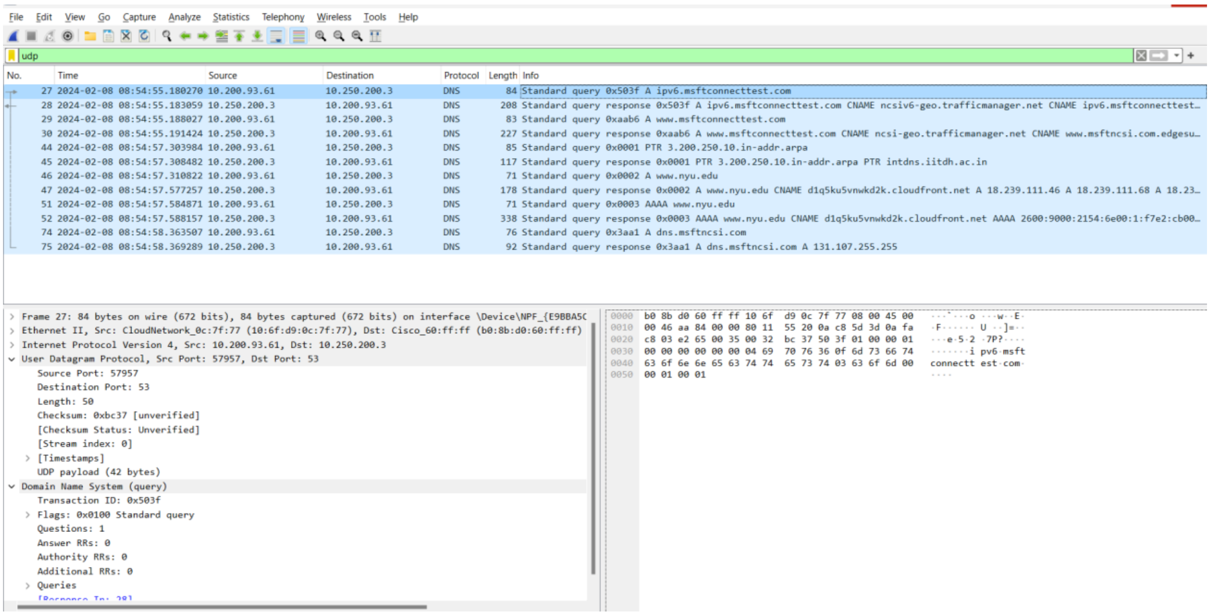
Assignment 6: UDP and Socket Programming

Hrishikesh Ravindra Karande 210010020

Part1:

Q1] Select the first UDP segment in your trace. What is the packet number of this segment in the trace file? What type of application-layer protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields are there in the UDP header? What are the names of these fields?

A] Packet Number or Frame Number of first UDP Segment is 27.
The Destination Port number is 53, this indicates that it is carrying DNS Protocol.
There are 4 Fields in UDP Header Source Port, Destination Port, Length and Checksum.



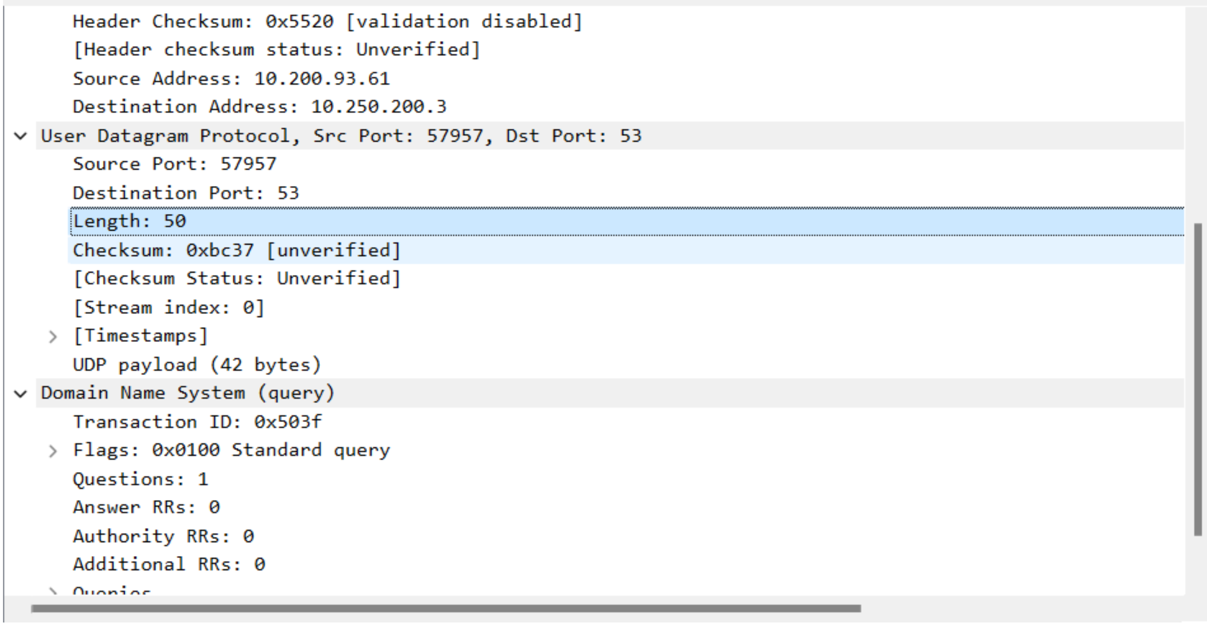
udp

```
No.  Time                        Source         Destination    Protocol Length Info
  27 2024-02-08 08:54:55.180270 10.200.93.61   10.250.200.3   DNS       84 Standard query 0x503f A ipv6.msftconnecttest.com
  28 2024-02-08 08:54:55.183059 10.250.200.3   10.200.93.61   DNS      208 Standard query response 0x503f A ipv6.msftconnecttest.com CNAME ncsiv6-geo.trafficmanager.net CNAME ipv6.msftconnecttest…
  29 2024-02-08 08:54:55.188027 10.200.93.61   10.250.200.3   DNS       83 Standard query 0xaab6 A www.msftconnecttest.com
  30 2024-02-08 08:54:55.191424 10.250.200.3   10.200.93.61   DNS      227 Standard query response 0xaab6 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesu…
  44 2024-02-08 08:54:57.303984 10.200.93.61   10.250.200.3   DNS       85 Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
  45 2024-02-08 08:54:57.308482 10.250.200.3   10.200.93.61   DNS      117 Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in
  46 2024-02-08 08:54:57.310822 10.200.93.61   10.250.200.3   DNS       71 Standard query 0x0002 A www.nyu.edu
  47 2024-02-08 08:54:57.577257 10.250.200.3   10.200.93.61   DNS      178 Standard query response 0x0002 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 18.239.111.46 A 18.239.111.68 A 18.23…
  51 2024-02-08 08:54:57.584871 10.200.93.61   10.250.200.3   DNS       71 Standard query 0x0003 AAAA www.nyu.edu
  52 2024-02-08 08:54:57.588157 10.250.200.3   10.200.93.61   DNS      338 Standard query response 0x0003 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:2154:6e00:1:f7e2:cb00…
  74 2024-02-08 08:54:58.363507 10.200.93.61   10.250.200.3   DNS       76 Standard query 0x3aa1 A dns.msftncsi.com
  75 2024-02-08 08:54:58.369289 10.250.200.3   10.200.93.61   DNS       92 Standard query response 0x3aa1 A dns.msftncsi.com A 131.107.255.255
```

```
> Frame 27: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{E9BBA5C
> Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
> Internet Protocol Version 4, Src: 10.200.93.61, Dst: 10.250.200.3
v User Datagram Protocol, Src Port: 57957, Dst Port: 53
    Source Port: 57957
    Destination Port: 53
    Length: 50
    Checksum: 0xbc37 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (42 bytes)
v Domain Name System (query)
    Transaction ID: 0x503f
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 28]
```

```
0000  b0 8b d0 60 ff ff 10 6f  d9 0c 7f 77 08 00 45 00   ···`···o ···w··E·
0010  00 46 aa 84 00 00 80 11  55 20 0a c8 5d 3d 0a fa   ·F······ U ··]=··
0020  c8 03 e2 65 00 35 00 32  bc 37 50 3f 01 00 00 01   ···e·5·2 ·7P?····
0030  00 00 00 00 00 00 04 69  70 76 36 0f 6d 73 66 74   ·······i pv6·msft
0040  63 6f 6e 6e 65 63 74 74  65 73 74 03 63 6f 6d 00   connectt est·com·
0050  00 01 00 01                                        ····
```

Q2] By consulting the displayed information in Wireshark's packet content field for this packet, what is the length (in bytes) of each of the UDP header fields?



```
      Header Checksum: 0x5520 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.200.93.61
      Destination Address: 10.250.200.3
  ⌄ User Datagram Protocol, Src Port: 57957, Dst Port: 53
      Source Port: 57957
      Destination Port: 53
      Length: 50
      Checksum: 0xbc37 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
    > [Timestamps]
      UDP payload (42 bytes)
  ⌄ Domain Name System (query)
      Transaction ID: 0x503f
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
```

A] The UDP contains 4 headers of total length = 8 bytes therefore each will be of length = 2 bytes. This is always fixed.

Q3] The value in the Length field is the length of what? Verify your claim with your captured UDP packet

A] The Value in length field is the length of Payload + Headers that is sent in through the packet. This can be seen from Q2 screenshot.

45+8=53 total length displayed in screenshot

Q4] What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

A] UDP Segment header length = 32+32 = 64 bits
1 bytes = 8bits, therefore 8 bytes is length of the header field.
Clicking on length field in Wireshark gives 2bytes = 16bits.
Total Length = 2^16-1 = UDP payload + UDP header
UDP payload=(2^16-1)bytes – 8bytes = 65535 bytes – 8 bytes = **65527 bytes.**

Q5] What is the largest possible source port number? (Hint: see the hint in 4.)

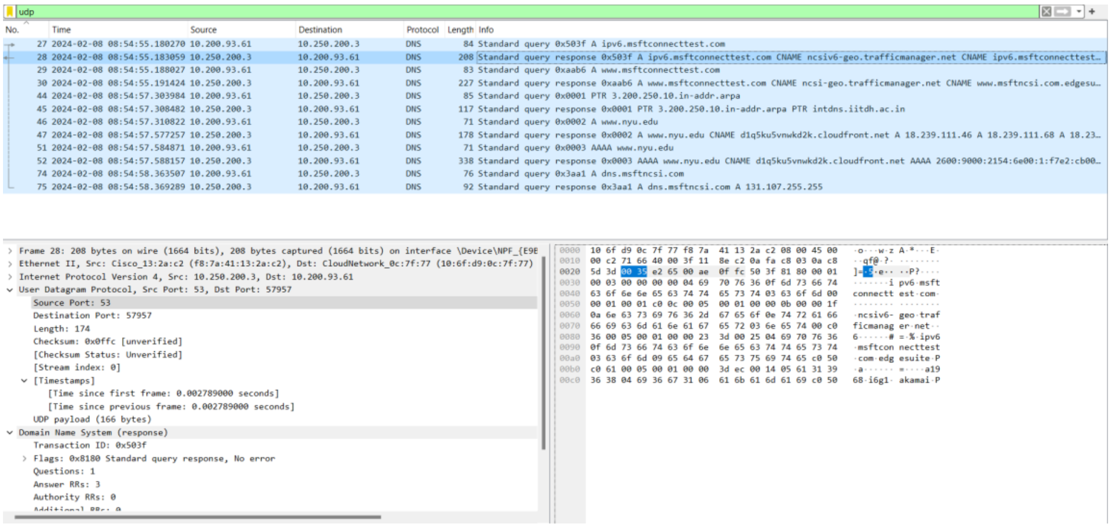
A] source port number is 2 bytes field = 16 bits therefore largest possible source port number = **2^16-1 = 65535**

Q6] What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment.

A] In the IP Datagram protocol field the length of UDP can be seen as 1 byte corresponding Hexadecimal notation is represented in the right side of screen as **11**(Hex value) this converted to Decimal gives **17.**

Q7] Examine the pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). What is the packet number of the first of these two UDP segments in the trace file? What is the packet number of the second of these two UDP segments in the trace file? Describe the relationship between the port numbers in the two packets.

A] The request is in Packet with frame number 27 and the response is in packet with frame number 28. The source and Destination ports in response packet are reversed as that of the previous packet(request).



```
udp
No.  Time                       Source         Destination    Protocol Length Info
  27 2024-02-08 08:54:55.180270 10.200.93.61   10.250.200.3   DNS       84 Standard query 0x503f A ipv6.msftconnecttest.com
  28 2024-02-08 08:54:55.183059 10.250.200.3   10.200.93.61   DNS      208 Standard query response 0x503f A ipv6.msftconnecttest.com CNAME ncsiv6-geo.trafficmanager.net CNAME ipv6.msftconnecttest…
  29 2024-02-08 08:54:55.188027 10.200.93.61   10.250.200.3   DNS       83 Standard query 0xaab6 A www.msftconnecttest.com
  30 2024-02-08 08:54:55.191424 10.250.200.3   10.200.93.61   DNS      227 Standard query response 0xaab6 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesu…
  44 2024-02-08 08:54:57.303984 10.200.93.61   10.250.200.3   DNS       85 Standard query 0x0001 PTR 3.200.250.10.in-addr.arpa
  45 2024-02-08 08:54:57.308482 10.250.200.3   10.200.93.61   DNS      117 Standard query response 0x0001 PTR 3.200.250.10.in-addr.arpa PTR intdns.iitdh.ac.in
  46 2024-02-08 08:54:57.310822 10.200.93.61   10.250.200.3   DNS       71 Standard query 0x0002 A www.nyu.edu
  47 2024-02-08 08:54:57.577257 10.250.200.3   10.200.93.61   DNS      178 Standard query response 0x0002 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 18.239.111.46 A 18.239.111.68 A 18.23…
  51 2024-02-08 08:54:57.584871 10.200.93.61   10.250.200.3   DNS       71 Standard query 0x0003 AAAA www.nyu.edu
  52 2024-02-08 08:54:57.588157 10.250.200.3   10.200.93.61   DNS      338 Standard query response 0x0003 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:2154:6e00:1:f7e2:cb00…
  74 2024-02-08 08:54:58.363507 10.200.93.61   10.250.200.3   DNS       76 Standard query 0x3aa1 A dns.msftncsi.com
  75 2024-02-08 08:54:58.369289 10.250.200.3   10.200.93.61   DNS       92 Standard query response 0x3aa1 A dns.msftncsi.com A 131.107.255.255
```

```
> Frame 28: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{E9E
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77)
> Internet Protocol Version 4, Src: 10.250.200.3, Dst: 10.200.93.61
v User Datagram Protocol, Src Port: 53, Dst Port: 57957
    Source Port: 53
    Destination Port: 57957
    Length: 174
    Checksum: 0x0ffc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  v [Timestamps]
      [Time since first frame: 0.002789000 seconds]
      [Time since previous frame: 0.002789000 seconds]
    UDP payload (166 bytes)
v Domain Name System (response)
    Transaction ID: 0x503f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
```

```
0000  10 6f d9 0c 7f 77 f8 7a  41 13 2a c2 08 00 45 00   ·o···w·z A·*···E·
0010  00 c2 71 66 40 00 3f 11  8e c2 0a fa c8 03 0a c8   ··qf@·?· ········
0020  5d 3d 00 35 e2 65 00 ae  0f fc 50 3f 81 80 00 01   ]=·5·e·· ··P?····
0030  00 03 00 00 00 00 04 69  70 76 36 0f 6d 73 66 74   ·······i pv6·msft
0040  63 6f 6e 6e 65 63 74 74  65 73 74 03 63 6f 6d 00   connectt est·com·
0050  00 01 00 01 c0 0c 00 05  00 01 00 00 0b 00 00 1f   ········ ········
0060  0a 6e 63 73 69 76 36 2d  67 65 6f 0e 74 72 61 66   ·ncsiv6- geo·traf
0070  66 69 63 6d 61 6e 61 67  65 72 03 6e 65 74 00 c0   ficmanag er·net··
0080  36 00 05 00 01 00 00 23  3d 00 25 04 69 70 76 36   6······# =·%·ipv6
0090  0f 6d 73 66 74 63 6f 6e  6e 65 63 74 74 65 73 74   ·msftcon necttest
00a0  03 63 6f 6d 09 65 64 67  65 73 75 69 74 65 c0 50   ·com·edg esuite·P
00b0  c0 61 00 05 00 01 00 00  3d ec 00 14 05 61 31 39   ·a······ =····a19
00c0  36 38 04 69 36 67 31 06  61 6b 61 6d 61 69 c0 50   68·i6g1· akamai·P
```