21CY681 - INTERNET PROTOCOL LAB - IV

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 30th October 2022

Assignment Topic: Analyzing Transport Layer Protocols using Wireshark

AIM:

To Analyze TCP and UDP using Wireshark.pdf

TOOLS REQUIRED:

Wireshark

PROCEDURE:

1. Open the pcap file “tcp” in Wireshark to answer the following questions.

a. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

Ans :

Time	No.	Source	Destination	Protocol	Length	Info
2004/234 19:14:20.5…	1	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2004/234 19:14:20.5…	2	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
2004/234 19:14:20.5…	3	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
2004/234 19:14:20.5…	4	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 reassembl
2004/234 19:14:20.6…	5	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 reasse
2004/234 19:14:20.6…	6	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
2004/234 19:14:20.6…	7	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 reassemble
2004/234 19:14:20.6…	8	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 reassemble
2004/234 19:14:20.6…	9	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
2004/234 19:14:20.6…	10	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 reassemble
2004/234 19:14:20.6…	11	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 reassemble
2004/234 19:14:20.6…	12	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0

IP address : 192.168.1.102

TCP port number : 1161

b. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Ans :

Time	No.	Source	Destination	Protocol	Length	Info
2004/234 19:14:20.5…	1	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM

Time	No.	Source	Destination	Protocol	Length	Info
2004/234 19:14:20.5…	1	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2004/234 19:14:20.5…	2	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
2004/234 19:14:20.5…	3	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
2004/234 19:14:20.5…	4	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
2004/234 19:14:20.6…	5	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
2004/234 19:14:20.6…	6	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
2004/234 19:14:20.6…	7	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
2004/234 19:14:20.6…	8	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
2004/234 19:14:20.6…	9	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
2004/234 19:14:20.6…	10	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
2004/234 19:14:20.6…	11	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
2004/234 19:14:20.6…	12	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
2004/234 19:14:20.6…	13	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147

IP address : 128.119.245.12

Port Number : 80

c. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Ans : sequence number of the TCP SYN segment = 0

2004/234 19:14:20.5…	1	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM

Time	No.	Source	Destination	Protocol	Length	Info
2004/234 19:14:20.5…	1	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2004/234 19:14:20.5…	2	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
2004/234 19:14:20.5…	3	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
2004/234 19:14:20.5…	4	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 reassembl
2004/234 19:14:20.6…	5	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 reasse
2004/234 19:14:20.6…	6	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
2004/234 19:14:20.6…	7	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 reassemble
2004/234 19:14:20.6…	8	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 reassemble
2004/234 19:14:20.6…	9	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
2004/234 19:14:20.6…	10	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 reassemble
2004/234 19:14:20.6…	11	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 reassemble
2004/234 19:14:20.6…	12	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0

```
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced: Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: ··********S·]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s··  ··p···E·
0010  00 30 1e 1d 40 00 80 06  a5 18 c0 a8 01 66 80 77   ·0··@··· ·····f·w
0020  f5 0c 04 89 00 50 0d d6  01 f4 00 00 00 00 70 02   ·····P·· ######p·
0030  40 00 f6 e9 00 00 02 04  05 b4 01 01 04 02         @····### ######
```

The below figure identifies the segment as a SYN segment

```
Flags: 0x002 (SYN)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced: Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: ··********S·]
Window: 16384
[Calculated window size: 16384]
```

```
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
    [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
```

d. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Ans : Sequence number of the SYNACK segment = 0

Value of the Acknowledgement field in the SYNACK segment = 1

Computer A transmits a SYNchronize packet to computer B, which sends back a SYNchronize-ACKnowledge packet to A. Computer A then transmits an ACKnowledge packet to B, and the connection is established.

Computer A will send SYN and ACK to computer B .Then computer B will respond to computer A.The ACK of computer B equals to SYN of computer A and ACK of computer A equals to increment of SYN of computer.

We can identify it from the figure because it is showing SYN,ACK value

2004/234 19:14:20.5…	2 128.119.245.12	192.168.1.102	TCP	62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

```
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 232129013
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.]
```

```
Sequence Number (raw): 883061785
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 232129013
0111 .... = Header Length: 28 bytes (7)
Flags: 0x012 (SYN, ACK)
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 (N
[Timestamps]
[SEQ/ACK analysis]
```

e. What is the sequence number of the TCP segment containing the HTTP POST command?Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

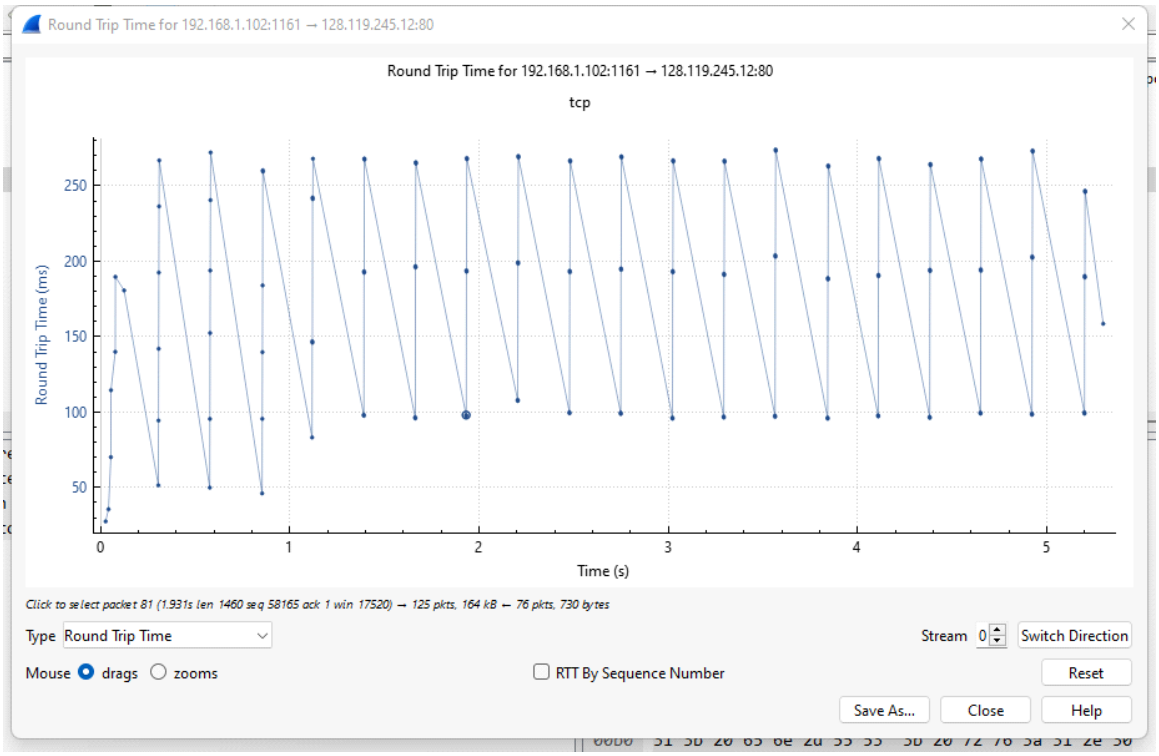
Ans :Sequence number of the TCP segment =1

2004/234 19:14:20.5…	4 192.168.1.102	128.119.245.12	TCP	619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembl

128.119.245.12	TCP	619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]	1161	80	128.119.245.12

f. Plot the RTT graph using Wireshark.

Ans :Navigate to statistcis ->tcp stream graph



g. What is the length of each of the first six TCP segments (HTTP POST)?

Ans :We found it when we went to http post

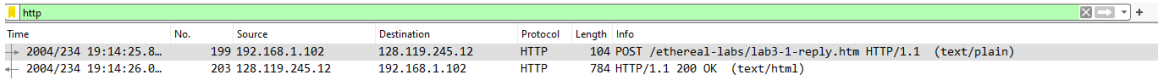
But to find the manually search for the first tcp segment of a reassembled and in that we find 2 lengths

619=packet length

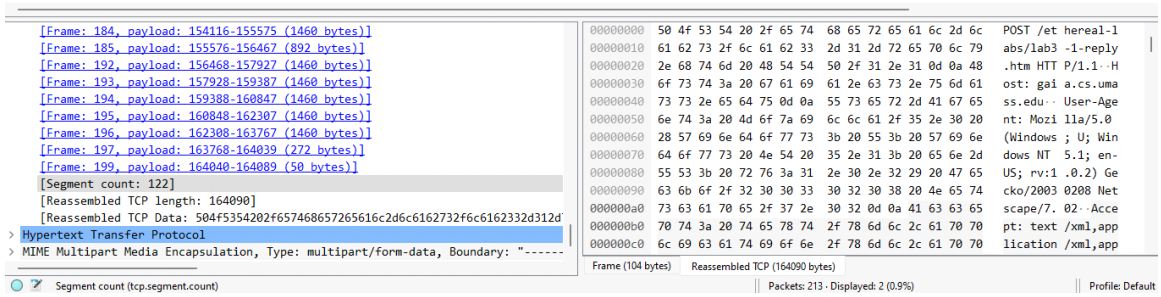
565=tcp segment length with header

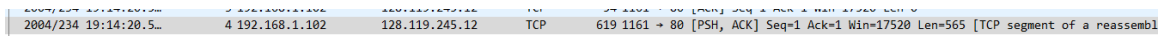
Maximum segment size =1460

```
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(14
  [Frame: 4, payload: 0-564 (565 bytes)]
```



Time	No.	Source	Destination	Protocol	Length	Info
2004/234 19:14:25.8…	199	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
2004/234 19:14:26.0…	203	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)

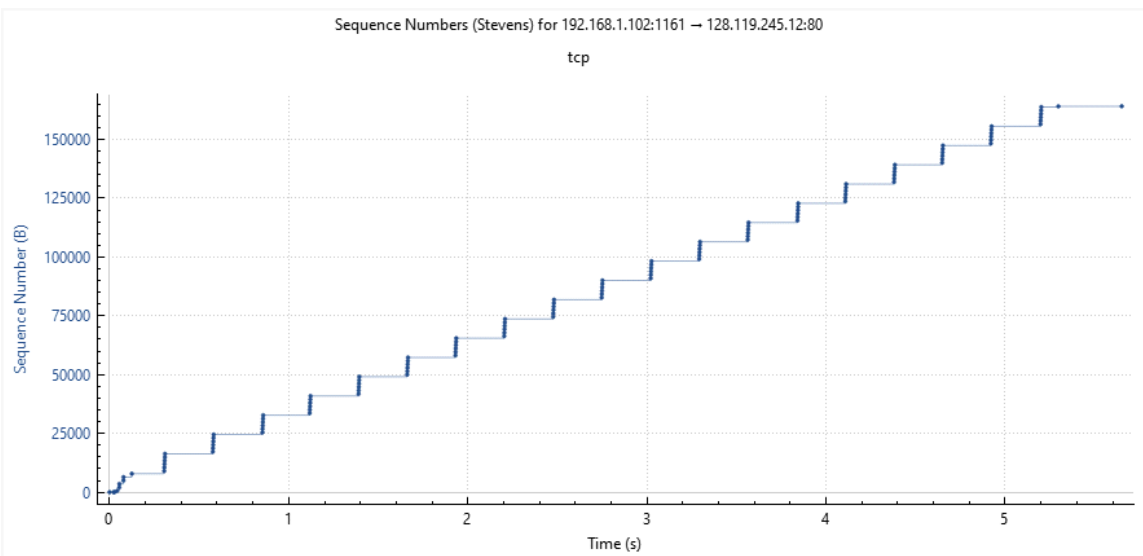




2004/234 19:14:20.5…	4	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembl

h. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

Ans : No



As time increases sequence number is also increasing that is no dropping in the graph.Here Acknowledgement number is not repeating thus no retransmission.If there is a drop , it will start from the start .So now here there is no drop as this is monotonical

case of graph as the graph is btw time and sequence .Retransmission same number will repeat with that the graph falls.

i. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Ans : Total amount of data transfered / Total time taken for data transmission.

164090/5.429353 = 30,222.754 bytes per second

= 30.222 kilo bytes per second

2. Open the pcap file “udp” in Wireshark to answer the following questions

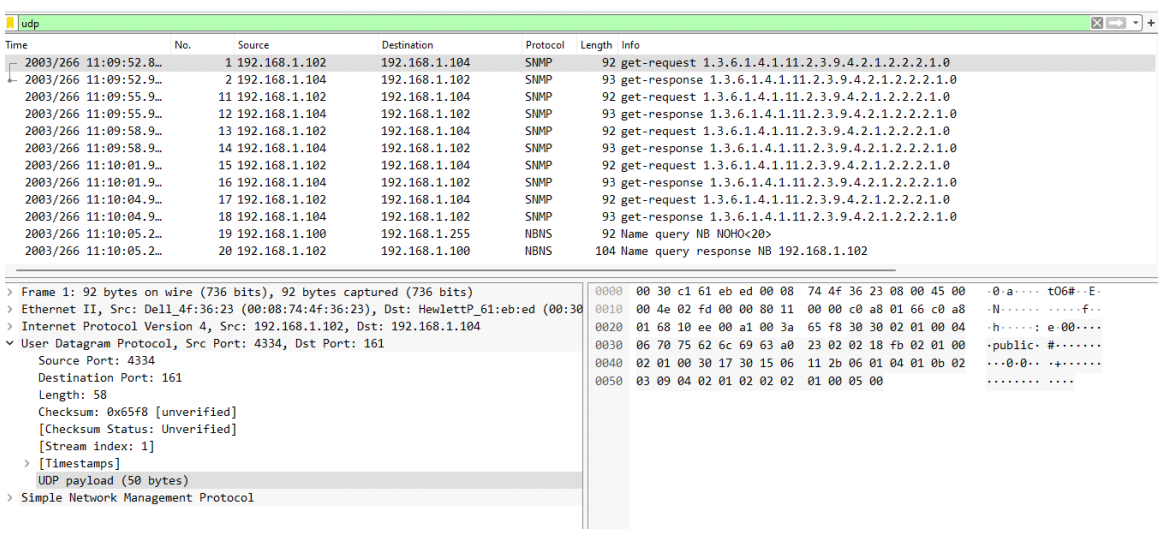
j. Select one UDP packet from your trace. From this packet, determine how many fields the are in the UDP header. Name these fields.

Ans : Source Port

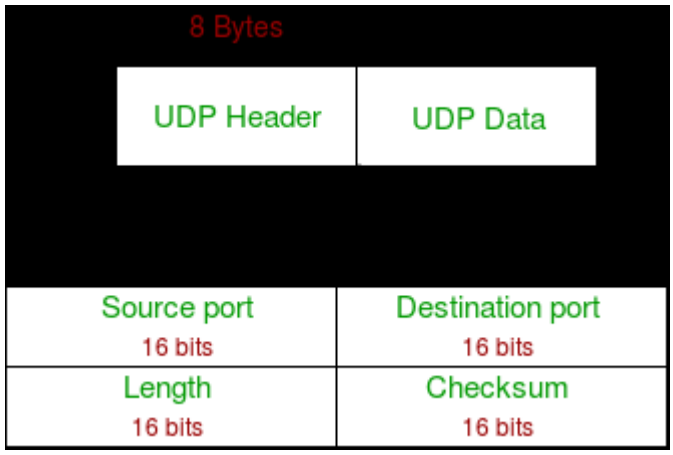
Destination Port

Length

Checksum



```
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: 1]
  > [Timestamps]
    UDP payload (50 bytes)
> Simple Network Management Protocol
```



k. 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.

Ans :When we select particular udp header we see in the below that 2 bytes are selected.

```
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: 1]
  > [Timestamps]
    UDP payload (50 bytes)
> Simple Network Management Protocol
```

Source Port (udp.srcport), 2 bytes

```
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: 1]
  > [Timestamps]
    UDP payload (50 bytes)
> Simple Network Management Protocol
```

Destination Port (udp.dstport), 2 bytes

```
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: 1]
  > [Timestamps]
    UDP payload (50 bytes)
> Simple Network Management Protocol
```

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

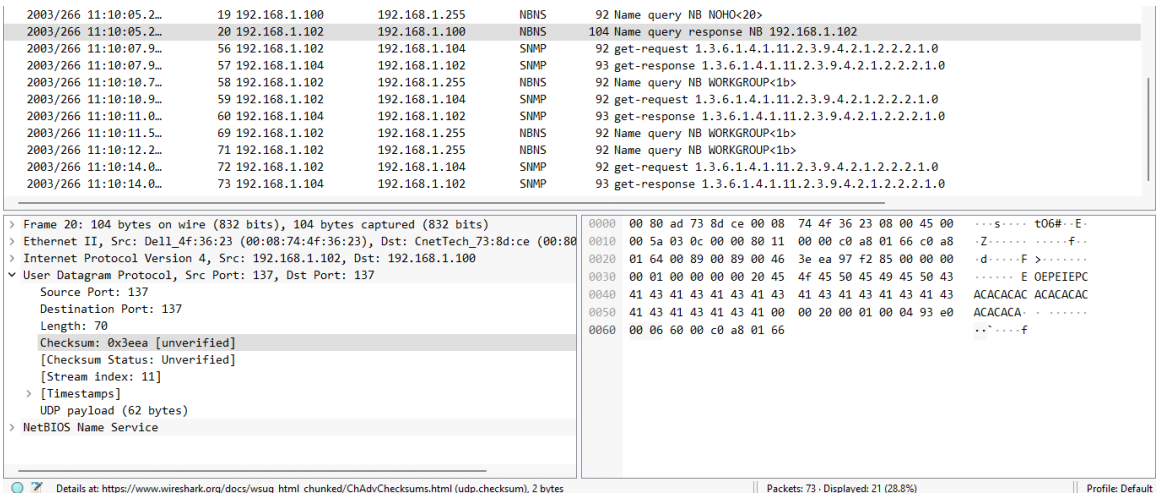
l. The value in the Length field is the length of what? Verify your claim with your

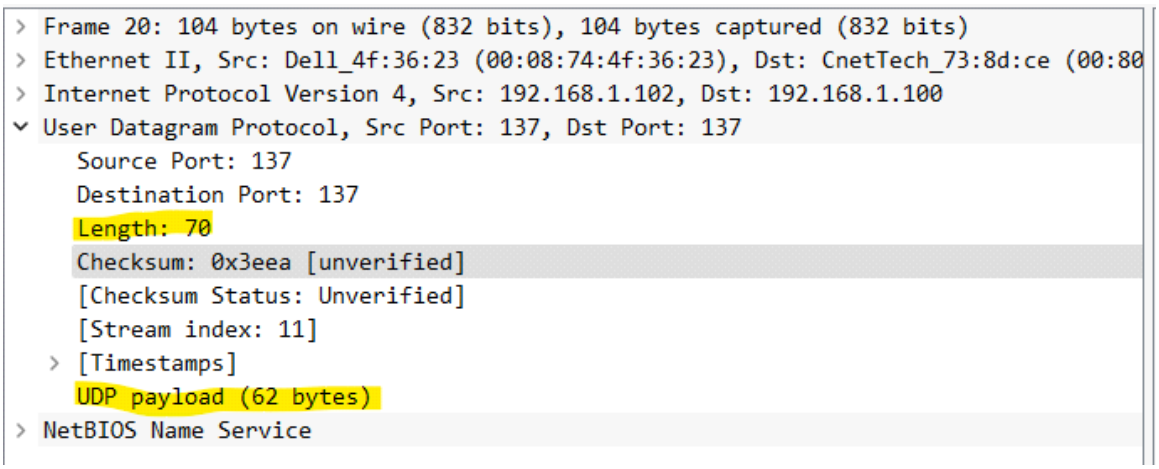
captured UDP packet.

Ans : Value in the Length field is the length of UDP header

As we know the value of header is 2,2,2,2 = 8

so, we add 62+8=70





m. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

Ans:Protocol number for UDP = 17

Decimal notation =17

Hexadeciaml notation =11

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 90
    Identification: 0x030c (780)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 192.168.1.100
```

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 90
  Identification: 0x030c (780)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]

0000  00 80 ad 73 8d ce 00 08  74 4f 36 23 08 00 45 00   ···s···· tO6#··E·
0010  00 5a 03 0c 00 00 80 11  00 00 c0 a8 01 66 c0 a8   ·Z····· ·····f··
0020  01 64 00 89 00 89 00 46  3e ea 97 f2 85 00 00 00   ·d·····F >·******
0030  00 01 00 00 00 00 20 45  4f 45 50 45 49 45 50 43   ****** E OEPEIEPC
0040  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0050  41 43 41 43 41 43 41 00  00 20 00 01 00 04 93 e0   ACACACA· · ******
0060  00 06 60 00 c0 a8 01 66                            ··`····f
```

n. 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.

Ans :From source IP it is going to destination IP and from destination IP it is getting the response.

Time	No.	Source	Destination	Protocol	Length	Info
2003/266 11:09:52.8…	1	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
2003/266 11:09:52.9…	2	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

address	port	i
4334	161	1
161	4334	1
4336	161	1

RESULT:

We have successfully Analyzed TCP and UDP using Wireshark