Network Traffic Capture and Protocol Analysis

This report documents the capture and analysis of live network traffic using Wireshark. It identifies key protocols observed during the capture and provides packet-level observations that demonstrate typical network behavior.

Tools & Resources Used

- Wireshark (for capturing and analyzing network packets).
- Active Ethernet/Wi■Fi network adapter to monitor traffic.
- Internet connection used to generate live traffic during capture.

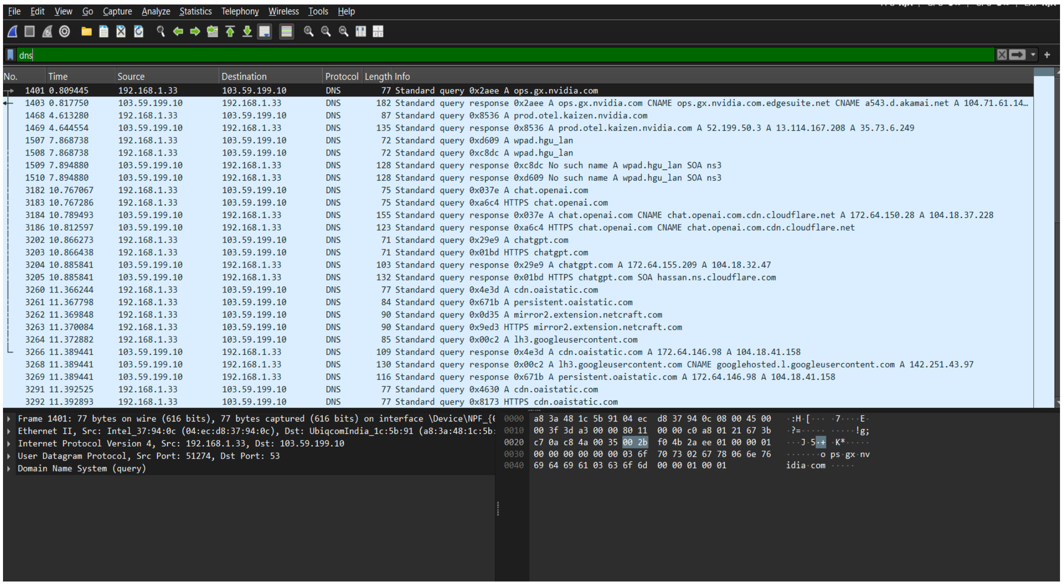
Procedure

1. Installed and launched Wireshark with necessary privileges.
2. Selected the active network interface and started packet capture.
3. Generated traffic by browsing and pinging external servers for ~1 minute.
4. Stopped the capture and applied filters (tcp, udp, dns) to focus analysis.
5. Saved the capture as a .pcap file for submission.

Findings & Analysis

TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol that ensures reliable data delivery. Observed a TLSv1.2 session over TCP between the local host (192.168.1.33) and a remote server (163.70.143.60) on port 443. The capture shows the expected three-way handshake (SYN, SYN-ACK, ACK) and subsequent encrypted application data frames.



```
dns
```

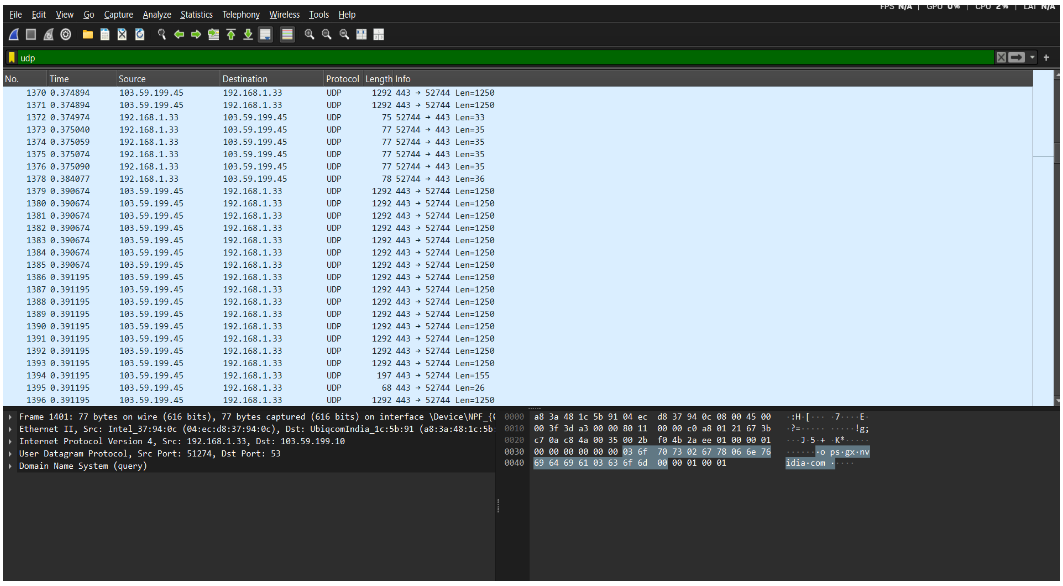
```
No.   Time      Source         Destination    Protocol Length Info
 1401 0.809445  192.168.1.33   103.59.199.10  DNS       77 Standard query 0x2aee A ops.gx.nvidia.com
 1403 0.817750  103.59.199.10  192.168.1.33   DNS      182 Standard query response 0x2aee A ops.gx.nvidia.com CNAME ops.gx.nvidia.com.edgesuite.net CNAME a543.d.akamai.net A 104.71.61.14…
 1468 4.613280  192.168.1.33   103.59.199.10  DNS       87 Standard query 0x8536 A prod.otel.kaizen.nvidia.com
 1469 4.644554  103.59.199.10  192.168.1.33   DNS      135 Standard query response 0x8536 A prod.otel.kaizen.nvidia.com A 52.199.50.3 A 13.114.167.208 A 35.73.6.249
 1507 7.868738  192.168.1.33   103.59.199.10  DNS       72 Standard query 0xd609 A wpad.hgu_lan
 1508 7.868738  192.168.1.33   103.59.199.10  DNS       72 Standard query 0xc8dc A wpad.hgu_lan
 1509 7.894880  103.59.199.10  192.168.1.33   DNS      128 Standard query response 0xc8dc No such name A wpad.hgu_lan SOA ns3
 1510 7.894880  103.59.199.10  192.168.1.33   DNS      128 Standard query response 0xd609 No such name A wpad.hgu_lan SOA ns3
 3182 10.767067 192.168.1.33   103.59.199.10  DNS       75 Standard query 0x037e A chat.openai.com
 3183 10.767286 192.168.1.33   103.59.199.10  DNS       75 Standard query 0xa6c4 HTTPS chat.openai.com
 3184 10.789493 103.59.199.10  192.168.1.33   DNS      155 Standard query response 0x037e A chat.openai.com CNAME chat.openai.com.cdn.cloudflare.net A 172.64.150.28 A 104.18.37.228
 3186 10.812597 103.59.199.10  192.168.1.33   DNS      123 Standard query response 0xa6c4 HTTPS chat.openai.com CNAME chat.openai.com.cdn.cloudflare.net
 3202 10.866273 192.168.1.33   103.59.199.10  DNS       71 Standard query 0x29e9 A chatgpt.com
 3203 10.866438 192.168.1.33   103.59.199.10  DNS       71 Standard query 0x01bd HTTPS chatgpt.com
 3204 10.885841 103.59.199.10  192.168.1.33   DNS      103 Standard query response 0x29e9 A chatgpt.com A 172.64.155.209 A 104.18.32.47
 3205 10.885841 103.59.199.10  192.168.1.33   DNS      132 Standard query response 0x01bd HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
 3260 11.366244 192.168.1.33   103.59.199.10  DNS       77 Standard query 0x4e3d A cdn.oaistatic.com
 3261 11.367798 192.168.1.33   103.59.199.10  DNS       84 Standard query 0x671b A persistent.oaistatic.com
 3262 11.369848 192.168.1.33   103.59.199.10  DNS       90 Standard query 0x0d35 A mirror2.extension.netcraft.com
 3263 11.370084 192.168.1.33   103.59.199.10  DNS       90 Standard query 0x9ed3 HTTPS mirror2.extension.netcraft.com
 3264 11.372882 192.168.1.33   103.59.199.10  DNS       85 Standard query 0x00c2 A lh3.googleusercontent.com
 3266 11.389441 103.59.199.10  192.168.1.33   DNS      109 Standard query response 0x4e3d A cdn.oaistatic.com A 172.64.146.98 A 104.18.41.158
 3268 11.389441 103.59.199.10  192.168.1.33   DNS      130 Standard query response 0x00c2 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.251.43.97
 3269 11.389441 103.59.199.10  192.168.1.33   DNS      116 Standard query response 0x671b A persistent.oaistatic.com A 172.64.146.98 A 104.18.41.158
 3291 11.392525 192.168.1.33   103.59.199.10  DNS       77 Standard query 0x4630 A cdn.oaistatic.com
 3292 11.392893 192.168.1.33   103.59.199.10  DNS       77 Standard query 0x8173 HTTPS cdn.oaistatic.com
```

```
› Frame 1401: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{(
› Ethernet II, Src: Intel_37:94:0c (04:ec:d8:37:94:0c), Dst: UbiqcomIndia_1c:5b:91 (a8:3a:48:1c:5b:
› Internet Protocol Version 4, Src: 192.168.1.33, Dst: 103.59.199.10
› User Datagram Protocol, Src Port: 51274, Dst Port: 53
› Domain Name System (query)
```

```
0000  a8 3a 48 1c 5b 91 04 ec  d8 37 94 0c 08 00 45 00   ·:H·[··· ·7····E·
0010  00 3f 3d a3 00 00 80 11  00 00 c0 a8 01 21 67 3b   ·?=····· ·····!g;
0020  c7 0a c8 4a 00 35 00 2b  f0 4b 2a ee 01 00 00 01   ···J·5·+ ·K*·····
0030  00 00 00 00 00 00 03 6f  70 73 02 67 78 06 6e 76   ·······o ps·gx·nv
0040  69 64 69 61 03 63 6f 6d  00 00 01 00 01            idia·com ·····
```

UDP (User Datagram Protocol)

UDP is a connectionless protocol used for low-latency transmissions. The capture includes repetitive UDP packets between the remote host 103.59.199.45 and the local machine 192.168.1.33, some of which are related to quick query/response traffic.



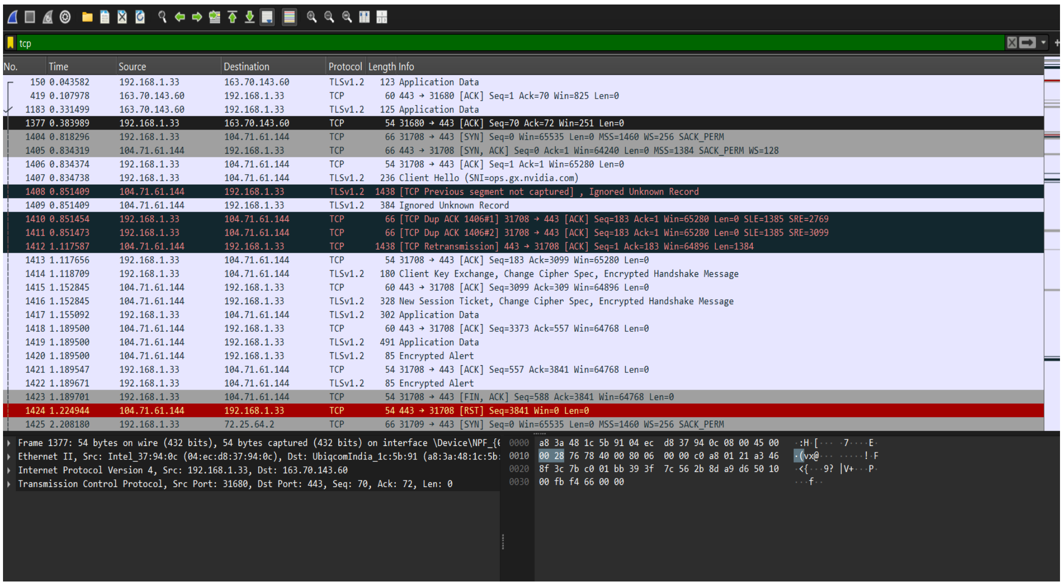
```
No.  Time     Source         Destination    Protocol Length Info
1370 0.374894 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1371 0.374894 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1372 0.374974 192.168.1.33   103.59.199.45  UDP        75 52744 → 443 Len=33
1373 0.375040 192.168.1.33   103.59.199.45  UDP        77 52744 → 443 Len=35
1374 0.375059 192.168.1.33   103.59.199.45  UDP        77 52744 → 443 Len=35
1375 0.375074 192.168.1.33   103.59.199.45  UDP        77 52744 → 443 Len=35
1376 0.375090 192.168.1.33   103.59.199.45  UDP        77 52744 → 443 Len=35
1378 0.384077 192.168.1.33   103.59.199.45  UDP        78 52744 → 443 Len=36
1379 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1380 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1381 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1382 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1383 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1384 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1385 0.390674 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1386 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1387 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1388 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1389 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1390 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1391 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1392 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1393 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
1394 0.391195 103.59.199.45  192.168.1.33   UDP       197 443 → 52744 Len=155
1395 0.391195 103.59.199.45  192.168.1.33   UDP        68 443 → 52744 Len=26
1396 0.391195 103.59.199.45  192.168.1.33   UDP      1292 443 → 52744 Len=1250
```

```
Frame 1401: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{(
Ethernet II, Src: Intel_37:94:0c (04:ec:d8:37:94:0c), Dst: UbiqcomIndia_1c:5b:91 (a8:3a:48:1c:5b:
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 103.59.199.10
User Datagram Protocol, Src Port: 51274, Dst Port: 53
Domain Name System (query)
```

```
0000  a8 3a 48 1c 5b 91 04 ec  d8 37 94 0c 08 00 45 00   ·:H·[···  ·7····E·
0010  00 3f 3d a3 00 00 80 11  00 00 c0 a8 01 21 67 3b   ·?=·····  ·····!g;
0020  c7 0a c8 4a 00 35 00 2b  f0 4b 2a ee 01 00 00 01   ···J·5·+  ·K*·····
0030  00 00 00 00 00 00 03 6f  70 73 02 67 78 06 6e 76   ·······o ps·gx·nv
0040  69 64 69 61 03 63 6f 6d  00 00 01 00 01            idia·com ·····
```

DNS (Domain Name System)

DNS resolves domain names to IP addresses. The capture shows queries from 192.168.1.33 to a DNS resolver (103.59.199.10) for domains such as chat.openai.com, ops.gx.nvidia.com, and cdn.oai-static.com. Responses included A and CNAME records.



```
No.  Time     Source         Destination    Protocol Length Info
 150 0.043582 192.168.1.33   163.70.143.60  TLSv1.2   123 Application Data
 419 0.107978 163.70.143.60  192.168.1.33   TCP        60 443 → 31680 [ACK] Seq=1 Ack=70 Win=825 Len=0
1183 0.331499 163.70.143.60  192.168.1.33   TLSv1.2   125 Application Data
1377 0.383989 192.168.1.33   163.70.143.60  TCP        54 31680 → 443 [ACK] Seq=70 Ack=72 Win=251 Len=0
1404 0.818296 192.168.1.33   104.71.61.144  TCP        66 31708 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1405 0.834319 104.71.61.144  192.168.1.33   TCP        66 443 → 31708 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
1406 0.834374 192.168.1.33   104.71.61.144  TCP        54 31708 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1407 0.834738 192.168.1.33   104.71.61.144  TLSv1.2   236 Client Hello (SNI=ops.gx.nvidia.com)
1408 0.851409 104.71.61.144  192.168.1.33   TLSv1.2  1438 [TCP Previous segment not captured] , Ignored Unknown Record
1409 0.851409 104.71.61.144  192.168.1.33   TLSv1.2   384 Ignored Unknown Record
1410 0.851454 192.168.1.33   104.71.61.144  TCP        66 [TCP Dup ACK 1406#1] 31708 → 443 [ACK] Seq=183 Ack=1 Win=65280 Len=0 SLE=1385 SRE=2769
1411 0.851473 192.168.1.33   104.71.61.144  TCP        66 [TCP Dup ACK 1406#2] 31708 → 443 [ACK] Seq=183 Ack=1 Win=65280 Len=0 SLE=1385 SRE=3099
1412 1.117587 104.71.61.144  192.168.1.33   TCP      1438 [TCP Retransmission] 443 → 31708 [ACK] Seq=1 Ack=183 Win=64896 Len=1384
1413 1.117656 192.168.1.33   104.71.61.144  TCP        54 31708 → 443 [ACK] Seq=183 Ack=3099 Win=65280 Len=0
1414 1.118709 192.168.1.33   104.71.61.144  TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1415 1.152845 104.71.61.144  192.168.1.33   TCP        60 443 → 31708 [ACK] Seq=3099 Ack=309 Win=64896 Len=0
1416 1.152845 104.71.61.144  192.168.1.33   TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1417 1.155092 192.168.1.33   104.71.61.144  TLSv1.2   302 Application Data
1418 1.189500 104.71.61.144  192.168.1.33   TCP        60 443 → 31708 [ACK] Seq=3373 Ack=557 Win=64768 Len=0
1419 1.189500 104.71.61.144  192.168.1.33   TLSv1.2   491 Application Data
1420 1.189500 104.71.61.144  192.168.1.33   TLSv1.2    85 Encrypted Alert
1421 1.189547 192.168.1.33   104.71.61.144  TCP        54 31708 → 443 [ACK] Seq=557 Ack=3841 Win=64768 Len=0
1422 1.189671 192.168.1.33   104.71.61.144  TLSv1.2    85 Encrypted Alert
1423 1.189701 192.168.1.33   104.71.61.144  TCP        54 31708 → 443 [FIN, ACK] Seq=588 Ack=3841 Win=64768 Len=0
1424 1.224944 104.71.61.144  192.168.1.33   TCP        54 443 → 31708 [RST] Seq=3841 Win=0 Len=0
1425 2.208180 192.168.1.33   72.25.64.2     TCP        66 31709 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
Frame 1377: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{(
Ethernet II, Src: Intel_37:94:0c (04:ec:d8:37:94:0c), Dst: UbiqcomIndia_1c:5b:91 (a8:3a:48:1c:5b:
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 163.70.143.60
Transmission Control Protocol, Src Port: 31680, Dst Port: 443, Seq: 70, Ack: 72, Len: 0
```

```
0000  a8 3a 48 1c 5b 91 04 ec  d8 37 94 0c 08 00 45 00   ·:H·[···  ·7····E·
0010  00 28 76 78 40 00 80 06  00 00 c0 a8 01 21 a3 46   ·(vx@···  ·····!·F
0020  8f 3c 7b c0 01 bb 39 3f  7c 56 2b 8d a9 d6 50 10   ·<{···9?  |V+···P·
0030  00 fb f4 66 00 00                                  ···f··
```

Conclusion

The capture demonstrates how TCP, UDP, and DNS operate together during normal internet activity: DNS resolves names, UDP handles lightweight/fast exchanges, and TCP carries reliable, often encrypted, sessions. The .pcap file captures these interactions and can be reviewed for deeper packet-level analysis.