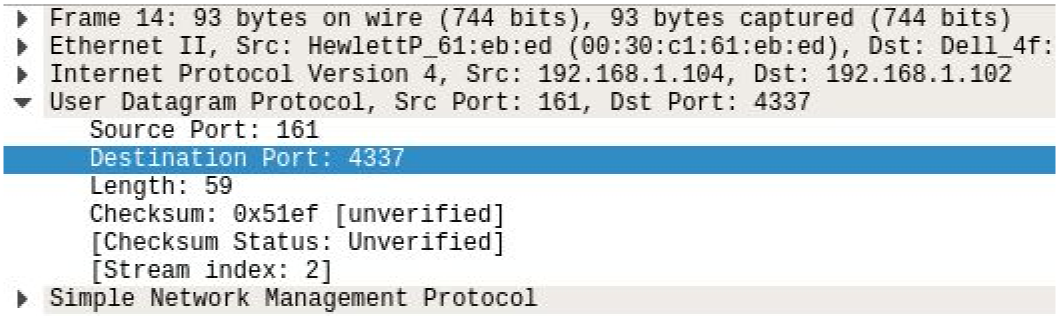
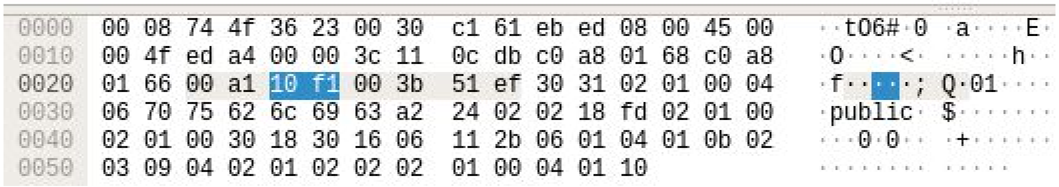
Lyndon Renaud
104 566 776
Computer Networks
Lab 2 TCP

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.**
   The fields in the UDP header are: Source Port, Destination Port, Length, and 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.**
   Each of the UDP header fields are two bytes long.



```
▶ Frame 14: 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:
▶ Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
▼ User Datagram Protocol, Src Port: 161, Dst Port: 4337
      Source Port: 161
      Destination Port: 4337
      Length: 59
      Checksum: 0x51ef [unverified]
      [Checksum Status: Unverified]
      [Stream index: 2]
▶ Simple Network Management Protocol
```



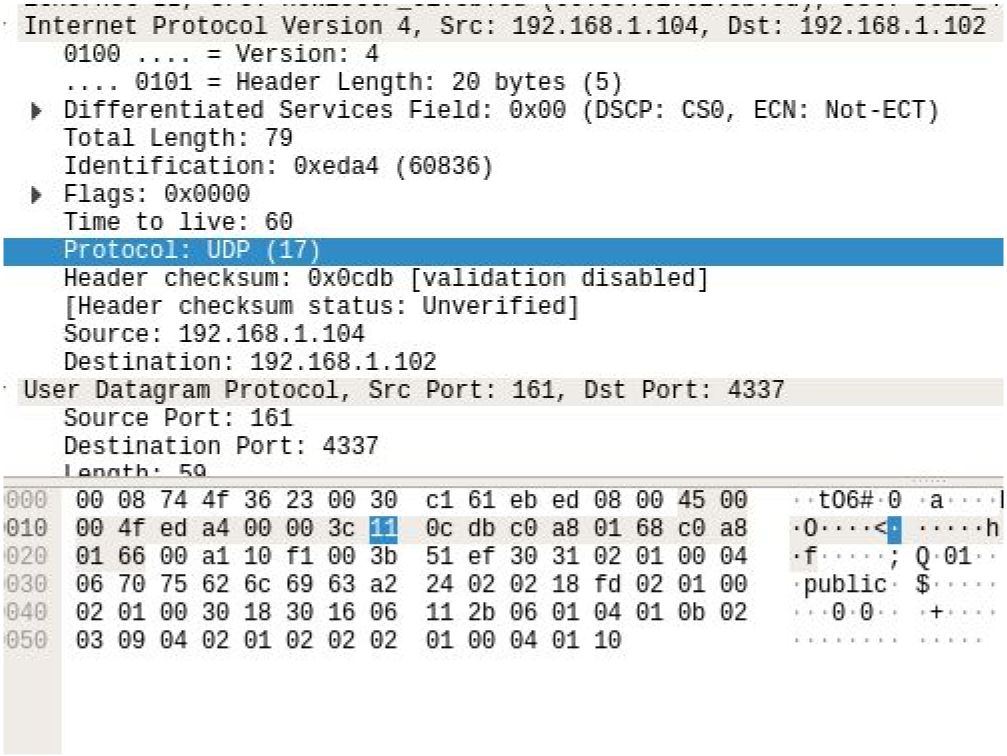
```
0000  00 08 74 4f 36 23 00 30  c1 61 eb ed 08 00 45 00   ··tO6#·0 ·a····E·
0010  00 4f ed a4 00 00 3c 11  0c db c0 a8 01 68 c0 a8   ·O····<· ·····h··
0020  01 66 00 a1 10 f1 00 3b  51 ef 30 31 02 01 00 04   ·f·····; Q·01····
0030  06 70 75 62 6c 69 63 a2  24 02 02 18 fd 02 01 00   ·public· $·······
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            ········ ·····
```

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.**
   The value in the length field is the sum of the UDP header fields in bytes + the amount of bytes in the SNMP header. In the above photo, the UDP header bytes are highlighted in a light grey. These bytes + the rest of the bytes following them equal to 59, which is the length of the packet.

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)**
   The maximum number of bytes that can be included in a UDP payload can be found by subtracting the UDP header size from the maximum length of a packet (2^16). This is 65 536 - 8 = 65 528.
5. **What is the largest possible source port number? (Hint: see the hint in 4.)**
   Since there can only be two bytes for the length, it has a max value of 2^16 or 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).**

   The IPv4 header flag 'protocol' shows UDP is using port 17. This is 11h as shown in the packet content field.



```
· Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0xeda4 (60836)
  ▶ Flags: 0x0000
    Time to live: 60
    Protocol: UDP (17)
    Header checksum: 0x0cdb [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.104
    Destination: 192.168.1.102
· User Datagram Protocol, Src Port: 161, Dst Port: 4337
    Source Port: 161
    Destination Port: 4337
    Length: 59

000  00 08 74 4f 36 23 00 30  c1 61 eb ed 08 00 45 00   ··tO6#·0 ·a····
010  00 4f ed a4 00 00 3c 11  0c db c0 a8 01 68 c0 a8   ·O····<· ·····h
020  01 66 00 a1 10 f1 00 3b  51 ef 30 31 02 01 00 04   ·f·····; Q·01··
030  06 70 75 62 6c 69 63 a2  24 02 02 18 fd 02 01 00   ·public· $······
040  02 01 00 30 18 30 16 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
050  03 09 04 02 01 02 02 02  01 00 04 01 10            ········ ·····
```

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.**

   Host A is sending a packet through port 161 and host B is receiving it at port 4338. In the next frame, Host B is sending a packet through port 161 and host A is receiving it at port 4338. These two hosts both send udp packets through the same port, and receive udp packets through the same port.