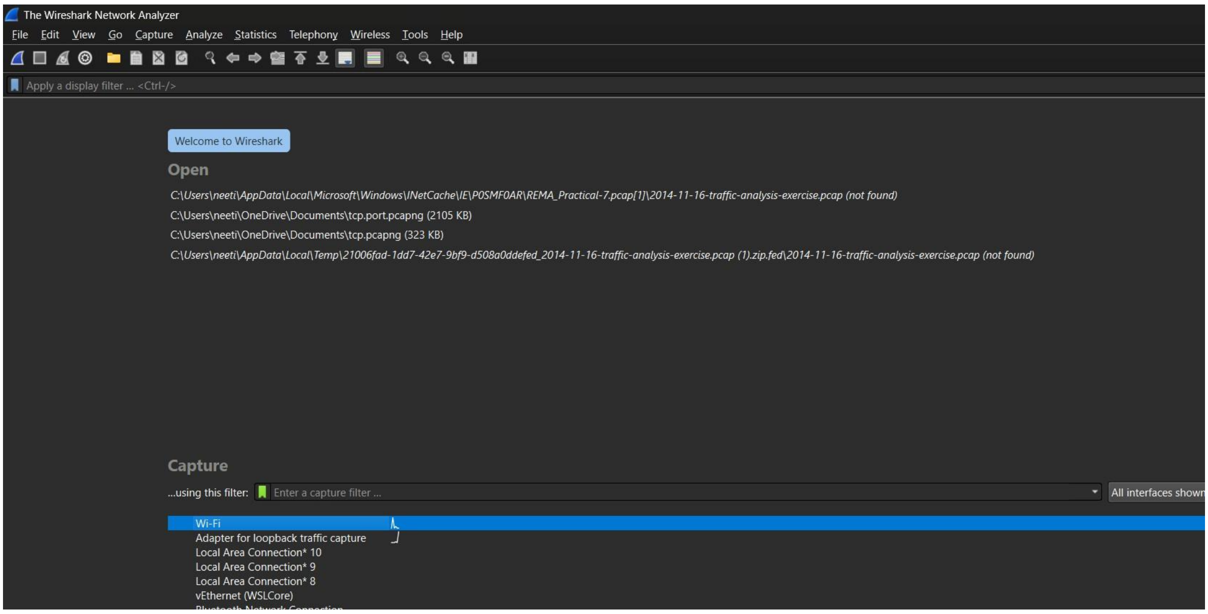
CYBER SECURITY INTERNSHIP

Task 5: 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.



Apply a display filter ... <Ctrl-/>

Open

```
C:\Users\neeti\AppData\Local\Microsoft\Windows\INetCache\IE\P0SMF0AR\REMA_Practical-7.pcap[1]\2014-11-16-traffic-analysis-exercise.pcap (not found)
C:\Users\neeti\OneDrive\Documents\tcp.port.pcapng (2105 KB)
C:\Users\neeti\OneDrive\Documents\tcp.pcapng (323 KB)
C:\Users\neeti\AppData\Local\Temp\21006fad-1dd7-42e7-9bf9-d508a0ddefed_2014-11-16-traffic-analysis-exercise.pcap (1).zip.fed\2014-11-16-traffic-analysis-exercise.pcap (not found)
```

Capture

...using this filter: Enter a capture filter ...

```
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
vEthernet (WSLCore)
Bluetooth Network Connection
```

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

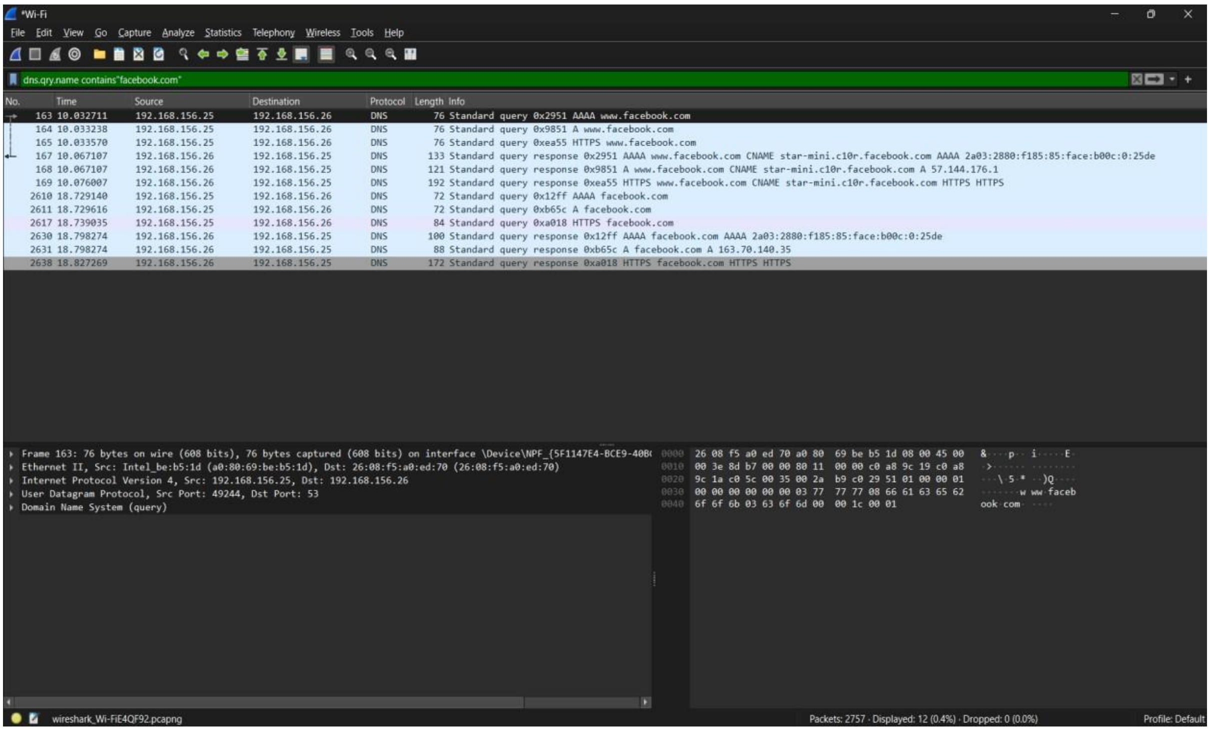
Use the filter bar to examine specific protocols:

- 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:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns.qry.name contains"facebook.com"
```

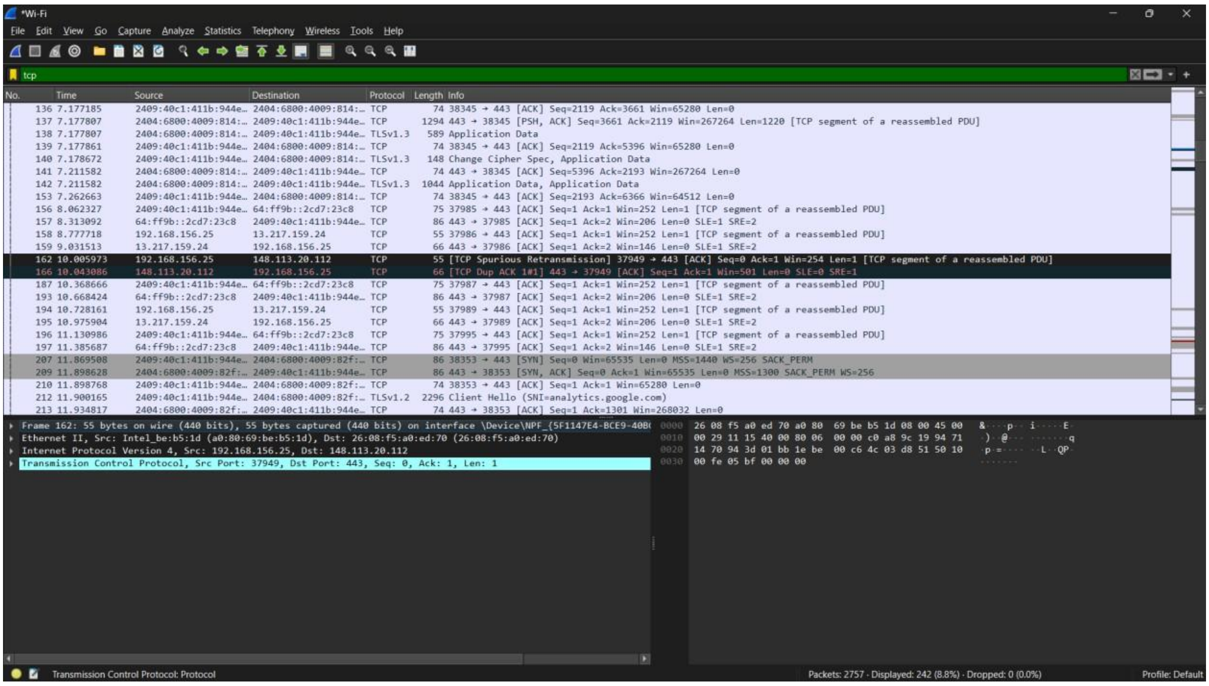
```
No.   Time       Source          Destination     Protocol Length Info
  163 10.032711  192.168.156.25  192.168.156.26  DNS       76 Standard query 0x2951 AAAA www.facebook.com
  164 10.033238  192.168.156.25  192.168.156.26  DNS       76 Standard query 0x9851 A www.facebook.com
  165 10.033570  192.168.156.25  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
 2610 18.729140  192.168.156.25  192.168.156.26  DNS       72 Standard query 0x12ff AAAA facebook.com
 2611 18.729616  192.168.156.25  192.168.156.26  DNS       72 Standard query 0xb65c A facebook.com
 2617 18.739035  192.168.156.25  192.168.156.26  DNS       84 Standard query 0xa018 HTTPS facebook.com
 2630 18.798274  192.168.156.26  192.168.156.25  DNS      100 Standard query response 0x12ff AAAA facebook.com AAAA 2a03:2880:f185:85:face:b00c:0:25de
 2631 18.798274  192.168.156.26  192.168.156.25  DNS       88 Standard query response 0xb65c A facebook.com A 163.70.140.35
 2638 18.827269  192.168.156.26  192.168.156.25  DNS      172 Standard query response 0xa018 HTTPS facebook.com HTTPS HTTPS
```

```
▸ Frame 163: 76 bytes on wire (608 bits), 76 bytes captured (608 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 4, Src: 192.168.156.25, Dst: 192.168.156.26
▸ User Datagram Protocol, Src Port: 49244, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  26 08 f5 a0 ed 70 a0 80  69 be b5 1d 08 00 45 00   &···p··i·····E·
0010  00 3e 8d b7 00 00 80 11  00 00 c0 a8 9c 19 c0 a8   ·>··············
0020  9c 1a c0 5c 00 35 00 2a  b9 c0 29 51 01 00 00 01   ···\·5·*··)Q····
0030  00 00 00 00 00 00 03 77  77 77 08 66 61 63 65 62   ·······w ww·faceb
0040  6f 6f 6b 03 63 6f 6d 00  00 1c 00 01               ook·com·····
```

wireshark_Wi-FiE4QF92.pcapng   Packets: 2757 · Displayed: 12 (0.4%) · Dropped: 0 (0.0%)   Profile: Default

TCP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

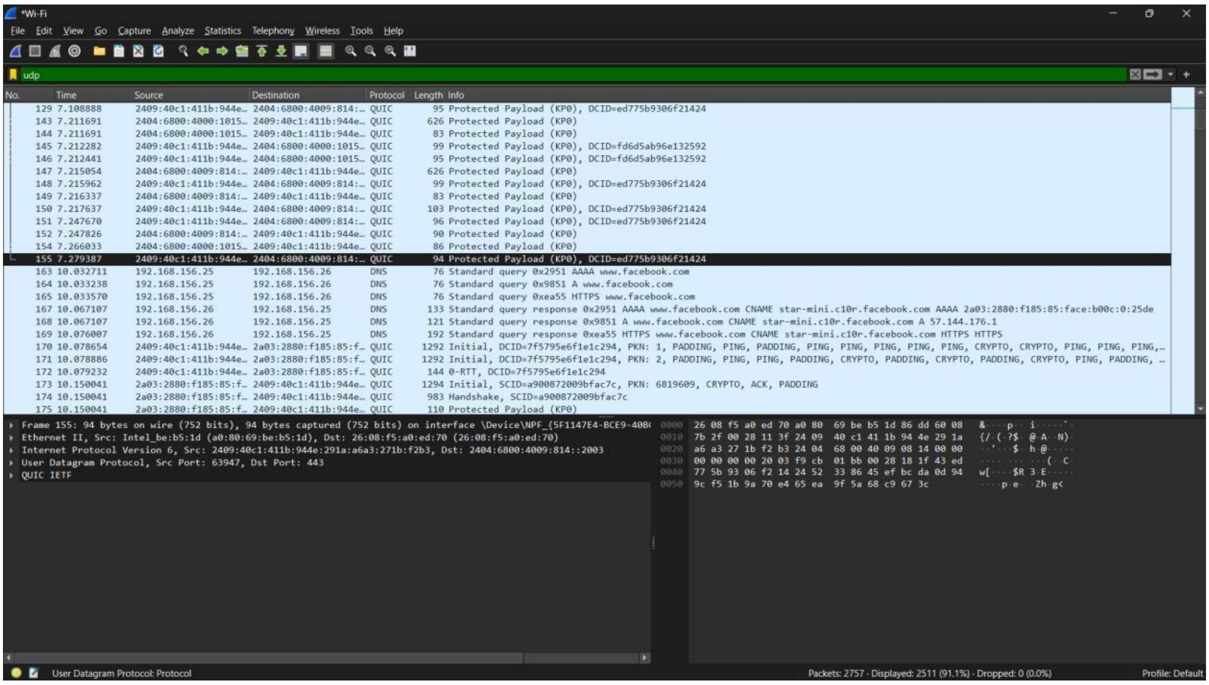
```
No.  Time       Source                Destination           Protocol Length Info
 136 7.177185   2409:40c1:411b:944e…  2404:6800:4009:814:…  TCP        74 38345 → 443 [ACK] Seq=2119 Ack=3661 Win=65280 Len=0
 137 7.177807   2404:6800:4009:814:…  2409:40c1:411b:944e…  TCP      1294 443 → 38345 [PSH, ACK] Seq=3661 Ack=2119 Win=267264 Len=1220 [TCP segment of a reassembled PDU]
 138 7.177807   2404:6800:4009:814:…  2409:40c1:411b:944e…  TLSv1.3   589 Application Data
 139 7.177861   2409:40c1:411b:944e…  2404:6800:4009:814:…  TCP        74 38345 → 443 [ACK] Seq=2119 Ack=5396 Win=65280 Len=0
 140 7.178672   2409:40c1:411b:944e…  2404:6800:4009:814:…  TLSv1.3   148 Change Cipher Spec, Application Data
 141 7.211582   2404:6800:4009:814:…  2409:40c1:411b:944e…  TCP        74 443 → 38345 [ACK] Seq=5396 Ack=2193 Win=267264 Len=0
 142 7.211582   2404:6800:4009:814:…  2409:40c1:411b:944e…  TLSv1.3  1044 Application Data, Application Data
 153 7.262663   2409:40c1:411b:944e…  2404:6800:4009:814:…  TCP        74 38345 → 443 [ACK] Seq=2193 Ack=6366 Win=64512 Len=0
 156 8.062327   2409:40c1:411b:944e…  64:ff9b::2cd7:23c8    TCP        75 37985 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
 157 8.313092   64:ff9b::2cd7:23c8    2409:40c1:411b:944e…  TCP        86 443 → 37985 [ACK] Seq=1 Ack=2 Win=206 Len=0 SLE=1 SRE=2
 158 8.777718   192.168.156.25        13.217.159.24         TCP        55 37986 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
 159 9.031513   13.217.159.24         192.168.156.25        TCP        66 443 → 37986 [ACK] Seq=1 Ack=2 Win=146 Len=0 SLE=1 SRE=2
 162 10.005973  192.168.156.25        148.113.20.112        TCP        55 [TCP Spurious Retransmission] 37949 → 443 [ACK] Seq=0 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
 166 10.043086  148.113.20.112        192.168.156.25        TCP        66 [TCP Dup ACK 1#1] 443 → 37949 [ACK] Seq=1 Ack=1 Win=501 Len=0 SLE=0 SRE=1
 187 10.368666  2409:40c1:411b:944e…  64:ff9b::2cd7:23c8    TCP        75 37987 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
 193 10.668424  64:ff9b::2cd7:23c8    2409:40c1:411b:944e…  TCP        86 443 → 37987 [ACK] Seq=1 Ack=2 Win=206 Len=0 SLE=1 SRE=2
 194 10.728161  192.168.156.25        13.217.159.24         TCP        55 37989 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
 195 10.975904  13.217.159.24         192.168.156.25        TCP        66 443 → 37989 [ACK] Seq=1 Ack=2 Win=206 Len=0 SLE=1 SRE=2
 196 11.130986  2409:40c1:411b:944e…  64:ff9b::2cd7:23c8    TCP        75 37995 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
 197 11.385687  64:ff9b::2cd7:23c8    2409:40c1:411b:944e…  TCP        86 443 → 37995 [ACK] Seq=1 Ack=2 Win=146 Len=0 SLE=1 SRE=2
 207 11.869508  2409:40c1:411b:944e…  2404:6800:4009:82f:…  TCP        86 38353 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 209 11.898628  2404:6800:4009:82f:…  2409:40c1:411b:944e…  TCP        86 443 → 38353 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM WS=256
 210 11.898768  2409:40c1:411b:944e…  2404:6800:4009:82f:…  TCP        74 38353 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 212 11.900165  2409:40c1:411b:944e…  2404:6800:4009:82f:…  TLSv1.2  2296 Client Hello (SNI=analytics.google.com)
 213 11.934817  2404:6800:4009:82f:…  2409:40c1:411b:944e…  TCP        74 443 → 38353 [ACK] Seq=1 Ack=1301 Win=268032 Len=0
```

```
▸ Frame 162: 55 bytes on wire (440 bits), 55 bytes captured (440 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 4, Src: 192.168.156.25, Dst: 148.113.20.112
▸ Transmission Control Protocol, Src Port: 37949, Dst Port: 443, Seq: 0, Ack: 1, Len: 1
```

```
0000  26 08 f5 a0 ed 70 a0 80  69 be b5 1d 08 00 45 00   &···p··i·····E·
0010  00 29 11 15 40 00 80 06  00 00 c0 a8 9c 19 94 71   ·)··@··········q
0020  14 70 94 3d 01 bb 1e be  00 c6 4c 03 d8 51 50 10   ·p·=······L··QP·
0030  00 fe 05 bf 00 00 00                               ·······
```

Transmission Control Protocol: Protocol   Packets: 2757 · Displayed: 242 (8.8%) · Dropped: 0 (0.0%)   Profile: Default

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, 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
```

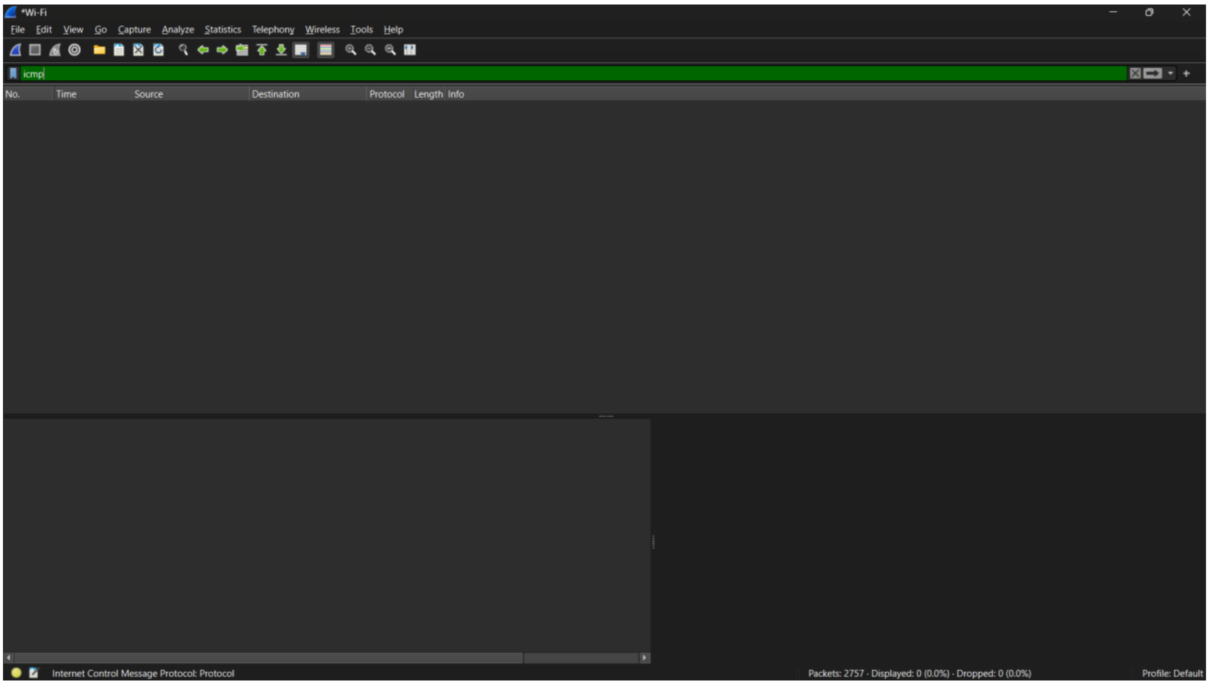
```
0000  26 08 f5 a0 ed 70 a0 80  69 be b5 1d 86 dd 60 08   &····p·· i·····`·
0010  7b 2f 00 28 11 3f 24 09  40 c1 41 1b 94 4e 29 1a   {/·(·?$· @·A··N)·
0020  a6 a3 27 1b f2 b3 24 04  68 00 40 09 08 14 00 00   ··'···$· h·@·····
0030  00 00 00 00 20 03 f9 cb  01 bb 00 28 18 1f 43 ed   ···· ··· ···(··C·
0040  77 5b 93 06 f2 14 24 52  33 86 45 ef bc da 0d 94   w[····$R 3·E·····
0050  9c f5 1b 9a 70 e4 65 ea  9f 5a 68 c9 67 3c         ····p·e· ·Zh·g<
```

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

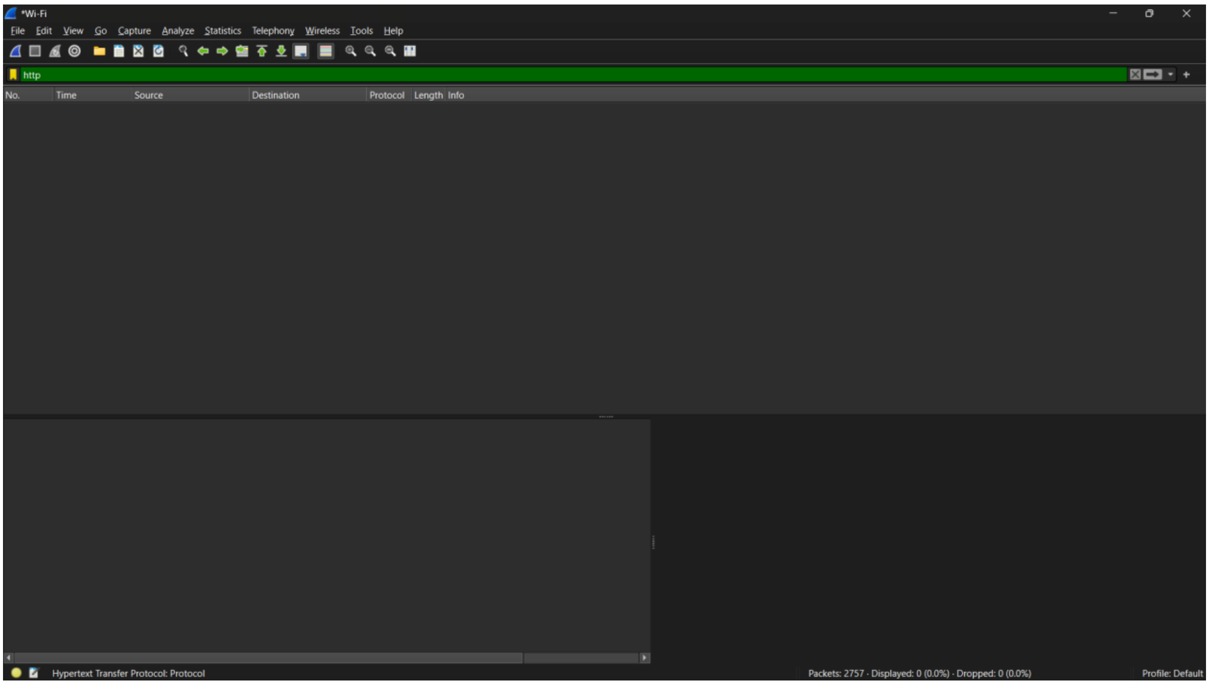
```
No.   Time       Source                Destination           Protocol Length Info
```

Internet Control Message Protocol: Protocol

Packets: 2757 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

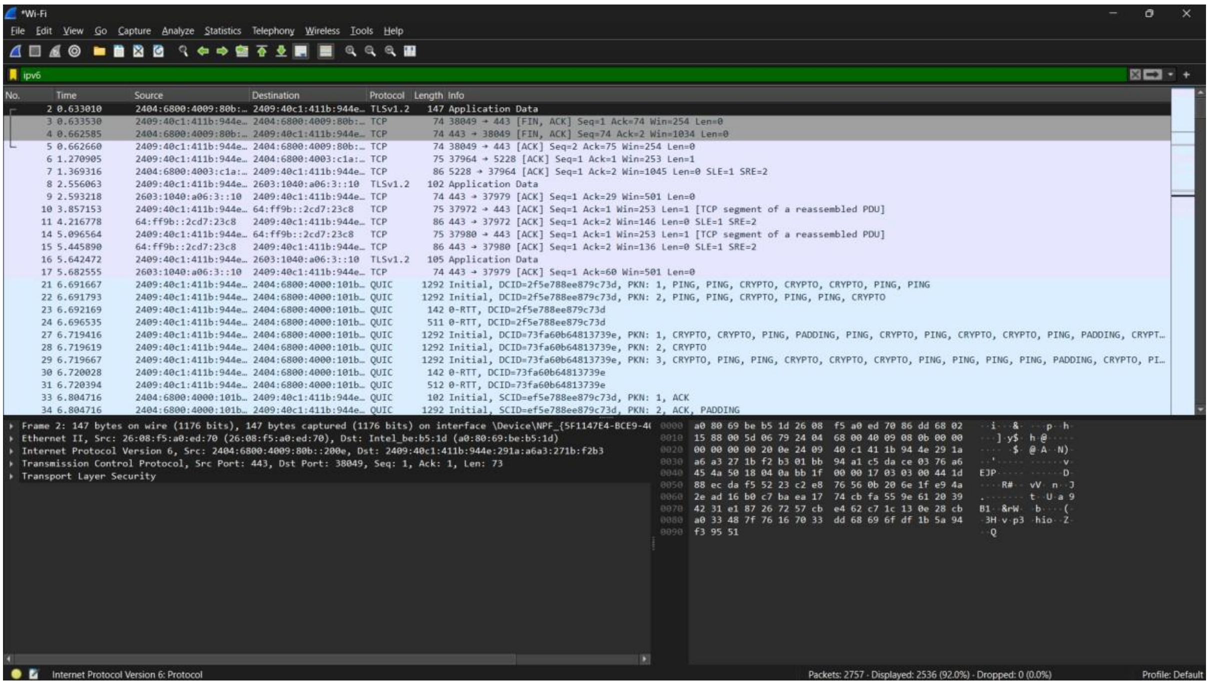
HTTP:


*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

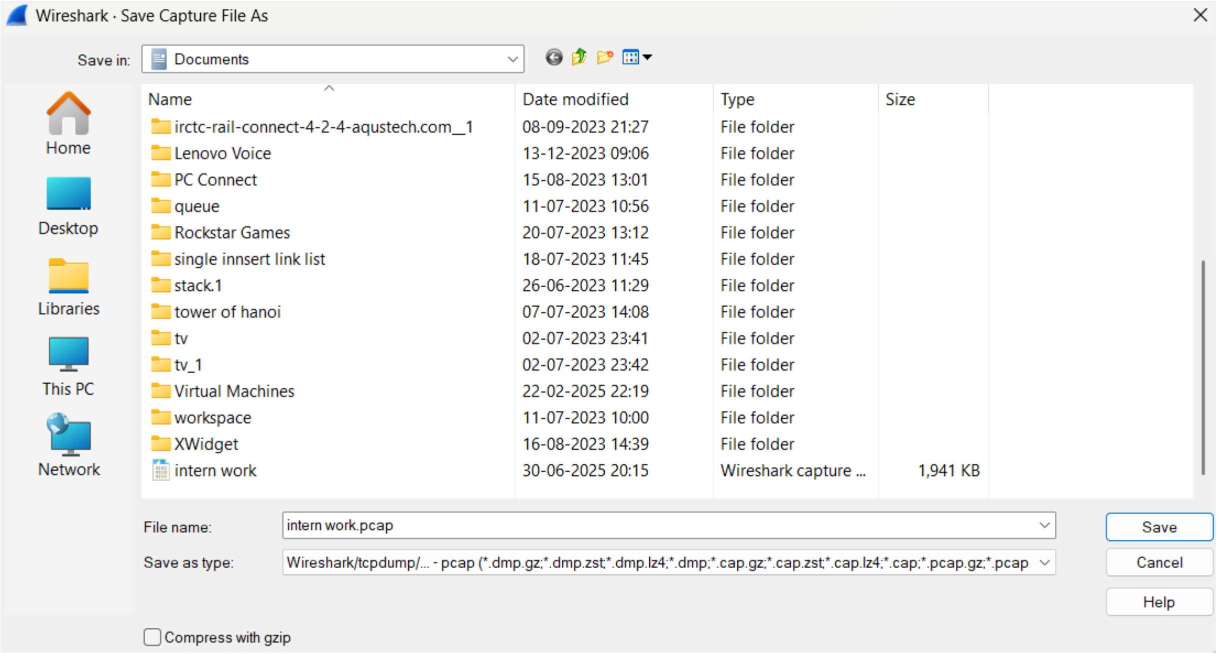
```
ipv6
No.  Time      Source                 Destination            Protocol Length Info
 2 0.633010  2404:6800:4009:80b:…  2409:40c1:411b:944e…  TLSv1.2   147 Application Data
 3 0.633530  2409:40c1:411b:944e…  2404:6800:4009:80b:…  TCP        74 38049 → 443 [FIN, ACK] Seq=1 Ack=74 Win=254 Len=0
 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
```

```
0000  a0 80 69 be b5 1d 26 08  f5 a0 ed 70 86 dd 68 02   ··i···&· ···p··h·
0010  15 88 00 5d 06 79 24 04  68 00 40 09 08 0b 00 00   ···]·y$· h·@·····
0020  00 00 00 00 20 0e 24 09  40 c1 41 1b 94 4e 29 1a   ···· ·$· @·A··N)·
0030  a6 a3 27 1b f2 b3 01 bb  94 a1 c5 da ce 03 76 a6   ··'····· ······v·
0040  45 4a 50 18 04 0a bb 1f  00 00 17 03 03 00 44 1d   EJP····· ······D·
0050  88 ec da f5 52 23 c2 e8  76 56 0b 20 6e 1f e9 4a   ····R#·· vV· n··J
0060  2e ad 16 b0 c7 ba ea 17  74 cb fa 55 9e 61 20 39   .······· t··U·a 9
0070  42 31 e1 87 26 72 57 cb  e4 62 c7 1c 13 0e 28 cb   B1··&rW· ·b····(·
0080  a0 33 48 7f 76 16 70 33  dd 68 69 6f df 1b 5a 94   ·3H·v·p3 ·hio··Z·
0090  f3 95 51                                           ··Q
```

```
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.



Save in: Documents

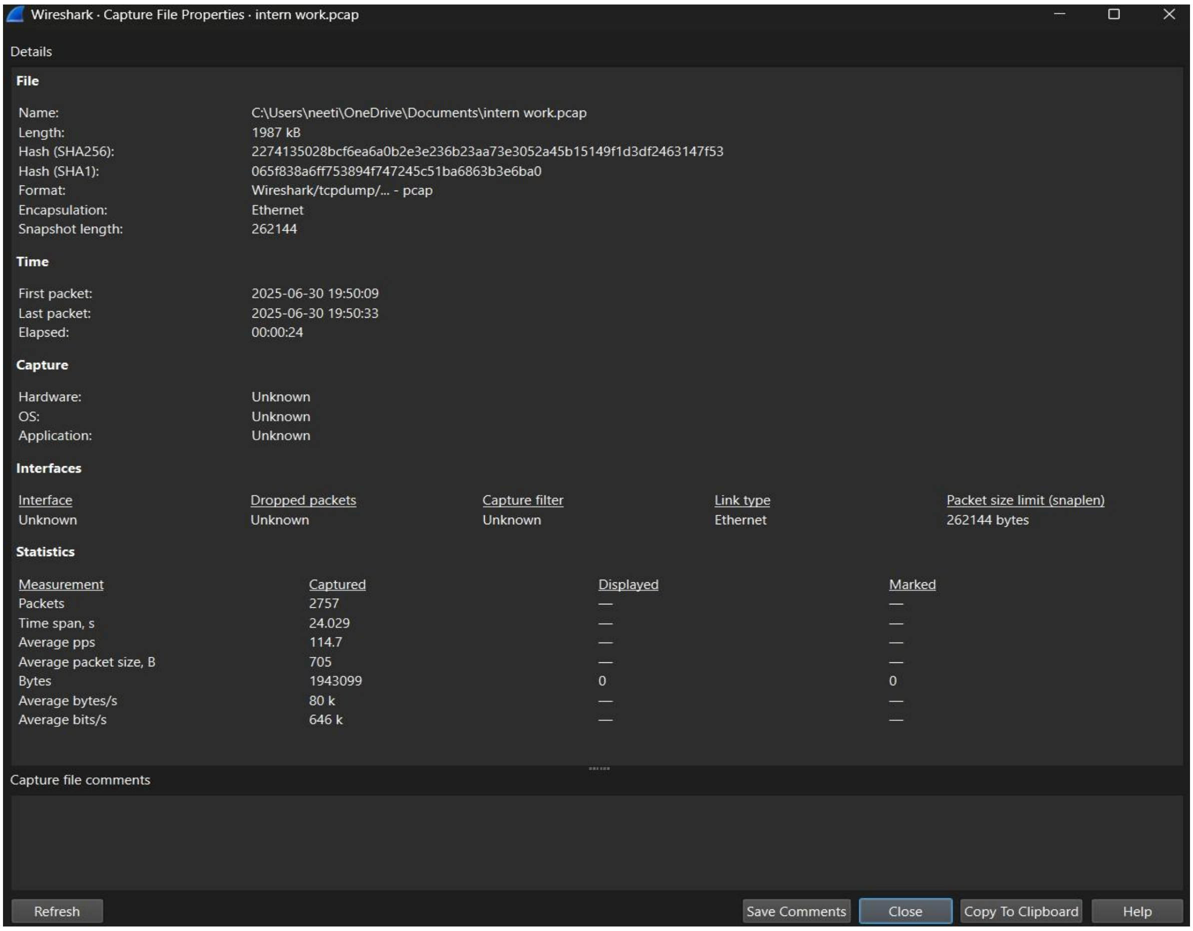
Name	Date modified	Type	Size
irctc-rail-connect-4-2-4-aqustech.com_1	08-09-2023 21:27	File folder	
Lenovo Voice	13-12-2023 09:06	File folder	
PC Connect	15-08-2023 13:01	File folder	
queue	11-07-2023 10:56	File folder	
Rockstar Games	20-07-2023 13:12	File folder	
single innsert link list	18-07-2023 11:45	File folder	
stack.1	26-06-2023 11:29	File folder	
tower of hanoi	07-07-2023 14:08	File folder	
tv	02-07-2023 23:41	File folder	
tv_1	02-07-2023 23:42	File folder	
Virtual Machines	22-02-2025 22:19	File folder	
workspace	11-07-2023 10:00	File folder	
XWidget	16-08-2023 14:39	File folder	
intern work	30-06-2025 20:15	Wireshark capture ...	1,941 KB

File name: intern work.pcap

Save as type: Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.zst;*.dmp.lz4;*.dmp;*.cap.gz;*.cap.zst;*.cap.lz4;*.cap;*.pcap.gz;*.pcap

□ Compress with gzip

6. Findings and packets details.



Details

File

Name:	C:\Users\neeti\OneDrive\Documents\intern work.pcap
Length:	1987 kB
Hash (SHA256):	2274135028bcf6ea6a0b2e3e236b23aa73e3052a45b15149f1d3df2463147f53
Hash (SHA1):	065f838a6ff753894f747245c51ba6863b3e6ba0
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	262144

Time

First packet:	2025-06-30 19:50:09
Last packet:	2025-06-30 19:50:33
Elapsed:	00:00:24

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

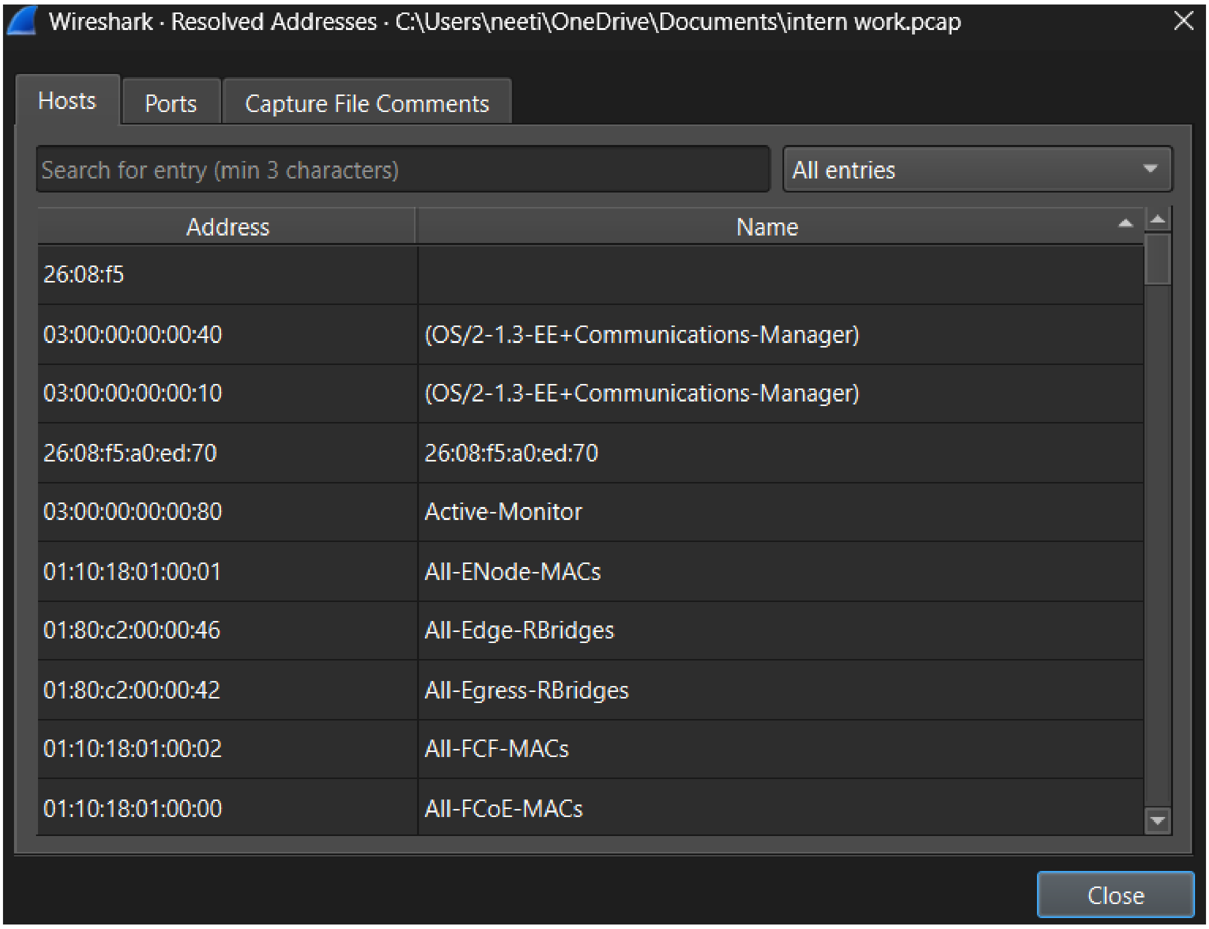
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	262144 bytes

Statistics

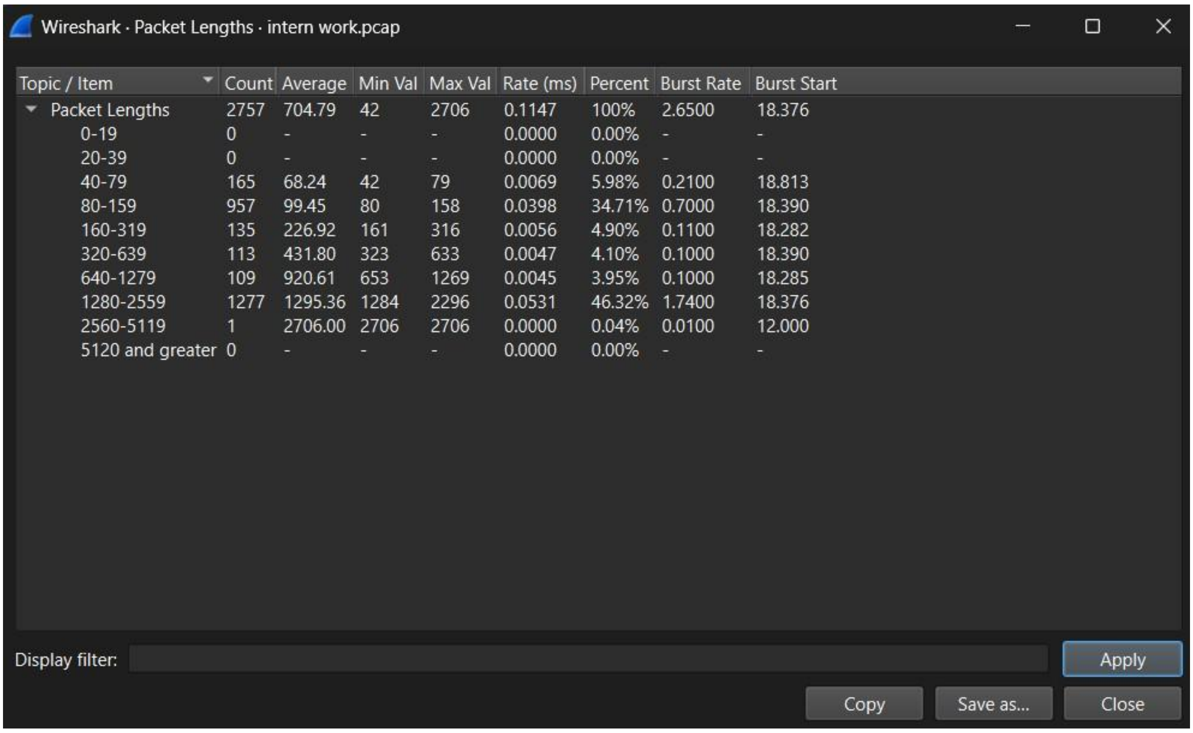
Measurement	Captured	Displayed	Marked
Packets	2757	—	—
Time span, s	24.029	—	—
Average pps	114.7	—	—
Average packet size, B	705	—	—
Bytes	1943099	0	0
Average bytes/s	80 k	—	—
Average bits/s	646 k	—	—

Capture file comments


Wireshark · Resolved Addresses · C:\Users\neeti\OneDrive\Documents\intern work.pcap
Hosts
Ports
Capture File Comments
Search for entry (min 3 characters)
Close

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



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%	-	-