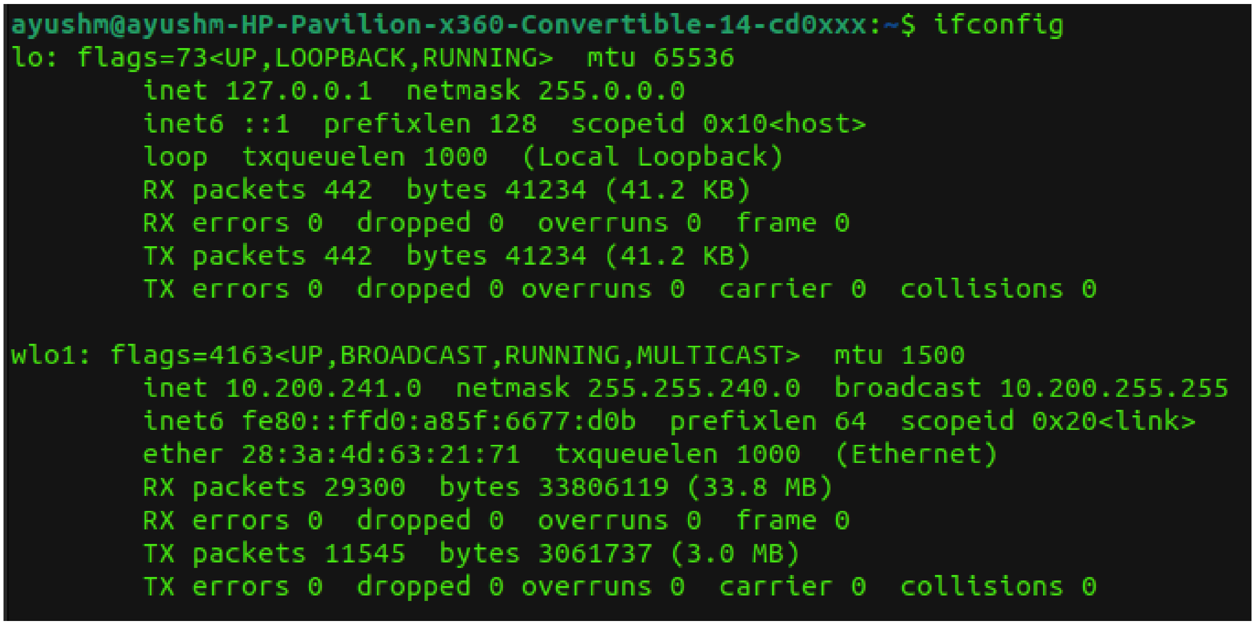
CS 315 : Computer Networks Lab
Assignment - 7
Wireshark Lab: IP

Ayush Mallick
CS22BT008

Part-0



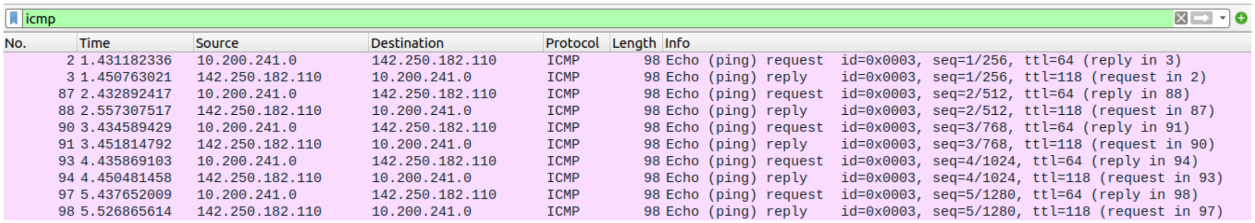
```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 442  bytes 41234 (41.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 442  bytes 41234 (41.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.200.241.0  netmask 255.255.240.0  broadcast 10.200.255.255
        inet6 fe80::ffd0:a85f:6677:d0b  prefixlen 64  scopeid 0x20<link>
        ether 28:3a:4d:63:21:71  txqueuelen 1000  (Ethernet)
        RX packets 29300  bytes 33806119 (33.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11545  bytes 3061737 (3.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Part-1

1.1

Source IP : *10.200.241.0*
Destination IP : *142.250.182.110*



icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	1.431182336	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 3)
3	1.450763021	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=118 (request in 2)
87	2.432892417	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply in 88)
88	2.557307517	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=118 (request in 87)
90	3.434589429	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply in 91)
91	3.451814792	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=118 (request in 90)
93	4.435869103	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (reply in 94)
94	4.450481458	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=118 (request in 93)
97	5.437652009	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (reply in 98)
98	5.526865614	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=118 (request in 97)

1.2

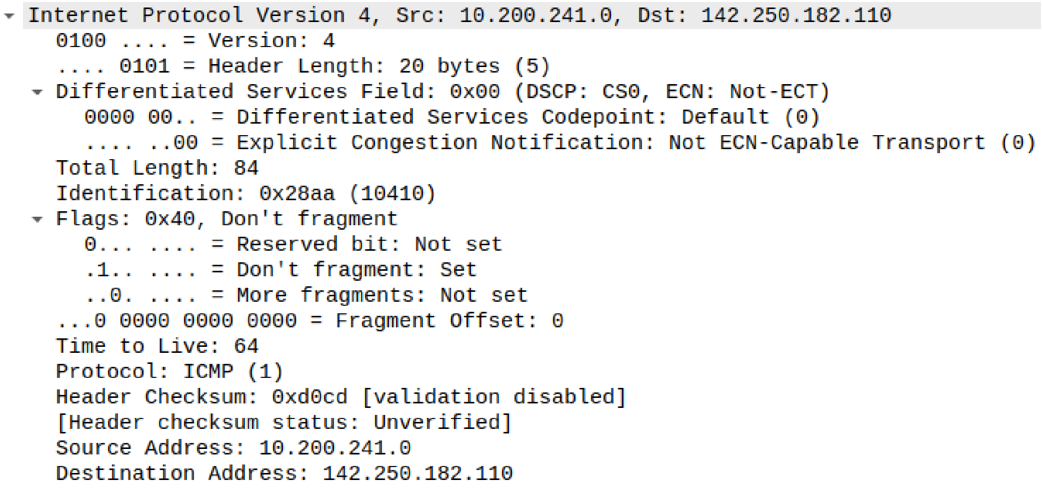
ICMP (1)

1.3

There are a total of *12* fields in the IPv4 header, excluding sub-fields.

- Version (*4* bits)
- Header Length (*4* bits)
- Differentiated Services Field (*8* bits)
  - Differentiated Services Codepoint (*6* bits)
  - Explicit Congestion Notification (*2* bits)
- Total Length (*16* bits)
- Identification (*16* bits)
- Flags (*3* bits)
  - Reserved bit (*1* bit)
  - Don’t fragment (*1* bit)
  - More fragments (*1* bit)
- Fragment Offset (*13* bits)
- Time to Live (*8* bits)
- Protocol (*8* bits)
- Header Checksum (*16* bits)
- Source Address (*32* bits)
- Destination Address (*32* bits)

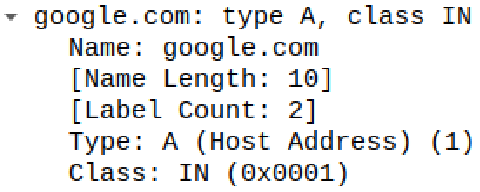
The size of the IPv4 header is *20* bytes, as mentioned in the Header Length field.



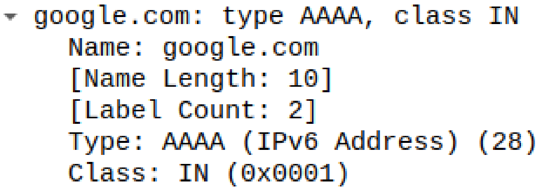
```
▾ Internet Protocol Version 4, Src: 10.200.241.0, Dst: 142.250.182.110
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x28aa (10410)
  ▾ Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xd0cd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.241.0
    Destination Address: 142.250.182.110
```

1.4

There are *2* types of queries observed. *A* query type is observed for *IPv4*, and *AAAA* query type is observed for *IPv6*.



```
▾ google.com: type A, class IN
    Name: google.com
    [Name Length: 10]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```



```
▾ google.com: type AAAA, class IN
    Name: google.com
    [Name Length: 10]
    [Label Count: 2]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
```

1.5

Time to Live (TTL) : *64*

1.6

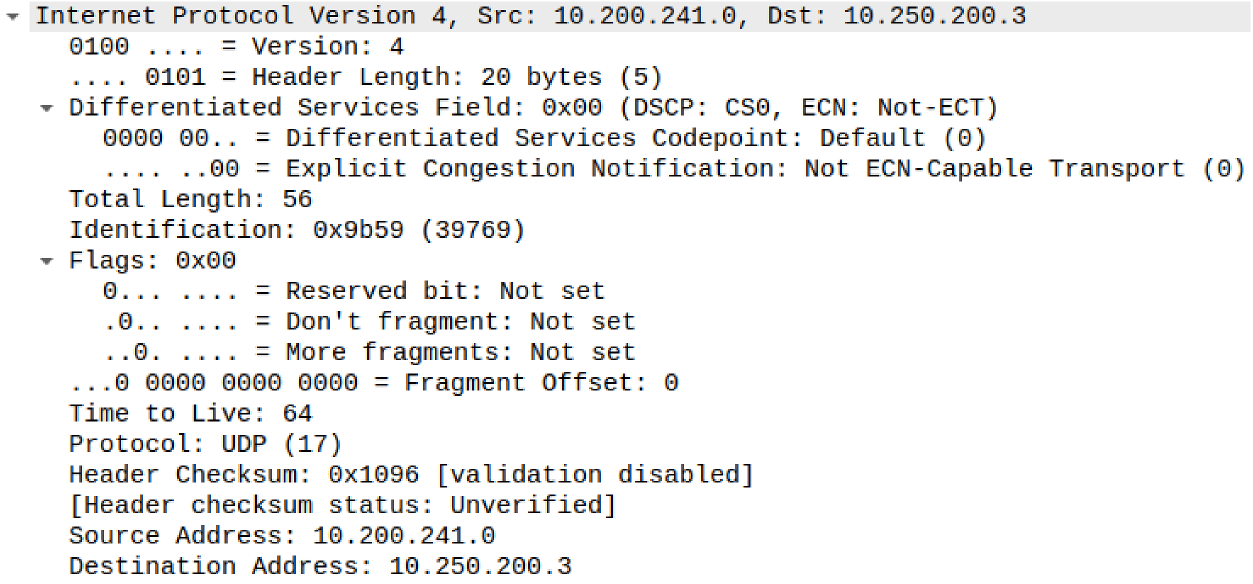
Protocol : *UDP (17)*

1.7

Number of bytes in payload of IP datagram =
Total Length - Header Length
= *56* - *20* = *36* bytes

1.8

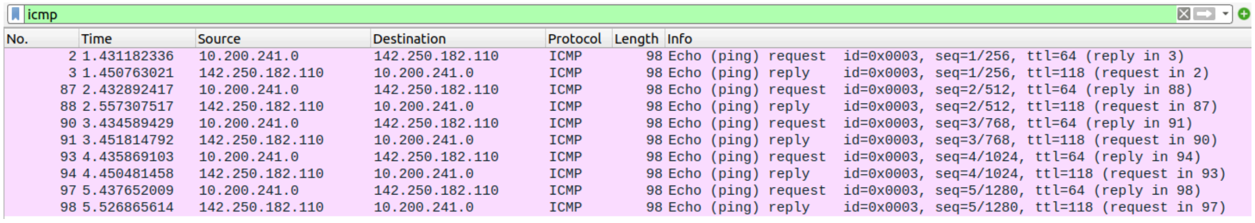
No, the IP datagram is not fragmented, as indicated by the More fragments bit, which is set to 0 (not set), and the Fragment offset field is set to 0.



```
▾ Internet Protocol Version 4, Src: 10.200.241.0, Dst: 10.250.200.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x9b59 (39769)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x1096 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.241.0
    Destination Address: 10.250.200.3
```

1.9

Requests sent : *5*
Replies received : *5*



icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	1.431182336	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 3)
3	1.450763021	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=118 (request in 2)
87	2.432892417	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply in 88)
88	2.557307517	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=118 (request in 87)
90	3.434589429	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply in 91)
91	3.451814792	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=118 (request in 90)
93	4.435869103	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (reply in 94)
94	4.450481458	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=118 (request in 93)
97	5.437652009	10.200.241.0	142.250.182.110	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (reply in 98)
98	5.526865614	142.250.182.110	10.200.241.0	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=118 (request in 97)

1.10

ICMP type for requests sent : *8 (Echo (ping) request)*
ICMP type for replies received : *0 (Echo (ping) reply)*

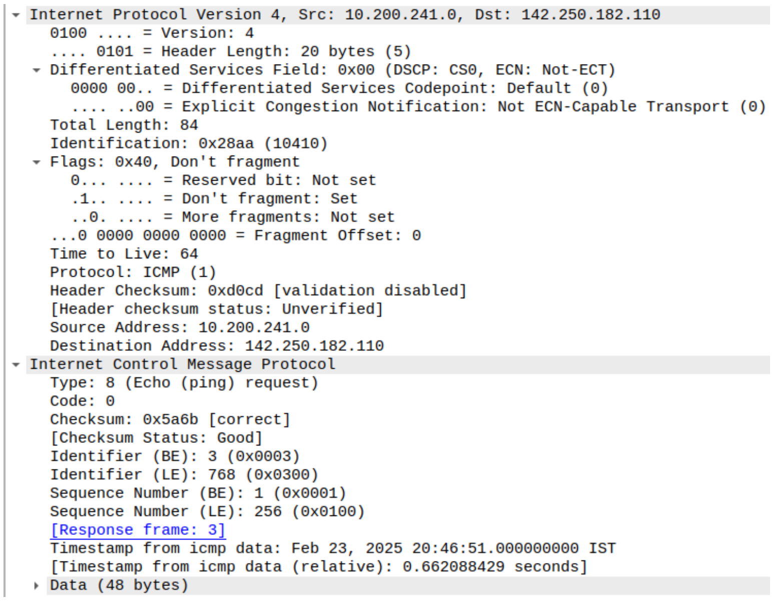
1.11

Fields that vary :

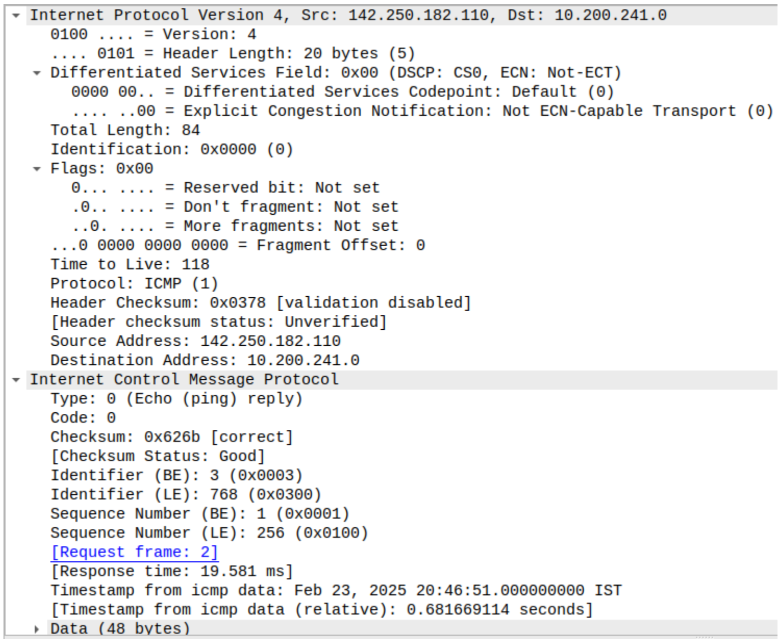
Identification, Flags, Time to Live, Source Address, Destination Address

Fields that remain same :

Version, Header Length, Differentiated Services Field, Total Length, Protocol



```
Internet Protocol Version 4, Src: 10.200.241.0, Dst: 142.250.182.110
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 84
  Identification: 0x28aa (10410)
  Flags: 0x40, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0xd0cd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.200.241.0
  Destination Address: 142.250.182.110
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x5a6b [correct]
  [Checksum Status: Good]
  Identifier (BE): 3 (0x0003)
  Identifier (LE): 768 (0x0300)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 3]
  Timestamp from icmp data: Feb 23, 2025 20:46:51.000000000 IST
  [Timestamp from icmp data (relative): 0.662088429 seconds]
  Data (48 bytes)
```



```
Internet Protocol Version 4, Src: 142.250.182.110, Dst: 10.200.241.0
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 84
  Identification: 0x0000 (0)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 118
  Protocol: ICMP (1)
  Header Checksum: 0x0378 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 142.250.182.110
  Destination Address: 10.200.241.0
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x626b [correct]
  [Checksum Status: Good]
  Identifier (BE): 3 (0x0003)
  Identifier (LE): 768 (0x0300)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Request frame: 2]
  [Response time: 19.581 ms]
  Timestamp from icmp data: Feb 23, 2025 20:46:51.000000000 IST
  [Timestamp from icmp data (relative): 0.681669114 seconds]
  Data (48 bytes)
```

Part-2

2.1

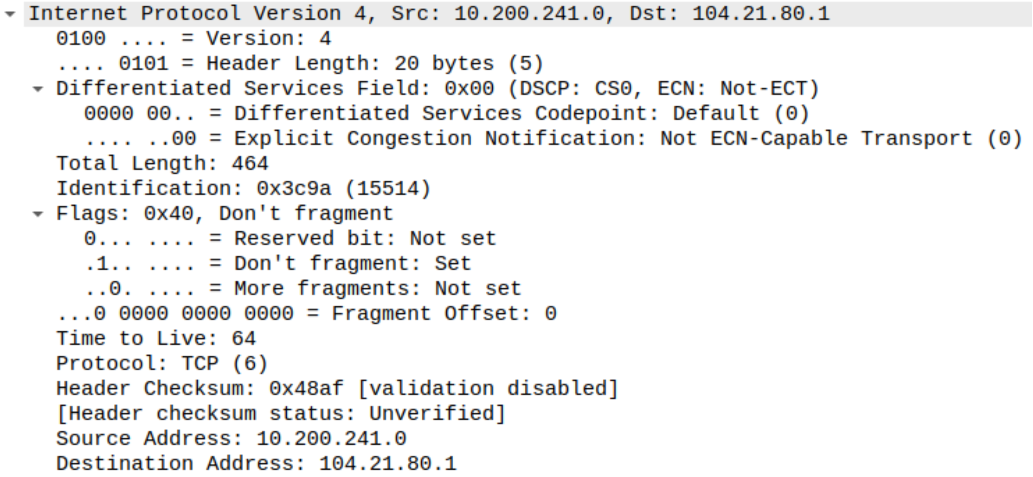
Client IP address : *10.200.241.0*
Domain IP address : *104.21.80.1*

2.2

Protocol : *TCP (6)*

2.3

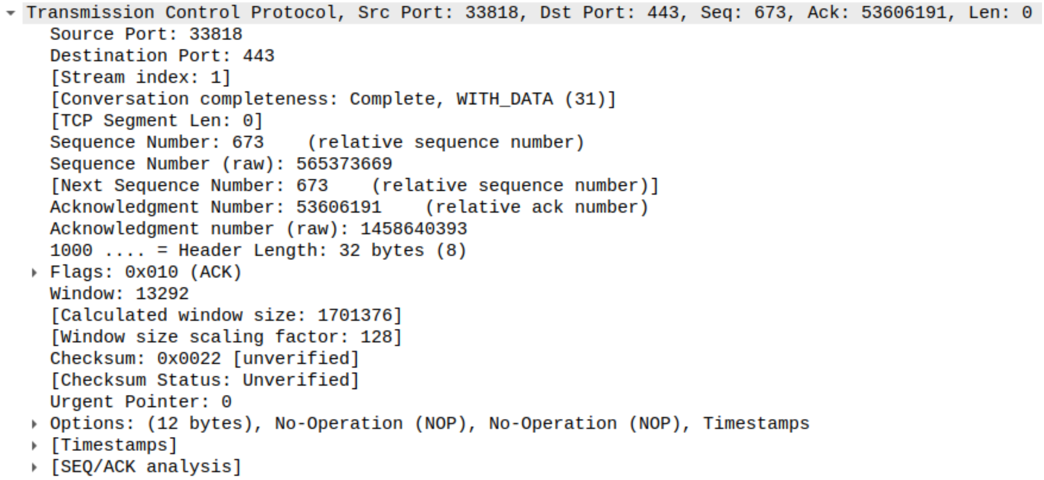
Internet Protocol Version 4 (IPv4)



```
▾ Internet Protocol Version 4, Src: 10.200.241.0, Dst: 104.21.80.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 464
    Identification: 0x3c9a (15514)
  ▾ Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x48af [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.241.0
    Destination Address: 104.21.80.1
```

2.4

Acknowledgement number (relative) : *53606191*
Acknowledgement number (raw) : *1458640393*
The last ACK number is the acknowledgment of the final data segment sent. This indicates that the entire file is received, and the connection is closing.



```
▾ Transmission Control Protocol, Src Port: 33818, Dst Port: 443, Seq: 673, Ack: 53606191, Len: 0
    Source Port: 33818
    Destination Port: 443
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 673    (relative sequence number)
    Sequence Number (raw): 565373669
    [Next Sequence Number: 673    (relative sequence number)]
    Acknowledgment Number: 53606191    (relative ack number)
    Acknowledgment number (raw): 1458640393
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window: 13292
    [Calculated window size: 1701376]
    [Window size scaling factor: 128]
    Checksum: 0x0022 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

Part-3

3.1

Source IPv6 Address : 2601:193:8302:4620:215c:f5ae:8b40:a27a
Destination IPv6 Address : 2001:558:feed::1

3.2

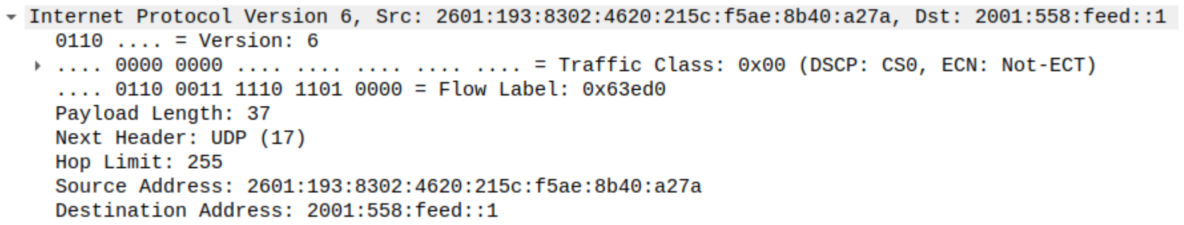
Flow Label for youtube.com : *0x63ed0*
Flow Label for www.youtube.com : *0x8f0f4*

3.3

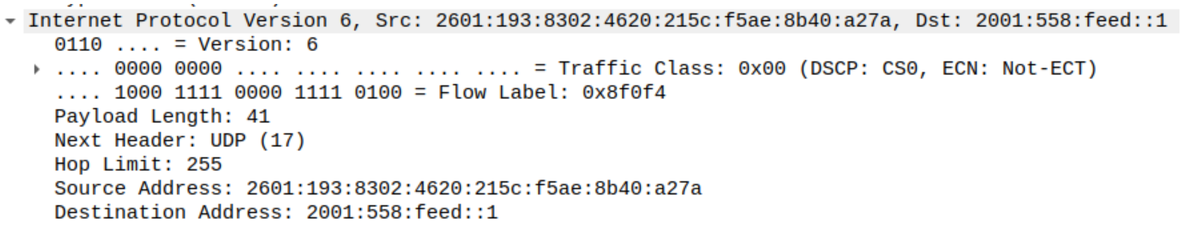
Payload Length for youtube.com : *37*
Payload Length for www.youtube.com : *41*

3.4

UDP (17)



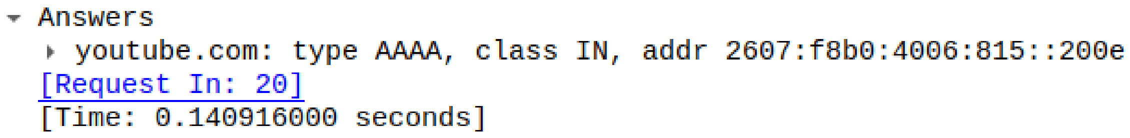
```
▾ Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Dst: 2001:558:feed::1
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0110 0011 1110 1101 0000 = Flow Label: 0x63ed0
    Payload Length: 37
    Next Header: UDP (17)
    Hop Limit: 255
    Source Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a
    Destination Address: 2001:558:feed::1
```



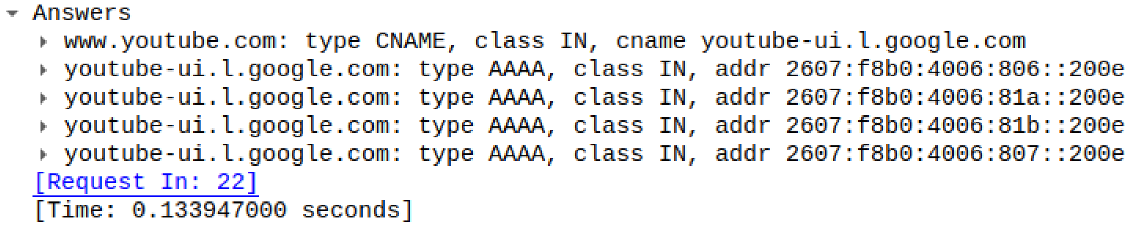
```
▾ Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Dst: 2001:558:feed::1
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1000 1111 0000 1111 0100 = Flow Label: 0x8f0f4
    Payload Length: 41
    Next Header: UDP (17)
    Hop Limit: 255
    Source Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a
    Destination Address: 2001:558:feed::1
```

3.5

Number of IPv6 addresses returned for youtube.com : *1*
Number of IPv6 addresses returned for www.youtube.com : *5*



```
▾ Answers
   ▸ youtube.com: type AAAA, class IN, addr 2607:f8b0:4006:815::200e
  [Request In: 20]
  [Time: 0.140916000 seconds]
```



```
▾ Answers
  ▸ www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
  ▸ youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:806::200e
  ▸ youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81a::200e
  ▸ youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81b::200e
  ▸ youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:807::200e
  [Request In: 22]
  [Time: 0.133947000 seconds]
```