

Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

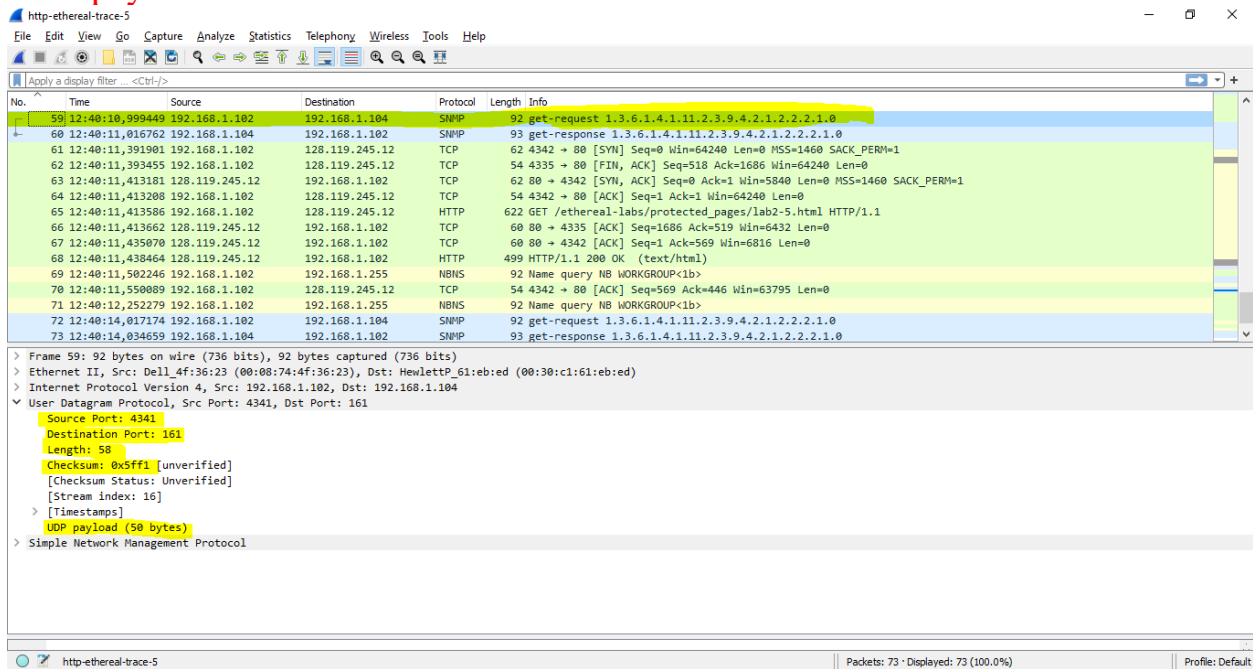
LAB 3b

(Sử dụng file http-ethereal-trace-5.)

Question 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:

Trong tiêu đề UDP có 5 field là source port, destination port, length, checksum
UDP payload



Question 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:

Độ dài của các header:
- Source port: 2 bytes.

http-ethereal-trace-5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|---------------|---------------|----------|--------|---|
| 59 | 12:40:10.999449 | 192.168.1.102 | 192.168.1.104 | SNMP | 92 | get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |
| 60 | 12:40:11.016762 | 192.168.1.104 | 192.168.1.102 | SNMP | 93 | get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |

> Frame 59: 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: 4341, Dst Port: 161

Source Port: 4341

Destination Port: 161

Length: 58

Checksum: 0x5ff1 [unverified]

[Checksum Status: Unverified]

[Stream index: 16]

> [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  0-a-----tOG#-E-
0010  00 4e 03 20 00 00 00 11 00 00 c0 a8 01 66 c0 a8  0-N-----f-
0020  01 68 10 75 00 a1 00 3a 5f f1 30 30 02 01 00 04  0-h-:--00-
0030  06 70 75 62 6c 69 63 a0 23 02 02 19 01 02 01 00  0-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 byte(s)

Packets: 73 · Displayed: 73 (100.0%)

Profile: Default

- Destination port: 2 bytes

http-ethereal-trace-5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|---------------|---------------|----------|--------|---|
| 59 | 12:40:10.999449 | 192.168.1.102 | 192.168.1.104 | SNMP | 92 | get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |
| 60 | 12:40:11.016762 | 192.168.1.104 | 192.168.1.102 | SNMP | 93 | get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |

> Frame 59: 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: 4341, Dst Port: 161

Source Port: 4341

Destination Port: 161

Length: 58

Checksum: 0x5ff1 [unverified]

[Checksum Status: Unverified]

[Stream index: 16]

> [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  0-a-----tOG#-E-
0010  00 4e 03 20 00 00 00 11 00 00 c0 a8 01 66 c0 a8  0-N-----f-
0020  01 68 10 75 00 a1 00 3a 5f f1 30 30 02 01 00 04  0-h-:--00-
0030  06 70 75 62 6c 69 63 a0 23 02 02 19 01 02 01 00  0-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

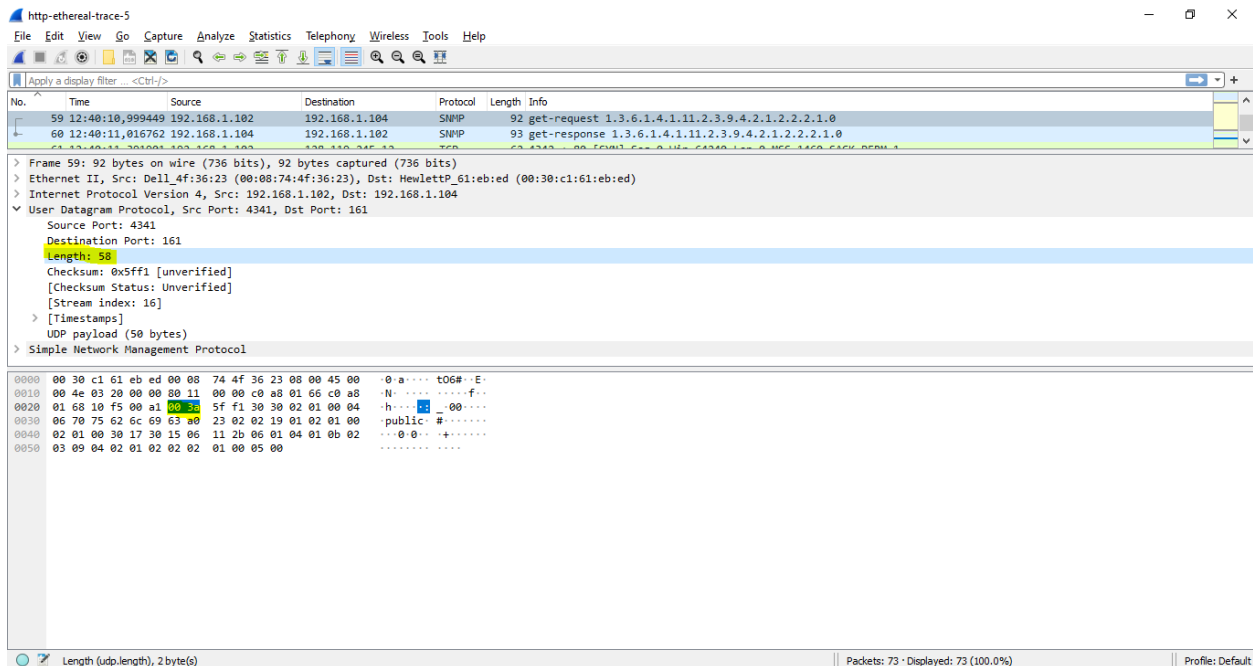
```

Destination Port (udp.dstport), 2 byte(s)

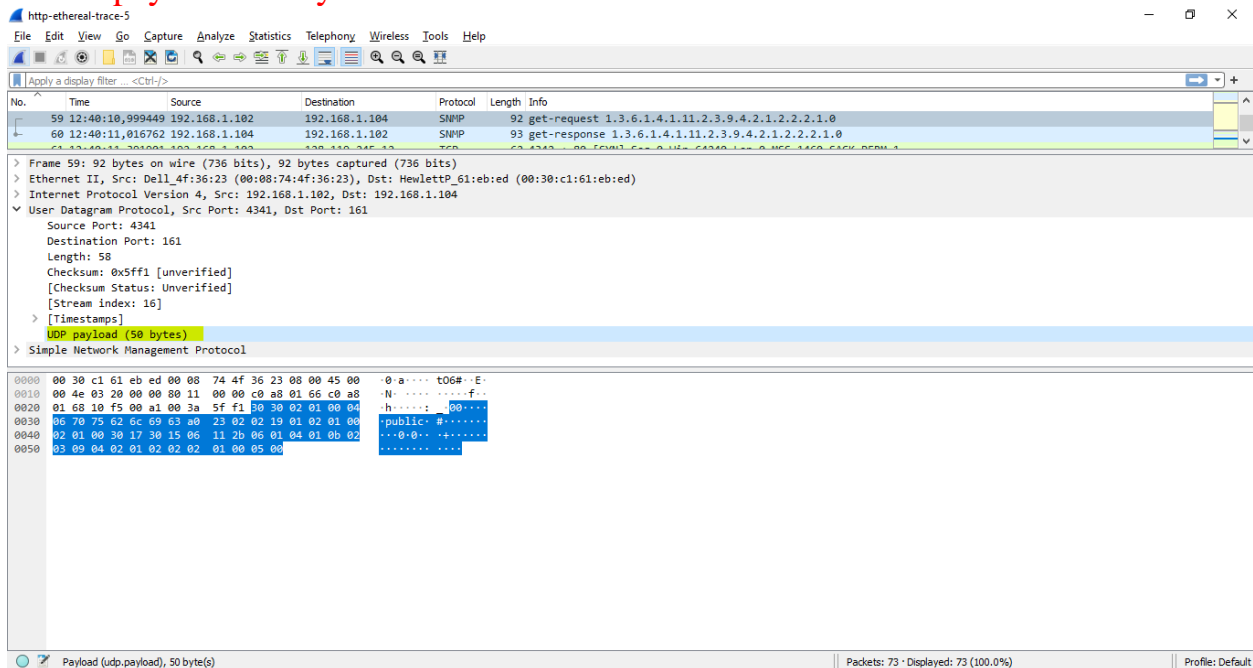
Packets: 73 · Displayed: 73 (100.0%)

Profile: Default

- Length: 2 bytes



- UDP payload: 50 bytes



Question 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:

Length field = 59 bytes. Trong đó:

+ 8 bytes: header field

+ 51 bytes dữ liệu còn lại: trong gói tin

Question 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:

Số lượng bytes tối đa có thể nằm trong UDP payload = $2^{16} - 8 = 65528$ bytes.

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

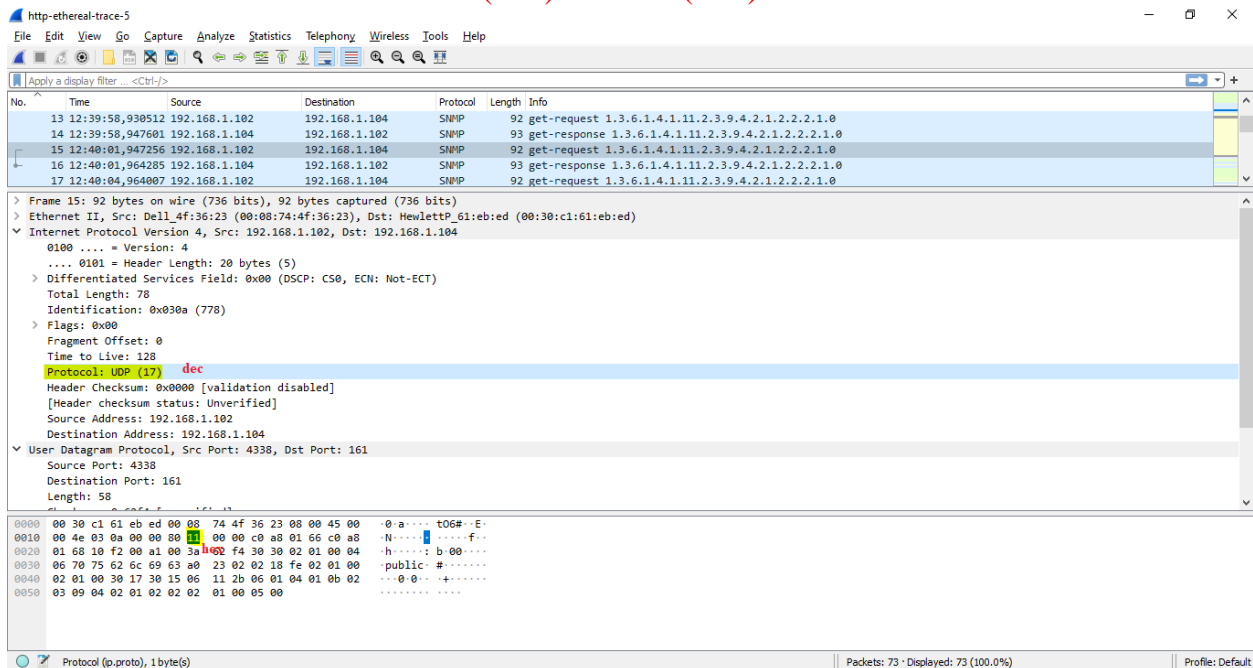
ANSWER:

Source port number lớn nhất có thể = $2^{16} = 65536$

Question 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:

Protocol number for UDP = 17 (dec) = 0x11 (hex)



Question 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:

Relationship:

- + Source port của gói tin gửi = Destination port của gói tin nhận.
- + Source port của gói tin nhận = Destination port của gói tin gửi.

http-ethereal-trace-5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|----------------|----------------|----------|--------|--|
| 1 | 12:39:52,896793 | 192.168.1.102 | 192.168.1.104 | SNMP | 92 | get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |
| 2 | 12:39:52,913753 | 192.168.1.104 | 192.168.1.102 | SNMP | 93 | get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |
| 3 | 12:39:55,382679 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 4335 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 4 | 12:39:55,402929 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 5 | 12:39:55,402959 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 4335 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=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: 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 ..a....tO6#...E.
0010 00 4e 02 fd 00 00 00 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 00 15 06 11 2b 06 01 04 01 0b 02 ..0.0..+.....
0050 03 09 04 02 01 02 02 02 01 00 05 06
.....

Payload (udp.payload), 50 byte(s) Packets: 73 · Displayed: 73 (100.0%) Profile: Default

http-ethereal-trace-5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|----------------|----------------|----------|--------|--|
| 1 | 12:39:52,896793 | 192.168.1.102 | 192.168.1.104 | SNMP | 92 | get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |
| 2 | 12:39:52,913753 | 192.168.1.104 | 192.168.1.102 | SNMP | 93 | get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0 |
| 3 | 12:39:55,382679 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 4335 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 4 | 12:39:55,402929 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 5 | 12:39:55,402959 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 4335 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |

> Frame 2: 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: 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 3c c1 61 eb ed 00 00 45 00 ..tO6#..a....E.
0010 00 4f ed a2 00 00 3c 11 0c dd c0 a8 01 68 c0 a8 0.....<.....h..
0020 01 66 00 a1 10 ee 00 3b 53 f2 30 31 02 01 00 04 f.....S01...
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 fb 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
.....

Payload (udp.payload), 51 byte(s) Packets: 73 · Displayed: 73 (100.0%) Profile: Default