21CY681 - INTERNET PROTOCOL LAB

Name: KARTHIKA P Date: 27th October 2022

Assignment Topic: TCP AND UDP

Register Number: CB. EN. P2CYS22001

AIM:

To analyse TCP and UDP using wireshark.

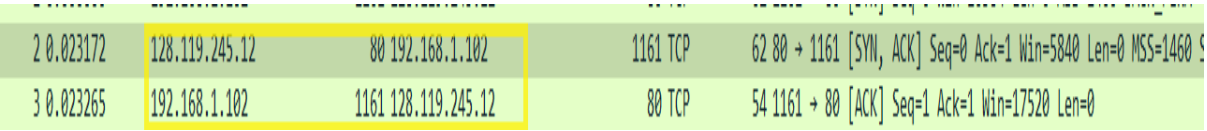
APPARATUS REQUIRED:

Wireshark

QUESTIONS:

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?



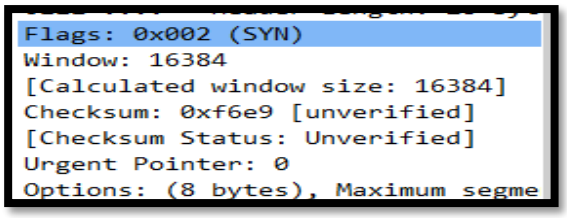
Source ip address :192.168.1.102

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?

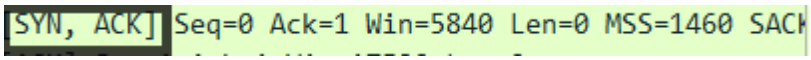
Ip address of gaia.cs.umass.edu:128.119.245.12

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?

Sequence number for TCP SYN segment is 0.



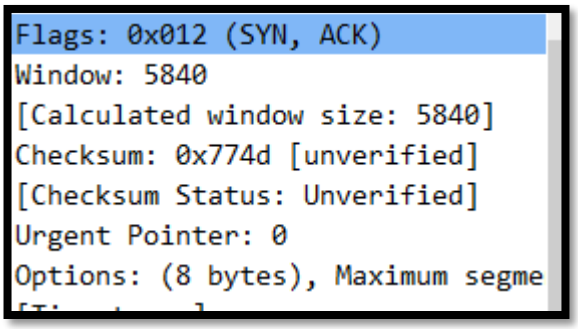
d) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK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



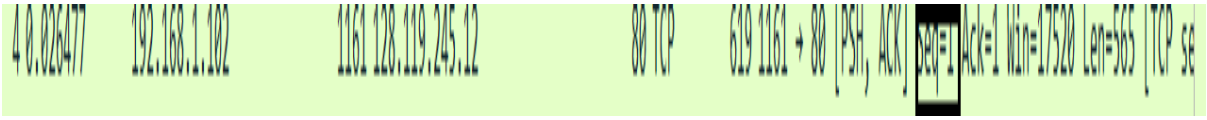
Sequence number of SYNACK segment is 0.

The value of acknowledgement field is 1.

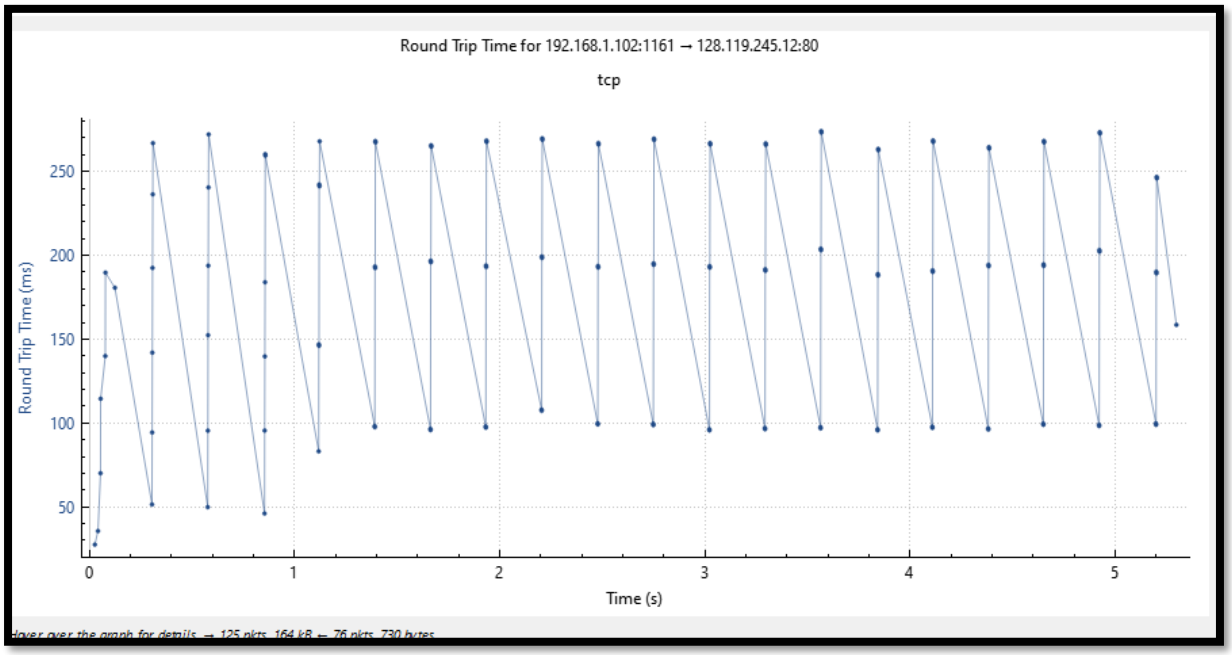
Since SYN , ACK is notified in that sequence.



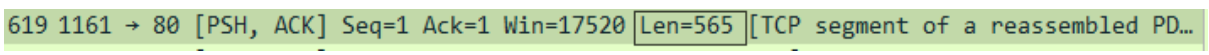
e) What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.



f) Plot the RTT graph using Wireshark.



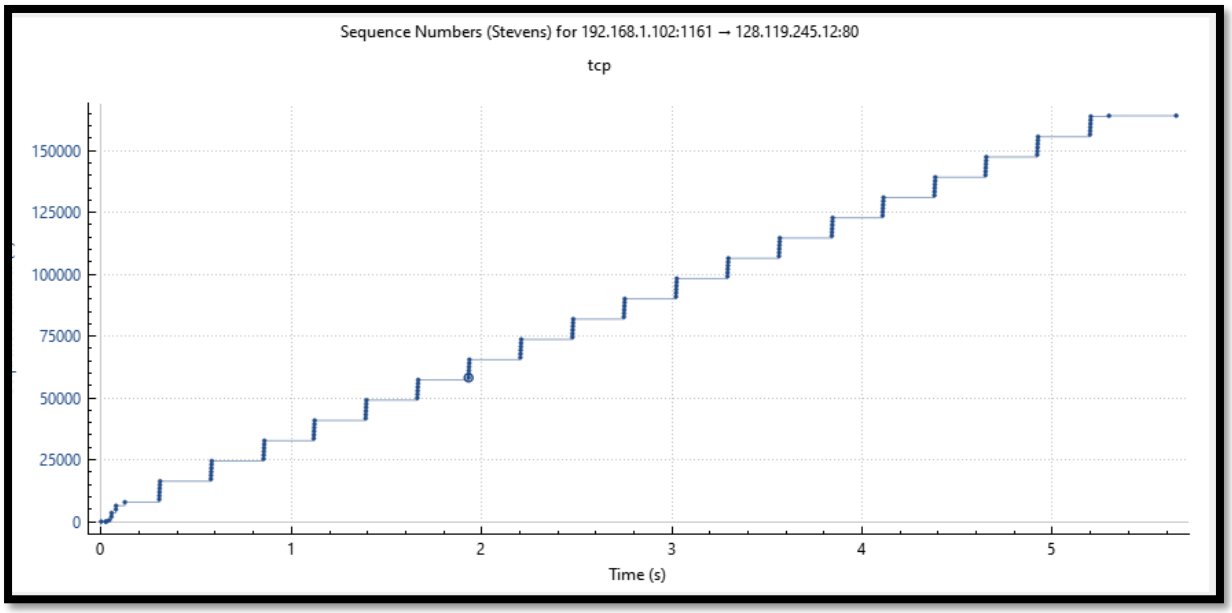
g) What is the length of each of the first six TCP segments (HTTP POST)?



The length of each segments is separated as 565 bytes.

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

Since there is no dropping in the graph ,so there is no retransmitted segments.



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

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

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

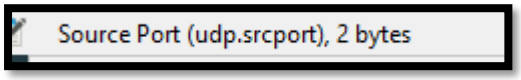
J)Select one UDP packet from your trace. From this packet, determine how many fields the are in the UDP header. Name these fields.

```
Source Port: 4334
Destination Port: 161
<Source or Destination Port: 4334>
<Source or Destination Port: 161>
Length: 58
Checksum: 0x65f8 [unverified]
[Checksum Status: Unverified]
```

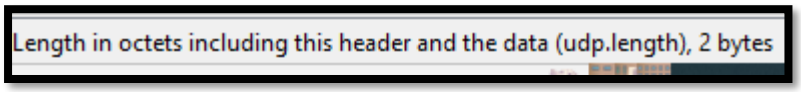
There are four fields ,they are source port, destination port, length,checksum.

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.

The length of source port is 2 bytes.

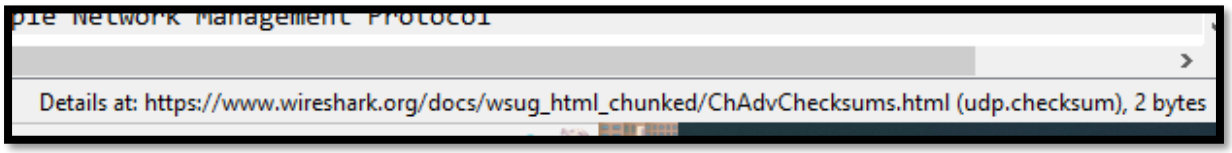


the length of the data length is 2 bytes.

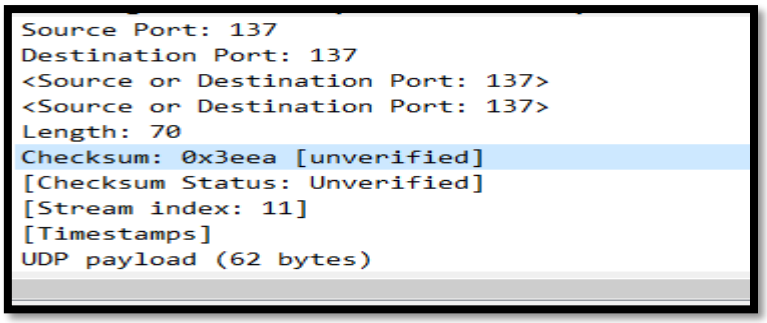


The length of destination port is 2 bytes.

The length of checksum is 2 bytes.



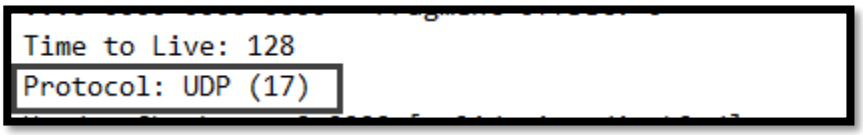
l) The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

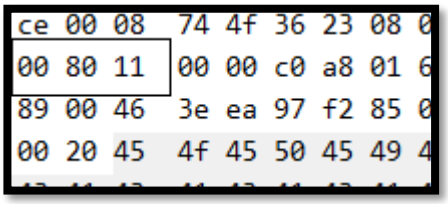


Here , the payload is 62 bytes and 8 bytes for the four header.

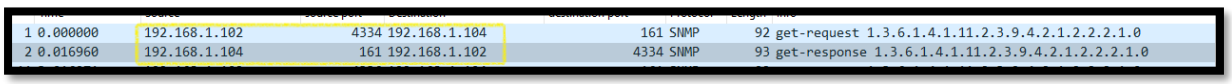
m) What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

The protocol number of udp is 17.





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.



Here we can identify that from source ip has been transferred to the destination and then from destination ip it got response to the source.

RESULT:

Thus, we have analysed TCP and UDP using wireshark.