Lab 3

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

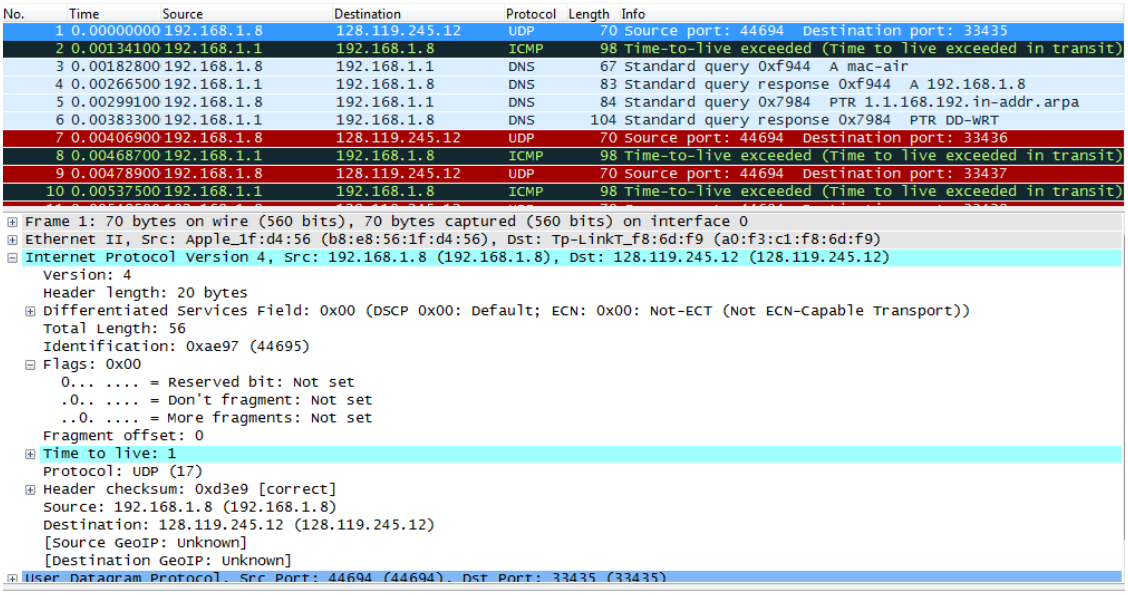


Figure 1

According to the figure 1, the IP address of my computer is 192.168.1.8.

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

Answer

According to the figure 1, within the IP packet header, the value in the upper layer protocol field is UDP (17)

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

According to the figure 1, the header length is 20 bytes and the total length is 56 bytes. Therefore, the payload of the IP datagram should be 36 bytes (56 bytes – 20 bytes).

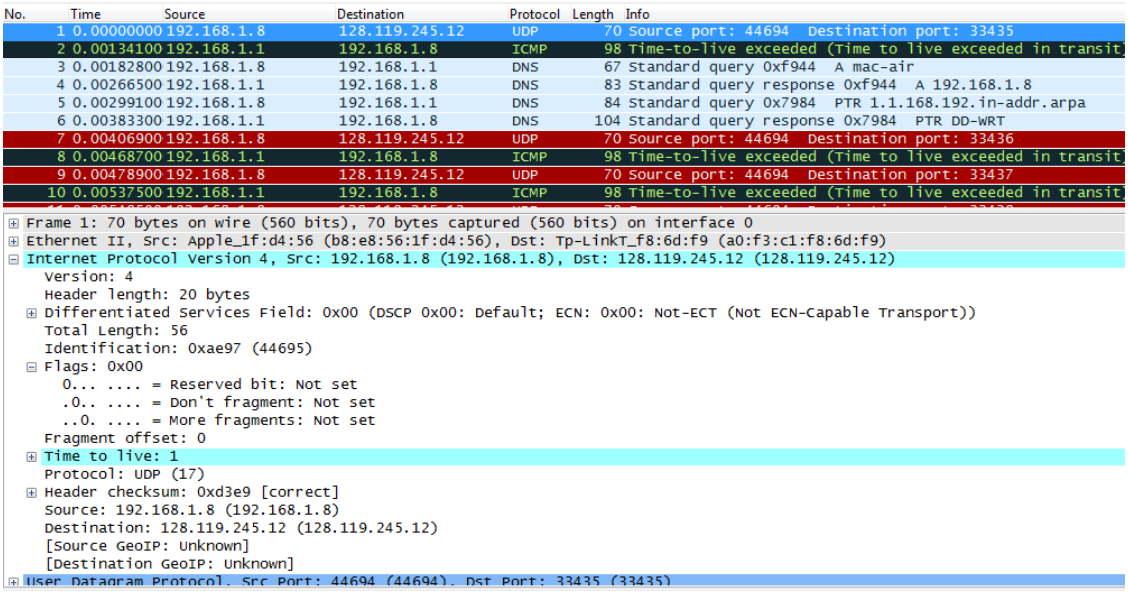
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

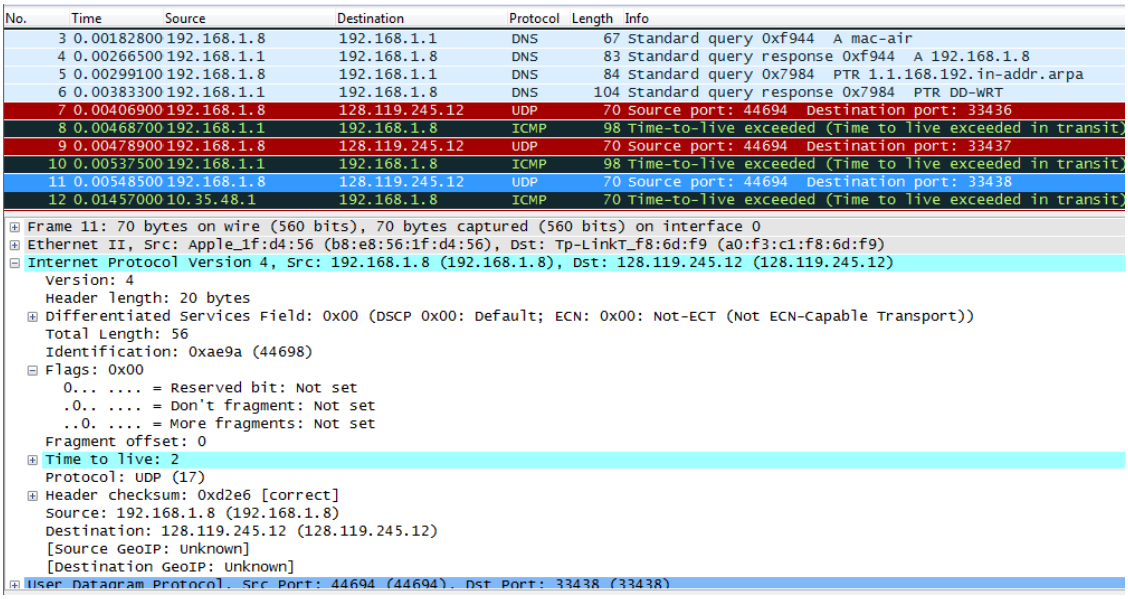
Answer

According to the figure 1, under flags section, the more fragments bit = 0, so the data is not fragmented.

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





According to above two screenshots, identification, Time to live and Header checksum always change.

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:

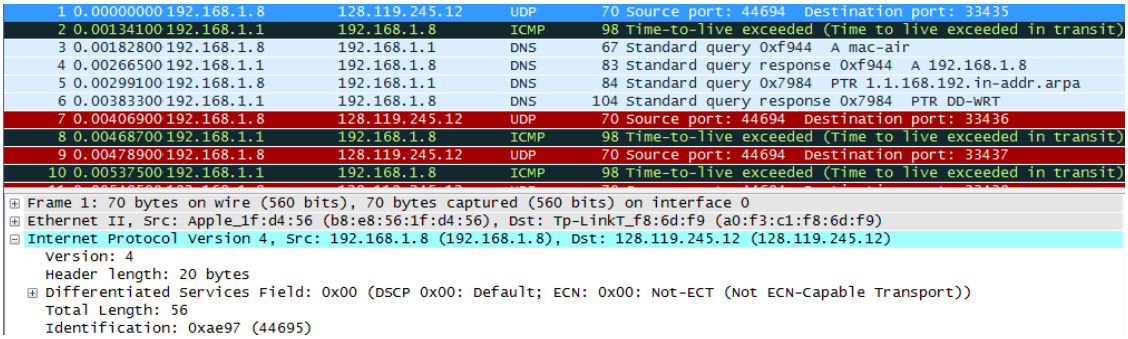
Version (since we are using IPv4), header length (since these are UDP packets), source IP (since all packets are sent from my computer), destination IP (since we are sending to the same host), Differentiated Services (since all packets are UDP), Upper Layer Protocol (since these are UDP packets)

The fields that must change are:

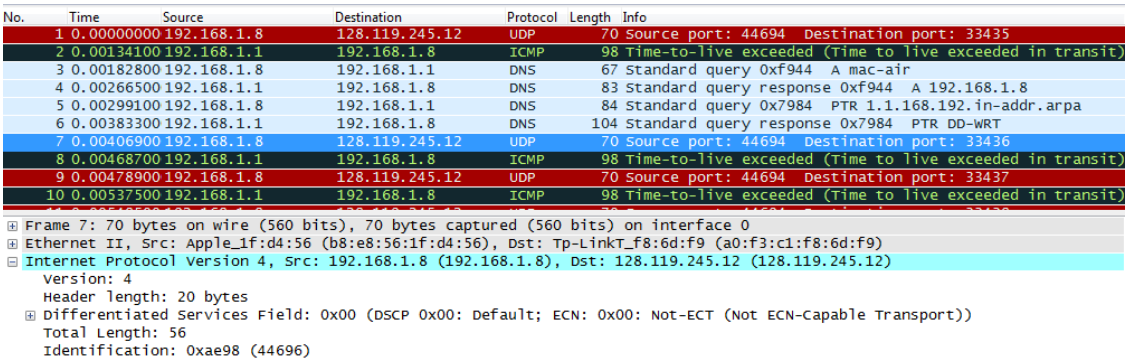
Identification (IP packets have different ids), Time to live (traceroute increments each packet), Header checksum (since header changes)

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

Answer



The first request, values in the identification: 44695

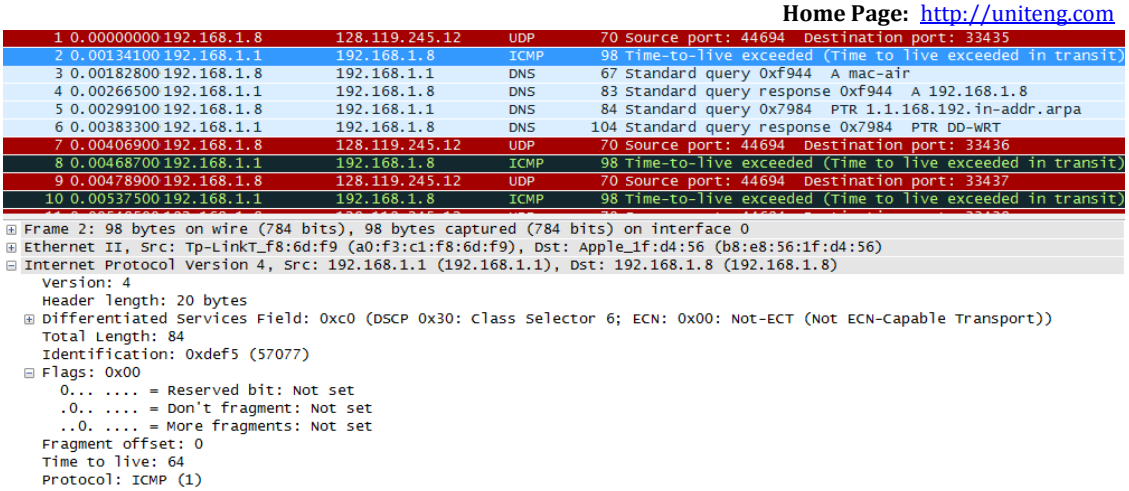


The second request, values in the identification: 44696

According to above two screenshots, the pattern is the IP header Identification field increment with each UDP request.

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

Answer



According to above screenshot, Identification: 57077, TTL: 64

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?

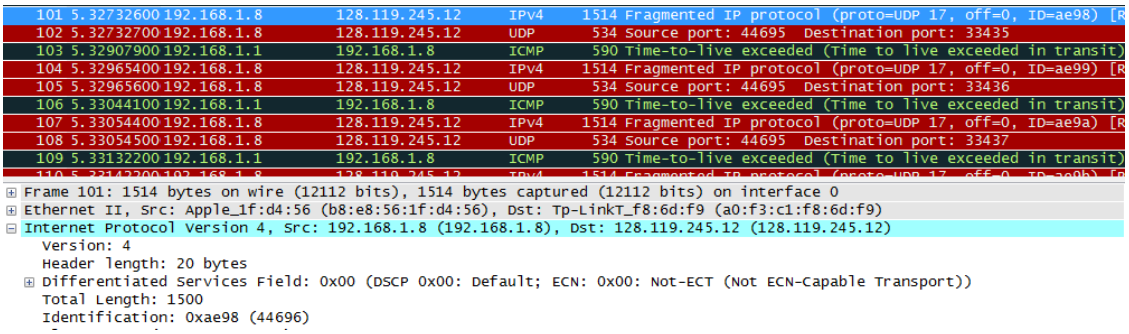
Answer

The values of identification field changes for all the ICMP TTL-exceeded replies since the identification field is a unique value. If two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

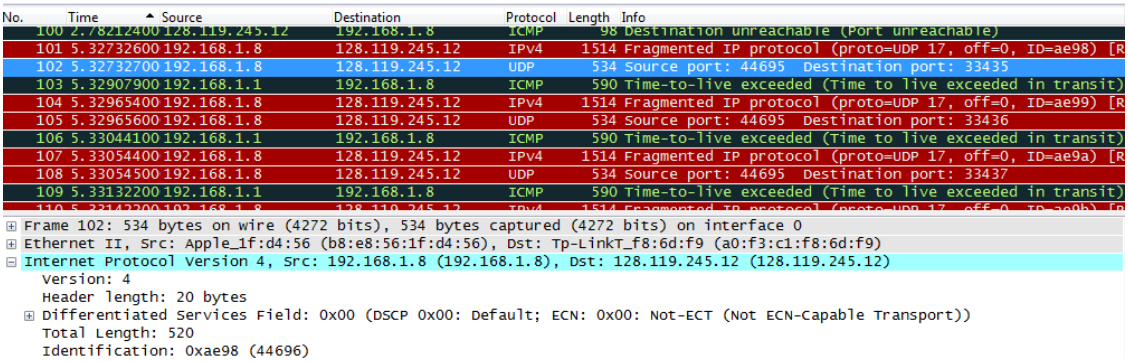
The TTL field was unchanged since the TTL for the nearest router is always the same (Linux, TTL 64).

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



No. 101 has identification: 44696

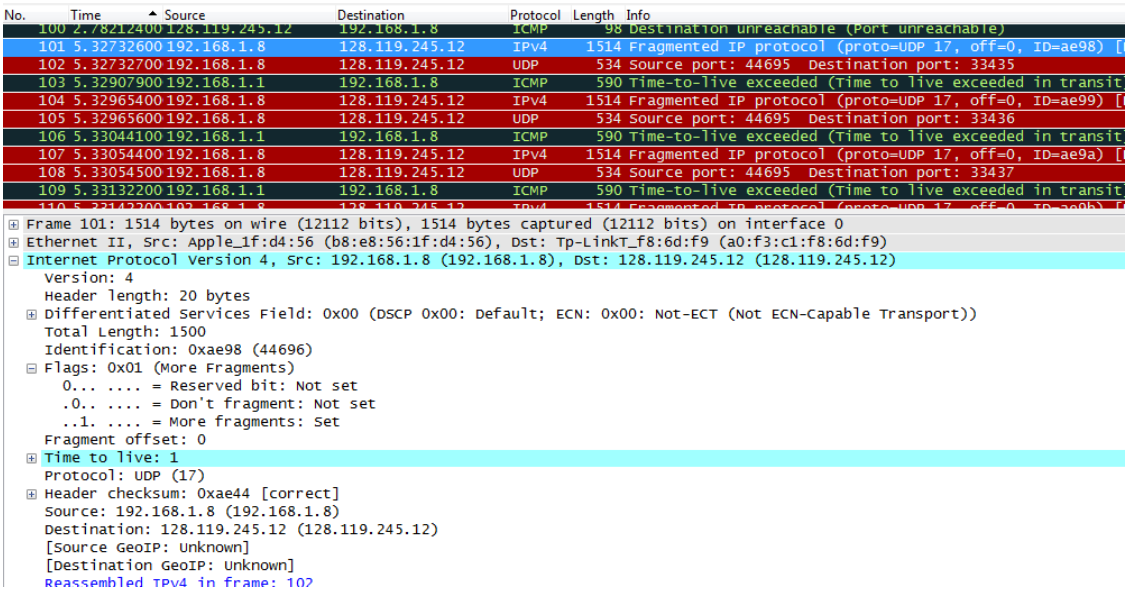


No. 102 has identification: 44696

According to above to screenshots, above 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?

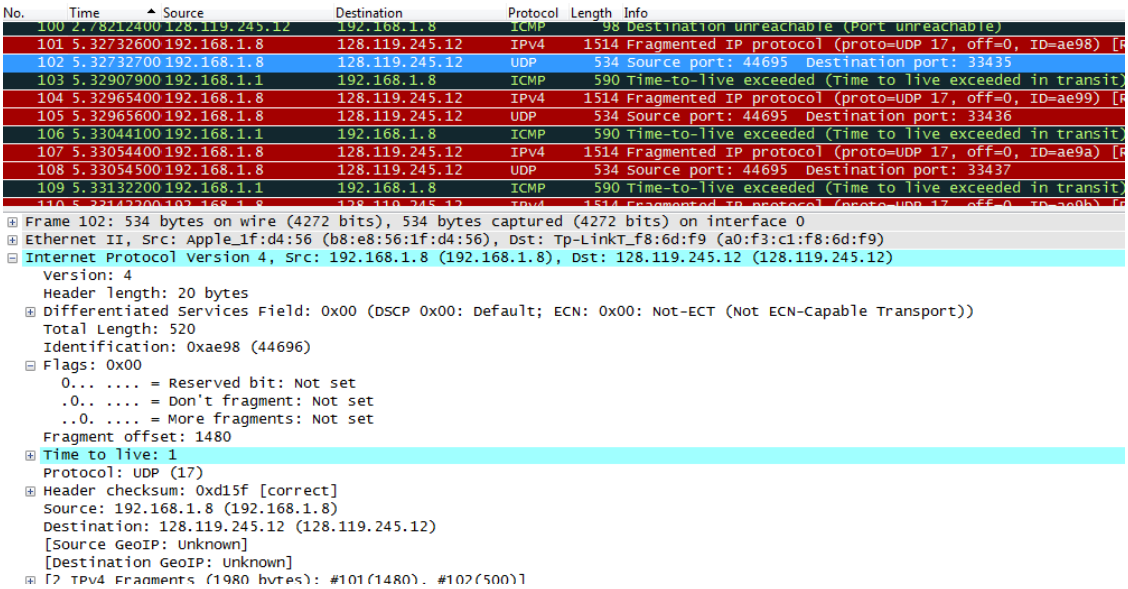
Answer



According to above screenshot, The Flags bit for more fragments is set which means the datagram has been fragmented. The fragment offset is 0, we know this is the first fragment. The length of this first datagram is 1500 including the header.

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.

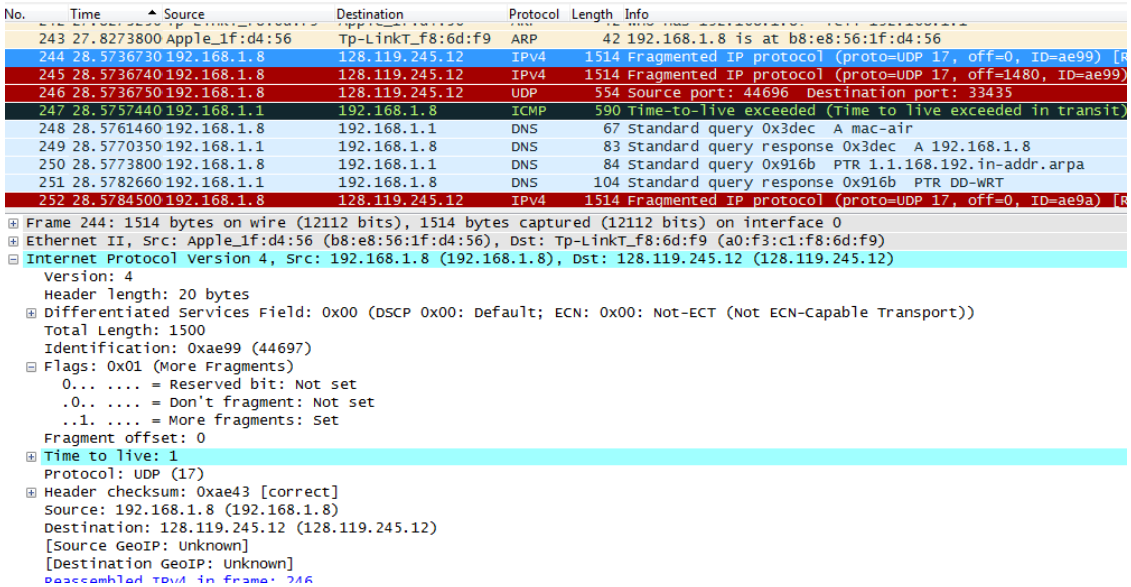
13. What fields change in the IP header between the first and second fragment?

Answer

Total length, flags, fragment offset, and checksum.

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

Answer



According to above screenshot, 3 packets created from the original datagram.

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

Answer

Fragment offset, checksum. Moreover, for the first two packets, the total length is 1500 with the more fragments flag set to 1, and the third packet's total length is 540 with the more fragments flag set to 0.