

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

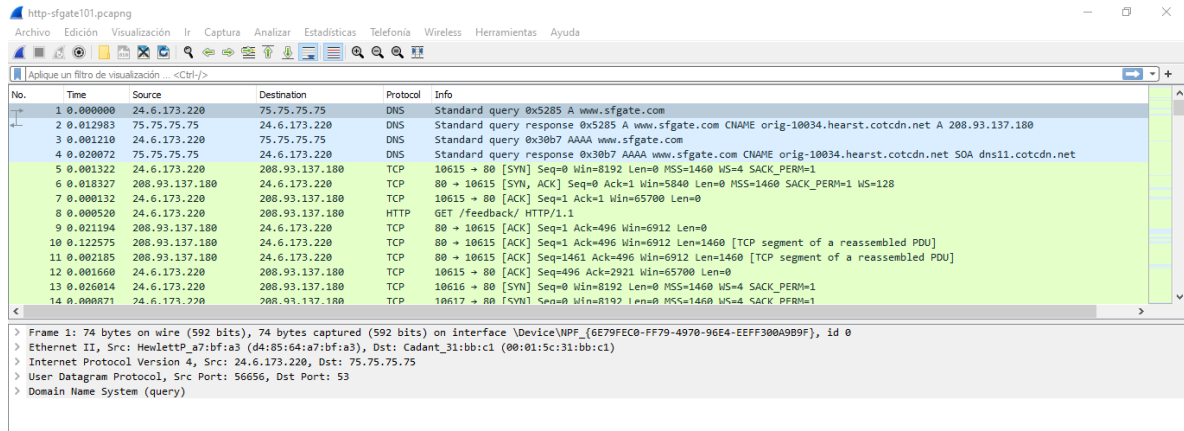
**Lab14 - Use Auto-Complete to Find
Traffic to a Specific HTTP Server**

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab14 - Use Auto-Complete to Find Traffic to a Specific HTTP Server

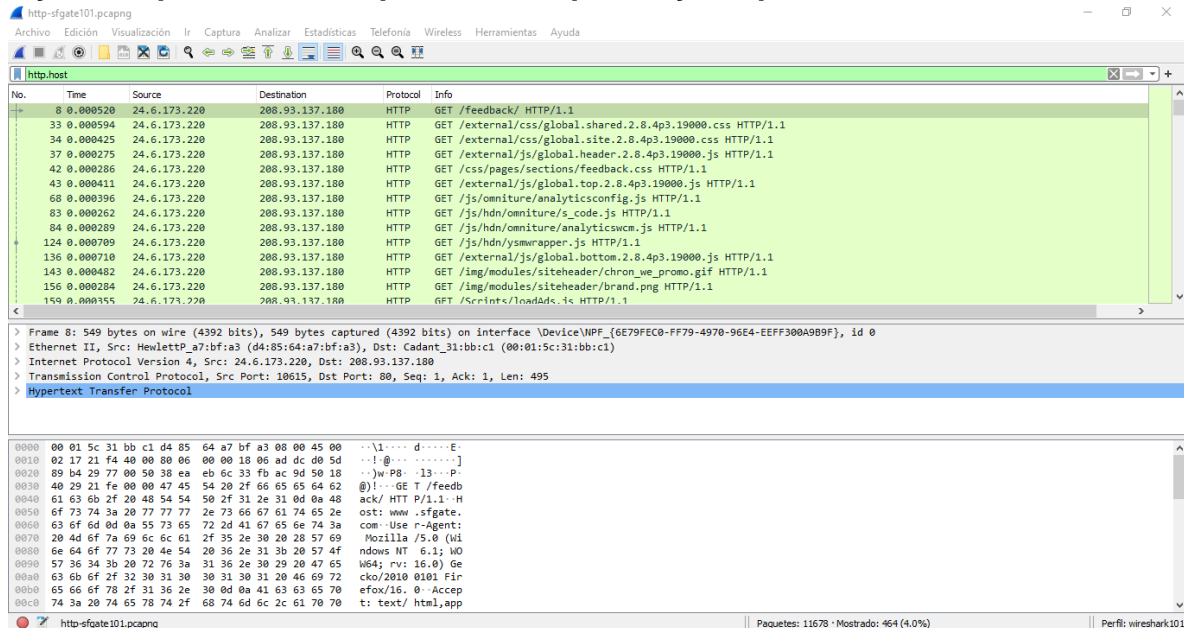
1. Abrimos el archivo http-sfgate101.pcapng y podemos observar que los tráficos es de DNS y HTTP



The screenshot shows the Wireshark interface with the file 'http-sfgate101.pcapng' open. The packet list on the left shows a sequence of packets: a DNS standard query (No. 1), a DNS standard query response (No. 2), another DNS standard query (No. 3), a DNS standard query response (No. 4), a TCP SYN packet (No. 5), a TCP ACK packet (No. 6), a TCP ACK packet (No. 7), a GET /feedback/ HTTP/1.1 packet (No. 8), a TCP ACK packet (No. 9), a TCP ACK packet (No. 10), a TCP ACK packet (No. 11), a TCP ACK packet (No. 12), a TCP SYN packet (No. 13), and a TCP ACK packet (No. 14). The packet details pane for packet 8 shows the following information:

- Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
- Ethernet II, Src: HewlettP_a7:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
- User Datagram Protocol, Src Port: 56656, Dst Port: 53
- Domain Name System (query)

2 y 3 En aplicar un filtro ponemos http.host y lo aplicamos



The screenshot shows the Wireshark interface with the file 'http-sfgate101.pcapng' open. A filter 'http.host' has been applied to the packet list. The packet list now shows only HTTP traffic, starting with packet 8 (GET /feedback/ HTTP/1.1) and ending with packet 14 (GET /css/int<loadAd<.css HTTP/1.1). The packet details pane for packet 8 shows the following information:

- 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:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.93.137.180
- Transmission Control Protocol, Src Port: 10615, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
- Hypertext Transfer Protocol

The packet bytes pane at the bottom shows the raw data of the selected packet, which is a GET request for /css/int<loadAd<.css.

Podemos observar que en la parte de display indica 464 paquetes se muestran.

Paquetes: 11678 · Mostrado: 464 (4.0%)

4. En Hypertext Transfer Protocol, buscamos Host y lo aplicamos como columna

http-sfgate01.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

No.	Time	Source	Destination	Protocol	Host	Info
8	0.000520	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1
33	0.000594	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	0.000425	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	0.000275	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	0.000286	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /css/pages/sections/feedback.css HTTP/1.1
43	0.000411	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	0.000396	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/omniture/analyticsconfig.js HTTP/1.1
83	0.000262	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/s_code.js HTTP/1.1
84	0.000289	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
124	0.000709	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/ysmwrapper.js HTTP/1.1
136	0.000710	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	0.000482	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
156	0.000284	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/brand.png HTTP/1.1
159	0.000355	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1
181	0.000339	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1

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

Hypertext Transfer Protocol

GET /feedback/ HTTP/1.1\r\n

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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US;q=0.5\r\n

Accept-Encoding: deflate\r\n

5. En aplicar un filtro lo cambiamos por http.request.method=="POST" le damos en aplicar y podemos observar que tenemos cambia el tipo de Report method.

No.	Time	Source	Destination	Protocol	Host	Info
8	0.000520	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1
33	0.000594	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	0.000425	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	0.000275	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	0.000286	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /css/pages/sections/feedback.css HTTP/1.1
43	0.000411	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	0.000396	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/omniture/analyticsconfig.js HTTP/1.1
83	0.000262	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/s_code.js HTTP/1.1
84	0.000289	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
124	0.000709	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /js/hdn/ysmwrapper.js HTTP/1.1
136	0.000710	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	0.000482	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
156	0.000284	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com	GET /img/modules/siteheader/brand.png HTTP/1.1
159	0.000355	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1

< GET /css/pages/sections/feedback.css HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /css/pages/sections/feedback.css HTTP/1.1\r\n]

Request Method: GET

Request URI: /css/pages/sections/feedback.css

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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US;q=0.5\r\n

Accept-Encoding: deflate\r\n

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Host	Info
859	0.000644	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
864	0.000235	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
865	0.000430	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
897	0.000381	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
898	0.000324	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
2043	0.001817	24.6.173.220	67.192.92.227	HTTP	ad.auditude.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=56
3418	0.001861	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
3419	0.000360	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
3476	0.015034	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)
10022	0.000862	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	0.016505	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
10578	0.000853	24.6.173.220	67.192.92.227	HTTP	ad.auditude.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=56

<

> 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

7 En el paquete 10022 podemos observar el mensaje que se había posteado, podemos ver el mensaje del remitente

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Host	Info
859	0.000644	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
864	0.000235	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
865	0.000430	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
897	0.000381	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
898	0.000324	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
2043	0.001817	24.6.173.220	67.192.92.227	HTTP	ad.auditude.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=56
3418	0.001861	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
3419	0.000360	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
3476	0.015034	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)
10022	0.000862	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	0.016505	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
10578	0.000853	24.6.173.220	67.192.92.227	HTTP	ad.auditude.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=56

< >

> 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

< >

0420 75 42 50 69 41 34 78 39 39 5a 56 34 69 65 43 36 uBPIA4x9 92V4ieC6

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 2d 66 6f 72 6d 2d 75 ion/x-www-form-u

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

0470 6e 74 2d 4c 65 6e 67 74 68 3a 20 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=londe ring+abo

HTTP Request Method (http.request.method), 4 byte(s)

Paquetes: 11678 · Mostrado: 12 (0.1%)

Perf: wireshark101