

Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 3a

(Using the file tcpethereal-trace-1)

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

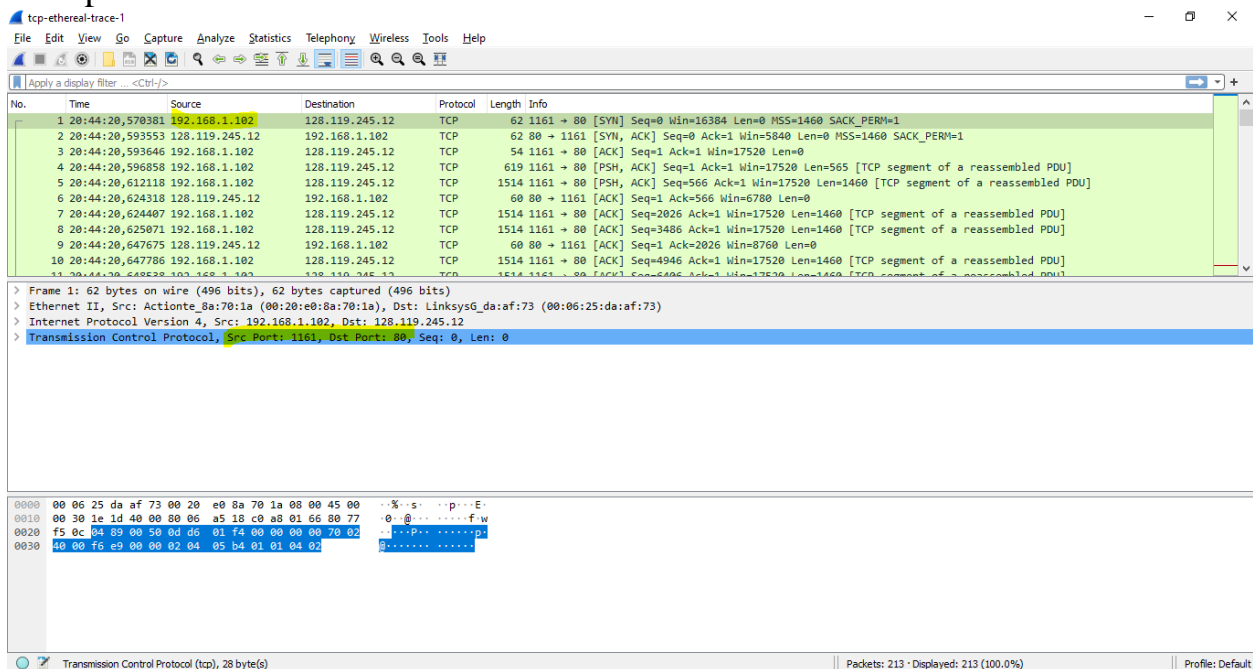
2. A first look at the captured trace

Question 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? 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” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you're uncertain about the Wireshark windows).

ANSWER:

IP address of client: 192.168.1.102

TCP port number: 1161



Question 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?

ANSWER:

- IP address of gaia server: 128.119.245.12
- Port number is it sending and receiving TCP segments: 80

tcp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	20:44:20.570361	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	20:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	20:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	20:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	20:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	20:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	20:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	20:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	20:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	20:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	20:44:20.648238	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_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

```

0000  00 06 25 da af 73 00 20 e0 8a 70 1a 00 00 45 00  ..K.s..p...E
0010  00 30 1e 1d 40 00 00 06 a5 18 c0 a8 01 66 80 77  0 @ ..f.w
0020  f5 0c 04 89 00 50 d6 01 f4 00 00 00 00 70 02    ....P.....p
0030  40 00 f6 e9 00 00 02 04 05 b4 01 01 04 02      @.....
  
```

Transmission Control Protocol (tcp), 28 byte(s)

Packets: 213 · Displayed: 213 (100.0%)

Profile: Default

Question 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?

ANSWER:

(use sample file)

3. TCP Basics

Question 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?

ANSWER:

TCP SYN segment: 0

SYN Flags = 1 -> segment as SYN segment

tcp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	20:44:20.570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	20:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	20:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	20:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	20:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	20:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	20:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	20:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	20:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	20:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	20:44:20.648838	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

000. = Reserved: Not set
...0 = Nonce: Not set
....0 = Congestion Window Reduced (CWR): Not set
....0 = ECN-Echo: Not set
....0 = Urgent: Not set
....0 = Acknowledgment: Not set
....0 = Push: Not set
....0 = Reset: Not set
>1 = Syn: Set
....0 = Fin: Not set
[TCP Flags:S]
Window: 16384
[Calculated window size: 16384]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 00 00 45 00 ..K..s..p...E
0010 00 30 1e 1d 40 00 00 06 a5 18 c0 a8 01 66 00 77 0 @...f.w
0020 f5 0c 04 89 00 50 d0 d6 01 f4 00 00 00 70 32P.....p
0030 40 00 f6 e9 00 00 02 04 05 b4 01 01 04 02 @.....

Syn (tcp.flags.syn), 1 byte(s) | Packets: 213 · Displayed: 213 (100.0%) | Profile: Default

Question 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?

ANSWER:

Sequence number of the SYNACK segment: 0

SYNACK segment: SYN flag = ACK flag = 1

tcp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	20:44:20.570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	20:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	20:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	20:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	20:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	20:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	20:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	20:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	20:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	20:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	20:44:20.648838	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

[Stream index: 0]
[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)
Acknowledgment number (raw): 232129013
0111 = Header Length: 28 bytes (7)
▼ Flags: 0x012 (SYN, ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
....0 = Congestion Window Reduced (CWR): Not set
....0 = ECN-Echo: Not set
....0 = Urgent: Not set
....1 = Acknowledgment: Set
....0 = Push: Not set
....0 = Reset: Not set
>1 = Syn: Set

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 00 00 45 00 ..p...X...s..E
0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c c0 a8 0 @...7...6.w
0020 01 66 00 50 04 89 34 a2 74 19 0d d6 01 f5 70 12 -f-P-4...t...p
0030 16 d0 77 4d 00 00 02 04 05 b4 01 01 04 02 -wM...@.....

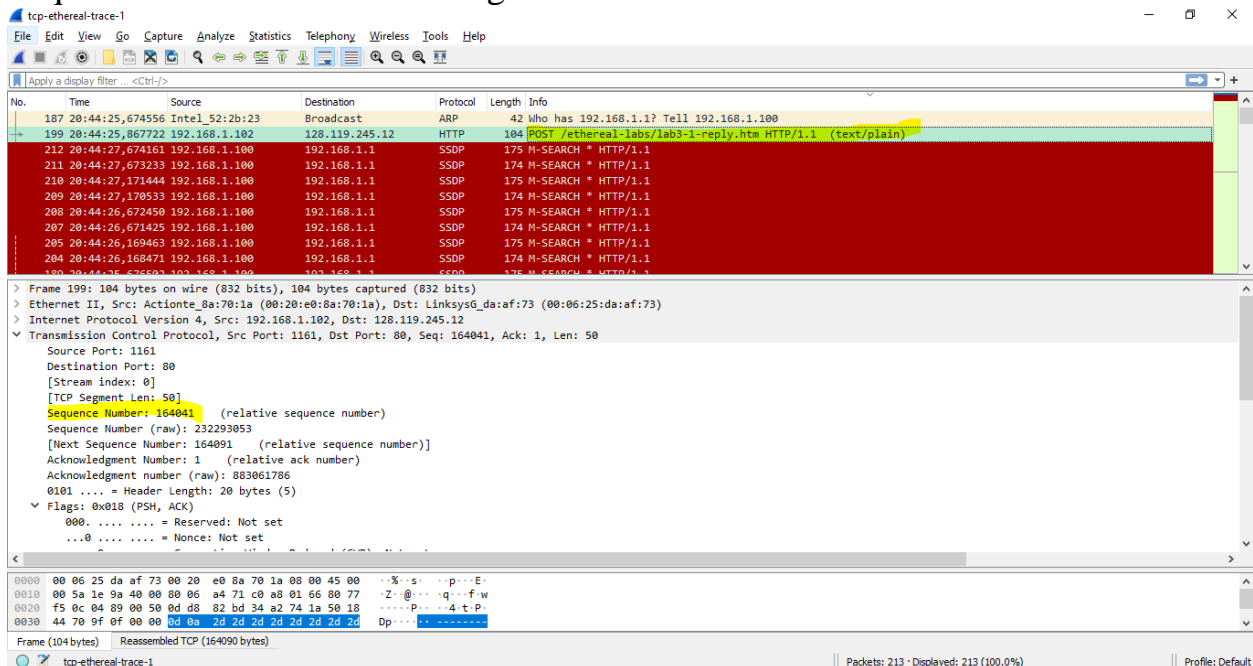
Syn (tcp.flags.syn), 1 byte(s) | Packets: 213 · Displayed: 213 (100.0%) | Profile: Default

*The gaia.cs.umass.edu server adds 1 to the initial sequence number of the SYN segment from the client computer. For this case, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the acknowledgement field in the SYN_ACK segment is 1. A segment will be identified as a SYN_ACK segment if both SYN flag and ACKnowledgement flag in the segment are set to 1.

Question 6: What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

ANSWER:

Sequence number of the TCP segment: 1



Question 7: Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? 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? What is the *EstimatedRTT* value (see Section 3.5.3, page 242 in text) after the receipt of each ACK?

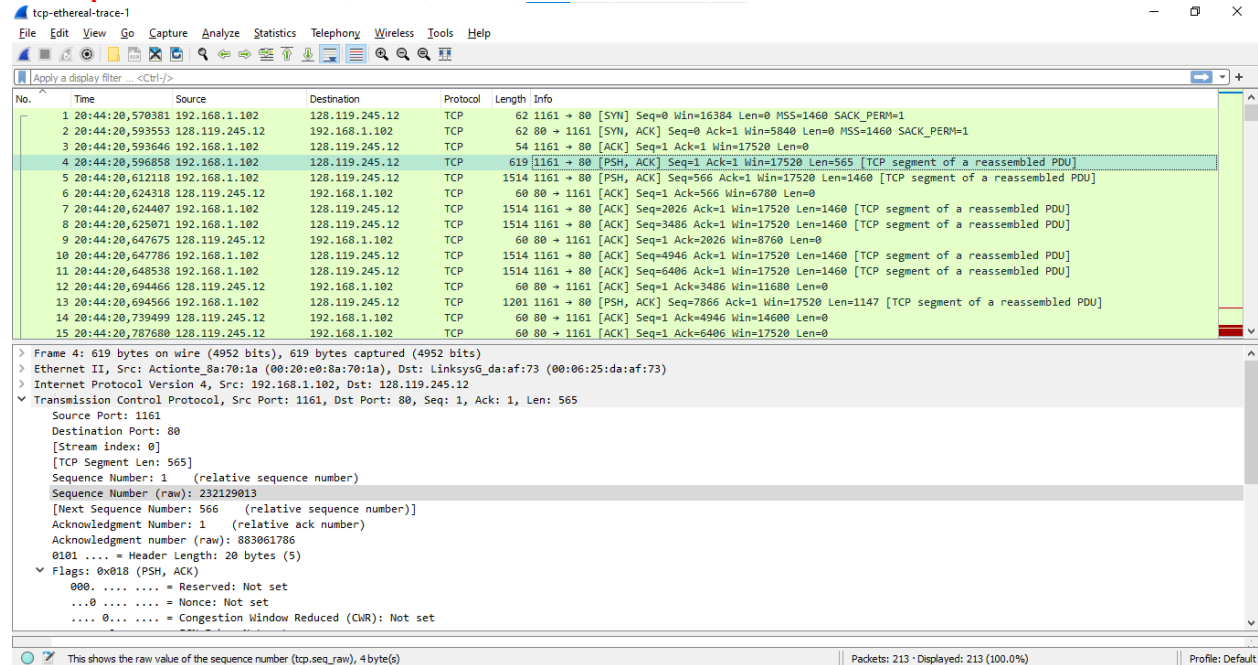
ANSWER:

TCP segment 1-6:

+ Packet: 4, 5, 7, 8, 10, 11

+ ACK: 9, 12, 14, 15, 16, 17

+ Sequence number: 1, 566, 2026, 3486, 4946, 6406



*_EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

Segment	Send time	ACK received	RTT(s)	Estimated RTT after the receipt of each ACK
1	20.596868	20.647675	0.050807	0.050807
2	20.612118	20.694466	0.082348	0.054749625
3	20.654407	20.739499	0.085092	0.082691
4	20.625071	20.78768	0.162609	0.094781625
5	20.647786	20.838183	0.190397	0.1660825
6	20.648538	20.875188	0.22665	0.194928625

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

ANSWER:

The length of the first 6 TCP segments is 565 bytes.

Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 232129013
[Next Sequence Number: 566 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1fbd [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (565 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (565 bytes)

The length of the remaining TCP segments is 1460 bytes.

Sequence Number: 566 (relative sequence number)
Sequence Number (raw): 232129578
[Next Sequence Number: 2026 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x3be5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1460 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (1460 bytes)

Question 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?

ANSWER:

The minimum amount of available buffer space advertised at the received is 17520 bytes.

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 566, Ack: 1, Len: 1460

Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence Number: 566 (relative sequence number)
Sequence Number (raw): 232129578
[Next Sequence Number: 2026 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 ... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x3be5 [unverified]
[Checksum Status: Unverified]

This shows the raw value of the sequence number (tcp.seq_raw), 4 byte(s)

Packets: 213 • Displayed: 213 (100.0%)

Profile: Default

Question 10: Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

ANSWER:

No there is no retransmitted segments in the trace file.

Question 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 (see Table 3.2 on page 250 in the text).

ANSWER:

*ACK data = ACK sequence number - ACK sequence number

	ACK sequence number	ACK data
ACK1	2026	2026
ACK2	3486	1460
ACK3	4946	1460
ACK4	6406	1460
ACK5	7866	1460
ACK6	9013	1147

...		

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

ANSWER:

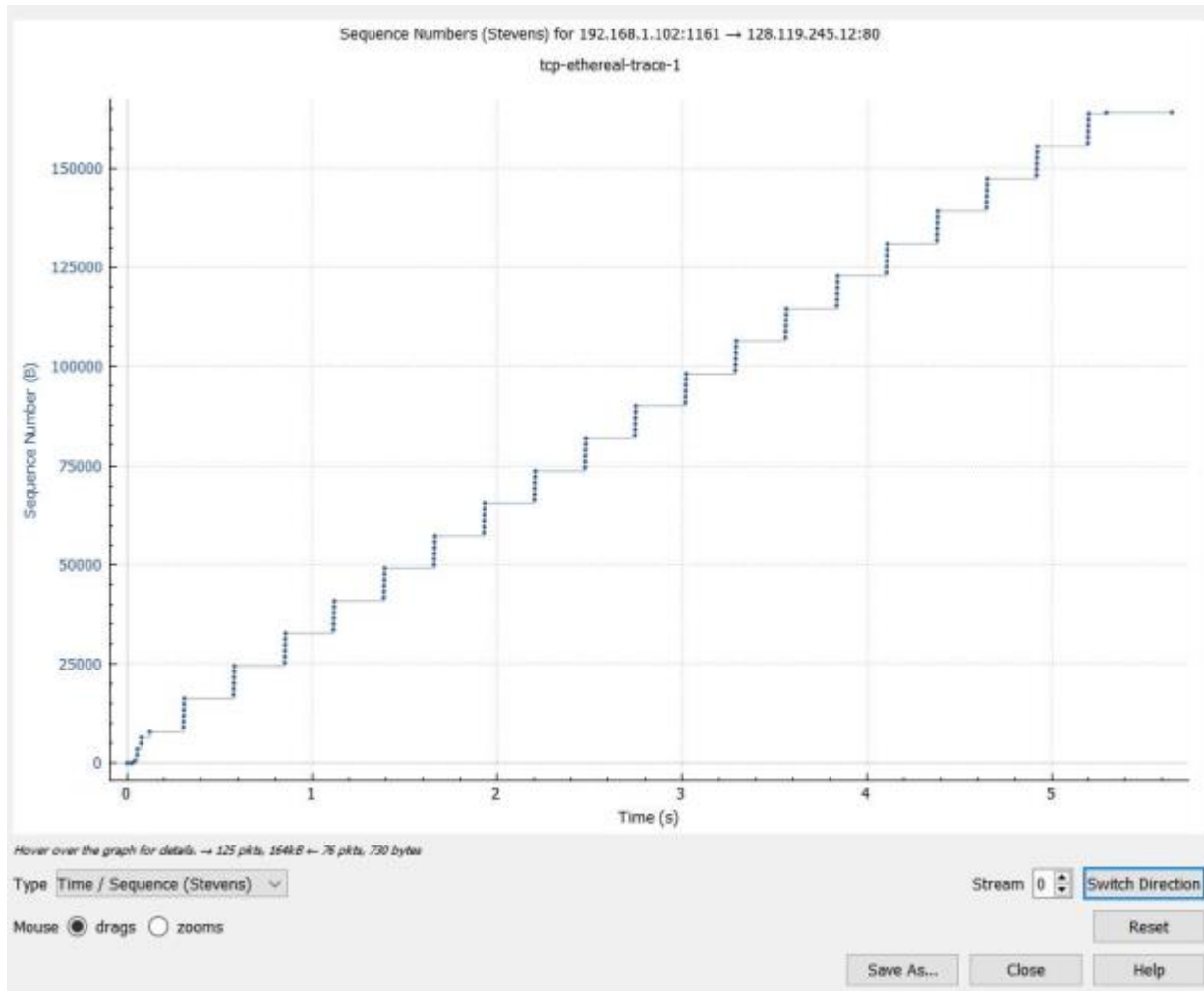
$$\text{Through-put} = \frac{\text{Amount of data transmitted}}{\text{time incurred}} = \frac{181283}{26.221522 - 20.596858} = 32230 \text{ bytes/s}$$

4. TCP congestion control in action

Question 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

ANSWER:

Where congestion avoidance takes over: 0.04s
 ⇒ Continuous + evenly distributed until the end



Question 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

ANSWER:

Done