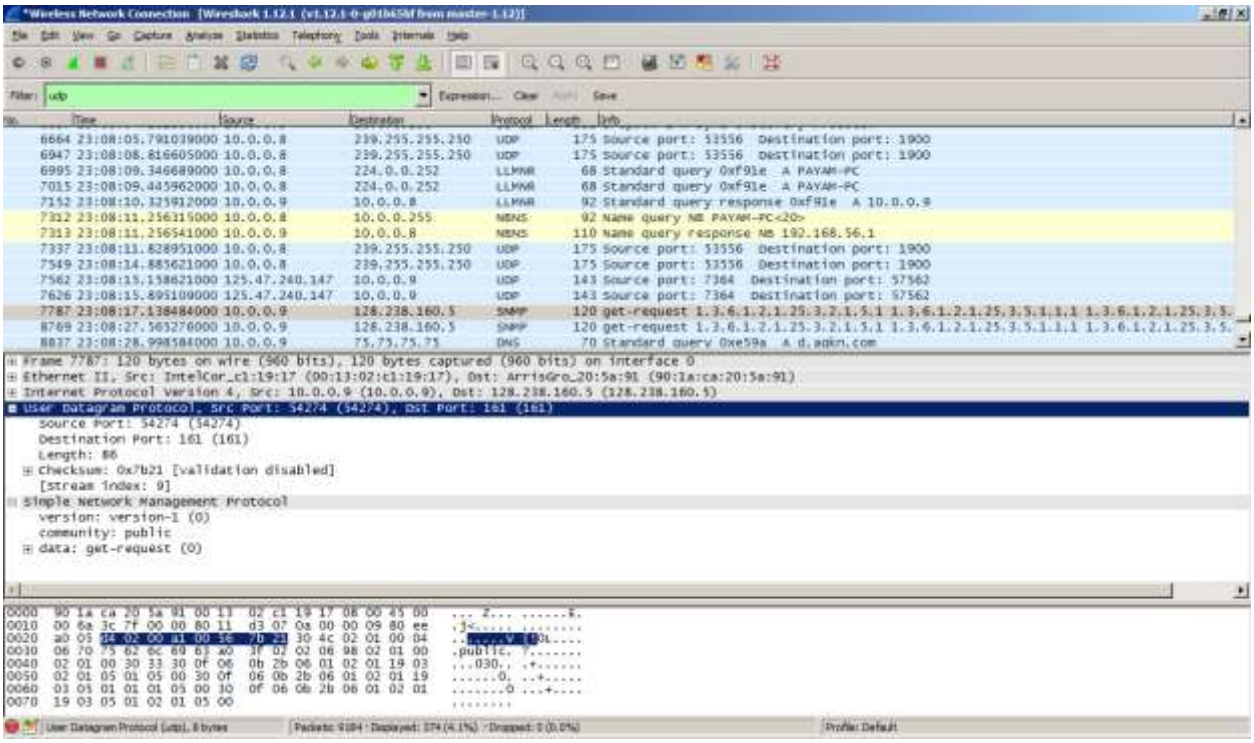
# WireShark Lab – UDP

Payam Rastogi
(pr1228@nyu.edu)

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



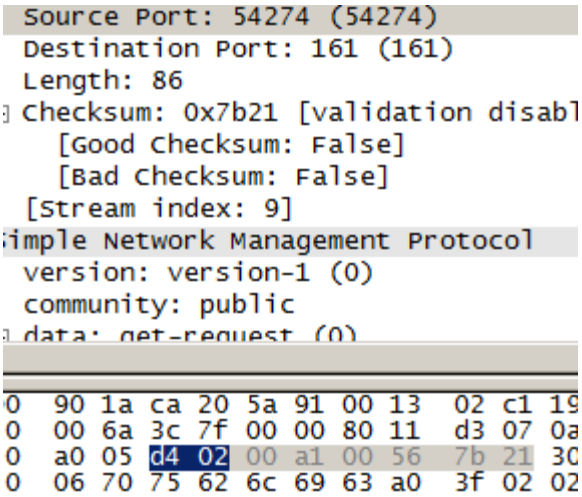

**Answer 1:** There are 4 fields in UDP header.

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.

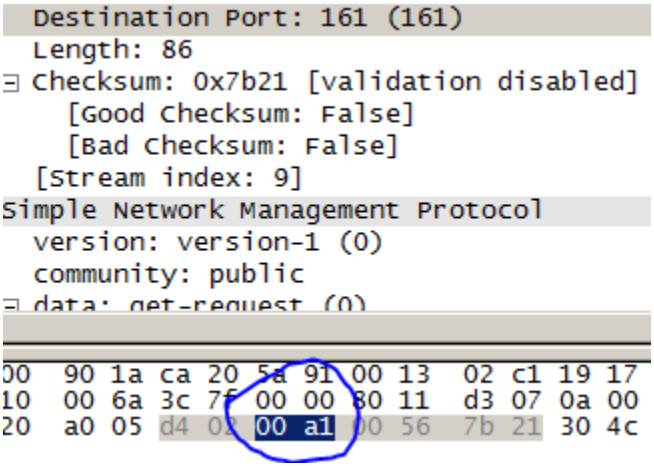
**Answer 2:** Total header length 8 bytes (each field is 2 bytes)

- Source port : 16 bit or 2 bytes

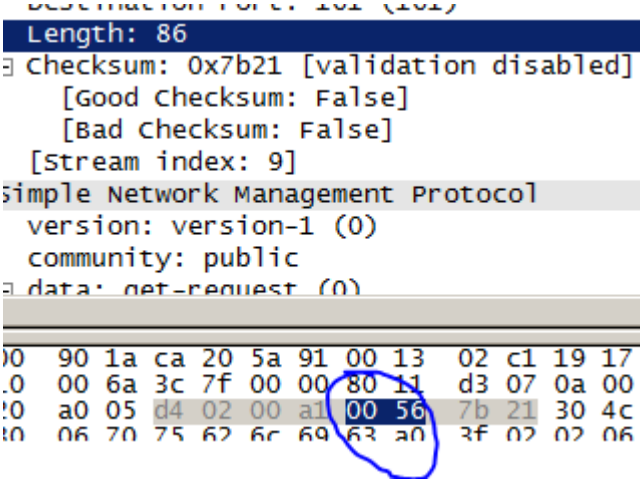


Payam Rastogi
(pr1228@nyu.edu)

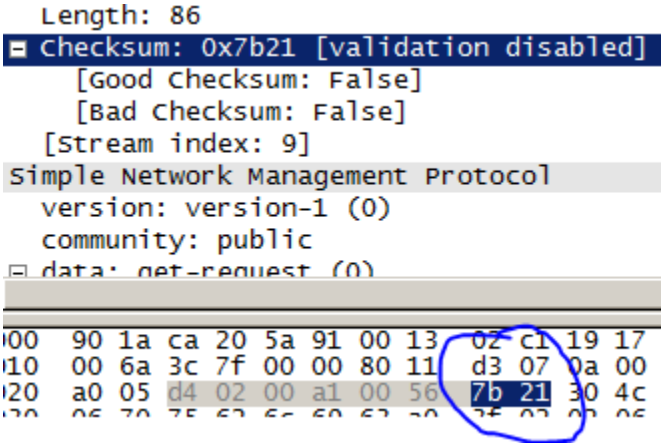
- Destination port : 16 bit or 2 bytes




- Length: 16 bit or 2 bytes

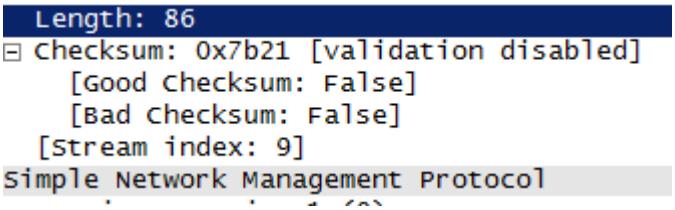



- Checksum: 16 bit or 2 bytes



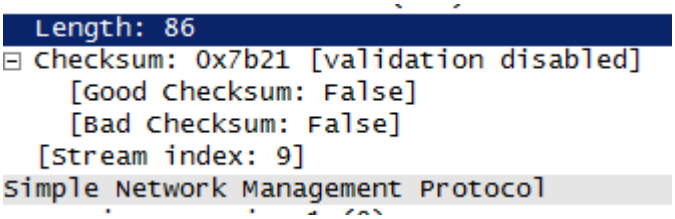
Payam Rastogi
(pr1228@nyu.edu)

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.



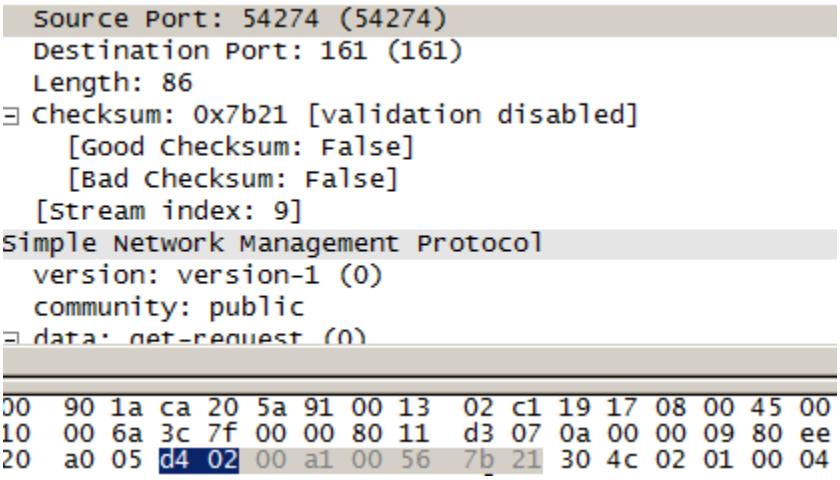

**Answer 3**: A length specifies the length in bytes of the UDP header and UDP data

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 4**: The field size sets a theoretical limit of 65,535 bytes (8 byte header + 65,527 bytes of data) for a UDP datagram (as length of "length field is 16 bit hence total $2^{16}$ bytes can be identified). Hence the theoretical UDP payload limit is 65527 bytes.

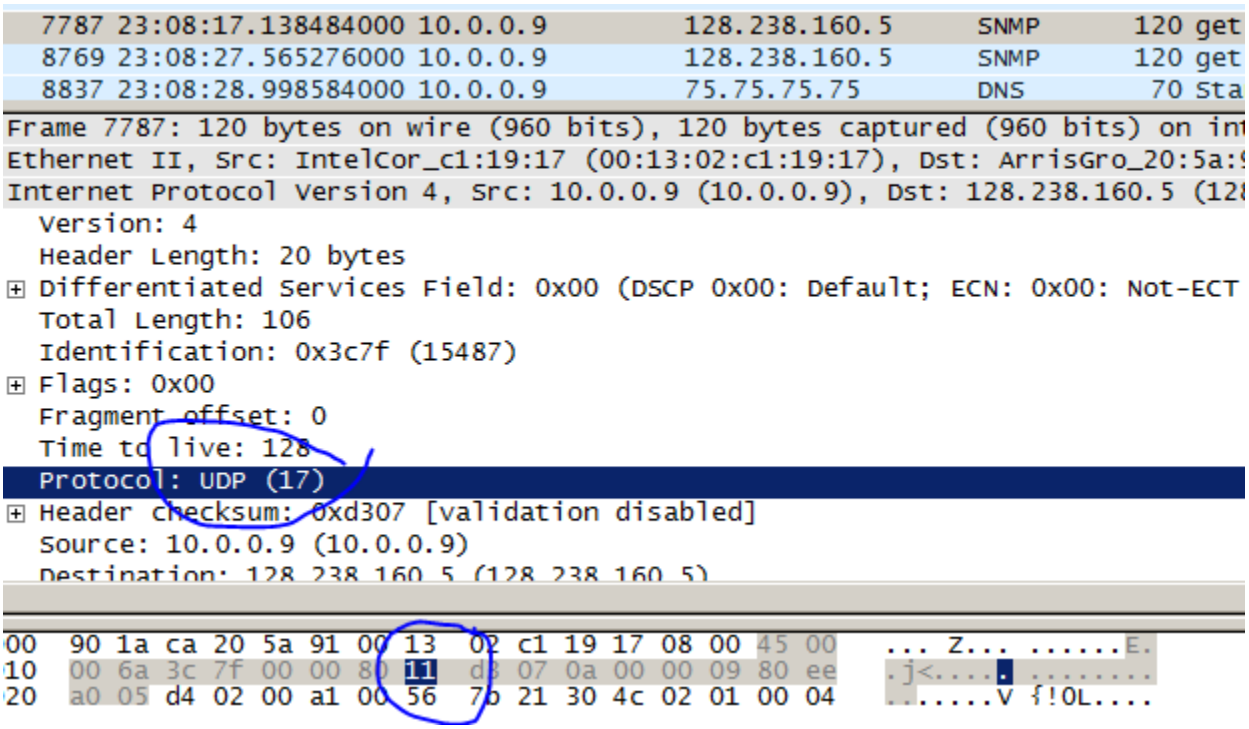
5. What is the largest possible source port number? (Hint: see the hint in 4.)




**Answer 5:** a 16 bit integer value, allowing for port numbers between 0 and 65535
Hence the largest port number is 65535.

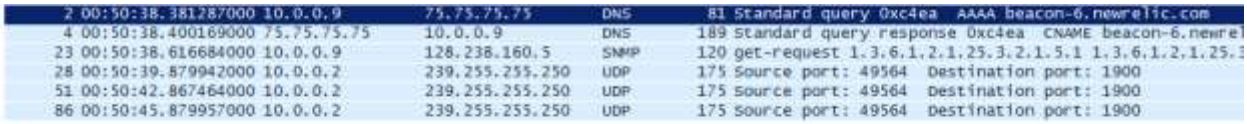
Payam Rastogi
(pr1228@nyu.edu)

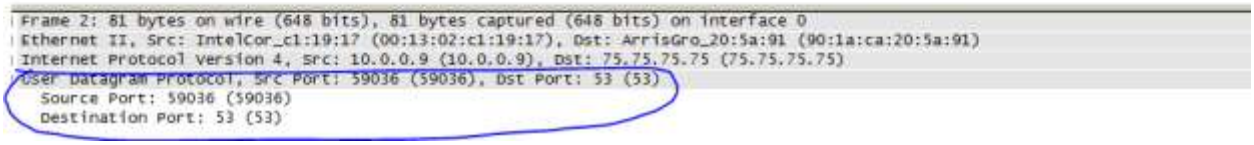
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).




**Answer 6:** Protocol number for UDP is 17 (hexadecimal: 11)

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.



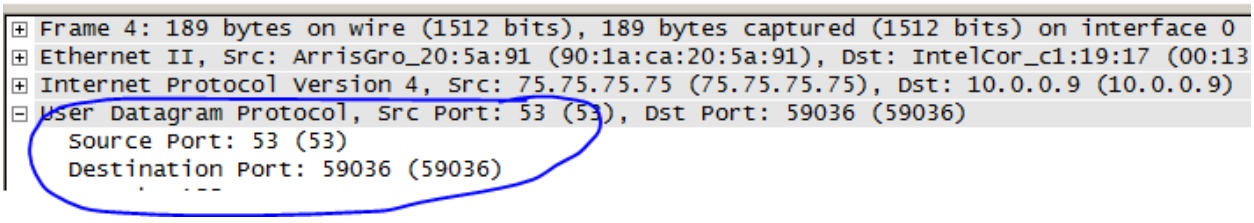




**Answer 7:** In UDP packet from 10.0.0.9 -> 75.75.75.75
**Source port:** 59036
**Destination port:** 53

# WireShark Lab – UDP

Payam Rastogi
(pr1228@nyu.edu)

| | | | | | |
|---|---|---|---|---|---|
| 2 | 00:50:38.381287000 | 10.0.0.9 | 75.75.75.75 | DNS | 81 Standard que |
| 4 | 00:50:38.400169000 | 75.75.75.75 | 10.0.0.9 | DNS | 189 Standard que |
| 23 | 00:50:38.616684000 | 10.0.0.9 | 128.238.160.5 | SNMP | 120 get-request |
| 28 | 00:50:39.879942000 | 10.0.0.2 | 239.255.255.250 | UDP | 175 Source port: |
| 51 | 00:50:42.867464000 | 10.0.0.2 | 239.255.255.250 | UDP | 175 Source port: |
| 86 | 00:50:45.879957000 | 10.0.0.2 | 239.255.255.250 | UDP | 175 Source port: |




In UDP Packet from 75.75.75.75 -> 10.0.0.9

**Source Port: 53**

**Destination Port: 59036**

The source port no. in the UDP packet from the client to server becomes destination port no. in the UDP packet from server to client.