

CS315 : Computer Networks Lab

Assignment 5

Sourabh Bhosale (200010004)

January 31, 2023

1 Part 1: Capturing a bulk TCP transfer from your computer to a remote server

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.42.0.25	172.253.118.188	TCP	54	49438 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
2	0.070444	172.253.118.188	10.42.0.25	TCP	66	[TCP ACKed unseen segment] 5228 → 49438 [ACK] Seq=1 Ack=2 Win=275 Len=0 TSval=494097115 TSecr=6425
3	0.766866	34.120.52.64	10.42.0.25	TLSv1	93	Application Data
4	0.767836	10.42.0.25	34.120.52.64	TCP	66	49802 → 443 [ACK] Seq=1 Ack=28 Win=2047 Len=0 TSval=3435209135 TSecr=93385026
5	0.768326	10.42.0.25	34.120.52.64	TLSv1	97	Application Data
6	0.771273	34.120.52.64	10.42.0.25	TCP	66	443 → 49602 [ACK] Seq=28 Ack=32 Win=1091 Len=0 TSval=93385027 TSecr=3435209137
7	1.985762	10.42.0.25	142.250.76.42	TLSv1	164	Application Data
8	1.985970	10.42.0.25	142.250.76.42	TLSv1	105	Application Data
9	1.986069	10.42.0.25	142.250.76.42	TLSv1	178	Application Data
10	1.910489	10.42.0.25	128.119.245.12	TCP	66	49625 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2058 Len=0 TSval=3967574639 TSecr=93381477
11	1.910848	10.42.0.25	128.119.245.12	TCP	78	49629 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2400015025 TSecr=0 SACK_PERM
12	1.911175	10.42.0.25	128.119.245.12	TCP	78	49630 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2310718919 TSecr=0 SACK_PERM
13	1.912082	10.42.0.25	142.250.195.110	TLSv1	145	Application Data
14	1.912155	10.42.0.25	142.250.195.110	TLSv1	185	Application Data
15	1.912279	10.42.0.25	142.250.195.110	TLSv1	532	Application Data
16	1.915674	128.119.245.12	10.42.0.25	TCP	74	80 → 49629 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=93385142 TSecr=240001503
17	1.915751	10.42.0.25	128.119.245.12	TCP	66	49629 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2400015030 TSecr=93385142
18	1.916149	10.42.0.25	128.119.245.12	TCP	791	49629 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=725 TSval=2400015030 TSecr=93385142 [TCP segment of
19	1.916818	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=726 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
20	1.916824	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=2174 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
21	1.916826	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=3622 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
22	1.916828	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=5070 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
23	1.916830	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=6518 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of

> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: IntelCor_70:0b:a7 (64:6e:e0:70:0b:a7), Dst: Apple_ad:cf:45 (14:7d:da:ad:cf:45)
> Internet Protocol Version 4, Src: 172.253.118.188, Dst: 10.42.0.25
> Transmission Control Protocol, Src Port: 5228, Dst Port: 49438, Seq: 1, Ack: 2, Len: 0

Transmission Control Protocol: Protocol Packets: 222 · Displayed: 222 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Figure 1: Wireshark window : Part-1

2 Part 2: 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 alice.txt file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window"

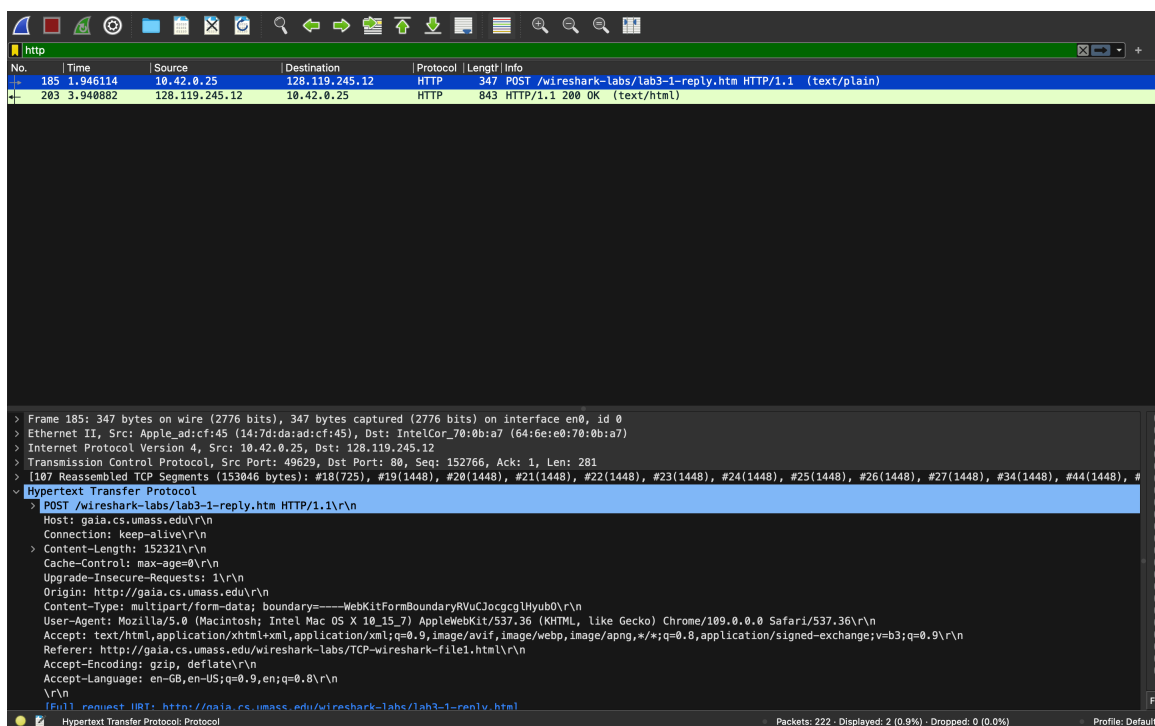
IP address (source) : 10.42.0.25

TCP port number (source) : 49629

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?

IP address (destination) : 128.119.245.12

TCP port number (destination) : 80



3 Part 3: TCP Basics

1. 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 this TCP segment that identifies the segment as a SYN segment?

Sequence number : 0. In the Flags section, the **Syn** flag is set to 1 which indicates that this segment is a SYN segment.

The image shows a Wireshark packet capture of a TCP connection. The top pane displays a list of packets, with packet 2 highlighted. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.42.0.25	172.253.118.188	TCP	54	49438 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
2	0.070444	172.253.118.188	10.42.0.25	TCP	66	[TCP ACKed unseq. segment] 5228 → 49438 [ACK] Seq=1 Ack=2 Win=275 Len=0 TSval=494097115 TSecr=6425
3	0.766866	34.120.52.64	10.42.0.25	TLSv1	93	Application Data
4	0.767836	10.42.0.25	34.120.52.64	TCP	66	49602 → 443 [ACK] Seq=1 Ack=28 Win=2047 Len=0 TSval=3435209135 TSecr=93385026
5	0.768326	10.42.0.25	34.120.52.64	TLSv1	97	Application Data
6	0.771273	34.120.52.64	10.42.0.25	TCP	66	443 → 49602 [ACK] Seq=28 Ack=32 Win=1091 Len=0 TSval=93385027 TSecr=3435209137
7	1.985762	10.42.0.25	142.250.76.42	TLSv1	164	Application Data
8	1.985970	10.42.0.25	142.250.76.42	TLSv1	185	Application Data
9	1.986069	10.42.0.25	142.250.76.42	TLSv1	178	Application Data
10	1.910489	10.42.0.25	128.119.245.12	TCP	66	49625 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2050 Len=0 TSval=3967574639 TSecr=93381477
11	1.910834	10.42.0.25	128.119.245.12	TCP	78	49629 → 80 [SYN, Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2400015025 TSecr=0 SACK_PERM
12	1.911175	10.42.0.25	128.119.245.12	TCP	78	49630 → 80 [SYN, Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2310718919 TSecr=0 SACK_PERM
13	1.912082	10.42.0.25	142.250.195.110	TLSv1	145	Application Data
14	1.912155	10.42.0.25	142.250.195.110	TLSv1	185	Application Data
15	1.912279	10.42.0.25	142.250.195.110	TLSv1	532	Application Data
16	1.915674	128.119.245.12	10.42.0.25	TCP	74	80 → 49629 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=93385142 TSecr=2400015031
17	1.915751	10.42.0.25	128.119.245.12	TCP	66	49629 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2400015030 TSecr=93385142
18	1.916149	10.42.0.25	128.119.245.12	TCP	791	49629 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=725 TSval=2400015030 TSecr=93385142 [TCP segment of
19	1.916818	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=726 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
20	1.916824	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=2174 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
21	1.916826	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=3622 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
22	1.916828	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=5870 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of
23	1.916830	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=6518 Ack=1 Win=131712 Len=1448 TSval=2400015031 TSecr=93385142 [TCP segment of

Packet Details:

(Conversation: 10.42.0.25 → 128.119.245.12)

(TCP Segment Len: 0)

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 1084356102

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1011 ... = Header Length: 44 bytes (11)

Flags: 0x002 (SYN)

000 ... = Reserved: Not set

...0 ... = 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

...0 ... = Fin: Not set

[TCP Flags:S.]

Window: 65535

Syn (tcp.flags.syn), 1 byte

Packets: 222 · Displayed: 222 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

2. 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 it in the segment that identifies the segment as a SYNACK segment? What is the value of the Acknowledgement field in the SYNACK segment? How did `gaia.cs.umass.edu` determine that value?

Sequence number : 0. A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1. The value of the acknowledgement field in the SYNACK segment is 1. We can say that, `gaia.cs.umass.edu` determines that value as the server adds 1 to the initial sequence number of SYN segment from the client computer. In this case, the initial sequence number of SYN segment from the client computer is 0, thus the value of the Acknowledgement field in the SYNACK segment is 1.

3. What is the sequence number of the TCP segment containing the header of the HTTP POST command? Note that in order to find the POST message header, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text "POST" within its DATA field. How many bytes of data are contained in the payload (data) field of this TCP segment? Did all of the data in the transferred file `alice.txt` fit into this single segment?

Sequence number : 152766. 281 bytes of data are contained in the payload (data) field of this TCP segment. No, all of the data in the transferred file `alice.txt` doesn't fit into this single segment.

4. Consider the TCP segment containing the HTTP "POST" as the first segment in the data transfer part of the TCP connection.

i. At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent?

Time : 1.916149 seconds.

ii. At what time was the ACK for this first data-containing segment received?

Time : 1.919794 seconds.

iii. What is the RTT for this first data-containing segment?

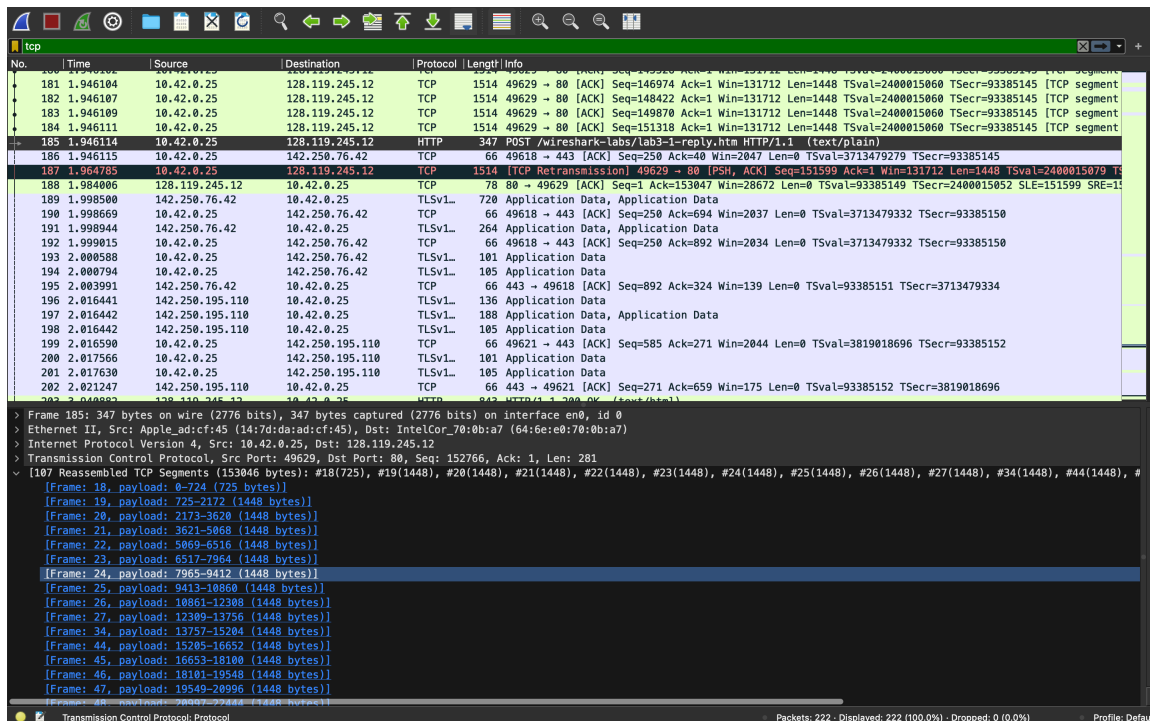
The RTT for this segment was: 0.003645000 seconds.

iv. What is the RTT value of the second data-carrying TCP segment and its ACK?

The RTT to this segment was: 0.005061000 seconds.

5. What is the length (header + payload) of each of the first four data-carrying TCP segments?

Length of each of the first four data-carrying TCP segments is (32 + 725) 757, (32 + 1448) 1480, (32 + 1448) 1480 and (32 + 1448) 1480 bytes respectively.



The image shows a Wireshark packet capture of a TCP connection. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Length. The bottom pane shows the details of the selected packet (No. 187), including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol details. The TCP details pane shows the segment's sequence number (1514), acknowledgment number (80), and window size (2047). The packet list shows the first four data-carrying TCP segments (Nos. 181, 182, 183, 184) and their corresponding ACKs (Nos. 185, 186, 187, 188).

No.	Time	Source	Destination	Protocol	Length	Info
181	1.946184	10.42.0.25	128.119.245.12	TCP	757	1514 → 80 [ACK] Seq=146974 Ack=1 Win=131712 Len=1448 TSval=2400015060 TSecr=93385145 [TCP segment of data flow 0x00000000 → 0x00000000] (text/plain)
182	1.946187	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=148422 Ack=1 Win=131712 Len=1448 TSval=2400015060 TSecr=93385145 [TCP segment of data flow 0x00000000 → 0x00000000] (text/plain)
183	1.946189	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=149870 Ack=1 Win=131712 Len=1448 TSval=2400015060 TSecr=93385145 [TCP segment of data flow 0x00000000 → 0x00000000] (text/plain)
184	1.946111	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=151318 Ack=1 Win=131712 Len=1448 TSval=2400015060 TSecr=93385145 [TCP segment of data flow 0x00000000 → 0x00000000] (text/plain)
185	1.946114	10.42.0.25	128.119.245.12	HTTP	347	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
186	1.946115	10.42.0.25	142.250.76.42	TCP	66	49618 → 443 [ACK] Seq=250 Ack=40 Win=2047 Len=0 TSval=3713479279 TSecr=93385145
187	1.964785	10.42.0.25	128.119.245.12	TCP	1514	[TCP Retransmission] 49629 → 80 [PSH, ACK] Seq=151599 Ack=1 Win=131712 Len=1448 TSval=2400015079 TSecr=93385145
188	1.984086	128.119.245.12	10.42.0.25	TCP	78	80 → 49629 [ACK] Seq=1 Ack=153047 Win=28672 Len=0 TSval=93385149 TSecr=2400015052 SLE=151599 SRE=151599
189	1.998500	142.250.76.42	10.42.0.25	TLSh1..	720	Application Data, Application Data
190	1.998669	10.42.0.25	142.250.76.42	TCP	66	49618 → 443 [ACK] Seq=250 Ack=694 Win=2037 Len=0 TSval=3713479332 TSecr=93385150
191	1.998944	142.250.76.42	10.42.0.25	TLSh1..	264	Application Data, Application Data
192	1.999015	10.42.0.25	142.250.76.42	TCP	66	49618 → 443 [ACK] Seq=250 Ack=892 Win=2034 Len=0 TSval=3713479332 TSecr=93385150
193	2.000588	10.42.0.25	142.250.76.42	TLSh1..	101	Application Data
194	2.000794	10.42.0.25	142.250.76.42	TLSh1..	105	Application Data
195	2.003991	142.250.76.42	10.42.0.25	TCP	66	443 → 49618 [ACK] Seq=892 Ack=324 Win=139 Len=0 TSval=93385151 TSecr=3713479334
196	2.016441	142.250.195.110	10.42.0.25	TLSh1..	136	Application Data
197	2.016442	142.250.195.110	10.42.0.25	TLSh1..	188	Application Data, Application Data
198	2.016442	142.250.195.110	10.42.0.25	TLSh1..	105	Application Data
199	2.016590	10.42.0.25	142.250.195.110	TCP	66	49621 → 443 [ACK] Seq=585 Ack=271 Win=2044 Len=0 TSval=3819018696 TSecr=93385152
200	2.017566	10.42.0.25	142.250.195.110	TLSh1..	101	Application Data
201	2.017630	10.42.0.25	142.250.195.110	TLSh1..	105	Application Data
202	2.021247	142.250.195.110	10.42.0.25	TCP	66	443 → 49621 [ACK] Seq=271 Ack=659 Win=175 Len=0 TSval=93385152 TSecr=3819018696
203	2.040893	128.119.245.12	10.42.0.25	HTTP	842	HTTP/1.1 200 OK (text/html)

Frame 185: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface en0, id 0
> Ethernet II, Src: Apple_Ad:cf:45 (14:7d:da:ad:cf:45), Dst: IntelCor_70:0b:a7 (64:6e:e0:70:0b:a7)
> Internet Protocol Version 4, Src: 10.42.0.25, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49629, Dst Port: 80, Seq: 152766, Ack: 1, Len: 281
[107 Reassembled TCP Segments (153046 bytes): #18(725), #19(1448), #20(1448), #21(1448), #22(1448), #23(1448), #24(1448), #25(1448), #26(1448), #27(1448), #34(1448), #44(1448), #

Transmission Control Protocol: Protocol Packets: 222 · Displayed: 222 (100.0%) · Dropped: 0 (0.0%) Profile: Default

6. What is the minimum amount of available buffer space advertised to the client by `gaia.cs.umass.edu` among these first four data-carrying TCP segments? Does the lack of receiver buffer space ever throttle the sender for these first four data-carrying segments?

The minimum amount of available buffer space (receiver window) advertised at `gaia.cs.umass.edu` is 16000 bytes, which shows in the first acknowledgement from the server. This receiver window grows steadily. The sender is never throttled due to lacking of receiver buffer space by inspecting this trace.

7. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

There are no retransmitted segments in the trace file. We can verify this by checking the sequence numbers of the TCP segments in the trace file. In the Time-Sequence-Graph (Stevens) of this trace, all sequence numbers from the source to the destination are increasing monotonically with respect to time. If there is a retransmitted segment, the sequence number of this retransmitted segment should be smaller than those of its neighboring segments.

8. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to `gaia.cs.umass.edu`? Can you identify cases where the receiver is ACKing every other received segment among these first ten data-carrying segments?

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. The receiver typically acknowledges 1460 bytes in an ack. By inspecting the amount of acknowledged data by each ACK, I haven't seen any ACKing between every other received segment.

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

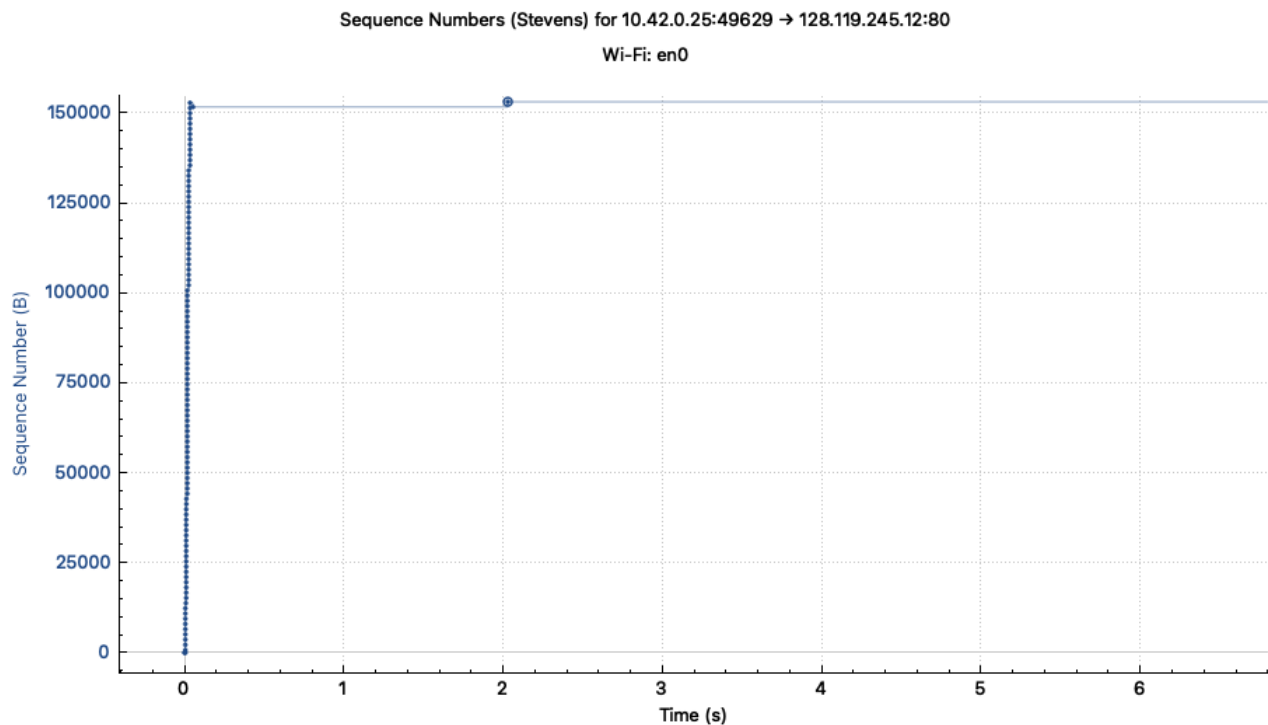
No.	Time	Source	Destination	Protocol	Length	Info
183	1.946109	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=149870 Ack=1 Win=131712 Len=1448 TSval=2400015060 TSecr=93385145 [TCP segment ...]
184	1.946111	10.42.0.25	128.119.245.12	TCP	1514	49629 → 80 [ACK] Seq=151318 Ack=1 Win=131712 Len=1448 TSval=2400015060 TSecr=93385145 [TCP segment ...]
185	1.946114	10.42.0.25	128.119.245.12	HTTP	347	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
186	1.946115	10.42.0.25	142.250.76.42	TCP	66	49618 → 443 [ACK] Seq=250 Ack=40 Win=2047 Len=0 TSval=3713479279 TSecr=93385145
187	1.964785	10.42.0.25	128.119.245.12	TCP	1514	[TCP Retransmission] 49629 → 80 [PSH, ACK] Seq=151599 Ack=1 Win=131712 Len=1448 TSval=2400015079 TSecr=93385145
188	1.984006	128.119.245.12	10.42.0.25	TCP	78	80 → 49629 [ACK] Seq=1 Ack=153047 Win=28672 Len=0 TSval=93385149 TSecr=2400015052 SLE=151599 SRE=151599
189	1.998500	142.250.76.42	10.42.0.25	TLShv1..	720	Application Data, Application Data
190	1.998669	10.42.0.25	142.250.76.42	TCP	66	49618 → 443 [ACK] Seq=250 Ack=694 Win=2037 Len=0 TSval=3713479332 TSecr=93385150
191	1.998944	142.250.76.42	10.42.0.25	TLShv1..	264	Application Data, Application Data
192	1.999015	10.42.0.25	142.250.76.42	TCP	66	49618 → 443 [ACK] Seq=250 Ack=892 Win=2034 Len=0 TSval=3713479332 TSecr=93385150
193	2.000588	10.42.0.25	142.250.76.42	TLShv1..	101	Application Data
194	2.000794	10.42.0.25	142.250.76.42	TLShv1..	105	Application Data
195	2.003991	142.250.76.42	10.42.0.25	TCP	66	443 → 49618 [ACK] Seq=892 Ack=324 Win=139 Len=0 TSval=93385151 TSecr=3713479334
196	2.016441	142.250.195.110	10.42.0.25	TLShv1..	136	Application Data
197	2.016442	142.250.195.110	10.42.0.25	TLShv1..	188	Application Data, Application Data
198	2.016442	142.250.195.110	10.42.0.25	TLShv1..	105	Application Data
199	2.016590	10.42.0.25	142.250.195.110	TCP	66	49621 → 443 [ACK] Seq=585 Ack=271 Win=2044 Len=0 TSval=3819018696 TSecr=93385152
200	2.017566	10.42.0.25	142.250.195.110	TLShv1..	101	Application Data
201	2.017630	10.42.0.25	142.250.195.110	TLShv1..	105	Application Data
202	2.021247	142.250.195.110	10.42.0.25	TCP	66	443 → 49621 [ACK] Seq=271 Ack=659 Win=175 Len=0 TSval=93385152 TSecr=3819018696
203	3.940862	128.119.245.12	10.42.0.25	HTTP	843	HTTP/1.1 200 OK (text/html)
204	3.941016	10.42.0.25	128.119.245.12	TCP	66	49629 → 80 [ACK] Seq=153047 Ack=778 Win=130944 Len=0 TSval=2400017056 TSecr=93385340

... = header Length: 32 bytes (0)
 > Flags: 0x010 (PSH, ACK)
 Window: 2058
 [calculated window size: 131712]
 [Window size scaling factor: 64]
 Checksum: 0x849c [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 [Timestamps]
 [Time since first frame in this TCP stream: 0.035266000 seconds]
 [Time since previous frame in this TCP stream: 0.000003000 seconds]
 > [SEQ/ACK analysis]
 [IRTT: 0.004903000 seconds]
 [Bytes in flight: 26345]
 [Bytes sent since last PSH flag: 152321]
 TCP payload (281 bytes)
 TCP segment data (281 bytes)
 > [107 Reassembled TCP Segments (153046 bytes): #18(725), #19(1448), #20(1448), #21(1448), #22(1448), #23(1448), #24(1448), #25(1448), #26(1448), #27(1448), #34(1448), #44(1448), #...

Total no. of bytes transferred is 153048 and the difference between first frame (0.035266000 seconds) and the last (0.000003000 seconds) came to be 0.035263 seconds. So the throughput will be 153048 bytes / 0.035263 seconds = 4340186.59785 bytes / seconds.

4 Part 4: TCP congestion control in action

1. 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 slow start phase begins and ends, and where congestion avoidance takes over?



Slow start phase begins at around 0 seconds and ends at around 0.04 seconds and then congestion takes over.