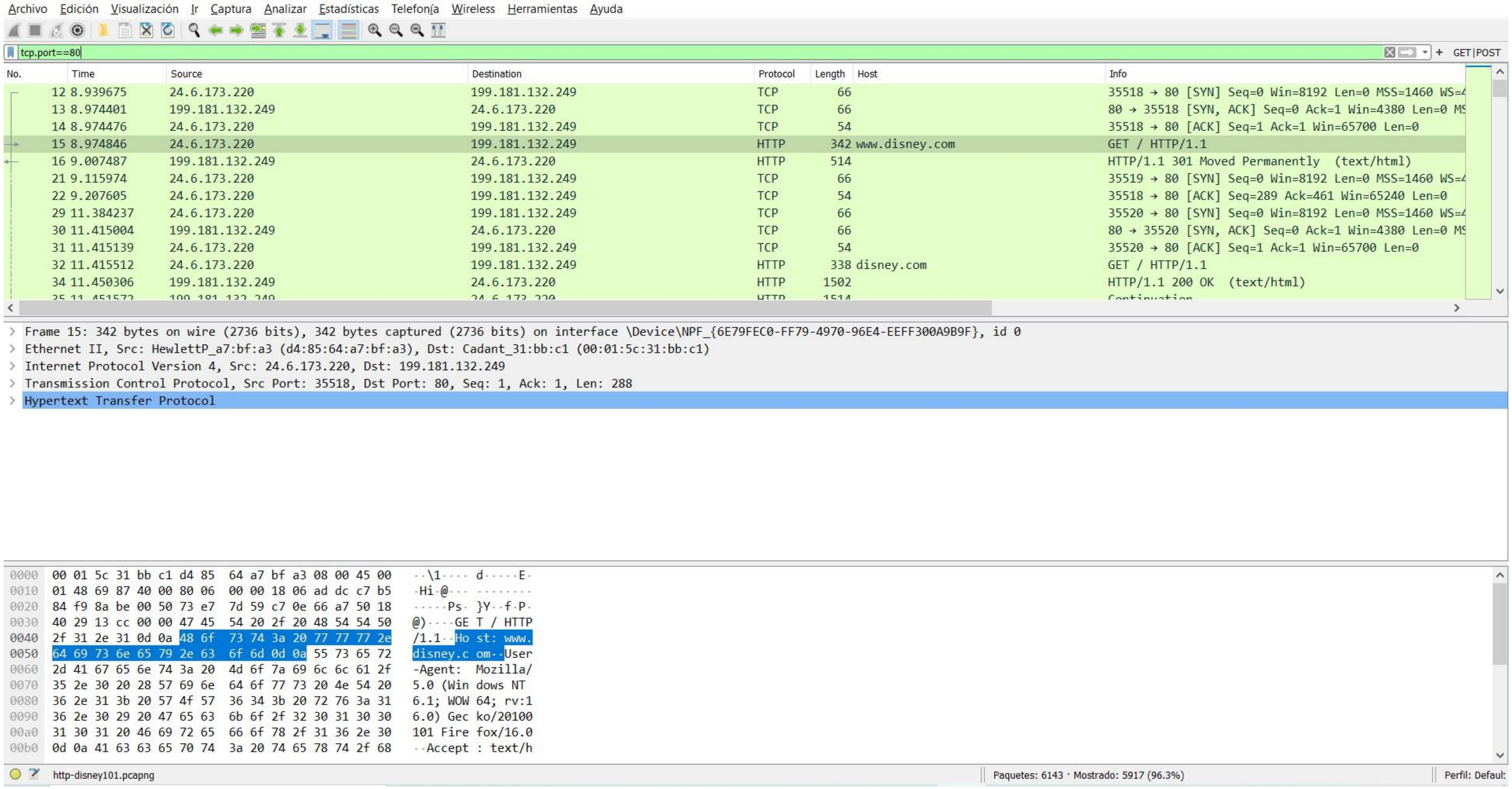
```
15 8.974846    24.6.173.220      199.181.132.249   HTTP   342 www.disney.com        GET / HTTP/1.1
16 9.007487    199.181.132.249   24.6.173.220      HTTP   514                       HTTP/1.1 301 Moved Permanently  (text/html)
32 11.415512   24.6.173.220      199.181.132.249   HTTP   338 disney.com            GET / HTTP/1.1
34 11.450306   199.181.132.249   24.6.173.220      HTTP  1502                       HTTP/1.1 200 OK  (text/html)
35 11.451572   199.181.132.249   24.6.173.220      HTTP  1514                       Continuation
36 11.451575   199.181.132.249   24.6.173.220      HTTP  1514                       Continuation
47 11.485659   199.181.132.249   24.6.173.220      HTTP  1514                       Continuation
48 11.486924   199.181.132.249   24.6.173.220      HTTP  1514                       Continuation
49 11.486928   199.181.132.249   24.6.173.220      HTTP  1514                       Continuation
50 11.486930   199.181.132.249   24.6.173.220      HTTP  1514                       Continuation
70 11.515813   24.6.173.220      208.111.148.6     HTTP   401 cdnvideo.dolimg.com   GET /cdn_assets/314da08c2cc0c65e47e89c1c092812dbffa
77 11.516667   24.6.173.220      208.111.148.6     HTTP   401 cdnvideo.dolimg.com   GET /cdn_assets/9d31accc4393a7912869c8d837e51aba206
78 11.516916   24.6.173.220      208.111.148.6     HTTP   401 cdnvideo.dolimg.com   GET /cdn_assets/69d7937a4e5ed43103011adb5a79afb6e77
```

```
> Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 199.181.132.249
> Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
> Hypertext Transfer Protocol
```

```
0000  00 01 5c 31 bb c1 d4 85  64 a7 bf a3 08 00 45 00   ··\1···· d·····E·
0010  01 48 69 87 40 00 80 06  00 00 18 06 ad dc c7 b5   ·Hi·@··· ········
0020  84 f9 8a be 00 50 73 e7  7d 59 c7 0e 66 a7 50 18   ·····Ps· }Y··f·P·
0030  40 29 13 cc 00 00 47 45  54 20 2f 20 48 54 54 50   @)····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  64 69 73 6e 65 79 2e 63  6f 6d 0d 0a 55 73 65 72   disney.c om··User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT 
0080  36 2e 31 3b 20 57 4f 57  36 34 3b 20 72 76 3a 31   6.1; WOW 64; rv:1
0090  36 2e 30 29 20 47 65 63  6b 6f 2f 32 30 31 30 30   6.0) Gec ko/20100
00a0  31 30 31 20 46 69 72 65  66 6f 78 2f 31 36 2e 30   101 Fire fox/16.0
00b0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
```

Hypertext Transfer Protocol: Protocol | Paquetes: 6143 · Mostrado: 4093 (66.6%) | Perfil: Default

Ilustración 15 Laboratorio16



```
tcp.port==80
```

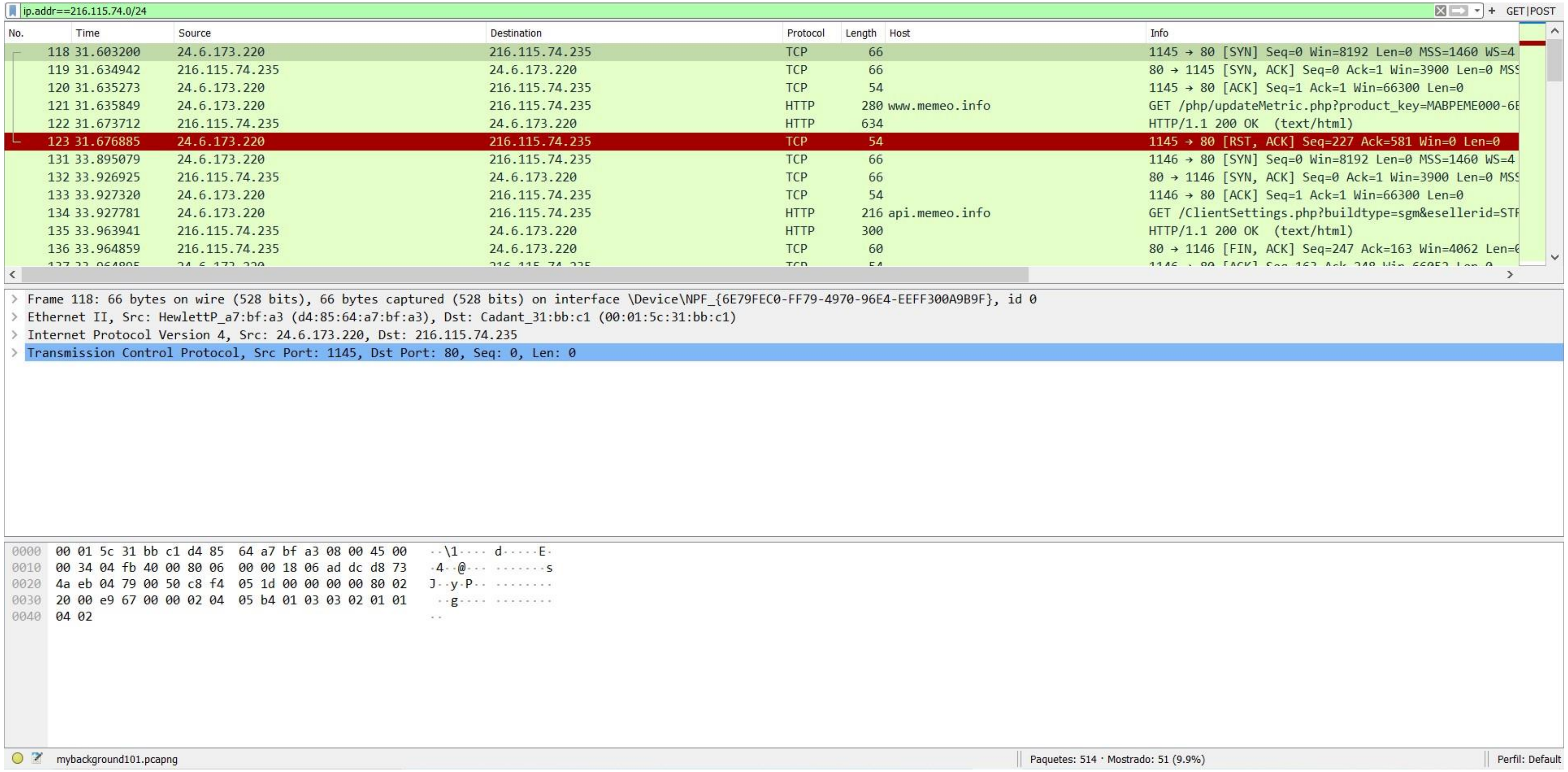
```
No.    Time       Source            Destination       Protocol  Length Host            Info
    12 8.939675   24.6.173.220      199.181.132.249   TCP           66                 35518 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
    13 8.974401   199.181.132.249   24.6.173.220      TCP           66                 80 → 35518 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MS
    14 8.974476   24.6.173.220      199.181.132.249   TCP           54                 35518 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
    15 8.974846   24.6.173.220      199.181.132.249   HTTP         342 www.disney.com  GET / HTTP/1.1
    16 9.007487   199.181.132.249   24.6.173.220      HTTP         514                 HTTP/1.1 301 Moved Permanently  (text/html)
    21 9.115974   24.6.173.220      199.181.132.249   TCP           66                 35519 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
    22 9.207605   24.6.173.220      199.181.132.249   TCP           54                 35518 → 80 [ACK] Seq=289 Ack=461 Win=65240 Len=0
    29 11.384237  24.6.173.220      199.181.132.249   TCP           66                 35520 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
    30 11.415004  199.181.132.249   24.6.173.220      TCP           66                 80 → 35520 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MS
    31 11.415139  24.6.173.220      199.181.132.249   TCP           54                 35520 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
    32 11.415512  24.6.173.220      199.181.132.249   HTTP         338 disney.com      GET / HTTP/1.1
    34 11.450306  199.181.132.249   24.6.173.220      HTTP        1502                 HTTP/1.1 200 OK  (text/html)
    35 11.451572  199.181.132.249   24.6.173.220      HTTP        1514                 Continuation
```

```
> Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 199.181.132.249
> Transmission Control Protocol, Src Port: 35518, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
> Hypertext Transfer Protocol
```

```
0000  00 01 5c 31 bb c1 d4 85  64 a7 bf a3 08 00 45 00   ··\1···· d·····E·
0010  01 48 69 87 40 00 80 06  00 00 18 06 ad dc c7 b5   ·Hi·@··· ········
0020  84 f9 8a be 00 50 73 e7  7d 59 c7 0e 66 a7 50 18   ·····Ps· }Y··f·P·
0030  40 29 13 cc 00 00 47 45  54 20 2f 20 48 54 54 50   @)····GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  64 69 73 6e 65 79 2e 63  6f 6d 0d 0a 55 73 65 72   disney.c om··User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT 
0080  36 2e 31 3b 20 57 4f 57  36 34 3b 20 72 76 3a 31   6.1; WOW 64; rv:1
0090  36 2e 30 29 20 47 65 63  6b 6f 2f 32 30 31 30 30   6.0) Gec ko/20100
00a0  31 30 31 20 46 69 72 65  66 6f 78 2f 31 36 2e 30   101 Fire fox/16.0
00b0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
```

http-disney101.pcapng | Paquetes: 6143 · Mostrado: 5917 (96.3%) | Perfil: Defaul:

Ilustración 16 Laboratorio16b



ip.addr==216.115.74.0/24

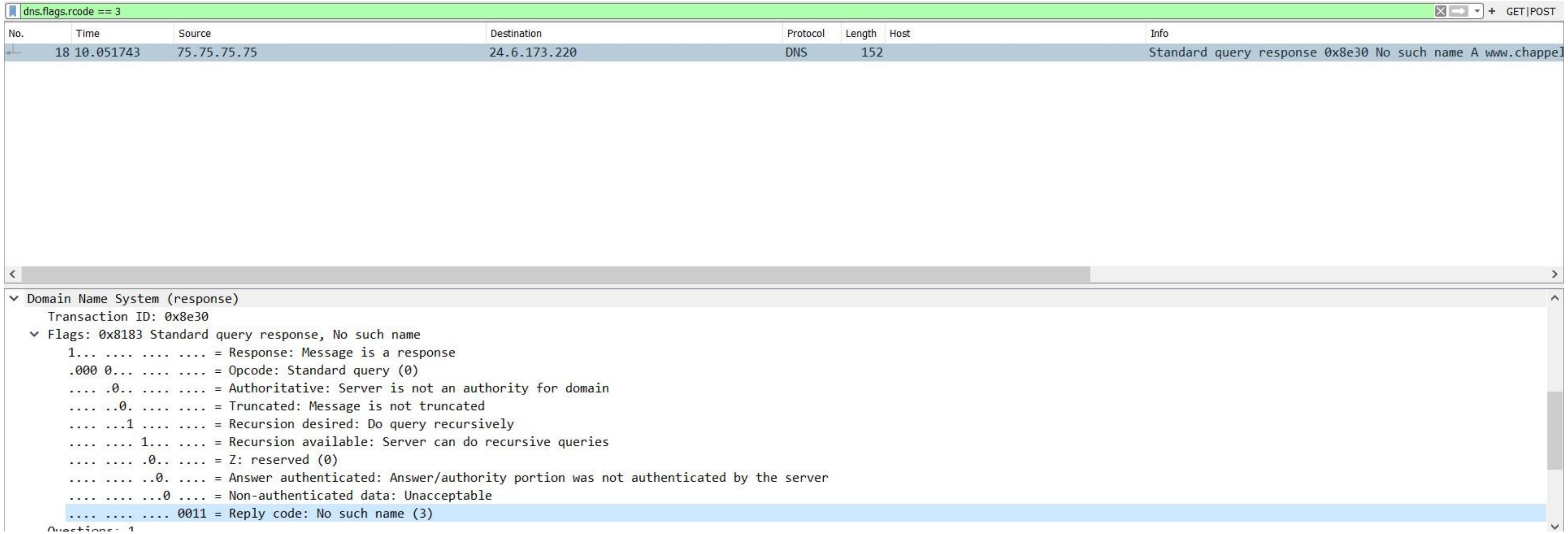
No.	Time	Source	Destination	Protocol	Length	Host	Info
118	31.603200	24.6.173.220	216.115.74.235	TCP	66		1145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
119	31.634942	216.115.74.235	24.6.173.220	TCP	66		80 → 1145 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS
120	31.635273	24.6.173.220	216.115.74.235	TCP	54		1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
121	31.635849	24.6.173.220	216.115.74.235	HTTP	280	www.memeo.info	GET /php/updateMetric.php?product_key=MABPEME000-6E
122	31.673712	216.115.74.235	24.6.173.220	HTTP	634		HTTP/1.1 200 OK (text/html)
123	31.676885	24.6.173.220	216.115.74.235	TCP	54		1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0
131	33.895079	24.6.173.220	216.115.74.235	TCP	66		1146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
132	33.926925	216.115.74.235	24.6.173.220	TCP	66		80 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS
133	33.927320	24.6.173.220	216.115.74.235	TCP	54		1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
134	33.927781	24.6.173.220	216.115.74.235	HTTP	216	api.memeo.info	GET /ClientSettings.php?buildtype=sgm&esellerid=STF
135	33.963941	216.115.74.235	24.6.173.220	HTTP	300		HTTP/1.1 200 OK (text/html)
136	33.964859	216.115.74.235	24.6.173.220	TCP	60		80 → 1146 [FIN, ACK] Seq=247 Ack=163 Win=4062 Len=(

```
> Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 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: Default

Ilustración 17 Laboratorio17

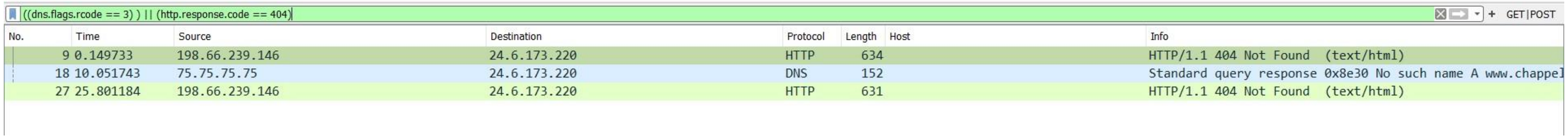


```
dns.flags.rcode == 3
```

```
No.   Time        Source          Destination     Protocol  Length  Host  Info
   18 10.051743   75.75.75.75     24.6.173.220    DNS        152          Standard query response 0x8e30 No such name A www.chappel
```

```
Domain Name System (response)
    Transaction ID: 0x8e30
  Flags: 0x8183 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
```

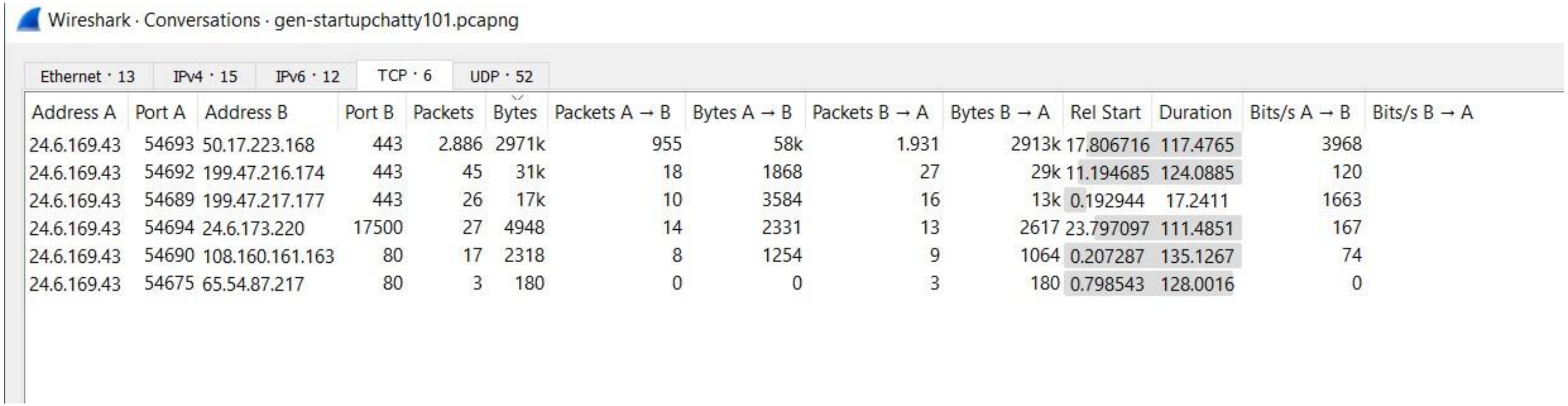
Ilustración 18 Laboratorio 18



```
((dns.flags.rcode == 3) ) || (http.response.code == 404)
```

```
No.   Time        Source           Destination     Protocol  Length  Host  Info
    9 0.149733    198.66.239.146   24.6.173.220    HTTP       634          HTTP/1.1 404 Not Found  (text/html)
   18 10.051743   75.75.75.75      24.6.173.220    DNS        152          Standard query response 0x8e30 No such name A www.chappel
   27 25.801184   198.66.239.146   24.6.173.220    HTTP       631          HTTP/1.1 404 Not Found  (text/html)
```

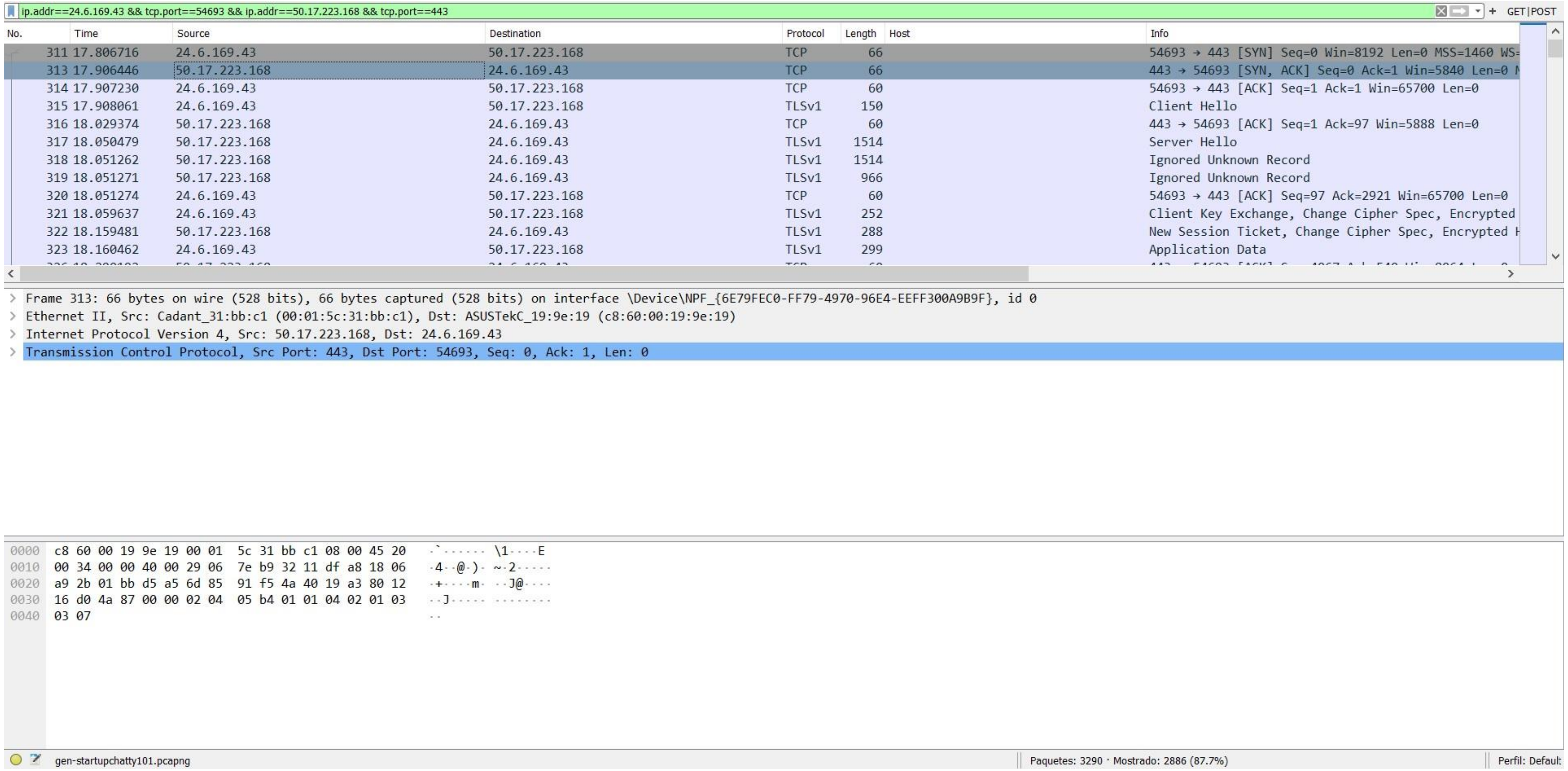
Ilustración 19 Laboratorio18b



Wireshark · Conversations · gen-startupchatty101.pcapng

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	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	

Ilustración 20 Laboratorio19



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

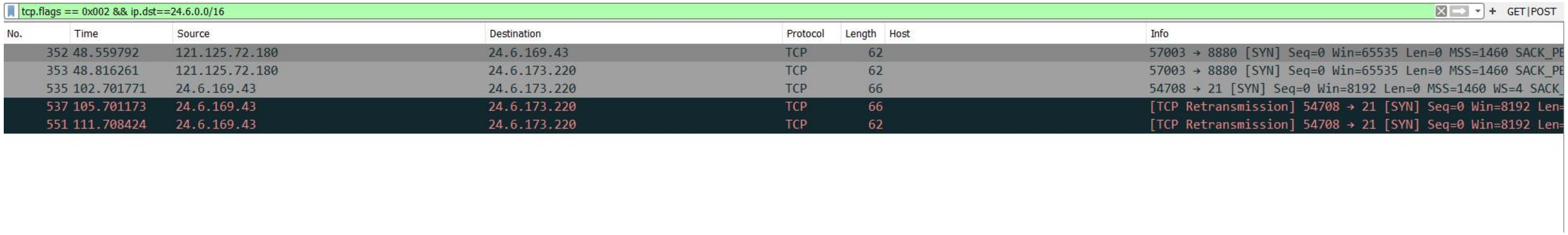
```
No.    Time        Source          Destination     Protocol  Length  Host  Info
   311 17.806716   24.6.169.43     50.17.223.168   TCP           66        54693 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
   313 17.906446   50.17.223.168   24.6.169.43     TCP           66        443 → 54693 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
   314 17.907230   24.6.169.43     50.17.223.168   TCP           60        54693 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   315 17.908061   24.6.169.43     50.17.223.168   TLSv1        150        Client Hello
   316 18.029374   50.17.223.168   24.6.169.43     TCP           60        443 → 54693 [ACK] Seq=1 Ack=97 Win=5888 Len=0
   317 18.050479   50.17.223.168   24.6.169.43     TLSv1       1514        Server Hello
   318 18.051262   50.17.223.168   24.6.169.43     TLSv1       1514        Ignored Unknown Record
   319 18.051271   50.17.223.168   24.6.169.43     TLSv1        966        Ignored Unknown Record
   320 18.051274   24.6.169.43     50.17.223.168   TCP           60        54693 → 443 [ACK] Seq=97 Ack=2921 Win=65700 Len=0
   321 18.059637   24.6.169.43     50.17.223.168   TLSv1        252        Client Key Exchange, Change Cipher Spec, Encrypted
   322 18.159481   50.17.223.168   24.6.169.43     TLSv1        288        New Session Ticket, Change Cipher Spec, Encrypted H
   323 18.160462   24.6.169.43     50.17.223.168   TLSv1        299        Application Data
```

```
> Frame 313: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: ASUSTekC_19:9e:19 (c8:60:00:19:9e:19)
> Internet Protocol Version 4, Src: 50.17.223.168, Dst: 24.6.169.43
> Transmission Control Protocol, Src Port: 443, Dst Port: 54693, Seq: 0, Ack: 1, Len: 0
```

```
0000  c8 60 00 19 9e 19 00 01  5c 31 bb c1 08 00 45 20   ·`······ \1····E
0010  00 34 00 00 40 00 29 06  7e b9 32 11 df a8 18 06   ·4··@·)· ~·2·····
0020  a9 2b 01 bb d5 a5 6d 85  91 f5 4a 40 19 a3 80 12   ·+····m· ··J@····
0030  16 d0 4a 87 00 00 02 04  05 b4 01 01 04 02 01 03   ··J····· ········
0040  03 07                                              ··
```

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

Ilustración 21 Laboratorio19b



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

No.	Time	Source	Destination	Protocol	Length	Host	Info
352	48.559792	121.125.72.180	24.6.169.43	TCP	62		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PE
353	48.816261	121.125.72.180	24.6.173.220	TCP	62		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PE
535	102.701771	24.6.169.43	24.6.173.220	TCP	66		54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_
537	105.701173	24.6.169.43	24.6.173.220	TCP	66		[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=
551	111.708424	24.6.169.43	24.6.173.220	TCP	62		[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=

Ilustración 22 Laboratorio20