

**COMPUTER NETWORKS**  
**ASSIGNMENT 3**  
**SUSHMITHA NAGARAJAN**  
**1001556348**

## QUESTION 1: -

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.

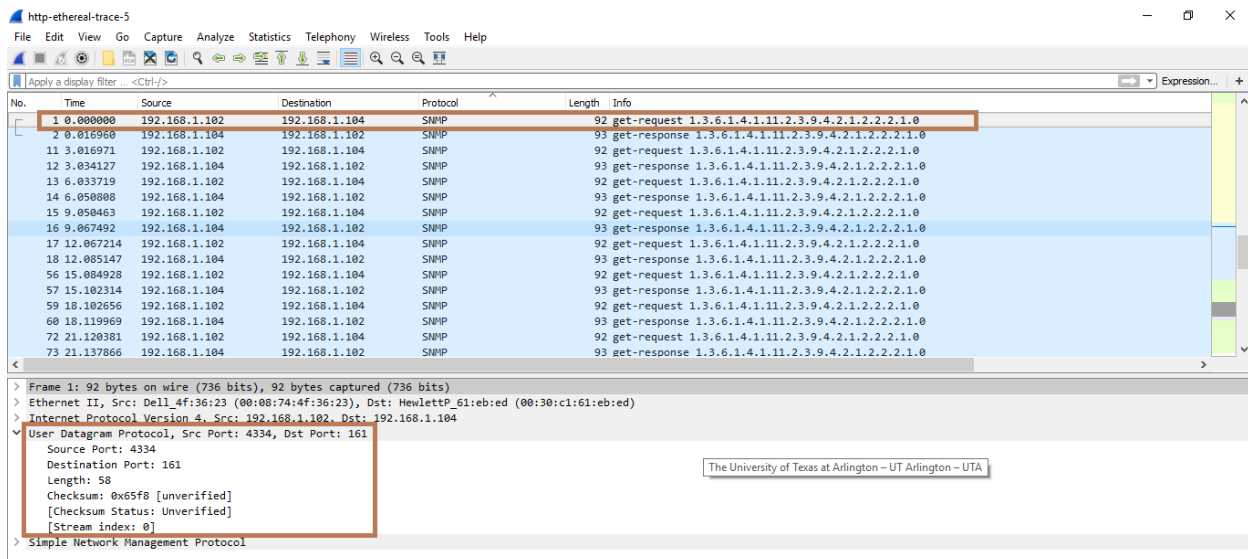
Answer: The screenshot describes the first packet of the UDP in the captured file.

It explains in the information section that it has UDP fields.

The UDP packet contains four fields in the UDP header.

They are as follows :

- Source Port
- Destination Port
- Length
- Checksum



## QUESTION 2:

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: The length(in bytes) of each of the UDP header fields are as follows:

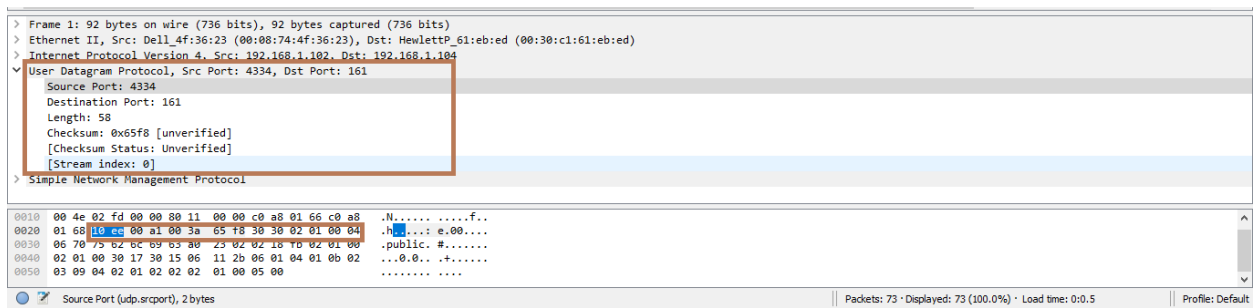
Each field has 2 bytes.

Source port: 2 bytes

Destination port: 2 bytes

Length: 2 bytes

Checksum: 2 bytes



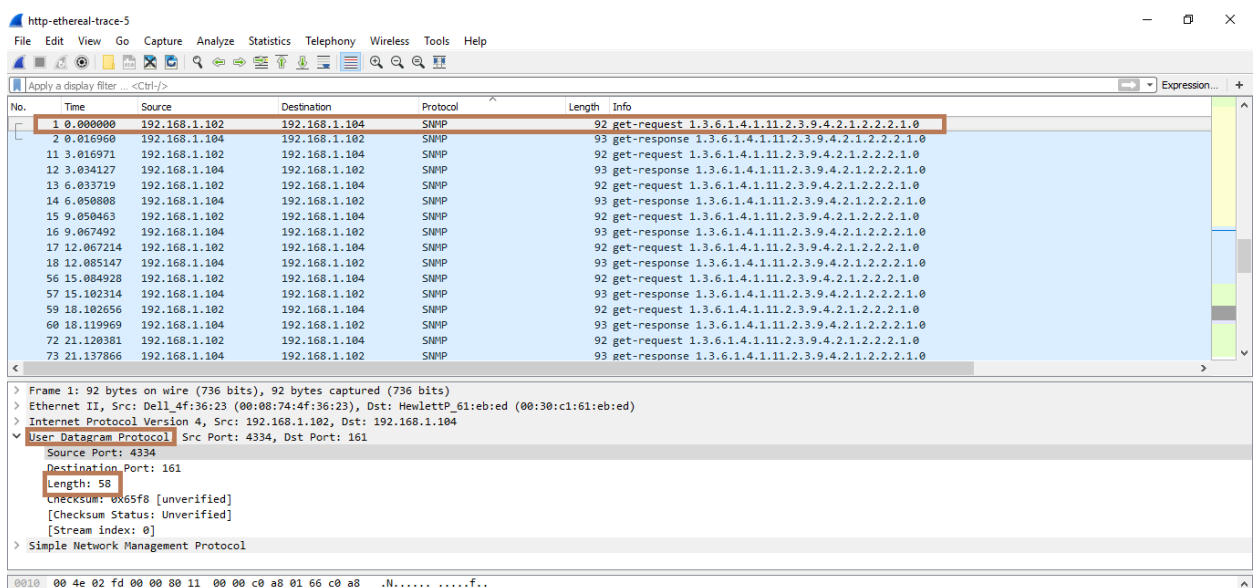
This explains that the UDP packet header and each of its fields contain only 2 bytes.

## QUESTION 3

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 value of the Length field in the Length- UDP packet is 58 bytes.

The length field provides the number of bytes in the UDP segment (header information + data information) which explains that 8 bytes are the sum of the header bytes and the remaining data bytes encapsulated in the UDP packet itself.



#### QUESTION 4

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:

The maximum possible number of bytes that can be included in a UDP payload are  $2^{16} = 65535$ . The bytes already used by the header field is 8 bytes. Thus, the maximum payload would be  $65535 - 8 = 65527$ .

#### QUESTION 5

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

Answer:

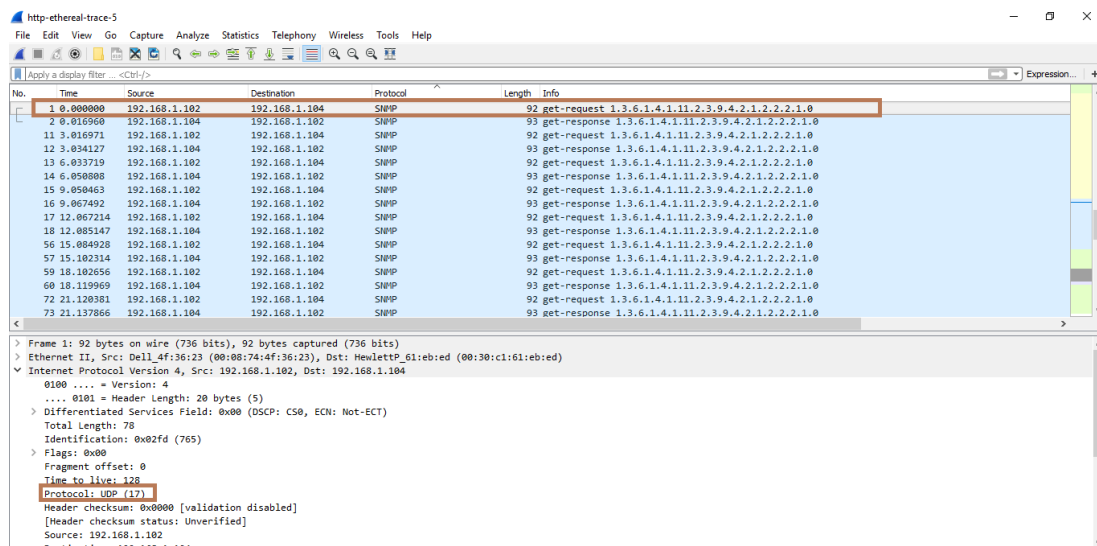
The largest possible source port number =  $2^{16} = 65535$ .

#### QUESTION 6

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 for UDP is 17 in decimal notation that is equivalent to 0x11 in the hexadecimal notation. The screenshot describes the UDP protocol number as 17.



http-ethereal-trace-5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.016950	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
11	3.016971	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
12	3.034127	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
13	6.033719	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
14	6.050808	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
15	9.050463	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
16	9.067492	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	12.067214	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
18	12.085147	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
56	15.084928	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
57	15.102314	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
59	18.102656	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
60	18.119969	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
72	21.120381	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
73	21.137866	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 78  
 Identification: 0x02fd (765)  
 > Flags: 0x00  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: UDP (17)

```

0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a....t0G#.E.
0010 00 4e 02 fd 00 00 00 00 00 00 c0 a8 01 56 c0 a8 .N.....f...
0020 01 68 10 ee 00 01 00 00 65 f8 30 30 02 01 00 04 .h.....e.00...
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00 .public.#.....
0040 02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02 ..0.0..+.....
0050 03 09 04 02 01 02 02 01 00 05 00 .....
  
```

## QUESTION 7

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 relationship between these two port numbers in these two packets are the source port on the send message will act as a destination port of the receive message.

The destination port is used to the send message acts as the source port for the receive message. UDP sent from the host are as follows

http-ethereal-trace-5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.016950	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
11	3.016971	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
12	3.034127	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
13	6.033719	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
14	6.050808	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
15	9.050463	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
16	9.067492	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	12.067214	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
18	12.085147	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
56	15.084928	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
57	15.102314	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
59	18.102656	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
60	18.119969	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
72	21.120381	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
73	21.137866	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)  
 > Ethernet II, Src: Dell\_4f:36:23 (08:00:74:4f:36:23), Dst: HewlettP\_61:eb:ed (00:30:c1:61:eb:ed)  
 > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104  
 > User Datagram Protocol, Src Port: 4334, Dst Port: 161  
   Source Port: 4334  
   Destination Port: 161  
   Length: 58  
   Checksum: 0x65f8 [unverified]  
   [Checksum Status: Unverified]  
   [Stream index: 0]  
 > Simple Network Management Protocol

## UDP reply to the host

The image shows a Wireshark packet capture window titled "http-ethereal-trace-5". The main pane displays a list of 73 packets. Packet 2, at time 0.016960, is a UDP response from 192.168.1.104 to 192.168.1.102. It is highlighted with a red box. The packet details pane below shows the following structure:

- Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
- Ethernet II, Src: HewlettP\_61:eb:red (00:30:c1:61:eb:red), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)
- Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
- User Datagram Protocol, Src Port: 161, Dst Port: 4334
  - Length: 59
  - Checksum: 0x53f2 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 0]
- Simple Network Management Protocol