21CY681– Internet Protocol lab

ASSIGNMENT -4

Name: B.Shebu

Register Number : CYS22005

Title: Analyzing Transport Layer Protocols using Wireshark.

Date of Assignment provided: 27/10/2022

Aim: To analyse transport layer protocols using wireshark.

TCP

1 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?

Source	Src.port
192.168.1.102	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?

Destination	dpt port	Protocol
128.119.245.12	80	TCP

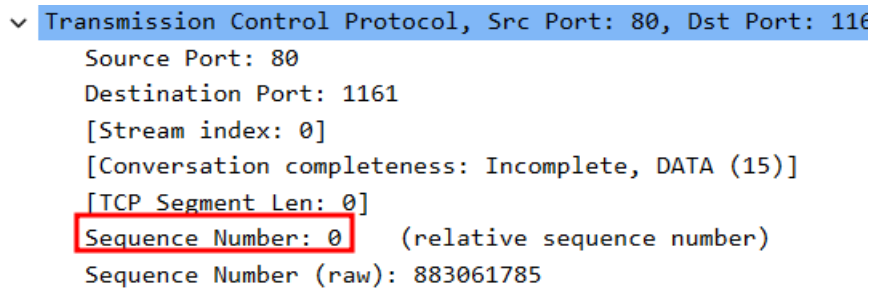
c) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Info
1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM

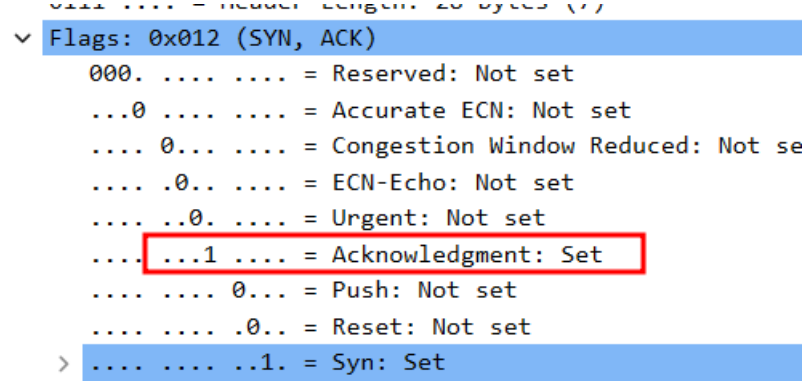
```
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
```

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?

The sequence number of the SYNACK segment sent is 0.

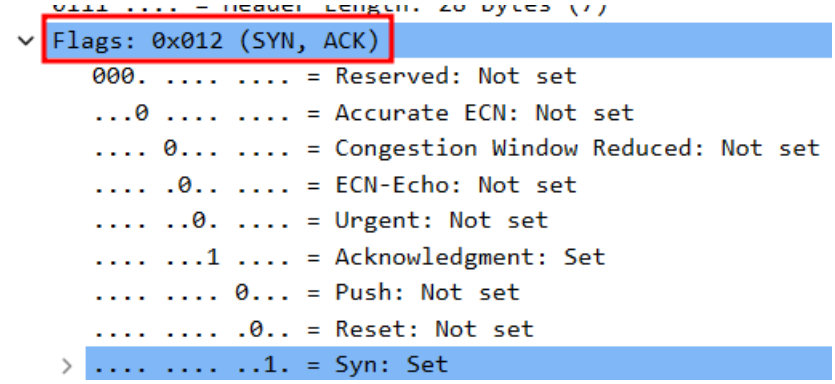


The value of ACK in SYNACK segment is 1.



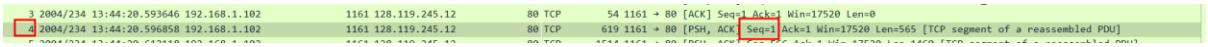
If SYN & ACK packets have been sent then in the SYNACK segment both the SYN & ACK flags will be set to 1

The SYN,ACK flag identifies it is a SYNACK segment



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.

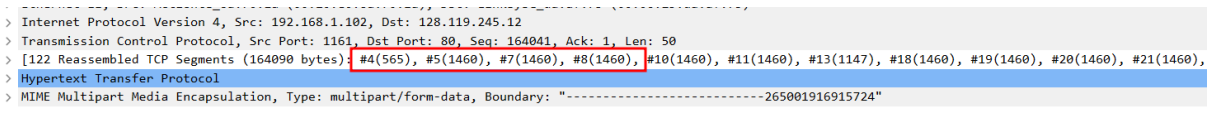
In order to find the SEQ number of the POST command , we need to see the SEQ number of the first transferred packet which had the data .



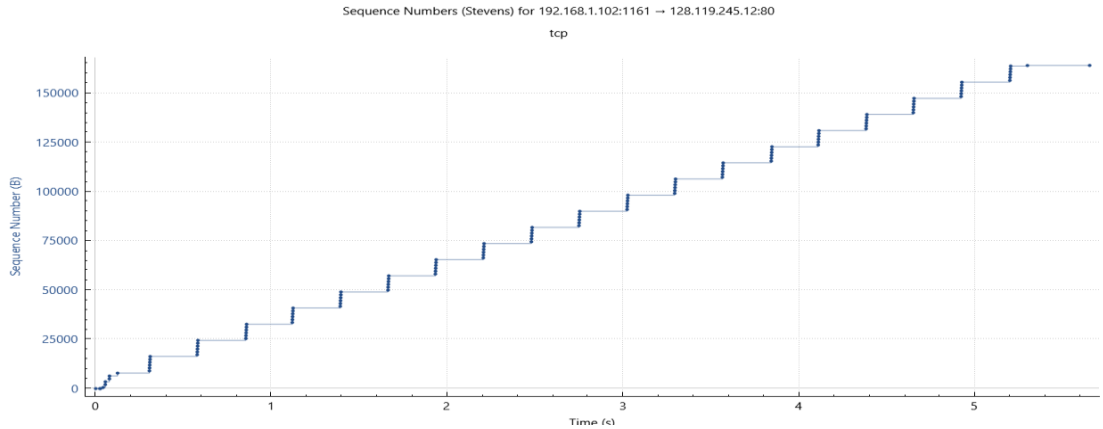
f) Plot the RTT graph using Wireshark.

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

The length of first 6 TCP packet segments are 565, 1460, 1460,1460, 1460, 1460



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



No there are no retransmitted segments in the file since there is no drop in the graph

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

Throughput = Total amount of data transferred / Total amount of time

The final value of ACK packet is 164091 , so the total amount of data transferred is 164091.

```
  60 80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
 784 HTTP/1.1 200 OK  (text/html)
```

Time of first packet since reference is 0.026477000

```
[Time delta from previous displayed frame: 0.003212000 seconds]
[Time since reference or first frame: 0.026477000 seconds]
```

Time of last packet since reference is 5.455830000

```
[Time delta from previous displayed frame: 0.007943000 seconds]
[Time since reference or first frame: 5.455830000 seconds]
```

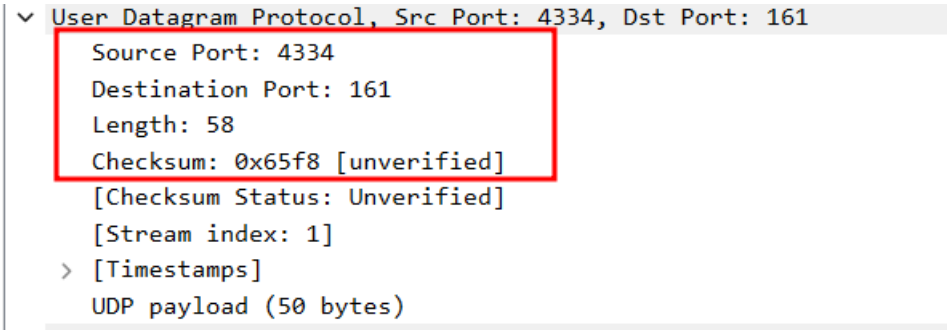
Throughput = 164090/(5.455830000 – 0.026477000)

= 302222 bytes => **30 kilobytes per second**

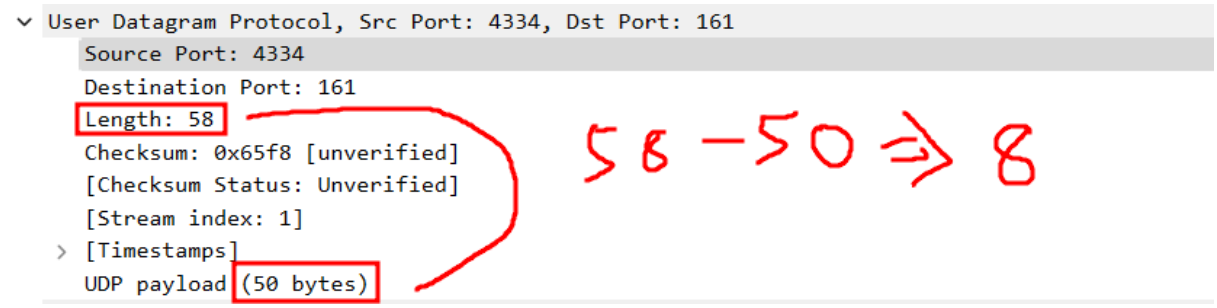
UDP

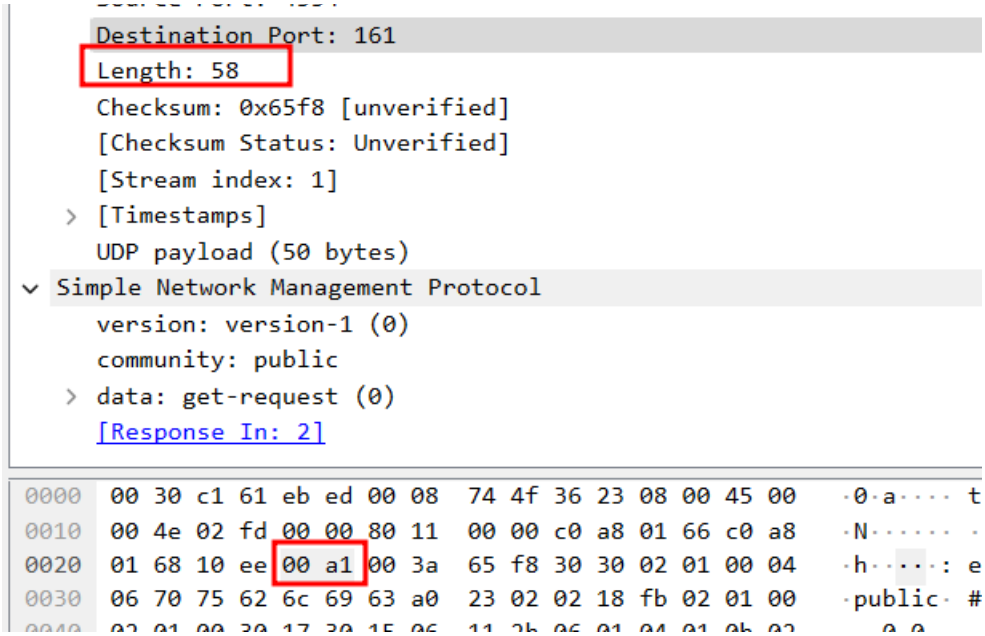
j) Select one UDP packet from your trace. From this packet, determine how many fields the are in the UDP header. Name these fields

There are 4 fields in UDP header.



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.

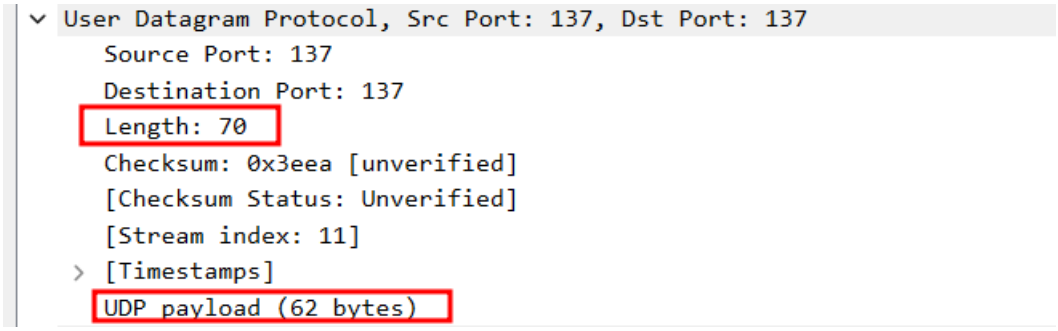




From the above , we can see that each field has length 2 bytes. So total length is 8 bytes.

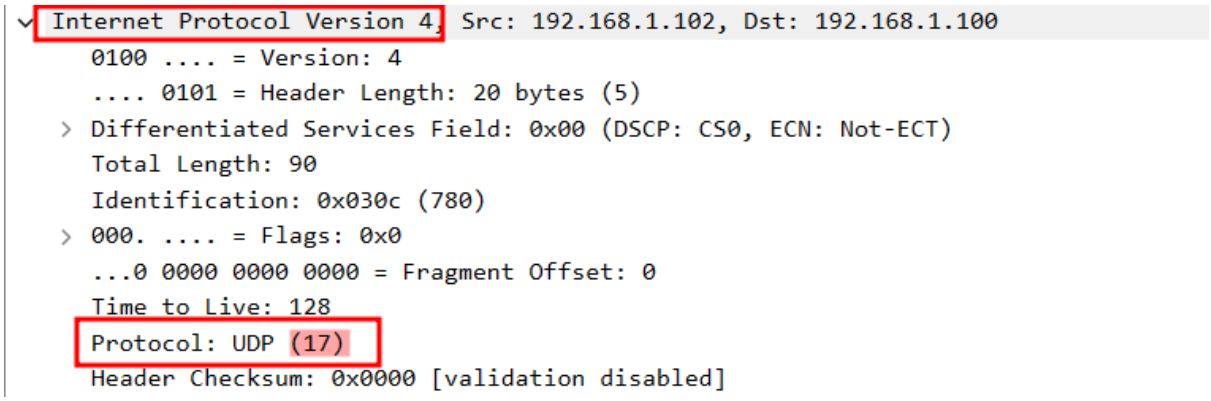
l) The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

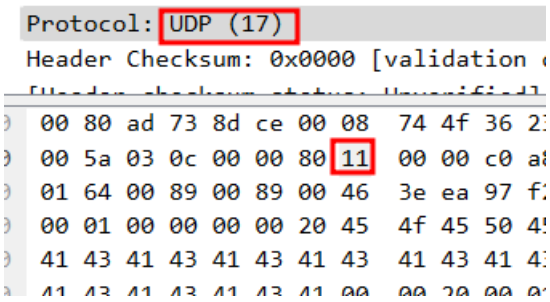
Size of the UDP payload is 62 . Size of each field is 2 . So total length kof fields is 8 .The total length of the TCP packet is 70(62+8).



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

The protocol number for UDP is 17. In hexadecimal it is 0x11.





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.

When 4334 is the source address the destination is 161 in request. In response it is the exact opposite.

Src.port	Destination	dpt port
4334	192.168.1.104	161
161	192.168.1.102	4334

RESULT –

Thus , we have successfully analyzed TCP and UDP using wiresharkl.