

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header.

1975	10.826627	10.25.2.125	64.233.164.113	UDP	1392	52608 → 443 Len=1350
▼ User Datagram Protocol, Src Port: 52608, Dst Port: 443						
Source Port: 52608						
Destination Port: 443						
Length: 1358						
Checksum: 0x03d5 [unverified]						

Answer: 4 fields: Source port, Destination Port, Length, Checksum

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.

▼ User Datagram Protocol, Src Port: 52608, Dst Port: 443	
Source Port: 52608	
Destination Port: 443	
Length: 1358	
Checksum: 0x03d5 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 4]	
> [Timestamps]	
> Data (1350 bytes)	

0020	a4 71 cd 80 01 bb 05 4e 03 d5 c3 51 30 34 36 50	·q·····N···Q046P
0030	c1 e2 20 c8 c3 9b c7 e3 00 00 00 01 e5 f7 07 1d	·····M

▼ User Datagram Protocol, Src Port: 52608, Dst Port: 443	
Source Port: 52608	
Destination Port: 443	
Length: 1358	
Checksum: 0x03d5 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 4]	
> [Timestamps]	
> Data (1350 bytes)	

0020	a4 71 cd 80 01 bb 05 4e 03 d5 c3 51 30 34 36 50	·q·····N···Q046P
0030	c1 e2 20 c8 c3 9b c7 e3 00 00 00 01 e5 f7 07 1d	·····M

User Datagram Protocol, Src Port: 52608, Dst Port: 443
 Source Port: 52608
 Destination Port: 443
 Length: 1358
 Checksum: 0x03d5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 4]
 > [Timestamps]
 > Data (1350 bytes)

0020 a4 71 cd 80 01 bb 05 4e 03 d5 c3 51 30 34 36 50 ·q····N···Q046P

User Datagram Protocol, Src Port: 52608, Dst Port: 443
 Source Port: 52608
 Destination Port: 443
 Length: 1358
 Checksum: 0x03d5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 4]
 > [Timestamps]
 > Data (1350 bytes)

0020 a4 71 cd 80 01 bb 05 4e 03 d5 c3 51 30 34 36 50 ·q····N···Q046P

Answer: Each field/header is two bytes

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.

User Datagram Protocol, Src Port: 52608, Dst Port: 443
 Source Port: 52608
 Destination Port: 443
 Length: 1358
 Checksum: 0x03d5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 4]
 > [Timestamps]
 > Data (1350 bytes)
 Data: c35130343650c1e220c8c39bc7e30000004e5f7974de448...
 [Length: 1350]

Answer: Value of Length field is length of UDP header with UDP data.

Length: 1358, Data: 1350, Header: 4*2. (1358 = 1350 + 8)

4. What is the maximum number of bytes that can be included in a UDP payload?

Answer: $2^{16} - 1 - 8 = 65527$, thus max UDP payload is 65527 bytes

5. What is the largest possible source port number?

Answer: $2^{16} - 1 = 65535$, thus max 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

```

Internet Protocol Version 4, Src: 10.25.2.125, Dst: 64.233.164.113
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1378
    Identification: 0xc834 (51252)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x3b66 [validation disabled]
0010  05 62 c8 34 40 00 80 11 3b 66 0a 19 02 7d 40 e9  ·b·4@···;f···}@·
0020  a4 71 cd 80 01 bb 05 4e 03 d5 c3 51 30 34 36 50  ·q·····N···Q046P
0030  c1 e2 20 c8 c3 9b c7 e3 00 00 00 04 e5 f7 97 4d  ······M

```

Answer: Decimal: 17, Hexadecimal: 0x11

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. Describe the relationship between the port numbers in the two packets.

Frame	Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Length
509	17.315521	91.108.8.5	10.25.2.125	UDP	234	522 → 22767	Len=192
510	17.338279	10.25.2.125	91.108.8.5	UDP	218	22767 → 522	Len=176

```

> Frame 509: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_
> Ethernet II, Src: Cisco_66:73:bf (10:05:ca:66:73:bf), Dst: ASUSTekC_2e:21:96 (ac:9e:17:2e:21:96)
> Internet Protocol Version 4, Src: 91.108.8.5, Dst: 10.25.2.125
> User Datagram Protocol, Src Port: 522, Dst Port: 22767
  Source Port: 522
  Destination Port: 22767
  Length: 200
  Checksum: 0x038c [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  > Data (192 bytes)

```

Frame	Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Length
509	17.315521	91.108.8.5	10.25.2.125	UDP	234	522 → 22767	Len=192
510	17.338279	10.25.2.125	91.108.8.5	UDP	218	22767 → 522	Len=176

```

> Frame 510: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface \Device\NPF_{
> Ethernet II, Src: ASUSTekC_2e:21:96 (ac:9e:17:2e:21:96), Dst: Cisco_66:73:bf (10:05:ca:66:73:bf)
> Internet Protocol Version 4, Src: 10.25.2.125, Dst: 91.108.8.5
> User Datagram Protocol, Src Port: 22767, Dst Port: 522
  Source Port: 22767
  Destination Port: 522
  Length: 184
  Checksum: 0xb0be [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  > Data (176 bytes)

```

Answer: Ones 'Source Port' others 'Destination Port' as well as ones 'Destination Port' others 'Source Port'