

Project 3

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.

Sol: The UDP header contains 4 fields: source port, destination port, length, and checksum.

```
> 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]
```

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.

Sol: The length of each UDP header field is 2 bytes. The UDP header has a fixed length of 8 bytes

```
> 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 (4334), Dst Port: 161 (161)
  Source Port: 4334
  Destination Port: 161
  Length: 58
  > Checksum: 0x65f8 [validation disabled]
  [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.... t06#..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

```

> 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 (4334), Dst Port: 161 (161)
  Source Port: 4334
  Destination Port: 161
  Length: 58
  > Checksum: 0x65f8 [validation disabled]
    [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.... t06#..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

```

> 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 (4334), Dst Port: 161 (161)
  Source Port: 4334
  Destination Port: 161
  Length: 58
  > Checksum: 0x65f8 [validation disabled]
    [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.... t06#..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

```

> 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 (4334), Dst Port: 161 (161)
  Source Port: 4334
  Destination Port: 161
  Length: 58
  > Checksum: 0x65f8 [validation disabled]
    [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.... t06#..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.....: e00....
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_html_chunked/ChAdvChecksums.html (udp.checksum), 2 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.

Sol: The length field specifies the number of bytes in the UDP segment (header plus data). So the length is 58 (50 (data length in bytes) + 8 (header fields length in bytes)).

```

> 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 (4334), Dst Port: 161 (161)
  Source Port: 4334
  Destination Port: 161
  Length: 58
  > Checksum: 0x65f8 [validation disabled]
    [Stream index: 0]
  > Simple Network Management Protocol

```

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)

Sol. The maximum number of bytes that can be included in a UDP payload is $(2_{16} - 1) - 8$. This gives $65535 - 8 = 65527$ bytes. 8 is the UDP header field length.

5. What is the largest possible source port number?

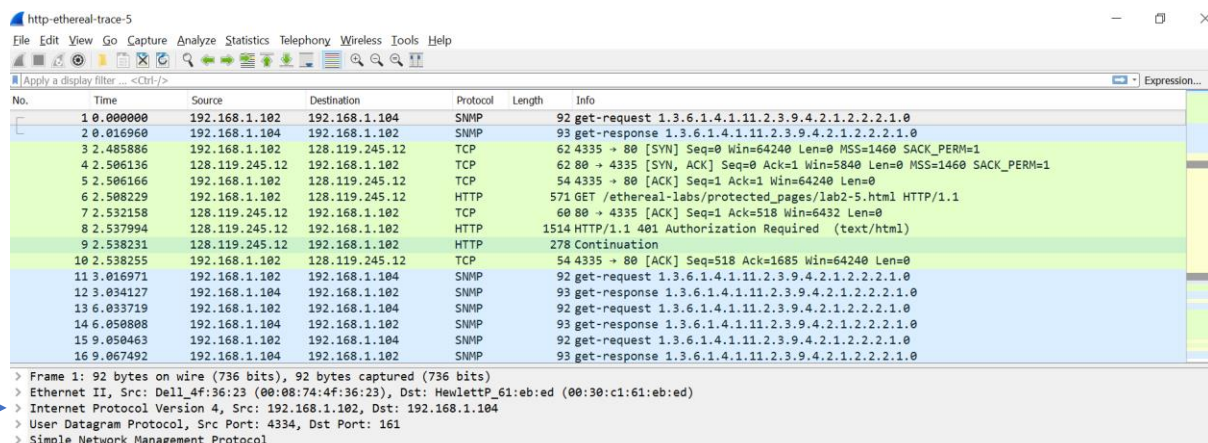
Sol: The largest possible source port number is $2_{16} - 1 = 65535$

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 (see Figure 4.13 in the text, and the discussion of IP header fields).

Sol: The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

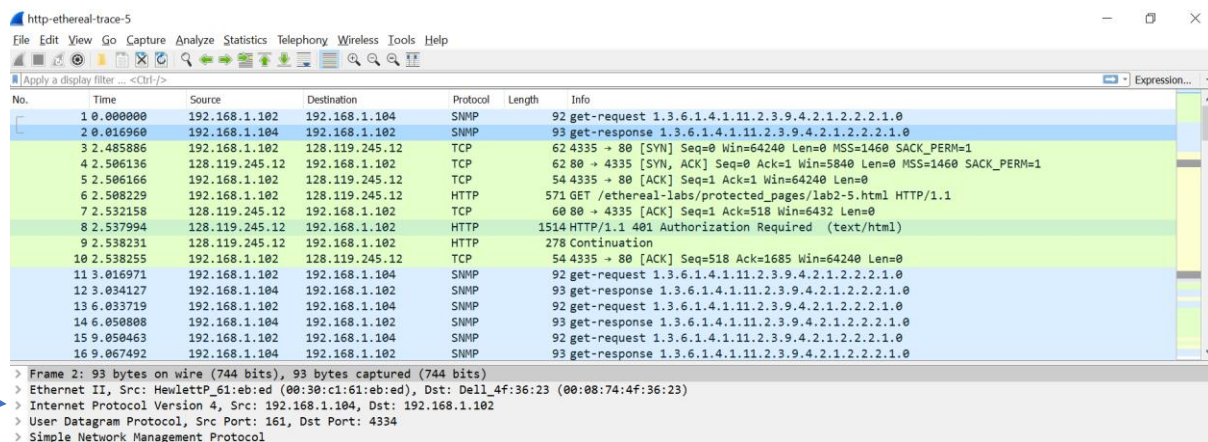
7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

Sol: The source port of the UDP packet sent by the host is the same as the destination port of the reply packet and the second UDP packet has the source port number and the destination port number as reverse of the first packet.



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
3	2.485886	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	2.506136	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	2.506166	192.168.1.102	128.119.245.12	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	2.508229	192.168.1.102	128.119.245.12	HTTP	571	GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
7	2.532158	128.119.245.12	192.168.1.102	TCP	60	80 → 4335 [ACK] Seq=1 Ack=518 Win=6432 Len=0
8	2.537994	128.119.245.12	192.168.1.102	HTTP	1514	HTTP/1.1 401 Authorization Required (text/html)
9	2.538231	128.119.245.12	192.168.1.102	HTTP	278	Continuation
10	2.538255	192.168.1.102	128.119.245.12	TCP	54	4335 → 80 [ACK] Seq=518 Ack=1685 Win=64240 Len=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

> 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
 > Simple Network Management Protocol



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
3	2.485886	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	2.506136	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	2.506166	192.168.1.102	128.119.245.12	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	2.508229	192.168.1.102	128.119.245.12	HTTP	571	GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
7	2.532158	128.119.245.12	192.168.1.102	TCP	60	80 → 4335 [ACK] Seq=1 Ack=518 Win=6432 Len=0
8	2.537994	128.119.245.12	192.168.1.102	HTTP	1514	HTTP/1.1 401 Authorization Required (text/html)
9	2.538231	128.119.245.12	192.168.1.102	HTTP	278	Continuation
10	2.538255	192.168.1.102	128.119.245.12	TCP	54	4335 → 80 [ACK] Seq=518 Ack=1685 Win=64240 Len=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

> 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
 > Simple Network Management Protocol

Reference Note: All the above observations has been performed considering the “http-ethereal-trace-5” file from the zip file reference (<http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>) provided in the project information document.