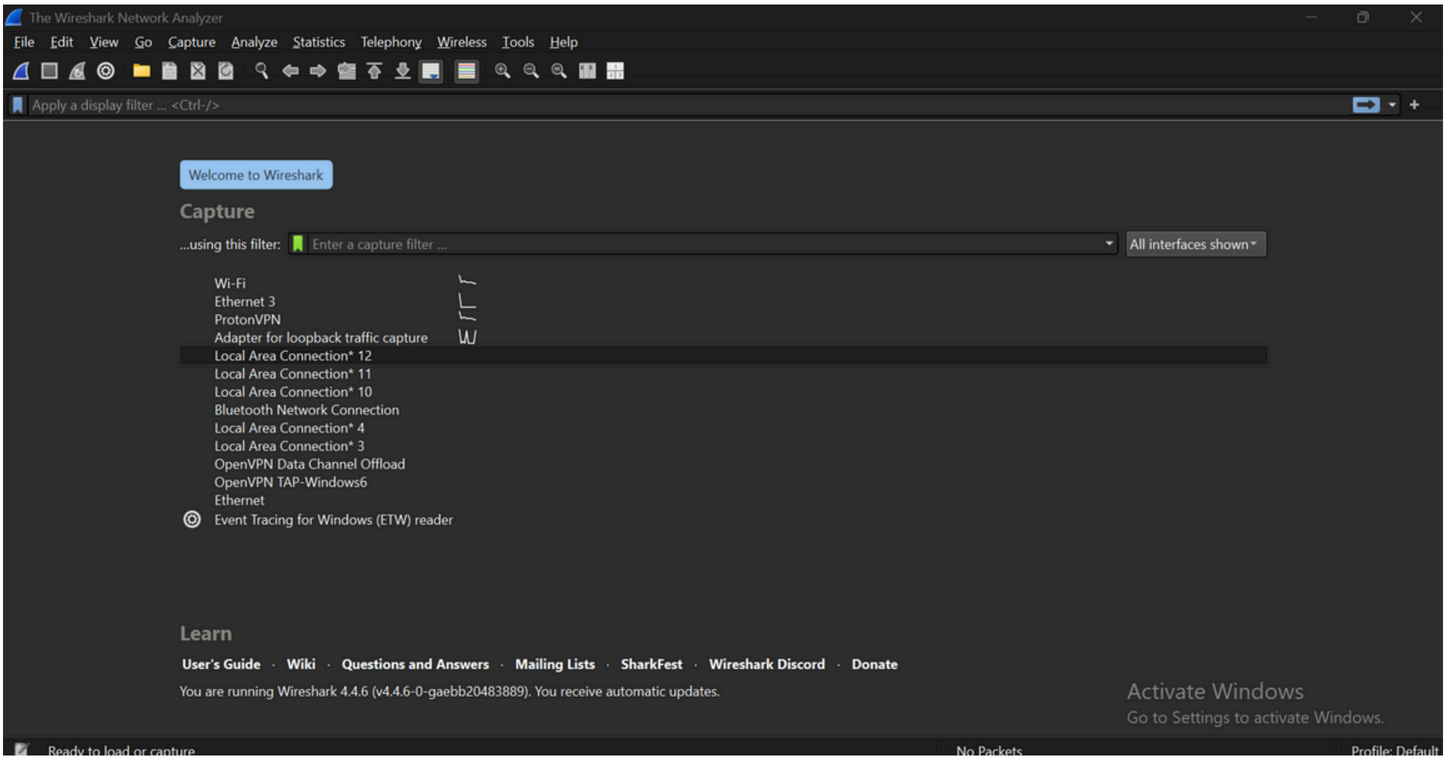
Wireshark Packet Capture Report

1. Install Wireshark

- Download from https://www.wireshark.org/
- Install with default settings. Grant permission to capture packets.

2. Start Capturing

- Open Wireshark.
- Select your **active network interface** (usually Wi-Fi or Ethernet).
- Click the blue **shark fin icon** to start capturing.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Activate Windows
Go to Settings to activate Windows.
Ready to load or capture
No Packets
Profile: Default

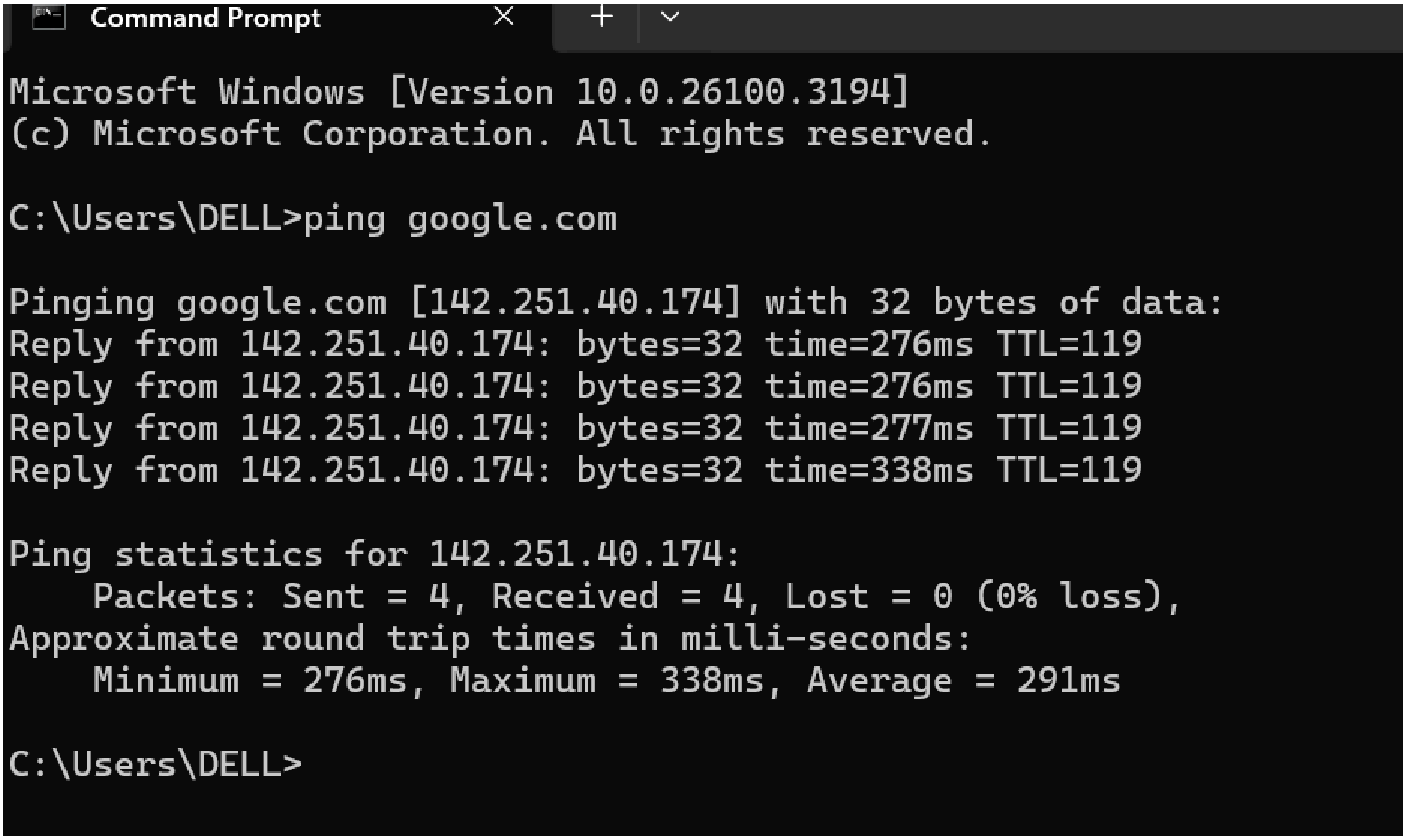
Wi-Fi
Ethernet 3
ProtonVPN
Adapter for loopback traffic capture
Local Area Connection* 12
Local Area Connection* 11
Local Area Connection* 10
Bluetooth Network Connection
Local Area Connection* 4
Local Area Connection* 3
OpenVPN Data Channel Offload
OpenVPN TAP-Windows6
Ethernet
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.4.6 (v4.4.6-0-gaebb20483889). You receive automatic updates.

3. Generate Network Traffic

While capturing:

- Open a browser and visit a few websites (e.g., example.com, openai.com).
- Open terminal or command prompt and run:
- **Command:** ping google.com



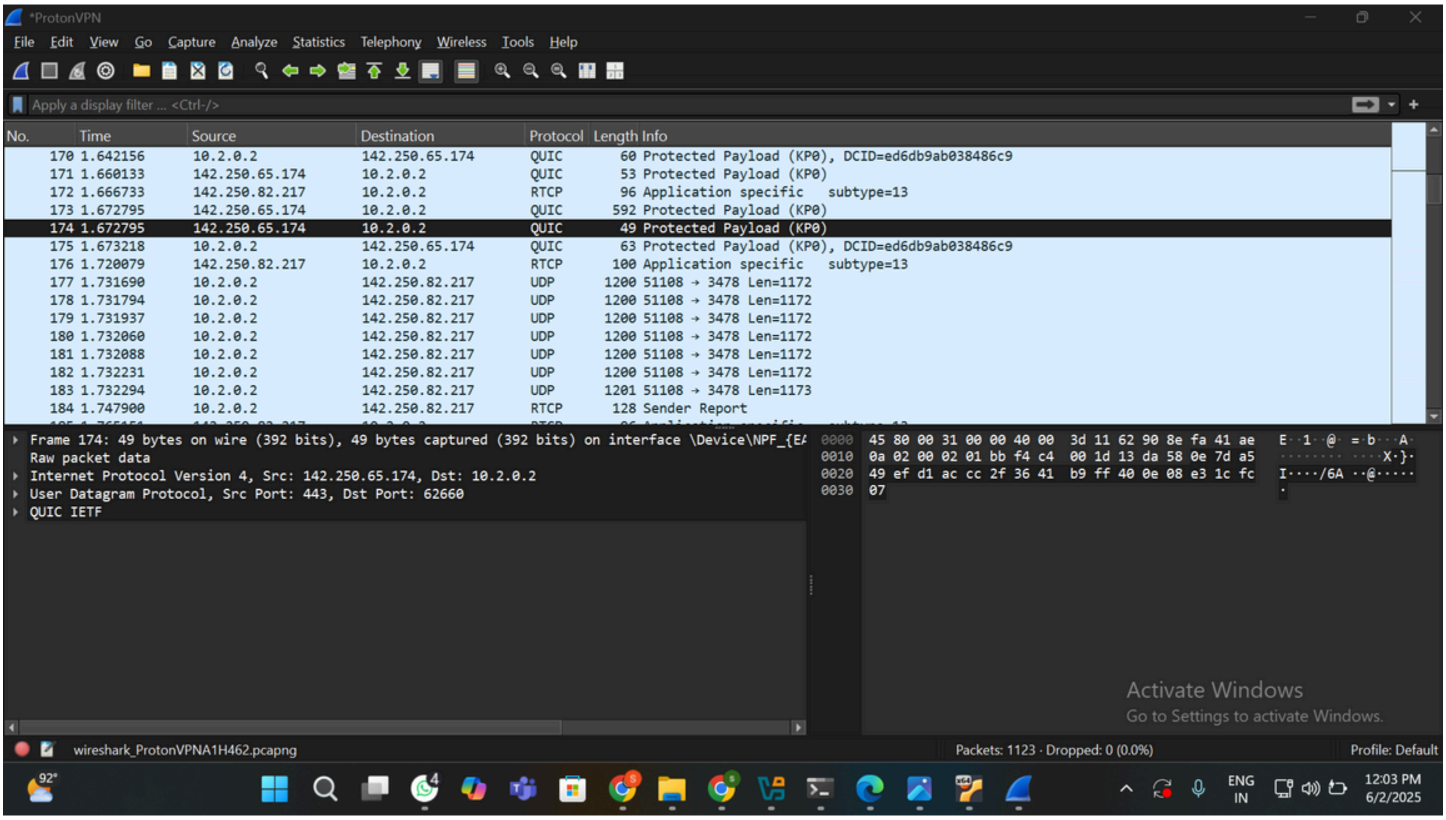
```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping google.com

Pinging google.com [142.251.40.174] with 32 bytes of data:
Reply from 142.251.40.174: bytes=32 time=276ms TTL=119
Reply from 142.251.40.174: bytes=32 time=276ms TTL=119
Reply from 142.251.40.174: bytes=32 time=277ms TTL=119
Reply from 142.251.40.174: bytes=32 time=338ms TTL=119

Ping statistics for 142.251.40.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 276ms, Maximum = 338ms, Average = 291ms

C:\Users\DELL>
```


*ProtonVPN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
wireshark_ProtonVPNA1H462.pcapng
Packets: 1123 · Dropped: 0 (0.0%)
Profile: Default
92°
ENG
IN
12:03 PM
6/2/2025

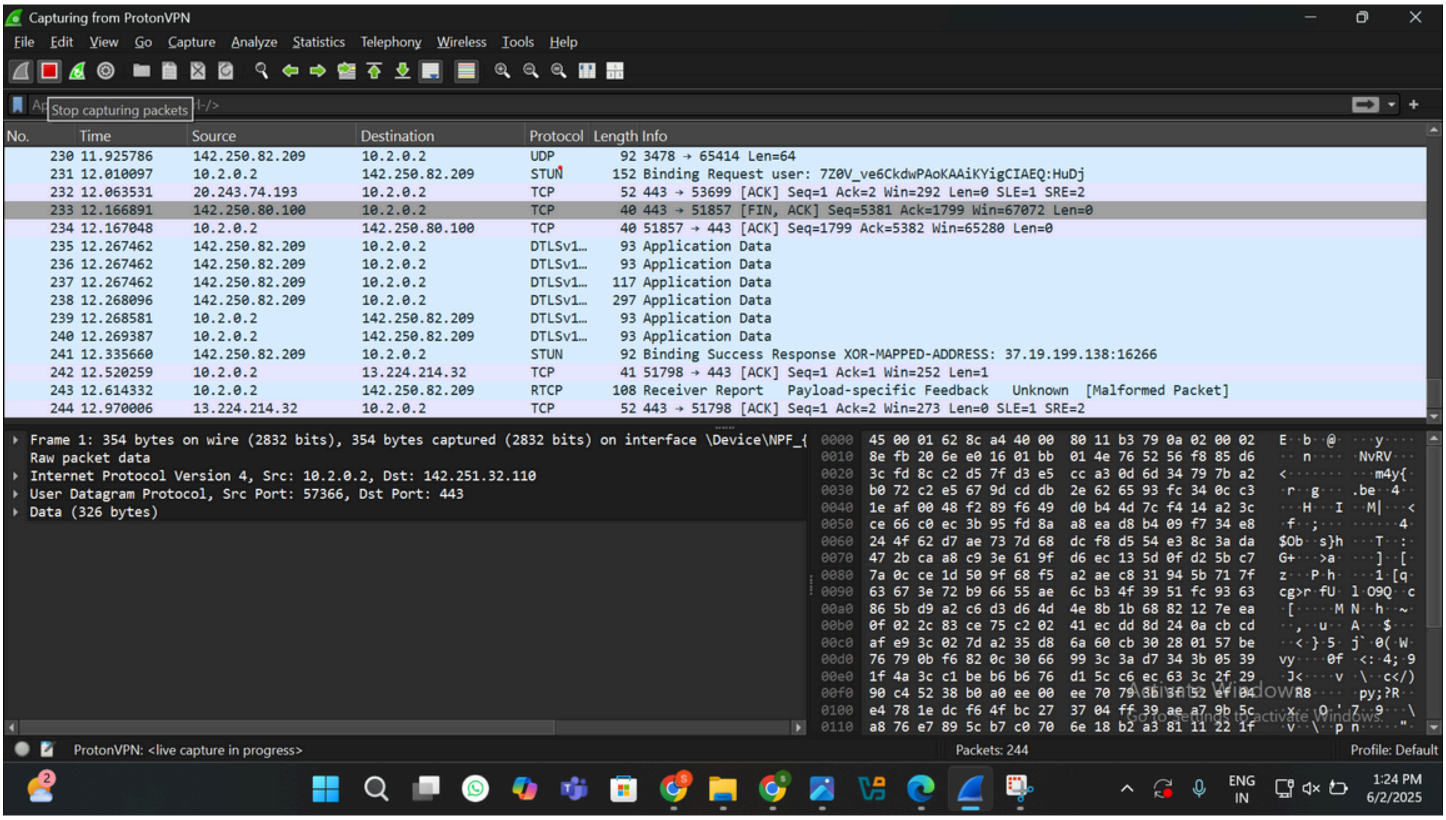
```
No.   Time      Source          Destination     Protocol Length Info
  170 1.642156  10.2.0.2        142.250.65.174  QUIC       60 Protected Payload (KP0), DCID=ed6db9ab038486c9
  171 1.660133  142.250.65.174  10.2.0.2        QUIC       53 Protected Payload (KP0)
  172 1.666733  142.250.82.217  10.2.0.2        RTCP       96 Application specific   subtype=13
  173 1.672795  142.250.65.174  10.2.0.2        QUIC      592 Protected Payload (KP0)
  174 1.672795  142.250.65.174  10.2.0.2        QUIC       49 Protected Payload (KP0)
  175 1.673218  10.2.0.2        142.250.65.174  QUIC       63 Protected Payload (KP0), DCID=ed6db9ab038486c9
  176 1.720079  142.250.82.217  10.2.0.2        RTCP      100 Application specific   subtype=13
  177 1.731690  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  178 1.731794  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  179 1.731937  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  180 1.732060  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  181 1.732088  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  182 1.732231  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  183 1.732294  10.2.0.2        142.250.82.217  UDP      1201 51108 → 3478 Len=1173
  184 1.747900  10.2.0.2        142.250.82.217  RTCP      128 Sender Report

> Frame 174: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface \Device\NPF_{EA
  Raw packet data
> Internet Protocol Version 4, Src: 142.250.65.174, Dst: 10.2.0.2
> User Datagram Protocol, Src Port: 443, Dst Port: 62660
> QUIC IETF

0000  45 80 00 31 00 00 40 00  3d 11 62 90 8e fa 41 ae   E··1··@· =·b···A·
0010  0a 02 00 02 01 bb f4 c4  00 1d 13 da 58 0e 7d a5   ········ ····X·}·
0020  49 ef d1 ac cc 2f 36 41  b9 ff 40 0e 08 e3 1c fc   I····/6A ··@·····
0030  07                                                 ·
```

4. Stop Capture

- After about 1 minute, click the red square **Stop** button.


Capturing from ProtonVPN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Stop capturing packets

```
No.  Time       Source          Destination     Protocol Length Info
 230 11.925786  142.250.82.209  10.2.0.2        UDP       92 3478 → 65414 Len=64
 231 12.010097  10.2.0.2        142.250.82.209  STUN     152 Binding Request user: 7Z0V_ve6CkdwPAoKAAiKYigCIAEQ:HuDj
 232 12.063531  20.243.74.193   10.2.0.2        TCP       52 443 → 53699 [ACK] Seq=1 Ack=2 Win=292 Len=0 SLE=1 SRE=2
 233 12.166891  142.250.80.100  10.2.0.2        TCP       40 443 → 51857 [FIN, ACK] Seq=5381 Ack=1799 Win=67072 Len=0
 234 12.167048  10.2.0.2        142.250.80.100  TCP       40 51857 → 443 [ACK] Seq=1799 Ack=5382 Win=65280 Len=0
 235 12.267462  142.250.82.209  10.2.0.2        DTLSv1…   93 Application Data
 236 12.267462  142.250.82.209  10.2.0.2        DTLSv1…   93 Application Data
 237 12.267462  142.250.82.209  10.2.0.2        DTLSv1…  117 Application Data
 238 12.268096  142.250.82.209  10.2.0.2        DTLSv1…  297 Application Data
 239 12.268581  10.2.0.2        142.250.82.209  DTLSv1…   93 Application Data
 240 12.269387  10.2.0.2        142.250.82.209  DTLSv1…   93 Application Data
 241 12.335660  142.250.82.209  10.2.0.2        STUN      92 Binding Success Response XOR-MAPPED-ADDRESS: 37.19.199.138:16266
 242 12.520259  10.2.0.2        13.224.214.32   TCP       41 51798 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
 243 12.614332  10.2.0.2        142.250.82.209  RTCP     108 Receiver Report   Payload-specific Feedback   Unknown  [Malformed Packet]
 244 12.970006  13.224.214.32   10.2.0.2        TCP       52 443 → 51798 [ACK] Seq=1 Ack=2 Win=273 Len=0 SLE=1 SRE=2
```

```
> Frame 1: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface \Device\NPF_{
  Raw packet data
> Internet Protocol Version 4, Src: 10.2.0.2, Dst: 142.251.32.110
> User Datagram Protocol, Src Port: 57366, Dst Port: 443
> Data (326 bytes)
```

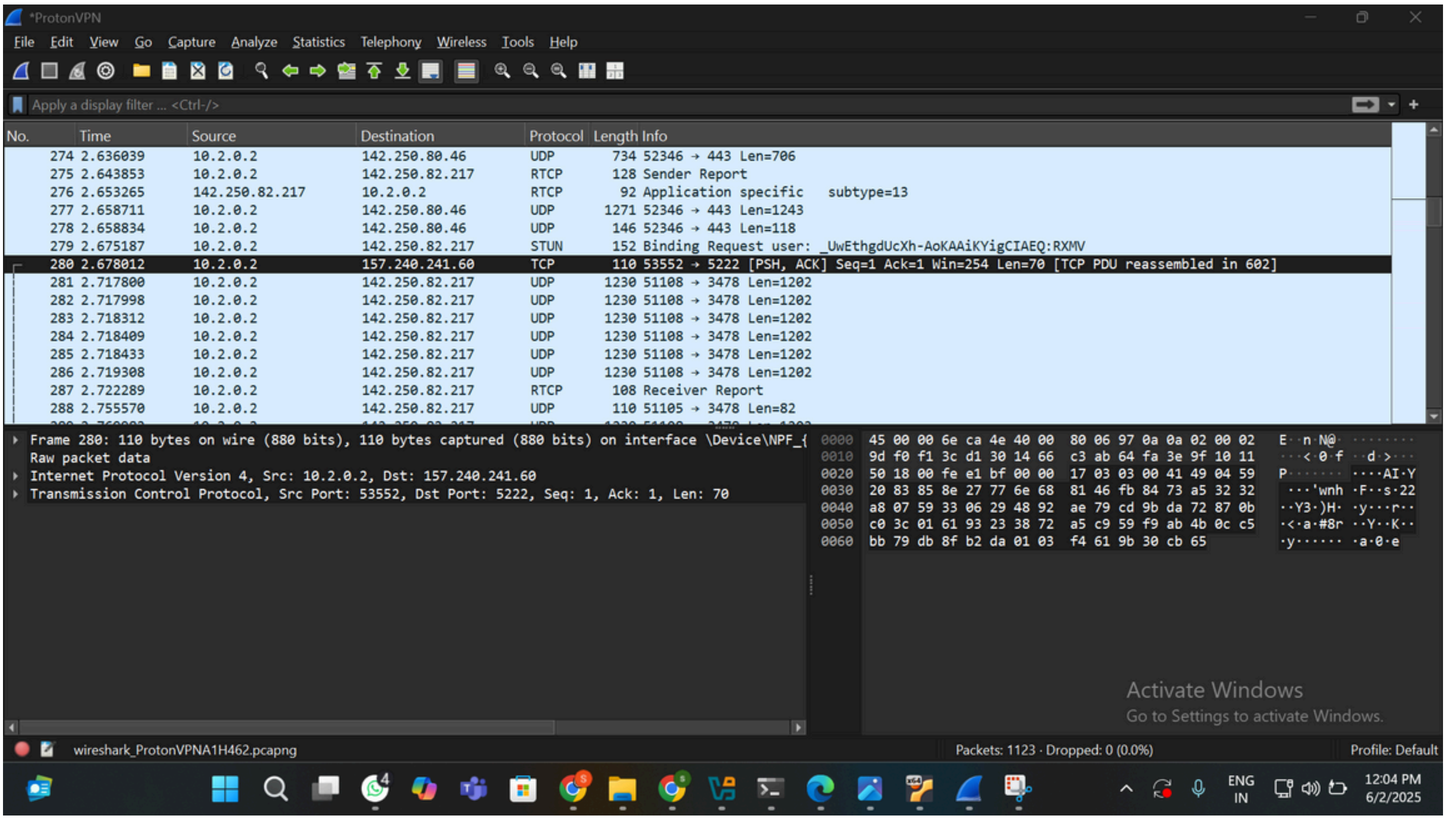
```
0000  45 00 01 62 8c a4 40 00  80 11 b3 79 0a 02 00 02
0010  8e fb 20 6e e0 16 01 bb  01 4e 76 52 56 f8 85 d6
0020  3c fd 8c c2 d5 7f d3 e5  cc a3 0d 6d 34 79 7b a2
0030  b0 72 c2 e5 67 9d cd db  2e 62 65 93 fc 34 0c c3
0040  1e af 00 48 f2 89 f6 49  d0 b4 4d 7c f4 14 a2 3c
0050  ce 66 c0 ec 3b 95 fd 8a  a8 ea d8 b4 09 f7 34 e8
0060  24 4f 62 d7 ae 73 7d 68  dc f8 d5 54 e3 8c 3a da
0070  47 2b ca a8 c9 3e 61 9f  d6 ec 13 5d 0f d2 5b c7
0080  7a 0c ce 1d 50 9f 68 f5  a2 ae c8 31 94 5b 71 7f
0090  63 67 3e 72 b9 66 55 ae  6c b3 4f 39 51 fc 93 63
00a0  86 5b d9 a2 c6 d3 d6 4d  4e 8b 1b 68 82 12 7e ea
00b0  0f 02 2c 83 ce 75 c2 02  41 ec dd 8d 24 0a cb cd
00c0  af e9 3c 02 7d a2 35 d8  6a 60 cb 30 28 01 57 be
00d0  76 79 0b f6 82 0c 30 66  99 3c 3a d7 34 3b 05 39
00e0  1f 4a 3c c1 be b6 b6 76  d1 5c c6 ec 63 3c 2f 29
00f0  90 c4 52 38 b0 a0 ee 00  ee 70 79 3b 3f 52 ef 04
0100  e4 78 1e dc f6 4f bc 27  37 04 ff 39 ae a7 9b 5c
0110  a8 76 e7 89 5c b7 c0 70  6e 18 b2 a3 81 11 22 1f
```

Activate Windows
Go to Settings to activate Windows.
ProtonVPN: <live capture in progress>
Packets: 244
Profile: Default
ENG
IN
1:24 PM
6/2/2025

5. Filter Traffic

Use Wireshark filters in the top filter bar to isolate specific protocols:

- TCP – to analyze **TCP** connections


*ProtonVPN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

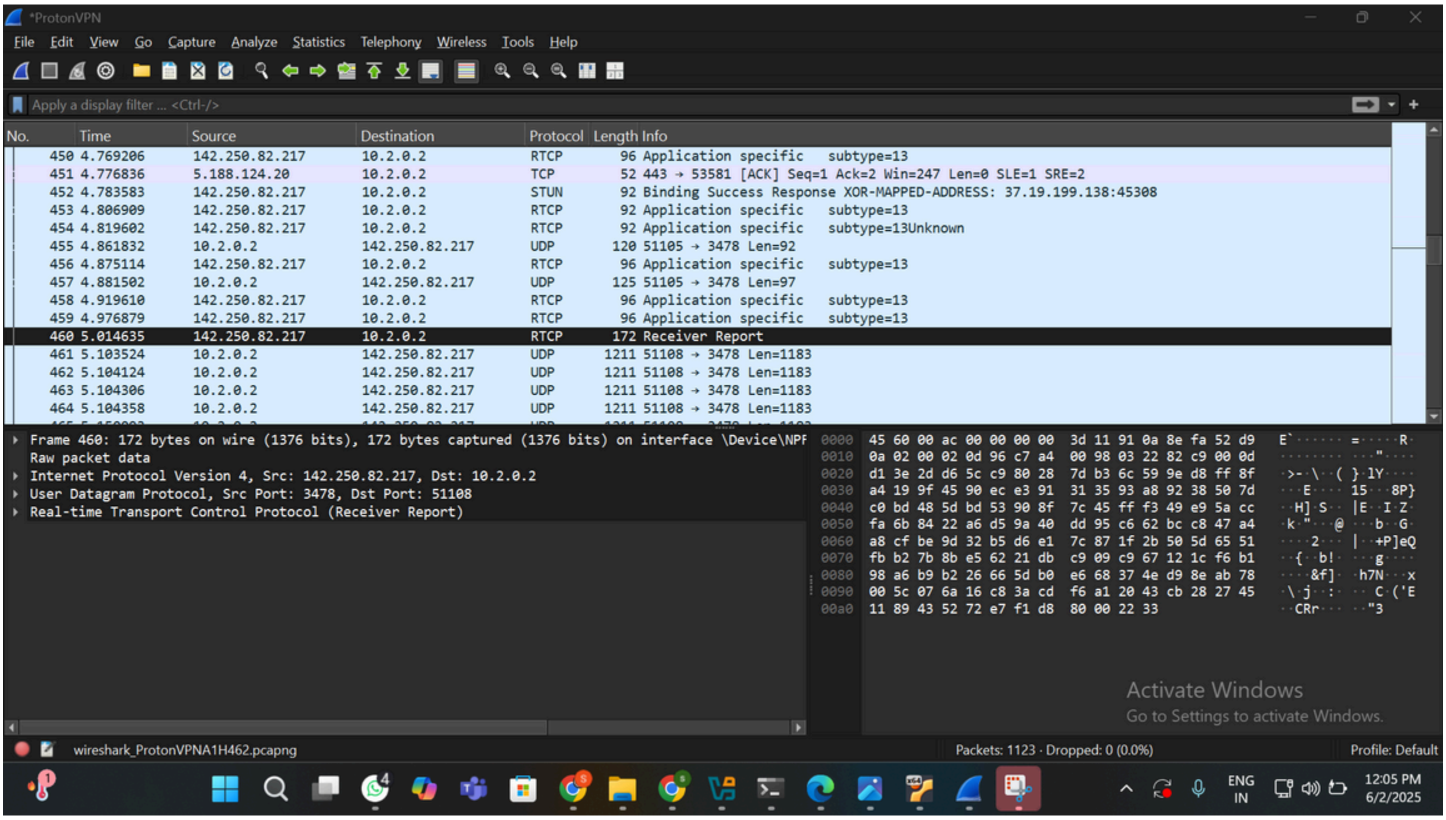
```
No.  Time      Source          Destination     Protocol Length Info
 274 2.636039  10.2.0.2        142.250.80.46   UDP       734 52346 → 443 Len=706
 275 2.643853  10.2.0.2        142.250.82.217  RTCP      128 Sender Report
 276 2.653265  142.250.82.217  10.2.0.2        RTCP       92 Application specific   subtype=13
 277 2.658711  10.2.0.2        142.250.80.46   UDP      1271 52346 → 443 Len=1243
 278 2.658834  10.2.0.2        142.250.80.46   UDP       146 52346 → 443 Len=118
 279 2.675187  10.2.0.2        142.250.82.217  STUN      152 Binding Request user: _UwEthgdUcXh-AoKAAiKYigCIAEQ:RXMV
 280 2.678012  10.2.0.2        157.240.241.60  TCP       110 53552 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=70 [TCP PDU reassembled in 602]
 281 2.717800  10.2.0.2        142.250.82.217  UDP      1230 51108 → 3478 Len=1202
 282 2.717998  10.2.0.2        142.250.82.217  UDP      1230 51108 → 3478 Len=1202
 283 2.718312  10.2.0.2        142.250.82.217  UDP      1230 51108 → 3478 Len=1202
 284 2.718409  10.2.0.2        142.250.82.217  UDP      1230 51108 → 3478 Len=1202
 285 2.718433  10.2.0.2        142.250.82.217  UDP      1230 51108 → 3478 Len=1202
 286 2.719308  10.2.0.2        142.250.82.217  UDP      1230 51108 → 3478 Len=1202
 287 2.722289  10.2.0.2        142.250.82.217  RTCP      108 Receiver Report
 288 2.755570  10.2.0.2        142.250.82.217  UDP       110 51105 → 3478 Len=82
```

```
> Frame 280: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{
  Raw packet data
> Internet Protocol Version 4, Src: 10.2.0.2, Dst: 157.240.241.60
> Transmission Control Protocol, Src Port: 53552, Dst Port: 5222, Seq: 1, Ack: 1, Len: 70
```

```
0000  45 00 00 6e ca 4e 40 00  80 06 97 0a 0a 02 00 02
0010  9d f0 f1 3c d1 30 14 66  c3 ab 64 fa 3e 9f 10 11
0020  50 18 00 fe e1 bf 00 00  17 03 03 00 41 49 04 59
0030  20 83 85 8e 27 77 6e 68  81 46 fb 84 73 a5 32 32
0040  a8 07 59 33 06 29 48 92  ae 79 cd 9b da 72 87 0b
0050  c0 3c 01 61 93 23 38 72  a5 c9 59 f9 ab 4b 0c c5
0060  bb 79 db 8f b2 da 01 03  f4 61 9b 30 cb 65
```

Activate Windows
Go to Settings to activate Windows.
wireshark_ProtonVPNA1H462.pcapng
Packets: 1123 · Dropped: 0 (0.0%)
Profile: Default
ENG
IN
12:04 PM
6/2/2025

- RTCP – to view **RTCP (Real-Time Control Protocol)** traffic



*ProtonVPN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

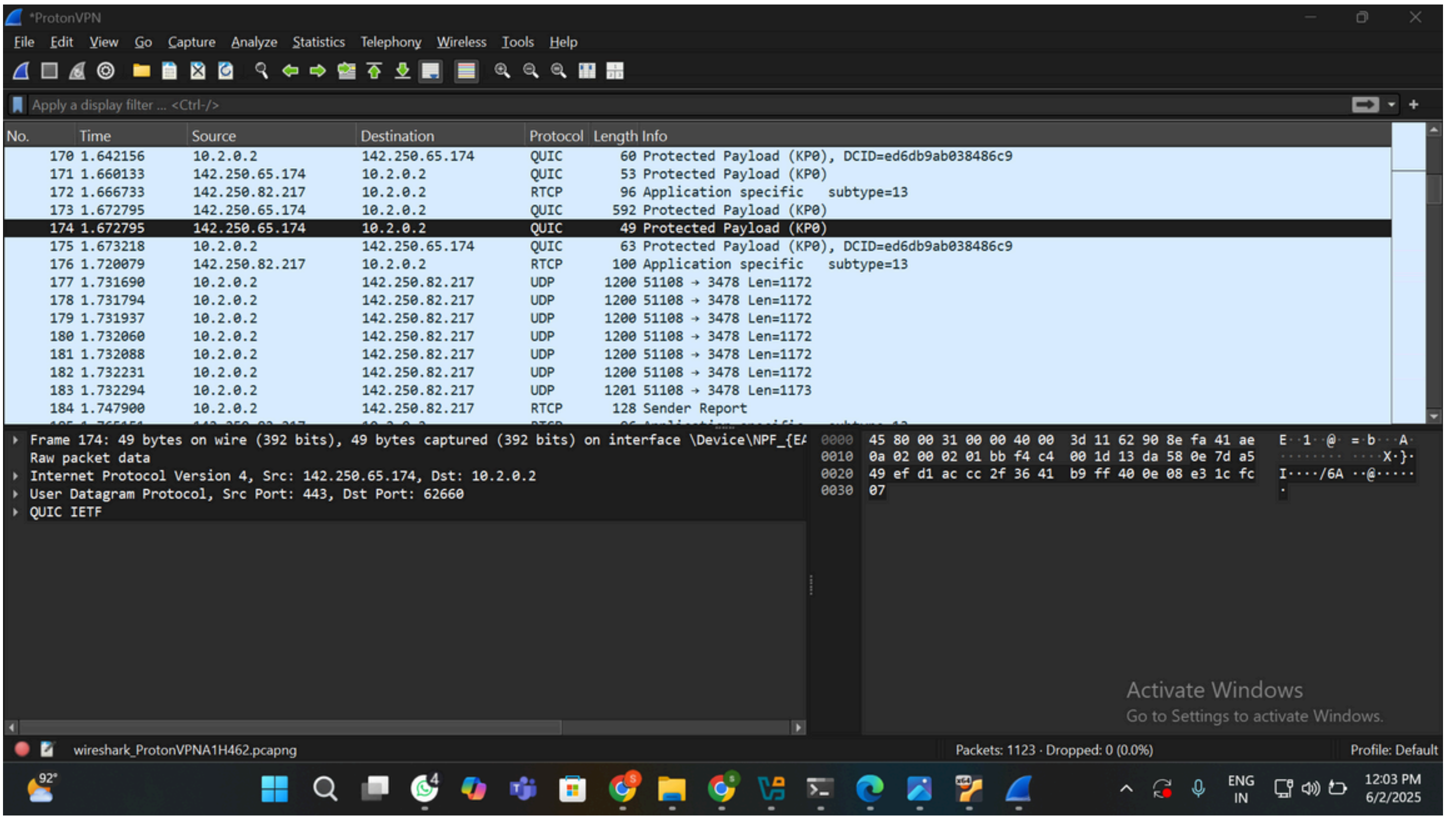
```
No.   Time      Source          Destination     Protocol Length Info
  450 4.769206  142.250.82.217  10.2.0.2        RTCP       96 Application specific   subtype=13
  451 4.776836  5.188.124.20    10.2.0.2        TCP        52 443 → 53581 [ACK] Seq=1 Ack=2 Win=247 Len=0 SLE=1 SRE=2
  452 4.783583  142.250.82.217  10.2.0.2        STUN       92 Binding Success Response XOR-MAPPED-ADDRESS: 37.19.199.138:45308
  453 4.806909  142.250.82.217  10.2.0.2        RTCP       92 Application specific   subtype=13
  454 4.819602  142.250.82.217  10.2.0.2        RTCP       92 Application specific   subtype=13Unknown
  455 4.861832  10.2.0.2        142.250.82.217  UDP       120 51105 → 3478 Len=92
  456 4.875114  142.250.82.217  10.2.0.2        RTCP       96 Application specific   subtype=13
  457 4.881502  10.2.0.2        142.250.82.217  UDP       125 51105 → 3478 Len=97
  458 4.919610  142.250.82.217  10.2.0.2        RTCP       96 Application specific   subtype=13
  459 4.976879  142.250.82.217  10.2.0.2        RTCP       96 Application specific   subtype=13
  460 5.014635  142.250.82.217  10.2.0.2        RTCP      172 Receiver Report
  461 5.103524  10.2.0.2        142.250.82.217  UDP      1211 51108 → 3478 Len=1183
  462 5.104124  10.2.0.2        142.250.82.217  UDP      1211 51108 → 3478 Len=1183
  463 5.104306  10.2.0.2        142.250.82.217  UDP      1211 51108 → 3478 Len=1183
  464 5.104358  10.2.0.2        142.250.82.217  UDP      1211 51108 → 3478 Len=1183
```

```
› Frame 460: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface \Device\NPF
  Raw packet data
› Internet Protocol Version 4, Src: 142.250.82.217, Dst: 10.2.0.2
› User Datagram Protocol, Src Port: 3478, Dst Port: 51108
› Real-time Transport Control Protocol (Receiver Report)
```

```
0000  45 60 00 ac 00 00 00 00  3d 11 91 0a 8e fa 52 d9   E`······ =·····R·
0010  0a 02 00 02 0d 96 c7 a4  00 98 03 22 82 c9 00 0d   ········ ···"····
0020  d1 3e 2d d6 5c c9 80 28  7d b3 6c 59 9e d8 ff 8f   ·>-·\··( }·lY····
0030  a4 19 9f 45 90 ec e3 91  31 35 93 a8 92 38 50 7d   ···E···· 15···8P}
0040  c0 bd 48 5d bd 53 90 8f  7c 45 ff f3 49 e9 5a cc   ··H]·S·· |E··I·Z·
0050  fa 6b 84 22 a6 d5 9a 40  dd 95 c6 62 bc c8 47 a4   ·k·"···@ ···b··G·
0060  a8 cf be 9d 32 b5 d6 e1  7c 87 1f 2b 50 5d 65 51   ····2··· |··+P]eQ
0070  fb b2 7b 8b e5 62 21 db  c9 09 c9 67 12 1c f6 b1   ··{··b!· ···g····
0080  98 a6 b9 b2 26 66 5d b0  e6 68 37 4e d9 8e ab 78   ····&f]· ·h7N···x
0090  00 5c 07 6a 16 c8 3a cd  f6 a1 20 43 cb 28 27 45   ·\·j··:· ·· C·('E
00a0  11 89 43 52 72 e7 f1 d8  80 00 22 33               ··CRr··· ··"3
```

wireshark_ProtonVPNA1H462.pcapng   Packets: 1123 · Dropped: 0 (0.0%)   Profile: Default

- QUIC – to capture **QUIC** protocol packets (used by **HTTP/3**, over UDP)



*ProtonVPN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
  170 1.642156  10.2.0.2        142.250.65.174  QUIC       60 Protected Payload (KP0), DCID=ed6db9ab038486c9
  171 1.660133  142.250.65.174  10.2.0.2        QUIC       53 Protected Payload (KP0)
  172 1.666733  142.250.82.217  10.2.0.2        RTCP       96 Application specific   subtype=13
  173 1.672795  142.250.65.174  10.2.0.2        QUIC      592 Protected Payload (KP0)
  174 1.672795  142.250.65.174  10.2.0.2        QUIC       49 Protected Payload (KP0)
  175 1.673218  10.2.0.2        142.250.65.174  QUIC       63 Protected Payload (KP0), DCID=ed6db9ab038486c9
  176 1.720079  142.250.82.217  10.2.0.2        RTCP      100 Application specific   subtype=13
  177 1.731690  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  178 1.731794  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  179 1.731937  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  180 1.732060  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  181 1.732088  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  182 1.732231  10.2.0.2        142.250.82.217  UDP      1200 51108 → 3478 Len=1172
  183 1.732294  10.2.0.2        142.250.82.217  UDP      1201 51108 → 3478 Len=1173
  184 1.747900  10.2.0.2        142.250.82.217  RTCP      128 Sender Report
```

```
› Frame 174: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface \Device\NPF_{EA
  Raw packet data
› Internet Protocol Version 4, Src: 142.250.65.174, Dst: 10.2.0.2
› User Datagram Protocol, Src Port: 443, Dst Port: 62660
› QUIC IETF
```

```
0000  45 80 00 31 00 00 40 00  3d 11 62 90 8e fa 41 ae   E··1··@· =·b···A·
0010  0a 02 00 02 01 bb f4 c4  00 1d 13 da 58 0e 7d a5   ········ ····X·}·
0020  49 ef d1 ac cc 2f 36 41  b9 ff 40 0e 08 e3 1c fc   I····/6A ··@·····
0030  07                                                 ·
```

wireshark_ProtonVPNA1H462.pcapng   Packets: 1123 · Dropped: 0 (0.0%)   Profile: Default

6. Identify Protocols

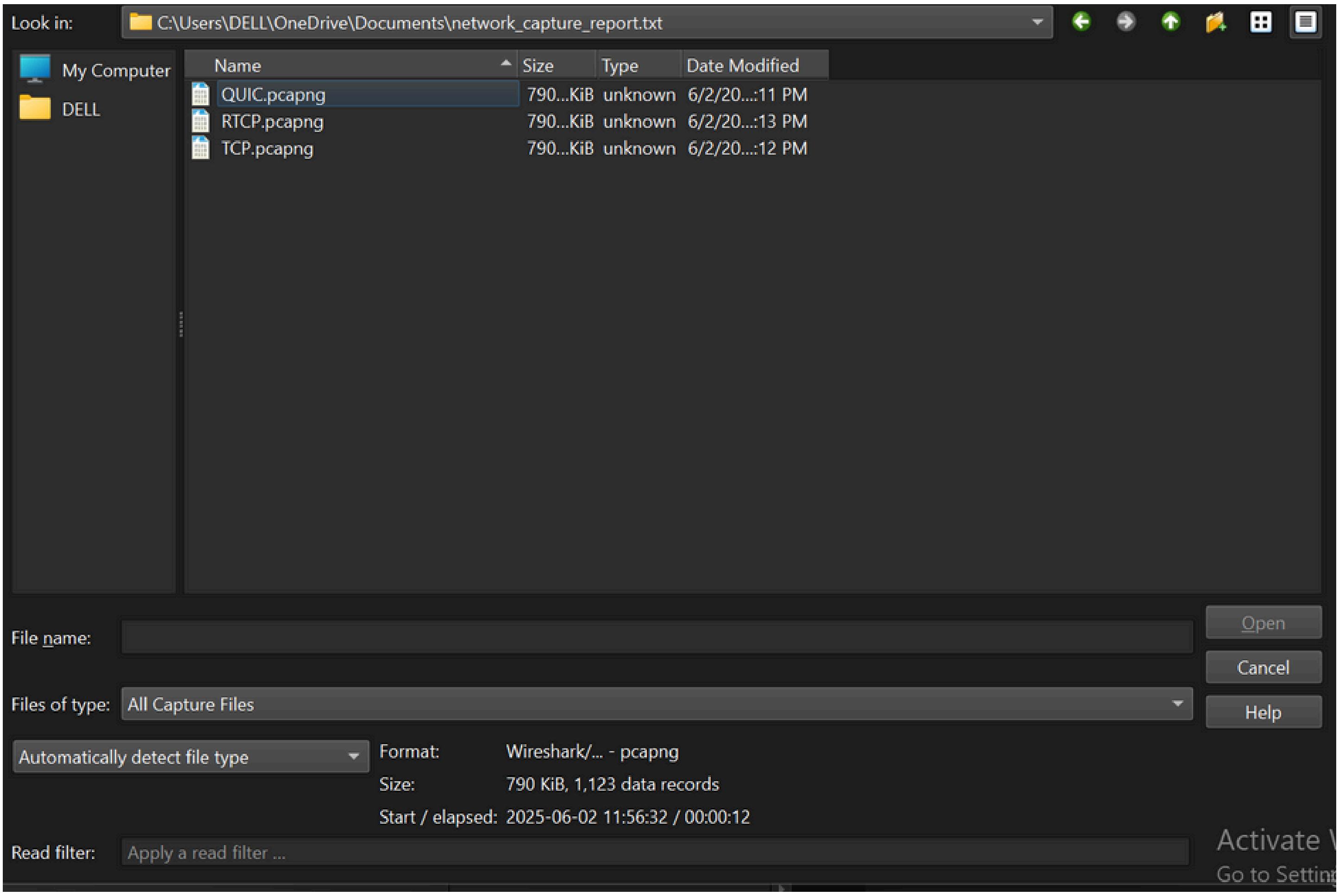
Find at least **3 distinct protocols** such as:

- DNS
- HTTP/HTTPS
- TCP

- RTCP
- ICMP
- QUIC

7. Export .pcap File

- File → Export Specified Packets → Save as .pcap



Look in: C:\Users\DELL\OneDrive\Documents\network_capture_report.txt

Name	Size	Type	Date Modified
QUIC.pcapng	790...KiB	unknown	6/2/20...:11 PM
RTCP.pcapng	790...KiB	unknown	6/2/20...:13 PM
TCP.pcapng	790...KiB	unknown	6/2/20...:12 PM

File name:

Files of type: All Capture Files

Automatically detect file type

Format: Wireshark/... - pcapng

Size: 790 KiB, 1,123 data records

Start / elapsed: 2025-06-02 11:56:32 / 00:00:12

Read filter: Apply a read filter ...

Conclusion

This hands-on activity using Wireshark helped demonstrate how different network protocols operate and how to identify them in live traffic. By applying protocol filters such as tcp, rtcp, and quic, we were able to isolate and analyze specific types of network communication, including real-time control packets, modern web traffic using QUIC, and traditional TCP connections.

Through this process, we developed key skills in:

- Capturing live packets,
- Filtering by protocol,
- Recognizing traffic patterns and behaviors,
- And understanding how protocols like TCP, RTCP, and QUIC function in real-world networks.

This activity enhances both **technical troubleshooting abilities** and **protocol awareness**, which are essential for cybersecurity and network analysis roles.