Computer Networks 1

Lab 3b

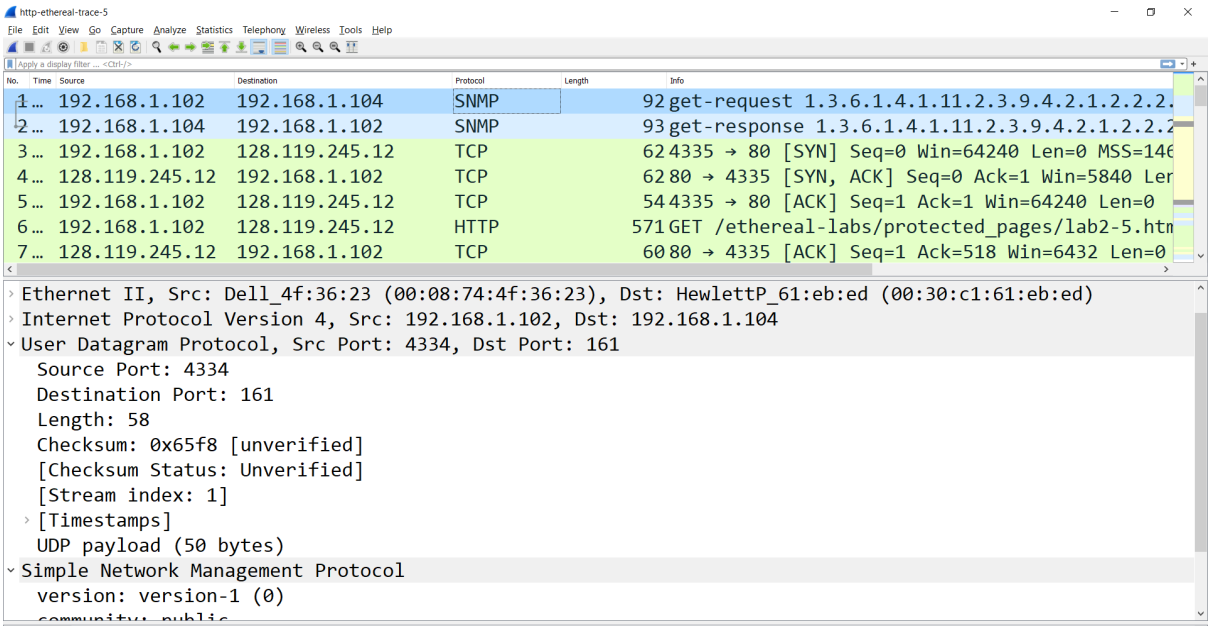
Wireshark Lab: UDP v8.0

Student Name: **Nguyễn Quý Hải**

Student No.: **2052974**

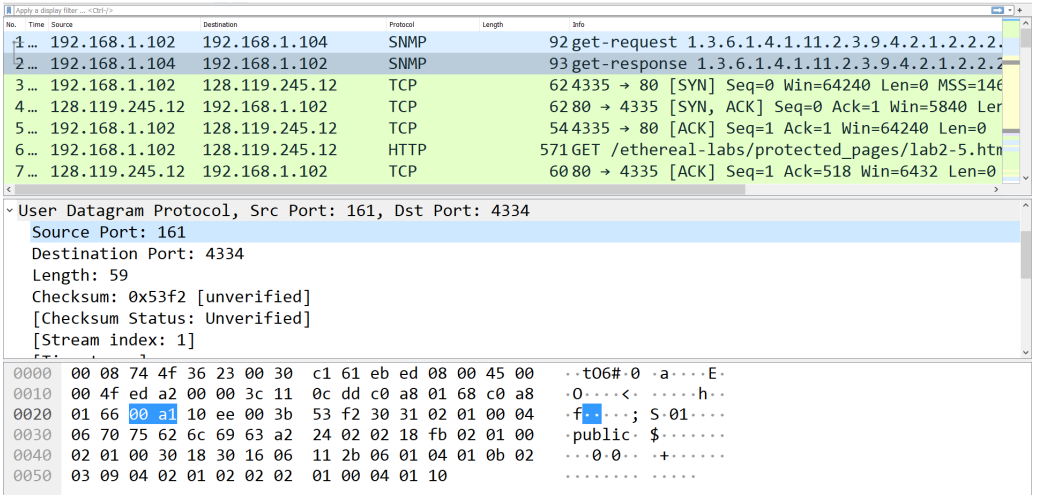
- Q1: Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

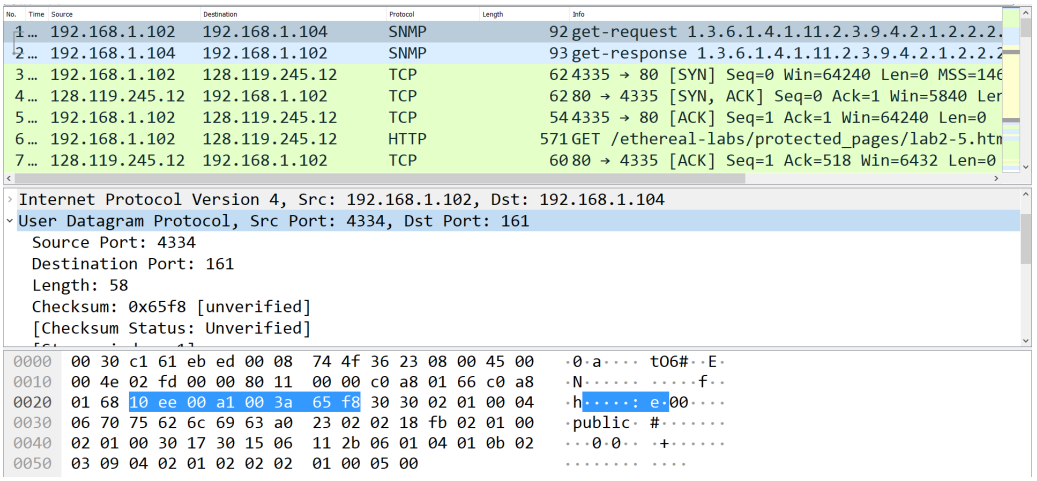
  Answer: 4 fields: Source port, Destination port, Length, CheckSum



- Q2. 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.

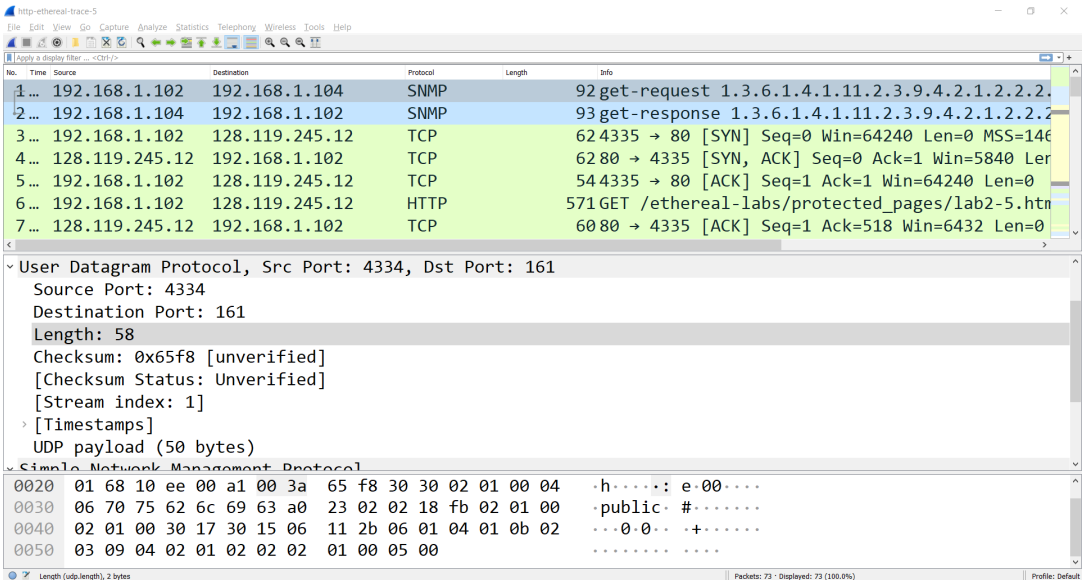
  Answer: Each of the UDP header fields is 2 bytes. Altogether, is 2 * 4 = 8 bytes





- Q3. 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: Length = UDP payload + UDP header. As we can see that, Length = 58 is the sum of UDP payload (50) and UDP header (8) as I calculated above



- Q4. 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)

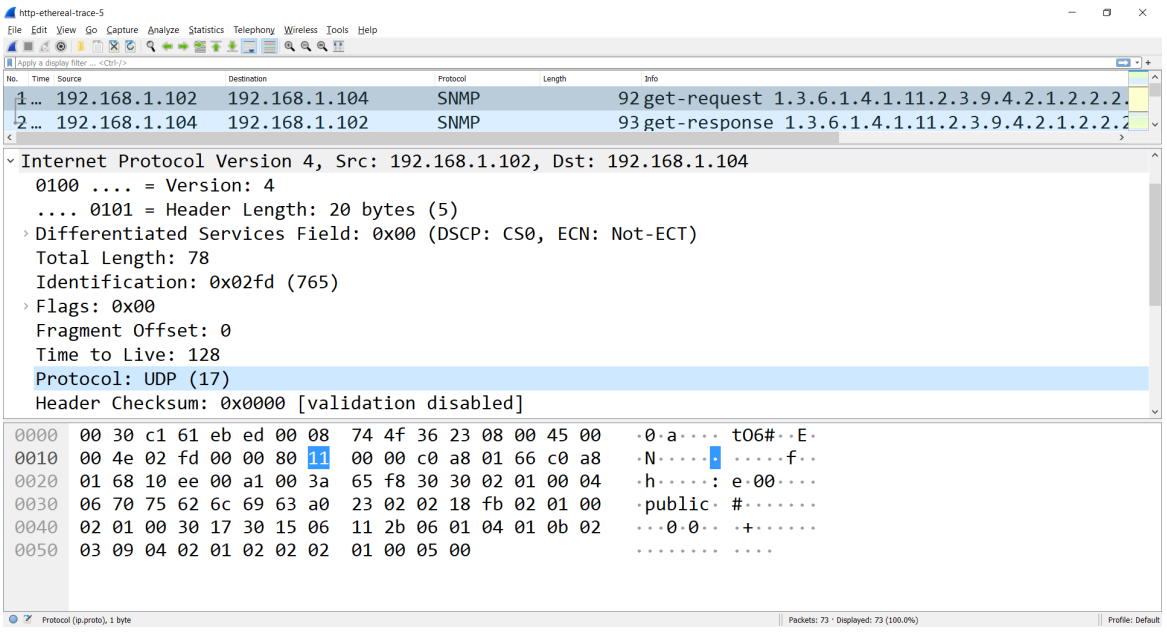
  Answer: The maximum number of bytes of UDP payload is $2^{16} - 1$ = 65535 bytes. So the maximum number of bytes that can be included in a UDP payload is 65535 - 8 = 65527 bytes

- Q5. What is the largest possible source port number? (Hint: see the hint in 4.)

  Answer: $2^{16} - 1$ = 65535 bytes.

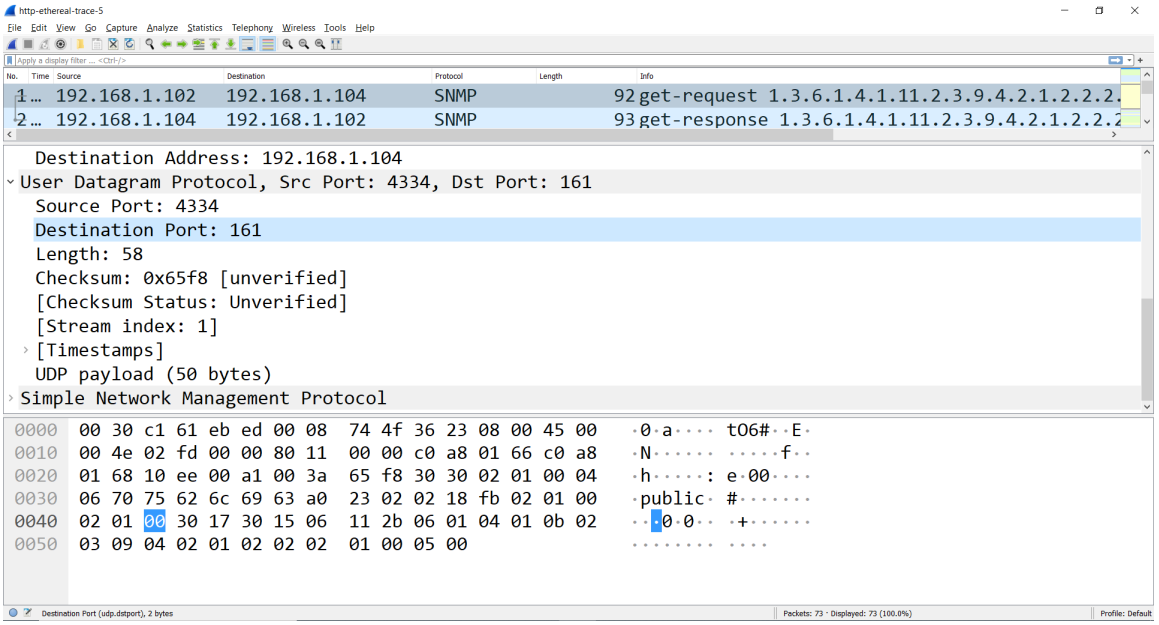
- Q6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

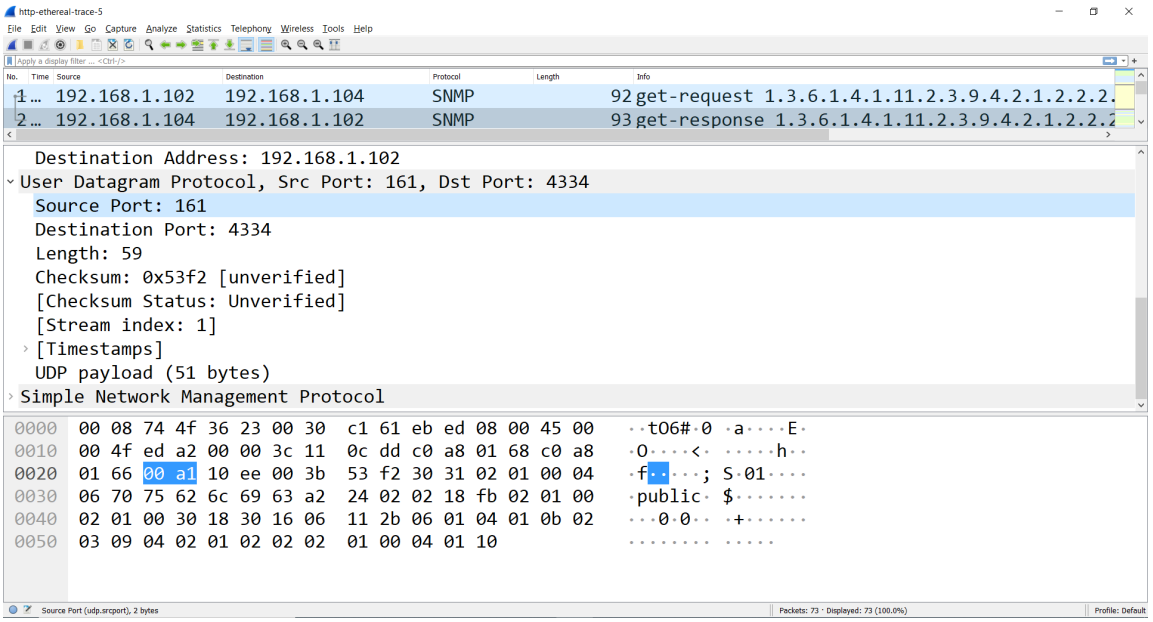
  Answer: It is **17** in decimal (11 in hexadecimal)



- Q7. 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: Destination port number of the first packet is the same as source port number of the second packet, that is 161. Furthermore, source port number of the first packet is the same as destination port number of the second packet (4334).


http-ethereal-trace-5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 … 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
2 … 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
Destination Address: 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: 1]
[Timestamps]
UDP payload (50 bytes)
Simple Network Management Protocol
0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00
0010 00 4e 02 fd 00 00 80 11 00 00 c0 a8 01 66 c0 a8
0020 01 68 10 ee 00 a1 00 3a 65 f8 30 30 02 01 00 04
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00
0040 02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02
0050 03 09 04 02 01 02 02 02 01 00 05 00
Destination Port (udp.dstport), 2 bytes
Packets: 73 · Displayed: 73 (100.0%)
Profile: Default


http-ethereal-trace-5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 … 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
2 … 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
Destination Address: 192.168.1.102
User Datagram Protocol, Src Port: 161, Dst Port: 4334
Source Port: 161
Destination Port: 4334
Length: 59
Checksum: 0x53f2 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
UDP payload (51 bytes)
Simple Network Management Protocol
0000 00 08 74 4f 36 23 00 30 c1 61 eb ed 08 00 45 00
0010 00 4f ed a2 00 00 3c 11 0c dd c0 a8 01 68 c0 a8
0020 01 66 00 a1 10 ee 00 3b 53 f2 30 31 02 01 00 04
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 fb 02 01 00
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02
0050 03 09 04 02 01 02 02 02 01 00 04 01 10
Source Port (udp.srcport), 2 bytes
Packets: 73 · Displayed: 73 (100.0%)
Profile: Default