LINUX NETWORKING MODULE 7 AND 8 ASSESSMENT SOLUTION

-BY SAKTHI KUMAR S

2. Use Wireshark to capture and analyse DNS, TCP, UDP traffic and packet header, packet flow, options and flags.

Ethernet Header (Layer 2 – Data Link Layer)

- **Destination MAC Address**: The recipient's MAC address.
- **Source MAC Address**: The sender's MAC address.
- **EtherType**: Indicates the payload type (e.g., IPv4, IPv6).

IP Header (Layer 3 – Network Layer)

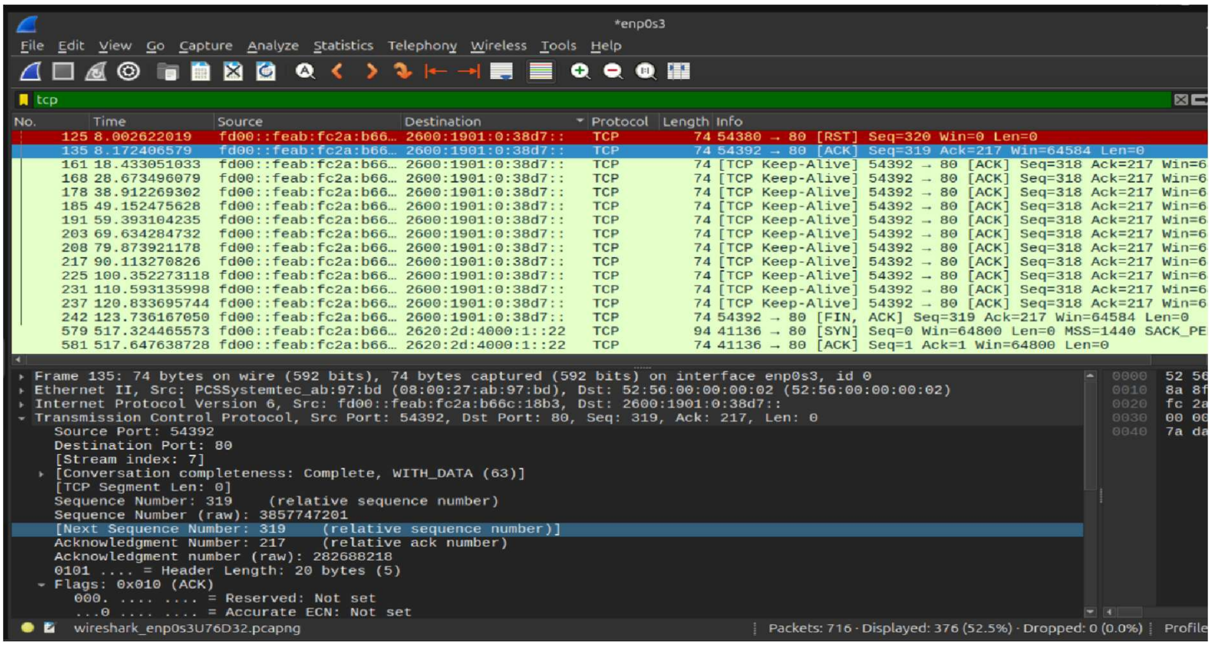
- **Version**: IPv4 (4) or IPv6 (6).
- **Header Length**: Specifies the length of the IP header.
- **Source IP Address**: The sender's IP address.
- **Destination IP Address**: The receiver's IP address.
- **Time to Live (TTL)**: Limits how long a packet exists before being discarded.
- **Protocol**: Identifies the transport layer protocol (TCP = 6, UDP = 17).
- **Checksum**: Ensures integrity of the IP header.

TCP Header (Layer 4 – Transport Layer)

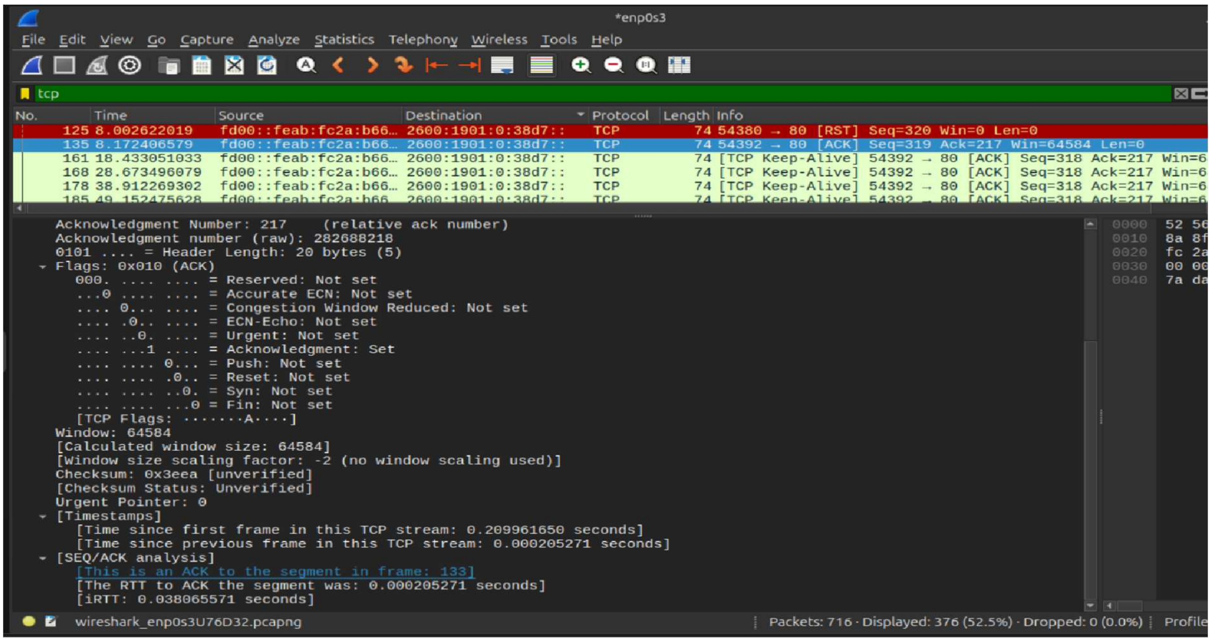
TCP provides **reliable, connection-oriented communication**.

- **Source & Destination Ports**: Identifies the application/service.
- **Sequence Number**: Tracks packet ordering.
- **Acknowledgment Number**: Confirms receipt of previous packets.
- **Flags**: Controls the connection state:
  - SYN: Initiates a connection.
  - ACK: Acknowledges a packet.
  - FIN: Terminates a connection.
  - RST: Resets a connection.
  - PSH: Forces immediate data transfer.
  - URG: Marks urgent data.
- **Window Size**: Controls data flow.

- **Checksum**: Ensures data integrity.


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.    Time           Source              Destination          Protocol Length Info
   125 8.002622019    fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 54380 → 80 [RST] Seq=320 Win=0 Len=0
   135 8.172406579    fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 54392 → 80 [ACK] Seq=319 Ack=217 Win=64584 Len=0
   161 18.433051033   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   168 28.673496079   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   178 38.912269302   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   185 49.152475628   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   191 59.393104235   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   203 69.634284732   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   208 79.873921178   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   217 90.113270826   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   225 100.352273118  fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   231 110.593135998  fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   237 120.833695744  fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   242 123.736167050  fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 54392 → 80 [FIN, ACK] Seq=319 Ack=217 Win=64584 Len=0
   579 517.324465573  fd00::feab:fc2a:b66… 2620:2d:4000:1::22  TCP       94 41136 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PE
   581 517.647638728  fd00::feab:fc2a:b66… 2620:2d:4000:1::22  TCP       74 41136 → 80 [ACK] Seq=1 Ack=1 Win=64800 Len=0

▸ Frame 135: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0      0000  52 56
▸ Ethernet II, Src: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd), Dst: 52:56:00:00:00:02 (52:56:00:00:00:02)  0010  8a 8f
▸ Internet Protocol Version 6, Src: fd00::feab:fc2a:b66c:18b3, Dst: 2600:1901:0:38d7::                   0020  fc 2a
▾ Transmission Control Protocol, Src Port: 54392, Dst Port: 80, Seq: 319, Ack: 217, Len: 0             0030  00 00
    Source Port: 54392                                                                                  0040  7a da
    Destination Port: 80
    [Stream index: 7]
  ▸ [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 319    (relative sequence number)
    Sequence Number (raw): 3857747201
    [Next Sequence Number: 319    (relative sequence number)]
    Acknowledgment Number: 217    (relative ack number)
    Acknowledgment number (raw): 282688218
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set

wireshark_enp0s3U76D32.pcapng          Packets: 716 · Displayed: 376 (52.5%) · Dropped: 0 (0.0%)  Profile
```


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

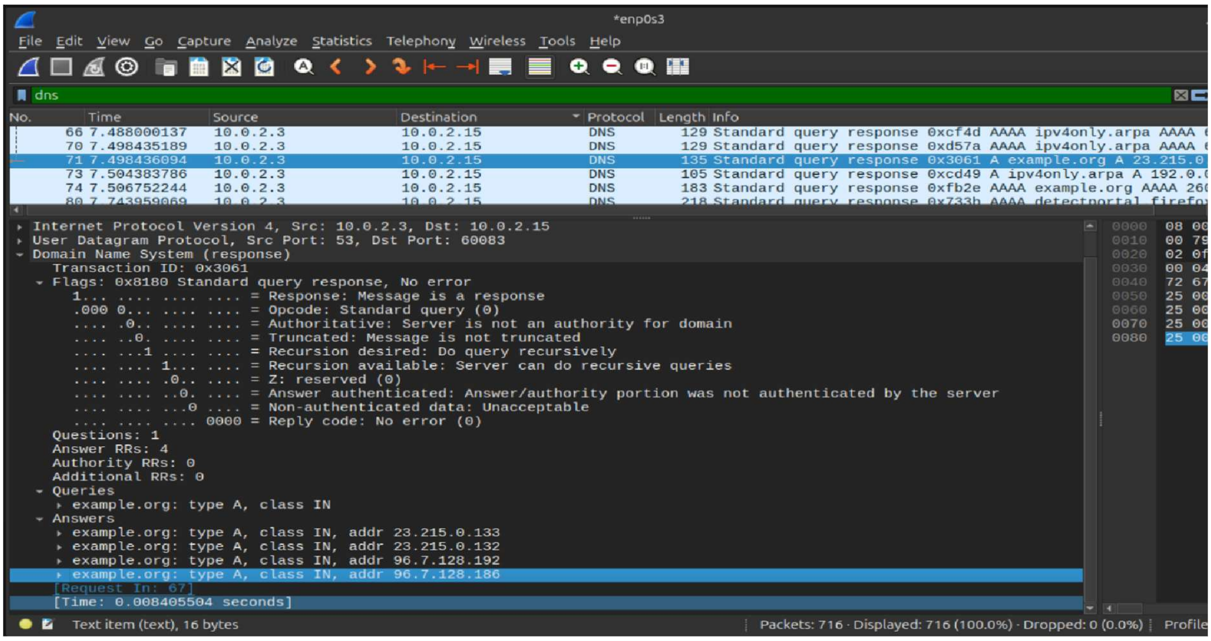
```
No.    Time           Source              Destination          Protocol Length Info
   125 8.002622019    fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 54380 → 80 [RST] Seq=320 Win=0 Len=0
   135 8.172406579    fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 54392 → 80 [ACK] Seq=319 Ack=217 Win=64584 Len=0
   161 18.433051033   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   168 28.673496079   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6
   178 38.912269302   fd00::feab:fc2a:b66… 2600:1901:0:38d7::  TCP       74 [TCP Keep-Alive] 54392 → 80 [ACK] Seq=318 Ack=217 Win=6

    Acknowledgment Number: 217    (relative ack number)                 0000  52 56
    Acknowledgment number (raw): 282688218                              0010  8a 8f
    0101 .... = Header Length: 20 bytes (5)                             0020  fc 2a
  ▾ Flags: 0x010 (ACK)                                                  0030  00 00
      000. .... .... = Reserved: Not set                                0040  7a da
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window: 64584
    [Calculated window size: 64584]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x3eea [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.209961650 seconds]
      [Time since previous frame in this TCP stream: 0.000205271 seconds]
  ▾ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 133]
      [The RTT to ACK the segment was: 0.000205271 seconds]
      [iRTT: 0.038065571 seconds]

wireshark_enp0s3U76D32.pcapng          Packets: 716 · Displayed: 376 (52.5%) · Dropped: 0 (0.0%)  Profile
```

DNS Header (Layer 7 – Application Layer)

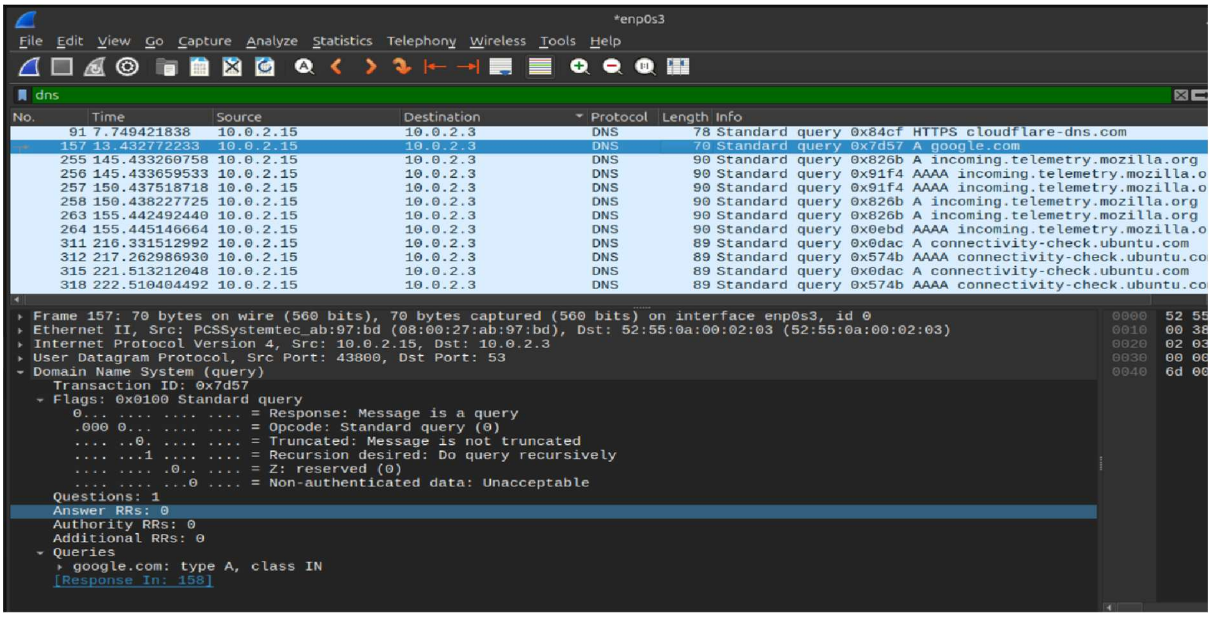
DNS resolves **domain names to IP addresses** and operates over UDP (by default) or TCP (for large queries).

- **Transaction ID**: A unique identifier for each query.
- **Flags**: Indicates query/response type and recursion status.

- **Questions & Answers**: Specifies domain name resolutions.
- **TTL (Time to Live)**: Determines how long the response is valid.


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns

No.     Time          Source        Destination     Protocol Length Info
     66 7.488000137   10.0.2.3      10.0.2.15       DNS        129 Standard query response 0xcf4d AAAA ipv4only.arpa AAAA
     70 7.498435189   10.0.2.3      10.0.2.15       DNS        129 Standard query response 0xd57a AAAA ipv4only.arpa AAAA
     71 7.498436094   10.0.2.3      10.0.2.15       DNS        135 Standard query response 0x3061 A example.org A 23.215.0
     73 7.504383786   10.0.2.3      10.0.2.15       DNS        105 Standard query response 0xcd49 A ipv4only.arpa A 192.0.
     74 7.506752244   10.0.2.3      10.0.2.15       DNS        183 Standard query response 0xfb2e AAAA example.org AAAA 26
     80 7.743959069   10.0.2.3      10.0.2.15       DNS        218 Standard query response 0x733b AAAA detectportal.firefo

▸ Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 60083
▾ Domain Name System (response)
    Transaction ID: 0x3061
  ▾ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ example.org: type A, class IN
  ▾ Answers
    ▸ example.org: type A, class IN, addr 23.215.0.133
    ▸ example.org: type A, class IN, addr 23.215.0.132
    ▸ example.org: type A, class IN, addr 96.7.128.192
    ▸ example.org: type A, class IN, addr 96.7.128.186
    [Request In: 67]
    [Time: 0.008405504 seconds]

0000  08 00
0010  00 79
0020  02 0f
0030  00 04
0040  72 67
0050  25 00
0060  25 00
0070  25 00
0080  25 00

Text item (text), 16 bytes        Packets: 716 · Displayed: 716 (100.0%) · Dropped: 0 (0.0%)   Profile
```

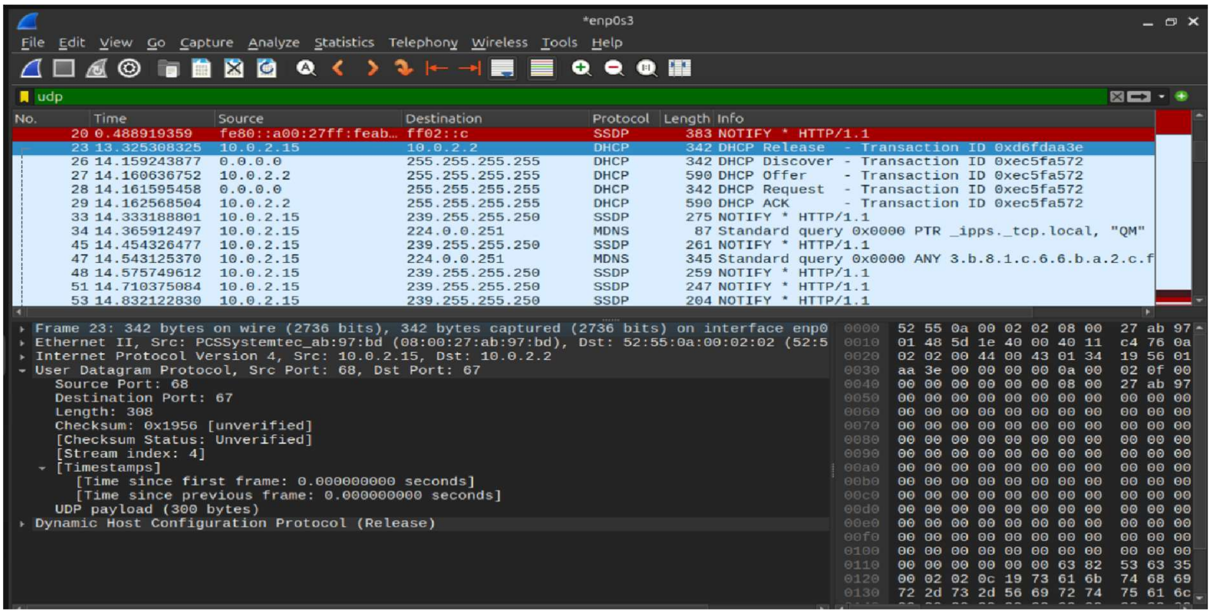

*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns

No.     Time           Source        Destination     Protocol Length Info
     91 7.749421838    10.0.2.15     10.0.2.3        DNS         78 Standard query 0x84cf HTTPS cloudflare-dns.com
    157 13.432772233   10.0.2.15     10.0.2.3        DNS         70 Standard query 0x7d57 A google.com
    255 145.433260758  10.0.2.15     10.0.2.3        DNS         90 Standard query 0x826b A incoming.telemetry.mozilla.org
    256 145.433659533  10.0.2.15     10.0.2.3        DNS         90 Standard query 0x91f4 AAAA incoming.telemetry.mozilla.o
    257 150.437518718  10.0.2.15     10.0.2.3        DNS         90 Standard query 0x91f4 AAAA incoming.telemetry.mozilla.o
    258 150.438227725  10.0.2.15     10.0.2.3        DNS         90 Standard query 0x826b A incoming.telemetry.mozilla.org
    263 155.442492440  10.0.2.15     10.0.2.3        DNS         90 Standard query 0x826b A incoming.telemetry.mozilla.org
    264 155.445146664  10.0.2.15     10.0.2.3        DNS         90 Standard query 0x0ebd AAAA incoming.telemetry.mozilla.o
    311 216.331512992  10.0.2.15     10.0.2.3        DNS         89 Standard query 0x0dac A connectivity-check.ubuntu.com
    312 217.262986930  10.0.2.15     10.0.2.3        DNS         89 Standard query 0x574b AAAA connectivity-check.ubuntu.co
    315 221.513212048  10.0.2.15     10.0.2.3        DNS         89 Standard query 0x0dac A connectivity-check.ubuntu.com
    318 222.510404492  10.0.2.15     10.0.2.3        DNS         89 Standard query 0x574b AAAA connectivity-check.ubuntu.co

▸ Frame 157: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
▸ User Datagram Protocol, Src Port: 43800, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x7d57
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ google.com: type A, class IN
    [Response In: 158]

0000  52 55
0010  00 38
0020  02 03
0030  00 00
0040  6d 00
```

UDP Header (Layer 4 – Transport Layer)

UDP provides **fast, connectionless communication** with minimal overhead.

- **Source & Destination Ports**: Identifies application endpoints.
- **Length**: Specifies packet size.
- **Checksum**: Validates integrity.



udp

```
No.   Time          Source                   Destination        Protocol  Length Info
   20 0.488919359   fe80::a00:27ff:feab…     ff02::c            SSDP       383 NOTIFY * HTTP/1.1
   23 13.325308325  10.0.2.15                10.0.2.2           DHCP       342 DHCP Release   - Transaction ID 0xd6fdaa3e
   26 14.159243877  0.0.0.0                  255.255.255.255    DHCP       342 DHCP Discover - Transaction ID 0xec5fa572
   27 14.160636752  10.0.2.2                 255.255.255.255    DHCP       590 DHCP Offer     - Transaction ID 0xec5fa572
   28 14.161595458  0.0.0.0                  255.255.255.255    DHCP       342 DHCP Request   - Transaction ID 0xec5fa572
   29 14.162568504  10.0.2.2                 255.255.255.255    DHCP       590 DHCP ACK       - Transaction ID 0xec5fa572
   33 14.333188801  10.0.2.15                239.255.255.250    SSDP       275 NOTIFY * HTTP/1.1
   34 14.365912497  10.0.2.15                224.0.0.251        MDNS        87 Standard query 0x0000 PTR _ipps._tcp.local, "QM"
   45 14.454326477  10.0.2.15                239.255.255.250    SSDP       261 NOTIFY * HTTP/1.1
   47 14.543125370  10.0.2.15                224.0.0.251        MDNS       345 Standard query 0x0000 ANY 3.b.8.1.c.6.6.b.a.2.c.f
   48 14.575749612  10.0.2.15                239.255.255.250    SSDP       259 NOTIFY * HTTP/1.1
   51 14.710375084  10.0.2.15                239.255.255.250    SSDP       247 NOTIFY * HTTP/1.1
   53 14.832122830  10.0.2.15                239.255.255.250    SSDP       204 NOTIFY * HTTP/1.1
```

```
▸ Frame 23: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface enp0
▸ Ethernet II, Src: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd), Dst: 52:55:0a:00:02:02 (52:5
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2
▾ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0x1956 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  ▾ [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (300 bytes)
▸ Dynamic Host Configuration Protocol (Release)
```

```
0000  52 55 0a 00 02 02 08 00  27 ab 97
0010  01 48 5d 1e 40 00 40 11  c4 76 0a
0020  02 02 00 44 00 43 01 34  19 56 01
0030  aa 3e 00 00 00 00 0a 00  02 0f 00
0040  00 00 00 00 00 00 08 00  27 ab 97
0050  00 00 00 00 00 00 00 00  00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00
0110  00 00 00 00 00 00 63 82  53 63 35
0120  00 02 02 0c 19 73 61 6b  74 68 69
0130  72 2d 73 2d 56 69 72 74  75 61 6c
```