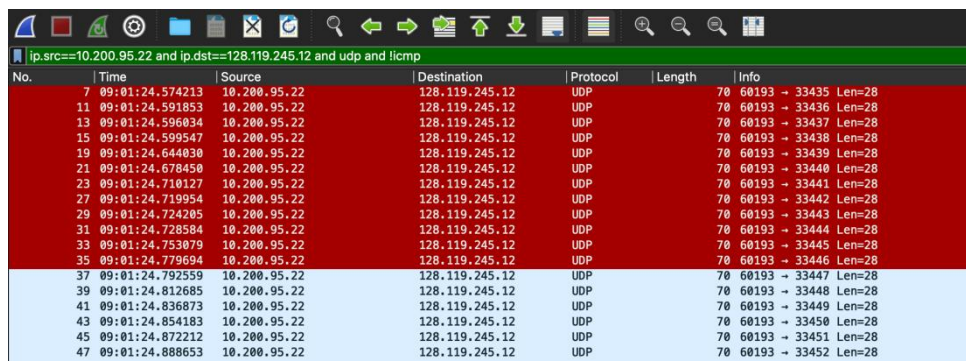# Assignment 7
210010033
Om Deshmukh

Part 1:

```
> Frame 7: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
> Ethernet II, Src: Apple_13:ba:45 (b0:be:83:13:ba:45), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
∨ Internet Protocol Version 4, Src: 10.200.95.22, 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: 0xeb22 (60194)
  > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
  ∨ Time to Live: 1
     > [Expert Info (Note/Sequence): "Time To Live" only 1]
     Protocol: UDP (17)
     Header Checksum: 0xef30 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 10.200.95.22
     Destination Address: 128.119.245.12
> User Datagram Protocol, Src Port: 60193, Dst Port: 33435
> Data (28 bytes)
```

1. The ip address of my computer is 10.200.95.22

2. The TTL value for the first UDP packet sent is 1.

3. UDP is the upper layer protocol here in this case.

4. The size of the IP header is 20 bytes.

5. The payload length is 36 bytes

6. No.
   Since more fragments flag is not set.

7. Identification and Header Checksum are the fields which change from one datagram to another. Also, TTL changes after every 3 datagrams.

8. The fields that remain constant include
   a) Version (since we are using IPv4 for all packets)
   b) Header length (since these are ICMP packets)
   c) Source IP (since we are sending from the same source)
   d) Destination IP (since we are sending to the same destination)
   e) Differentiated Services (since all packets are ICMP they use the same Type of Service class)
   f) Upper Layer Protocol (since these are ICMP packets)

9. The identification values in the consecutive IP datagrams changes by 1 hex unit.

10. ICMP is the upper layer protocol specified in the IP datagrams returned from the routers.

11. No, the changes in values in the identification field is completely different than the case in question 9. Here, in this case it is changing randomly.

12. Yes, the TTL values are nearly similar for the consecutive IP datagrams. However, in some cases they differ as well.

Part 2:

1. Yes, the IP datagrams have been fragmented. .

2.

```
∨  001. .... = Flags: 0x1, More fragments
       0... .... = Reserved bit: Not set
       .0.. .... = Don't fragment: Not set
       ..1. .... = More fragments: Set
   ...0 0000 0000 0000 = Fragment Offset: 0
```

We can be sure since MORE FRAGMENTS bit is Set

3. Fragment offset is 0 for the first fragment whereas its non zero for other fragments.

4. The total size of the datagram(header + payload) is 1500 bytes.

5. Fragment offset and Header Checksum change between the first and second fragments.

6.

```
∨  000. .... = Flags: 0x0
       0... .... = Reserved bit: Not set
       .0.. .... = Don't fragment: Not set
       ..0. .... = More fragments: Not set
   ...0 0001 0111 0010 = Fragment Offset: 2960
```

```
15 10:35:20.955728  10.200.95.22    128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=b77a) [Reassembled in #17]
16 10:35:20.955765  10.200.95.22    128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=b77a) [Reassembled in #17]
17 10:35:20.955775  10.200.95.22    128.119.245.12    UDP     54 46969 → 33435 Len=2972
```

Packet number 17 here is the IP datagram containing the third fragment of the original UDP segment. The fact that MORE FRAGMENTS have not been set represents that this is the last fragment of the segment.

Part 3:

1. Source Address of computer making the DNS query is 2601:193:8302:4620:215c:f5ae:8b40:a27a

2. Destination Address is 2001:558:feed::1

3. Flow Label value of this datagram is 0x63ed0

4. 37 bytes

5. UDP protocol is the upper layer protocol of this datagram.

6. Only 1 IPV6 address is returned in response.

7. Address returned is 2607:f8b0:4006:815::200e