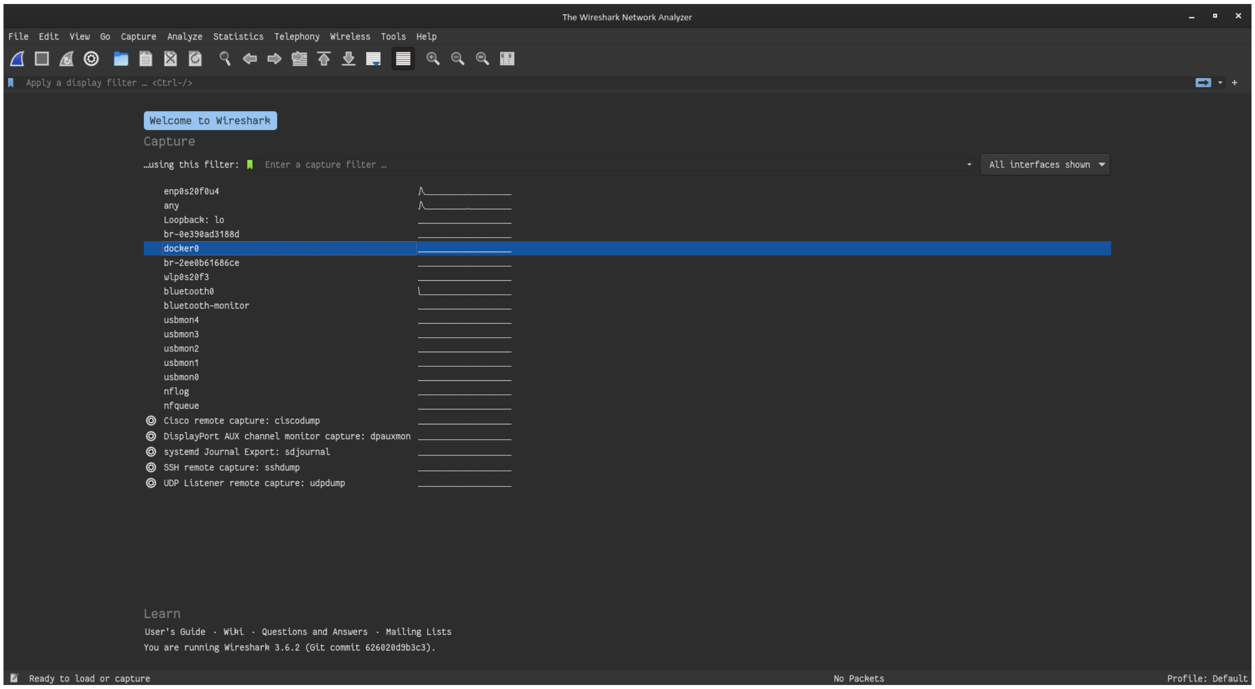
CN-Lab03

20051554 CSE 4

Wireshark Application

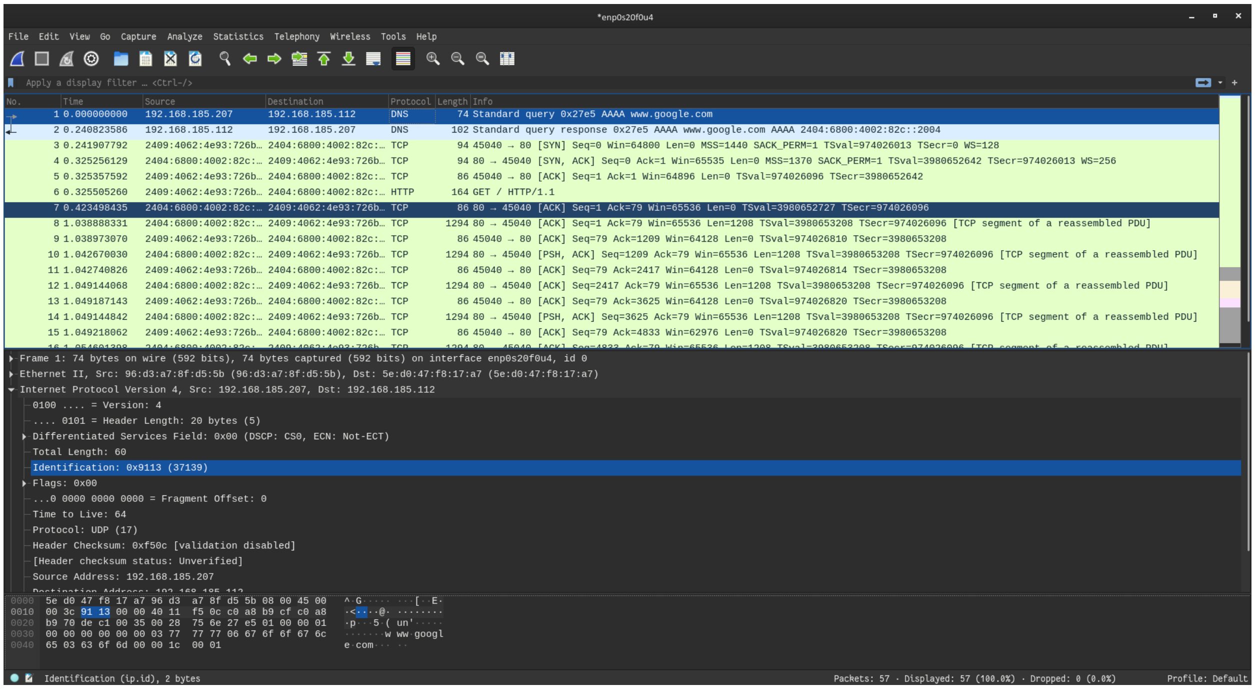


```
enp0s20f0u4
any
Loopback: lo
br-0e390ad3188d
docker0
br-2ee0b61686ce
wlp0s20f3
bluetooth0
bluetooth-monitor
usbmon4
usbmon3
usbmon2
usbmon1
usbmon0
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

You are running Wireshark 3.6.2 (Git commit 626020d9b3c3).

Ready to load or capture   No Packets   Profile: Default

Use “DNS” as a filter.



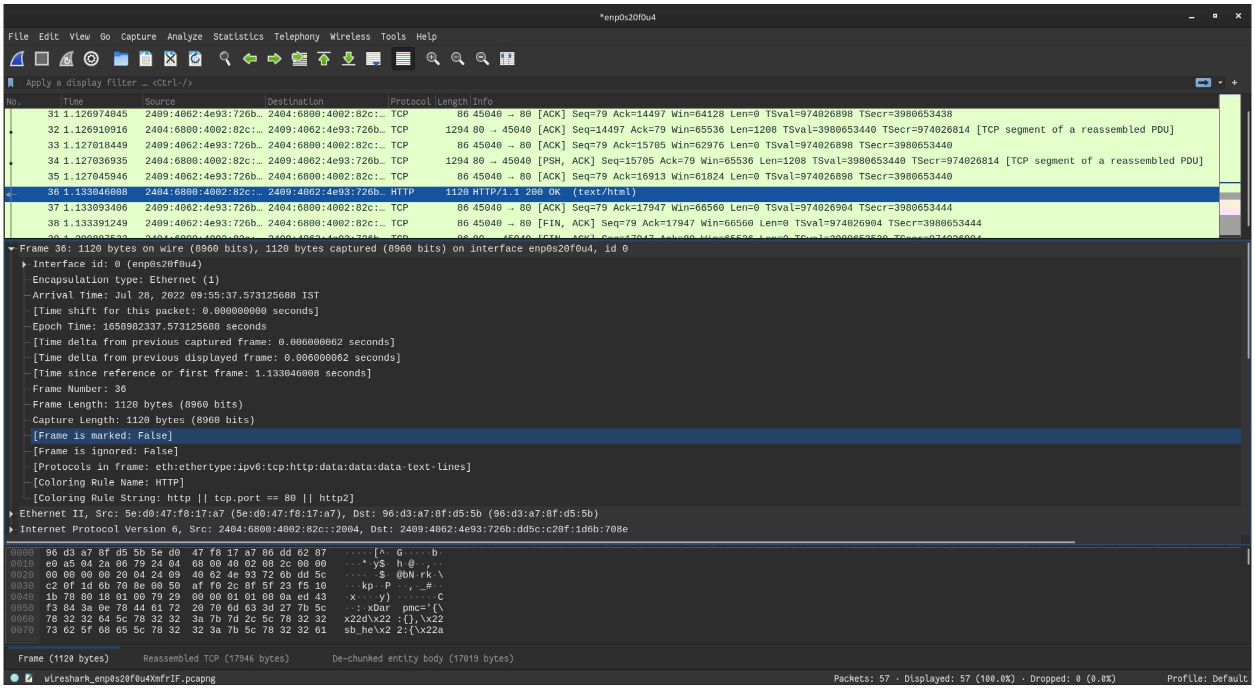
*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source              Destination         Protocol Length Info
   1 0.000000000  192.168.185.207     192.168.185.112     DNS        74 Standard query 0x27e5 AAAA www.google.com
   2 0.240823586  192.168.185.112     192.168.185.207     DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
   3 0.241907792  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      94 45040 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=974026013 TSecr=0 WS=128
   4 0.325256129  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP      94 80 → 45040 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 TSval=3980652642 TSecr=974026013 WS=256
   5 0.325357592  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=974026096 TSecr=3980652642
   6 0.325505260  2409:4062:4e93:726b… 2404:6800:4002:82c:… HTTP    164 GET / HTTP/1.1
   7 0.423498435  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP      86 80 → 45040 [ACK] Seq=1 Ack=79 Win=65536 Len=0 TSval=3980652727 TSecr=974026096
   8 1.038888331  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=1 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   9 1.038973070  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=1209 Win=64128 Len=0 TSval=974026810 TSecr=3980653208
  10 1.042670030  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [PSH, ACK] Seq=1209 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
  11 1.042740826  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=2417 Win=64128 Len=0 TSval=974026814 TSecr=3980653208
  12 1.049144068  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=2417 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
  13 1.049187143  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=3625 Win=64128 Len=0 TSval=974026820 TSecr=3980653208
  14 1.049144842  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [PSH, ACK] Seq=3625 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
  15 1.049218062  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=4833 Win=62976 Len=0 TSval=974026820 TSecr=3980653208
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s20f0u4, id 0
▸ Ethernet II, Src: 96:d3:a7:8f:d5:5b (96:d3:a7:8f:d5:5b), Dst: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7)
▾ Internet Protocol Version 4, Src: 192.168.185.207, Dst: 192.168.185.112
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x9113 (37139)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xf50c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.185.207
```

```
0000  5e d0 47 f8 17 a7 96 d3  a7 8f d5 5b 08 00 45 00   ^·G·····  ···[··E·
0010  00 3c 91 13 00 00 40 11  f5 0c c0 a8 b9 cf c0 a8   ·<····@·  ········
0020  b9 70 de c1 00 35 00 28  75 6e 27 e5 01 00 00 01   ·p···5·(  un'·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w  ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01                     e·com···  ··
```

```
Identification (ip.id), 2 bytes          Packets: 57 · Displayed: 57 (100.0%) · Dropped: 0 (0.0%)     Profile: Default
```



*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

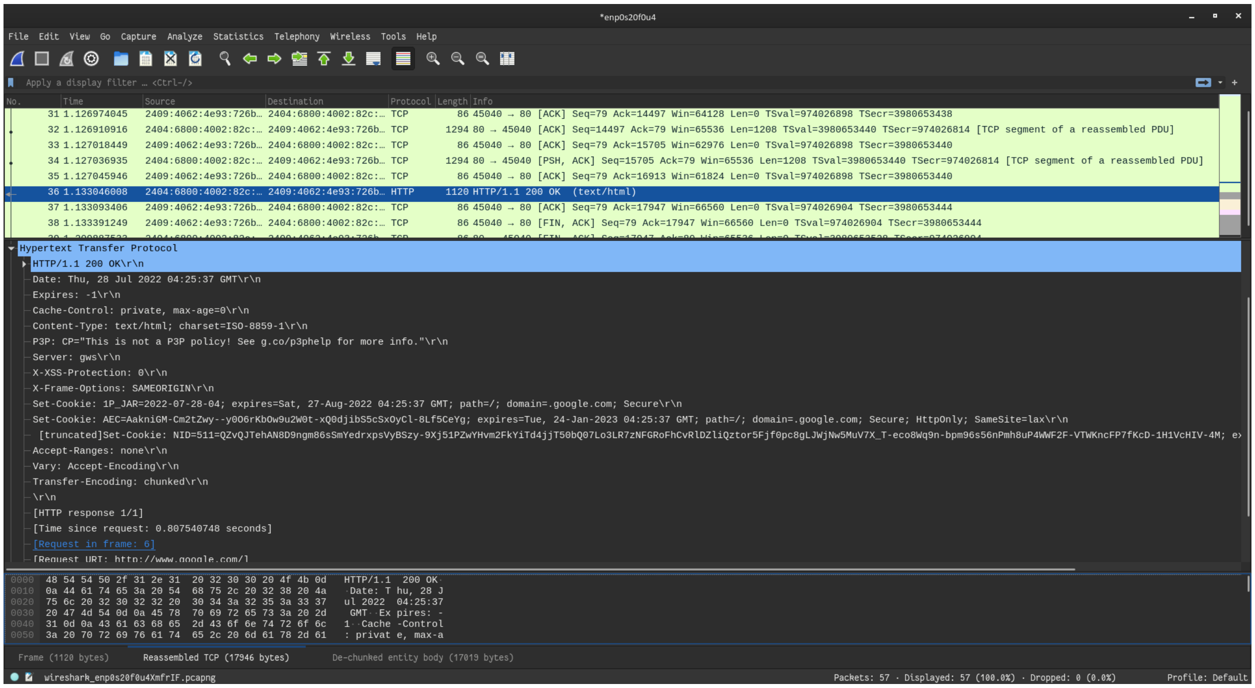
```
No.  Time         Source              Destination         Protocol Length Info
  31 1.126974045  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=14497 Win=64128 Len=0 TSval=974026898 TSecr=3980653438
  32 1.126910916  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=14497 Ack=79 Win=65536 Len=1208 TSval=3980653440 TSecr=974026814 [TCP segment of a reassembled PDU]
  33 1.127018449  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=15705 Win=62976 Len=0 TSval=974026898 TSecr=3980653440
  34 1.127036935  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [PSH, ACK] Seq=15705 Ack=79 Win=65536 Len=1208 TSval=3980653440 TSecr=974026814 [TCP segment of a reassembled PDU]
  35 1.127045946  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=16913 Win=61824 Len=0 TSval=974026898 TSecr=3980653440
  36 1.133046008  2404:6800:4002:82c:… 2409:4062:4e93:726b… HTTP   1120 HTTP/1.1 200 OK  (text/html)
  37 1.133093406  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=17947 Win=66560 Len=0 TSval=974026904 TSecr=3980653444
  38 1.133391249  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [FIN, ACK] Seq=79 Ack=17947 Win=66560 Len=0 TSval=974026904 TSecr=3980653444
```

```
▾ Frame 36: 1120 bytes on wire (8960 bits), 1120 bytes captured (8960 bits) on interface enp0s20f0u4, id 0
  ▸ Interface id: 0 (enp0s20f0u4)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 28, 2022 09:55:37.573125688 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1658982337.573125688 seconds
    [Time delta from previous captured frame: 0.006000062 seconds]
    [Time delta from previous displayed frame: 0.006000062 seconds]
    [Time since reference or first frame: 1.133046008 seconds]
    Frame Number: 36
    Frame Length: 1120 bytes (8960 bits)
    Capture Length: 1120 bytes (8960 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:http:data:data:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▸ Ethernet II, Src: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7), Dst: 96:d3:a7:8f:d5:5b (96:d3:a7:8f:d5:5b)
▸ Internet Protocol Version 6, Src: 2404:6800:4002:82c::2004, Dst: 2409:4062:4e93:726b:dd5c:c20f:1d6b:708e
```

```
0000  96 d3 a7 8f d5 5b 5e d0  47 f8 17 a7 86 dd 62 87   ·····[^·  G·····b·
0010  e0 a5 04 2a 06 79 24 04  68 00 40 02 08 2c 00 00   ···*·y$·  h·@··,··
0020  00 00 00 00 20 04 24 09  40 62 4e 93 72 6b dd 5c   ···· ·$·  @bN·rk·\
0030  c2 0f 1d 6b 70 8e 00 50  af f0 2c 8f 5f 23 f5 10   ···kp··P  ··,·_#··
0040  1b 78 80 18 01 00 79 29  00 00 01 01 08 0a ed 43   ·x····y)  ·······C
0050  f3 84 3a 0e 78 44 61 72  20 70 6d 63 3d 27 7b 5c   ··:·xDar   pmc='{\
0060  78 32 32 64 5c 78 32 32  3a 7b 7d 2c 5c 78 32 32   x22d\x22  :{},\x22
0070  73 62 5f 68 65 5c 78 32  32 3a 7b 5c 78 32 32 61   sb_he\x2  2:{\x22a
```

```
Frame (1120 bytes)     Reassembled TCP (17946 bytes)     De-chunked entity body (17019 bytes)
```

```
wireshark_enp0s20f0u4XmfrIF.pcapng          Packets: 57 · Displayed: 57 (100.0%) · Dropped: 0 (0.0%)     Profile: Default
```


*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

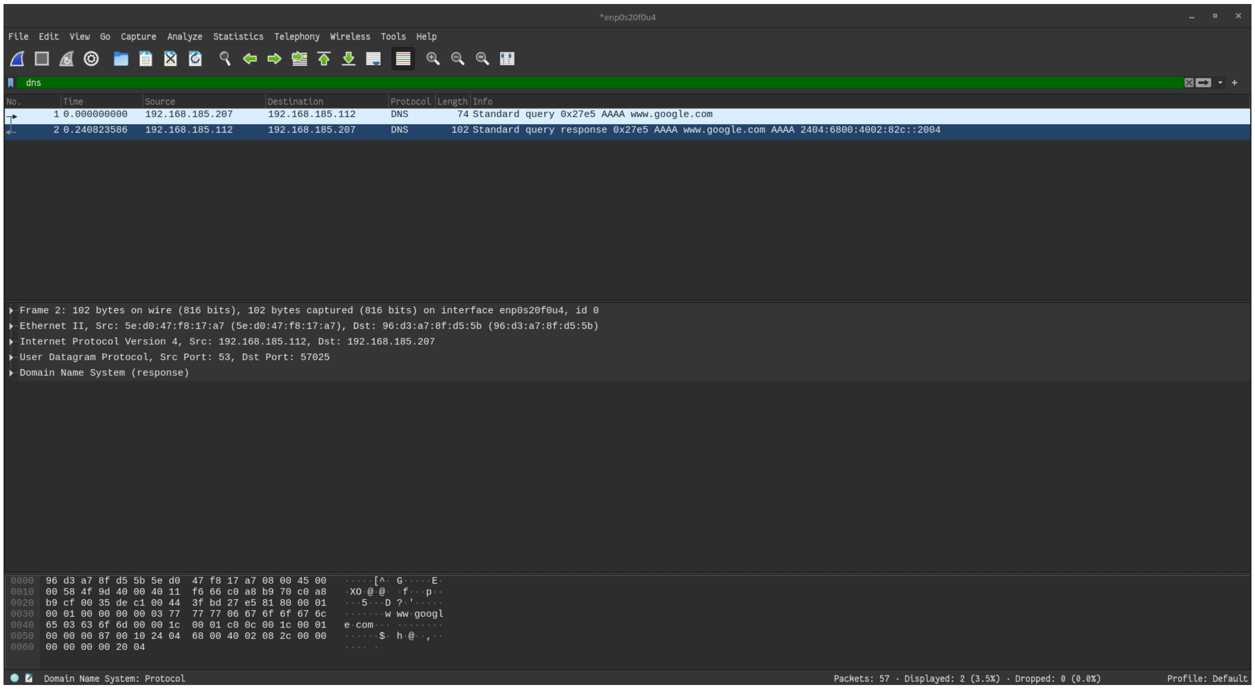
```
No.   Time         Source                    Destination               Protocol Length Info
   31 1.126974045  2409:4062:4e93:726b…  2404:6800:4002:82c:…  TCP        86 45040 → 80 [ACK] Seq=79 Ack=14497 Win=64128 Len=0 TSval=974026898 TSecr=3980653438
   32 1.126910916  2404:6800:4002:82c:…  2409:4062:4e93:726b…  TCP      1294 80 → 45040 [ACK] Seq=14497 Ack=79 Win=65536 Len=1208 TSval=3980653440 TSecr=974026814 [TCP segment of a reassembled PDU]
   33 1.127018449  2409:4062:4e93:726b…  2404:6800:4002:82c:…  TCP        86 45040 → 80 [ACK] Seq=79 Ack=15705 Win=62976 Len=0 TSval=974026898 TSecr=3980653440
   34 1.127036935  2404:6800:4002:82c:…  2409:4062:4e93:726b…  TCP      1294 80 → 45040 [PSH, ACK] Seq=15705 Ack=79 Win=65536 Len=1208 TSval=3980653440 TSecr=974026814 [TCP segment of a reassembled PDU]
   35 1.127045946  2409:4062:4e93:726b…  2404:6800:4002:82c:…  TCP        86 45040 → 80 [ACK] Seq=79 Ack=16913 Win=61824 Len=0 TSval=974026898 TSecr=3980653440
   36 1.133046008  2404:6800:4002:82c:…  2409:4062:4e93:726b…  HTTP     1120 HTTP/1.1 200 OK  (text/html)
   37 1.133093406  2409:4062:4e93:726b…  2404:6800:4002:82c:…  TCP        86 45040 → 80 [ACK] Seq=79 Ack=17947 Win=66560 Len=0 TSval=974026904 TSecr=3980653444
   38 1.133391249  2409:4062:4e93:726b…  2404:6800:4002:82c:…  TCP        86 45040 → 80 [FIN, ACK] Seq=79 Ack=17947 Win=66560 Len=0 TSval=974026904 TSecr=3980653444
```

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 28 Jul 2022 04:25:37 GMT\r\n
  Expires: -1\r\n
  Cache-Control: private, max-age=0\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
  P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."\r\n
  Server: gws\r\n
  X-XSS-Protection: 0\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  Set-Cookie: 1P_JAR=2022-07-28-04; expires=Sat, 27-Aug-2022 04:25:37 GMT; path=/; domain=.google.com; Secure\r\n
  Set-Cookie: AEC=AakniGM-Cm2tZwy--y0O6rKbOw9u2W0t-xQ0djibS5cSxOyCl-8Lf5CeYg; expires=Tue, 24-Jan-2023 04:25:37 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax\r\n
   [truncated]Set-Cookie: NID=511=QZvQJTehAN8D9ngm86sSmYedrxpsVyBSzy-9Xj51PZwYHvm2FkYiTd4jjT50bQ07Lo3LR7zNFGRoFhCvRlDZliQztor5Fjf0pc8gLJWjNw5MuV7X_T-eco8Wq9n-bpm96s56nPmh8uP4WWF2F-VTWKncFP7fKcD-1H1VcHIV-4M; e›
  Accept-Ranges: none\r\n
  Vary: Accept-Encoding\r\n
  Transfer-Encoding: chunked\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.807540748 seconds]
  [Request in frame: 6]
  [Request URI: http://www.google.com/]
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 54  68 75 2c 20 32 38 20 4a   ·Date: T hu, 28 J
0020  75 6c 20 32 30 32 32 20  30 34 3a 32 35 3a 33 37   ul 2022  04:25:37
0030  20 47 4d 54 0d 0a 45 78  70 69 72 65 73 3a 20 2d    GMT··Ex pires: -
0040  31 0d 0a 43 61 63 68 65  2d 43 6f 6e 74 72 6f 6c   1··Cache -Control
0050  3a 20 70 72 69 76 61 74  65 2c 20 6d 61 78 2d 61   : privat e, max-a
```

Frame (1120 bytes)
Reassembled TCP (17946 bytes)
De-chunked entity body (17019 bytes)
wireshark_enp0s20f0u4XmfrIF.pcapng
Packets: 57 · Displayed: 57 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Use “DNS” as a filter.


*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

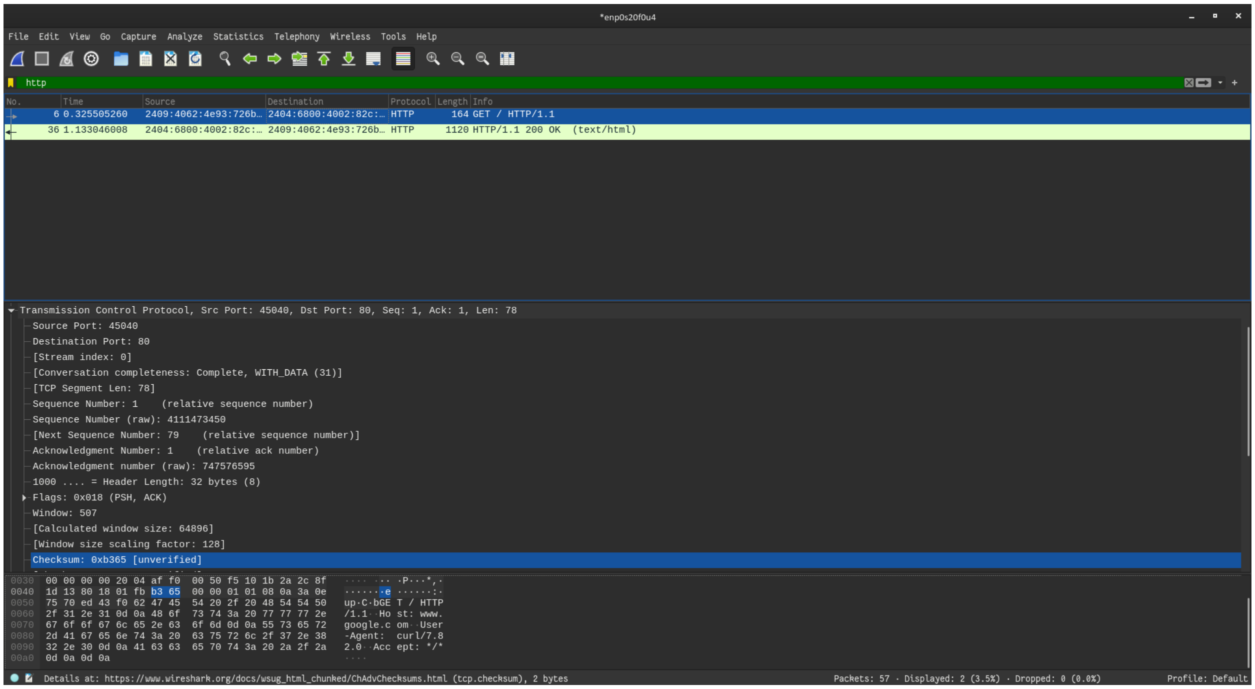
```
No.   Time         Source           Destination      Protocol Length Info
    1 0.000000000  192.168.185.207  192.168.185.112  DNS        74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586  192.168.185.112  192.168.185.207  DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
```

```
Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp0s20f0u4, id 0
Ethernet II, Src: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7), Dst: 96:d3:a7:8f:d5:5b (96:d3:a7:8f:d5:5b)
Internet Protocol Version 4, Src: 192.168.185.112, Dst: 192.168.185.207
User Datagram Protocol, Src Port: 53, Dst Port: 57025
Domain Name System (response)
```

```
0000  96 d3 a7 8f d5 5b 5e d0  47 f8 17 a7 08 00 45 00   ·····[^· G·····E·
0010  00 58 4f 9d 40 00 40 11  f6 66 c0 a8 b9 70 c0 a8   ·XO·@·@· ·f···p··
0020  b9 cf 00 35 de c1 00 44  3f bd 27 e5 81 80 00 01   ···5···D ?·'·····
0030  00 01 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 1c 00 01   e·com··· ········
0050  00 00 00 87 00 10 24 04  68 00 40 02 08 2c 00 00   ······$· h·@··,··
0060  00 00 00 00 20 04                                  ···· ·
```

Domain Name System: Protocol
Packets: 57 · Displayed: 2 (3.5%) · Dropped: 0 (0.0%)
Profile: Default

Use “HTTP” as a filter.



```
http
```

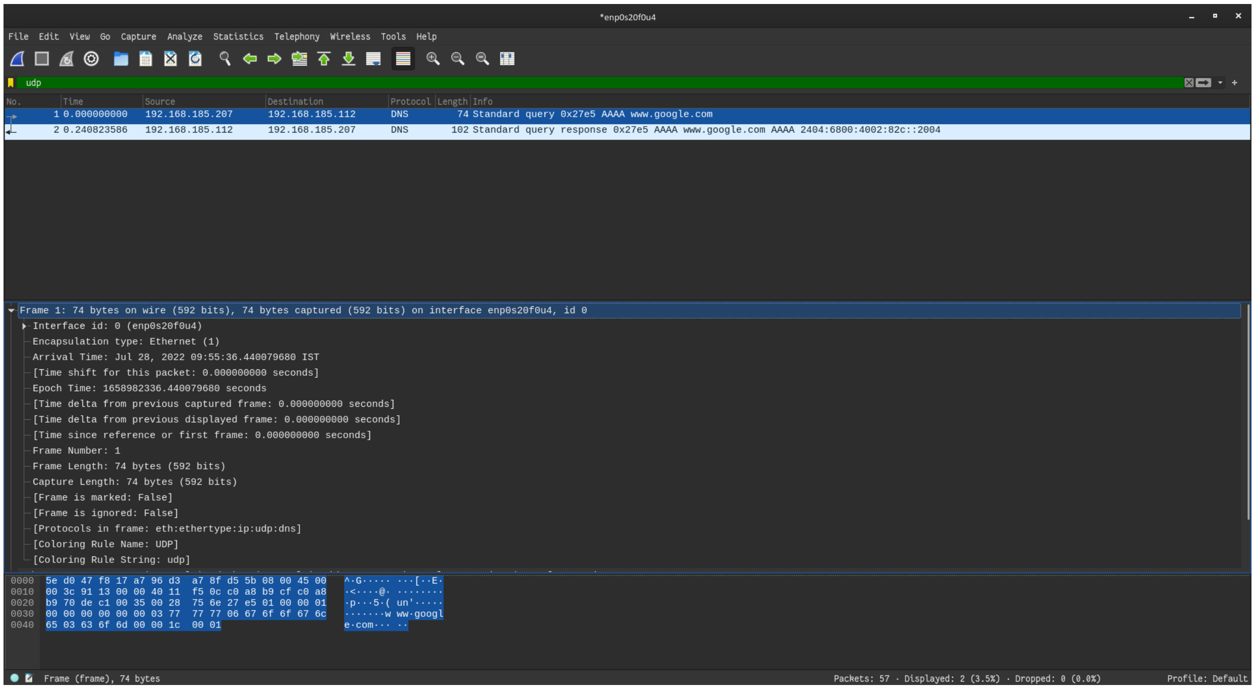
```
No.   Time         Source               Destination          Protocol Length Info
    6 0.325505260  2409:4062:4e93:726b… 2404:6800:4002:82c:… HTTP        164 GET / HTTP/1.1
   36 1.133046008  2404:6800:4002:82c:… 2409:4062:4e93:726b… HTTP       1120 HTTP/1.1 200 OK  (text/html)
```

```
Transmission Control Protocol, Src Port: 45040, Dst Port: 80, Seq: 1, Ack: 1, Len: 78
    Source Port: 45040
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 78]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4111473450
    [Next Sequence Number: 79    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 747576595
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 507
    [Calculated window size: 64896]
    [Window size scaling factor: 128]
    Checksum: 0xb365 [unverified]
```

```
0030  00 00 00 00 20 04 af f0  00 50 f5 10 1b 2a 2c 8f   ···· ·· ·P···*,·
0040  1d 13 80 18 01 fb b3 65  00 00 01 01 08 0a 3a 0e   ······ ·e ······:·
0050  75 70 ed 43 f0 62 47 45  54 20 2f 20 48 54 54 50   up·C·bGE T / HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0070  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om··User
0080  2d 41 67 65 6e 74 3a 20  63 75 72 6c 2f 37 2e 38   -Agent:  curl/7.8
0090  32 2e 30 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   2.0··Acc ept: */*
00a0  0d 0a 0d 0a                                        ····
```

```
Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum), 2 bytes    Packets: 57 · Displayed: 2 (3.5%) · Dropped: 0 (0.0%)    Profile: Default
```

Use “UDP” as a filter.



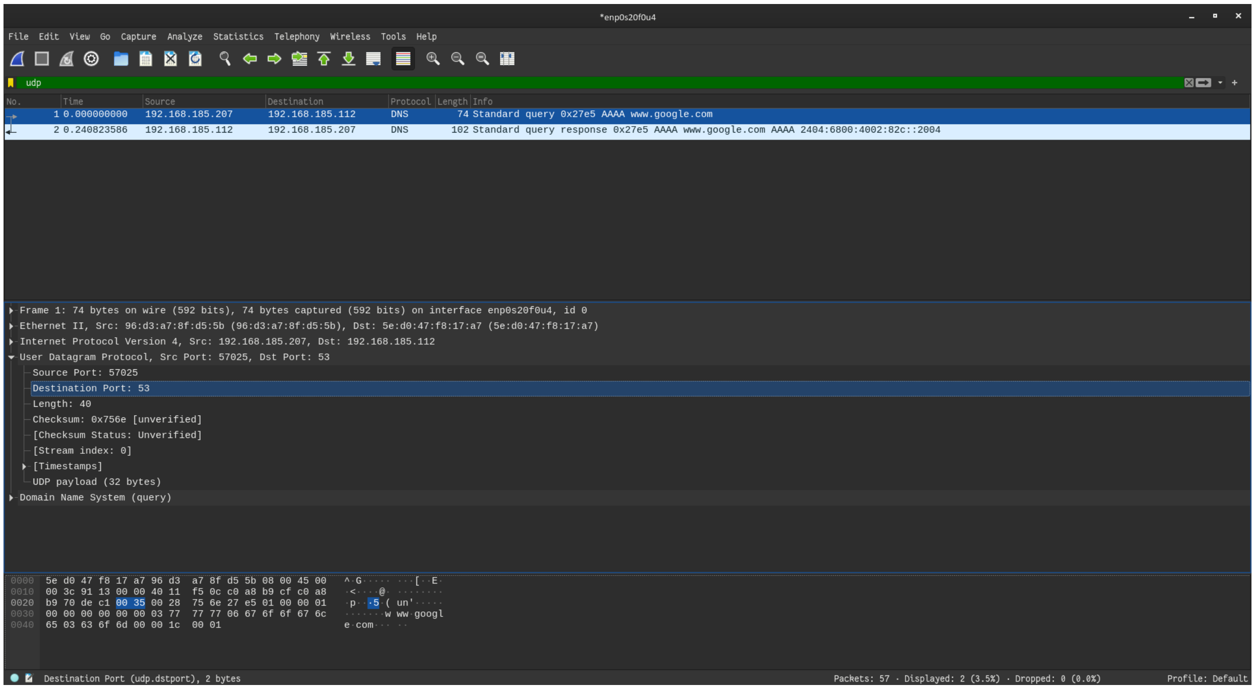
```
udp
```

```
No.   Time         Source           Destination      Protocol Length Info
    1 0.000000000  192.168.185.207  192.168.185.112  DNS          74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586  192.168.185.112  192.168.185.207  DNS         102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
```

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s20f0u4, id 0
  > Interface id: 0 (enp0s20f0u4)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 28, 2022 09:55:36.440079680 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1658982336.440079680 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    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:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

```
0000  5e d0 47 f8 17 a7 96 d3  a7 8f d5 5b 08 00 45 00   ^·G····· ···[··E·
0010  00 3c 91 13 00 00 40 11  f5 0c c0 a8 b9 cf c0 a8   ·<····@· ········
0020  b9 70 de c1 00 35 00 28  75 6e 27 e5 01 00 00 01   ·p···5·( un'·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01                     e·com··· ··
```

```
Frame (frame), 74 bytes    Packets: 57 · Displayed: 2 (3.5%) · Dropped: 0 (0.0%)    Profile: Default
```

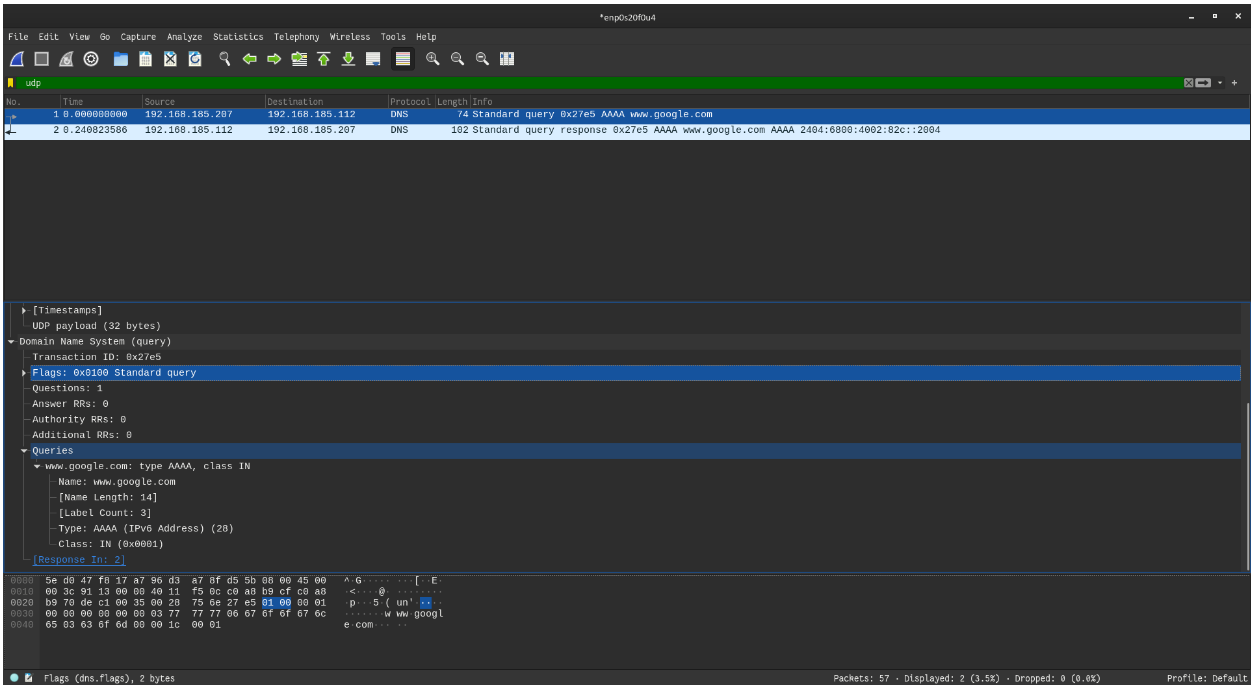

*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.   Time          Source            Destination       Protocol Length Info
    1 0.000000000   192.168.185.207   192.168.185.112   DNS        74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586   192.168.185.112   192.168.185.207   DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s20f0u4, id 0
▸ Ethernet II, Src: 96:d3:a7:8f:d5:5b (96:d3:a7:8f:d5:5b), Dst: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7)
▸ Internet Protocol Version 4, Src: 192.168.185.207, Dst: 192.168.185.112
▾ User Datagram Protocol, Src Port: 57025, Dst Port: 53
    Source Port: 57025
    Destination Port: 53
    Length: 40
    Checksum: 0x756e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (32 bytes)
▸ Domain Name System (query)
```

```
0000  5e d0 47 f8 17 a7 96 d3  a7 8f d5 5b 08 00 45 00   ^·G····· ···[··E·
0010  00 3c 91 13 00 00 40 11  f5 0c c0 a8 b9 cf c0 a8   ·<····@· ········
0020  b9 70 de c1 00 35 00 28  75 6e 27 e5 01 00 00 01   ·p···5·( un'·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01                     e·com··· ··
```

```
Destination Port (udp.dstport), 2 bytes          Packets: 57 · Displayed: 2 (3.5%) · Dropped: 0 (0.0%)          Profile: Default
```


*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

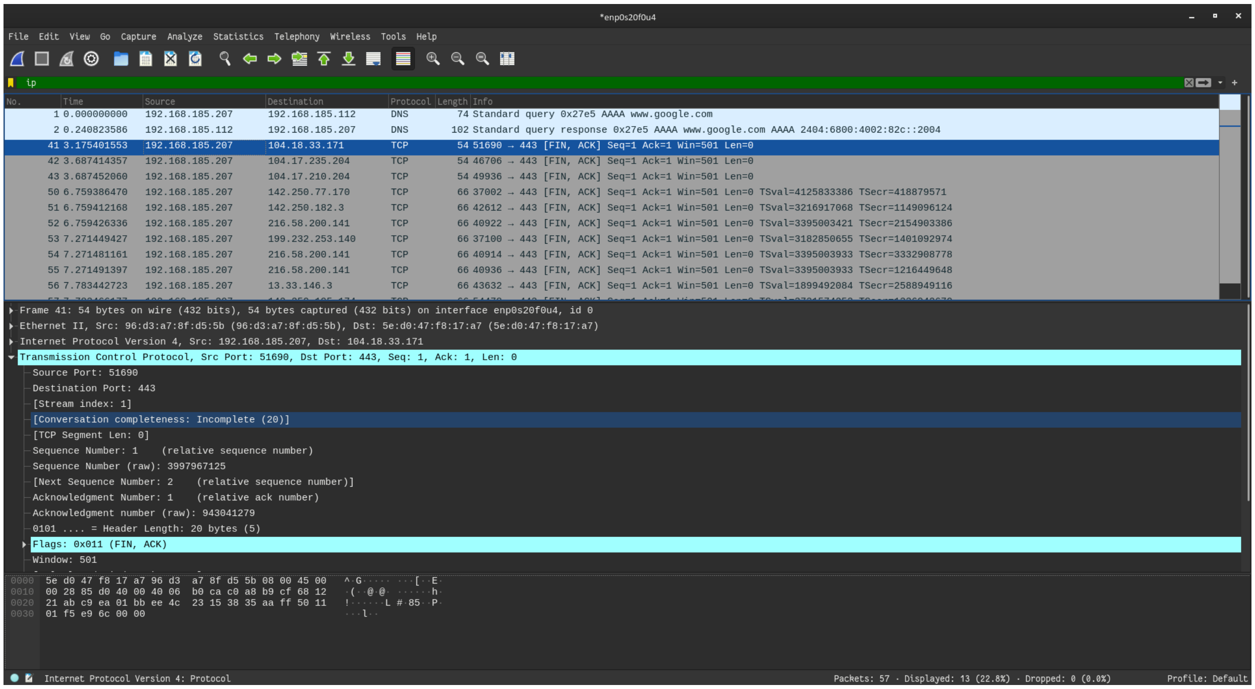
```
No.   Time          Source            Destination       Protocol Length Info
    1 0.000000000   192.168.185.207   192.168.185.112   DNS        74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586   192.168.185.112   192.168.185.207   DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
```

```
  ▸ [Timestamps]
    UDP payload (32 bytes)
▾ Domain Name System (query)
    Transaction ID: 0x27e5
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.google.com: type AAAA, class IN
        Name: www.google.com
        [Name Length: 14]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    [Response In: 2]
```

```
0000  5e d0 47 f8 17 a7 96 d3  a7 8f d5 5b 08 00 45 00   ^·G····· ···[··E·
0010  00 3c 91 13 00 00 40 11  f5 0c c0 a8 b9 cf c0 a8   ·<····@· ········
0020  b9 70 de c1 00 35 00 28  75 6e 27 e5 01 00 00 01   ·p···5·( un'·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01                     e·com··· ··
```

```
Flags (dns.flags), 2 bytes          Packets: 57 · Displayed: 2 (3.5%) · Dropped: 0 (0.0%)          Profile: Default
```

Use “IP” as a filter.



```
ip
```

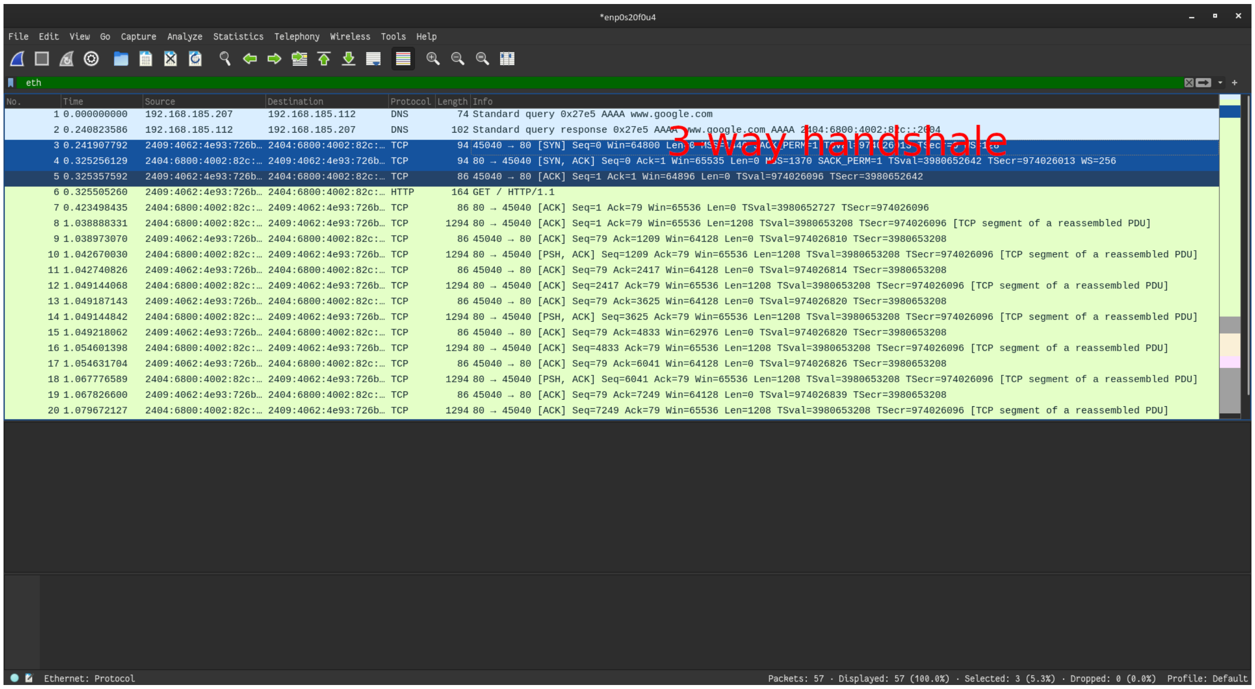
```
No.   Time         Source            Destination       Protocol Length Info
    1 0.000000000  192.168.185.207   192.168.185.112   DNS        74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586  192.168.185.112   192.168.185.207   DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
   41 3.175401553  192.168.185.207   104.18.33.171     TCP        54 51690 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
   42 3.687414357  192.168.185.207   104.17.235.204    TCP        54 46706 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
   43 3.687452060  192.168.185.207   104.17.210.204    TCP        54 49936 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
   50 6.759386470  192.168.185.207   142.250.77.170    TCP        66 37002 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4125833386 TSecr=418879571
   51 6.759412168  192.168.185.207   142.250.182.3     TCP        66 42612 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3216917068 TSecr=1149096124
   52 6.759426336  192.168.185.207   216.58.200.141    TCP        66 40922 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3395003421 TSecr=2154903386
   53 7.271449427  192.168.185.207   199.232.253.140   TCP        66 37100 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3182850655 TSecr=1401092974
   54 7.271481161  192.168.185.207   216.58.200.141    TCP        66 40914 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3395003933 TSecr=3332908778
   55 7.271491397  192.168.185.207   216.58.200.141    TCP        66 40936 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3395003933 TSecr=1216449648
   56 7.783442723  192.168.185.207   13.33.146.3       TCP        66 43632 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1899492084 TSecr=2588949116
```

```
▸ Frame 41: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s20f0u4, id 0
▸ Ethernet II, Src: 96:d3:a7:8f:d5:5b (96:d3:a7:8f:d5:5b), Dst: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7)
▸ Internet Protocol Version 4, Src: 192.168.185.207, Dst: 104.18.33.171
▾ Transmission Control Protocol, Src Port: 51690, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 51690
    Destination Port: 443
    [Stream index: 1]
    [Conversation completeness: Incomplete (20)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3997967125
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 943041279
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x011 (FIN, ACK)
    Window: 501
```

```
0000  5e d0 47 f8 17 a7 96 d3  a7 8f d5 5b 08 00 45 00   ^·G·····  ···[··E·
0010  00 28 85 d0 40 00 40 06  b0 ca c0 a8 b9 cf 68 12   ·(··@·@·  ······h·
0020  21 ab c9 ea 01 bb ee 4c  23 15 38 35 aa ff 50 11   !······L #·85··P·
0030  01 f5 e9 6c 00 00                                  ···l··
```

```
Internet Protocol Version 4: Protocol        Packets: 57 · Displayed: 13 (22.8%) · Dropped: 0 (0.0%)        Profile: Default
```

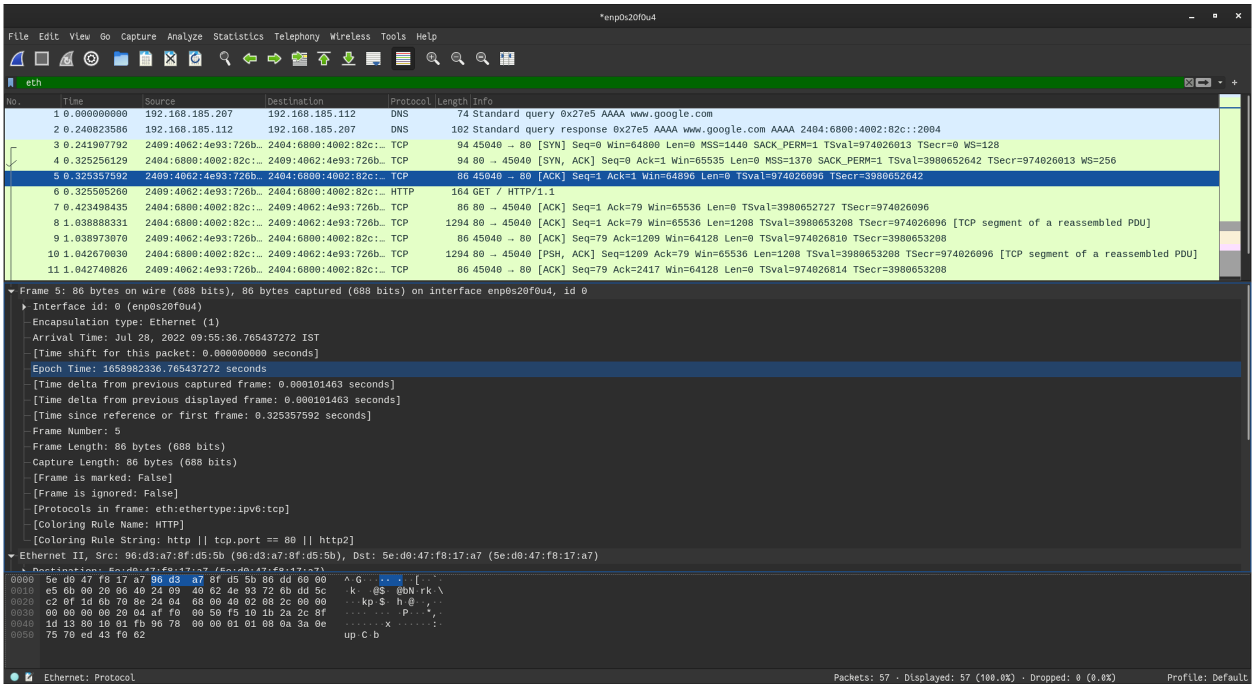
Use “eth0” as a filter.



```
eth
```

```
No.   Time         Source              Destination         Protocol Length Info
    1 0.000000000  192.168.185.207     192.168.185.112     DNS        74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586  192.168.185.112     192.168.185.207     DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
    3 0.241907792  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      94 45040 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=974026013 TSecr=0 WS=128
    4 0.325256129  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP      94 80 → 45040 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 TSval=3980652642 TSecr=974026013 WS=256
    5 0.325357592  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=974026096 TSecr=3980652642
    6 0.325505260  2409:4062:4e93:726b… 2404:6800:4002:82c:… HTTP    164 GET / HTTP/1.1
    7 0.423498435  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP      86 80 → 45040 [ACK] Seq=1 Ack=79 Win=65536 Len=0 TSval=3980652727 TSecr=974026096
    8 1.038888331  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=1 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
    9 1.038973070  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=1209 Win=64128 Len=0 TSval=974026810 TSecr=3980653208
   10 1.042670030  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [PSH, ACK] Seq=1209 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   11 1.042740826  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=2417 Win=64128 Len=0 TSval=974026814 TSecr=3980653208
   12 1.049144068  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=2417 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   13 1.049187143  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=3625 Win=64128 Len=0 TSval=974026820 TSecr=3980653208
   14 1.049144842  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [PSH, ACK] Seq=3625 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   15 1.049218062  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=4833 Win=62976 Len=0 TSval=974026820 TSecr=3980653208
   16 1.054601398  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=4833 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   17 1.054631704  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=6041 Win=64128 Len=0 TSval=974026826 TSecr=3980653208
   18 1.067776589  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [PSH, ACK] Seq=6041 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   19 1.067826600  2409:4062:4e93:726b… 2404:6800:4002:82c:… TCP      86 45040 → 80 [ACK] Seq=79 Ack=7249 Win=64128 Len=0 TSval=974026839 TSecr=3980653208
   20 1.079672127  2404:6800:4002:82c:… 2409:4062:4e93:726b… TCP    1294 80 → 45040 [ACK] Seq=7249 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
```

```
Ethernet: Protocol        Packets: 57 · Displayed: 57 (100.0%) · Selected: 3 (5.3%) · Dropped: 0 (0.0%)  Profile: Default
```



*enp0s20f0u4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eth

```
No.   Time         Source                 Destination            Protocol Length Info
    1 0.000000000  192.168.185.207        192.168.185.112        DNS        74 Standard query 0x27e5 AAAA www.google.com
    2 0.240823586  192.168.185.112        192.168.185.207        DNS       102 Standard query response 0x27e5 AAAA www.google.com AAAA 2404:6800:4002:82c::2004
    3 0.241907792  2409:4062:4e93:726b…   2404:6800:4002:82c:…   TCP        94 45040 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=974026013 TSecr=0 WS=128
    4 0.325256129  2404:6800:4002:82c:…   2409:4062:4e93:726b…   TCP        94 80 → 45040 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM=1 TSval=3980652642 TSecr=974026013 WS=256
    5 0.325357592  2409:4062:4e93:726b…   2404:6800:4002:82c:…   TCP        86 45040 → 80 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=974026096 TSecr=3980652642
    6 0.325505260  2409:4062:4e93:726b…   2404:6800:4002:82c:…   HTTP      164 GET / HTTP/1.1
    7 0.423498435  2404:6800:4002:82c:…   2409:4062:4e93:726b…   TCP        86 80 → 45040 [ACK] Seq=1 Ack=79 Win=65536 Len=0 TSval=3980652727 TSecr=974026096
    8 1.038888331  2404:6800:4002:82c:…   2409:4062:4e93:726b…   TCP      1294 80 → 45040 [ACK] Seq=1 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
    9 1.038973070  2409:4062:4e93:726b…   2404:6800:4002:82c:…   TCP        86 45040 → 80 [ACK] Seq=79 Ack=1209 Win=64128 Len=0 TSval=974026810 TSecr=3980653208
   10 1.042670030  2404:6800:4002:82c:…   2409:4062:4e93:726b…   TCP      1294 80 → 45040 [PSH, ACK] Seq=1209 Ack=79 Win=65536 Len=1208 TSval=3980653208 TSecr=974026096 [TCP segment of a reassembled PDU]
   11 1.042740826  2409:4062:4e93:726b…   2404:6800:4002:82c:…   TCP        86 45040 → 80 [ACK] Seq=79 Ack=2417 Win=64128 Len=0 TSval=974026814 TSecr=3980653208
```

```
Frame 5: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s20f0u4, id 0
  Interface id: 0 (enp0s20f0u4)
  Encapsulation type: Ethernet (1)
  Arrival Time: Jul 28, 2022 09:55:36.765437272 IST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1658982336.765437272 seconds
  [Time delta from previous captured frame: 0.000101463 seconds]
  [Time delta from previous displayed frame: 0.000101463 seconds]
  [Time since reference or first frame: 0.325357592 seconds]
  Frame Number: 5
  Frame Length: 86 bytes (688 bits)
  Capture Length: 86 bytes (688 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ipv6:tcp]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: 96:d3:a7:8f:d5:5b (96:d3:a7:8f:d5:5b), Dst: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7)
  Destination: 5e:d0:47:f8:17:a7 (5e:d0:47:f8:17:a7)
```

```
0000  5e d0 47 f8 17 a7 96 d3  a7 8f d5 5b 86 dd 60 00   ^·G·········[··`·
0010  e5 6b 00 20 06 40 24 09  40 62 4e 93 72 6b dd 5c   ·k· ·@$· @bN·rk·\
0020  c2 0f 1d 6b 70 8e 24 04  68 00 40 02 08 2c 00 00   ···kp·$· h·@··,··
0030  00 00 00 00 20 04 af f0  00 50 f5 10 1b 2a 2c 8f   ···· ··· ·P···*,·
0040  1d 13 80 10 01 fb 96 78  00 00 01 01 08 0a 3a 0e   ·······x ······:·
0050  75 70 ed 43 f0 62                                  up·C·b
```

```
Ethernet: Protocol                    Packets: 57 · Displayed: 57 (100.0%) · Dropped: 0 (0.0%)     Profile: Default
```

20051554

Dipankar Das

Lab03