Assignment 7

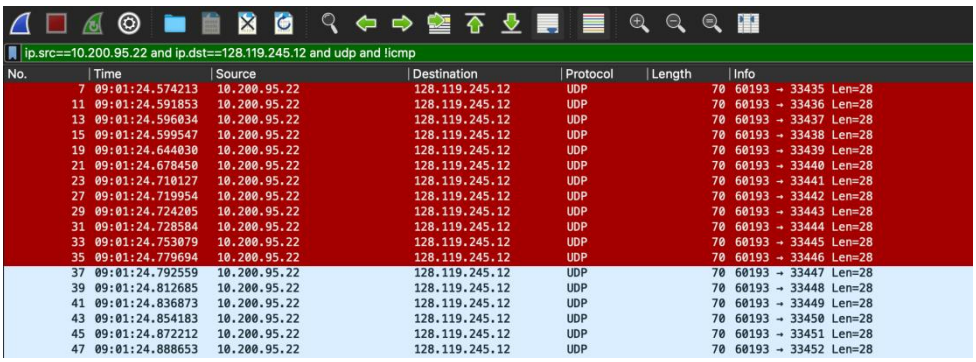
210010033

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)
v 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
  v 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.



ip.src==10.200.95.22 and ip.dst==128.119.245.12 and udp and !icmp

No.	Time	Source	Destination	Protocol	Length	Info
7	09:01:24.574213	10.200.95.22	128.119.245.12	UDP	70	60193 → 33435 Len=28
11	09:01:24.591853	10.200.95.22	128.119.245.12	UDP	70	60193 → 33436 Len=28
13	09:01:24.596034	10.200.95.22	128.119.245.12	UDP	70	60193 → 33437 Len=28
15	09:01:24.599547	10.200.95.22	128.119.245.12	UDP	70	60193 → 33438 Len=28
19	09:01:24.644030	10.200.95.22	128.119.245.12	UDP	70	60193 → 33439 Len=28
21	09:01:24.678450	10.200.95.22	128.119.245.12	UDP	70	60193 → 33440 Len=28
23	09:01:24.710127	10.200.95.22	128.119.245.12	UDP	70	60193 → 33441 Len=28
27	09:01:24.719954	10.200.95.22	128.119.245.12	UDP	70	60193 → 33442 Len=28
29	09:01:24.724205	10.200.95.22	128.119.245.12	UDP	70	60193 → 33443 Len=28
31	09:01:24.728584	10.200.95.22	128.119.245.12	UDP	70	60193 → 33444 Len=28
33	09:01:24.753079	10.200.95.22	128.119.245.12	UDP	70	60193 → 33445 Len=28
35	09:01:24.779694	10.200.95.22	128.119.245.12	UDP	70	60193 → 33446 Len=28
37	09:01:24.792559	10.200.95.22	128.119.245.12	UDP	70	60193 → 33447 Len=28
39	09:01:24.812685	10.200.95.22	128.119.245.12	UDP	70	60193 → 33448 Len=28
41	09:01:24.836873	10.200.95.22	128.119.245.12	UDP	70	60193 → 33449 Len=28
43	09:01:24.854183	10.200.95.22	128.119.245.12	UDP	70	60193 → 33450 Len=28
45	09:01:24.872212	10.200.95.22	128.119.245.12	UDP	70	60193 → 33451 Len=28
47	09:01:24.888653	10.200.95.22	128.119.245.12	UDP	70	60193 → 33452 Len=28

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.

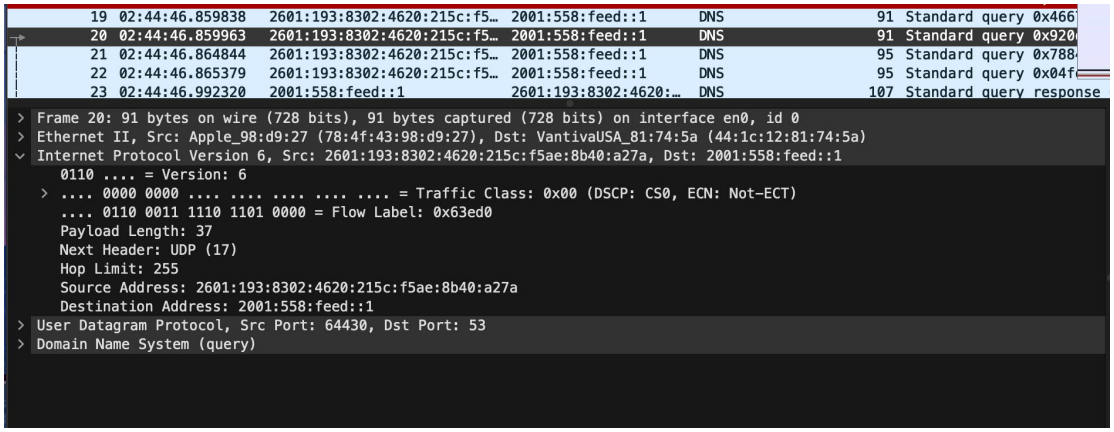
6.

```
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:



19	02:44:46.859838	2601:193:8302:4620:215c:f5…	2001:558:feed::1	DNS	91	Standard query 0x466
20	02:44:46.859963	2601:193:8302:4620:215c:f5…	2001:558:feed::1	DNS	91	Standard query 0x920
21	02:44:46.864844	2601:193:8302:4620:215c:f5…	2001:558:feed::1	DNS	95	Standard query 0x788
22	02:44:46.865379	2601:193:8302:4620:215c:f5…	2001:558:feed::1	DNS	95	Standard query 0x04f
23	02:44:46.992320	2001:558:feed::1	2601:193:8302:4620:…	DNS	107	Standard query response

```
> 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)
v 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. 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