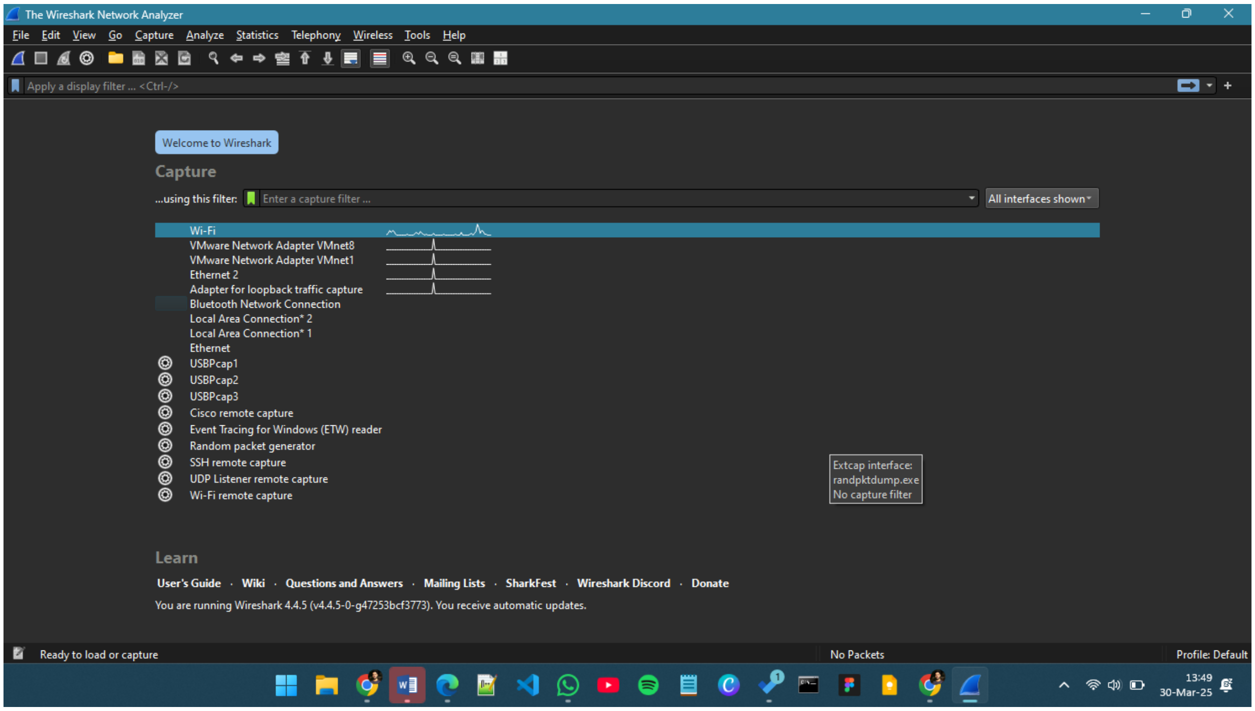
Wireshark Task 1


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

Capture

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

Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 2
Adapter for loopback traffic capture
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Ethernet
USBPcap1
USBPcap2
USBPcap3
Cisco remote capture
Event Tracing for Windows (ETW) reader
Random packet generator
SSH remote capture
UDP Listener remote capture
Wi-Fi remote capture

Extcap interface: randpktdump.exe
No capture filter

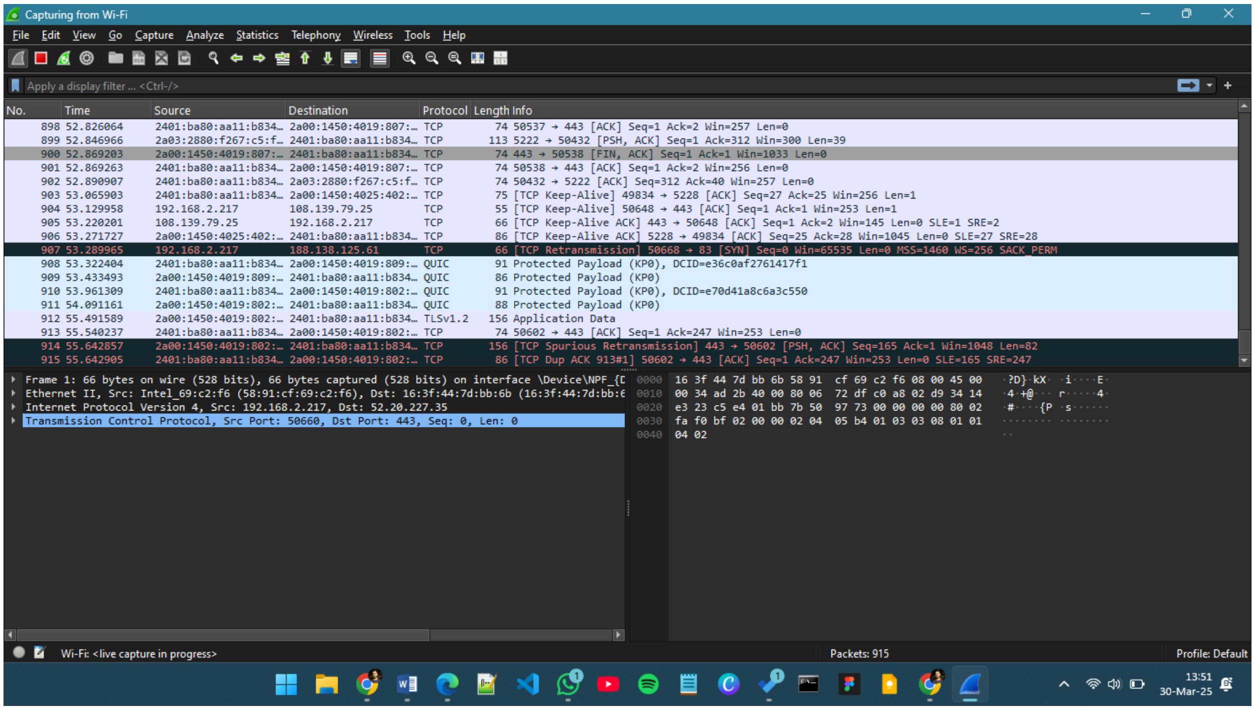
You are running Wireshark 4.4.5 (v4.4.5-0-g47253bcf3773). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default

13:49
30-Mar-25


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

```
No.   Time      Source                 Destination            Protocol Length Info
  898 52.826064 2401:ba80:aa11:b834… 2a00:1450:4019:807:… TCP       74 50537 → 443 [ACK] Seq=1 Ack=2 Win=257 Len=0
  899 52.846966 2a03:2880:f267:c5:f… 2401:ba80:aa11:b834… TCP      113 5222 → 50432 [PSH, ACK] Seq=1 Ack=312 Win=300 Len=39
  900 52.869203 2a00:1450:4019:807:… 2401:ba80:aa11:b834… TCP       74 443 → 50538 [FIN, ACK] Seq=1 Ack=1 Win=1033 Len=0
  901 52.869263 2401:ba80:aa11:b834… 2a00:1450:4019:807:… TCP       74 50538 → 443 [ACK] Seq=1 Ack=2 Win=256 Len=0
  902 52.890907 2401:ba80:aa11:b834… 2a03:2880:f267:c5:f… TCP       74 50432 → 5222 [ACK] Seq=312 Ack=40 Win=257 Len=0
  903 53.065903 2401:ba80:aa11:b834… 2a00:1450:4025:402:… TCP       75 [TCP Keep-Alive] 49834 → 5228 [ACK] Seq=27 Ack=25 Win=256 Len=1
  904 53.129958 192.168.2.217        108.139.79.25        TCP       55 [TCP Keep-Alive] 50648 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
  905 53.220201 108.139.79.25        192.168.2.217        TCP       66 [TCP Keep-Alive ACK] 443 → 50648 [ACK] Seq=1 Ack=2 Win=145 Len=0 SLE=1 SRE=2
  906 53.271727 2a00:1450:4025:402:… 2401:ba80:aa11:b834… TCP       86 [TCP Keep-Alive ACK] 5228 → 49834 [ACK] Seq=25 Ack=28 Win=1045 Len=0 SLE=27 SRE=28
  907 53.289965 192.168.2.217        188.138.125.61       TCP       66 [TCP Retransmission] 50668 → 83 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  908 53.322404 2401:ba80:aa11:b834… 2a00:1450:4019:809:… QUIC      91 Protected Payload (KP0), DCID=e36c0af2761417f1
  909 53.433493 2a00:1450:4019:809:… 2401:ba80:aa11:b834… QUIC      86 Protected Payload (KP0)
  910 53.961309 2401:ba80:aa11:b834… 2a00:1450:4019:802:… QUIC      91 Protected Payload (KP0), DCID=e70d41a8c6a3c550
  911 54.091161 2a00:1450:4019:802:… 2401:ba80:aa11:b834… QUIC      88 Protected Payload (KP0)
  912 55.491589 2a00:1450:4019:802:… 2401:ba80:aa11:b834… TLSv1.2  156 Application Data
  913 55.540237 2401:ba80:aa11:b834… 2a00:1450:4019:802:… TCP       74 50602 → 443 [ACK] Seq=1 Ack=247 Win=253 Len=0
  914 55.642857 2a00:1450:4019:802:… 2401:ba80:aa11:b834… TCP      156 [TCP Spurious Retransmission] 443 → 50602 [PSH, ACK] Seq=165 Ack=1 Win=1048 Len=82
  915 55.642905 2401:ba80:aa11:b834… 2a00:1450:4019:802:… TCP       86 [TCP Dup ACK 913#1] 50602 → 443 [ACK] Seq=1 Ack=247 Win=253 Len=0 SLE=165 SRE=247
```

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D
▸ Ethernet II, Src: Intel_69:c2:f6 (58:91:cf:69:c2:f6), Dst: 16:3f:44:7d:bb:6b (16:3f:44:7d:bb:6
▸ Internet Protocol Version 4, Src: 192.168.2.217, Dst: 52.20.227.35
▸ Transmission Control Protocol, Src Port: 50660, Dst Port: 443, Seq: 0, Len: 0
```

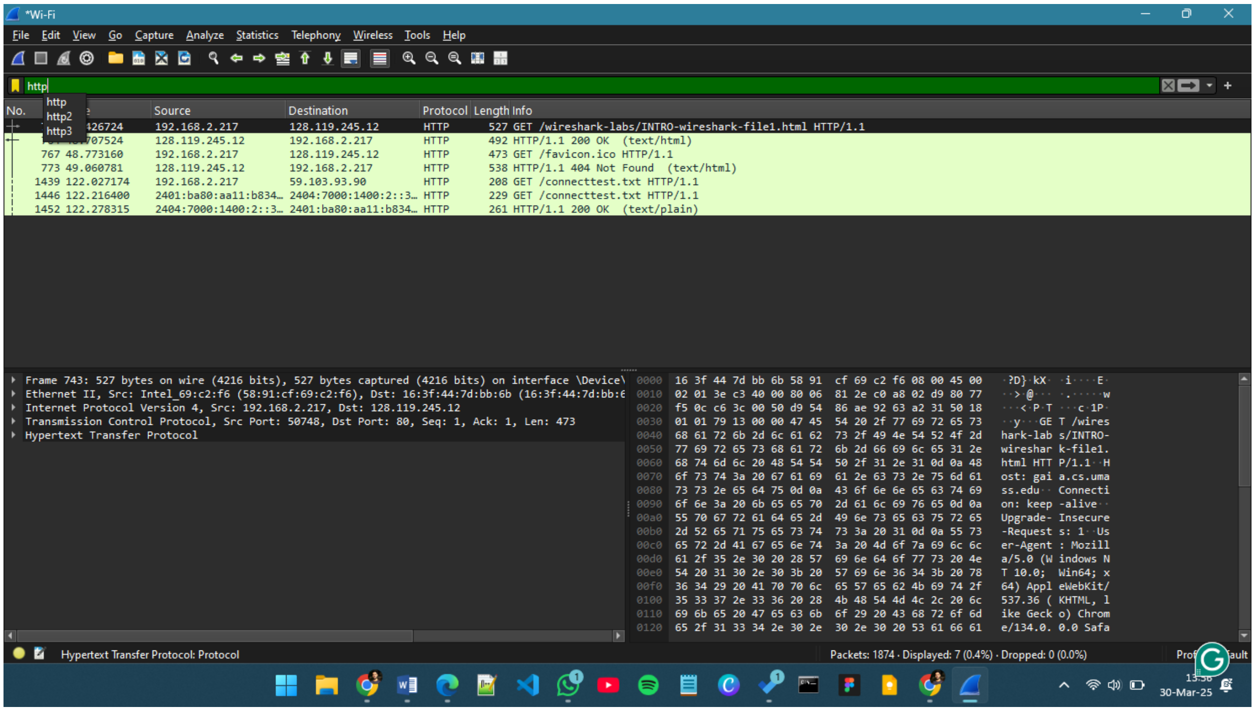
```
0000  16 3f 44 7d bb 6b 58 91  cf 69 c2 f6 08 00 45 00   ·?D}·kX· ·i····E·
0010  00 34 ad 2b 40 00 80 06  72 df c0 a8 02 d9 34 14   ·4·+@··· r·····4·
0020  e3 23 c5 e4 01 bb 7b 50  97 73 00 00 00 00 80 02   ·#····{P ·s······
0030  fa f0 bf 02 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Wi-Fi: <live capture in progress>

Packets: 915

Profile: Default

13:51
30-Mar-25


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3

```
No.        e          Source                Destination          Protocol Length Info
      426724          192.168.2.217         128.119.245.12       HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
      707524          128.119.245.12        192.168.2.217        HTTP      492 HTTP/1.1 200 OK  (text/html)
  767 48.773160       192.168.2.217         128.119.245.12       HTTP      473 GET /favicon.ico HTTP/1.1
  773 49.060781       128.119.245.12        192.168.2.217        HTTP      538 HTTP/1.1 404 Not Found  (text/html)
 1439 122.027174      192.168.2.217         59.103.93.90         HTTP      208 GET /connecttest.txt HTTP/1.1
 1446 122.216400      2401:ba80:aa11:b834… 2404:7000:1400:2::3… HTTP      229 GET /connecttest.txt HTTP/1.1
 1452 122.278315      2404:7000:1400:2::3… 2401:ba80:aa11:b834… HTTP      261 HTTP/1.1 200 OK  (text/plain)
```

```
Frame 743: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\
Ethernet II, Src: Intel_69:c2:f6 (58:91:cf:69:c2:f6), Dst: 16:3f:44:7d:bb:6b (16:3f:44:7d:bb:6
Internet Protocol Version 4, Src: 192.168.2.217, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50748, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
Hypertext Transfer Protocol
```

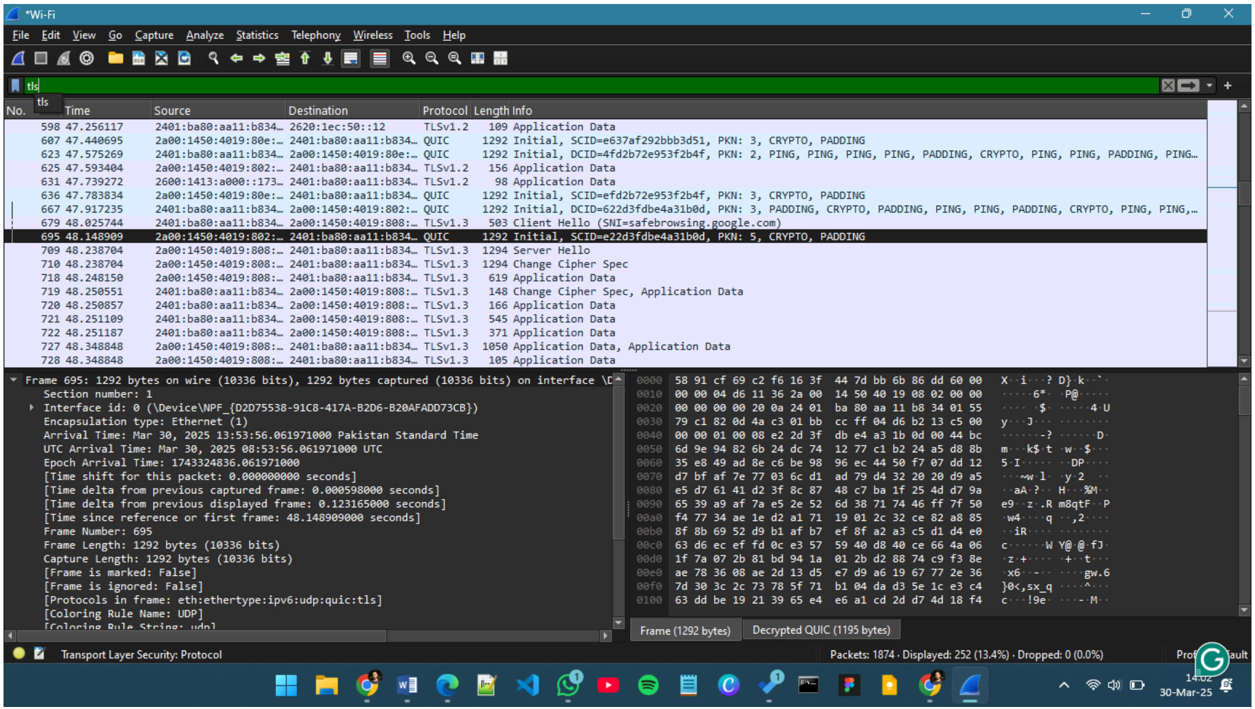
```
0000  16 3f 44 7d bb 6b 58 91  cf 69 c2 f6 08 00 45 00   ·?D}·kX· ·i····E·
0010  02 01 3e c3 40 00 80 06  81 2e c0 a8 02 d9 80 77   ··>·@··· ·.·····w
0020  f5 0c c6 3c 00 50 d9 54  86 ae 92 63 a2 31 50 18   ···<·P·T ···c·1P·
0030  01 01 79 13 00 00 47 45  54 20 2f 77 69 72 65 73   ··y···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0120  65 2f 31 33 34 2e 30 2e  30 2e 30 20 53 61 66 61   e/134.0. 0.0 Safa
```

Hypertext Transfer Protocol: Protocol

Packets: 1874 · Displayed: 7 (0.4%) · Dropped: 0 (0.0%)

Questions:

1. **Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark "protocol" column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?**
   All of them were shown


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

```
No.  Time      Source               Destination          Protocol Length Info
 598 47.256117 2401:ba80:aa11:b834… 2620:1ec:50::12      TLSv1.2   109 Application Data
 607 47.440695 2a00:1450:4019:80e:… 2401:ba80:aa11:b834… QUIC     1292 Initial, SCID=e637af292bbb3d51, PKN: 3, CRYPTO, PADDING
 623 47.575269 2401:ba80:aa11:b834… 2a00:1450:4019:80e:… QUIC     1292 Initial, DCID=4fd2b72e953f2b4f, PKN: 2, PING, PING, PING, PING, PADDING, CRYPTO, PING, PING, PADDING, PING…
 625 47.593404 2a00:1450:4019:802:… 2401:ba80:aa11:b834… TLSv1.2   156 Application Data
 631 47.739272 2600:1413:a000::173… 2401:ba80:aa11:b834… TLSv1.2    98 Application Data
 636 47.783834 2a00:1450:4019:80e:… 2401:ba80:aa11:b834… QUIC     1292 Initial, SCID=efd2b72e953f2b4f, PKN: 3, CRYPTO, PADDING
 667 47.917235 2401:ba80:aa11:b834… 2a00:1450:4019:802:… QUIC     1292 Initial, DCID=622d3fdbe4a31b0d, PKN: 3, PADDING, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, PING, PING,…
 679 48.025744 2401:ba80:aa11:b834… 2a00:1450:4019:808:… TLSv1.3   503 Client Hello (SNI=safebrowsing.google.com)
 695 48.148909 2a00:1450:4019:802:… 2401:ba80:aa11:b834… QUIC     1292 Initial, SCID=e22d3fdbe4a31b0d, PKN: 5, CRYPTO, PADDING
 709 48.238704 2a00:1450:4019:808:… 2401:ba80:aa11:b834… TLSv1.3  1294 Server Hello
 710 48.238704 2a00:1450:4019:808:… 2401:ba80:aa11:b834… TLSv1.3  1294 Change Cipher Spec
 718 48.248150 2a00:1450:4019:808:… 2401:ba80:aa11:b834… TLSv1.3   619 Application Data
 719 48.250551 2401:ba80:aa11:b834… 2a00:1450:4019:808:… TLSv1.3   148 Change Cipher Spec, Application Data
 720 48.250857 2401:ba80:aa11:b834… 2a00:1450:4019:808:… TLSv1.3   166 Application Data
 721 48.251109 2401:ba80:aa11:b834… 2a00:1450:4019:808:… TLSv1.3   545 Application Data
 722 48.251187 2401:ba80:aa11:b834… 2a00:1450:4019:808:… TLSv1.3   371 Application Data
 727 48.348848 2a00:1450:4019:808:… 2401:ba80:aa11:b834… TLSv1.3  1050 Application Data, Application Data
 728 48.348848 2a00:1450:4019:808:… 2401:ba80:aa11:b834… TLSv1.3   105 Application Data
```

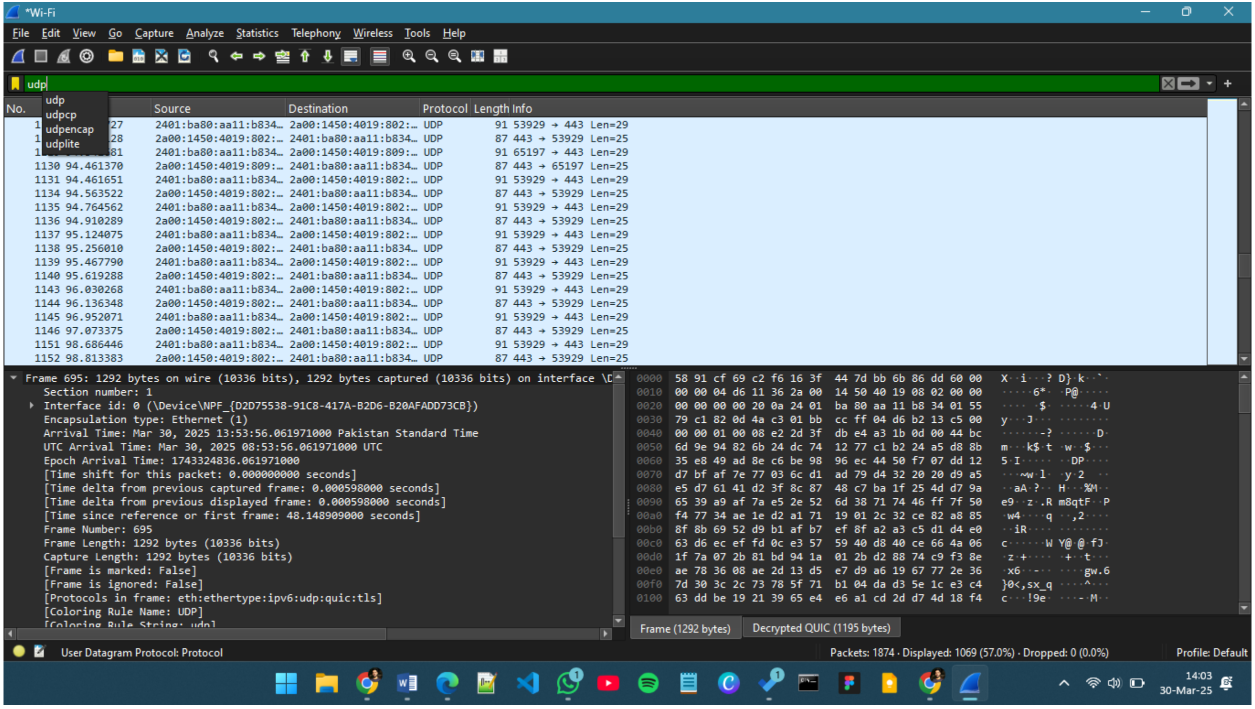
```
Frame 695: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \D
    Section number: 1
  Interface id: 0 (\Device\NPF_{D2D75538-91C8-417A-B2D6-B20AFADD73CB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 30, 2025 13:53:56.061971000 Pakistan Standard Time
    UTC Arrival Time: Mar 30, 2025 08:53:56.061971000 UTC
    Epoch Arrival Time: 1743324836.061971000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000598000 seconds]
    [Time delta from previous displayed frame: 0.123165000 seconds]
    [Time since reference or first frame: 48.148909000 seconds]
    Frame Number: 695
    Frame Length: 1292 bytes (10336 bits)
    Capture Length: 1292 bytes (10336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:quic:tls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

```
0000  58 91 cf 69 c2 f6 16 3f  44 7d bb 6b 86 dd 60 00   X·i···? D}·k··`·
0010  00 00 04 d6 11 36 2a 00  14 50 40 19 08 02 00 00   ·····6*· ·P@····
0020  00 00 00 00 20 0a 24 01  ba 80 aa 11 b8 34 01 55   ···· ·$· ·····4·U
0030  79 c1 82 0d 4a c3 01 bb  cc ff 04 d6 b2 13 c5 00   y···J··· ········
0040  00 00 01 00 08 e2 2d 3f  db e4 a3 1b 0d 00 44 bc   ······-? ······D·
0050  6d 9e 94 82 6b 24 dc 74  12 77 c1 b2 24 a5 d8 8b   m···k$·t ·w··$···
0060  35 e8 49 ad 8e c6 be 98  96 ec 44 50 f7 07 dd 12   5·I····· ··DP····
0070  d7 bf af 7e 77 03 6c d1  ad 79 d4 32 20 20 d9 a5   ···~w·l· ·y·2  ··
0080  e5 d7 61 41 d2 3f 8c 87  48 c7 ba 1f 25 4d d7 9a   ··aA·?·· H···%M··
0090  65 39 a9 af 7a e5 2e 52  6d 38 71 74 46 ff 7f 50   e9··z·.R m8qtF··P
00a0  f4 77 34 ae 1e d2 a1 71  19 01 2c 32 ce 82 a8 85   ·w4····q ··,2····
00b0  8f 8b 69 52 d9 b1 af b7  ef 8f a2 a3 c5 d1 d4 e0   ··iR···· ········
00c0  63 d6 ec ef fd 0c e3 57  59 40 d8 40 ce 66 4a 06   c······W Y@·@·fJ·
00d0  1f 7a 07 2b 81 bd 94 1a  01 2b d2 88 74 c9 f3 8e   ·z·+···· ·+··t···
00e0  ae 78 36 08 ae 2d 13 d5  e7 d9 a6 19 67 77 2e 36   ·x6··-·· ····gw.6
00f0  7d 30 3c 2c 73 78 5f 71  b1 04 da d3 5e 1c e3 c4   }0<,sx_q ····^···
0100  63 dd be 19 21 39 65 e4  e6 a1 cd 2d d7 4d 18 f4   c···!9e· ···-·M··
```

Frame (1292 bytes)
Decrypted QUIC (1195 bytes)
Transport Layer Security: Protocol

Packets: 1874 · Displayed: 252 (13.4%) · Dropped: 0 (0.0%)

Prof ault
14:02
30-Mar-25

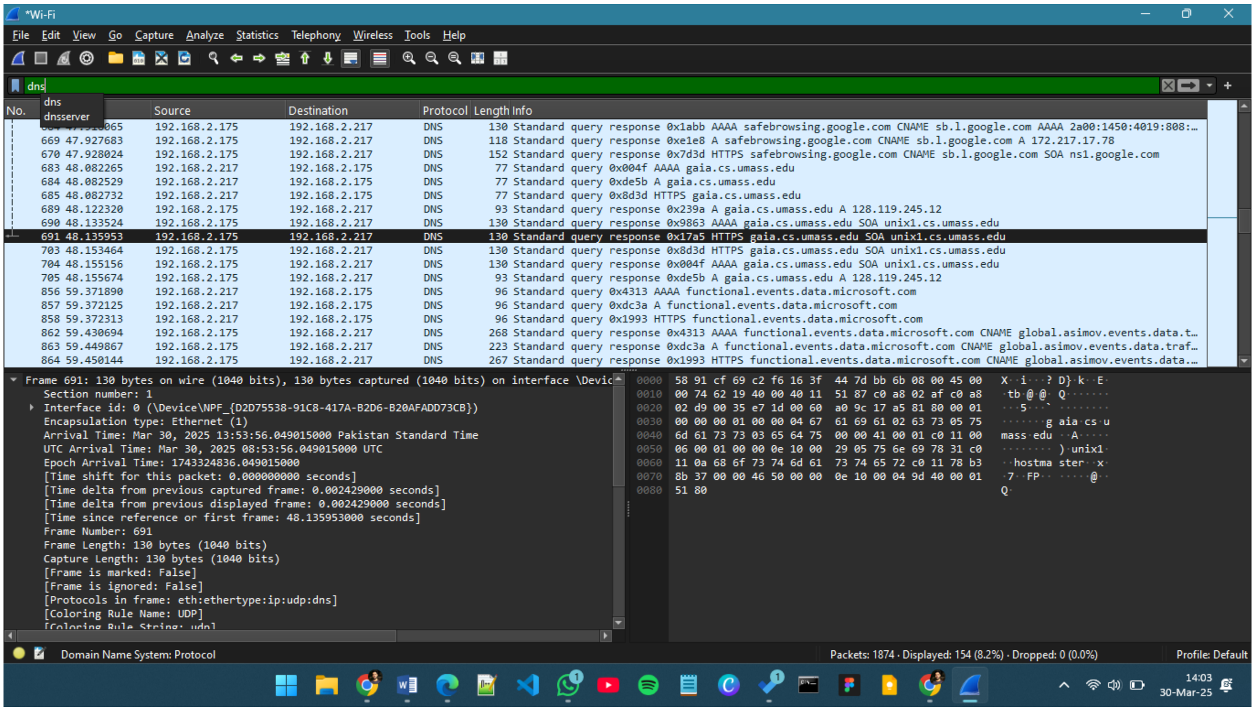

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
udp
udpcp
udpencap
udplite

```
No.  Time      Source               Destination          Protocol Length Info
   1       27  2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
   1       28  2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
   1       81  2401:ba80:aa11:b834… 2a00:1450:4019:809:… UDP        91 65197 → 443 Len=29
1130 94.461370 2a00:1450:4019:809:… 2401:ba80:aa11:b834… UDP        87 443 → 65197 Len=25
1131 94.461651 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1134 94.563522 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
1135 94.764562 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1136 94.910289 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
1137 95.124075 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1138 95.256010 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
1139 95.467790 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1140 95.619288 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
1143 96.030268 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1144 96.136348 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
1145 96.952071 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1146 97.073375 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
1151 98.686446 2401:ba80:aa11:b834… 2a00:1450:4019:802:… UDP        91 53929 → 443 Len=29
1152 98.813383 2a00:1450:4019:802:… 2401:ba80:aa11:b834… UDP        87 443 → 53929 Len=25
```

```
Frame 695: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \D
    Section number: 1
  Interface id: 0 (\Device\NPF_{D2D75538-91C8-417A-B2D6-B20AFADD73CB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 30, 2025 13:53:56.061971000 Pakistan Standard Time
    UTC Arrival Time: Mar 30, 2025 08:53:56.061971000 UTC
    Epoch Arrival Time: 1743324836.061971000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000598000 seconds]
    [Time delta from previous displayed frame: 0.000598000 seconds]
    [Time since reference or first frame: 48.148909000 seconds]
    Frame Number: 695
    Frame Length: 1292 bytes (10336 bits)
    Capture Length: 1292 bytes (10336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:quic:tls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

```
0000  58 91 cf 69 c2 f6 16 3f  44 7d bb 6b 86 dd 60 00   X·i···? D}·k··`·
0010  00 00 04 d6 11 36 2a 00  14 50 40 19 08 02 00 00   ·····6*· ·P@····
0020  00 00 00 00 20 0a 24 01  ba 80 aa 11 b8 34 01 55   ···· ·$· ·····4·U
0030  79 c1 82 0d 4a c3 01 bb  cc ff 04 d6 b2 13 c5 00   y···J··· ········
0040  00 00 01 00 08 e2 2d 3f  db e4 a3 1b 0d 00 44 bc   ······-? ······D·
0050  6d 9e 94 82 6b 24 dc 74  12 77 c1 b2 24 a5 d8 8b   m···k$·t ·w··$···
0060  35 e8 49 ad 8e c6 be 98  96 ec 44 50 f7 07 dd 12   5·I····· ··DP····
0070  d7 bf af 7e 77 03 6c d1  ad 79 d4 32 20 20 d9 a5   ···~w·l· ·y·2  ··
0080  e5 d7 61 41 d2 3f 8c 87  48 c7 ba 1f 25 4d d7 9a   ··aA·?·· H···%M··
0090  65 39 a9 af 7a e5 2e 52  6d 38 71 74 46 ff 7f 50   e9··z·.R m8qtF··P
00a0  f4 77 34 ae 1e d2 a1 71  19 01 2c 32 ce 82 a8 85   ·w4····q ··,2····
00b0  8f 8b 69 52 d9 b1 af b7  ef 8f a2 a3 c5 d1 d4 e0   ··iR···· ········
00c0  63 d6 ec ef fd 0c e3 57  59 40 d8 40 ce 66 4a 06   c······W Y@·@·fJ·
00d0  1f 7a 07 2b 81 bd 94 1a  01 2b d2 88 74 c9 f3 8e   ·z·+···· ·+··t···
00e0  ae 78 36 08 ae 2d 13 d5  e7 d9 a6 19 67 77 2e 36   ·x6··-·· ····gw.6
00f0  7d 30 3c 2c 73 78 5f 71  b1 04 da d3 5e 1c e3 c4   }0<,sx_q ····^···
0100  63 dd be 19 21 39 65 e4  e6 a1 cd 2d d7 4d 18 f4   c···!9e· ···-·M··
```

Packets: 1874 · Displayed: 1069 (57.0%) · Dropped: 0 (0.0%)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver
14:03
30-Mar-25

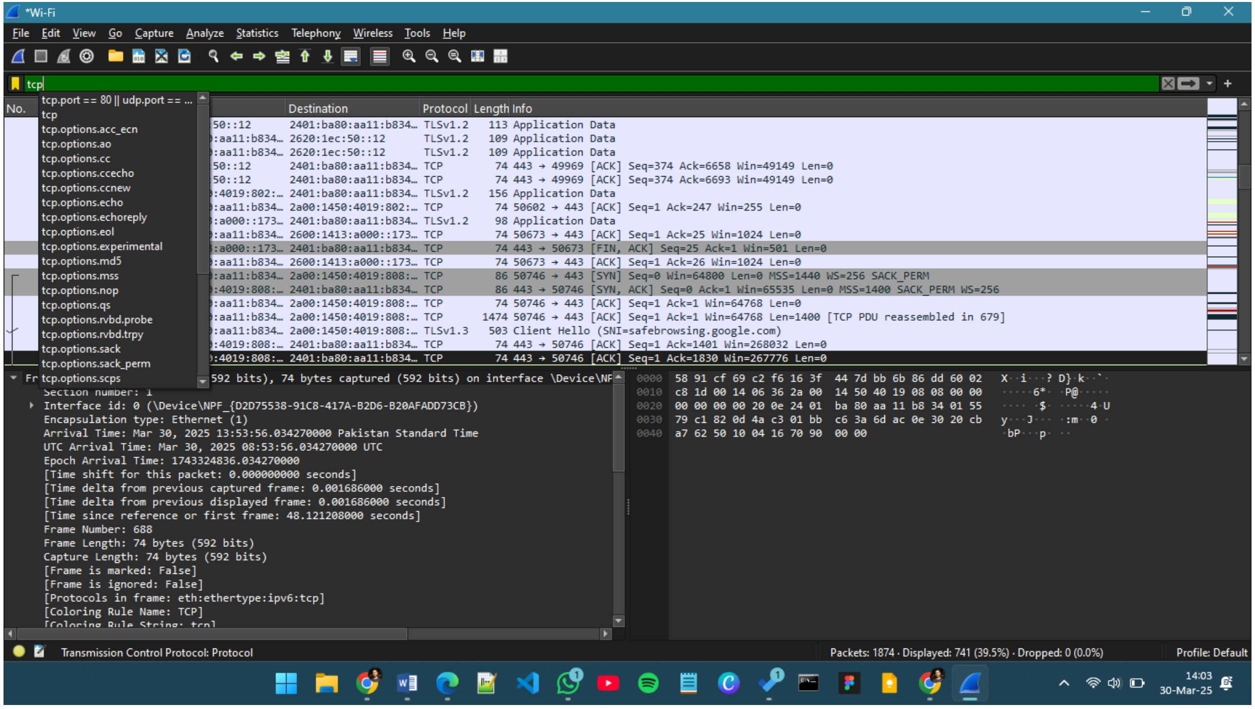
```
No.                      Source          Destination     Protocol Length Info
         065             192.168.2.175   192.168.2.217   DNS      130 Standard query response 0x1abb AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2a00:1450:4019:808:…
    669 47.927683        192.168.2.175   192.168.2.217   DNS      118 Standard query response 0xe1e8 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.17.78
    670 47.928024        192.168.2.175   192.168.2.217   DNS      152 Standard query response 0x7d3d HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
    683 48.082265        192.168.2.217   192.168.2.175   DNS       77 Standard query 0x004f AAAA gaia.cs.umass.edu
    684 48.082529        192.168.2.217   192.168.2.175   DNS       77 Standard query 0xde5b A gaia.cs.umass.edu
    685 48.082732        192.168.2.217   192.168.2.175   DNS       77 Standard query 0x8d3d HTTPS gaia.cs.umass.edu
    689 48.122320        192.168.2.175   192.168.2.217   DNS       93 Standard query response 0x239a A gaia.cs.umass.edu A 128.119.245.12
    690 48.133524        192.168.2.175   192.168.2.217   DNS      130 Standard query response 0x9863 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
    691 48.135953        192.168.2.175   192.168.2.217   DNS      130 Standard query response 0x17a5 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu
    703 48.153464        192.168.2.175   192.168.2.217   DNS      130 Standard query response 0x8d3d HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu
    704 48.155156        192.168.2.175   192.168.2.217   DNS      130 Standard query response 0x004f AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
    705 48.155674        192.168.2.175   192.168.2.217   DNS       93 Standard query response 0xde5b A gaia.cs.umass.edu A 128.119.245.12
    856 59.371890        192.168.2.217   192.168.2.175   DNS       96 Standard query 0x4313 AAAA functional.events.data.microsoft.com
    857 59.372125        192.168.2.217   192.168.2.175   DNS       96 Standard query 0xdc3a A functional.events.data.microsoft.com
    858 59.372313        192.168.2.217   192.168.2.175   DNS       96 Standard query 0x1993 HTTPS functional.events.data.microsoft.com
    862 59.430694        192.168.2.175   192.168.2.217   DNS      268 Standard query response 0x4313 AAAA functional.events.data.microsoft.com CNAME global.asimov.events.data.t…
    863 59.449867        192.168.2.175   192.168.2.217   DNS      223 Standard query response 0xdc3a A functional.events.data.microsoft.com CNAME global.asimov.events.data.traf…
    864 59.450144        192.168.2.175   192.168.2.217   DNS      267 Standard query response 0x1993 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.…
```

```
Frame 691: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Devic
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D2D75538-91C8-417A-B2D6-B20AFADD73CB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 30, 2025 13:53:56.049015000 Pakistan Standard Time
    UTC Arrival Time: Mar 30, 2025 08:53:56.049015000 UTC
    Epoch Arrival Time: 1743324836.049015000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.002429000 seconds]
    [Time delta from previous displayed frame: 0.002429000 seconds]
    [Time since reference or first frame: 48.135953000 seconds]
    Frame Number: 691
    Frame Length: 130 bytes (1040 bits)
    Capture Length: 130 bytes (1040 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

```
0000  58 91 cf 69 c2 f6 16 3f  44 7d bb 6b 08 00 45 00   X··i···? D}·k··E·
0010  00 74 62 19 40 00 40 11  51 87 c0 a8 02 af c0 a8   ·tb·@·@· Q·······
0020  02 d9 00 35 e7 1d 00 60  a0 9c 17 a5 81 80 00 01   ···5···` ········
0030  00 00 00 01 00 00 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 41 00 01 c0 11 00   mass·edu ··A·····
0050  06 00 01 00 00 0e 10 00  29 05 75 6e 69 78 31 c0   ········ )·unix1·
0060  11 0a 68 6f 73 74 6d 61  73 74 65 72 c0 11 78 b3   ··hostma ster··x·
0070  8b 37 00 00 46 50 00 00  0e 10 00 04 9d 40 00 01   ·7··FP·· ·····@··
0080  51 80                                              Q·
```

Domain Name System: Protocol

Packets: 1874 · Displayed: 154 (8.2%) · Dropped: 0 (0.0%)   Profile: Default



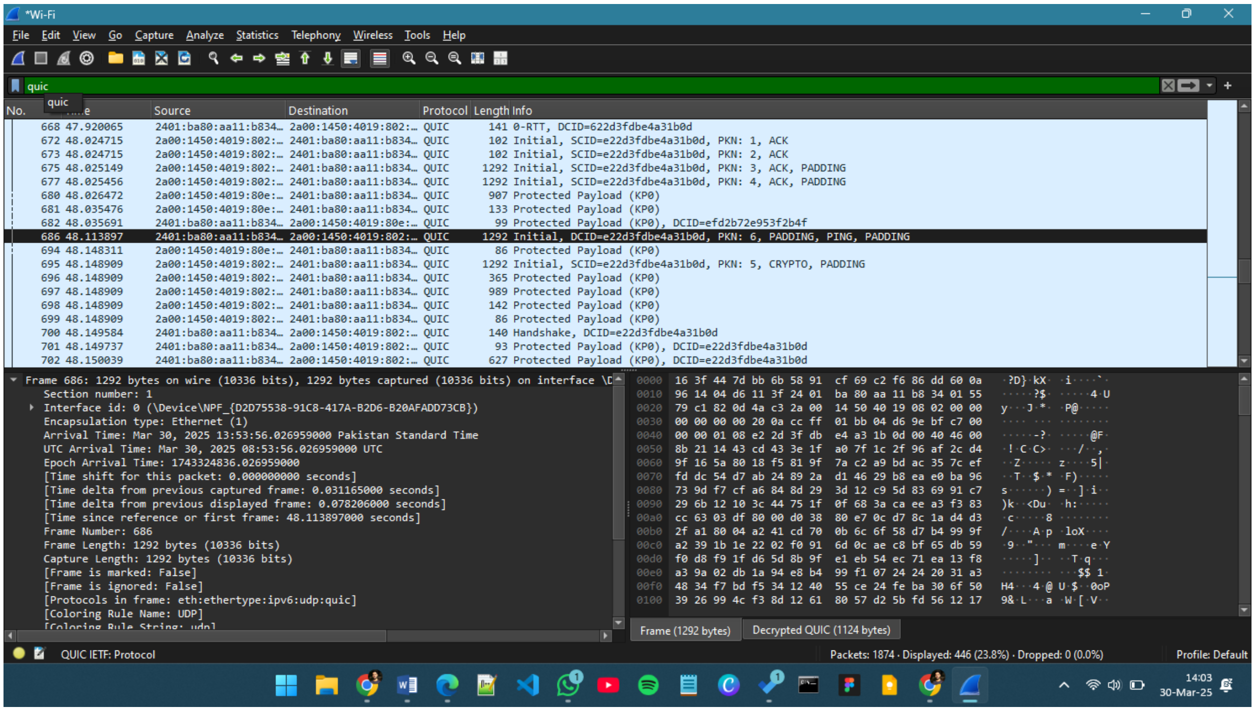
```
No.                         Destination          Protocol Length Info
             50::12         2401:ba80:aa11:b834… TLSv1.2   113 Application Data
             :aa11:b834…    2620:1ec:50::12      TLSv1.2   109 Application Data
             :aa11:b834…    2620:1ec:50::12      TLSv1.2   109 Application Data
             50::12         2401:ba80:aa11:b834… TCP        74 443 → 49969 [ACK] Seq=374 Ack=6658 Win=49149 Len=0
             50::12         2401:ba80:aa11:b834… TCP        74 443 → 49969 [ACK] Seq=374 Ack=6693 Win=49149 Len=0
             :4019:802:…    2401:ba80:aa11:b834… TLSv1.2   156 Application Data
             :aa11:b834…    2a00:1450:4019:802:… TCP        74 50602 → 443 [ACK] Seq=1 Ack=247 Win=255 Len=0
             :a000::173…    2401:ba80:aa11:b834… TLSv1.2    98 Application Data
             :aa11:b834…    2600:1413:a000::173… TCP        74 50673 → 443 [ACK] Seq=1 Ack=25 Win=1024 Len=0
             :a000::173…    2401:ba80:aa11:b834… TCP        74 443 → 50673 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
             :aa11:b834…    2600:1413:a000::173… TCP        74 50673 → 443 [ACK] Seq=1 Ack=26 Win=1024 Len=0
             :aa11:b834…    2a00:1450:4019:808:… TCP        86 50746 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
             :4019:808:…    2401:ba80:aa11:b834… TCP        86 443 → 50746 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=256
             :aa11:b834…    2a00:1450:4019:808:… TCP        74 50746 → 443 [ACK] Seq=1 Ack=1 Win=64768 Len=0
             :aa11:b834…    2a00:1450:4019:808:… TCP      1474 50746 → 443 [ACK] Seq=1 Ack=1 Win=64768 Len=1400 [TCP PDU reassembled in 679]
             :aa11:b834…    2a00:1450:4019:808:… TLSv1.3   503 Client Hello (SNI=safebrowsing.google.com)
             :4019:808:…    2401:ba80:aa11:b834… TCP        74 443 → 50746 [ACK] Seq=1 Ack=1401 Win=268032 Len=0
             :4019:808:…    2401:ba80:aa11:b834… TCP        74 443 → 50746 [ACK] Seq=1 Ack=1830 Win=267776 Len=0
```

```
Fr                      592 bits), 74 bytes captured (592 bits) on interface \Device\NF
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D2D75538-91C8-417A-B2D6-B20AFADD73CB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 30, 2025 13:53:56.034270000 Pakistan Standard Time
    UTC Arrival Time: Mar 30, 2025 08:53:56.034270000 UTC
    Epoch Arrival Time: 1743324836.034270000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.001686000 seconds]
    [Time delta from previous displayed frame: 0.001686000 seconds]
    [Time since reference or first frame: 48.121208000 seconds]
    Frame Number: 688
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

```
0000  58 91 cf 69 c2 f6 16 3f  44 7d bb 6b 86 dd 60 02   X··i···? D}·k··`·
0010  c8 1d 00 14 06 36 2a 00  14 50 40 19 08 08 00 00   ·····6*· ·P@·····
0020  00 00 00 00 20 0e 24 01  ba 80 aa 11 b8 34 01 55   ···· ·$· ·····4·U
0030  79 c1 82 0d 4a c3 01 bb  c6 3a 6d ac 0e 30 20 cb   y···J··· ·:m··0 ·
0040  a7 62 50 10 04 16 70 90  00 00                     ·bP···p· ··
```

Transmission Control Protocol: Protocol

Packets: 1874 · Displayed: 741 (39.5%) · Dropped: 0 (0.0%)   Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
quic
quic
Frame (1292 bytes)
Decrypted QUIC (1124 bytes)
14:03
30-Mar-25

```
No.           e   Source                 Destination            Protocol Length Info
   668 47.920065  2401:ba80:aa11:b834…  2a00:1450:4019:802:…  QUIC      141 0-RTT, DCID=622d3fdbe4a31b0d
   672 48.024715  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC      102 Initial, SCID=e22d3fdbe4a31b0d, PKN: 1, ACK
   673 48.024715  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC      102 Initial, SCID=e22d3fdbe4a31b0d, PKN: 2, ACK
   675 48.025149  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC     1292 Initial, SCID=e22d3fdbe4a31b0d, PKN: 3, ACK, PADDING
   677 48.025456  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC     1292 Initial, SCID=e22d3fdbe4a31b0d, PKN: 4, ACK, PADDING
   680 48.026472  2a00:1450:4019:80e:…  2401:ba80:aa11:b834…  QUIC      907 Protected Payload (KP0)
   681 48.035476  2a00:1450:4019:80e:…  2401:ba80:aa11:b834…  QUIC      133 Protected Payload (KP0)
   682 48.035691  2401:ba80:aa11:b834…  2a00:1450:4019:80e:…  QUIC       99 Protected Payload (KP0), DCID=efd2b72e953f2b4f
   686 48.113897  2401:ba80:aa11:b834…  2a00:1450:4019:802:…  QUIC     1292 Initial, DCID=e22d3fdbe4a31b0d, PKN: 6, PADDING, PING, PADDING
   694 48.148311  2a00:1450:4019:80e:…  2401:ba80:aa11:b834…  QUIC       86 Protected Payload (KP0)
   695 48.148909  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC     1292 Initial, SCID=e22d3fdbe4a31b0d, PKN: 5, CRYPTO, PADDING
   696 48.148909  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC      365 Protected Payload (KP0)
   697 48.148909  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC      989 Protected Payload (KP0)
   698 48.148909  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC      142 Protected Payload (KP0)
   699 48.148909  2a00:1450:4019:802:…  2401:ba80:aa11:b834…  QUIC       86 Protected Payload (KP0)
   700 48.149584  2401:ba80:aa11:b834…  2a00:1450:4019:802:…  QUIC      140 Handshake, DCID=e22d3fdbe4a31b0d
   701 48.149737  2401:ba80:aa11:b834…  2a00:1450:4019:802:…  QUIC       93 Protected Payload (KP0), DCID=e22d3fdbe4a31b0d
   702 48.150039  2401:ba80:aa11:b834…  2a00:1450:4019:802:…  QUIC      627 Protected Payload (KP0), DCID=e22d3fdbe4a31b0d
```

```
Frame 686: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \D
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D2D75538-91C8-417A-B2D6-B20AFADD73CB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 30, 2025 13:53:56.026959000 Pakistan Standard Time
    UTC Arrival Time: Mar 30, 2025 08:53:56.026959000 UTC
    Epoch Arrival Time: 1743324836.026959000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.031165000 seconds]
    [Time delta from previous displayed frame: 0.078206000 seconds]
    [Time since reference or first frame: 48.113897000 seconds]
    Frame Number: 686
    Frame Length: 1292 bytes (10336 bits)
    Capture Length: 1292 bytes (10336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:quic]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

```
0000  16 3f 44 7d bb 6b 58 91  cf 69 c2 f6 86 dd 60 0a   ·?D}·kX··i····`·
0010  96 14 04 d6 11 3f 24 01  ba 80 aa 11 b8 34 01 55   ·····?$······4·U
0020  79 c1 82 0d 4a c3 2a 00  14 50 40 19 08 02 00 00   y···J·*··P@·····
0030  00 00 00 00 20 0a cc ff  01 bb 04 d6 9e bf c7 00   ················
0040  00 00 01 08 e2 2d 3f db  e4 a3 1b 0d 00 40 46 00   ·····-?······@F·
0050  8b 21 14 43 cd 43 3e 1f  a0 7f 1c 2f 96 af 2c d4   ·!·C·C>····/··,·
0060  9f 16 5a 80 18 f5 81 9f  7a c2 a9 bd ac 35 7c ef   ··Z·····z····5|·
0070  fd dc 54 d7 ab 24 89 2a  d1 46 29 b8 ea e0 ba 96   ··T··$·*·F)·····
0080  73 9d f7 cf a6 84 8d 29  3d 12 c9 5d 83 69 91 c7   s······)=··]·i··
0090  29 6b 12 10 3c 44 75 1f  0f 68 3a ca ee a3 f3 83   )k··<Du··h:·····
00a0  cc 63 03 df 80 00 d0 38  80 e7 0c d7 8c 1a d4 d3   ·c·····8········
00b0  2f a1 80 04 a2 41 cd 70  0b 6c 6f 58 d7 b4 99 9f   /····A·p·loX····
00c0  a2 39 1b 1e 22 02 f0 91  6d 0c ae c8 bf 65 db 59   ·9··"···m····e·Y
00d0  f0 d8 f9 1f d6 5d 8b 9f  e1 eb 54 ec 71 ea 13 f8   ·····]····T·q···
00e0  a3 9a 02 db 1a 94 e8 b4  99 f1 07 24 24 20 31 a3   ···········$$ 1·
00f0  48 34 f7 bd f5 34 12 40  55 ce 24 fe ba 30 6f 50   H4···4·@U·$··0oP
0100  39 26 99 4c f3 8d 12 61  80 57 d2 5b fd 56 12 17   9&·L···a·W·[·V··
```

QUIC IETF: Protocol

Packets: 1874 · Displayed: 446 (23.8%) · Dropped: 0 (0.0%)

Profile: Default

2. **How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. (If you want to display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)**

   About 2 seconds

3. **What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?**

   128.119.245.12

4. **Expand the information on the HTTP message in the Wireshark "Details of selected packet" window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the "User Agent:" field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are using.]**

   - **Firefox, Safari, Microsoft Internet Edge, Other**

   Microsoft NCSI\r\n

5. **Expand the information on the Transmission Control Protocol for this packet in the Wireshark "Details of selected packet" window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the**

number following “Dest Port:” for the TCP segment containing the HTTP request) to which this HTTP request is being sent?
Port 80

6. **Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.**
[Atteched]