

1. Command: http or dns

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays a series of DNS queries and responses. The packet details pane shows the structure of a DNS query packet, including the Ethernet II header, Internet Protocol Version 6 header, User Datagram Protocol header, and Domain Name System (query) header. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
9909	66.684270	fe80::c9a4:956f:df7...	fe80::1	DNS	97	Standard query 0xbf22 AAAA bh.contextweb.com
9910	66.684480	fe80::c9a4:956f:df7...	fe80::1	DNS	97	Standard query 0x217e HTTPS bh.contextweb.com
9911	66.684765	fe80::c9a4:956f:df7...	fe80::1	DNS	94	Standard query 0xf4da A eu-u.openx.net
9912	66.684995	fe80::c9a4:956f:df7...	fe80::1	DNS	94	Standard query 0x905f AAAA eu-u.openx.net
9913	66.685182	fe80::c9a4:956f:df7...	fe80::1	DNS	94	Standard query 0x1b7f HTTPS eu-u.openx.net
9957	66.775533	fe80::c9a4:956f:df7...	fe80::1	DNS	95	Standard query 0x69fe A csync.loopme.me
9958	66.775776	fe80::c9a4:956f:df7...	fe80::1	DNS	95	Standard query 0x5796 AAAA csync.loopme.me
9959	66.775991	fe80::c9a4:956f:df7...	fe80::1	DNS	95	Standard query 0x1d3b HTTPS csync.loopme.me
10082	66.804437	192.168.1.1	192.168.1.6	DNS	426	Standard query response 0x6758 A dt.adsafeprotected.com CNAME vadt.adsafeprotected.com CNAME dt-external-217593033.us-east-1.elb...
10092	66.805021	192.168.1.1	192.168.1.6	DNS	522	Standard query response 0x473b AAAA dt.adsafeprotected.com CNAME vadt.adsafeprotected.com CNAME dt-external-217593033.us-east-1.e...
10093	66.805021	192.168.1.1	192.168.1.6	DNS	243	Standard query response 0xfce1 HTTPS dt.adsafeprotected.com CNAME vadt.adsafeprotected.com CNAME dt-external-217593033.us-east-1.e...
10118	66.812399	192.168.1.1	192.168.1.6	DNS	356	Standard query response 0x167d A f-log-extension.grammarly.io A 18.235.187.54 A 3.228.122.249 A 3.209.185.9 A 34.206.189.106 A 3...
10119	66.812399	192.168.1.1	192.168.1.6	DNS	175	Standard query response 0xe532 AAAA f-log-extension.grammarly.io SOA ns-1768.awsdns-29.co.uk
10120	66.812399	192.168.1.1	192.168.1.6	DNS	175	Standard query response 0x6f42 HTTPS f-log-extension.grammarly.io SOA ns-1768.awsdns-29.co.uk
10122	66.812672	192.168.1.1	192.168.1.6	DNS	326	Standard query response 0xd3f0 A static.adsafeprotected.com CNAME d162h6x3rxav67.cloudfront.net A 143.204.215.77 A 143.204.215.20...
10123	66.812672	192.168.1.1	192.168.1.6	DNS	486	Standard query response 0x64a8 AAAA static.adsafeprotected.com CNAME d162h6x3rxav67.cloudfront.net AAAA 2600:9000:21f3:4400:8:48e...
10124	66.812672	192.168.1.1	192.168.1.6	DNS	206	Standard query response 0x1b9b HTTPS static.adsafeprotected.com CNAME d162h6x3rxav67.cloudfront.net SOA ns-56.awsdns-07.com
10156	66.861811	192.168.1.1	192.168.1.6	DNS	164	Standard query response 0xe406 HTTPS b1sync.zemanta.com CNAME zemanta-nychi.zemanta.com SOA ian.ns.cloudflare.com
10157	66.861811	fe80::1	fe80::c9a4:956f:df7...	DNS	163	Standard query response 0xf6da A bh.contextweb.com CNAME sic-bh.contextweb.com CNAME sic-direct-beo.contextweb.com A 74.214.196.1...

Frame 209: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF_{7E6BD555...} (d8:f3:bc:de:ee:af), Src: LiteonTe_de:ee:af (d8:f3:bc:de:ee:af), Dst: TaicangT_9e:84:50 (5c:f9:fd:9e:84:50)

Ethernet II, Src: LiteonTe_de:ee:af (d8:f3:bc:de:ee:af), Dst: TaicangT_9e:84:50 (5c:f9:fd:9e:84:50)

Internet Protocol Version 6, Src: fe80::c9a4:956f:df78:7e8c, Dst: fe80::1

User Datagram Protocol, Src Port: 50633, Dst Port: 53

Domain Name System (query)

0000 5c f9 fd 9e 84 50 d8 f3 bc de ee af 86 dd 60 0d \...P... ..
0010 49 9f 00 29 11 40 fe 80 00 00 00 00 00 c9 a4 I...} @... ..
0020 95 6f df 78 7e 8c fe 80 00 00 00 00 00 00 00 o x... ..
0030 00 00 00 00 00 01 c5 c9 00 35 00 29 35 65 a9 3d5...)Se...
0040 01 00 00 01 00 00 00 00 00 00 04 61 70 69 73 06apis...
0050 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 google:c om....

2. Command: tcp.port==80

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays a series of TCP connections and responses. The packet details pane shows the structure of a TCP packet, including the Ethernet II header, Internet Protocol Version 6 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.423855	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	112	80 → 56761 [PSH, ACK] Seq=1 Ack=1 Win=638 Len=38
12	0.477716	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	74	56761 → 80 [ACK] Seq=1 Ack=39 Win=514 Len=0
42	2.201603	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	267	80 → 56761 [PSH, ACK] Seq=39 Ack=1 Win=638 Len=193
43	2.247502	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	74	56761 → 80 [ACK] Seq=1 Ack=232 Win=513 Len=0
44	2.254474	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	120	56761 → 80 [PSH, ACK] Seq=1 Ack=232 Win=513 Len=46
46	2.417650	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	74	80 → 56761 [ACK] Seq=232 Ack=47 Win=638 Len=0
93	3.557622	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	138	80 → 56761 [PSH, ACK] Seq=232 Ack=47 Win=638 Len=64
101	3.567627	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	245	56761 → 80 [PSH, ACK] Seq=47 Ack=296 Win=513 Len=171
102	3.567725	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	120	56761 → 80 [PSH, ACK] Seq=218 Ack=296 Win=513 Len=46
104	3.596729	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	74	80 → 56761 [ACK] Seq=296 Ack=218 Win=649 Len=0
105	3.596729	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	74	80 → 56761 [ACK] Seq=296 Ack=264 Win=649 Len=0
109	3.836383	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	540	80 → 56761 [PSH, ACK] Seq=296 Ack=264 Win=649 Len=466
111	3.880119	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	74	56761 → 80 [ACK] Seq=264 Ack=762 Win=511 Len=0
194	8.080940	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	110	80 → 56761 [PSH, ACK] Seq=762 Ack=264 Win=649 Len=36
206	8.127140	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	74	56761 → 80 [ACK] Seq=264 Ack=798 Win=511 Len=0
347	8.870603	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	99	56761 → 80 [PSH, ACK] Seq=264 Ack=798 Win=511 Len=25
349	8.898989	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	74	80 → 56761 [ACK] Seq=798 Ack=289 Win=649 Len=0
1485	43.379476	2401:4900:1c96:c9e0...	2a03:2880:f237:c7:f...	TCP	109	56761 → 80 [PSH, ACK] Seq=289 Ack=798 Win=511 Len=35
1486	43.410536	2a03:2880:f237:c7:f...	2401:4900:1c96:c9e0...	TCP	74	80 → 56761 [ACK] Seq=798 Ack=324 Win=649 Len=0

Frame 11: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{7E6BD555...} (d8:f3:bc:de:ee:af), Src: TaicangT_9e:84:50 (5c:f9:fd:9e:84:50), Dst: LiteonTe_de:ee:af (d8:f3:bc:de:ee:af)

Ethernet II, Src: TaicangT_9e:84:50 (5c:f9:fd:9e:84:50), Dst: LiteonTe_de:ee:af (d8:f3:bc:de:ee:af)

Internet Protocol Version 6, Src: 2a03:2880:f237:c7:face:b00c:0:7260, Dst: 2401:4900:1c96:c9e0:d4f8:b3f

Transmission Control Protocol, Src Port: 80, Dst Port: 56761, Seq: 1, Ack: 1, Len: 38

0000 d8 f3 bc de ee af 5c f9 fd 9e 84 50 86 dd 68 c0 \...P...h...
0010 00 00 00 3a 06 39 2a 03 28 80 f2 37 00 c7 fa ce:9* (:7....
0020 b0 0c 00 00 72 60 24 01 49 00 1c 96 c9 e0 d4 f8r"\$- I.....
0030 b3 f2 b0 b0 5b 97 00 50 dd b9 47 33 b6 e8 51 84[-P...G3...Q
0040 b4 c9 50 18 02 7e ab 6b 00 00 00 00 23 4a 37 4a ...P...k ...#773
0050 71 b7 8b 43 21 f3 d9 32 41 ad ed 7a 0a b1 e3 e8 q...Cl...2 A...z...
0060 2f b7 b6 5b 3c 9c 5a ed 55 91 a5 ea bc a6 2d a9 /...[c-z U.....

3) Command: tcp.flags.reset==0

Wireshark capture showing TCP packets with the filter `tcp.flags.reset==0`. The packet list displays several TCP segments, including SYN, ACK, and client hello messages. The packet details pane shows the structure of a TCP segment, including the header and payload.

No.	Time	Source	Destination	Protocol	Length	Info
2026	54.900070	18.66.37.217	192.168.1.6	TCP	54	443 → 57893 [ACK] Seq=6396 Ack=1625 Win=68608 Len=0
2031	54.900070	18.139.212.159	192.168.1.6	TCP	66	443 → 57896 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=256
2032	54.900433	192.168.1.6	18.139.212.159	TCP	54	57896 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2036	54.901198	192.168.1.6	18.139.212.159	TLSv1.2	571	Client Hello
2041	54.933375	23.106.127.160	192.168.1.6	TCP	66	443 → 57898 [SYN, ACK] Seq=0 Ack=1 Win=7300 Len=0 MSS=1412 SACK_PERM WS=8
2042	54.933519	192.168.1.6	23.106.127.160	TCP	54	57898 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2043	54.933593	23.106.127.160	192.168.1.6	TCP	66	443 → 57899 [SYN, ACK] Seq=0 Ack=1 Win=7300 Len=0 MSS=1412 SACK_PERM WS=8
2044	54.933629	192.168.1.6	23.106.127.160	TCP	54	57899 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2045	54.933830	192.168.1.6	23.106.127.160	TLSv1.2	571	Client Hello
2046	54.934089	192.168.1.6	23.106.127.160	TLSv1.2	571	Client Hello
2048	54.958096	52.192.169.200	192.168.1.6	TCP	66	443 → 57892 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=256
2049	54.958227	192.168.1.6	52.192.169.200	TCP	54	57892 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2050	54.958452	192.168.1.6	52.192.169.200	TLSv1.2	571	Client Hello
2055	54.984400	18.139.212.159	192.168.1.6	TCP	54	443 → 57896 [ACK] Seq=1 Ack=518 Win=28160 Len=0
2056	54.984400	18.139.212.159	192.168.1.6	TLSv1.2	1466	[TCP Previous segment not captured], Ignored Unknown Record
2057	54.984400	18.139.212.159	192.168.1.6	TCP	1466	[TCP Out-Of-Order] 443 → 57896 [ACK] Seq=1 Ack=518 Win=28160 Len=1412
2058	54.984400	18.139.212.159	192.168.1.6	TLSv1.2	1185	[TCP Previous segment not captured], Ignored Unknown Record
2059	54.984400	18.139.212.159	192.168.1.6	TCP	1466	[TCP Out-Of-Order] 443 → 57896 [ACK] Seq=2825 Ack=518 Win=28160 Len=1412
2060	54.984570	192.168.1.6	18.139.212.159	TCP	66	[TCP Out-Of-Order] 57896 → 443 [ACK] Seq=518 Ack=1 Win=131072 Len=0 SILENCE=2825

Frame 11: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{7E68D55...}

Ethernet II, Src: TaicangT_9e:84:50 (Sc:f9:fd:9e:84:50), Dst: LiteonTe_de:ee:af (d8:f3:bc:de:ee:af)

Internet Protocol Version 6, Src: 2a03:2880:f237:c7:face:b00c:0:7260, Dst: 2401:4900:1c96:c9e0:d4f8:b3f

Transmission Control Protocol, Src Port: 80, Dst Port: 56761, Seq: 1, Ack: 1, Len: 38

4) Command: http.request

Wireshark capture showing HTTP requests with the filter `http.request`. The packet list displays several HTTP GET requests. The packet details pane shows the structure of an HTTP request, including the header and payload.

No.	Time	Source	Destination	Protocol	Length	Info
13754	112.950695	2401:4900:1c96:c9e0...	2600:140f:b800:1a9:...	HTTP	301	GET / HTTP/1.1
13883	113.522112	2401:4900:1c96:c9e0...	2402:6800:764:a000:...	HTTP	355	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?1112c17cc72fcee HTTP/1.1
14228	115.105055	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
14860	116.110023	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
15045	117.110583	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
15054	118.114747	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18138	235.102606	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18147	236.107751	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18160	237.116673	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18183	238.125754	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21279	355.117412	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21308	356.123842	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21346	357.134980	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21390	358.138981	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24748	475.130319	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24762	476.135616	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24776	477.147686	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24783	478.155980	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
27578	595.135147	192.168.1.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 21390: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{7E68D55...}

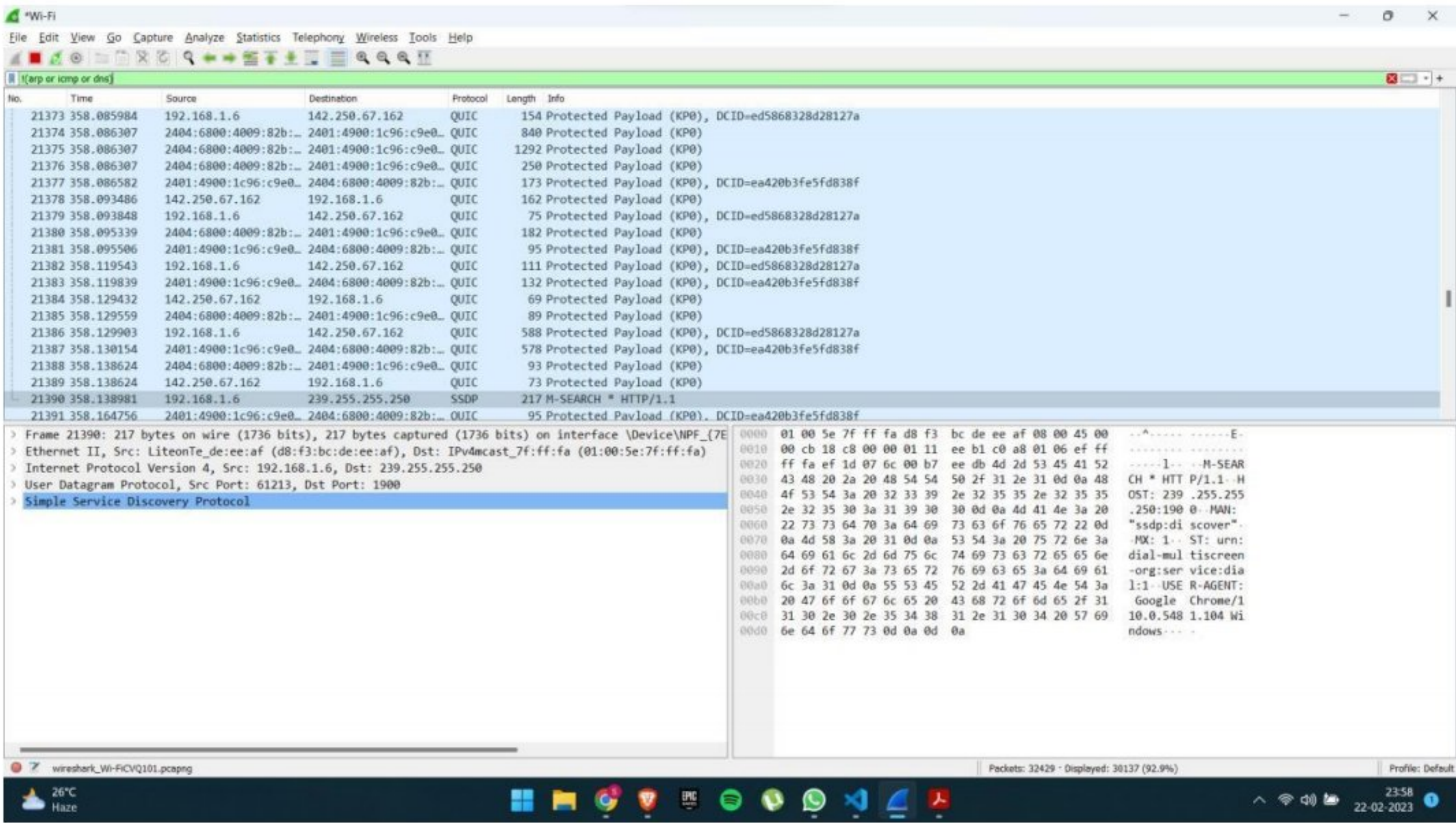
Ethernet II, Src: LiteonTe_de:ee:af (d8:f3:bc:de:ee:af), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.1.6, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 61213, Dst Port: 1900

Simple Service Discovery Protocol

5) Command: !(arp or icmp or dns)



6) Command: not (tcp.port == 80) and not (tcp.port == 25)

