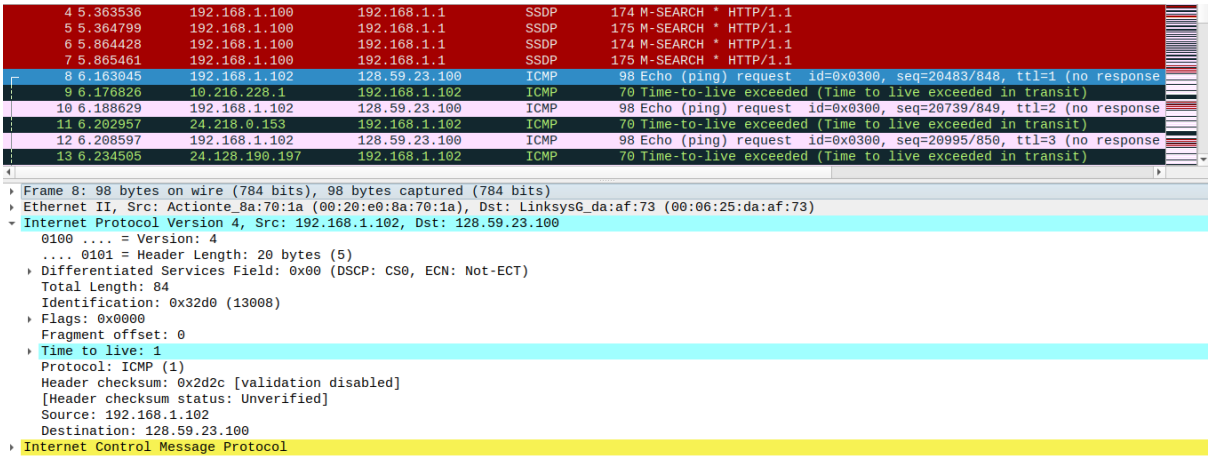
Lab_4a_Wireshark_IP_v8.0

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 192.168.1.162

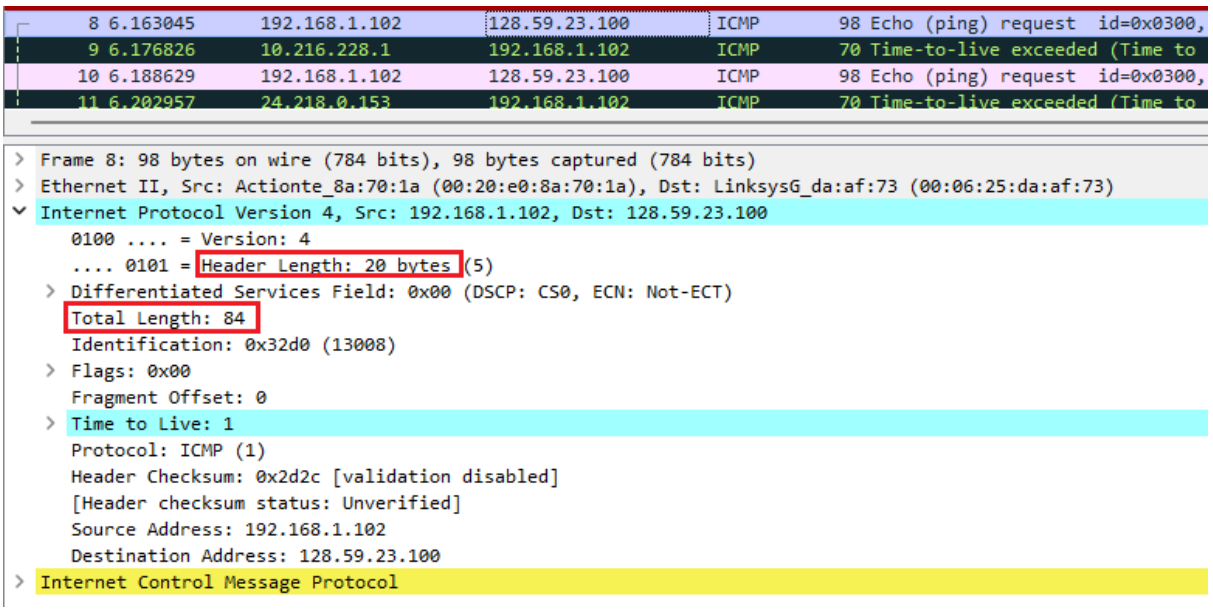
2. Within the IP packet header, what is the value in the upper layer protocol field?

Answer:

The value of the upper layer protocol field is ICMP

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 which leaves 64 bytes for the payload of the IP datagram because we were sending a packet of length 84 bytes.

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

Answer: Not fragmented. b/c The more fragments bit = 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:

Time to live, Identifier and header checksum always change from one datagram to the next.

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 (since we are using IPv4)
    + Header length (since these are UDP packets)
    + Source IP (since all packets are sent from my computer)
    + Destination IP (since we are sending to the same host)
    + Differentiated Services (since all packets are UDP)
    + Upper Layer Protocol (since these are UDP packets)
- The fields that must stay constant are:
    + Version (since we are using IPv4)
    + Header length (since these are UDP packets)
    + Source IP (since all packets are sent from my computer)
    + Destination IP (since we are sending to the same host)
    + Differentiated Services (since all packets are UDP)
    + Upper Layer Protocol (since these are UDP packets)
- The fields that must change are:
    + Identification (IP packets have different ids)
    + Time to live (traceroute increments each packet)
    + Header checksum (since header changes)

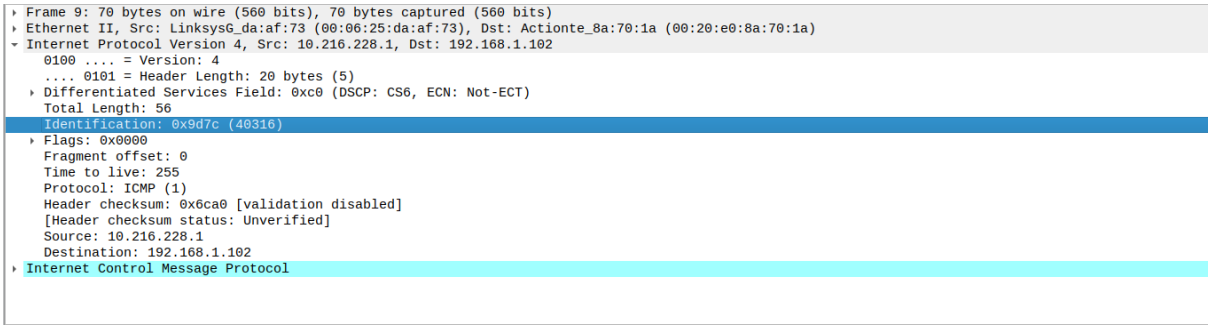
7. Describe the pattern you see in the values in the Identification field of the IP datagram

Answer:

The pattern in the identification field is that the field increases by one in each strand of echo requests.

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

Answer:



Identification: 40316
TTL: 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:

- The Identification field changes from all of the replies because this field has to have a unique value. If they(2 or more replies) have the same value then the replies must be fragments of a bigger packet.
- The TLL field does not change because the time to live to the first hop router is always the same.

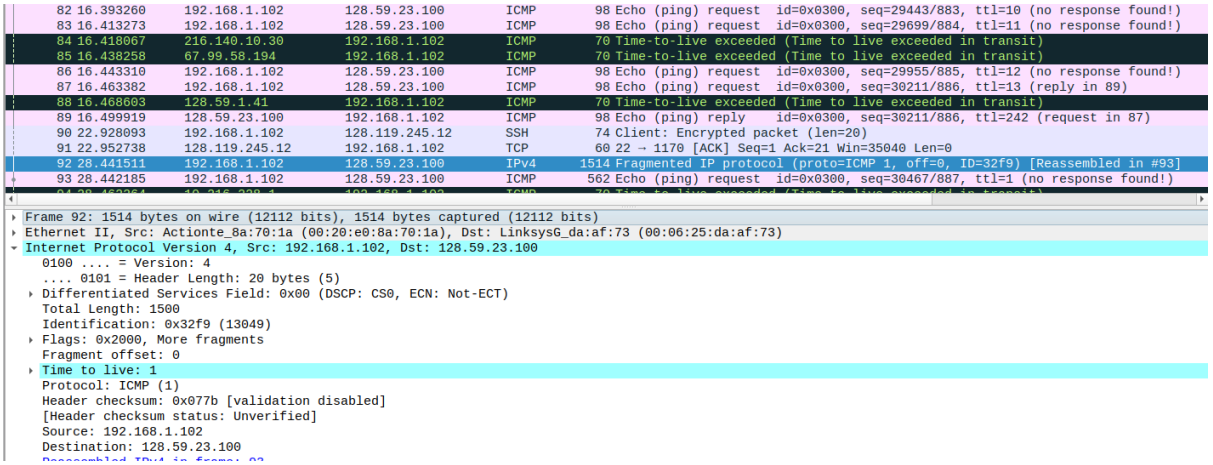
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]

Answer:

This packet has been fragmented across more than one IP datagram

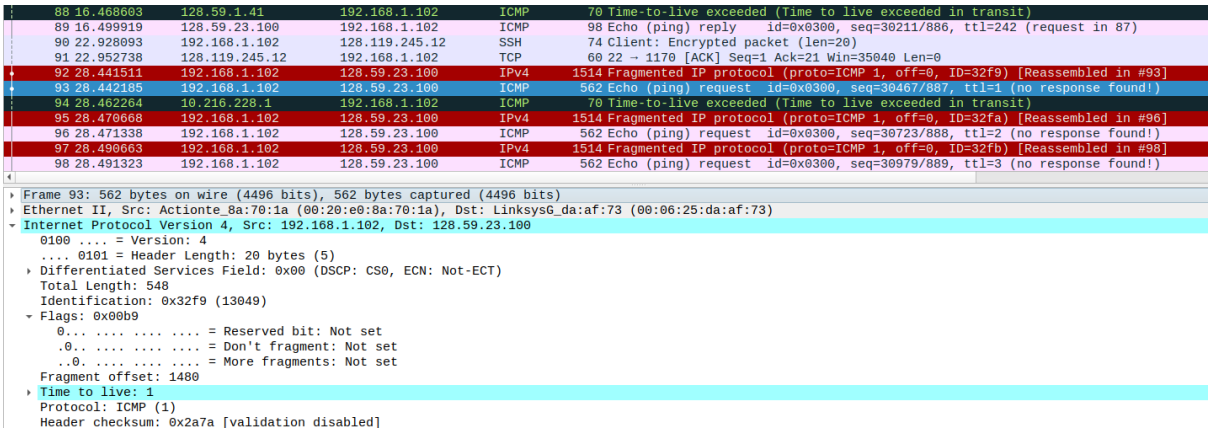
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

Answer:



- The Flags bit for more fragments is set, indicating that the datagram has been fragmented.
- Since the fragment offset is 0, we know that this is the first fragment.
- This first datagram has a 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:

According to above screenshot, this is not the first fragment since the fragment offset is 1480 and this should be the last fragment, since the status of more fragments flag is not set.

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

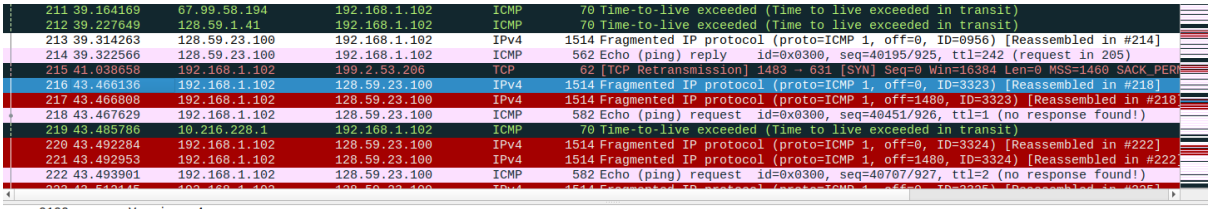
Answer: Total length, flags, fragment offset, and checksum.

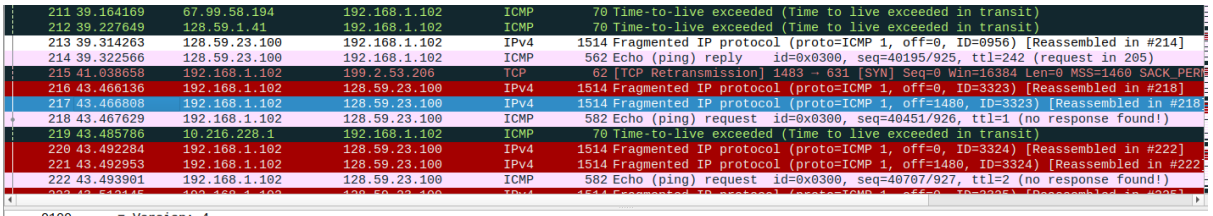
14. How many fragments were created from the original datagram?

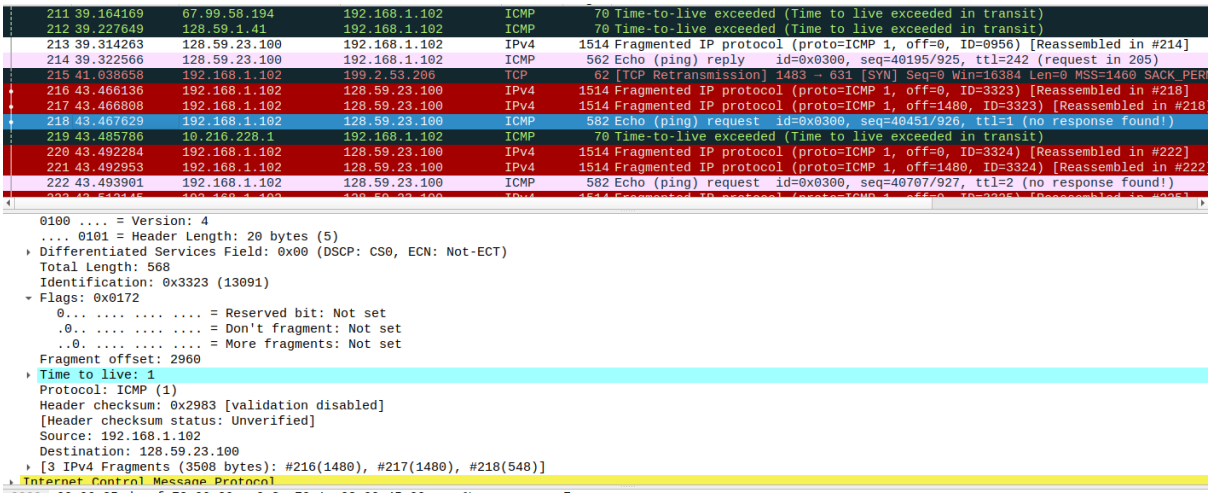
Answer: there are 3 packets created from the original datagram.

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

Answer:







- The IP header fields that changed between all of the packets are: fragment offset, and checksum.
- The first two packets have a total length of 1500, with the more fragments bit set to 1
- The last packet has a total length of 568, with the more fragments bit set to 0.