Ho Chi Minh City University of Technology

COMPUTER NETWORK

LAB PART II

Student: Nguyen Minh Hung – 2052504

Lecturer: TS. Nguyen Le Duy Lai

FACULTY of COMPUTER SCIENCE and COMPUTER ENGINEERING

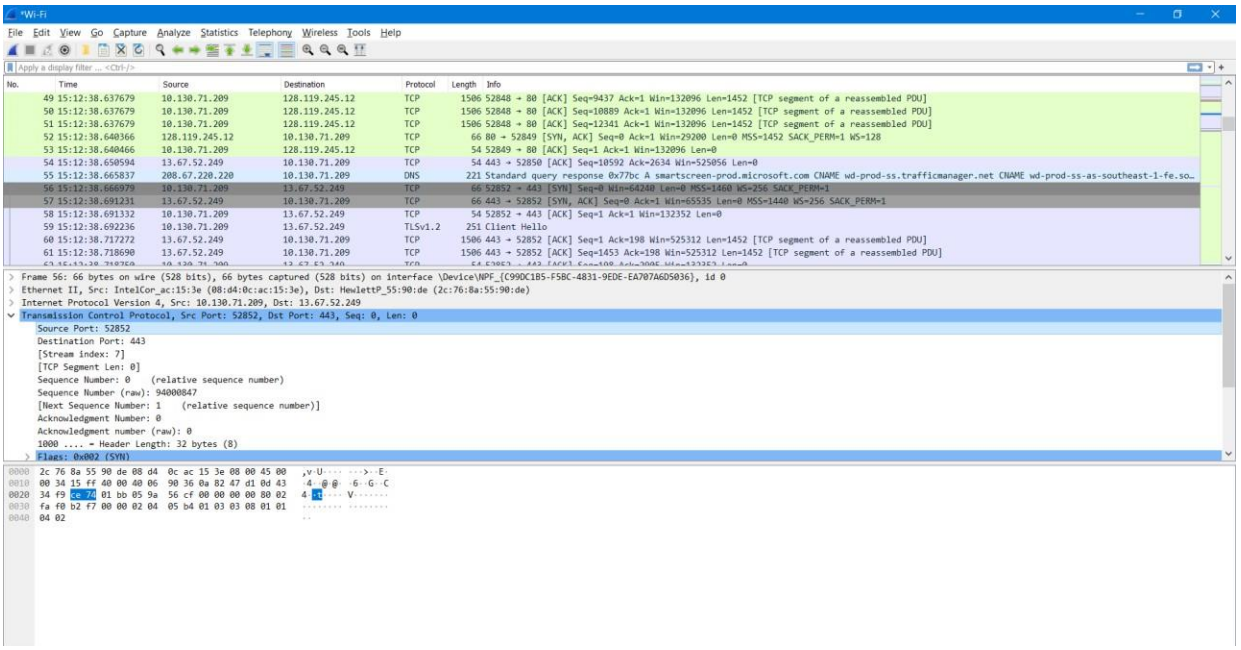
Ho Chi Minh City , November 2022

LAB 4A - WIRESHARK LAB: TCP

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:

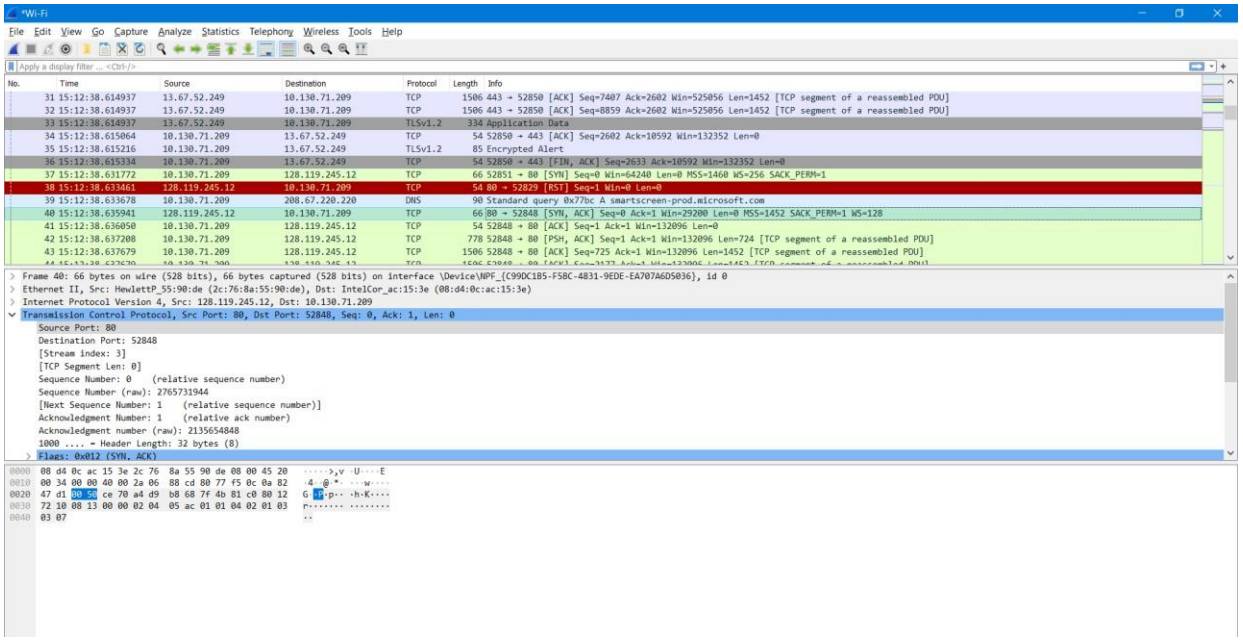
The IP address of the source is 10.130.71.209.
TCP port number used by the client computer 52851.



2. 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:

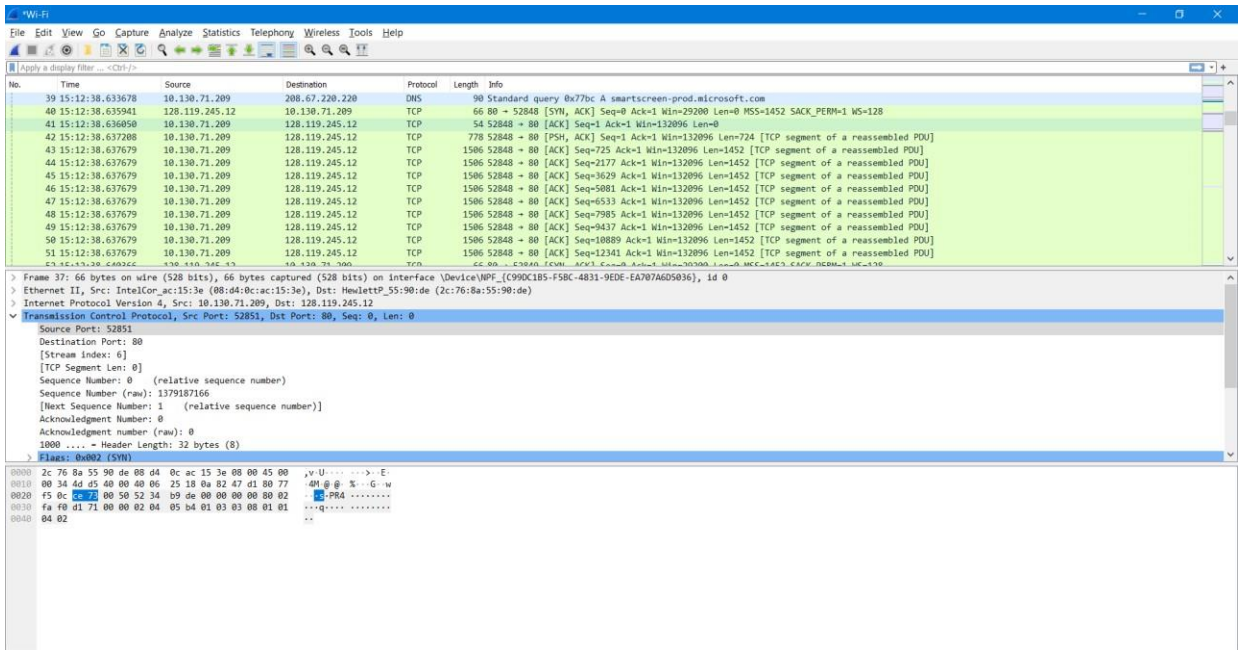
The IP address of gaia.cs.umass.edu is 128.119.245.12.
The port number it's sending and receiving TCP segments for this connection is 80.



3. 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:

With the IP address 10.130.71.209 and TCP port number 52848 that my client computer transfer the file to gaia.cs.umass.edu

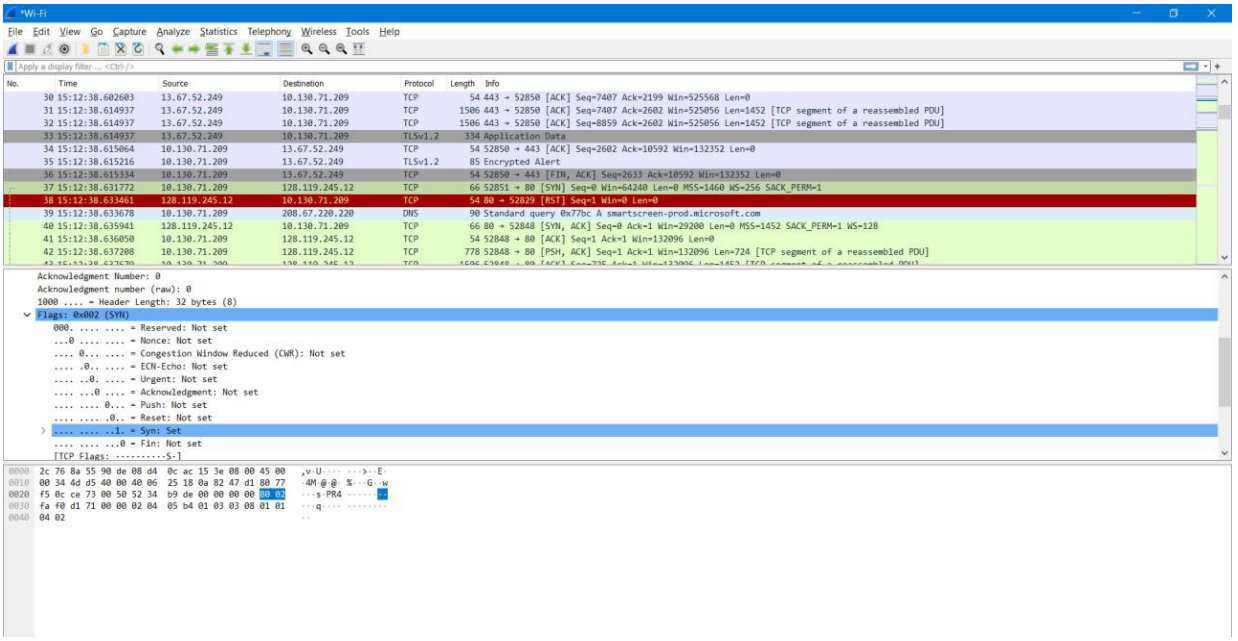


4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is

it in the segment that identifies the segment as a SYN segment?

Answer:

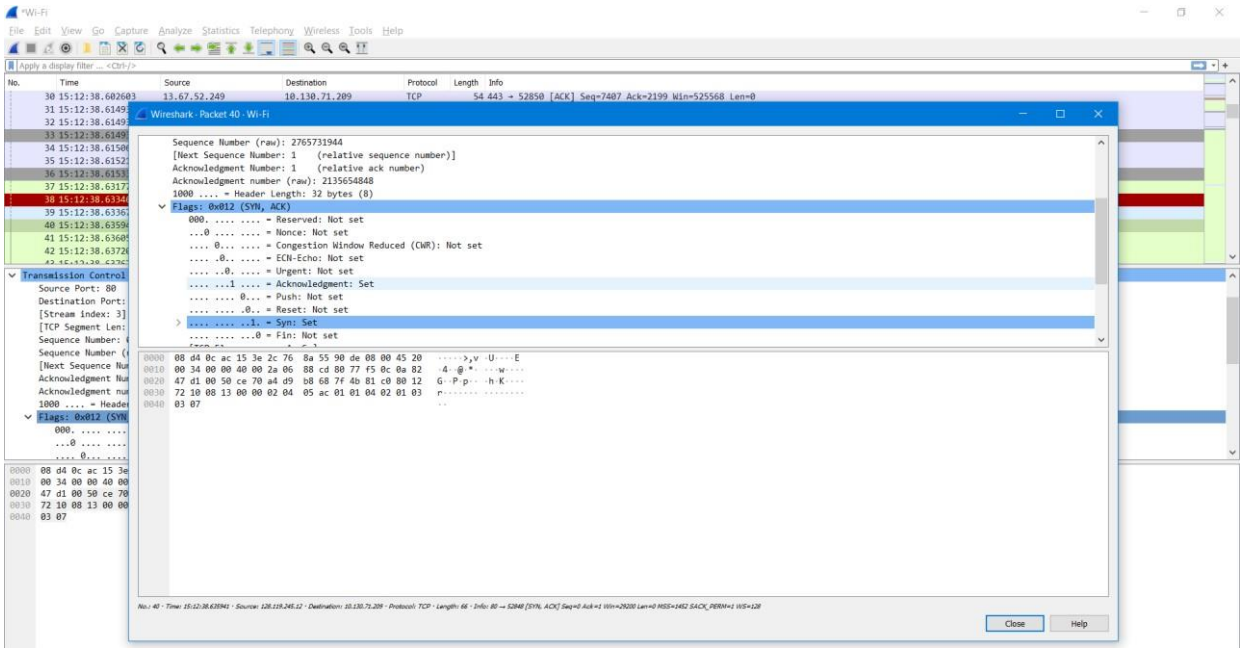
The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 0.
In the Flags section, the SYN flag is set to 1 which identifies the segment as a SYN segment.



5. 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:

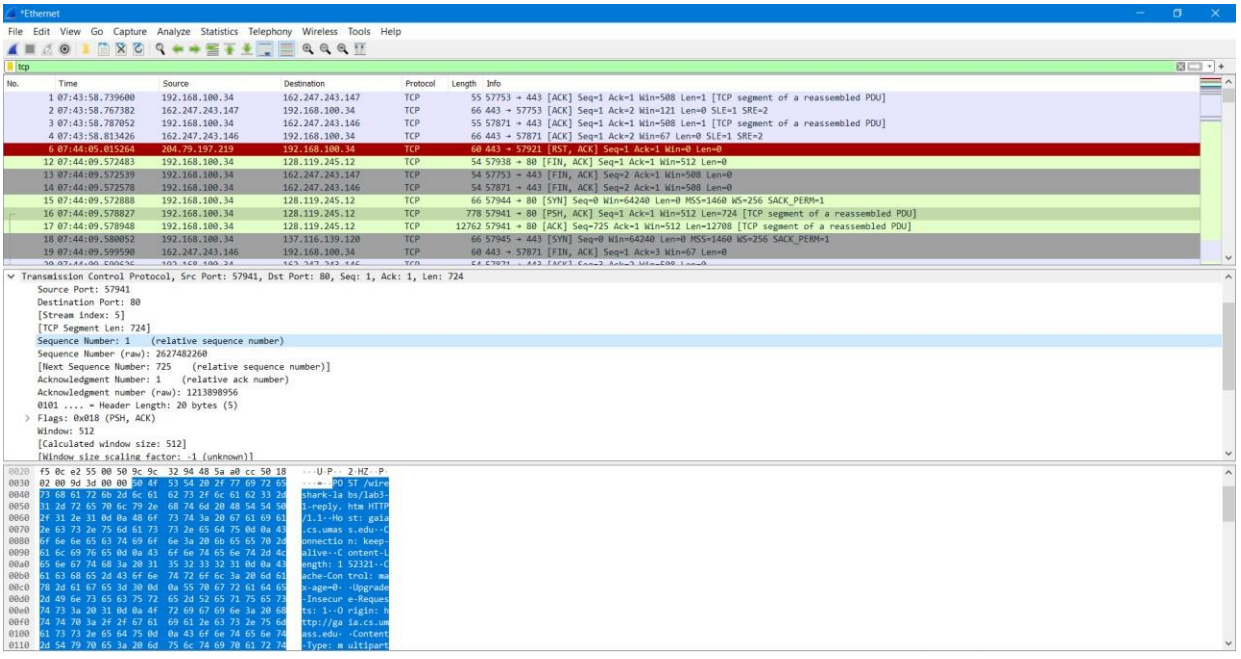
The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.
The value of the acknowledgement field in the SYNACK segment is 1.
The server gaia.cs.umass.edu determined that value by adding 1 to the initial sequence number of the SYN segment from the client computer. In this case, the initial sequence number of the SYN segment from the client computer is 0. So that the value of the acknowledgement field in the SYNACK segment is 1.
The segment that identifies the segment as a SYNACK segment is when both SYN flag and Acknowlegment flag in the segment are set to 1.



6. 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:

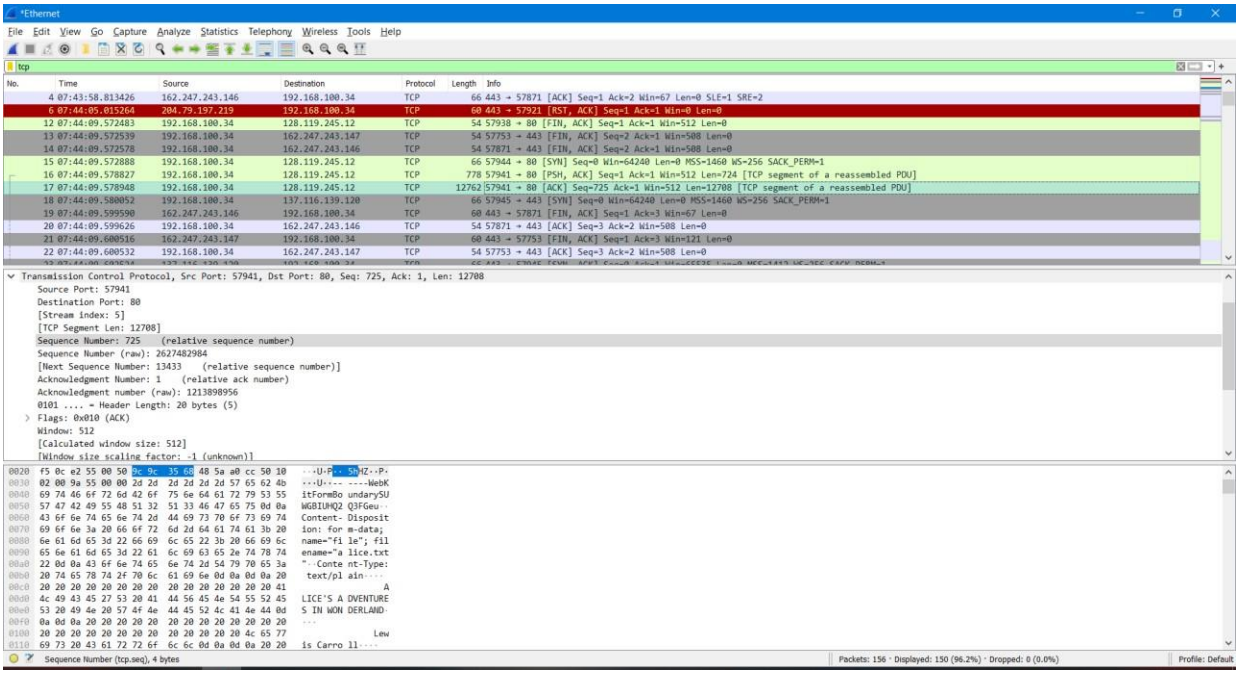
The sequence number of the TCP segment containing the HTTP Post command is 1.



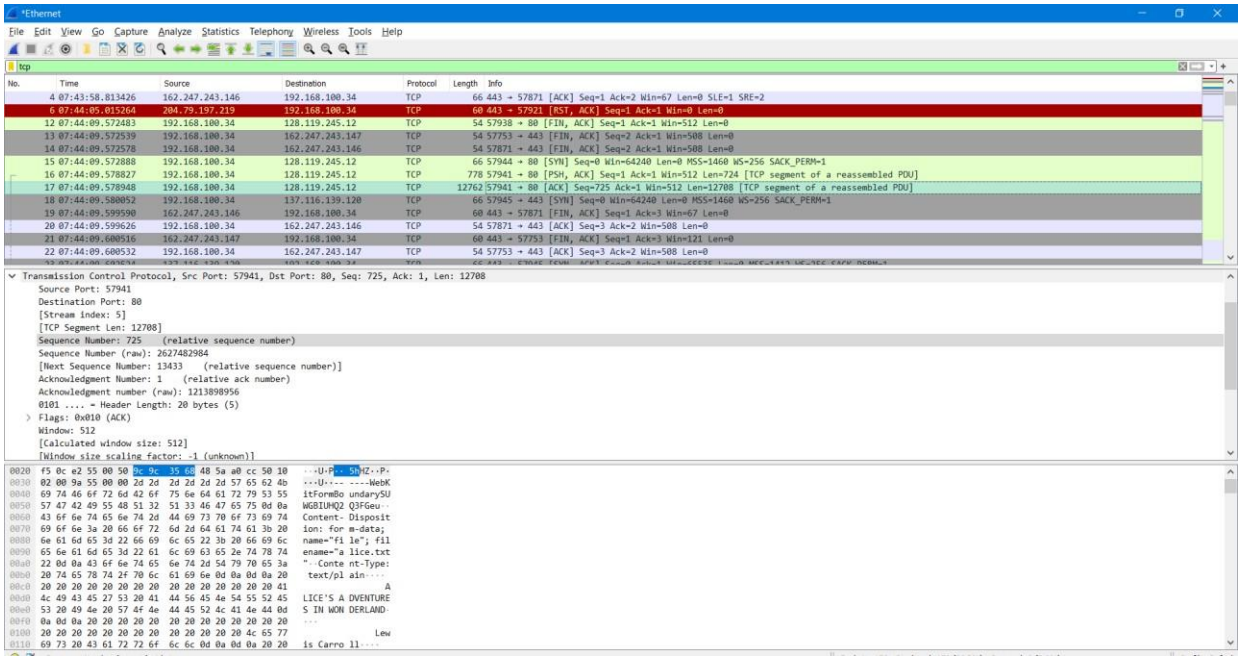
7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? 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:

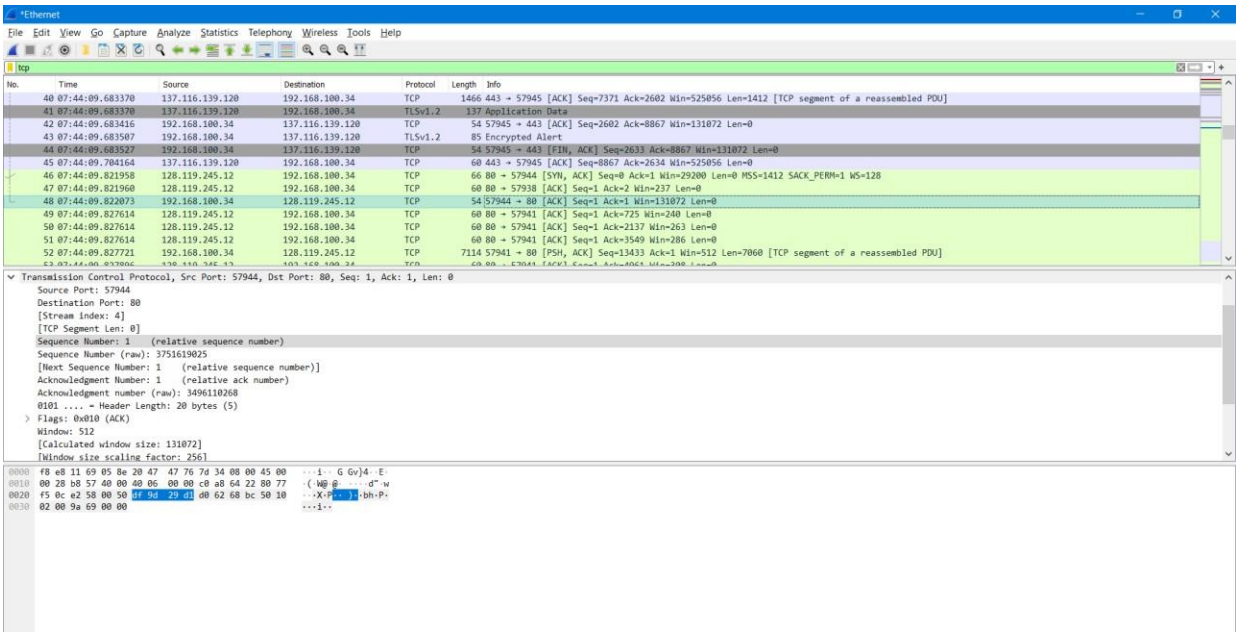
The sequence number for segment 1 is 1. The sequence number for segment 2 is 725.



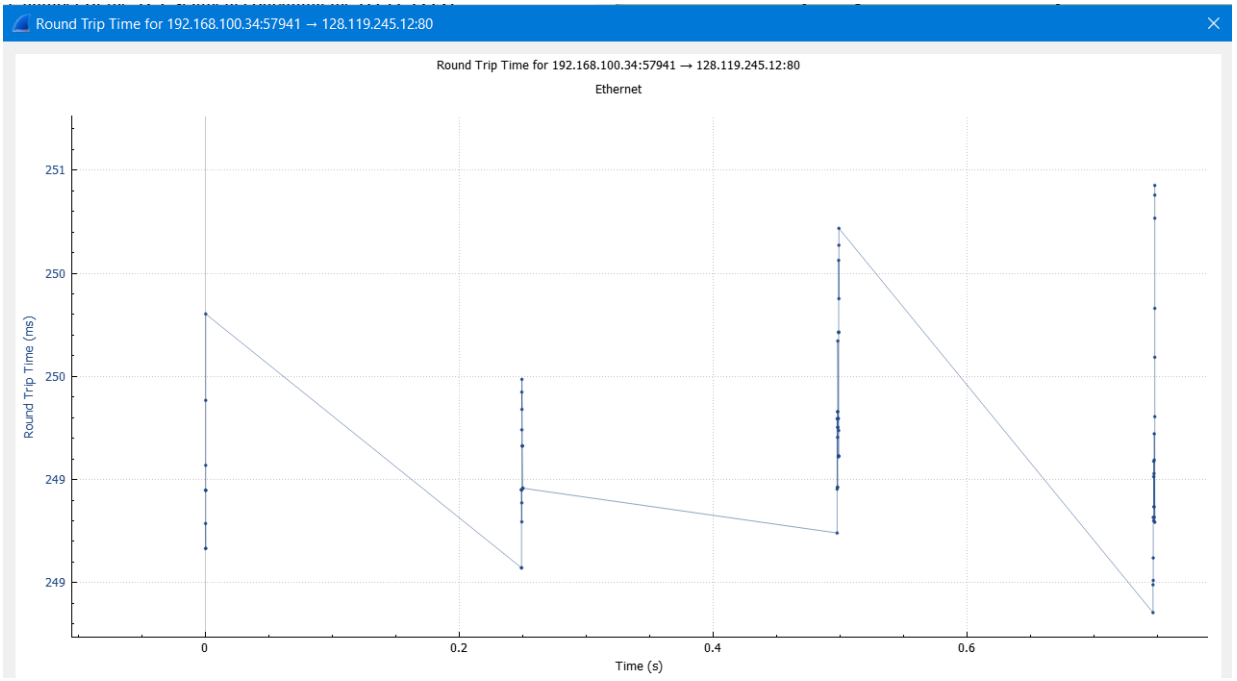
The segment 1 was sent at 07:44:09.578827
The segment 2 was sent at 07:44:09.578948



The ACK for segment 1 was received at 07:44:09.822073
The ACK for segment 2 was received at 07:44:09.827634



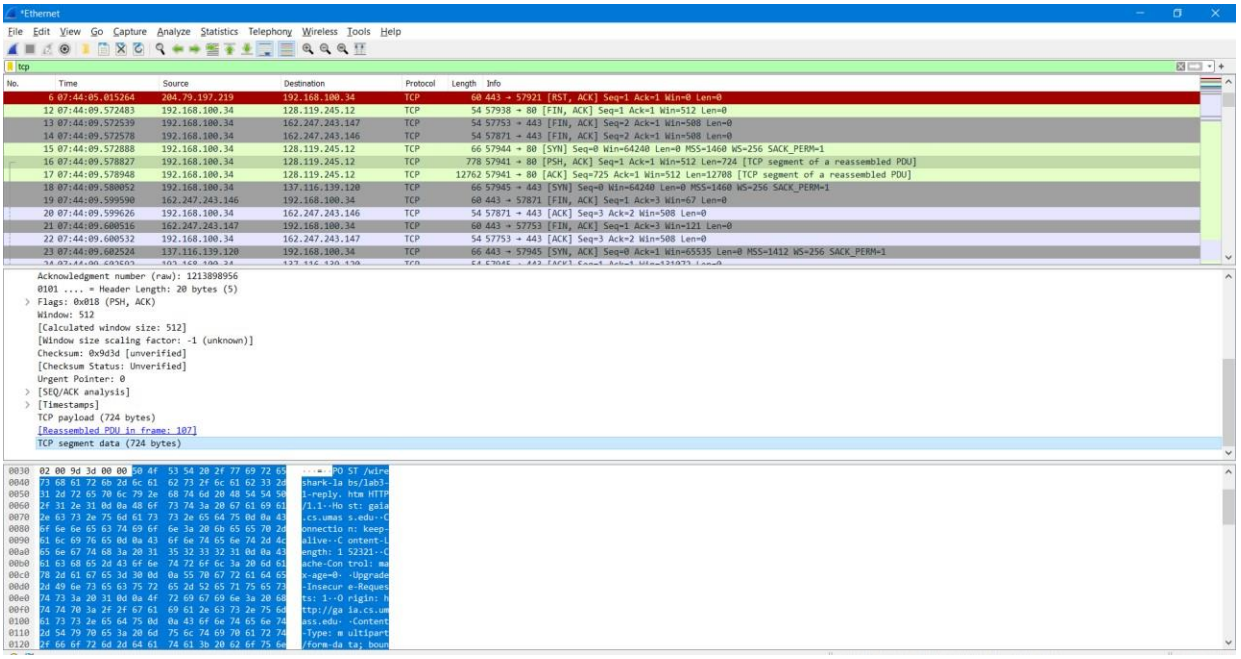
The round trip time for each of the segment sent:



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

Answer:

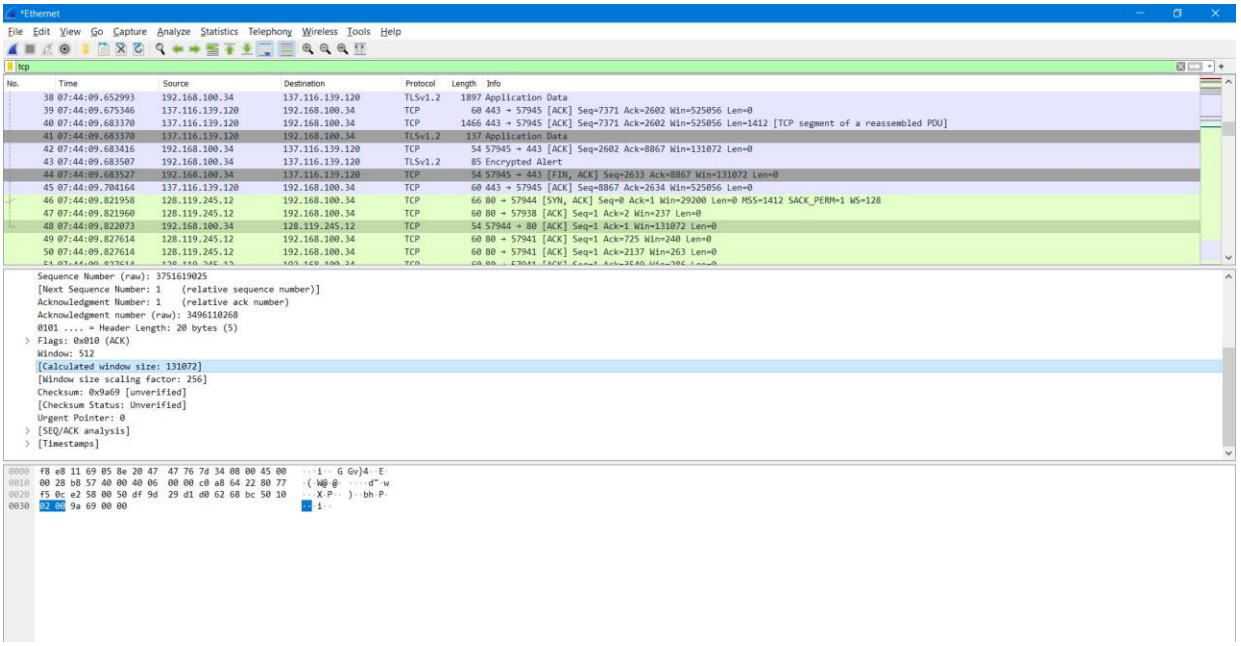
The length of each of the first TCP segment is 724 bytes. From the second TCP segment on, it would be 1412 bytes for each.



9. 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 advertised at the received of the entire trace is 240.



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

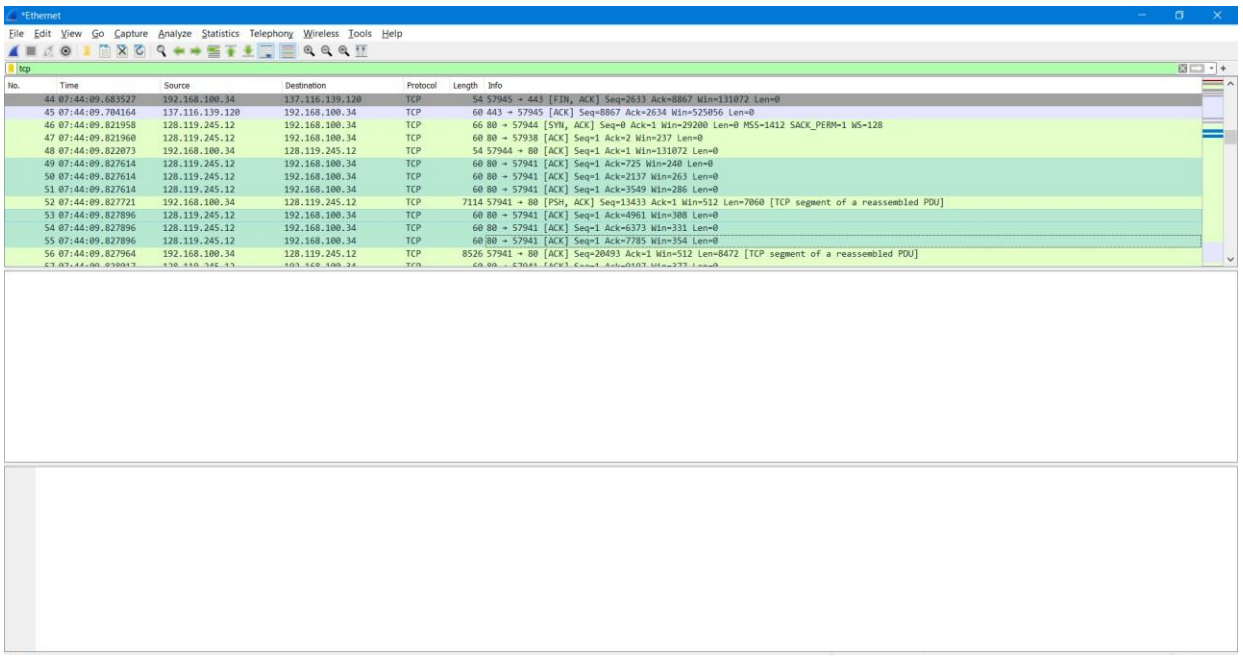
Answer:

No, there are no retransmitted segment in the trace file. I can check for it because there are no packet with the same sequence number at the different time.

11. 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:

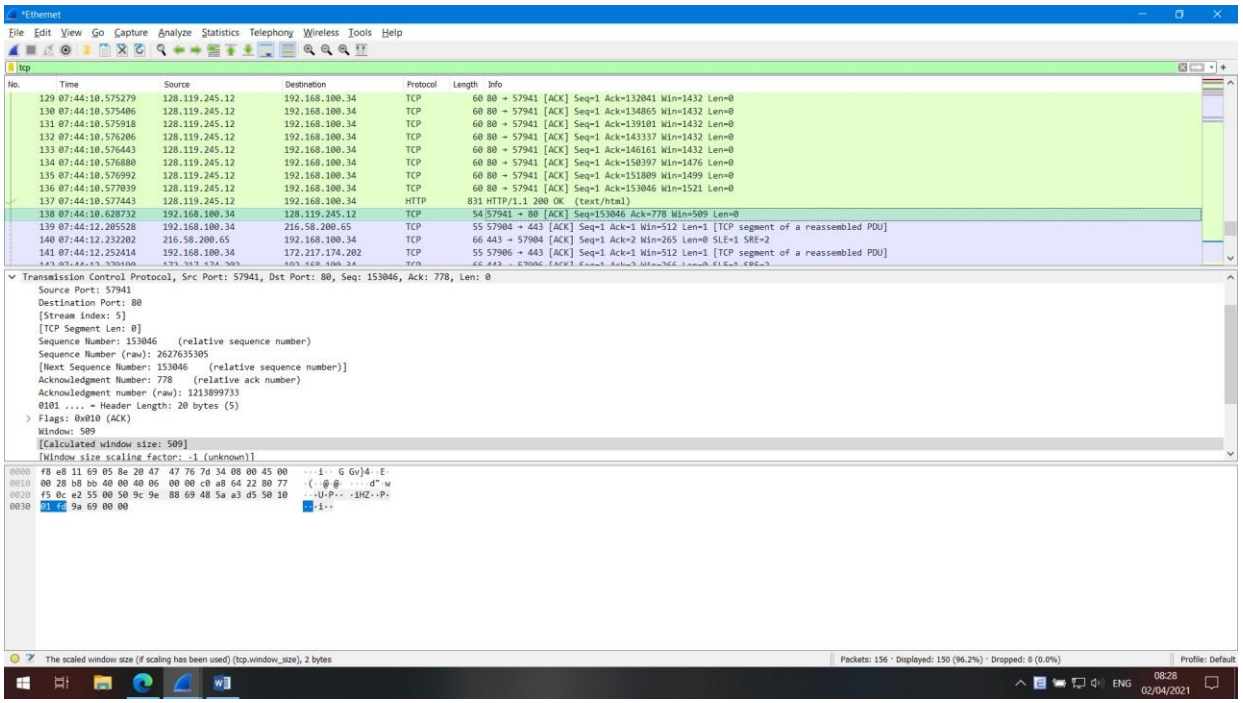
The screenshot below illustrates that the ACK numbers increase from 1 to 725 in the first segment. From the second segment on, it increase by 1412 bytes (725, 2137, 3549 and so on). The ACK numbers increases by 1412 each time, indicating that the receiver can acknowledge 1412 bytes.



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

Answer:

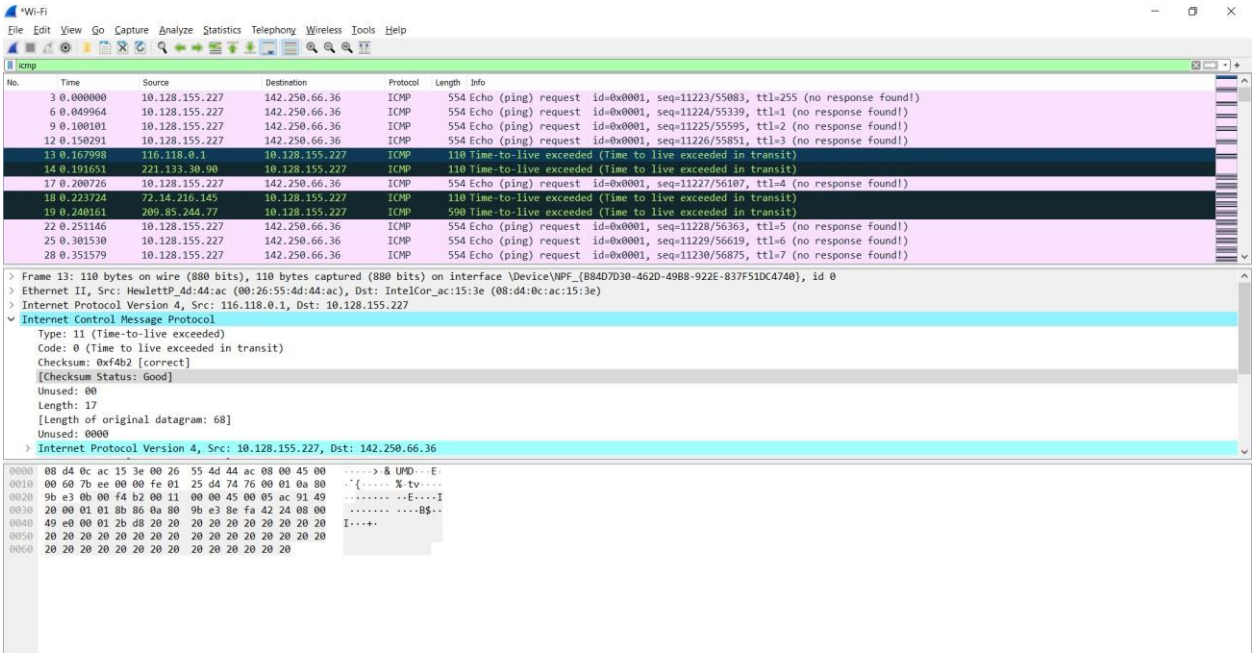
Throughput can be calculated by dividing the amount of data transmitted with the time incurred.
Amount of data transmitted is 153046 bytes
Time incurred is 7:44:09:822073 – 7:44:10.577039 = 0.754966 s
Throughput = 153046/0.754966 = 202719.0628 kbytes/s



LAB 5A – Wireshark : IP

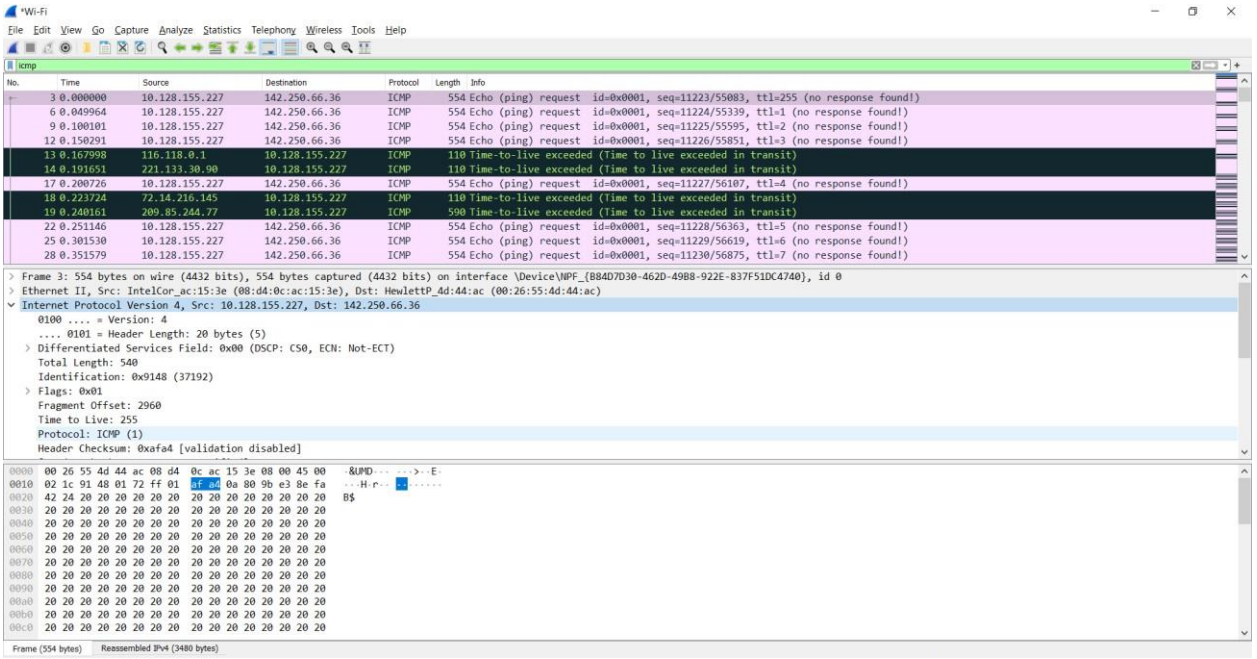
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

Answer: The IP address of my computer is 10.128.155.227



2. Within the IP packet header, what is the value in the upper layer protocol field?

Answer: Within the IP packet header, the value in the upper layer protocol field is ICMP (1)

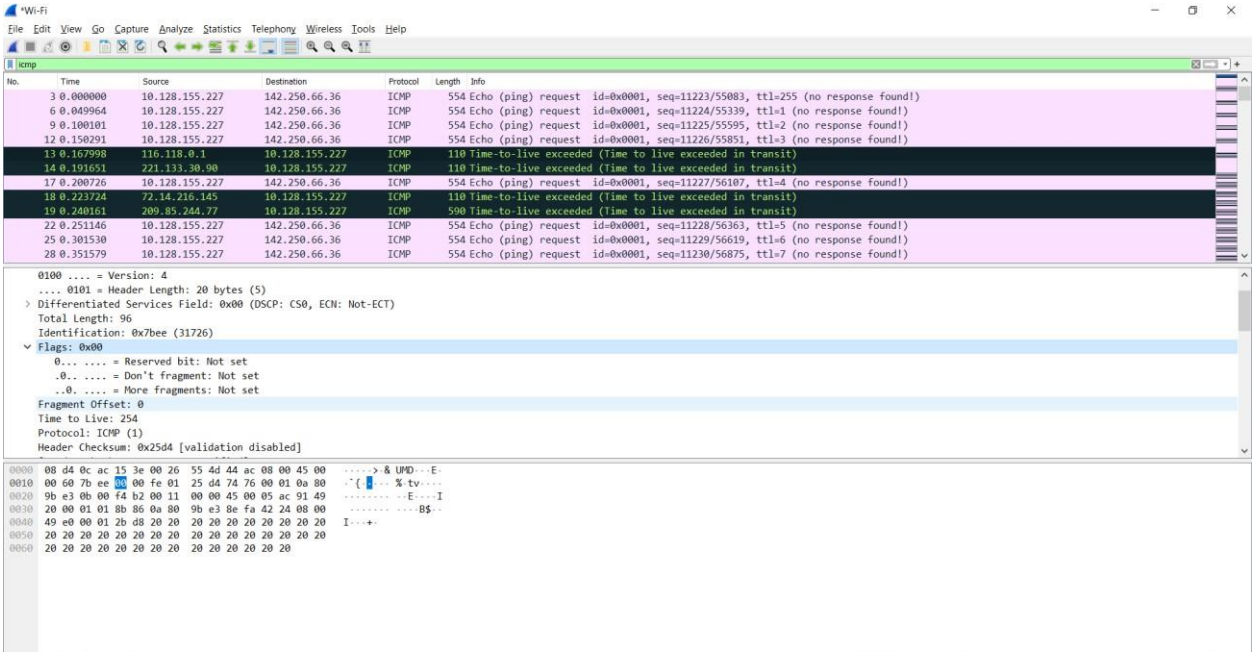


3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Answer: There are 20 bytes in the IP header. 36 bytes are in the payload of the IP datagram. We can determine the number of payload bytes by subtracting total bytes (in this case is 56) with IP header bytes (20 bytes).

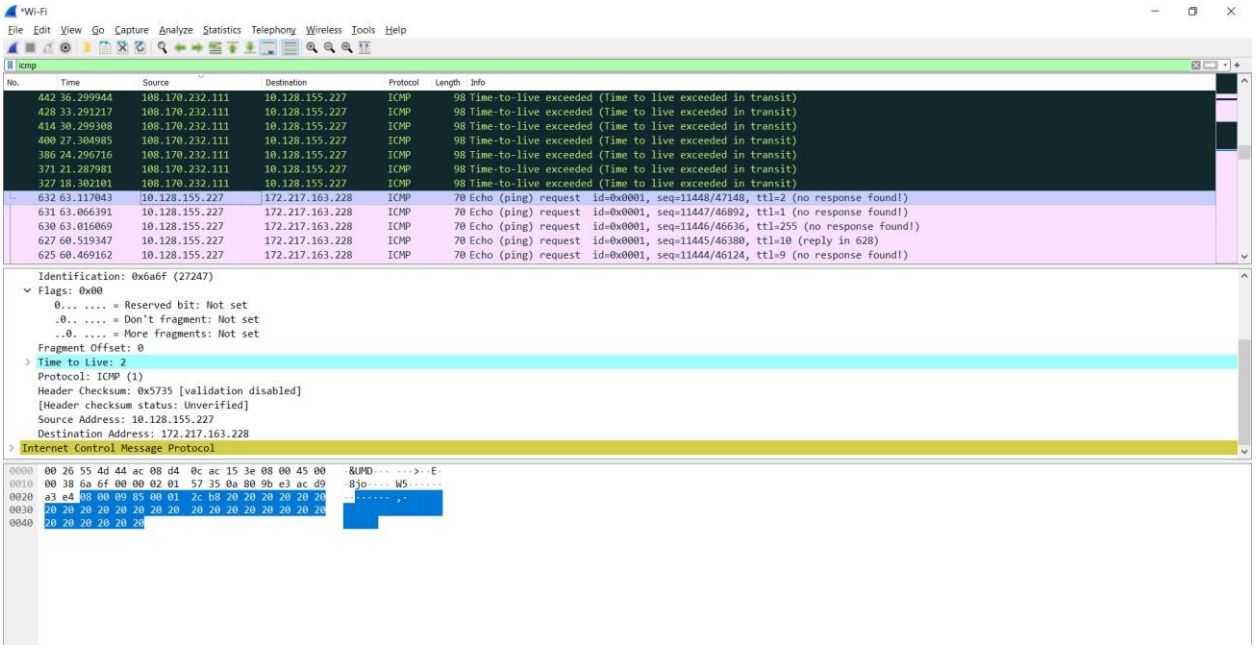
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

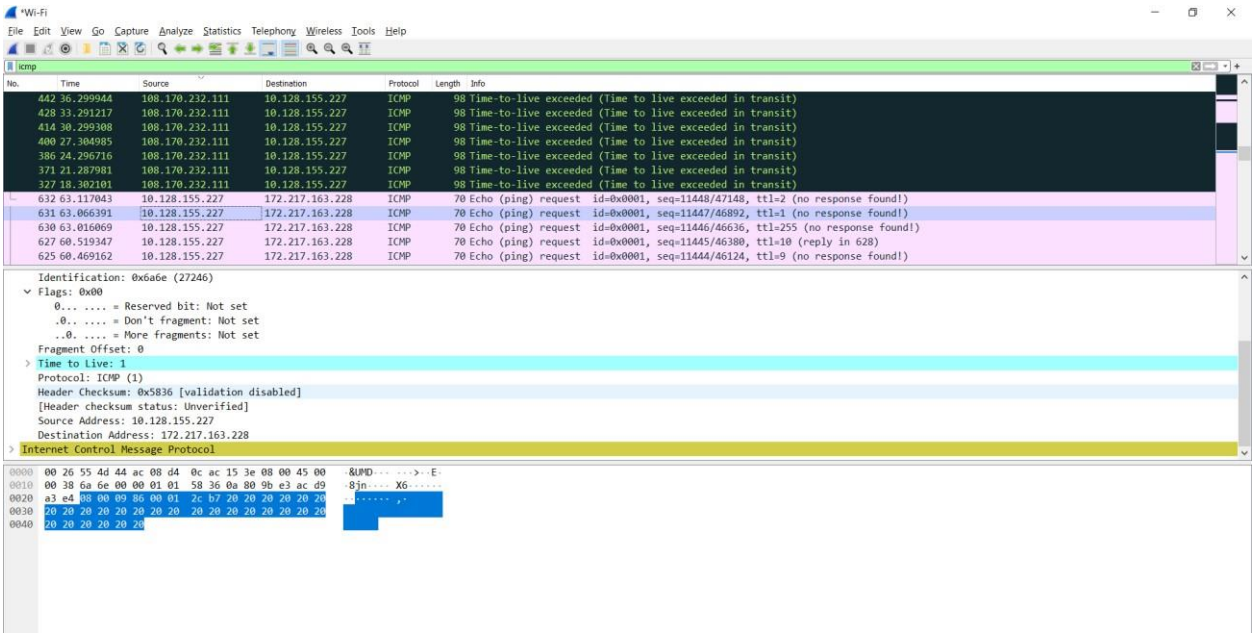
Answer: This IP datagram has not been fragmented because the reverse bits = 0.



5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Answer: The Identification, Time to Live and Header Checksum fields always change from one diagram to the next within this series of ICMP messages.





6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Answer:

+ The fields that stay constant are:

    - Version (IPv4 for all packets)
    - Header length (all of these are ICMP packets)
    - Source IP (the packets are sent from the same source)
    - Destination IP (the packets are sent to the same destination)

- Differentiated Services (all packets are ICMP and they all use the same type of service class)

- Upper Layer Protocol (all of these are ICMP packets)

+ The fields that must stay constant are:

- Version (IPv4 for all packets)

- Header length (all of these are ICMP packets)

- Source IP (the packets are sent from the same source)

- Destination IP (the packets are sent to the same destination)

- Differentiated Services (all packets are ICMP they all use the same type of service class)

- Upper Layer Protocol (all of these are ICMP packets)

+ The fields that must change are:

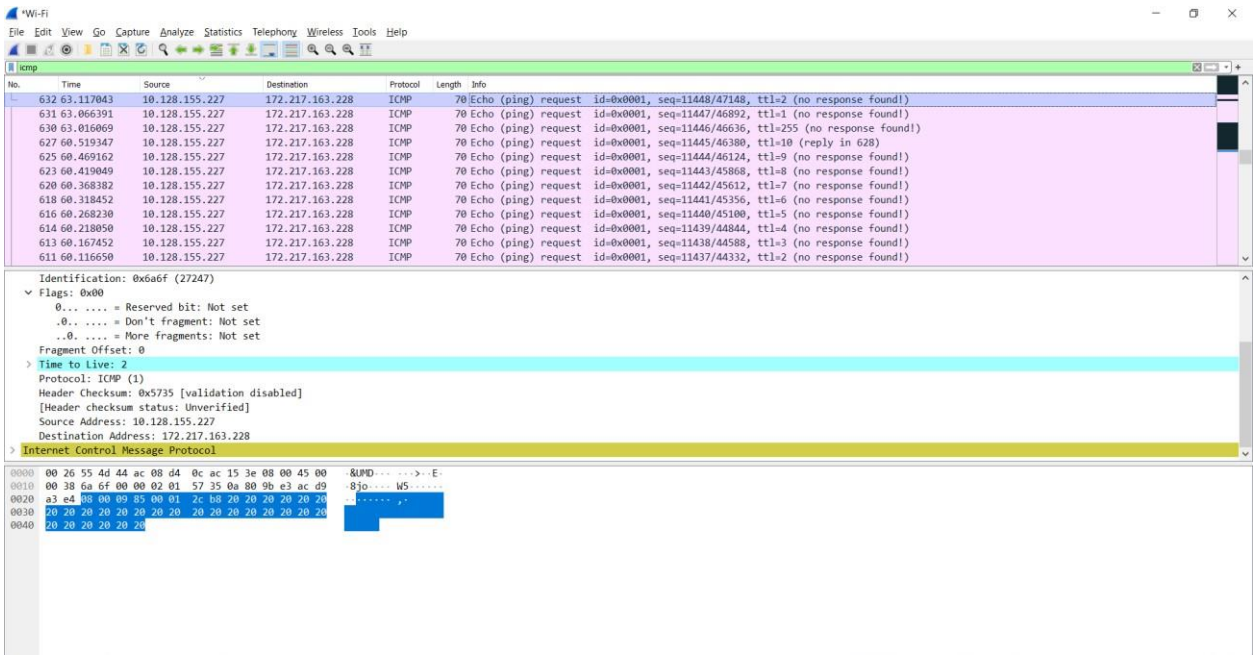
- Identification (each IP packet has unique ID)

- Time to live (traceroute increments each subsequent packet)

- Header checksum (header changes constantly, so we must checksum)

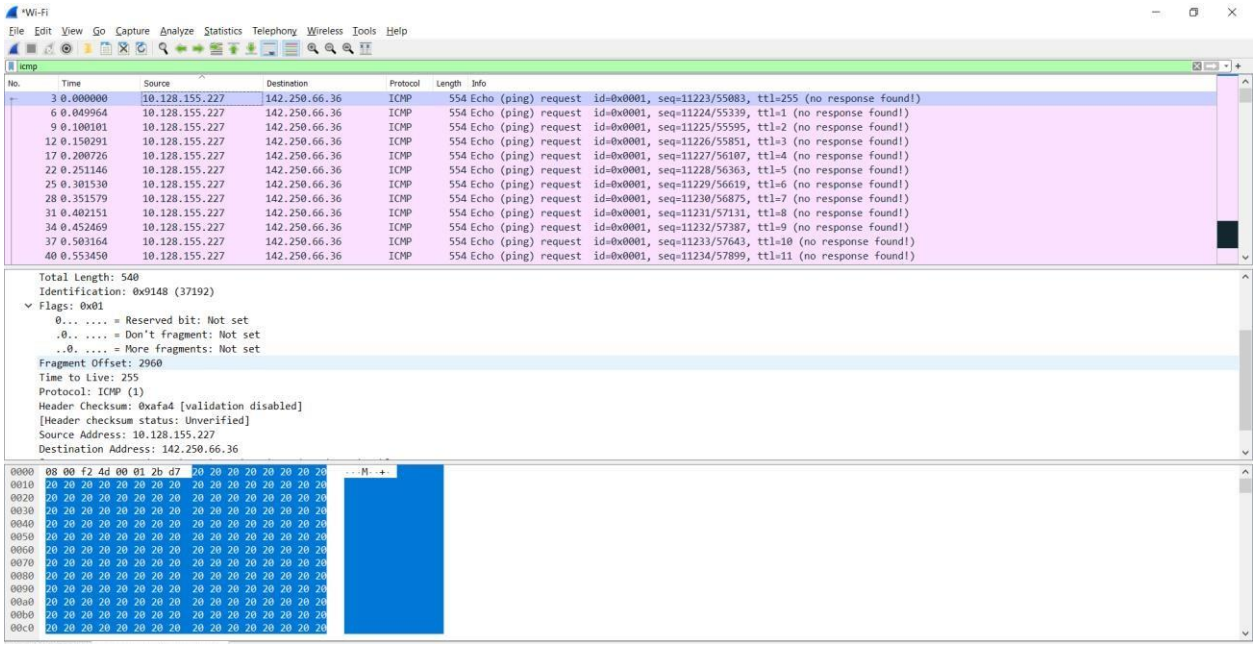
7. Describe the pattern you see in the values in the Identification field of the IP datagram.

Answer: The values in the Identification field of the IP datagram increases by 1 for each subsequent packet.



8. What is the value in the Identification field and the TTL field?

Answer: The value in the Identification field is 37192 and the value in TTL field is 255.

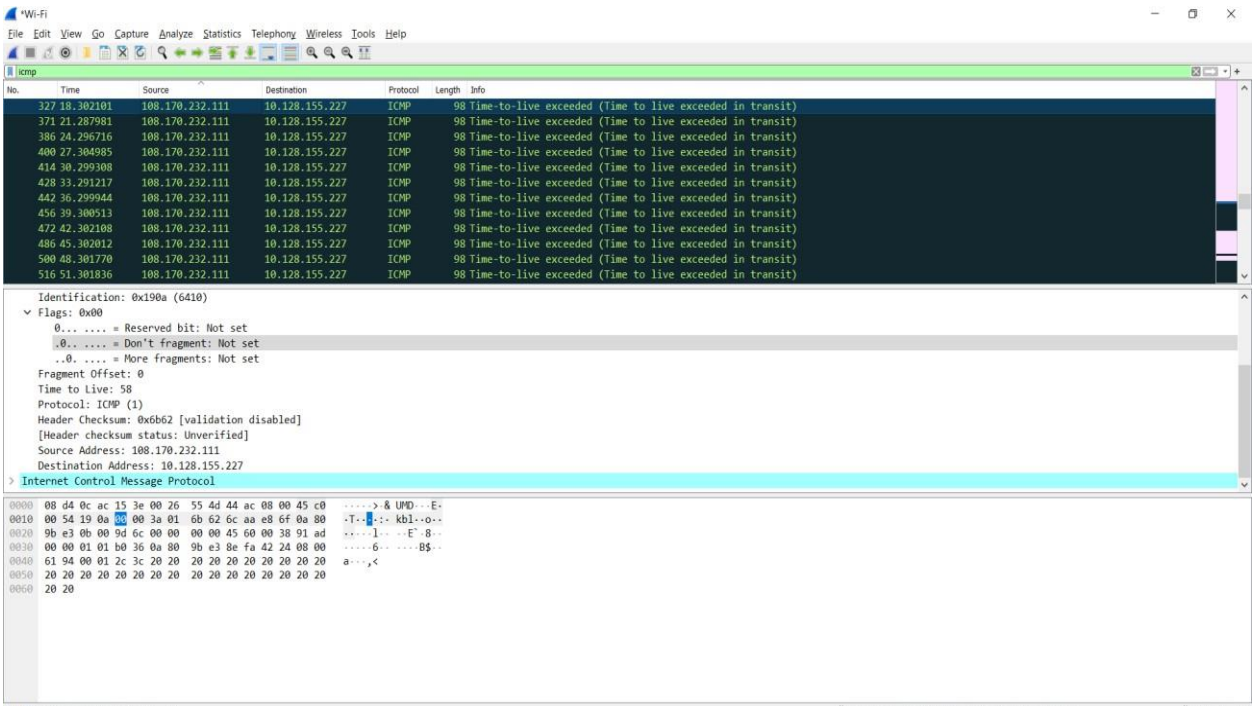


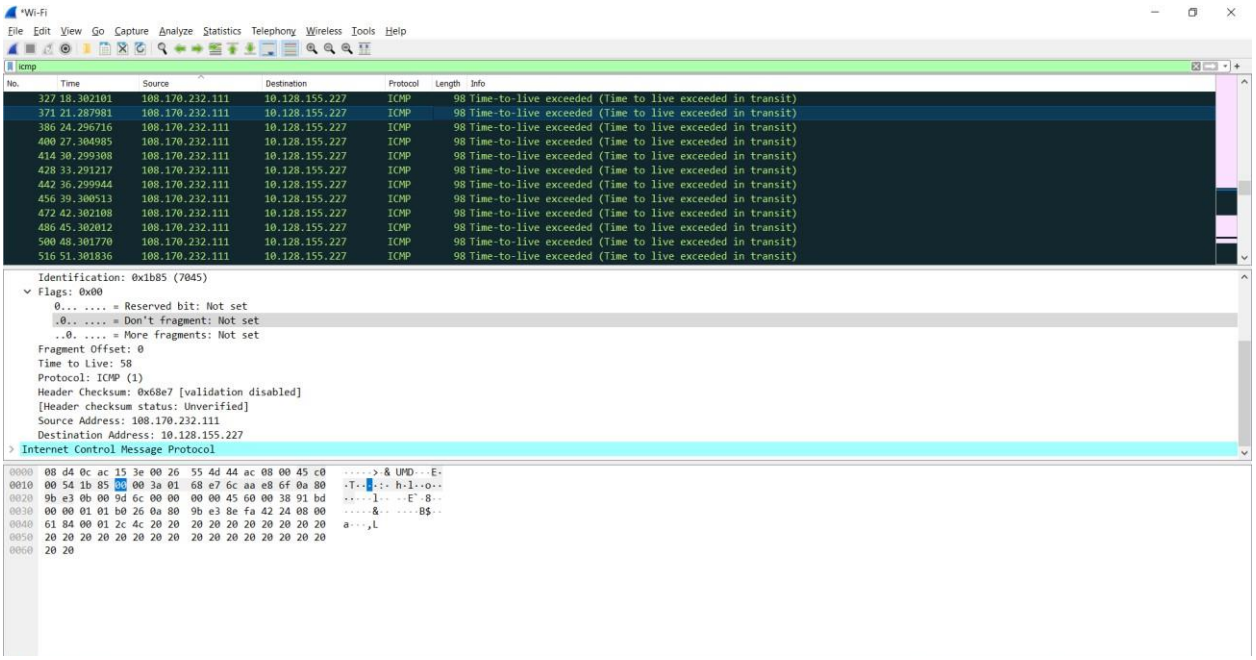
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Answer: These values doesn't remain unchanged for all of the ICMP TTL-exceeded replies sent to my computer by the nearest (first hop) router.

The identification field changes for all of the ICMP TTL-exceeded replies due to its uniqueness.

The TTL field will remain unchanged because the TTL for the first hop router is always the same.

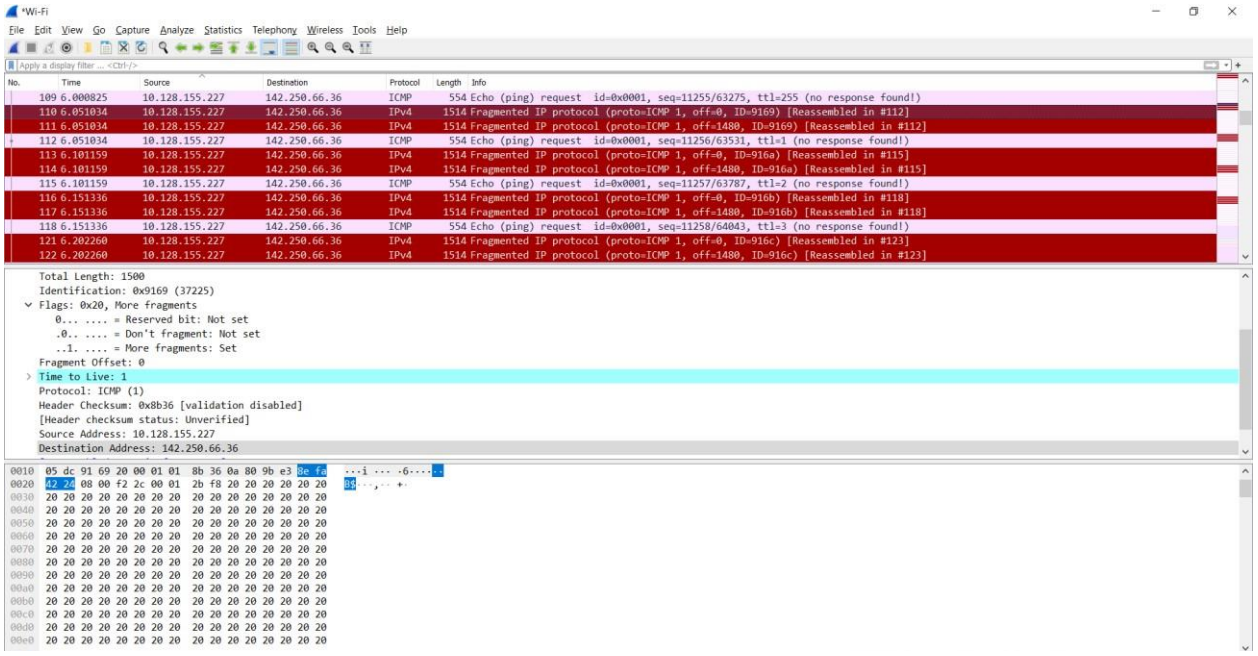




Fragmentation

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Answer: That message has been fragmented across more than one IP datagram.

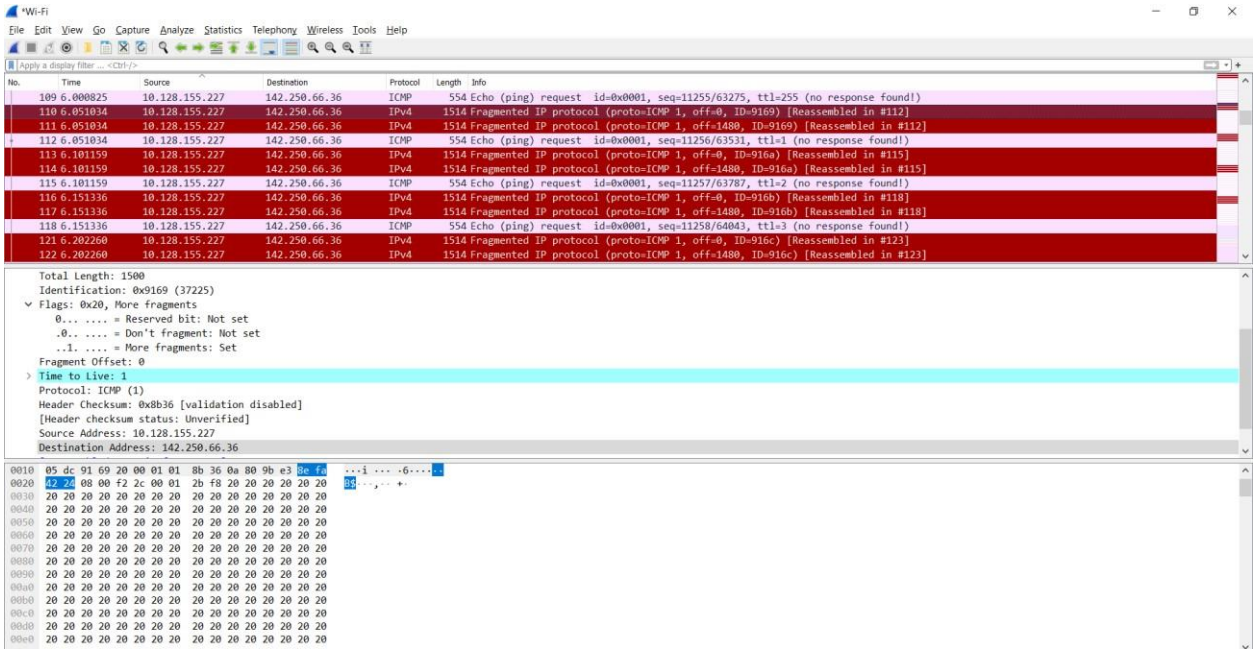


11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

Answer: The "More fragments" line in the Flags field combined with the "set" indicator in the "More fragments" subfield notifies us about the fragmentation in the datagram.

The "Fragment Offset: 0" in the IP header gives us a glimpse of the fact that this is the first fragment versus a latter fragment.

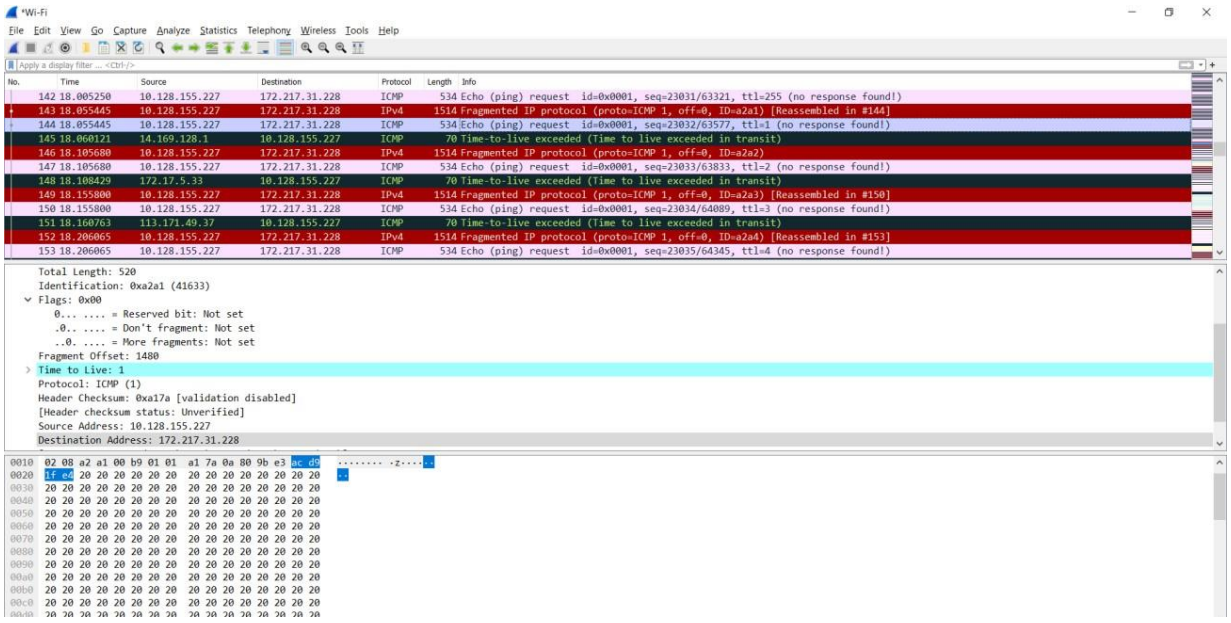
This IP datagram has the total length of 1500.



12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

Answer: This is not the first datagram fragment because its "Fragment offset" is not 0 but 1480 instead.

There are no more fragments because the "More fragments" subfield gives out the "Not set" indicator.



13. What fields change in the IP header between the first and second fragment?

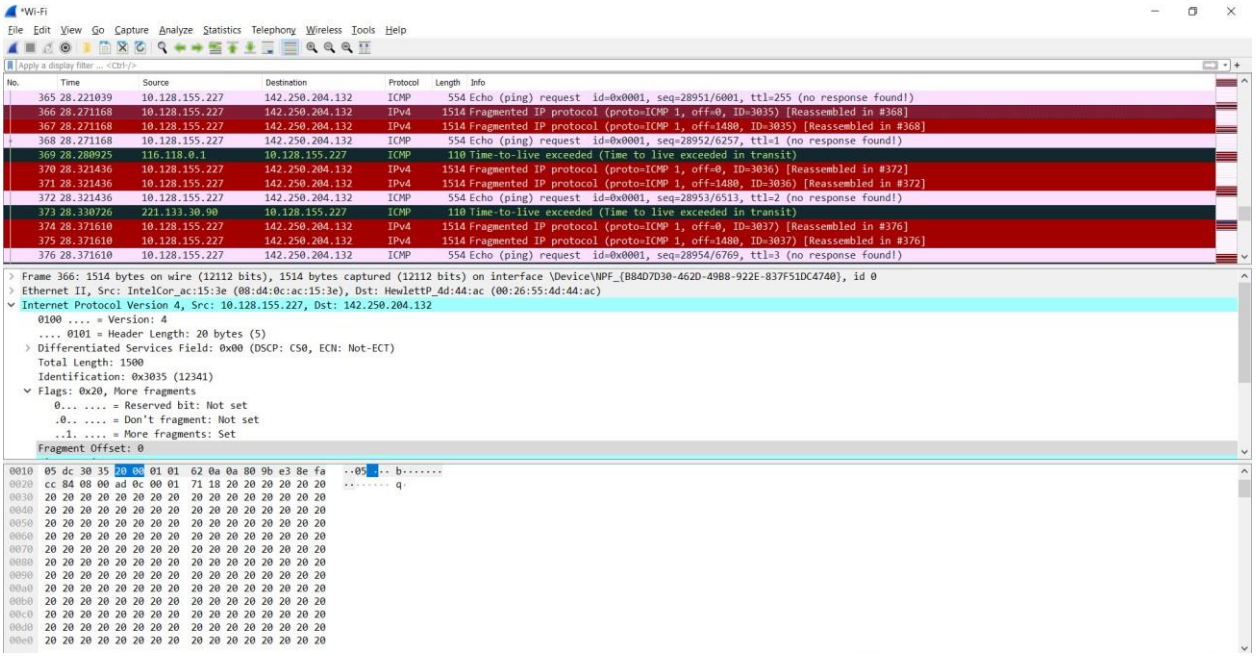
Answer: The fields which change in the IP header between the first and second fragment are:

- Total length
- Flags
- Fragment Offset
- Header checksum

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

14. How many fragments were created from the original datagram?

Answer: There were 3 fragments created from the original datagram.

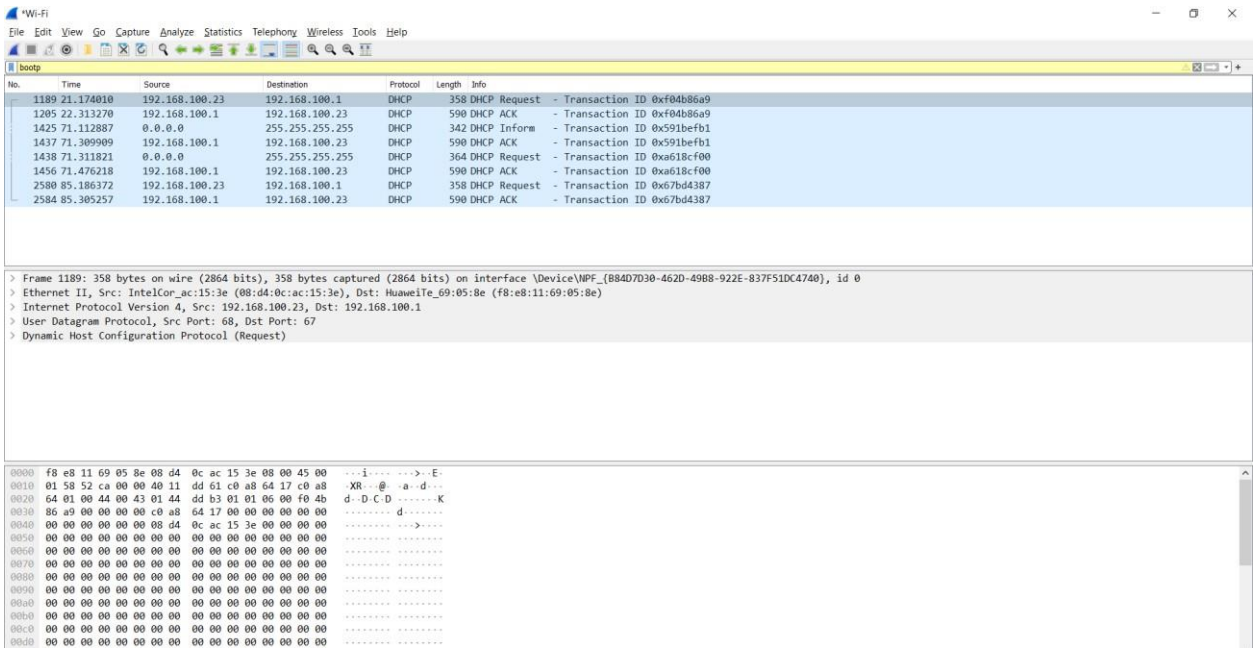


15. What fields change in the IP header among the fragments?

Answer: The fields which change in the IP header among the fragments are:

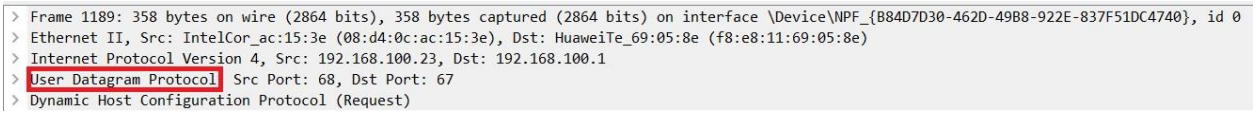
- Total length (The first and second fragment are identical but the third one is different)
- Flags (Same with the first and second fragment but the third one is different)
- Fragment Offset (Different for each fragment)
- Header Checksum (Different for each fragment)

LAB 5B – WIRESHARK: DHCP



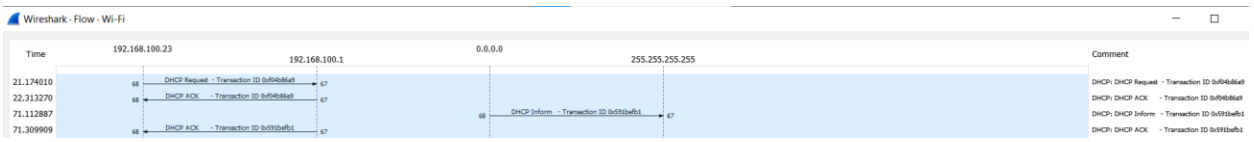
1. Are DHCP messages sent over UDP or TCP?

Answer: DHCP messages are sent over UDP (User Diagram Protocol).



2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

Answer: The port numbers are the same as in the example given in this lab assigment



3. What is the link-layer (e.g., Ethernet) address of your host?

Answer: The link-layer address of my host is (08:d4:0c:ac:15:3e)

```
(08:d4:0c:ac:15:3e)
```

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

Answer: I didn't receive any DHCP discover messages following the instruction.

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

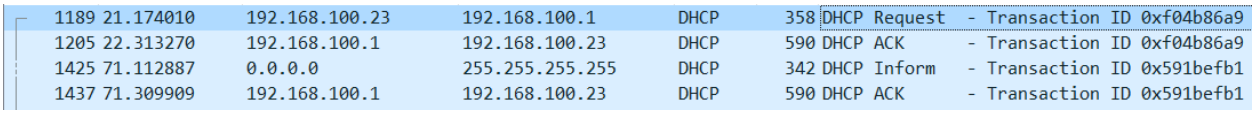
Answer:

Request - Transaction ID 0xf04b86a9

ACK - Transaction ID 0xf04b86a9

Inform - Transaction ID 0x591befb1

ACK - Transaction ID 0x591befb1



1189	21.174010	192.168.100.23	192.168.100.1	DHCP	358	DHCP Request - Transaction ID 0xf04b86a9
1205	22.313270	192.168.100.1	192.168.100.23	DHCP	590	DHCP ACK - Transaction ID 0xf04b86a9
1425	71.112887	0.0.0.0	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x591befb1
1437	71.309909	192.168.100.1	192.168.100.23	DHCP	590	DHCP ACK - Transaction ID 0x591befb1

6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

Answer: The DCHP client and server both use 255.255.255.255 as the destination address. The client uses source IP address 0.0.0.0, while the server uses its actual IP address as the source.

1205	22.313270	192.168.100.1	192.168.100.23	DHCP
1425	71.112887	0.0.0.0	255.255.255.255	DHCP
1437	71.309909	192.168.100.1	192.168.100.23	DHCP
1438	71.311821	0.0.0.0	255.255.255.255	DHCP

7. What is the IP address of your DHCP server?

Answer: The IP address of my DHCP server is 192.168.100.1

192.168.100.1	192.168.100.23	DHCP

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

Answer: I didn't receive any DHCP offer messages following the instruction.

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

Answer:

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

Answer: The router line indicates to the client what its default gateway. The subnet mask line tells the client which subnet mask it can use.

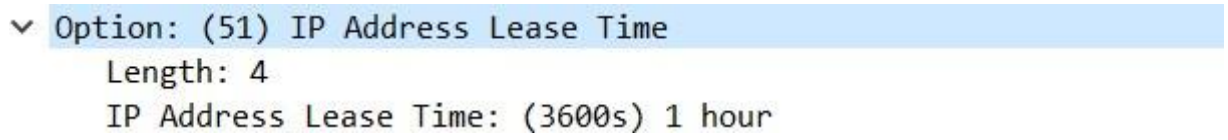
```
Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
Option: (3) Router
    Length: 4
    Router: 192.168.100.1
```

11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

Answer: I didn't receive any DHCP discover messages following the instruction.

12. Explain the purpose of the lease time. How long is the lease time in your experiment?

Answer: The lease time is the total amount of time the DHCP server assigns an IP address to a client. During the lease time, the DHCP server will not assign the IP given to the client to another client, unless it is released by the client. Once the lease time has expired, the IP address can be reused by the DHCP server to give to another client. In my experiment, the lease time is 1 hour.



13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

Answer: The client sends a DHCP Release message to cancel its lease on the IP address given to it by the DHCP server.

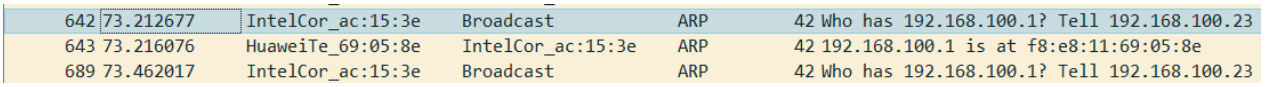
The DHCP server does not send a message back to the client acknowledging the DHCP Release message.

If the DHCP Release message from the client is lost, the DHCP server would have to wait until the lease period is over for that IP address until it could reuse it for another client.

14. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of

those ARP packets.

Answer: There were 2 ARP packets sent or received during the DHCP packet-exchange period.



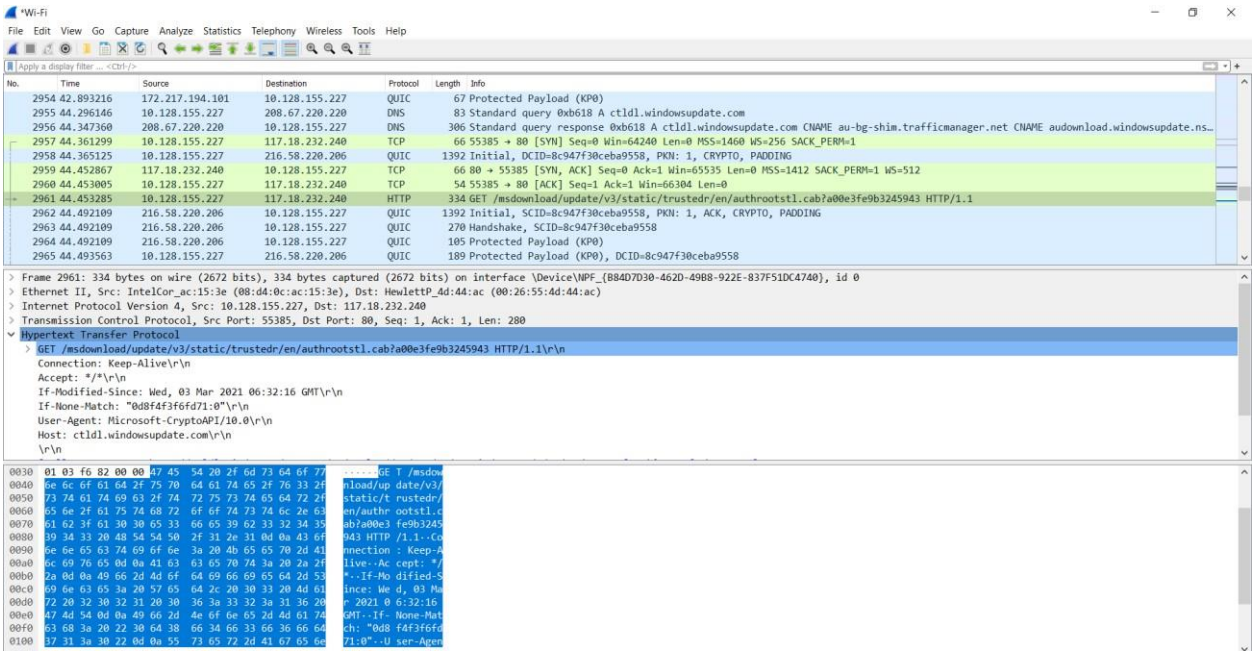
642	73.212677	IntelCor_ac:15:3e	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.23
643	73.216076	HuaweiTe_69:05:8e	IntelCor_ac:15:3e	ARP	42	192.168.100.1 is at f8:e8:11:69:05:8e
689	73.462017	IntelCor_ac:15:3e	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.23

The purpose of these ARP packets are keeping a record of each IP address and its matching MAC address. Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed.

LAB 5C – WIRESHARK: NAT

1. What is the IP address of the client?

Answer: The IP address of the client is 10.128.155.227

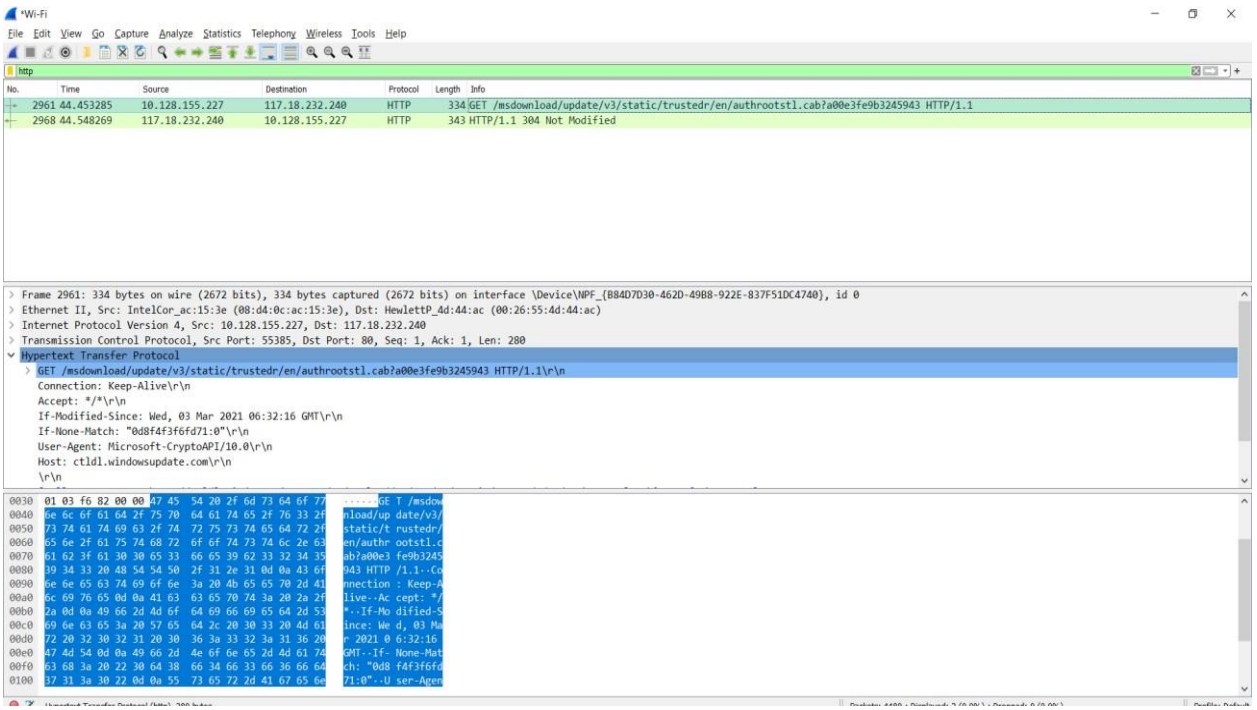


2. The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression "http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark.

3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Answer: The source: 10.128.155.227, port 55835

The destination: 117.18.232.240, port 80

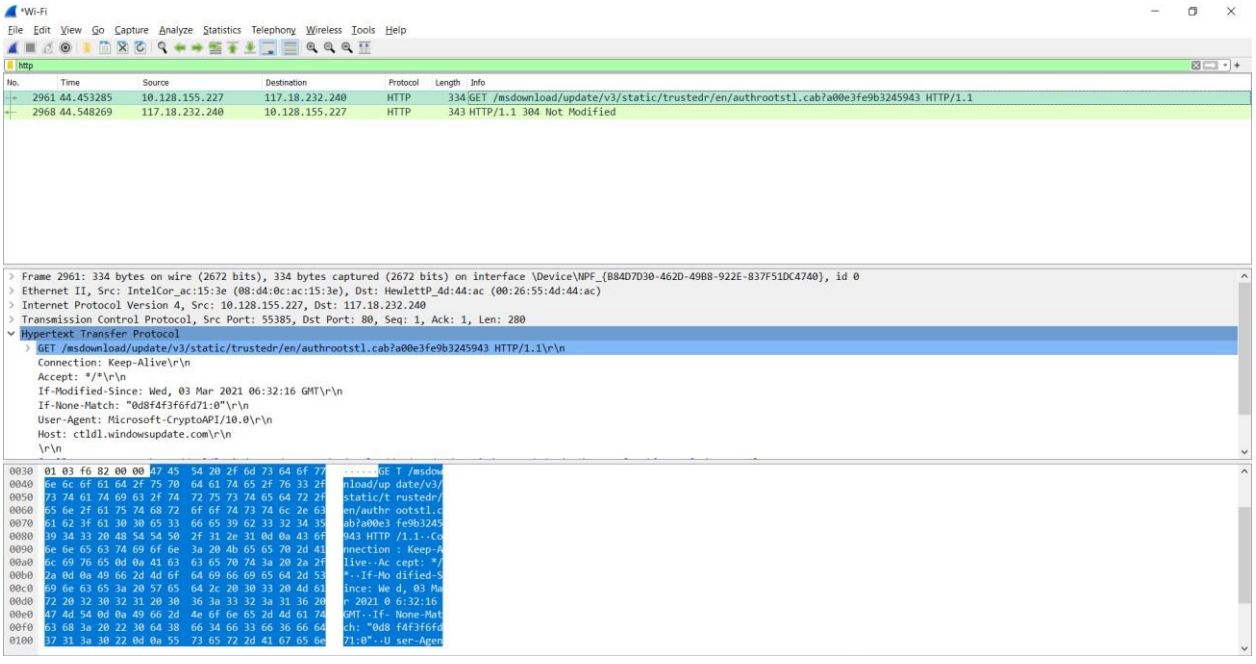


4. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Answer: The corresponding 200 OK HTTP message from the Google server is received at 44.548269

The source: 117.18.232.240, port 80

The destination: 10.128.155.227, port 55835

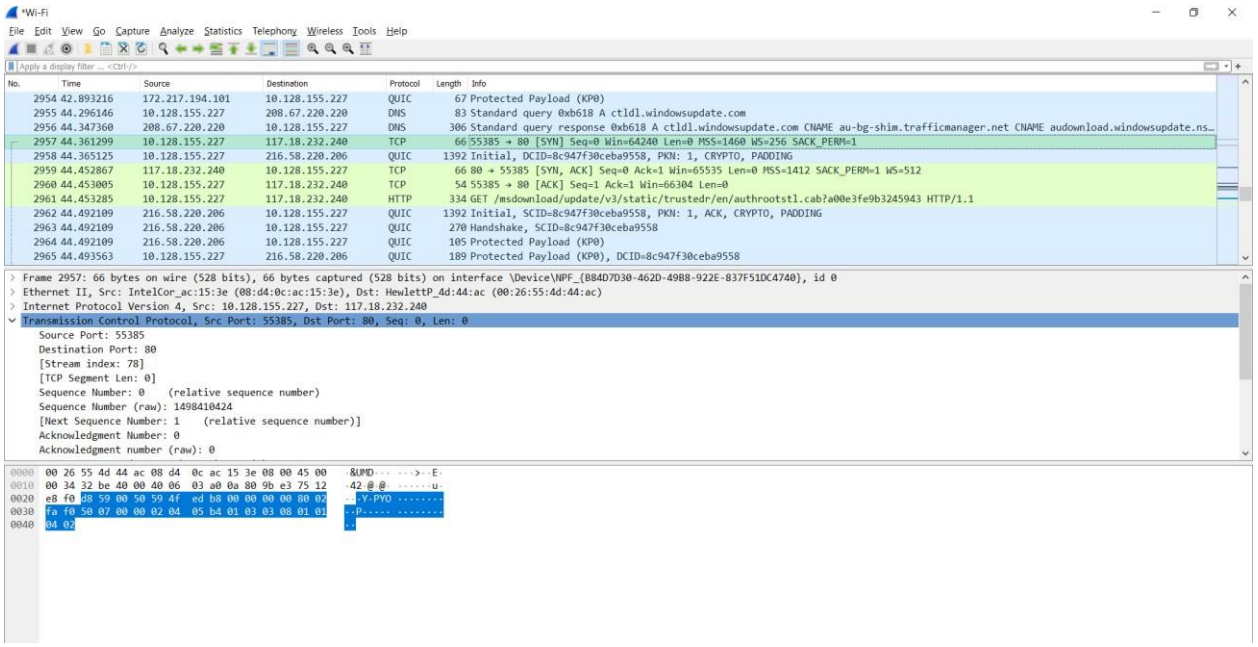


5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark).

Answer: The client-to-server TCP SYN segment that gets up the connection used by the GET sent at time 7.109267 is sent at 44.361299

The source for the TCP SYN segment: 10.128.155.227, port 55385

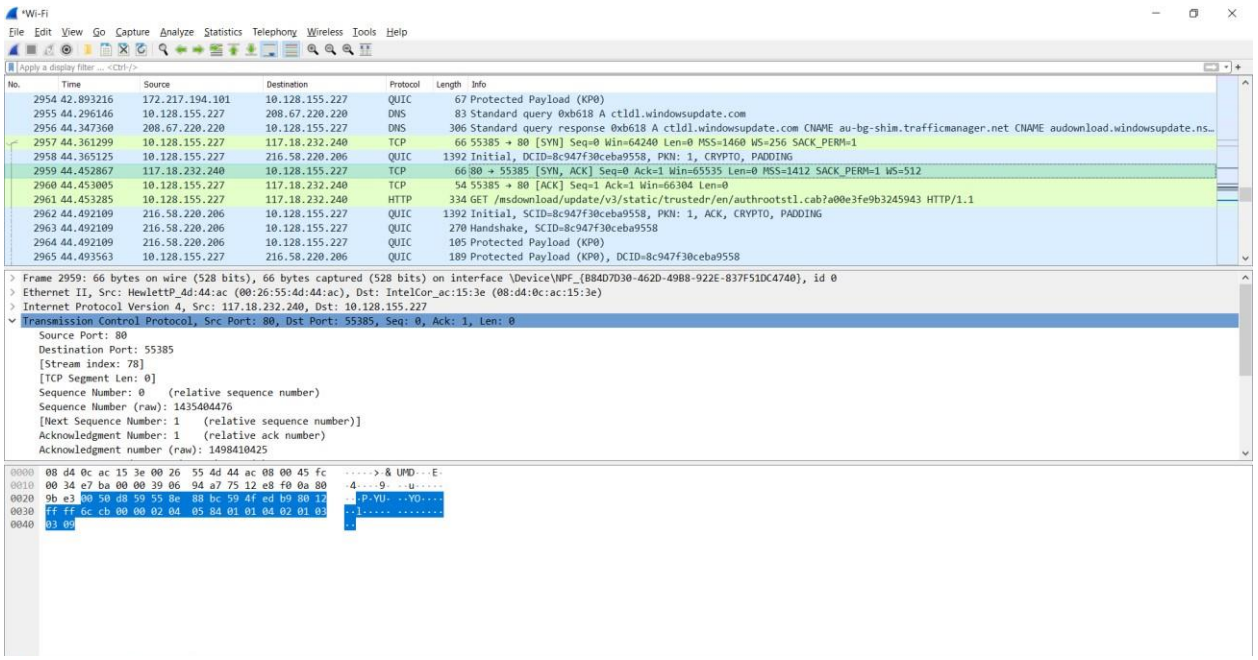
The destination for the TCP SYN segment: 117.18.232.240, port 80



The source for the TCP ACK segment: 117.18.232.240, port 80

The destination for the TCP ACK segment: 10.128.155.227, port 55835

This ACK segment is received at 44.452867



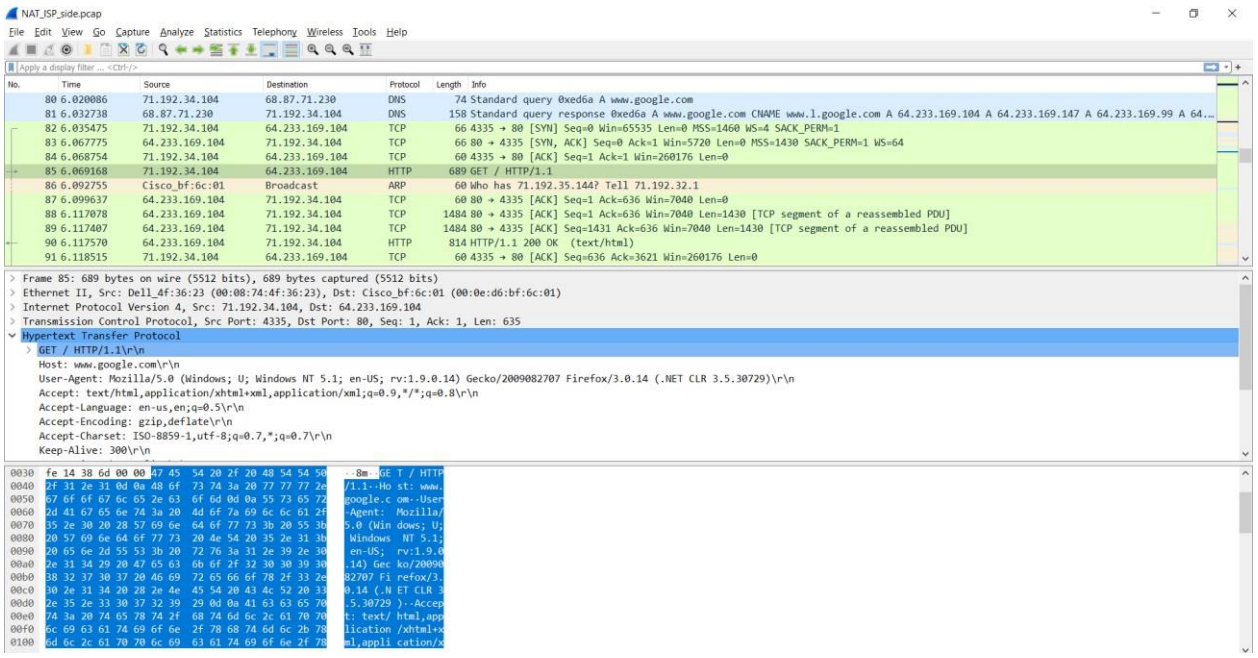
6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

Answer: This message appears in the NAT_ISP_side trace file at 6.069168

The source: 71.192.34.104, port 4335

The destination: 64.233.169.104, port 80

The destination is the same as the question 3 above but the source IP address are different.



7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Answer: There are no fields in the HTTP GET message changed.

In the IP datagram carrying the HTTP GET: the Version, Header Length and Flags remains the same but the Checksum has changed.

The reason for the changing of the Checksum is the source IP has changed.

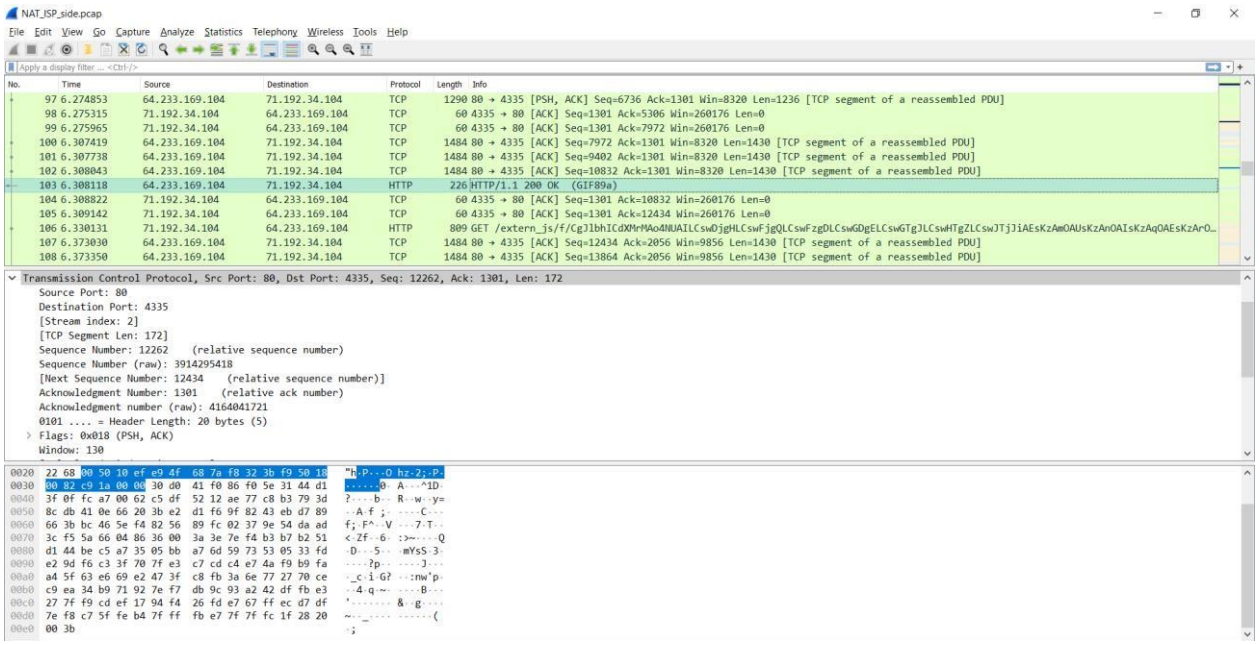
8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

Answer: The first 200 OK HTTP message received at 6.308118

The source: 64.233.169.104, port 80

The destination: 71.192.34.104, port 4335

All of these fields are the same except the destination IP address.



9. In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

Answer: The time for SYN is 6.035475

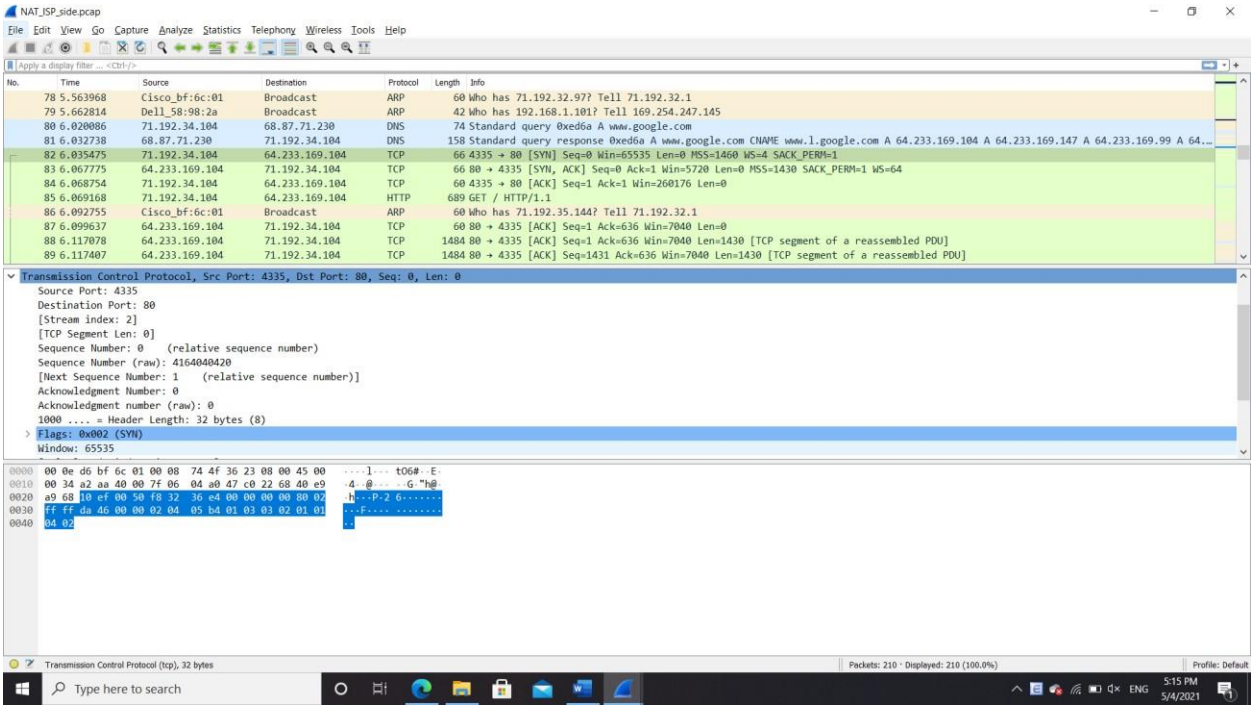
The time for ACK is 6.067775

The source for the SYN is 71.192.34.104, port 4335

The destination for the SYN is 64.233.169.104, port 80

The source for the ACK is 64.233.169.104, port 80

The destination for the ACK is 71.192.34.104, port 4335



For the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged.

10. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

Answer:

NAT Translate Table	**NAT Translate Table**
WAN side	**LAN side**
71.192.34.104	**64.233.69.104**
Port: 4335	**Port: 4335**

Extra Credit: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and write a half page explanation of the purpose of each of these messages.