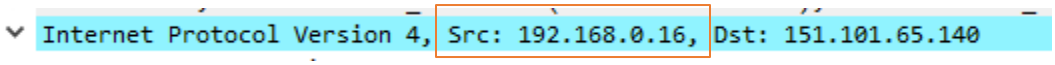
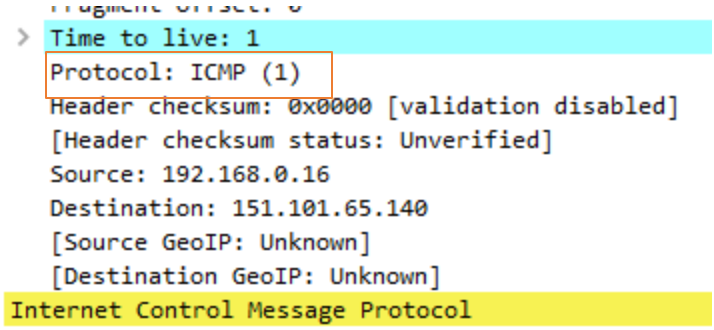
Erin Alltop
CS372 – Spring 2018
Lab 4

1. What is the IP address of your computer?



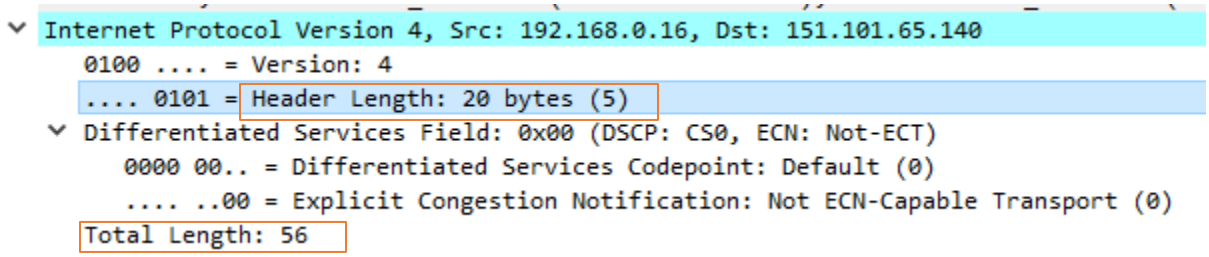
My computer's IP address is 192.168.0.16.

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



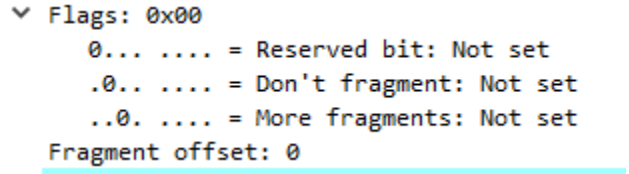
The value in the upper layer protocol field is ICMP (1).

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.



There are 20 bytes in the IP header and 56 total length. Total length minus the bytes in the header equals the payload of the IP datagram which is 36.

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



No, the IP datagram has not been fragmented. You can see this because the "More fragments" flag has not been set.

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

The fields in the IP datagram that always change from one datagram to the next within the series of ICMP messages sent by your computer are Identification, Time-to-live and Header checksum.

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

The fields that stay constant are –

a. Version (we are using IPv4 for all packets)
b. Header Length (because these are ICMP packets)
c. source IP (the source stays the same)
d. destination IP (the destination stays the same)
e. Differentiated Services (all packets have the same Type of Service class)
f. Upper Layer Protocol (because these are ICMP packets)

All of the fields above must stay constant for the stated reasons above.

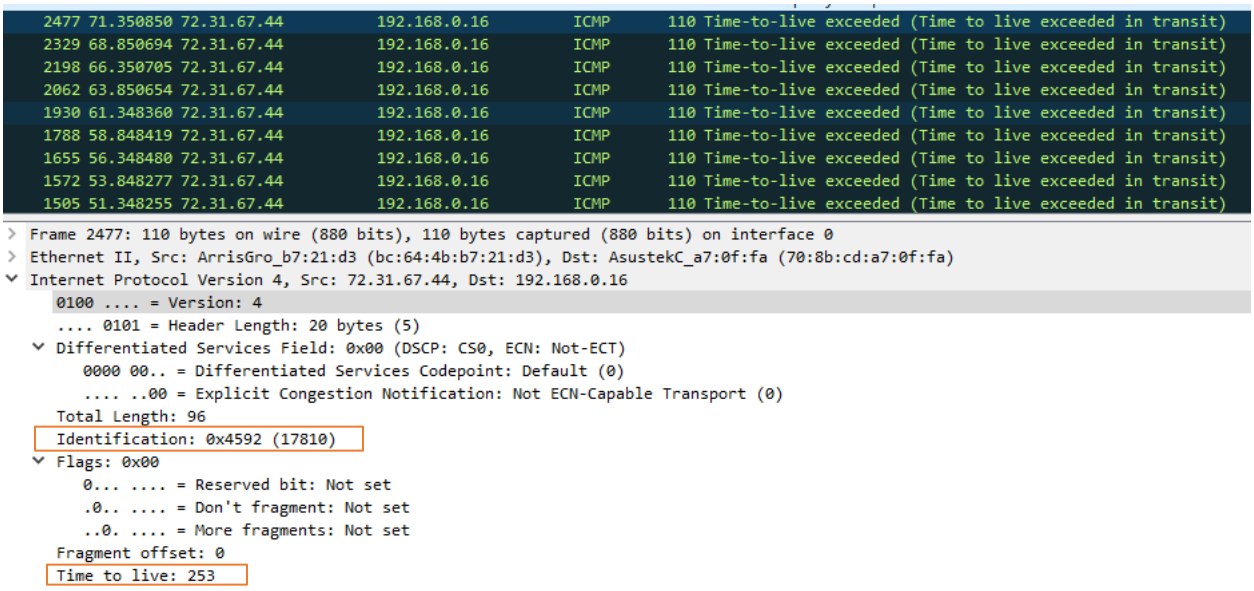
The fields that must change are –

a. Time-to-live (the changes based on traceroute and what packet we are one)
b. Identification (must change depending on what packet we are on)
c. Header checksum (changes with the header)

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

The pattern in the values in the Identification field of the UP datagram is that the fields increment with each ICMP Echo request.

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



The value in the Identification field is 17810 and is it 253 in the TTL field.

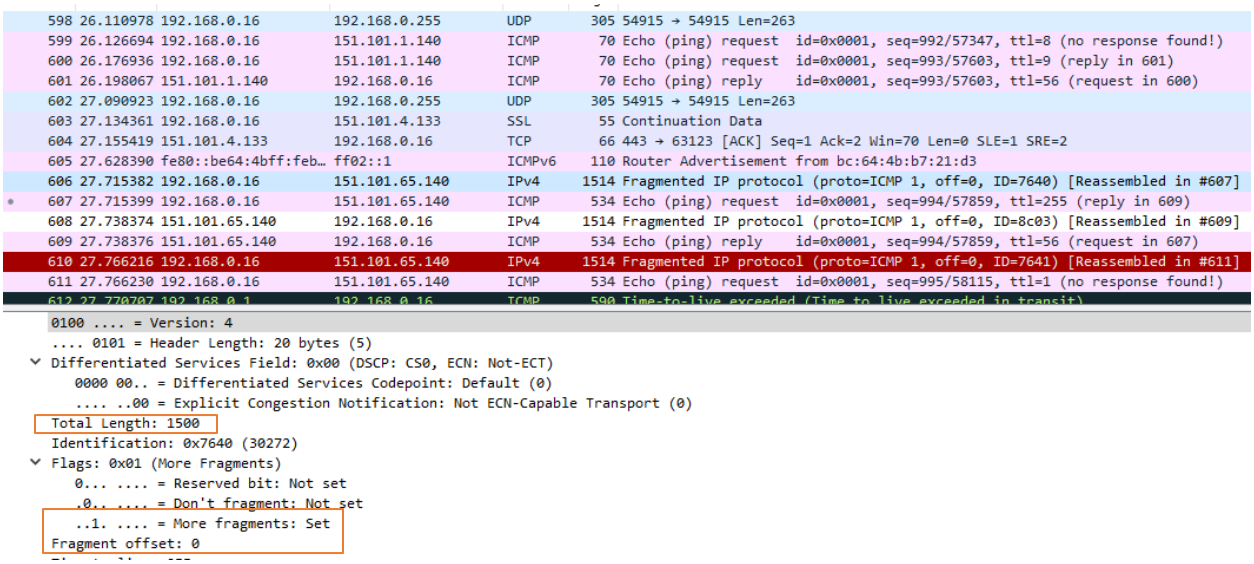
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

No – because each datagram has a unique Identification field, any new datagram will have a changed Identification field. If the field hasn't changed then we know that the datagram is apart of the same IP datagram, broken into parts.

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?

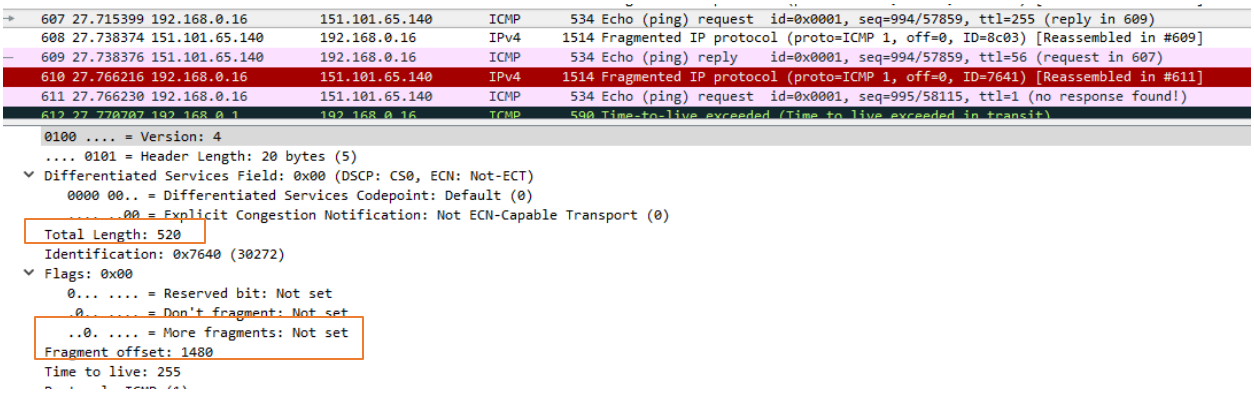
Yes, after changing the Packet Size in pingplotter to be 2000, the message has been fragmented across more than one IP datagram.

11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram has 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?



We know that the datagram has been fragmented because the "More fragment" flag has been set to 1. We can also tell that this is the first fragment because the Fragment offset is 0. The datagram has a Total Length of 1500 (including the header).

12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

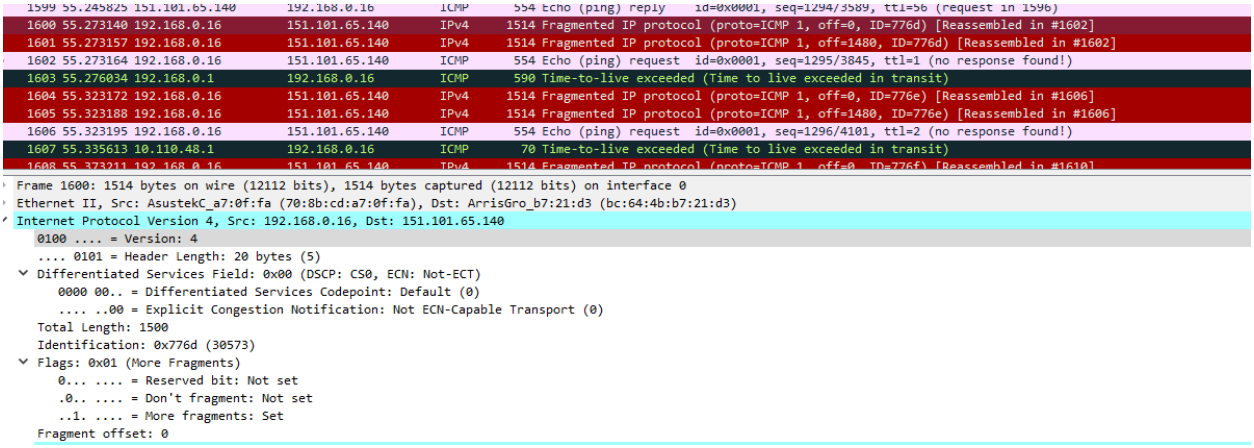


You can tell that this is not the first datagram fragment because the Fragment offset is not 0 (it is 1480). You can also tell that there are not any more fragments because the “More fragments” flag is set to 0.

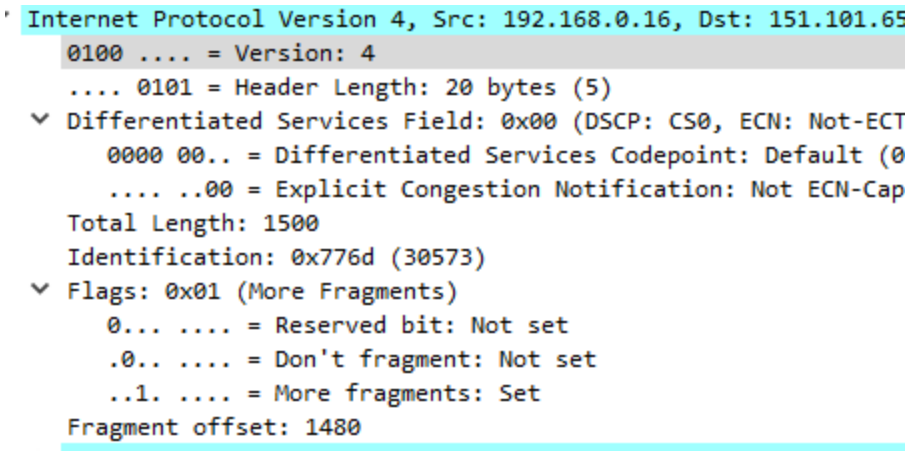
13. What fields change in the IP header between the first and second fragment?

The fields that changed in the IP header between the first and second fragments are the total length flags, fragment offset, checksum, and the flags. Everything else remained the same.

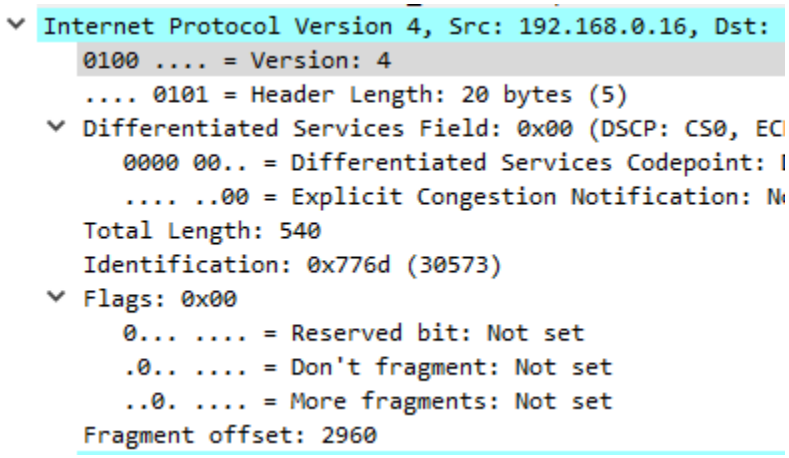
14. How many fragments were created from the original datagram?



First fragment after changing Packet Size in pingplotter to be 3500.



Second Fragment.



Third Fragment.

There were three fragments created from the original datagram. You can see this because the first datagram has a total length of 1500 with “More fragments” set to 1 and a Fragment offset of 0.

The second packet has a total length of 1500 with “More fragments” set to 1 and a Fragment offset of 1480.

And the third packet has a total length of 540 with “More fragments” set to 0 and a Fragment offset of 2960.

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

The Total Length stays the same for packets one and two, but change for packet three. The Fragment Offset changes for all three packets. And the “More fragments” flag stays the same for packets one and two, but change for packet three.