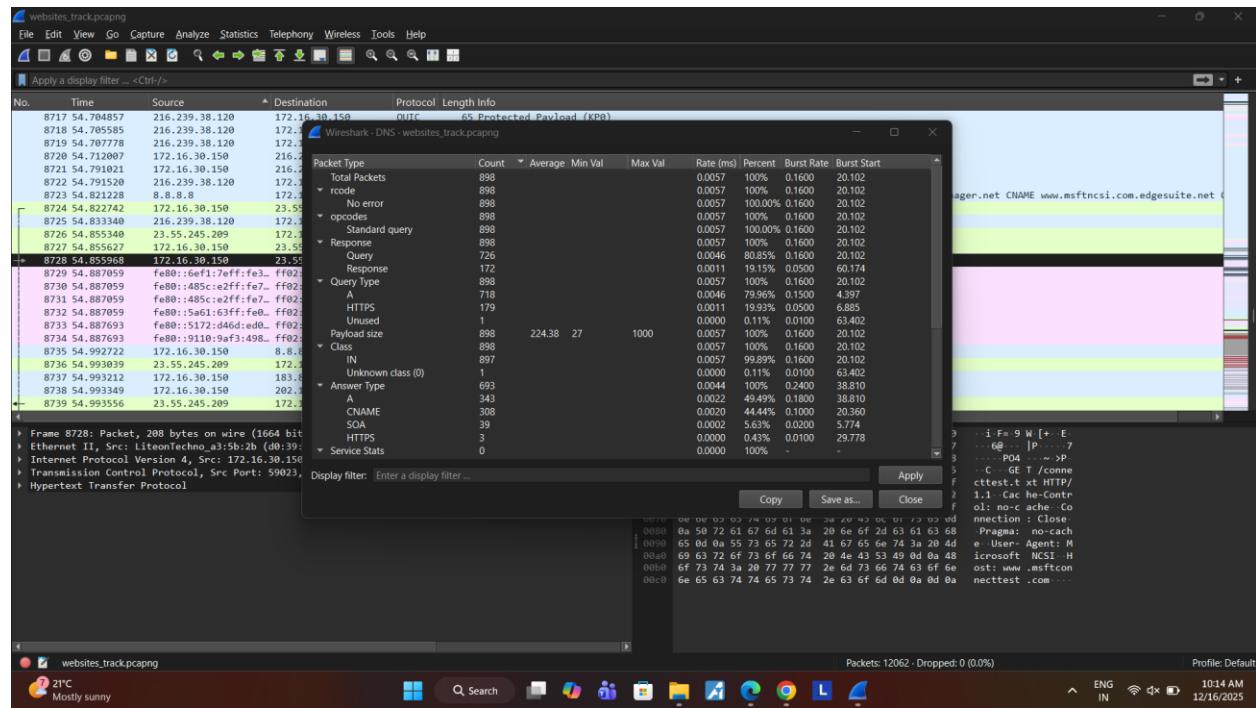
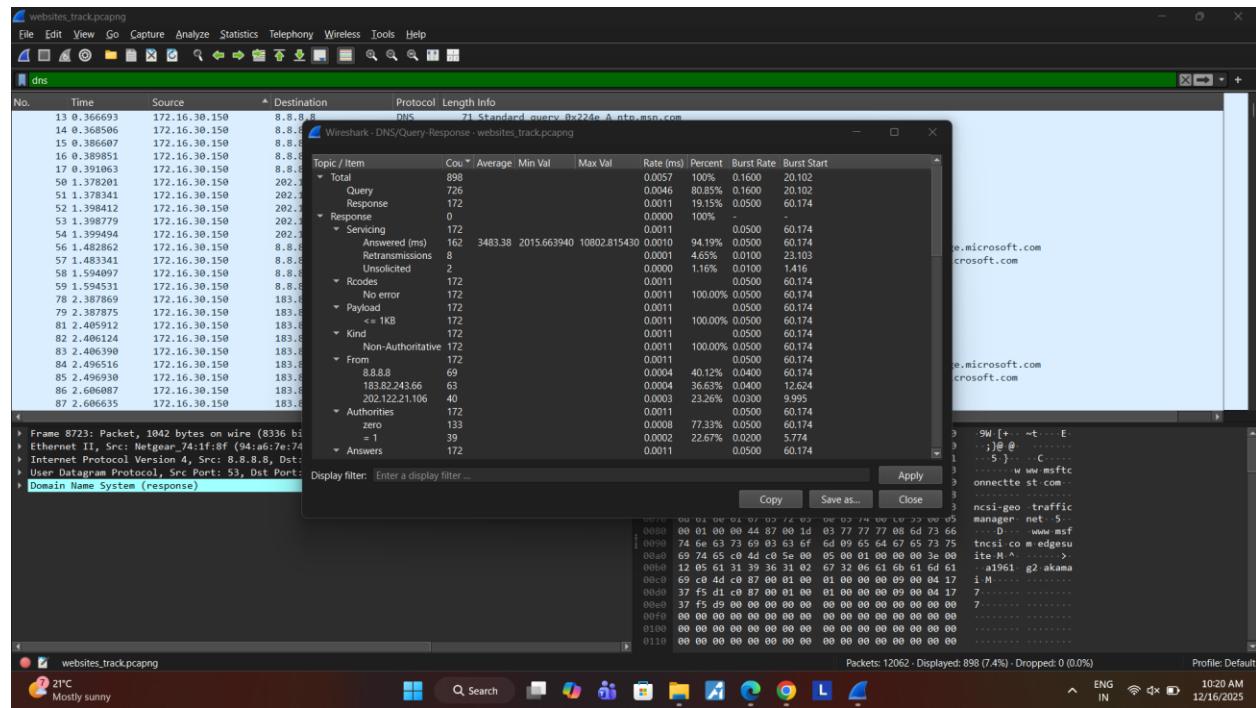


TASK 1

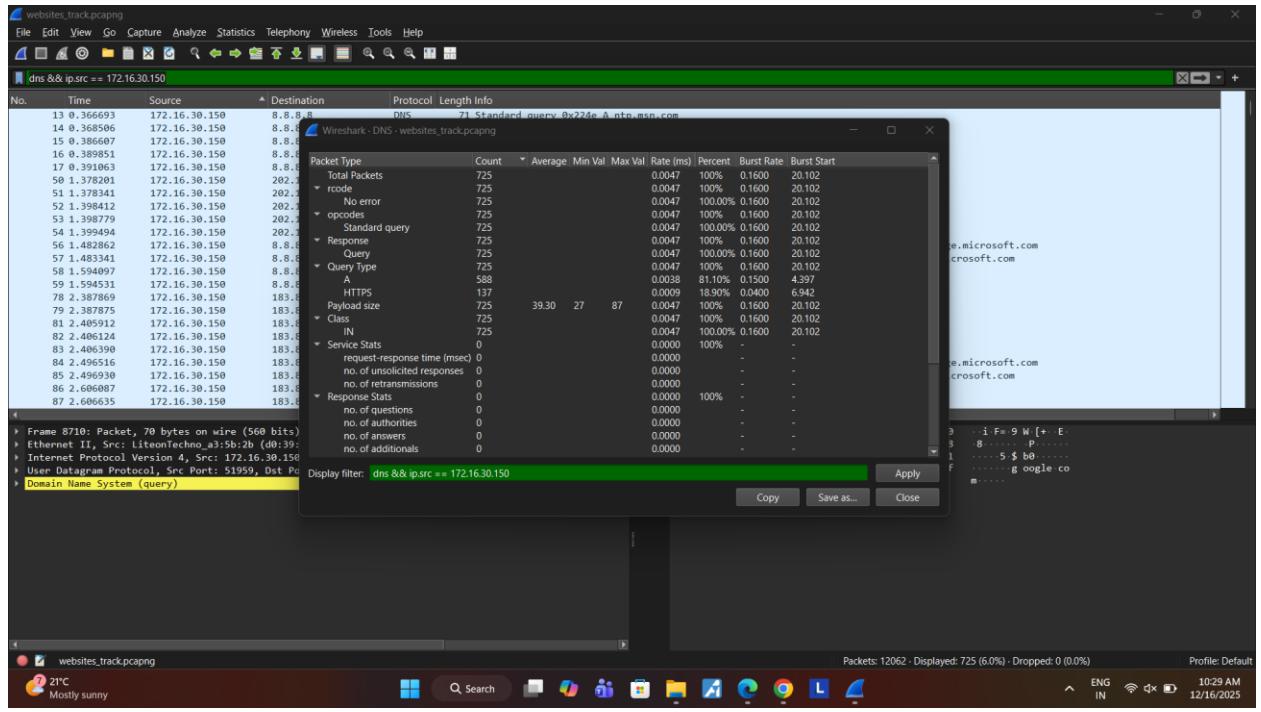
How many DNS queries are sent from your browser (host machine) to DNS Server(s) ?



How many DNS servers are involved



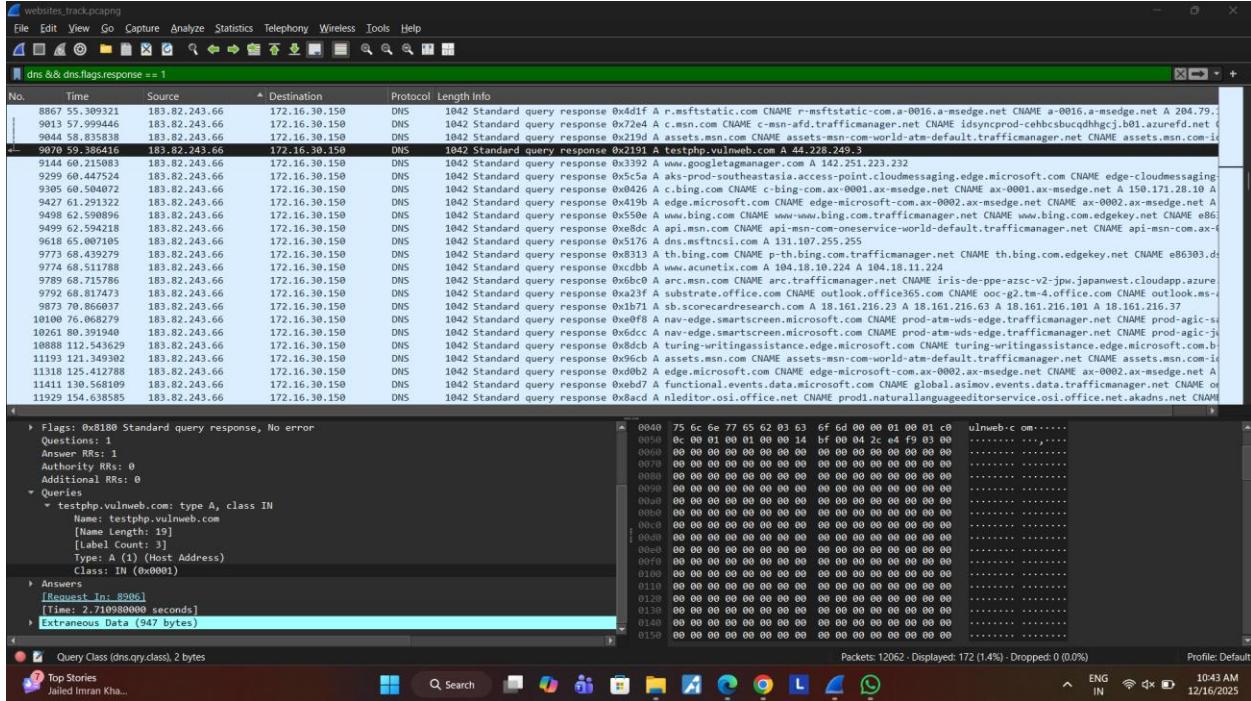
Which DNS Server replies with actual IP Address(es).



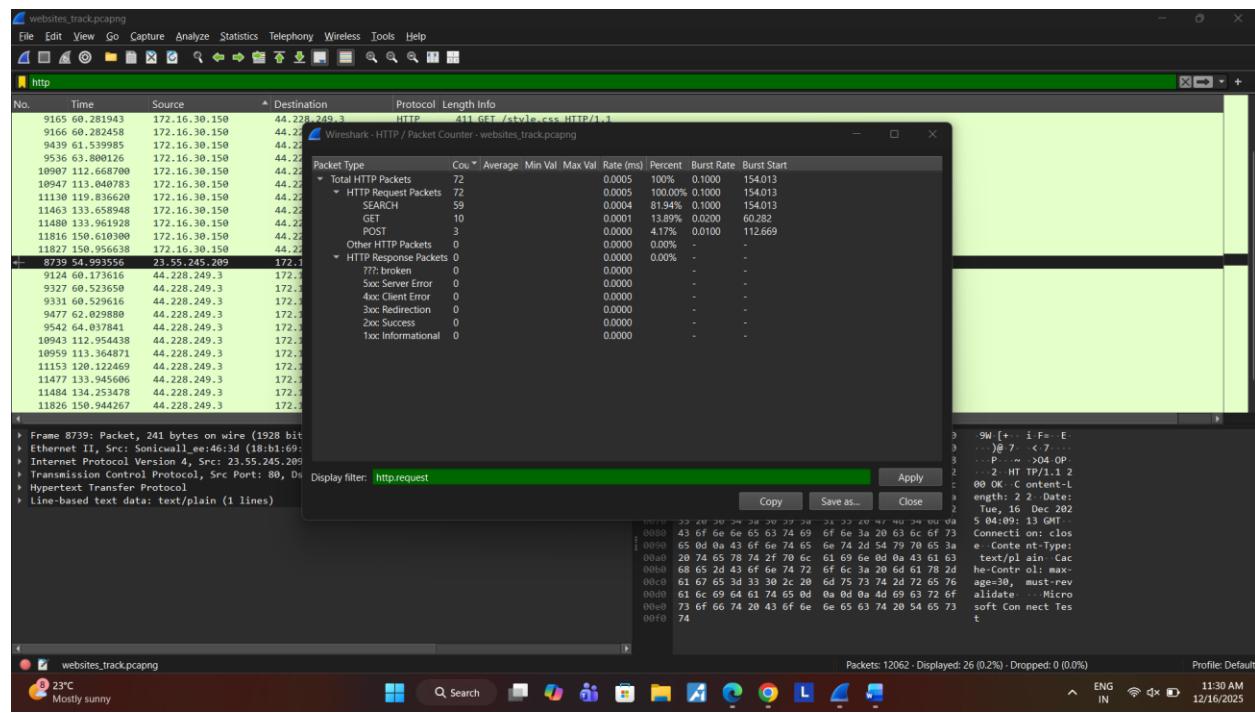
Do all DNS servers respond

Ans: NO

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 query/queries and response/answer(s).



2nd:



websites_trackpcapng

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	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
9439	61.539985	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
10907	112.658700	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
10947	113.040783	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11130	119.836620	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11463	133.658948	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11488	133.961928	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11816	150.610300	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11827	150.956638	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
+ 8739	54.993556	23.55.245.209	172.1	HTTP	411 GET /style.css HTTP/1.1
9124	60.173616	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9327	60.523650	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9331	60.529616	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9477	62.029880	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9542	64.037841	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
10943	112.954438	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
10959	113.364871	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11153	120.122469	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11477	133.945606	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11484	134.253478	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11826	150.944267	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1

Frame 8739: Packet, 241 bytes on wire (1928 bit)
Ethernet II, Src: Sonicwall_ee:46:3d (18:81:69:
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)

Display filter: http.response

Copy Save as... Apply Close

9W [+ . i F= E
...)@ 7. < 7 ...
... P ~w >04 OP
... 2 HT TP/1.1 2
... 00 OK -C ontent-L
length 2 2 : Date:
Tue, 16 Dec 202
5 04:09: 13 GMT
Connect: clos
e-Content-Type:
text/plain -Cac
he-Contr ol: max
age=30, must-rev
alidate ...Micro
soft Con nect Tes
t

Packets: 12062 - Displayed: 26 (0.2%) - Dropped: 0 (0.0%) Profile: Default

websites_trackpcapng

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	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
9439	61.539985	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
10907	112.658700	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
10947	113.040783	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11130	119.836620	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11463	133.658948	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11488	133.961928	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11816	150.610300	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11827	150.956638	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
+ 8739	54.993556	23.55.245.209	172.1	HTTP	411 GET /style.css HTTP/1.1
9124	60.173616	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9327	60.523650	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9331	60.529616	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9477	62.029880	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9542	64.037841	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
10943	112.954438	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
10959	113.364871	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11153	120.122469	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11477	133.945606	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11484	134.253478	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11826	150.944267	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1

Frame 8739: Packet, 241 bytes on wire (1928 bit)
Ethernet II, Src: Sonicwall_ee:46:3d (18:81:69:
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)

Display filter: Enter a display filter ...

Copy Save as... Apply Close

9W [+ . i F= E
...)@ 7. < 7 ...
... P ~w >04 OP
... 2 HT TP/1.1 2
... 00 OK -C ontent-L
length 2 2 : Date:
Tue, 16 Dec 202
5 04:09: 13 GMT
Connect: clos
e-Content-Type:
text/plain -Cac
he-Contr ol: max
age=30, must-rev
alidate ...Micro
soft Con nect Tes
t

Packets: 12062 - Displayed: 26 (0.2%) - Dropped: 0 (0.0%) Profile: Default

websites_trackpcapng

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	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
9439	61.539985	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
10907	112.658700	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
10947	113.040783	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11130	119.836620	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11463	133.658948	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11488	133.961928	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11816	150.610300	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
11827	150.956638	172.16.30.150	44.228.249.3	HTTP	411 GET /style.css HTTP/1.1
+ 8739	54.993556	23.55.245.209	172.1	HTTP	411 GET /style.css HTTP/1.1
9124	60.173616	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9327	60.523650	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9331	60.529616	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9477	62.029880	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
9542	64.037841	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
10943	112.954438	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
10959	113.364871	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11153	120.122469	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11477	133.945606	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11484	134.253478	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1
11826	150.944267	44.228.249.3	172.1	HTTP	411 GET /style.css HTTP/1.1

Frame 8739: Packet, 241 bytes on wire (1928 bit)
Ethernet II, Src: Sonicwall_ee:46:3d (18:81:69:
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)

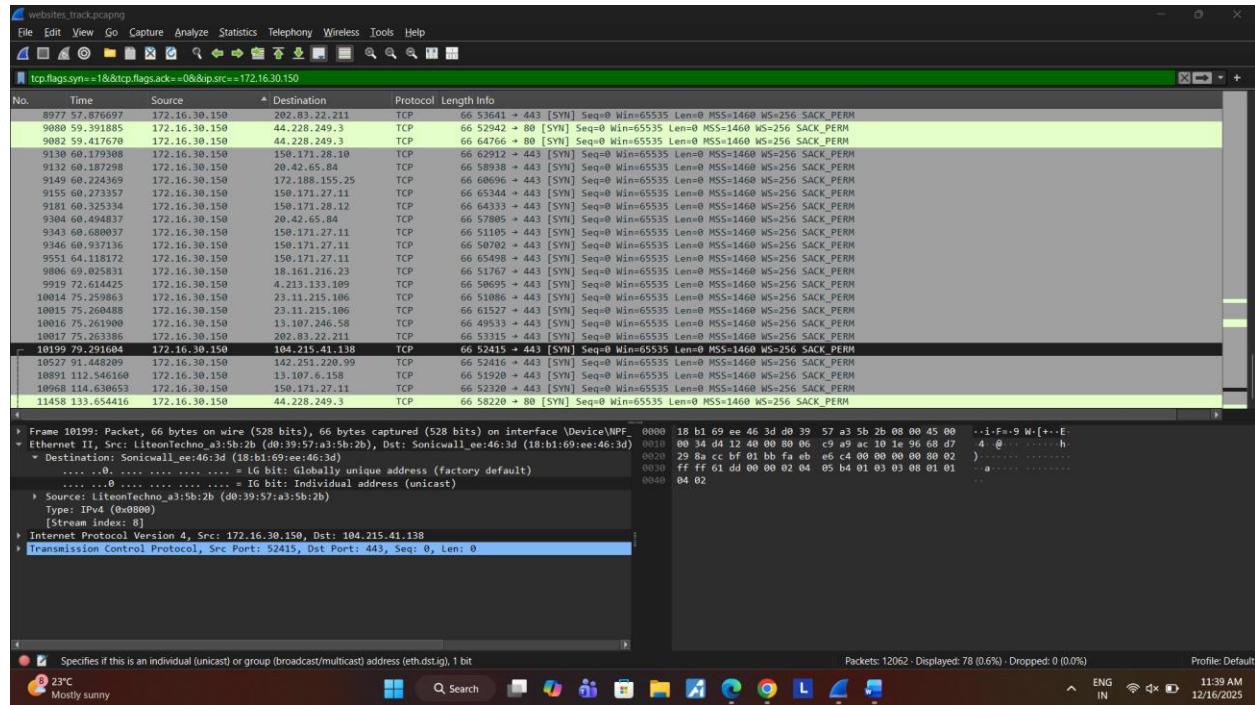
Display filter: Enter a display filter ...

Copy Save as... Apply Close

9W [+ . i F= E
...)@ 7. < 7 ...
... P ~w >04 OP
... 2 HT TP/1.1 2
... 00 OK -C ontent-L
length 2 2 : Date:
Tue, 16 Dec 202
5 04:09: 13 GMT
Connect: clos
e-Content-Type:
text/plain -Cac
he-Contr ol: max
age=30, must-rev
alidate ...Micro
soft Con nect Tes
t

Packets: 12062 - Displayed: 26 (0.2%) - Dropped: 0 (0.0%) Profile: Default

3rd:



Screenshot of Wireshark showing network traffic analysis. The interface is set to 'tcp.flags.syn==1&&tcp.flags.ack==1'. The packet list shows various TCP connections, primarily between 172.16.30.150 and 172.188.155.25, involving TLSv1.3 and TLSv1.2 protocols. The details pane displays the configuration for a selected connection, including source and destination ports, protocol, length, and info. The bytes pane shows the raw hex and ASCII data of the selected packet.

Packets: 12062 - Displayed: 5288 (43.8%) - Dropped: 0 (0.0%) Profile: Default

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
9255	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
9258	60.420066	172.16.30.150	150.171.27.11	TCP	54	65344 + 443 [ACK] Seq=2701 Ack=43489 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=5668 Win=65280 Len=0
9281	60.429907	172.16.30.150	172.188.155.25	TCP	54	60696 + 443 [ACK] Seq=5146 Ack=59624 Win=65280 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)
9292	60.439122	172.16.30.150	150.171.28.12	TCP	54	64333 + 443 [ACK] Seq=2481 Ack=4448 Win=65280 Len=0
9297	60.441956	172.16.30.150	150.171.28.12	TCP	54	64333 + 443 [ACK] Seq=2481 Ack=6158 Win=65280 Len=0
9298	60.442819	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=419 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=419 Ack=4621 Win=65280 Len=0

Frame 9285: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\WIFI_0
 Ethernet II, Src: LitenTecho_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..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Individual address (unicast)
 Source: LitenTecho_a3:5b:2b (d0:39:57:a3:5b:2b)
0..... = LG bit: Globally unique address (factory default)
0..... = LG 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

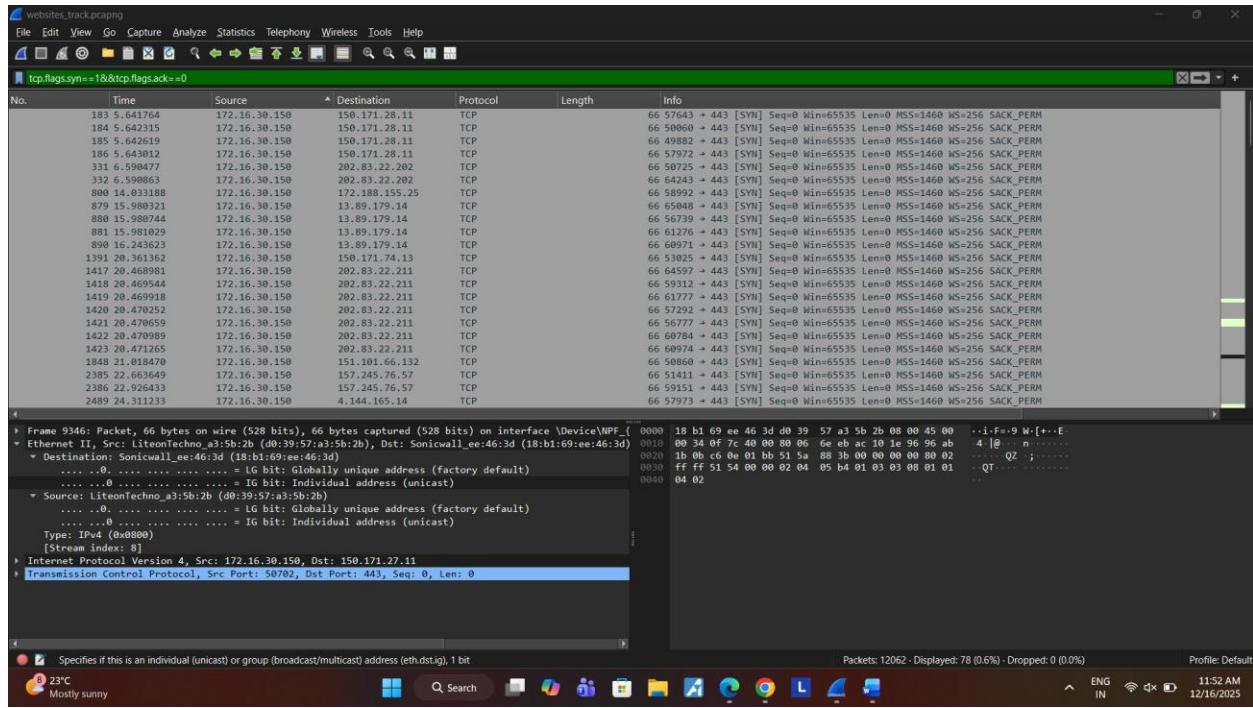
Frame 9285: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\WIFI_0
 Ethernet II, Src: LitenTecho_a3:5b:2b (d0:39:57:a3:5b:2b), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
 Destination: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Individual address (unicast)
 Source: LitenTecho_a3:5b:2b (d0:39:57:a3:5b:2b)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG 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

Frame 9285: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\WIFI_0
 Ethernet II, Src: LitenTecho_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..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Individual address (unicast)
 Source: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG 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

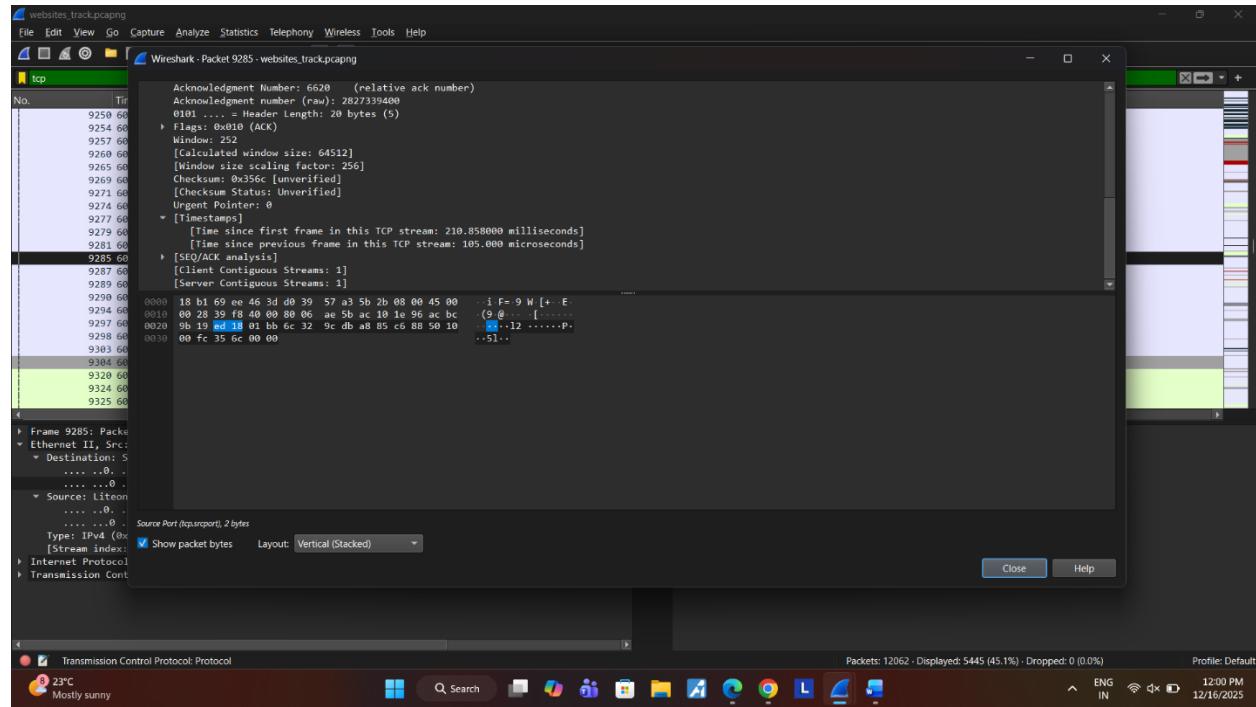
Frame 9286: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\WIFI_0
 Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
 Destination: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Individual address (unicast)
 Source: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG 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

Frame 9286: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\WIFI_0
 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..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Individual address (unicast)
 Source: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG 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

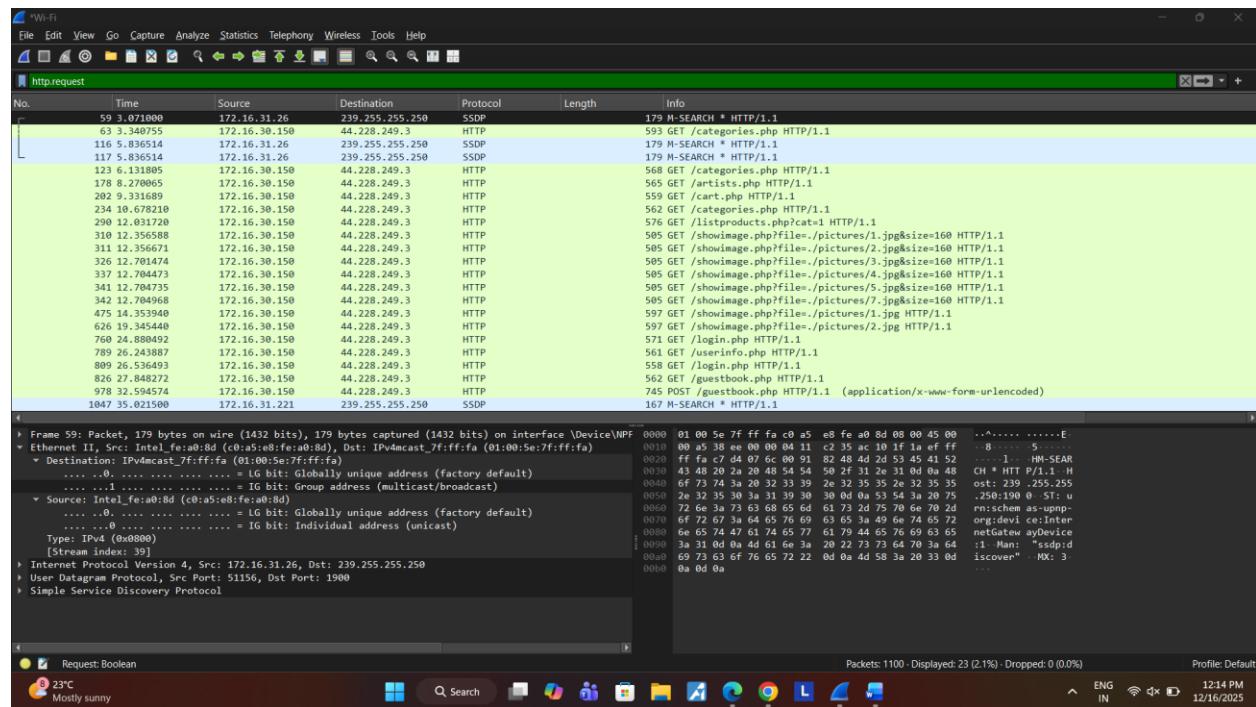
Frame 9286: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\WIFI_0
 Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
 Destination: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Individual address (unicast)
 Source: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
0..... = LG bit: Globally unique address (factory default)
0..... = LG bit: Globally unique address (factory default)
0..... = LG 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



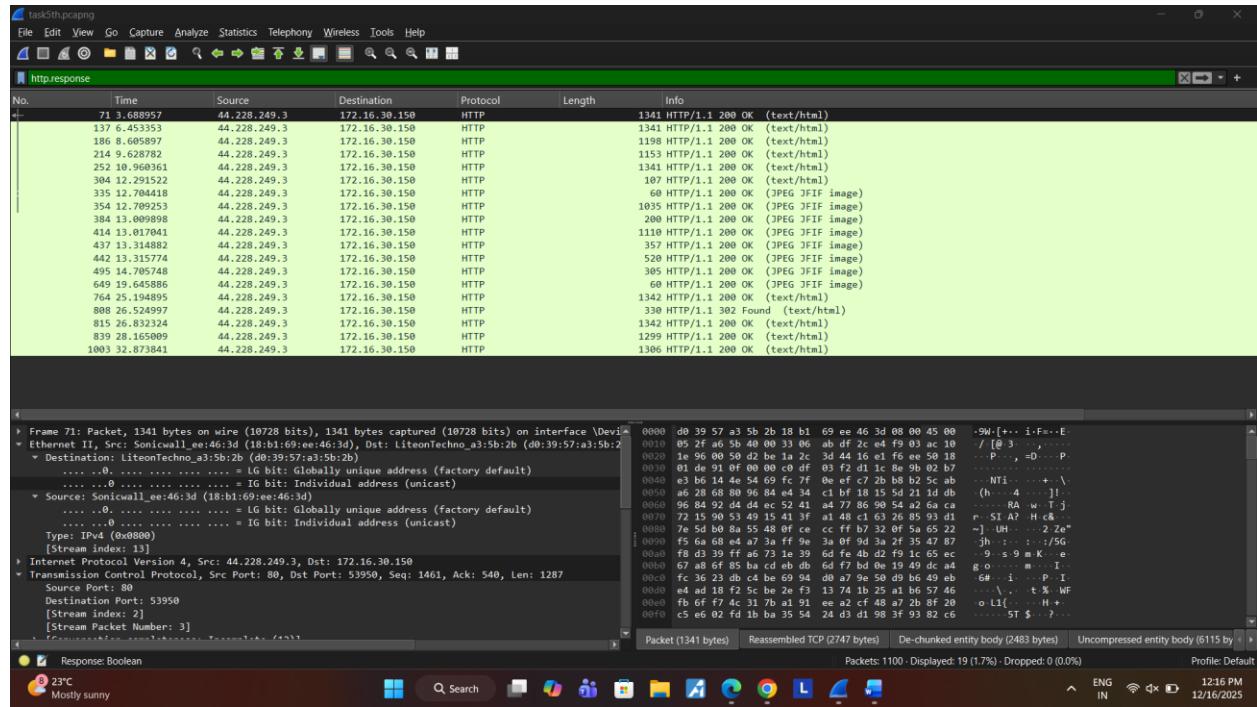
4th:



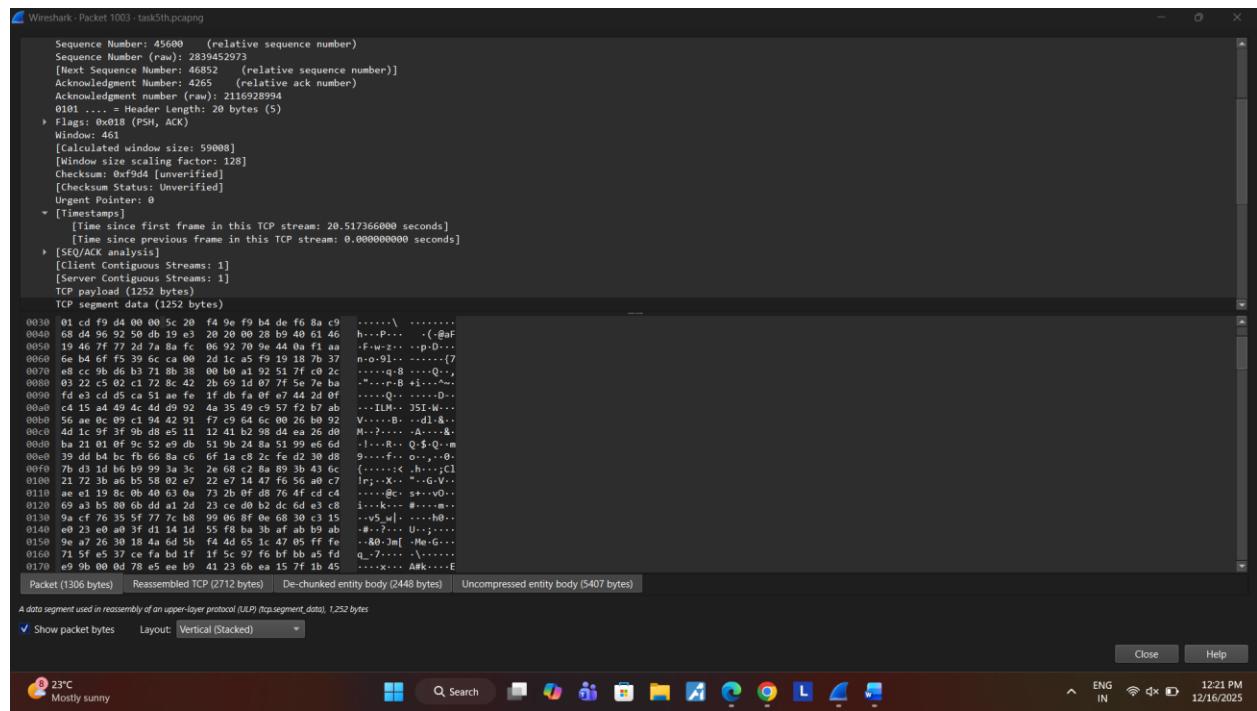
5th:



6th:

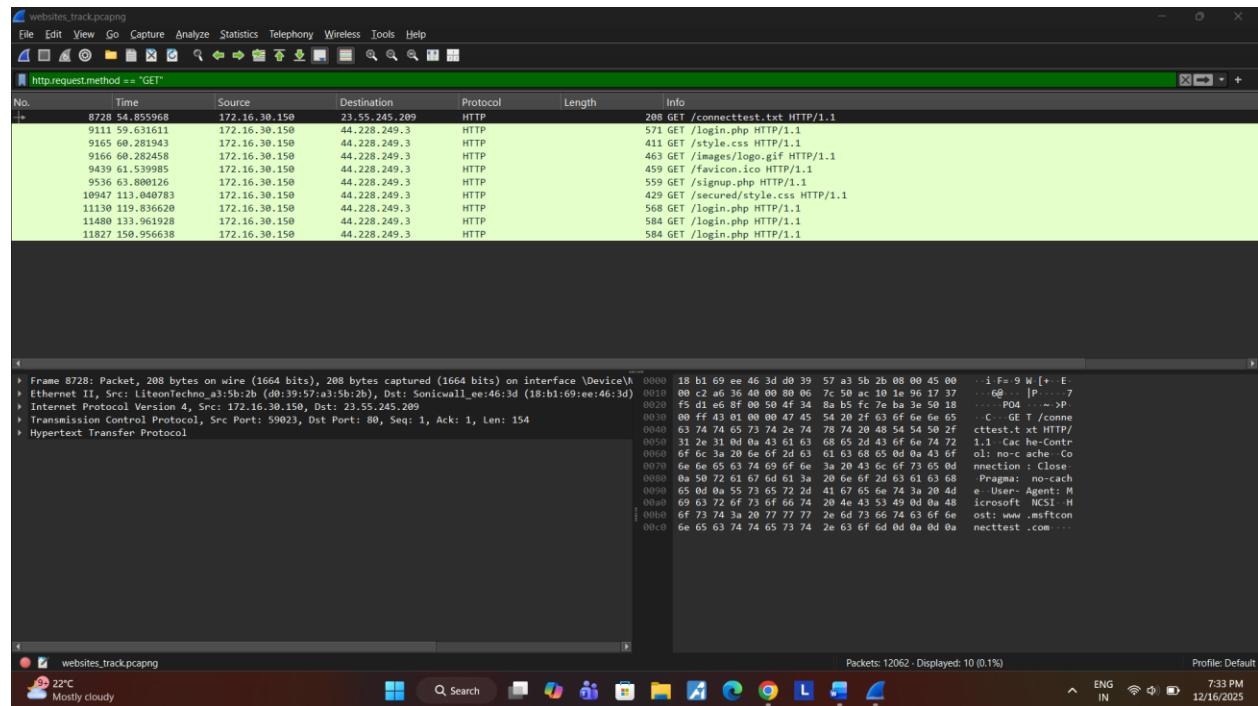


7th:

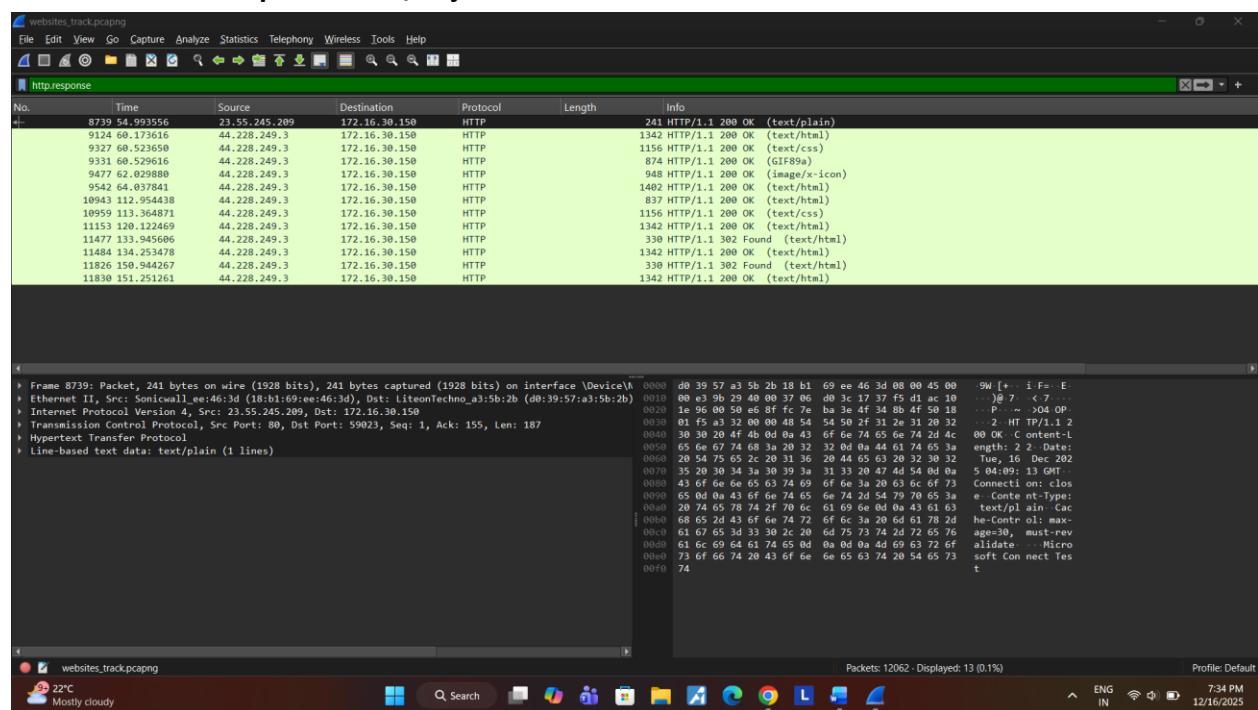


Task 2:

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



Make a list for each of the file/object downloaded, how many times the server sends the full contents of the respective file/object ?



List the headers of HTTP which influence this functionality.

Screenshot of NetworkMiner tool showing captured traffic and a detailed packet analysis window.

Captured Traffic:

- No. 8728: Source 172.16.30.150, Destination 23.55.245.209, Protocol HTTP, Info: 208 GET /connecttest.txt HTTP/1.1
- No. 8739: Source 172.16.30.150, Destination 172.16.30.150, Protocol HTTP, Info: 241 HTTP/1.1 200 OK (text/plain)
- No. 9111: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 571 GET /login.php HTTP/1.1
- No. 9124: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 1342 HTTP/1.1 200 OK (text/html)
- No. 9165: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 411 GET /style.css HTTP/1.1
- No. 9166: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 463 GET /images/logo.gif HTTP/1.1
- No. 9327: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 1156 HTTP/1.1 200 OK (text/css)
- No. 9331: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 874 HTTP/1.1 200 OK (GIF89a)
- No. 9439: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 459 GET /favicon.ico HTTP/1.1
- No. 9477: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 948 HTTP/1.1 200 OK (image/x-icon)
- No. 9536: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 559 GET /signup.php HTTP/1.1
- No. 9542: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 1402 HTTP/1.1 200 OK (text/html)
- No. 10932: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 858 POST /second/register.php HTTP/1.1 (application/x-www-form-urlencoded)
- No. 10943: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 837 GET /index.php HTTP/1.1 (text/html)
- No. 10947: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 429 GET /secure/style.css HTTP/1.1
- No. 10959: Source 44.228.249.3, Destination 172.16.30.150, Protocol HTTP, Info: 1156 HTTP/1.1 200 OK (text/css)
- No. 11130: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 568 GET /login.php HTTP/1.1
- No. 11153: Source 120.122469, Destination 172.16.30.150, Protocol HTTP, Info: 1342 HTTP/1.1 200 OK (text/html)
- No. 11463: Source 172.16.30.150, Destination 44.228.249.3, Protocol HTTP, Info: 722 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Detailed Packet Analysis:

```

Frame 9111: Packet, 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface '\Device\N
Ethernet II, Src: LitonTechno a3:5b:2b (d0:39:57:a3:5b:2b), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
Internet Protocol Version 4, Src: 172.16.30.150, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 52942, Dst Port: 80, Seq: 1, Ack: 1, Len: 517
HyperText Transfer Protocol
  > GET /login.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
    Referer: http://www.google.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  \r\n
[Response in frame: 9124]
[Full request URI: http://testphp.vulnweb.com/login.php]
```

Packets: 12062 - Displayed: 26 (0.2%)

Profile: Default

7:35 PM
ENG IN
12/16/2025

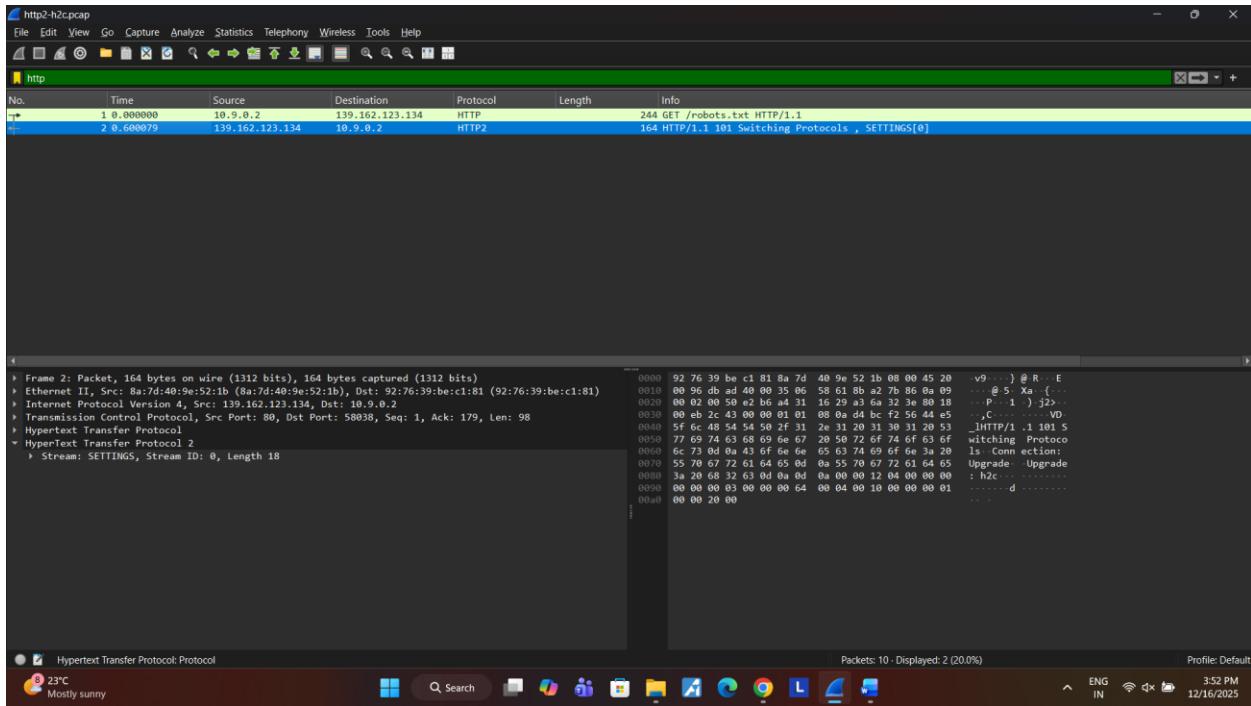
Task3:

Analyze the attached HTTP/2 packet (http2-h2c.pcap: Included in zip file) capture using Wireshark to answer the following (Hint : Use Statistics->HTTP, HTTP2 windows).

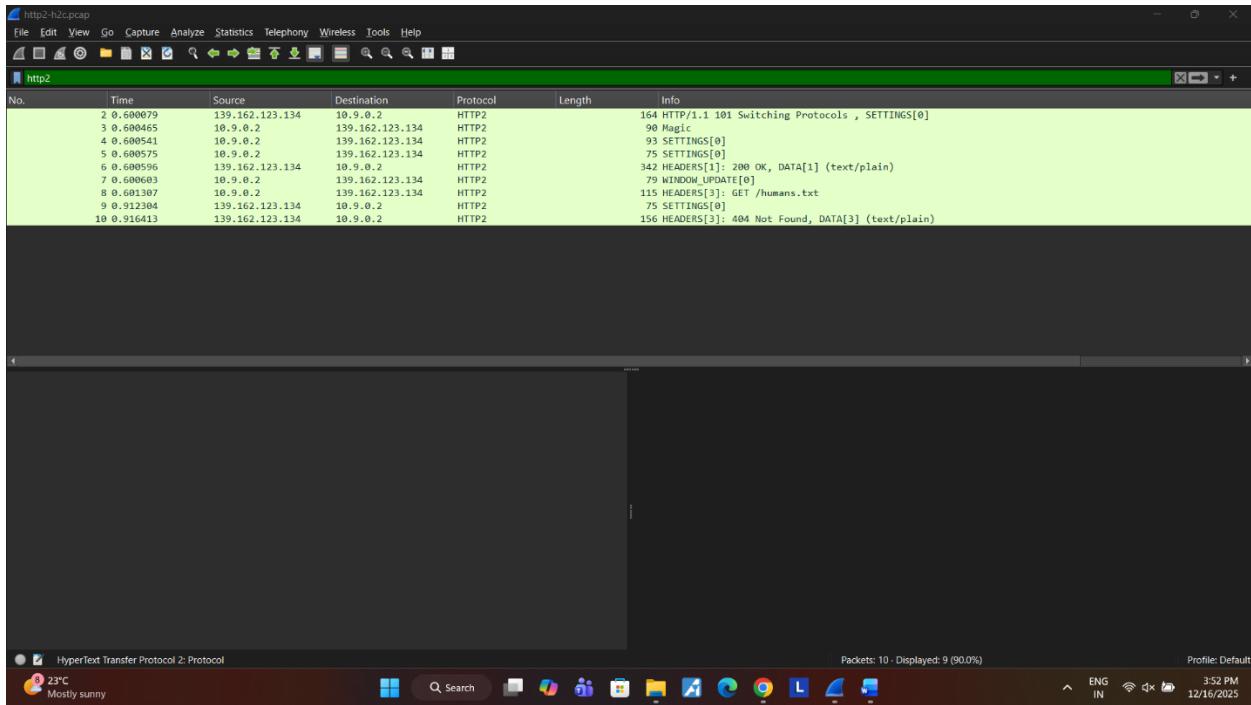
1: How many HTTP/2 and HTTP/1.1 packets are present?

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Statistics Menu:** Statistics, Network Statistics, Protocols, Applications, Services, Topology, History, Session, Cache.
- Selected Column:** http.response
- Packet List:** Shows 1830 total packets. The first few are listed below:
 - No. 6729 54.093556 23.55.245.209 172.16.30.150 HTTP 241 HTTP/1.1 200 OK (text/plain)
 - No. 9124 60.173616 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
 - No. 9327 60.523650 44.228.249.3 172.16.30.150 HTTP 1156 HTTP/1.1 200 OK (text/css)
 - No. 9331 60.529616 44.228.249.3 172.16.30.150 HTTP 874 HTTP/1.1 200 OK (GIF89a)
 - No. 9477 62.029880 44.228.249.3 172.16.30.150 HTTP 948 HTTP/1.1 200 OK (image/x-icon)
 - No. 9542 64.037841 44.228.249.3 172.16.30.150 HTTP 1402 HTTP/1.1 200 OK (text/html)
 - No. 10943 112.954438 44.228.249.3 172.16.30.150 HTTP 837 HTTP/1.1 200 OK (text/html)
 - No. 10959 113.364871 44.228.249.3 172.16.30.150 HTTP 1156 HTTP/1.1 200 OK (text/css)
 - No. 11153 120.122461 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
 - No. 11477 133.945606 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
 - No. 11484 134.253478 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
 - No. 11826 150.944267 44.228.249.3 172.16.30.150 HTTP 330 HTTP/1.1 302 Found (text/html)
 - No. 11830 151.251261 44.228.249.3 172.16.30.150 HTTP 1342 HTTP/1.1 200 OK (text/html)
- Selected Packet:** Frame 8739: Packet, 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface '\Device\NPF_{...}'
 - Hex View:** Shows raw bytes from 0x0000 to 0x00f0.
 - Text View:** Shows the ASCII representation of the captured data.
- Bottom Status Bar:** Packets: 12062 - Displayed: 13 (0.1%). Profile: Default.
- System Icons:** Weather (22°C), Cloudiness (Mostly cloudy), Battery, Network, Sound, Volume, and Date/Time (12/16/2025, 7:34 PM).



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 ?

