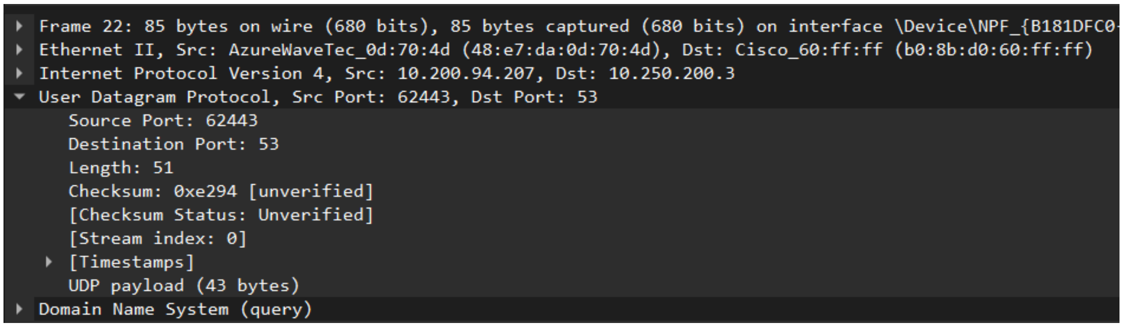
Computer Networks Lab

ASSIGNMENT – 6

Rahul Cheryala, 210010012

PART – 1

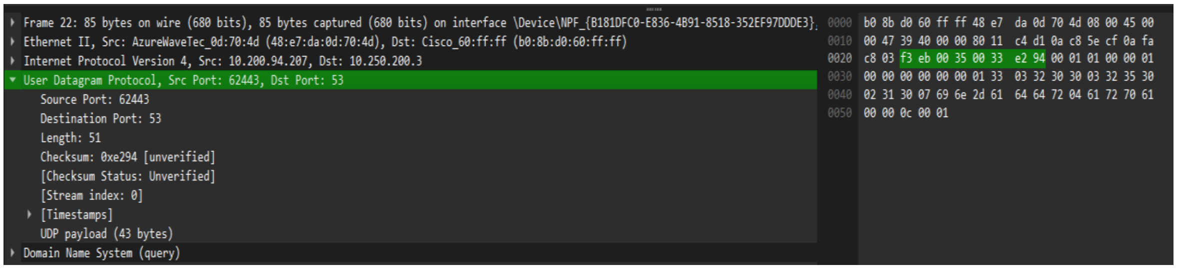
1.



```
▸ Frame 22: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{B181DFC0-
▸ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
▸ Internet Protocol Version 4, Src: 10.200.94.207, Dst: 10.250.200.3
▾ User Datagram Protocol, Src Port: 62443, Dst Port: 53
    Source Port: 62443
    Destination Port: 53
    Length: 51
    Checksum: 0xe294 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (43 bytes)
▸ Domain Name System (query)
```

- Packet number of the First UDP segment – 22 (Frame 22)
- UDP (User Datagram Protocol) is used to carry out the UDP segments
- UDP header contains 4 fields:
    1. source port
    2. destination port
    3. length
    4. Checksum

2.



```
▸ Frame 22: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}
▸ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
▸ Internet Protocol Version 4, Src: 10.200.94.207, Dst: 10.250.200.3
▾ User Datagram Protocol, Src Port: 62443, Dst Port: 53
    Source Port: 62443
    Destination Port: 53
    Length: 51
    Checksum: 0xe294 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (43 bytes)
▸ Domain Name System (query)
```

```
0000  b0 8b d0 60 ff ff 48 e7  da 0d 70 4d 08 00 45 00
0010  00 47 39 40 00 00 80 11  c4 d1 0a c8 5e cf 0a fa
0020  c8 03 f3 eb 00 35 00 33  e2 94 00 01 01 00 00 01
0030  00 00 00 00 00 00 01 33  03 32 30 30 03 32 35 30
0040  02 31 30 07 69 6e 2d 61  64 64 72 04 61 72 70 61
0050  00 00 0c 00 01
```

- The length of UDP headers in this case is 8 bytes

- The length of each field in the header is 2 bytes

3. The length field specifies the number of bytes in the UDP segment (header & data combined). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.

The length of UDP payload for selected packet is 51 bytes - 8 bytes = 43 bytes

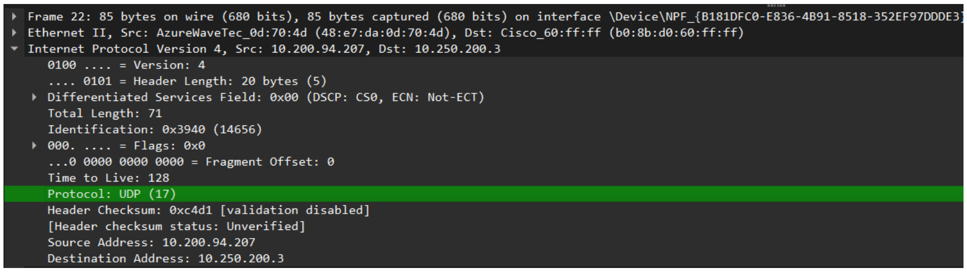
4. Max length of the UDP segment = 2^{16} - bytes used by the header (8)

= 65535 – 8
= 65527 bytes.

5. Each field in the header is of 2 bytes. So, Source port – 2 bytes

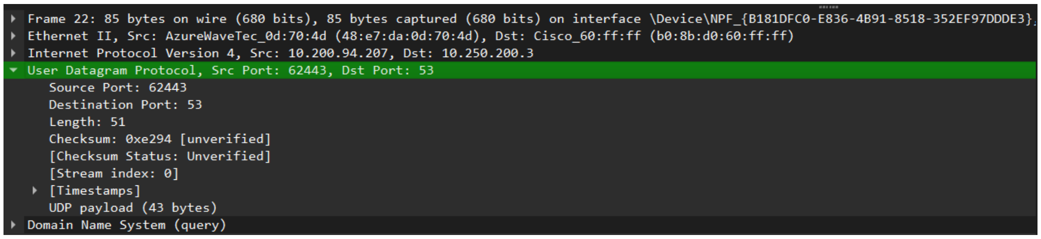
Largest possible Source port is = $2^{16} – 1$ = 65535

6. Protocol number for the UDP segment is 17 (0x11 hex)



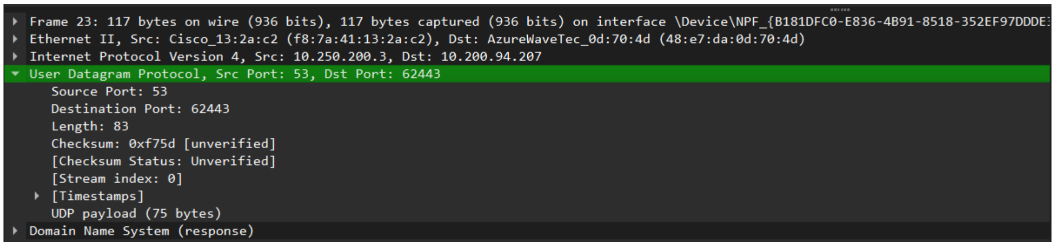
```
▸ Frame 22: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3}
▸ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
▾ Internet Protocol Version 4, Src: 10.200.94.207, Dst: 10.250.200.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 71
    Identification: 0x3940 (14656)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xc4d1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.200.94.207
    Destination Address: 10.250.200.3
```

7. Frame 22 – Request is sent (Packet number 22)



```
▸ Frame 22: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE3},
▸ Ethernet II, Src: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
▸ Internet Protocol Version 4, Src: 10.200.94.207, Dst: 10.250.200.3
▾ User Datagram Protocol, Src Port: 62443, Dst Port: 53
    Source Port: 62443
    Destination Port: 53
    Length: 51
    Checksum: 0xe294 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (43 bytes)
▸ Domain Name System (query)
```

Frame 23 – Received reply (Packet number 23)



```
Frame 23: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{B181DFC0-E836-4B91-8518-352EF97DDDE
Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: AzureWaveTec_0d:70:4d (48:e7:da:0d:70:4d)
Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.200.94.207
User Datagram Protocol, Src Port: 53, Dst Port: 62443
    Source Port: 53
    Destination Port: 62443
    Length: 83
    Checksum: 0xf75d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (75 bytes)
Domain Name System (response)
```

The packet number of the first UDP segment in the trace file is 22, and the packet number of the second UDP segment is 23.

In the first UDP packet:

- Source Port: 62443
- Destination Port: 53

In the second UDP packet (response to the first packet):

- Source Port: 53
- Destination Port: 62443

The relationship between the port numbers in the two packets is that they are reversed. This is typical in DNS communication, where the client sends the DNS query from a random high-numbered port (in this case, 62443), and the server responds from port 53, the well-known port for DNS. This reversal of ports allows the client to receive the response on the same port it used for the query.