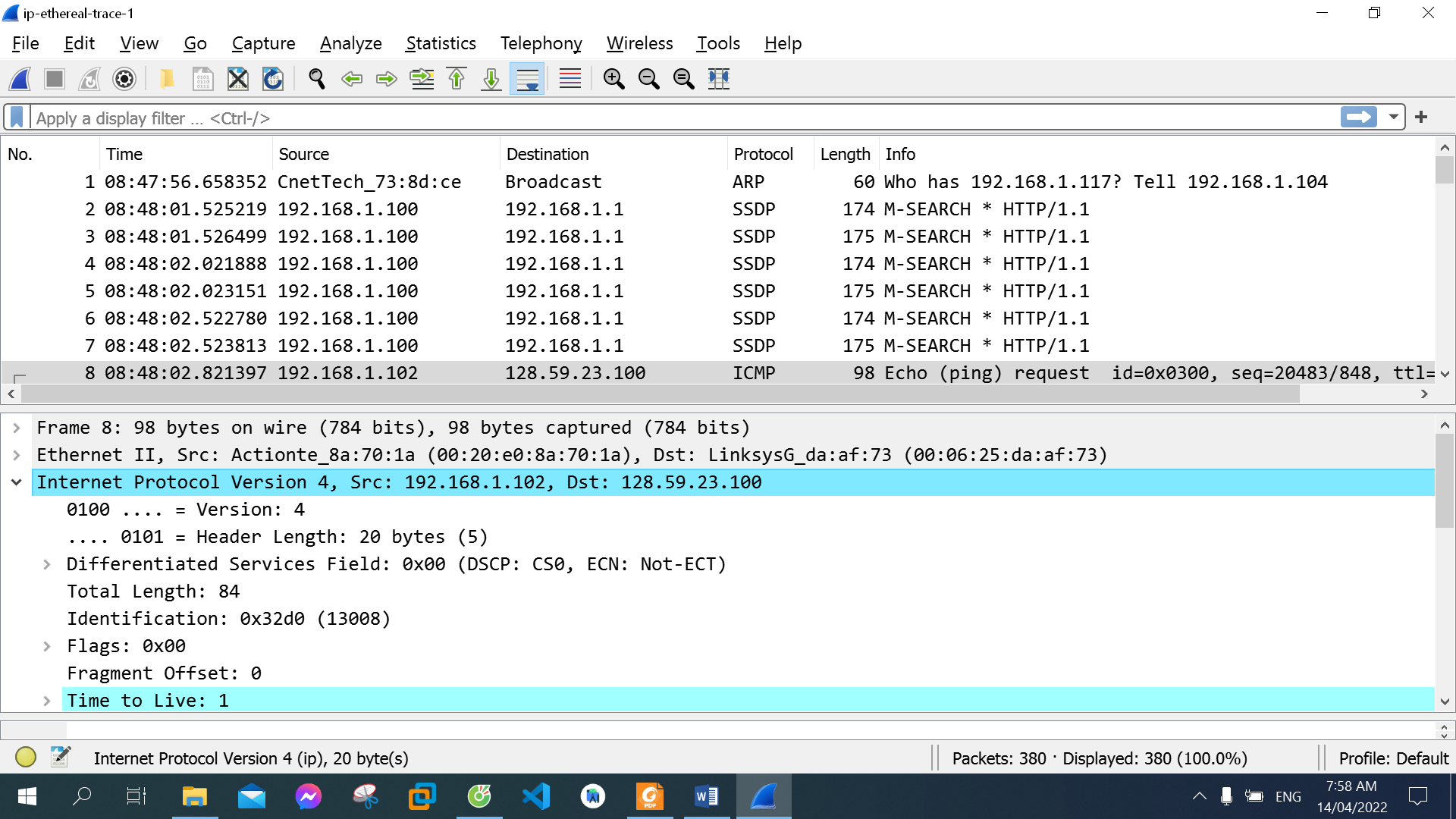
**LAB 4A**

**Wireshark Lab: IP v8.0**

**Name: Hồ Đức Trí**

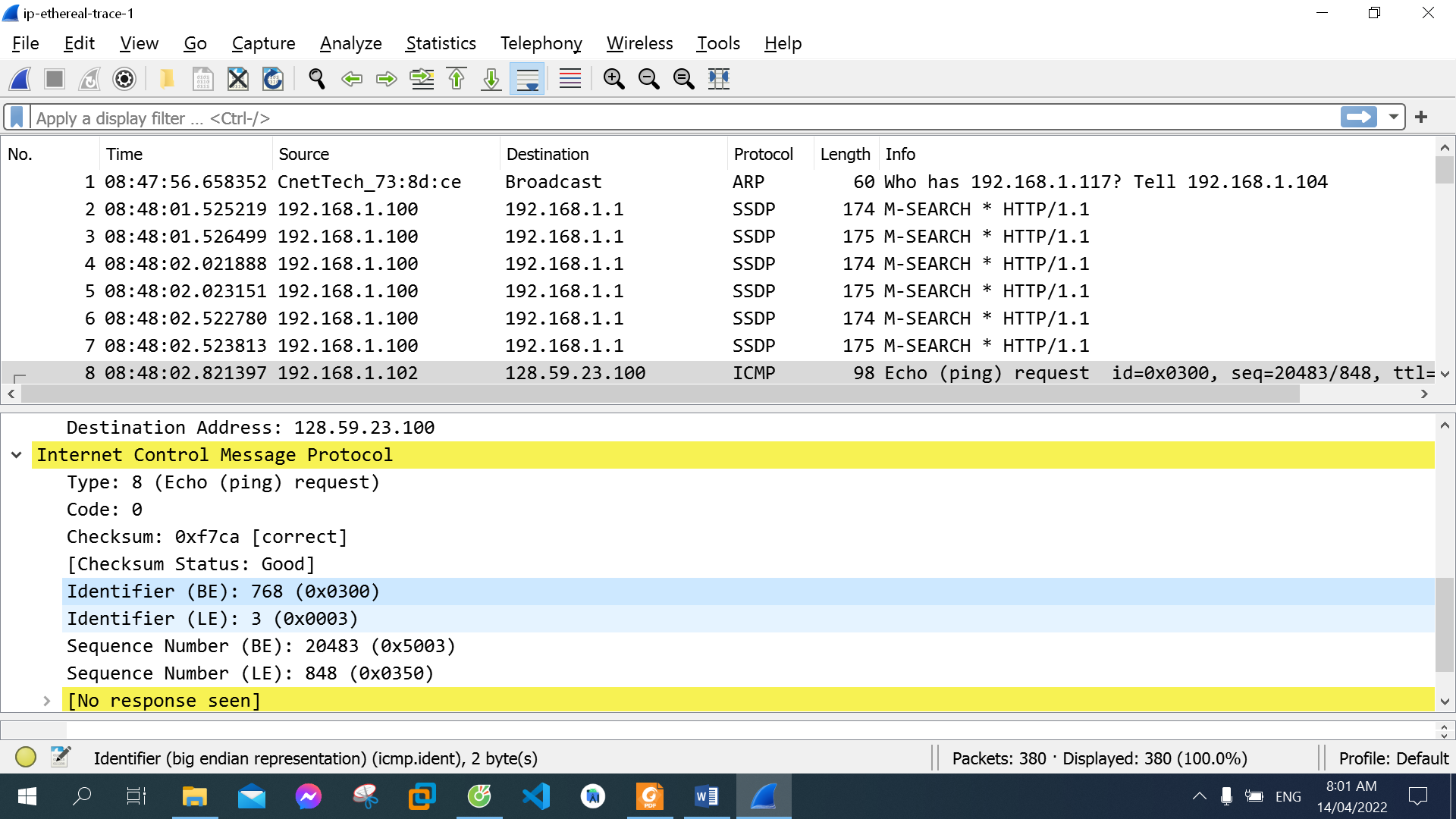
**Student No: 1912288**

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?



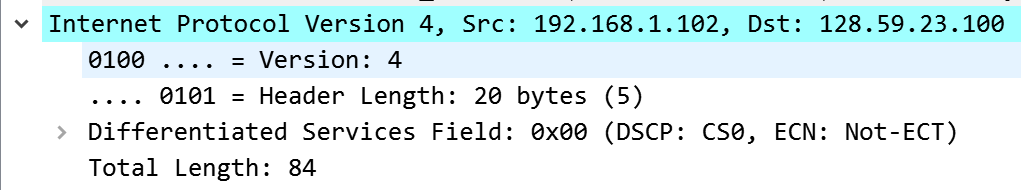
IP address of my computer: 192.168.1.102

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



The value in the upper layer protocol field: 0x03

1. 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.

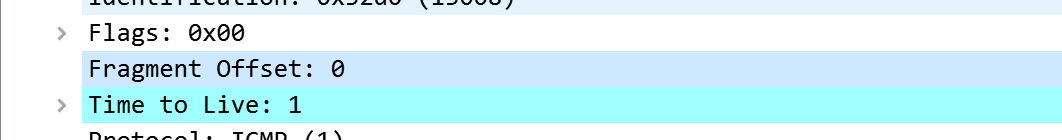


20 bytes in the IP header

64 bytes in the payload

Total length = 84 = header + payload = 20 + 64

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



This IP datagram has not been fragmented. Because the Fragment Offset is 0.

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

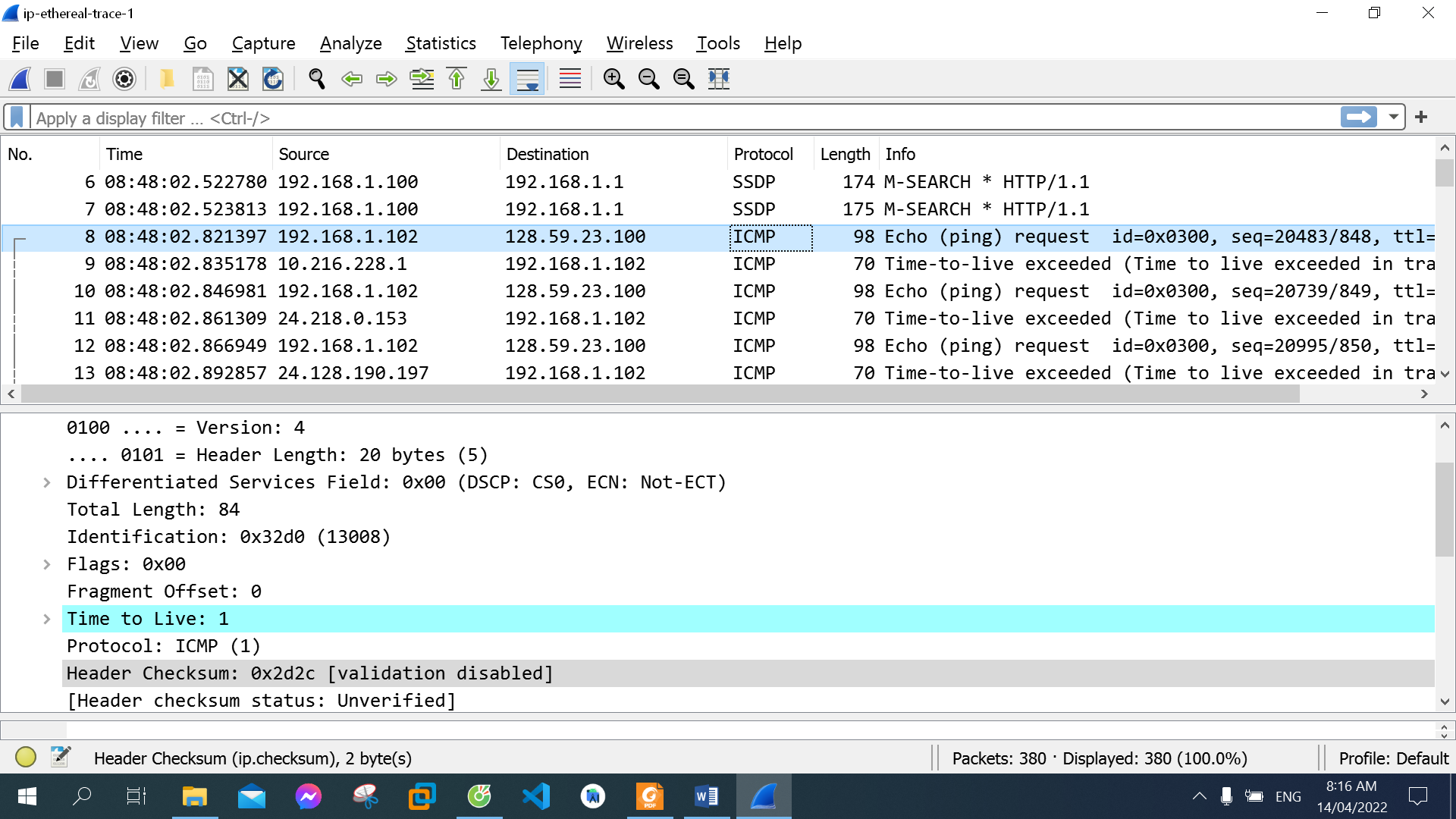
Identification, Header Checksum, Time to live always change from one datagram to the next within this series of ICMP messages

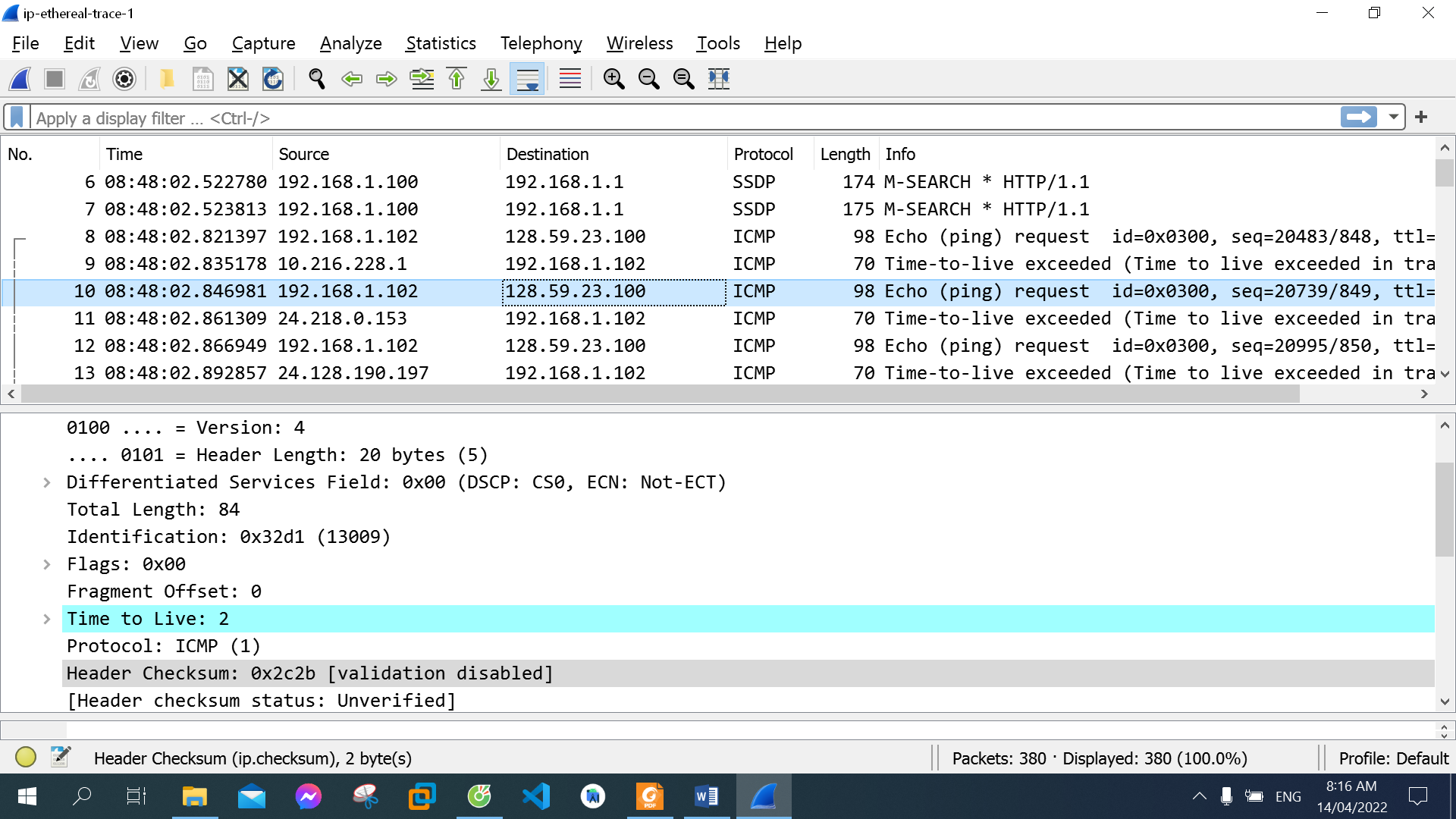
1. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Fields stay constant and must stay constant: Version (we are using IPv4 for all packets), Header Length (these are ICMP packets), Source Address (we are sending from the same source), Destination Address (we are sending to the same destination) Differentiated Services Field all packets are ICMP they use the same Type of Service class), Protocol these are ICMP packets)

Fields must change: Identification(IP packets must have different ids), Time to live (traceroute increments each subsequent packet), Header checksum (header changes, so must checksum)

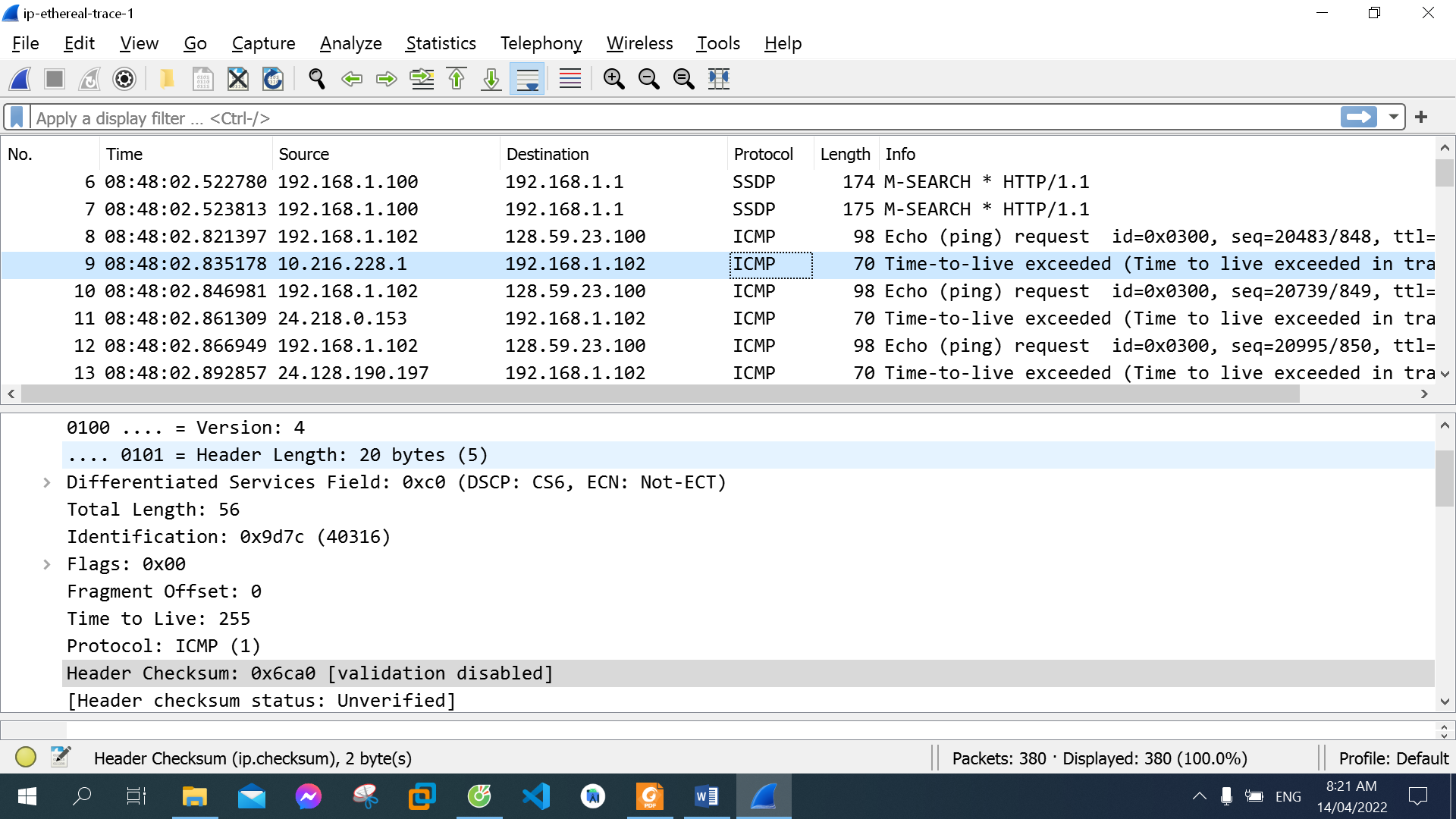
1. Describe the pattern you see in the values in the Identification field of the IP datagram





The pattern in the identification field is that the field increases by one in each  strand of echo requests (0x32d0 -> 0x32d1)

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



Identification: 0x9d7c (40316)

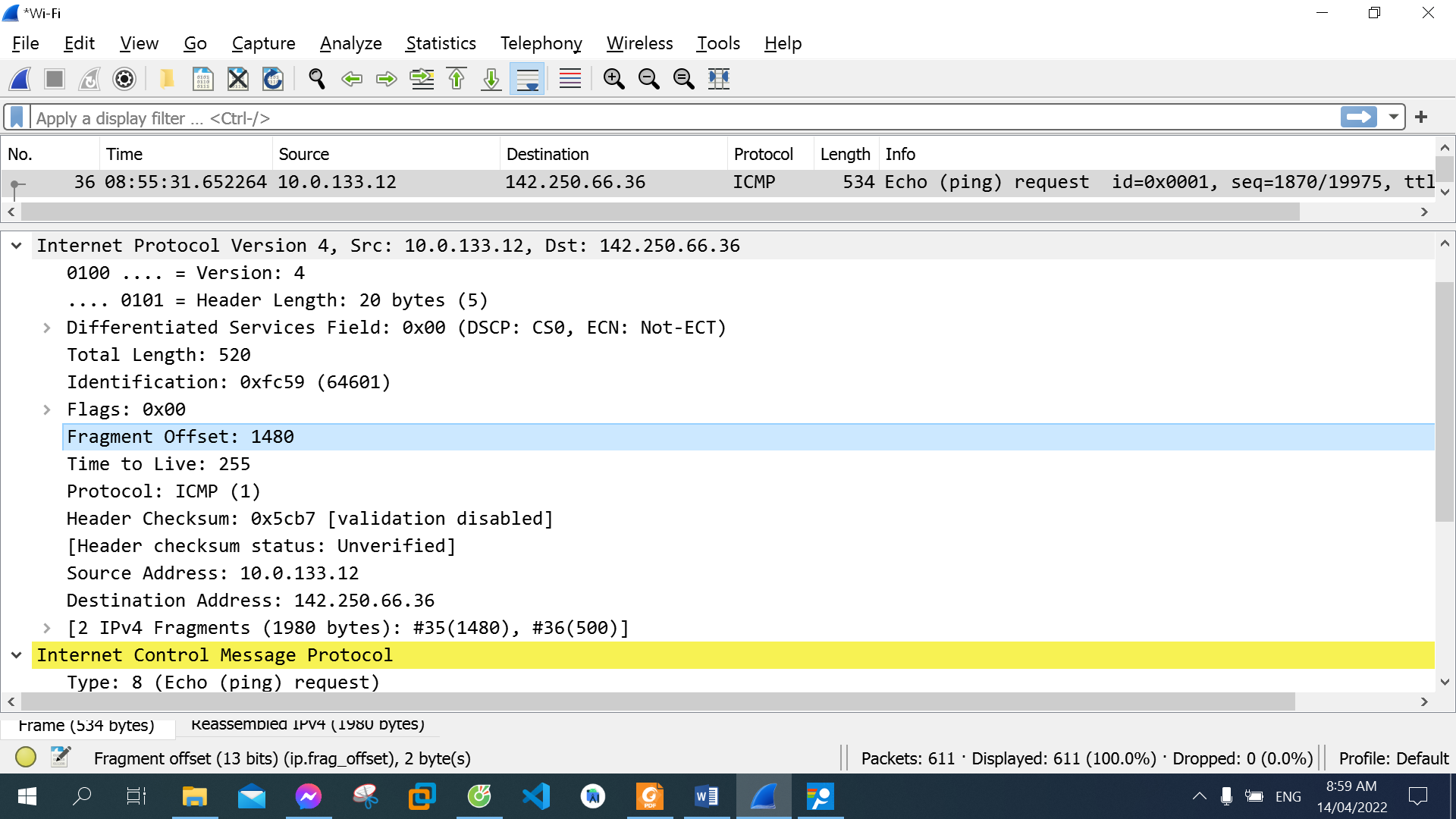
TTL: 255

1. 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, they are not. Identification changes because IP packets must have different ids, Time to live changes because traceroute increments each subsequent packet

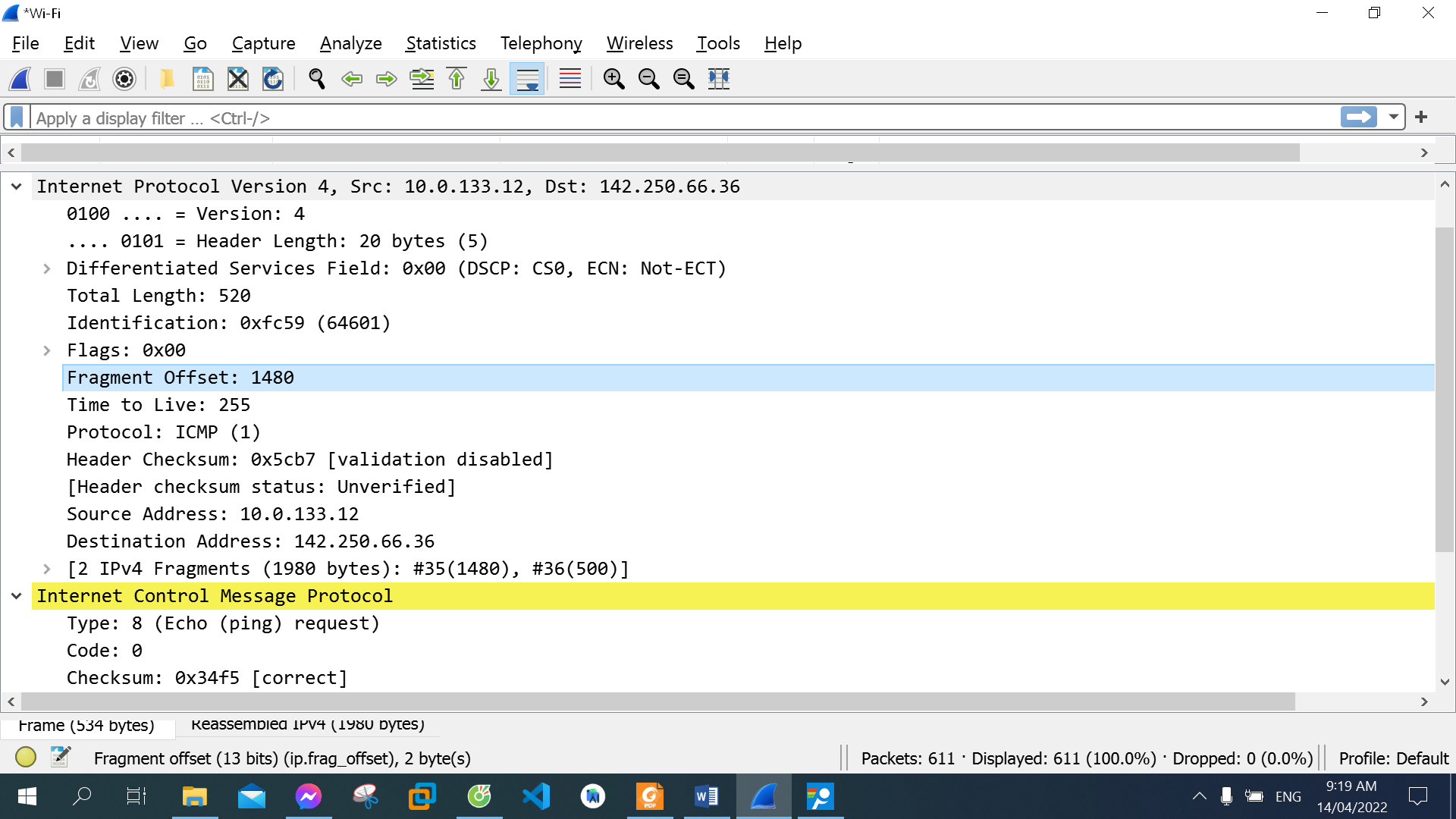
1. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

**Use**: *gaia.cs.umass.edu* for Question 10,11,12,13,14,15



Yes, it has. (Fragment Offset > 0)

1. 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?

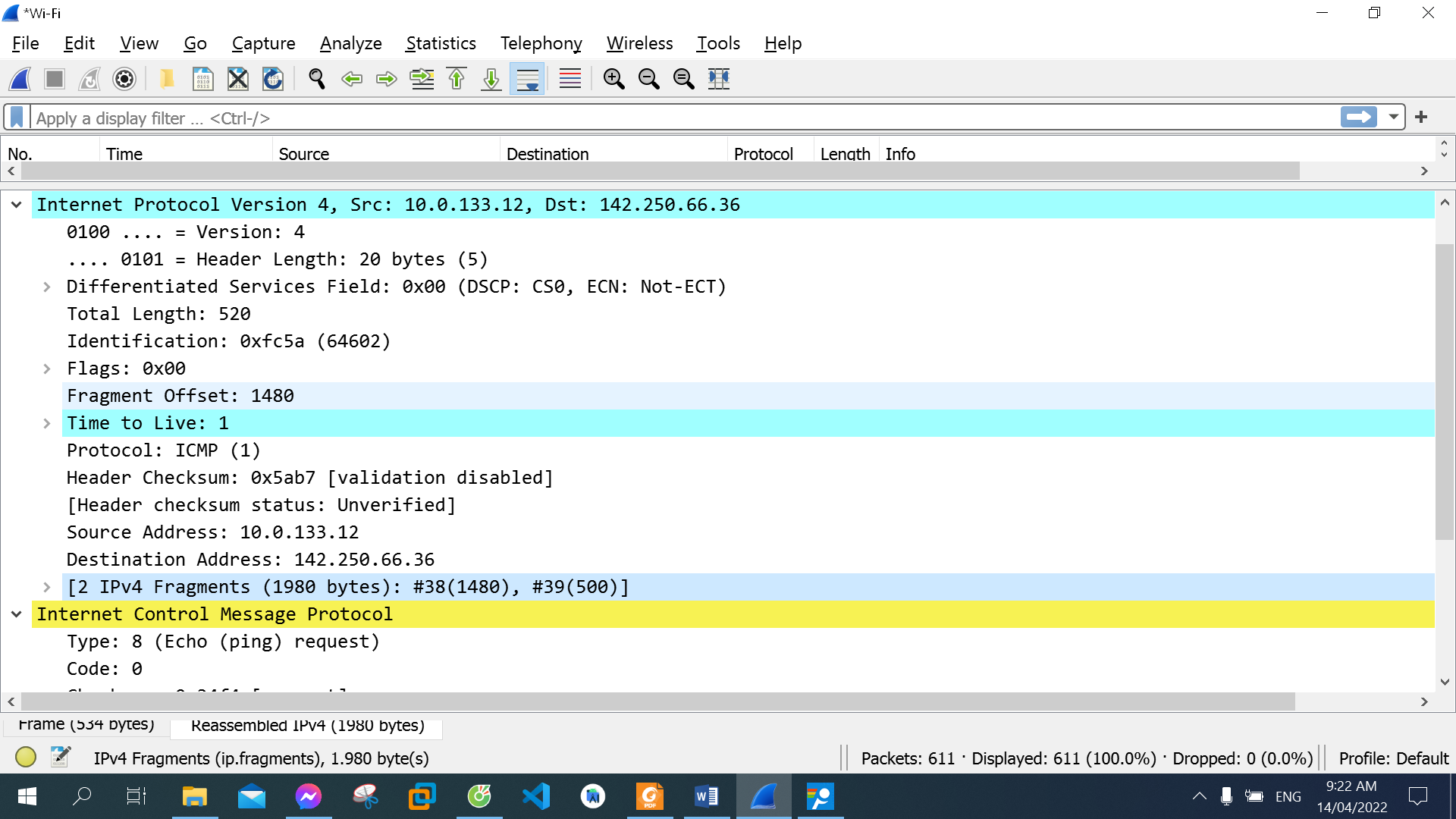


  Fragment Offset: 1480 indicates that the datagram been fragmented

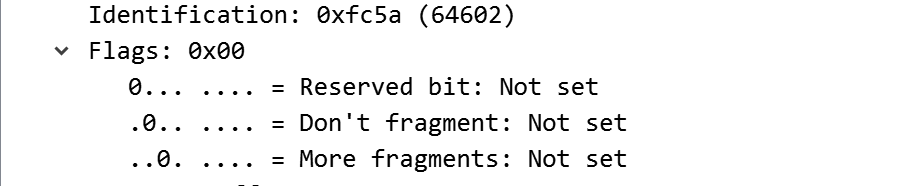
Information in the IP header indicates whether this is the first fragment: Fragments number is the smallest (#35)

This IP datagram: 520

1. 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?



It’s Fragments number (#38) is greater than the first datagram fragment.



There is no more fragments. Because Flags More fragments is not set.

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

Time to live, Identification, 2 IPv4 Fragments

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

3 fragments were created from the original datagram

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



Time to live, Identification, 3 IPv4 Fragments