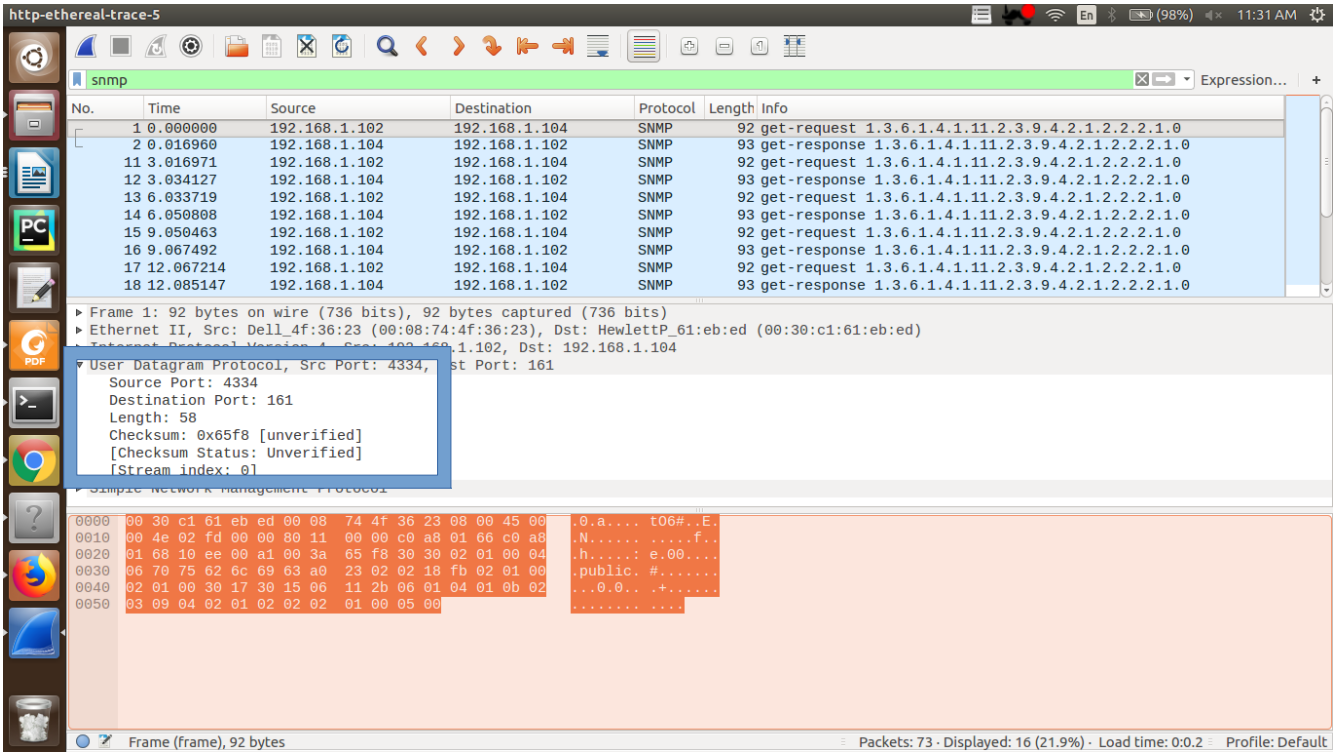
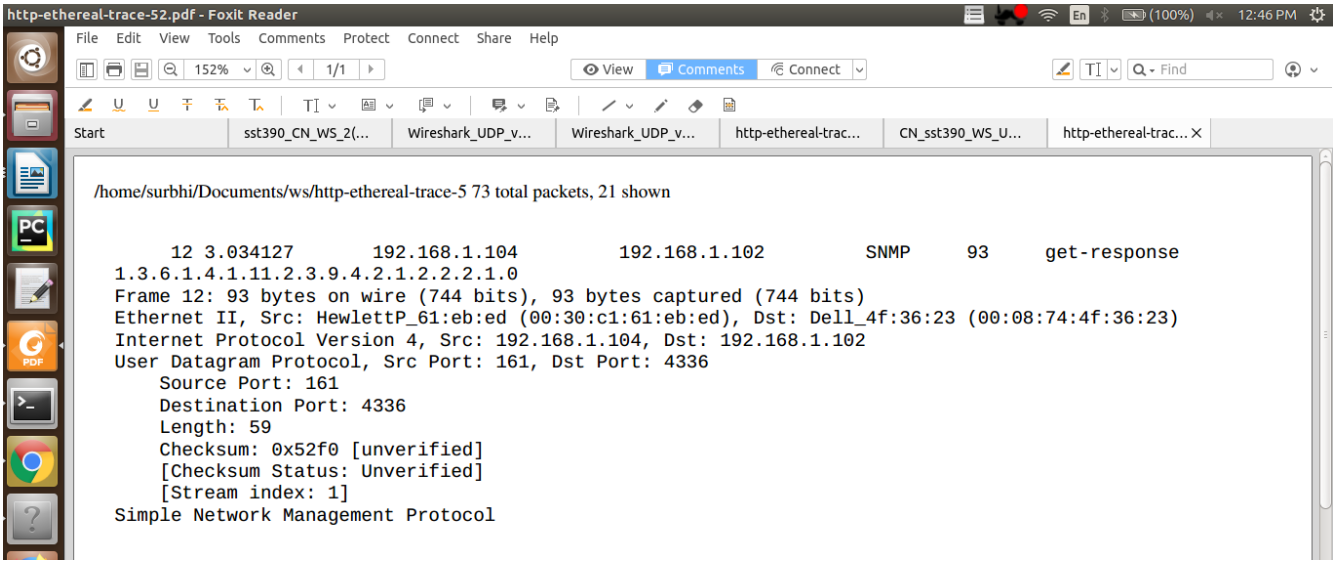


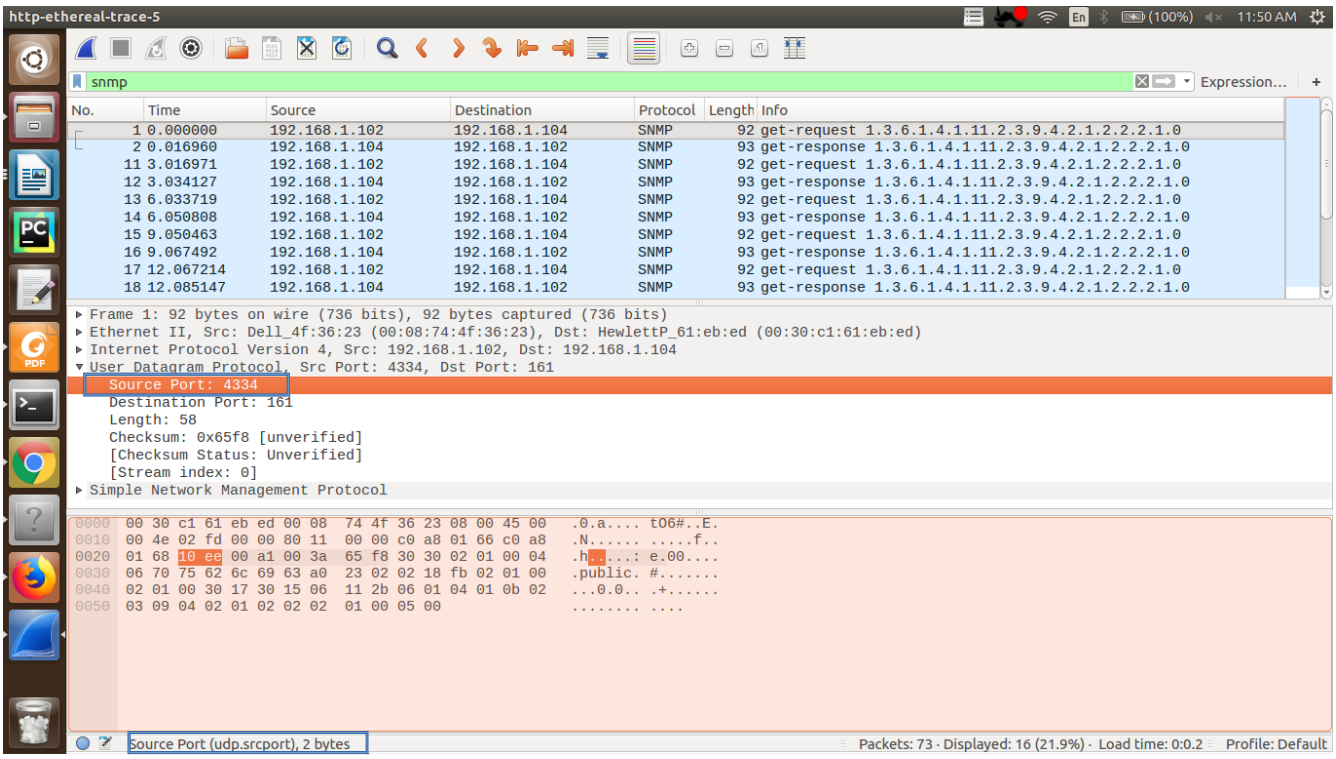
1) 1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header.

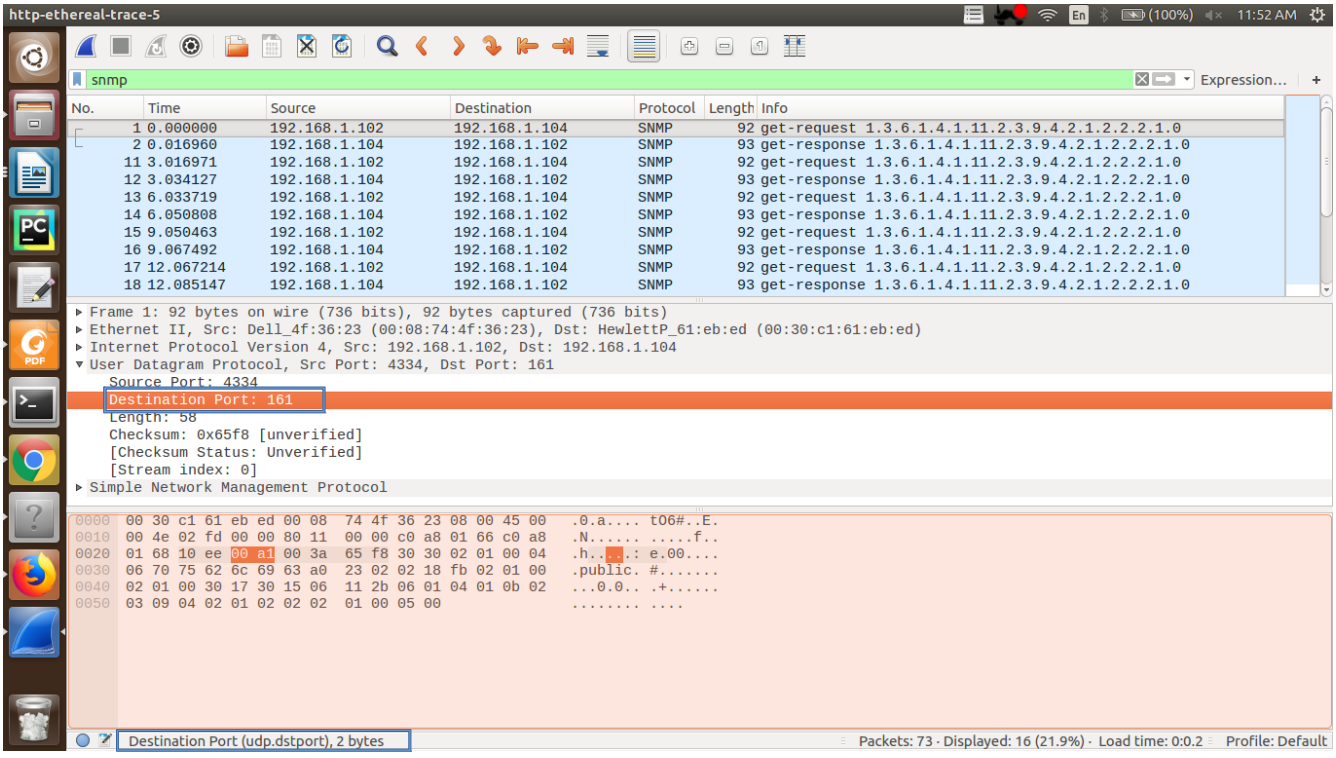
Ans: a) Source Port b) Destination Port c) Length d) Checksum

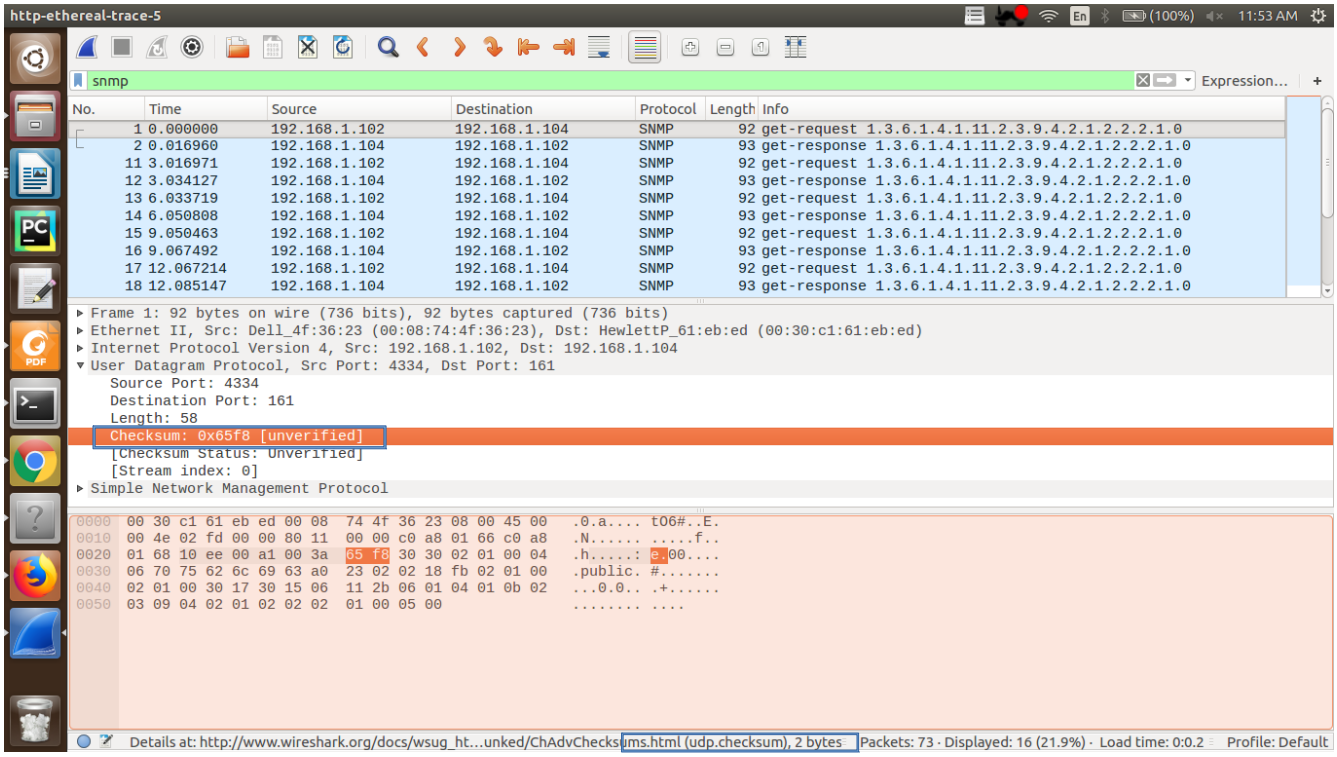


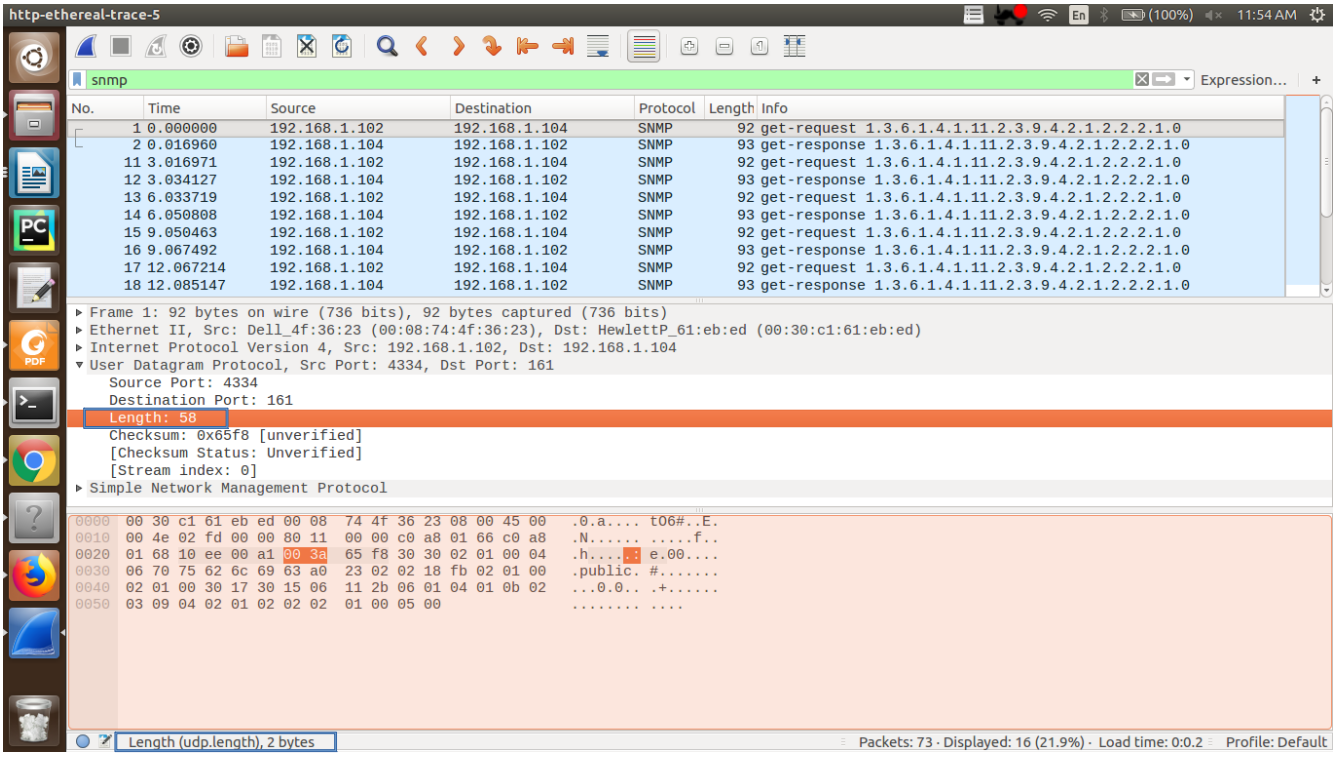
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Ans: The total length of UDP Header is 8 Bytes. For each field it is 2 Bytes. Can be seen from below Screen shots.


http-ethereal-trace-5
11:50 AM
snmp
Expression...
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 0.016960 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
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f: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
0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a.... tO6#..E.
0010 00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8 .N..... .....f..
0020 01 68 10 ee 00 a1 00 3a 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 02 01 00 05 00 ....
Source Port (udp.srcport), 2 bytes
Packets: 73 · Displayed: 16 (21.9%) · Load time: 0:0.2
Profile: Default

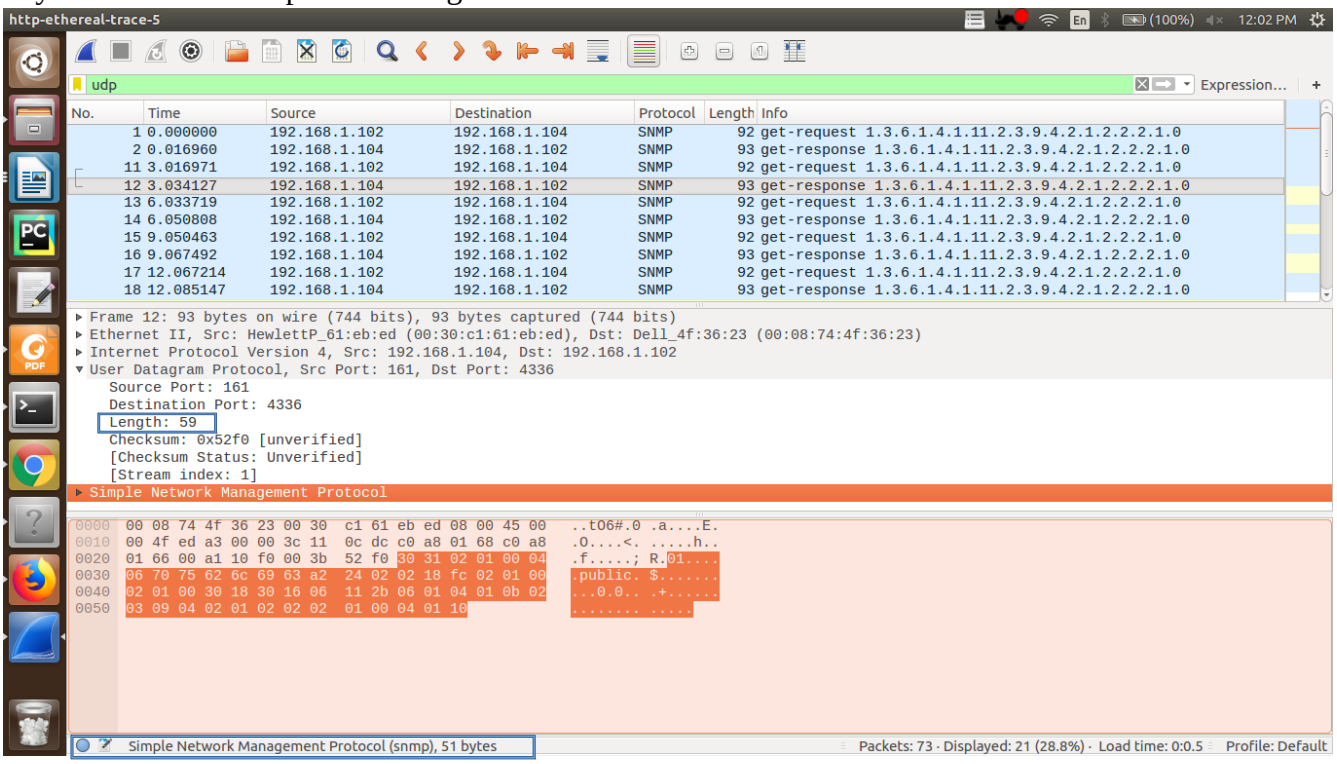

http-ethereal-trace-5
11:52 AM
snmp
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2 0.016960 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
11 3.016971 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
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f: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
0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a.... tO6#..E.
0010 00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8 .N..... .....f..
0020 01 68 10 ee 00 a1 00 3a 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 02 01 00 05 00 ....
Destination Port (udp.dstport), 2 bytes
Packets: 73 · Displayed: 16 (21.9%) · Load time: 0:0.2
Profile: Default

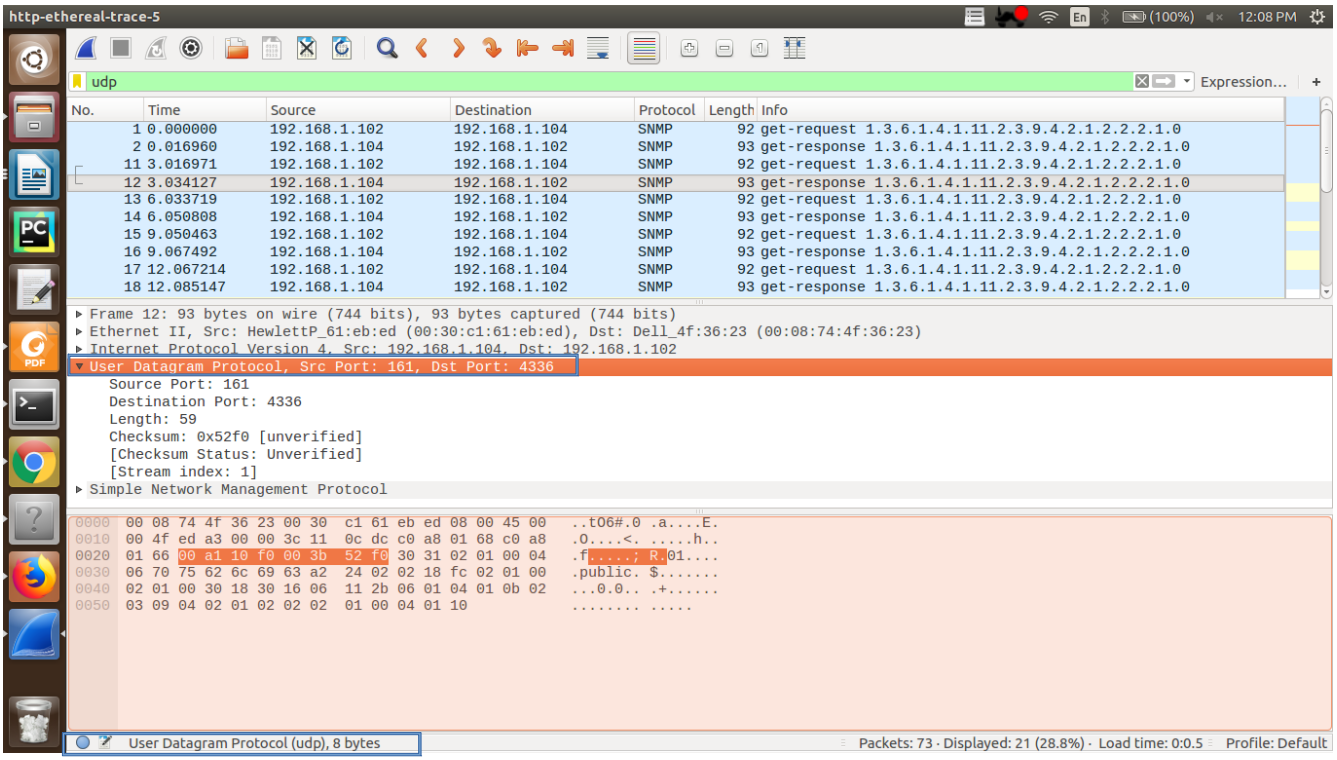

http-ethereal-trace-5
11:53 AM
snmp
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2 0.016960 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
11 3.016971 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
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f: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
0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a.... tO6#..E.
0010 00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8 .N..... .....f..
0020 01 68 10 ee 00 a1 00 3a 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 02 01 00 05 00 ....
Details at: http://www.wireshark.org/docs/wsug_ht...unked/ChAdvChecksums.html (udp.checksum), 2 bytes
Packets: 73 · Displayed: 16 (21.9%) · Load time: 0:0.2
Profile: Default


http-ethereal-trace-5
11:54 AM
snmp
Expression...
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 0.016960 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
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f: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
0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a.... tO6#..E.
0010 00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8 .N..... .....f..
0020 01 68 10 ee 00 a1 00 3a 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 02 01 00 05 00 ....
Length (udp.length), 2 bytes
Packets: 73 · Displayed: 16 (21.9%) · Load time: 0:0.2
Profile: Default

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.

Ans: Total value in length field = 59 bytes. (i.e. 8 bytes of UDP header + 51 bytes of payload)
Payload is SNMP Response message. Can be verified from below Screen Shot.

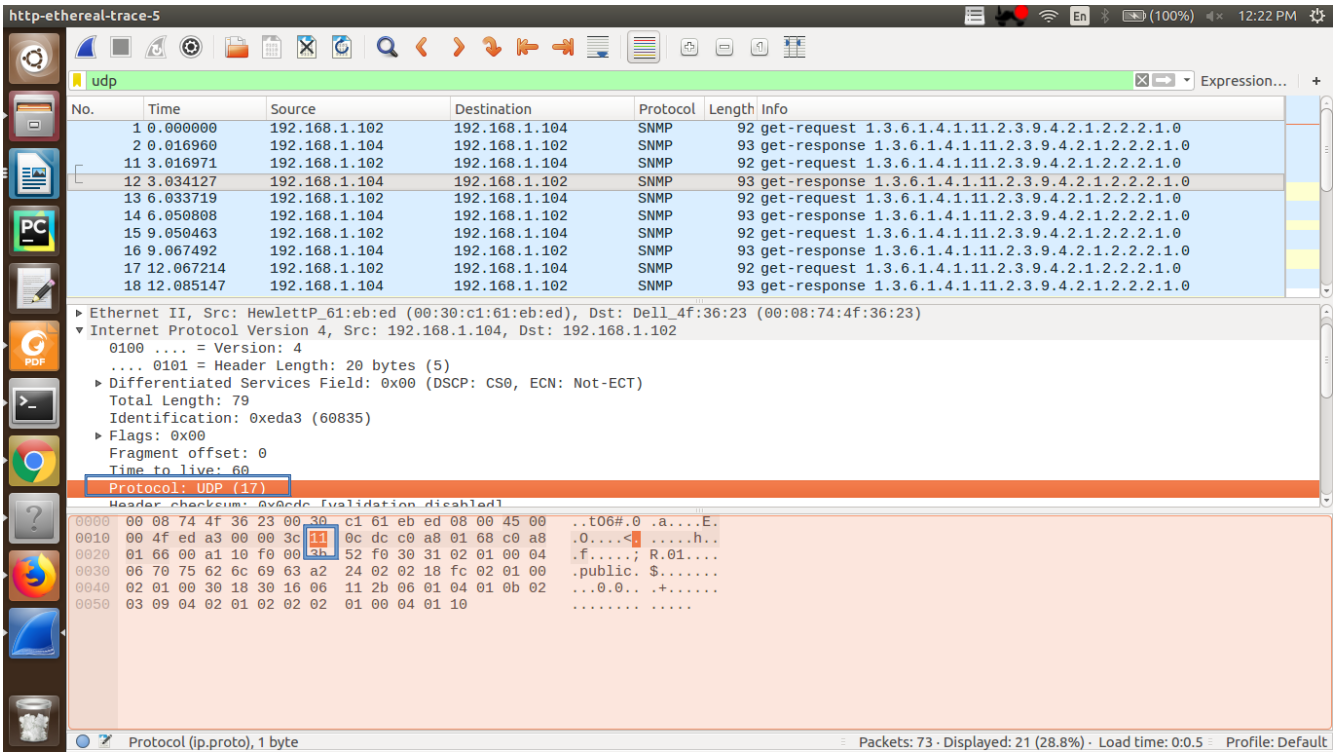




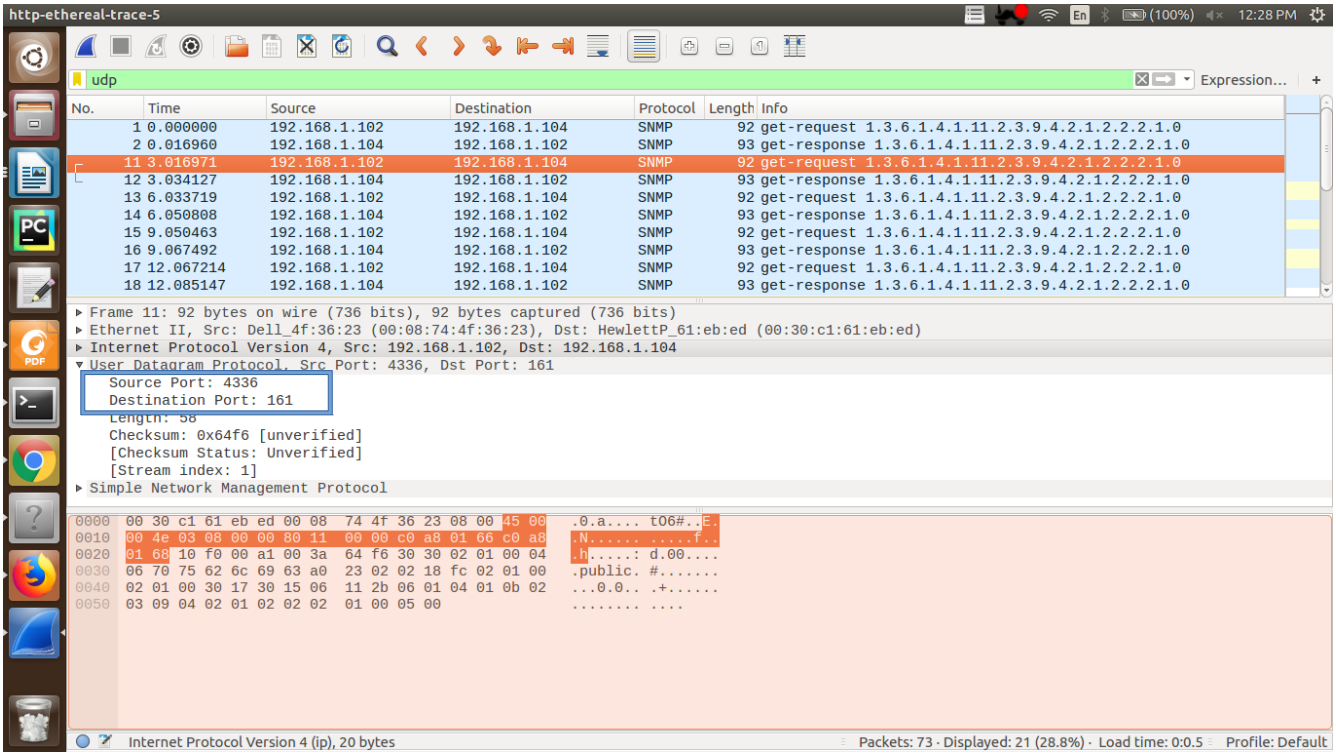
4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)
Ans:- The size of length field in UPD Header is 2 Bytes as shown above in Question 2nd.
2 Bytes = 16 Bits. Therefore the total length that can be stored is : 2^16 -1 = 65535, which is the total length of UDP Packet. The UDP Header is of 8 bytes.
Therefore the payload data can be : 65535 – 8 = 65527 Bytes.

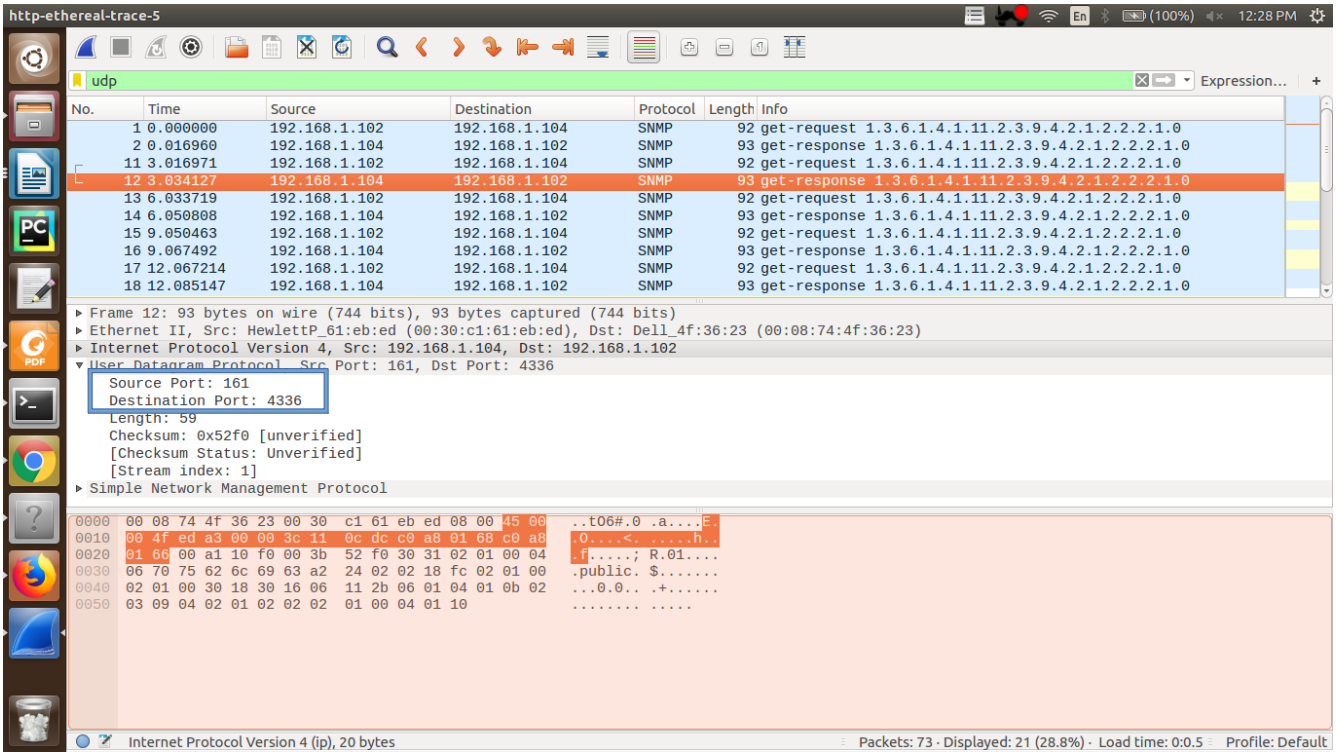
5. What is the largest possible source port number?
Ans: The largest possible source port number is : 65535.
The source port number is of 2 bytes → 16 bits. Therefore, 2^ 16 – 1= 65535

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.
Ans: The protocol number for UDP is 17 in decimal and 0x11 in Hexadecimal notation.
Can be verified from below attached Screen Shot.



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.
Ans: The Get Request UDP packet has:
Source Port number : 4336 and Destination Port Number : 161.
The Response UDP packet consists:
Source port Number : 161
Destination port Number : 4336. This can be verified from attached screen shots. Thus, the port on which we request data from the host ie the source port becomes the destination port when responding the request.


http-ethereal-trace-5
udp
Expression...
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 0.016960 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
Frame 11: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f: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: 4336, Dst Port: 161
Source Port: 4336
Destination Port: 161
Length: 58
Checksum: 0x64f6 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Simple Network Management Protocol
0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a.... tO6#..E.
0010 00 4e 03 08 00 00 80 11 00 00 c0 a8 01 66 c0 a8 .N..... .....f..
0020 01 68 10 f0 00 a1 00 3a 64 f6 30 30 02 01 00 04 .h.....: d.00....
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 fc 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 02 01 00 05 00 ....
Internet Protocol Version 4 (ip), 20 bytes
Packets: 73 · Displayed: 21 (28.8%) · Load time: 0:0.5
Profile: Default


http-ethereal-trace-5
udp
Expression...
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 0.016960 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
Frame 12: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
Ethernet II, Src: HewlettP_61:eb:ed (00:30:c1:61:eb:ed), 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: 4336
Source Port: 161
Destination Port: 4336
Length: 59
Checksum: 0x52f0 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Simple Network Management Protocol
0000 00 08 74 4f 36 23 00 30 c1 61 eb ed 08 00 45 00 ..tO6#.0 .a....E.
0010 00 4f ed a3 00 00 3c 11 0c dc c0 a8 01 68 c0 a8 .O....<. .....h..
0020 01 66 00 a1 10 f0 00 3b 52 f0 30 31 02 01 00 04 .f.....; R.01....
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 fc 02 01 00 .public. $.......
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02 ...0.0.. .+......
0050 03 09 04 02 01 02 02 02 01 00 04 01 10 ....
Internet Protocol Version 4 (ip), 20 bytes
Packets: 73 · Displayed: 21 (28.8%) · Load time: 0:0.5
Profile: Default