

21CY682- IP LAB ASSIGNMENT 4

Analysing TCP and UDP using Wireshark

Name:Ramya Ajay

RollNo:CB.EN.P2CYS22004

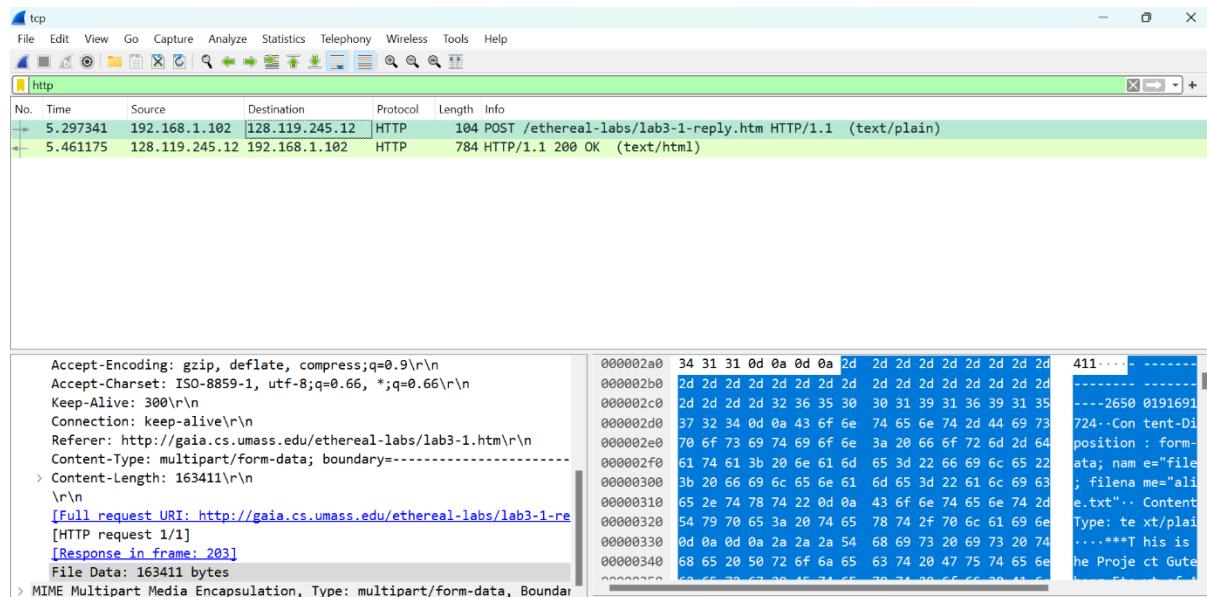
Date:29-10-2022

AIM:Analyze TCP and UDP using wireshark

Tools:Wireshark

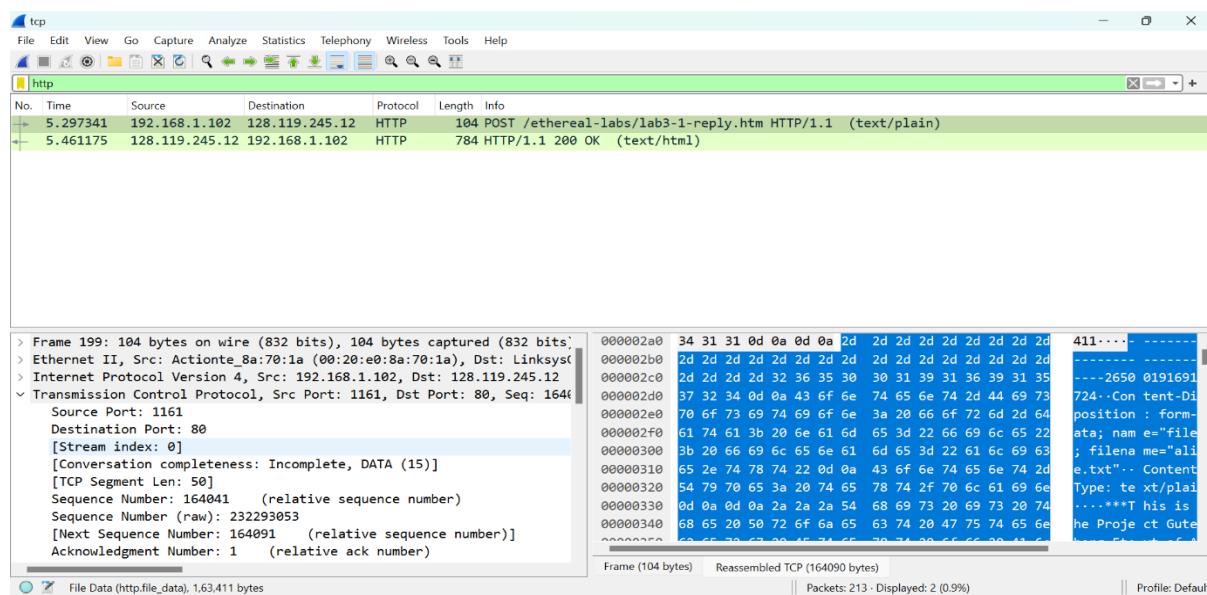
TCP

1 a)IP Addresss:192.168.1.103, source port:1161



b)IP Address:128.119.245.12

Destination Port:80



c)Sequence Number:0

[SYN] -0x002

The Wireshark interface shows a list of network packets. The first packet is highlighted in green and has the following details:

- No. 1. Time 0.000000
- Source 192.168.1.102
- Destination 128.119.245.12
- Protocol TCP
- Length 62
- Info [SYN] Seq=0 Win=16384

The packet bytes pane shows the raw hex and ASCII data for this SYN packet.

Packet Details:

- Sequence Number (raw): 232129012
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 0111 = Header Length: 28 bytes (7)
- > Flags: 0x002 (SYN)
- Window: 16384
- [Calculated window size: 16384]
- Checksum: 0xf6e9 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- > Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Op
- > [Timestamps]

d)Sequence Number:0 and Acknowledgement Number:1

New acknowledgement number is the incremented value of previous sequence number.

New sequence number is the previous acknowledgment number.

[SYN,ACK]

The Wireshark interface shows a list of network packets. The second packet is highlighted in green and has the following details:

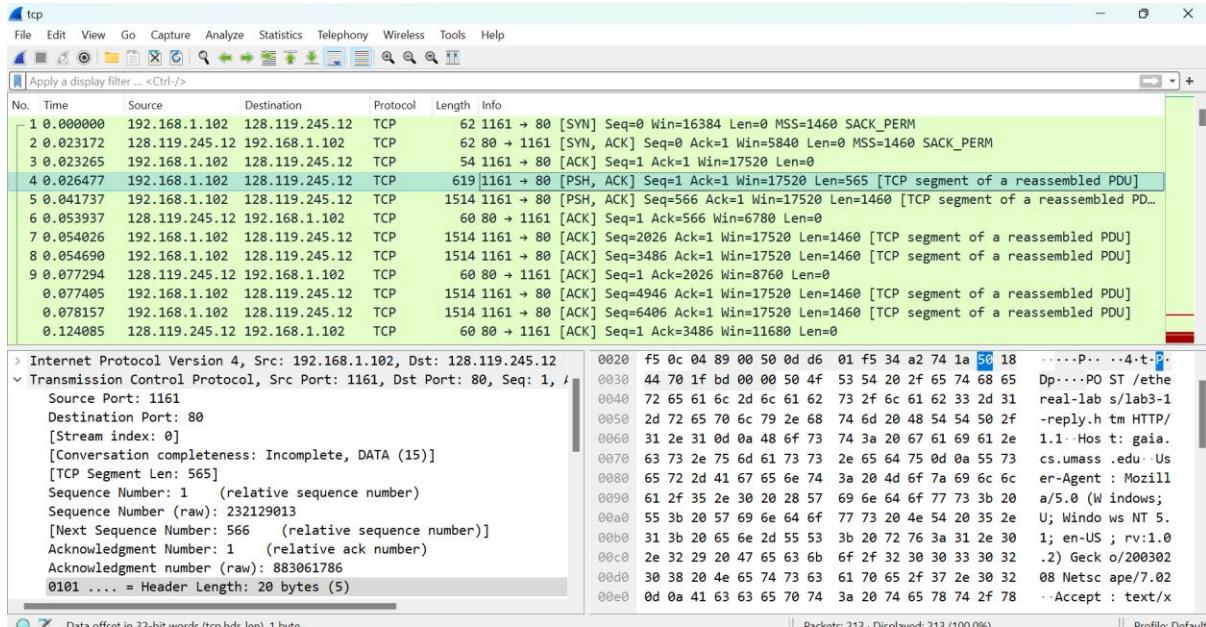
- No. 2. Time 0.023172
- Source 128.119.245.12
- Destination 192.168.1.102
- Protocol TCP
- Length 62
- Info [SYN, ACK] Seq=0 Win=5840

The packet bytes pane shows the raw hex and ASCII data for this SYN-ACK packet.

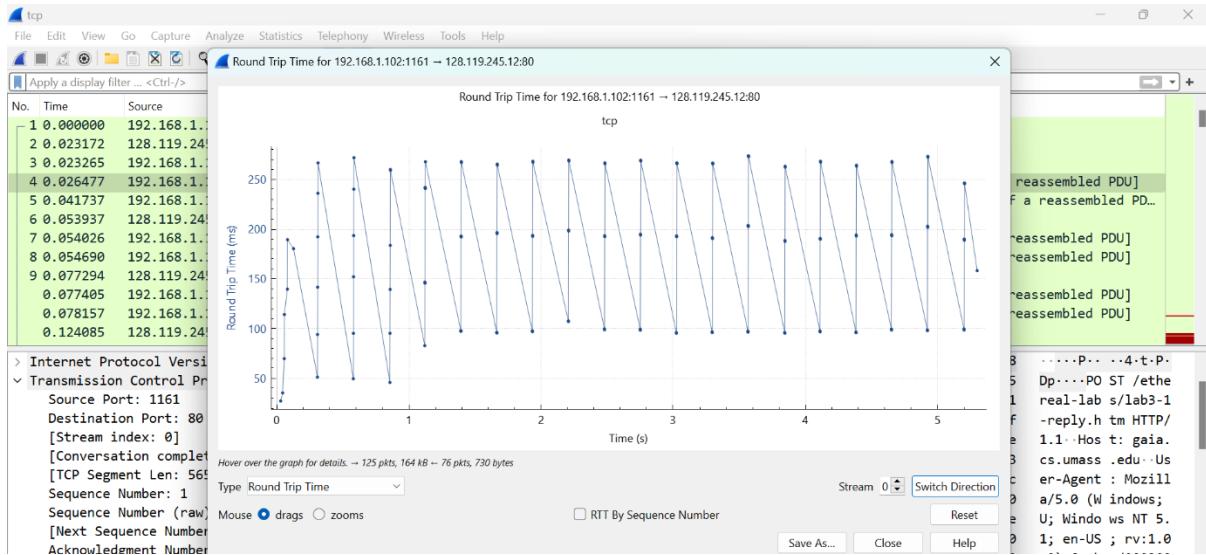
Packet Details:

- 0111 = Header Length: 28 bytes (7)
- > Flags: 0x012 (SYN, ACK)
- 000 = Reserved: Not set
- ...0 = Accurate ECN: Not set
- 0.... = Congestion Window Reduced: Not set
-0.... = ECN-Echo: Not set
-0.... = Urgent: Not set
-1.... = Acknowledgment: Set
- 0.... = Push: Not set
-0.... = Reset: Not set
- >1.... = Syn: Set
-0.... = Fin: Not set
- [TCP Flags:A..S..]

e) Sequence number is 1



f) RTTxTime Graph



g)#4- 565

#5,#7,#8,#10,#11- 1460

Total Length: 164090

The screenshot displays two separate network captures in Wireshark:

Top Capture:

- Protocol: http
- Source: 192.168.1.102
- Destination: 128.119.245.12
- Protocol: HTTP
- Length: 104 (POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain))
- Length: 784 (HTTP/1.1 200 OK (text/html))

Detailed View (Reassembled TCP Segments):

- [Frame: 4, payload: 0-564 (565 bytes)]
- [Frame: 5, payload: 565-2024 (1460 bytes)]
- [Frame: 7, payload: 2025-3484 (1460 bytes)]
- [Frame: 8, payload: 3485-4944 (1460 bytes)]
- [Frame: 10, payload: 4945-6404 (1460 bytes)]
- [Frame: 11, payload: 6405-7864 (1460 bytes)]
- [Frame: 13, payload: 7865-9011 (147 bytes)]
- [Frame: 18, payload: 9012-10471 (1460 bytes)]
- [Frame: 19, payload: 10472-11931 (1460 bytes)]
- [Frame: 20, payload: 11932-13391 (1460 bytes)]
- [Frame: 21, payload: 13392-14851 (1460 bytes)]
- [Frame: 22, payload: 14852-16311 (1460 bytes)]

Bottom Capture:

- Protocol: http
- Source: 192.168.1.102
- Destination: 128.119.245.12
- Protocol: HTTP
- Length: 104 (POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain))
- Length: 784 (HTTP/1.1 200 OK (text/html))

Detailed View (HTTP Headers):

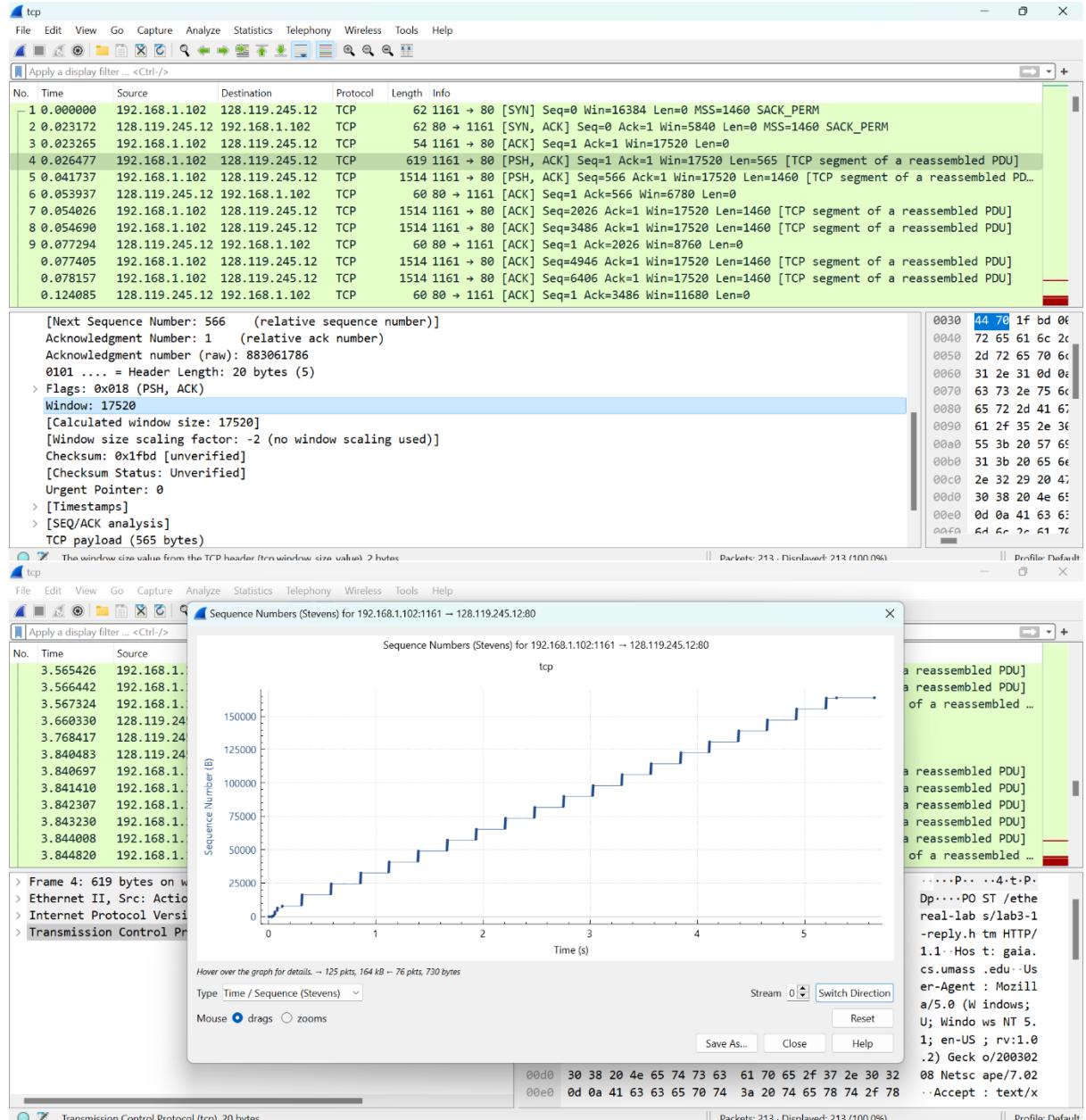
- [Frame: 193, payload: 157928-159387 (1460 bytes)]
- [Frame: 194, payload: 159388-160847 (1460 bytes)]
- [Frame: 195, payload: 160848-162307 (1460 bytes)]
- [Frame: 196, payload: 162308-163767 (1460 bytes)]
- [Frame: 197, payload: 163768-164039 (272 bytes)]
- [Frame: 199, payload: 164040-164089 (50 bytes)]

Segment count: 122
[Reassembled TCP length: 164090]
[Reassembled TCP Data: 504f5354202f657468657265616c2d6c6162732f6c6162332d312d7265706c792e68746d...]

Hypertext Transfer Protocol

- > POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1\r\n
- Host: gaiia.cs.umass.edu\r\n
- User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n

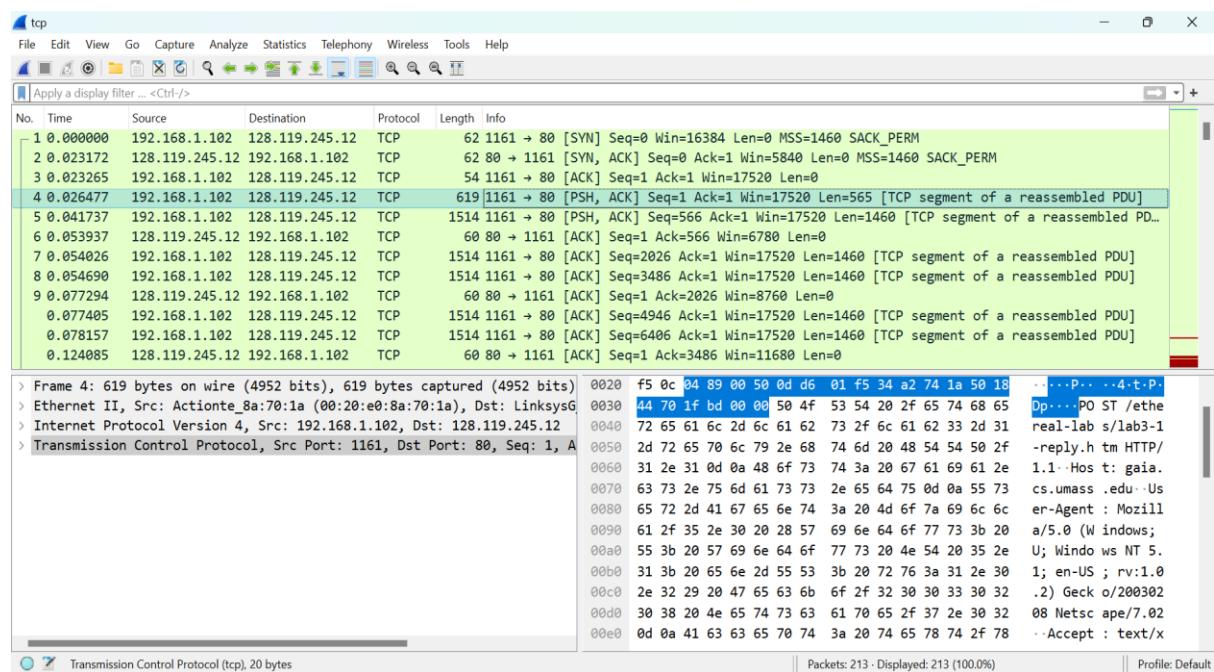
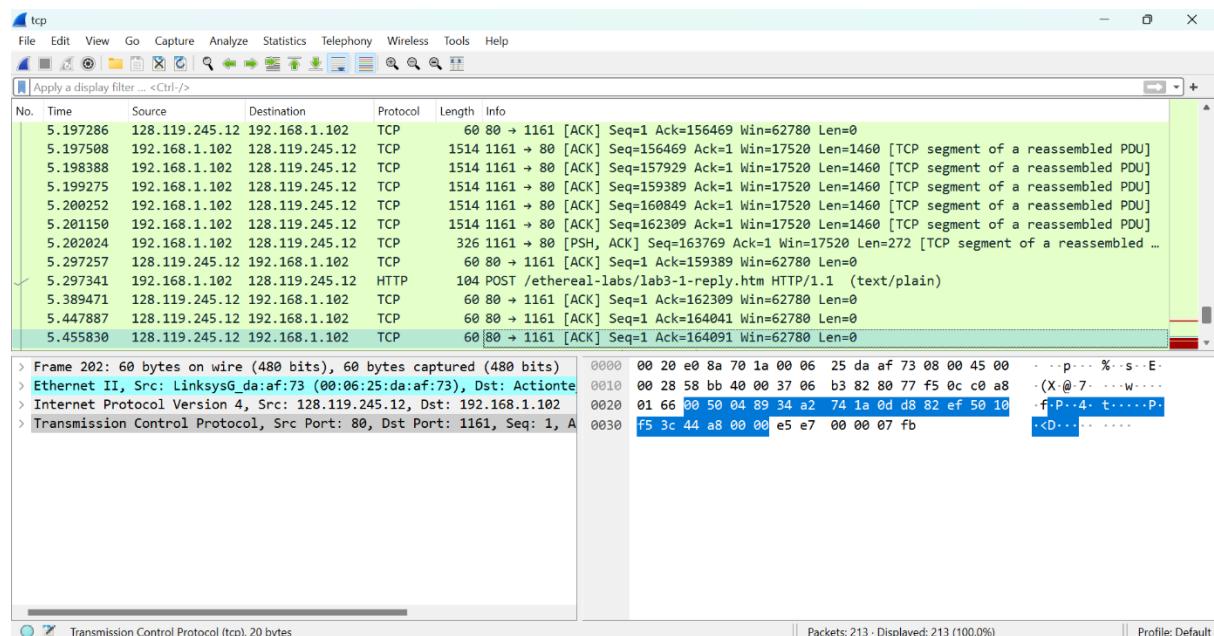
h) Data has not been transmitted since there is no drop in the Sequence Number X Time graph and no sequence number are repeated in the data.



i) throughput=No of bytes transferred/time

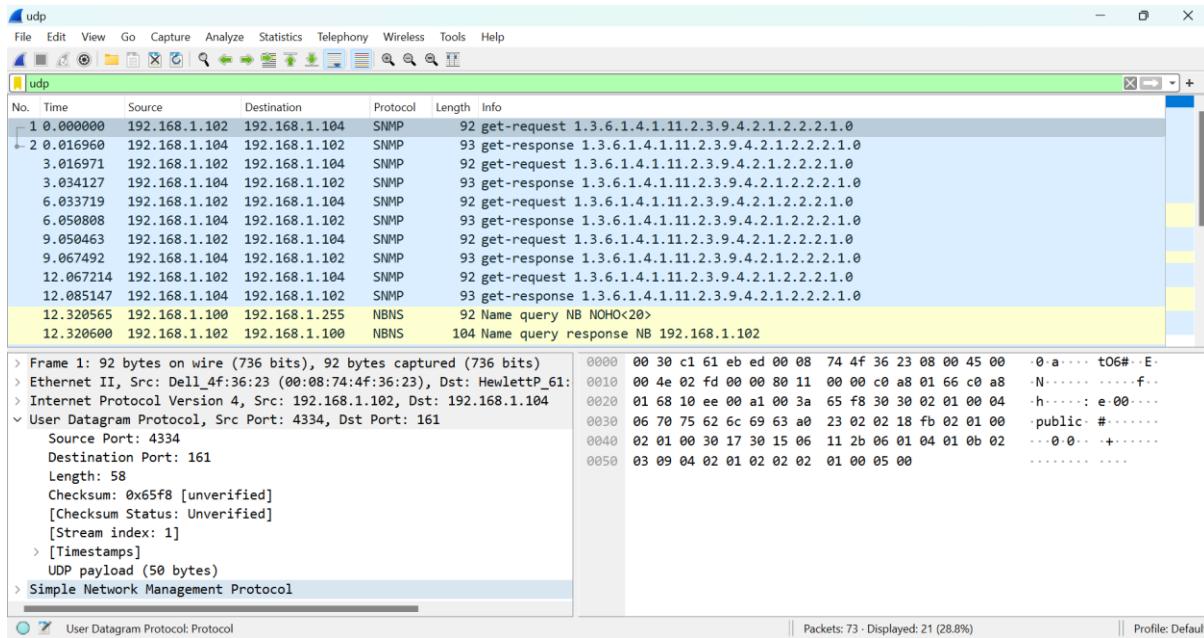
$$=[164091(\text{Final Ack})-1(\text{Initial Ack})]/[5.455(\text{Final timestamp})-0.0264(\text{Initial timestamp})]$$

$$=30,224 \text{ bytes}=30.224 \text{KB}$$

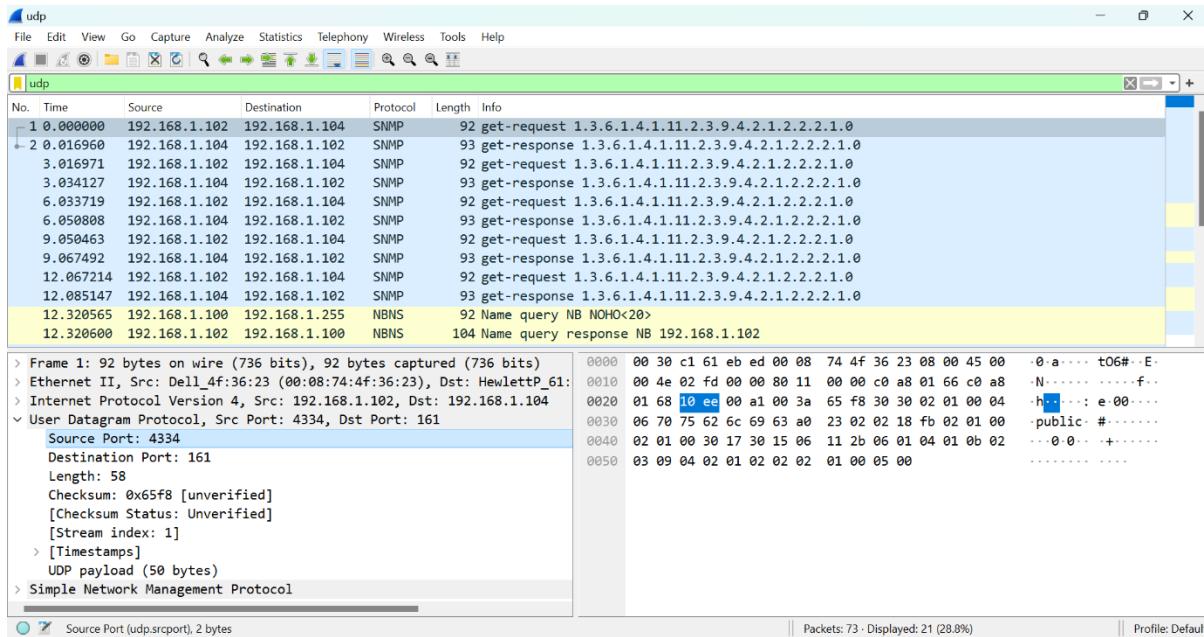


UDP

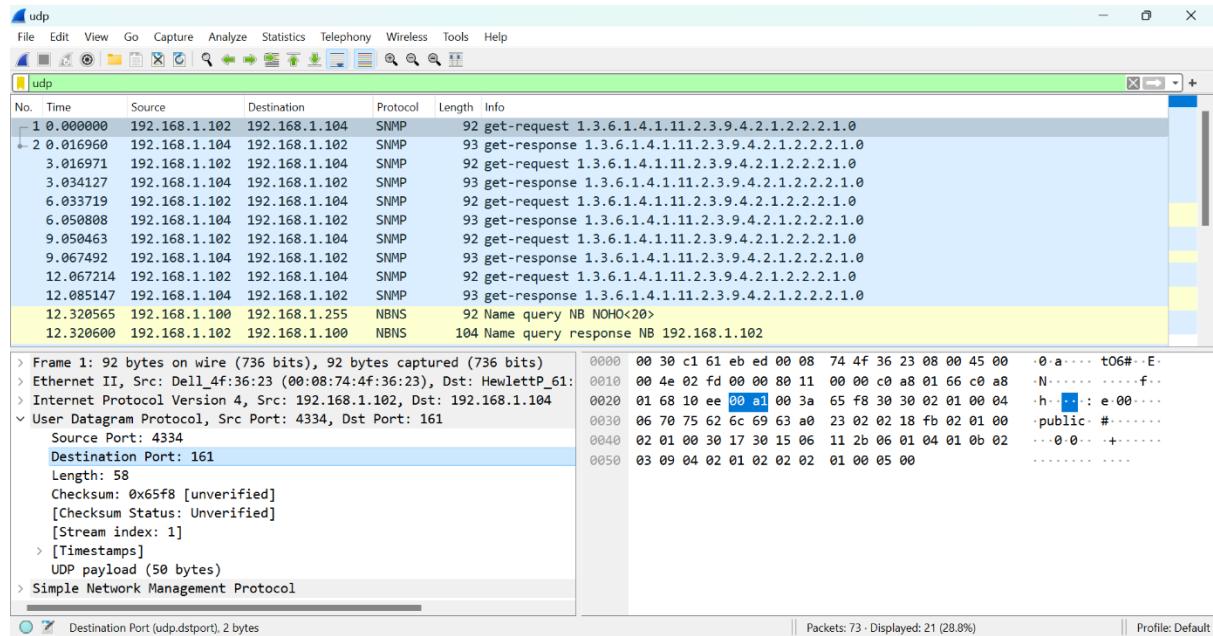
j)4 fields:Source Port, Destination Port, Checksum, Length



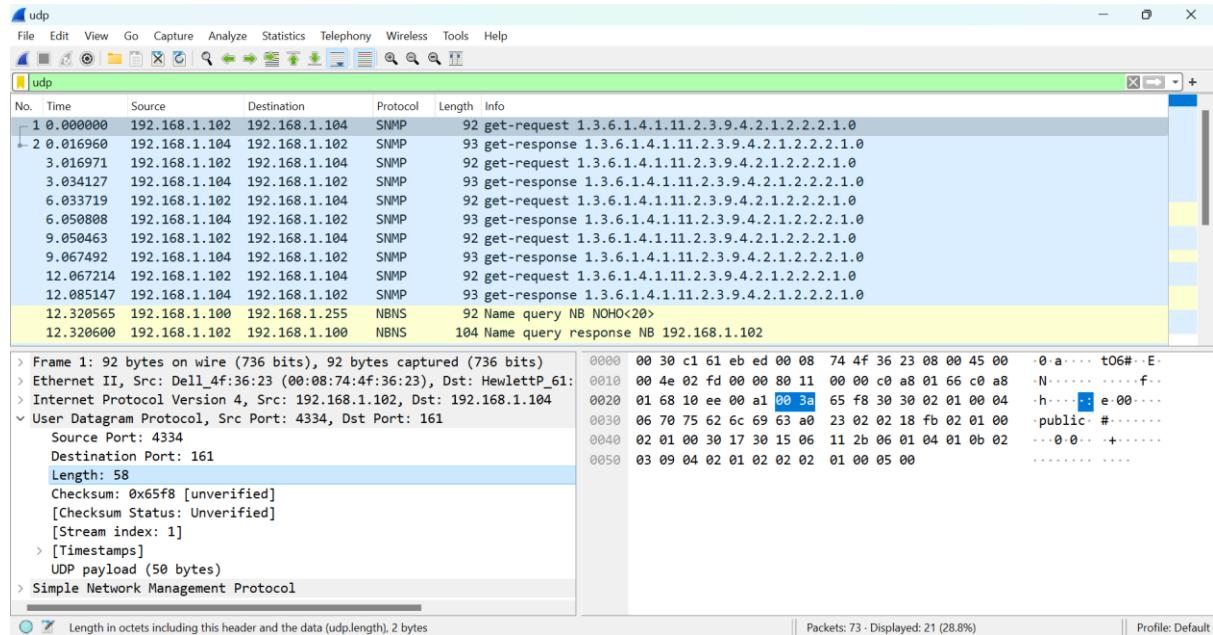
k)Source Port :2 Bytes



Destination Port:2 Bytes



Length:2 Bytes



Checksum:2 bytes

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes

Packets: 73 · Displayed: 21 (28.8%) · Profile: Default

I) Data+header = length

Header=Source port+Destination Port+Length+Checksum=2+2+2+2=8 Bytes

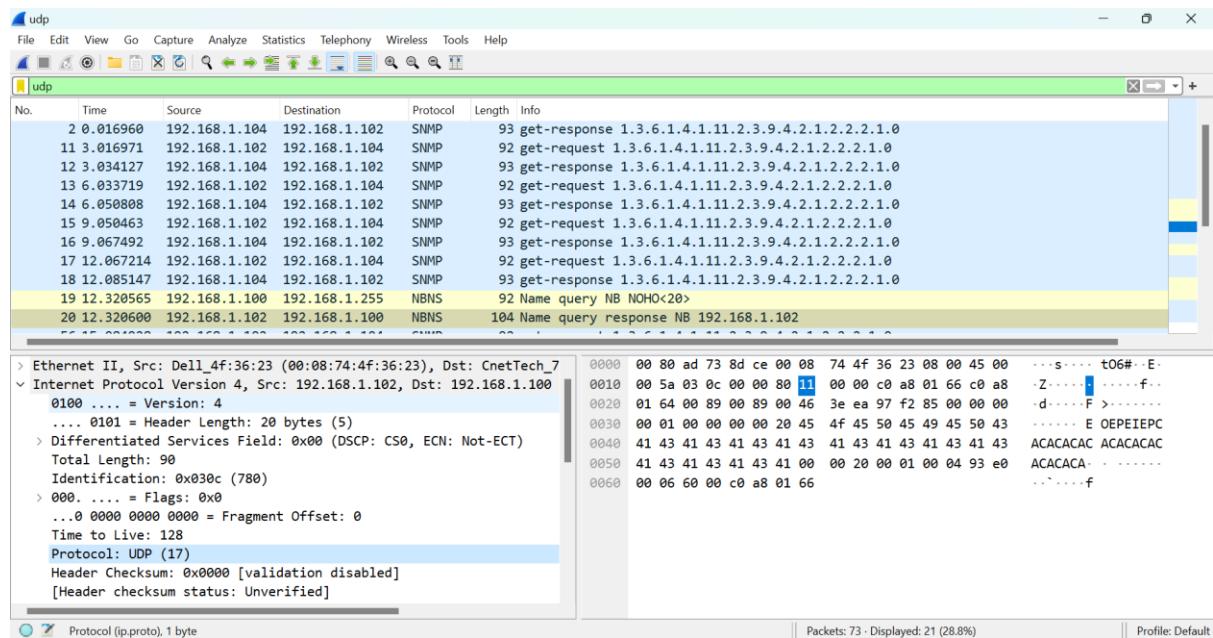
Data= 62 Bytes

Value of the Length Field is $62+8 = 70$ Bytes

Length in octets including this header and the data (udp.length), 2 bytes

Packets: 73 · Displayed: 21 (28.8%) · Profile: Default

m)Protocol Number of UDP is 17 in decimal and 11 in Hexadecimal



n)Source code of the packet is destination code for the second packet and vice versa.

