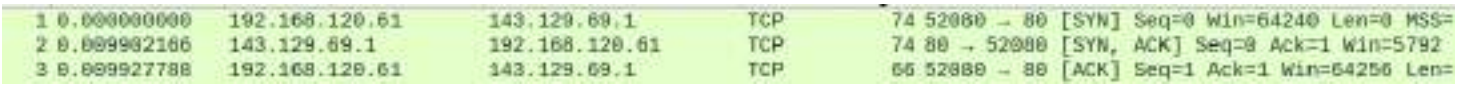
Wireshark – TCP Assignement

Name : Serena Anthony **Roll.NO** : B210031CS

1. What are the packets involved in 3-way handshake (provide packet id and highlight those packets in screenshot)?



SYN: This packet is sent from the client to the server to initiate the connection.

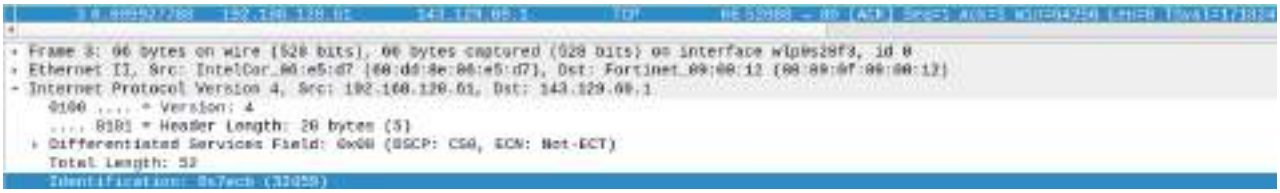
Identification: 0x7eca (32458)

SYN-ACK: This packet is sent from the server back to the client in response to the SYN packet.

Identification: 0x2d50 (11600)

ACK: This packet Is sent from the client to the server to acknowledge the receipt of the SYN-ACK packet.

Identification: 0x7ecb (32459)



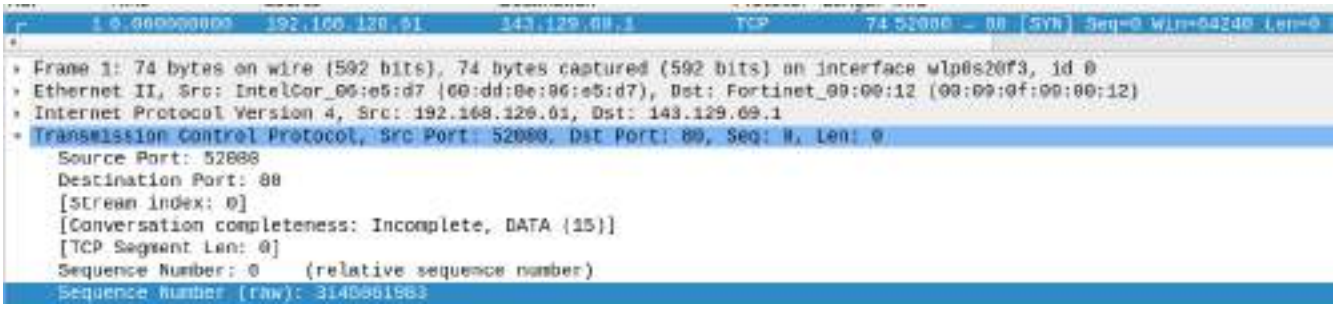
2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the your client computer (your machine) and http://fimi.uantwerpen.be/data/?

   Ans:

   We find the sequence number of the TCP SYN segment by looking into the TCP SYN packet in the 3-way handshake. This value is usually a random value generated by the client to initiate connection.

   Sequence Number: 0 (relative sequence number)

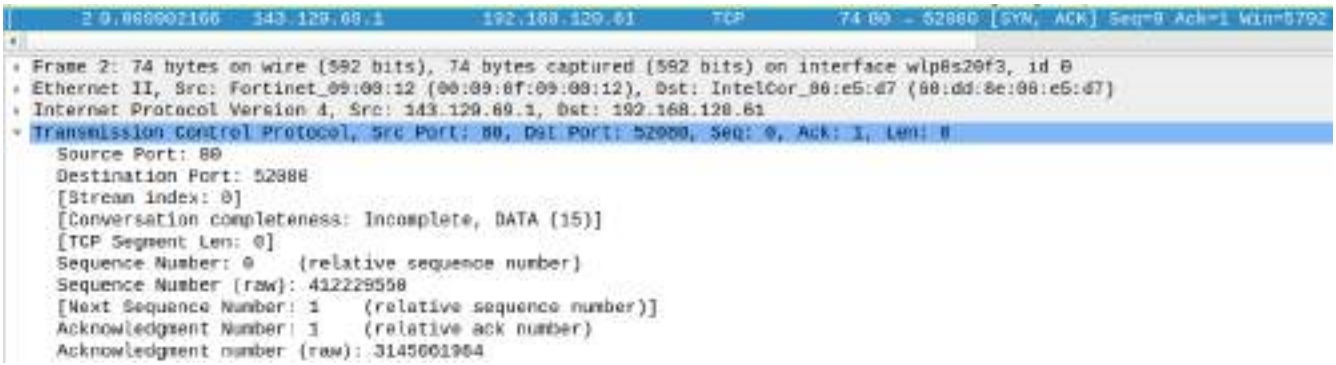
   Sequence Number (raw): 3145061983



3. What is the sequence number of the SYNACK segment sent by http://fimi.uantwerpen.be/ to the client computer in reply to the SYN? What is the value of the Acknowledgment field in the SYNACK segment?

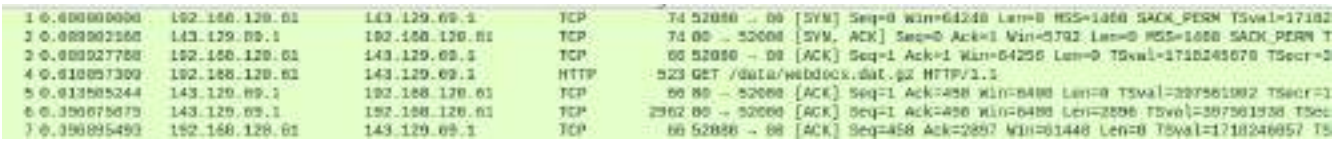
The sequence number of the SYNACK segment is generally a random value generated by the server. The acknowledgment field acknowledges the SYN segment from the client.

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 412229550
Acknowledgment Number: 1 (relative ack number)



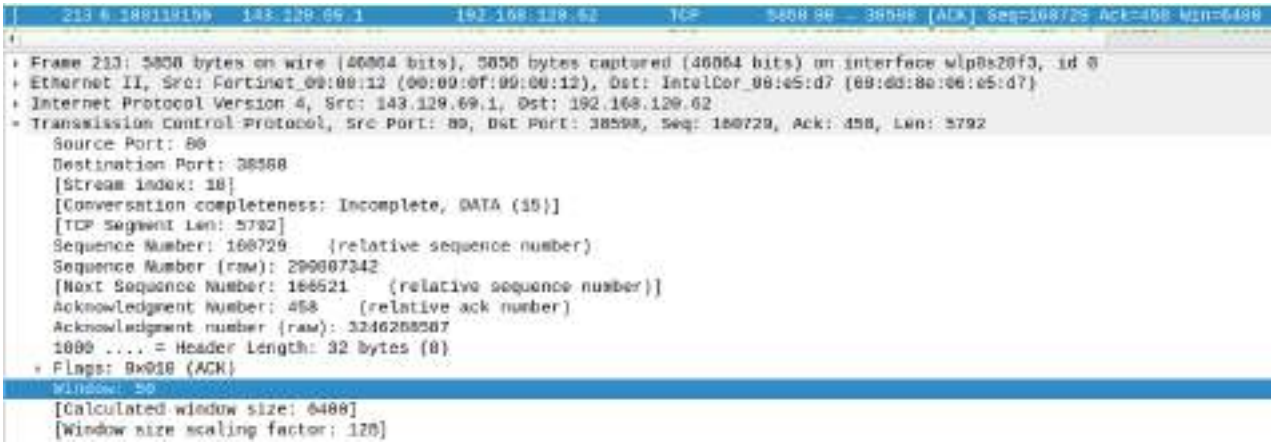
Acknowledgment number (raw): 3145061984

4. What is the length of each of the first six TCP segments?



TCP Packet 1 len = 0
TCP Packet 2 len = 0
TCP Packet 3 len = 0
HTTP packet len = 457
TCP Packet 4 len = 0
TCP Packet 5 len = 2896
TCP Packet 6 len = 0

5. What is the minimum amount of available buffer space advertised at the received for the entire trace?

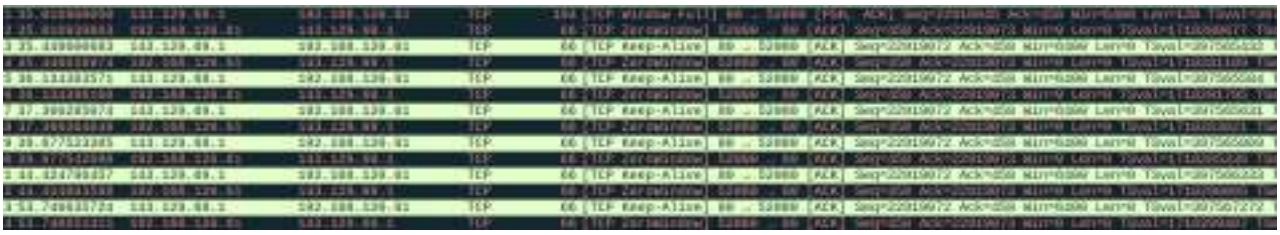


imum amount of buffer space advertised at the received for the entire trace is **50**

6. What did you observe in the packet trace when you pause the downloading in between?

   Ans:

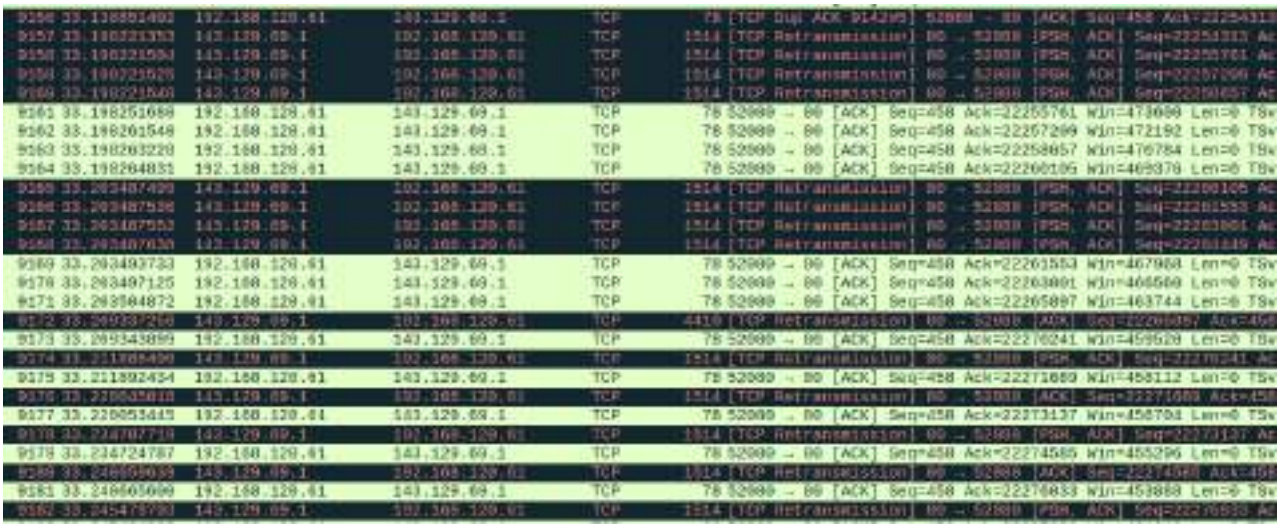
   When the download was paused in between I observed a stream of TCP Keep-Alive, TCP Window Full and TCP ZeroWindow packets.



7. Are there any TCP Out-Of-Order and/or TCP Fast Retransmission segments on the collected trace? Discuss?

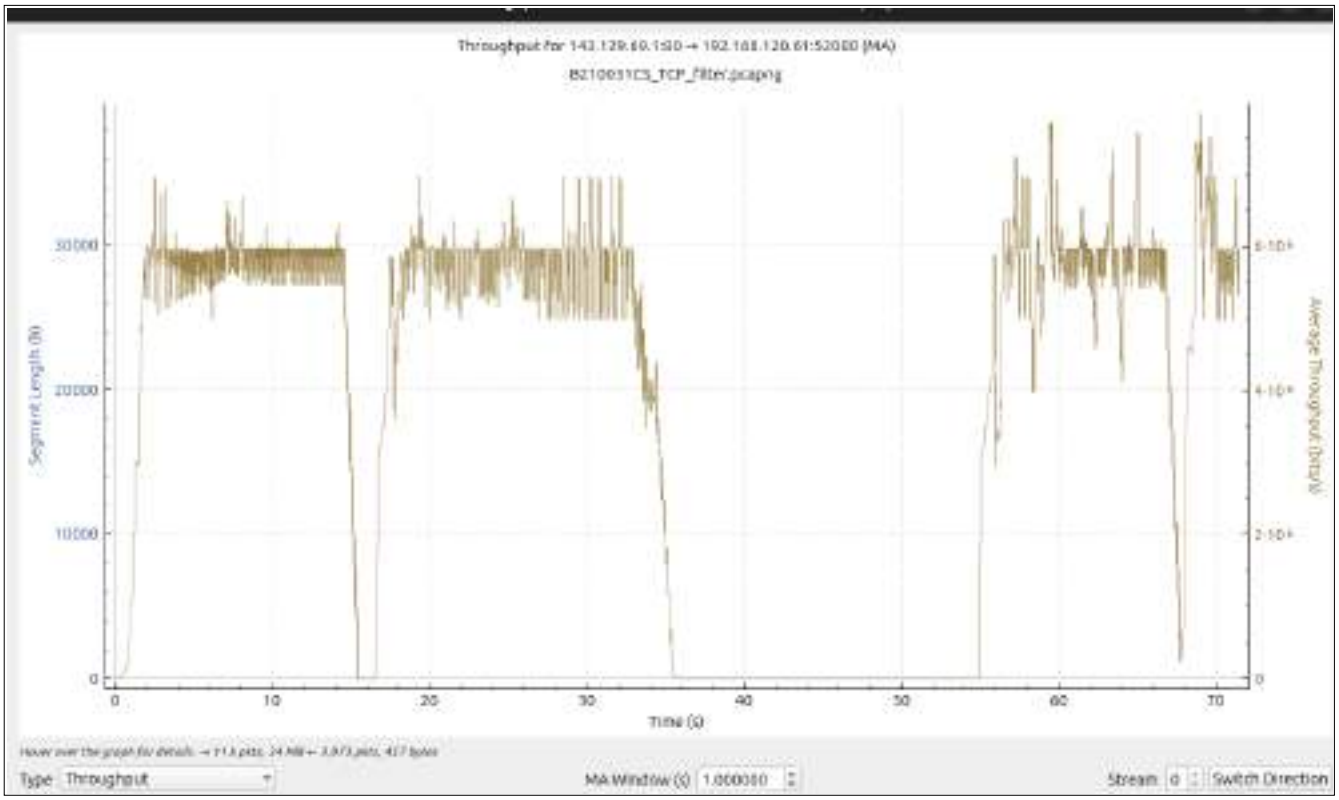
   Ans:

There are no tcp out-of-order and/or tcp-fast retransmission segments rather there is tcp-retransmission segments which indicate packet loss during the process. (as seen from image below)



8. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value. In addition, add the screenshot by doing the following step:Select one of the TCP segments, then select the menu : Statistics->TCP Stream Graph-> Throughput.

   The maximum throughput value for the TCP connection is approximately **7.842* 10^6 bits/s.** (We get this value by observing the highest value from the graph below)



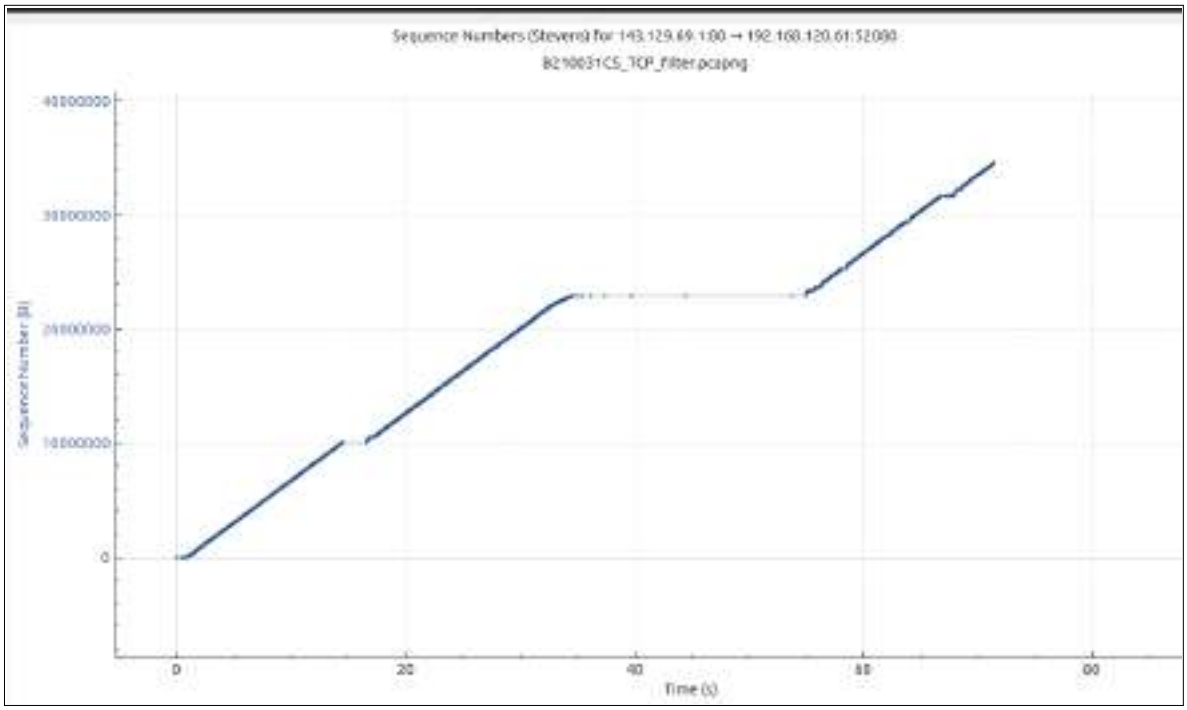
9. Select one of the TCP segments, then select the menu : Statistics->TCP Stream Graph-> Time-SequenceGraph (Stevens). From the graph answer the questions below:
    1. Where and when the slow start phase begins and ends (also attach the zoomed plot)? You can zoom the graph and see it.

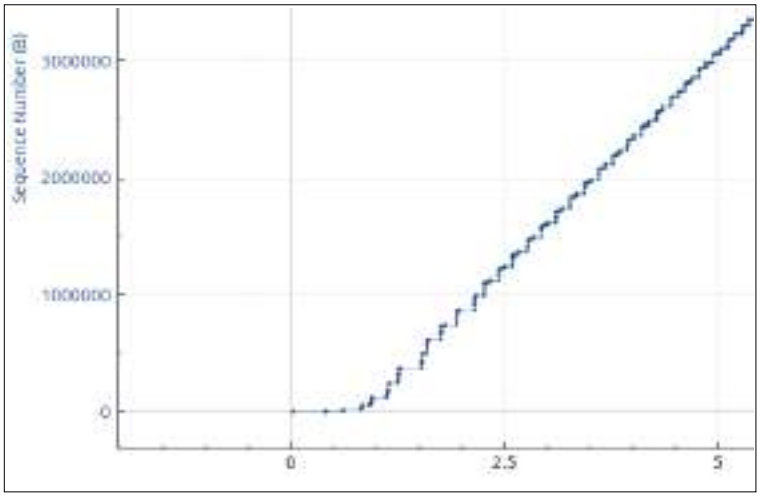
       Ans:

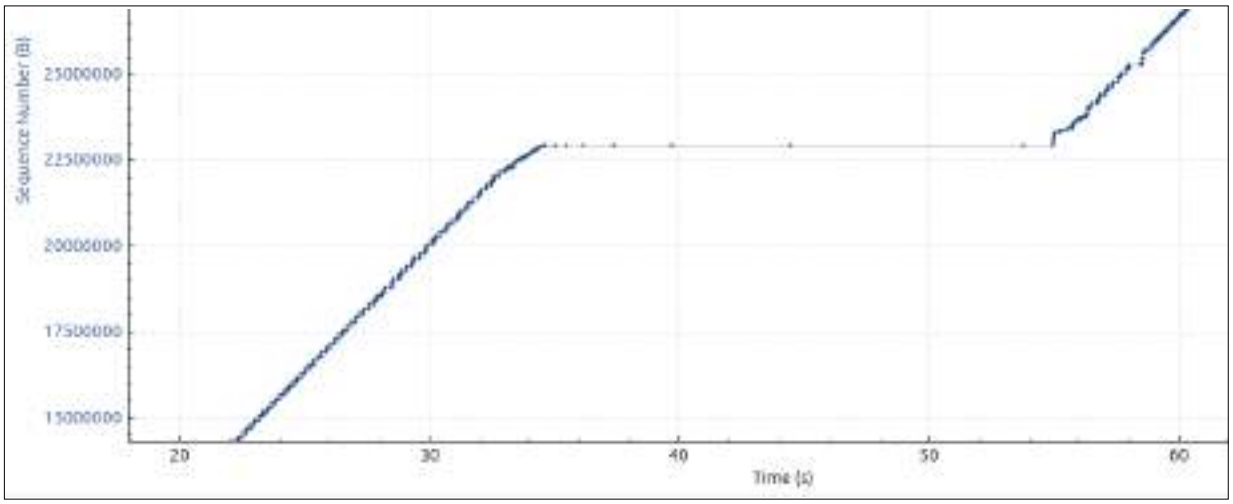
       The slow start phase is an initial phase in the TCP congestion control algorithm (begins at the start of the TCP connection or after a period of idle time where no segments are being transmitted.) It is designed to gradually increase the sending rate of data packets from the sender to probe the available network capacity and avoid overwhelming the network with traffic.

The end of the slow start phase is marked by the sender reaching either the congestion avoidance threshold or experiencing congestion, whichever comes first

From the graph, the slow start phase begins at around **1 second** and the slow end phase ends at around **32 seconds.**





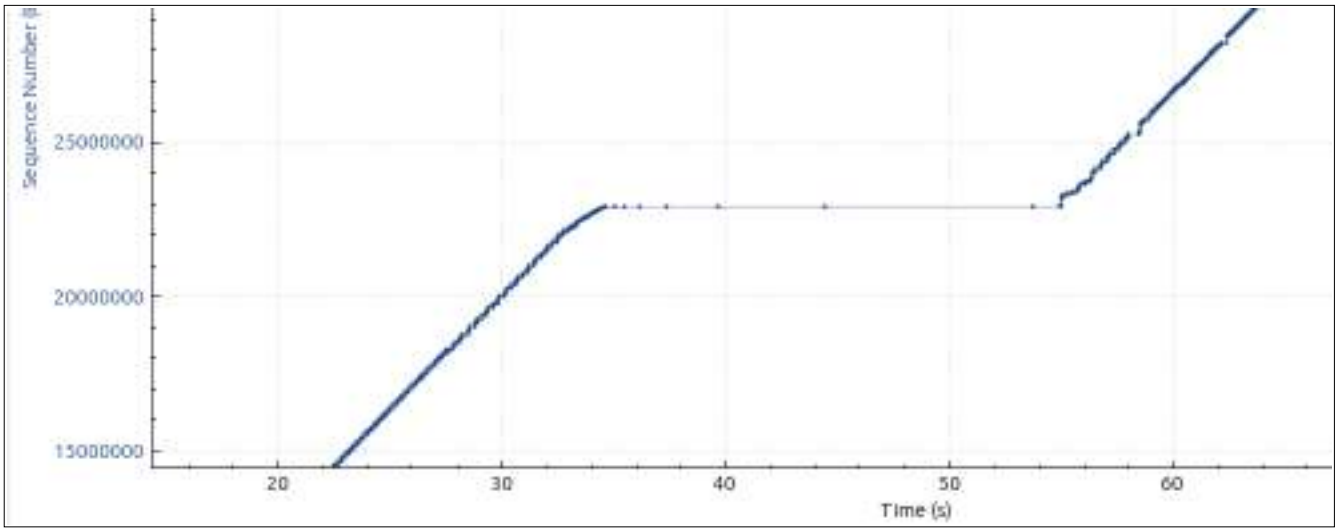


2. Where and when congestion avoidance takes over? You can zoom the graph and see it.

Ans:

Congestion avoidance takes place after the slow start phase in the TCP congestion control algorithm. Once the sender's congestion window size reaches a predefined threshold known as the congestion avoidance threshold, the congestion avoidance phase begins.

In the graph below, Congestion avoidance takes over at around **55 seconds**.



PLAGIARISM STATEMENT

I certify that this assignment/report is my own work, based on my personal study and/or research on my personal/lab equipment and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@NITC. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.

Name:Serena Anthony

Date:17/04/2024

Signature: S.A