Task - 1

Wireshark · DNS · Wi-Fi

Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	397				0.0087	100%	0.1000	11.160
Answer Type	541				0.0119	100%	0.2300	20.586
A	445				0.0098	82.26%	0.1800	20.586
SOA	51				0.0011	9.43%	0.0200	12.907
CNAME	41				0.0009	7.58%	0.0400	20.586
HTTPS	4				0.0001	0.74%	0.0100	8.606
rcode	397				0.0087	100%	0.1000	11.160
No error	397				0.0087	100.00%	0.1000	11.160
opcodes	397				0.0087	100%	0.1000	11.160
Standard query	397				0.0087	100.00%	0.1000	11.160
Response	397				0.0087	100%	0.1000	11.160
Query	234				0.0051	58.94%	0.0800	9.129
Response	163				0.0036	41.06%	0.0400	20.586
Query Type	397				0.0087	100%	0.1000	11.160
A	246				0.0054	61.96%	0.0500	11.160
HTTPS	151				0.0033	38.04%	0.0500	11.161
Payload size	397	433.64	32	1000	0.0087	100%	0.1000	11.160
Class	397				0.0087	100%	0.1000	11.160
IN	397				0.0087	100.00%	0.1000	11.160
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	161	2560.87	1845.317993	4646.401855	0.0035		0.0400	20.586
no. of retransmissions	2				0.0000		0.0200	36.363

Display filter: Enter a display filter ... Apply

Copy Save as... Close

Wireshark · DNS/Query-Response · Wi-Fi

Topic / Item	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total	397				0.0087	100%	0.1000	11.160
Query	234				0.0051	58.94%	0.0800	9.129
Response	163				0.0036	41.06%	0.0400	20.586
Response	0				0.0000	100%	-	-
Servicing	163				0.0036		0.0400	20.586
Answered (ms)	161	2560.87	1845.317993	4646.401855	0.0035	98.77%	0.0400	20.586
Retransmissions	2				0.0000	1.23%	0.0200	36.363
Unsolicited	0				0.0000	0.00%	-	-
Rcodes	163				0.0036		0.0400	20.586
No error	163				0.0036	100.00%	0.0400	20.586
Payload	163				0.0036		0.0400	20.586
<= 1KB	163				0.0036	100.00%	0.0400	20.586
Kind	163				0.0036		0.0400	20.586
Non-Authoritative	163				0.0036	100.00%	0.0400	20.586
From	163				0.0036		0.0400	20.586
8.8.8.8	58				0.0013	35.58%	0.0400	20.586
202.122.21.106	55				0.0012	33.74%	0.0300	10.446
183.82.243.66	50				0.0011	30.67%	0.0300	9.833
Authorities	163				0.0036		0.0400	20.586
zero	112				0.0025	68.71%	0.0300	18.945
= 1	51				0.0011	31.29%	0.0200	12.907
Answers	163				0.0036		0.0400	20.586

Display filter: Enter a display filter ... Apply

Copy Save as... Close

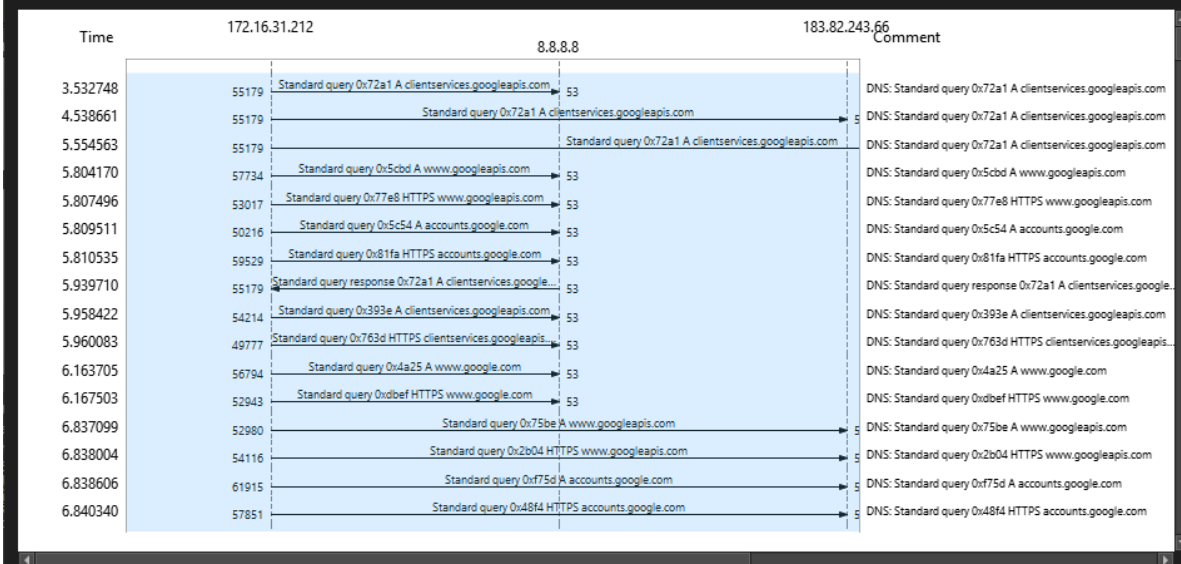
Wireshark · IPv4 Statistics / All Addresses · Wi-Fi

Topic / Item	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	1616				0.0279	100%	1.4500	38.095
172.16.31.212	1377				0.0238	85.21%	1.4200	38.110
216.239.38.120	217				0.0037	13.43%	0.7100	15.460
142.251.222.138	200				0.0035	12.38%	1.3900	38.110
8.8.8.8	140				0.0024	8.66%	0.0800	9.129
202.122.21.106	133				0.0023	8.23%	0.1000	11.160
183.82.243.66	124				0.0021	7.67%	0.0800	10.141
224.0.0.251	111				0.0019	6.87%	0.0400	7.373
142.251.223.14	83				0.0014	5.14%	0.2600	24.191
172.217.24.138	78				0.0013	4.83%	0.1400	18.275
142.250.207.78	70				0.0012	4.33%	0.2200	48.916
239.255.255.250	52				0.0009	3.22%	0.0600	51.509
44.228.249.3	49				0.0008	3.03%	0.0600	23.109
172.16.31.100	42				0.0007	2.60%	0.0700	45.775
74.125.68.84	39				0.0007	2.41%	0.1300	17.207
142.250.205.46	38				0.0007	2.35%	0.3000	25.897
172.16.31.8	35				0.0006	2.17%	0.0200	27.649
172.217.24.110	32				0.0006	1.98%	0.1900	20.671
142.251.43.67	31				0.0005	1.92%	0.1500	20.670
142.251.43.74	29				0.0005	1.79%	0.1500	48.437
142.250.205.99	29				0.0005	1.79%	0.1800	21.053
172.16.30.147	28				0.0005	1.73%	0.0300	0.922

Display filter: Enter a display filter ... Apply

Copy Save as... Close

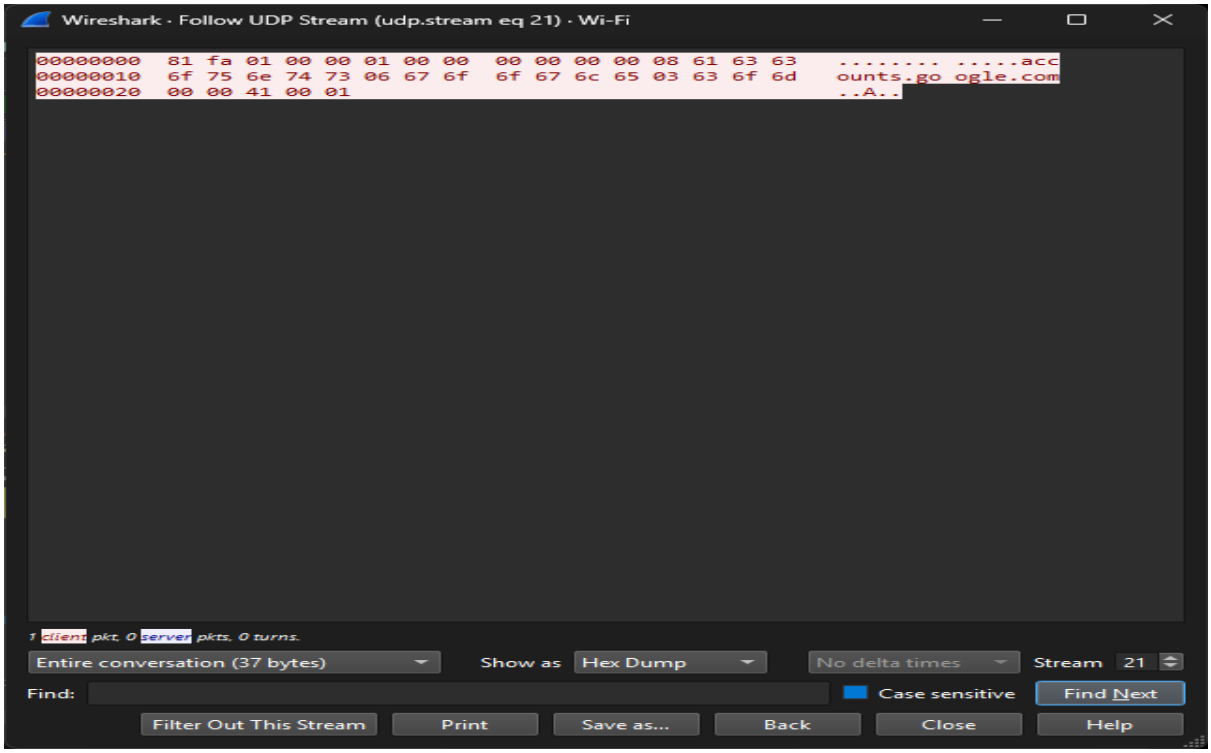
Wireshark · Flow · Wi-Fi



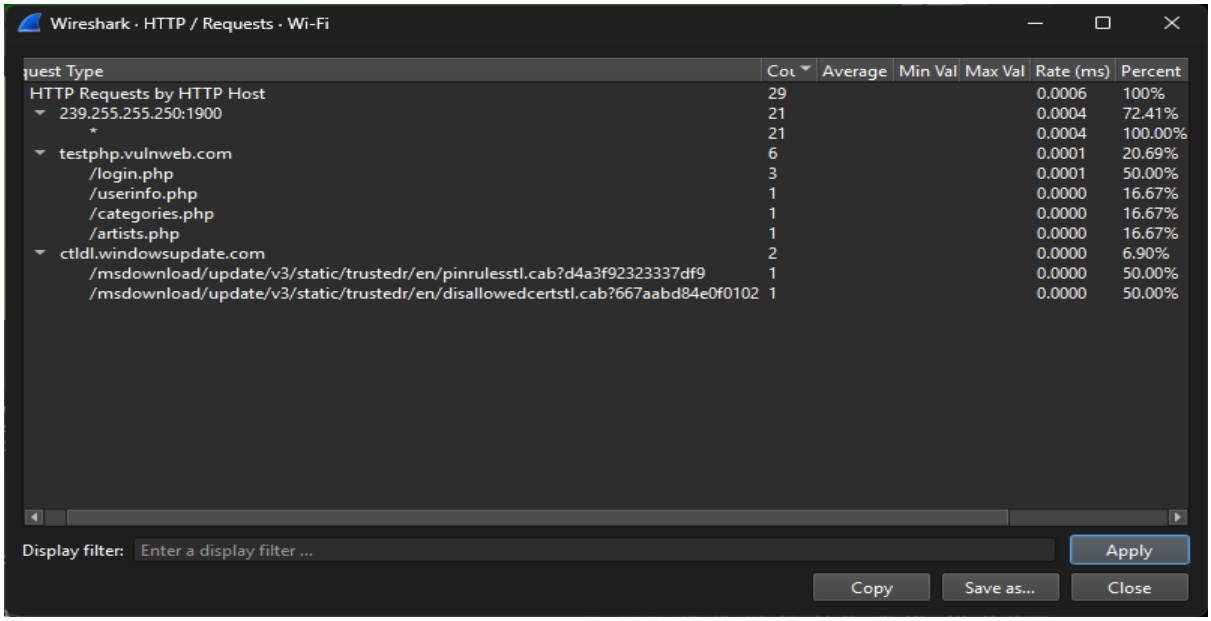
4 nodes, 397 items

Limit to display filter Flow type: All Flows Addresses: Any

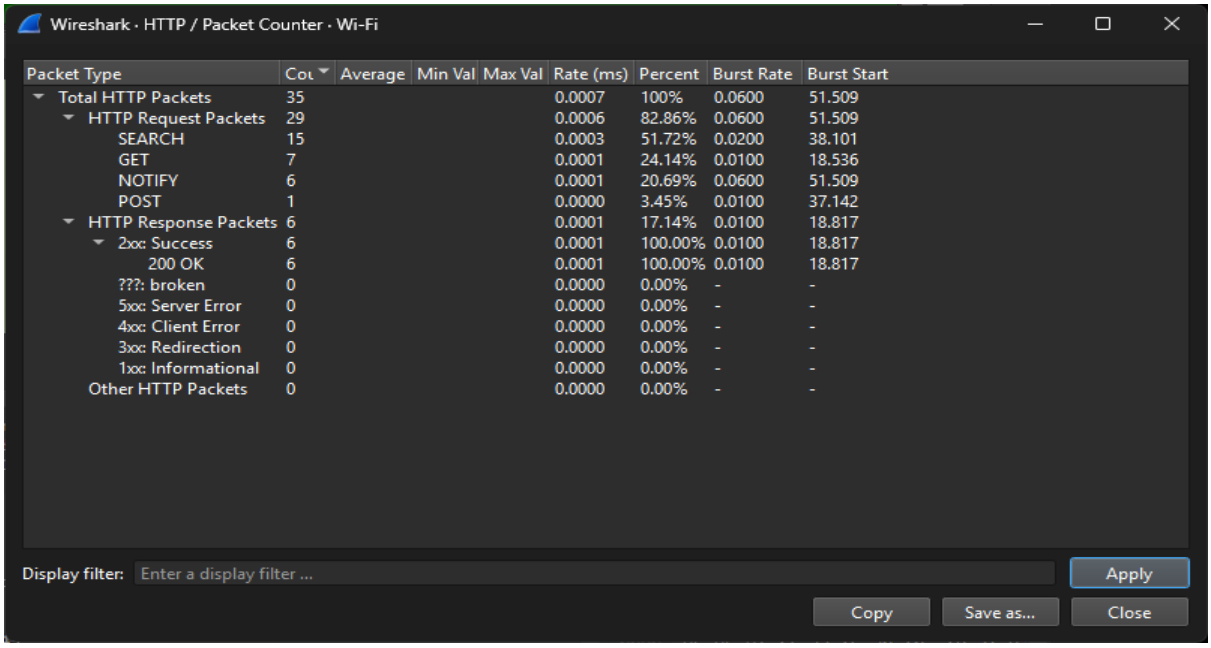
Reset Diagram Export Close Help



2.)

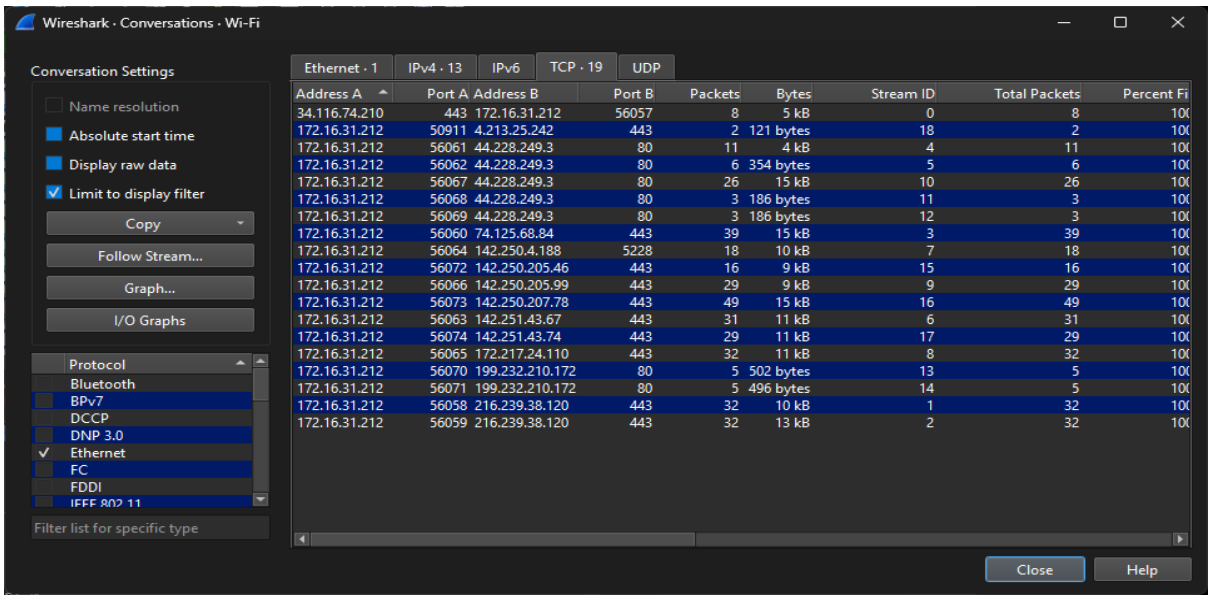


uest Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent
HTTP Requests by HTTP Host	29				0.0006	100%
239.255.255.250:1900	21				0.0004	72.41%
*	21				0.0004	100.00%
testphp.vulnweb.com	6				0.0001	20.69%
/login.php	3				0.0001	50.00%
/userinfo.php	1				0.0000	16.67%
/categories.php	1				0.0000	16.67%
/artists.php	1				0.0000	16.67%
ctldl.windowsupdate.com	2				0.0000	6.90%
/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?d4a3f92323337df9	1				0.0000	50.00%
/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?667aabd84e0f0102	1				0.0000	50.00%



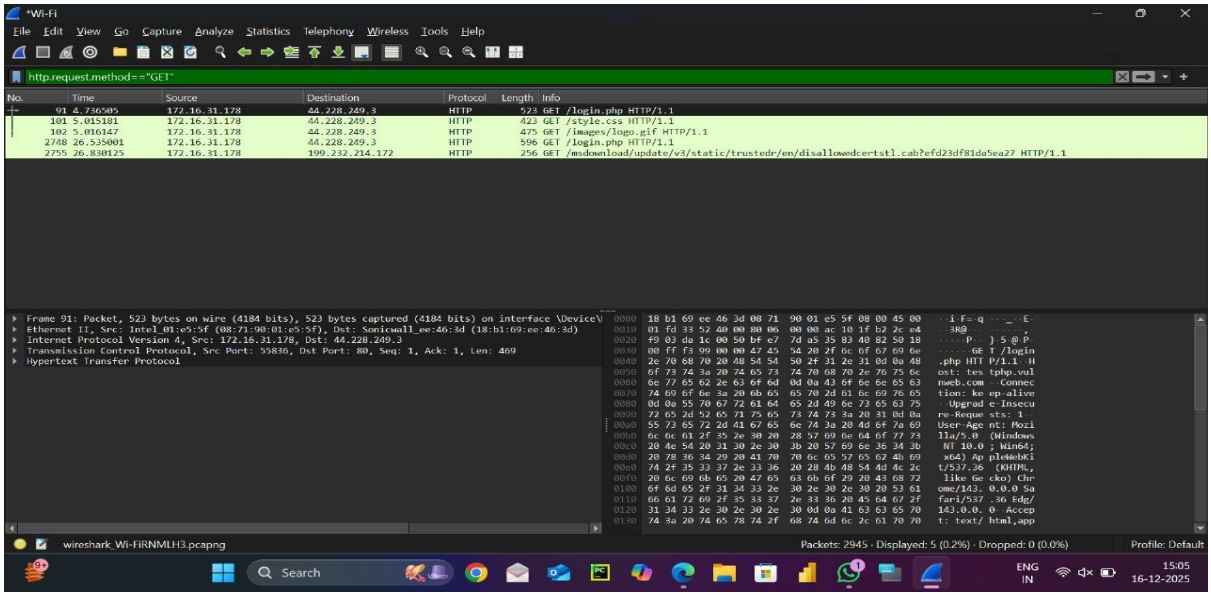
Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	35				0.0007	100%	0.0600	51.509
HTTP Request Packets	29				0.0006	82.86%	0.0600	51.509
SEARCH	15				0.0003	51.72%	0.0200	38.101
GET	7				0.0001	24.14%	0.0100	18.536
NOTIFY	6				0.0001	20.69%	0.0600	51.509
POST	1				0.0000	3.45%	0.0100	37.142
HTTP Response Packets	6				0.0001	17.14%	0.0100	18.817
2xx: Success	6				0.0001	100.00%	0.0100	18.817
200 OK	6				0.0001	100.00%	0.0100	18.817
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
Other HTTP Packets	0				0.0000	0.00%	-	-

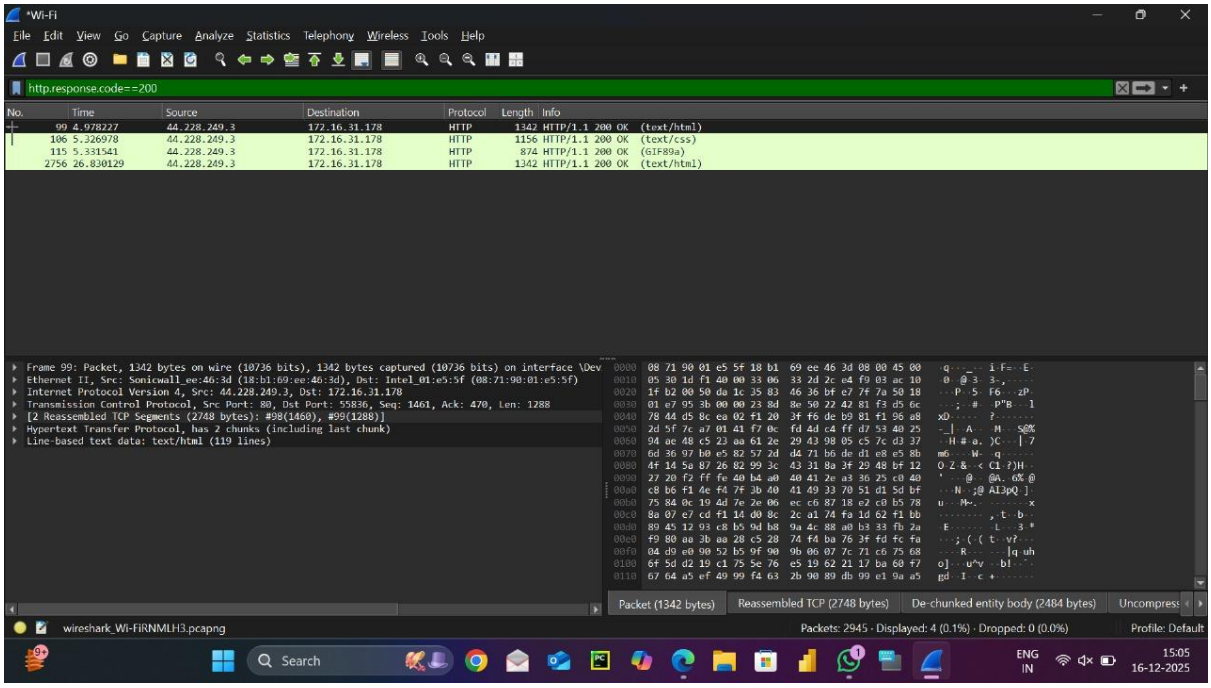
3.) & 4.)

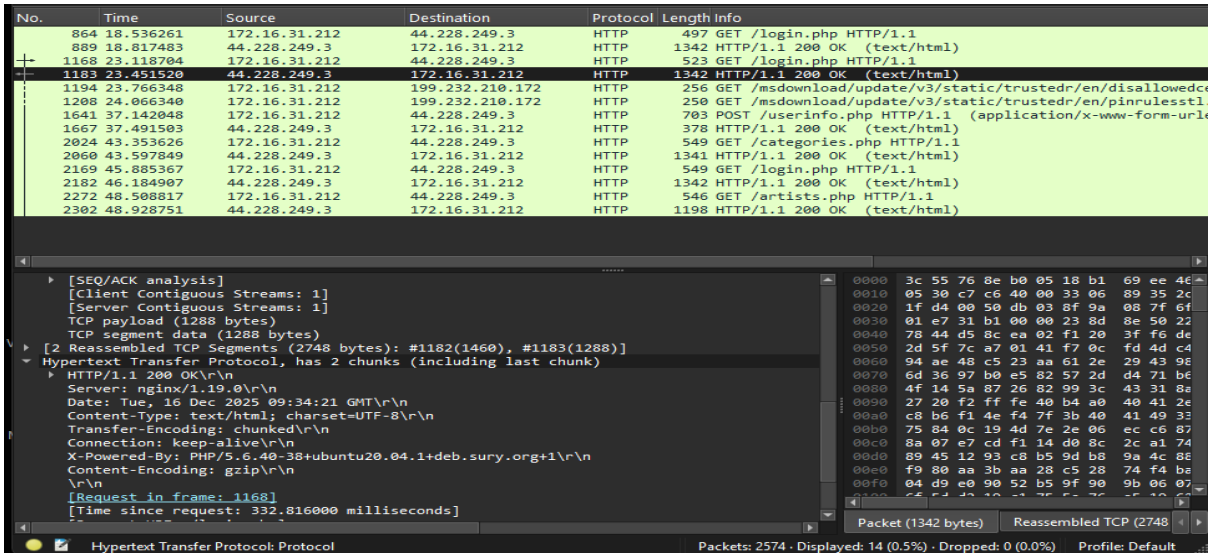


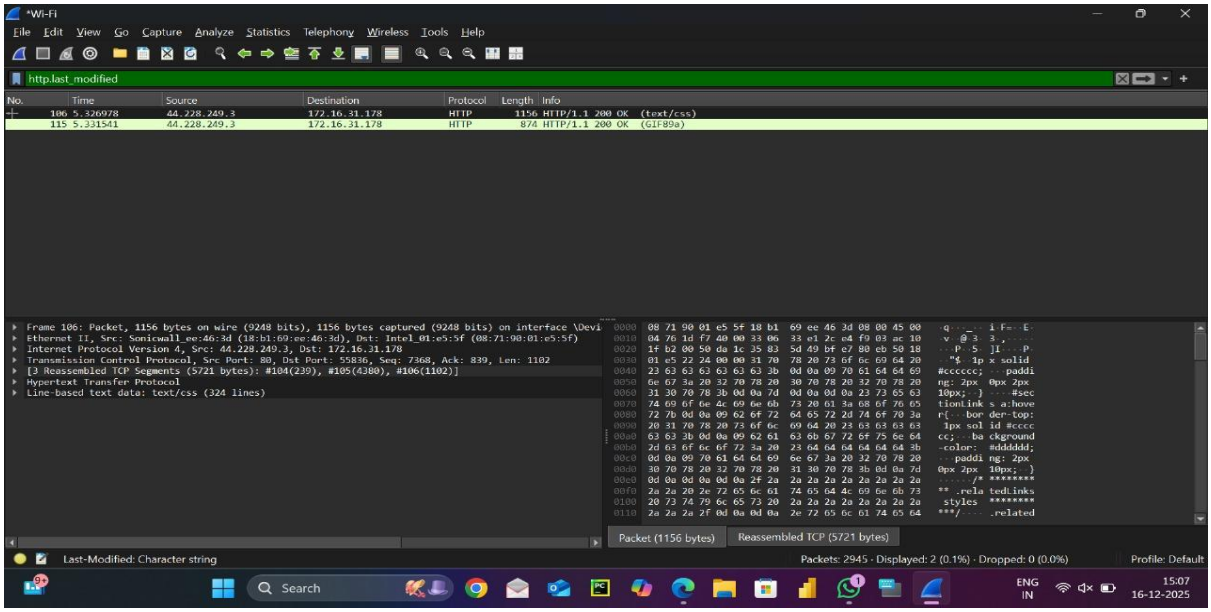
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Fi
34.116.74.210	443	172.16.31.212	56057	8	5 kB	0	8	10
172.16.31.212	50911	4.213.25.242	443	2	121 bytes	18	2	10
172.16.31.212	56061	44.228.249.3	80	11	4 kB	4	11	10
172.16.31.212	56062	44.228.249.3	80	6	354 bytes	5	6	10
172.16.31.212	56067	44.228.249.3	80	26	15 kB	10	26	10
172.16.31.212	56068	44.228.249.3	80	3	186 bytes	11	3	10
172.16.31.212	56069	44.228.249.3	80	3	186 bytes	12	3	10
172.16.31.212	56060	74.125.68.84	443	39	15 kB	3	39	10
172.16.31.212	56064	142.250.4.188	5228	18	10 kB	7	18	10
172.16.31.212	56072	142.250.205.46	443	16	9 kB	15	16	10
172.16.31.212	56066	142.250.205.99	443	29	9 kB	9	29	10
172.16.31.212	56073	142.250.207.78	443	49	15 kB	16	49	10
172.16.31.212	56063	142.251.43.67	443	31	11 kB	6	31	10
172.16.31.212	56074	142.251.43.74	443	29	11 kB	17	29	10
172.16.31.212	56065	172.217.24.110	443	32	11 kB	8	32	10
172.16.31.212	56070	199.232.210.172	80	5	502 bytes	13	5	10
172.16.31.212	56071	199.232.210.172	80	5	496 bytes	14	5	10
172.16.31.212	56058	216.239.38.120	443	32	10 kB	1	32	10
172.16.31.212	56059	216.239.38.120	443	32	13 kB	2	32	10

Task – 2

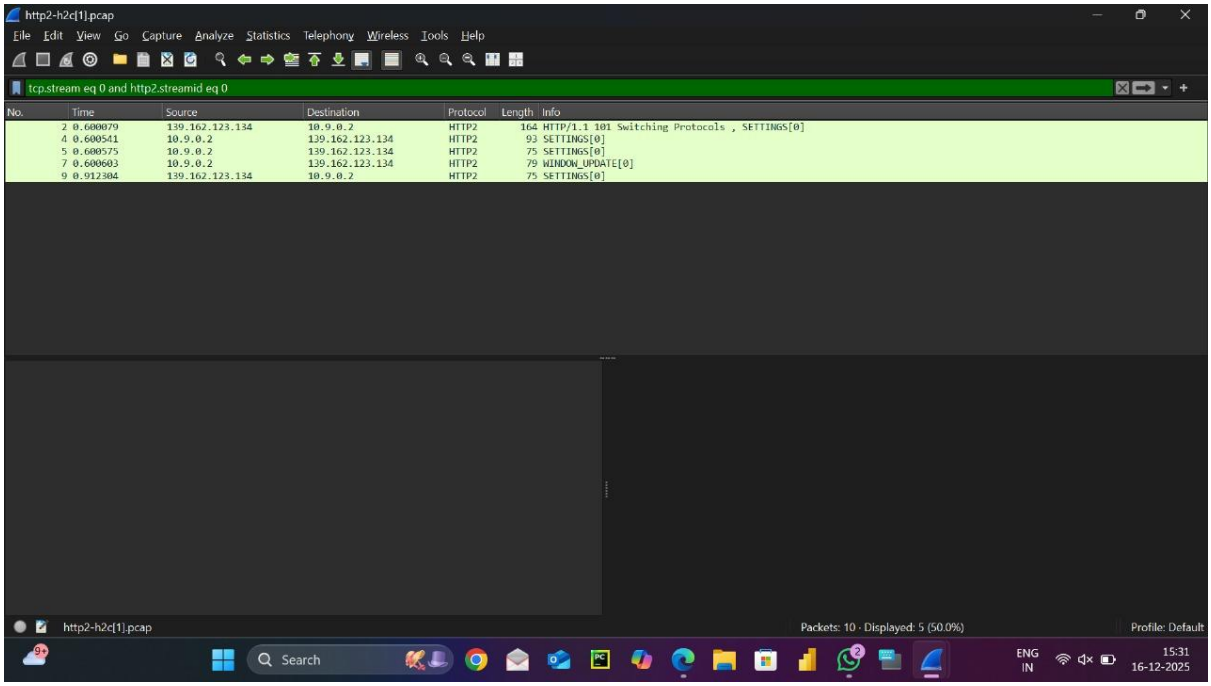

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method==*GET*
No. Time Source Destination Protocol Length Info
91 4.736505 172.16.31.178 44.228.249.3 HTTP 523 GET /login.php HTTP/1.1
101 5.015181 172.16.31.178 44.228.249.3 HTTP 423 GET /style.css HTTP/1.1
102 5.016147 172.16.31.178 44.228.249.3 HTTP 475 GET /images/logo.gif HTTP/1.1
2748 26.535001 172.16.31.178 44.228.249.3 HTTP 596 GET /login.php HTTP/1.1
2755 26.830125 172.16.31.178 199.232.214.172 HTTP 256 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?efd23df81da5ea27 HTTP/1.1
Frame 91: Packet, 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface \Device\
Ethernet II, Src: Intel_01:e5:5f (08:71:90:01:e5:5f), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
Internet Protocol Version 4, Src: 172.16.31.178, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 55836, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
Hypertext Transfer Protocol
wireshark_Wi-FiRNMLH3.pcapng
Packets: 2945 · Displayed: 5 (0.2%) · Dropped: 0 (0.0%)
Profile: Default
Search
ENG IN
15:05 16-12-2025

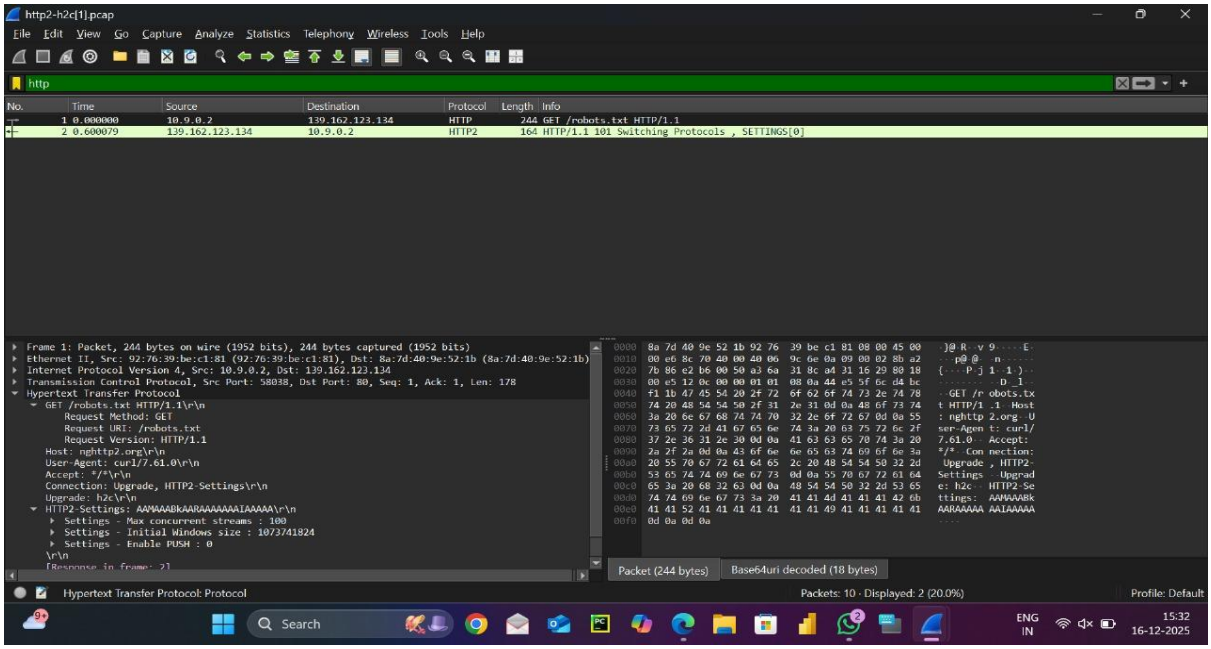

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response.code==200
No. Time Source Destination Protocol Length Info
99 4.978227 44.228.249.3 172.16.31.178 HTTP 1342 HTTP/1.1 200 OK (text/html)
106 5.326978 44.228.249.3 172.16.31.178 HTTP 1156 HTTP/1.1 200 OK (text/css)
115 5.331541 44.228.249.3 172.16.31.178 HTTP 874 HTTP/1.1 200 OK (GIF89a)
2756 26.830129 44.228.249.3 172.16.31.178 HTTP 1342 HTTP/1.1 200 OK (text/html)
Frame 99: Packet, 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on interface \Dev
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: Intel_01:e5:5f (08:71:90:01:e5:5f)
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.31.178
Transmission Control Protocol, Src Port: 80, Dst Port: 55836, Seq: 1461, Ack: 470, Len: 1288
[2 Reassembled TCP Segments (2748 bytes): #98(160), #99(1288)]
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
Line-based text data: text/html (119 lines)
Packet (1342 bytes)
Reassembled TCP (2748 bytes)
De-chunked entity body (2484 bytes)
wireshark_Wi-FiRNMLH3.pcapng
Packets: 2945 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
Search
ENG IN
15:05 16-12-2025


No. Time Source Destination Protocol Length Info
864 18.536261 172.16.31.212 44.228.249.3 HTTP 497 GET /login.php HTTP/1.1
889 18.817483 44.228.249.3 172.16.31.212 HTTP 1342 HTTP/1.1 200 OK (text/html)
1168 23.118704 172.16.31.212 44.228.249.3 HTTP 523 GET /login.php HTTP/1.1
1183 23.451520 44.228.249.3 172.16.31.212 HTTP 1342 HTTP/1.1 200 OK (text/html)
1194 23.766348 172.16.31.212 199.232.210.172 HTTP 256 GET /msdownload/update/v3/static/trustedr/en/disallowedc
1208 24.066340 172.16.31.212 199.232.210.172 HTTP 250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl
1641 37.142048 172.16.31.212 44.228.249.3 HTTP 703 POST /userinfo.php HTTP/1.1 (application/x-www-form-urle
1667 37.491503 44.228.249.3 172.16.31.212 HTTP 378 HTTP/1.1 200 OK (text/html)
2024 43.353626 172.16.31.212 44.228.249.3 HTTP 549 GET /categories.php HTTP/1.1
2060 43.597849 44.228.249.3 172.16.31.212 HTTP 1341 HTTP/1.1 200 OK (text/html)
2169 45.885367 172.16.31.212 44.228.249.3 HTTP 549 GET /login.php HTTP/1.1
2182 46.184907 44.228.249.3 172.16.31.212 HTTP 1342 HTTP/1.1 200 OK (text/html)
2272 48.508817 172.16.31.212 44.228.249.3 HTTP 546 GET /artists.php HTTP/1.1
2302 48.928751 44.228.249.3 172.16.31.212 HTTP 1198 HTTP/1.1 200 OK (text/html)
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
TCP payload (1288 bytes)
TCP segment data (1288 bytes)
[2 Reassembled TCP Segments (2748 bytes): #1182(1460), #1183(1288)]
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
HTTP/1.1 200 OK\r\n
Server: nginx/1.19.0\r\n
Date: Tue, 16 Dec 2025 09:34:21 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n
Content-Encoding: gzip\r\n
\r\n
[Request in frame: 1168]
[Time since request: 332.816000 milliseconds]
Packet (1342 bytes)
Reassembled TCP (2748
Hypertext Transfer Protocol: Protocol
Packets: 2574 · Displayed: 14 (0.5%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.last_modified
No. Time Source Destination Protocol Length Info
106 5.326978 44.228.249.3 172.16.31.178 HTTP 1156 HTTP/1.1 200 OK (text/css)
115 5.331541 44.228.249.3 172.16.31.178 HTTP 874 HTTP/1.1 200 OK (GIF89a)
Frame 106: Packet, 1156 bytes on wire (9248 bits), 1156 bytes captured (9248 bits) on interface \Devi
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: Intel_01:e5:5f (08:71:90:01:e5:5f)
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.31.178
Transmission Control Protocol, Src Port: 80, Dst Port: 55836, Seq: 7368, Ack: 839, Len: 1102
[3 Reassembled TCP Segments (5721 bytes): #104(239), #105(4380), #106(1102)]
Hypertext Transfer Protocol
Line-based text data: text/css (324 lines)
Packet (1156 bytes)
Reassembled TCP (5721 bytes)
Last-Modified: Character string
Packets: 2945 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
Search
ENG
IN
15:07
16-12-2025

Task - 3


http2-h2c[1].pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0 and http2.streamid eq 0
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]
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]
7 0.600603 10.9.0.2 139.162.123.134 HTTP2 79 WINDOW_UPDATE[0]
9 0.912304 139.162.123.134 10.9.0.2 HTTP2 75 SETTINGS[0]
http2-h2c[1].pcap
Packets: 10 · Displayed: 5 (50.0%)
Profile: Default
Search
ENG IN
15:31 16-12-2025


http2-h2c[1].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 0.600079 139.162.123.134 10.9.0.2 HTTP2 164 HTTP/1.1 101 Switching Protocols , SETTINGS[0]
Frame 1: Packet, 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 1, Ack: 1, Len: 178
Hypertext Transfer Protocol
GET /robots.txt HTTP/1.1\r\n
Request Method: GET
Request URI: /robots.txt
Request Version: HTTP/1.1
Host: nghttp2.org\r\n
User-Agent: curl/7.61.0\r\n
Accept: */*\r\n
Connection: Upgrade, HTTP2-Settings\r\n
Upgrade: h2c\r\n
HTTP2-Settings: AAMAAABkAARAAAAAAAIAAAAA\r\n
Settings - Max concurrent streams : 100
Settings - Initial Windows size : 1073741824
Settings - Enable PUSH : 0
\r\n
Packet (244 bytes)
Base64uri decoded (18 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 10 · Displayed: 2 (20.0%)
Profile: Default
Search
ENG IN
15:32 16-12-2025

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	0.600079	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 capture
Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:
Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq
Hypertext Transfer Protocol
  HTTP/1.1 101 Switching Protocols\r\n
    Response Version: HTTP/1.1
    Status Code: 101
    [Status Code Description: Switching Protocols]
    Response Phrase: Switching Protocols
  Connection: Upgrade\r\n
  Upgrade: h2c\r\n
  \r\n
  [Request in frame: 1]
  [Time since request: 600.079000 milliseconds]
  [Request URI: /robots.txt]
  [Full request URI: http://nghttp2.org/robots.txt]
HyperText Transfer Protocol 2
  Stream: SETTINGS, Stream ID: 0, Length 18
    Length: 18
    Type: SETTINGS (4)
    Flags: 0x00
      0000 000. = Unused: 0x00
      .... ...0 = ACK: False
    0... .... .... .... .... .... .... .... = Reserved: 0x0
    .000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier
    Settings - Max concurrent streams : 100
      Settings Identifier: Max concurrent streams (3)
      Max concurrent streams: 100
    Settings - Initial Windows size : 1048576
      Settings Identifier: Initial Windows size (4)
      Initial Window Size: 1048576
    Settings - Header table size : 8192
      Settings Identifier: Header table size (1)
      Header table size: 8192
```

```
0000  92 76 39 be c1 81 8a 7d  40 9e 52 1b 08 00 45 20   ·v9····} @
0010  00 96 db ad 40 00 35 06  58 61 8b a2 7b 86 0a 09   ····@ 5· X
0020  00 02 00 50 e2 b6 a4 31  16 29 a3 6a 32 3e 80 18   ···P···1 ·
0030  00 eb 2c 43 00 00 01 01  08 0a d4 bc f2 56 44 e5   ··,C····
0040  5f 6c 48 54 54 50 2f 31  2e 31 20 31 30 31 20 53   _lHTTP/1 .
0050  77 69 74 63 68 69 6e 67  20 50 72 6f 74 6f 63 6f   witching
0060  6c 73 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   ls··Conn e
0070  55 70 67 72 61 64 65 0d  0a 55 70 67 72 61 64 65   Upgrade··
0080  3a 20 68 32 63 0d 0a 0d  0a 00 00 12 04 00 00 00   : h2c···
0090  00 00 00 03 00 00 00 64  00 04 00 10 00 00 00 01   ·····d ·
00a0  00 00 20 00                                        ··
```