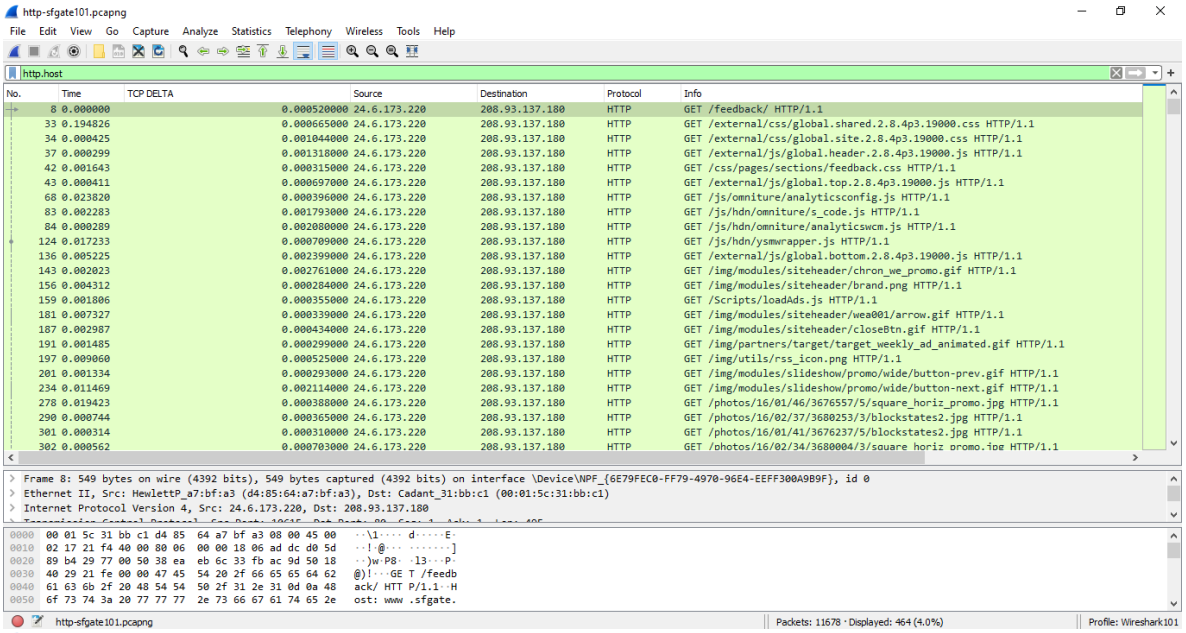
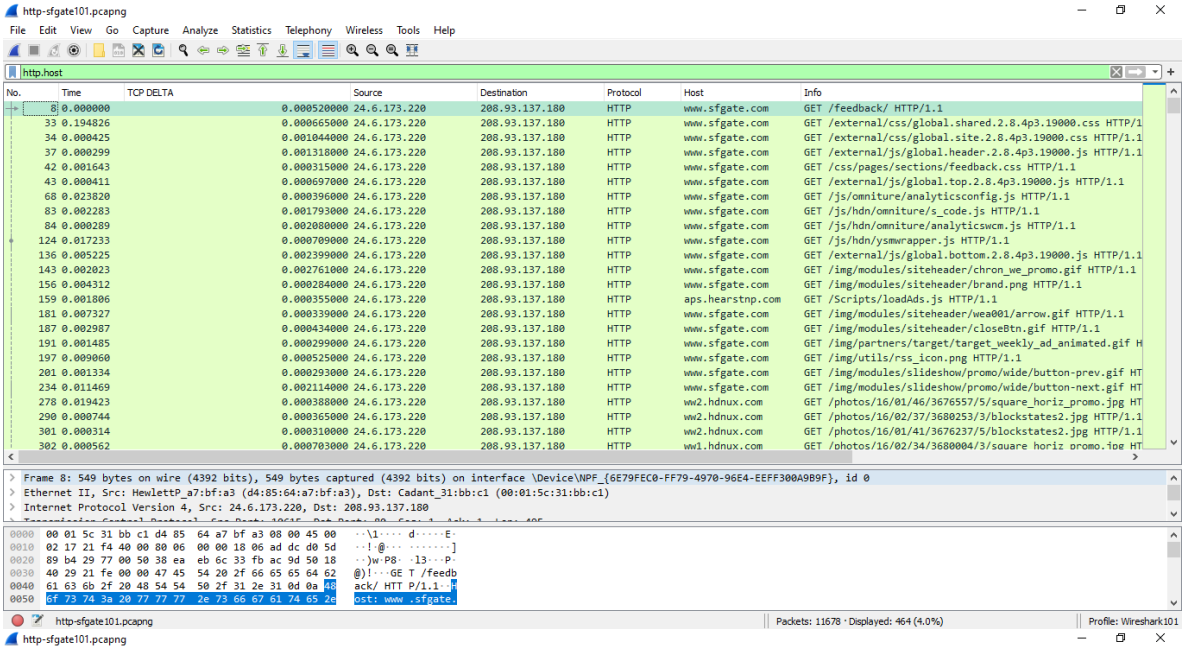
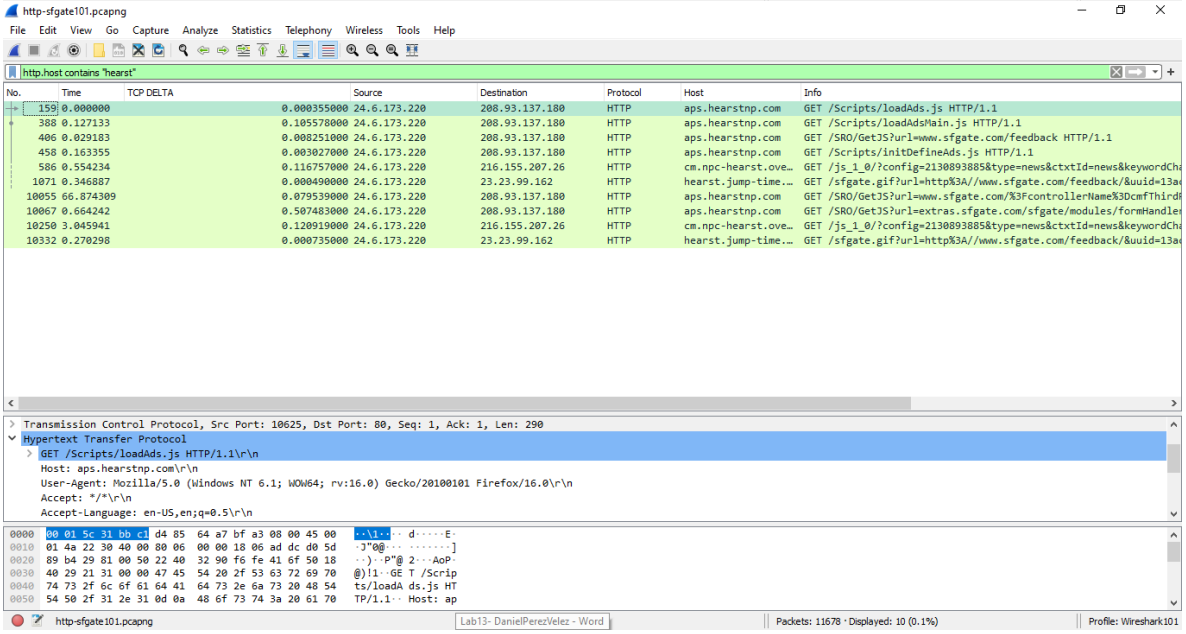
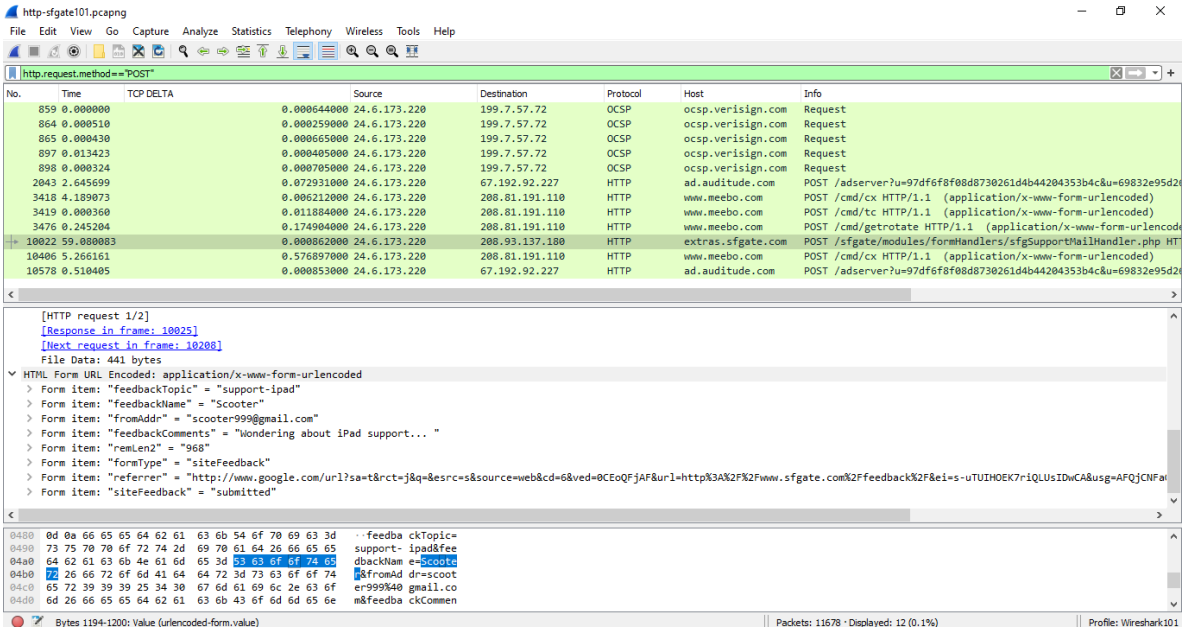
Laboratorio 14
Wireshark

Wilmer Rodríguez Jiménez
Fundamentos de telecomunicaciones
Prof: Ismael Jimenez Sanchez
Periodo Ago – Dic


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host
No. Time TCP DELTA Source Destination Protocol Info
8 0.000000 0.000520000 24.6.173.220 208.93.137.180 HTTP GET /feedback/ HTTP/1.1
33 0.194826 0.000665000 24.6.173.220 208.93.137.180 HTTP 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 GET /external/css/global.site.2.8.4p3.19000.css HTTP/1.1
37 0.000299 0.001318000 24.6.173.220 208.93.137.180 HTTP GET /external/js/global.header.2.8.4p3.19000.js HTTP/1.1
42 0.001643 0.000315000 24.6.173.220 208.93.137.180 HTTP GET /css/pages/sections/feedback.css HTTP/1.1
43 0.000411 0.000697000 24.6.173.220 208.93.137.180 HTTP GET /external/js/global.top.2.8.4p3.19000.js HTTP/1.1
68 0.023820 0.000396000 24.6.173.220 208.93.137.180 HTTP GET /js/omniture/analyticsconfig.js HTTP/1.1
83 0.002283 0.001793000 24.6.173.220 208.93.137.180 HTTP GET /js/hdn/omniture/s_code.js HTTP/1.1
84 0.000289 0.002080000 24.6.173.220 208.93.137.180 HTTP GET /js/hdn/omniture/analyticswcm.js HTTP/1.1
124 0.017233 0.000709000 24.6.173.220 208.93.137.180 HTTP GET /js/hdn/ysmwrapper.js HTTP/1.1
136 0.005225 0.002399000 24.6.173.220 208.93.137.180 HTTP GET /external/js/global.bottom.2.8.4p3.19000.js HTTP/1.1
143 0.002023 0.002761000 24.6.173.220 208.93.137.180 HTTP GET /img/modules/siteheader/chron_we_promo.gif HTTP/1.1
156 0.004312 0.000284000 24.6.173.220 208.93.137.180 HTTP GET /img/modules/siteheader/brand.png HTTP/1.1
159 0.001806 0.000355000 24.6.173.220 208.93.137.180 HTTP GET /Scripts/loadAds.js HTTP/1.1
181 0.007327 0.000339000 24.6.173.220 208.93.137.180 HTTP GET /img/modules/siteheader/wea001/arrow.gif HTTP/1.1
187 0.002987 0.000434000 24.6.173.220 208.93.137.180 HTTP GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
191 0.001485 0.000299000 24.6.173.220 208.93.137.180 HTTP GET /img/partners/target/target_weekly_ad_animated.gif HTTP/1.1
197 0.009060 0.000525000 24.6.173.220 208.93.137.180 HTTP GET /img/utils/rss_icon.png HTTP/1.1
201 0.001334 0.000293000 24.6.173.220 208.93.137.180 HTTP GET /img/modules/slideshow/promo/wide/button-prev.gif HTTP/1.1
234 0.011469 0.002114000 24.6.173.220 208.93.137.180 HTTP GET /img/modules/slideshow/promo/wide/button-next.gif HTTP/1.1
278 0.019423 0.000388000 24.6.173.220 208.93.137.180 HTTP GET /photos/16/01/46/3676557/5/square_horiz_promo.jpg HTTP/1.1
290 0.000744 0.000365000 24.6.173.220 208.93.137.180 HTTP GET /photos/16/02/37/3680253/3/blockstates2.jpg HTTP/1.1
301 0.000314 0.000310000 24.6.173.220 208.93.137.180 HTTP GET /photos/16/01/41/3676237/5/blockstates2.jpg HTTP/1.1
302 0.000562 0.000703000 24.6.173.220 208.93.137.180 HTTP GET /photos/16/02/34/3680004/3/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
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.
http-sfgate101.pcapng
Packets: 11678 · Displayed: 464 (4.0%)
Profile: Wireshark101


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host
No. Time TCP DELTA Source Destination Protocol Host Info
8 0.000000 0.000520000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /feedback/ HTTP/1.1
33 0.194826 0.000665000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /external/css/global.shared.2.8.4p3.19000.css HTTP/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 0.000299 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 0.001643 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 0.023820 0.000396000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /js/omniture/analyticsconfig.js HTTP/1.1
83 0.002283 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/analyticswcm.js HTTP/1.1
124 0.017233 0.000709000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /js/hdn/ysmwrapper.js HTTP/1.1
136 0.005225 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 0.002023 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 0.004312 0.000284000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /img/modules/siteheader/brand.png HTTP/1.1
159 0.001806 0.000355000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /Scripts/loadAds.js HTTP/1.1
181 0.007327 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 0.002987 0.000434000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
191 0.001485 0.000299000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /img/partners/target/target_weekly_ad_animated.gif H
197 0.009060 0.000525000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /img/utils/rss_icon.png HTTP/1.1
201 0.001334 0.000293000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /img/modules/slideshow/promo/wide/button-prev.gif HT
234 0.011469 0.002114000 24.6.173.220 208.93.137.180 HTTP www.sfgate.com GET /img/modules/slideshow/promo/wide/button-next.gif HT
278 0.019423 0.000388000 24.6.173.220 208.93.137.180 HTTP ww2.hdnux.com GET /photos/16/01/46/3676557/5/square_horiz_promo.jpg HT
290 0.000744 0.000365000 24.6.173.220 208.93.137.180 HTTP ww2.hdnux.com GET /photos/16/02/37/3680253/3/blockstates2.jpg HTTP/1.1
301 0.000314 0.000310000 24.6.173.220 208.93.137.180 HTTP ww2.hdnux.com GET /photos/16/01/41/3676237/5/blockstates2.jpg HTTP/1.1
302 0.000562 0.000703000 24.6.173.220 208.93.137.180 HTTP ww1.hdnux.com GET /photos/16/02/34/3680004/3/square_horiz_promo.jpg HT
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
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.
http-sfgate101.pcapng
Packets: 11678 · Displayed: 464 (4.0%)
Profile: Wireshark101


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host contains "hearst"
No. Time TCP DELTA Source Destination Protocol Host Info
159 0.000000 0.000355000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /Scripts/loadAds.js HTTP/1.1
388 0.127133 0.105578000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /Scripts/loadAdsMain.js HTTP/1.1
406 0.029183 0.008251000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /SRO/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458 0.163355 0.003027000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /Scripts/initDefineAds.js HTTP/1.1
586 0.554234 0.116757000 24.6.173.220 216.155.207.26 HTTP cm.npc-hearst.ove… GET /js_1_0/?config=2130893885&type=news&ctxtId=news&keywordCha
1071 0.346887 0.000490000 24.6.173.220 23.23.99.162 HTTP hearst.jump-time.… GET /sfgate.gif?url=http%3A//www.sfgate.com/feedback/&uuid=13a
10055 66.874309 0.079539000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmfThirdF
10067 0.664242 0.507483000 24.6.173.220 208.93.137.180 HTTP aps.hearstnp.com GET /SRO/GetJS?url=extras.sfgate.com/sfgate/modules/formHandle
10250 3.045941 0.120919000 24.6.173.220 216.155.207.26 HTTP cm.npc-hearst.ove… GET /js_1_0/?config=2130893885&type=news&ctxtId=news&keywordCha
10332 0.270298 0.000735000 24.6.173.220 23.23.99.162 HTTP hearst.jump-time.… GET /sfgate.gif?url=http%3A//www.sfgate.com/feedback/&uuid=13a
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
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
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
http-sfgate101.pcapng
Lab13- DanielPerezVelez - Word
Packets: 11678 · Displayed: 10 (0.1%)
Profile: Wireshark101


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method=="POST"
No. Time TCP DELTA Source Destination Protocol Host Info
859 0.000000 0.000644000 24.6.173.220 199.7.57.72 OCSP ocsp.verisign.com Request
864 0.000510 0.000259000 24.6.173.220 199.7.57.72 OCSP ocsp.verisign.com Request
865 0.000430 0.000665000 24.6.173.220 199.7.57.72 OCSP ocsp.verisign.com Request
897 0.013423 0.000405000 24.6.173.220 199.7.57.72 OCSP ocsp.verisign.com Request
898 0.000324 0.000705000 24.6.173.220 199.7.57.72 OCSP ocsp.verisign.com Request
2043 2.645699 0.072931000 24.6.173.220 67.192.92.227 HTTP ad.auditude.com POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d2
3418 4.189073 0.006212000 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 0.011884000 24.6.173.220 208.81.191.110 HTTP www.meebo.com POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
3476 0.245204 0.174904000 24.6.173.220 208.81.191.110 HTTP www.meebo.com POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencod
10022 59.080083 0.000862000 24.6.173.220 208.93.137.180 HTTP extras.sfgate.com POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HT
10406 5.266161 0.576897000 24.6.173.220 208.81.191.110 HTTP www.meebo.com POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
10578 0.510405 0.000853000 24.6.173.220 67.192.92.227 HTTP ad.auditude.com POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d2
[HTTP request 1/2]
[Response in frame: 10025]
[Next request in frame: 10208]
File Data: 441 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "feedbackTopic" = "support-ipad"
Form item: "feedbackName" = "Scooter"
Form item: "fromAddr" = "scooter999@gmail.com"
Form item: "feedbackComments" = "Wondering about iPad support... "
Form item: "remLen2" = "968"
Form item: "formType" = "siteFeedback"
Form item: "referrer" = "http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CEoQFjAF&url=http%3A%2F%2Fwww.sfgate.com%2Ffeedback%2F&ei=s-uTUIHOEK7riQLUsIDwCA&usg=AFQjCNFa
Form item: "siteFeedback" = "submitted"
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=Scote
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
Bytes 1194-1200: Value (urlencoded-form.value)
Packets: 11678 · Displayed: 12 (0.1%)
Profile: Wireshark101