CS4392/5376: Computer Networks/Communication Networks

Summer II 2021

Homework #4

• Full name only: \_\_\_\_\_\_\_\_\_Chen Zhang\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

• Release date: July 28th, 2021 (Wednesday)

• Due date: August 3rd, 2021 (Tuesday) before midnight, 11:59 PM

• It should be done INDIVIDUALLY; Show ALL your work – include a screen copy to support your

answer; Write your answer in a Word file and submit it through the Blackboard; You can screen

capture for print.

• Total: 15 pts

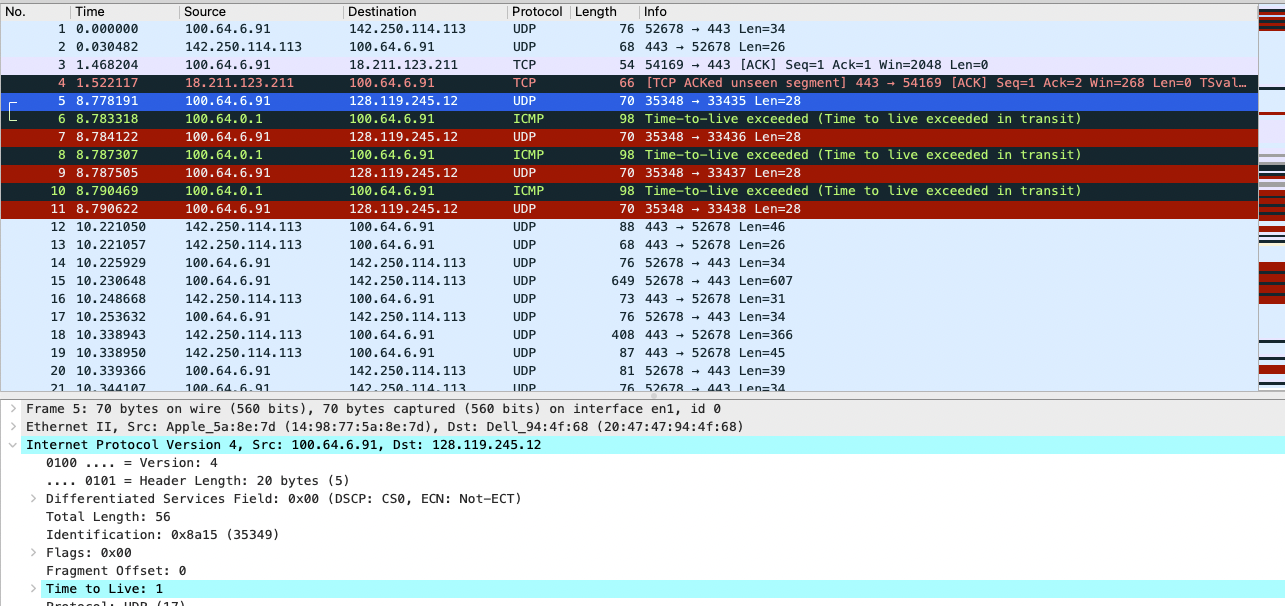
1. Read “Wireshark Lab: IP” and answer all 15 questions.

[15 pts]

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:



Based on the screenshot, my IP is 100.64.6.91

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

Answer:

The value in the upper layer protocol field is UDP.

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:

Based on the previous screenshot, the header length is 20 bytes and the total length is 56, therefore the payload should be 36 bytes.

4. Has this IP datagram been fragmented? Explain how you determined whether or

not the datagram has been fragmented.

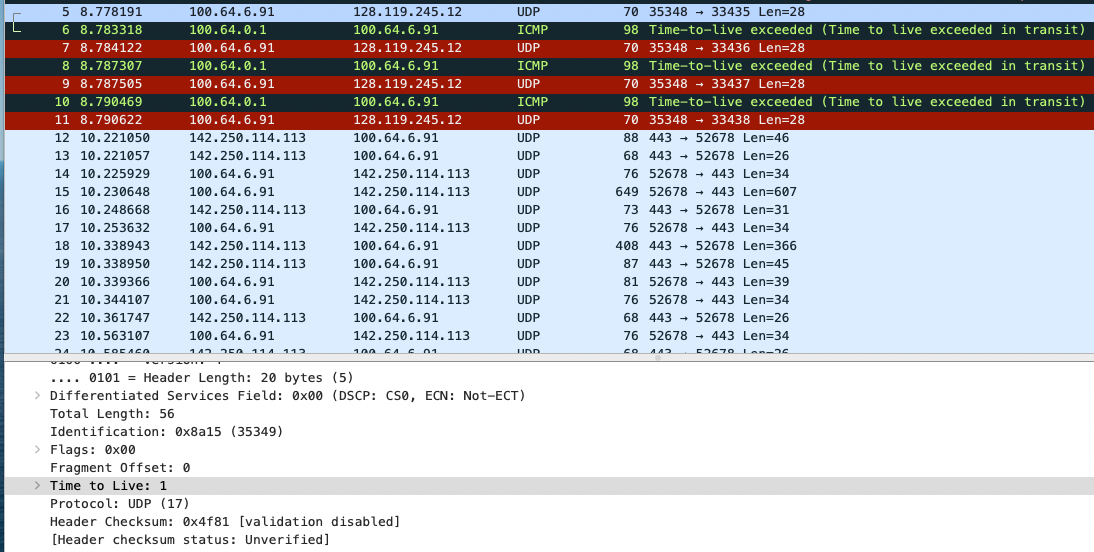
Answer:

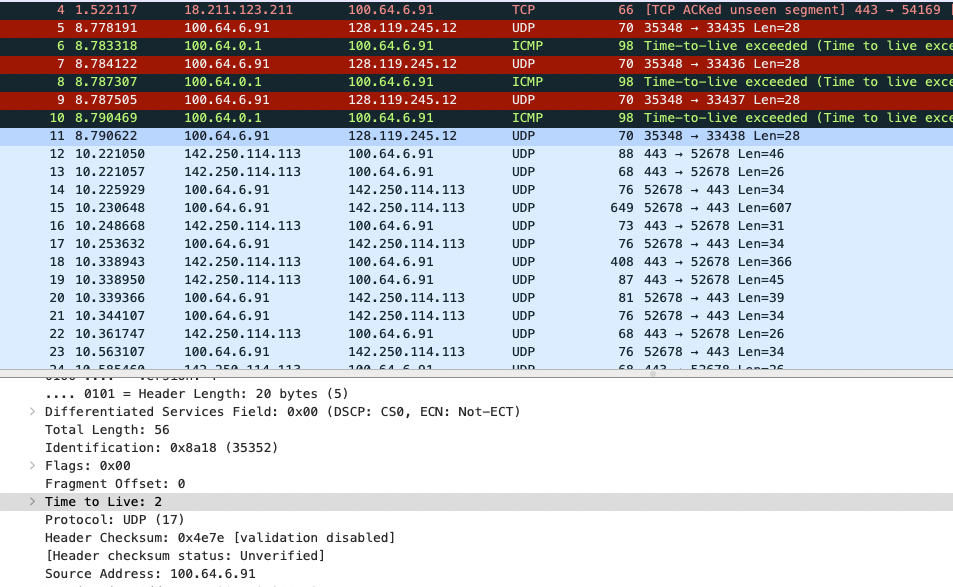
Not fragmented because the flag is 0.

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:





From those two screenshots, the TTL and Header checksum keep changing.

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

must change? Why?

Answer:

Version,header length,source IP,destination IP,Differentiated Services,Upper Layer Protocol are constant, because all the test data is sent from my computer to the same destination and based on IPv4, all the packets are UDP.

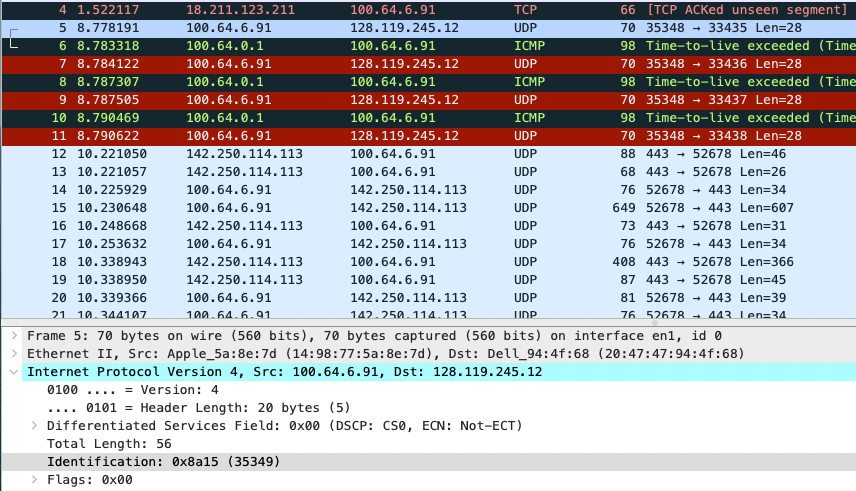
The must stay constant fields are the same with the previous fields.

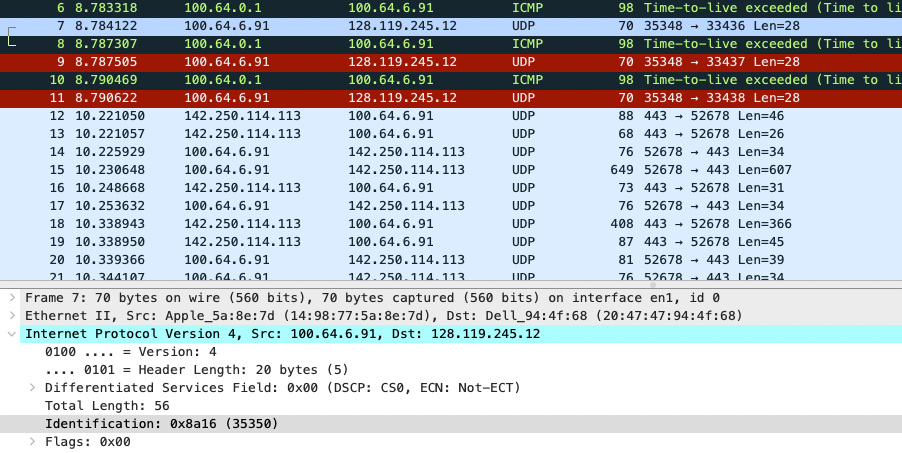
The fields that must change are Identification, TTL, and Header checksum. Because packets have different id's and the header changes all the time.

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

datagram

Answer:

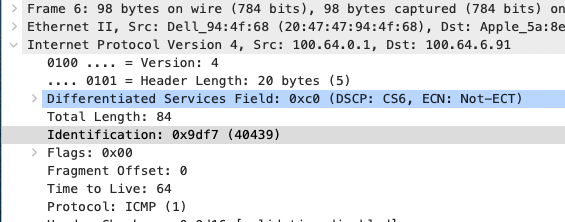




The identification field increased by 1 for each UDP request. From 35349 to 35350.

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

Answer:



The Identification is 40439 and the TTL is 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 identification field changes because it’s a unique value but the TTL stays 64 since the router is the same one.

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

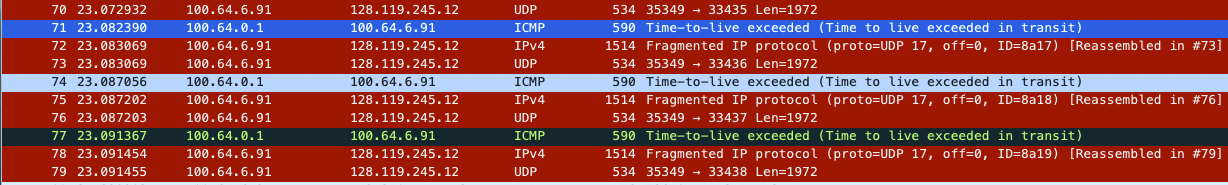
not been fragmented, you should download the zip file

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 is the first ICMP Echo because there are fragmented packets followed.

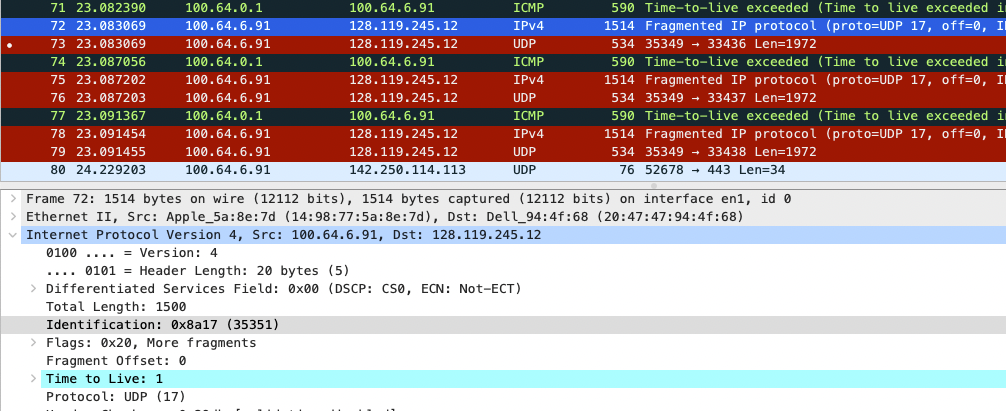
11. Print out the first fragment of the fragmented IP datagram. What information in

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:



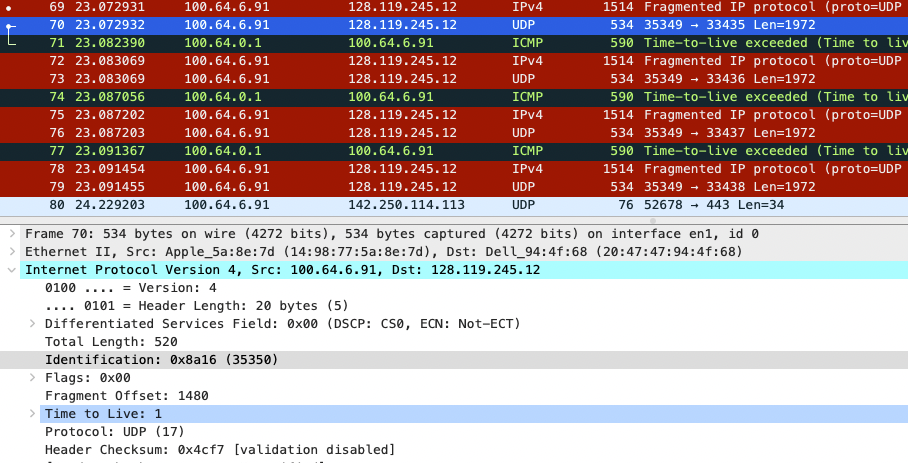
This screenshot shows that the flags bit set to 0x20 due to the datagram has been fragmented. The length of this datagram is 1500 (header included).

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:



Based on the screenshot, the fragment offset is 1480 and there are no more fragments because the fragment flag is not set.

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

Answer:

Total length,fragment offset,flags and checksum.

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

Answer:

There are three packets created.

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

Answer:

Fragment offset, checksum, and the total length are changed.