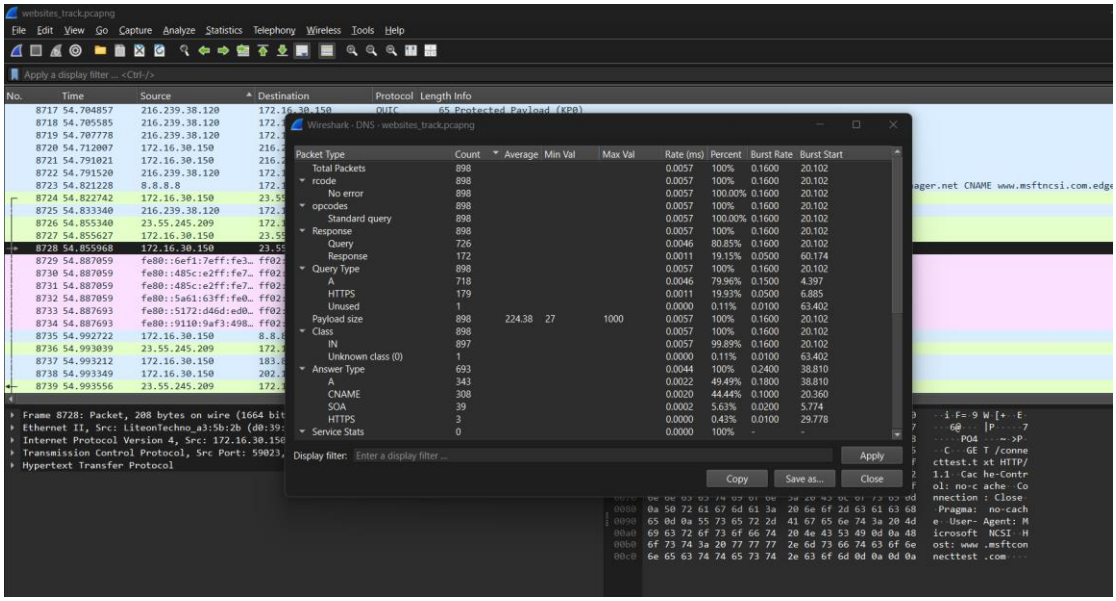
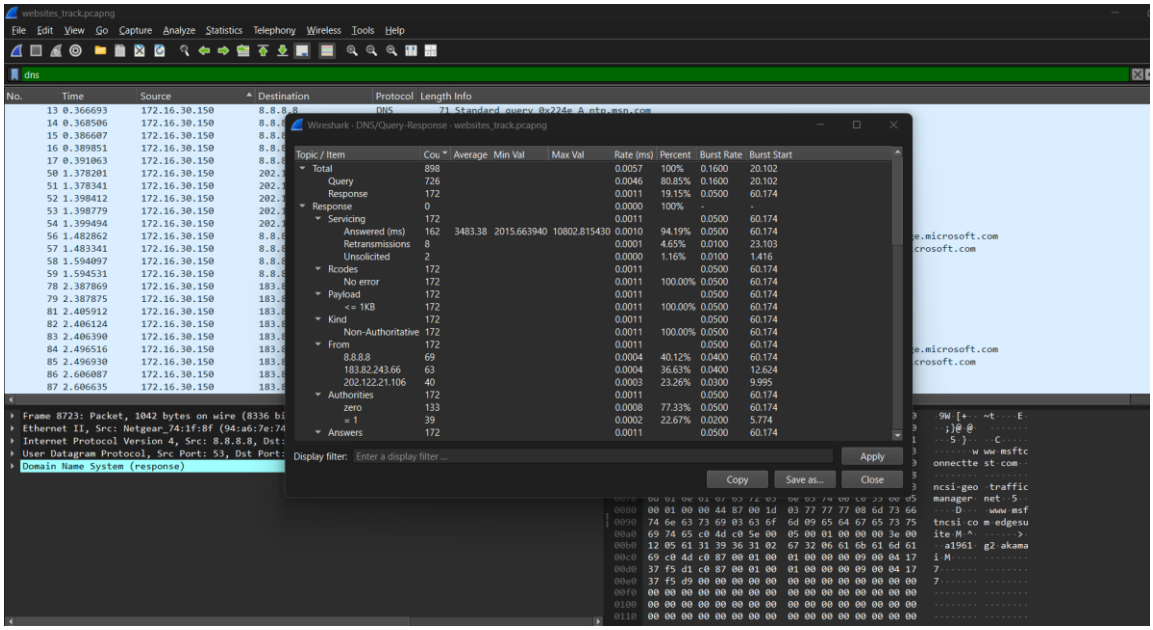
Task1:

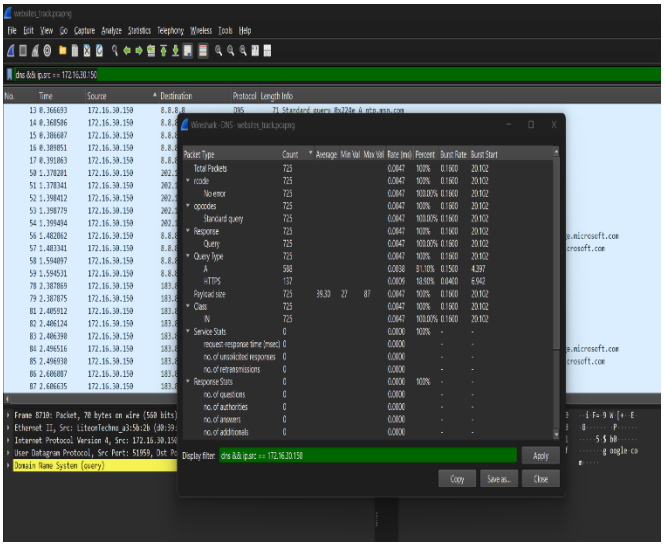
Dns queries are sent from your browser to dns server.



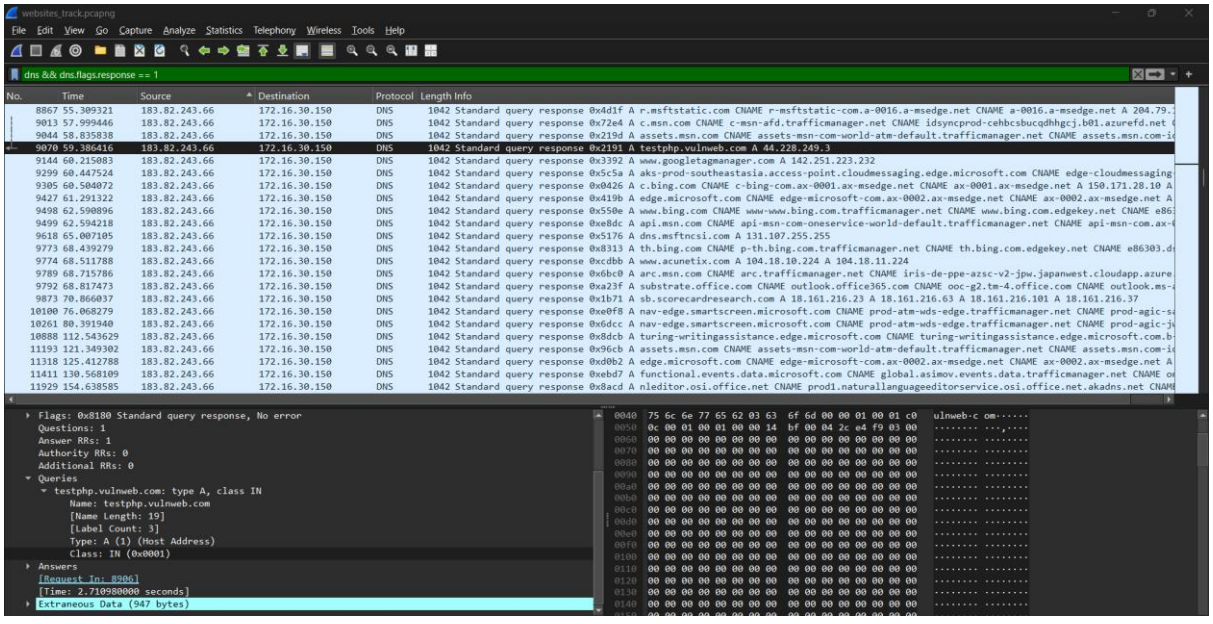
DNS servers are involved

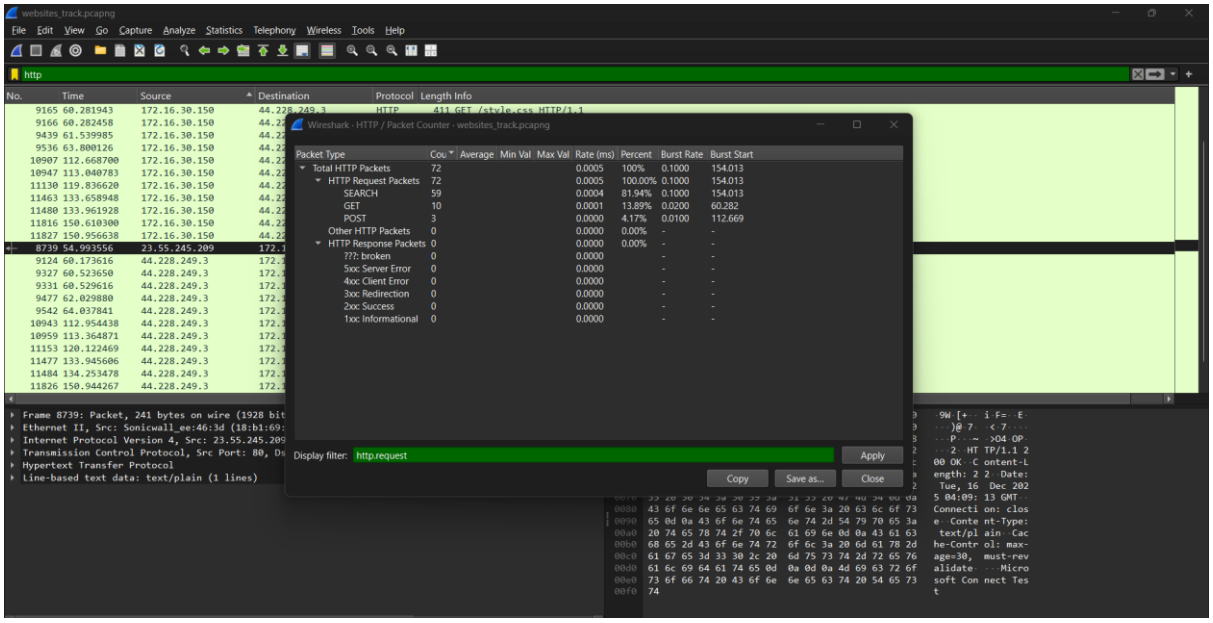


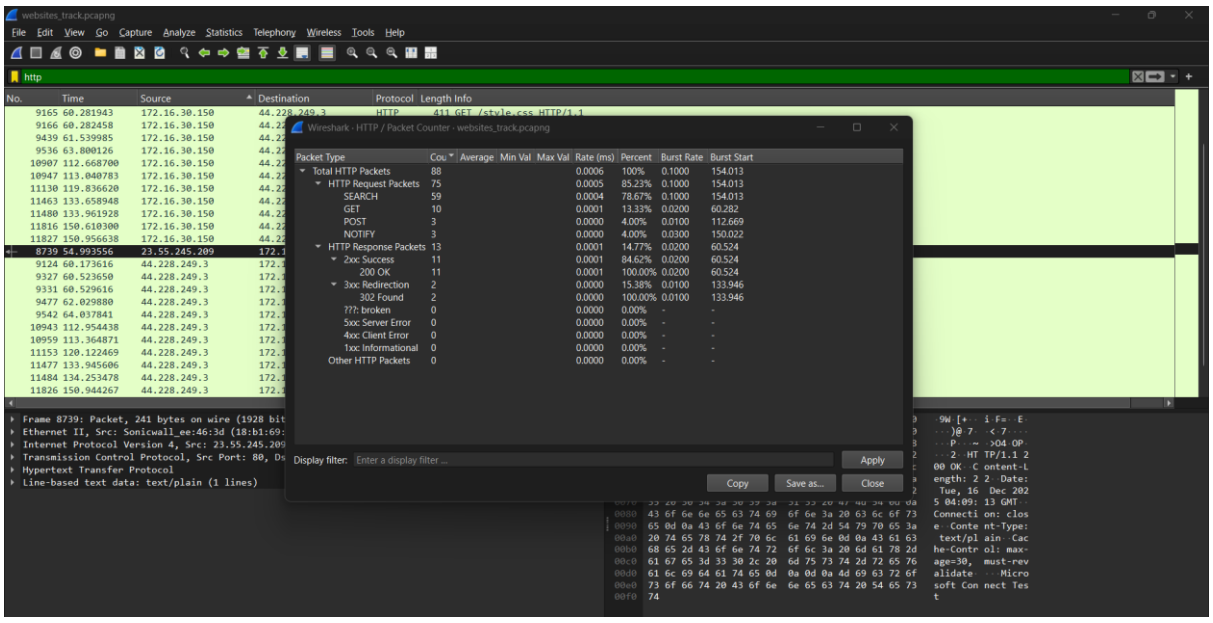
Which DNS Server replies with actual IP Address.

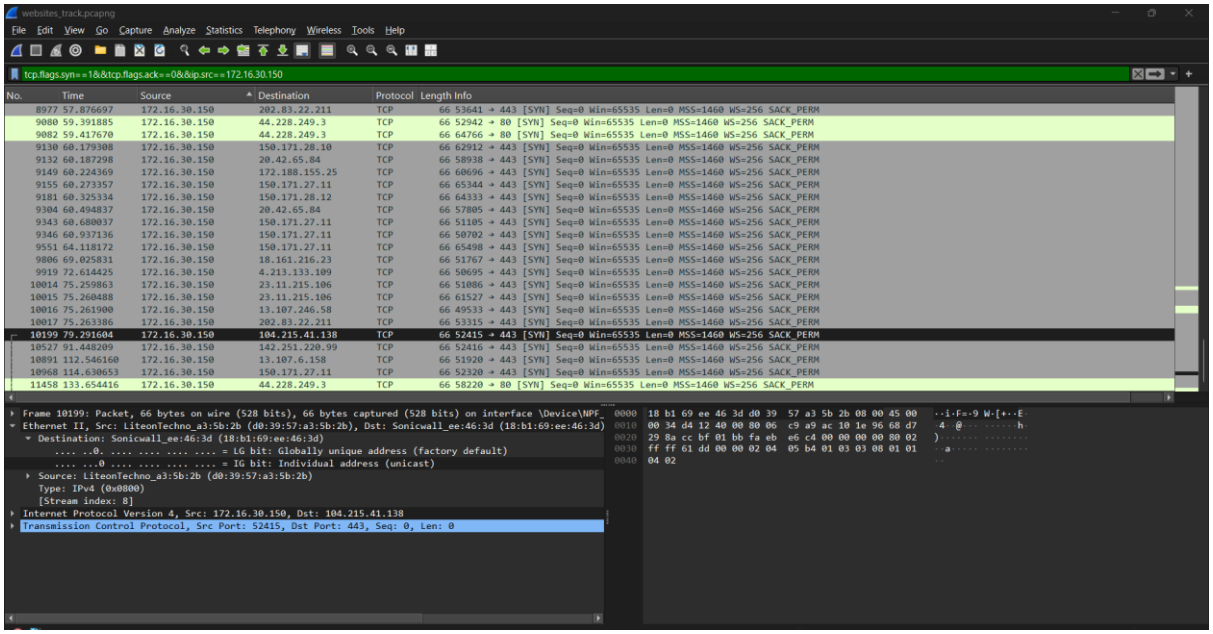


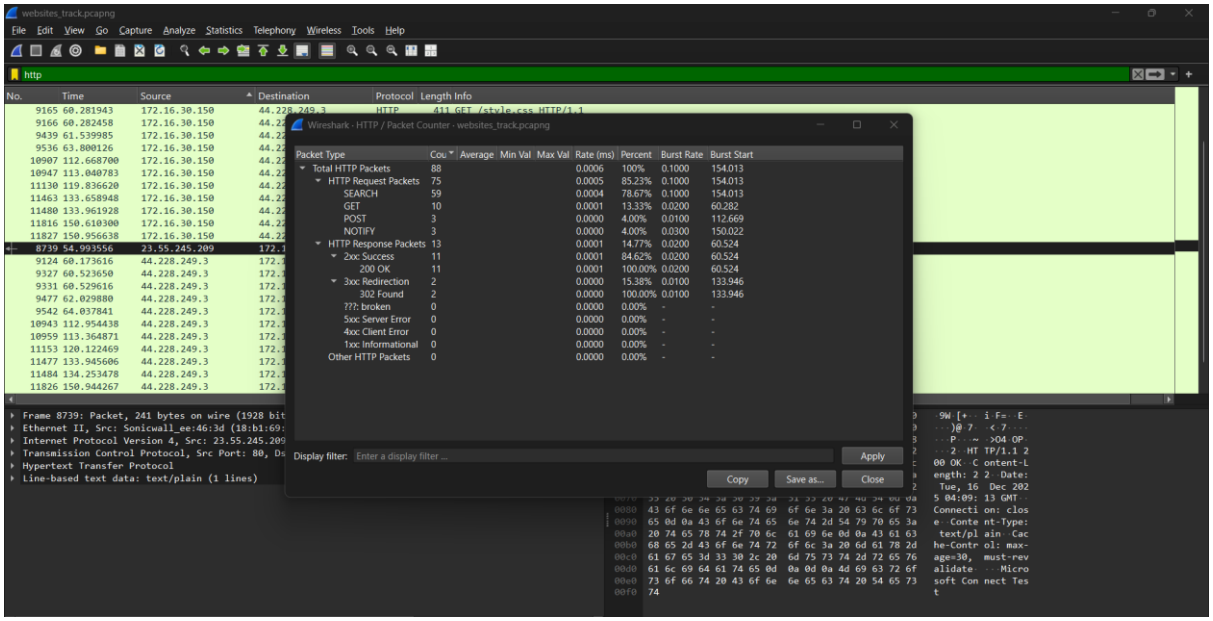
Clearly list the resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation including queries and response.

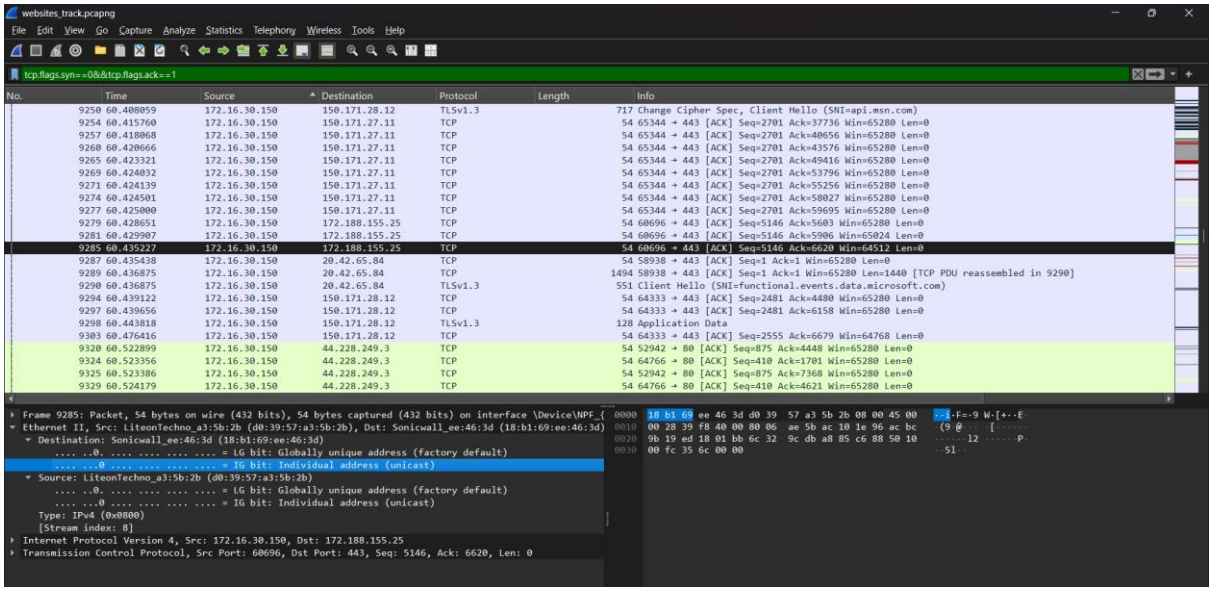


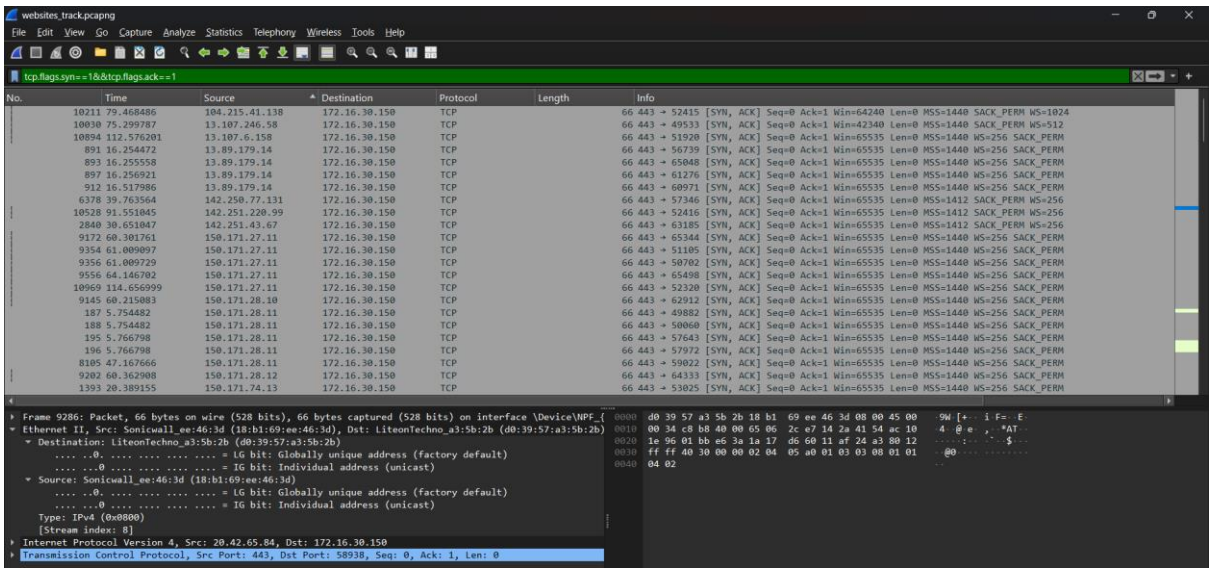

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9165 60.281943 172.16.30.150 44.228.249.3 HTTP 411 GET /style.css HTTP/1.1
9166 60.282458 172.16.30.150 44.22
9439 61.539985 172.16.30.150 44.22
9536 63.800126 172.16.30.150 44.22
10907 112.668700 172.16.30.150 44.22
10947 113.040783 172.16.30.150 44.22
11130 119.836620 172.16.30.150 44.22
11463 133.658948 172.16.30.150 44.22
11480 133.961928 172.16.30.150 44.22
11816 150.610300 172.16.30.150 44.22
11827 150.956638 172.16.30.150 44.22
8739 54.993556 23.55.245.209 172.1
9124 60.173616 44.228.249.3 172.1
9327 60.523650 44.228.249.3 172.1
9331 60.529616 44.228.249.3 172.1
9477 62.029880 44.228.249.3 172.1
9542 64.037841 44.228.249.3 172.1
10943 112.954438 44.228.249.3 172.1
10959 113.364871 44.228.249.3 172.1
11153 120.122469 44.228.249.3 172.1
11477 133.945606 44.228.249.3 172.1
11484 134.253478 44.228.249.3 172.1
11826 150.944267 44.228.249.3 172.1
Frame 8739: Packet, 241 bytes on wire (1928 bit
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:
Internet Protocol Version 4, Src: 23.55.245.209
Transmission Control Protocol, Src Port: 80, Ds
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
Wireshark · HTTP / Packet Counter · websites_track.pcapng
Packet Type Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Total HTTP Packets 72 0.0005 100% 0.1000 154.013
HTTP Request Packets 72 0.0005 100.00% 0.1000 154.013
SEARCH 59 0.0004 81.94% 0.1000 154.013
GET 10 0.0001 13.89% 0.0200 60.282
POST 3 0.0000 4.17% 0.0100 112.669
Other HTTP Packets 0 0.0000 0.00% - -
HTTP Response Packets 0 0.0000 0.00% - -
???: broken 0 0.0000 - -
5xx: Server Error 0 0.0000 - -
4xx: Client Error 0 0.0000 - -
3xx: Redirection 0 0.0000 - -
2xx: Success 0 0.0000 - -
1xx: Informational 0 0.0000 - -
Display filter: http.request
Apply
Copy
Save as...
Close

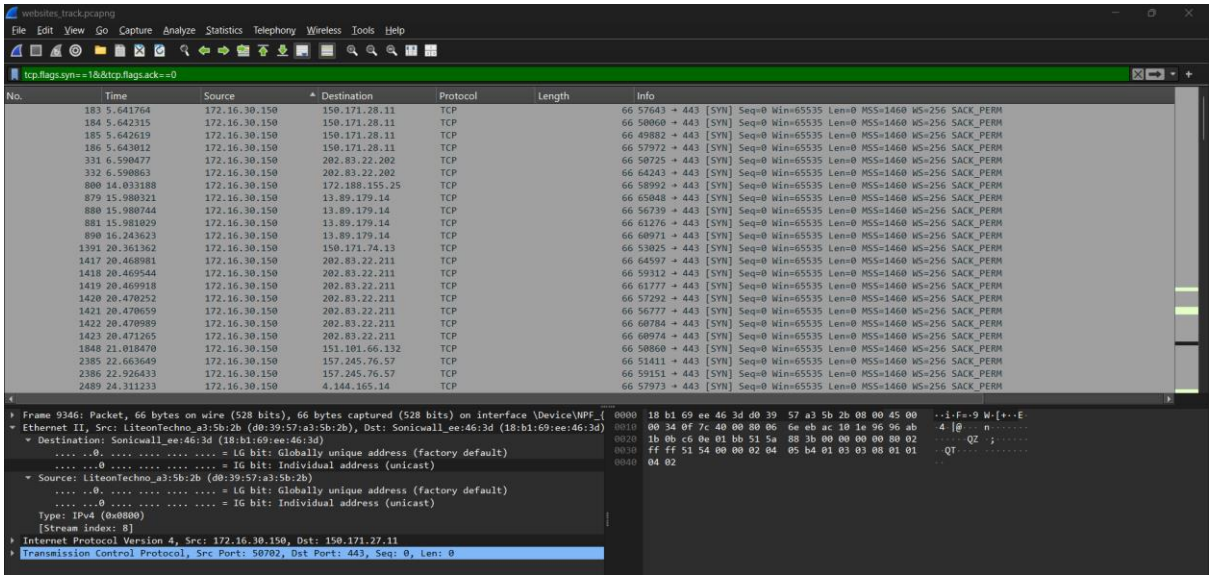

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9165 60.281943 172.16.30.150 44.228.249.3 HTTP 411 GET /style.css HTTP/1.1
9166 60.282458 172.16.30.150 44.22
9439 61.539985 172.16.30.150 44.22
9536 63.800126 172.16.30.150 44.22
10907 112.668700 172.16.30.150 44.22
10947 113.040783 172.16.30.150 44.22
11130 119.836620 172.16.30.150 44.22
11463 133.658948 172.16.30.150 44.22
11480 133.961928 172.16.30.150 44.22
11816 150.610300 172.16.30.150 44.22
11827 150.956638 172.16.30.150 44.22
8739 54.993556 23.55.245.209 172.1
9124 60.173616 44.228.249.3 172.1
9327 60.523650 44.228.249.3 172.1
9331 60.529616 44.228.249.3 172.1
9477 62.029880 44.228.249.3 172.1
9542 64.037841 44.228.249.3 172.1
10943 112.954438 44.228.249.3 172.1
10959 113.364871 44.228.249.3 172.1
11153 120.122469 44.228.249.3 172.1
11477 133.945606 44.228.249.3 172.1
11484 134.253478 44.228.249.3 172.1
11826 150.944267 44.228.249.3 172.1
Frame 8739: Packet, 241 bytes on wire (1928 bit
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:
Internet Protocol Version 4, Src: 23.55.245.209
Transmission Control Protocol, Src Port: 80, Ds
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
Wireshark · HTTP / Packet Counter · websites_track.pcapng
Packet Type Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Total HTTP Packets 88 0.0006 100% 0.1000 154.013
HTTP Request Packets 75 0.0005 85.23% 0.1000 154.013
SEARCH 59 0.0004 78.67% 0.1000 154.013
GET 10 0.0001 13.33% 0.0200 60.282
POST 3 0.0000 4.00% 0.0100 112.669
NOTIFY 3 0.0000 4.00% 0.0300 150.022
HTTP Response Packets 13 0.0001 14.77% 0.0200 60.524
2xx: Success 11 0.0001 84.62% 0.0200 60.524
200 OK 11 0.0001 100.00% 0.0200 60.524
3xx: Redirection 2 0.0000 15.38% 0.0100 133.946
302 Found 2 0.0000 100.00% 0.0100 133.946
???: broken 0 0.0000 0.00% - -
5xx: Server Error 0 0.0000 0.00% - -
4xx: Client Error 0 0.0000 0.00% - -
1xx: Informational 0 0.0000 0.00% - -
Other HTTP Packets 0 0.0000 0.00% - -
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

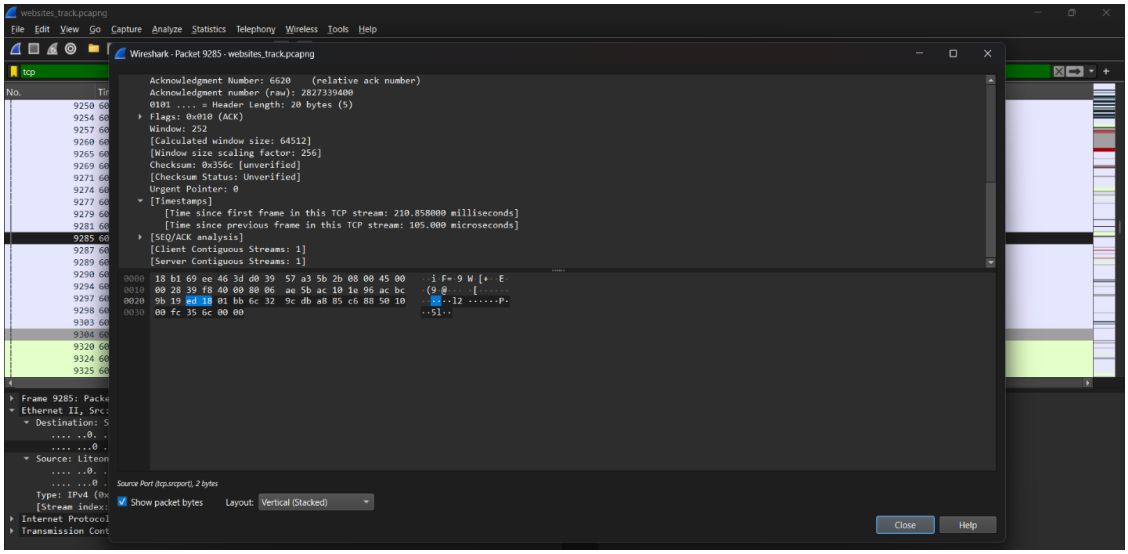

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1&&tcp.flags.ack==0&&ip.src==172.16.30.150
No. Time Source Destination Protocol Length Info
8977 57.876697 172.16.30.150 202.83.22.211 TCP 66 53641 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9080 59.391885 172.16.30.150 44.228.249.3 TCP 66 52942 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9082 59.417670 172.16.30.150 44.228.249.3 TCP 66 64766 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9130 60.179308 172.16.30.150 150.171.28.10 TCP 66 62912 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9132 60.187298 172.16.30.150 20.42.65.84 TCP 66 58938 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9149 60.224369 172.16.30.150 172.188.155.25 TCP 66 60696 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9155 60.273357 172.16.30.150 150.171.27.11 TCP 66 65344 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9181 60.325334 172.16.30.150 150.171.28.12 TCP 66 64333 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9304 60.494837 172.16.30.150 20.42.65.84 TCP 66 57805 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9343 60.680037 172.16.30.150 150.171.27.11 TCP 66 51105 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9346 60.937136 172.16.30.150 150.171.27.11 TCP 66 50702 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9551 64.118172 172.16.30.150 150.171.27.11 TCP 66 65498 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9806 69.025831 172.16.30.150 18.161.216.23 TCP 66 51767 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9919 72.614425 172.16.30.150 4.213.133.109 TCP 66 50695 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10014 75.259863 172.16.30.150 23.11.215.106 TCP 66 51086 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10015 75.260488 172.16.30.150 23.11.215.106 TCP 66 61527 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10016 75.261900 172.16.30.150 13.107.246.58 TCP 66 49533 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10017 75.263386 172.16.30.150 202.83.22.211 TCP 66 53315 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10199 79.291604 172.16.30.150 104.215.41.138 TCP 66 52415 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10527 91.448209 172.16.30.150 142.251.220.99 TCP 66 52416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10891 112.546160 172.16.30.150 13.107.6.158 TCP 66 51920 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10968 114.630653 172.16.30.150 150.171.27.11 TCP 66 52320 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11458 133.654416 172.16.30.150 44.228.249.3 TCP 66 58220 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Frame 10199: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_
Ethernet II, Src: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
Destination: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
Type: IPv4 (0x0800)
[Stream index: 8]
Internet Protocol Version 4, Src: 172.16.30.150, Dst: 104.215.41.138
Transmission Control Protocol, Src Port: 52415, Dst Port: 443, Seq: 0, Len: 0
0000 18 b1 69 ee 46 3d d0 39 57 a3 5b 2b 08 00 45 00
0010 00 34 d4 12 40 00 80 06 c9 a9 ac 10 1e 96 68 d7
0020 29 8a cc bf 01 bb fa eb e6 c4 00 00 00 00 80 02
0030 ff ff 61 dd 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02

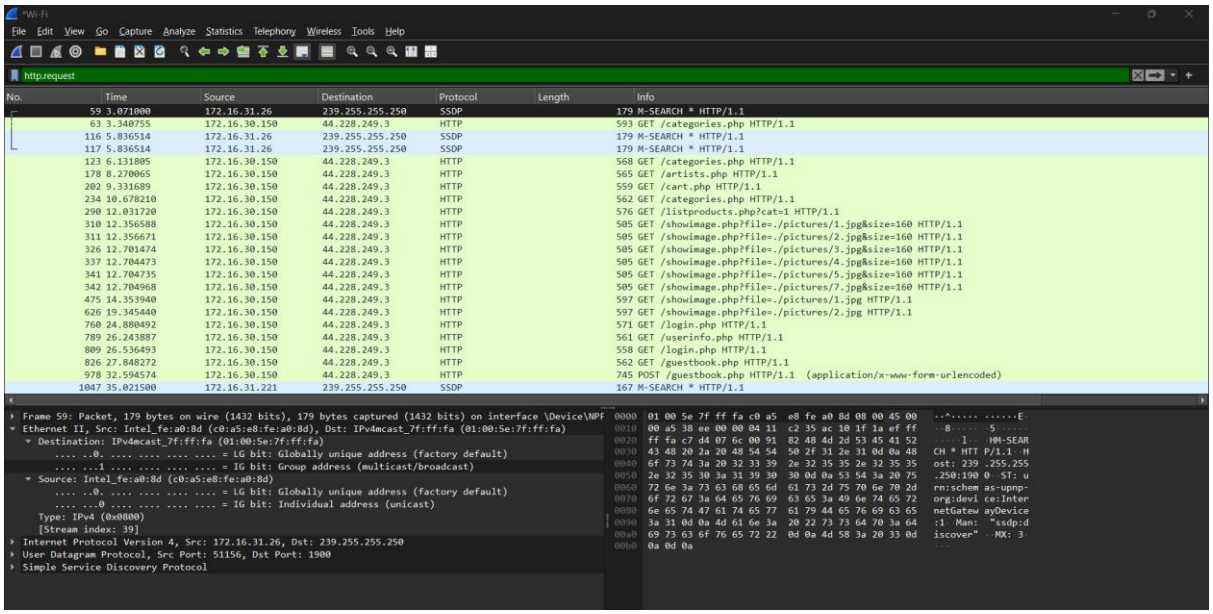

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9165 60.281943 172.16.30.150 44.228.249.3 HTTP 411 GET /style.css HTTP/1.1
9166 60.282458 172.16.30.150 44.22
9439 61.539985 172.16.30.150 44.22
9536 63.800126 172.16.30.150 44.22
10907 112.668700 172.16.30.150 44.22
10947 113.040783 172.16.30.150 44.22
11130 119.836620 172.16.30.150 44.22
11463 133.658948 172.16.30.150 44.22
11480 133.961928 172.16.30.150 44.22
11816 150.610300 172.16.30.150 44.22
11827 150.956638 172.16.30.150 44.22
8739 54.993556 23.55.245.209 172.1
9124 60.173616 44.228.249.3 172.1
9327 60.523650 44.228.249.3 172.1
9331 60.529616 44.228.249.3 172.1
9477 62.029880 44.228.249.3 172.1
9542 64.037841 44.228.249.3 172.1
10943 112.954438 44.228.249.3 172.1
10959 113.364871 44.228.249.3 172.1
11153 120.122469 44.228.249.3 172.1
11477 133.945606 44.228.249.3 172.1
11484 134.253478 44.228.249.3 172.1
11826 150.944267 44.228.249.3 172.1
Wireshark · HTTP / Packet Counter · websites_track.pcapng
Packet Type Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Total HTTP Packets 88 0.0006 100% 0.1000 154.013
HTTP Request Packets 75 0.0005 85.23% 0.1000 154.013
SEARCH 59 0.0004 78.67% 0.1000 154.013
GET 10 0.0001 13.33% 0.0200 60.282
POST 3 0.0000 4.00% 0.0100 112.669
NOTIFY 3 0.0000 4.00% 0.0300 150.022
HTTP Response Packets 13 0.0001 14.77% 0.0200 60.524
2xx: Success 11 0.0001 84.62% 0.0200 60.524
200 OK 11 0.0001 100.00% 0.0200 60.524
3xx: Redirection 2 0.0000 15.38% 0.0100 133.946
302 Found 2 0.0000 100.00% 0.0100 133.946
???: broken 0 0.0000 0.00% - -
5xx: Server Error 0 0.0000 0.00% - -
4xx: Client Error 0 0.0000 0.00% - -
1xx: Informational 0 0.0000 0.00% - -
Other HTTP Packets 0 0.0000 0.00% - -
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
Frame 8739: Packet, 241 bytes on wire (1928 bit
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:
Internet Protocol Version 4, Src: 23.55.245.209
Transmission Control Protocol, Src Port: 80, Ds
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)

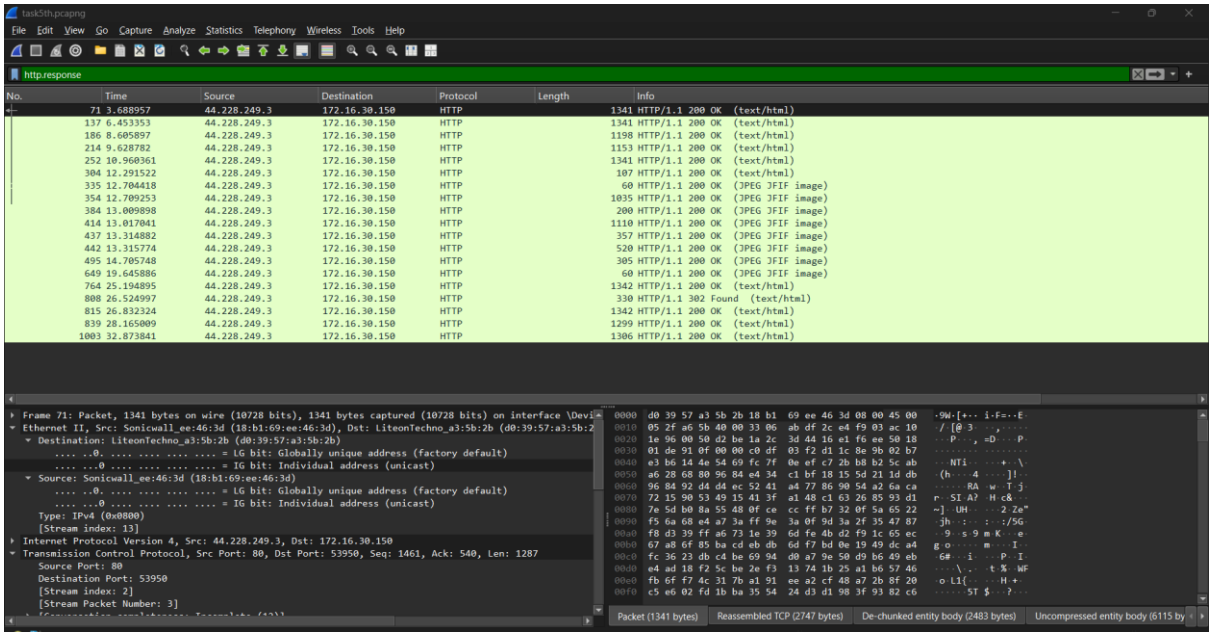

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==0&&tcp.flags.ack==1
No. Time Source Destination Protocol Length Info
9250 60.408059 172.16.30.150 150.171.28.12 TLSv1.3 717 Change Cipher Spec, Client Hello (SNI=api.msn.com)
9254 60.415760 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=37736 Win=65280 Len=0
9257 60.418068 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=40656 Win=65280 Len=0
9260 60.420666 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=43576 Win=65280 Len=0
9265 60.423321 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=49416 Win=65280 Len=0
9269 60.424032 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=53796 Win=65280 Len=0
9271 60.424139 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=55256 Win=65280 Len=0
9274 60.424501 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=58027 Win=65280 Len=0
9277 60.425000 172.16.30.150 150.171.27.11 TCP 54 65344 → 443 [ACK] Seq=2701 Ack=59695 Win=65280 Len=0
9279 60.428651 172.16.30.150 172.188.155.25 TCP 54 60696 → 443 [ACK] Seq=5146 Ack=5603 Win=65280 Len=0
9281 60.429907 172.16.30.150 172.188.155.25 TCP 54 60696 → 443 [ACK] Seq=5146 Ack=5906 Win=65024 Len=0
9285 60.435227 172.16.30.150 172.188.155.25 TCP 54 60696 → 443 [ACK] Seq=5146 Ack=6620 Win=64512 Len=0
9287 60.435438 172.16.30.150 20.42.65.84 TCP 54 58938 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
9289 60.436875 172.16.30.150 20.42.65.84 TCP 1494 58938 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1440 [TCP PDU reassembled in 9290]
9290 60.436875 172.16.30.150 20.42.65.84 TLSv1.3 551 Client Hello (SNI=functional.events.data.microsoft.com)
9294 60.439122 172.16.30.150 150.171.28.12 TCP 54 64333 → 443 [ACK] Seq=2481 Ack=4480 Win=65280 Len=0
9297 60.439656 172.16.30.150 150.171.28.12 TCP 54 64333 → 443 [ACK] Seq=2481 Ack=6158 Win=65280 Len=0
9298 60.443818 172.16.30.150 150.171.28.12 TLSv1.3 128 Application Data
9303 60.476416 172.16.30.150 150.171.28.12 TCP 54 64333 → 443 [ACK] Seq=2555 Ack=6679 Win=64768 Len=0
9320 60.522899 172.16.30.150 44.228.249.3 TCP 54 52942 → 80 [ACK] Seq=875 Ack=4448 Win=65280 Len=0
9324 60.523356 172.16.30.150 44.228.249.3 TCP 54 64766 → 80 [ACK] Seq=410 Ack=1701 Win=65280 Len=0
9325 60.523386 172.16.30.150 44.228.249.3 TCP 54 52942 → 80 [ACK] Seq=875 Ack=7368 Win=65280 Len=0
9329 60.524179 172.16.30.150 44.228.249.3 TCP 54 64766 → 80 [ACK] Seq=410 Ack=4621 Win=65280 Len=0
Frame 9285: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{
Ethernet II, Src: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
Destination: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 8]
Internet Protocol Version 4, Src: 172.16.30.150, Dst: 172.188.155.25
Transmission Control Protocol, Src Port: 60696, Dst Port: 443, Seq: 5146, Ack: 6620, Len: 0
0000 18 b1 69 ee 46 3d d0 39 57 a3 5b 2b 08 00 45 00
0010 00 28 39 f0 40 00 80 06 ae 5b ac 10 1e 96 ac bc
0020 9b 19 ed 18 01 bb 6c 32 9c db a8 85 c6 88 50 10
0030 00 fc 35 6c 00 00

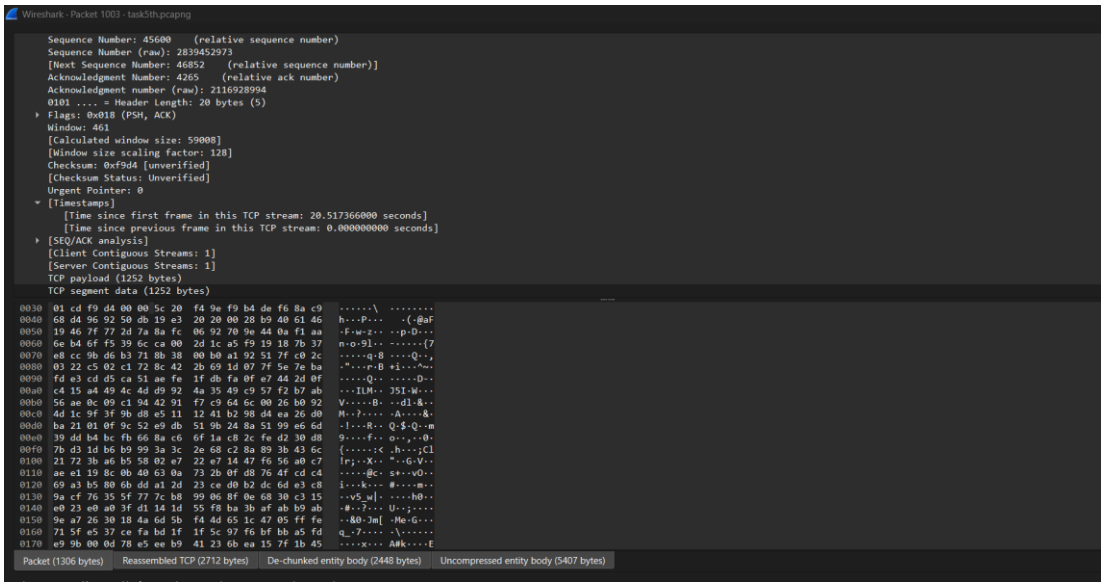

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1&&tcp.flags.ack==1
No. Time Source Destination Protocol Length Info
10211 79.468486 104.215.41.138 172.16.30.150 TCP 66 443 → 52415 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM WS=1024
10030 75.299787 13.107.246.58 172.16.30.150 TCP 66 443 → 49533 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1440 SACK_PERM WS=512
10894 112.576201 13.107.6.158 172.16.30.150 TCP 66 443 → 51920 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
891 16.254472 13.89.179.14 172.16.30.150 TCP 66 443 → 56739 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
893 16.255558 13.89.179.14 172.16.30.150 TCP 66 443 → 65048 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
897 16.256921 13.89.179.14 172.16.30.150 TCP 66 443 → 61276 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
912 16.517986 13.89.179.14 172.16.30.150 TCP 66 443 → 60971 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
6378 39.763564 142.250.77.131 172.16.30.150 TCP 66 443 → 57346 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
10528 91.551045 142.251.220.99 172.16.30.150 TCP 66 443 → 52416 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
2840 30.651047 142.251.43.67 172.16.30.150 TCP 66 443 → 63185 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
9172 60.301761 150.171.27.11 172.16.30.150 TCP 66 443 → 65344 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
9354 61.009097 150.171.27.11 172.16.30.150 TCP 66 443 → 51105 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
9356 61.009729 150.171.27.11 172.16.30.150 TCP 66 443 → 50702 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
9556 64.146702 150.171.27.11 172.16.30.150 TCP 66 443 → 65498 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
10969 114.656999 150.171.27.11 172.16.30.150 TCP 66 443 → 52320 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
9145 60.215083 150.171.28.10 172.16.30.150 TCP 66 443 → 62912 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
187 5.754482 150.171.28.11 172.16.30.150 TCP 66 443 → 49882 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
188 5.754482 150.171.28.11 172.16.30.150 TCP 66 443 → 50060 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
195 5.766798 150.171.28.11 172.16.30.150 TCP 66 443 → 57643 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
196 5.766798 150.171.28.11 172.16.30.150 TCP 66 443 → 57972 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
8105 47.167666 150.171.28.11 172.16.30.150 TCP 66 443 → 59022 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
9202 60.362908 150.171.28.12 172.16.30.150 TCP 66 443 → 64333 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
1393 20.389155 150.171.74.13 172.16.30.150 TCP 66 443 → 53025 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
Frame 9286: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
Destination: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 8]
Internet Protocol Version 4, Src: 20.42.65.84, Dst: 172.16.30.150
Transmission Control Protocol, Src Port: 443, Dst Port: 58938, Seq: 0, Ack: 1, Len: 0
0000 d0 39 57 a3 5b 2b 18 b1 69 ee 46 3d 08 00 45 00
0010 00 34 c8 b8 40 00 65 06 2c e7 14 2a 41 54 ac 10
0020 1e 96 01 bb e6 3a 1a 17 d6 60 11 af 24 a3 80 12
0030 ff ff 40 30 00 00 02 04 05 a0 01 03 03 08 01 01
0040 04 02


websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1&&tcp.flags.ack==0
No. Time Source Destination Protocol Length Info
183 5.641764 172.16.30.150 150.171.28.11 TCP 66 57643 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
184 5.642315 172.16.30.150 150.171.28.11 TCP 66 50060 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
185 5.642619 172.16.30.150 150.171.28.11 TCP 66 49882 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
186 5.643012 172.16.30.150 150.171.28.11 TCP 66 57972 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
331 6.590477 172.16.30.150 202.83.22.202 TCP 66 50725 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
332 6.590863 172.16.30.150 202.83.22.202 TCP 66 64243 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
800 14.033188 172.16.30.150 172.188.155.25 TCP 66 58992 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
879 15.980321 172.16.30.150 13.89.179.14 TCP 66 65048 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
880 15.980744 172.16.30.150 13.89.179.14 TCP 66 56739 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
881 15.981029 172.16.30.150 13.89.179.14 TCP 66 61276 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
890 16.243623 172.16.30.150 13.89.179.14 TCP 66 60971 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1391 20.361362 172.16.30.150 150.171.74.13 TCP 66 53025 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1417 20.468981 172.16.30.150 202.83.22.211 TCP 66 64597 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1418 20.469544 172.16.30.150 202.83.22.211 TCP 66 59312 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1419 20.469918 172.16.30.150 202.83.22.211 TCP 66 61777 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1420 20.470252 172.16.30.150 202.83.22.211 TCP 66 57292 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1421 20.470659 172.16.30.150 202.83.22.211 TCP 66 56777 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1422 20.470989 172.16.30.150 202.83.22.211 TCP 66 60784 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1423 20.471265 172.16.30.150 202.83.22.211 TCP 66 60974 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1848 21.018470 172.16.30.150 151.101.66.132 TCP 66 50860 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2385 22.663649 172.16.30.150 157.245.76.57 TCP 66 51411 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2386 22.926433 172.16.30.150 157.245.76.57 TCP 66 59151 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2489 24.311233 172.16.30.150 4.144.165.14 TCP 66 57973 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Frame 9346: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{
Ethernet II, Src: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
Destination: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 8]
Internet Protocol Version 4, Src: 172.16.30.150, Dst: 150.171.27.11
Transmission Control Protocol, Src Port: 58702, Dst Port: 443, Seq: 0, Len: 0
0000 18 b1 69 ee 46 3d d0 39 57 a3 5b 2b 08 00 45 00
0010 00 34 0f 7c 40 00 80 06 6e eb ac 10 1e 96 96 ab
0020 1b 0b c6 0e 01 bb 51 5a 88 3b 00 00 00 00 80 02
0030 ff ff 51 54 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02


websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark - Packet 9285 - websites_track.pcapng
Acknowledgment Number: 6620 (relative ack number)
Acknowledgment number (raw): 2827339400
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 252
[Calculated window size: 64512]
[Window size scaling factor: 256]
Checksum: 0x356c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 210.858000 milliseconds]
[Time since previous frame in this TCP stream: 105.000 microseconds]
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
0000 18 b1 69 ee 46 3d d0 39 57 a3 5b 2b 08 00 45 00
0010 00 28 39 f8 40 00 80 06 ae 5b ac 10 1e 96 ac bc
0020 9b 19 ed 18 01 bb 6c 32 9c db a8 85 c6 88 50 10
0030 00 fc 35 6c 00 00
Source Port (tcp.srcport), 2 bytes
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

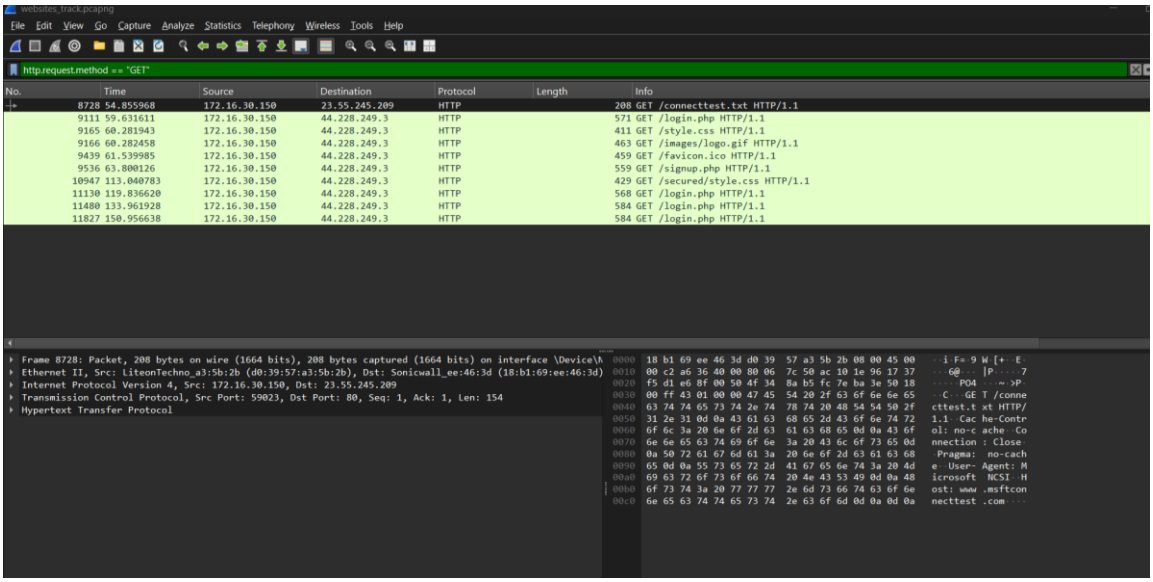

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination Protocol Length Info
59 3.071000 172.16.31.26 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
63 3.340755 172.16.30.150 44.228.249.3 HTTP 593 GET /categories.php HTTP/1.1
116 5.836514 172.16.31.26 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
117 5.836514 172.16.31.26 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
123 6.131805 172.16.30.150 44.228.249.3 HTTP 568 GET /categories.php HTTP/1.1
178 8.270065 172.16.30.150 44.228.249.3 HTTP 565 GET /artists.php HTTP/1.1
202 9.331689 172.16.30.150 44.228.249.3 HTTP 559 GET /cart.php HTTP/1.1
234 10.678210 172.16.30.150 44.228.249.3 HTTP 562 GET /categories.php HTTP/1.1
290 12.031720 172.16.30.150 44.228.249.3 HTTP 576 GET /listproducts.php?cat=1 HTTP/1.1
310 12.356588 172.16.30.150 44.228.249.3 HTTP 585 GET /showimage.php?file=./pictures/1.jpg&size=160 HTTP/1.1
311 12.356671 172.16.30.150 44.228.249.3 HTTP 585 GET /showimage.php?file=./pictures/2.jpg&size=160 HTTP/1.1
326 12.701474 172.16.30.150 44.228.249.3 HTTP 585 GET /showimage.php?file=./pictures/3.jpg&size=160 HTTP/1.1
337 12.704473 172.16.30.150 44.228.249.3 HTTP 585 GET /showimage.php?file=./pictures/4.jpg&size=160 HTTP/1.1
341 12.704735 172.16.30.150 44.228.249.3 HTTP 585 GET /showimage.php?file=./pictures/5.jpg&size=160 HTTP/1.1
342 12.704968 172.16.30.150 44.228.249.3 HTTP 585 GET /showimage.php?file=./pictures/7.jpg&size=160 HTTP/1.1
475 14.353940 172.16.30.150 44.228.249.3 HTTP 597 GET /showimage.php?file=./pictures/1.jpg HTTP/1.1
626 19.345440 172.16.30.150 44.228.249.3 HTTP 597 GET /showimage.php?file=./pictures/2.jpg HTTP/1.1
760 24.880492 172.16.30.150 44.228.249.3 HTTP 571 GET /login.php HTTP/1.1
789 26.243887 172.16.30.150 44.228.249.3 HTTP 561 GET /userinfo.php HTTP/1.1
809 26.536493 172.16.30.150 44.228.249.3 HTTP 558 GET /login.php HTTP/1.1
826 27.848272 172.16.30.150 44.228.249.3 HTTP 562 GET /guestbook.php HTTP/1.1
978 32.594574 172.16.30.150 44.228.249.3 HTTP 745 POST /guestbook.php HTTP/1.1 (application/x-www-form-urlencoded)
1047 35.021500 172.16.31.221 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
Frame 59: Packet, 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF
Ethernet II, Src: Intel_fe:a0:8d (c0:a5:e8:fe:a0:8d), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
.... ..0. .... = LG bit: Globally unique address (factory default)
....1 .... = IG bit: Group address (multicast/broadcast)
Source: Intel_fe:a0:8d (c0:a5:e8:fe:a0:8d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 39]
Internet Protocol Version 4, Src: 172.16.31.26, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 51156, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa c0 a5 e8 fe a0 8d 08 00 45 00
0010 00 a5 38 ee 00 00 04 11 c2 35 ac 10 1f 1a ef ff
0020 ff fa c7 d4 07 6c 00 91 82 48 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 20 75
0060 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d
0070 6f 72 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72
0080 6e 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65
0090 3a 31 0d 0a 4d 61 6e 3a 20 22 73 73 64 70 3a 64
00a0 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 20 33 0d
00b0 0a 0d 0a


task5th.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response
No. Time Source Destination Protocol Length Info
71 3.688957 44.228.249.3 172.16.30.150 HTTP 1341 HTTP/1.1 200 OK (text/html)
137 6.453353 44.228.249.3 172.16.30.150 HTTP 1341 HTTP/1.1 200 OK (text/html)
186 8.605897 44.228.249.3 172.16.30.150 HTTP 1198 HTTP/1.1 200 OK (text/html)
214 9.628782 44.228.249.3 172.16.30.150 HTTP 1153 HTTP/1.1 200 OK (text/html)
252 10.960361 44.228.249.3 172.16.30.150 HTTP 1341 HTTP/1.1 200 OK (text/html)
304 12.291522 44.228.249.3 172.16.30.150 HTTP 107 HTTP/1.1 200 OK (text/html)
335 12.704418 44.228.249.3 172.16.30.150 HTTP 60 HTTP/1.1 200 OK (JPEG JFIF image)
354 12.709253 44.228.249.3 172.16.30.150 HTTP 1035 HTTP/1.1 200 OK (JPEG JFIF image)
384 13.009898 44.228.249.3 172.16.30.150 HTTP 200 HTTP/1.1 200 OK (JPEG JFIF image)
414 13.017041 44.228.249.3 172.16.30.150 HTTP 1110 HTTP/1.1 200 OK (JPEG JFIF image)
437 13.314882 44.228.249.3 172.16.30.150 HTTP 357 HTTP/1.1 200 OK (JPEG JFIF image)
442 13.315774 44.228.249.3 172.16.30.150 HTTP 520 HTTP/1.1 200 OK (JPEG JFIF image)
495 14.705748 44.228.249.3 172.16.30.150 HTTP 305 HTTP/1.1 200 OK (JPEG JFIF image)
649 19.645886 44.228.249.3 172.16.30.150 HTTP 60 HTTP/1.1 200 OK (JPEG JFIF image)
764 25.194895 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
808 26.524997 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
815 26.832324 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
839 28.165009 44.228.249.3 172.16.30.150 HTTP 1299 HTTP/1.1 200 OK (text/html)
1003 32.873841 44.228.249.3 172.16.30.150 HTTP 1306 HTTP/1.1 200 OK (text/html)
Frame 71: Packet, 1341 bytes on wire (10728 bits), 1341 bytes captured (10728 bits) on interface \Devi
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2
Destination: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 13]
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.30.150
Transmission Control Protocol, Src Port: 80, Dst Port: 53950, Seq: 1461, Ack: 540, Len: 1287
Source Port: 80
Destination Port: 53950
[Stream index: 2]
[Stream Packet Number: 3]
0000 d0 39 57 a3 5b 2b 18 b1 69 ee 46 3d 08 00 45 00
0010 05 2f a6 5b 40 00 33 06 ab df 2c e4 f9 03 ac 10
0020 1e 96 00 50 d2 be 1a 2c 3d 44 16 e1 f6 ee 50 18
0030 01 de 91 0f 00 00 c0 df 03 f2 d1 1c 8e 9b 02 b7
0040 e3 b6 14 4e 54 69 fc 7f 0e ef c7 2b b8 b2 5c ab
0050 a6 28 68 80 96 84 e4 34 c1 bf 18 15 5d 21 1d db
0060 96 84 92 d4 d4 ec 52 41 a4 77 86 90 54 a2 6a ca
0070 72 15 90 53 49 15 41 3f a1 48 c1 63 26 85 93 d1
0080 7e 5d b0 8a 55 48 0f ce cc ff b7 32 0f 5a 65 22
0090 f5 6a 68 e4 a7 3a ff 9e 3a 0f 9d 3a 2f 35 47 87
00a0 f8 d3 39 ff a6 73 1e 39 6d fe 4b d2 f9 1c 65 ec
00b0 67 a8 6f 85 ba cd eb db 6d f7 bd 0e 19 49 dc a4
00c0 fc 36 23 db c4 be 69 94 d0 a7 9e 50 d9 b6 49 eb
00d0 e4 ad 18 f2 5c be 2e f3 13 74 1b 25 a1 b6 57 46
00e0 fb 6f f7 4c 31 7b a1 91 ee a2 cf 48 a7 2b 8f 20
00f0 c5 e6 02 fd 1b ba 35 54 24 d3 d1 98 3f 93 82 c6
Packet (1341 bytes)
Reassembled TCP (2747 bytes)
De-chunked entity body (2483 bytes)
Uncompressed entity body (6115 by

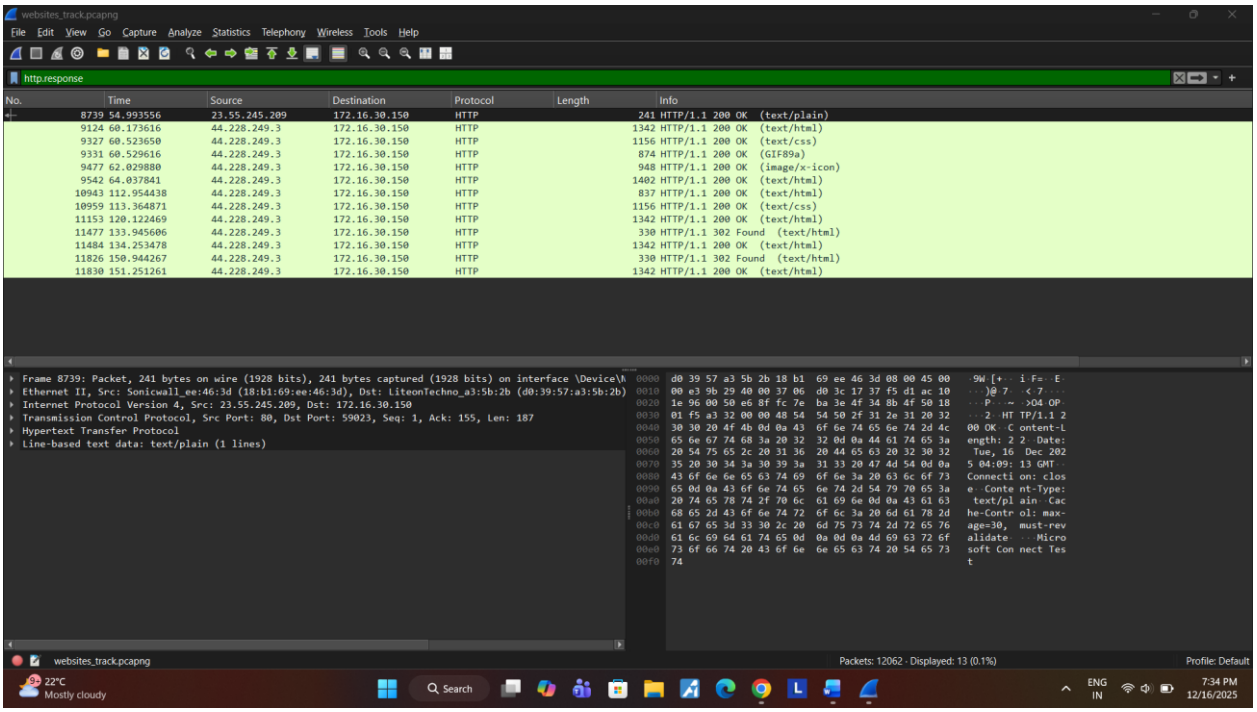

Wireshark · Packet 1003 · task5th.pcapng
Sequence Number: 45600 (relative sequence number)
Sequence Number (raw): 2839452973
[Next Sequence Number: 46852 (relative sequence number)]
Acknowledgment Number: 4265 (relative ack number)
Acknowledgment number (raw): 2116928994
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 461
[Calculated window size: 59008]
[Window size scaling factor: 128]
Checksum: 0xf9d4 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 20.517366000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
TCP payload (1252 bytes)
TCP segment data (1252 bytes)
0030 01 cd f9 d4 00 00 5c 20 f4 9e f9 b4 de f6 8a c9
0040 68 d4 96 92 50 db 19 e3 20 20 00 28 b9 40 61 46
0050 19 46 7f 77 2d 7a 8a fc 06 92 70 9e 44 0a f1 aa
0060 6e b4 6f f5 39 6c ca 00 2d 1c a5 f9 19 18 7b 37
0070 e8 cc 9b d6 b3 71 8b 38 00 b0 a1 92 51 7f c0 2c
0080 03 22 c5 02 c1 72 8c 42 2b 69 1d 07 7f 5e 7e ba
0090 fd e3 cd d5 ca 51 ae fe 1f db fa 0f e7 44 2d 0f
00a0 c4 15 a4 49 4c 4d d9 92 4a 35 49 c9 57 f2 b7 ab
00b0 56 ae 0c 09 c1 94 42 91 f7 c9 64 6c 00 26 b0 92
00c0 4d 1c 9f 3f 9b d8 e5 11 12 41 b2 98 d4 ea 26 d0
00d0 ba 21 01 0f 9c 52 e9 db 51 9b 24 8a 51 99 e6 6d
00e0 39 dd b4 bc fb 66 8a c6 6f 1a c8 2c fe d2 30 d8
00f0 7b d3 1d b6 b9 99 3a 3c 2e 68 c2 8a 89 3b 43 6c
0100 21 72 3b a6 b5 58 02 e7 22 e7 14 47 f6 56 a0 c7
0110 ae e1 19 8c 0b 40 63 0a 73 2b 0f d8 76 4f cd c4
0120 69 a3 b5 80 6b dd a1 2d 23 ce d0 b2 dc 6d e3 c8
0130 9a cf 76 35 5f 77 7c b8 99 06 8f 0e 68 30 c3 15
0140 e0 23 e0 a0 3f d1 14 1d 55 f8 ba 3b af ab b9 ab
0150 9e a7 26 30 18 4a 6d 5b f4 4d 65 1c 47 05 ff fe
0160 71 5f e5 37 ce fa bd 1f 1f 5c 97 f6 bf bb a5 fd
0170 e9 9b 00 0d 78 e5 ee b9 41 23 6b ea 15 7f 1b 45
Packet (1306 bytes)
Reassembled TCP (2712 bytes)
De-chunked entity body (2448 bytes)
Uncompressed entity body (5407 bytes)

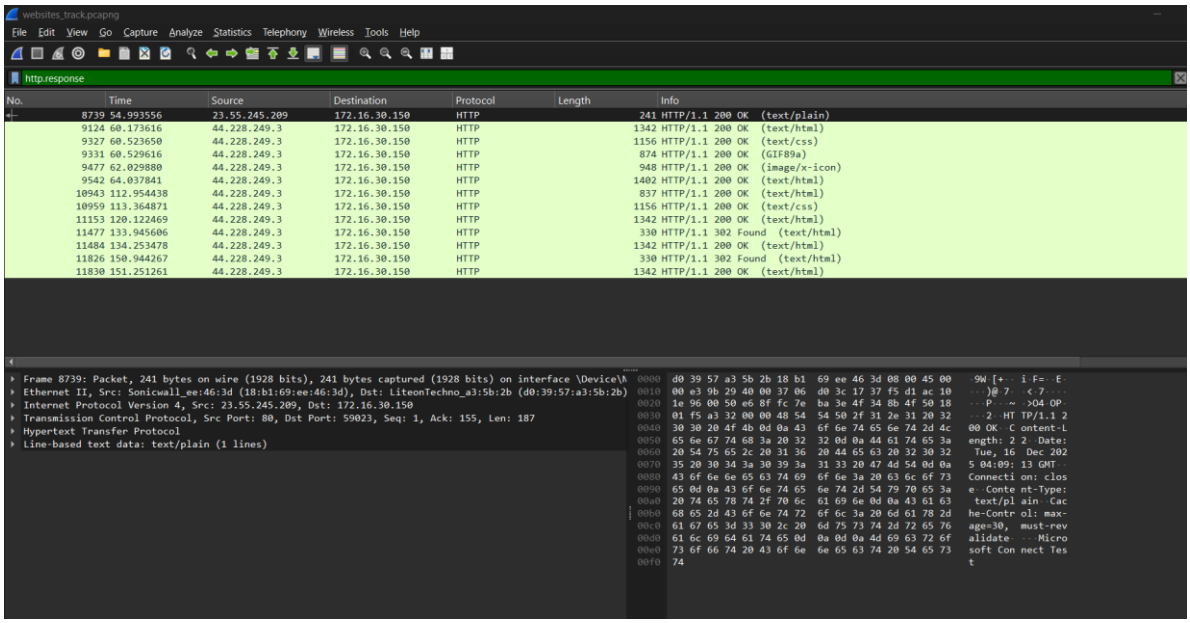
Task 2:

How many conditional GETs are sent by browser to the server ?

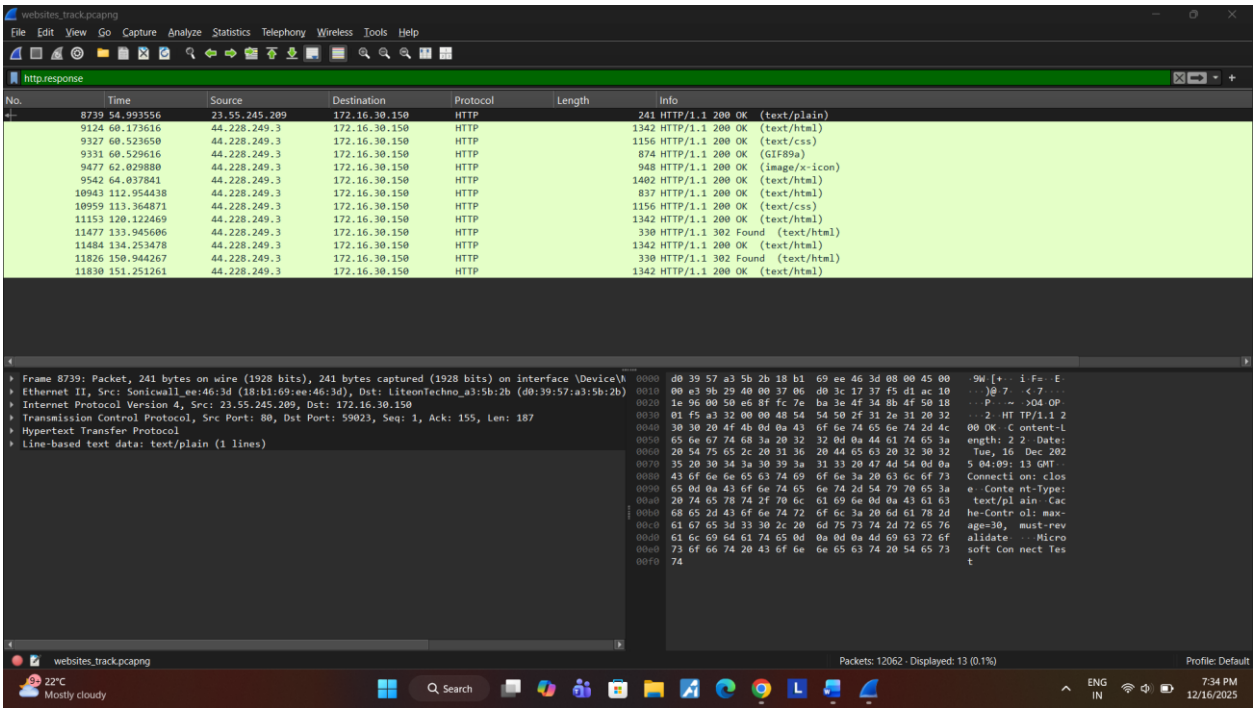


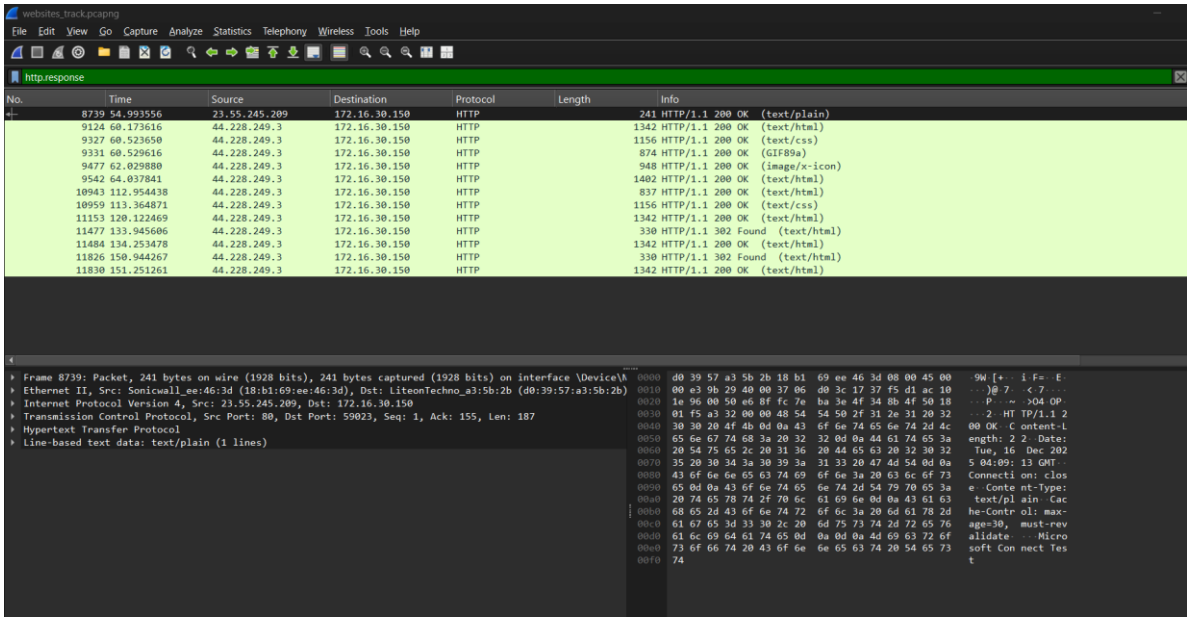
Make a list for each of the file/object downloaded.

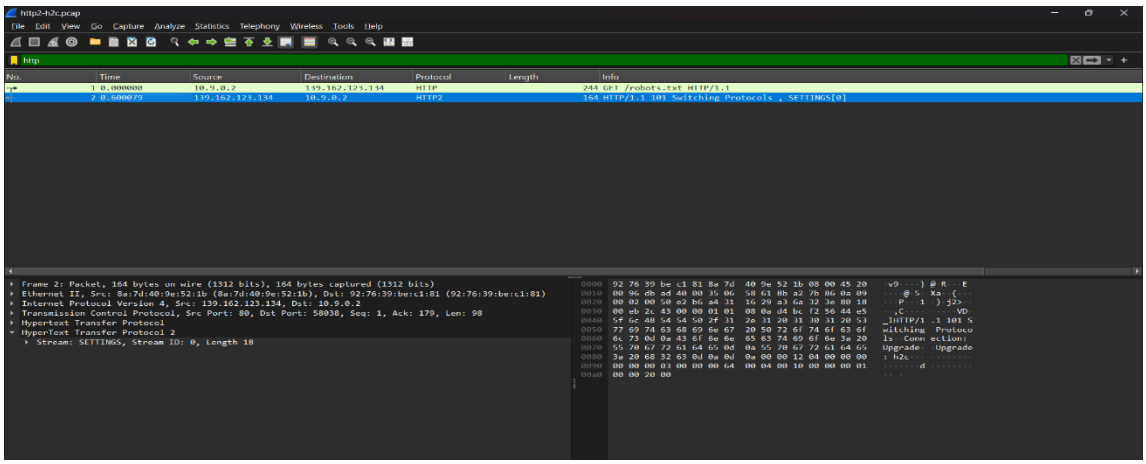


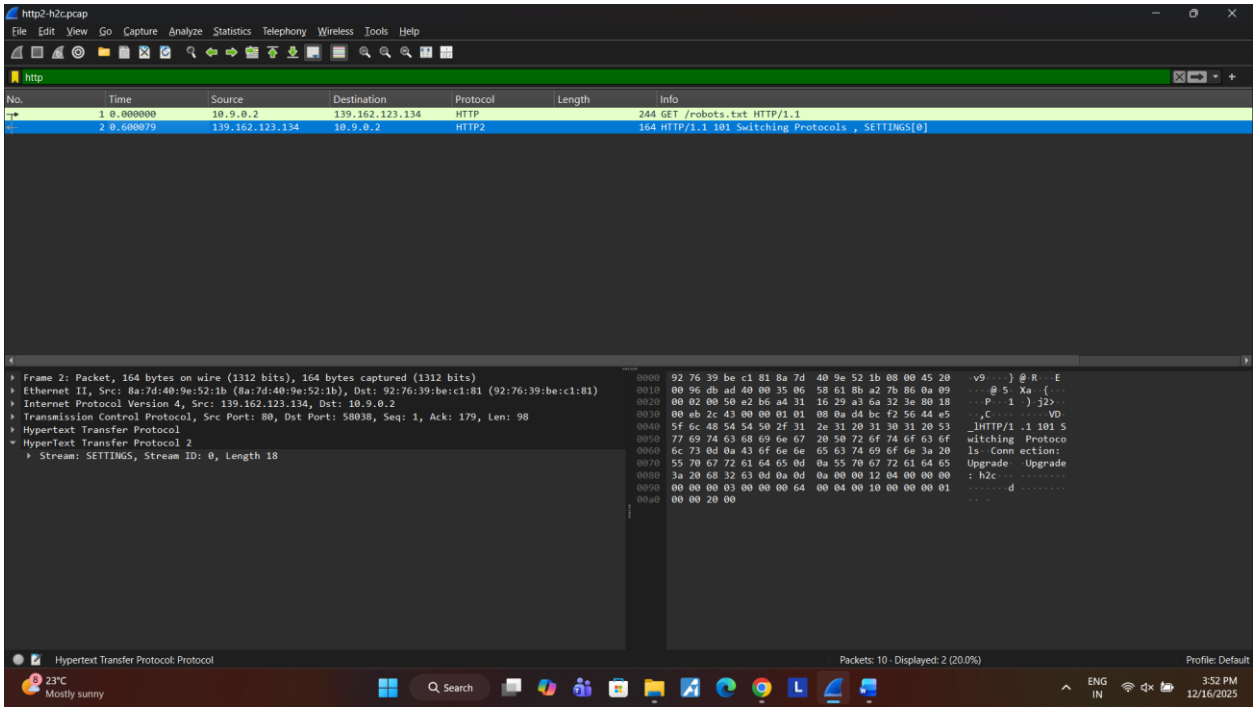

websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response
No. Time Source Destination Protocol Length Info
8739 54.993556 23.55.245.209 172.16.30.150 HTTP 241 HTTP/1.1 200 OK (text/plain)
9124 60.173616 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
9327 60.523650 44.228.249.3 172.16.30.150 HTTP 1156 HTTP/1.1 200 OK (text/css)
9331 60.529616 44.228.249.3 172.16.30.150 HTTP 874 HTTP/1.1 200 OK (GIF89a)
9477 62.029880 44.228.249.3 172.16.30.150 HTTP 948 HTTP/1.1 200 OK (image/x-icon)
9542 64.037841 44.228.249.3 172.16.30.150 HTTP 1402 HTTP/1.1 200 OK (text/html)
10943 112.954438 44.228.249.3 172.16.30.150 HTTP 837 HTTP/1.1 200 OK (text/html)
10959 113.364871 44.228.249.3 172.16.30.150 HTTP 1156 HTTP/1.1 200 OK (text/css)
11153 120.122469 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
11477 133.945606 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
11484 134.253478 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
11826 150.944267 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
11830 151.251261 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
Frame 8739: Packet, 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\N
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
Internet Protocol Version 4, Src: 23.55.245.209, Dst: 172.16.30.150
Transmission Control Protocol, Src Port: 80, Dst Port: 59023, Seq: 1, Ack: 155, Len: 187
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
0000 d0 39 57 a3 5b 2b 18 b1 69 ee 46 3d 08 00 45 00
0010 00 e3 9b 29 40 00 37 06 d0 3c 17 37 f5 d1 ac 10
0020 1e 96 00 50 e6 8f fc 7e ba 3e 4f 34 8b 4f 50 18
0030 01 f5 a3 32 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c
0050 65 6e 67 74 68 3a 20 32 32 0d 0a 44 61 74 65 3a
0060 20 54 75 65 2c 20 31 36 20 44 65 63 20 32 30 32
0070 35 20 30 34 3a 30 39 3a 31 33 20 47 4d 54 0d 0a
0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73
0090 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a
00a0 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 61 63
00b0 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d
00c0 61 67 65 3d 33 30 2c 20 6d 75 73 74 2d 72 65 76
00d0 61 6c 69 64 61 74 65 0d 0a 0d 0a 4d 69 63 72 6f
00e0 73 6f 66 74 20 43 6f 6e 6e 65 63 74 20 54 65 73
00f0 74

1: How many HTTP/2 and HTTP/1.1 packets are present?

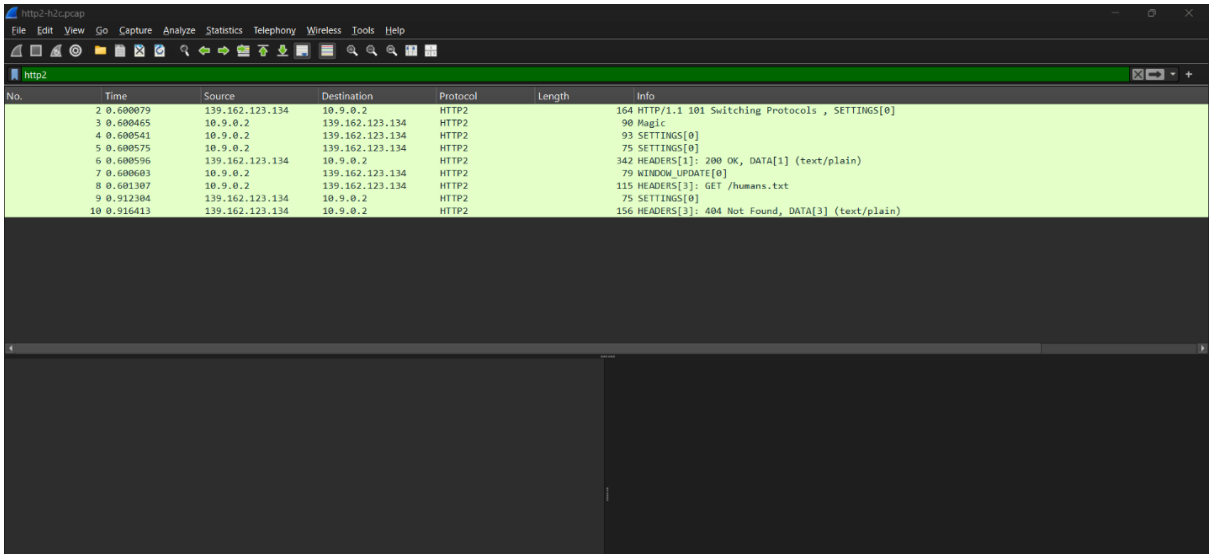



websites_track.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response
No. Time Source Destination Protocol Length Info
8739 54.993556 23.55.245.209 172.16.30.150 HTTP 241 HTTP/1.1 200 OK (text/plain)
9124 60.173616 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
9327 60.523650 44.228.249.3 172.16.30.150 HTTP 1156 HTTP/1.1 200 OK (text/css)
9331 60.529616 44.228.249.3 172.16.30.150 HTTP 874 HTTP/1.1 200 OK (GIF89a)
9477 62.029880 44.228.249.3 172.16.30.150 HTTP 948 HTTP/1.1 200 OK (image/x-icon)
9542 64.037841 44.228.249.3 172.16.30.150 HTTP 1402 HTTP/1.1 200 OK (text/html)
10943 112.954438 44.228.249.3 172.16.30.150 HTTP 837 HTTP/1.1 200 OK (text/html)
10959 113.364871 44.228.249.3 172.16.30.150 HTTP 1156 HTTP/1.1 200 OK (text/css)
11153 120.122469 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
11477 133.945606 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
11484 134.253478 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
11826 150.944267 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
11830 151.251261 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
Frame 8739: Packet, 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\N
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
Internet Protocol Version 4, Src: 23.55.245.209, Dst: 172.16.30.150
Transmission Control Protocol, Src Port: 80, Dst Port: 59023, Seq: 1, Ack: 155, Len: 187
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
0000 d0 39 57 a3 5b 2b 18 b1 69 ee 46 3d 08 00 45 00
0010 00 e3 9b 29 40 00 37 06 d0 3c 17 37 f5 d1 ac 10
0020 1e 96 00 50 e6 8f fc 7e ba 3e 4f 34 8b 4f 50 18
0030 01 f5 a3 32 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c
0050 65 6e 67 74 68 3a 20 32 32 0d 0a 44 61 74 65 3a
0060 20 54 75 65 2c 20 31 36 20 44 65 63 20 32 30 32
0070 35 20 30 34 3a 30 39 3a 31 33 20 47 4d 54 0d 0a
0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73
0090 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a
00a0 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 61 63
00b0 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d
00c0 61 67 65 3d 33 30 2c 20 6d 75 73 74 2d 72 65 76
00d0 61 6c 69 64 61 74 65 0d 0a 0d 0a 4d 69 63 72 6f
00e0 73 6f 66 74 20 43 6f 6e 6e 65 63 74 20 54 65 73
00f0 74

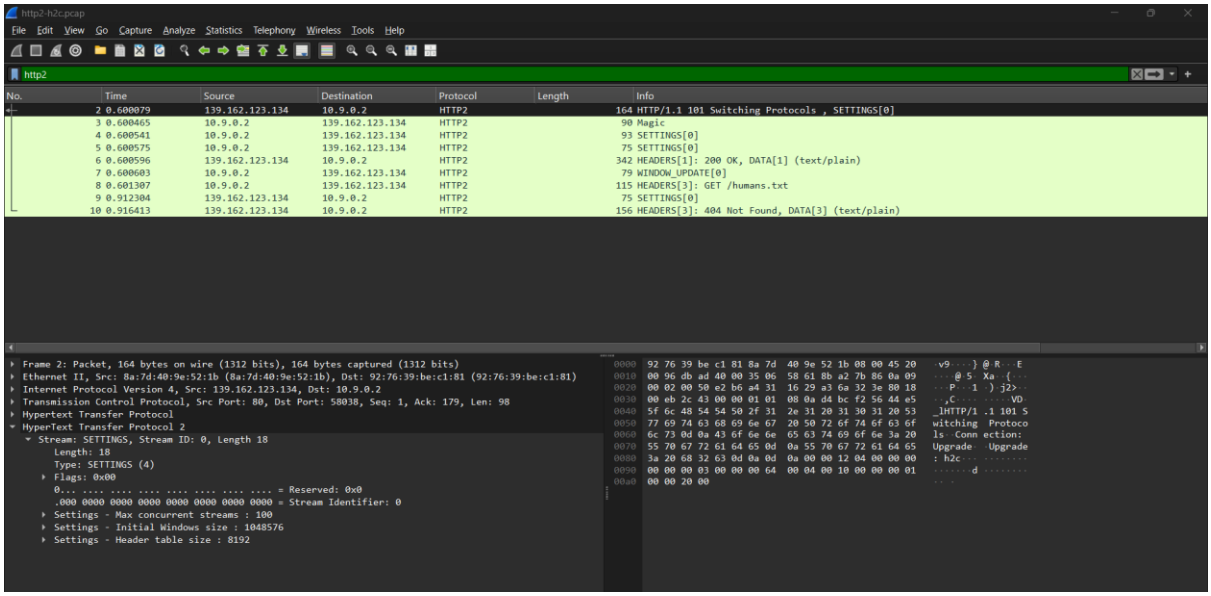

http2-h2c.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1 0.000000 10.9.0.2 139.162.123.134 HTTP 244 GET /robots.txt HTTP/1.1
2 0.000079 139.162.123.134 10.9.0.2 HTTP2 164 HTTP/1.1 101 Switching Protocols , SETTINGS[0]
Frame 2: Packet, 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:c1:81 (92:76:39:be:c1:81)
Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 1, Ack: 179, Len: 98
Hypertext Transfer Protocol
HyperText Transfer Protocol 2
Stream: SETTINGS, Stream ID: 0, Length 18
0000 92 76 39 be c1 81 8a 7d 40 9e 52 1b 08 00 45 20
0010 00 96 db a5 40 00 35 06 58 61 8b a2 7b 96 0a 09
0020 00 02 00 50 e2 b6 a4 31 1b 29 a3 6a 32 3e 80 18
0030 00 eb 2c 43 00 00 01 01 08 0a d4 bc f2 56 44 e5
0040 5f 6c 48 54 54 50 2f 31 2e 31 20 31 30 31 20 53
0050 77 69 74 63 68 69 6e 67 20 50 72 6f 74 6f 63 6f
0060 6c 73 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20
0070 55 70 67 72 61 64 65 0d 0a 55 70 67 72 61 64 65
0080 3a 20 68 32 63 0d 0a 0d 0a 00 00 12 04 00 00 00
0090 00 00 03 00 00 00 64 00 04 00 10 00 00 00 01
00a0 00 00 20 00



2: How many HTTP/2 packets are exchanged between client and server here before the first object is fetched ?



3: What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets ?


http2-h2c.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http2
No. Time Source Destination Protocol Length Info
2 0.600079 139.162.123.134 10.9.0.2 HTTP2 164 HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3 0.600465 10.9.0.2 139.162.123.134 HTTP2 90 Magic
4 0.600541 10.9.0.2 139.162.123.134 HTTP2 93 SETTINGS[0]
5 0.600575 10.9.0.2 139.162.123.134 HTTP2 75 SETTINGS[0]
6 0.600596 139.162.123.134 10.9.0.2 HTTP2 342 HEADERS[1]: 200 OK, DATA[1] (text/plain)
7 0.600603 10.9.0.2 139.162.123.134 HTTP2 79 WINDOW_UPDATE[0]
8 0.601307 10.9.0.2 139.162.123.134 HTTP2 115 HEADERS[3]: GET /humans.txt
9 0.912304 139.162.123.134 10.9.0.2 HTTP2 75 SETTINGS[0]
10 0.916413 139.162.123.134 10.9.0.2 HTTP2 156 HEADERS[3]: 404 Not Found, DATA[3] (text/plain)
Frame 2: Packet, 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:c1:81 (92:76:39:be:c1:81)
Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 1, Ack: 179, Len: 98
Hypertext Transfer Protocol
HyperText Transfer Protocol 2
Stream: SETTINGS, Stream ID: 0, Length 18
Length: 18
Type: SETTINGS (4)
Flags: 0x00
0... .... = Reserved: 0x0
.000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier: 0
Settings - Max concurrent streams : 100
Settings - Initial Windows size : 1048576
Settings - Header table size : 8192
0000 92 76 39 be c1 81 8a 7d 40 9e 52 1b 08 00 45 20
0010 00 96 db ad 40 00 35 06 58 61 8b a2 7b 86 0a 09
0020 00 02 00 50 e2 b6 a4 31 16 29 a3 6a 32 3e 80 18
0030 00 eb 2c 43 00 00 01 01 08 0a d4 bc f2 56 44 e5
0040 5f 6c 48 54 54 50 2f 31 2e 31 20 31 30 31 20 53
0050 77 69 74 63 68 69 6e 67 20 50 72 6f 74 6f 63 6f
0060 6c 73 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20
0070 55 70 67 72 61 64 65 0d 0a 55 70 67 72 61 64 65
0080 3a 20 68 32 63 0d 0a 0d 0a 00 00 12 04 00 00 00
0090 00 00 00 03 00 00 00 64 00 04 00 10 00 00 00 01
00a0 00 00 20 00