



LAB REPORT 3

Subject: TCP/UDP PROTOCOL

Student information	Student 1 ID: 22520836 Name: Ngo Thi Hong Ly Student 2 ID: 22521099 Name: Le Hoang Thien Phu Student 3 ID: 22521237 Name: Pham Quang Dai Phuc Student 4 ID: 22521240 Name: Le Minh Sang
Class	CS4283.O21.CTTT.1
Work division:	[Student 1]: Do question 9,10,11,12 task 3 and support the other [Student 2]: Do question 4,5,6,7,8 task 3 and support the other [Student 3]: Do the task 2, 4 and support the other [Student 4]: Do the task 1 and support the other
Video link of implementation (if required)	
Opinions (if any) + Difficulties encountered + Suggestions, comments...	

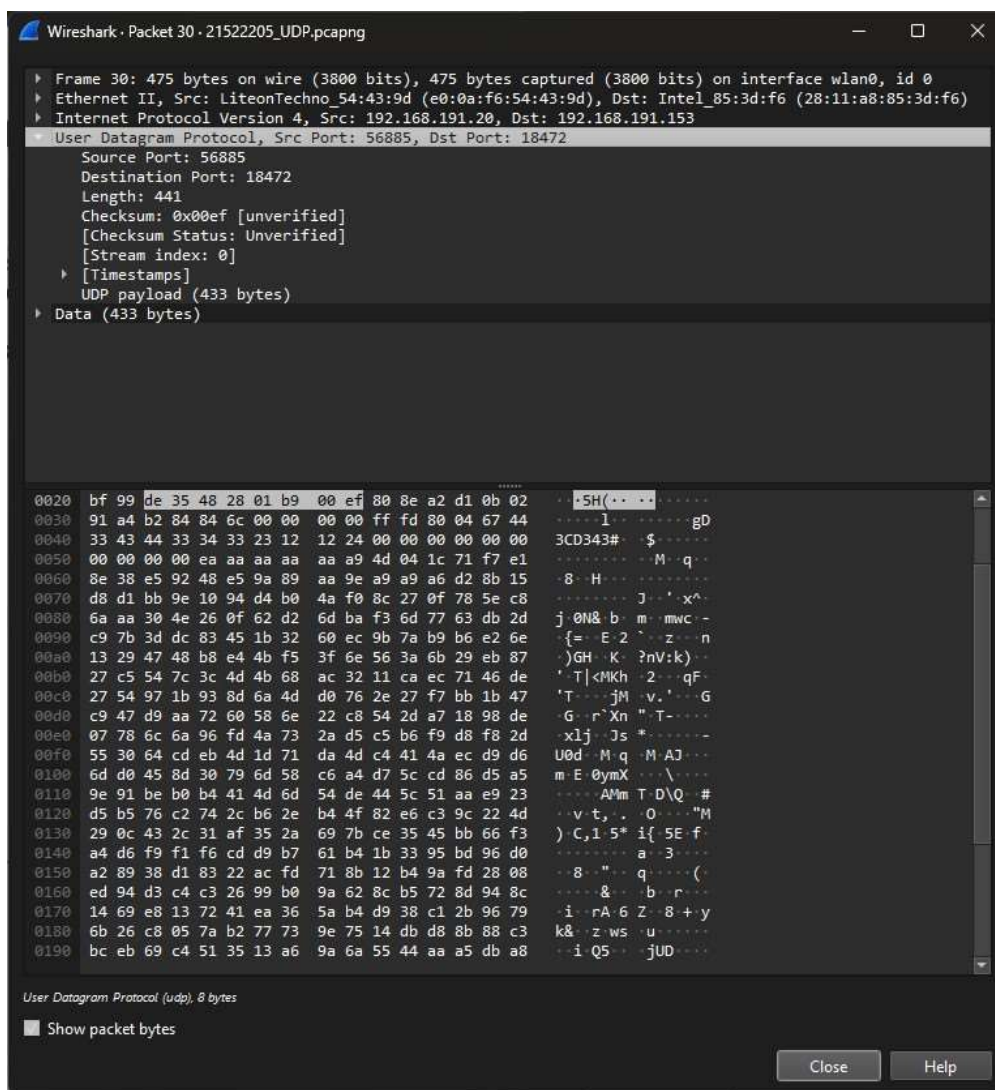


Task 1

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header.

→ From the selected UDP packet, observe the UDP header fields. Common fields in the UDP header include:

- Source Port: 56886
- Destination Port: 18474
- Length: 1408 bytes
- Checksum: 0x2c6e

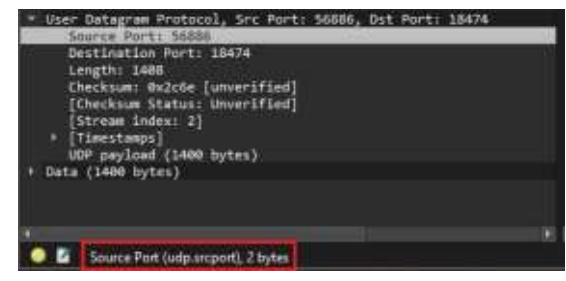
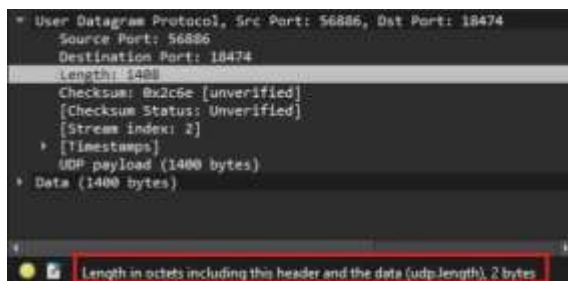
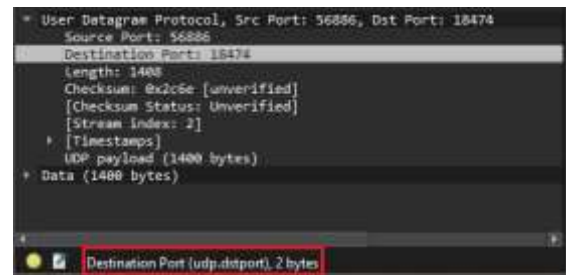
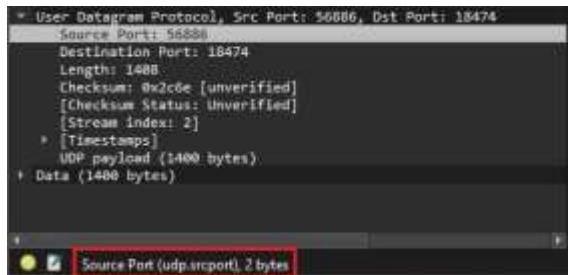




2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

→ There are four UDP header fields:

- Source Port: 2 bytes
- Destination Port: 2 bytes
- Length: 2 bytes
- Checksum: 2 bytes



3. The value in the Length field is the length of what?

→ **Length Field in UDP Header:** is the length of the entire datagram

$$\text{Length} = \text{UDP header} + \text{UDP payload}$$

In UDP header field, each field is 2 bytes long. Therefore the total length of the UDP header is 8 bytes. Beside that, the UDP payload is 443 bytes long. Therefore, the Length = UDP header + UDP payload = 441

- UDP header: 8 bytes
- UDP payload: 443 bytes
- Length: 441



```
▶ Frame 28: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface 0  
▶ Ethernet II, Src: LiteonTechno_54:43:9d (e0:0a:f6:54:43:9d), Dst: 192.168.191.20  
▶ Internet Protocol Version 4, Src: 192.168.191.20, Dst: 192.168.191.20  
  User Datagram Protocol, Src Port: 56885, Dst Port: 18472  
    Source Port: 56885  
    Destination Port: 18472  
    Length: 441  
    Checksum: 0xb89c [unverified]  
    [Checksum Status: Unverified]  
    [Stream index: 0]  
    [Timestamps]  
    UDP payload (433 bytes)  
  Data (433 bytes)  
    Data [truncated]: 808ea2d00b028871b284846c00000000fffd80047734  
    [Length: 433]
```

User Datagram Protocol (udp), 8 bytes

4. What is the maximum number of bytes that can be included in a UDP payload?

→ The maximum number of bytes that a UDP payload can contain (including UDP header and IP header) is $2^{16} - 1 = 65535$ (bytes). (Length)

- Which: $\text{Length} = \text{Data Length} + \text{UDP header Length} + \text{IP header Length}$.
- In there:
 - Our UDP header is fixed at 8 bytes (as described above)
 - Because we use IPv4, our IP header is 20 bytes.

```
▶ Frame 30: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface 0  
▶ Ethernet II, Src: LiteonTechno_54:43:9d (e0:0a:f6:54:43:9d), Dst: 192.168.191.20  
▶ Internet Protocol Version 4, Src: 192.168.191.20, Dst: 192.168.191.20  
  0100 .... = Version: 4  
  .... 0101 = Header Length: 20 bytes (5)  
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
    Total Length: 461  
    Identification: 0xb7ea (47082)
```



5. What is the largest possible source port number?

→ The largest possible source port number is determined by the size of the field allocated for port numbers in the UDP header. Typically, it's 16 bits, allowing for a maximum value of $2^{16} - 1 = 65535$.

6. What is the protocol number for UDP?

→ The protocol number for UDP (User Datagram Protocol) is 17 in decimal notation and 0x11 in hexadecimal notation.

```
▶ Frame 28: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface 0
▶ Ethernet II, Src: LiteonTechno_54:43:9d (e0:0a:f6:54:43:9d), Dst: 08:00:27:00:00:00
▶ Internet Protocol Version 4, Src: 192.168.191.20, Dst: 192.168.191.153
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 461
    Identification: 0xb7e8 (47080)
    ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x8138 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.191.20
    Destination Address: 192.168.191.153
    ▶ User Datagram Protocol, Src Port: 56885, Dst Port: 18472
    ▶ Data (433 bytes)
```

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet.

→ Relationship between Port Numbers:

- **First UDP Packet (Frame 25):**
 - Source Port: 18474
 - Destination Port: 56886

```
▶ Frame 25: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: Intel 85:3d:f6 (28:11:a8:85:3d:f6), Dst: LiteonTechno_54:43:9d (e0:0a:f6:54:43:9d)
▶ User Datagram Protocol, Src Port: 18474, Dst Port: 56886
    Source Port: 18474
    Destination Port: 56886
    Length: 20
    Checksum: 0x0025 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    ▶ [Timestamps]
    UDP payload (12 bytes)
    ▶ Data (12 bytes)
```

- **Second UDP Packet (Frame 32) (Reply to the first packet):**
 - Source Port: 56886
 - Destination Port: 18474



```
* Frame 32: 1442 bytes on wire (11536 bits), 1442 bytes captured () 0000 28 11 a8 85 3d f6 e0 0a f6 54 43 9d 08 00 55 00 (.....)
* Ethernet II, Src: LiteonTechno_54:43:9d (e0:0a:f6:54:43:9d), Dst: 0010 05 94 b7 e2 00 00 80 11 7d 77 c0 a8 bf 14 c0 a0
* Internet Protocol Version 4, Src: 192.168.191.20, Dst: 192.168.11 0020 bf 09 de 36 48 2a 05 80 bf bb 80 60 bf 5e 0b 02
* User Datagram Protocol, Src Port: 56886, Dst Port: 18474 0030 94 05 66 a7 5d 97 5c 81 9a a3 49 a8 41 6c 99 4c
  Source Port: 56886 0040 0f ff 8f 25 b8 56 20 12 fe 85 8d be 6d 75 b8 74
  Destination Port: 18474 0050 e7 95 06 5b ac 2b 40 f2 a6 12 0f 47 0b 35 b4 69
  Length: 1408 0060 f7 fe 8d 15 c2 a8 95 e9 19 09 3c 9f 1f 65 59 1f
  Checksum: 0x0fbb [unverified] 0070 5f 90 e6 b7 ba 2b 2e 28 1d 61 a4 ca ba 18 59 88
  [Checksum Status: Unverified] 0080 ff 5f 85 bb 99 b3 3f fd d8 5e e5 c9 41 fd 2f b5
  [Stream index: 2] 0090 96 7a 88 79 3c 7c fd f8 e6 95 d2 4f 01 4f ec da
  [Timestamps] 00a0 c4 61 43 1f c2 91 ba 0a 1c 1f 70 97 1c 3a 7b 12
```


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?

→ Client computer

IP address: 192.168.191.20

Port number: 65022

[illegible]



Task 3

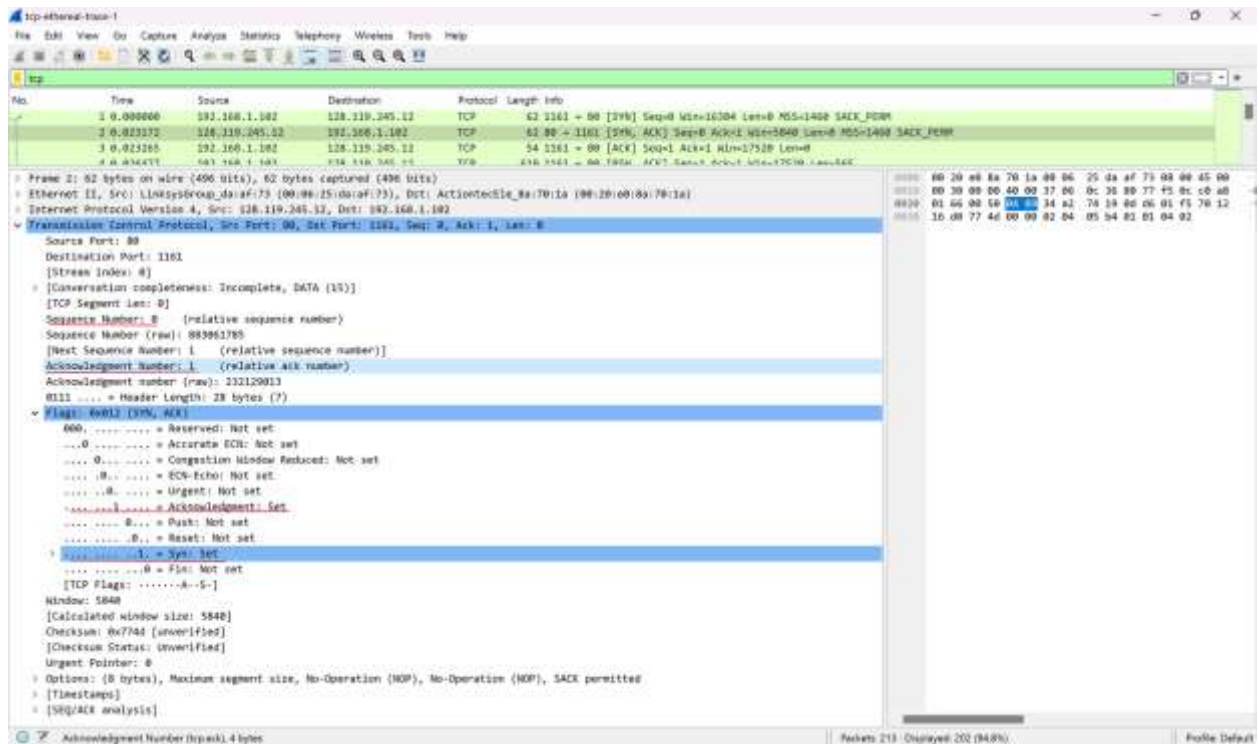
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

- 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: 0
- In a Flags field, the SYN flag is set = 1 that identifies the segment as a SYN segment.

```
[Stream index: 0]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
▼ 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...1. = Syn: Set
  ....0...0 = Fin: Not set
[TCP Flags: .....S.]
Window: 16384
```

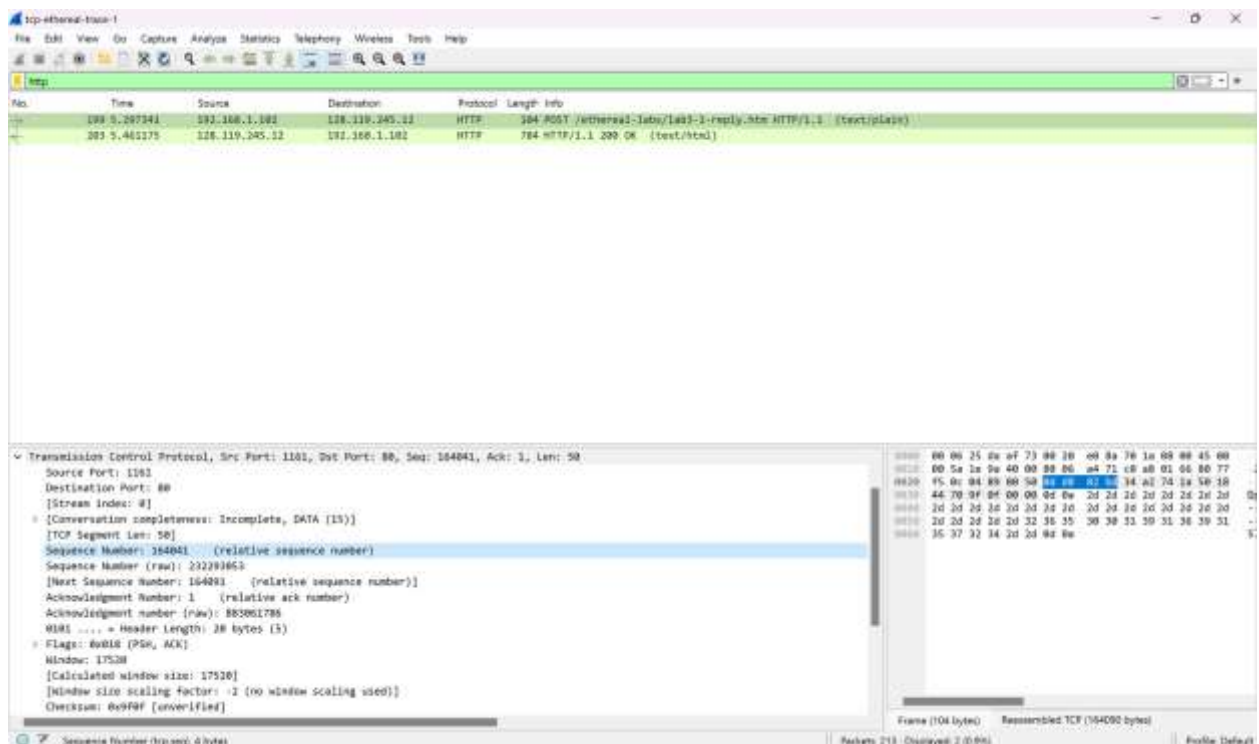
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

- The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN: 0
- The value of the Acknowledgement field in the SYNACK segment: 1
- In a Flags field, the (SYN, ACK) flag and the Acknowledgement flag is set = 1 that identifies the segment as a SYNACK segment.



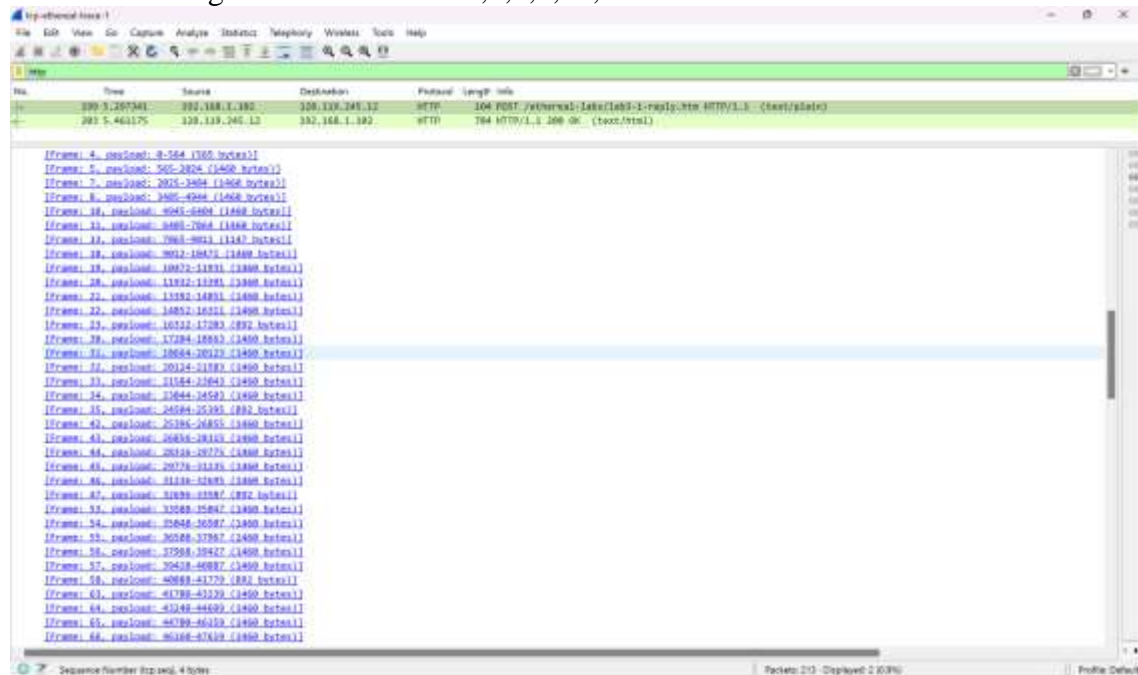
6. What is the sequence number of the TCP segment containing the HTTP POST command?

→ The sequence number of the TCP segment containing the HTTP POST command: 164041

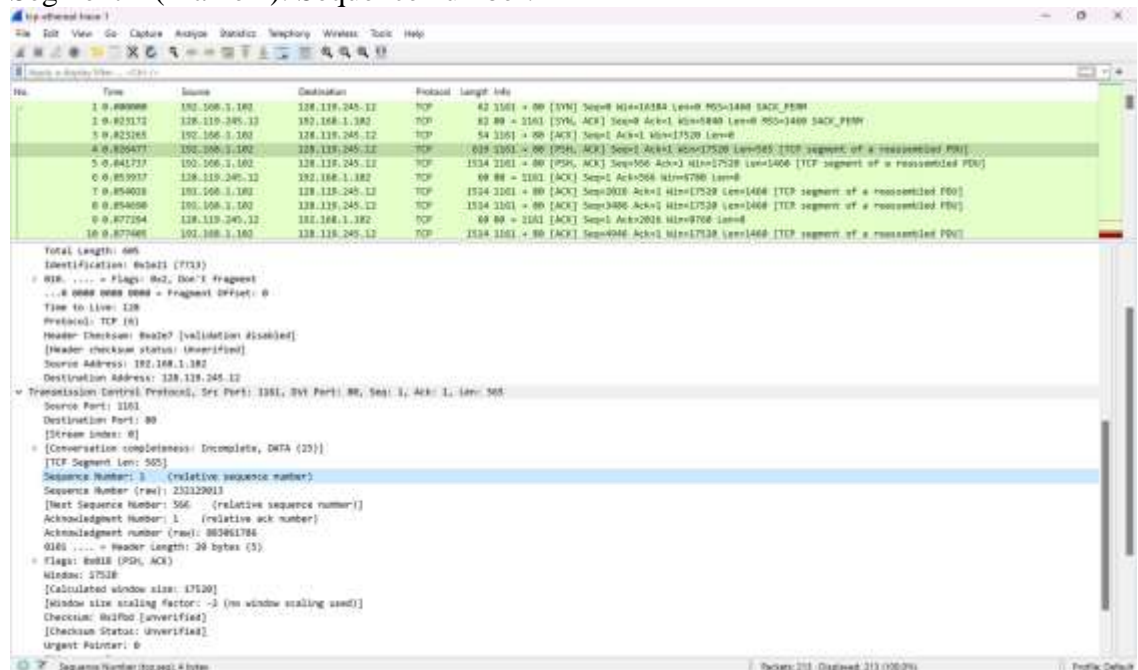


7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? 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 after the receipt of each ACK?

- First six sent segments in the TCP: 4,5,7,8,10,11



- Segment 1 (Frame 4): Sequence number: 1





- Segment 2 (Frame 5): Sequence number: 566

The screenshot shows the Wireshark interface with a packet capture of a TCP segment. The packet list shows a packet with sequence number 566. The packet details pane shows the following information:

- Total Length: 1500
- Identification: 81622 (7734)
- 018 = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header (checksum: 0x9f67 [validation disabled])
- [Header checksum status: Unverified]
- Source Address: 192.168.1.102
- Destination Address: 128.119.245.12
- Transmission Control Protocol, Seq Port: 1181, Dest Port: 80, Seq: 566, Ack: 1, Len: 1460
- Source Port: 1181
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (13)]
- [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): 863061796
- 0102 = Header Length: 20 bytes (5)
- Flags: 0x010 (PSH, ACK)
- Window: 17520
- [Calculated window size: 17520]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0x30a5 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0

- Segment 3 (Frame 7): Sequence number: 2026

The screenshot shows the Wireshark interface with a packet capture of a TCP segment. The packet list shows a packet with sequence number 2026. The packet details pane shows the following information:

- Total Length: 1500
- Identification: 81623 (7735)
- 018 = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header (checksum: 0x9f66 [validation disabled])
- [Header checksum status: Unverified]
- Source Address: 192.168.1.102
- Destination Address: 128.119.245.12
- Transmission Control Protocol, Seq Port: 1181, Dest Port: 80, Seq: 2026, Ack: 1, Len: 1400
- Source Port: 1181
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (13)]
- [TCP Segment Len: 1400]
- Sequence Number: 2026 (relative sequence number)
- Sequence Number (raw): 232130030
- [Next Sequence Number: 3486 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 863061796
- 0102 = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- Window: 17520
- [Calculated window size: 17520]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xd98e [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0



- Segment 4 (Frame 8): Sequence number: 3486

Wireshark packet capture analysis of Segment 4 (Frame 8). The packet list shows a TCP segment with sequence number 3486. The packet details pane shows the TCP header and options, including the sequence number 3486 and the acknowledgment number 1.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.041737	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=566 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
9	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=8760 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=2026 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
8	0.054090	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=3486 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077400	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=4946 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=5496 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
12	0.104890	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	60	1201 → 1161 [ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
14	0.169128	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0

Total Length: 1500
Identification: 0x1e24 (7736)
018 = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header (checksum: 0x9f65 [validation disabled])
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.119.245.12
= Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 3486, Ack: 1, Len: 1460
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (13)]
[TCP Segment Len: 1460]
Sequence Number: 3486 (relative sequence number)
Sequence Number (raw): 23212436
[Next Sequence Number: 4946 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061794
0102 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x9f65 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Sequence Number (tcp.seq): 4 bytes
Packets: 213 / Displayed: 213 (100.0%)
Profile: Default

- Segment 5 (Frame 10): Sequence number: 4946

Wireshark packet capture analysis of Segment 5 (Frame 10). The packet list shows a TCP segment with sequence number 4946. The packet details pane shows the TCP header and options, including the sequence number 4946 and the acknowledgment number 1.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.041737	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=566 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
9	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=8760 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=2026 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
8	0.054090	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=3486 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077400	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=4946 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	60	1514 → 1161 [ACK] Seq=5496 Ack=1 Win=17520 Len=0 [TCP segment of a reassembled PDU]
12	0.104890	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	60	1201 → 1161 [ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
14	0.169128	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0

Total Length: 1500
Identification: 0x1e25 (7737)
018 = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header (checksum: 0x9f64 [validation disabled])
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.119.245.12
= Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 4946, Ack: 1, Len: 1460
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (13)]
[TCP Segment Len: 1460]
Sequence Number: 4946 (relative sequence number)
Sequence Number (raw): 23213058
[Next Sequence Number: 6406 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061794
0102 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x9f64 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Sequence Number (tcp.seq): 4 bytes
Packets: 213 / Displayed: 213 (100.0%)
Profile: Default



- Segment 6 (Frame 11): Sequence number: 6406

Wireshark packet capture analysis of Segment 6 (Frame 11). The packet list shows a TCP segment with sequence number 6406. The packet details pane shows the TCP header and options, including the acknowledgment number 1181 and the window size 17520. The packet bytes pane shows the raw data of the segment.

- The ACK for each segment:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.026477	192.168.1.102	128.119.245.12	TCP	60	60 → 1181 [ACK] Seq=566 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	60	60 → 1181 [ACK] Seq=566 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
6	0.054026	128.119.245.12	192.168.1.102	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
7	0.054690	192.168.1.102	128.119.245.12	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
8	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
9	0.077405	192.168.1.102	128.119.245.12	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
10	0.078157	128.119.245.12	192.168.1.102	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
13	0.124185	192.168.1.102	128.119.245.12	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
14	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
15	0.217299	192.168.1.102	128.119.245.12	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1181 [ACK] Seq=2026 Ack=1 Wln=17520 Len=0 [TCP segment of a reassembled PDU]

Segment	Sent time	ACK received time	RTT (seconds)
1	0.026477	0.053937	0.02746
2	0.041737	0.077294	0.035557
3	0.054026	0.124085	0.070059
4	0.054690	0.169118	0.114428
5	0.077405	0.217299	0.139894
6	0.078157	0.267802	0.189645

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

→ The length of the first TCP segment is 565 bytes:

The screenshot shows a Wireshark packet capture of a TCP connection. The first six segments are highlighted in the packet list:

- Frame 1: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=1, Len=565, TCP segment of a reassembled PDU.
- Frame 2: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=565, Len=1460, TCP segment of a reassembled PDU.
- Frame 3: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=1130, Len=1460, TCP segment of a reassembled PDU.
- Frame 4: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=1695, Len=1460, TCP segment of a reassembled PDU.
- Frame 5: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=2260, Len=1460, TCP segment of a reassembled PDU.
- Frame 6: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=2825, Len=1460, TCP segment of a reassembled PDU.

The packet details pane for the first segment shows:

- Source Port: 1131
- Destination Port: 80
- Stream index: 0
- Conservative completeness: Incomplete, Data (15)
- TCP Segment Len: 565
- Sequence Number: 1 (relative sequence number)
- Next Sequence Number: 565 (relative sequence number)
- Acknowledgment Number: 1 (relative ack number)
- Flags: RST (RST, ACK)
- Window: 17520
- Checksum: 0x0000 (unverified)
- Urgent Pointer: 0

→ The length of each of the following four TCP segments is 1460 bytes:

The screenshot shows the next four segments in the Wireshark packet capture:

- Frame 2: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=565, Len=1460, TCP segment of a reassembled PDU.
- Frame 3: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=1130, Len=1460, TCP segment of a reassembled PDU.
- Frame 4: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=1695, Len=1460, TCP segment of a reassembled PDU.
- Frame 5: 1.0.0.0.0.0.0.0 → 10.0.0.0.0.0.0.0, Seq=2260, Len=1460, TCP segment of a reassembled PDU.

The packet details pane for the second segment shows:

- Source Port: 1131
- Destination Port: 80
- Stream index: 0
- Conservative completeness: Incomplete, Data (21)
- TCP Segment Len: 1460
- Sequence Number: 565 (relative sequence number)
- Next Sequence Number: 1130 (relative sequence number)
- Acknowledgment Number: 1 (relative ack number)
- Flags: RST (RST, ACK)
- Window: 17520
- Checksum: 0x0000 (unverified)
- Urgent Pointer: 0

Wireshark

File Edit View Go Capture Analysis Statistics Network Windows Help

Packet List | Packet Details | Packet Bytes

Filter: tcp.flags.reset

No. Time Source Destination Protocol Length Info

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
1	0.001272	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
2	0.001572	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
3	0.001872	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
4	0.002172	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
5	0.002472	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
6	0.002772	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
7	0.003072	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
8	0.003372	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
9	0.003672	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
10	0.003972	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
11	0.004272	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
12	0.004572	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
13	0.004872	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
14	0.005172	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
15	0.005472	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
16	0.005772	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
17	0.006072	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
18	0.006372	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
19	0.006672	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
20	0.006972	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
21	0.007272	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
22	0.007572	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
23	0.007872	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
24	0.008172	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
25	0.008472	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
26	0.008772	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
27	0.009072	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
28	0.009372	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
29	0.009672	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
30	0.009972	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
31	0.010272	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
32	0.010572	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
33	0.010872	192.168.1.101	192.168.1.102	TCP	60	5182 → 5181 [RST] Seq=5182884464 Win=0 Len=0 RST (RST)
34	0.011172	192.168.1.101	192.168			

[illegible]

→ The length of the sixth TCP segment is 1147 bytes:

[illegible]

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?

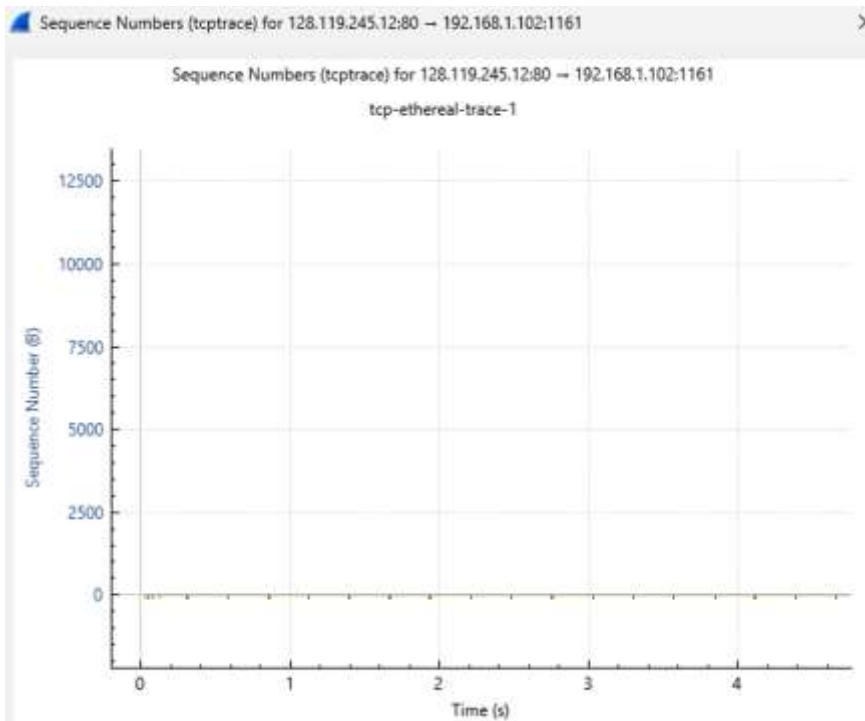
- The minimum amount of available buffer space advertised at the received for the entire trace: 5840
- The lack of receiver buffer space never ever throttle the sender

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 88 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.003272	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Min=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 88 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	618	1161 → 88 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 88 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1468 [TCP segment of a reassembled PDU]
6	0.051937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6788 Len=0
7	0.054826	192.168.1.102	128.119.245.12	TCP	1514	1161 → 88 [ACK] Seq=2926 Ack=1 Win=17520 Len=1468 [TCP segment of a reassembled PDU]
8	0.054880	192.168.1.102	128.119.245.12	TCP	1514	1161 → 88 [ACK] Seq=3486 Ack=1 Win=17520 Len=1468 [TCP segment of a reassembled PDU]
9	0.077204	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=8740 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 88 [ACK] Seq=4946 Ack=1 Win=17520 Len=1468 [TCP segment of a reassembled PDU]
11	0.079357	192.168.1.102	128.119.245.12	TCP	1514	1161 → 88 [ACK] Seq=6406 Ack=1 Win=17520 Len=1468 [TCP segment of a reassembled PDU]
12	0.124005	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11880 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1281	1161 → 88 [PSH, ACK] Seq=7806 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]

10. 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 (192.168.1.102) to the destination (128.119.245.12) 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.





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).

	acknowledged sequence number	acknowledged data
ACK 1	566	565
ACK 2	2026	1460
ACK 3	3486	1460
ACK 4	4946	1460
ACK 5	6406	1460
ACK 6	7866	1460
ACK 7	9013	1147

Example for the ACK 6:



tcp-ethereal-trace-1						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK]
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq
19	0.305012	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq

> Frame 11: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:2b: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: 6406, Ack: 1, Len: 1460

Source Port: 1161

Destination Port: 80

[Stream index: 0]

> [Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 1460]

Sequence Number: 6406 (relative sequence number)

Sequence Number (raw): 232135418

[Next Sequence Number: 7866 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. By inspecting the amount of acknowledged data by each ACK, there are cases where the receiver is ACKing every other segment. For example, segment of No. 80 acknowledged data with 2920 bytes = 1460*2 bytes.

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

The computation of TCP throughput largely depends on the selection of averaging time period. As a common throughput computation, in this question, we select the average time period as the whole connection time. Then, the average throughput for this TCP connection is computed as the ratio between the total amount data and the total transmission time. The total amount data transmitted can be computed by the difference between the sequence number of the first TCP segment (i.e. 1 byte for No. 4 segment)



and the acknowledged sequence number of the last ACK (164091 bytes for No. 202 segment). Therefore, the total data are $164091 - 1 = 164090$ bytes. The whole transmission time is the difference of the time instant of the first TCP segment (i.e., 0.026477 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 202 segment). Therefore, the total transmission time is $5.455830 - 0.026477 = 5.4294$ seconds. Hence, the throughput for the TCP connection is computed as $164090/5.4294 = 30.222$ KByte/sec.

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
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520 Len=0
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=17520 Len=0
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780 Len=0
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/html)
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
204	5.598090	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
205	5.599082	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
207	6.101044	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
208	6.102069	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
209	6.600152	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
210	6.601063	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1

> Frame 202: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: LinksysGroup_dca:af:73 (00:06:25:da:af:73), Dst: ActiontecEle_8a:70:1a (00:20:00:08:00:1a)

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

Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 0

Source Port: 80

Destination Port: 1161

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 883061786

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

Acknowledgment Number: 164091 (relative ack number)

Acknowledgment number (raw): 232293103

0101 = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window: 62780

[Calculated window size: 62780]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x04a8 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[Time since first frame in this TCP stream: 5.455830000 seconds]

[Time since previous frame in this TCP stream: 0.007943000 seconds]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 199]

[The RTT to ACK the segment was: 0.158489000 seconds]

[iRTT: 0.023265000 seconds]

Acknowledgment Number (tcp.ack), 4 bytes

Packets: 213 - Displayed: 213 (100.0%)

Profile: Default

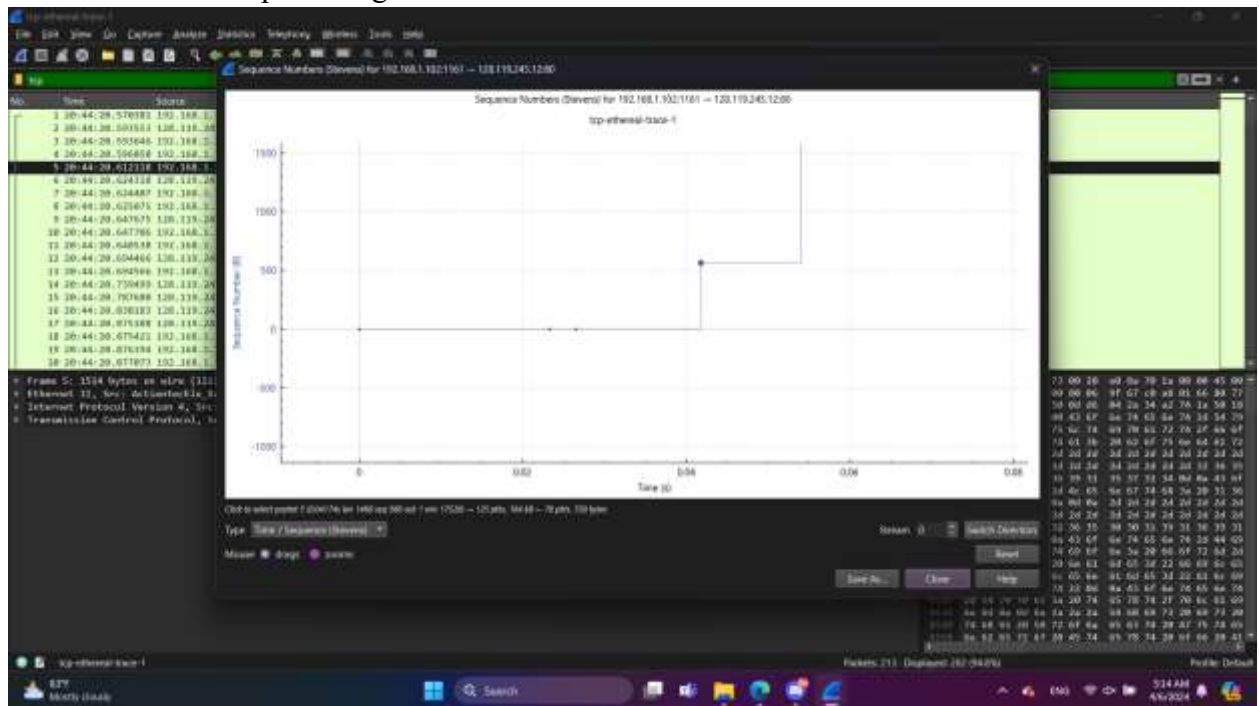
No.4 segment:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [

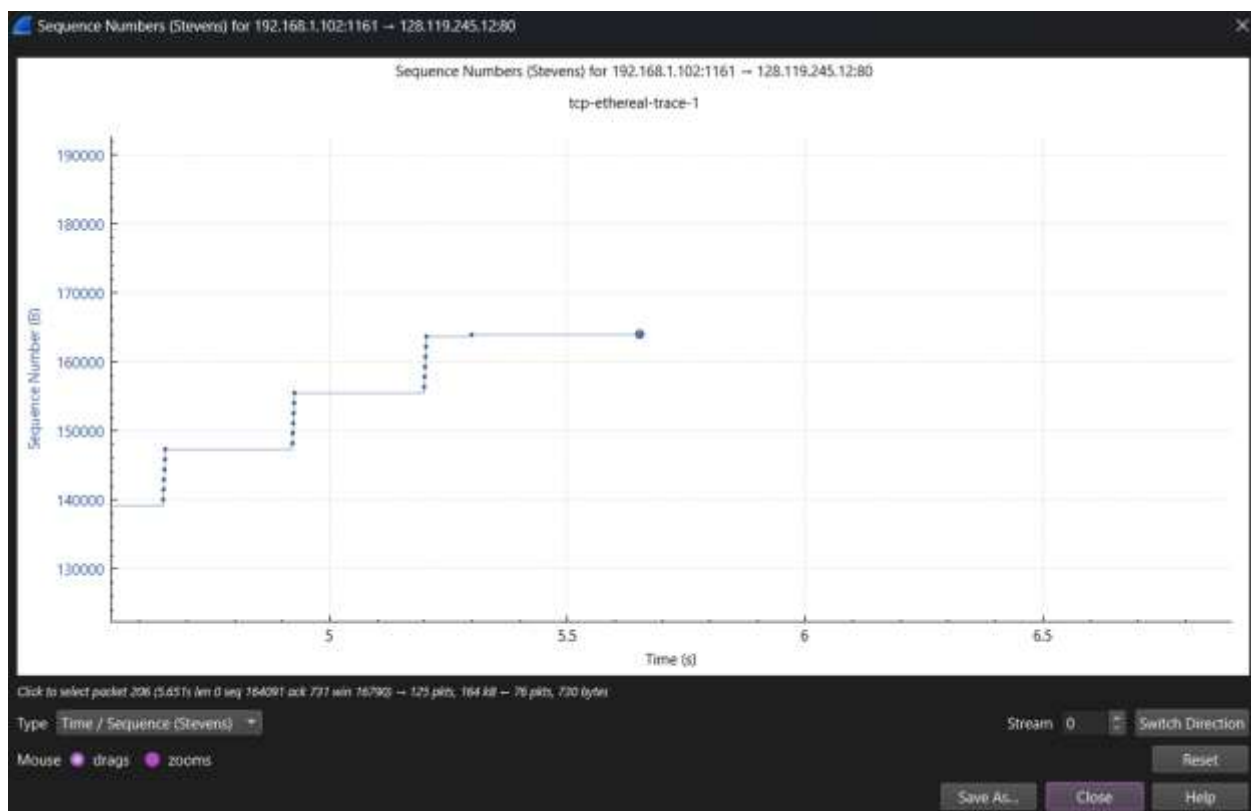
Task 4

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.

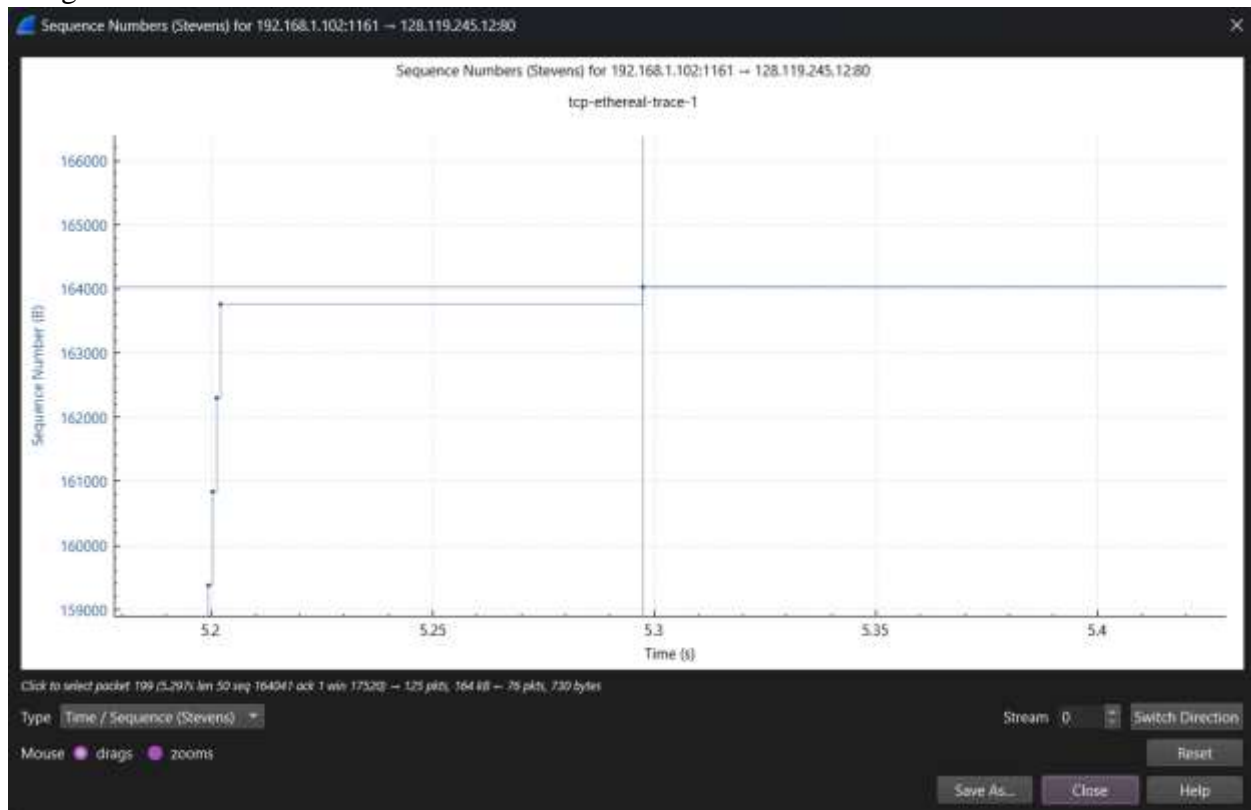
→ TCP's slowstart phase begins:



TCP's slowstart phase ends:



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:

By observing the plot, we can see that the slow-start phase only lasts for first 1-1.5 second. Afterwards, it seems that the TCP session is always in congestion avoidance state. In this case, we do not observe the expected linear increase behaviour, i.e. the TCP transmit window does not grow linearly during this phase. In fact, it appears that the sender transmits packets in batches of 6. This does not seem to be caused by flow control since the receiver advertised window is significantly larger than 5 packets. The reason for this behaviour might be due to the fact that the HTTP server has enforced a rate-limit of some sort.

