CS 428
Lab 3
Baptiste Saliba

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

   Answer)
   There are 4 headers. Source port, destination port, length, checksum.

   User Datagram Protocol, Src Port: 57621, Dst Port: 57621
       Source Port: 57621
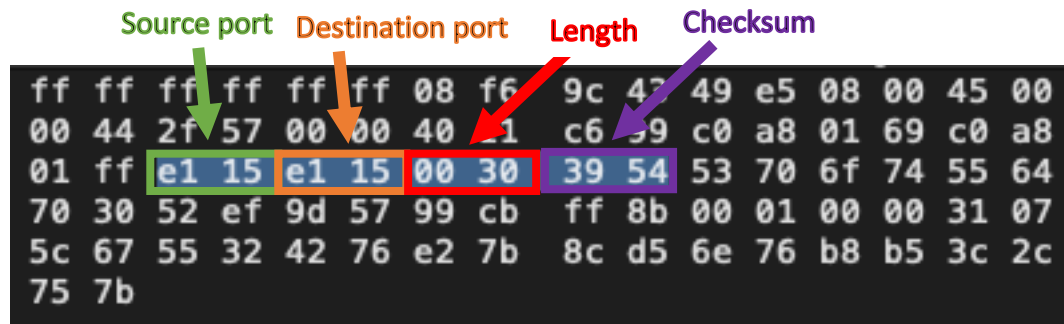   *Destination Port: 57621*
       Length: 48
       Checksum: 0x3954 [unverified]

2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

   Answer)
   Each of these headers is two bytes.

   Source port   Destination port   Length   Checksum
   ```
   ff ff ff ff ff ff 08 f6   9c 4  49 e5 08 00 45 00
   00 44 2f 57 00 00 40  1   c6  9 c0 a8 01 69 c0 a8
   01 ff e1 15 e1 15 00 30   39 54 53 70 6f 74 55 64
   70 30 52 ef 9d 57 99 cb   ff 8b 00 01 00 00 31 07
   5c 67 55 32 42 76 e2 7b   8c d5 6e 76 b8 b5 3c 2c
   75 7b
   ```

3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

   Answer)
   The length field is the length of the headers plus the length of the data.

   Headers: 4 headers, 2 bytes each, 8 bytes total
   Data: 40 bytes

   Length = headers_length + data_length = 48 bytes

   User Datagram Protocol, Src Port: 57621, Dst Port: 57621

Source Port: 57621
Destination Port: 57621
Length: 48
Checksum: 0x3954 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Data (40 bytes)

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)

    Answer)
    Seeing as the length field is 2 bytes this would mean that you can have a length between 2_{16}-1, so 0 – 65535. That means that the whole UDP message can be 65535 bytes but the data can only be 65527 bytes because 8 bytes are reserved for the headers.

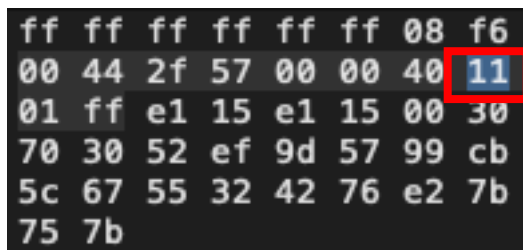5. What is the largest possible source port number? (Hint: see the hint in 4.)

    Answer)
    The 'source port' field length is also 2 bytes meaning that you can have a source port number between 2_{16}-1, so 0 – 65535. The largest possible source port number is 65535.

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

    Answer)
    The protocol number in hex is 0x11 and in decimal notation it is 17
    Protocol: UDP (17)

7. Examine a 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). Describe the relationship between the port numbers in the two packets.

    Answer)

The source port and destination port are flipped in the received packet

Sent

```
User Datagram Protocol, S
    Source Port: 50781
    Destination Port: 443
```

Received

```
User Datagram Protocol, Sr
    Source Port: 443
    Destination Port: 50781
```