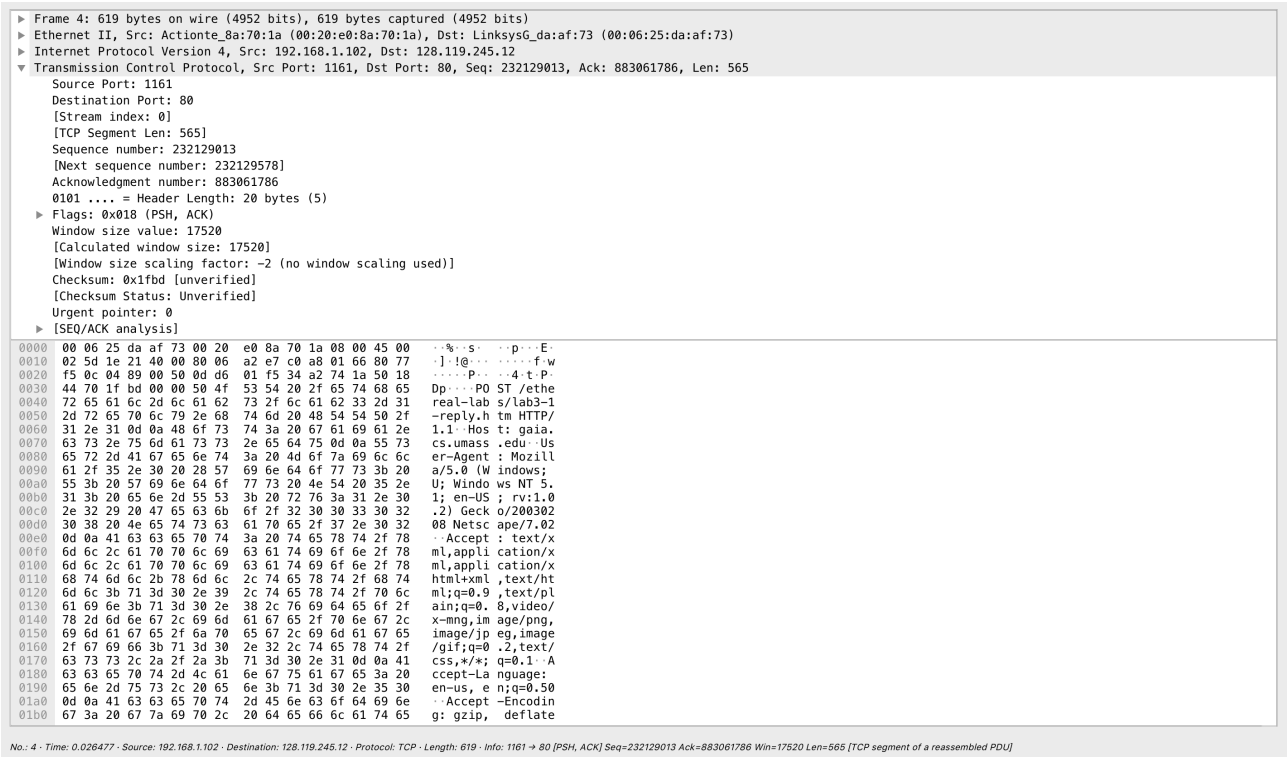
Exercise 1: Understanding TCP using Wireshark

Question 1. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? 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?

- IP address of gaia.cs.umass.edu : 128.119.245.12
- Source Port: 1161, Destination Port: 80
- Client Computer IP: 192.168.1.102
- TCP port number used by the client computer is Port 1161

Question 2. What is the sequence number of the TCP segment containing the HTTP POST command?

- sequence number: 232129013



Question 3 & Question 4.

	Sequence Numbers (From Client to Server)	Sent Time	ACK received Time	RTT	EstimateRTT	Length of TCP segment
1	232129013	0.026477	0.053937	0.027460	0.027460	565
2	232129578	0.041737	0.077294	0.035557	0.028472	1460
3	232131038	0.054026	0.124085	0.070059	0.033670	1460
4	232132498	0.054690	0.169118	0.114428	0.043765	1460
5	232133958	0.077405	0.217299	0.139894	0.055781	1460
6	232135418	0.078157	0.267802	0.189645	0.072514	1460

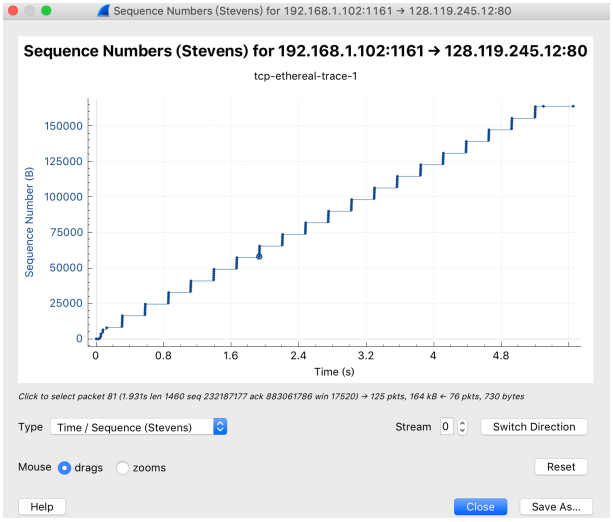
EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

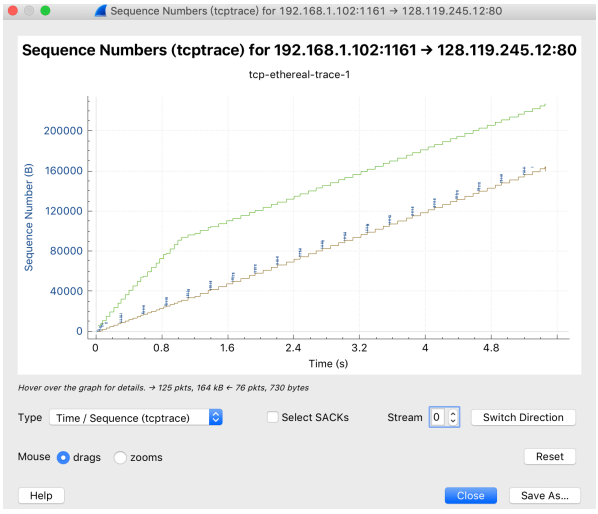
Question 5. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

- Minimum amount of available buffer space at the receiver: 5840 bytes(windows size).
- It does not throttle the sender. The sender is never throttle due to lacking of receiver buffer space in this case, see that the buffer space is always larger than segment size.

Question 6. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

- No, there is no retransmitted segments in the trace file.
- I check for if there are any packets with the same sequence number at different time. And did not find any. All sequence number of segment increasing respect to time.





Question 7. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment?

- Most of ACKs acknowledged 1460 bytes, so the receiver typically acknowledge in an ACK is 1460 bytes.
- The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the amount of data received by the server between these 2 ACKs. By inspecting the amount of acknowledged data by each ACK, there are some cases where the receiver is ACKing every other segments. For example, segment of 80 acknowledged data with 2920 bytes = 1460 * 2 bytes.

Question 8. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

TCP throughput depends on the selection of average time period. TCP throughput is calculated as the ratio between the total amount data and the total transmission time. So R = TotalData / TotalTime.

Total data amount: the acknowledged sequence number of the last ACK(232293103) - the sequence number of the first TCP segment(232129013) = 164090 bytes.

Total time: the last ACK send time(5.455830) - the first time transmission(after TCP connection establishment 0.026477) = 5.429353 sec

Throughout R for the TCP connection = 164090 byte/5.429353 sec = **30222 bytes/sec**

Exercise 2: TCP Connection Management

Question 1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server?

- sequence number of the TCP SYN segment is **2818463618**

Question 2. What is the sequence number of the SYN ACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYN ACK segment? How did the server determine that value?

- sequence number is 1247095790
- value of the Acknowledgement field: 2818463619
- This ACK value is determined by the client SYN seq number + 1

Question 3. What is the sequence number of the ACK segment sent by the client computer in response to the SYNACK? What is the value of the Acknowledgment field in this ACK segment? Does this segment contain any data?

- sequence number response to the SYNACK: **2818463619**
- value of the Acknowledgement field: **1247095791**
- No, this segment does not contain any data.

Question 4. Who has done the active close? client or the server? how you have determined this? What type of closure has been performed? 3 Segment (FIN/ FINACK/ACK), 4 Segment (FIN/ACK/FIN/ACK) or Simultaneous close?

- Both Client and Server does the active close. Because in No.304 and No.305 contain FIN flag as well as ACK.
- The type of closure has been performed is Simultaneous close.

Question 5. How many data bytes have been transferred from the client to the server and from the server to the client during the whole duration of the connection? What relationship does this have with the Initial Sequence Number and the final ACK received from the other side?

- 33 bytes data transferred from the client to the server(1 byte SYN, 1 byte FIN), 40 bytes data transferred from the server to the client(1 byte SYN, 1 byte FIN).
- Data transferred equal to the difference of the Initial Sequence Number and the final ACK received from the other side. That is Final ACK received from the other side = ISN + SYN(1 byte) + The value of bytes transferred + FIN(1 byte)

	Client	Server
ISN	2818463618	1247095790
SYN	1	1
DATA	33	40
FIN	1	1
Total	281846353 (Final ACK of the Server)	1247095832 (Final ACK of the Client)