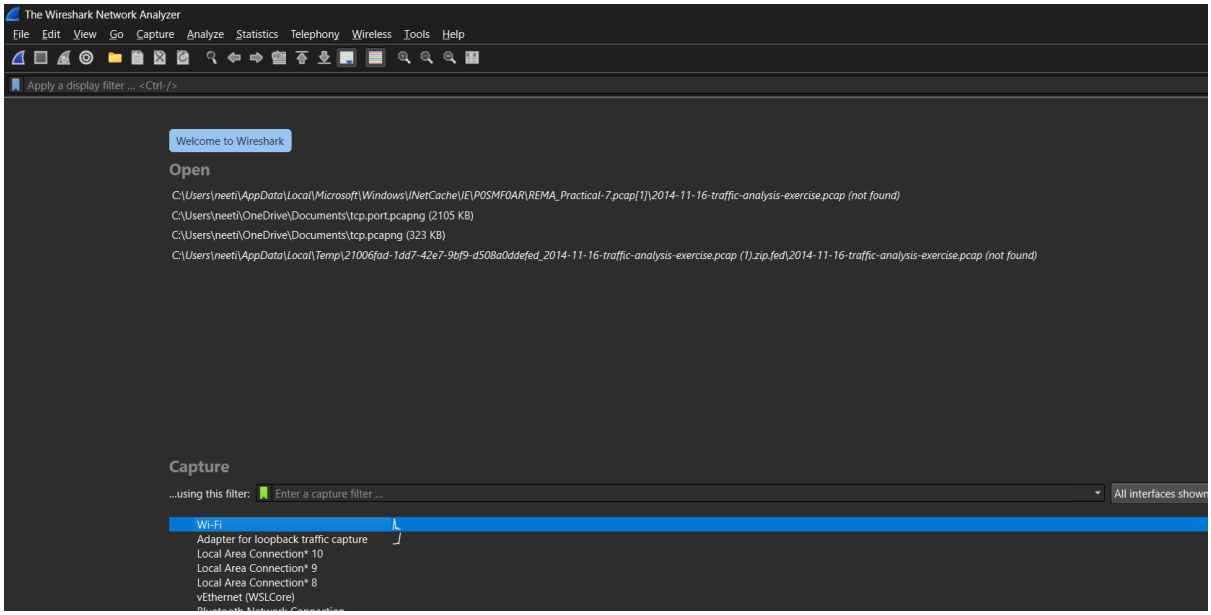
CYBER SECURITY INTERNSHIP

Task 1: Capture and Analyze Network Traffic Using Wireshark**.**

Objective: Capture live network packets and identify basic protocols and traffic types

Tools: Wireshark

1.Open Wireshark and Start capturing on your active network interface.



You'll see a list of available network interfaces (e.g: Ethernet, Wi-Fi).

Identify your active network interface (e.g: one showing live traffic).

Click on the interface to start capturing.

2.Browse a website or ping a server to generate traffic.

Open a web browser and visit a few websites (e.g: facebook.com, google.com)

3. Stop Capturing After About 1 Minute

- Click the red square ("**Stop**") icon in Wireshark.

4. Apply Protocol Filters

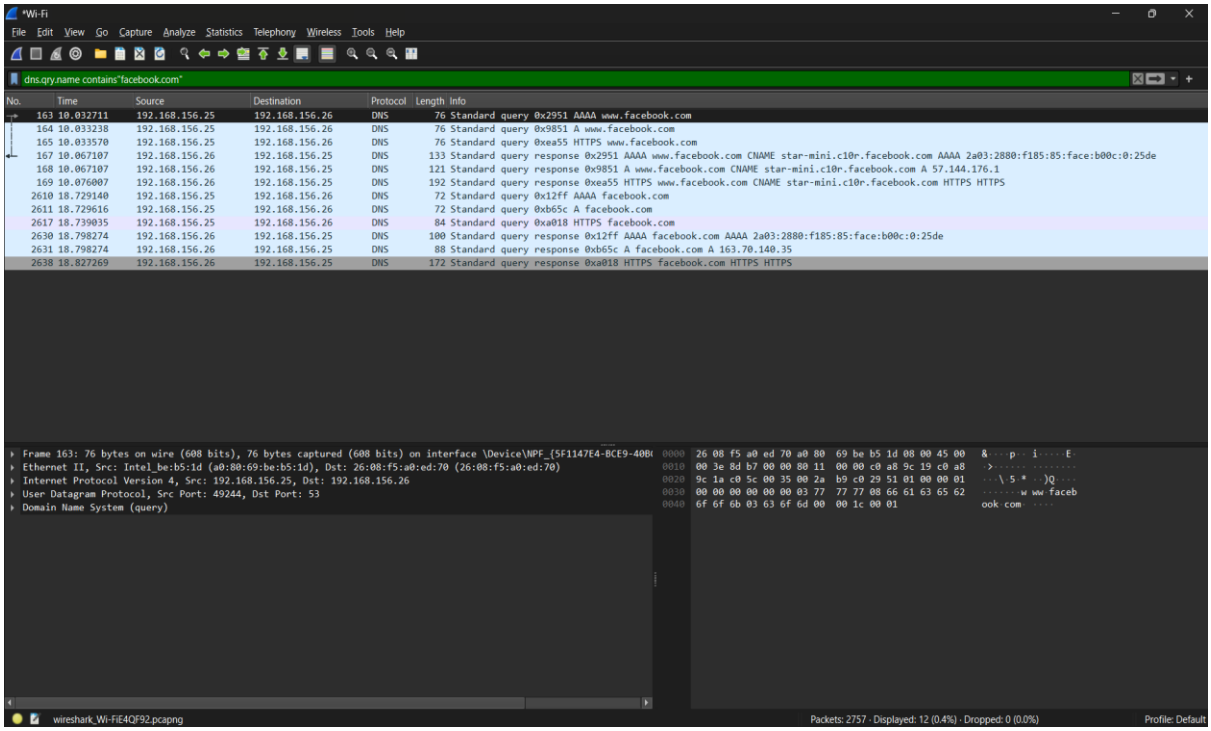
Use the filter bar to examine specific protocols:

- http – shows HTTP requests/responses.

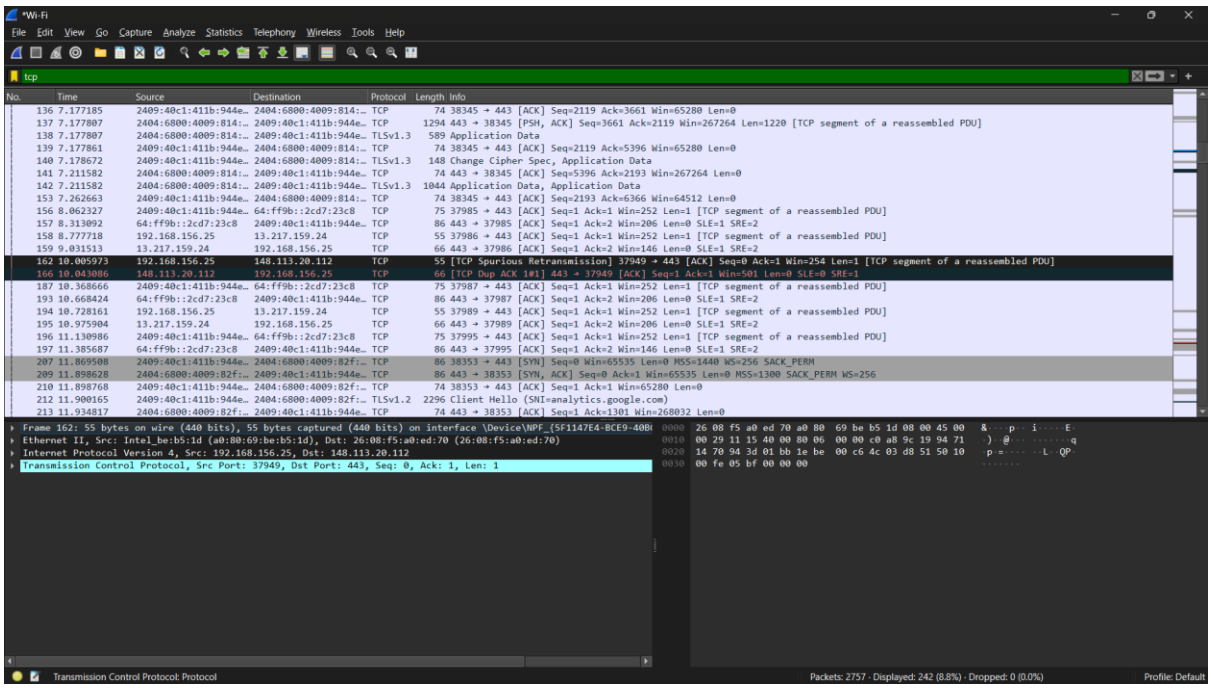
- dns – shows DNS lookups (name resolution).
- icmp – shows ping-related traffic.
- tcp / udp – shows transport-layer activity.

Apply each filter one at a time to analyze

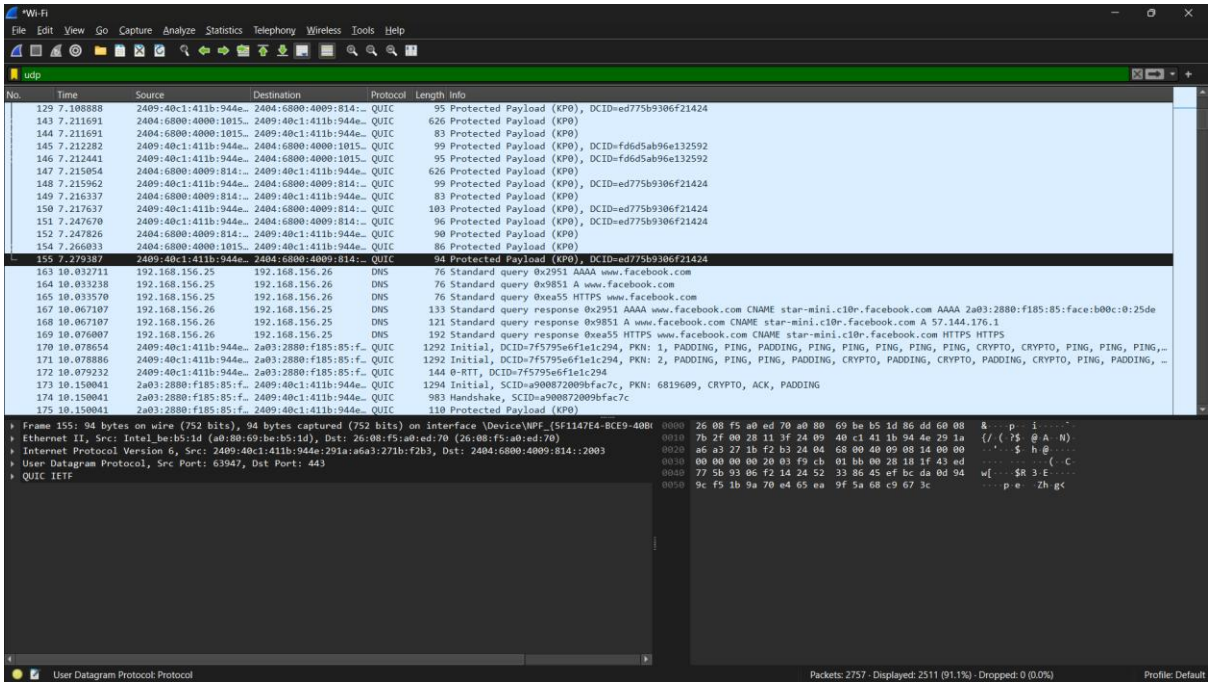
By using DNS:



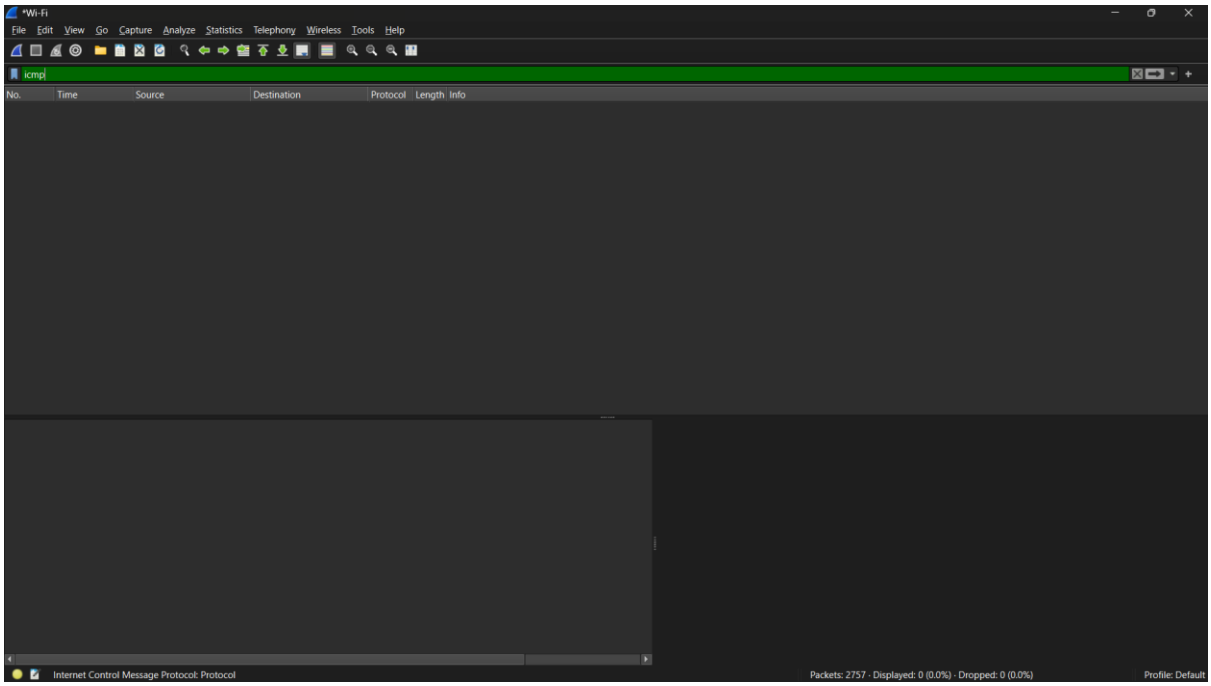
TCP:



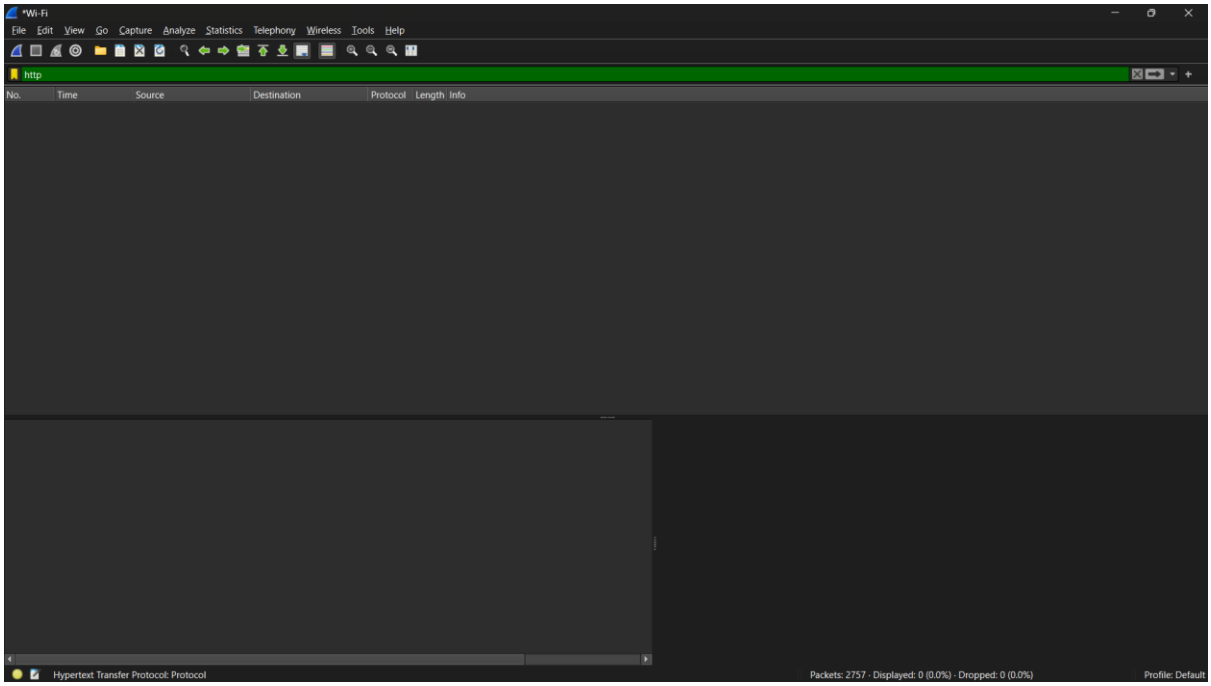
UDP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
129 7.108888 2409:40c1:411b:944e… 2404:6800:4009:814:… QUIC 95 Protected Payload (KP0), DCID=ed775b9306f21424
143 7.211691 2404:6800:4000:1015… 2409:40c1:411b:944e… QUIC 626 Protected Payload (KP0)
144 7.211691 2404:6800:4000:1015… 2409:40c1:411b:944e… QUIC 83 Protected Payload (KP0)
145 7.212282 2409:40c1:411b:944e… 2404:6800:4000:1015… QUIC 99 Protected Payload (KP0), DCID=fd6d5ab96e132592
146 7.212441 2409:40c1:411b:944e… 2404:6800:4000:1015… QUIC 95 Protected Payload (KP0), DCID=fd6d5ab96e132592
147 7.215054 2404:6800:4009:814:… 2409:40c1:411b:944e… QUIC 626 Protected Payload (KP0)
148 7.215962 2409:40c1:411b:944e… 2404:6800:4009:814:… QUIC 99 Protected Payload (KP0), DCID=ed775b9306f21424
149 7.216337 2404:6800:4009:814:… 2409:40c1:411b:944e… QUIC 83 Protected Payload (KP0)
150 7.217637 2409:40c1:411b:944e… 2404:6800:4009:814:… QUIC 103 Protected Payload (KP0), DCID=ed775b9306f21424
151 7.247670 2409:40c1:411b:944e… 2404:6800:4009:814:… QUIC 96 Protected Payload (KP0), DCID=ed775b9306f21424
152 7.247826 2404:6800:4009:814:… 2409:40c1:411b:944e… QUIC 90 Protected Payload (KP0)
154 7.266033 2404:6800:4000:1015… 2409:40c1:411b:944e… QUIC 86 Protected Payload (KP0)
155 7.279387 2409:40c1:411b:944e… 2404:6800:4009:814:… QUIC 94 Protected Payload (KP0), DCID=ed775b9306f21424
163 10.032711 192.168.156.25 192.168.156.26 DNS 76 Standard query 0x2951 AAAA www.facebook.com
164 10.033238 192.168.156.25 192.168.156.26 DNS 76 Standard query 0x9851 A www.facebook.com
165 10.033570 192.168.156.25 192.168.156.26 DNS 76 Standard query 0xea55 HTTPS www.facebook.com
167 10.067107 192.168.156.26 192.168.156.25 DNS 133 Standard query response 0x2951 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f185:85:face:b00c:0:25de
168 10.067107 192.168.156.26 192.168.156.25 DNS 121 Standard query response 0x9851 A www.facebook.com CNAME star-mini.c10r.facebook.com A 57.144.176.1
169 10.076007 192.168.156.26 192.168.156.25 DNS 192 Standard query response 0xea55 HTTPS www.facebook.com CNAME star-mini.c10r.facebook.com HTTPS HTTPS
170 10.078654 2409:40c1:411b:944e… 2a03:2880:f185:85:f… QUIC 1292 Initial, DCID=7f5795e6f1e1c294, PKN: 1, PADDING, PING, PADDING, PING, PING, PING, PING, CRYPTO, CRYPTO, PING, PING, PING,…
171 10.078886 2409:40c1:411b:944e… 2a03:2880:f185:85:f… QUIC 1292 Initial, DCID=7f5795e6f1e1c294, PKN: 2, PADDING, PING, PING, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, PADDING, …
172 10.079232 2409:40c1:411b:944e… 2a03:2880:f185:85:f… QUIC 144 0-RTT, DCID=7f5795e6f1e1c294
173 10.150041 2a03:2880:f185:85:f… 2409:40c1:411b:944e… QUIC 1294 Initial, SCID=a900872009bfac7c, PKN: 6819609, CRYPTO, ACK, PADDING
174 10.150041 2a03:2880:f185:85:f… 2409:40c1:411b:944e… QUIC 983 Handshake, SCID=a900872009bfac7c
175 10.150041 2a03:2880:f185:85:f… 2409:40c1:411b:944e… QUIC 110 Protected Payload (KP0)
Frame 155: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{5F1147E4-BCE9-40B(
Ethernet II, Src: Intel_be:b5:1d (a0:80:69:be:b5:1d), Dst: 26:08:f5:a0:ed:70 (26:08:f5:a0:ed:70)
Internet Protocol Version 6, Src: 2409:40c1:411b:944e:291a:a6a3:271b:f2b3, Dst: 2404:6800:4009:814::2003
User Datagram Protocol, Src Port: 63947, Dst Port: 443
QUIC IETF
0000 26 08 f5 a0 ed 70 a0 80 69 be b5 1d 86 dd 60 08
0010 7b 2f 00 28 11 3f 24 09 40 c1 41 1b 94 4e 29 1a
0020 a6 a3 27 1b f2 b3 24 04 68 00 40 09 08 14 00 00
0030 00 00 00 00 20 03 f9 cb 01 bb 00 28 18 1f 43 ed
0040 77 5b 93 06 f2 14 24 52 33 86 45 ef bc da 0d 94
0050 9c f5 1b 9a 70 e4 65 ea 9f 5a 68 c9 67 3c
User Datagram Protocol: Protocol
Packets: 2757 · Displayed: 2511 (91.1%) · Dropped: 0 (0.0%)
Profile: Default

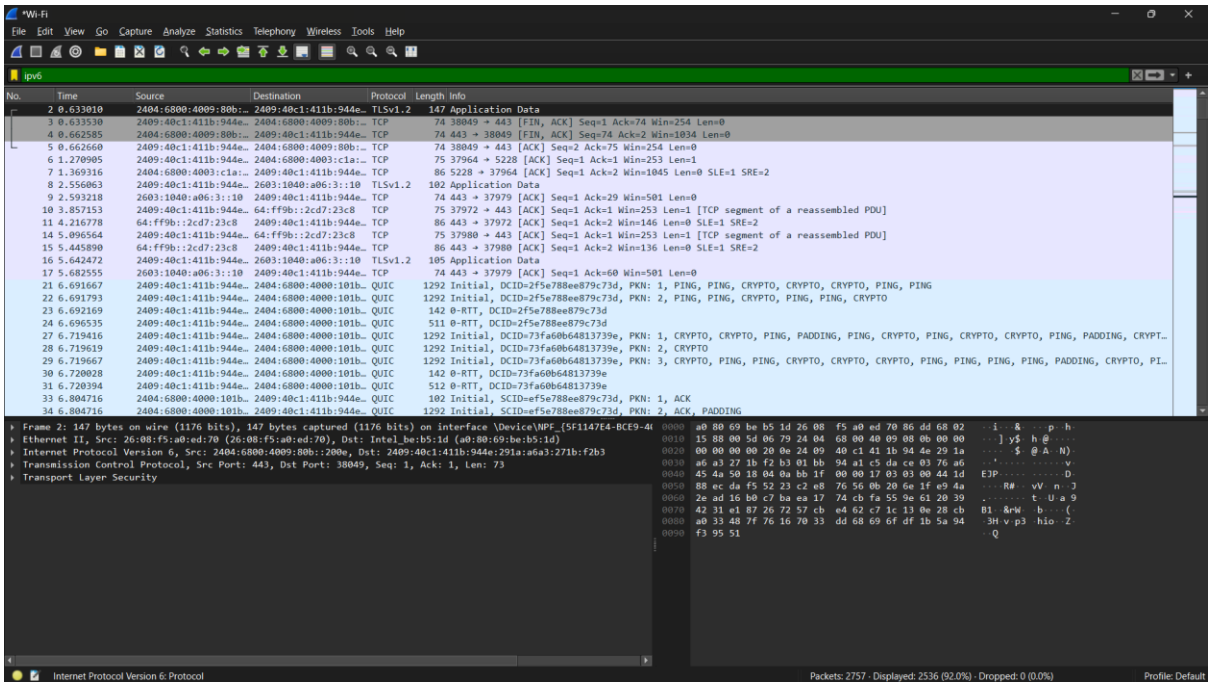
ICMP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
Internet Control Message Protocol: Protocol
Packets: 2757 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

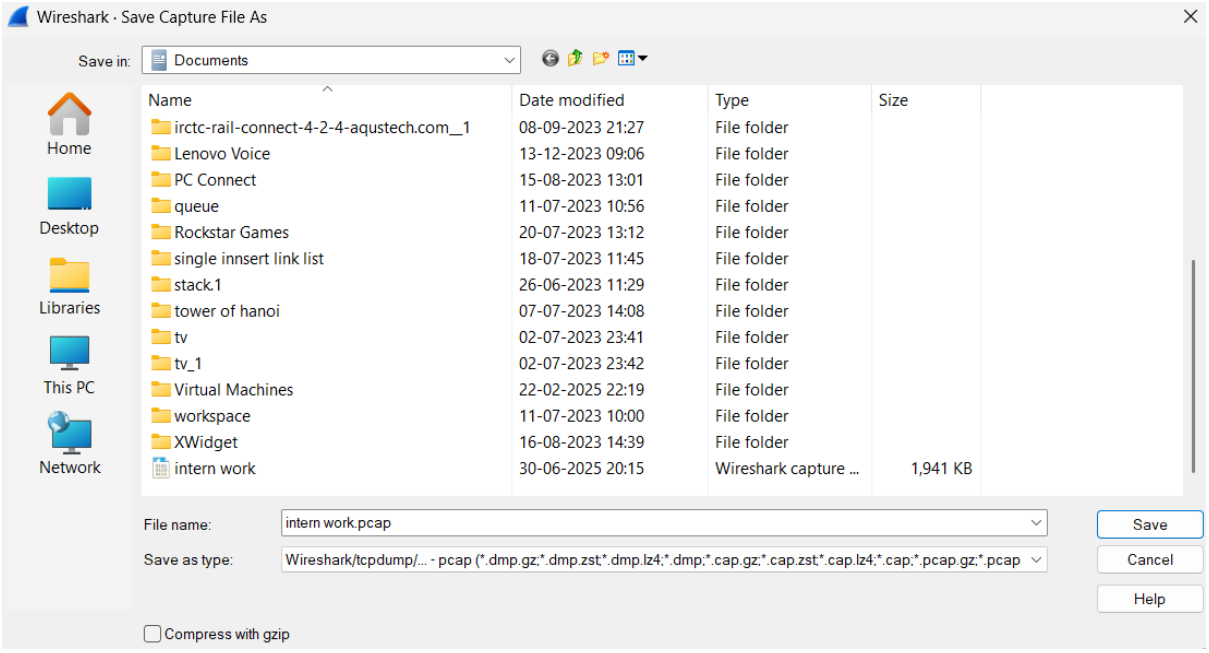
HTTP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
Hypertext Transfer Protocol: Protocol
Packets: 2757 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

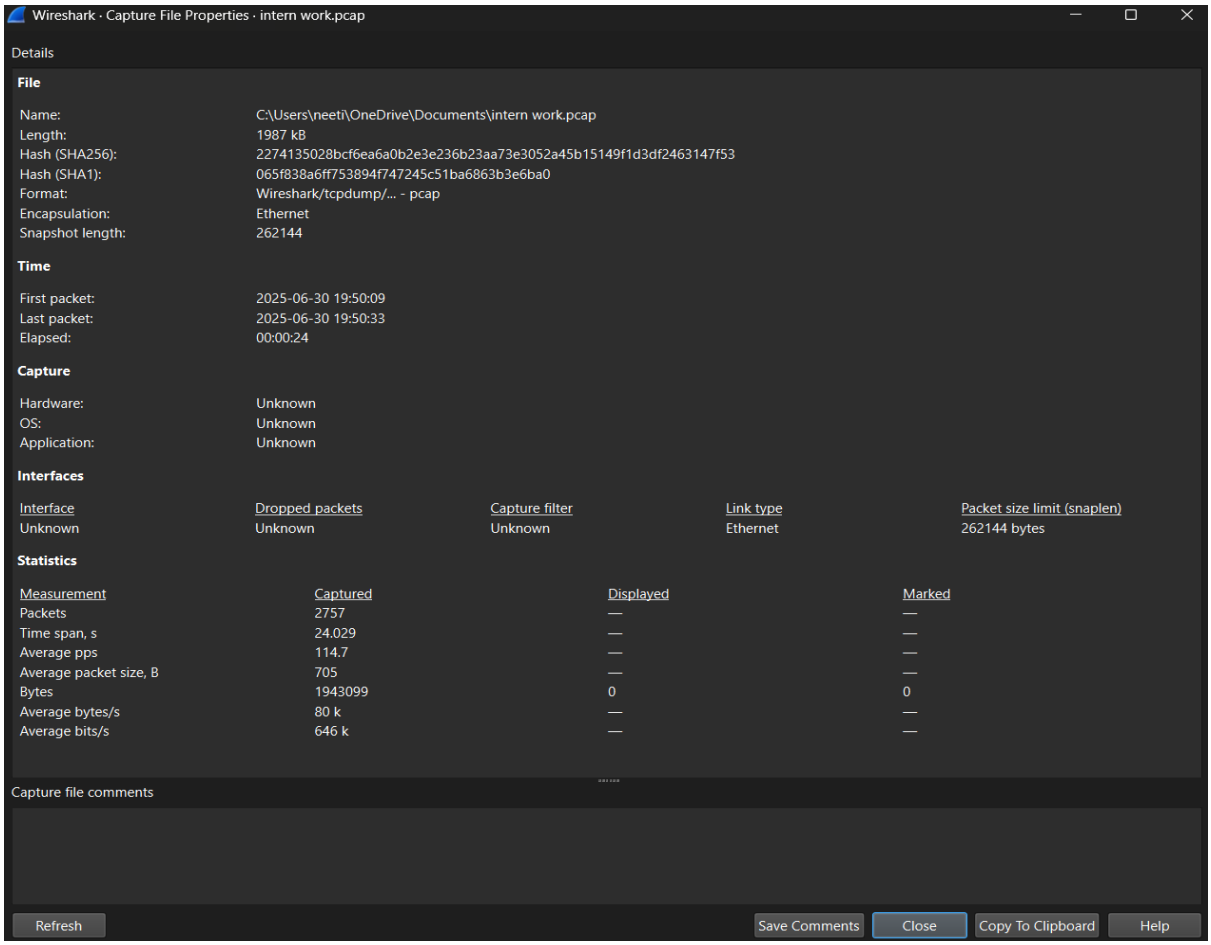
IPV6:

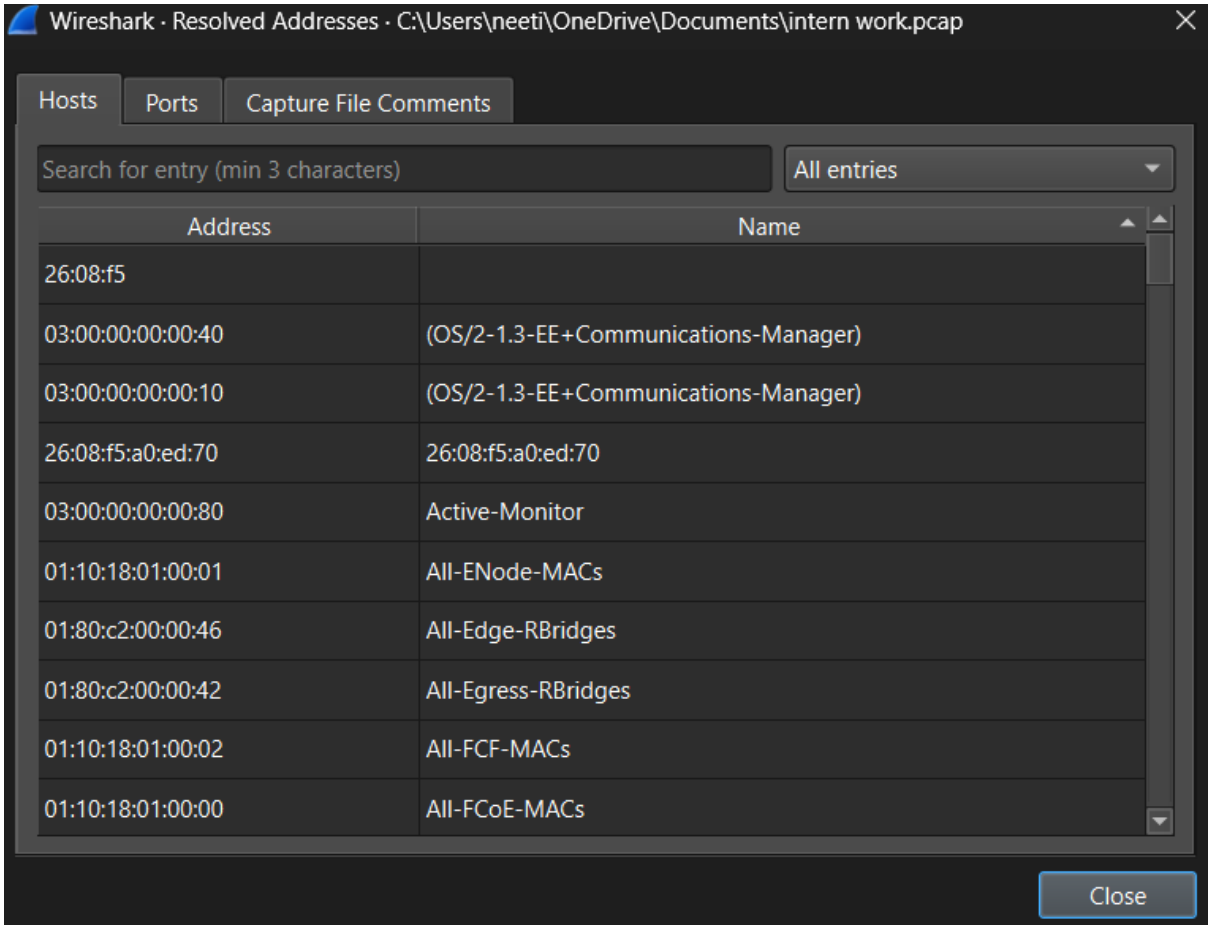

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6
No. Time Source Destination Protocol Length Info
2 0.633010 2404:6800:4009:80b:… 2409:40c1:411b:944e… TLSv1.2 147 Application Data
3 0.633530 2409:40c1:411b:944e… 2404:6800:4009:80b:… TCP 74 38049 → 443 [FIN, ACK] Seq=1 Ack=74 Win=254 Len=0
4 0.662585 2404:6800:4009:80b:… 2409:40c1:411b:944e… TCP 74 443 → 38049 [FIN, ACK] Seq=74 Ack=2 Win=1034 Len=0
5 0.662660 2409:40c1:411b:944e… 2404:6800:4009:80b:… TCP 74 38049 → 443 [ACK] Seq=2 Ack=75 Win=254 Len=0
6 1.270905 2409:40c1:411b:944e… 2404:6800:4003:c1a:… TCP 75 37964 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
7 1.369316 2404:6800:4003:c1a:… 2409:40c1:411b:944e… TCP 86 5228 → 37964 [ACK] Seq=1 Ack=2 Win=1045 Len=0 SLE=1 SRE=2
8 2.556063 2409:40c1:411b:944e… 2603:1040:a06:3::10 TLSv1.2 102 Application Data
9 2.593218 2603:1040:a06:3::10 2409:40c1:411b:944e… TCP 74 443 → 37979 [ACK] Seq=1 Ack=29 Win=501 Len=0
10 3.857153 2409:40c1:411b:944e… 64:ff9b::2cd7:23c8 TCP 75 37972 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
11 4.216778 64:ff9b::2cd7:23c8 2409:40c1:411b:944e… TCP 86 443 → 37972 [ACK] Seq=1 Ack=2 Win=146 Len=0 SLE=1 SRE=2
14 5.096564 2409:40c1:411b:944e… 64:ff9b::2cd7:23c8 TCP 75 37980 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
15 5.445890 64:ff9b::2cd7:23c8 2409:40c1:411b:944e… TCP 86 443 → 37980 [ACK] Seq=1 Ack=2 Win=136 Len=0 SLE=1 SRE=2
16 5.642472 2409:40c1:411b:944e… 2603:1040:a06:3::10 TLSv1.2 105 Application Data
17 5.682555 2603:1040:a06:3::10 2409:40c1:411b:944e… TCP 74 443 → 37979 [ACK] Seq=1 Ack=60 Win=501 Len=0
21 6.691667 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 1292 Initial, DCID=2f5e788ee879c73d, PKN: 1, PING, PING, CRYPTO, CRYPTO, CRYPTO, PING, PING
22 6.691793 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 1292 Initial, DCID=2f5e788ee879c73d, PKN: 2, PING, PING, CRYPTO, PING, PING, CRYPTO
23 6.692169 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 142 0-RTT, DCID=2f5e788ee879c73d
24 6.696535 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 511 0-RTT, DCID=2f5e788ee879c73d
27 6.719416 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 1292 Initial, DCID=73fa60b64813739e, PKN: 1, CRYPTO, CRYPTO, PING, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, PADDING, CRYPT…
28 6.719619 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 1292 Initial, DCID=73fa60b64813739e, PKN: 2, CRYPTO
29 6.719667 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 1292 Initial, DCID=73fa60b64813739e, PKN: 3, CRYPTO, PING, PING, CRYPTO, CRYPTO, CRYPTO, PING, PING, PING, PING, PADDING, CRYPTO, PI…
30 6.720028 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 142 0-RTT, DCID=73fa60b64813739e
31 6.720394 2409:40c1:411b:944e… 2404:6800:4000:101b… QUIC 512 0-RTT, DCID=73fa60b64813739e
33 6.804716 2404:6800:4000:101b… 2409:40c1:411b:944e… QUIC 102 Initial, SCID=ef5e788ee879c73d, PKN: 1, ACK
34 6.804716 2404:6800:4000:101b… 2409:40c1:411b:944e… QUIC 1292 Initial, SCID=ef5e788ee879c73d, PKN: 2, ACK, PADDING
Frame 2: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface \Device\NPF_{5F1147E4-BCE9-4
Ethernet II, Src: 26:08:f5:a0:ed:70 (26:08:f5:a0:ed:70), Dst: Intel_be:b5:1d (a0:80:69:be:b5:1d)
Internet Protocol Version 6, Src: 2404:6800:4009:80b::200e, Dst: 2409:40c1:411b:944e:291a:a6a3:271b:f2b3
Transmission Control Protocol, Src Port: 443, Dst Port: 38049, Seq: 1, Ack: 1, Len: 73
Transport Layer Security
Internet Protocol Version 6: Protocol
Packets: 2757 · Displayed: 2536 (92.0%) · Dropped: 0 (0.0%)
Profile: Default

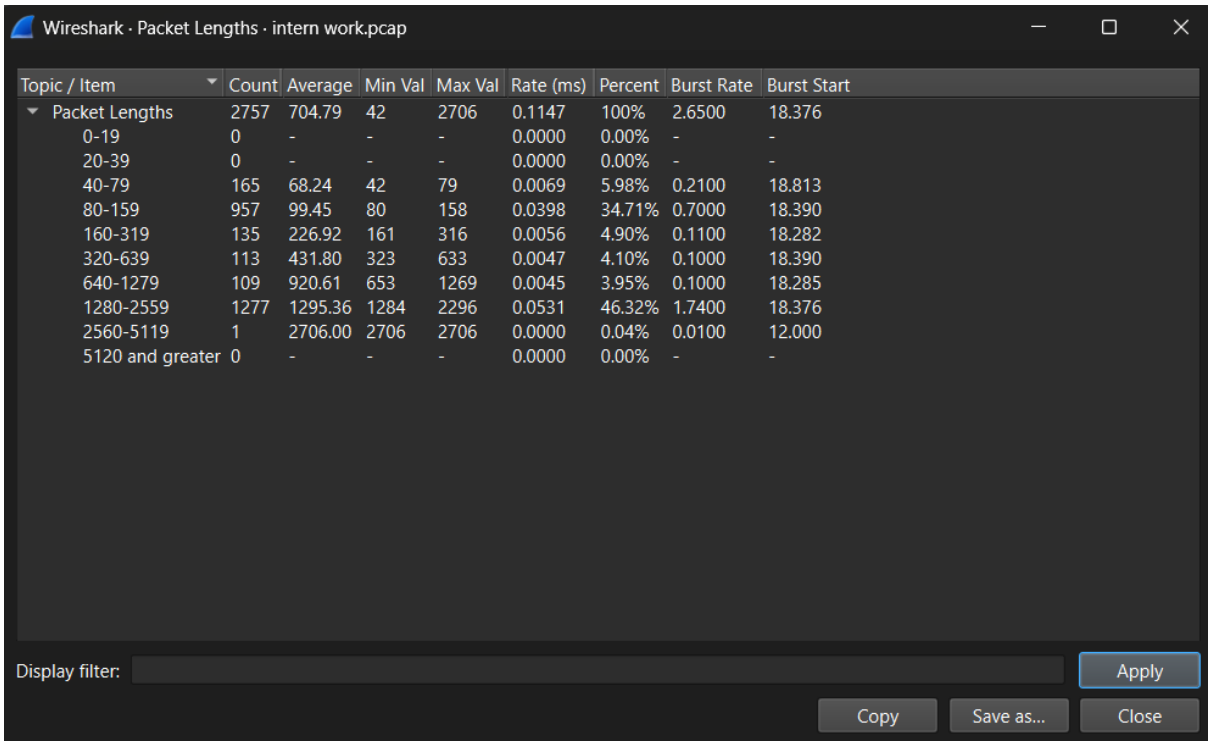
5.Export the capture as a .pcap file.



6.Findings and packets details.




Wireshark · Resolved Addresses · C:\Users\neeti\OneDrive\Documents\intern work.pcap
Hosts
Ports
Capture File Comments
Search for entry (min 3 characters)
All entries
Address
Name
26:08:f5
03:00:00:00:00:40
(OS/2-1.3-EE+Communications-Manager)
03:00:00:00:00:10
(OS/2-1.3-EE+Communications-Manager)
26:08:f5:a0:ed:70
26:08:f5:a0:ed:70
03:00:00:00:00:80
Active-Monitor
01:10:18:01:00:01
All-ENode-MACs
01:80:c2:00:00:46
All-Edge-RBridges
01:80:c2:00:00:42
All-Egress-RBridges
01:10:18:01:00:02
All-FCF-MACs
01:10:18:01:00:00
All-FCoE-MACs
Close


Wireshark · Packet Lengths · intern work.pcap
Topic / Item Count Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Packet Lengths 2757 704.79 42 2706 0.1147 100% 2.6500 18.376
0-19 0 - - - 0.0000 0.00% - -
20-39 0 - - - 0.0000 0.00% - -
40-79 165 68.24 42 79 0.0069 5.98% 0.2100 18.813
80-159 957 99.45 80 158 0.0398 34.71% 0.7000 18.390
160-319 135 226.92 161 316 0.0056 4.90% 0.1100 18.282
320-639 113 431.80 323 633 0.0047 4.10% 0.1000 18.390
640-1279 109 920.61 653 1269 0.0045 3.95% 0.1000 18.285
1280-2559 1277 1295.36 1284 2296 0.0531 46.32% 1.7400 18.376
2560-5119 1 2706.00 2706 2706 0.0000 0.04% 0.0100 12.000
5120 and greater 0 - - - 0.0000 0.00% - -
Display filter:
Apply
Copy
Save as...
Close