INTERNET PROTOCOL LAB ASSIGNMENT -4

Name: Siriparapu Sparshika

Roll No: CYS22006

Date: 27-10-2022

Analyzing TCP and UDP using Wireshark.pdf

AIM:

To Analyze TCP and UDP using Wireshark.pdf

PROCEDURE:

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

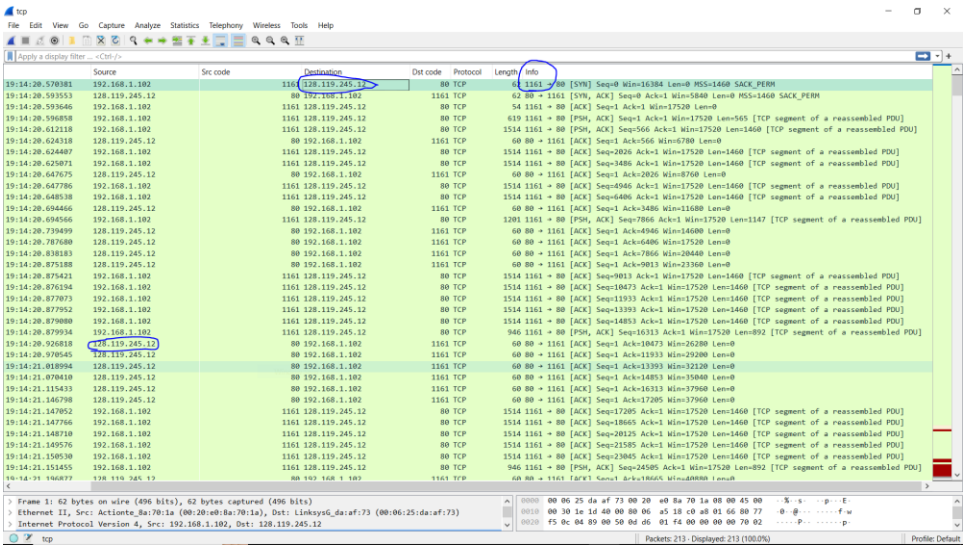
a. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

Destination	dpt port	Protocol
128.119.245.12	80	TCP

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?

Port no:80



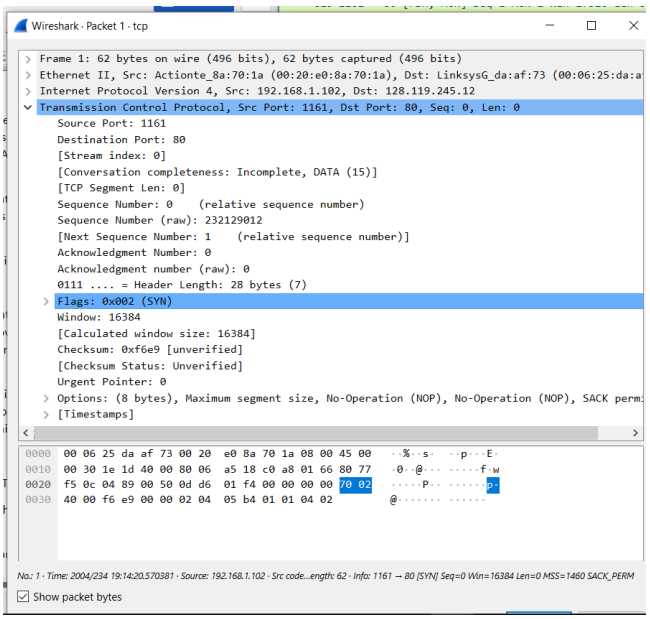
(Note: Wireshark->file->print- takes print out of the packet)

Since this lab is about TCP rather than HTTP, let's change Wireshark's "listing of captured packets" window so that it shows information about the TCP segments containing the HTTP messages rather than about the HTTP messages. To have Wireshark do this, select Analyze->Enabled Protocols. Then uncheck the HTTP box and select OK.

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?

Filter communication btw client and server and then identify first message.

Source port to destination port

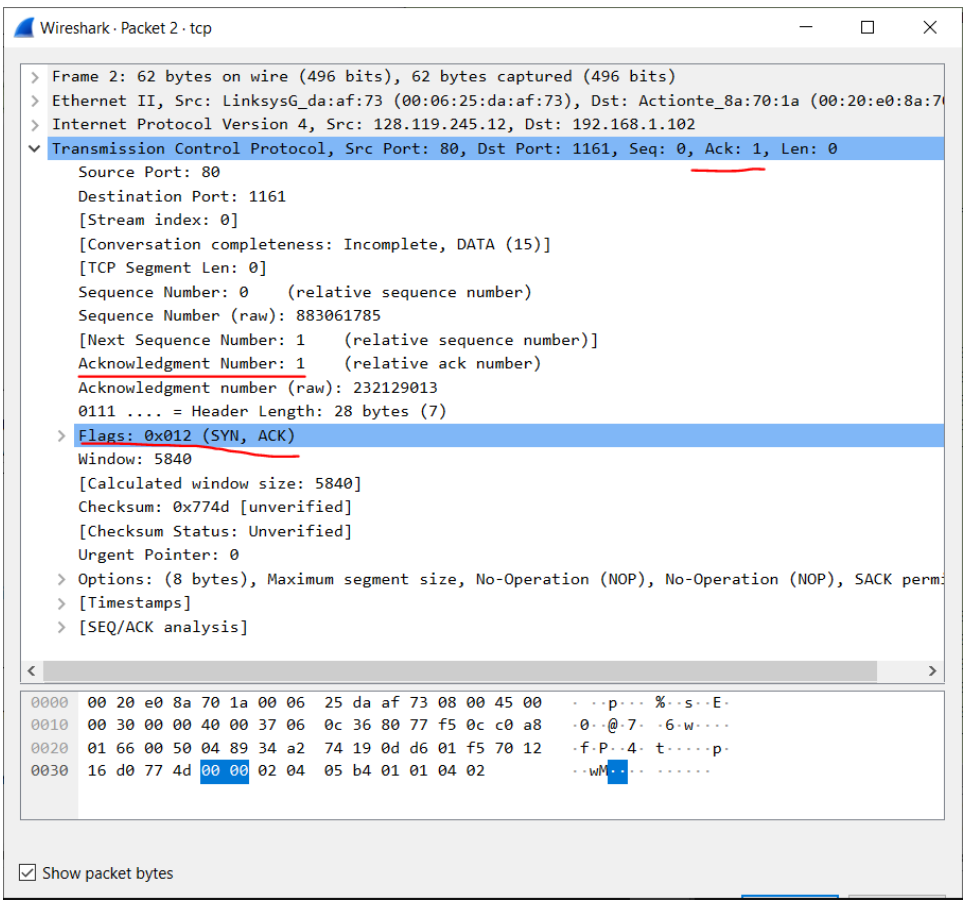


d. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK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

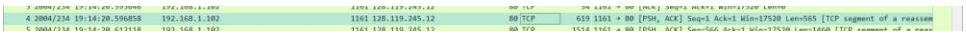
sequence number of the SYNACK segment sent=0

value of the Acknowledgement field=1

determine that value=flag 0*012



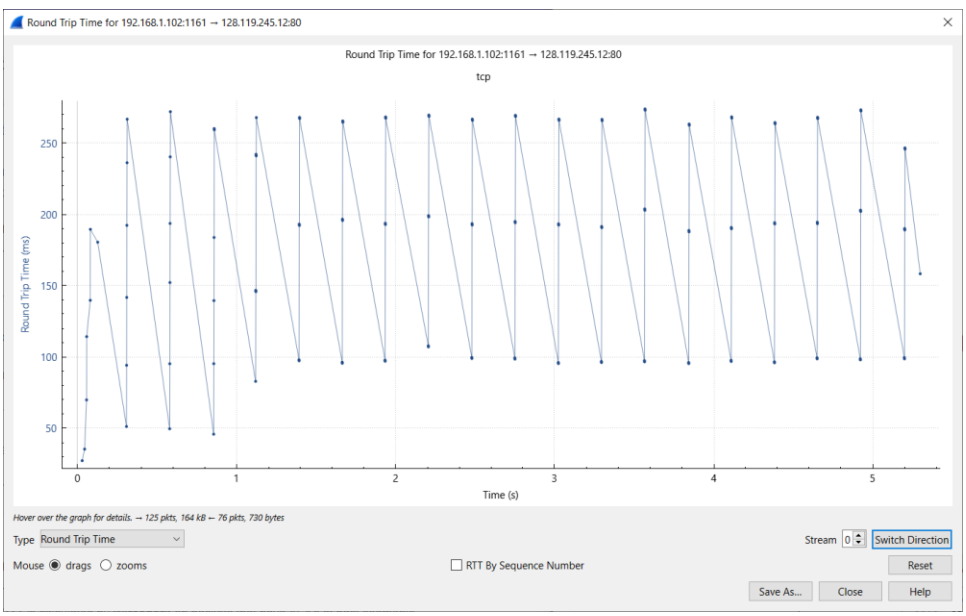
e. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.



Seq = 1

f. Plot the RTT graph using Wireshark.

Navigate to statistcis ->tcp stream grap



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

```
> 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), #13(1147),
```

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

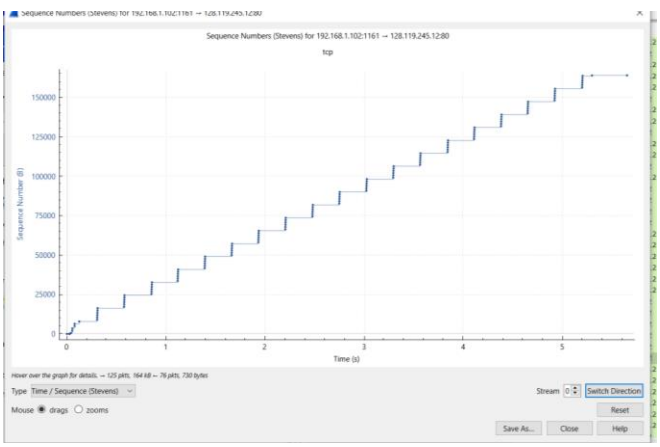
565=tcp segment length with header

1	0.000000	192.168.1.102	1161	128.119.245.12	80	TCP	62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	80	192.168.1.102	1161	TCP	62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.000093	192.168.1.102	1161	128.119.245.12	80	TCP	54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.003212	192.168.1.102	1161	128.119.245.12	80	TCP	619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]

Maximum segment size =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?

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

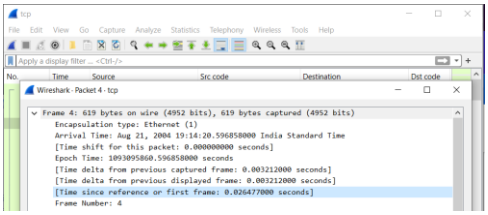
i. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

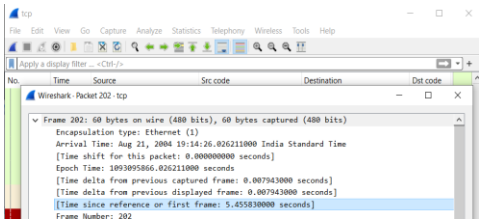
Throughput - total amount data/ total amount of time

First seq number Pack no-4 and last ack , pack no- 202

Data: (202 -packet no)164091-1(4-packet no)=164090

Time: 5.455830000-0.026477= 5.429353 => 164090





And divide with data 0.300 converted to kilo bites = 30.2 kB/sec

UDP:

Source Port (2 bytes)	Destination Port (2 bytes)
Length (2 bytes)	Checksum (2 bytes)

UDP Header

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.

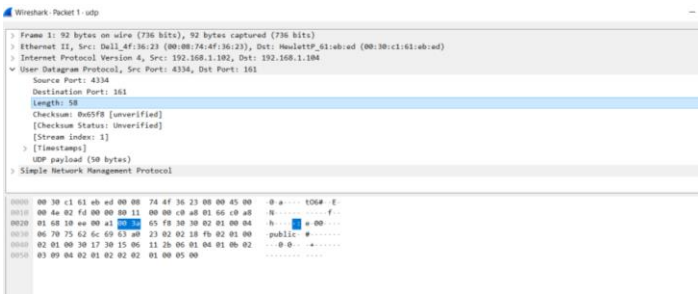
```
User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)
```

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.

Length – udp payload

Or

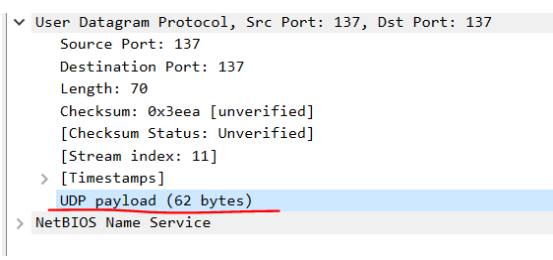
When we select particular udp header we see in the below that 2 bytes are selected.



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

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.

Decimal

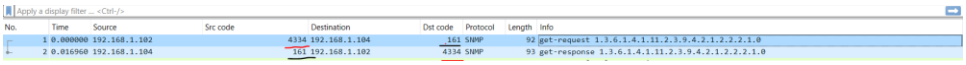
```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 78
    Identification: 0x02fd (765)
  > 000. .... = Flags: 0x0
    ...0 0000 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: 192.168.1.104
```

Hexadecimal

```
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 192.168.1.104
  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]

0000  00 30 c1 61 eb ed 00 08  74 4f 36 23 08 00 45 00   ·0·a···· tO6#··E·
0010  00 4e 02 fd 00 00 80 11  00 00 c0 a8 01 66 c0 a8   ·N····· ·····f··
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
```

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.



No.	Time	Source	Src code	Destination	Dst code	Protocol	Length	Info
1	0.000000	192.168.1.102	4334	192.168.1.104	161	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	161	192.168.1.102	4334	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

When source code is other destination and vice versa.

Result:

Thus , we have successfully Analyzed TCP and UDP using Wireshark

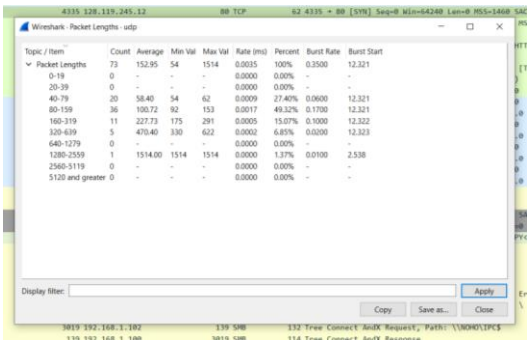
Points to be remembered:

How to specify the given graph is UDP:

So, it has no parameters and can't identify and we can do in application layer .

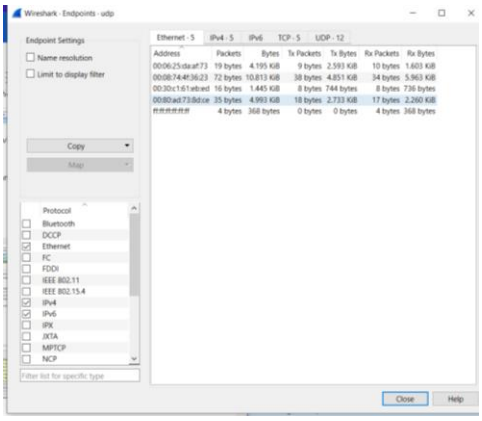
How to find packet length

Statistics-packet length



How to find total connections:

Exclude multicast address



And now in UDP –12 why do we have 12 its because:

Ip –4 and 9 new / unique port numbers are there

And now we should find unique IP address with new port address

One ip should use one port only no repetition.