ASSIGNMENT 2

Task 1: Study TCP through the given trace.

First of all after downloading the given trace we can open it in wireshark to study various aspects in detail after that the results obtained are given below :

- To find the IP address of mam’s laptop we can see which packet is contributing for the connection setup (i.e. the packet that carries the SYN packet) .Therefore the packet that consists this is the packet number 2 for which the source address is 192.168.0.106 which exactly is the IP address of mam’s laptop. The MAC address of mam’s laptop is given next :

- We can find all the MAC addresses of the trace in wireshark as statistics→conversations→ Ethernet .Here if we see all entries in it the client has a common address which is the MAC address of mam’s laptop which is cc:3d:82:9d:a9:cc.

- Now if we sort bytes In statistics→conversations we see that there is a large amount of data transfer (101M bytes) with 100M from client to server (client is mam’s laptop) therefore we can say that the dominic activity i.e. the connection X is upload from mam’s laptop to the server with the port number of mam as 57772 and the server as 443.We also know that the port number 443 is used by a web server therefore the connection X is that mam is uploading something on a web server.

- The IP address of the other end point i.e. the web server can be found by the same way we found the dominic activity i.e. the 100M bytes were transferred from client to server therefore we can found the server IP address from this which is 162.125.81.15 This IP address is owned by www.dropbox.com as we can see in frames 99-100 that a connections with dropbox is set up.

- We can find the the MAC address of the server also using the same feature we used for finding the MAC address of client by finding the packet that has the maximum bytes therefore the MAC address of server is 48:ee:0c:46:ab:2c

- The router IP address can be found from the first connection setup therefore router IP address is 52.114.40.57.

- We can see the connection setup frames as 2,5,6 which are the SYN, [SYN,ACK] and ACK of SYN packets which contribute to the 3 way handshake connection but this connection is between mam's laptop and router so the connection setup frames are 350,355 and 356 for connection between mam's laptop and end point.

- Now we will analyze the various fields as given in wireshark:
    - First is the frame number which also shows the number of bytes that were sent and the number of packets that are captured.
    - Now we also have the absolue arrival time of that particular frame in India Standard Time and we can also change the format of that .
    - We have Epoch time which is also known as UNIX time and it is the time in seconds after 1 Jan,1970 to the arrival of the frame.
    - We also have the information about the delta time since previously captured frame and previously displayed frame .The difference between these is known as Time shift for this packet.
    - After that we have the length of the frame and the also the number of bytes captured.
    - We also have the type of IP which is IPv4.
    - After that we have the IP addresses of the source and destination for that particular frame.
    - We also have the header length of that IPv4 in bytes.

- Now in TCP we have the port number of source as well as the destination along with the sequence number, acknowledgement number and the length.
- For sequence number and acknowledgement number we also have the raw (absolute) values of sequence number and acknowledgement number.
- Now we have the header length in TCP which is in bytes.
- We also have the info about the window size till that frame.
- We have the Timestamps which provides us the time since the first frame in that TCP segment and also the time since the previous frame in that TCP segment.
- Wireshark also provides the details of acknowledgement i.e. this acknowledgement is for which segment and also the RTT for that acknowledgement. We can compare this with the iRTT i.e. the Initial Round Trip Time which is the time for the first connection packet(SYN , SYN-ACK) transfer.

- The congestion window can be observed the time sequence (stevens) graph of wireshark. If we look into the initial part then we can see the slow start i.e. for every acknowledged packet the window size (cwnd) increases by MSS. And if we will see the I/O graph of wireshark then there we can infer that whenever there is a dup-ACK then there we can see the congestion avoidance. Therefore we can infer the congestion window increase till slow start and then at congestion avoidance there is decrease .

- We can see the effects of mam walking away from router from the RTT (Round Trip Time) graph (Statistics→TCP Steam Graphs→ Round Trip Time) as the RTT increases for a particular time which can be attributed to the time mam were away from router and then it reaches a maximum can be inferred as from where mam started walking back.

- There are various packets which are duplicate ACKs/Retransmissions some of the packets numbers are listed :
  Duplicate ACKs : 224,299,470 and more
  Retransmissions : 258,265,266 and more
  There are also some packets with TCP spurious retransmissions as :

Spurious Retransmission : 153,223 and more
In the packet of duplicate acknowledgement we see another column in the end which given us the information that this duplicate acknowledgement is for which frame and also that how many duplicate acks are received .

- We can see the effect of mam walking back from the RTT (Round Trip Time) graph (Statistics→TCP Steam Graphs→ Round Trip Time) as the RTT decreases after a certain time which could be attributed to the decrease in propagation time because it is directly proportional to the distance therefore as L decreases Tprop also decreases and hence RTT also decreases proportionally.

Task 2: Trace and analyze the network traffic characteristics of a video conferencing application

I was not able to find someone with whom I could have collaborated for this task so I have done this task by using 2 devices of my own with one connected to wifi and other to my mobile network.

The video calling platform chosen by me is ZOOM and below are the results for it :

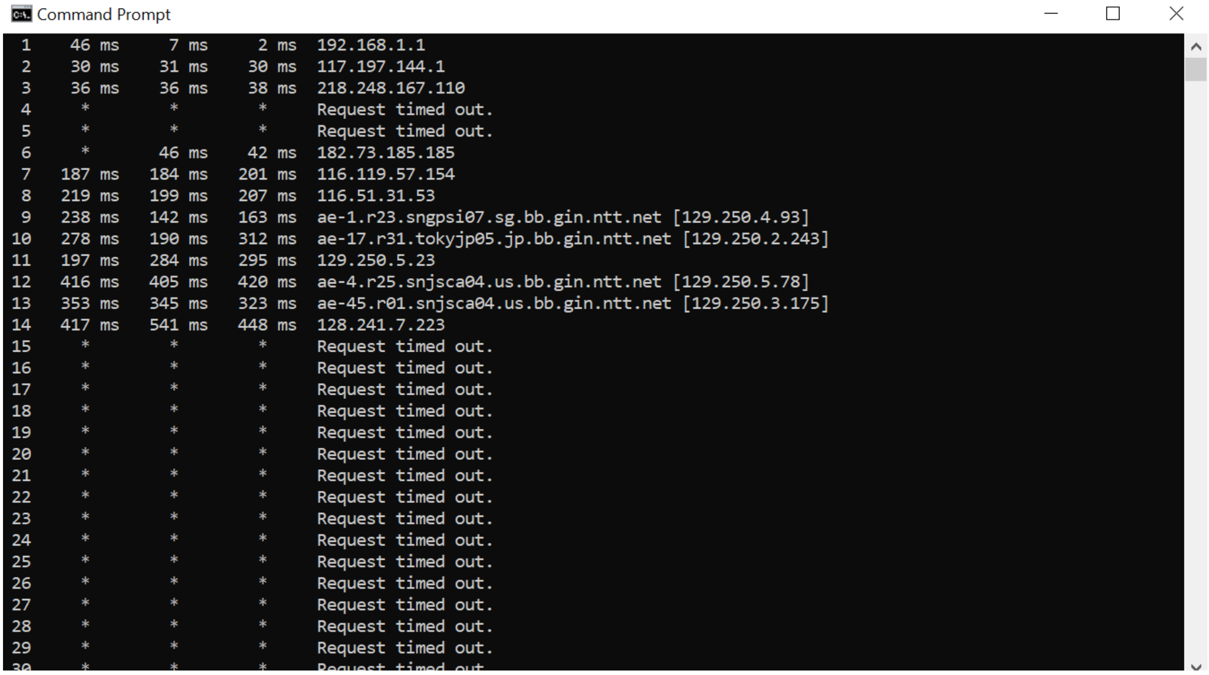
- Here if we will see the conversations table of this trace then we observe that most of the packets were between 2 IP addresses and from them one was for my laptop and the other was of zoom server. Therefore after observing some frames the IP address of my laptop is 192.168.1.107 .The ISP info that we got is that the address space it seems to own is 192.168.*.*

- The server IPv4 address is 144.195.41.40 (Zoom server address) and zoom does not seem to use any IPv6 address.

- The Transport layer used for Zoom is mainly UDP with a bit of TCP and it also uses a protocol called Wireguard to transport data.

- The application layer protocol for Zoom is http and also the port it uses is same as http which is 443.

- The application protocol of http was carried over TLS (Transport layer security) which is to protect the packets from any other third user this is because zoom does not provide end to end encryption therefore it uses TLS for security.

- 

```
  1    46 ms     7 ms     2 ms  192.168.1.1
  2    30 ms    31 ms    30 ms  117.197.144.1
  3    36 ms    36 ms    38 ms  218.248.167.110
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *       46 ms    42 ms  182.73.185.185
  7   187 ms   184 ms   201 ms  116.119.57.154
  8   219 ms   199 ms   207 ms  116.51.31.53
  9   238 ms   142 ms   163 ms  ae-1.r23.sngpsi07.sg.bb.gin.ntt.net [129.250.4.93]
 10   278 ms   190 ms   312 ms  ae-17.r31.tokyjp05.jp.bb.gin.ntt.net [129.250.2.243]
 11   197 ms   284 ms   295 ms  129.250.5.23
 12   416 ms   405 ms   420 ms  ae-4.r25.snjsca04.us.bb.gin.ntt.net [129.250.5.78]
 13   353 ms   345 ms   323 ms  ae-45.r01.snjsca04.us.bb.gin.ntt.net [129.250.3.175]
 14   417 ms   541 ms   448 ms  128.241.7.223
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.
```

- The route for the connection with zoom server is shown above however after 14 hops the packets were not able to move forward .

- Now if we will see the packet traffic from statistics→ Conversations→ UDP then we observe that the amount of packets sent from my laptop (wifi) to zoom is much greater than those received from zoom therefore we can conclude that either my camera was on for a longer duration due to which I was sending more packets or the network speed of the other end (my mobile network) was low. To check this we can see the bits/s column for A→B and B→A after seeing that we conclude the bits/s from my laptop (wifi) was much higher than received from zoom therefore we conclude that the network speed of my wifi was higher than mobile network.

  Some observations :

- There were some packets with protocols as MDNS which I could not understand properly .I opened the packet in detail and there was some mobile name in it "REDMI NOTE 10S" which is the mobile of my DAD and he was also using the same wifi so these packets gave information about the other devices connected with this network.

- There were also some packets with protocol IGMP and this also had the same MAC address as MDNS so I think these packets ask around if there is some other member of this network.

As some extra work I did an experiment by video calling myself with 2 devices and both devices connected to my wifi network and the result was quite interesting. And some of the observations are listed below :

- Along with the expected communication of my laptop with the zoom server a huge amount of packet transfer (11080 packets) was taking place directly between the 2 devices. Like the connection between my laptop and zoom was between IP addresses 192.168.1.107 and 144.195.41.40 but now huge amount of data transfer was between 192.168.1.107 and 192.168.1.108 with later being the IP address of my second device connected.