

**Instituto Tecnológico de Cancún**

**Fundamentos de Telecomunicaciones**

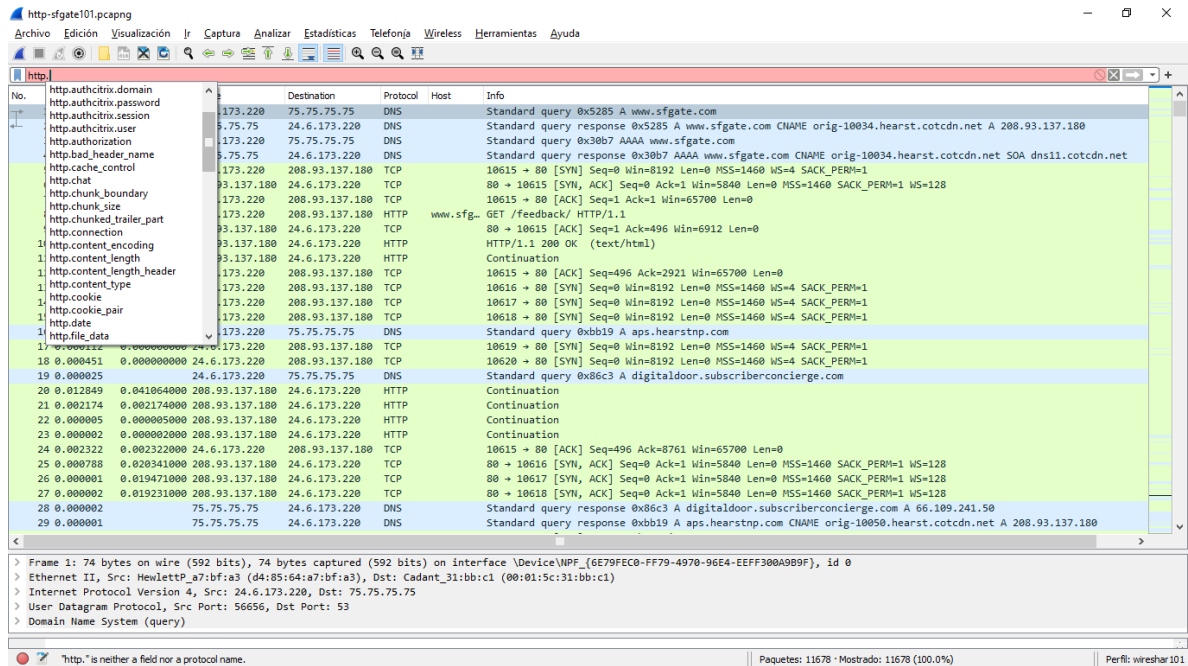
**Lab14 - Use Auto-Complete to Find  
Traffic to a Specific HTTP Server**

**Prof. Ismael Jiménez Sánchez**

**Alumno(a). Laury del Rosario Mex  
Martin**

**Ciclo 2020-B**

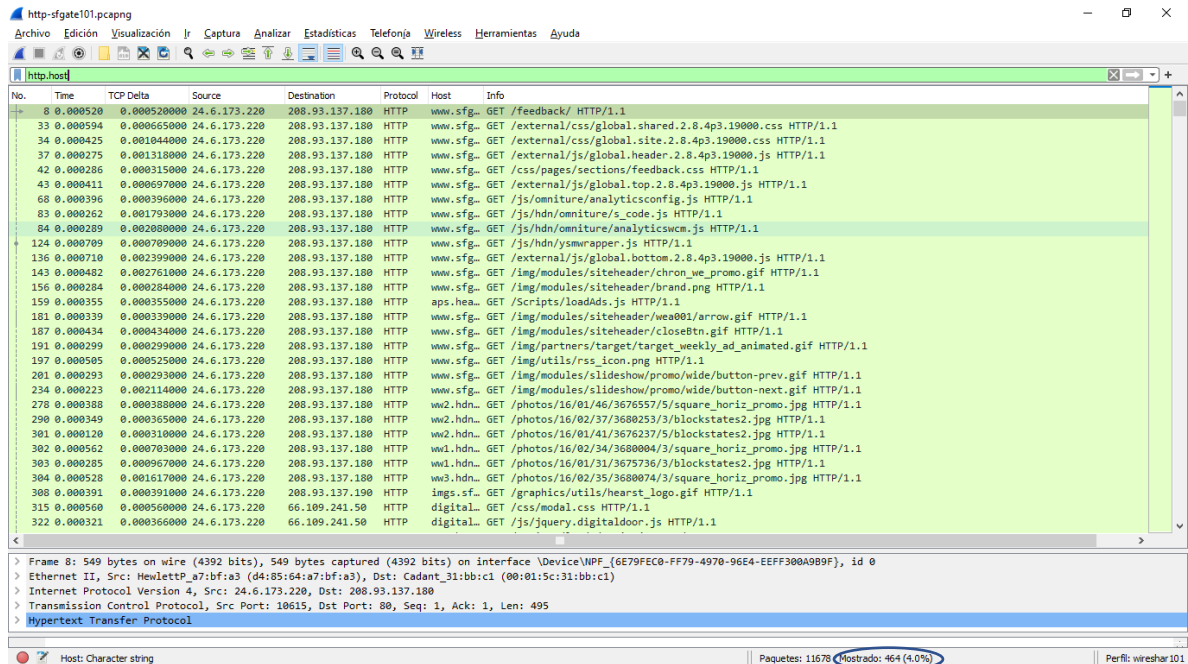
Paso 1: Usaremos el filtro **http** y veremos sus variantes para visualizar el flujo de datos.



The screenshot shows the Wireshark interface with the 'http' filter applied. The packet list displays various network packets, including DNS queries and HTTP GET requests. The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol.

No.	Time	Source	Destination	Protocol	Host	Info
173	0.000000	173.220	75.75.75.75	DNS		Standard query 0x5285 A www.sfgate.com
174	0.000000	173.220	75.75.75.75	DNS		Standard query response 0x5285 A www.sfgate.com CNAME orig-10034.hearst.cotcdn.net A 208.93.137.180
175	0.000000	173.220	75.75.75.75	DNS		Standard query response 0x30b7 AAAA www.sfgate.com CNAME orig-10034.hearst.cotcdn.net SOA dns11.cotcdn.net
176	0.000000	173.220	208.93.137.180	TCP		10615 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
177	0.000000	208.93.137.180	173.220	TCP		80 → 10615 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
178	0.000000	208.93.137.180	173.220	TCP		10615 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
179	0.000000	208.93.137.180	173.220	HTTP	www.sfgate.com	GET /feedback/ HTTP/1.1
180	0.000000	208.93.137.180	173.220	TCP		80 → 10615 [ACK] Seq=1 Ack=496 Win=6912 Len=0
181	0.000000	208.93.137.180	173.220	HTTP		HTTP/1.1 200 OK (text/html)
182	0.000000	208.93.137.180	173.220	HTTP		Continuation
183	0.000000	173.220	208.93.137.180	TCP		10615 → 80 [ACK] Seq=496 Ack=2921 Win=65700 Len=0
184	0.000000	173.220	208.93.137.180	TCP		10616 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
185	0.000000	173.220	208.93.137.180	TCP		10617 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
186	0.000000	173.220	208.93.137.180	TCP		10618 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
187	0.000000	173.220	75.75.75.75	DNS		Standard query 0xb19 A aps.hearstnp.com
188	0.000000	173.220	208.93.137.180	TCP		10619 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
189	0.000000	208.93.137.180	173.220	TCP		10620 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
190	0.000000	208.93.137.180	173.220	DNS		Standard query 0x86c3 A digitaldoor.subscriberconclerge.com
191	0.000000	208.93.137.180	173.220	HTTP		Continuation
192	0.000000	208.93.137.180	173.220	HTTP		Continuation
193	0.000000	208.93.137.180	173.220	HTTP		Continuation
194	0.000000	208.93.137.180	173.220	HTTP		Continuation
195	0.000000	208.93.137.180	173.220	TCP		10615 → 80 [ACK] Seq=496 Ack=8761 Win=65700 Len=0
196	0.000000	208.93.137.180	173.220	TCP		80 → 10616 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
197	0.000000	208.93.137.180	173.220	TCP		80 → 10617 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
198	0.000000	208.93.137.180	173.220	TCP		80 → 10618 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
199	0.000000	208.93.137.180	173.220	DNS		Standard query response 0xb19 A aps.hearstnp.com CNAME orig-10050.hearst.cotcdn.net A 208.93.137.180

Paso 2: Aplicaremos el filtro **http.host** y nos va a mostrar 464 paquetes que hay y en el laboratorio 4 anexamos la columna host y ahora podemos ver todos los host que hay sin necesidad de ir aun frame y visualizar los detalles de este.



The screenshot shows the Wireshark interface with the 'http.host' filter applied. The packet list displays various network packets, including HTTP GET requests to different hosts. The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol.

No.	Time	Source	Destination	Protocol	Host	Info
8	0.000528	0.000520000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /feedback/ HTTP/1.1
33	0.000594	0.000655000	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	0.001044000	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	0.001318000	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	0.000315000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /css/pages/sections/feedback.css HTTP/1.1
43	0.000411	0.000697000	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	0.000396000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /js/omniture/analyticsconfig.js HTTP/1.1
83	0.000262	0.001793000	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	0.002080000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /js/hdn/omniture/analyticswcw.js HTTP/1.1
124	0.000709	0.000709000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /js/hdn/ysmwrapper.js HTTP/1.1
136	0.000710	0.002399000	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	0.002761000	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	0.000284000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /img/modules/siteheader/brand.png HTTP/1.1
159	0.000355	0.000355000	24.6.173.220	208.93.137.180	HTTP	aps.hearst.com /Scripts/loadAds.js HTTP/1.1
181	0.000339	0.000339000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1
187	0.000434	0.000434000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
191	0.000299	0.000299000	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	0.000505	0.000525000	24.6.173.220	208.93.137.180	HTTP	www.sfgate.com GET /img/utills/rss_icon.png HTTP/1.1
201	0.000293	0.000293000	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	0.000223	0.002114000	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	0.000388	0.000388000	24.6.173.220	208.93.137.180	HTTP	www2.hdn.com GET /photos/16/02/46/3676557/5/square_horiz_promo.jpg HTTP/1.1
290	0.000349	0.000365000	24.6.173.220	208.93.137.180	HTTP	www2.hdn.com GET /photos/16/02/37/3680253/3/blockstates2.jpg HTTP/1.1
301	0.000120	0.000310000	24.6.173.220	208.93.137.180	HTTP	www2.hdn.com GET /photos/16/02/41/3676237/5/blockstates2.jpg HTTP/1.1
302	0.000562	0.000703000	24.6.173.220	208.93.137.180	HTTP	www1.hdn.com GET /photos/16/02/34/3680004/3/square_horiz_promo.jpg HTTP/1.1
303	0.000285	0.000967000	24.6.173.220	208.93.137.180	HTTP	www1.hdn.com GET /photos/16/01/31/3675736/3/blockstates2.jpg HTTP/1.1
304	0.000528	0.001617000	24.6.173.220	208.93.137.180	HTTP	www3.hdn.com GET /photos/16/02/35/3680074/3/square_horiz_promo.jpg HTTP/1.1
308	0.000391	0.000391000	24.6.173.220	208.93.137.190	HTTP	imgs.sf.com GET /graphics/utills/hearst_logo.gif HTTP/1.1
315	0.000560	0.000560000	24.6.173.220	66.109.241.50	HTTP	digital.com GET /css/modal.css HTTP/1.1
322	0.000321	0.000360000	24.6.173.220	66.109.241.50	HTTP	digital.com GET /js/jquery.digitaldoor.js HTTP/1.1

Paso 3: Ordenaremos la columna de host en orden alfabético y después aplicaremos el siguiente filtro que es **http.host contains “hearts”** y nos mostrara que hay 10 paquetes en este filtro y en el frame 159 nos muestra la palabra *hearts* en su host.

Wireshark capture showing a list of HTTP requests filtered by "http.host contains hearts". The list shows 10 packets. Packet 159 is expanded to show the GET request for /Scripts/loadAds.js from aps.hearstnp.com.

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
159	0.000355	0.000355000	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAds.js HTTP/1.1
388	0.032672	0.105570000	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/loadAdsMain.js HTTP/1.1
486	0.001269	0.000251000	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /SR0/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458	0.003027	0.003027000	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /Scripts/initDefineAds.js HTTP/1.1
586	0.005544	0.116757000	24.6.173.220	216.155.207.26	HTTP	cm.npc.com	GET /js_1_0/?config=2130893885&type=news&ctxId=news&keywordCharEnc=utf8&source=npc_hearst_sanfranciscochronicle_t...
10..	0.000490	0.000490000	24.6.173.220	23.23.99.162	HTTP	hearstnp.com	GET /sfgate.gif?url=http%3A/www.sfgate.com/feedback/&uid=13ac1d11a80-16d57cc1dedb3d3a&proj=sfgate&sec=home&ss=ho...
10..	0.004077	0.079539000	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /SR0/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmThirdPartyFooter HTTP/1.1
10..	0.092479	0.507483000	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	GET /SR0/GetJS?url=extras.sfgate.com/sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1
10..	0.009730	0.120919000	24.6.173.220	216.155.207.26	HTTP	cm.npc.com	GET /js_1_0/?config=2130893885&type=news&ctxId=news&keywordCharEnc=utf8&source=npc_hearst_sanfranciscochronicle_t...
10..	0.000735	0.000735000	24.6.173.220	23.23.99.162	HTTP	hearstnp.com	GET /sfgate.gif?url=http%3A/www.sfgate.com/feedback/&uid=13ac1d11a80-16d57cc1dedb3d3a&proj=sfgate&sec=home&ss=ho...

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

Hypertext Transfer Protocol  
 GET /Scripts/loadAds.js HTTP/1.1  
 Host: aps.hearstnp.com  
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0  
 Accept: \*/\*  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Connection: keep-alive  
 Referer: http://www.sfgate.com/feedback/  
 [Full request URI: http://aps.hearstnp.com/Scripts/loadAds.js]  
 [HTTP request 1/4]  
 [Response in frame 199]  
 [Next request in frame 388]

HTTP Host (http.host), 24 byte(s) | Paquetes: 11678 · Mostrado: 10 (0.1%) | Perfil: wireshark101

Paso 4: Aplicaremos un filtro donde nos mostrara el método **POST**, el cual es el siguiente **http.request.method== “POST”** y nos muestra 12 paquetes que contienen este método.

Wireshark capture showing a list of HTTP requests filtered by "http.request.method== POST". The list shows 12 packets. Packet 2043 is expanded to show the POST request for /assets/newsinc.com/[[IPORT]]/ndn.cdn.auditde.com/flash/modules/ndn-1.0/AuditdeAdUnit.swf.

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
859	0.000644	0.000644000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
864	0.000235	0.000259000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
865	0.000430	0.000665000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
897	0.000381	0.000405000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
898	0.000324	0.000705000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
20..	0.001817	0.072931000	24.6.173.220	67.192.92.227	HTTP	ad.audi...	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=5091281-20121102085039&of=1...
34..	0.001861	0.006212000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
34..	0.000360	0.011884000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
34..	0.015034	0.174904000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)
10..	0.000862	0.000862000	24.6.173.220	208.93.137.180	HTTP	extras...	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1 (application/x-www-form-urlencoded)
10..	0.016505	0.576897000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
10..	0.000853	0.000853000	24.6.173.220	67.192.92.227	HTTP	ad.audi...	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=5091281-20121102085149&of=1...

Frame 2043: 805 bytes on wire (6440 bits), 805 bytes captured (6440 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: 67.192.92.227  
 Transmission Control Protocol, Src Port: 10756, Dst Port: 80, Seq: 371, Ack: 527, Len: 751

Hypertext Transfer Protocol  
 POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=5091281-20121102085039&of=1.4&tm=15&g=1000002 HTTP/1.1  
 [Expert Info (Chat/Sequence): POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=5091281-20121102085039&of=1.4&tm=15&g=1000002 HTTP/1.1  
 Request Method: POST  
 Request URI: /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=5091281-20121102085039&of=1.4&tm=15&g=1000002  
 Request Version: HTTP/1.1  
 Host: ad.auditde.com  
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Connection: keep-alive  
 Referer: http://assets.newsinc.com/[[IPORT]]/ndn.cdn.auditde.com/flash/modules/ndn-1.0/AuditdeAdUnit.swf  
 Content-type: application/x-www-form-urlencoded

HTTP Request Method (http.request.method), 4 byte(s) | Paquetes: 11678 · Mostrado: 12 (0.1%) | Perfil: wireshark101

Paso 5: En el fram 10,022 podemos ver el host extra.sfgate que es un mensaje de Ipad support.

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.request.method=="POST"

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
859	0.000644	0.000644000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
864	0.000235	0.000259000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
865	0.000430	0.000655000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
897	0.000381	0.000405000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
898	0.000324	0.000705000	24.6.173.220	199.7.57.72	OCSP	ocsp.ve...	Request
2043	0.001817	0.072931000	24.6.173.220	67.192.92.227	HTTP	ad.audi...	POST /adserver?u=97df6f8f88d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=50912&l=20121102085039&of=
3418	0.001861	0.006212000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
3419	0.000360	0.011884000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
3476	0.015034	0.174904000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)
10022	0.000862	0.000862000	24.6.173.220	208.93.137.180	HTTP	extras...	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1 (application/x-www-form-urlencoded)
10406	0.016505	0.576897000	24.6.173.220	208.81.191.110	HTTP	www.mee...	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
10578	0.000853	0.000853000	24.6.173.220	67.192.92.227	HTTP	ad.audi...	POST /adserver?u=97df6f8f88d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=50912&l=20121102085149&of=

< Frame 10022: 1595 bytes on wire (12760 bits), 1595 bytes captured (12760 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: 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

> 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

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

Paquetes: 11678 · Mostrado: 12 (0.1%)

Perfil: wireshark101