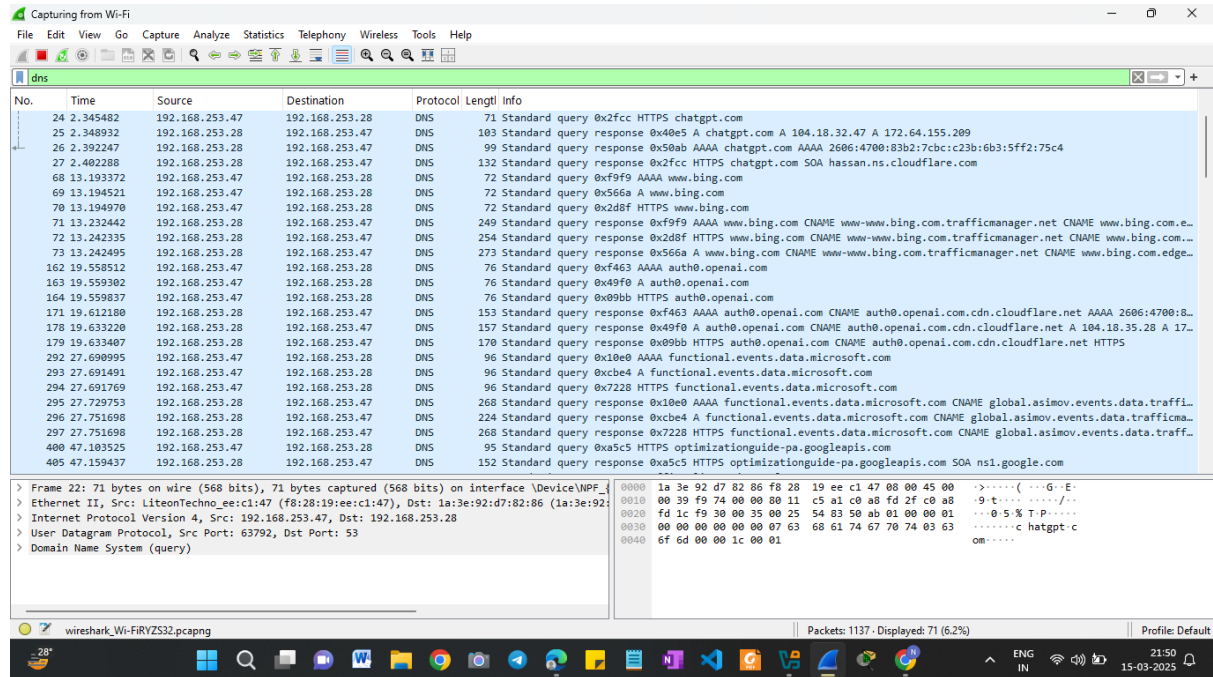


Q2. Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet header, packet flow, options and flags

DNS:

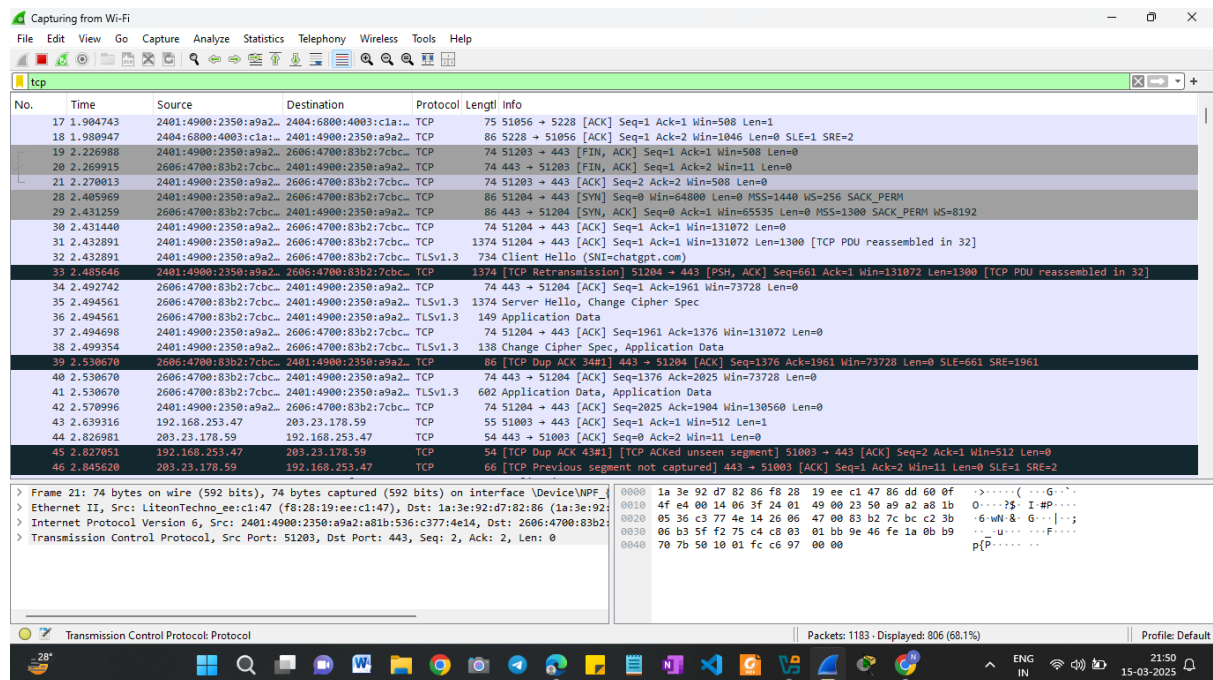


The image shows a Wireshark capture of DNS traffic. The packet list on the left shows 71 packets, all of which are DNS queries or responses. The packet details pane on the right shows the structure of a DNS query, including the question section with a query for 'chatgpt.com'.

No.	Time	Source	Destination	Protocol	Length	Info
24	2.345482	192.168.253.47	192.168.253.28	DNS	71	Standard query 0x2fcc HTTP5 chatgpt.com
25	2.348932	192.168.253.28	192.168.253.47	DNS	163	Standard query response 0x40e5 A chatgpt.com A 104.18.32.47 A 172.64.155.209
26	2.392247	192.168.253.28	192.168.253.47	DNS	99	Standard query response 0x50ab AAAA chatgpt.com AAAA 2606:4700:83b2:7cbc:c23b:6b3:5ff2:75c4
27	2.402288	192.168.253.28	192.168.253.47	DNS	132	Standard query response 0x2fcc HTTP5 chatgpt.com SOA hassan.ns.cloudflare.com
68	13.193372	192.168.253.47	192.168.253.28	DNS	72	Standard query 0xf9f9 AAAA www.bing.com
69	13.194521	192.168.253.47	192.168.253.28	DNS	72	Standard query 0x566a A www.bing.com
70	13.194970	192.168.253.47	192.168.253.28	DNS	72	Standard query 0x2d8f HTTPS www.bing.com
71	13.232442	192.168.253.28	192.168.253.47	DNS	249	Standard query response 0xf9f9 AAAA www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.e...
72	13.242335	192.168.253.28	192.168.253.47	DNS	254	Standard query response 0x2d8f HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com...
73	13.242495	192.168.253.28	192.168.253.47	DNS	273	Standard query response 0x566a A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edge...
162	19.555512	192.168.253.47	192.168.253.28	DNS	76	Standard query 0xf463 AAAA auth0.openai.com
163	19.559302	192.168.253.47	192.168.253.28	DNS	76	Standard query 0x49f0 A auth0.openai.com
164	19.559837	192.168.253.47	192.168.253.28	DNS	76	Standard query 0x89bb HTTPS auth0.openai.com
171	19.612180	192.168.253.28	192.168.253.47	DNS	153	Standard query response 0xf463 AAAA auth0.openai.com CNAME auth0.openai.com.cdn.cloudflare.net AAAA 2606:4700:8...
178	19.633220	192.168.253.28	192.168.253.47	DNS	157	Standard query response 0x49f0 A auth0.openai.com CNAME auth0.openai.com.cdn.cloudflare.net A 104.18.35.28 A 17...
179	19.633407	192.168.253.28	192.168.253.47	DNS	170	Standard query response 0x09bb HTTPS auth0.openai.com CNAME auth0.openai.com.cdn.cloudflare.net HTTPS
292	27.690995	192.168.253.47	192.168.253.28	DNS	96	Standard query 0x10e0 AAAA functional.events.data.microsoft.com
293	27.691491	192.168.253.47	192.168.253.28	DNS	96	Standard query 0xcbe4 A functional.events.data.microsoft.com
294	27.691769	192.168.253.47	192.168.253.28	DNS	96	Standard query 0x7228 HTTPS functional.events.data.microsoft.com
295	27.729753	192.168.253.28	192.168.253.47	DNS	268	Standard query response 0x10e0 AAAA functional.events.data.microsoft.com CNAME global.asimov.events.data.traffi...
296	27.751698	192.168.253.28	192.168.253.47	DNS	224	Standard query response 0xcbe4 A functional.events.data.microsoft.com CNAME global.asimov.events.data.traffica...
297	27.751698	192.168.253.28	192.168.253.47	DNS	268	Standard query response 0x7228 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.traff...
400	47.103525	192.168.253.47	192.168.253.28	DNS	95	Standard query 0xa5c5 HTTPS optimizationguide-pa.googleapis.com
405	47.159437	192.168.253.28	192.168.253.47	DNS	152	Standard query response 0xa5c5 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com

Frame 21: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF...  
> Ethernet II, Src: LiteonTechno\_ee:c1:47 (f8:28:19:ee:c1:47), Dst: 1a:3e:92:d7:82:86 (1a:3e:92:...) [0000 1a 3e 92 d7 82 86 f8 28 19 ee c1 47 00 00 45 00 ->.....(G-E-  
[0010 00 39 f9 74 00 00 00 11 c5 a1 c0 a8 fd 2f c0 a8 ->9...../  
[0020 fd 1c f9 30 00 35 00 25 54 83 50 ab 01 00 00 01 ->0 5% T:P.....  
[0030 00 00 00 00 00 07 63 68 61 74 67 70 74 03 63 ->.....c hatgpt:c  
[0040 6f 6d 00 00 1c 00 01 om.....

TCP:



The image shows a Wireshark capture of TCP traffic. The packet list on the left shows 46 packets, including a SYN exchange, a client hello, and a server hello. The packet details pane on the right shows the structure of a TCP segment, including the source and destination ports and the sequence number.

No.	Time	Source	Destination	Protocol	Length	Info
17	1.904743	2401:4900:2350:a9a2..	2404:6800:4003:c1a1..	TCP	75	51056 -> 5228 [ACK] Seq=1 Ack=1 Win=508 Len=1
18	1.980947	2404:6800:4003:c1a1..	2401:4900:2350:a9a2..	TCP	86	5228 -> 51056 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
19	2.226988	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	74	51203 -> 443 [FIN, ACK] Seq=1 Ack=1 Win=508 Len=0
20	2.269915	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TCP	74	443 -> 51203 [FIN, ACK] Seq=1 Ack=2 Win=11 Len=0
21	2.270013	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	74	51203 -> 443 [ACK] Seq=2 Ack=2 Win=508 Len=0
28	2.405969	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	86	51204 -> 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
29	2.431259	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TCP	86	443 -> 51204 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM WS=8192
30	2.431440	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	74	51204 -> 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
31	2.432891	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	1374	51204 -> 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1300 [TCP PDU reassembled in 32]
32	2.432891	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TLSv1.3	734	Client Hello (SNI=chatgpt.com)
33	2.455945	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	1374	[TCP Duplicate segment] 51204 -> 443 [PSH, ACK] Seq=661 Ack=1 Win=131072 Len=1300 [TCP PDU reassembled in 32]
34	2.492742	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TCP	74	443 -> 51204 [ACK] Seq=1 Ack=1961 Win=73728 Len=0
35	2.494561	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TLSv1.3	1374	Server Hello, Change Cipher Spec
36	2.494561	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TLSv1.3	149	Application Data
37	2.494698	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	74	51204 -> 443 [ACK] Seq=1961 Ack=1376 Win=131072 Len=0
38	2.499354	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TLSv1.3	138	Change Cipher Spec, Application Data
39	2.530670	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TCP	86	[TCP Dup ACK 34#1] 443 -> 51204 [ACK] Seq=1376 Ack=1961 Win=73728 Len=0 SLE=661 SRE=1961
40	2.530670	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TCP	74	443 -> 51204 [ACK] Seq=1376 Ack=2025 Win=73728 Len=0
41	2.530670	2606:4700:83b2:7cbc..	2401:4900:2350:a9a2..	TLSv1.3	602	Application Data, Application Data
42	2.570996	2401:4900:2350:a9a2..	2606:4700:83b2:7cbc..	TCP	74	51204 -> 443 [ACK] Seq=2025 Ack=1904 Win=130560 Len=0
43	2.639316	192.168.253.47	203.23.178.59	TCP	55	51003 -> 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
44	2.826981	203.23.178.59	192.168.253.47	TCP	54	443 -> 51003 [ACK] Seq=0 Ack=2 Win=11 Len=0
45	2.827051	192.168.253.47	203.23.178.59	TCP	54	[TCP Dup ACK 43#1] [TCP ACKed unseen segment] 51003 -> 443 [ACK] Seq=2 Ack=1 Win=512 Len=0
46	2.845620	203.23.178.59	192.168.253.47	TCP	66	[TCP Previous segment not captured] 443 -> 51003 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2

Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...  
> Ethernet II, Src: LiteonTechno\_ee:c1:47 (f8:28:19:ee:c1:47), Dst: 1a:3e:92:d7:82:86 (1a:3e:92:...) [0000 1a 3e 92 d7 82 86 f8 28 19 ee c1 47 86 dd 60 0f ->.....(G-  
[0010 4f e4 00 14 06 3f 24 01 49 00 23 50 a9 a2 a8 1b ->0...?\$. I-#P...  
[0020 05 36 c3 77 4e 14 26 06 47 00 83 b2 7c bc c2 3b ->6 W-& G...;  
[0030 06 b3 5f f2 75 c4 c8 03 01 bb 9e 46 fe 1a 0b b9 ->...u...F...  
[0040 70 7b 50 10 01 fc c6 97 00 00 p(P.....

UDP:

Wireshark packet capture showing UDP traffic. The packet list shows a series of UDP packets from 2401:4900:2350:a9a2:: to 2404:6800:4007:81e::. The packet details pane shows the structure of a UDP packet, including Ethernet II, Internet Protocol Version 6, User Datagram Protocol, and Data (24 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

TCP Packet Analysis

- Three-Way Handshake:
  - SYN (Client to Server)
  - SYN-ACK (Server to Client)
  - ACK (Client to Server)

## Filter Used:

tcp.flags.syn==1 || tcp.flags.ack==1

Wireshark packet capture window showing a list of network packets. The filter 'tcp.flags.syn==1 || tcp.flags.ack==1' is applied. The packet list shows various TCP and TLS packets. The packet details pane shows the structure of a packet, including Ethernet II, Internet Protocol Version 6, and Transmission Control Protocol. The packet bytes pane shows the raw hex and ASCII data.

## Flags and Options:

- **RST:** Connection reset.
- **FIN:** Connection termination.
- **PSH:** Data push without waiting for buffers.
- **Window Size & Sequence Number:** Found in the TCP header.

## Analyzing Packet Flow:

Wireshark packet flow diagram showing the sequence of packets in a TCP connection. The diagram illustrates the flow of data and control packets between two hosts. The flow type is set to 'TCP Flows'. The diagram shows the sequence of packets, including SYN, ACK, FIN, and PSH, and the corresponding sequence numbers and window sizes.

Wireshark - Conversations - Wi-Fi

Conversation Settings

☐ Name resolution

☐ Absolute start time

☒ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☐ IPv6

☐ IPX

☐ JXTA

☐ LTP

☐ MPTCP

☐ NCP

Filter list for specific type

Ethernet - 1

IPv4 - 16

IPv6 - 16

TCP - 51

UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A
192.168.253.47	51221	13.69.239.79	443	34	15 kB	32	34	100.00%	18	7 kB	16
192.168.253.47	51226	13.69.239.79	443	48	17 kB	37	48	100.00%	26	7 kB	22
192.168.253.47	51227	13.69.239.79	443	25	11 kB	38	25	100.00%	12	3 kB	13
192.168.253.47	51214	13.107.5.93	443	26	9 kB	18	26	100.00%	13	2 kB	13
192.168.253.47	51230	13.107.6.158	443	42	15 kB	42	42	100.00%	20	6 kB	22
192.168.253.47	51218	13.107.18.254	443	26	4 kB	29	26	100.00%	13	2 kB	13
192.168.253.47	51213	20.42.73.27	443	83	55 kB	17	83	100.00%	50	49 kB	33
192.168.253.47	51222	20.189.173.25	443	28	11 kB	33	28	100.00%	15	3 kB	13
192.168.253.47	51216	20.190.146.37	443	91	62 kB	27	91	100.00%	47	18 kB	44
192.168.253.47	51232	40.79.189.99	443	98	26 kB	44	98	100.00%	53	15 kB	45
192.168.253.47	51057	48.210.12.84	443	28	2 kB	7	28	100.00%	13	845 bytes	15
192.168.253.47	51206	51.104.15.253	443	51	16 kB	10	51	100.00%	28	7 kB	23
192.168.253.47	50993	91.108.56.114	443	1,204	632 kB	8	1,204	100.00%	516	80 kB	688
192.168.253.47	51233	91.108.56.114	443	39	22 kB	45	39	100.00%	18	2 kB	21
192.168.253.47	51234	91.108.56.114	80	8	746 bytes	46	8	100.00%	5	572 bytes	1
192.168.253.47	51234	91.189.91.98	80	11	891 bytes	35	11	100.00%	7	478 bytes	4
192.168.253.47	51237	185.125.190.96	80	9	783 bytes	49	9	100.00%	5	370 bytes	4
192.168.253.47	51219	204.79.197.222	443	29	10 kB	30	29	100.00%	13	2 kB	16
203.23.178.59	443	192.168.253.47	51003	194	11 kB	3	194	100.00%	97	6 kB	97
212.119.29.131	443	192.168.253.47	51107	94	17 kB	6	94	100.00%	52	5 kB	42
2401:4900:2350:a9a2:a81b:536:c377:4e14	51056	2404:6800:4003:c1a:bc	5228	27	2 kB	0	27	100.00%	13	1 kB	14
2401:4900:2350:a9a2:a81b:536:c377:4e14	51027	2600:1406:2400::173b:af80	443	1	74 bytes	25	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51033	2600:1406:2400::173b:af80	443	1	74 bytes	21	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51034	2600:1406:2400::173b:af80	443	1	74 bytes	24	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51035	2600:1406:2400::173b:af80	443	1	74 bytes	22	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51036	2600:1406:2400::173b:af80	443	1	74 bytes	23	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51037	2600:1406:2400::173b:af80	443	1	74 bytes	19	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51038	2600:1406:2400::173b:af80	443	1	74 bytes	20	2	50.00%	1	74 bytes	0
2401:4900:2350:a9a2:a81b:536:c377:4e14	51220	2600:1406:2400::173b:af80	443	36	12 kB	31	36	100.00%	18	5 kB	18
2401:4900:2350:a9a2:a81b:536:c377:4e14	51209	2603:1016:2402::5	443	28	11 kB	13	28	100.00%	15	2 kB	13
2401:4900:2350:a9a2:a81b:536:c377:4e14	51013	2603:1030:210:f:1	443	4	322 bytes	39	4	100.00%	2	150 bytes	1
2401:4900:2350:a9a2:a81b:536:c377:4e14	51231	2603:1046:1400:1:e	443	33	13 kB	43	33	100.00%	16	4 kB	17

Close

Help

28°

ENG IN

21:57 15-03-2025