src.html

Wireshark Lab: UDP

Nome:

Vinícius Gonzaga Rocha

Matrícula:

11511BCC019

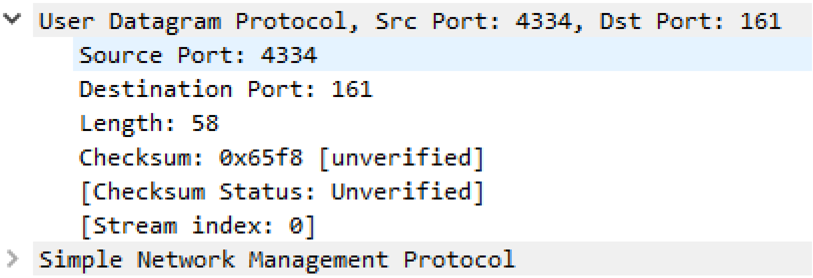
Descrição:

Atividade realizada para o aprofundamento do conhecimento do protocolo UDP.

---

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.

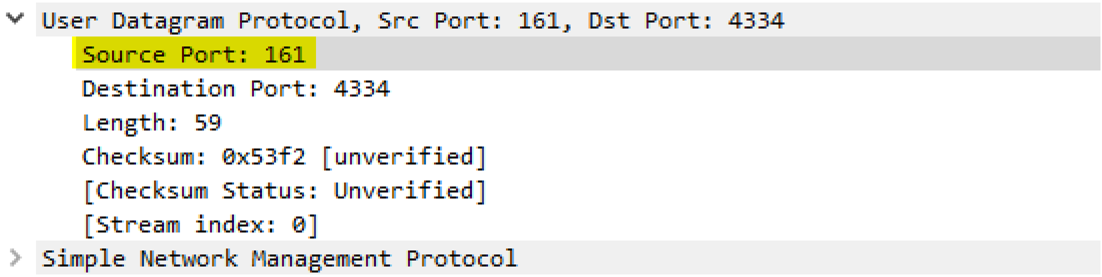
São 4 campos, conforme imagem: Source Port, Destination Port, Length, Checksum.



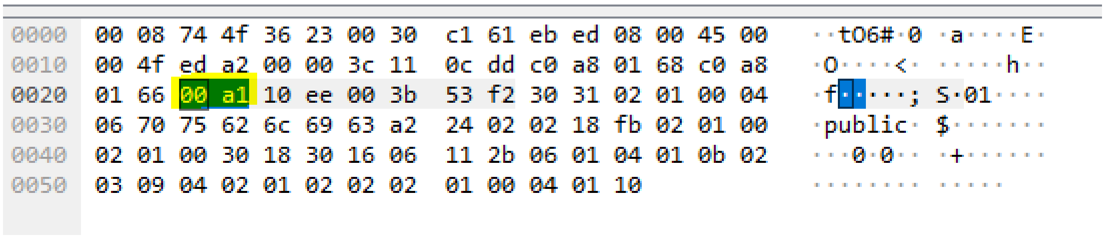
```
v User Datagram Protocol, Src Port: 4334, Dst Port: 161
     Source Port: 4334
     Destination Port: 161
     Length: 58
     Checksum: 0x65f8 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
> Simple Network Management Protocol
```

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.

2 bytes



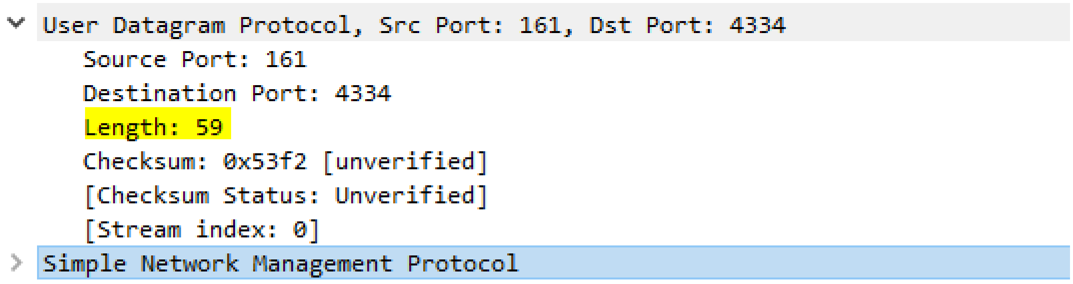
```
v User Datagram Protocol, Src Port: 161, Dst Port: 4334
      Source Port: 161
      Destination Port: 4334
      Length: 59
      Checksum: 0x53f2 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
> Simple Network Management Protocol
```



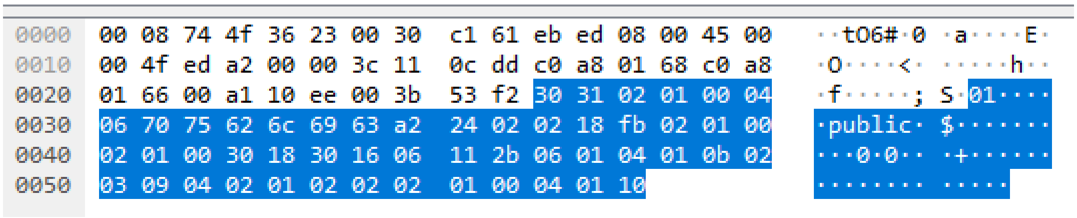
```
0000  00 08 74 4f 36 23 00 30  c1 61 eb ed 08 00 45 00   ··tO6#·0 ·a····E·
0010  00 4f ed a2 00 00 3c 11  0c dd c0 a8 01 68 c0 a8   ·O····<· ·····h··
0020  01 66 00 a1 10 ee 00 3b  53 f2 30 31 02 01 00 04   ·f·····; S·01····
0030  06 70 75 62 6c 69 63 a2  24 02 02 18 fb 02 01 00   ·public· $·······
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            ········ ·····
```

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.

É o comprimento da mensagem carregada pelo pacote UDP + o cabeçalho.



```
v 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: 0]
> 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 a2 00 00 3c 11  0c dd c0 a8 01 68 c0 a8   ·O····<· ·····h··
0020  01 66 00 a1 10 ee 00 3b  53 f2 30 31 02 01 00 04   ·f·····; S·01····
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            ········ ·····
```

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)

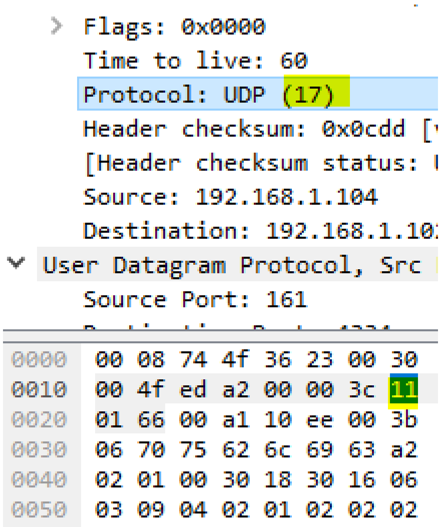
65535 bytes, pois esse é o meior numero que pode ser representado por 2 bytes hexadecimais.

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

65535 bytes, pois esse é o meior numero que pode ser representado por 2 bytes hexadecimais.

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).

Decimal	Hexadeciaml
17	11

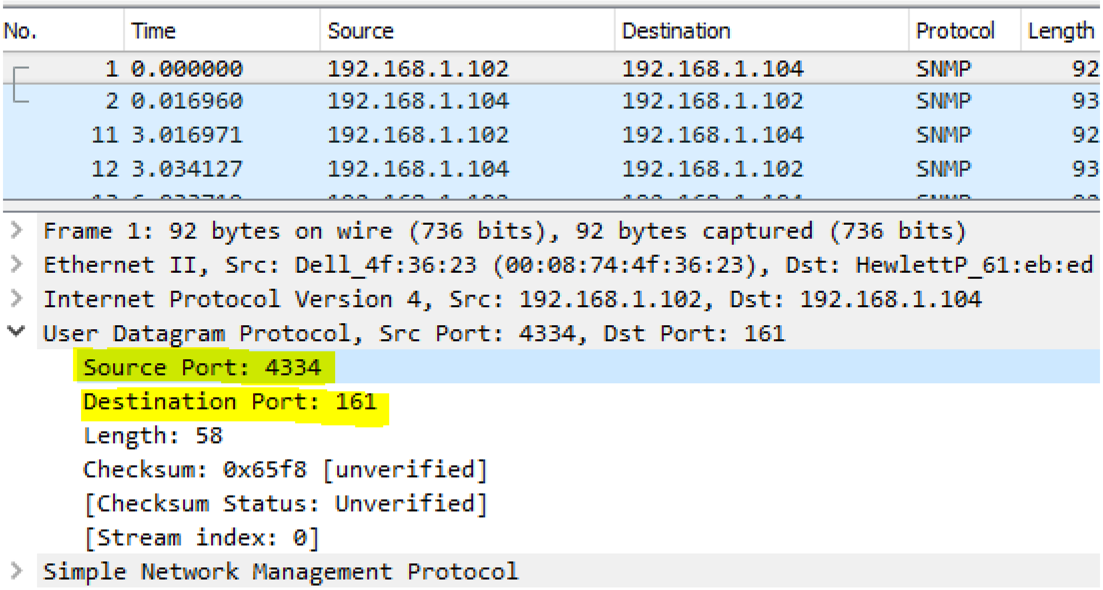


```
  > Flags: 0x0000
    Time to live: 60
    Protocol: UDP (17)
    Header checksum: 0x0cdd [
    [Header checksum status:
    Source: 192.168.1.104
    Destination: 192.168.1.10
v User Datagram Protocol, Src
    Source Port: 161
```

```
0000  00 08 74 4f 36 23 00 30
0010  00 4f ed a2 00 00 3c 11
0020  01 66 00 a1 10 ee 00 3b
0030  06 70 75 62 6c 69 63 a2
0040  02 01 00 30 18 30 16 06
0050  03 09 04 02 01 02 02 02
```

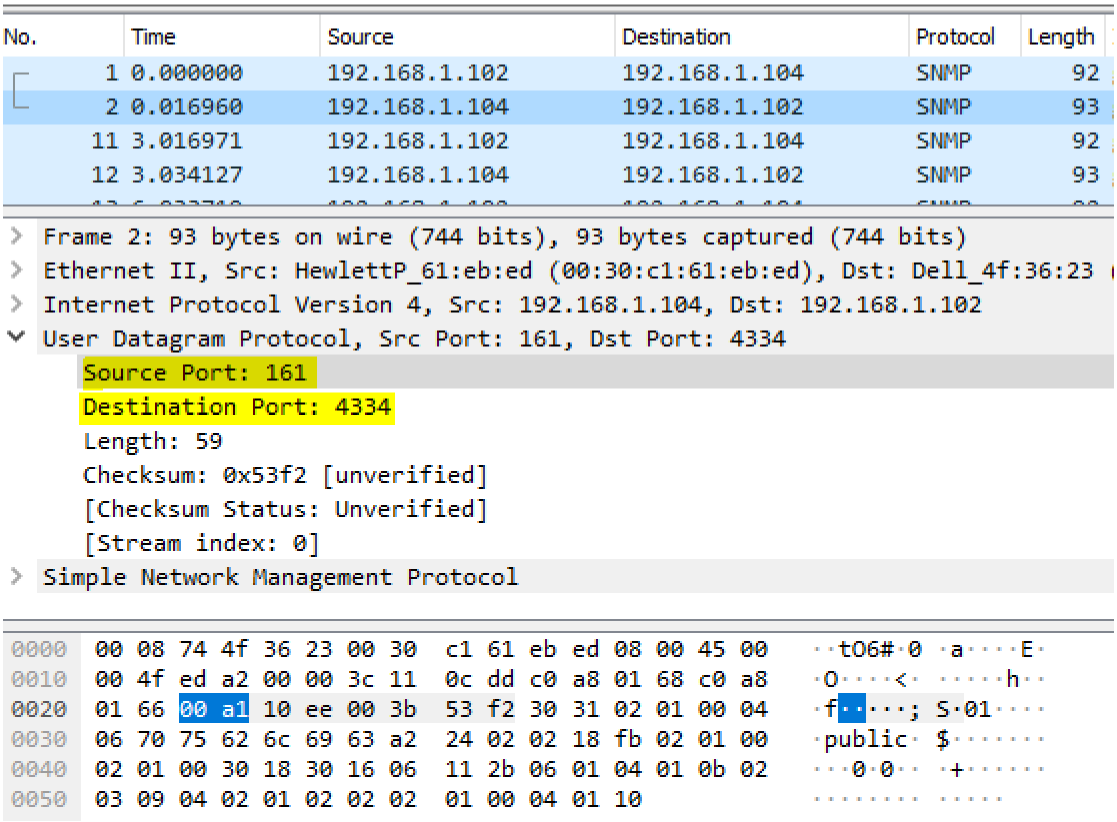
7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the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

Podemos observar que a porta de destino no primeiro pacote passa a ser a porta fonte no pacote de resposta. Essa inversão também ocorre com a porta fonte do primeiro pacote, que passou a ser a porta de destino na resposta.



```
No.     Time        Source          Destination     Protocol  Length
      1 0.000000    192.168.1.102   192.168.1.104   SNMP          92
      2 0.016960    192.168.1.104   192.168.1.102   SNMP          93
     11 3.016971    192.168.1.102   192.168.1.104   SNMP          92
     12 3.034127    192.168.1.104   192.168.1.102   SNMP          93

> 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
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
v 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]
> Simple Network Management Protocol
```



```
No.     Time        Source          Destination     Protocol  Length
      1 0.000000    192.168.1.102   192.168.1.104   SNMP          92
      2 0.016960    192.168.1.104   192.168.1.102   SNMP          93
     11 3.016971    192.168.1.102   192.168.1.104   SNMP          92
     12 3.034127    192.168.1.104   192.168.1.102   SNMP          93

> 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
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
v 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: 0]
> 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 a2 00 00 3c 11  0c dd c0 a8 01 68 c0 a8   ·O····<· ·····h··
0020  01 66 00 a1 10 ee 00 3b  53 f2 30 31 02 01 00 04   ·f·····; S·01····
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            ········ ·····
```