CS315: Assignment-5

Name: Shahil Patel

Roll No.: 200010039

Part-1: Wireshark UDP

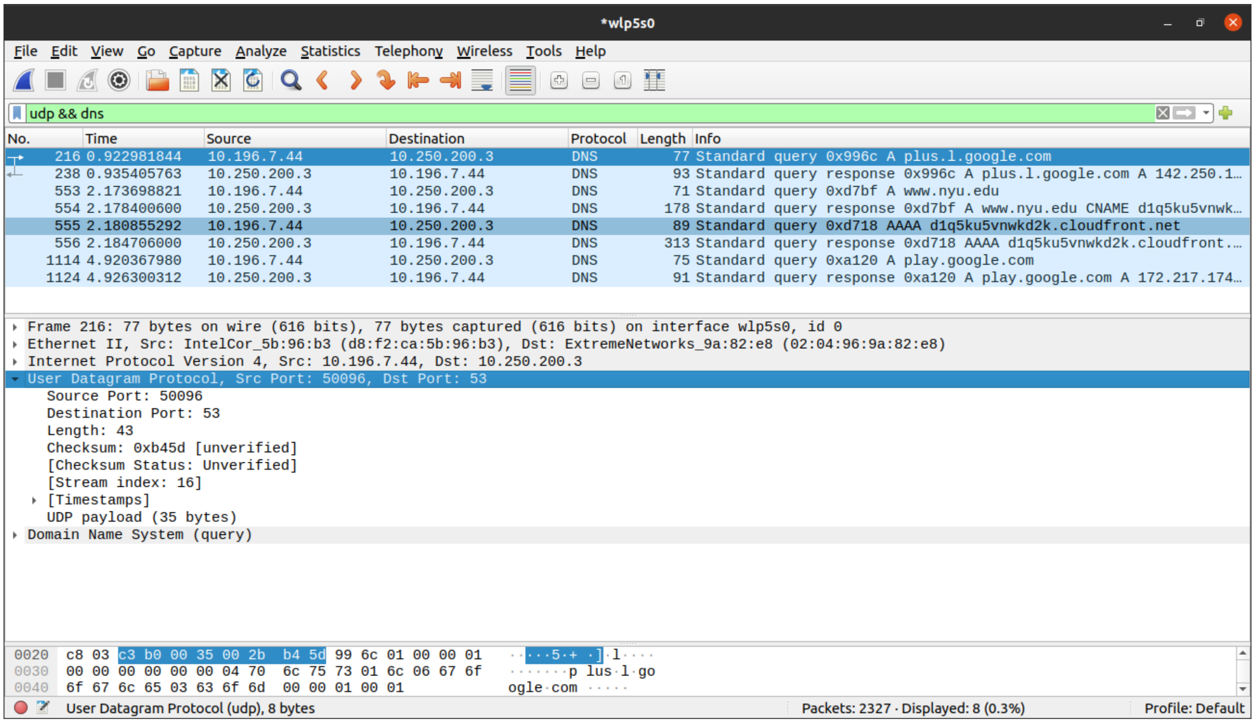
1. Select the first UDP segment in your trace. What is the packet number of this segment in the trace file? What type of application-layer protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields are there in the UDP header? What are the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

Ans: Packet number: ***216***

The type of application-layer protocol message being carried is: ***DNS***

The number of fields in the UDP header is ***4*** and they are::

- Source Port
- Destination Port
- Length
- Checksum


*wlp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp && dns
```

```
No.   Time         Source         Destination    Protocol Length Info
  216 0.922981844  10.196.7.44    10.250.200.3   DNS       77 Standard query 0x996c A plus.l.google.com
  238 0.935405763  10.250.200.3   10.196.7.44    DNS       93 Standard query response 0x996c A plus.l.google.com A 142.250.1…
  553 2.173698821  10.196.7.44    10.250.200.3   DNS       71 Standard query 0xd7bf A www.nyu.edu
  554 2.178400600  10.250.200.3   10.196.7.44    DNS      178 Standard query response 0xd7bf A www.nyu.edu CNAME d1q5ku5vnwk…
  555 2.180855292  10.196.7.44    10.250.200.3   DNS       89 Standard query 0xd718 AAAA d1q5ku5vnwkd2k.cloudfront.net
  556 2.184706000  10.250.200.3   10.196.7.44    DNS      313 Standard query response 0xd718 AAAA d1q5ku5vnwkd2k.cloudfront.…
 1114 4.920367980  10.196.7.44    10.250.200.3   DNS       75 Standard query 0xa120 A play.google.com
 1124 4.926300312  10.250.200.3   10.196.7.44    DNS       91 Standard query response 0xa120 A play.google.com A 172.217.174…
```

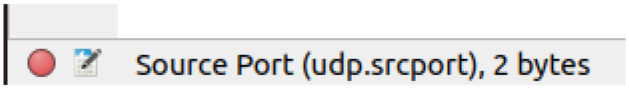
```
▸ Frame 216: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
▸ Internet Protocol Version 4, Src: 10.196.7.44, Dst: 10.250.200.3
▾ User Datagram Protocol, Src Port: 50096, Dst Port: 53
    Source Port: 50096
    Destination Port: 53
    Length: 43
    Checksum: 0xb45d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  ▸ [Timestamps]
    UDP payload (35 bytes)
▸ Domain Name System (query)
```

```
0020  c8 03 c3 b0 00 35 00 2b  b4 5d 99 6c 01 00 00 01   ·····5·+ ·]·l····
0030  00 00 00 00 00 00 04 70  6c 75 73 01 6c 06 67 6f   ·······p lus·l·go
0040  6f 67 6c 65 03 63 6f 6d  00 00 01 00 01            ogle·com ·····
```

```
User Datagram Protocol (udp), 8 bytes        Packets: 2327 · Displayed: 8 (0.3%)        Profile: Default
```

2. 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?

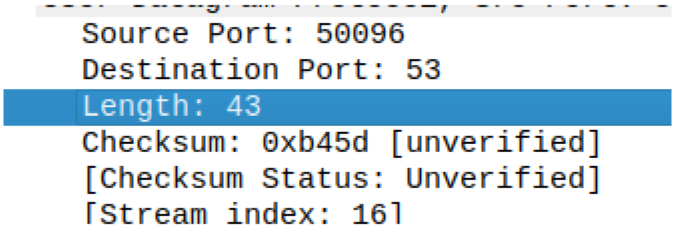
Ans: The length of each of the UDP header fields is: 2 bytes



```
Source Port (udp.srcport), 2 bytes
```

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

Ans: The value of the length field is: ***43***. The length of the entire UDP datagram, including the header and data, is indicated by the Length field of a UDP packet.



```
    Source Port: 50096
    Destination Port: 53
    Length: 43
    Checksum: 0xb45d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
```

4. 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)

Ans: The maximum number of bytes that can be included in a UDP payload will be:

Maximum UDP packet size - UDP header size = (2^16 - 1) - 8

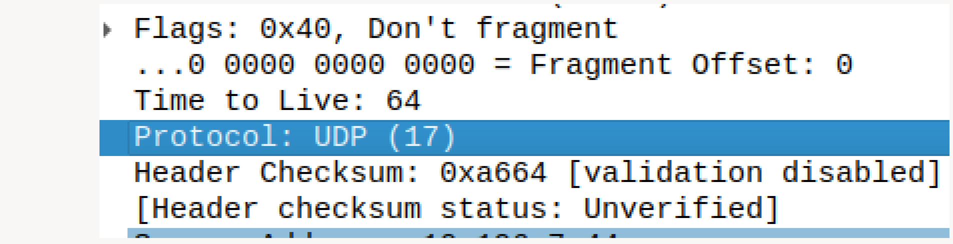
= ***65527***

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

Ans: The largest possible source port number is **2^16-1** = ***65535***

6. 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.

Ans: The protocol number for UDP is ***17*** in decimal notation which in hexadecimal notation is ***0x11***.



```
▸ Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xa664 [validation disabled]
  [Header checksum status: Unverified]
```

7. 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.

Ans: The packet number for the 1st UDP segment is: **216**

The packet number for the 2nd UDP segment is: **238**

For the UDP packet sent by the host, the source port is **50096** and the destination port is **53**

For the UDP packet sent as the reply of the first packet, the source port is **53**, and the destination port is: **50096**

Hence the source and destination ports for the 1st packet become the destination and source ports for the reply packet respectively. Thus, the port works as a source as well as a destination depending on the request or response packet.