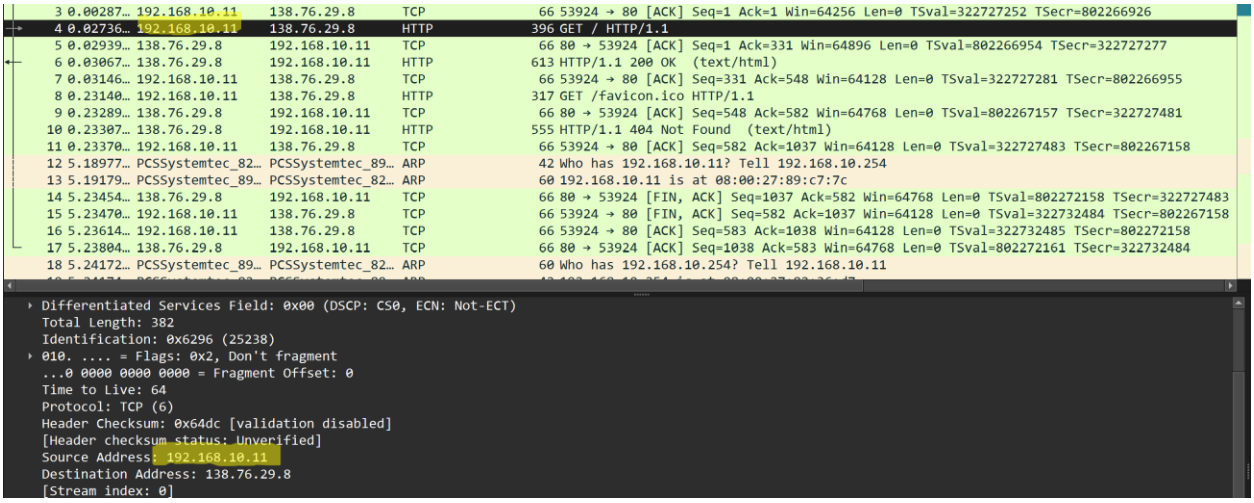
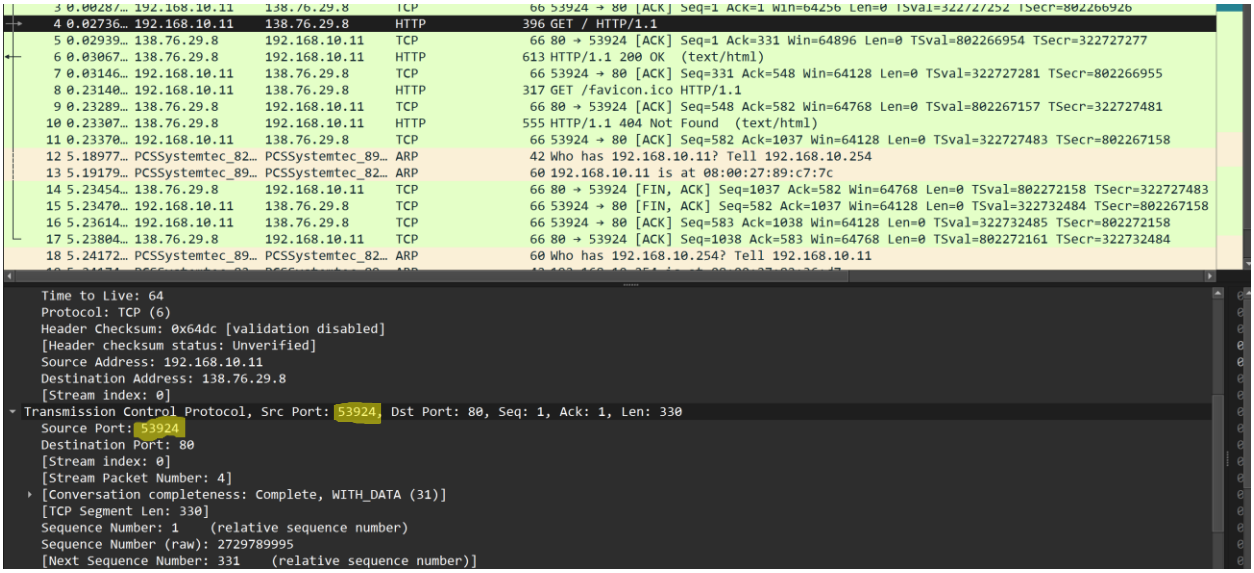
Question 1

1. What is the IP address of the client that sends the HTTP GET request in the nat-inside-wireshark-trace1-1.pcapng trace?
   Answer: 192.168.10.11
   Screenshot:



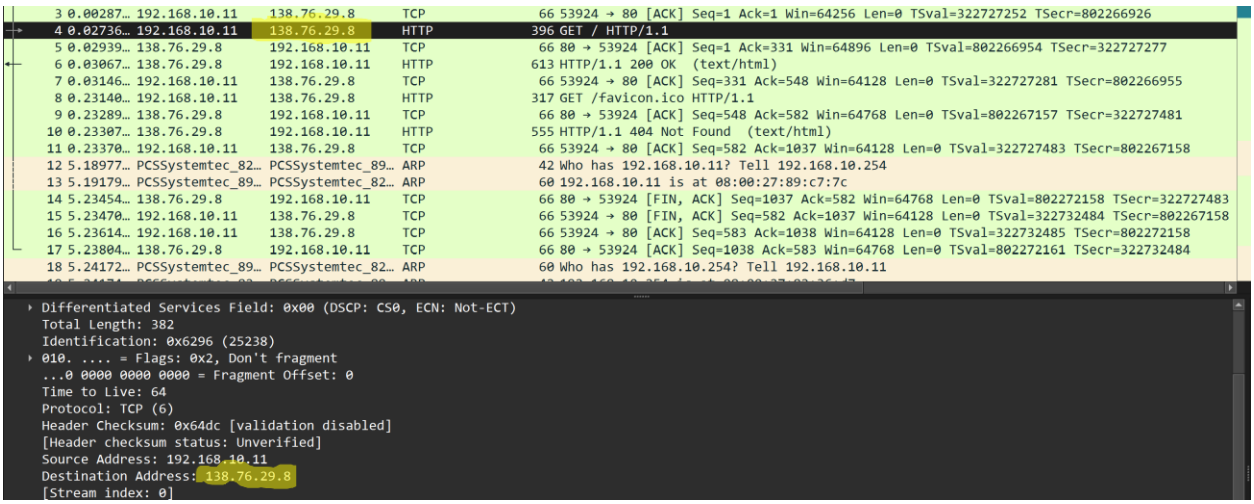
   Explanation: The HTTP GET request is packet 4 in the pcap. The source IP is 192.168.10.11.

2. What is the source port number of the TCP segment inside of this datagram containing the HTTP GET request sent by this client in the nat-inside-wireshark-trace1-1.pcapngh trace?
   Answer: 53924
   Screenshot:



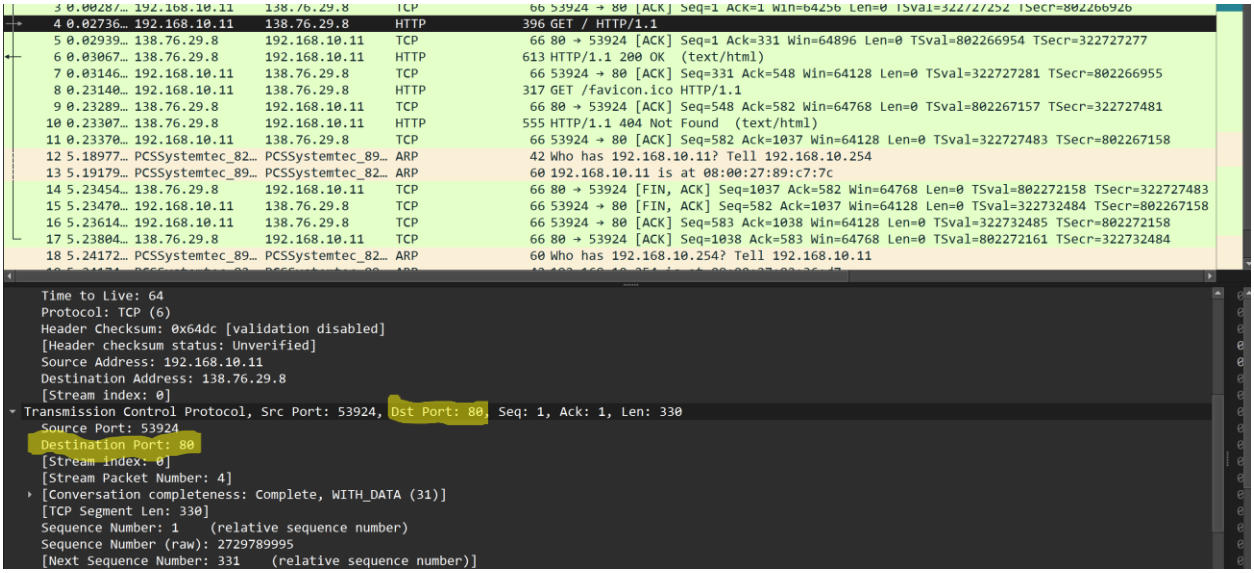
   Explanation: The HTTP GET message is 4 and under the TCP the source port is 53924.

3. What is the IP destination address of this datagram containing the HTTP GET request in the nat-inside-wireshark-trace1-1.pcapng trace?
   Answer: 138.76.29.8.
   Screenshot:



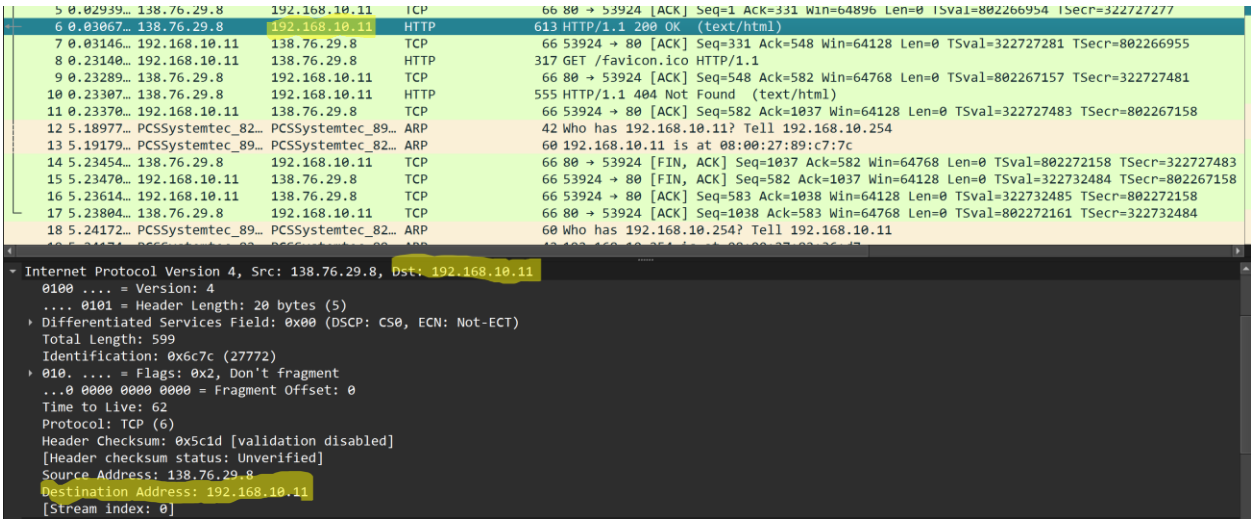
   Explanation: This is the same packet number 4 so if you look in the Internet Protocol tab it says Destination Address: 138.76.29.8.

4. What is the destination port number of the TCP segment in this datagram containing the HTTP GET request sent by this client in the nat-inside-wireshark-trace1-1.pcapng trace?
   Answer: 80.
   Screenshot:



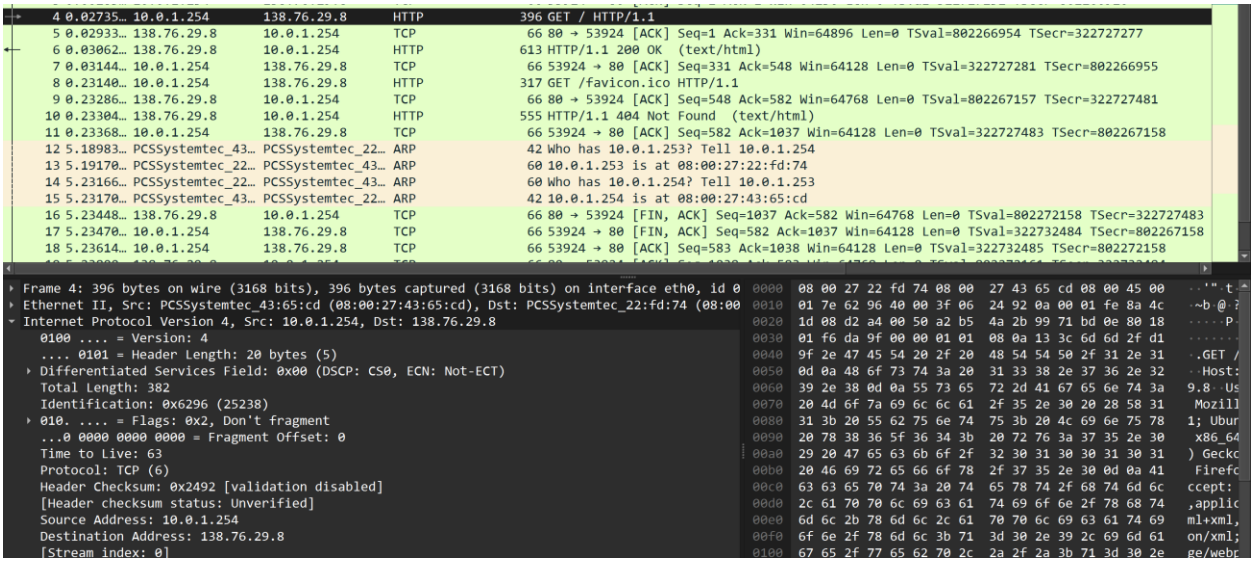
   Explanation: We are still in packet 4 which is the HTTP GET message. If you look under the transmission control protocol section it says destination port 80.

5. What is the destination IP address of the IP datagram carrying this HTTP 200 OK message?
   Answer: 192.168.10.11.
   Screenshot:



   Explanation: The HTTP OK message is sent in packet 6 so if you look under the Internet Protocol Version under Destination Address it is 192.169.10.11.

6. What is the source IP address of the IP datagram carrying this HTTP GET message (as recorded in the nat-outside-wireshark-trace1-1.pcapng trace file)?
   Answer: 10.0.1.254
   Screenshot:

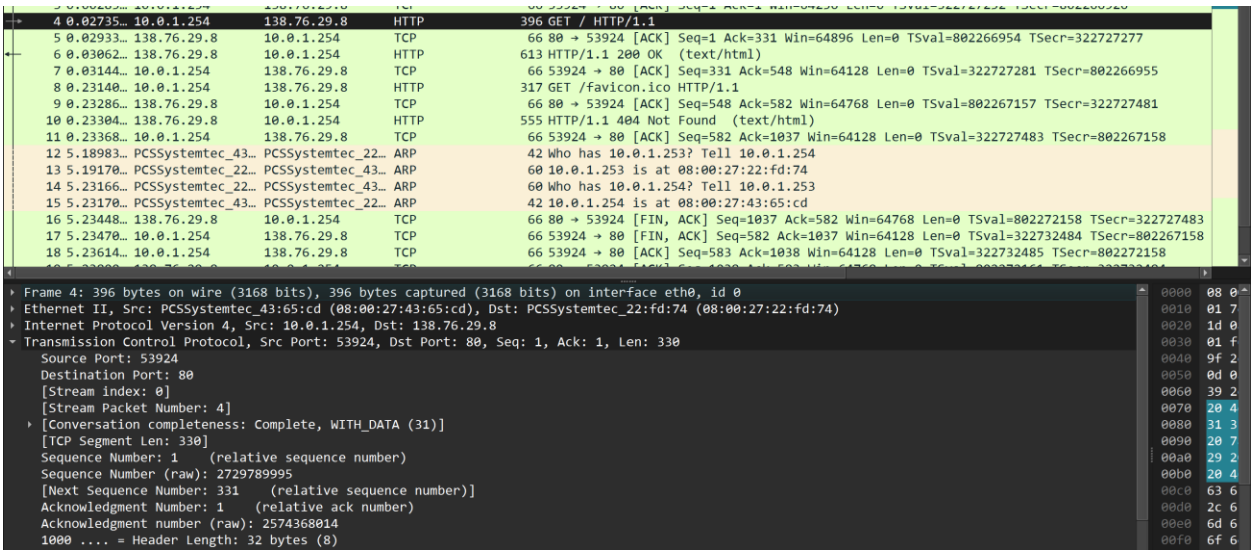


   Explanation: The packet is packet 4 so if you look under the Internet Protocol Version tab and look for source address 10.0.1.254.

7. What is the source port number of the TCP segment in the IP datagram carrying this HTTP GET message?

   Answer: 53924

   Screenshot:

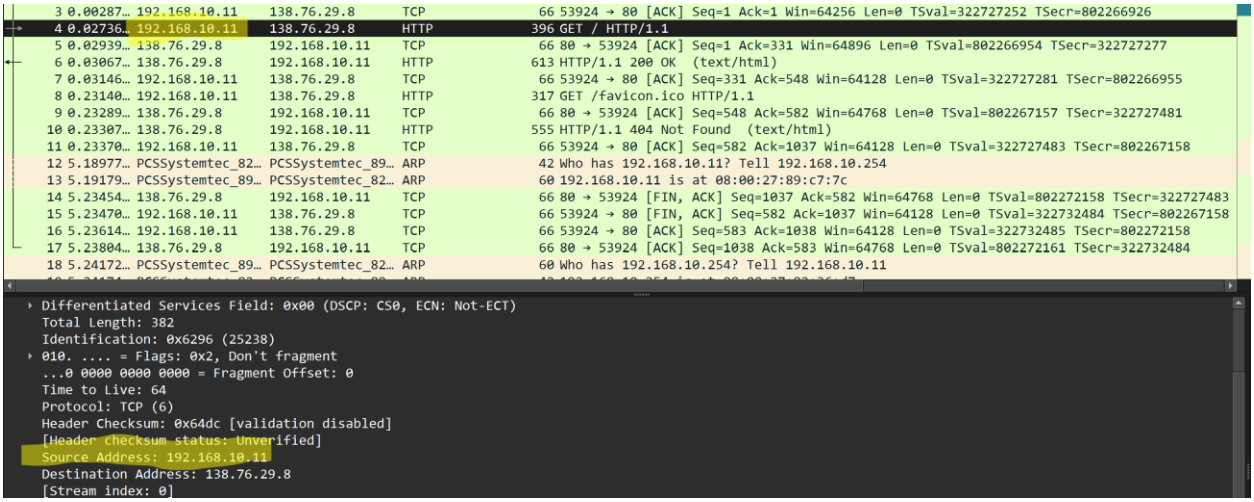


   Explanation: This is the same packet as the last question but to find the TCP source port look under the Transmission Control Protocol tab and by source port which is 53924.

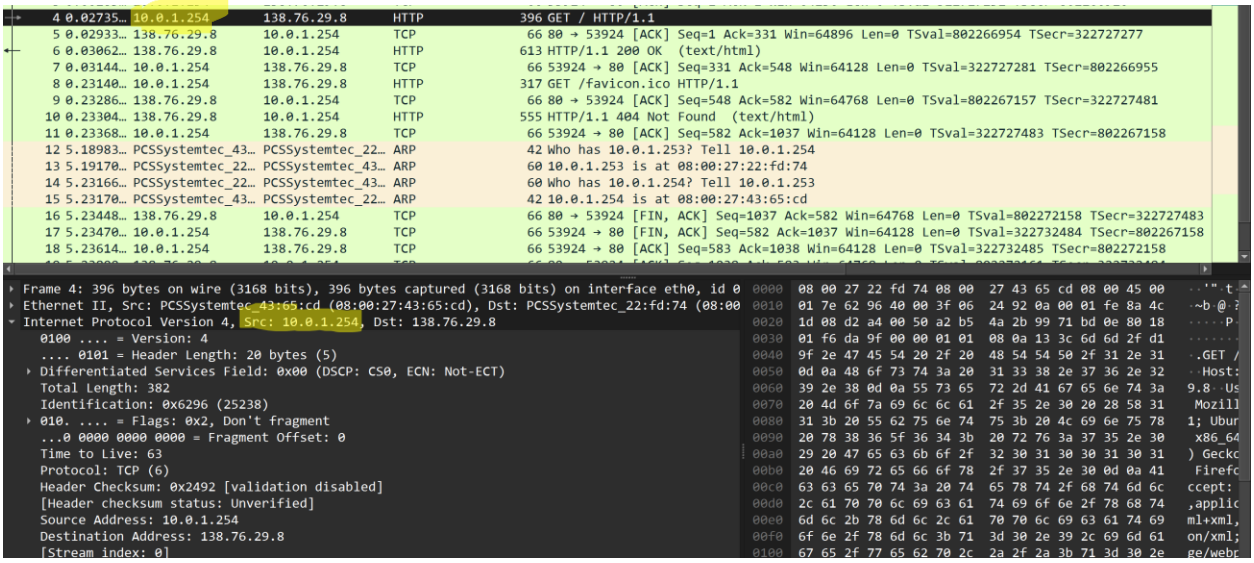
8. Which of these four fields – IP source and destination addresses and TCP source and destination port numbers – are changed as the datagram carrying the HTTP GET message passed through the NAT router?

   Answer: IP source address

   Screenshot: inside



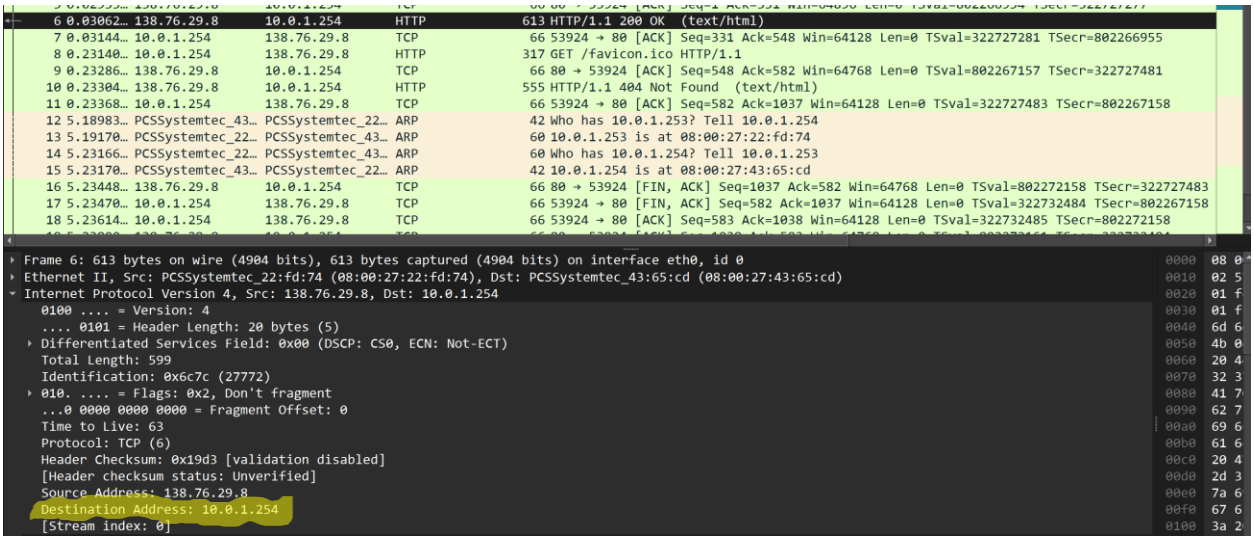
   Outside



Explanation: The IP source address in the inside file is 192.168.10.11 and when you look at the outside file it is 10.0.1.254.

9. Which of the following fields in the IP datagram carrying the HTTP GET are changed from the datagram received on the local area network (inside) to the corresponding datagram forwarded on the Internet side (outside) of the NAT router?
   Answer:
   Screenshot:
   Explanation:

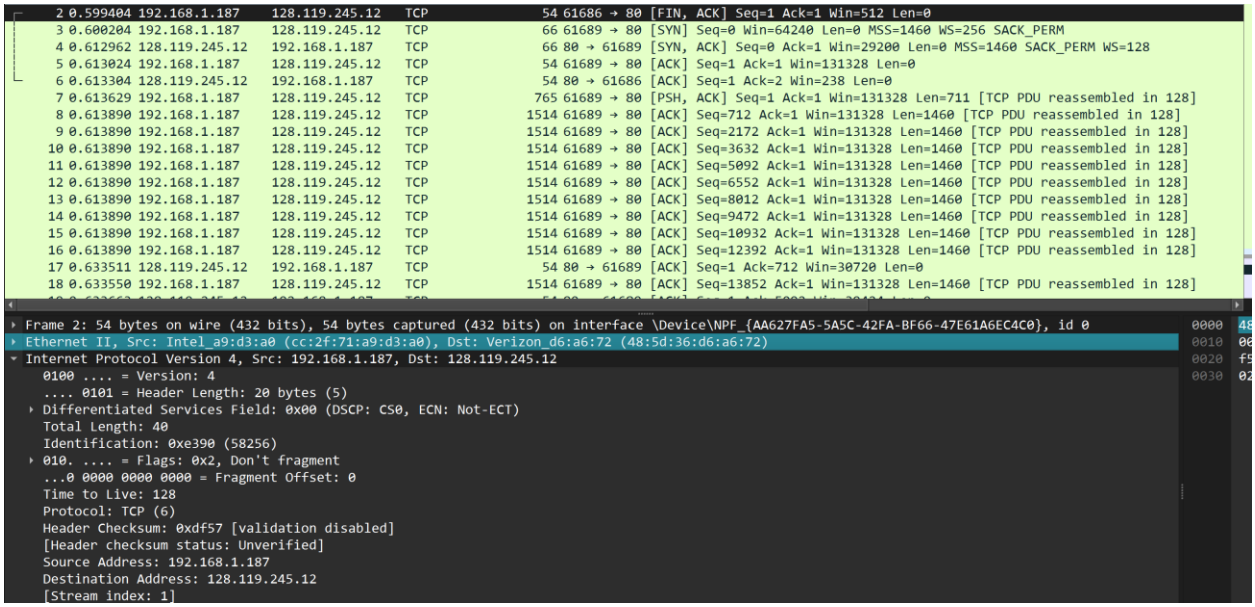
10. What is the destination IP address of the IP datagram carrying this HTTP reply ("200 OK") message that is forwarded from the router to the destination host?
    Answer: 10.0.1.254
    Screenshot:



Explanation: Since this message is coming from the router we have to look at the outside pcap. If you look at the HTTP OK under Internet Protocol Version you will find the destination address as 10.0.1.254.

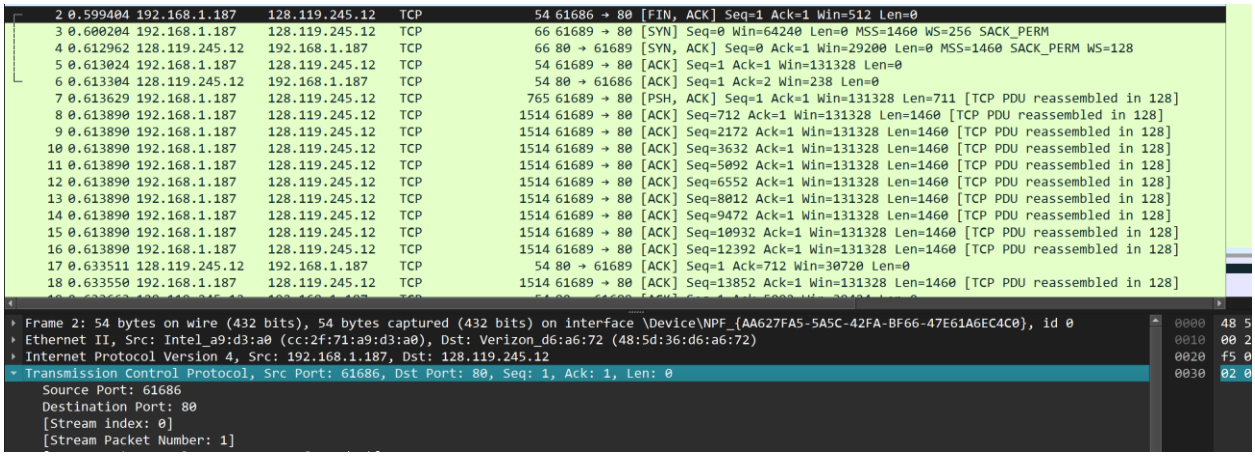
Question 2

1. What is the IP address of the client computer (source) that is transferring the file to gaia.cs.umass.edu? Enter the IP address in dotted decimal notation (include each dot, and omit any leading zeros for any byte, e.g., 10.1.216.54):
   Answer: 192.168.1.187
   Screenshot:



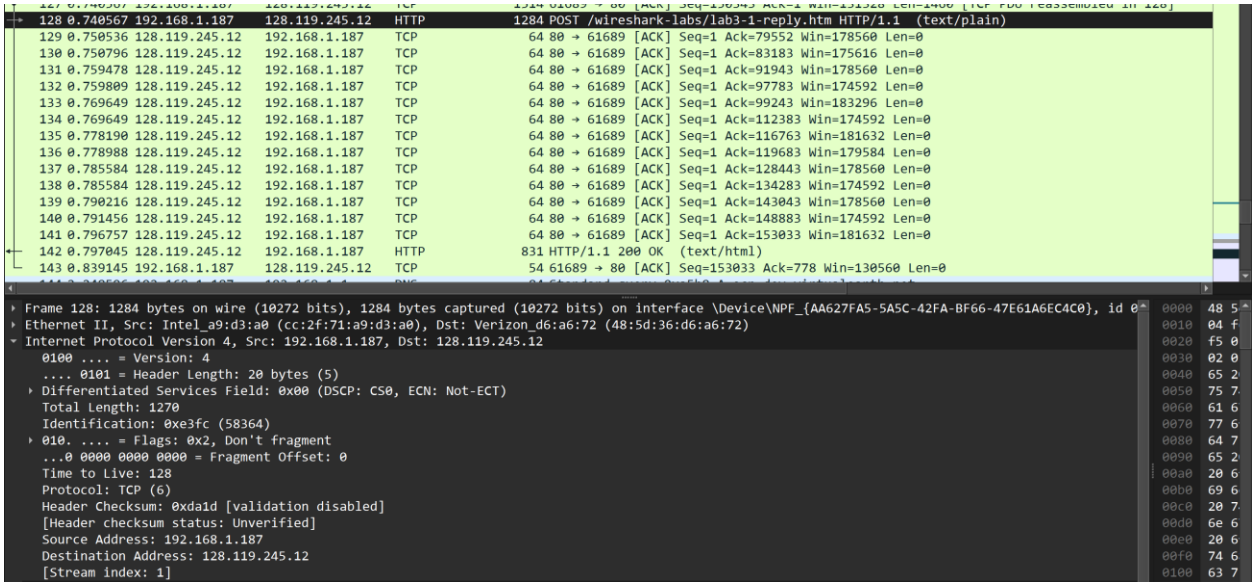
   Explanation: This is the beginning of the file transfer so I looked to see what the source is under Internet Protocol Version tab. It is 192.168.1.187.

2. What is the client-side port number of the client computer (source) that is transferring the file to gaia.cs.umass.edu? Enter the port integer port number (digits only, no commas), with no leading 0's:
   Answer: 6186
   Screenshot:



Explanation: This is in packet 2 so if you look under the transmission control protocol tab you will see source port. The source port is equal to 61686.

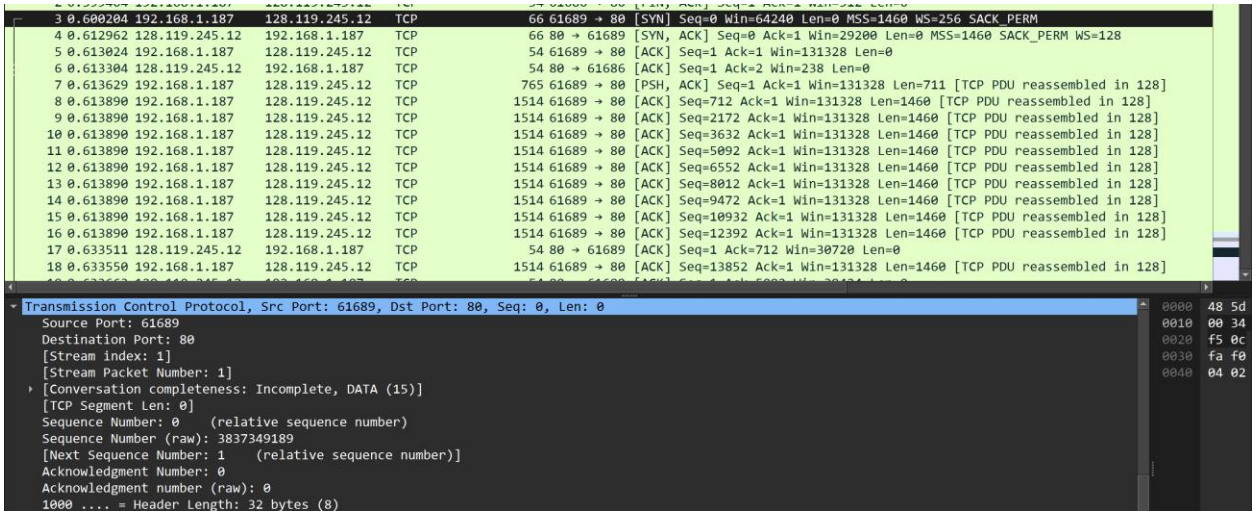
3. What is the IP address of the gaia.cs.umass.edu server to which the alice.txt file will be uploaded via the HTTP POST? Enter the IP address in dotted decimal notation (include each dot, and omit any leading zeros for any byte, e.g., 10.1.216.54):
   Answer: 128.119.245.12
   Screenshot:



   Explanation: The HTTP POST packet number is 128. If you look under the Internet Protocol Version tab you should then look under Destination address and you will see 128.119.245.12

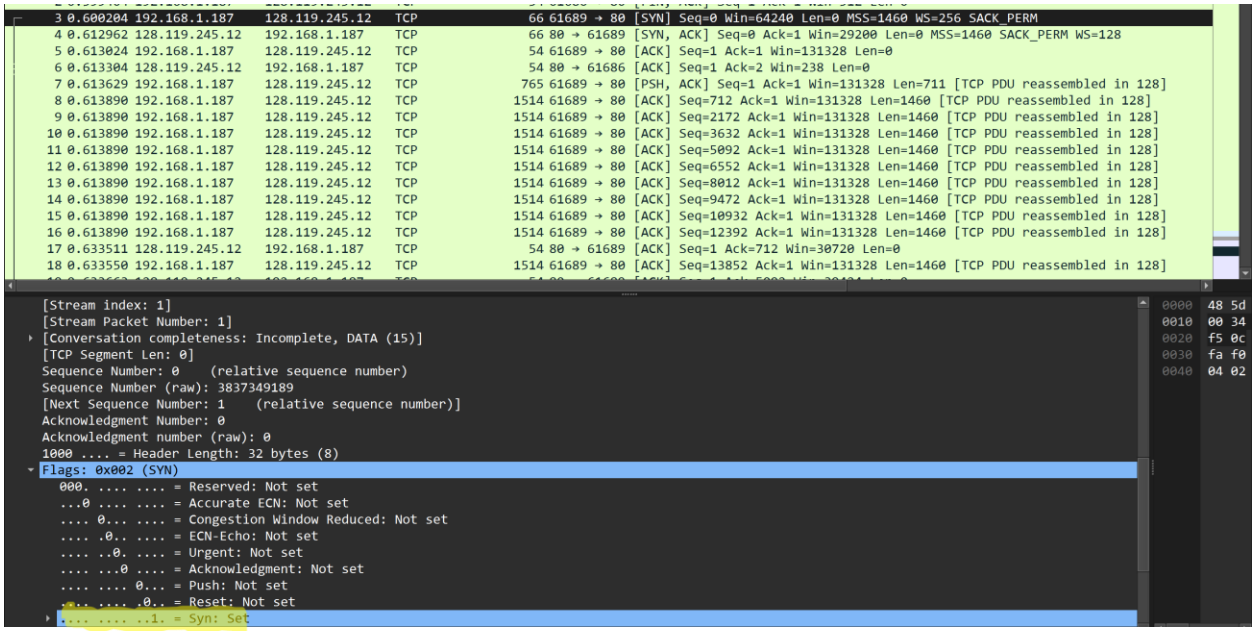
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? Enter the sequence number (digits only, no commas), with no leading 0's:
   Answer: 0 (relative) and 3837349189 (raw)

Screenshot:



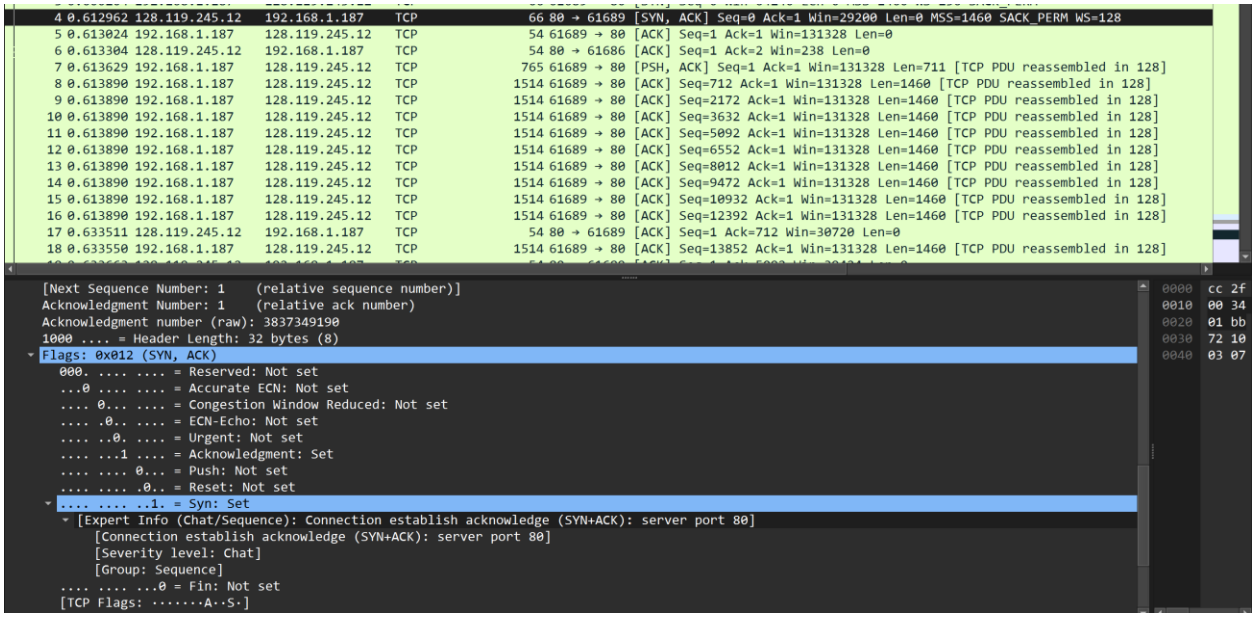
Explanation: The TCP SYN message is the first one that starts the file transfer. If you look under the transmission control protocol tab you can see the sequence number. The relative sequence number is 0 and the raw sequence number is 3837349189. I included both just in case.

5. What is it in this TCP segment that identifies the segment as a SYN segment?
   Answer: The SYN Flag is set by being set to 1.
   Screenshot:



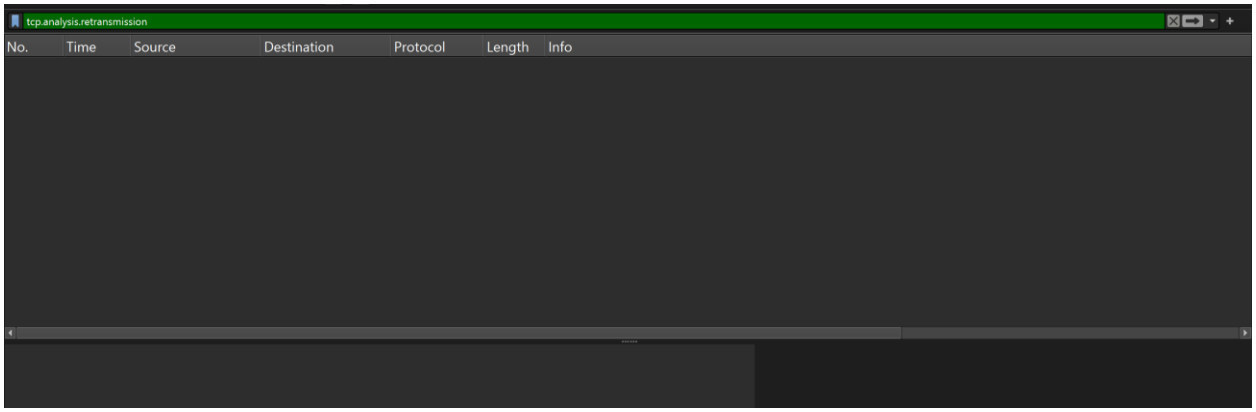
Explanation: If you look in packet 3 under the transmission control protocol tab you will be the flags section. This identifies packets. In our selected packet you can see that the Syn flag is set by being set to 1.

6. What is the value in the Acknowledgment field of the TCP SYNACK segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? Enter the acknowledgment number (digits only, no commas), with no leading 0's:
   Answer: 1 (relative ack) and 3837349190 (raw)
   Screenshot:



   Explanation: If you look in packet 4 which is the TCP SYNACK packet under the transmission control protocol tab you will see the acknowledgement numbers. The relative number is 1 and the raw number is 3837349190.

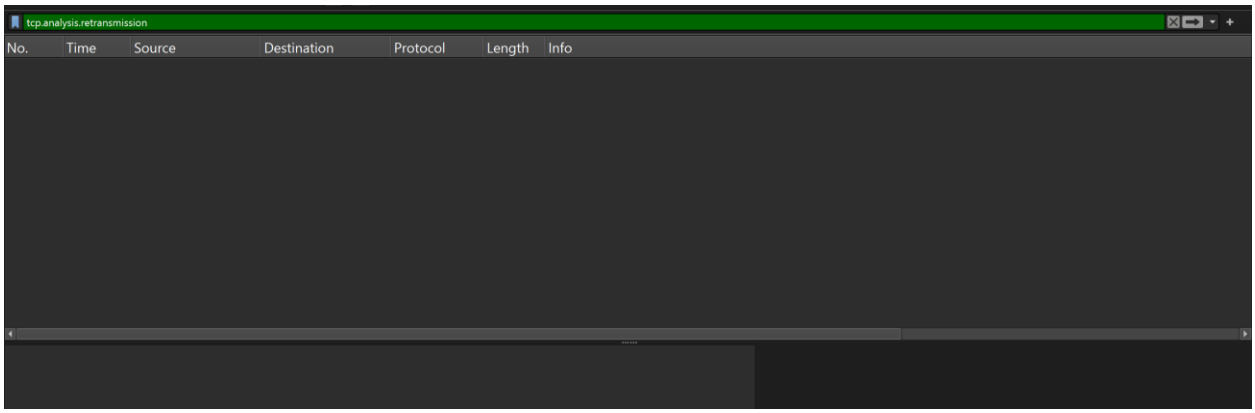
7. Are there any retransmitted segments in the trace file? YES or NO:
   Answer: No
   Screenshot:



   Explanation: There is nothing shown when I filter for tcp.analysis.retransmission.

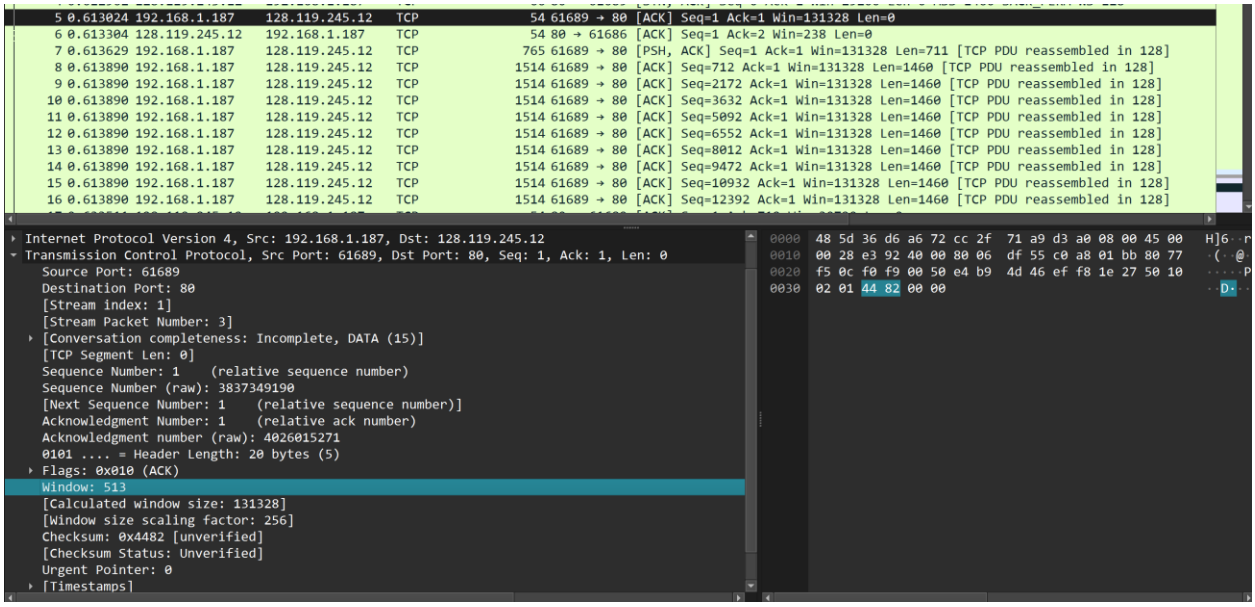
8. How did you determine whether or not there were retransmitted segments?

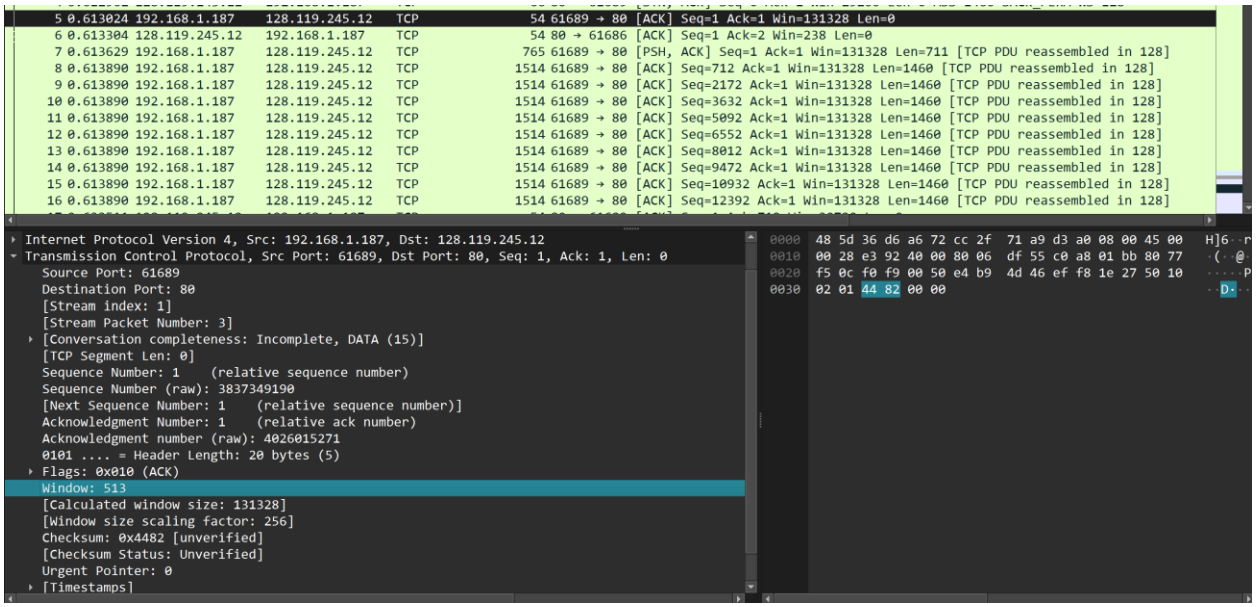
Answer: I filtered the packets with tcp.analysis.retransmission.
Screenshot:



Explanation: This scans to see if any empty window sizes are sent. This sees if any not complete ones make it.

9. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to gaia.cs.umass.edu?
Answer: Mainly 513
Screenshot:



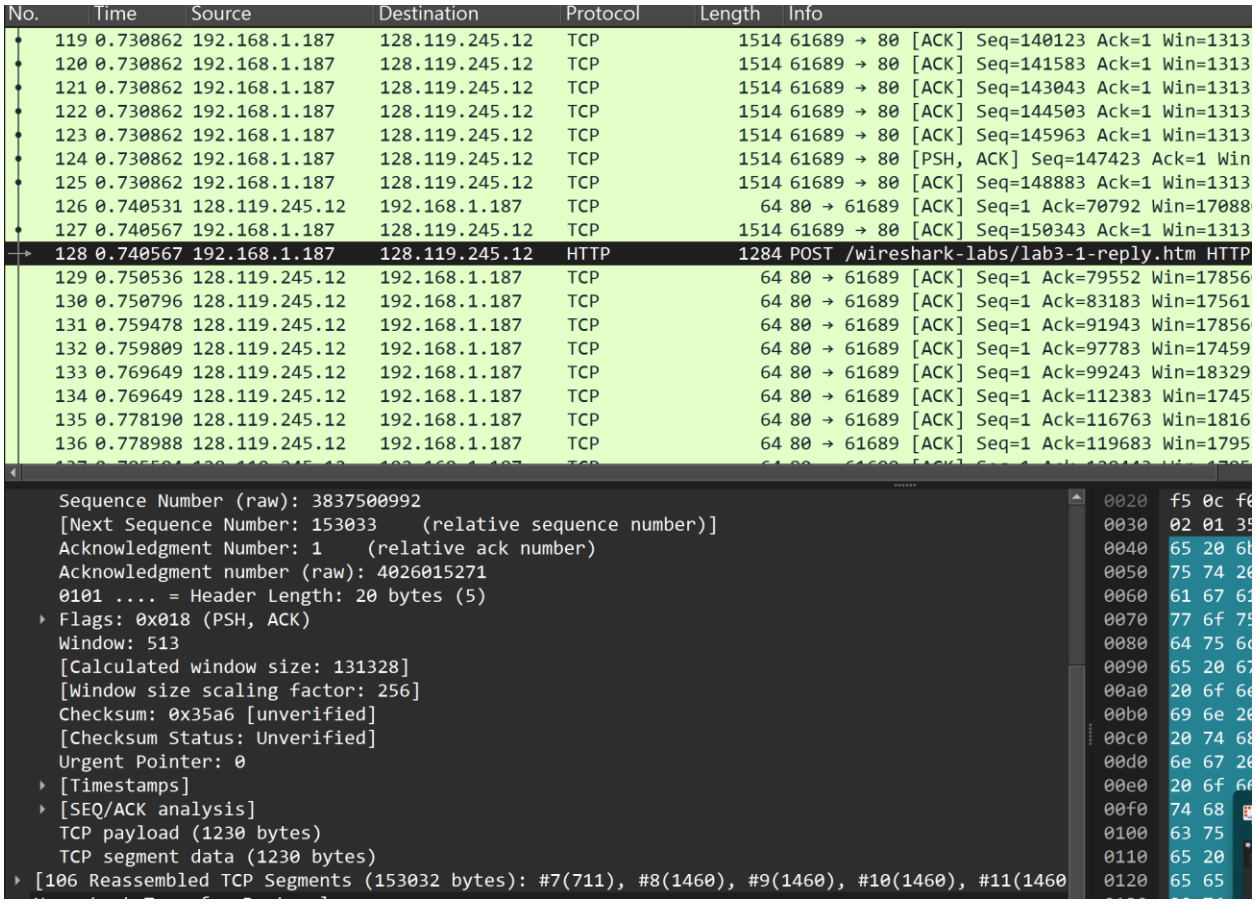


Explanation: Most of them transmit 513 bytes but one does 238.

10. What is the throughput (bytes transferred per unit time) for the TCP connection?

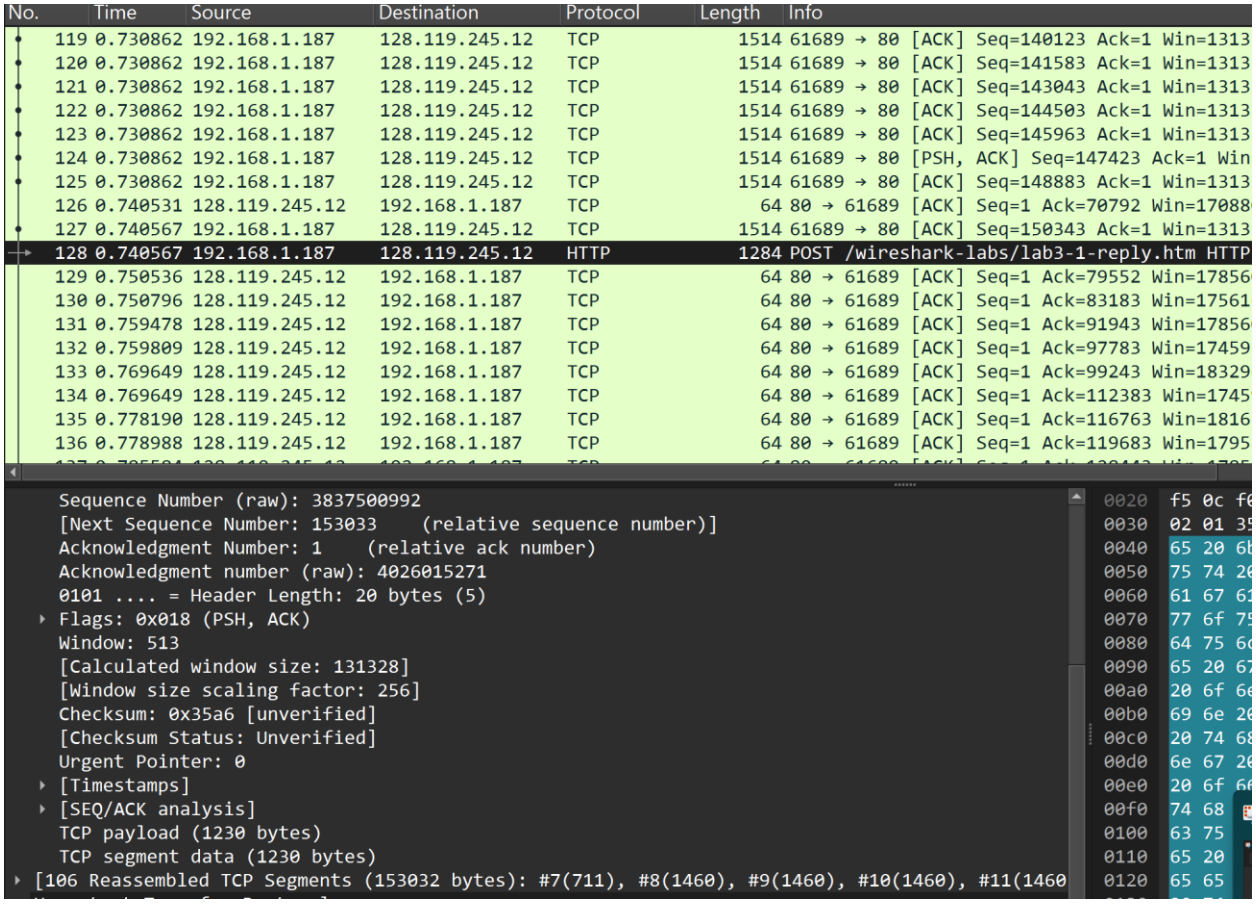
    Answer: 153032bytes / 0.740567seconds

    Screenshot:



Explanation: Divide 153032 / 0.740567. This is taken by the TCP segments 153032 bytes and the time that was found then.

11. How did you calculate the throughput (bytes transferred per unit time) for the TCP connection?
    Answer: You take the total bytes that are sent and divide it by the time at the final TCP connection.
    Screenshot:



Explanation: This was found by looking at the POST reply and seeing the total bytes at that moment and divide it by that time.