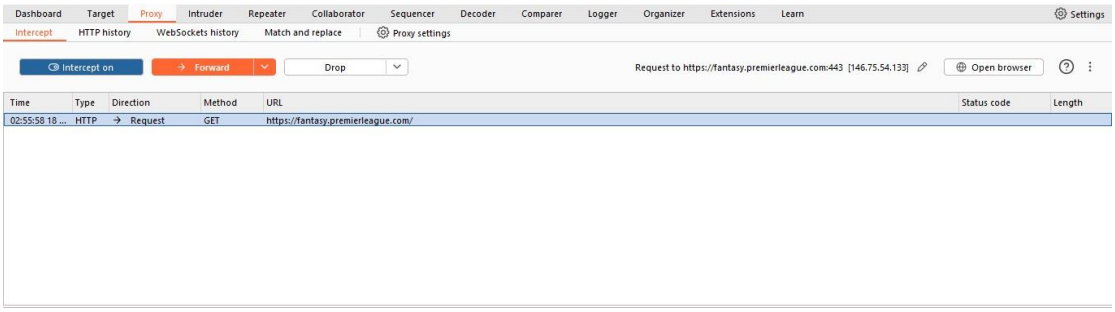
Networks

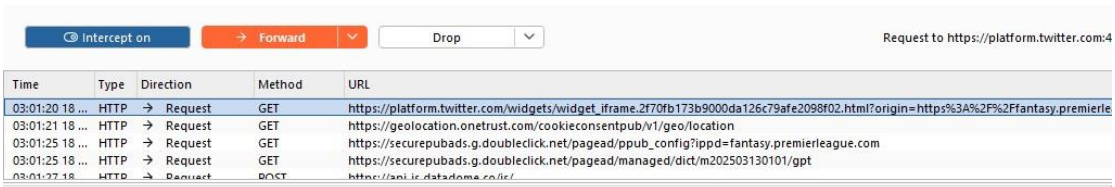
Lab 2

Name: مصطفى محمد رأفت عبد اللطيف
ID:20011947
Section : 1

Part I:
Introduction to Burp Suite and HTTP Interception:
GET Request to



Request Header :



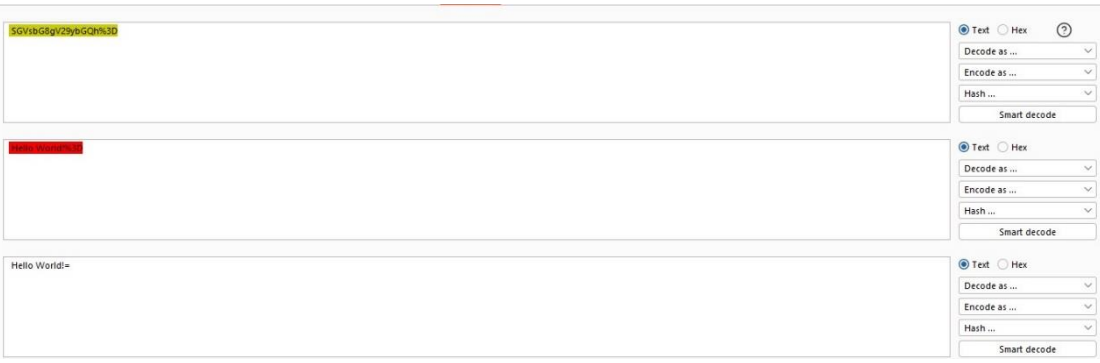
Part 2: Using Burp Decoder:

1-Encoded Input: SGVsbG8gd29ybGQh (Base64 encoded)

The Output:

2- Double encoded Input: SGVsbG8gV29ybGQh%3D (URL and base64 encoded)

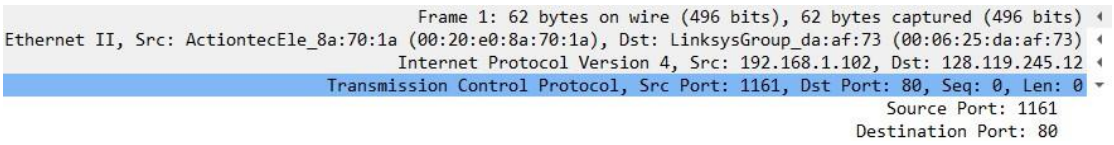
The Output:



TCP Lab:

Part I: A first look at the captured trace

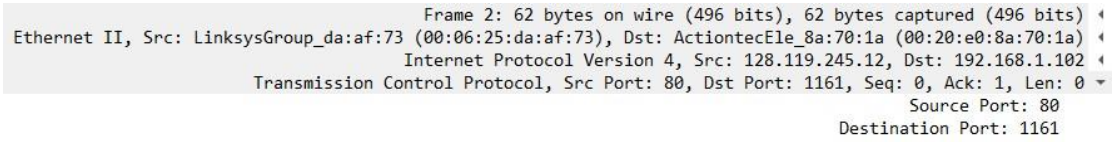
1-What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?



the IP address of source:192.168.1.102

TCP port number of source:1161

2-What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

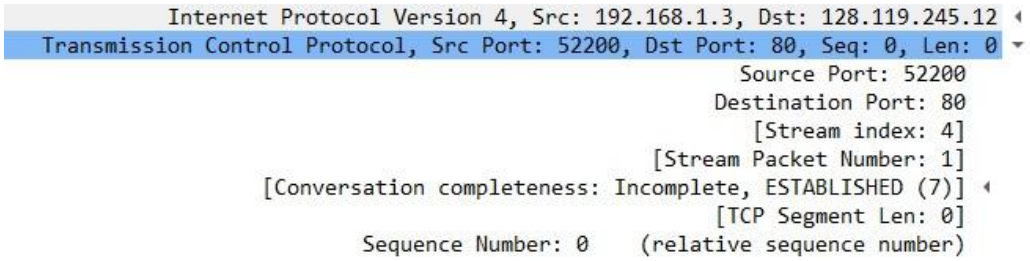


the IP address of gaia.cs.umass.edu:128.119.245.12

TCP sending port number of gaia.cs.umass.edu:80

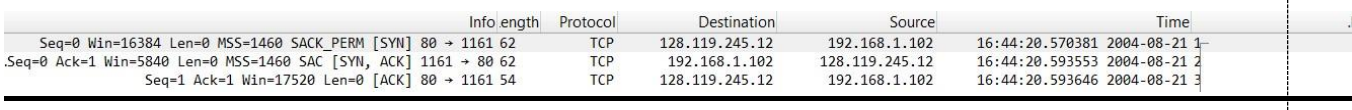
TCP receiving port number of gaia.cs.umass.edu:1161

3- What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?
source TCP port : 52200
IP:192.168.1.3



Part II:TCP basics:

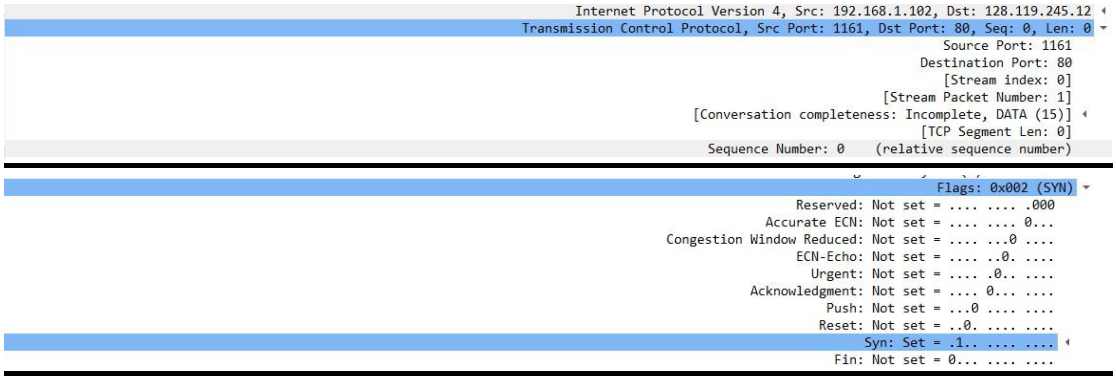
TCP Connection initiation:



4- 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 of the TCP SYN=0

Flags segment identifies it as a SYN segment as syn is set



5-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

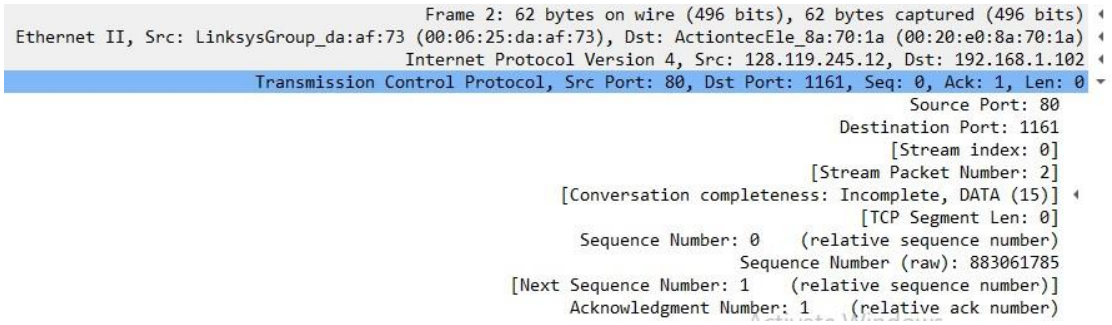
the segment that identifies the segment as a SYNACK segment?

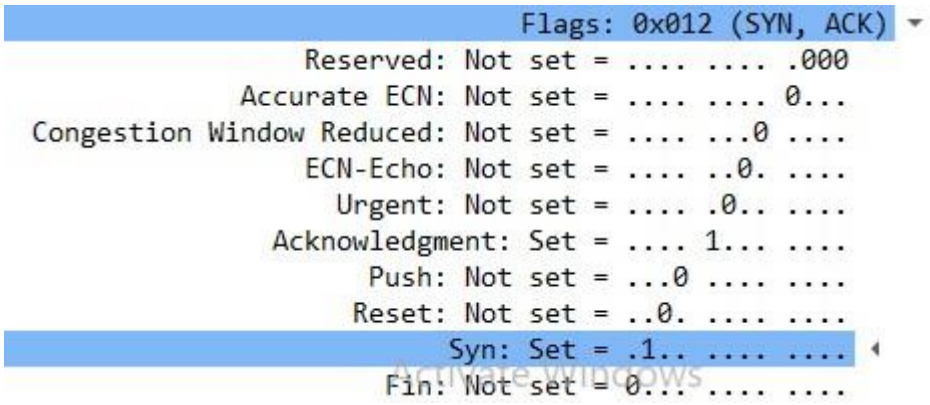
sequence number of the SYNACK segment: 0

Acknowledgement field in the SYNACK segment :1

Ack = Client's Initial Sequence Number + 1

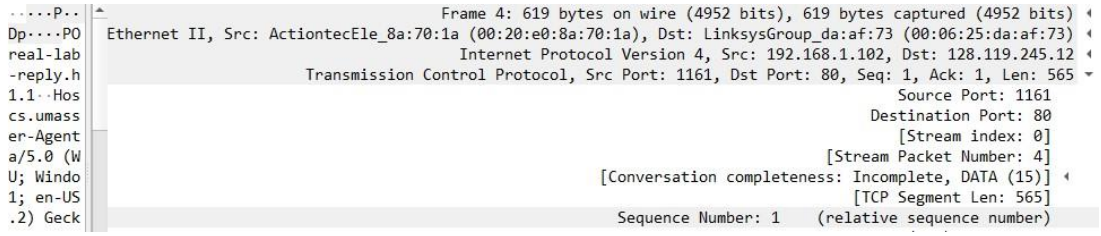
Flags segment identifies it as a SYNACK segment as Syn, Acknowledgement are set.





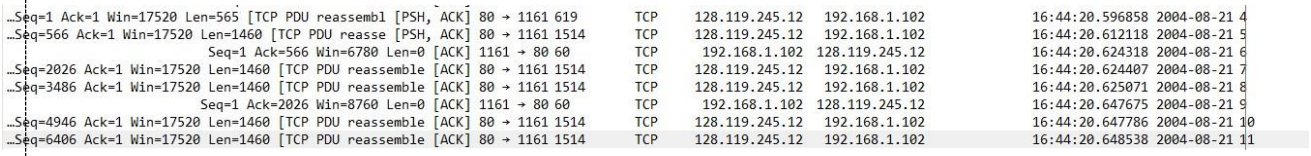
6- What is the sequence number of the TCP segment containing the HTTP POST command?

Seq number :1



7-What are the sequence numbers of the first six

segments in the TCP connection At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments?



…Seq=1 Ack=1 Win=17520 Len=565 [TCP PDU reassembl [PSH, ACK] 80 → 1161 619	TCP	128.119.245.12	192.168.1.102	16:44:20.596858 2004-08-21 4
…Seq=566 Ack=1 Win=17520 Len=1460 [TCP PDU reasse [PSH, ACK] 80 → 1161 1514	TCP	128.119.245.12	192.168.1.102	16:44:20.612118 2004-08-21 5
Seq=1 Ack=566 Win=6780 Len=0 [ACK] 1161 → 80 60	TCP	192.168.1.102	128.119.245.12	16:44:20.624318 2004-08-21 6
…Seq=2026 Ack=1 Win=17520 Len=1460 [TCP PDU reassemble [ACK] 80 → 1161 1514	TCP	128.119.245.12	192.168.1.102	16:44:20.624407 2004-08-21 7
…Seq=3486 Ack=1 Win=17520 Len=1460 [TCP PDU reassemble [ACK] 80 → 1161 1514	TCP	128.119.245.12	192.168.1.102	16:44:20.625071 2004-08-21 8
Seq=1 Ack=2026 Win=8760 Len=0 [ACK] 1161 → 80 60	TCP	192.168.1.102	128.119.245.12	16:44:20.647675 2004-08-21 9
…Seq=4946 Ack=1 Win=17520 Len=1460 [TCP PDU reassemble [ACK] 80 → 1161 1514	TCP	128.119.245.12	192.168.1.102	16:44:20.647786 2004-08-21 10
…Seq=6406 Ack=1 Win=17520 Len=1460 [TCP PDU reassemble [ACK] 80 → 1161 1514	TCP	128.119.245.12	192.168.1.102	16:44:20.648538 2004-08-21 11

Sequence number of Segment no 1: 1
Sequence number of Segment no 2: 566
Sequence number of Segment no 3: 2026
Sequence number of Segment no 4: 3486
Sequence number of Segment no 5: 4946
Sequence number of Segment no 6: 6406

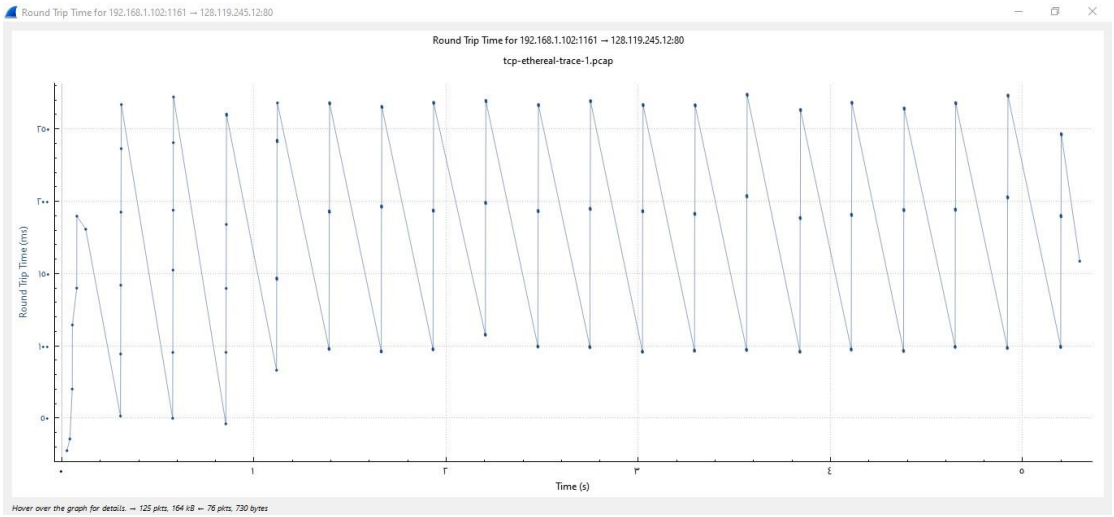
Time of Segment no 1 sent: 0.026477000 s
Time of Segment no 2 sent: 0.041737000 s
Time of Segment no 3 sent: 0.054026000 s
Time of Segment no 4 sent: 0.054690000 s
Time of Segment no 5 sent: 0.077405000 s
Time of Segment no 6 sent: 0.078157000 s

Time of Ack for Segment no 1 received: 0.053937000 s
Time of Ack for Segment no 2 received: 0.077294000 s
Time of Ack for Segment no 3 received: 0.124085000 s
Time of Ack for Segment no 4 received: 0.169118000 s
Time of Ack for Segment no 5 received: 0.217299000 s
Time of Ack for Segment no 6 received: 0.267802000 s

RTT of segment no 1 : 0.027460 s
RTT of segment no 2 : 0.035557 s

RTT of segment no 3 : 0.070059 s
RTT of segment no 4 : 0.114430 s
RTT of segment no 5 : 0.139890 s
RTT of segment no 6 : 0.189640 s

RTT graph:



Rule
EstimatedRTT = (1-0.125) * EstimatedRTT + 0.125 * SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1:
EstimatedRTT = RTT for Segment 1 = 0.02746 s

EstimatedRTT after the receipt of the ACK of segment 2:
EstimatedRTT = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.028472125 s

EstimatedRTT after the receipt of the ACK of segment 3:
EstimatedRTT = 0.875 * 0.028472125 + 0.125 * 0.070059 = =0.03367048438 s
EstimatedRTT after the receipt of the ACK of segment 4:
EstimatedRTT = 0.875 *0.03367048438 + 0.125 * 0.11443 = 0.04376542383 s

EstimatedRTT after the receipt of the ACK of segment 5:
EstimatedRTT = 0.875 * 0.04376542383 + 0.125 * 0.13989 = 0.05578099585 s
EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT = 0.875 * 0.055827 + 0.125 * 0.18964 = 0.07251337137 s

8-What is the length of each of the first six TCP segments?

Length of Segment no 1: 565 bytes
Length of Segment no 2: 1460 bytes
Length of Segment no 3: 1460 bytes
Length of Segment no 4: 1460 bytes
Length of Segment no 5: 1460 bytes
Length of Segment no 6: 1460 bytes

9- What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

min : 5840
max : 15720

Check if there's a tcp.window_size == 0
there's no lack

10- Are there any retransmitted segments in the trace file? What did you check for?

there is no transmitted segments in the trace file
check if there is any duplicated sequence number.

11- How much data does the receiver typically

acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment?

Check how much the acknowledgment number increases between successive ACKs

1st ACK : 566 , 2nd ACK : 2026 the difference = 1460
2nd ACK : 1460 , 3rd ACK : 3486 the difference = 1460
3rd ACK : 3486 , 4th ACK : 4946 the difference = 1460
4th ACK : 4946 , 5th ACK : 6406 the difference = 1460
5th ACK : 6406 , 6th ACK : 7866 the difference = 1460

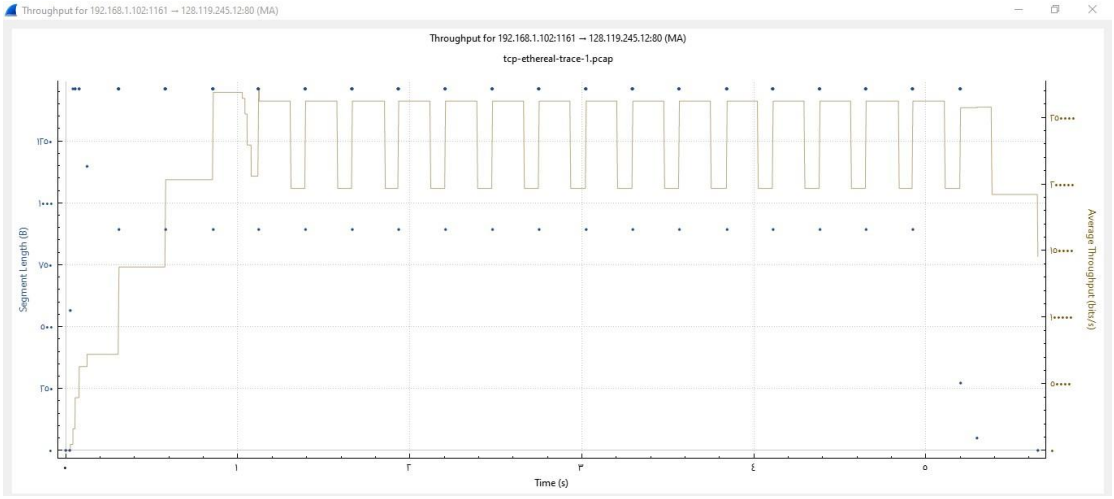
12- What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

throughput = total data sent in Tcp segment / total transmission time

Total data sent = last acked TCP sequence number– sequence number for first TCP =164091-1=164090 bytes

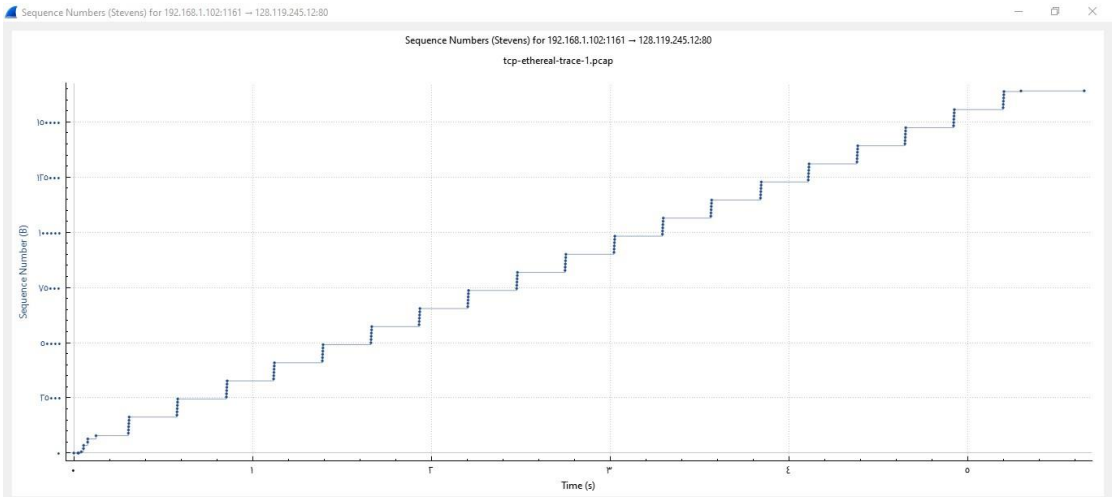
Total transmission time = First TCP sent time – Last Acknowledge sent time = 5.45583- 0.02746 =5.42837 sec

throughput = 164090 / 5.42837= 30.22822 KBps



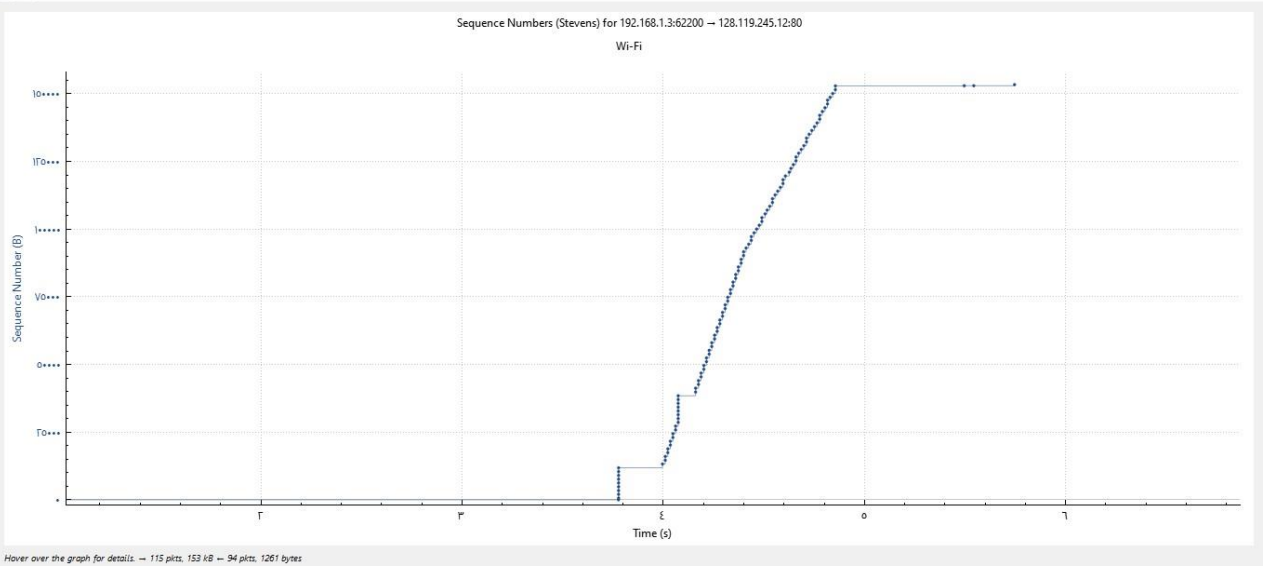
Part III: TCP congestion control in action

13- Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.



slowstart starts at 0 time and ends at 0.125s

14- Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu


Sequence Numbers (Stevens) for 192.168.1.3:62200 → 128.119.245.12:80
Wi-Fi
Sequence Number (B)
Time (s)
Hover over the graph for details. → 115 pkts, 153 kB ← 94 pkts, 1261 bytes