EECS 3214

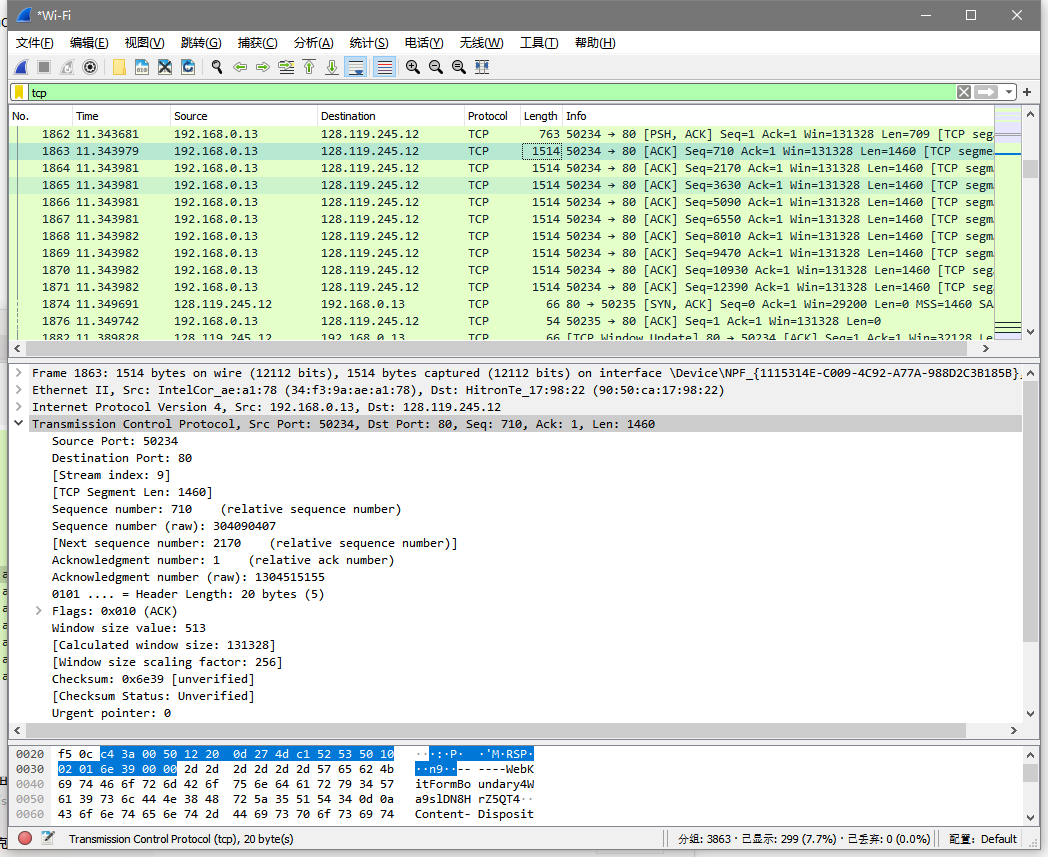
Assignment 3

Instructor: [Natalija Vlajic](http://www.cse.yorku.ca/~vlajic)

Student Name: Tingting Yang

Student ID: 215120579

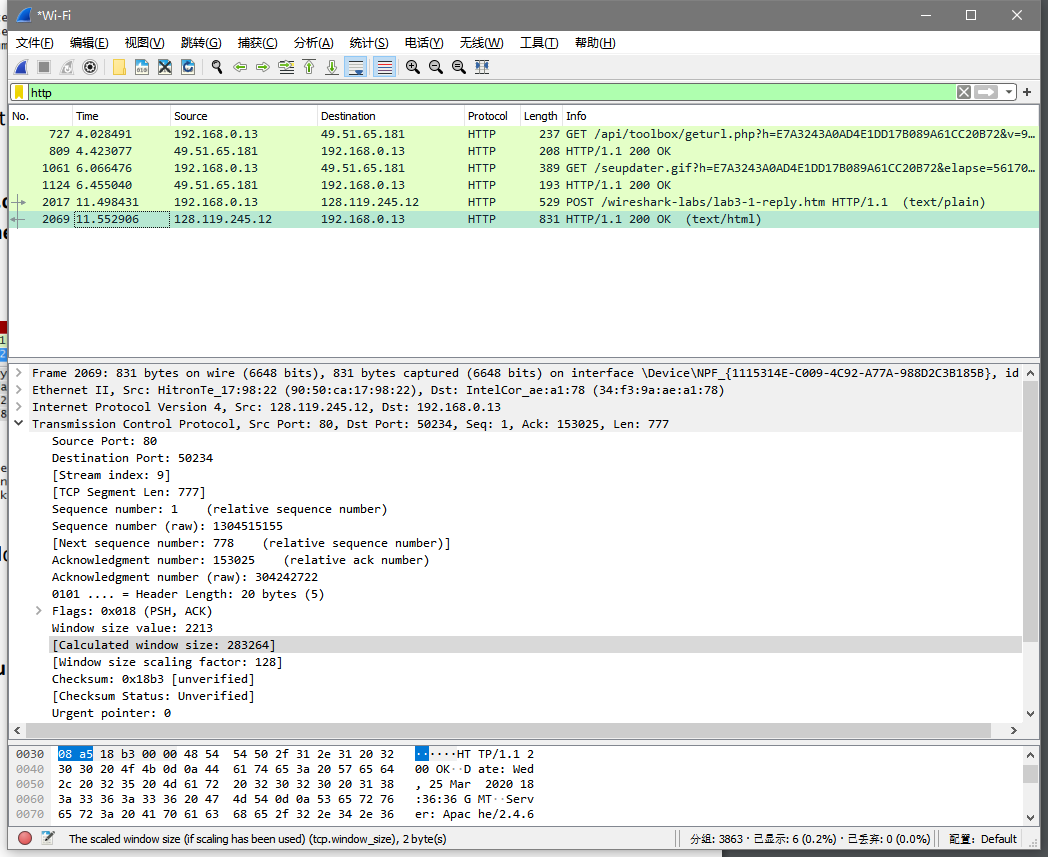
**Question 1:** What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window”.



IP Address: 192.168.0.13

TCP port number: 50234

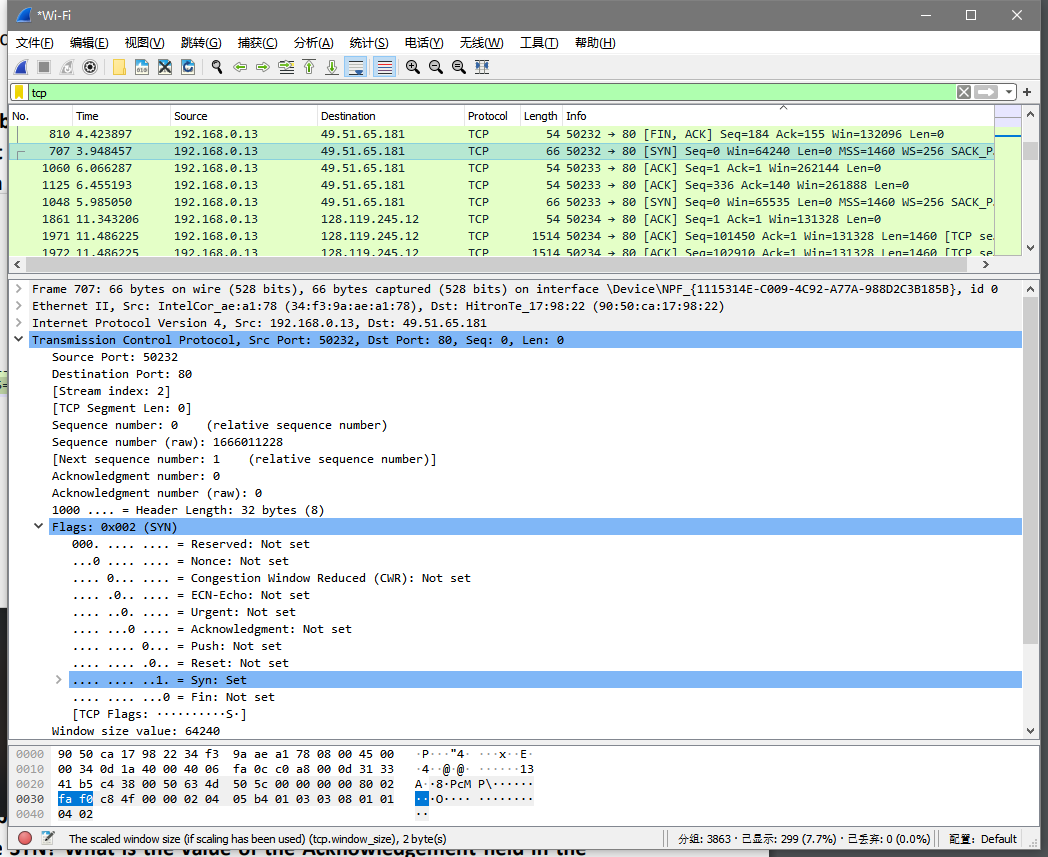
**Question 2**: What is the IP address of gaia.cs.umass.edu server? On what port number is it sending and receiving TCP segments for this connection? Since this lab is about TCP rather than HTTP, let’s change Wireshark’s “listing of captured packets” window so that it shows information about the TCP segments containing the HTTP messages, rather than about the HTTP messages. To have Wireshark do this, select Analyze -> Enabled Protocols. Then uncheck the HTTP box and select OK. Now, we will use the packet trace that you have captured (and/or the packet trace tcpethereal-trace-1 in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip; see earlier footnote) to study TCP behavior in the rest of this lab.



IP Address: 128.119.245.12

Port number: 80

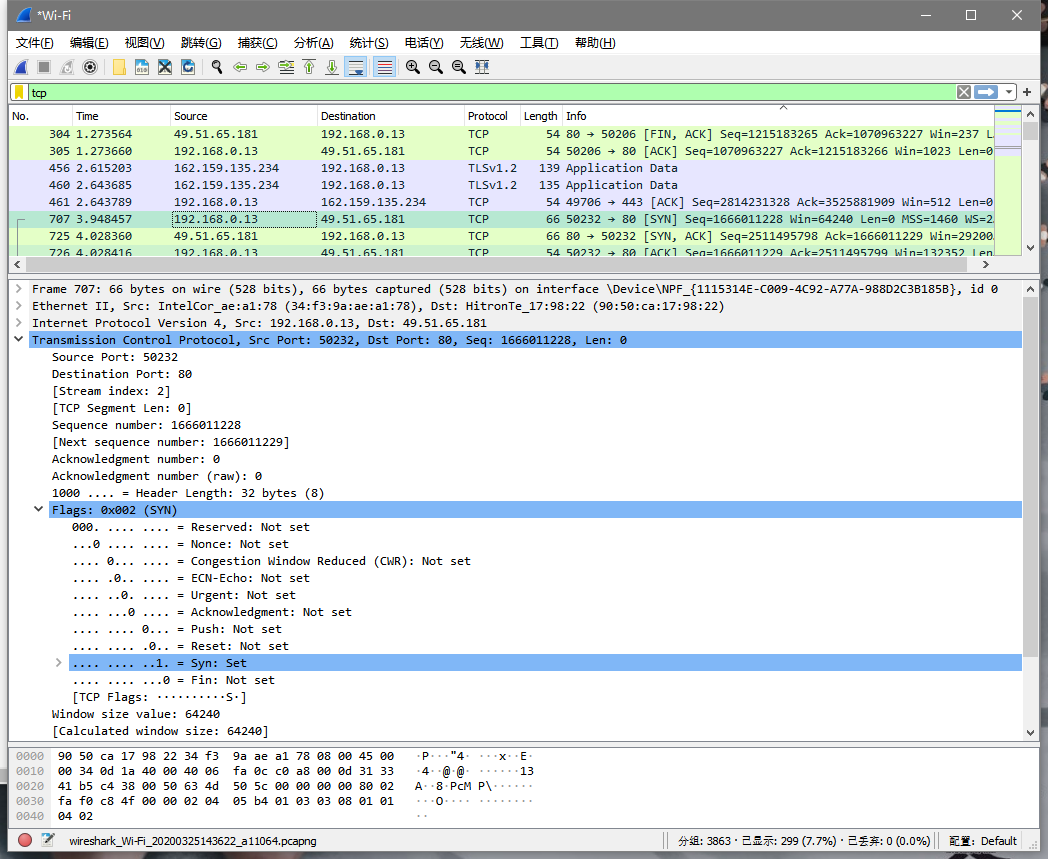
**Question 3**: What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu server? What is it in the segment that identifies the segment as a SYN segment?



Sequence number: 0

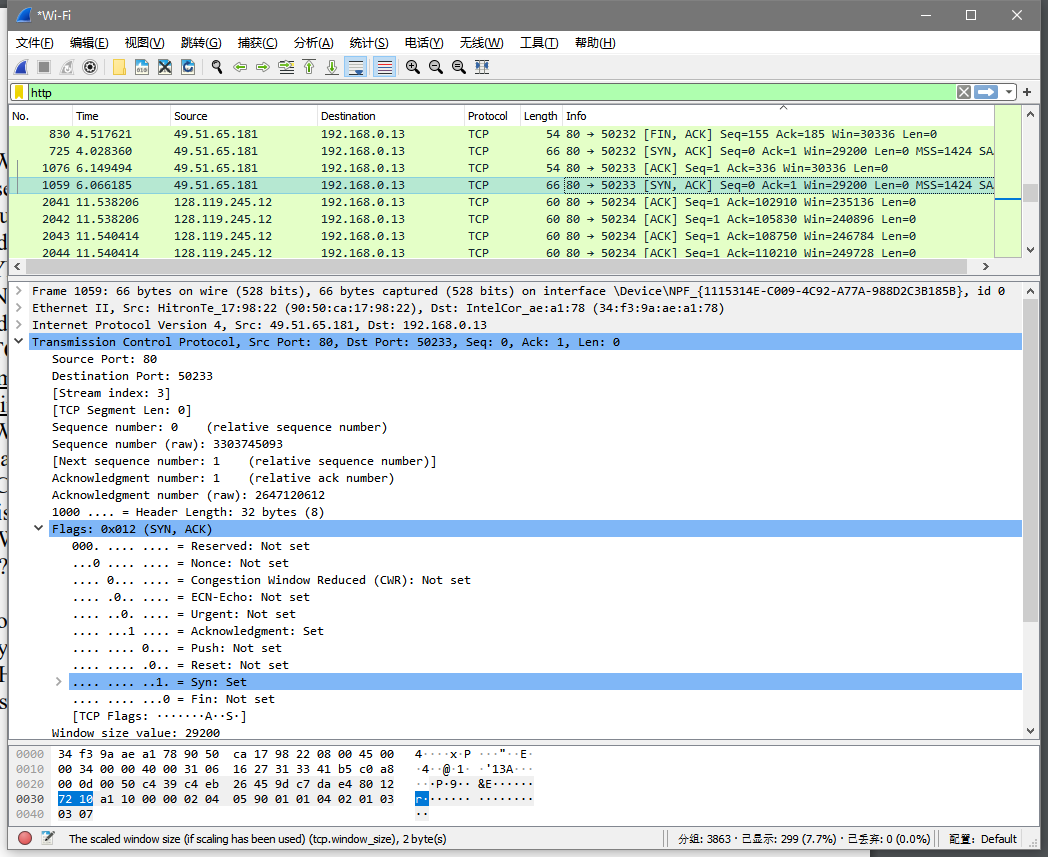
[SYN] flag equals to 1 identifies the segment as a SYN segment.

**Question 4**: In the given TCP SYN segment, Wireshark will most likely display the socalled ‘relative sequence number’. In order to see the actual sequence number, you need to change the TCP display preference by going to Edit -> Preferences -> Protocols -> TCP, and then unchecking the option ‘Relative sequence numbers’, as shown in the below figure. What is the actual sequence number of the (first) TCP SYN segment?



Sequence number: 1666011228

**Question 5**: What are both the relative and the actual sequence number of the SYN ACK segment sent by gaia.cs.umass.edu to the client computer in its reply to the SYN? What is the value of the Acknowledgement field in the SYN ACK segment? How did gaia.cs.umass.edu determine that value? What is it in this segment that identifies the segment as a SYN ACK segment?



5.1

Relative Sequence number: 0

Actual sequence number: 3303745093

5.2

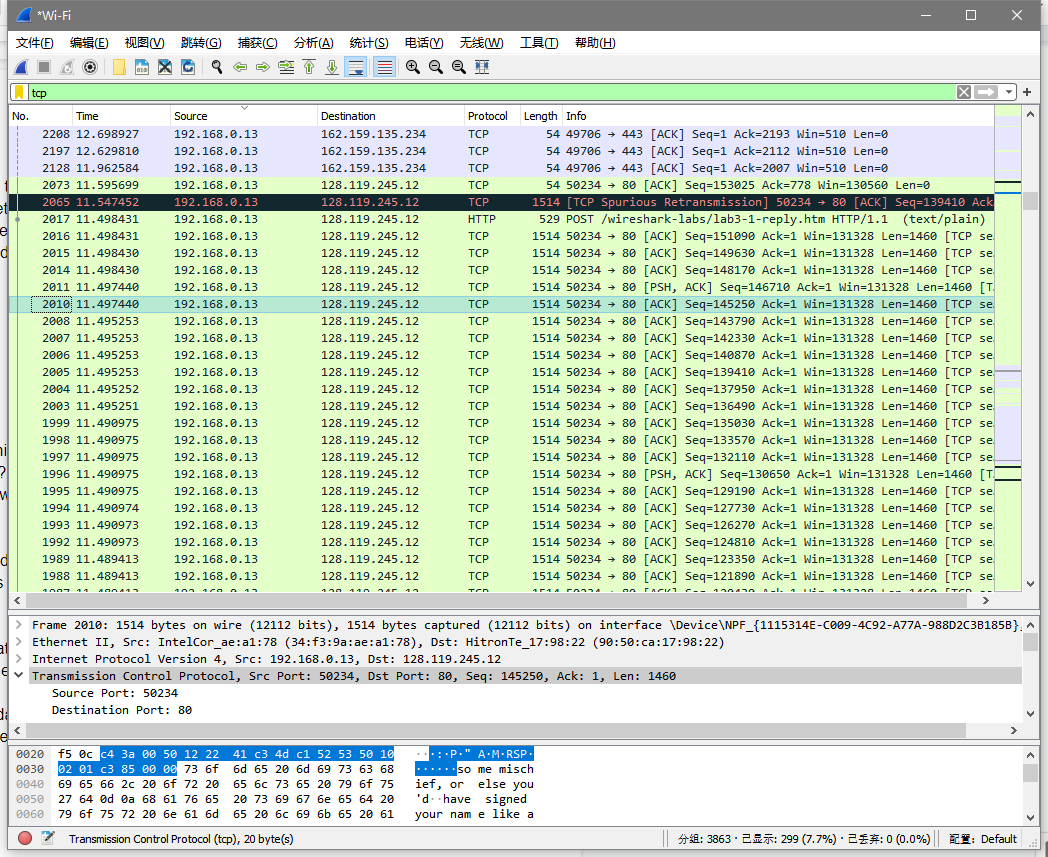
Acknowledgement field: 1

Determined by initial sequence number + 1

5.3

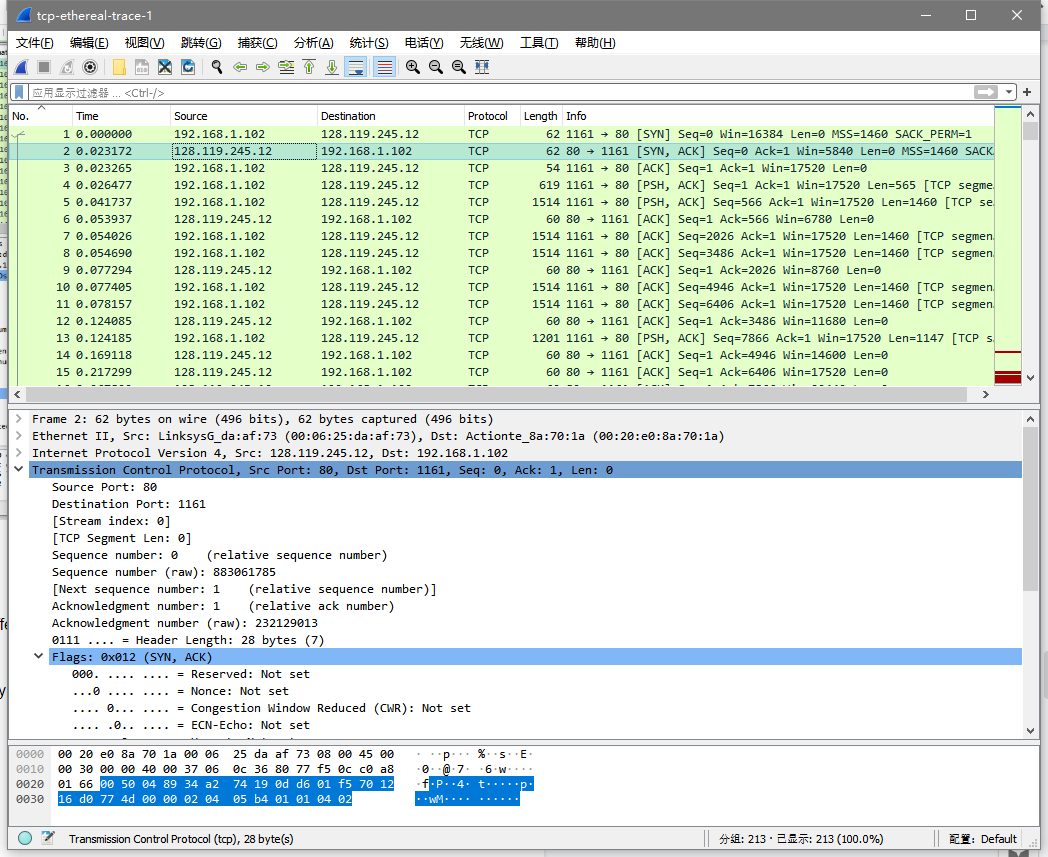
[SYN, ACK] flag identifies the segment as a SYN ACK segment.

**Question 6**: Now observe the TCP segments sent from your computer to gaia.cs.umass.edu server, starting from packet/segment number 8. What is the length of each of these TCP segments?3 (Here you need to read the value of LEN field in the actual TCP segment header, and not the value displayed under Length field/column of Wireshark’s main pane!)



Length: 1460

**Question 7**: What is the initially advertised available buffer space (i.e., Receive Window) of gaia.cs.umass.edu server? Does this value ever change during the lifetime of the observed TCP connection? If so, how, and what is the maximum values of Receive Window advertised by gaia.cs.umass.edu?

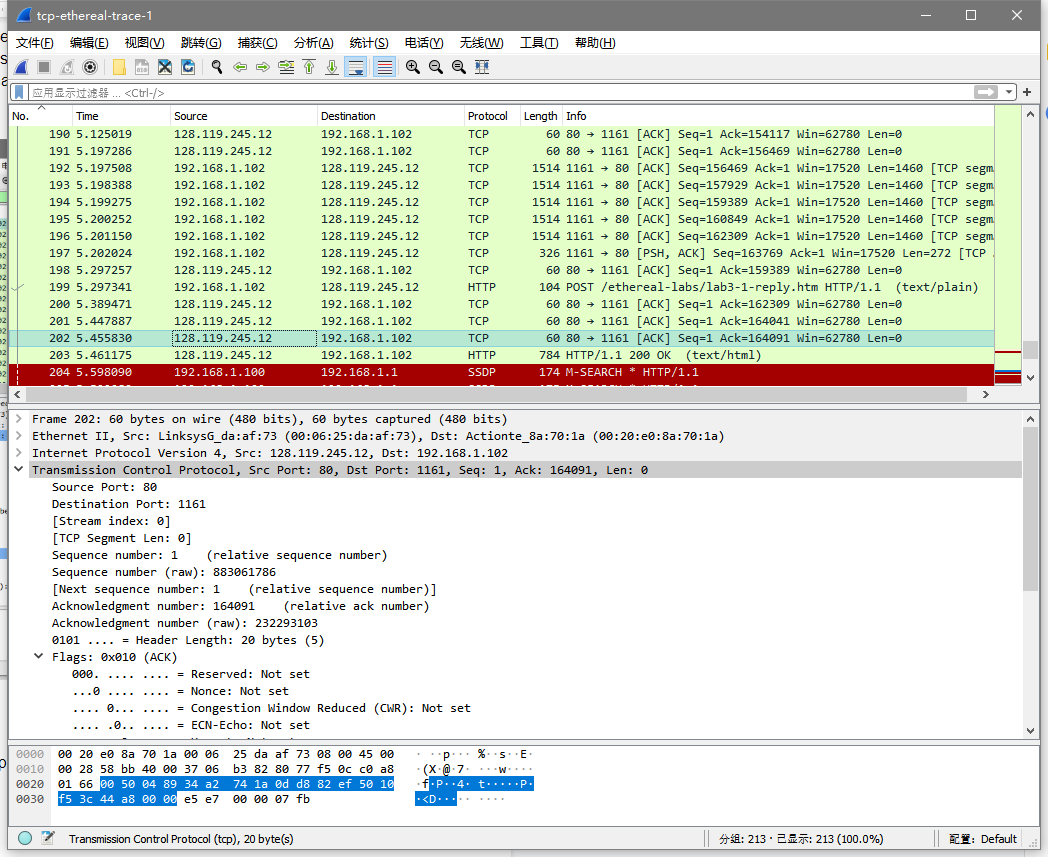


7.1

Initially advertised available buffer space: 5840

7.2

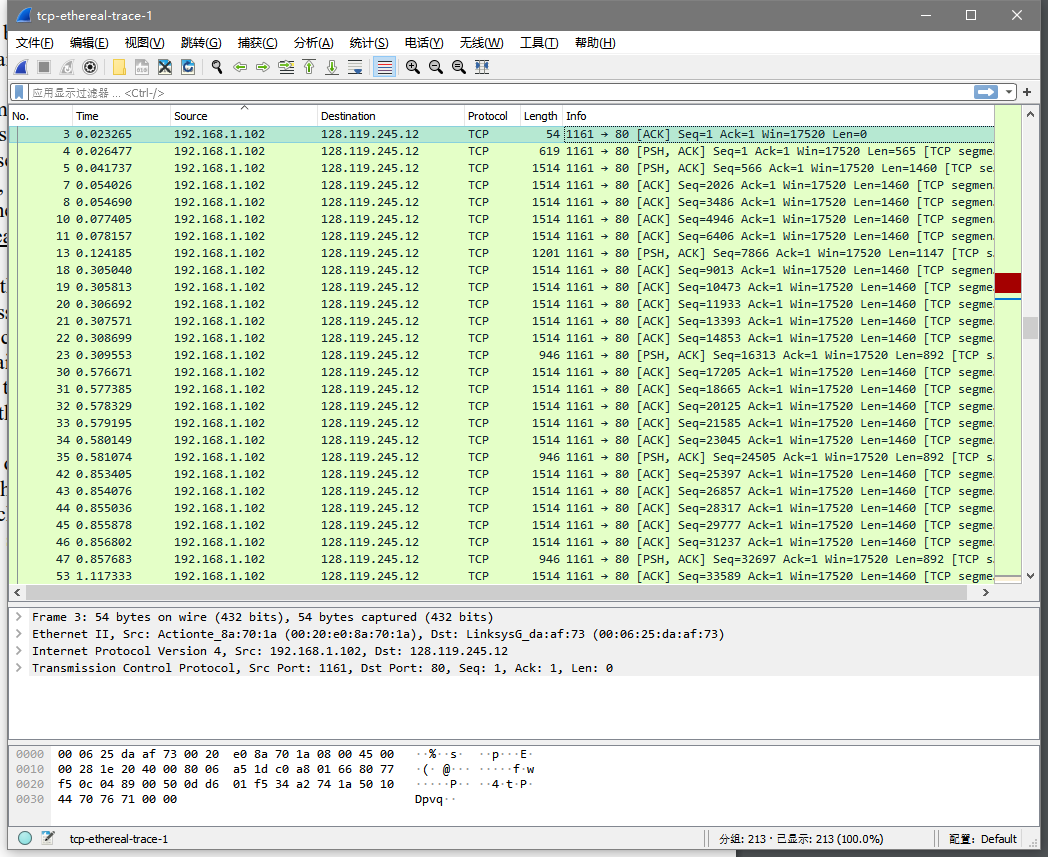
It would change ( grows steadily )



7.3

Maximum value: 62780

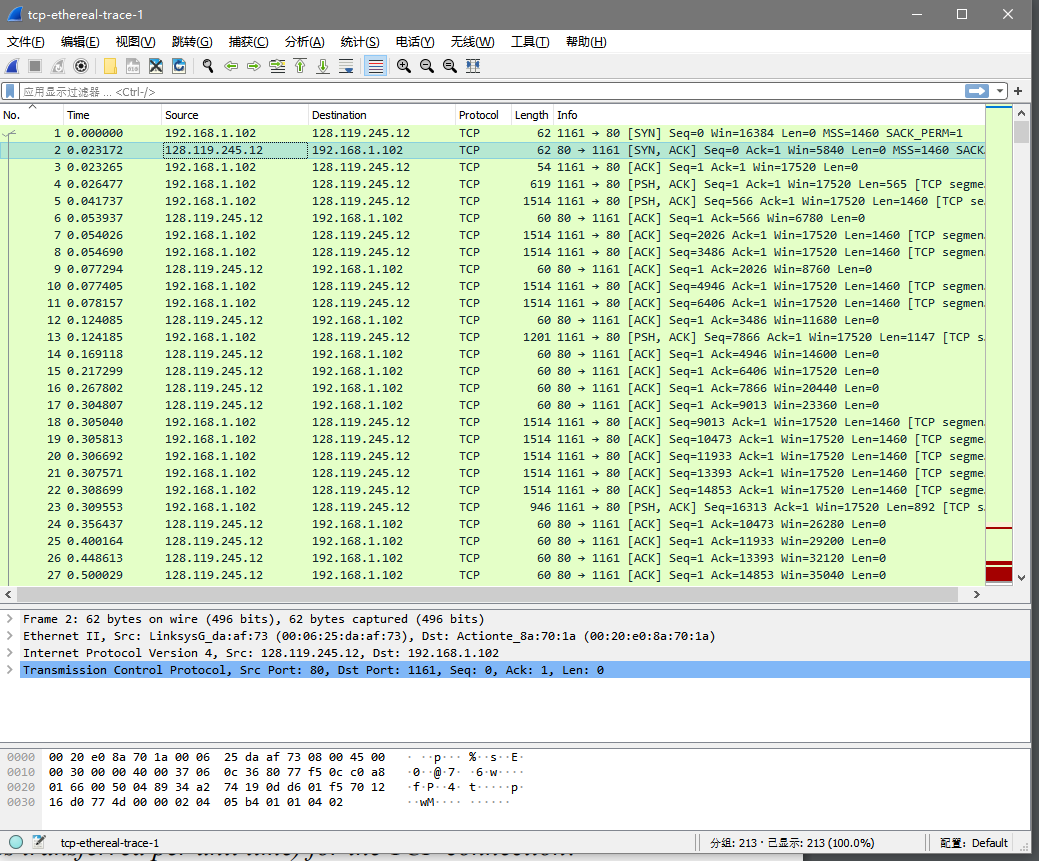
**Question 8**: What is the advertised buffer space (i.e., Receive Window) of your computer/client? Does this value ever change during the lifetime of the observed connection?



Advertised buffer space: 17520

Dosen’t change ( always 17520 )

**Question 9**: How much data does gaia.cs.umass.edu typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment?

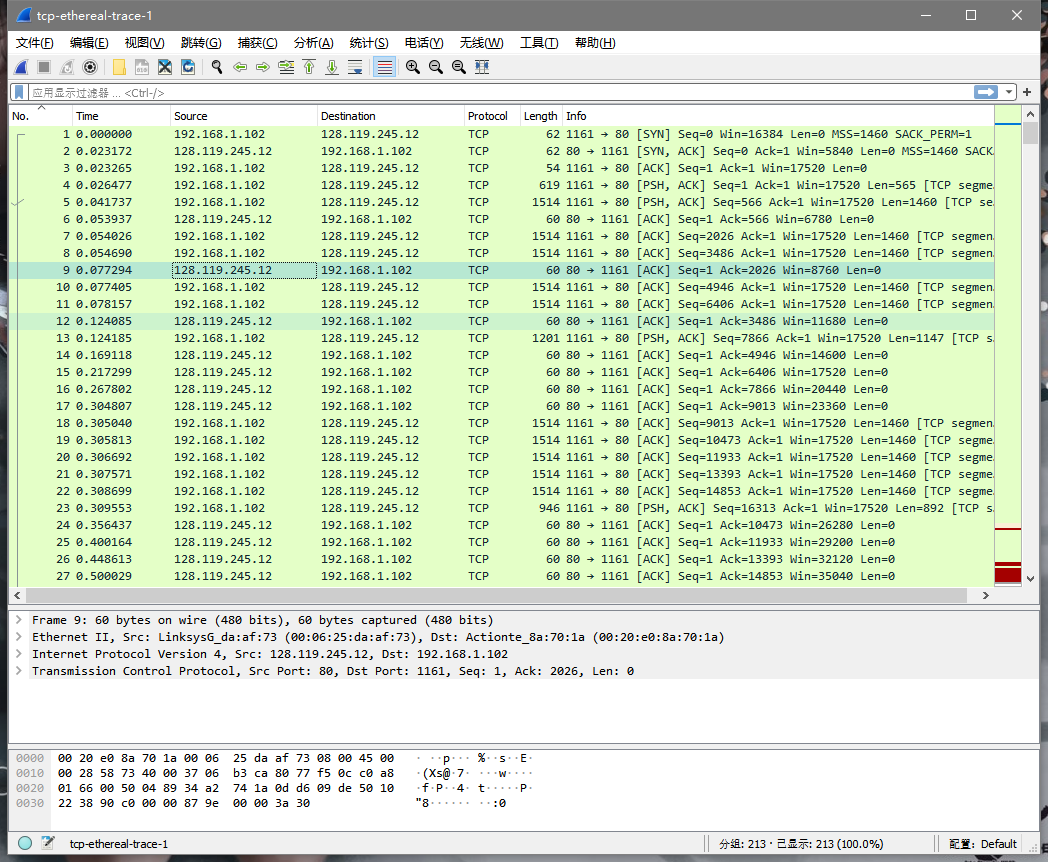


9.1

|  |  |  |
| --- | --- | --- |
|  | acknowledged sequence number | acknowledged data |
| ACK1 | 566 | 1460 |
| ACK2 | 2026 | 1460 |
| ACK3 | 3486 | 1460 |
| ACK4 | 4946 | 1460 |
| ACK5 | 6406 | 1460 |
| ACK6 | 7866 | 1460 |

**...**

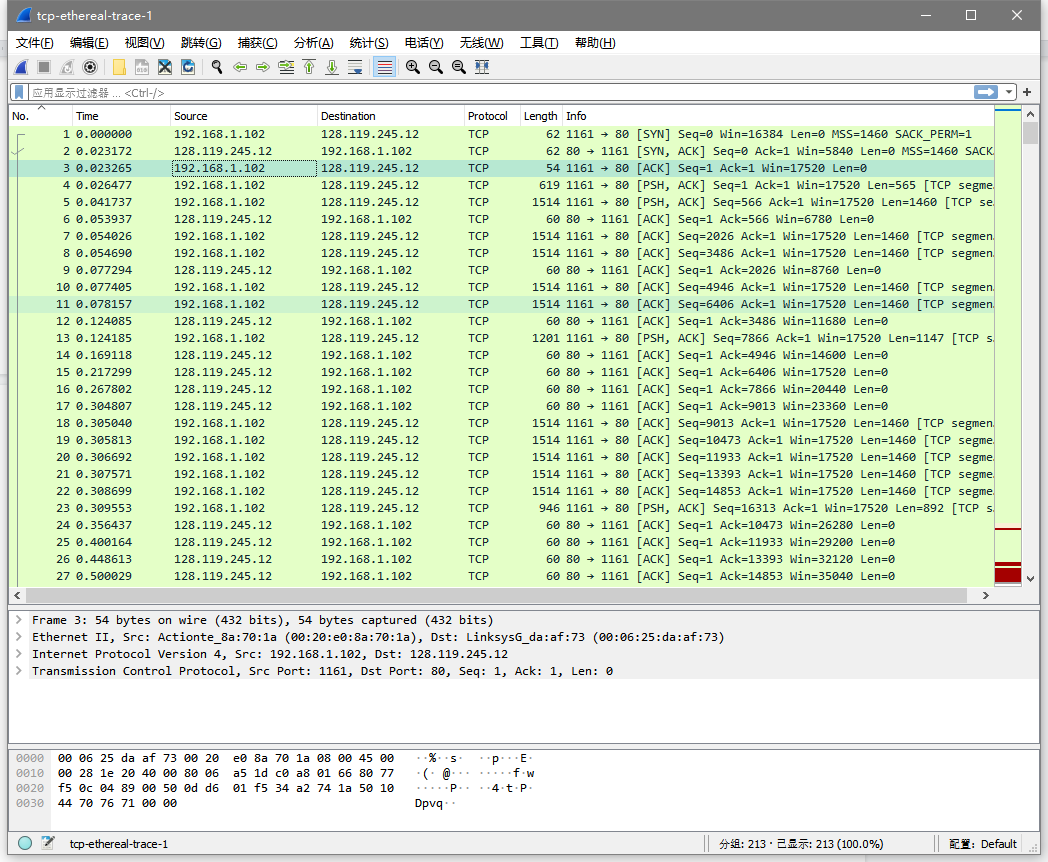
**…**



9.2

For example, at segment No.9, acknowledge data = 1460 = 1460 \* 1

**Question 10**: How much data does your computer/client typically acknowledge in an ACK? Your observation should be very different than in the case of Question 9. Why? Explain!



All the sequence number are 1, Len are 0.