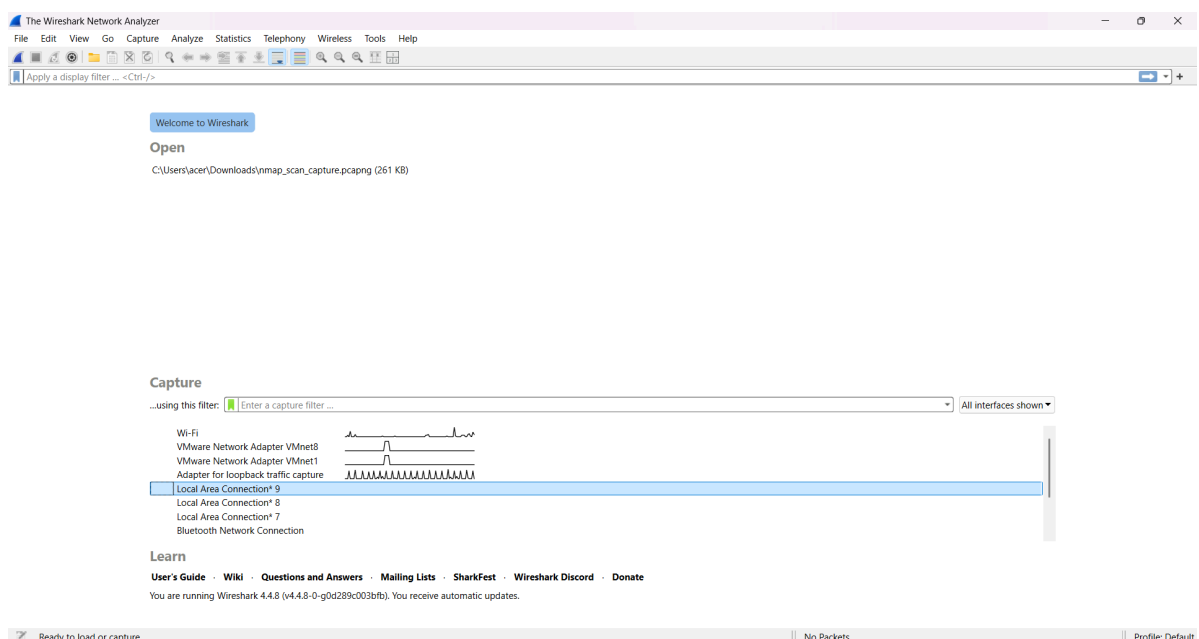


Capture and Analyze Network Traffic Using Wireshark

Step 1 Install Wireshark (and Npcap) on your Windows laptop

1. On your Windows machine, download the **latest stable Windows installer** of Wireshark from the official site (use the Windows 64-bit installer if your OS is 64-bit).
2. Right-click the installer and **Run as administrator**. (Capturing packets requires elevated rights; installing Npcap will ask for admin consent.)
3. During the installer steps:
 - **Allow** installation of **Npcap** (this is the packet capture driver).
 - If prompted, **enable the WinPcap API-compatibility** option (helps compatibility with some tools).
 - Leave default options unless you know you need monitor mode (don't enable advanced 802.11/raw options unless you understand them).
4. Finish installation and **reboot** if the installer asks.
5. After reboot, open Wireshark (you don't need to "Run as admin" every time, but you may if you get permission errors).
6. Verify installation: from the Wireshark menu choose **Help > About Wireshark** (note the version) and then **Capture > Options** you should see a list of network interfaces (Wi-Fi / Ethernet).



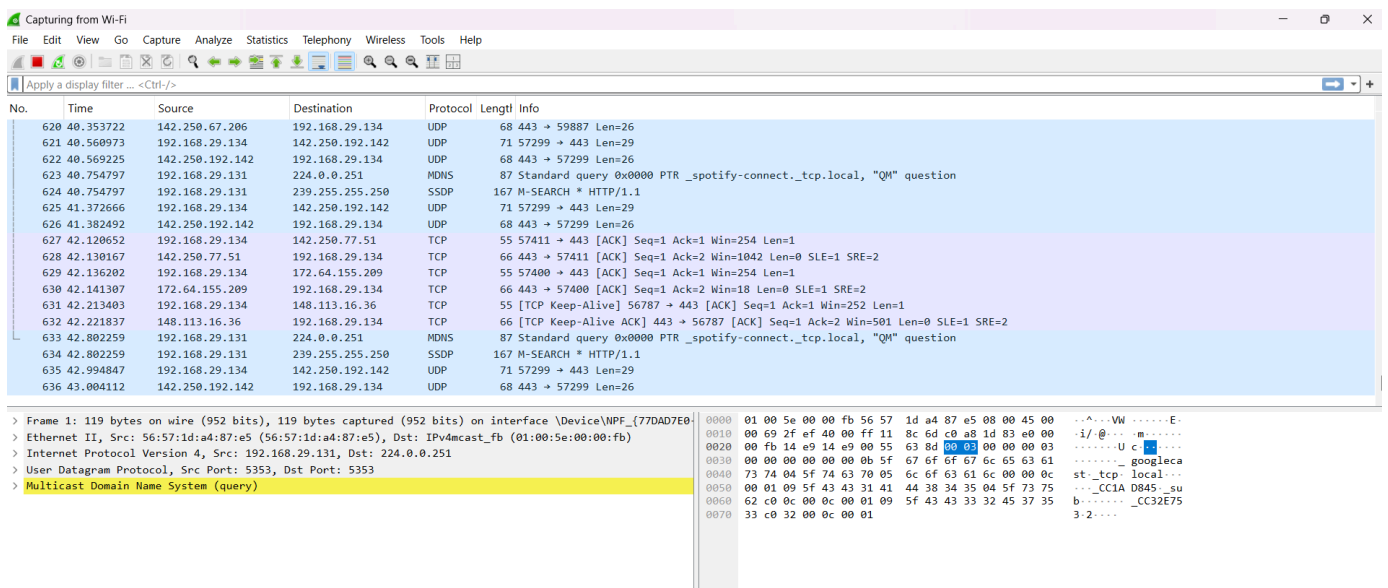
Step 2 Start a Packet Capture

1. Open Wireshark.
2. In the main window, under “**Capture**”, locate your active network interface:
 - If you’re on Wi-Fi, it will usually be named something like Wi-Fi or WLAN.
 - If you’re on Ethernet, it will be Ethernet.
3. **Click once** on your active interface to highlight it.

Capture



4. In the toolbar, click the blue shark fin icon (or press Ctrl + E) to start capturing packets.
5. You will now see packets scrolling in real time. This is your **raw packet capture**.

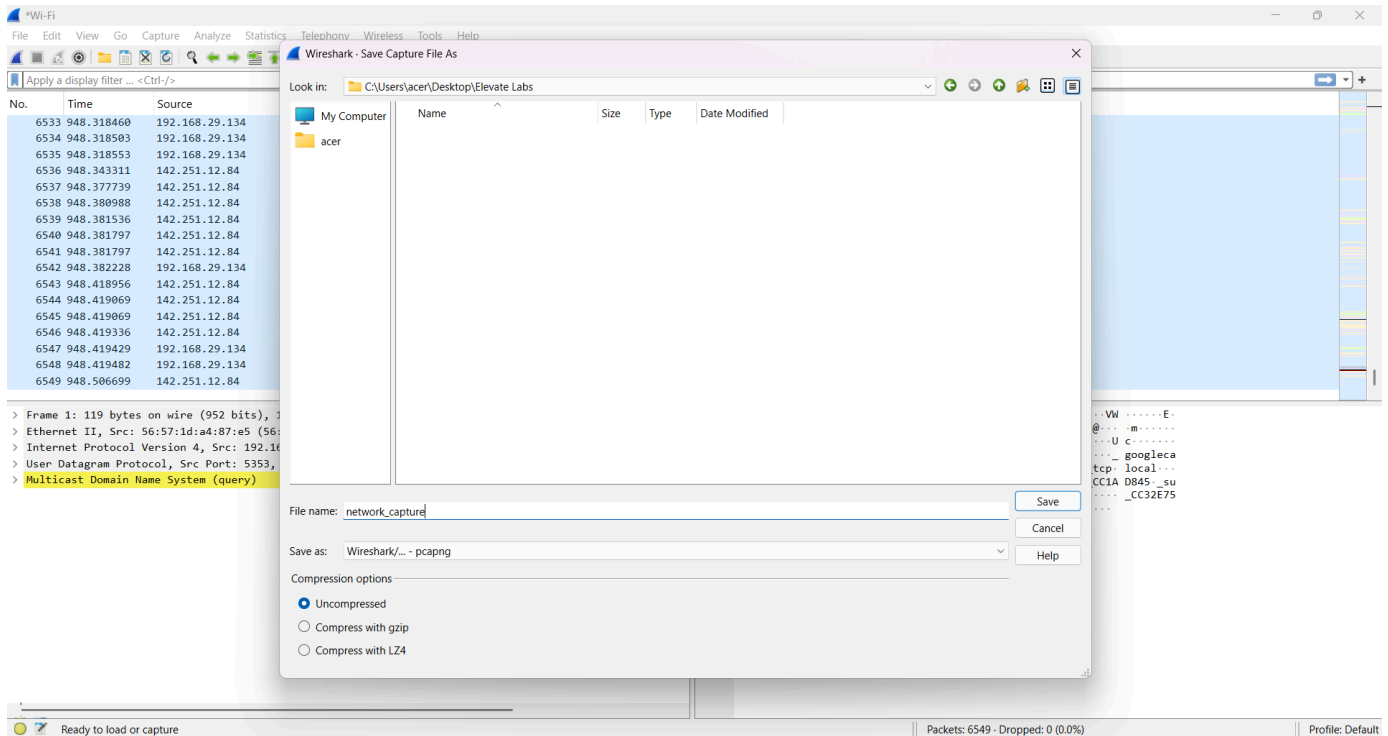


6. Let it run for **about 1–2 minutes** while you perform normal internet activity (e.g., open a few websites, check email). This will ensure you capture different protocols for later analysis.

Step 3 Save and Name the Capture

1. In Wireshark, click the Stop button beside the blue shark fin icon and then click File > Save As (or press Ctrl + S).
2. Choose a folder where you'll keep all internship-related files.
3. Give the file a descriptive name:
Network_capture.pcapng

(“.pcapng” is the default Wireshark format and keeps all capture details.)

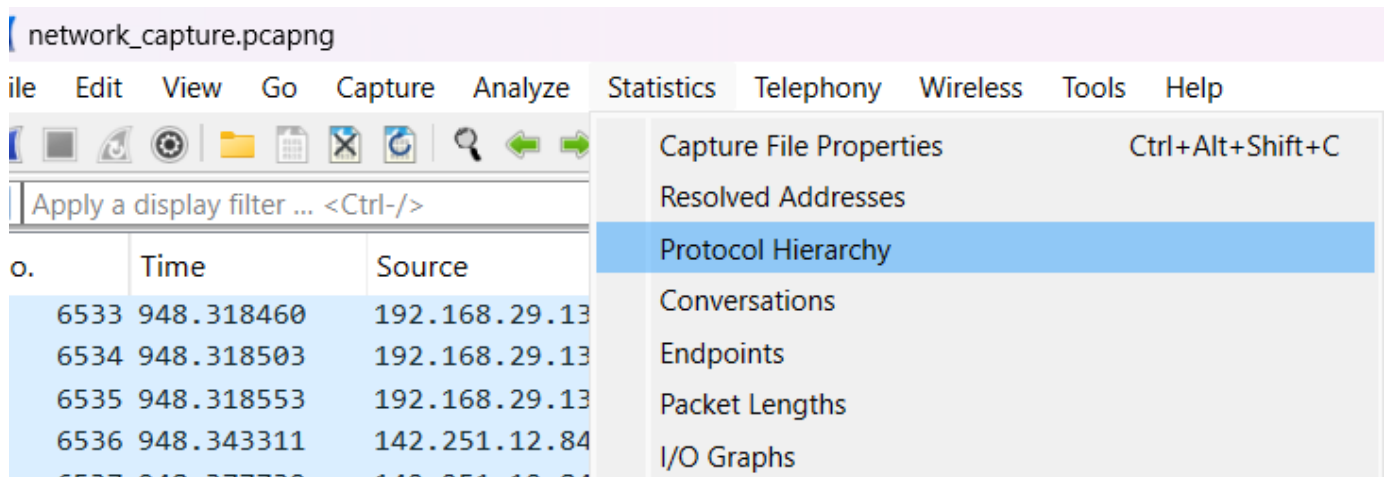


4. Click **Save**.

This saved file will be our **base dataset** for protocol analysis, TCP/IP inspection, troubleshooting, and filtering in the next steps.

Step 4 Protocol Identification & TCP/IP Analysis

1. With your capture file still open in Wireshark, go to **Statistics > Protocol Hierarchy**.



2. This will show you a breakdown of all protocols seen in the capture (e.g., Ethernet, IPv4, TCP, UDP, HTTP, DNS, TLS).

The image shows the 'Wireshark - Protocol Hierarchy Statistics - network_capture.pcapng' window. It displays a detailed breakdown of protocols seen in the capture. The table below represents the data shown in the window.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	6549	100.0	2568047	21 k	0	0	0	6549
Ethernet	100.0	6549	3.6	91766	773	0	0	0	6549
Internet Protocol Version 4	97.4	6376	5.0	128788	1086	0	0	0	6376
User Datagram Protocol	66.7	4365	1.4	34920	294	0	0	0	4365
Simple Service Discovery Protocol	1.2	80	0.4	11254	94	80	11254	94	80
QUIC IETF	46.4	3036	56.2	1442864	12 k	3036	1401582	11 k	3136
NetBIOS Datagram Service	0.0	1	0.0	82	0	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.0	119	1	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.0	33	0	1	33	0	1
Multicast Domain Name System	1.3	88	0.2	5035	42	88	5035	42	88
Echo	0.2	10	0.0	10	0	10	10	0	10
Domain Name System	4.2	272	0.8	20370	171	272	20370	171	272
Data	13.4	878	11.4	292298	2465	878	292298	2465	878
Transmission Control Protocol	25.9	1694	1.4	36552	308	1183	26332	222	1694
Transport Layer Security	6.9	451	18.9	486046	4099	451	389435	3284	461
Data	0.9	60	0.0	60	0	60	60	0	60
Internet Group Management Protocol	4.8	317	0.3	8152	68	317	8152	68	317
Address Resolution Protocol	2.6	173	0.2	4844	40	173	4844	40	173

3. Close the Protocol Hierarchy window.

4. From Protocol Hierarchy the capture of 6,549 packets:

Protocol	% Packets	% Bytes	Notes
Ethernet	100%	3.57%	Link-layer framing for all traffic
IPv4	97.36%	5.01%	Dominant network-layer protocol used
UDP	66.65%	1.36%	Transport protocol used for QUIC, DNS, mDNS
QUIC IETF	46.35%	56.18%	HTTP/3 traffic over UDP (port 443)
TCP	25.87%	1.42%	Small portion of connections still use TCP
TLS	6.88%	18.93%	Encrypted HTTPS over TCP
DNS	4.15%	0.79%	Domain resolution queries/responses
IGMP / ARP	4.84% / 2.64%	0.31% / 0.18%	Multicast group management and address resolution

5. QUIC Packet Layer Analysis

- In the filter bar, type: quic
- Press Enter, now you'll see only QUIC packets.
- Click one QUIC packet to select it.

The screenshot shows the Wireshark network capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The filter bar at the top left shows 'quic'. The packet list pane on the left displays a list of captured packets, with packet 48 selected. The packet details pane on the right shows the structure of packet 48, including the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (QUIC) headers. The packet bytes pane at the bottom shows the raw data of the packet, with the first 1292 bytes highlighted.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
48	8.420381	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=719d832263d9a326, PKN: 1, CRYPTO, PADDING, PING, PADDING, PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, P...
49	8.420661	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=719d832263d9a326, PKN: 2, CRYPTO
50	8.420744	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=719d832263d9a326, PKN: 3, PING, PING, PADDING, PING, CRYPTO, PADDING, PING, PING, CRYPTO, CRYPTO, PING, PADDING, ...
51	8.421110	192.168.29.134	142.250.143.94	QUIC	122	0-RTT, DCID=719d832263d9a326
52	8.422776	192.168.29.134	216.58.200.174	QUIC	1292	Initial, DCID=6a2a740a7e4a66f4, PKN: 1, CRYPTO, PING, PING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PING, PING, CRYPTO, PADDING
53	8.422957	192.168.29.134	216.58.200.174	QUIC	1292	Initial, DCID=6a2a740a7e4a66f4, PKN: 2, CRYPTO, PING, CRYPTO, PING, CRYPTO, CRYPTO, CRYPTO, PING, PING, CRYPTO
54	8.423362	192.168.29.134	216.58.200.174	QUIC	128	0-RTT, DCID=6a2a740a7e4a66f4
55	8.440890	142.250.143.94	192.168.29.134	QUIC	82	Initial, SCID=F19d832263d9a326, PKN: 1, ACK
56	8.441125	142.250.143.94	192.168.29.134	QUIC	82	Initial, SCID=F19d832263d9a326, PKN: 2, ACK
57	8.446926	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=F19d832263d9a326, PKN: 5, PADDING, PING, PING, PADDING, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, PADDING, CRYPTO, P...
58	8.447042	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=F19d832263d9a326, PKN: 6, PADDING, PING, PING, PING, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, CR...
59	8.456388	142.250.143.94	192.168.29.134	QUIC	1292	Initial, SCID=F19d832263d9a326, PKN: 3, ACK, PADDING
60	8.456492	142.250.143.94	192.168.29.134	QUIC	1292	Initial, SCID=F19d832263d9a326, PKN: 4, ACK, PADDING
61	8.456542	142.250.143.94	192.168.29.134	QUIC	1292	Initial, SCID=F19d832263d9a326, PKN: 5, ACK, PADDING
62	8.475805	142.250.143.94	192.168.29.134	QUIC	1292	Initial, SCID=F19d832263d9a326, PKN: 6, ACK, PADDING
63	8.476700	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=F19d832263d9a326, PKN: 8, PADDING, PING, PADDING
64	8.484296	142.250.143.94	192.168.29.134	QUIC	1292	Initial, SCID=F19d832263d9a326, PKN: 7, ACK, PADDING
65	8.516884	142.250.143.94	192.168.29.134	QUIC	1292	Initial, SCID=F19d832263d9a326, PKN: 8, CRYPTO, PADDING

Packet 48 Details:

- Section number: 1
- Interface id: 0 (\Device\NPF_{77DAD7E0-C65B-4C32-9F76-616988A50DC6})
- Interface name: \Device\NPF_{77DAD7E0-C65B-4C32-9F76-616988A50DC6}
- Interface description: Wi-Fi
- Encapsulation type: Ethernet (1)
- Arrival Time: Aug 11, 2025 09:12:35.257956000 India Standard Time
- UTC Arrival Time: Aug 11, 2025 03:42:35.257956000 UTC
- Epoch Arrival Time: 1754883755.257956000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.000616000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 8.420381000 seconds]
- Frame Number: 48
- Frame Length: 1292 bytes (10336 bits)
- Capture Length: 1292 bytes (10336 bits)
- [Frame is marked: False]
- [Frame is ignored: False]

Packet 48 Bytes:

```

0000 a8 da 0c b5 1b 2d 54 14 f3 b4 83 bd 08 00 45 b8 .....T.....E-
0010 04 fe 4c fc 40 00 80 11 00 00 c0 a8 1d 86 8e fa ..L@.....M..K
0020 8f 5e fd 27 01 bb 04 ea 9b 3d c1 00 00 00 01 08 qu"c"&@F...V
0030 71 9d 83 22 63 d9 a3 26 00 40 46 00 e2 09 12 56 g...t...R....
0040 67 de 95 a5 9a 74 8f 87 85 52 f1 98 06 ea dc b6 B&...jm{...
0050 14 42 d7 26 c5 ed 1c 0b 98 5d 6d cb 28 fb af aa .....1)...
0060 a1 88 fc 96 0b 83 ee ed 31 e8 29 5f b1 d1 d1 90 ..hwh...t...d
0070 d7 68 af 72 57 68 18 5f be 74 dc d3 e8 89 64 bd RD...#5v{...
0080 52 44 89 d7 5d 4c b7 23 35 76 5b 87 8a ce e3 c6 RD...-...M..K
0090 4c 44 72 49 a0 3b c6 7b 95 e9 07 a5 57 d2 5f db RD...-...M..K
00a0 20 10 95 ea 81 3a 6f bb 62 6d 9f fb 20 63 e9 87 .....bm...c"
00b0 df 7a 5d 94 9f a5 01 7c d5 ef 8f f6 02 5c 23 df [z]....[.....\w
00c0 40 45 22 7e a4 4a 1e 29 2a 8c f5 bf 64 be ca 67 [E"-D-) *...d.g
00d0 4c b0 92 9e af a7 34 28 4c ec 4f e8 e8 92 a9 a2 .....4(L.O....
00e0 8f 12 85 5a f5 02 f2 89 46 2c e6 51 db 21 e8 20 .....F...Q(1.)
00f0 1f 5d 15 7b 9d a2 53 75 c1 c2 cf 31 4d 83 71 0e [...]...Su...M-q
0100 83 2a ca 77 3b 98 cc 27 d8 da 3a 91 0e 9f de fb *w;...:.....
0110 a0 e2 2e 6f b7 14 2e 84 41 b8 b8 0f 78 e9 27 3c ..p...A...x'k
0120 f9 6d 61 bb 40 cd fe 95 8d fa 13 d2 fb 45 a3 39 ..ma;...:...E-9
0130 68 d0 9a 7b 25 a3 b9 c2 4f d7 a6 84 07 0f a6 f3 ...[X...O.....
0140 af ef 2d 86 46 42 07 d3 f0 c9 33 43 51 2a a9 15 ....FB...3CQ*..
  
```

Frame (1292 bytes) Decrypted QUIC (1144 bytes)

QUIC Packet Breakdown (Layer Analysis)

- **Frame Information:**

- Arrival Time: Aug 11, 2025, 09:12:35 IST
- Frame Length: 1292 bytes (10336 bits)
- Capture Interface: Wi-Fi (Npcap driver)

- **Ethernet II:**

- Source MAC: Intel_b4:83:bd (54:14:f3:b4:83:bd)
- Destination MAC: ServercomPri_b5:1b:2d (a8:da:0c:b5:1b:2d)
- Type: IPv4 (0x0800)

- **Internet Protocol Version 4 (IPv4):**

- Source IP: 192.168.29.134 (local device)
- Destination IP: 142.250.143.94 (Google server)
- TTL: 128
- Total Length: 1278 bytes

- **User Datagram Protocol (UDP):**

- Source Port: 64807
- Destination Port: 443 (HTTPS over QUIC)
- Length: 1258 bytes

- **QUIC IETF:**

- Packet Type: **Initial** (used for connection setup)
- Version: 1 (0x00000001) — HTTP/3 standard version
- Destination Connection ID Length: 8
- Destination Connection ID: 719d832263d9a326
- Contains: CRYPTO, PADDING, possibly handshake messages

Step 5 Filtering & Network Troubleshooting

We'll use filters in Wireshark to isolate and investigate different traffic types from your capture.

1. QUIC Traffic Analysis

Filter Used: quic

network_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

quic

No.	Time	Source	Destination	Protocol	Length	Info
4506	558.228336	192.168.29.134	142.251.42.14	QUIC	1292	Initial, DCID=663dec9e9a21afff, PKN: 1, PING, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PING, PADDI...
4507	558.228495	192.168.29.134	142.251.42.14	QUIC	1292	Initial, DCID=663dec9e9a21afff, PKN: 2, CRYPTO
4508	558.228552	192.168.29.134	142.251.42.14	QUIC	1292	Initial, DCID=663dec9e9a21afff, PKN: 3, PADDING, CRYPTO, PING, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO, PING, PADDING, PING
5273	636.125007	192.168.29.134	142.251.42.227	QUIC	1292	Initial, DCID=6668a489a0c000c0, PKN: 1, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PADDING, PING,...
5274	636.125263	192.168.29.134	142.251.42.227	QUIC	1292	Initial, DCID=6668a489a0c000c0, PKN: 2, CRYPTO
5275	636.125364	192.168.29.134	142.251.42.227	QUIC	1292	Initial, DCID=6668a489a0c000c0, PKN: 3, PING, CRYPTO, PING, CRYPTO, PING, PADDING, CRYPTO, PING, PADDING, PING, PING, PADDING, ...
52	8.422776	192.168.29.134	216.58.200.174	QUIC	1292	Initial, DCID=6a2a740a7e4a66f4, PKN: 1, CRYPTO, PING, PING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PING, PING, CRYPTO, PADDING
53	8.422957	192.168.29.134	216.58.200.174	QUIC	1292	Initial, DCID=6a2a740a7e4a66f4, PKN: 2, CRYPTO, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, PING, CRYPTO
48	8.420381	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=719d832263d9a326, PKN: 1, CRYPTO, PADDING, PING, PADDING, PING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, P...
49	8.420661	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=719d832263d9a326, PKN: 2, CRYPTO
50	8.420744	192.168.29.134	142.250.143.94	QUIC	1292	Initial, DCID=719d832263d9a326, PKN: 3, PING, PING, PADDING, PING, CRYPTO, PADDING, PING, PING, CRYPTO, CRYPTO, PING, PADDING, ...
1441	101.175976	192.168.29.134	142.250.192.174	QUIC	1292	Initial, DCID=71d897d577dfba52, PKN: 1, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDIN...
1442	101.176091	192.168.29.134	142.250.192.174	QUIC	1292	Initial, DCID=71d897d577dfba52, PKN: 2, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, PING
1445	101.208345	192.168.29.134	142.250.192.174	QUIC	1292	Initial, DCID=71d897d577dfba52, PKN: 5, PING, PING, CRYPTO, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, CRYPTO, CRYPTO...
1446	101.208458	192.168.29.134	142.250.192.174	QUIC	1292	Initial, DCID=71d897d577dfba52, PKN: 6, PADDING, PING, PADDING, CRYPTO, PING, CRYPTO, PING, CRYPTO, CRYPTO, CRYPTO, CRY...
1447	101.208482	192.168.29.134	142.250.192.174	QUIC	1292	Initial, DCID=71d897d577dfba52, PKN: 7, PADDING, PING, PADDING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, CRY...
5098	609.251759	192.168.29.134	142.250.182.100	QUIC	1292	Initial, DCID=7a1dad3b9e7fbb4a, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, PING, PING, CRYPTO
5099	609.252122	192.168.29.134	142.250.182.100	QUIC	1292	Initial, DCID=7a1dad3b9e7fbb4a, PKN: 2, PING, PING, CRYPTO, PING, CRYPTO, PING, CRYPTO

▼ Frame 48: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF...
Section number: 1
> Interface id: 0 (\Device\NPF_{77DAD7E0-C65B-4C32-9F76-616988450DC6})
Encapsulation type: Ethernet (1)
Arrival Time: Aug 11, 2025 09:12:35.257956000 India Standard Time
UTC Arrival Time: Aug 11, 2025 03:42:35.257956000 UTC
Epoch Arrival Time: 1754883755.257956000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000616000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 8.420381000 seconds]
Frame Number: 48
Frame Length: 1292 bytes (10336 bits)
Capture Length: 1292 bytes (10336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:udp:quic]
[Coloring Rule Name: UDP]

Frame (1292 bytes) Decrypted QUIC (1144 bytes)

Packets: 6549 · Displayed: 3036 (46.4%) · Dropped: 0 (0.0%) Profile: Default

Observations:

- Total QUIC packets: 3036
- Primary Destination IPs: 49.44.118.8
- Destination Ports: Mostly 443 (HTTPS over QUIC).
- Example Server: 142.250.143.94 (Google)
- Packet Types Seen: Initial, 0-RTT, Handshake, ACK.

2. DNS Traffic Analysis

Filter Used: dns

No.	dns	Source	Destination	Protocol	Length	Info
5383	dnsserver	192.168.29.1	192.168.29.134	DNS	125	Standard query response 0x99a0 HTTPS docs.google.com SOA ns1.google.com
5271	636.119715	192.168.29.1	192.168.29.134	DNS	138	Standard query response 0x9a59 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.251.42.227
5407	661.285717	192.168.29.1	192.168.29.134	DNS	103	Standard query response 0x9d4f A chatgpt.com A 172.64.155.209 A 104.18.32.47
2159	217.097236	192.168.29.1	192.168.29.134	DNS	138	Standard query response 0x9e4d A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.250.143.94
2759	310.901245	192.168.29.1	192.168.29.134	DNS	132	Standard query response 0x9fd7 HTTPS ssl.gstatic.com SOA ns1.google.com
3076	367.415908	192.168.29.1	192.168.29.134	DNS	152	Standard query response 0xa0a3 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
4048	486.505746	192.168.29.1	192.168.29.134	DNS	167	Standard query response 0xa3e0 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.google.com
4268	539.156278	192.168.29.1	192.168.29.134	DNS	358	Standard query response 0xa507 A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com
47	8.419765	192.168.29.1	192.168.29.134	DNS	86	Standard query response 0xa512 A google.com A 216.58.200.174
1558	104.038733	192.168.29.1	192.168.29.134	DNS	246	Standard query response 0xa993 A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com
1686	131.486067	192.168.29.1	192.168.29.134	DNS	172	Standard query response 0xa9a8 HTTPS browser-intake-datadoghq.com SOA ns-1907.awsdns-46.co.uk
1692	131.527610	192.168.29.1	192.168.29.134	DNS	87	Standard query response 0xab8b A bl.nel.goog A 142.250.122.94
5478	671.197763	192.168.29.1	192.168.29.134	DNS	136	Standard query response 0xad7 HTTPS waa-pa.clients6.google.com SOA ns1.google.com
2055	195.003300	192.168.29.1	192.168.29.134	DNS	351	Standard query response 0xaf92 A optimizationguide-pa.googleapis.com A 142.251.42.42 A 142.251.42.10 A 142.250.192.138 A 142.25...
1304	94.214695	192.168.29.1	192.168.29.134	DNS	132	Standard query response 0xb042 HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
4504	558.225983	192.168.29.1	192.168.29.134	DNS	119	Standard query response 0xb2c1 A clients4.google.com CNAME clients1.google.com A 142.251.42.14
6248	861.184835	192.168.29.1	192.168.29.134	DNS	125	Standard query response 0xb322 HTTPS play.google.com SOA ns1.google.com
4461	551.579276	192.168.29.1	192.168.29.134	DNS	87	Standard query response 0xb355 A bl.nel.eoog A 142.251.220.3

Frame 47: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{77DAD7E0-77DAD7E0-77DAD7E0-77DAD7E0} (Device\NPF_{77DAD7E0-77DAD7E0-77DAD7E0-77DAD7E0})

Section number: 1

Interface id: 0 ((Device\NPF_{77DAD7E0-77DAD7E0-77DAD7E0-77DAD7E0}))

Encapsulation type: Ethernet (1)

Arrival Time: Aug 11, 2025 09:12:35.257340000 India Standard Time

UTC Arrival Time: Aug 11, 2025 03:42:35.257340000 UTC

Epoch Arrival Time: 1754883755.257340000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.001839000 seconds]

[Time delta from previous displayed frame: 0.001839000 seconds]

[Time since reference or first frame: 8.419765000 seconds]

Frame Number: 47

Frame Length: 86 bytes (688 bits)

Capture Length: 86 bytes (688 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

0000 54 14 f3 b4 83 bd a8 da 0c b5 1b 2d 08 00 45 00 T.....E..

0010 00 48 69 f9 40 00 40 11 14 d4 c0 a8 1d 01 c0 a8 .H.@@.....

0020 1d 86 00 35 f7 b3 00 34 b0 96 a5 12 81 80 00 01 ...5...4.....

0030 00 01 00 00 00 06 67 6f 6f 67 6c 65 83 63 6fg oogle.co

0040 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 e5 e.....

0050 00 04 d8 3a c8 ae:

Observations:

- Total DNS packets: 272
- Common Queried Domains:
 - google.com
- DNS Response Codes: Mostly No error, no failed lookups found.

3. TCP Error Analysis

Filter Used: tcp.analysis.flags

The image shows a Wireshark network capture analysis. The top pane displays a list of network packets filtered by 'tcp.analysis.flags'. The packets are primarily TCP retransmissions and zero-window events. The bottom pane shows the details of a selected packet (Frame 17), including its section number, interface information, arrival time, and frame length. The packet details indicate it is a TCP segment with a length of 54 bytes (432 bits) and is marked as false for being marked or ignored. The packet bytes are displayed in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
1310	95.231457	172.64.155.209	192.168.29.134	TCP	85	[TCP Retransmission] 443 → 57400 [PSH, ACK] Seq=575 Ack=6497 Win=18 Len=31
16	4.586924	20.44.229.112	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57427 [FIN, ACK] Seq=1 Ack=2 Win=16305 Len=0
1766	131.762493	142.250.67.65	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57444 [FIN, ACK] Seq=11480 Ack=1814 Win=268032 Len=0
1813	147.965703	172.64.150.5	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57464 [FIN, ACK] Seq=4516 Ack=873 Win=131072 Len=0
2887	334.534094	20.44.229.112	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57480 [FIN, ACK] Seq=10752 Ack=7771 Win=4194560 Len=0
5846	736.139672	104.18.32.47	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57494 [FIN, ACK] Seq=2954 Ack=4567 Win=147456 Len=0
4136	490.486976	184.86.248.123	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57514 [FIN, ACK] Seq=4702 Ack=1898 Win=64128 Len=0
4384	546.805888	172.64.155.209	192.168.29.134	TCP	85	[TCP Retransmission] 443 → 57523 [PSH, ACK] Seq=4673 Ack=8655 Win=147456 Len=31
4555	561.758988	172.64.155.209	192.168.29.134	TCP	85	[TCP Retransmission] 443 → 57523 [PSH, ACK] Seq=5076 Ack=15137 Win=147456 Len=31
4633	566.056554	20.207.73.82	192.168.29.134	TCP	513	[TCP Retransmission] 443 → 57526 [PSH, ACK] Seq=12757 Ack=3768 Win=75776 Len=459 [TCP PDU reassembled in 4632]
5703	706.342255	49.44.173.162	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57533 [FIN, ACK] Seq=63334 Ack=1146 Win=31488 Len=0
5700	706.342255	49.44.63.33	192.168.29.134	TCP	54	[TCP Retransmission] 443 → 57537 [FIN, ACK] Seq=735 Ack=977 Win=31488 Len=0
5850	736.448146	192.168.29.134	104.18.32.47	TCP	54	[TCP Retransmission] 57494 → 443 [FIN, ACK] Seq=4567 Ack=2955 Win=64256 Len=0
4625	565.754511	20.207.73.82	192.168.29.134	TCP	481	[TCP Spurious Retransmission] 443 → 57526 [PSH, ACK] Seq=8022 Ack=3223 Win=72704 Len=427 [TCP PDU reassembled in 4622]
17	4.507005	192.168.29.134	20.44.229.112	TCP	54	[TCP ZeroWindow] 57427 → 443 [ACK] Seq=2 Ack=2 Win=0 Len=0
1727	131.762548	192.168.29.134	142.250.67.65	TCP	54	[TCP ZeroWindow] 57444 → 443 [ACK] Seq=1814 Ack=11481 Win=0 Len=0
2880	334.534152	192.168.29.134	20.44.229.112	TCP	54	[TCP ZeroWindow] 57480 → 443 [ACK] Seq=7771 Ack=10753 Win=0 Len=0

Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{77DAD7E0-C65B-4C32-9F76-616988450DC6} Section number: 1 Interface id: 0 (\Device\NPF_{77DAD7E0-C65B-4C32-9F76-616988450DC6}) Interface name: \Device\NPF_{77DAD7E0-C65B-4C32-9F76-616988450DC6} Interface description: Wi-Fi Encapsulation type: Ethernet (1) Arrival Time: Aug 11, 2025 09:12:31.344580000 India Standard Time UTC Arrival Time: Aug 11, 2025 03:42:31.344580000 UTC Epoch Arrival Time: 1754883751.344580000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000001000 seconds] [Time delta from previous displayed frame: 0.000001000 seconds] [Time since reference or first frame: 4.507005000 seconds] Frame Number: 17 Frame Length: 54 bytes (432 bits) Capture Length: 54 bytes (432 bits) [Frame is marked: False] [Frame is ignored: False]

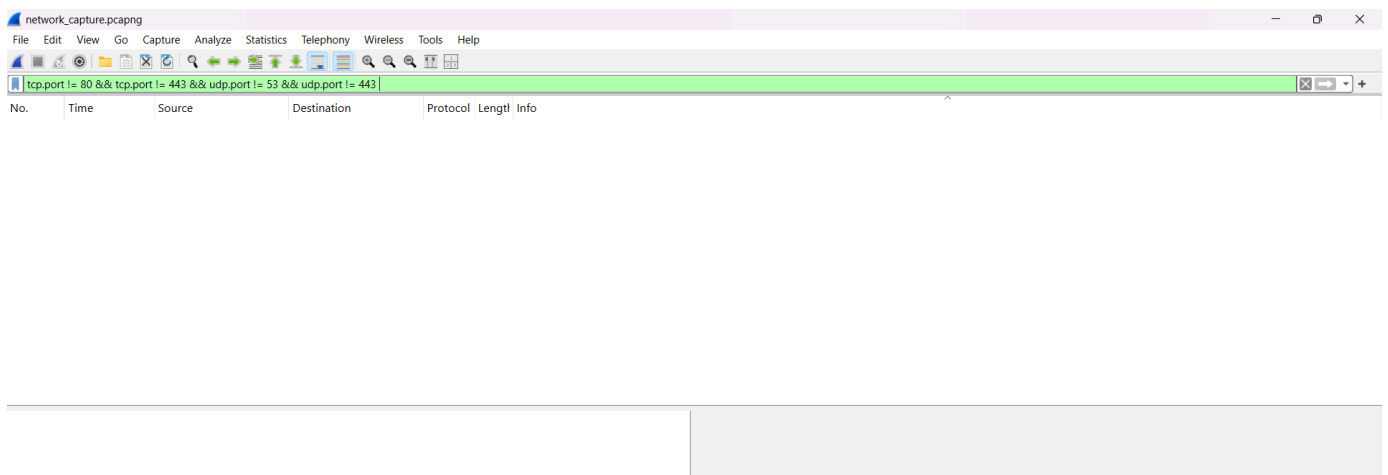
0000 a8 da 0c b5 1b 2d 54 14 f3 b4 83 bd 08 00 45 00T.....E-
0010 00 28 f4 cc 40 00 00 06 00 00 c0 a8 1d 86 14 2c@.....,
0020 e5 70 e0 53 01 bb d1 30 1e 8d b8 4e 66 0e 50 10 pS...0...NF-P-
0030 00 00 d7 e5 00 00

Observations:

- Total TCP anomaly packets: 373
- Error Types Found: Duplicate ACKs, Out-of-order packets.
- Possible Causes: Network congestion, Wi-Fi interference.

4. Non-Standard Port Analysis

Filter Used: tcp.port != 80 && tcp.port != 443 && udp.port != 53 && udp.port != 443



“No traffic detected on non-standard ports. All communications occurred over standard web (443) and DNS (53) ports.”

5. IP-Specific Traffic Analysis

Filter Used: ip.addr == 142.250.143.94

The screenshot shows a Wireshark network capture with a filter applied to traffic from IP 142.250.143.94. The packet list displays several QUIC frames, including Protected Payload (KP0) and frames with DCID values. The packet details pane for frame 2234 shows the following structure:

- Frame 2234: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{77DAD7E4...}
- Ethernet II, Src: ServercomPri_b5:1b:2d (a8:da:0c:b5:1b:2d), Dst: Intel_b4:83:bd (54:14:f3:b4:83:bd)
- Internet Protocol Version 4, Src: 142.250.143.94, Dst: 192.168.29.134
- User Datagram Protocol, Src Port: 443, Dst Port: 62199
- QUIC IETF

The packet bytes pane shows the raw data of the frame, including the QUIC header and payload.

Observations:

- All traffic to/from Google server over QUIC.
- Packet Types: Initial, ACK, CRYPTO frames.
- No retransmissions detected.

Step 6 Outcome & Final Report

The network traffic capture and analysis using Wireshark successfully met the objectives of the internship task.

Key Achievements:

- Installed and configured Wireshark with Npcap for packet capture on Windows.
- Captured **6,549 packets** over a live 1–2 minute session, covering multiple protocols.
- Identified the top protocols by packet volume, including **QUIC (46.35%)**, **UDP (66.65%)**, and **TCP (25.87%)**.
- Performed **layer-by-layer analysis** of QUIC packets to understand connection setup and handshake details.
- Applied targeted filters (quic, dns, tcp.analysis.flags) to isolate protocol-specific traffic and detect anomalies.
- Found minor TCP retransmission and duplicate ACKs, possibly due to network congestion or Wi-Fi interference.
- Confirmed that all communications occurred over standard secure ports (**443 for HTTPS** and **53 for DNS**), with no suspicious non-standard traffic detected.

Conclusion:

The captured data confirms that the monitored system primarily uses secure, encrypted channels (QUIC/HTTPS) with normal DNS resolution patterns. No signs of malicious activity or unusual port usage were found during this analysis. The filtering process proved effective in narrowing down protocol-specific data, highlighting Wireshark's value for both troubleshooting and security monitoring.