

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

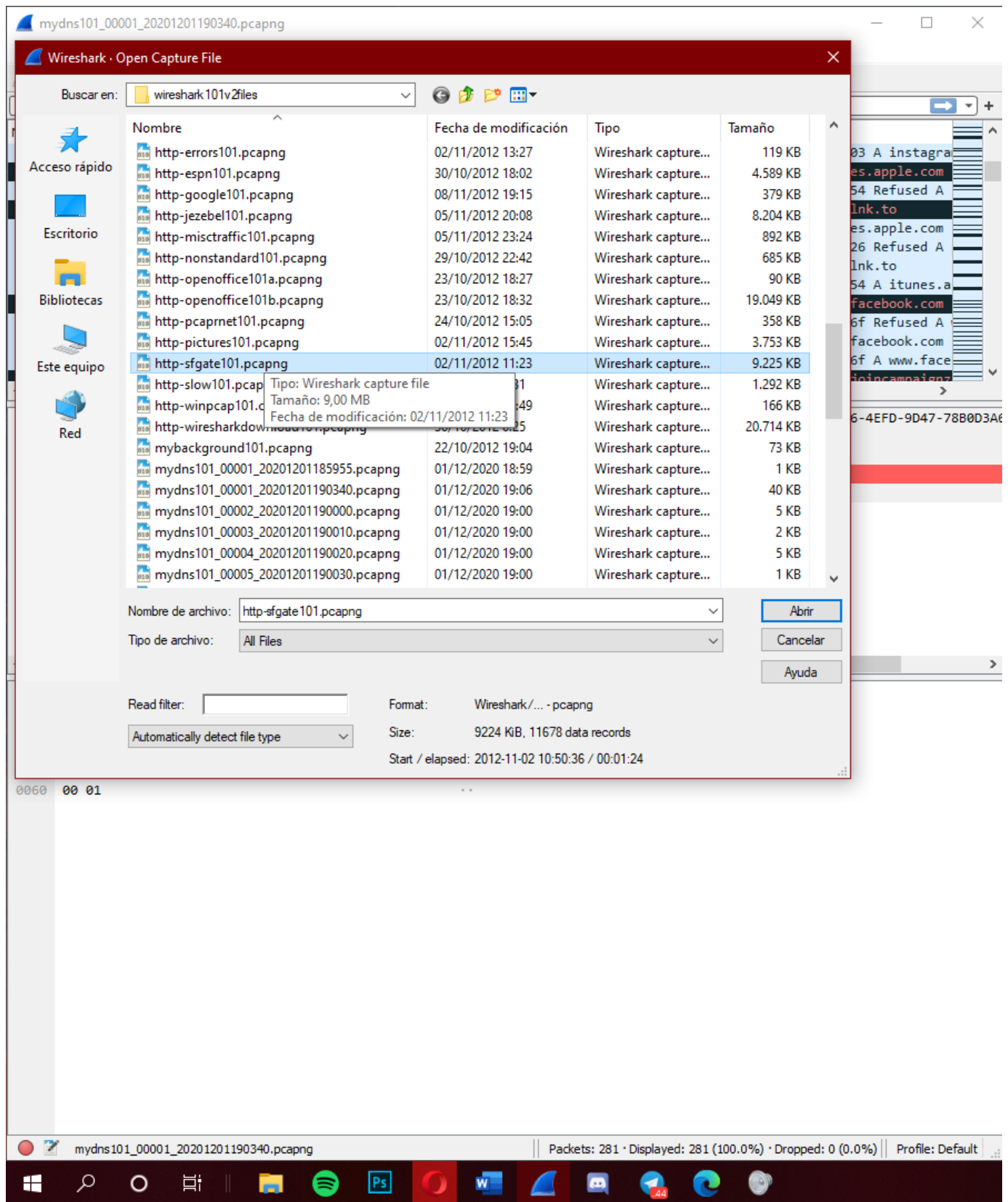
Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 14

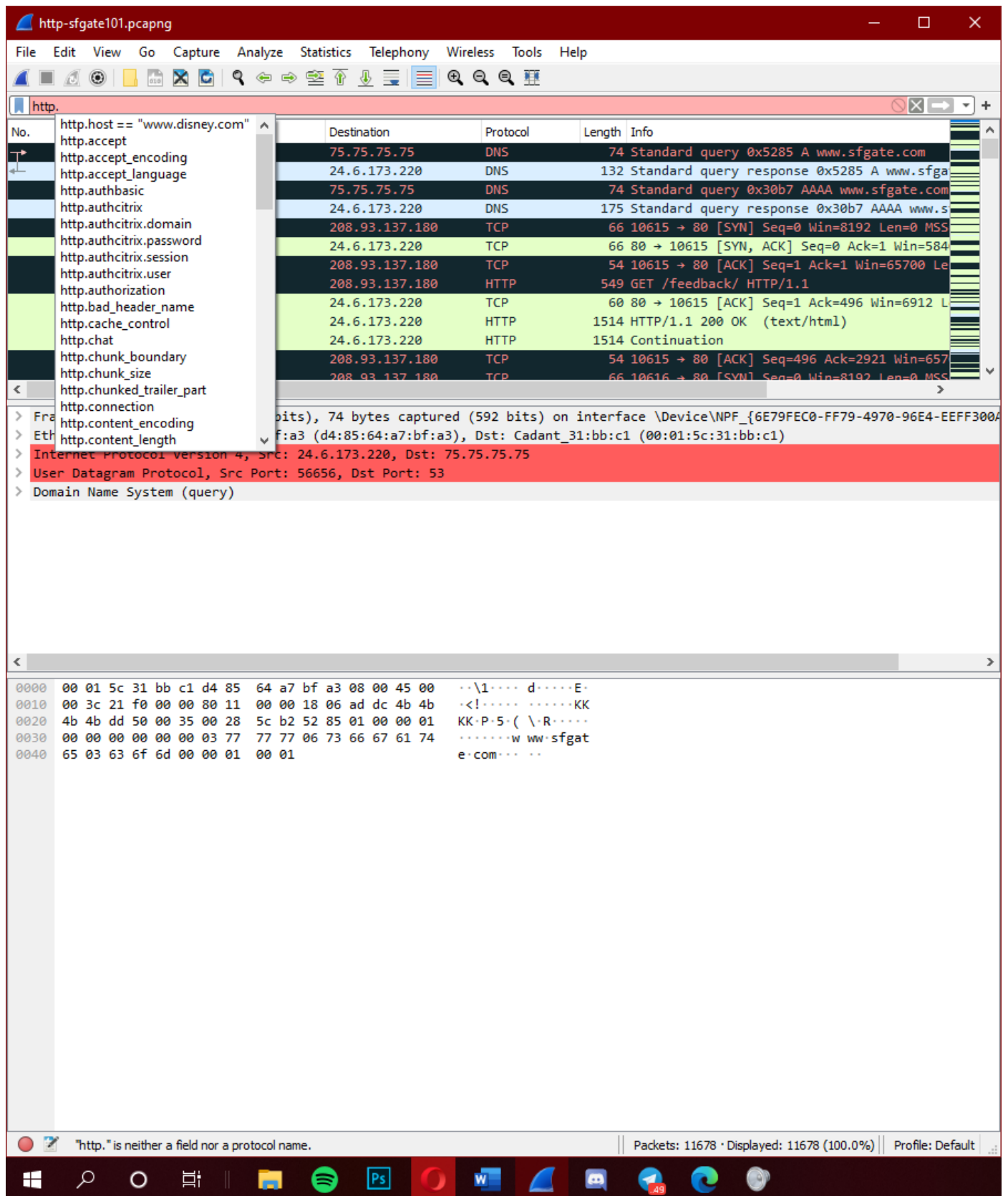
Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Paso 1:



Paso 2:



The image shows a Wireshark packet capture analysis of a file named `http-sfgate101.pcapng`. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a packet list pane on the left. The packet list pane shows a list of captured packets, with the first packet selected. The packet details pane on the right shows the structure of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane at the bottom shows the raw data of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header.

Packet List:

No.	Destination	Protocol	Length	Info
1	75.75.75.75	DNS	74	Standard query 0x5285 A www.sfgate.com
2	24.6.173.220	DNS	132	Standard query response 0x5285 A www.sfgate.com
3	75.75.75.75	DNS	74	Standard query 0x30b7 AAAA www.sfgate.com
4	24.6.173.220	DNS	175	Standard query response 0x30b7 AAAA www.sfgate.com
5	208.93.137.180	TCP	66	10615 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=
6	24.6.173.220	TCP	66	80 → 10615 [SYN, ACK] Seq=0 Ack=1 Win=584
7	208.93.137.180	TCP	54	10615 → 80 [ACK] Seq=1 Ack=1 Win=65700 Le
8	208.93.137.180	HTTP	549	GET /feedback/ HTTP/1.1
9	24.6.173.220	TCP	60	80 → 10615 [ACK] Seq=1 Ack=496 Win=6912 L
10	24.6.173.220	HTTP	1514	HTTP/1.1 200 OK (text/html)
11	24.6.173.220	HTTP	1514	Continuation
12	208.93.137.180	TCP	54	10615 → 80 [ACK] Seq=496 Ack=2921 Win=657
13	208.93.137.180	TCP	66	10616 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=

Packet Details:

- Ethernet II, Src: Intel E100 (00:00:00:00:00:00), Dst: Intel E100 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
- User Datagram Protocol, Src Port: 56656, Dst Port: 53
- Domain Name System (query)

Packet Bytes:

```
0000  00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00  ..\1.... d.....E
0010  00 3c 21 f0 00 00 80 11 00 00 18 06 ad dc 4b 4b  .<!..... ..KK
0020  4b 4b dd 50 00 35 00 28 5c b2 52 85 01 00 00 01  KK.P.5.( \.R.....
0030  00 00 00 00 00 00 03 77 77 77 06 73 66 67 61 74  ....w ww.sfgat
0040  65 03 63 6f 6d 00 00 01 00 01  e.com...
```

paso 3:

http-sfgate101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x5285 A www.sfgate.com
2	0.012983	75.75.75.75	24.6.173.220	DNS	132	Standard query response 0x5285 A www.sfgate.com
3	0.001210	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x30b7 AAAA www.sfgate.com
4	0.020072	75.75.75.75	24.6.173.220	DNS	175	Standard query response 0x30b7 AAAA www.sfgate.com
5	0.001322	24.6.173.220	208.93.137.180	TCP	66	10615 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=
6	0.018327	208.93.137.180	24.6.173.220	TCP	66	80 → 10615 [SYN, ACK] Seq=0 Ack=1 Win=5840
7	0.000132	24.6.173.220	208.93.137.180	TCP	54	10615 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	0.000520	24.6.173.220	208.93.137.180	HTTP	549	GET /feedback/ HTTP/1.1
9	0.021194	208.93.137.180	24.6.173.220	TCP	60	80 → 10615 [ACK] Seq=1 Ack=496 Win=6912 Len=0
10	0.122575	208.93.137.180	24.6.173.220	HTTP	1514	HTTP/1.1 200 OK (text/html)
11	0.002185	208.93.137.180	24.6.173.220	HTTP	1514	Continuation
12	0.001660	24.6.173.220	208.93.137.180	TCP	54	10615 → 80 [ACK] Seq=496 Ack=2921 Win=65700 Len=0
13	0.026014	24.6.173.220	208.93.137.180	TCP	66	10616 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A...}

> 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: 56656, 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 3c 21 f0 00 00 80 11 00 00 18 06 ad dc 4b 4b  <!.....KK
0020  4b 4b dd 50 00 35 00 28 5c b2 52 85 01 00 00 01  KK.P.5.( \R....
0030  00 00 00 00 00 00 03 77 77 77 06 73 66 67 61 74  ....w ww.sfgat
0040  65 03 63 6f 6d 00 00 01 00 01                    e.com...

```

"http.h" is neither a field nor a protocol name. | Packets: 11678 · Displayed: 11678 (100.0%) | Profile: Default

http-sfgate101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host

No.	Time	Source	Destination	Protocol	Length	Info
187	0.002987	24.6.173.220	208.93.137.180	HTTP	389	GET /img/modules/siteheader/closeBtn.gif
191	0.001485	24.6.173.220	208.93.137.180	HTTP	403	GET /img/partners/target/target_weekly_ad
197	0.009060	24.6.173.220	208.93.137.180	HTTP	376	GET /img/utills/rss_icon.png HTTP/1.1
201	0.001334	24.6.173.220	208.93.137.180	HTTP	402	GET /img/modules/slideshow/promo/wide/but
234	0.011469	24.6.173.220	208.93.137.180	HTTP	402	GET /img/modules/slideshow/promo/wide/but
278	0.019423	24.6.173.220	208.93.137.180	HTTP	401	GET /photos/16/01/46/3676557/5/square_hor
290	0.000744	24.6.173.220	208.93.137.180	HTTP	395	GET /photos/16/02/37/3680253/3/blockstate
301	0.000314	24.6.173.220	208.93.137.180	HTTP	395	GET /photos/16/01/41/3676237/5/blockstate
302	0.000562	24.6.173.220	208.93.137.180	HTTP	401	GET /photos/16/02/34/3680004/3/square_hor
303	0.000285	24.6.173.220	208.93.137.180	HTTP	395	GET /photos/16/01/31/3675736/3/blockstate
304	0.000528	24.6.173.220	208.93.137.180	HTTP	401	GET /photos/16/02/35/3680074/3/square_hor
308	0.008902	24.6.173.220	208.93.137.190	HTTP	385	GET /graphics/utills/hearst_logo.gif HTTP/
315	0.006826	24.6.173.220	66.109.241.50	HTTP	373	GET /css/modal.css HTTP/1.1

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

> 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 ..)wP8. .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/ HTTP/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

00c0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 t: text/ html,app

00d0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+x

00e0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x

00f0 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 ml;q=0.9 ,*/*;q=0

0100 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 .8..Acce pt-Langu

0110 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d age: en- US,en;q=

0120 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 0.5..Acc ept-Enco

0130 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl

0140 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a ate..Con nection:

0150 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 keep-al ive..Ref

0160 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 erer: ht tp://www

0170 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 72 6c 3f .google. com/url?

0180 73 61 3d 74 26 72 63 74 3d 6a 26 71 3d 26 65 73 sa=t&rct =j&q=&es

0190 72 63 3d 73 26 73 6f 75 72 63 65 3d 77 65 62 26 rc=s&sou rce=web&

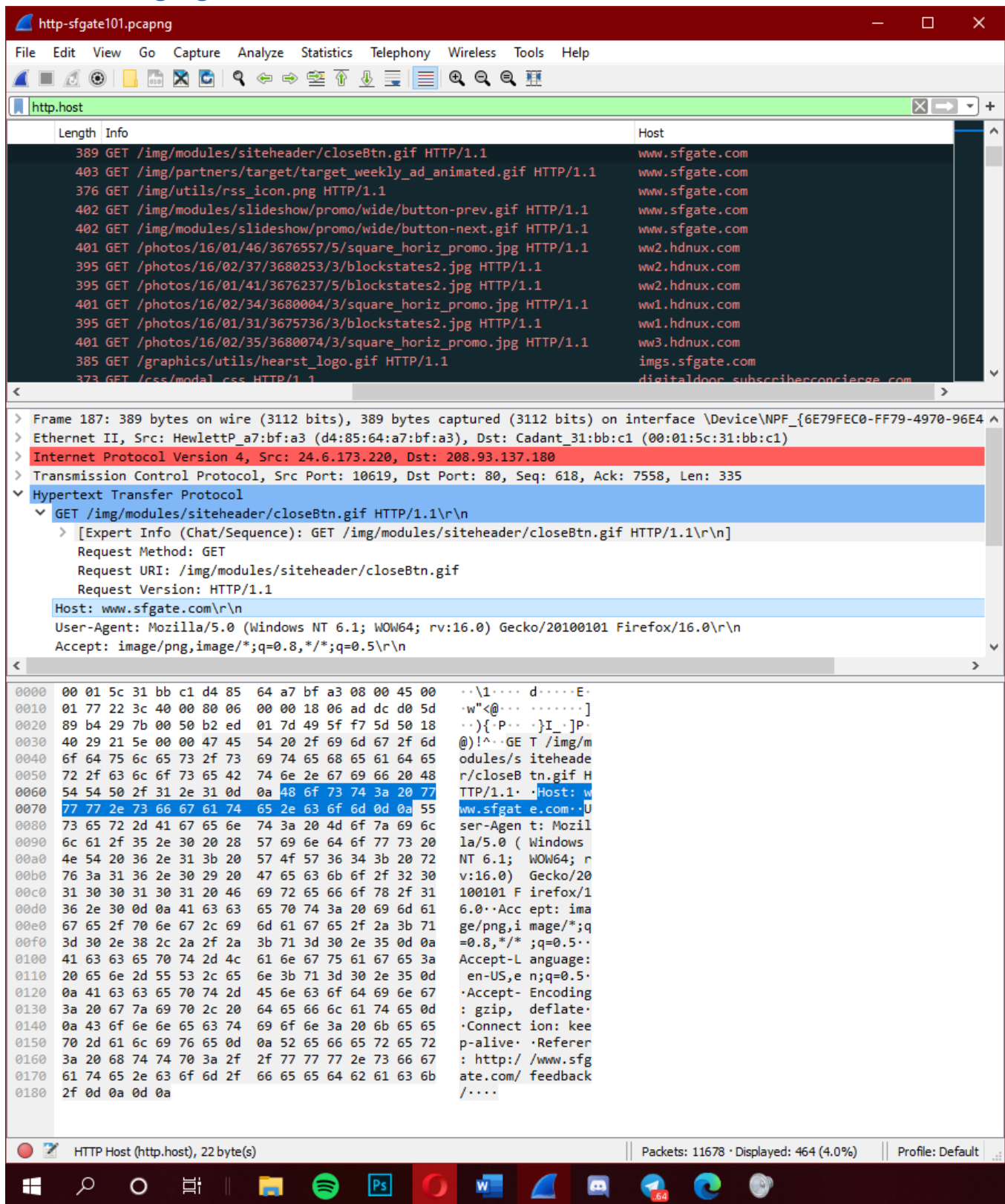
01a0 63 64 3d 36 26 76 65 64 3d 30 43 45 6f 51 46 6a cd=6&ved =0CEoQFj

http-sfgate101.pcapng

Packets: 11678 · Displayed: 464 (4.0%)

Profile: Default

Paso 4: se agrega la columna host



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with packet 187 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
389	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
403	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /img/partners/target/target_weekly_ad_animated.gif HTTP/1.1
376	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /img/utills/rss_icon.png HTTP/1.1
402	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /img/modules/slideshow/promo/wide/button-prev.gif HTTP/1.1
402	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /img/modules/slideshow/promo/wide/button-next.gif HTTP/1.1
401	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /photos/16/01/46/3676557/5/square_horiz_promo.jpg HTTP/1.1
395	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /photos/16/02/37/3680253/3/blockstates2.jpg HTTP/1.1
395	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /photos/16/01/41/3676237/5/blockstates2.jpg HTTP/1.1
401	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /photos/16/02/34/3680004/3/square_horiz_promo.jpg HTTP/1.1
395	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /photos/16/01/31/3675736/3/blockstates2.jpg HTTP/1.1
401	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /photos/16/02/35/3680074/3/square_horiz_promo.jpg HTTP/1.1
385	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /graphics/utills/hearst_logo.gif HTTP/1.1
373	0.000000	192.168.1.101	192.168.1.1	HTTP	335	GET /css/modal.css HTTP/1.1

Packet Details:

- Frame 187: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-...}
- 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: 10619, Dst Port: 80, Seq: 618, Ack: 7558, Len: 335
- Hypertext Transfer Protocol
 - GET /img/modules/siteheader/closeBtn.gif HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /img/modules/siteheader/closeBtn.gif HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /img/modules/siteheader/closeBtn.gif
 - Request Version: HTTP/1.1
 - Host: www.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: image/png,image/*;q=0.8,*/*;q=0.5\r\n

Packet Bytes:

```
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1.... d....E-
0010 01 77 22 3c 40 00 80 06 00 00 18 06 ad dc d0 5d .w"<@... .....]
0020 89 b4 29 7b 00 50 b2 ed 01 7d 49 5f f7 5d 50 18 ..){.P... }I..]P-
0030 40 29 21 5e 00 00 47 45 54 20 2f 69 6d 67 2f 6d @)!^...GE T /img/m
0040 6f 64 75 6c 65 73 2f 73 69 74 65 68 65 61 64 65 odules/s iteheade
0050 72 2f 63 6c 6f 73 65 42 74 6e 2e 67 69 66 20 48 r/closeB tn.gif H
0060 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 TTP/1.1. .Host: w
0070 77 77 2e 73 66 67 61 74 65 2e 63 6f 6d 0d 0a 55 ww.sfgat e.com..U
0080 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0090 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 ( Windows
00a0 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 NT 6.1; WOW64; r
00b0 76 3a 31 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 v:16.0) Gecko/20
00c0 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 100101 F irefox/1
00d0 36 2e 30 0d 0a 41 63 63 65 70 74 3a 20 69 6d 61 6.0..Acc ept: ima
00e0 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 2a 3b 71 ge/png,i mage/*;q
00f0 3d 30 2e 38 2c 2a 2f 2a 3b 71 3d 30 2e 35 0d 0a =0.8,*/* ;q=0.5..
0100 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a Accept-L anguage:
0110 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d en-US,e n;q=0.5.
0120 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 .Accept- Encoding
0130 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d : gzip, deflate.
0140 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 .Connect ion: kee
0150 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 p-alive. .Referer
0160 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 73 66 67 : http:/ /www.sfg
0170 61 74 65 2e 63 6f 6d 2f 66 65 65 64 62 61 63 6b ate.com/ feedback
0180 2f 0d 0a 0d 0a /....
```

Paso 5:

http-sfgate101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host contains "hearst"

No.	Time	Source	Destination	Protocol	Length	Info
159	0.000000	24.6.173.220	208.93.137.180	HTTP	344	GET /Scripts/loadAds.js HTTP/1.1
388	0.127133	24.6.173.220	208.93.137.180	HTTP	348	GET /Scripts/loadAdsMain.js HTTP/1.1
406	0.029183	24.6.173.220	208.93.137.180	HTTP	363	GET /SRO/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458	0.163355	24.6.173.220	208.93.137.180	HTTP	350	GET /Scripts/initDefineAds.js HTTP/1.1
586	0.554234	24.6.173.220	216.155.207.26	HTTP	1720	GET /js_1_0/?config=2130893885&type=news&ctxtId=
1071	0.346887	24.6.173.220	23.23.99.162	HTTP	1037	GET /sfgate.gif?url=http%3A/www.sfgate.com/feed
10055	66.874309	24.6.173.220	208.93.137.180	HTTP	420	GET /SRO/GetJS?url=www.sfgate.com/%3Fcontroller
10067	0.664242	24.6.173.220	208.93.137.180	HTTP	437	GET /SRO/GetJS?url=extras.sfgate.com/sfgate/modu
10250	3.045941	24.6.173.220	216.155.207.26	HTTP	1846	GET /js_1_0/?config=2130893885&type=news&ctxtId=
10332	0.270298	24.6.173.220	23.23.99.162	HTTP	1041	GET /sfgate.gif?url=http%3A/www.sfgate.com/feed

< >

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

> [Expert Info (Chat/Sequence): GET /Scripts/loadAds.js HTTP/1.1\r\n]

Request Method: GET

Request URI: /Scripts/loadAds.js

Request Version: HTTP/1.1

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

< >

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1.... d.....E.
0010 01 4a 22 30 40 00 80 06 00 00 18 06 ad dc d0 5d .J"0@...

0020 89 b4 29 81 00 50 22 40 32 90 f6 fe 41 6f 50 18 ..)..P"@ 2...AoP.
0030 40 29 21 31 00 00 47 45 54 20 2f 53 63 72 69 70 @)!1..GE T /Scrip
0040 74 73 2f 6c 6f 61 64 41 64 73 2e 6a 73 20 48 54 ts/loadA ds.js HT
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 lla/5.0 (Windows
0090 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 NT 6.1; WOW64;
00a0 72 76 3a 31 36 2e 30 29 20 47 65 63 6b 6f 2f 32 rv:16.0) Gecko/2
00b0 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
00c0 31 36 2e 30 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 16.0..Ac cept: */
00d0 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 *..Accep t-Langua
00e0 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 ge: en-U S,en;q=0
00f0 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 .5..Acce pt-Encod
0100 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 ing: gzi p, defla
0110 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 te..Conn ection:
0120 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 keep-ali ve..Refe
0130 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e rer: htt p://www.
0140 73 66 67 61 74 65 2e 63 6f 6d 2f 66 65 65 64 62 sfgate.c om/feedb
0150 61 63 6b 2f 0d 0a 0d 0a ack/....

HTTP Host (http.host), 24 byte(s) | Packets: 11678 · Displayed: 10 (0.1%) | Profile: Default

Paso 6:

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. Packet 859 is selected, showing an HTTP POST request to 199.7.57.72. The middle pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
859	0.000000	24.6.173.220	199.7.57.72	OCSP	522	Request
864	0.000510	24.6.173.220	199.7.57.72	OCSP	522	Request
865	0.000430	24.6.173.220	199.7.57.72	OCSP	522	Request
897	0.013423	24.6.173.220	199.7.57.72	OCSP	522	Request
898	0.000324	24.6.173.220	199.7.57.72	OCSP	522	Request
2043	2.645699	24.6.173.220	67.192.92.227	HTTP	805	POST /adserver?u=97df6f8f08d8730261d4b44204353b4
3418	4.189073	24.6.173.220	208.81.191.110	HTTP	944	POST /cmd/cx HTTP/1.1 (application/x-www-form-u
3419	0.000360	24.6.173.220	208.81.191.110	HTTP	1007	POST /cmd/tc HTTP/1.1 (application/x-www-form-u
3476	0.245204	24.6.173.220	208.81.191.110	HTTP	1338	POST /cmd/getrotate HTTP/1.1 (application/x-www
10022	59.080083	24.6.173.220	208.93.137.180	HTTP	1595	POST /sfgate/modules/formHandlers/sfgSupportMail
10406	5.266161	24.6.173.220	208.81.191.110	HTTP	1233	POST /cmd/cx HTTP/1.1 (application/x-www-form-u
10578	0.510405	24.6.173.220	67.192.92.227	HTTP	841	POST /adserver?u=97df6f8f08d8730261d4b44204353b4

Packet Details:

- Frame 859: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4}
- 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: 199.7.57.72
- Transmission Control Protocol, Src Port: 10672, Dst Port: 80, Seq: 1, Ack: 1, Len: 468
- Hypertext Transfer Protocol
 - POST / HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): POST / HTTP/1.1\r\n]
 - Request Method: POST
 - Request URI: /
 - Request Version: HTTP/1.1
 - Host: ocsp.verisign.com\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Raw Data:

```
0060 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0070 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 lla/5.0 (Windows
0080 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 NT 6.1; WOW64;
0090 72 76 3a 31 36 2e 30 29 20 47 65 63 6b 6f 2f 32 rv:16.0) Gecko/2
00a0 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
00b0 31 36 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 16.0..Ac cept: te
00c0 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 xt/html, applicat
00d0 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 ion/xhtm l+xml,ap
00e0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
00f0 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 0.9,*/*; q=0.8..A
0100 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccept-La nguage:
0110 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a en-US,en ;q=0.5..
0120 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Acce pt-E ncoding:
0130 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate..
0140 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 Connecti on: keep
0150 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d -alive.. Content-
0160 4c 65 6e 67 74 68 3a 20 31 31 35 0d 0a 43 6f 6e Length: 115..Con
0170 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 tent-Typ e: appli
0180 63 61 74 69 6f 6e 2f 6f 63 73 70 2d 72 65 71 75 cation/o csp-requ
0190 65 73 74 0d 0a 0d 0a 30 71 30 6f 30 4d 30 4b 30 est...0 q000M0K0
01a0 49 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 6c 2b I0...+... ..l+
01b0 c5 5a af 8d 96 bf 06 ad f8 1d 02 3f 23 b4 8a 00 .Z...`...?#...
01c0 59 c2 04 14 a5 ef 0b 11 ce c0 41 03 a3 4a 65 90 Y... ..A..Je-
01d0 48 b2 1c e0 57 2d 7d 47 02 10 7a 8f 92 23 02 1a H...W-}G...z...#..
01e0 57 5e 7e b3 01 12 4a b9 61 50 a2 1e 30 1c 30 1a W^...~J- aP...0-0-
01f0 06 09 2b 06 01 05 05 07 30 01 04 04 0d 30 0b 06 ..+... ..0...0...
0200 09 2b 06 01 05 05 07 30 01 01 ..+... ..0...
```

Status Bar: HTTP Request Method (http.request.method), 4 byte(s) | Packets: 11678 · Displayed: 12 (0.1%) | Profile: Default

Paso 7:

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (Frame 10022), which is an HTTP POST request to `/sfgate/modules/formHandlers/sfgSupportMailHandler.php` on the host `extras.sfgate.com`. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

Protocol	Length	Info	Host
OCSP	522	Request	ocsp.verisign.com
OCSP	522	Request	ocsp.verisign.com
OCSP	522	Request	ocsp.verisign.com
OCSP	522	Request	ocsp.verisign.com
OCSP	522	Request	ocsp.verisign.com
HTTP	805	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae6...	ad.auditude.com
HTTP	944	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)	www.meebo.com
HTTP	1007	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)	www.meebo.com
HTTP	1338	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)	www.meebo.com
HTTP	1595	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1...	extras.sfgate.com
HTTP	1233	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)	www.meebo.com
HTTP	841	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae6...	ad.auditude.com

Packet Details (Frame 10022):

- 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
 - [Expert Info (Chat/Sequence): POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1\r\n]
 - Request Method: POST
 - Request URI: /sfgate/modules/formHandlers/sfgSupportMailHandler.php
 - Request Version: HTTP/1.1
 - 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

Raw Data (Hex/ASCII):

```
0390 29 3b 20 73 5f 76 69 3d 5b 43 53 5d 76 31 7c 32 ); s_vi= [CS]v1|2
03a0 38 34 39 46 35 45 39 38 35 31 36 33 30 37 41 2d 849F5E98 516307A-
03b0 36 30 30 30 30 31 41 31 43 30 30 30 30 31 45 600001A1 C000001E
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 6c 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 r&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
04e0 74 73 3d 57 6f 6e 64 65 72 69 6e 67 2b 61 62 6f ts=Wonde ring+abo
04f0 75 74 2b 69 50 61 64 2b 73 75 70 70 6f 72 74 2e ut+iPad+ support.
0500 2e 2e 2b 26 72 65 6d 4c 65 6e 32 3d 39 36 38 26 ..+&remL en2=968&
0510 66 6f 72 6d 54 79 70 65 3d 73 69 74 65 46 65 65 formType =siteFee
0520 64 62 61 63 6b 26 72 65 66 65 72 72 65 72 3d 68 dback&re ferrer=h
0530 74 74 70 25 33 41 25 32 46 25 32 46 77 77 77 2e ttp%3A%2 F%2Fwww.
```

Status Bar: Bytes 1181-1192: Key (urlencoded-form.key) | Packets: 11678 · Displayed: 12 (0.1%) | Profile: Default