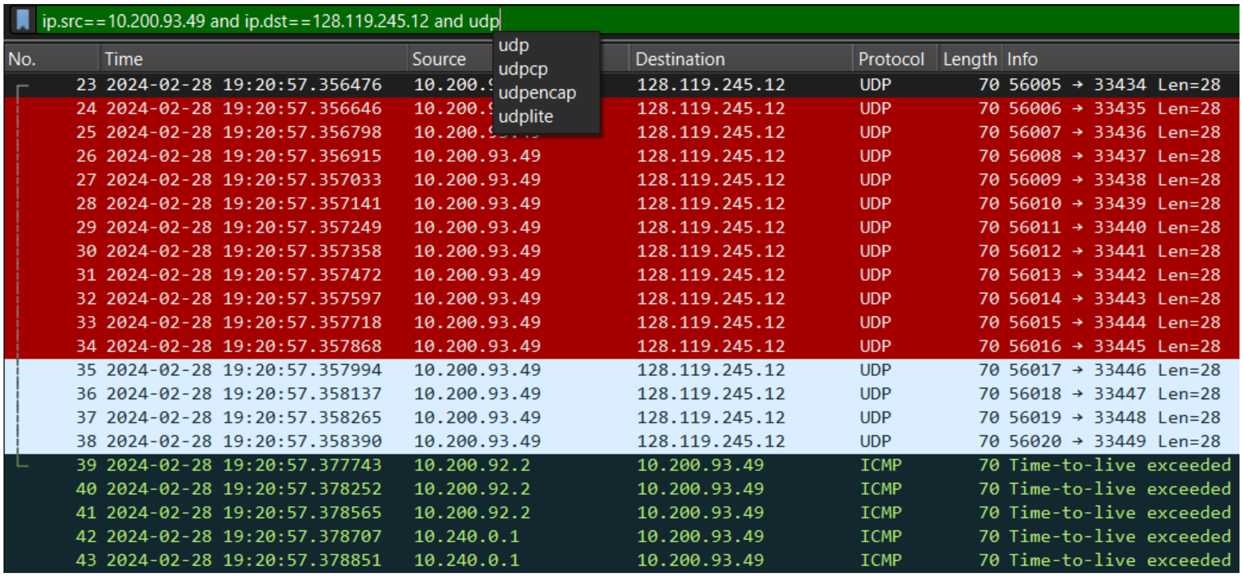
Computer Networks Lab

ASSIGNMENT – 7

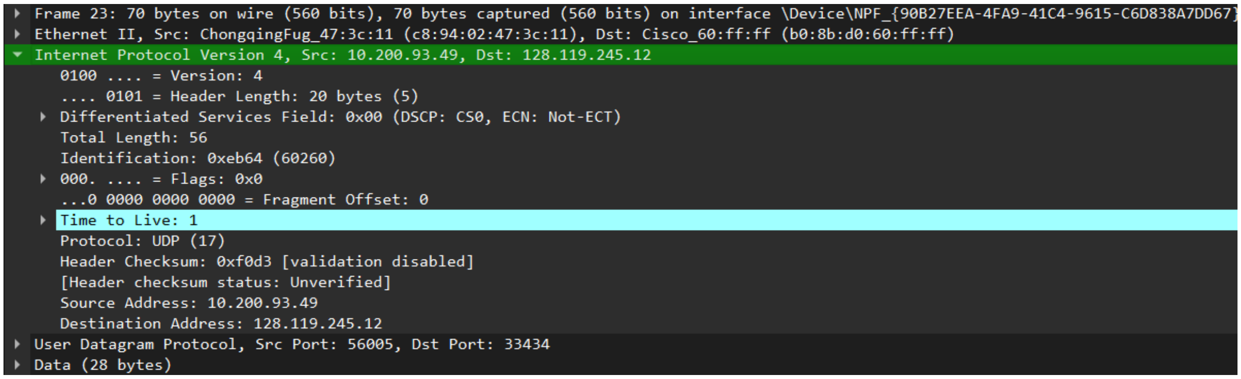
Rahul Cheryala, 210010012

PART – 1



```
ip.src==10.200.93.49 and ip.dst==128.119.245.12 and udp
```

```
No.   Time                        Source          Destination      Protocol  Length  Info
 23 2024-02-28 19:20:57.356476   10.200.9        128.119.245.12   UDP        70 56005 → 33434 Len=28
 24 2024-02-28 19:20:57.356646   10.200.9        128.119.245.12   UDP        70 56006 → 33435 Len=28
 25 2024-02-28 19:20:57.356798   10.200.9        128.119.245.12   UDP        70 56007 → 33436 Len=28
 26 2024-02-28 19:20:57.356915   10.200.93.49    128.119.245.12   UDP        70 56008 → 33437 Len=28
 27 2024-02-28 19:20:57.357033   10.200.93.49    128.119.245.12   UDP        70 56009 → 33438 Len=28
 28 2024-02-28 19:20:57.357141   10.200.93.49    128.119.245.12   UDP        70 56010 → 33439 Len=28
 29 2024-02-28 19:20:57.357249   10.200.93.49    128.119.245.12   UDP        70 56011 → 33440 Len=28
 30 2024-02-28 19:20:57.357358   10.200.93.49    128.119.245.12   UDP        70 56012 → 33441 Len=28
 31 2024-02-28 19:20:57.357472   10.200.93.49    128.119.245.12   UDP        70 56013 → 33442 Len=28
 32 2024-02-28 19:20:57.357597   10.200.93.49    128.119.245.12   UDP        70 56014 → 33443 Len=28
 33 2024-02-28 19:20:57.357718   10.200.93.49    128.119.245.12   UDP        70 56015 → 33444 Len=28
 34 2024-02-28 19:20:57.357868   10.200.93.49    128.119.245.12   UDP        70 56016 → 33445 Len=28
 35 2024-02-28 19:20:57.357994   10.200.93.49    128.119.245.12   UDP        70 56017 → 33446 Len=28
 36 2024-02-28 19:20:57.358137   10.200.93.49    128.119.245.12   UDP        70 56018 → 33447 Len=28
 37 2024-02-28 19:20:57.358265   10.200.93.49    128.119.245.12   UDP        70 56019 → 33448 Len=28
 38 2024-02-28 19:20:57.358390   10.200.93.49    128.119.245.12   UDP        70 56020 → 33449 Len=28
 39 2024-02-28 19:20:57.377743   10.200.92.2     10.200.93.49     ICMP       70 Time-to-live exceeded
 40 2024-02-28 19:20:57.378252   10.200.92.2     10.200.93.49     ICMP       70 Time-to-live exceeded
 41 2024-02-28 19:20:57.378565   10.200.92.2     10.200.93.49     ICMP       70 Time-to-live exceeded
 42 2024-02-28 19:20:57.378707   10.240.0.1      10.200.93.49     ICMP       70 Time-to-live exceeded
 43 2024-02-28 19:20:57.378851   10.240.0.1      10.200.93.49     ICMP       70 Time-to-live exceeded
```



```
Frame 23: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{90B27EEA-4FA9-41C4-9615-C6D838A7DD67}
Ethernet II, Src: ChongqingFug_47:3c:11 (c8:94:02:47:3c:11), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
Internet Protocol Version 4, Src: 10.200.93.49, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xeb64 (60260)
  000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xf0d3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.93.49
    Destination Address: 128.119.245.12
User Datagram Protocol, Src Port: 56005, Dst Port: 33434
Data (28 bytes)
```

1. Frame 23 is the first UDP packet sent via traceroute

   - IP Address of my computer is – 10.200.93.49

2. Time to live is 1

3. The upper layer protocol is in protocol field in IPv4 header: UDP (17)

4. Length of the header is 20 bytes

5. Payload can be calculated by the formula

Payload = length – header

Payload = 56 – 20 (in bytes)

Payload = 36 bytes

6. No, the IP datagram is not fragmented, we can check this from the **Fragment Offset** field in Flags (Fragment Offset: 0)

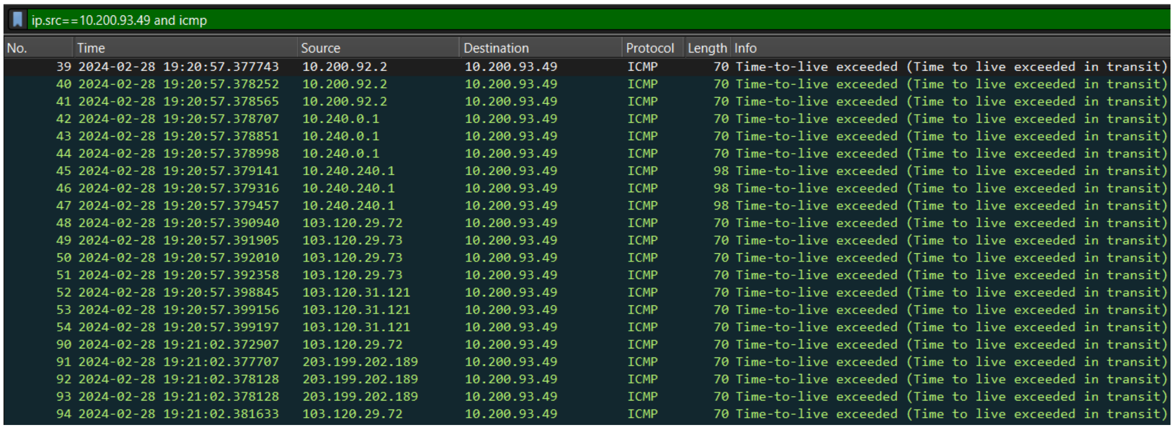
7. There are 3 components which are changing from packet to packet

   a. Identification Id, each IP datagram have a unique ID for identification
   b. Checksum, as the header changes from one to another datagram the checksum value also changes
   c. Traceroute, traceroute (tracert) works by sending packets with incrementally higher Time-To-Live (TTL) values. This approach enables traceroute to map out the network path that packets take to reach the destination.

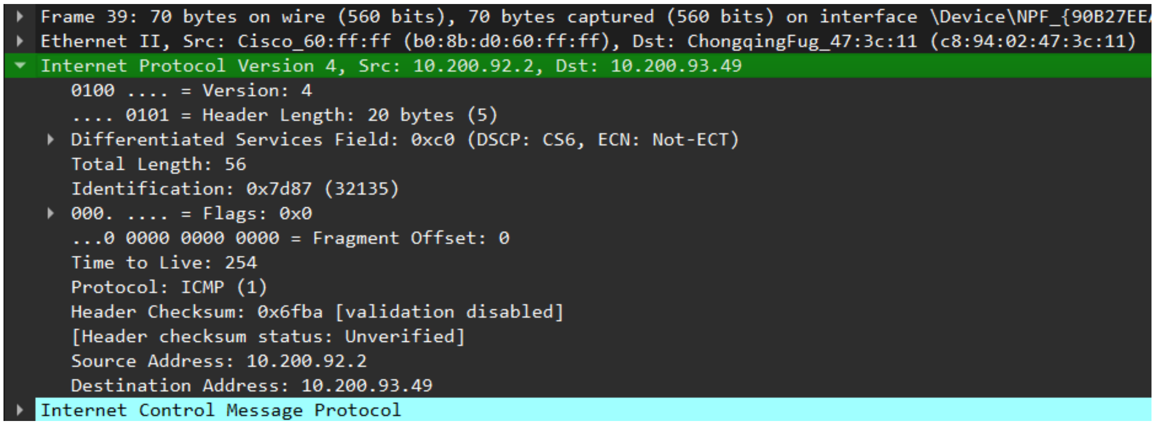
8. The fields that are unchanged are,

   a. Header length (since we are using the same IPv4 header format)
   b. Source IP
   c. Destination IP
   d. Upper layer protocol
   e. Differentiated services (group of fields, all are unchanged)
   f. Internet Protocol Version (IPv4)

9. The values in the Identification field are increasing sequentially



```
ip.src==10.200.93.49 and icmp
No.    Time                        Source            Destination     Protocol  Length Info
    39 2024-02-28 19:20:57.377743  10.200.92.2       10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    40 2024-02-28 19:20:57.378252  10.200.92.2       10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    41 2024-02-28 19:20:57.378565  10.200.92.2       10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    42 2024-02-28 19:20:57.378707  10.240.0.1        10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    43 2024-02-28 19:20:57.378851  10.240.0.1        10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    44 2024-02-28 19:20:57.378998  10.240.0.1        10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    45 2024-02-28 19:20:57.379141  10.240.240.1      10.200.93.49    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    46 2024-02-28 19:20:57.379316  10.240.240.1      10.200.93.49    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    47 2024-02-28 19:20:57.379457  10.240.240.1      10.200.93.49    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    48 2024-02-28 19:20:57.390940  103.120.29.72     10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    49 2024-02-28 19:20:57.391905  103.120.29.73     10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    50 2024-02-28 19:20:57.392010  103.120.29.73     10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    51 2024-02-28 19:20:57.392358  103.120.29.73     10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    52 2024-02-28 19:20:57.398845  103.120.31.121    10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    53 2024-02-28 19:20:57.399156  103.120.31.121    10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    54 2024-02-28 19:20:57.399197  103.120.31.121    10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    90 2024-02-28 19:21:02.372907  103.120.29.72     10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    91 2024-02-28 19:21:02.377707  203.199.202.189   10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    92 2024-02-28 19:21:02.378128  203.199.202.189   10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    93 2024-02-28 19:21:02.378128  203.199.202.189   10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    94 2024-02-28 19:21:02.381633  103.120.29.72     10.200.93.49    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
```



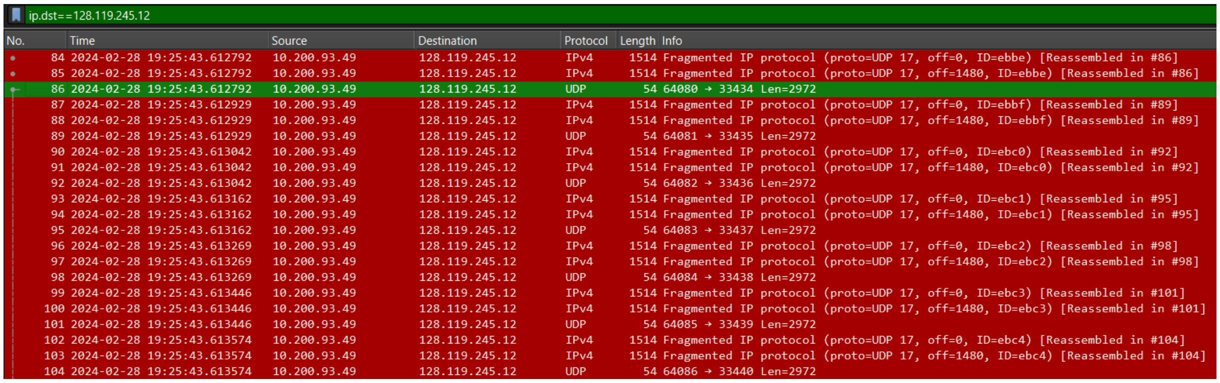
```
> Frame 39: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{90B27EE
> Ethernet II, Src: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff), Dst: ChongqingFug_47:3c:11 (c8:94:02:47:3c:11)
v Internet Protocol Version 4, Src: 10.200.92.2, Dst: 10.200.93.49
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x7d87 (32135)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 254
    Protocol: ICMP (1)
    Header Checksum: 0x6fba [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.92.2
    Destination Address: 10.200.93.49
> Internet Control Message Protocol
```

10. Upper layer protocol specified in the IP datagrams returned from the routers is ICMP (1)

11. Yes, in the ICMP packets used by traceroute, the Identification fields often change across the sequence of packets sent by each router. Typically, there is a serial increment in the Identification field as the packets traverse through different routers along the network path.

12. No, the TTL values are different for ICMP packets from all the routers

PART – 2



ip.dst==128.119.245.12

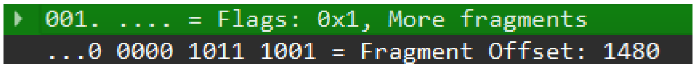
No.	Time	Source	Destination	Protocol	Length	Info
84	2024-02-28 19:25:43.612792	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebbe) [Reassembled in #86]
85	2024-02-28 19:25:43.612792	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebbe) [Reassembled in #86]
86	2024-02-28 19:25:43.612792	10.200.93.49	128.119.245.12	UDP	54	64080 → 33434 Len=2972
87	2024-02-28 19:25:43.612929	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebbf) [Reassembled in #89]
88	2024-02-28 19:25:43.612929	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebbf) [Reassembled in #89]
89	2024-02-28 19:25:43.612929	10.200.93.49	128.119.245.12	UDP	54	64081 → 33435 Len=2972
90	2024-02-28 19:25:43.613042	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebc0) [Reassembled in #92]
91	2024-02-28 19:25:43.613042	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebc0) [Reassembled in #92]
92	2024-02-28 19:25:43.613042	10.200.93.49	128.119.245.12	UDP	54	64082 → 33436 Len=2972
93	2024-02-28 19:25:43.613162	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebc1) [Reassembled in #95]
94	2024-02-28 19:25:43.613162	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebc1) [Reassembled in #95]
95	2024-02-28 19:25:43.613162	10.200.93.49	128.119.245.12	UDP	54	64083 → 33437 Len=2972
96	2024-02-28 19:25:43.613269	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebc2) [Reassembled in #98]
97	2024-02-28 19:25:43.613269	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebc2) [Reassembled in #98]
98	2024-02-28 19:25:43.613269	10.200.93.49	128.119.245.12	UDP	54	64084 → 33438 Len=2972
99	2024-02-28 19:25:43.613446	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebc3) [Reassembled in #101]
100	2024-02-28 19:25:43.613446	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebc3) [Reassembled in #101]
101	2024-02-28 19:25:43.613446	10.200.93.49	128.119.245.12	UDP	54	64085 → 33439 Len=2972
102	2024-02-28 19:25:43.613574	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ebc4) [Reassembled in #104]
103	2024-02-28 19:25:43.613574	10.200.93.49	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ebc4) [Reassembled in #104]
104	2024-02-28 19:25:43.613574	10.200.93.49	128.119.245.12	UDP	54	64086 → 33440 Len=2972

1. First IP datagram sent to the destination address is in **Frame 84**

Packets 84, 85, and 86 are three IP datagrams created by fragmenting the first single 3000-byte UDP segment sent to 128.119.145.12

Yes, it can be confirmed from the Fragment Offset field

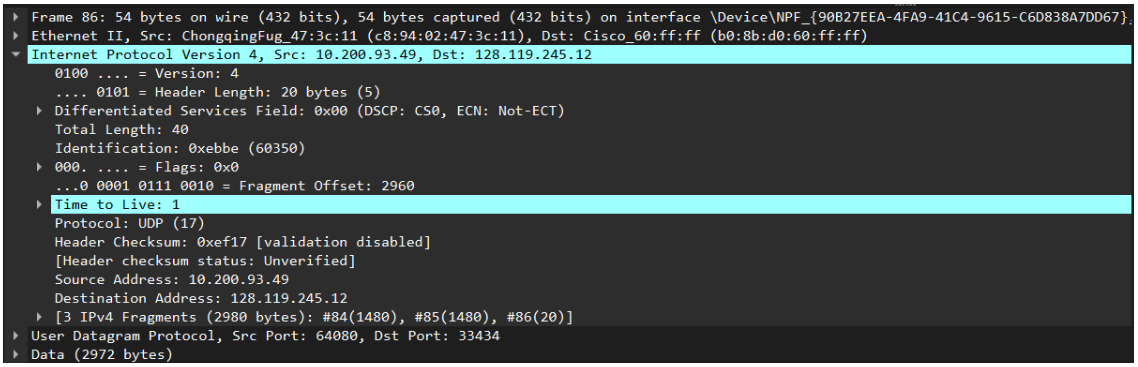
2.



```
001. .... = Flags: 0x1, More fragments
...0 0000 1011 1001 = Fragment Offset: 1480
```

More Fragments bit is set to 1 and Fragment Offset is set to a value

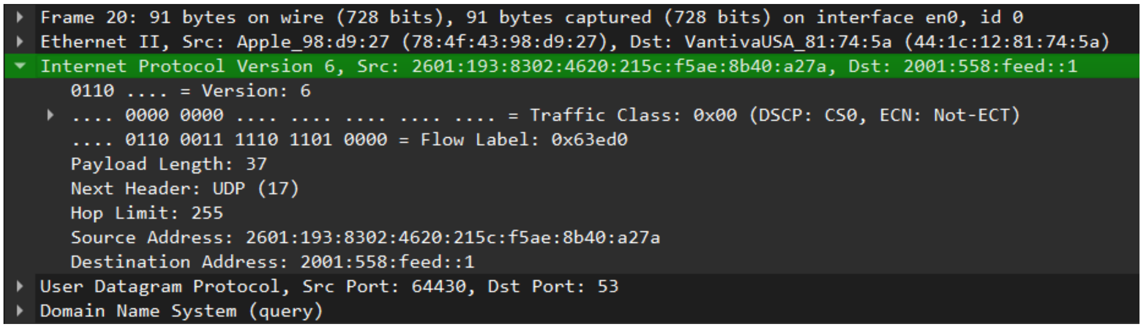
3. For the first fragment the value in the Fragment Offset is set to 0
4. The total length of the IP datagram is 1500 bytes
5. Fields changed are:
   a. More Fragments bit
   b. Fragment Offset
   c. Header Checksum



```
▸ Frame 86: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{90B27EEA-4FA9-41C4-9615-C6D838A7DD67},
▸ Ethernet II, Src: ChongqingFug_47:3c:11 (c8:94:02:47:3c:11), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
▾ Internet Protocol Version 4, Src: 10.200.93.49, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xebbe (60350)
  ▸ 000. .... = Flags: 0x0
    ...0 0001 0111 0010 = Fragment Offset: 2960
  ▸ Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xef17 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.93.49
    Destination Address: 128.119.245.12
  ▸ [3 IPv4 Fragments (2980 bytes): #84(1480), #85(1480), #86(20)]
▸ User Datagram Protocol, Src Port: 64080, Dst Port: 33434
▸ Data (2972 bytes)
```

6. In the first and second segment it is mentioned that segments are reassembled in Frame number 86, More Fragments bit is set to 0 in the Flags and we can see a header section with 3 IPv4 Fragments in the IPv4 header

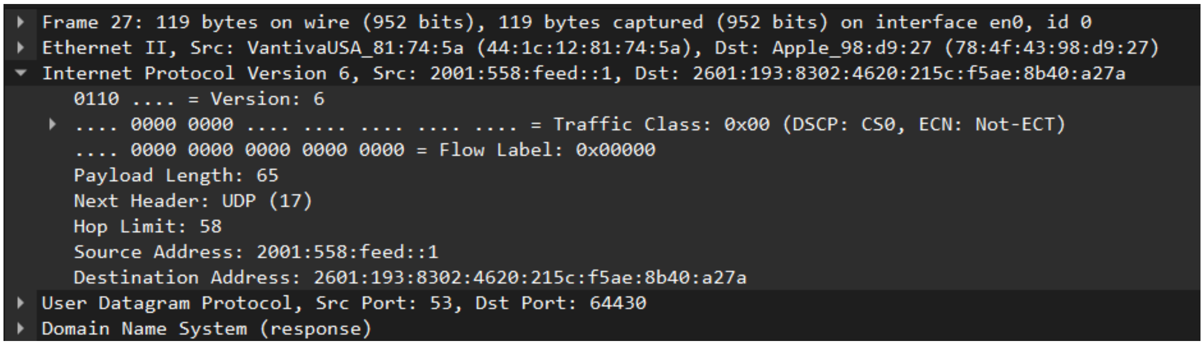
PART – 3



```
▸ Frame 20: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
▸ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: VantivaUSA_81:74:5a (44:1c:12:81:74:5a)
▾ 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
▸ User Datagram Protocol, Src Port: 64430, Dst Port: 53
▸ Domain Name System (query)
```

1. Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a
2. Internet Protocol Version 6, Dst: 2001:558:feed::1
3. Flow Label: 0x63ed0
4. Payload Length: 37
5. The upper layer protocol to which this datagram's payload will be delivered at the destination is UDP (17)

The IPv6 DNS response to the IPv6 DNS AAAA request made in the 20th packet is in Frame 27 (27th packet)



```
▸ Frame 27: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface en0, id 0
▸ Ethernet II, Src: VantivaUSA_81:74:5a (44:1c:12:81:74:5a), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
▾ Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:193:8302:4620:215c:f5ae:8b40:a27a
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 65
    Next Header: UDP (17)
    Hop Limit: 58
    Source Address: 2001:558:feed::1
    Destination Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a
▸ User Datagram Protocol, Src Port: 53, Dst Port: 64430
▸ Domain Name System (response)
```

6. One IPv6 address is returned in the response to this AAAA request in Frame 27

7. 2607:f8b0:4006:815::200e is the first of the IPv6 addresses returned by the DNS for youtube.com. The IPv6 address "2607:f8b0:4006:815::200e" is already in its exact shorthand form, as displayed in the Wireshark window. No further modification is needed.