Wireshark Packet Capture Report

Introduction

This report summarizes the findings from a packet capture performed using Wireshark. The objective of this task was to capture live network packets, identify the protocols in use, and analyze their roles in network communication.

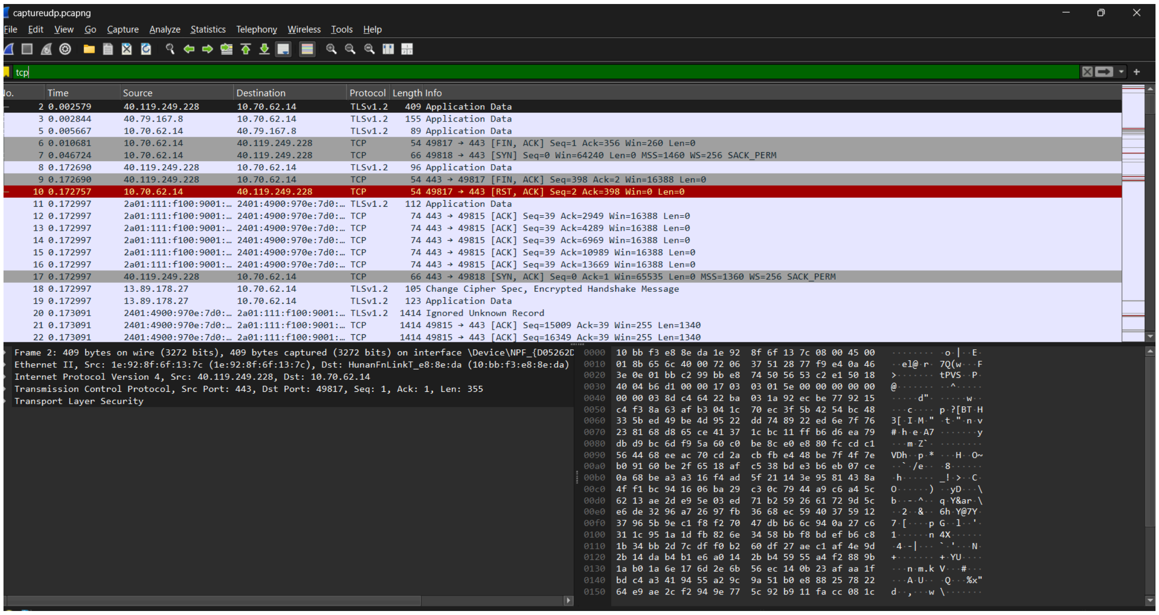
Capture Summary

The packet capture was performed on the active network interface while browsing websites and running basic commands to generate traffic. The capture lasted approximately one minute and was saved as a .pcap file.

Protocols Observed

1. TCP (Transmission Control Protocol)

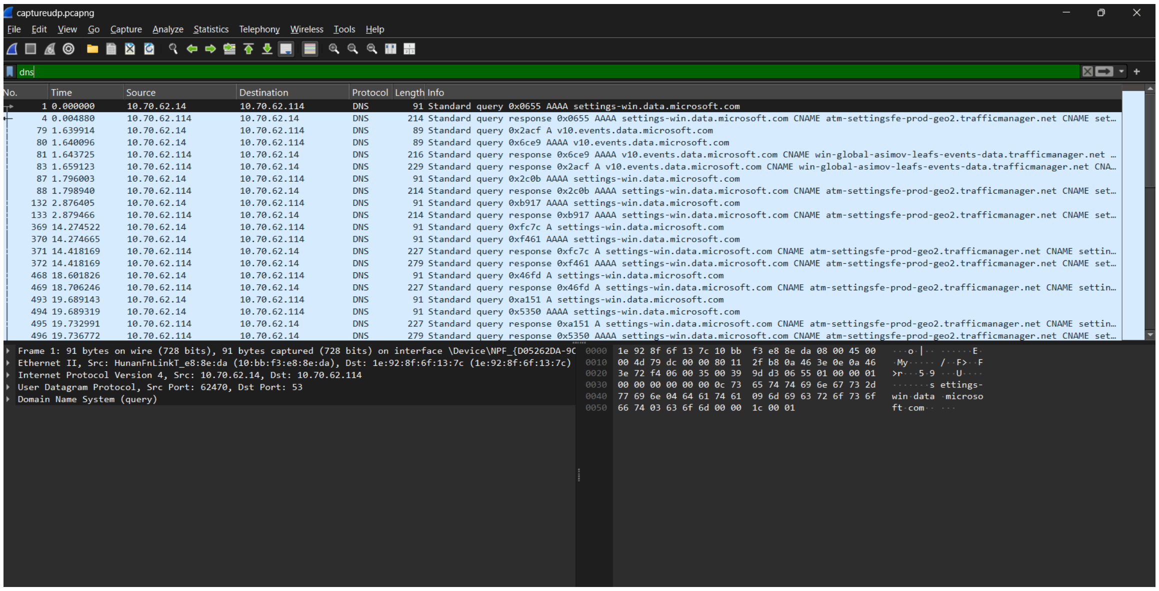
TCP appeared frequently in the capture. It acts as the delivery service of the internet, ensuring that data arrives reliably and in the correct order. For example, when accessing websites, TCP handled the transfer of webpage content between the client and the server.


captureudp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.  Time      Source                Destination           Protocol Length Info
   2 0.002579  40.119.249.228        10.70.62.14           TLSv1.2   409 Application Data
   3 0.002844  40.79.167.8           10.70.62.14           TLSv1.2   155 Application Data
   5 0.005667  10.70.62.14           40.79.167.8           TLSv1.2    89 Application Data
   6 0.010681  10.70.62.14           40.119.249.228        TCP        54 49817 → 443 [FIN, ACK] Seq=1 Ack=356 Win=260 Len=0
   7 0.046724  10.70.62.14           40.119.249.228        TCP        66 49818 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   8 0.172690  40.119.249.228        10.70.62.14           TLSv1.2    96 Application Data
   9 0.172690  40.119.249.228        10.70.62.14           TCP        54 443 → 49817 [FIN, ACK] Seq=398 Ack=2 Win=16388 Len=0
  10 0.172757  10.70.62.14           40.119.249.228        TCP        54 49817 → 443 [RST, ACK] Seq=2 Ack=398 Win=0 Len=0
  11 0.172997  2a01:111:f100:9001:…  2401:4900:970e:7d0:…  TLSv1.2   112 Application Data
  12 0.172997  2a01:111:f100:9001:…  2401:4900:970e:7d0:…  TCP        74 443 → 49815 [ACK] Seq=39 Ack=2949 Win=16388 Len=0
  13 0.172997  2a01:111:f100:9001:…  2401:4900:970e:7d0:…  TCP        74 443 → 49815 [ACK] Seq=39 Ack=4289 Win=16388 Len=0
  14 0.172997  2a01:111:f100:9001:…  2401:4900:970e:7d0:…  TCP        74 443 → 49815 [ACK] Seq=39 Ack=6969 Win=16388 Len=0
  15 0.172997  2a01:111:f100:9001:…  2401:4900:970e:7d0:…  TCP        74 443 → 49815 [ACK] Seq=39 Ack=10989 Win=16388 Len=0
  16 0.172997  2a01:111:f100:9001:…  2401:4900:970e:7d0:…  TCP        74 443 → 49815 [ACK] Seq=39 Ack=13669 Win=16388 Len=0
  17 0.172997  40.119.249.228        10.70.62.14           TCP        66 443 → 49818 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=256 SACK_PERM
  18 0.172997  13.89.178.27          10.70.62.14           TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  19 0.172997  13.89.178.27          10.70.62.14           TLSv1.2   123 Application Data
  20 0.173091  2401:4900:970e:7d0:…  2a01:111:f100:9001:…  TLSv1.2  1414 Ignored Unknown Record
  21 0.173091  2401:4900:970e:7d0:…  2a01:111:f100:9001:…  TCP      1414 49815 → 443 [ACK] Seq=15009 Ack=39 Win=255 Len=1340
  22 0.173091  2401:4900:970e:7d0:…  2a01:111:f100:9001:…  TCP      1414 49815 → 443 [ACK] Seq=16349 Ack=39 Win=255 Len=1340

Frame 2: 409 bytes on wire (3272 bits), 409 bytes captured (3272 bits) on interface \Device\NPF_{D05262D
Ethernet II, Src: 1e:92:8f:6f:13:7c (1e:92:8f:6f:13:7c), Dst: HunanFnLinkT_e8:8e:da (10:bb:f3:e8:8e:da)
Internet Protocol Version 4, Src: 40.119.249.228, Dst: 10.70.62.14
Transmission Control Protocol, Src Port: 443, Dst Port: 49817, Seq: 1, Ack: 1, Len: 355
Transport Layer Security

0000  10 bb f3 e8 8e da 1e 92  8f 6f 13 7c 08 00 45 00   ········ ·o·|··E·
0010  01 8b 65 6c 40 00 72 06  37 51 28 77 f9 e4 0a 46   ··el@·r· 7Q(w···F
0020  3e 0e 01 bb c2 99 bb e8  74 50 56 53 c2 e1 50 18   >······· tPVS··P·
0030  40 04 b6 d1 00 00 17 03  03 01 5e 00 00 00 00 00   @······· ··^·····
0040  00 00 03 8d c4 64 22 ba  03 1a 92 ec be 77 92 15   ·····d"· ·····w··
0050  c4 f3 8a 63 af b3 04 1c  70 ec 3f 5b 42 54 bc 48   ···c···· p·?[BT·H
0060  33 5b ed 49 be 4d 95 22  dd 74 89 22 ed 6e 7f 76   3[·I·M·" ·t·"·n·v
0070  23 81 68 d8 65 ce 41 37  1c bc 11 ff b6 d6 ea 79   #·h·e·A7 ·······y
0080  db d9 bc 6d f9 5a 60 c0  be 8c e0 e8 80 fc cd c1   ···m·Z`· ········
0090  56 44 68 ee ac 70 cd 2a  cb fb e4 48 be 7f 4f 7e   VDh··p·* ···H··O~
00a0  b0 91 60 be 2f 65 18 af  c5 38 bd e3 b6 eb 07 ce   ··`·/e·· ·8······
00b0  0a 68 be a3 a3 16 f4 ad  5f 21 14 3e 95 81 43 8a   ·h······ _!·>··C·
00c0  4f f1 bc 94 16 06 ba 29  c3 0c 79 44 a9 c6 a4 5c   O······) ··yD···\
00d0  62 13 ae 2d e9 5e 03 ed  71 b2 59 26 61 72 9d 5c   b··-·^·· q·Y&ar·\
00e0  e6 de 32 96 a7 26 97 fb  36 68 ec 59 40 37 59 12   ··2··&·· 6h·Y@7Y·
00f0  37 96 5b 9e c1 f8 f2 70  47 db b6 6c 94 0a 27 c6   7·[····p G··l··'·
0100  31 1c 95 1a 1d fb 82 6e  34 58 bb f8 bd ef b6 c8   1······n 4X······
0110  1b 34 bb 2d 7c df f0 b2  60 df 27 ae c1 af 4e 9d   ·4·-|··· `·'···N·
0120  2b 14 da b4 b1 e6 a0 14  2b b4 59 55 a4 f2 88 9b   +······· +·YU····
0130  1a b0 1a 6e 17 6d 2e 6b  56 ec 14 0b 23 af aa 1f   ···n·m.k V···#···
0140  bd c4 a3 41 94 55 a2 9c  9a 51 b0 e8 88 25 78 22   ···A·U·· ·Q···%x"
0150  64 e9 ae 2c f2 94 9e 77  5c 92 b9 11 fa cc 08 1c   d··,···w \·······
```

2. DNS (Domain Name System)

DNS queries were visible in the capture whenever a website was visited. DNS functions like the phone book of the internet, translating human-readable names (e.g., google.com) into IP addresses that computers can use. This allows users to connect to websites without needing to remember numerical IP addresses.


captureudp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

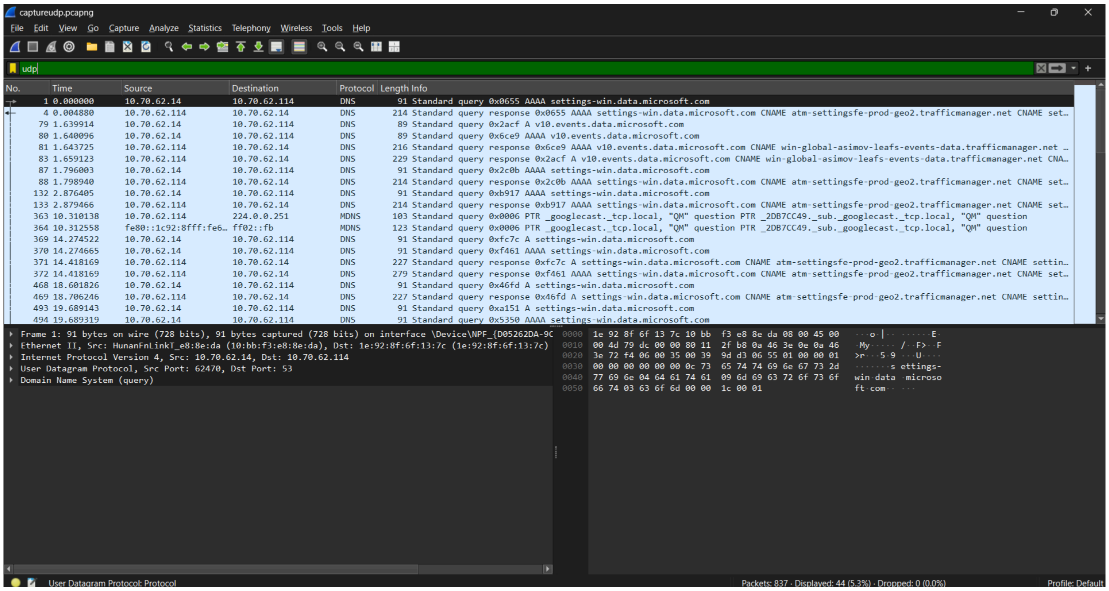
```
No.   Time       Source        Destination   Protocol Length Info
    1 0.000000   10.70.62.14   10.70.62.114  DNS       91 Standard query 0x0655 AAAA settings-win.data.microsoft.com
    4 0.004880   10.70.62.114  10.70.62.14   DNS      214 Standard query response 0x0655 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
   79 1.639914   10.70.62.14   10.70.62.114  DNS       89 Standard query 0x2acf A v10.events.data.microsoft.com
   80 1.640096   10.70.62.14   10.70.62.114  DNS       89 Standard query 0x6ce9 AAAA v10.events.data.microsoft.com
   81 1.643725   10.70.62.114  10.70.62.14   DNS      216 Standard query response 0x6ce9 AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net …
   83 1.659123   10.70.62.114  10.70.62.14   DNS      229 Standard query response 0x2acf A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNA…
   87 1.796003   10.70.62.14   10.70.62.114  DNS       91 Standard query 0x2c0b AAAA settings-win.data.microsoft.com
   88 1.798940   10.70.62.114  10.70.62.14   DNS      214 Standard query response 0x2c0b AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
  132 2.876405   10.70.62.14   10.70.62.114  DNS       91 Standard query 0xb917 AAAA settings-win.data.microsoft.com
  133 2.879466   10.70.62.114  10.70.62.14   DNS      214 Standard query response 0xb917 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
  369 14.274522  10.70.62.14   10.70.62.114  DNS       91 Standard query 0xfc7c A settings-win.data.microsoft.com
  370 14.274665  10.70.62.14   10.70.62.114  DNS       91 Standard query 0xf461 AAAA settings-win.data.microsoft.com
  371 14.418169  10.70.62.114  10.70.62.14   DNS      227 Standard query response 0xfc7c A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
  372 14.418169  10.70.62.114  10.70.62.14   DNS      279 Standard query response 0xf461 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
  468 18.601826  10.70.62.14   10.70.62.114  DNS       91 Standard query 0x46fd A settings-win.data.microsoft.com
  469 18.706246  10.70.62.114  10.70.62.14   DNS      227 Standard query response 0x46fd A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
  493 19.689143  10.70.62.14   10.70.62.114  DNS       91 Standard query 0xa151 A settings-win.data.microsoft.com
  494 19.689319  10.70.62.14   10.70.62.114  DNS       91 Standard query 0x5350 AAAA settings-win.data.microsoft.com
  495 19.732991  10.70.62.114  10.70.62.14   DNS      227 Standard query response 0xa151 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
  496 19.736772  10.70.62.114  10.70.62.14   DNS      279 Standard query response 0x5350 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
```

```
Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{D05262DA-9C
Ethernet II, Src: HunanFnLinkT_e8:8e:da (10:bb:f3:e8:8e:da), Dst: 1e:92:8f:6f:13:7c (1e:92:8f:6f:13:7c)
Internet Protocol Version 4, Src: 10.70.62.14, Dst: 10.70.62.114
User Datagram Protocol, Src Port: 62470, Dst Port: 53
Domain Name System (query)
```

```
0000  1e 92 8f 6f 13 7c 10 bb  f3 e8 8e da 08 00 45 00   ···o·|·· ······E·
0010  00 4d 79 dc 00 00 80 11  2f b8 0a 46 3e 0e 0a 46   ·My····· /··F>··F
0020  3e 72 f4 06 00 35 00 39  9d d3 06 55 01 00 00 01   >r···5·9 ···U····
0030  00 00 00 00 00 00 0c 73  65 74 74 69 6e 67 73 2d   ·······s ettings-
0040  77 69 6e 04 64 61 74 61  09 6d 69 63 72 6f 73 6f   win·data ·microso
0050  66 74 03 63 6f 6d 00 00  1c 00 01                  ft·com·· ···
```

3. HTTP (Hypertext Transfer Protocol)

HTTP packets were observed when browsing websites. HTTP is the protocol responsible for transferring web pages, images, and other resources from a web server to the browser. In simple terms, it is the language that browsers and servers use to communicate.


captureudp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.   Time       Source                Destination   Protocol Length Info
    1 0.000000   10.70.62.14           10.70.62.114  DNS       91 Standard query 0x0655 AAAA settings-win.data.microsoft.com
    4 0.004880   10.70.62.114          10.70.62.14   DNS      214 Standard query response 0x0655 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
   79 1.639914   10.70.62.14           10.70.62.114  DNS       89 Standard query 0x2acf A v10.events.data.microsoft.com
   80 1.640096   10.70.62.14           10.70.62.114  DNS       89 Standard query 0x6ce9 AAAA v10.events.data.microsoft.com
   81 1.643725   10.70.62.114          10.70.62.14   DNS      216 Standard query response 0x6ce9 AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net …
   83 1.659123   10.70.62.114          10.70.62.14   DNS      229 Standard query response 0x2acf A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNA…
   87 1.796003   10.70.62.14           10.70.62.114  DNS       91 Standard query 0x2c0b AAAA settings-win.data.microsoft.com
   88 1.798940   10.70.62.114          10.70.62.14   DNS      214 Standard query response 0x2c0b AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
  132 2.876405   10.70.62.14           10.70.62.114  DNS       91 Standard query 0xb917 AAAA settings-win.data.microsoft.com
  133 2.879466   10.70.62.114          10.70.62.14   DNS      214 Standard query response 0xb917 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
  363 10.310138  10.70.62.114          224.0.0.251   MDNS     103 Standard query 0x0006 PTR _googlecast._tcp.local, "QM" question PTR _2DB7CC49._sub._googlecast._tcp.local, "QM" question
  364 10.312558  fe80::1c92:8fff:fe6…  ff02::fb      MDNS     123 Standard query 0x0006 PTR _googlecast._tcp.local, "QM" question PTR _2DB7CC49._sub._googlecast._tcp.local, "QM" question
  369 14.274522  10.70.62.14           10.70.62.114  DNS       91 Standard query 0xfc7c A settings-win.data.microsoft.com
  370 14.274665  10.70.62.14           10.70.62.114  DNS       91 Standard query 0xf461 AAAA settings-win.data.microsoft.com
  371 14.418169  10.70.62.114          10.70.62.14   DNS      227 Standard query response 0xfc7c A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
  372 14.418169  10.70.62.114          10.70.62.14   DNS      279 Standard query response 0xf461 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set…
  468 18.601826  10.70.62.14           10.70.62.114  DNS       91 Standard query 0x46fd A settings-win.data.microsoft.com
  469 18.706246  10.70.62.114          10.70.62.14   DNS      227 Standard query response 0x46fd A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
  493 19.689143  10.70.62.14           10.70.62.114  DNS       91 Standard query 0xa151 A settings-win.data.microsoft.com
  494 19.689319  10.70.62.14           10.70.62.114  DNS       91 Standard query 0x5350 AAAA settings-win.data.microsoft.com
```

```
Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{D05262DA-9C
Ethernet II, Src: HunanFnLinkT_e8:8e:da (10:bb:f3:e8:8e:da), Dst: 1e:92:8f:6f:13:7c (1e:92:8f:6f:13:7c)
Internet Protocol Version 4, Src: 10.70.62.14, Dst: 10.70.62.114
User Datagram Protocol, Src Port: 62470, Dst Port: 53
Domain Name System (query)
```

```
0000  1e 92 8f 6f 13 7c 10 bb  f3 e8 8e da 08 00 45 00   ···o·|·· ······E·
0010  00 4d 79 dc 00 00 80 11  2f b8 0a 46 3e 0e 0a 46   ·My····· /··F>··F
0020  3e 72 f4 06 00 35 00 39  9d d3 06 55 01 00 00 01   >r···5·9 ···U····
0030  00 00 00 00 00 00 0c 73  65 74 74 69 6e 67 73 2d   ·······s ettings-
0040  77 69 6e 04 64 61 74 61  09 6d 69 63 72 6f 73 6f   win·data ·microso
0050  66 74 03 63 6f 6d 00 00  1c 00 01                  ft·com·· ···
```

```
User Datagram Protocol: Protocol          Packets: 837 · Displayed: 44 (5.3%) · Dropped: 0 (0.0%)          Profile: Default
```

Conclusion

The packet capture demonstrated the use of multiple protocols working together to enable everyday internet activities. TCP provided reliable data transfer, DNS resolved domain names to IP addresses, and HTTP delivered web content. This exercise highlighted how different protocols cooperate seamlessly in network communication.