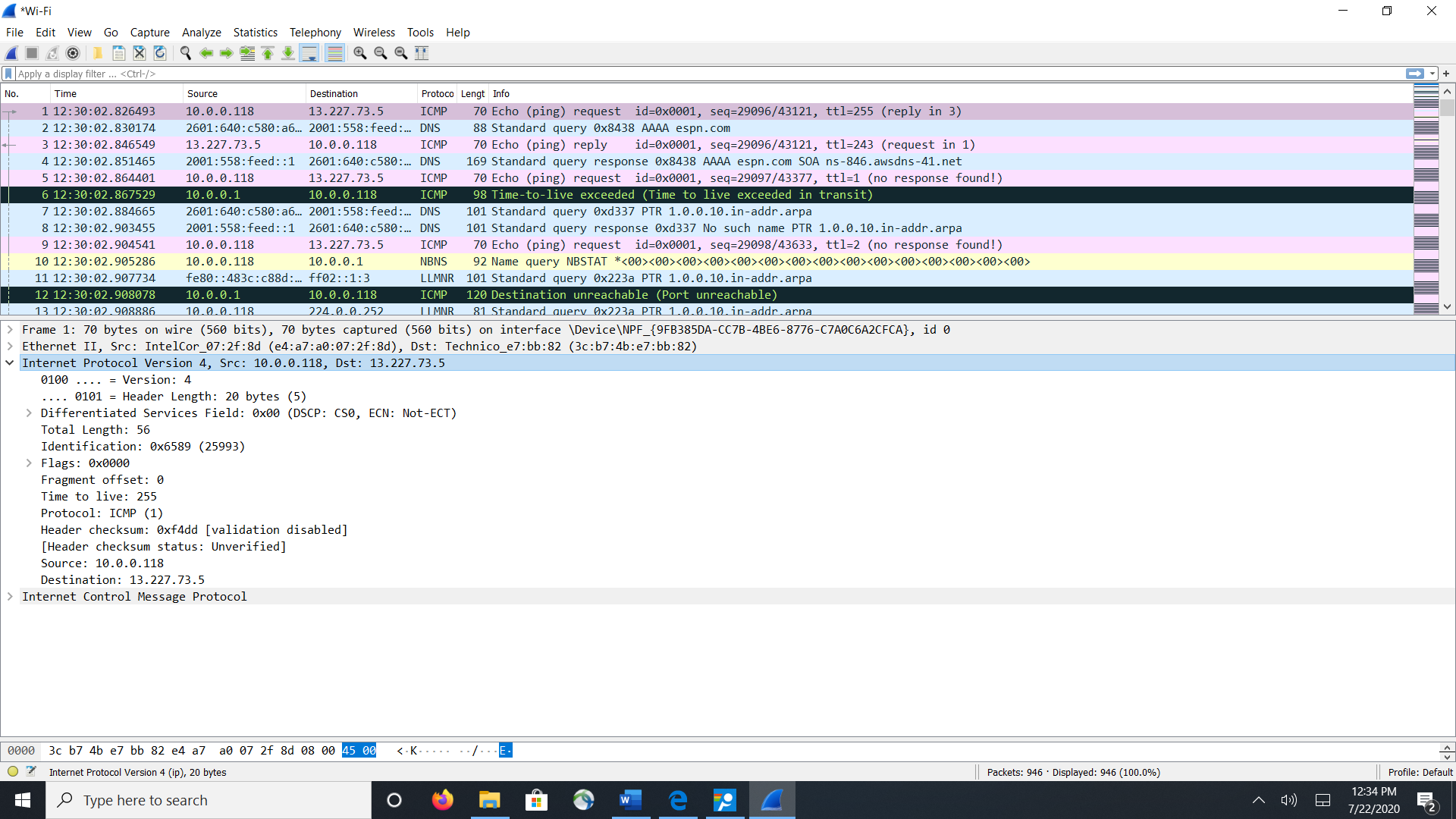
Justin Phillips

cs372 summer2020

Lab4

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?

10.0.0.118 is the IP of my pc



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

Protocol: ICMP (1) ( as seen above)

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.

as shown above in 1 the length of the IP header is (.... 0101 = Header Length: 20 bytes (5))

Total Length: 56 bytes - Header Length: 20 bytes (5) = 36 bytes ( payload) ( as seen above)

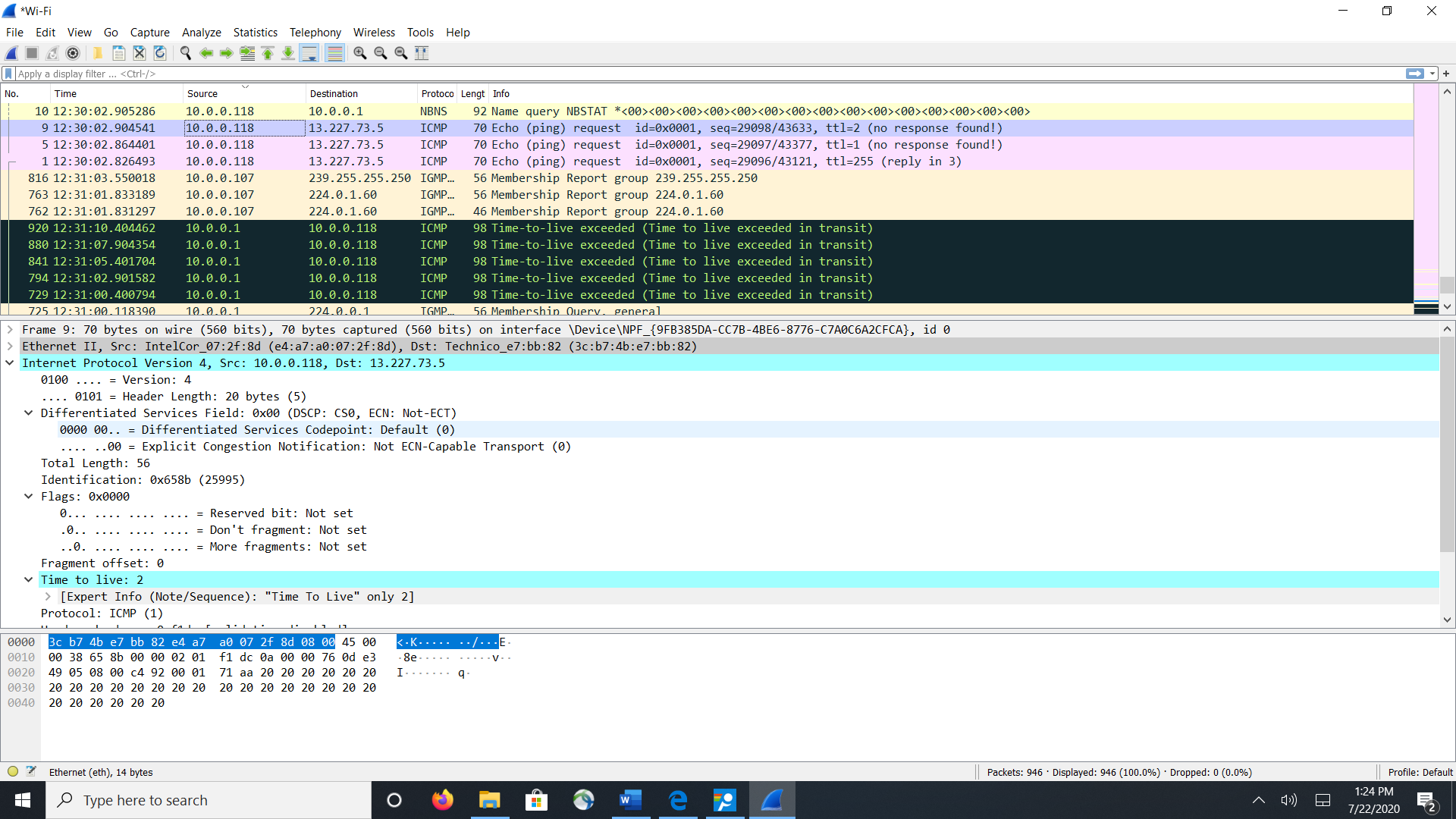
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

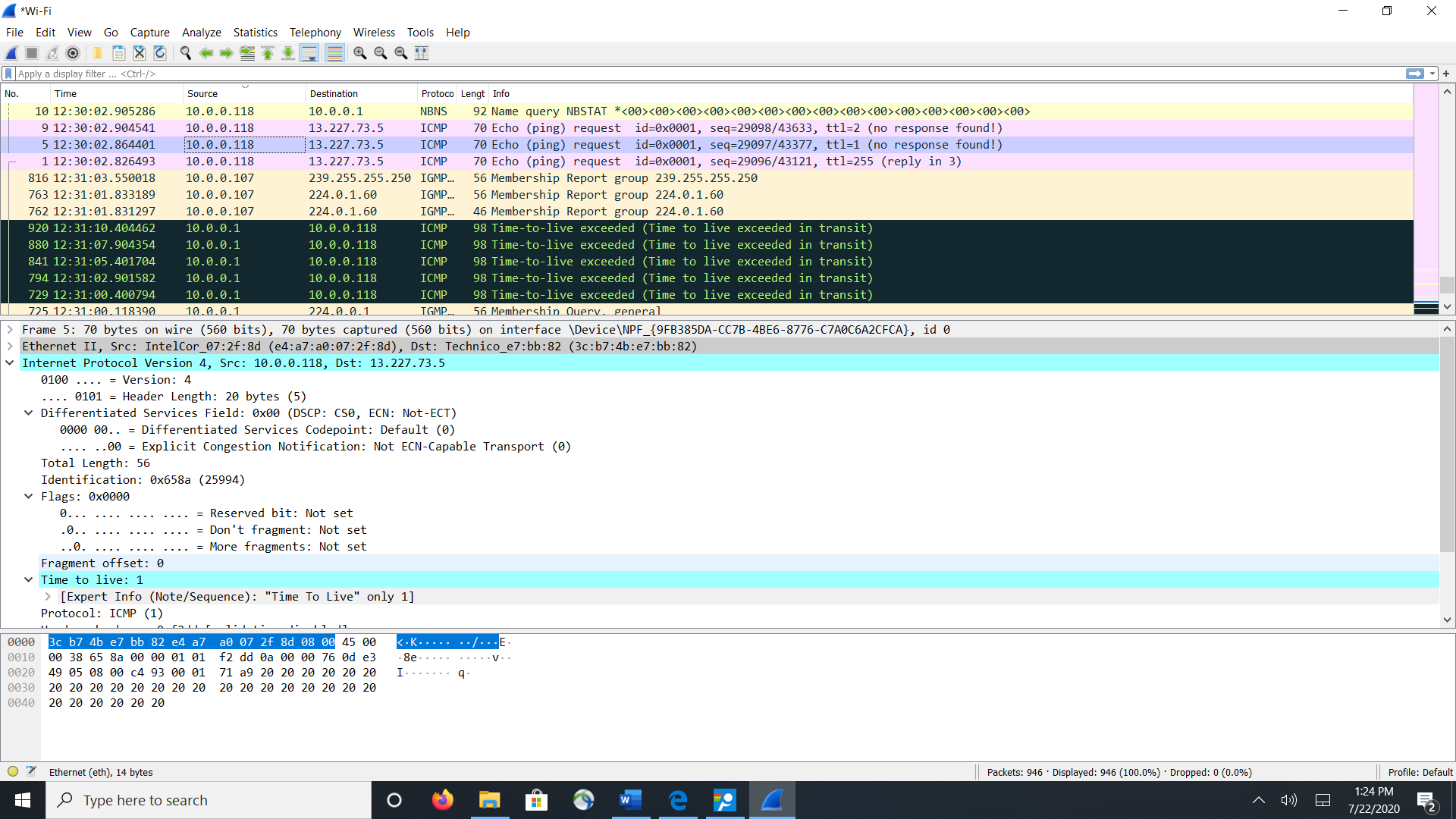
Fragment offset: 0, no it isn’t fragment because the bit is set to zero ( as seen above)

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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?

The Time to Live and Identification changes every packet





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

the header Length, version, total length, Ip source and dst, differentiated services and protocol all remain constant. The fields that must remain constant are the addresses, version, and header length. The fields that must change are the TTL and identification. These must change because in the TTL this is how we trace the route and Identification changes because this is how we track the datagram. ( This is observed in the screen shot above even though it’s a small sample size we can still observe it)

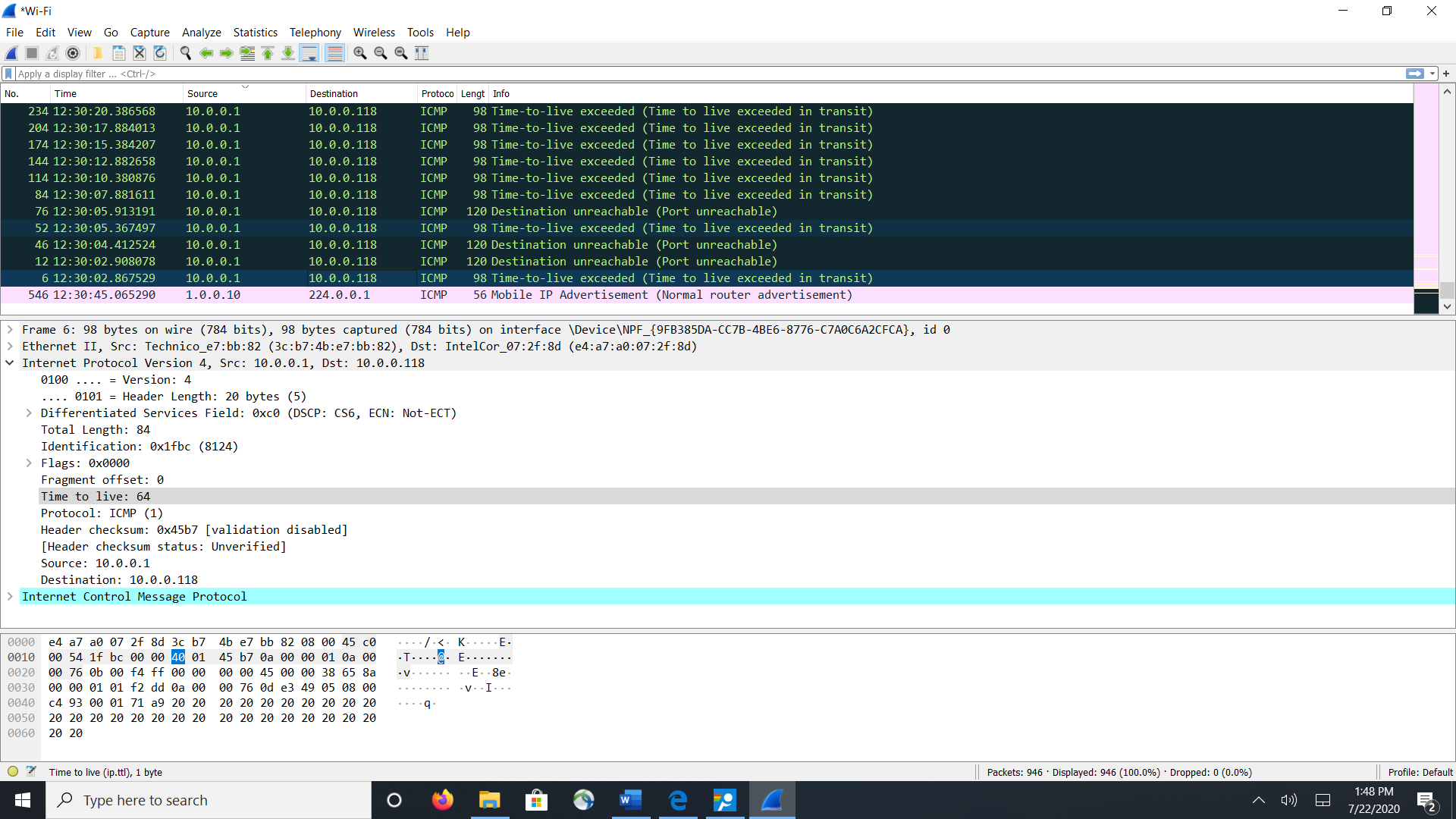
7. Describe the pattern you see in the values in the Identification field of the IP datagram

The next id field gets incremented by 1. ( This is observed in the screen shot above)

Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.

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

Identification: 0x1fbc (8124) Time to live: 64



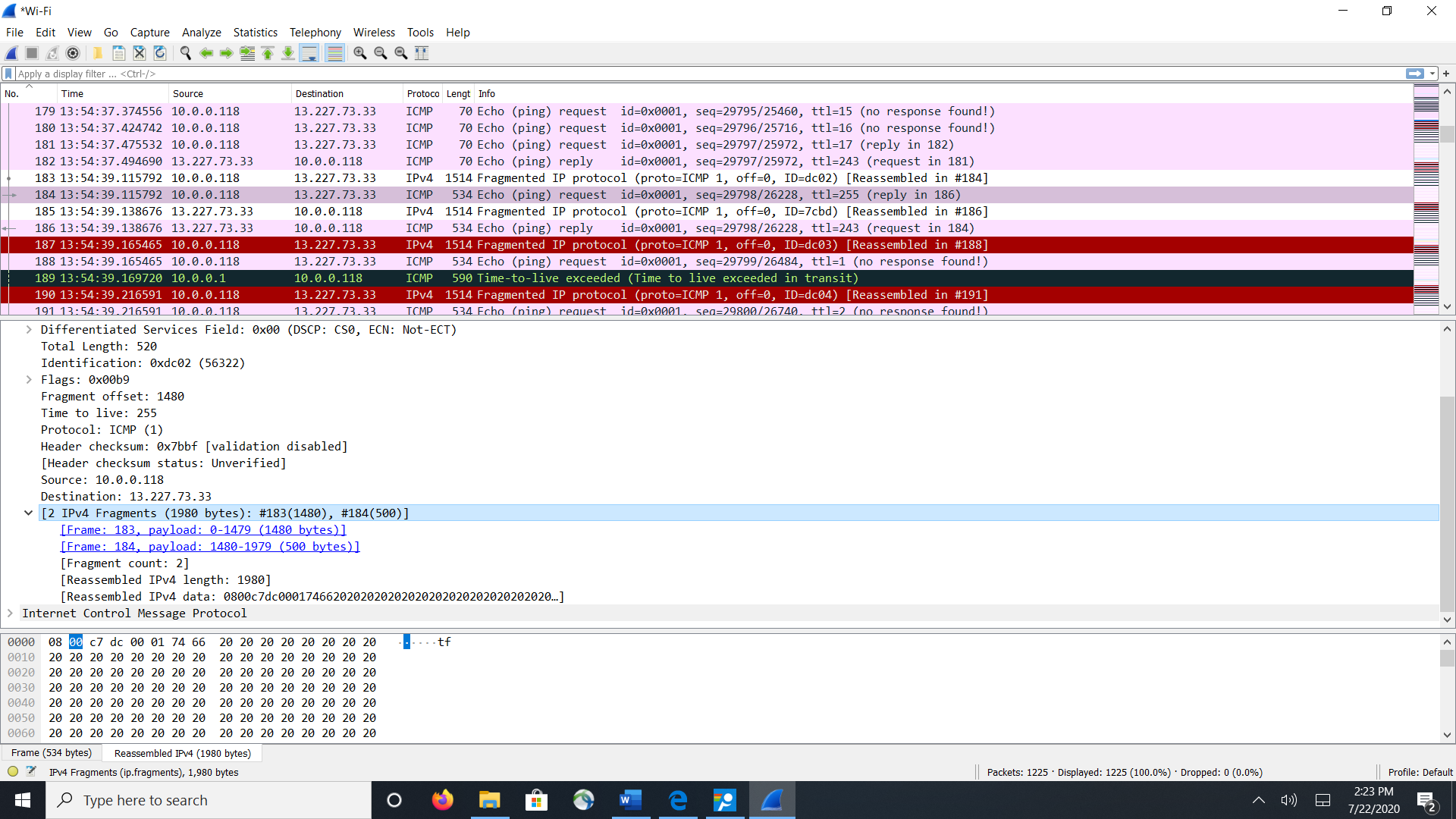
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The TTL remains the same because it hasn’t left this hop yet.

Fragmentation, Sort the packet listing according to time again by clicking on the Time column.

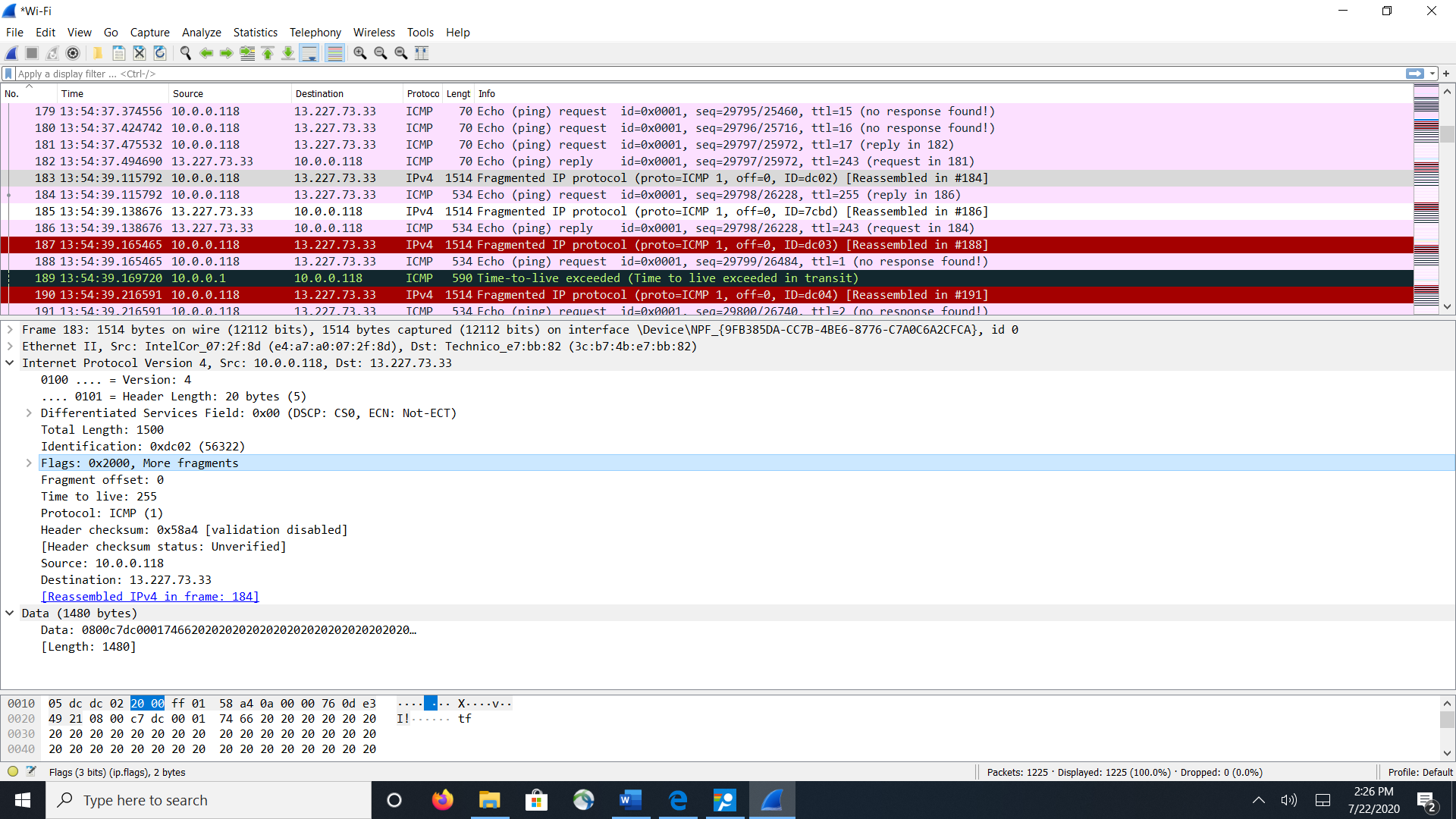
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

The packet has been fragmented across more then one datagram



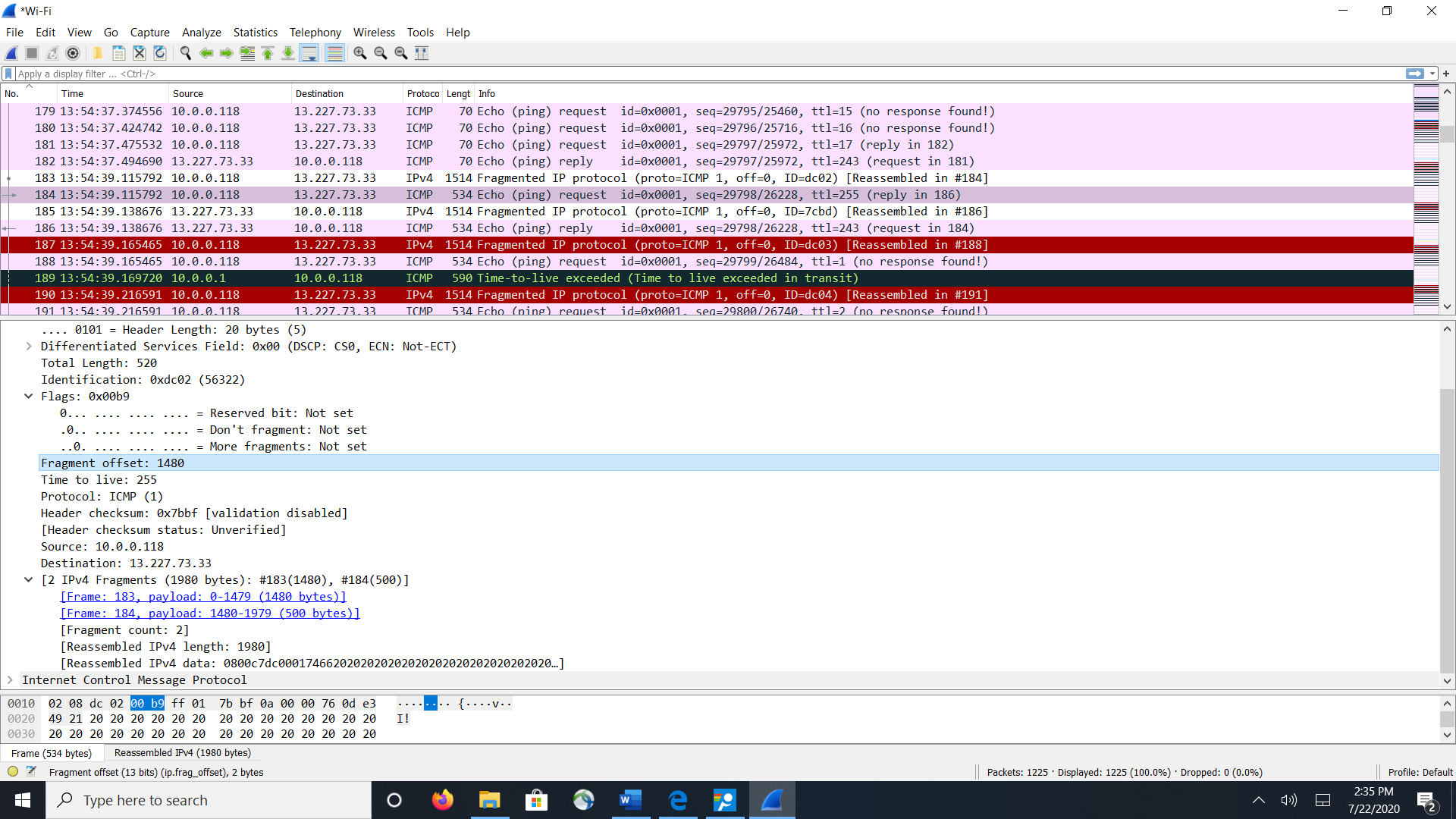
11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

In flags it states that that there’s more fragments, the frag offset is set to zero and the total length of this is 1500 – 20 (header) = 1480bytes of data



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 the more fragments? How can you tell?

The info stating that it isn’t the 1st datagram is the offset is set to 1480 and it also states that there are 2 payloads in the fragment section



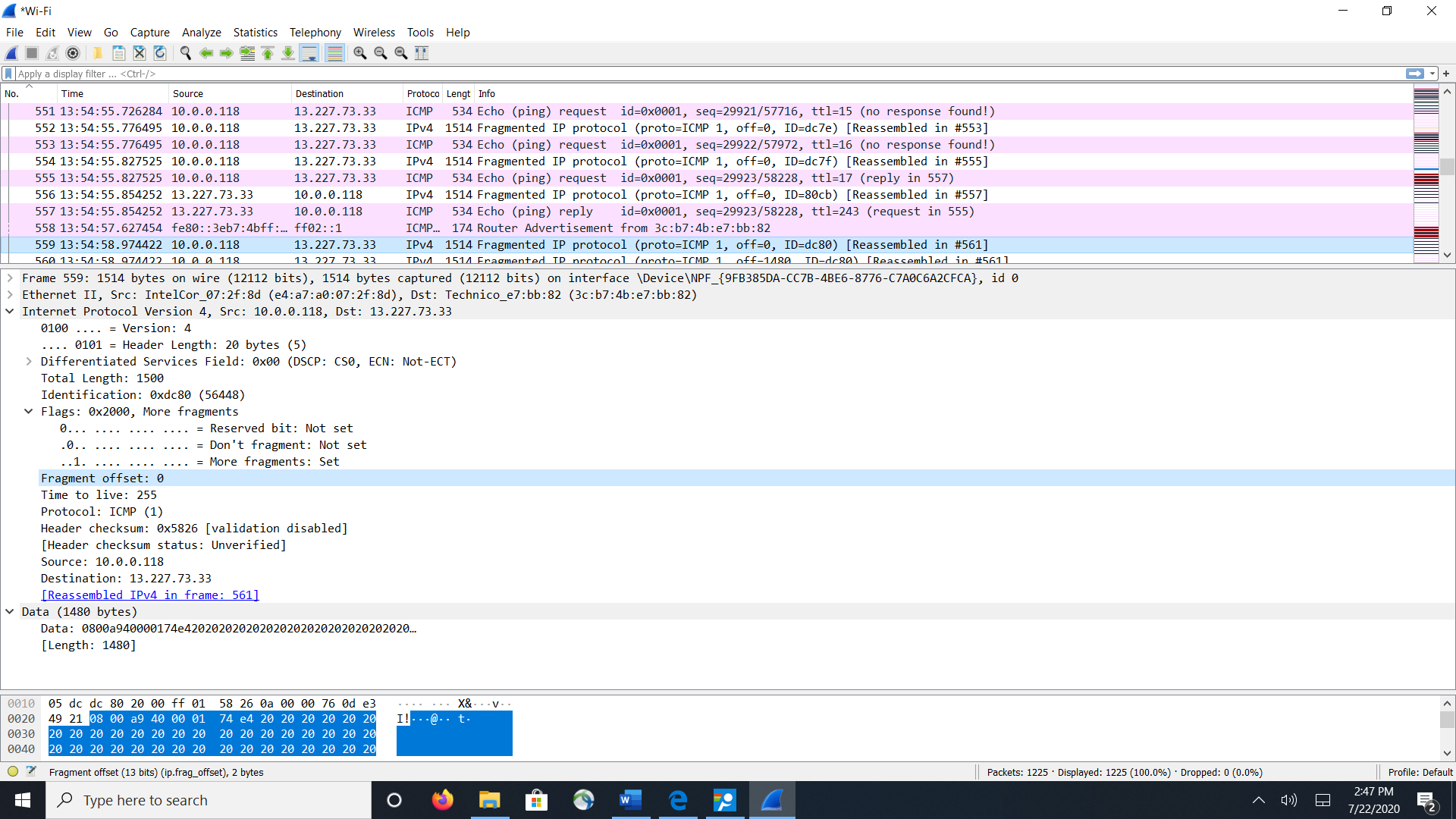
13. What fields change in the IP header between the first and second fragment?

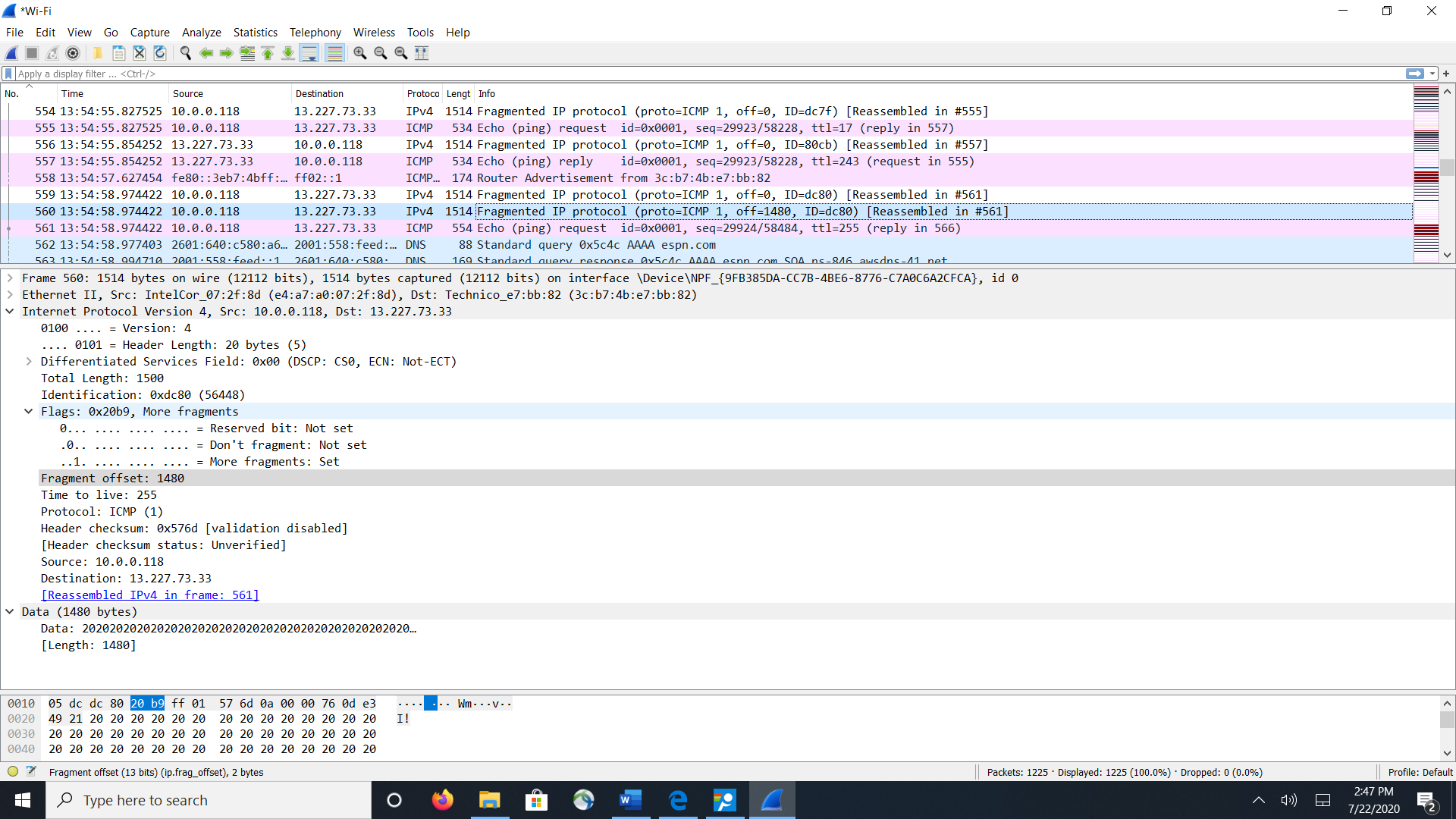
The fragment offset, total length, more fragments bit and flags remained the same between the first and second fragments

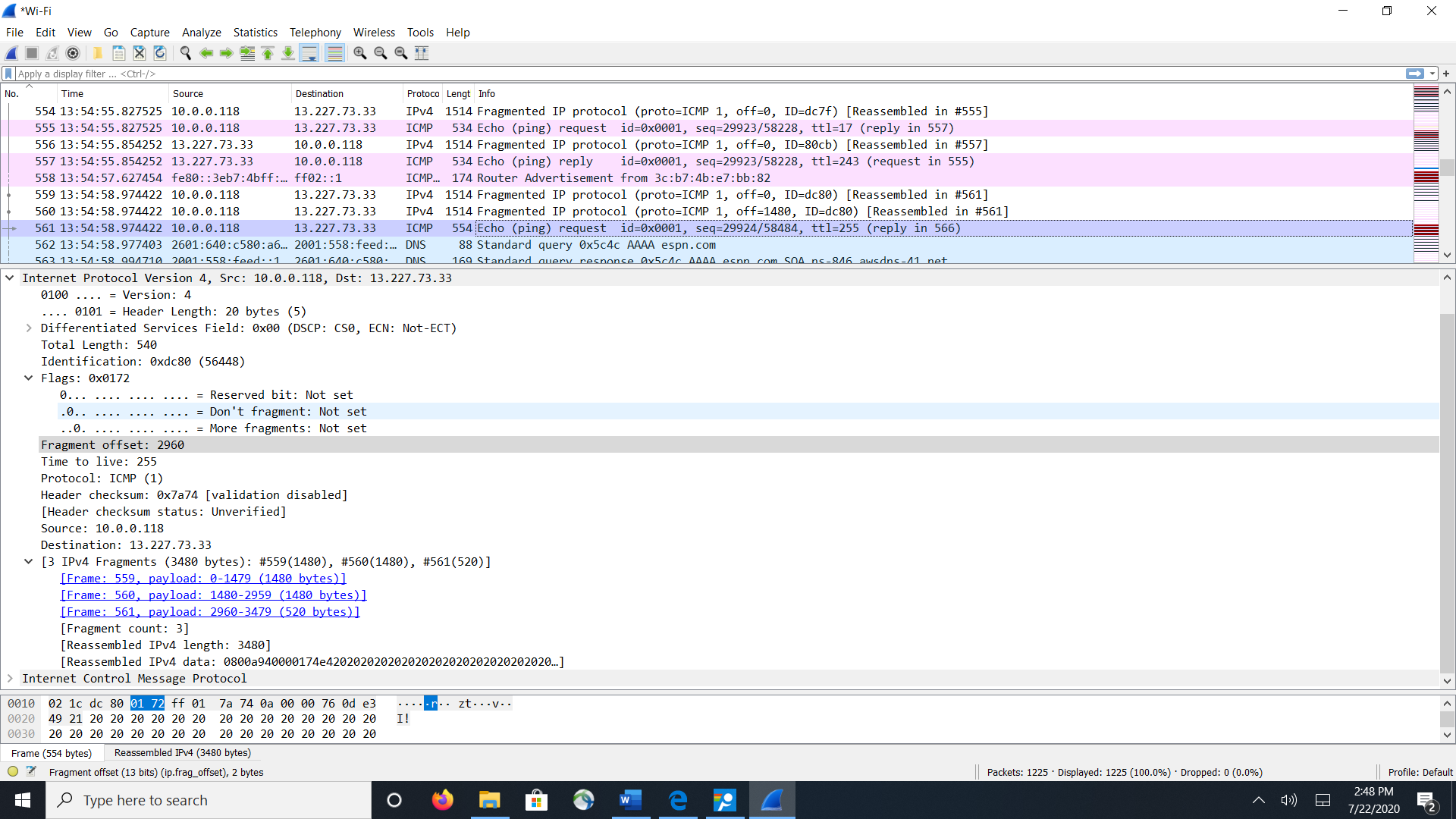
Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

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

As one can see in the last screen shot there was 3 fragments created from the original







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

The fragment offset, total length, more fragments bit and flags are not the same in all 3, some are the same in the 1st and 2nd