CSC 138

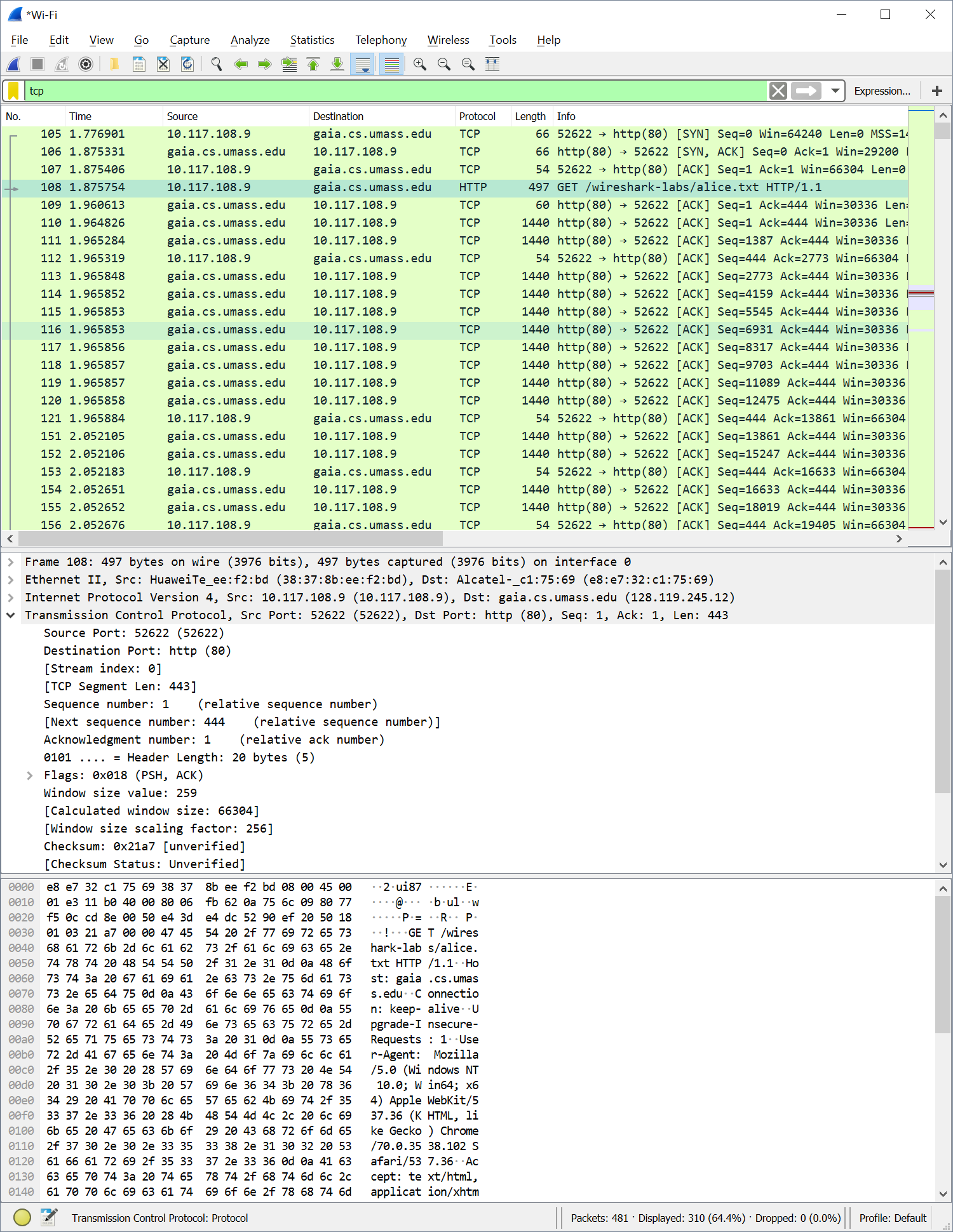
Talal Jawaid

Wireshark Lab 3

12/2/18

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:** The IP Address is 10.117.108.9 and the TCP port is 52662



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?**

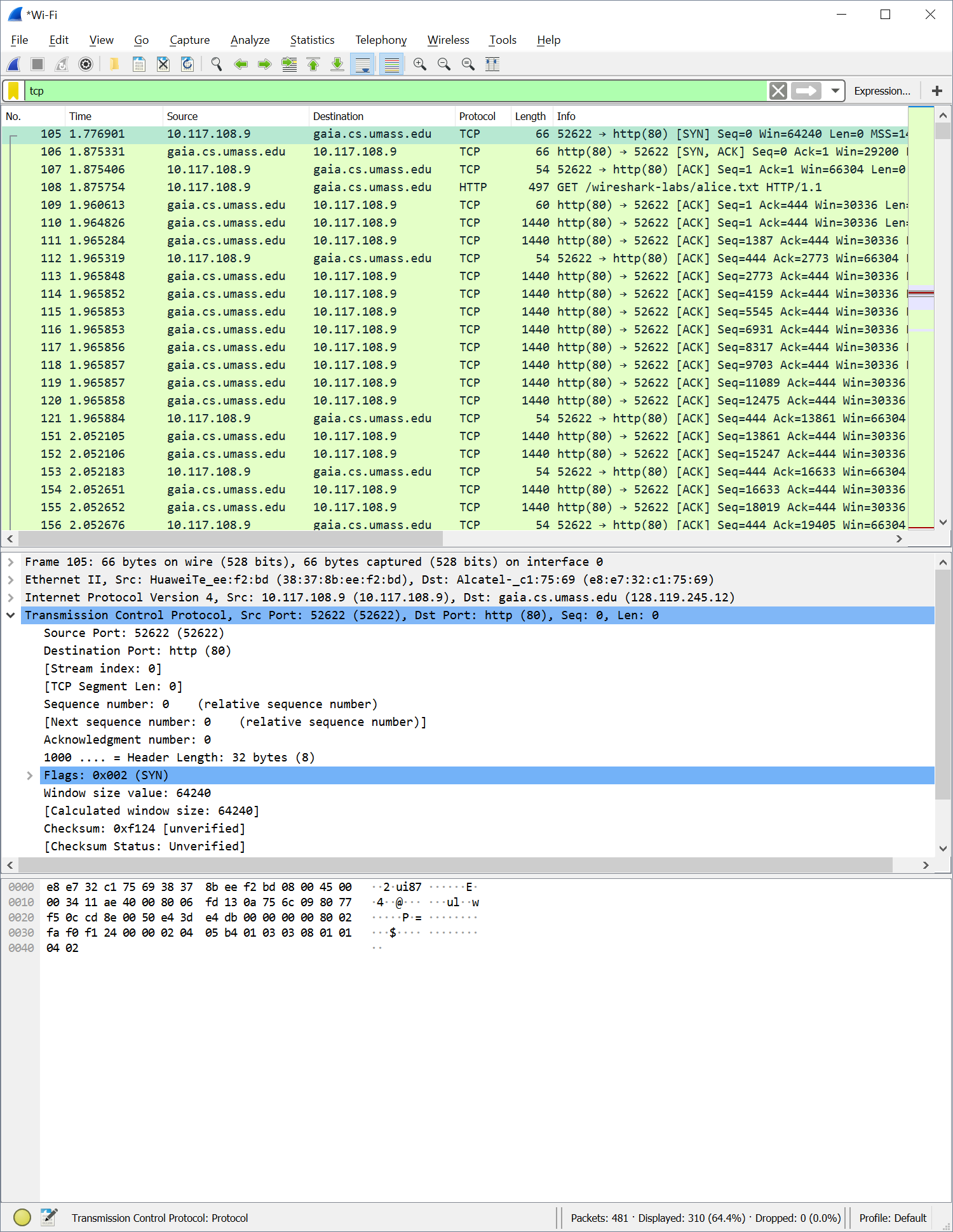
**Answer:** The IP address is 128.119.245.12 and the TCP port is 80 for both sending and receiving

1. **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:** The IP Address is 10.117.108.9 and the TCP port is 52662

1. **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:** The sequence number is 0, the flag 0x002 identifies it as a SYN segment

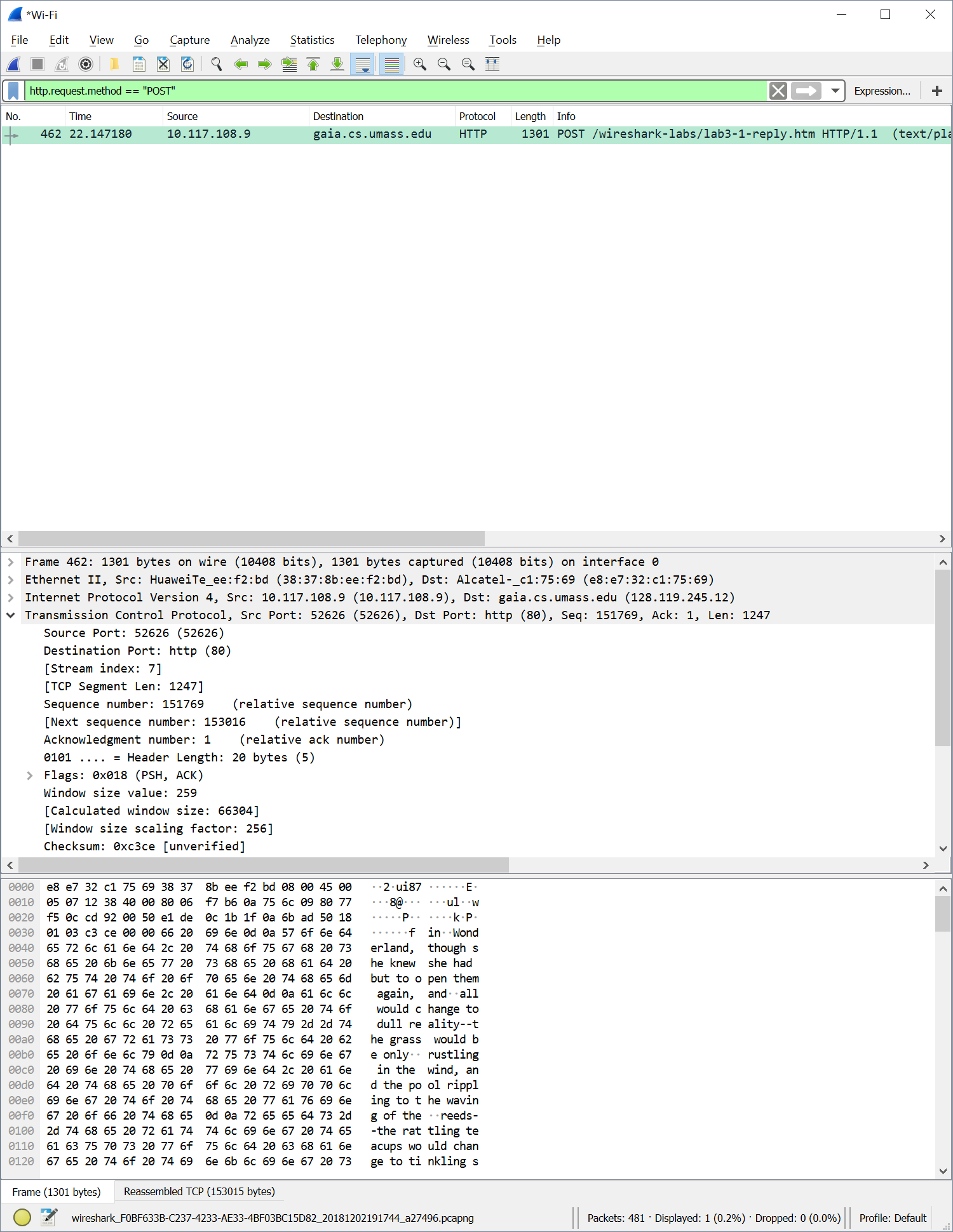


1. **What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a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

**Answer:** The sequence number is 0 and the acknowledgement number is 1. The flag 0x012 identifies it as a SYNACK segment.

1. **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:** The sequence number is 151769

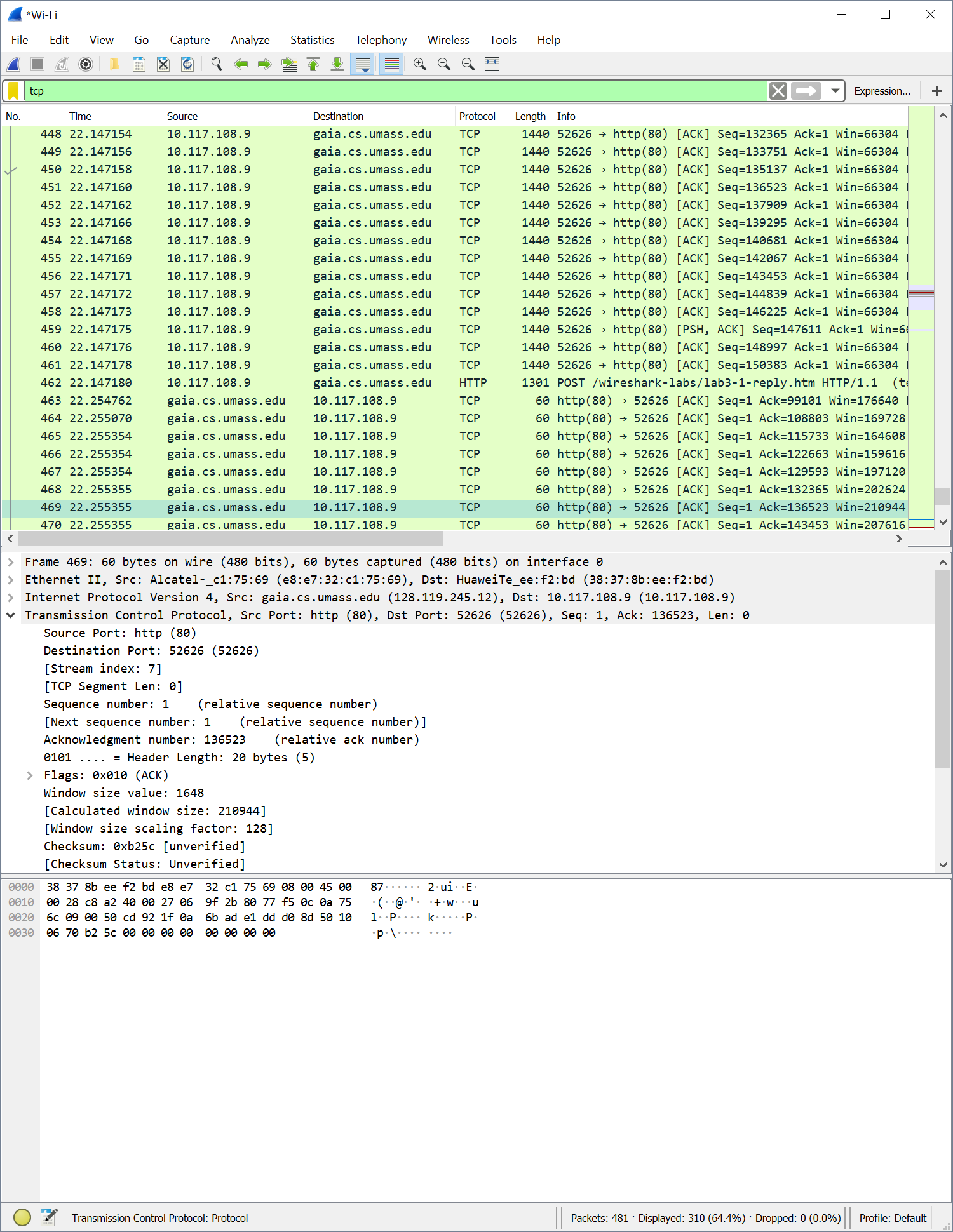


1. **Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? 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?** Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph- >Round Trip Time Graph.

**Answer:** The sequence number for the first six segments are all 1 except for the HTTP post which is 151769

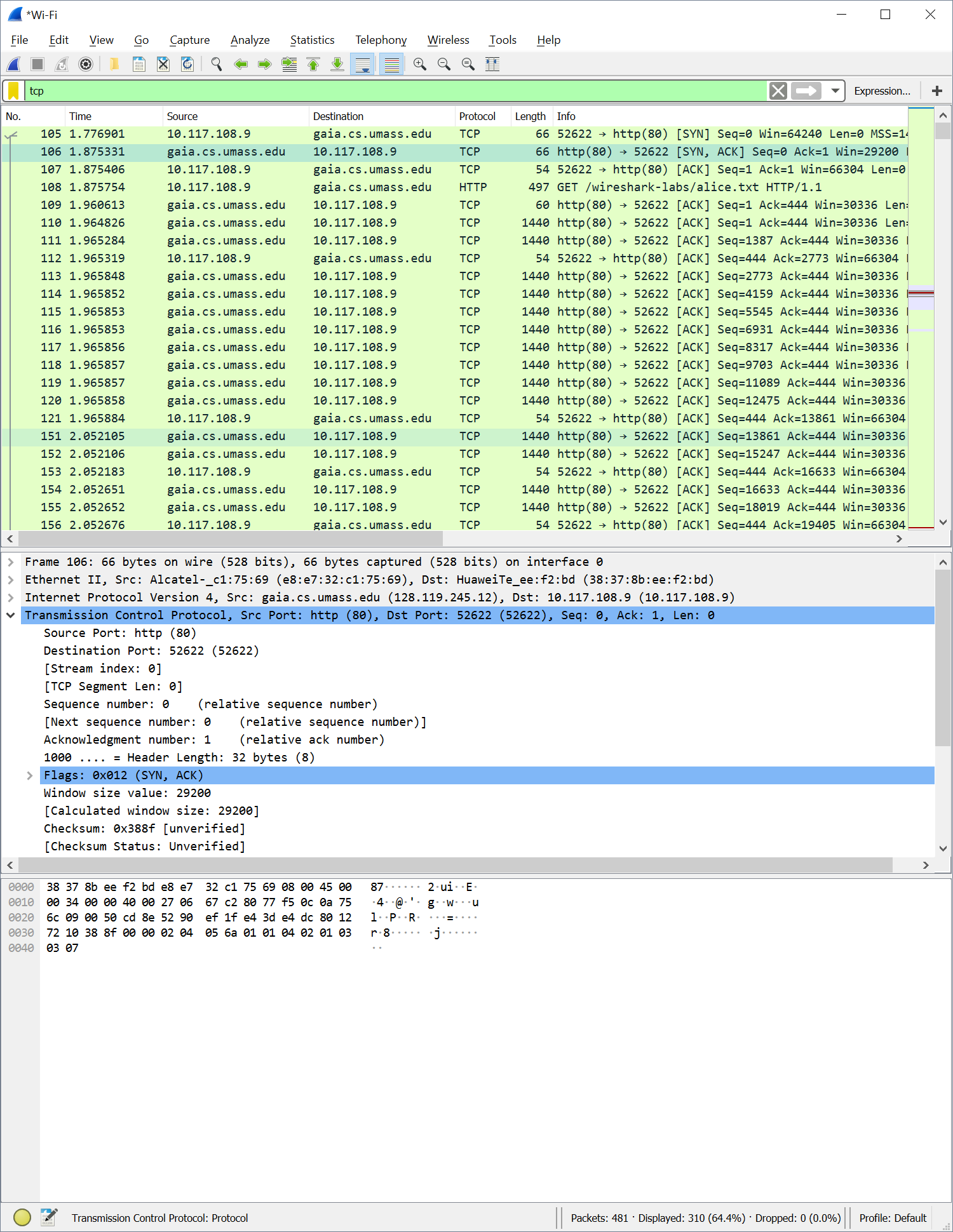
1. **What is the length of each of the first six TCP segments?**

**Answer:** The TCP segment length for the first sex segments is listed as 0



1. **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 is 29200 bytes

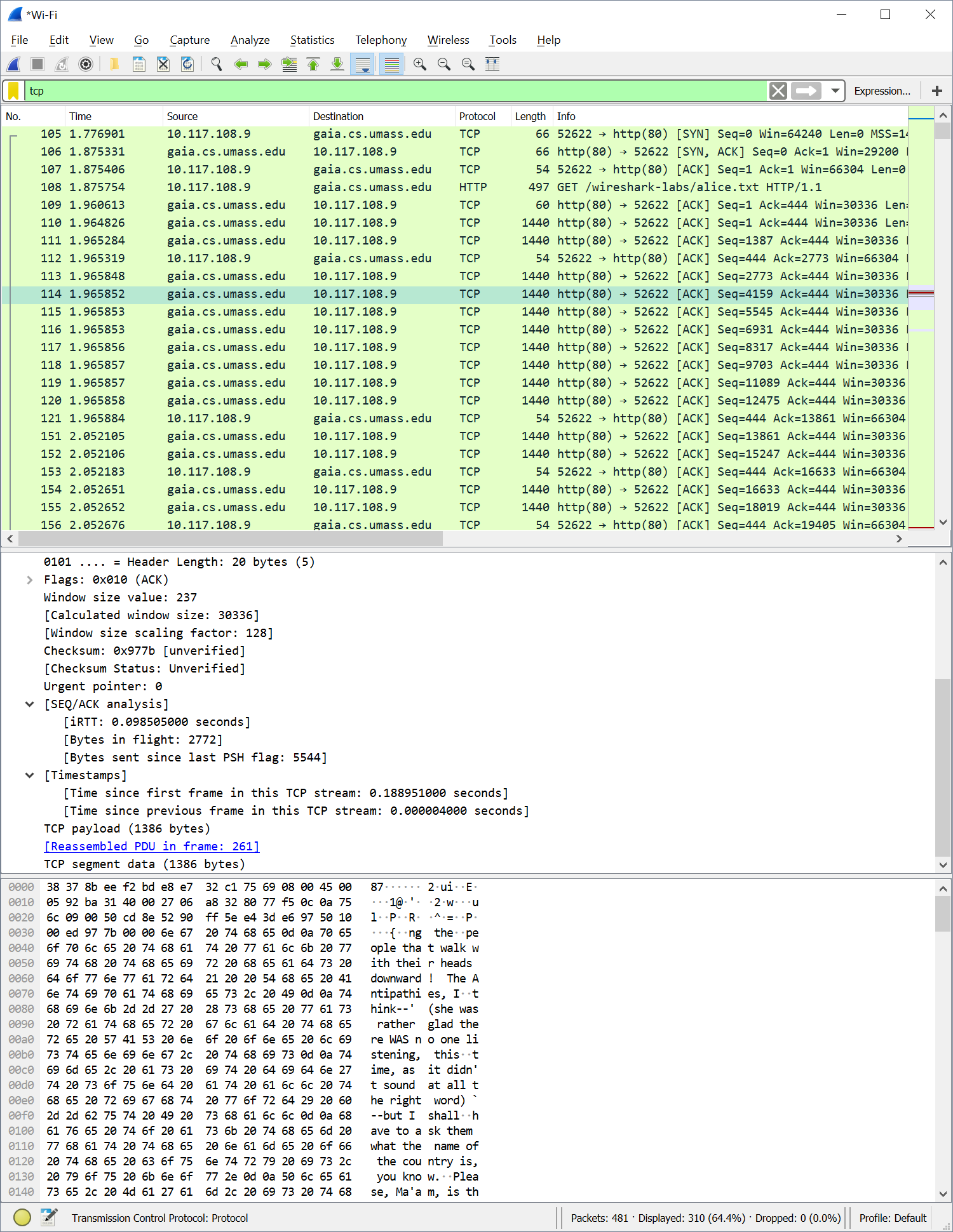


1. **Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?**

**Answer:** I checked sequence numbers of the packets and there were no repeating ones, so there aren’t any retransmitted segments in the trace file

1. **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:** On average it acknowledges about 2772 bytes

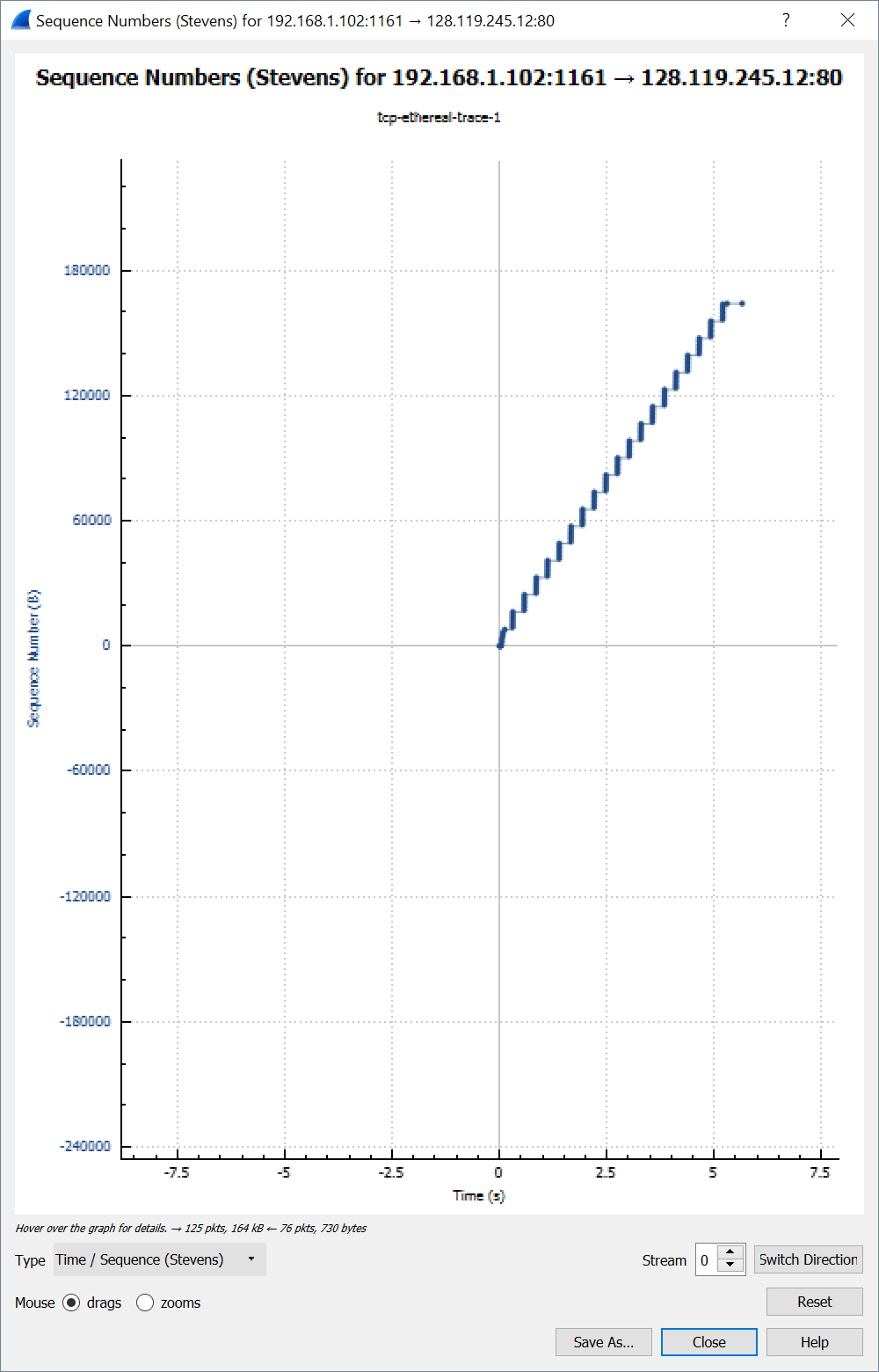


1. **What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.**

**Answer:** By using the file size of the alice file (155,648 bytes) and dividing it by the time spent total for the TCP connection, which was 1.16 seconds, I got a throughput of 133,458 bytes/second.

1. **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:** From packet 0 to packet 5 is where the slow start phase of the tCP connection lasts. After that, congestion avoidance takes over



1. **. 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: There is a major difference in the way my stevens graph looks compared to the one made from the capture file. I suspect this is due to large number of other packets that were captured unrelated to the lab**

