Assignment – 3 (TCP)

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

The packet ids are 0xd702,0x0000 and 0xd703.

1. 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/?

A.

Sequence number of the TCP SYN segment used for connection initiation
is 0.

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

A. Sequence number of the TCP SYN /ACK segment sent by server to client
   is 0.
   Acknowledgement field value in the SYN/ACK segment is 1.

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.1.15	143.129.69.1	TCP	74	52920 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1901704.
2 0.190669061	143.129.69.1	192.168.1.15	TCP	74	80 → 52920 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
3 0.190742347	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1901704631 TSecr=132
4 0.191092598	192.168.1.15	143.129.69.1	HTTP	550	GET /data/webdocs.dat.gz HTTP/1.1
5 0.349309554	143.129.69.1	192.168.1.15	TCP	66	80 → 52920 [ACK] Seq=1 Ack=485 Win=30080 Len=0 TSval=1322289462 TSecr=1
6 0.556116541	143.129.69.1	192.168.1.15	TCP	14266	80 → 52920 [ACK] Seq=1 Ack=485 Win=30080 Len=14200 TSval=1322289569 TSe

▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp8s0, id 0
▶ Ethernet II, Src: Serverco_19:98:f0 (b4:a7:c6:19:98:f0), Dst: IntelCor_71:fa:4d (b8:9a:2a:71:fa:4d)
▶ Internet Protocol Version 4, Src: 143.129.69.1, Dst: 192.168.1.15
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 52920, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 52920
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0   (relative sequence number)
    Sequence Number (raw): 161164584
    [Next Sequence Number: 1   (relative sequence number)]
    Acknowledgment Number: 1   (relative ack number)
    Acknowledgment number (raw): 3701405470
    1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x012 (SYN, ACK)
    Window: 28960
    [Calculated window size: 28960]
    Checksum: 0x6971 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]

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

A. The length of each of the first six TCP segments are 74,74,66,66,14266
   and 66 bytes respectively.

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.1.15	143.129.69.1	TCP	74	52920 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1901704.
2 0.190669061	143.129.69.1	192.168.1.15	TCP	74	80 → 52920 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
3 0.190742347	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1901704631 TSecr=132
4 0.191092598	192.168.1.15	143.129.69.1	HTTP	550	GET /data/webdocs.dat.gz HTTP/1.1
5 0.349309554	143.129.69.1	192.168.1.15	TCP	66	80 → 52920 [ACK] Seq=1 Ack=485 Win=30080 Len=0 TSval=1322289462 TSecr=1
6 0.556116541	143.129.69.1	192.168.1.15	TCP	14266	80 → 52920 [ACK] Seq=1 Ack=485 Win=30080 Len=14200 TSval=1322289569 TSe
7 0.556205785	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=485 Ack=14201 Win=50176 Len=0 TSval=1901704997 TSe
8 0.759438770	143.129.69.1	192.168.1.15	TCP	11426	80 → 52920 [ACK] Seq=14201 Ack=485 Win=30080 Len=11360 TSval=1322289825
9 0.759562707	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=485 Ack=25561 Win=48768 Len=0 TSval=1901705200 TSe

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

A. Minimum amount of available buffer space advertised at the received for the entire trace is 28960 bytes

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.1.15	143.129.69.1	TCP	74	52920 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1901704.
2 0.190669061	143.129.69.1	192.168.1.15	TCP	74	80 → 52920 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
3 0.190742347	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1901704631 TSecr=132
4 0.191092598	192.168.1.15	143.129.69.1	HTTP	550	GET /data/webdocs.dat.gz HTTP/1.1
5 0.349309554	143.129.69.1	192.168.1.15	TCP	66	80 → 52920 [ACK] Seq=1 Ack=485 Win=30080 Len=0 TSval=1322289462 TSecr=1
6 0.556116541	143.129.69.1	192.168.1.15	TCP	14266	80 → 52920 [ACK] Seq=1 Ack=485 Win=30080 Len=14200 TSval=1322289569 TSe
7 0.556205785	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=485 Ack=14201 Win=50176 Len=0 TSval=1901704997 TSe
8 0.759438770	143.129.69.1	192.168.1.15	TCP	11426	80 → 52920 [ACK] Seq=14201 Ack=485 Win=30080 Len=11360 TSval=1322289825
9 0.759562707	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=485 Ack=25561 Win=48768 Len=0 TSval=1901705200 TSe

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

A. When I paused the download mid-TCP connection, I observed packets such as Window-Full, Zero Window, Keep Alive, and Window Update indicating flow control and congestion management in the network communication.

No.	Time	Source	Destination	Protocol	Length	Info
2425	32.068266170	143.129.69.1	192.168.1.15	TCP	21366	80 → 52920 [ACK] Seq=13964281 Ack=485 Win=30080 Len=21300 TSval=13
2426	32.068346424	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=485 Ack=13985581 Win=1280 Len=0 TSval=1901736
2427	32.704583474	143.129.69.1	192.168.1.15	TCP	1346	[TCP Window Full] 80 → 52920 [PSH, ACK] Seq=13985581 Ack=485 Win=3
2428	32.704651785	192.168.1.15	143.129.69.1	TCP	66	[TCP ZeroWindow] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=0 Len=0
2429	33.322639169	143.129.69.1	192.168.1.15	TCP	66	[TCP Keep-Alive] 80 → 52920 [ACK] Seq=13986860 Ack=485 Win=30080 L
2430	33.322700188	192.168.1.15	143.129.69.1	TCP	66	[TCP ZeroWindow] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=0 Len=0
2431	34.285998123	143.129.69.1	192.168.1.15	TCP	66	[TCP Keep-Alive] 80 → 52920 [ACK] Seq=13986860 Ack=485 Win=30080 L
2432	34.286075361	192.168.1.15	143.129.69.1	TCP	66	[TCP ZeroWindow] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=0 Len=0
2433	36.088143840	143.129.69.1	192.168.1.15	TCP	66	[TCP Keep-Alive] 80 → 52920 [ACK] Seq=13986860 Ack=485 Win=30080 L
2434	36.088202779	192.168.1.15	143.129.69.1	TCP	66	[TCP ZeroWindow] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=0 Len=0
2435	39.773906953	143.129.69.1	192.168.1.15	TCP	66	[TCP Keep-Alive] 80 → 52920 [ACK] Seq=13986860 Ack=485 Win=30080 L
2436	39.773967698	192.168.1.15	143.129.69.1	TCP	66	[TCP ZeroWindow] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=0 Len=0
2437	41.919677920	192.168.1.15	143.129.69.1	TCP	66	[TCP Window Update] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=1817
2438	41.931270658	192.168.1.15	143.129.69.1	TCP	66	[TCP Window Update] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=3880
2439	41.932839203	192.168.1.15	143.129.69.1	TCP	66	[TCP Window Update] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=7879
2440	41.936258966	192.168.1.15	143.129.69.1	TCP	66	[TCP Window Update] 52920 → 80 [ACK] Seq=485 Ack=13986861 Win=1577
2441	42.129229030	143.129.69.1	192.168.1.15	TCP	5746	80 → 52920 [ACK] Seq=13986861 Ack=485 Win=30080 Len=5680 TSval=132
2442	42.129311215	192.168.1.15	143.129.69.1	TCP	66	52920 → 80 [ACK] Seq=485 Ack=13992541 Win=1577984 Len=0 TSval=1901
2443	42.129229354	143.129.69.1	192.168.1.15	TCP	8586	80 → 52920 [ACK] Seq=13992541 Ack=485 Win=30080 Len=8520 TSval=132

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

A. The collected trace reveals TCP out-of-order segments and TCP fast re-transmissions.
   Out-of-order segments may stem from network congestion or routing changes, while fast re-transmissions occur due to detected packet loss. These issues indicate potential network instability.

No.	Time	Source	Destination	Protocol	Length	Info
68	1.788662538	143.129.69.1	192.168.1.15	TCP	5746	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=363521 Ack=485 Win=30080 L
70	1.788757801	143.129.69.1	192.168.1.15	TCP	17106	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=369201 Ack=485 Win=30080 L
272	3.169148766	143.129.69.1	192.168.1.15	TCP	15686	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1306401 Ack=485 Win=30080
274	3.171044788	143.129.69.1	192.168.1.15	TCP	5746	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1322021 Ack=485 Win=30080
276	3.172392903	143.129.69.1	192.168.1.15	TCP	28466	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1327701 Ack=485 Win=30080
278	3.172506204	143.129.69.1	192.168.1.15	TCP	11426	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1356101 Ack=485 Win=30080
280	3.302002293	143.129.69.1	192.168.1.15	TCP	1486	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1367461 Ack=485 Win=30080
282	3.324438056	143.129.69.1	192.168.1.15	TCP	11426	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1368881 Ack=485 Win=30080
284	3.324598171	143.129.69.1	192.168.1.15	TCP	5746	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1380241 Ack=485 Win=30080
285	3.324598239	143.129.69.1	192.168.1.15	TCP	1486	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1385921 Ack=485 Win=30080
288	3.326383687	143.129.69.1	192.168.1.15	TCP	2906	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1478221 Ack=485 Win=30080
401	4.603291921	143.129.69.1	192.168.1.15	TCP	2906	[TCP Fast Retransmission] 80 → 52920 [ACK] Seq=1946821 Ack=485 Win
403	4.603862837	143.129.69.1	192.168.1.15	TCP	2906	[TCP Out-Of-Order] 80 → 52920 [PSH, ACK] Seq=1949661 Ack=485 Win=3
405	4.603862936	143.129.69.1	192.168.1.15	TCP	2906	[TCP Out-Of-Order] 80 → 52920 [ACK] Seq=1952501 Ack=485 Win=30080

7. 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.

A.

Throughput for 143.129.69.1:80 → 192.168.1.15:52920 (MA)

B210437CS_TCP_Filter.pcapng
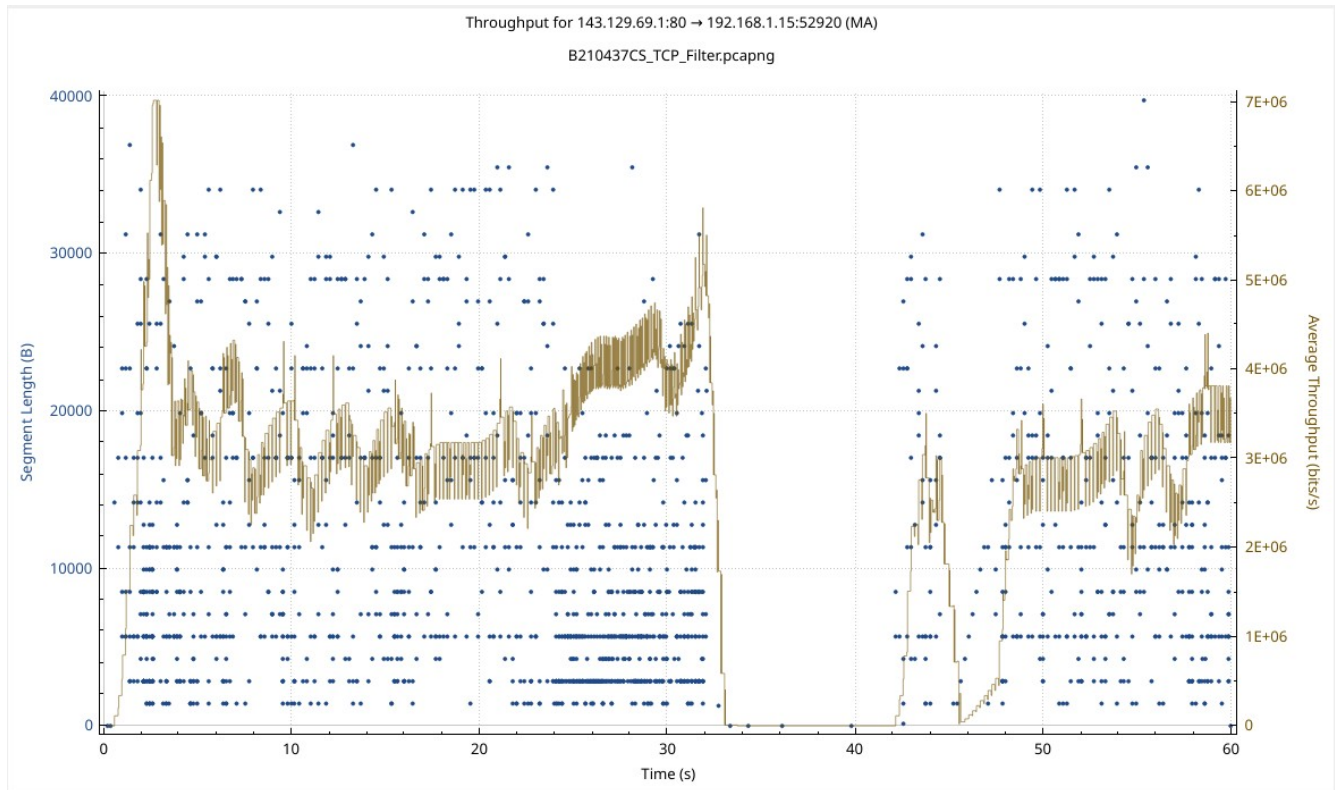
To determine the throughput for a TCP connection, I first measured the total amount of data transferred during the connection and then calculated the time taken for the transfer to occur. Once I had these two values, I divided the amount of data transferred by the time taken to get the throughput.

The TCP connection started with a sequence number of 0 at 0 seconds and ended with a sequence number of 19564761 at 59.69 seconds. Calculating the

difference between the sequence numbers and dividing by the time elapsed yields an average throughput of approximately 0.327X10^6 bytes per second.

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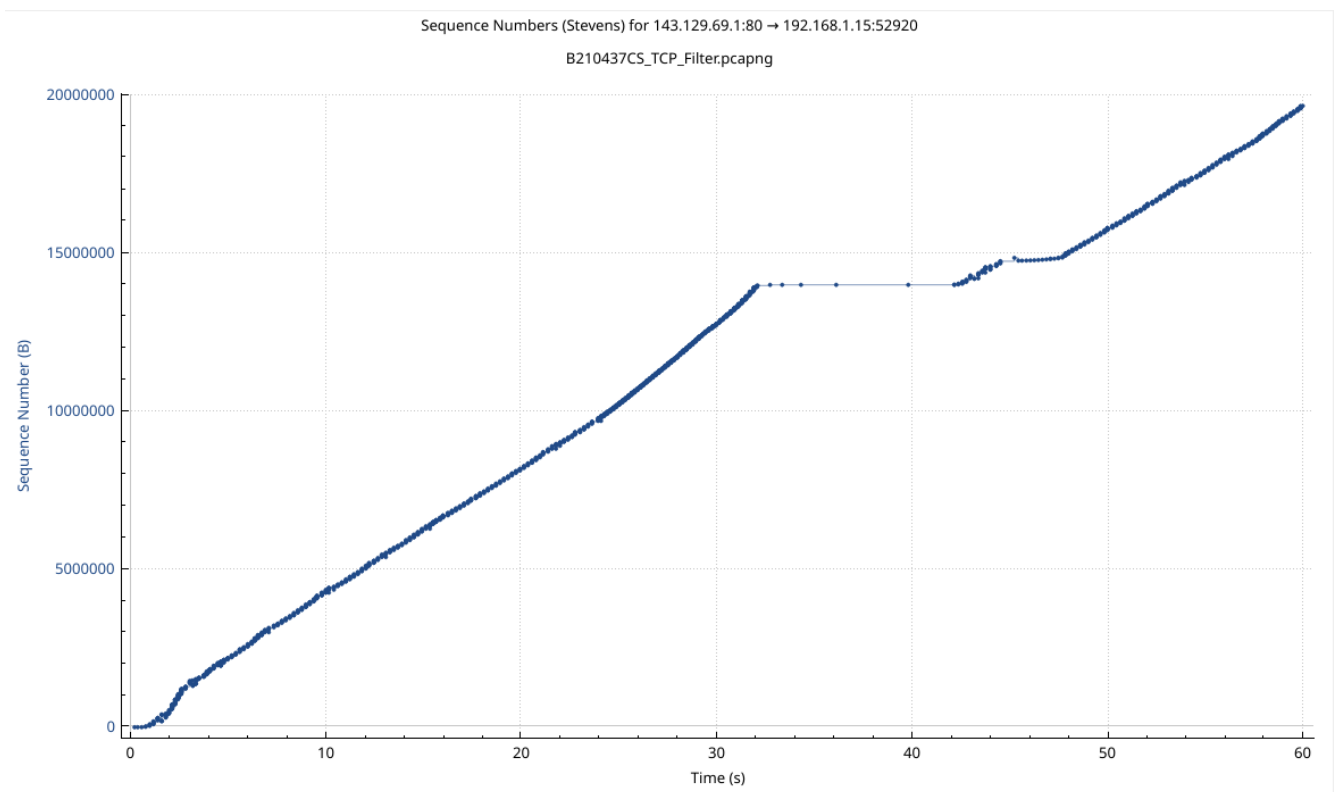
A.

The slow start phase begins when a connection is established, i.e., at 0 seconds, and continues until approximately 3 seconds.

Click to select packet 259 (2.805s len 22720 seq 1283681 ack 485 win 30080) → 1,7
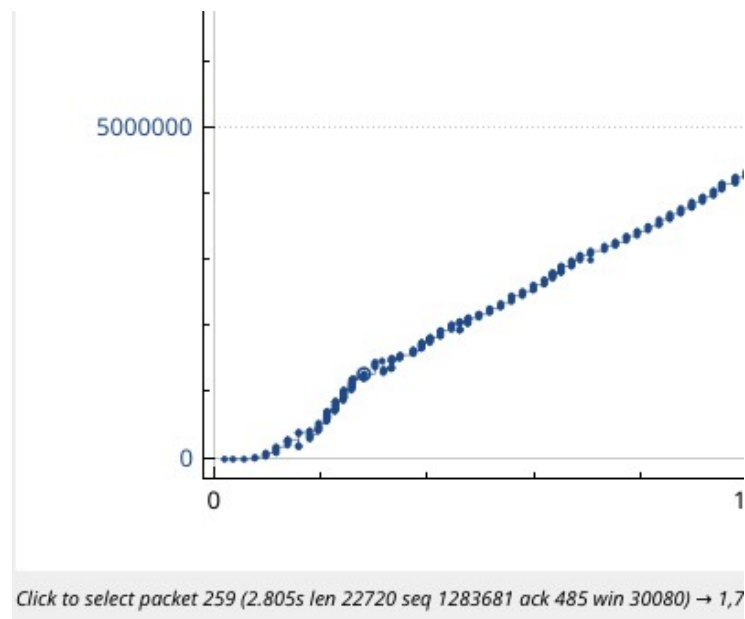
b. Where and when congestion avoidance takes over? You can zoom the graph and see it.

A.

Congestion avoidance takes over after the slow start phase, which lasts approximately 3 seconds, and continues until 32.07 seconds.

15000000

30

Click to select packet 2425 (32.07s len 21300 seq 13964281 ack 485 win 30080) →

Sequence Numbers (Stevens) for 143.129.69.1:80 → 192.168.1.15:52920

B210437CS_TCP_Filter.pcapng
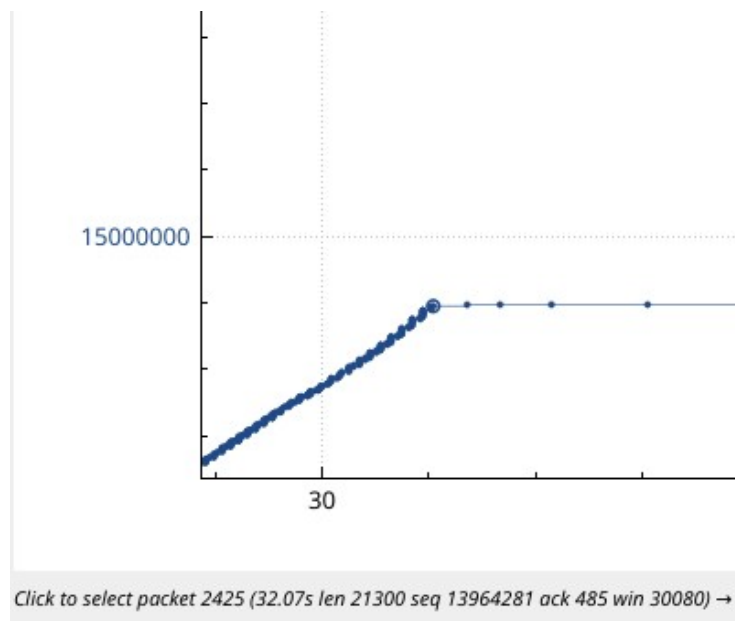
PLAGIARISM STATEMENT

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: Vedurupaka Venkata Sai

Date: 17-Apr-2024

Signature: Vedurupaka Venkata Sai