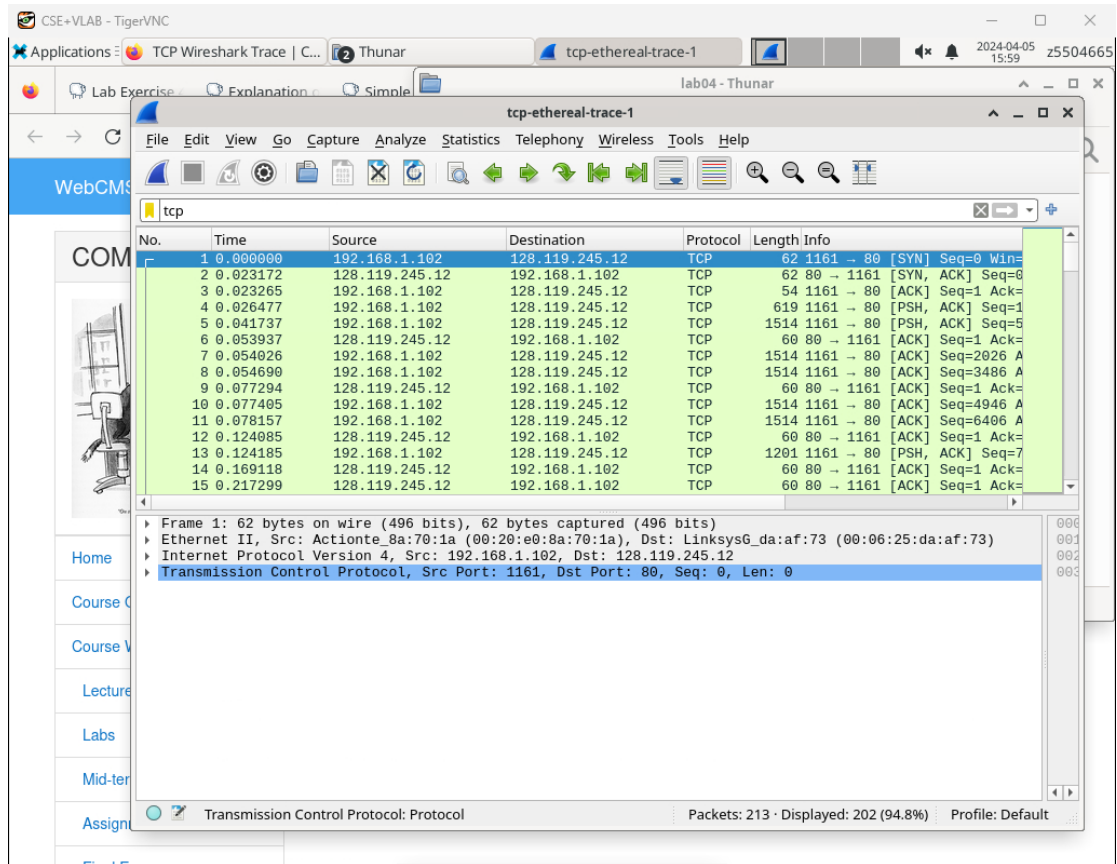


Lab4

Exercise 1

Q1

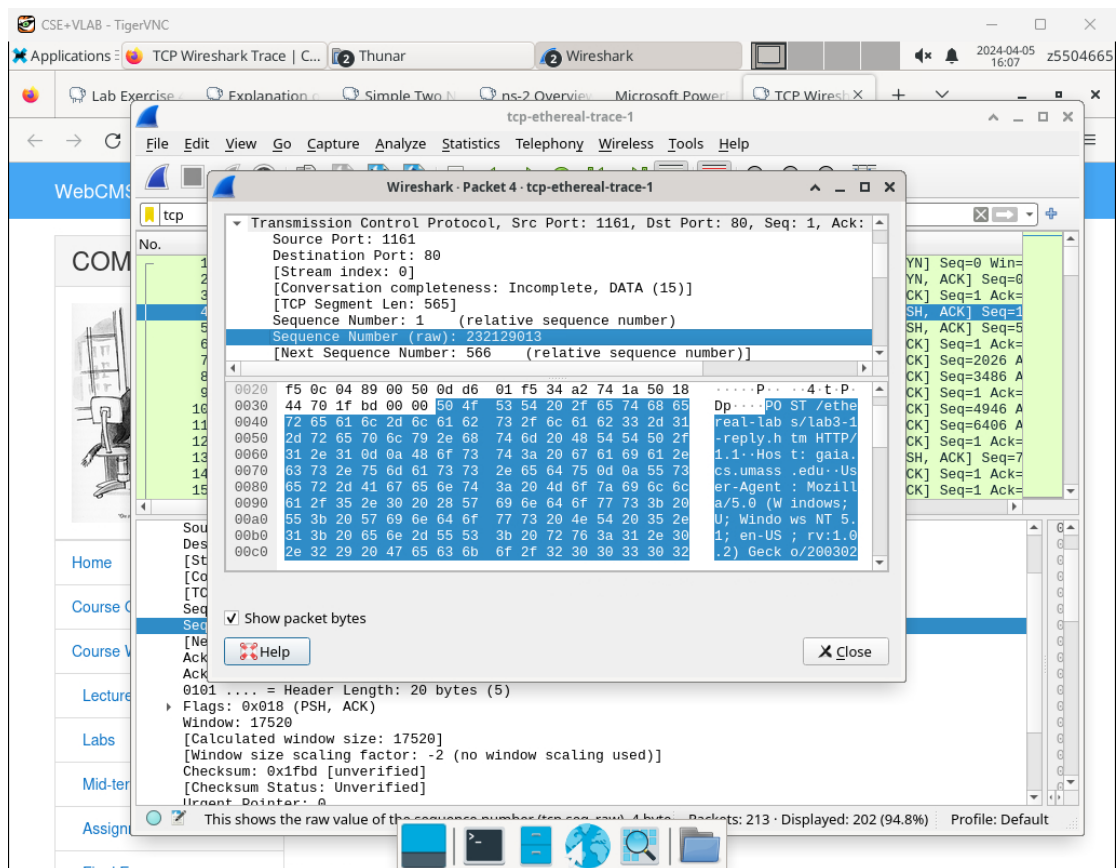


The IP address of gaia.cs.umass.edu: 128.119.245.12

Sending port: 1161 Receiving port: 80

IP and port: 192.168.1.102:1161

Q2



Sequence Number: 232129013

Q3

a)

The image shows a Wireshark packet capture of a TCP connection. The packet list displays 15 packets. Packet 4 is selected, showing details for a TCP segment. The details pane shows the following information:

- Source Port: 1161
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 565]
- 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

The status bar at the bottom indicates: This shows the raw value of the sequence number (tcp.seq_raw), 4 byte Packets: 213 · Displayed: 202 (94.8%) Profile: Default

The sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST) sent from the client to the webserver are 1,566,2026,3486,4946,6406.

Because the source IP and destination IP are the same which are 192.168.1.102 and 128.119.245.12

b)

The screenshot shows a Wireshark capture of outgoing traffic. The filter is set to 'tcp && (ip.src == 192.168.1.102 && ip.dst == 128.119.245.12)'. The packet list shows 21 packets. The first packet is a SYN packet (No. 1, Time 0.000000, Length 62). The subsequent packets are data packets (Nos. 3, 4, 5, 7, 8, 10, 11, 13, 18, 19, 20, 21) with lengths of 54, 619, 1514, 1514, 1514, 1514, 1514, 1201, 1514, 1514, 1514, and 1514 respectively. The packet details pane shows the selected packet (No. 4) with its TCP and IP headers.

No.	Time	Source	Destination	Length
1	0.000000	192.168.1.102	128.119.245.12	62
3	0.023265	192.168.1.102	128.119.245.12	54
4	0.026477	192.168.1.102	128.119.245.12	619
5	0.041737	192.168.1.102	128.119.245.12	1514
7	0.054026	192.168.1.102	128.119.245.12	1514
8	0.054690	192.168.1.102	128.119.245.12	1514
10	0.077405	192.168.1.102	128.119.245.12	1514
11	0.078157	192.168.1.102	128.119.245.12	1514
13	0.124185	192.168.1.102	128.119.245.12	1201
18	0.305040	192.168.1.102	128.119.245.12	1514
19	0.305813	192.168.1.102	128.119.245.12	1514
20	0.306692	192.168.1.102	128.119.245.12	1514
21	0.307571	192.168.1.102	128.119.245.12	1514

Sending time: 0.026477, 0.041737, 0.054026, 0.054690, 0.077405, 0.078157

The screenshot shows a Wireshark capture of incoming traffic. The filter is set to 'tcp && (ip.dst == 192.168.1.102 && ip.src == 128.119.245.12)'. The packet list shows 16 packets. The first packet is a SYN packet (No. 2, Time 0.023172, Length 62). The subsequent packets are data packets (Nos. 6, 9, 12, 14, 15, 16, 17, 24, 25, 26, 27, 28) with lengths of 60, 60, 60, 60, 60, 60, 60, 60, 60, 60, 60, and 60 respectively. The packet details pane shows the selected packet (No. 9) with its TCP and IP headers.

No.	Time	Source	Destination	Length
2	0.023172	128.119.245.12	192.168.1.102	62
6	0.053937	128.119.245.12	192.168.1.102	60
9	0.077294	128.119.245.12	192.168.1.102	60
12	0.124085	128.119.245.12	192.168.1.102	60
14	0.169118	128.119.245.12	192.168.1.102	60
15	0.217299	128.119.245.12	192.168.1.102	60
16	0.267002	128.119.245.12	192.168.1.102	60
17	0.394807	128.119.245.12	192.168.1.102	60
24	0.356437	128.119.245.12	192.168.1.102	60
25	0.400164	128.119.245.12	192.168.1.102	60
26	0.448613	128.119.245.12	192.168.1.102	60
27	0.500029	128.119.245.12	192.168.1.102	60
28	0.545052	128.119.245.12	192.168.1.102	60

Receiving time: 0.053937, 0.077294, 0.124085, 0.169118, 0.217299, 0.267002

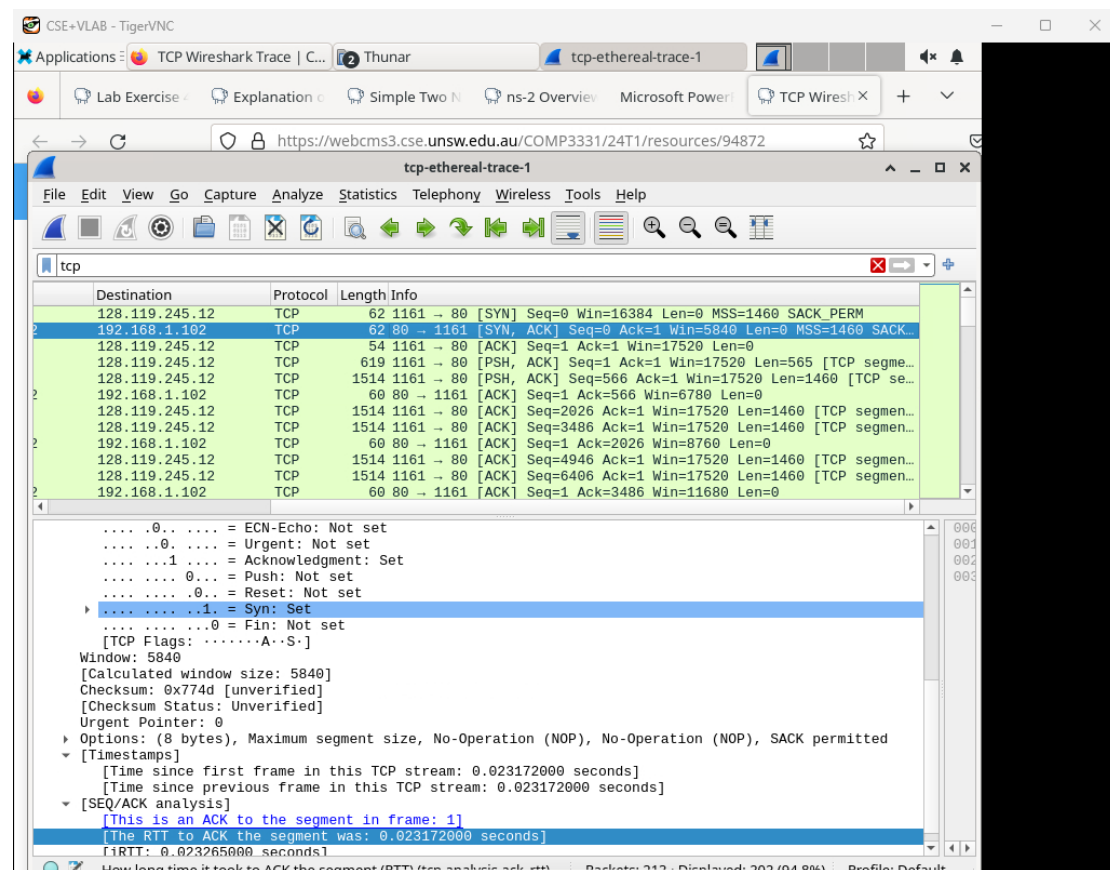
RTT:0.02746, 0.035557, 0.70059, 0.114428, 0.139894, 0.189645

c)

EstimatedRTT=(1-a)×EstimatedRTT+a×SampleRTT,a=0.125

EstimatedRTT: 0.02746, 0.028472, 0.033670, 0.043765, 0.055781, 0.072514

Q4



1)The minimum amount of available buffer space advertised at the receiver for the entire trace is 5840

2)No, it doesn't. Because $5840 > 4MSS=1460*4$

Q5

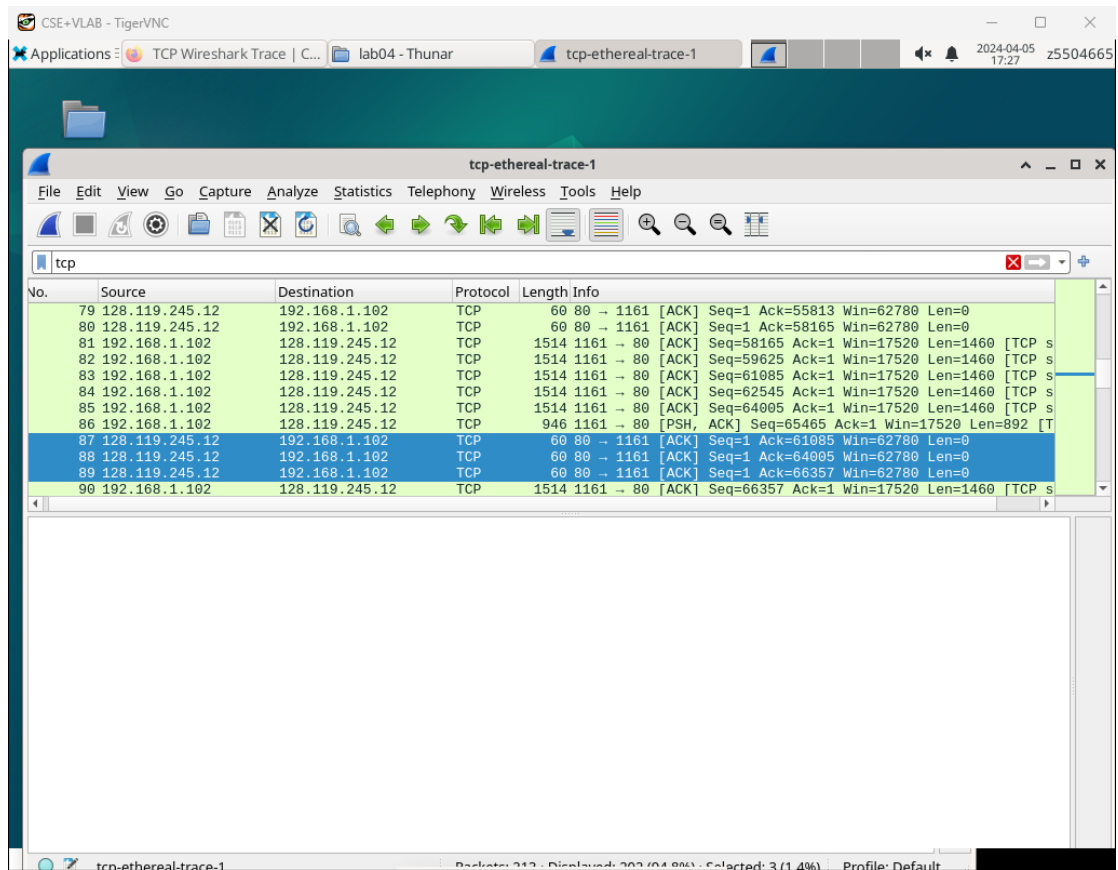
No, there are not. Because there are no packets have the same seq number.

Q6

1)

Most of it are 1460bytes

2)



We can observe that the 89th packet is an acknowledgment of the cumulative acknowledgments before the 86th packet

Q7

The screenshot shows a Wireshark capture of a TCP connection establishment sequence. The packet list table is as follows:

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=
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
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
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=0
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=0
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	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=0
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=0
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0

The packet details pane for packet 4 shows the following TCP flags and window information:

- ECN-Echo: Not set
- Urgent: Not set
- Acknowledgment: Set
- Push: Set
- Reset: Not set
- Syn: Not set
- Fin: Not set
- [TCP Flags:AP...]
- Window: 17520
- [Calculated window size: 17520]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xf574 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [Flags: 0x0100 (ACK)]
- Reserved: Not set
- Accurate ECN: Not set
- Congestion Window Reduced: Not set
- ECN-Echo: Not set

The screenshot shows the continuation of the TCP connection and an HTTP POST request. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
194	5.199275	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=159389 Ack=1 Win=17520
195	5.200252	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=160849 Ack=1 Win=17520
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=17520
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790
213	7.595557	192.168.1.102	199.2.53.206	TCP	62	1162 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=

The packet details pane for packet 206 shows the following TCP flags and window information:

- ECN-Echo: Not set
- Urgent: Not set
- Acknowledgment: Set
- Push: Not set
- Reset: Not set
- Syn: Not set
- Fin: Not set
- [TCP Flags:A...]
- Window: 16790
- [Calculated window size: 16790]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xf574 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [Flags: 0x0100 (ACK)]
- Reserved: Not set
- Accurate ECN: Not set
- Congestion Window Reduced: Not set
- ECN-Echo: Not set

The total elapsed time is calculated by subtracting the time of the first packet transmission

from the time of the last packet transmission.

The throughput is approximate

$$164091 \times 8 / (5.651141 - 0.026477) \approx 233288.86 \text{bps.}$$

Exercise 2

Q1

2818463618

Q2

1)

The sequence number: 1247095790

2)

The value of the Acknowledgement field in the SYNACK segment is 281843619

3)

ack value = sequence number of syn segment + 1

Q3

1)

The sequence number: 2818463619

2)

The value of the Acknowledgement field: 1247095791

3)

No, it doesn't. Because it need building the connect first.

Q4

Both client and server do. The type of closure is Simultaneous close.

Q5

From the client to the server: $2818463653 - 2818463618 - 2 \text{ (syn,fin)} = 33 \text{ bytes}$

From the server to the client: $1247095832 - 1247095790 - 2 \text{ (syn,fin)} = 40 \text{ bytes}$