

21CY682- IP LAB ASSIGNMENT 4

Analyzing TCP and UDP using

Wireshark

Name: Meera E Timothy

Roll no: CB.EN.P2CYS22002

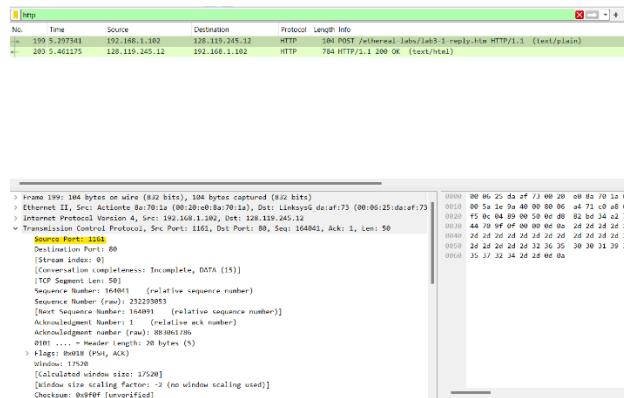
AIM: Analyze TCP and UDP using wireshark

Tool: Wireshark

TCP

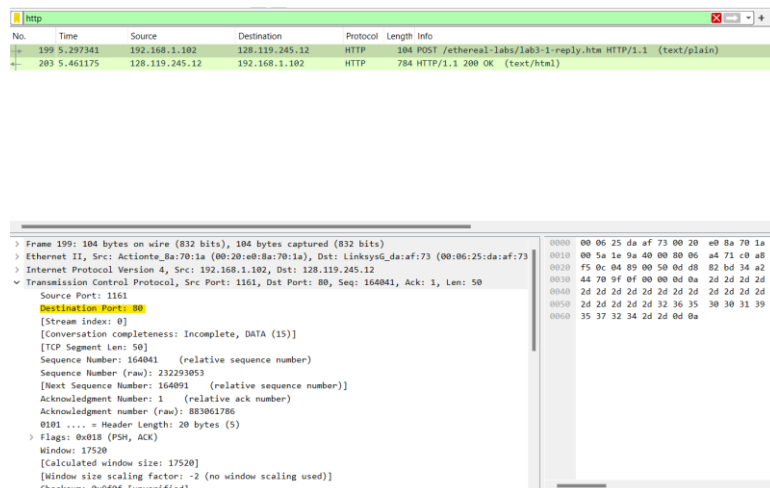
1 a) IP Address: 192.168.1.102

source port: 1161



b) IP Address: 128.119.245.12

Destination Port: 80



c) Sequence Number - 0

[SYN] -0x002

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
14	0.160118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=14600 Len=0

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12	0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00P.....E
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0	0010 00 30 1e 1d 40 00 06 a5 18 c0 a0 01 66 80 77	0 @ 7 . 6
Source Port: 1161	0020 f5 0c 04 89 00 50 d6 01 f4 00 00 00 70 02P.....P
Destination Port: 80	0030 40 00 f6 e9 00 00 02 04 05 b4 01 01 04 02	@
[Stream index: 0]		
[Conversation completeness: Incomplete, DATA (15)]		
[TCP Segment Len: 0]		
Sequence Number: 0 (relative sequence number)		
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: 0xf6e0 [unverified]		
[Checksum Status: Unverified]		

d) Sequence Number : 0

Acknowledgement Number : 1

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

New sequence number is the previous acknowledgment number.

[SYN, ACK]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
14	0.160118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=14600 Len=0

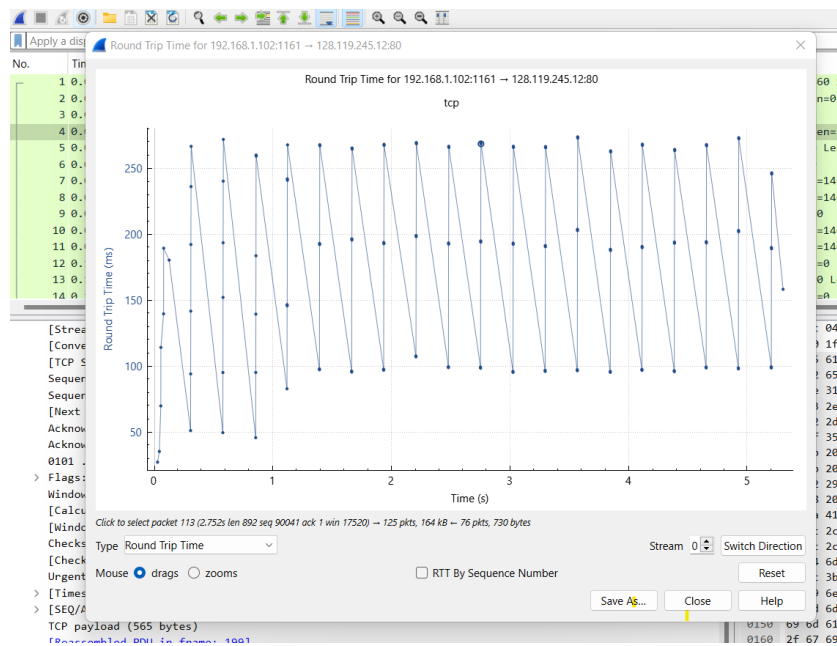
0111 = Header Length: 28 bytes (7)	0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00P.....E
Flags: 0x012 (SYN, ACK)	0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c a0	0 @ 7 . 6
0000 = Reserved: Not set	0020 01 66 80 50 04 89 34 a2 74 19 0d 06 01 f5 70 12	f P . 4 t
0000 = Accurate ECH: Not set	0030 16 d0 77 4d 00 00 02 04 05 b4 01 01 04 02	..M.....
0000 = Congestion Window Reduced: Not set		
0000 = ECH-Echo: Not set		
0000 = Urgent: Not set		
0000 = Acknowledgment: Set		
0000 = Push: Not set		
0000 = Reset: Not set		
0000 = SYN: Set		
0000 = FIN: Not set		
[TCP Flags:A-S-]		
Window: 5840		
[Calculated window size: 5840]		
Checksum: 0x774d [unverified]		
[Checksum Status: Unverified]		
Urgent Pointer: 0		
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted		
[Timestamps]		
[SEQ/ACK analysis]		

e) Sequence number is 1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
14	0.160118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=14600 Len=0

[Stream index: 0]	0020 f5 0c 04 89 00 50 d6 01 f5 34 a2 74 1a 50 18P.....t-P
[Conversation completeness: Incomplete, DATA (15)]	0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65	Dp...PO ST /ethe
[TCP Segment Len: 565]	0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31	real-lab s /lab3-1
Sequence Number: 1 (relative sequence number)	0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 50 2f	-reply.h t m HTTP/
Sequence Number (raw): 232129013	0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e	1.1 :Hos t: gaia.
[Next Sequence Number: 566 (relative sequence number)]	0070 63 73 2e 75 6d 61 73 73 2e 65 64 75 04 0a 55 73	cs.umass.edu Us
Acknowledgment Number: 1 (relative ack number)	0080 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c	er-Agent : Mozilla
Acknowledgment number (raw): 883861786	0090 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20	a/5.0 (Windows;
0101 = Header Length: 20 bytes (5)	00a0 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e	U; Windo ws NT 5.
Flags: 0x018 (PSH, ACK)	00b0 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 30	1; en-US ; rv:1.0
Window: 17520	00c0 2e 32 29 20 47 65 63 6b 6f 2f 32 30 30 33 30 32	-2) Geck o/280382
[Calculated window size: 17520]	00d0 30 38 20 4e 65 74 73 63 61 70 65 2f 37 2e 30 32	00 Metric spt/7.02
[Window size scaling factor: -2 (no window scaling used)]	00e0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78	-Accept : text/x
Checksum: 0xf1bd [unverified]	00f0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,appli cation/x
[Checksum Status: Unverified]	0100 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,appli cation/x
Urgent Pointer: 0	0110 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74	html=ml ,text/ht
[Timestamps]	0120 6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c	ml;q=0.9 ,text/pl
[SEQ/ACK analysis]	0130 61 69 6e 3b 71 3d 30 2e 38 2c 76 69 64 65 6f 2f	ain;q=0.8 ,video/
TCP payload (565 bytes)	0140 78 2d 6d 6e 67 2c 69 6d 61 67 65 2f 70 6e 67 2c	x-mng,im age/png,
[Reassembled PDU in frame: 199]	0150 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67 65	image/jp eg,image
	0160 2f 67 69 66 3b 71 3d 30 2e 32 2c 74 65 78 74 2f	/gif;q=0.2 ,text/

f) RTTTime Graph

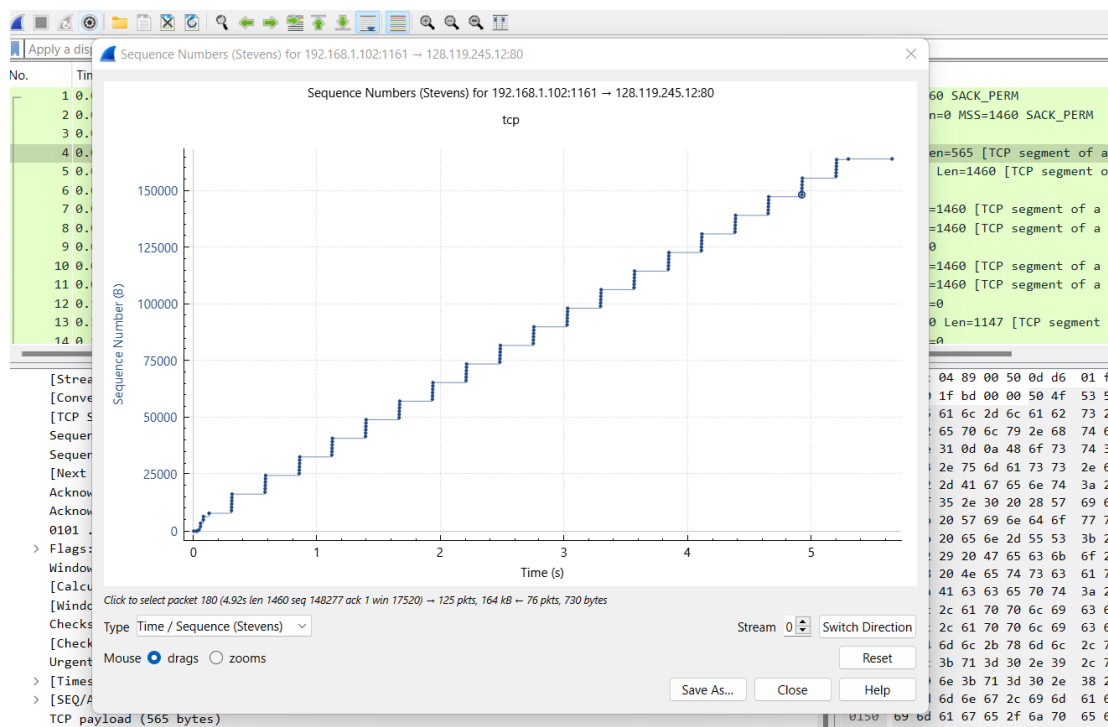


g) The length of first 6 packets are 565, 1460, 1460, 1460, 1460

Total Length: 164090

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
 [122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460)
 Hypertext Transfer Protocol

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



i) throughput = No of bytes transferred/time

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

= 30,224 byte

= 30.224KB

The top screenshot shows a Wireshark capture of network traffic. The packet list on the left shows several TCP segments. The selected packet (No. 5) is a TCP segment from 192.168.1.102 to 128.119.245.12, Seq=1, Ack=156469, Win=62780, Len=0. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the TCP segment.

The bottom screenshot shows a Wireshark capture of network traffic. The packet list on the left shows several TCP segments. The selected packet (No. 4) is a TCP segment from 192.168.1.102 to 128.119.245.12, Seq=1, Ack=1, Win=17520, Len=565. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the TCP segment, which includes an HTTP GET request.

UDP

2) a) In UDP header there are 4 fields :

Source Port, Destination Port, Checksum, Length

▼ User Datagram Protocol, Src Port: 4334, Dst Port: 161	0030	06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00	public #.....
Source Port: 4334	0040	02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02	--0-0--++.....
Destination Port: 161	0050	03 09 04 02 01 02 02 02 01 00 05 00
Length: 58			
Checksum: 0x65f8 [unverified]			
[Checksum Status: Unverified]			
[Stream index: 1]			
> [Timestamps]			
UDP payload (50 bytes)			
> Simple Network Management Protocol			

User Datagram Protocol Protocol Packets: 73 · Displayed: 21 (28.8%) Profile

b) No. of bytes for source port = 2

```
Source Port: 4334
Destination Port: 161
Length: 58
Checksum: 0x65f8 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
> [Timestamps]
UDP payload (50 bytes)
Simple Network Management Protocol
```

Source Port (udp.srcport), 2 bytes

No. of bytes for destination port = 2

```
Source Port: 4334
Destination Port: 161
Length: 58
Checksum: 0x65f8 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
> [Timestamps]
UDP payload (50 bytes)
Simple Network Management Protocol
```

Destination Port (udp.dstport), 2 bytes

No. of bytes for length = 2

```
Source Port: 4334
Destination Port: 161
Length: 58
Checksum: 0x65f8 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
UDP payload (50 bytes)
Simple Network Management Protocol
```

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

No. of bytes for checksums = 2

```
Source Port: 4334
Destination Port: 161
Length: 58
Checksum: 0x65f8 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
UDP payload (50 bytes)
imple Network Management Protocol
```

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

c) Length = Data + header

Header = Source port + Destination Port + Length + Checksum

= 2+2+2+2

= 8 Bytes

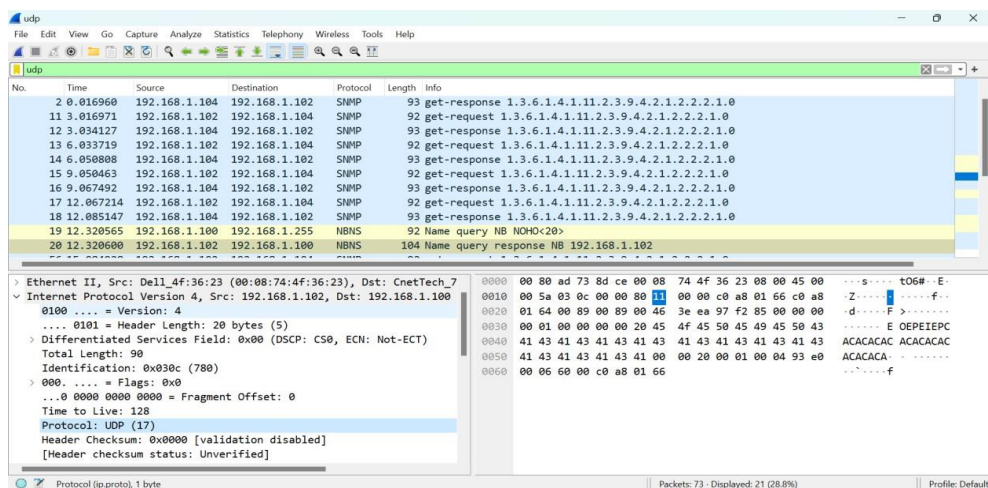
Data = 62 bytes

Value of the Length Field = 62+8

= 70 Bytes



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



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

Apply a display filter ... <Ctrl-/>						
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
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