

CS-315 COMPUTER NETWORKS LAB-6

PART-1

1. The packet number of the trace is 60. The type of application-layer protocol message being carried in this UDP segment is DNS.

60	23:24:58.210052299	10.200.241.140	10.250.200.3	DNS	71 Standard query 0x5de7 A www.nyu.edu
61	23:24:58.050650771	10.250.200.2	10.200.241.140	DNS	100 Standard query response 0x5fd1 A n2a

The UDP header has 4 primary fields: Source port, Destination port, Length and Checksum.

```

7 Internet Protocol Version 4, Src: 10.200.241.140, Dst: 10.2
- User Datagram Protocol, Src Port: 37333, Dst Port: 53
    Source Port: 37333
    Destination Port: 53
    Length: 37
    Checksum: 0xcf88 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
- [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
    UDP payload (29 bytes)

```

2. The screenshot below shows that each field in the header has a size of 2 bytes (4 hexadecimal digits). There are 4 fields in the header as discussed above. Hence the header has a size of 8 bytes. Every field has a size of 2 bytes. It can also be confirmed from the value of checksum field = 0xcf88 which has 4 hexadecimal digits, hence 2 bytes.

```
44 b6 be 0a 9a f3 20 c1 9b 1f 79 8a 08 00 45 00 D . . . . . y . . |
00 39 e5 33 00 00 40 11 c6 2e 0a c8 f1 8c 0a fa . 9 . 3 . @ . . . .
c8 03 91 d5 00 35 00 25 cf 88 5d e7 01 00 00 01 . . . . 5 % . . ] . .
00 00 00 00 00 00 03 77 77 77 03 6e 79 75 03 65 . . . . . w ww nyu
64 75 00 00 01 00 01 du . . . . .
```

3. The value in the length field is the length of the UDP message which is the sum of the length of the UDP header and the length of the UDP payload. From the screenshot below, we can see that the UDP payload is 29 bytes and the header as discussed above is 8 bytes. Total sum = 37 bytes which is the same as the value in the length field.

```
Internet Protocol Version 4, Src: 10.200.241.140, Dst: 10.250.200.3
  User Datagram Protocol, Src Port: 37333, Dst Port: 53
    Source Port: 37333
    Destination Port: 53
    Length: 37
    Checksum: 0xcf88 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (29 bytes)
```

4. From the discussions above, we know that the checksum field, like other fields, has a size of 2 bytes which is 4 hexadecimal digits. So the maximum value would be FFFF which is 65535 bytes. Since the header has a size of 8 bytes. The maximum size of the payload would be $65535 - 8 = 65527$ bytes.
5. From the discussions above, we know that every field has a size of 2 bytes which is 4 hexadecimal digits. So, the source port number will also have a maximum value of FFFF which is 65535. Hence, the largest possible source port number is 65535.
6. Protocol Number for UDP = 17 as seen in the screenshot below.

```
Internet Protocol Version 4, Src: 10.200.241.140, 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: 57
  Identification: 0xe533 (58675)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xc62e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.200.241.140
  Destination Address: 10.250.200.3
```

7. The packet number of the first(query) UDP packet is 60 and the packet number of the second(response) UDP packet is 82.

60	23:24:58.210052299	10.200.241.140	10.250.200.3	DNS	71 Standard query 0x5de7 A www.nyu.edu
64	23:24:58.959659771	10.250.200.3	10.200.241.140	DNS	189 Standard query response 0x6fd4 A p3a-json.brave.com CNAME dualstack.k.sni.globa...
82	23:25:01.533938481	10.250.200.3	10.200.241.140	DNS	178 Standard query response 0x5de7 A www.nyu.edu CNAME d1q5ku5vmwkd2k.cloudfront.ne...

Internet Protocol Version 4, Src: 10.200.241.140, Dst: 10.250.200.3
▼ User Datagram Protocol, Src Port: 37333, Dst Port: 53
Source Port: 37333
Destination Port: 53
Length: 37
Checksum: 0xcf88 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
▼ [Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]
UDP payload (29 bytes)
Destination Address: 10.250.200.3
▼ User Datagram Protocol, Src Port: 53, Dst Port: 37333
Source Port: 53
Destination Port: 37333
Length: 144
Checksum: 0x4f2f [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
▼ [Timestamps]
[Time since first frame: 3.323886182 seconds]
[Time since previous frame: 3.323886182 seconds]
UDP payload (136 bytes)
Source Address: 10.250.200.3

In the first UDP packet, we see that the source port is 37333 and the destination port is 53. In the second UDP packet, we see that the source port is 53 and the destination port is 37333. So, The source port of the first(query) UDP packet sent by the host is the same as the destination port of the second(response) UDP packet, and the destination port of the first(query) UDP packet sent by the host is the same as the source port of the second(response) UDP packet.