

Networks

Lab 2

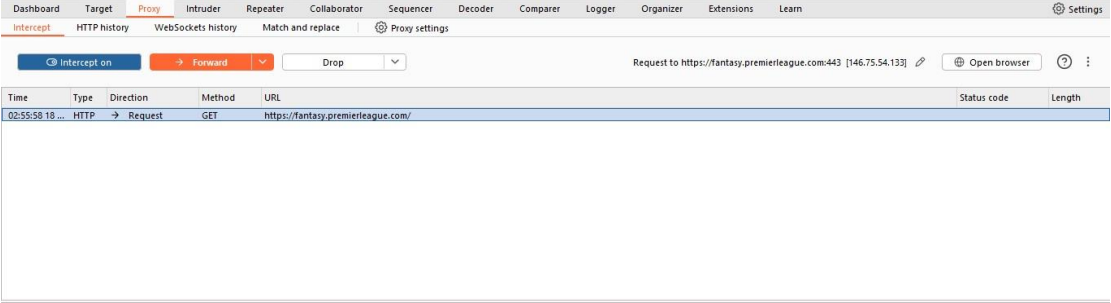
Name: مصطفى محمد رأفت عبد اللطيف

ID:20011947

Section : 1

Part I:

Introduction to Burp Suite and HTTP Interception: GET Request to



Request Header :

Time	Type	Direction	Method	URL
02:55:58 18...	HTTP	→ Request	GET	https://fantasy.premierleague.com/

Request

PrettyRawHex

1GET / HTTP/1.1

2Host: fantasy.premierleague.com

3Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"

4Sec-Ch-Ua-Mobile: ?0

5Sec-Ch-Ua-Platform: "Windows"

6Accept-Language: en-US,en;q=0.9

7Upgrade-Insecure-Requests: 1

8User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36

9Accept:

10text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11Sec-Fetch-Site: none

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Accept-Encoding: gzip, deflate, br

16Priority: u=0, i

17Connection: keep-alive

18

Intercept onForwardDrop

Request to https://platform.twitter.com:4

Time	Type	Direction	Method	URL
03:01:20 18...	HTTP	→ Request	GET	https://platform.twitter.com/widgets/widget_iframe.2f70fb173b9000da126c79afe2098f02.html?origin=https%3A%2F%2Ffantasy.premierleague.com
03:01:21 18...	HTTP	→ Request	GET	https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
03:01:25 18...	HTTP	→ Request	GET	https://securepubads.g.doubleclick.net/pagead/ppub_config?ppd=fantasy.premierleague.com
03:01:25 18...	HTTP	→ Request	GET	https://securepubads.g.doubleclick.net/pagead/managed/dict/m202503130101/gpt
03:01:27 18...	HTTP	→ Request	POST	https://api.ic.datadome.co/

Request

PrettyRawHex

1GET /widgets/widget_iframe.2f70fb173b9000da126c79afe2098f02.html?origin=https%3A%2F%2Ffantasy.premierleague.com HTTP/2

2Host: platform.twitter.com

3Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"

4Sec-Ch-Ua-Mobile: ?0

5Sec-Ch-Ua-Platform: "Windows"

6Accept-Language: en-US,en;q=0.9

7Upgrade-Insecure-Requests: 1

8User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36

9Accept:

10text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11Sec-Fetch-Site: cross-site

12Sec-Fetch-Mode: navigate

13Sec-Fetch-Storage-Access: active

14Accept-Encoding: gzip, deflate, br

15Priority: u=0, i

16

Time	Type	Direction	Method	URL	Status code
03:08:39 18 Mar 2025	HTTP	→ Request	GET	https://resources.premierleague.pulselive.com/photo-resources/2025/03/17/9ec58874-24db-4c1a-9407-9760909b4867/Munoz-Haaland.jpeg?width=400&height=400	200
03:08:43 18 Mar 2025	HTTP	→ Request	POST	https://analytics.google.com/g/collect?v=2&tid=G-844XQSF4K8&utm=45je53d3h1v890755852z872357611za200zb72357611&p=1742260114086&gcd=1313131313	200

Request

```

1 GET /photo-resources/2025/03/17/9ec58874-24db-4c1a-9407-9760909b4867/Munoz-Haaland.jpeg?width=400&height=400 HTTP/2
2 Host: resources.premierleague.pulselive.com
3 Sec-CH-UA-Platform: "Windows"
4 Accept-Language: en-US,en;q=0.9
5 Sec-CH-UA: "Chromium";v="133", "Not(A:Brand";v="99"
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
7 Sec-CH-UA-Mobile: ?0
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: cross-site
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Sec-Fetch-Storage-Access: active
13 Accept-Encoding: gzip, deflate, br
14 Priority: u=4, i

```

Inspector

Request attributes

Request query parameters

Request body parameters

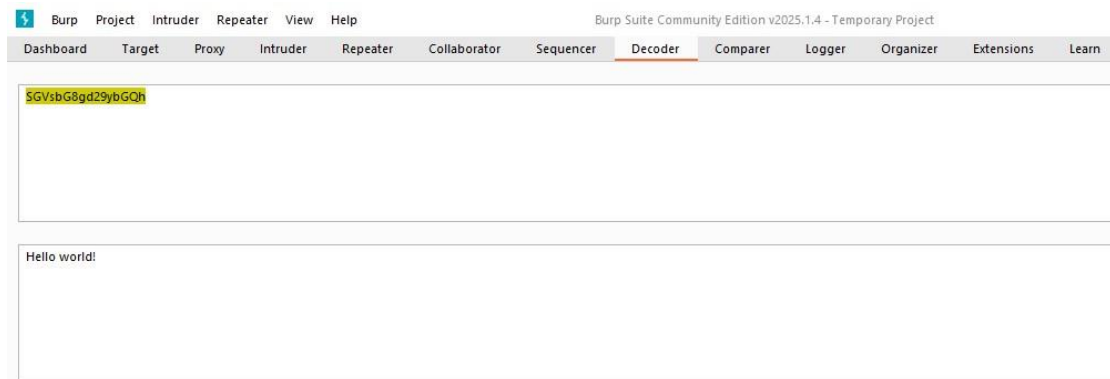
It's empty in here

Add

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?

```
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on 0  
Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)  
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0  
Source Port: 1161  
Destination Port: 80
```

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?

```
Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on 0  
Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102  
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0  
Source Port: 80  
Destination Port: 1161
```

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

```

Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52200, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 52200
    Destination Port: 80
    [Stream index: 4]
    [Stream Packet Number: 1]
    [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)

```

Part II: TCP basics:

TCP Connection initiation:

	Info	length	Protocol	Destination	Source	Time
Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM [SYN]	80 → 1161	62	TCP	128.119.245.12	192.168.1.102	16:44:20.570381 2004-08-21 1
.Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SAC [SYN, ACK]	1161 → 80	62	TCP	192.168.1.102	128.119.245.12	16:44:20.593553 2004-08-21 2
Seq=1 Ack=1 Win=17520 Len=0 [ACK]	80 → 1161	54	TCP	128.119.245.12	192.168.1.102	16:44:20.593646 2004-08-21 3

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

```

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Flags: 0x002 (SYN)
        Reserved: Not set = ... ..000
        Accurate ECN: Not set = ... ..0...
        Congestion Window Reduced: Not set = ... ..0...
        ECN-Echo: Not set = ... ..0...
        Urgent: Not set = ... ..0...
        Acknowledgment: Not set = ... ..0...
        Push: Not set = ... ..0...
        Reset: Not set = ... ..0...
        Syn: Set = ... ..1...
        Fin: Not set = ... ..0...

```

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.

```
Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on 0
Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [Stream Packet Number: 2]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 883061785
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)

Flags: 0x012 (SYN, ACK)
    Reserved: Not set = .... .000
    Accurate ECN: Not set = .... .0...
    Congestion Window Reduced: Not set = .... .0...
    ECN-Echo: Not set = .... .0. ....
    Urgent: Not set = .... .0.. ....
    Acknowledgment: Set = .... 1... ....
    Push: Not set = ...0 .... ....
    Reset: Not set = ..0. .... ....
    Syn: Set = .1.. .... ....
    Fin: Not set = 0... .... ....
```

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

Seq number :1

```
Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on 0
Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 4]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 565]
    Sequence Number: 1 (relative sequence number)
```

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

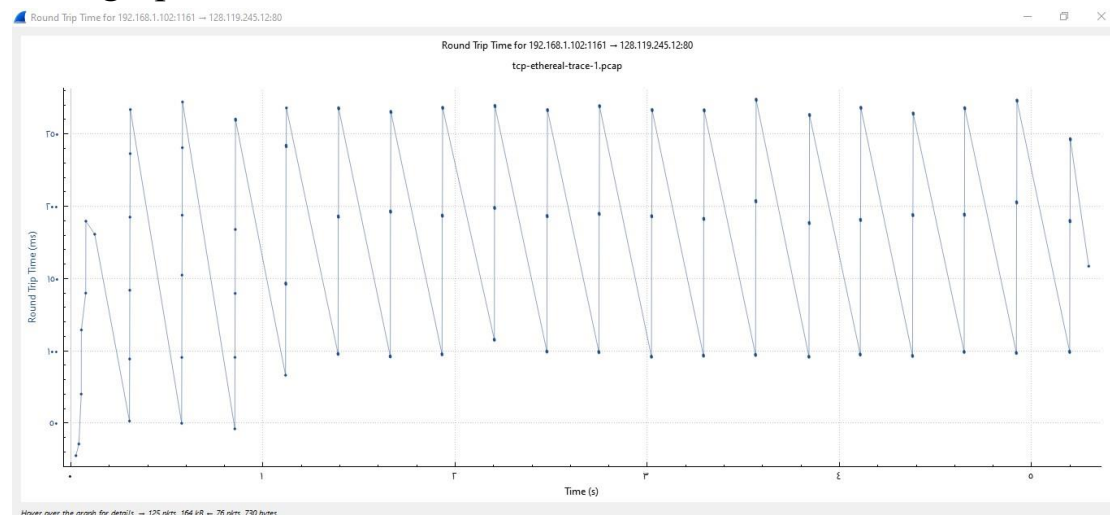
RTT of segment no 3 : 0.070059 s

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

$\text{EstimatedRTT} = (1-0.125) * \text{EstimatedRTT} + 0.125 *$

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:

$\text{EstimatedRTT} = 0.875 * 0.02746 + 0.125 * 0.035557 =$
0.028472125 s

EstimatedRTT after the receipt of the ACK of segment 3:

$\text{EstimatedRTT} = 0.875 * 0.028472125 + 0.125 * 0.070059 =$
=0.03367048438 s

EstimatedRTT after the receipt of the ACK of segment 4:

$\text{EstimatedRTT} = 0.875 * 0.03367048438 + 0.125 * 0.11443 =$
0.04376542383 s

EstimatedRTT after the receipt of the ACK of segment 5:

$$\text{EstimatedRTT} = 0.875 * 0.04376542383 + 0.125 * 0.13989 = 0.05578099585 \text{ s}$$

EstimatedRTT after the receipt of the ACK of segment 6:

$$\text{EstimatedRTT} = 0.875 * 0.055827 + 0.125 * 0.18964 = 0.07251337137 \text{ s}$$

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 receiver 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 retransmitted 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.

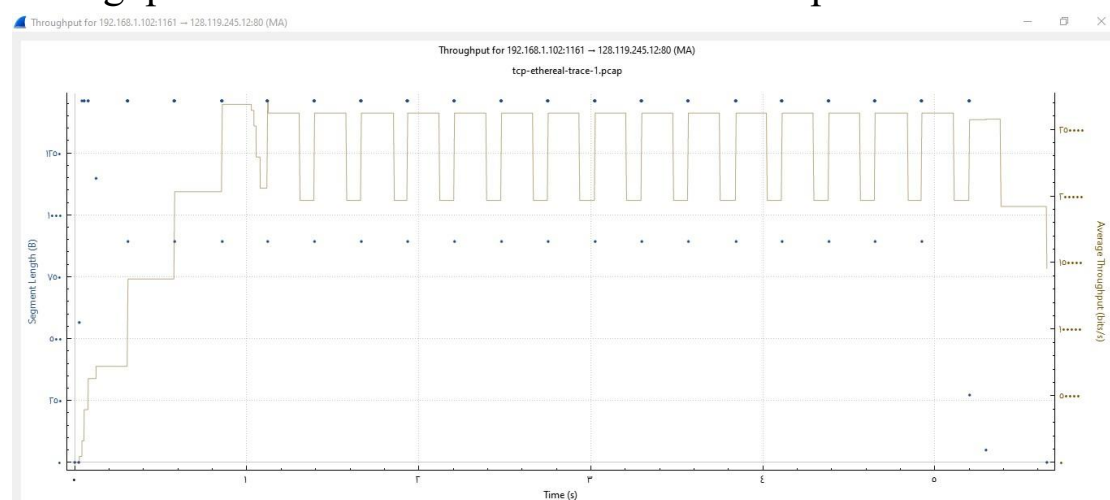
throughput = total data sent in Tcp segment / total transmission time

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

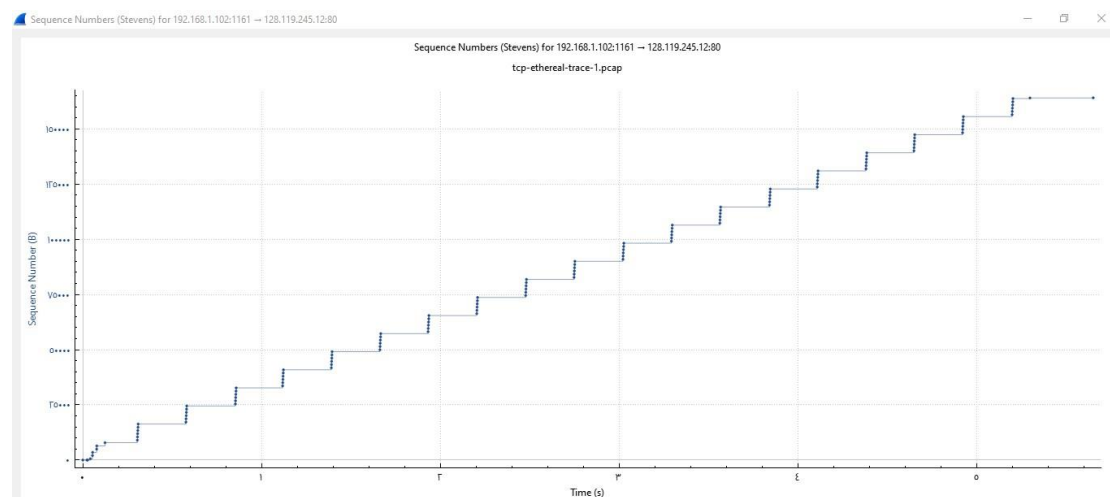
Acknowledge sent time = 5.45583 - 0.02746 = 5.42837 sec

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.

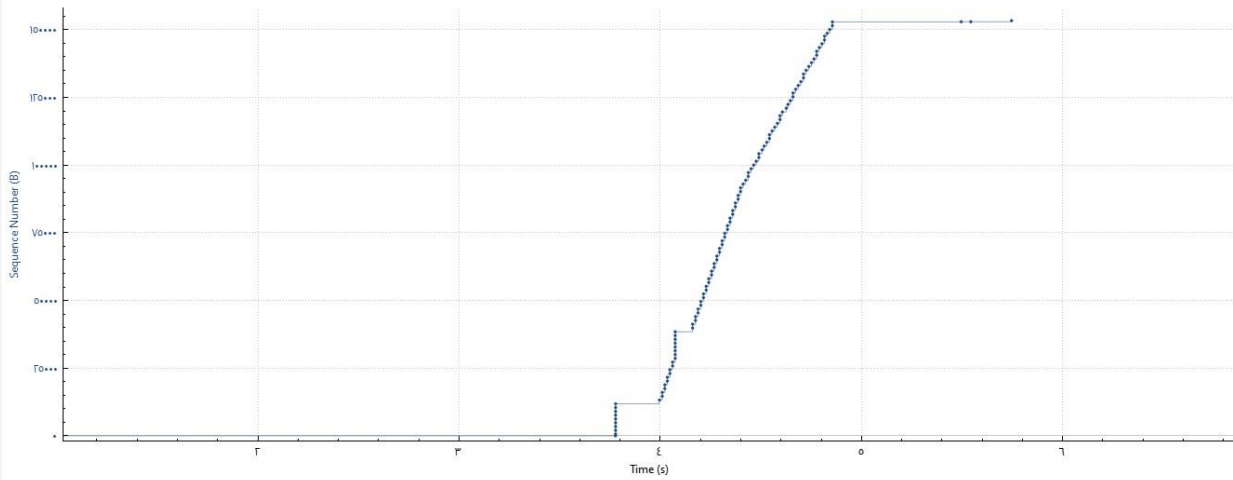


slowstart starts at 0 time and ends at 0.125s

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



Hover over the graph for details. — 115 pixels, 153 kB — 94 pixels, 1261 bytes