Wireshark Packet Capture & Protocol Analysis Report

Prepared by: Abhinraj K A
Date: 11 August 2025
Tool Used: Wireshark 4.4.7
Interface Used: eth0

---

1. Objective

The aim of this task was to capture live network packets using Wireshark, isolate specific protocol traffic (HTTP, DNS, TCP), and analyze the captured data for network behavior insights.

---

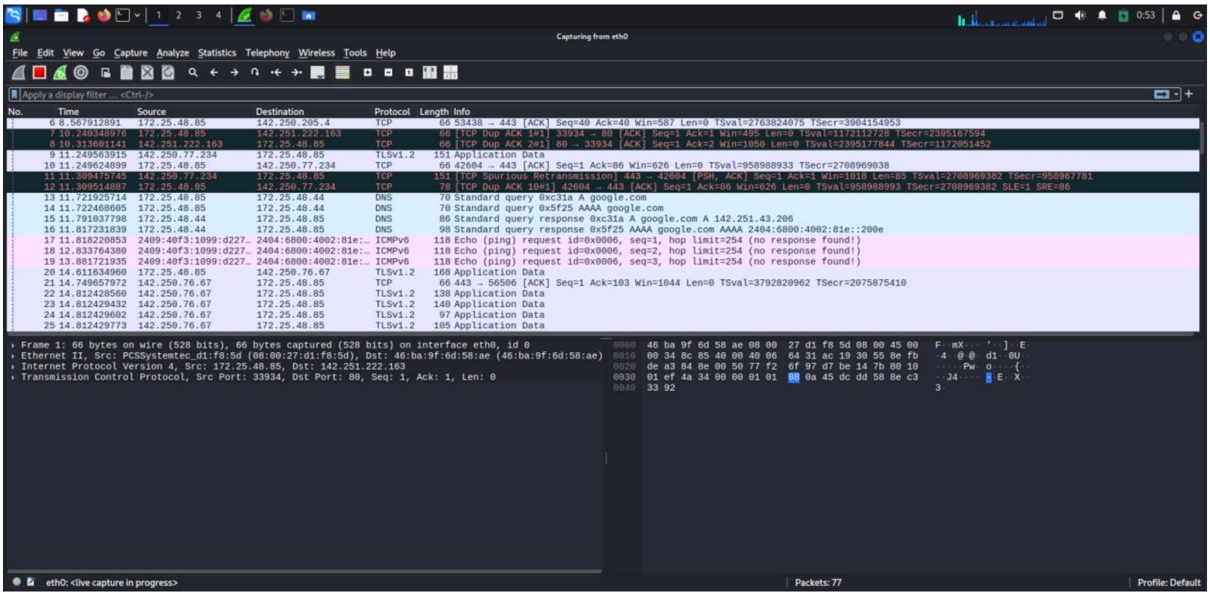
2. Methodology

1. Opened Wireshark and selected the active network interface (eth0).
2. Initiated live capture to record network packets.
3. Observed real-time data flow including multiple protocol types.
4. Applied protocol-specific filters:
   - http → for web requests and responses
   - dns → for domain resolution queries
   - tcp → for transport-layer inspection
5. Inspected packet headers and payload details for each protocol.

---

3. General Capture Overview

The first screenshot shows the start of the packet capture, with multiple protocols flowing over the network.
Observed protocols: TCP, DNS, TLS, ICMPv6, and HTTP.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time          Source               Destination          Protocol  Length Info
     6 8.567912891   172.25.48.85         142.250.205.4        TCP          66 53438 → 443 [ACK] Seq=40 Ack=40 Win=587 Len=0 TSval=2763824075 TSecr=3904154953
     7 10.240348976  172.25.48.85         142.251.222.163      TCP          66 [TCP Dup ACK 1#1] 33934 → 80 [ACK] Seq=1 Ack=1 Win=495 Len=0 TSval=1172112728 TSecr=2395167594
     8 10.313601141  142.251.222.163      172.25.48.85         TCP          66 [TCP Dup ACK 2#1] 80 → 33934 [ACK] Seq=1 Ack=2 Win=1050 Len=0 TSval=2395177844 TSecr=1172051452
     9 11.249563915  142.250.77.234       172.25.48.85         TLSv1.2     151 Application Data
    10 11.249624899  172.25.48.85         142.250.77.234       TCP          66 42604 → 443 [ACK] Seq=1 Ack=86 Win=626 Len=0 TSval=958988933 TSecr=2708969038
    11 11.309475745  142.250.77.234       172.25.48.85         TCP         151 [TCP Spurious Retransmission] 443 → 42604 [PSH, ACK] Seq=1 Ack=1 Win=1018 Len=85 TSval=2708969382 TSecr=958967781
    12 11.309514887  172.25.48.85         142.250.77.234       TCP          78 [TCP Dup ACK 10#1] 42604 → 443 [ACK] Seq=1 Ack=86 Win=626 Len=0 TSval=958988993 TSecr=2708969382 SLE=1 SRE=86
    13 11.721925714  172.25.48.85         172.25.48.44         DNS          70 Standard query 0xc31a A google.com
    14 11.722468605  172.25.48.85         172.25.48.44         DNS          70 Standard query 0x5f25 AAAA google.com
    15 11.791037798  172.25.48.44         172.25.48.85         DNS          86 Standard query response 0xc31a A google.com A 142.251.43.206
    16 11.817231839  172.25.48.44         172.25.48.85         DNS          98 Standard query response 0x5f25 AAAA google.com AAAA 2404:6800:4002:81e::200e
    17 11.818220853  2409:40f3:1099:d227… 2404:6800:4002:81e:… ICMPv6      118 Echo (ping) request id=0x0006, seq=1, hop limit=254 (no response found!)
    18 12.833764380  2409:40f3:1099:d227… 2404:6800:4002:81e:… ICMPv6      118 Echo (ping) request id=0x0006, seq=2, hop limit=254 (no response found!)
    19 13.881721935  2409:40f3:1099:d227… 2404:6800:4002:81e:… ICMPv6      118 Echo (ping) request id=0x0006, seq=3, hop limit=254 (no response found!)
    20 14.611634960  172.25.48.85         142.250.76.67        TLSv1.2     168 Application Data
    21 14.749657972  142.250.76.67        172.25.48.85         TCP          66 443 → 56506 [ACK] Seq=1 Ack=103 Win=1044 Len=0 TSval=3792820962 TSecr=2075875410
    22 14.812428560  142.250.76.67        172.25.48.85         TLSv1.2     138 Application Data
    23 14.812429432  142.250.76.67        172.25.48.85         TLSv1.2     140 Application Data
    24 14.812429602  142.250.76.67        172.25.48.85         TLSv1.2      97 Application Data
    25 14.812429773  142.250.76.67        172.25.48.85         TLSv1.2     105 Application Data
```

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 46:ba:9f:6d:58:ae (46:ba:9f:6d:58:ae)
▸ Internet Protocol Version 4, Src: 172.25.48.85, Dst: 142.251.222.163
▸ Transmission Control Protocol, Src Port: 33934, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  46 ba 9f 6d 58 ae 08 00  27 d1 f8 5d 08 00 45 00   F·mX··· '··]··E·
0010  00 34 8c 85 40 00 40 06  64 31 ac 19 30 55 8e fb   ·4··@·@· d1··0U··
0020  de a3 84 8e 00 50 77 f2  6f 97 d7 be 14 7b 80 10   ·····Pw· o····{··
0030  01 ef 4a 34 00 00 01 01  08 0a 45 dc dd 58 8e c3   ··J4···· ··E··X··
0040  33 92                                              3·
```

eth0: <live capture in progress>   Packets: 77   Profile: Default

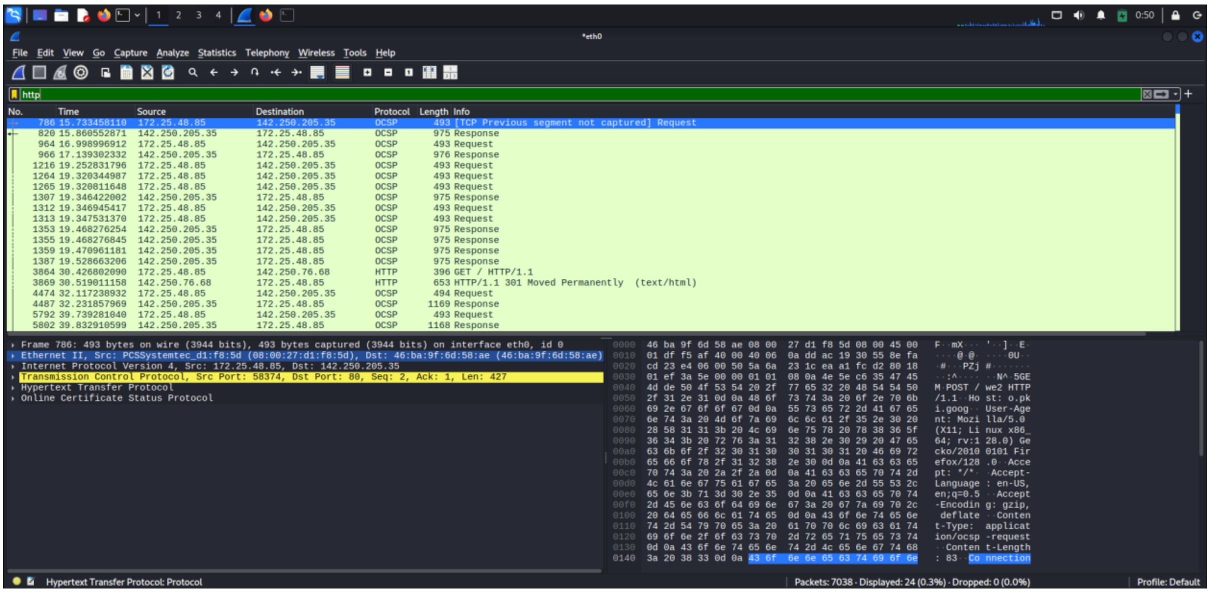
---

4. HTTP Traffic Analysis

Filter applied: http

Findings:

- Captured **HTTP GET** requests for web page retrieval.
- Detected **HTTP POST** requests, indicating data submission to servers.
- Server responses included status codes **200 OK** and **301 Moved Permanently**.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time          Source          Destination     Protocol  Length Info
   786 15.733458110  172.25.48.85    142.250.205.35  OCSP        493 [TCP Previous segment not captured] Request
   820 15.860552871  142.250.205.35  172.25.48.85    OCSP        975 Response
   964 16.998996912  172.25.48.85    142.250.205.35  OCSP        493 Request
   966 17.139302332  142.250.205.35  172.25.48.85    OCSP        976 Response
  1216 19.252831796  172.25.48.85    142.250.205.35  OCSP        493 Request
  1264 19.320344987  172.25.48.85    142.250.205.35  OCSP        493 Request
  1265 19.320811648  172.25.48.85    142.250.205.35  OCSP        493 Request
  1307 19.346422002  142.250.205.35  172.25.48.85    OCSP        975 Response
  1312 19.346945417  172.25.48.85    142.250.205.35  OCSP        493 Request
  1313 19.347531370  172.25.48.85    142.250.205.35  OCSP        493 Request
  1353 19.468276254  142.250.205.35  172.25.48.85    OCSP        975 Response
  1355 19.468276845  142.250.205.35  172.25.48.85    OCSP        975 Response
  1359 19.470961181  142.250.205.35  172.25.48.85    OCSP        975 Response
  1387 19.528663206  142.250.205.35  172.25.48.85    OCSP        975 Response
  3864 30.426802090  172.25.48.85    142.250.76.68   HTTP        396 GET / HTTP/1.1
  3869 30.519011158  142.250.76.68   172.25.48.85    HTTP        653 HTTP/1.1 301 Moved Permanently  (text/html)
  4474 32.117238932  172.25.48.85    142.250.205.35  OCSP        494 Request
  4487 32.231857969  142.250.205.35  172.25.48.85    OCSP       1169 Response
  5792 39.739281040  172.25.48.85    142.250.205.35  OCSP        493 Request
  5802 39.832910599  142.250.205.35  172.25.48.85    OCSP       1168 Response
```

```
▸ Frame 786: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 46:ba:9f:6d:58:ae (46:ba:9f:6d:58:ae)
▸ Internet Protocol Version 4, Src: 172.25.48.85, Dst: 142.250.205.35
▸ Transmission Control Protocol, Src Port: 58374, Dst Port: 80, Seq: 2, Ack: 1, Len: 427
▸ Hypertext Transfer Protocol
▸ Online Certificate Status Protocol
```

```
0000  46 ba 9f 6d 58 ae 08 00  27 d1 f8 5d 08 00 45 00   F·mX··· '··]··E·
0010  01 df f5 af 40 00 40 06  0a dd ac 19 30 55 8e fa   ····@·@· ····0U··
0020  cd 23 e4 06 00 50 5a 6a  23 1c ea a1 fc d2 80 18   ·#···PZj #·······
0030  01 ef 3a 5e 00 00 01 01  08 0a 4e 5e c6 35 47 45   ··:^···· ··N^·5GE
0040  4d de 50 4f 53 54 20 2f  77 65 32 20 48 54 54 50   M·POST / we2 HTTP
0050  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6f 2e 70 6b   /1.1··Ho st: o.pk
0060  69 2e 67 6f 6f 67 0d 0a  55 73 65 72 2d 41 67 65   i.goog·· User-Age
0070  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0
0080  28 58 31 31 3b 20 4c 69  6e 75 78 20 78 38 36 5f   (X11; Li nux x86_
0090  36 34 3b 20 72 76 3a 31  32 38 2e 30 29 20 47 65   64; rv:1 28.0) Ge
00a0  63 6b 6f 2f 32 30 31 30  30 31 30 31 20 46 69 72   cko/2010 0101 Fir
00b0  65 66 6f 78 2f 31 32 38  2e 30 0d 0a 41 63 63 65   efox/128 .0··Acce
00c0  70 74 3a 20 2a 2f 2a 0d  0a 41 63 63 65 70 74 2d   pt: */*· ·Accept-
00d0  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
00e0  65 6e 3b 71 3d 30 2e 35  0d 0a 41 63 63 65 70 74   en;q=0.5 ··Accept
00f0  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0100  20 64 65 66 6c 61 74 65  0d 0a 43 6f 6e 74 65 6e    deflate ··Conten
0110  74 2d 54 79 70 65 3a 20  61 70 70 6c 69 63 61 74   t-Type:  applicat
0120  69 6f 6e 2f 6f 63 73 70  2d 72 65 71 75 65 73 74   ion/ocsp -request
0130  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
0140  3a 20 38 33 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   : 83··Co nnection
```

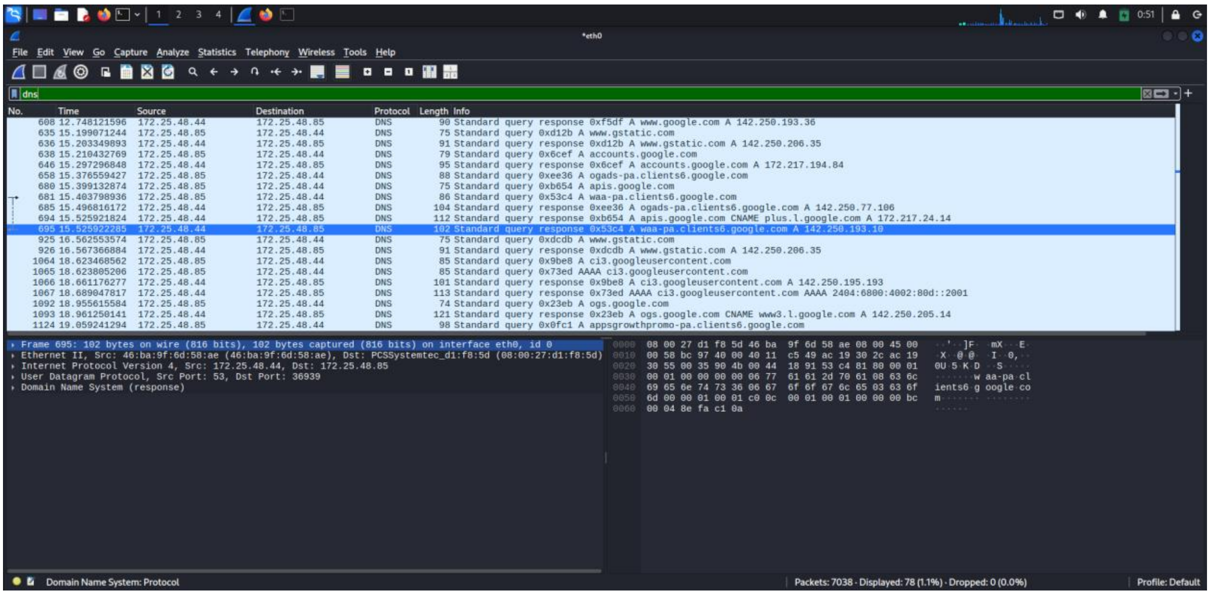
Hypertext Transfer Protocol: Protocol   Packets: 7038 · Displayed: 24 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

5. DNS Traffic Analysis

Filter applied: dns

Findings:

- Captured multiple **DNS queries** for various domains.
- Responses included both IPv4 (A) and IPv6 (AAAA) records.
- Query/response times were within normal range, indicating no DNS latency.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time            Source         Destination    Protocol Length Info
  608 12.748121596    172.25.48.44   172.25.48.85   DNS       90 Standard query response 0xf5df A www.google.com A 142.250.193.36
  635 15.199071244    172.25.48.85   172.25.48.44   DNS       75 Standard query 0xd12b A www.gstatic.com
  636 15.203349893    172.25.48.44   172.25.48.85   DNS       91 Standard query response 0xd12b A www.gstatic.com A 142.250.206.35
  638 15.210432769    172.25.48.85   172.25.48.44   DNS       79 Standard query 0x6cef A accounts.google.com
  646 15.297296848    172.25.48.44   172.25.48.85   DNS       95 Standard query response 0x6cef A accounts.google.com A 172.217.194.84
  658 15.376559427    172.25.48.85   172.25.48.44   DNS       88 Standard query 0xee36 A ogads-pa.clients6.google.com
  680 15.399132874    172.25.48.85   172.25.48.44   DNS       75 Standard query 0xb654 A apis.google.com
  681 15.403798936    172.25.48.85   172.25.48.44   DNS       86 Standard query 0x53c4 A waa-pa.clients6.google.com
  685 15.496816172    172.25.48.44   172.25.48.85   DNS      104 Standard query response 0xee36 A ogads-pa.clients6.google.com A 142.250.77.106
  694 15.525921824    172.25.48.44   172.25.48.85   DNS      112 Standard query response 0xb654 A apis.google.com CNAME plus.l.google.com A 172.217.24.14
  695 15.525922285    172.25.48.44   172.25.48.85   DNS      102 Standard query response 0x53c4 A waa-pa.clients6.google.com A 142.250.193.10
  925 16.562553574    172.25.48.85   172.25.48.44   DNS       75 Standard query 0xdcdb A www.gstatic.com
  926 16.567366884    172.25.48.44   172.25.48.85   DNS       91 Standard query response 0xdcdb A www.gstatic.com A 142.250.206.35
 1064 18.623468562    172.25.48.85   172.25.48.44   DNS       85 Standard query 0x9be8 A ci3.googleusercontent.com
 1065 18.623805206    172.25.48.85   172.25.48.44   DNS       85 Standard query 0x73ed AAAA ci3.googleusercontent.com
 1066 18.661176277    172.25.48.44   172.25.48.85   DNS      101 Standard query response 0x9be8 A ci3.googleusercontent.com A 142.250.195.193
 1067 18.689047817    172.25.48.44   172.25.48.85   DNS      113 Standard query response 0x73ed AAAA ci3.googleusercontent.com AAAA 2404:6800:4002:80d::2001
 1092 18.955615584    172.25.48.85   172.25.48.44   DNS       74 Standard query 0x23eb A ogs.google.com
 1093 18.961250141    172.25.48.44   172.25.48.85   DNS      121 Standard query response 0x23eb A ogs.google.com CNAME www3.l.google.com A 142.250.205.14
 1124 19.059241294    172.25.48.85   172.25.48.44   DNS       98 Standard query 0x0fc1 A appsgrowthpromo-pa.clients6.google.com
```

```
› Frame 695: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface eth0, id 0
› Ethernet II, Src: 46:ba:9f:6d:58:ae (46:ba:9f:6d:58:ae), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
› Internet Protocol Version 4, Src: 172.25.48.44, Dst: 172.25.48.85
› User Datagram Protocol, Src Port: 53, Dst Port: 36939
› Domain Name System (response)
```

```
0000  08 00 27 d1 f8 5d 46 ba  9f 6d 58 ae 08 00 45 00   ··'··]F· ·mX···E·
0010  00 58 bc 97 40 00 40 11  c5 49 ac 19 30 2c ac 19   ·X··@·@· ·I··0,··
0020  30 55 00 35 90 4b 00 44  18 91 53 c4 81 80 00 01   0U·5·K·D ··S·····
0030  00 01 00 00 00 00 06 77  61 61 2d 70 61 08 63 6c   ·······w aa-pa·cl
0040  69 65 6e 74 73 36 06 67  6f 6f 67 6c 65 03 63 6f   ients6·g oogle·co
0050  6d 00 00 01 00 01 c0 0c  00 01 00 01 00 00 00 bc   m······· ········
0060  00 04 8e fa c1 0a                                  ······
```

Domain Name System: Protocol | Packets: 7038 · Displayed: 78 (1.1%) · Dropped: 0 (0.0%) | Profile: Default

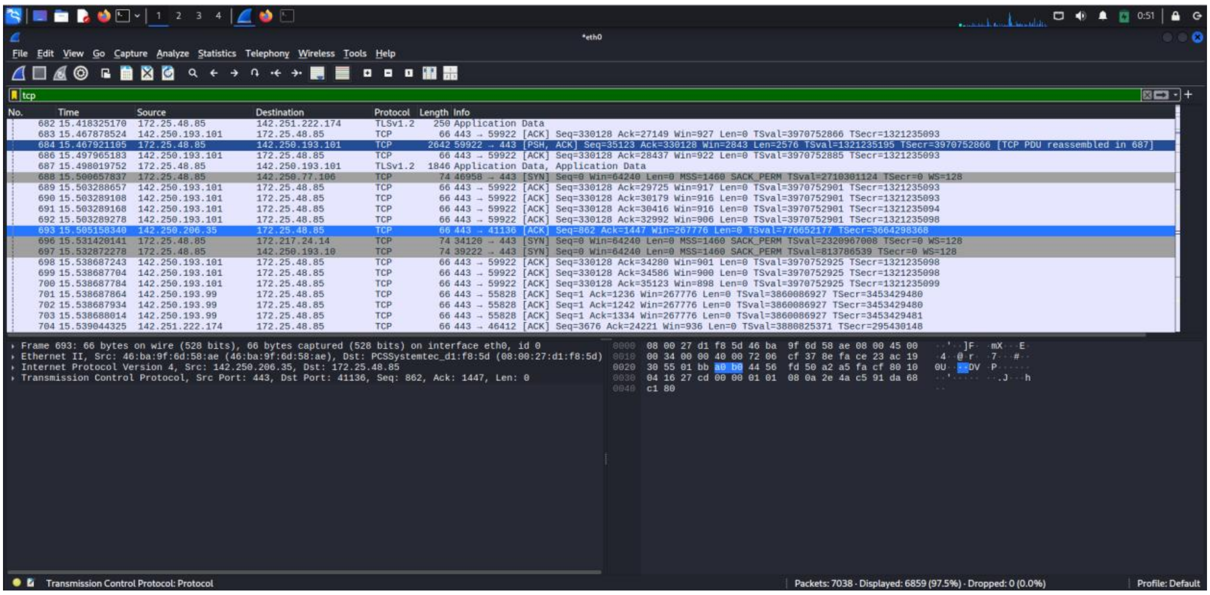
---

6. TCP Traffic Analysis

Filter applied: tcp

Findings:

- Observed **three-way handshakes** establishing TCP connections.
- Multiple TCP segments in both directions, confirming active communication.
- Sequence and acknowledgment numbers confirmed reliable delivery.



tcp

```
No.   Time         Source           Destination      Protocol Length Info
  682 15.418325170 172.25.48.85     142.251.222.174  TLSv1.2   250 Application Data
  683 15.467878524 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=27149 Win=927 Len=0 TSval=3970752866 TSecr=1321235093
  684 15.467921105 172.25.48.85     142.250.193.101  TCP      2642 59922 → 443 [PSH, ACK] Seq=35123 Ack=330128 Win=2843 Len=2576 TSval=1321235195 TSecr=3970752866 [TCP PDU reassembled in 687]
  686 15.497965183 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=28437 Win=922 Len=0 TSval=3970752885 TSecr=1321235093
  687 15.498019752 172.25.48.85     142.250.193.101  TLSv1.2  1846 Application Data, Application Data
  688 15.500657837 172.25.48.85     142.250.77.106   TCP        74 46958 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2710301124 TSecr=0 WS=128
  689 15.503288657 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=29725 Win=917 Len=0 TSval=3970752901 TSecr=1321235093
  690 15.503289108 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=30179 Win=916 Len=0 TSval=3970752901 TSecr=1321235093
  691 15.503289168 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=30416 Win=916 Len=0 TSval=3970752901 TSecr=1321235094
  692 15.503289278 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=32992 Win=906 Len=0 TSval=3970752901 TSecr=1321235098
  693 15.505158340 142.250.206.35   172.25.48.85     TCP        66 443 → 41136 [ACK] Seq=862 Ack=1447 Win=267776 Len=0 TSval=776652177 TSecr=3664298368
  696 15.531420141 172.25.48.85     172.217.24.14    TCP        74 34120 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2320967008 TSecr=0 WS=128
  697 15.532872278 172.25.48.85     142.250.193.10   TCP        74 39222 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=813786539 TSecr=0 WS=128
  698 15.538687243 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=34280 Win=901 Len=0 TSval=3970752925 TSecr=1321235098
  699 15.538687704 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=34586 Win=900 Len=0 TSval=3970752925 TSecr=1321235098
  700 15.538687784 142.250.193.101  172.25.48.85     TCP        66 443 → 59922 [ACK] Seq=330128 Ack=35123 Win=898 Len=0 TSval=3970752925 TSecr=1321235099
  701 15.538687864 142.250.193.99   172.25.48.85     TCP        66 443 → 55828 [ACK] Seq=1 Ack=1236 Win=267776 Len=0 TSval=3860086927 TSecr=3453429480
  702 15.538687934 142.250.193.99   172.25.48.85     TCP        66 443 → 55828 [ACK] Seq=1 Ack=1242 Win=267776 Len=0 TSval=3860086927 TSecr=3453429480
  703 15.538688014 142.250.193.99   172.25.48.85     TCP        66 443 → 55828 [ACK] Seq=1 Ack=1334 Win=267776 Len=0 TSval=3860086927 TSecr=3453429481
  704 15.539044325 142.251.222.174  172.25.48.85     TCP        66 443 → 46412 [ACK] Seq=3676 Ack=24221 Win=936 Len=0 TSval=3880825371 TSecr=295430148
```

```
› Frame 693: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
› Ethernet II, Src: 46:ba:9f:6d:58:ae (46:ba:9f:6d:58:ae), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
› Internet Protocol Version 4, Src: 142.250.206.35, Dst: 172.25.48.85
› Transmission Control Protocol, Src Port: 443, Dst Port: 41136, Seq: 862, Ack: 1447, Len: 0
```

```
0000  08 00 27 d1 f8 5d 46 ba  9f 6d 58 ae 08 00 45 00   ··'··]F· ·mX···E·
0010  00 34 00 00 40 00 72 06  cf 37 8e fa ce 23 ac 19   ·4··@·r· ·7···#··
0020  30 55 01 bb a0 b0 44 56  fd 50 a2 a5 fa cf 80 10   0U····DV ·P······
0030  04 16 27 cd 00 00 01 01  08 0a 2e 4a c5 91 da 68   ··'····· ···.J···h
0040  c1 80                                              ··
```

Transmission Control Protocol: Protocol | Packets: 7038 · Displayed: 6859 (97.5%) · Dropped: 0 (0.0%) | Profile: Default

8. Conclusion

The packet capture confirms active multi-protocol communication on the network.

Key points:

- **HTTP** requests and redirects occurred during normal browsing.
- **DNS** lookups resolved domains without delays.
- **TCP** traffic showed healthy connection establishment and packet exchange.