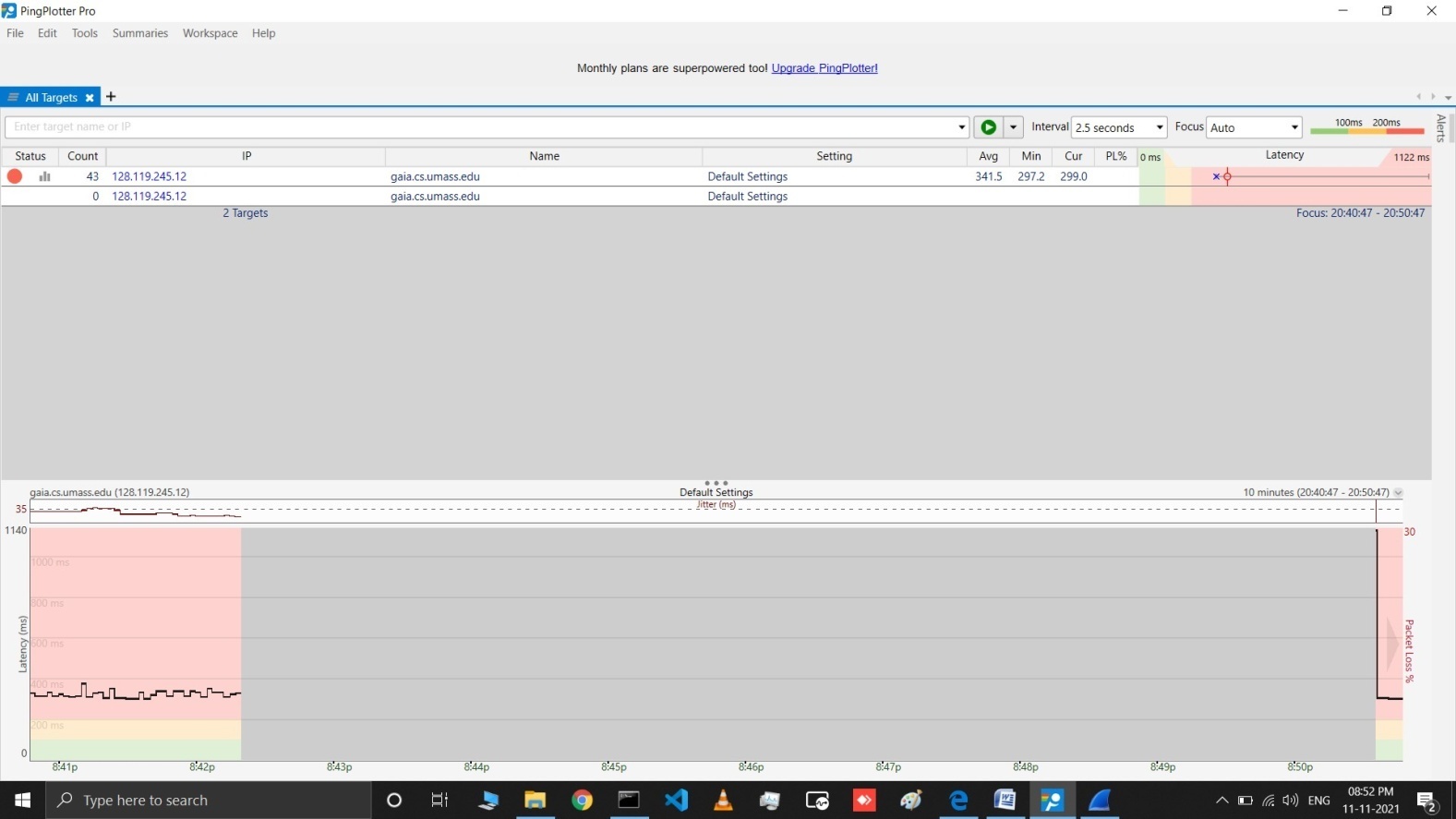
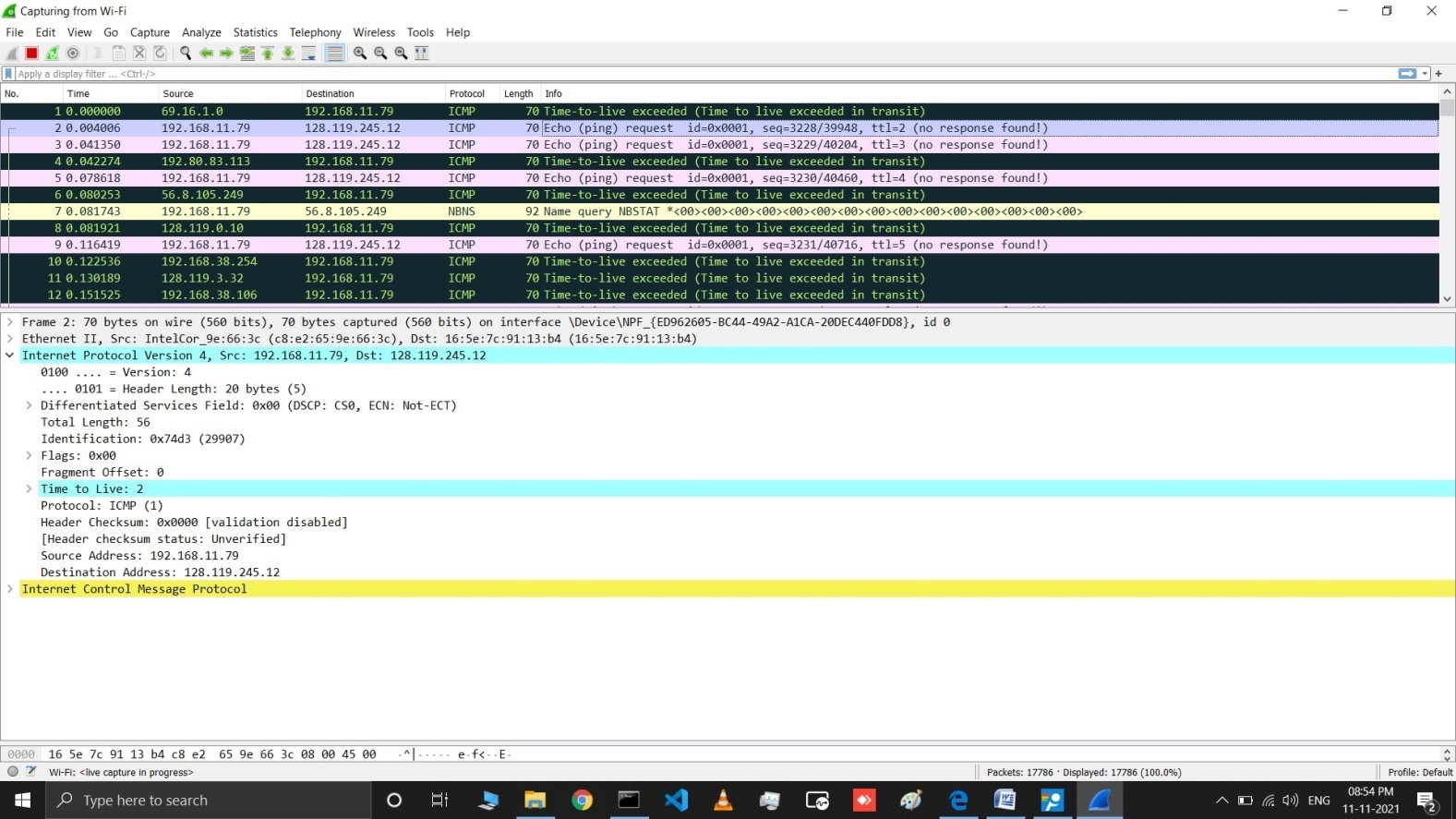
**PRACTICAL-9**

**Aim: IP packets -** Understand basic networking concept using Wire shark and capture HTTP Protocol Traffic

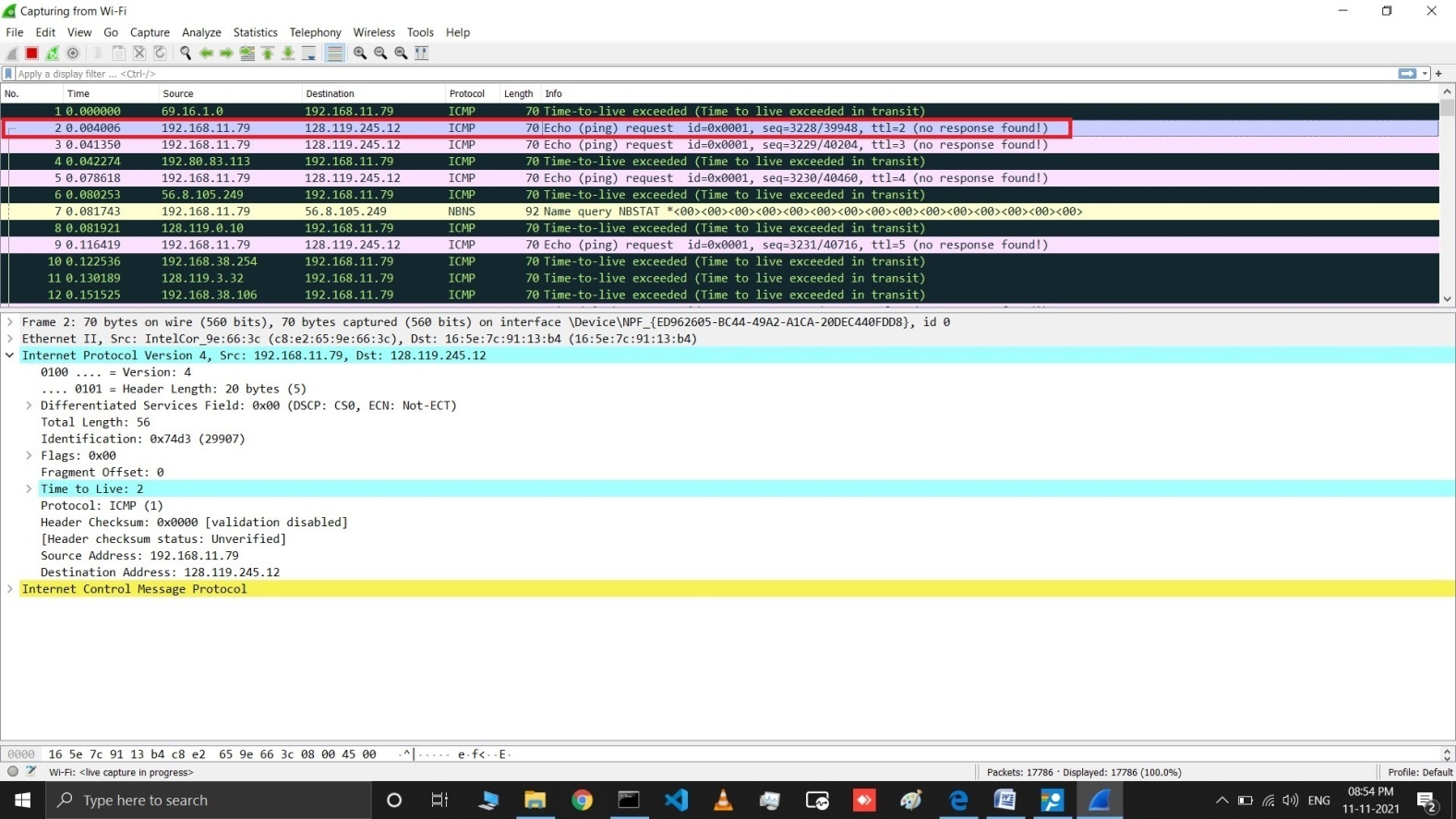


1. Select the first ICMP Echo Request message sent by your computer, andexpand the Internet Protocol part of the packet in the packet detailswindow.



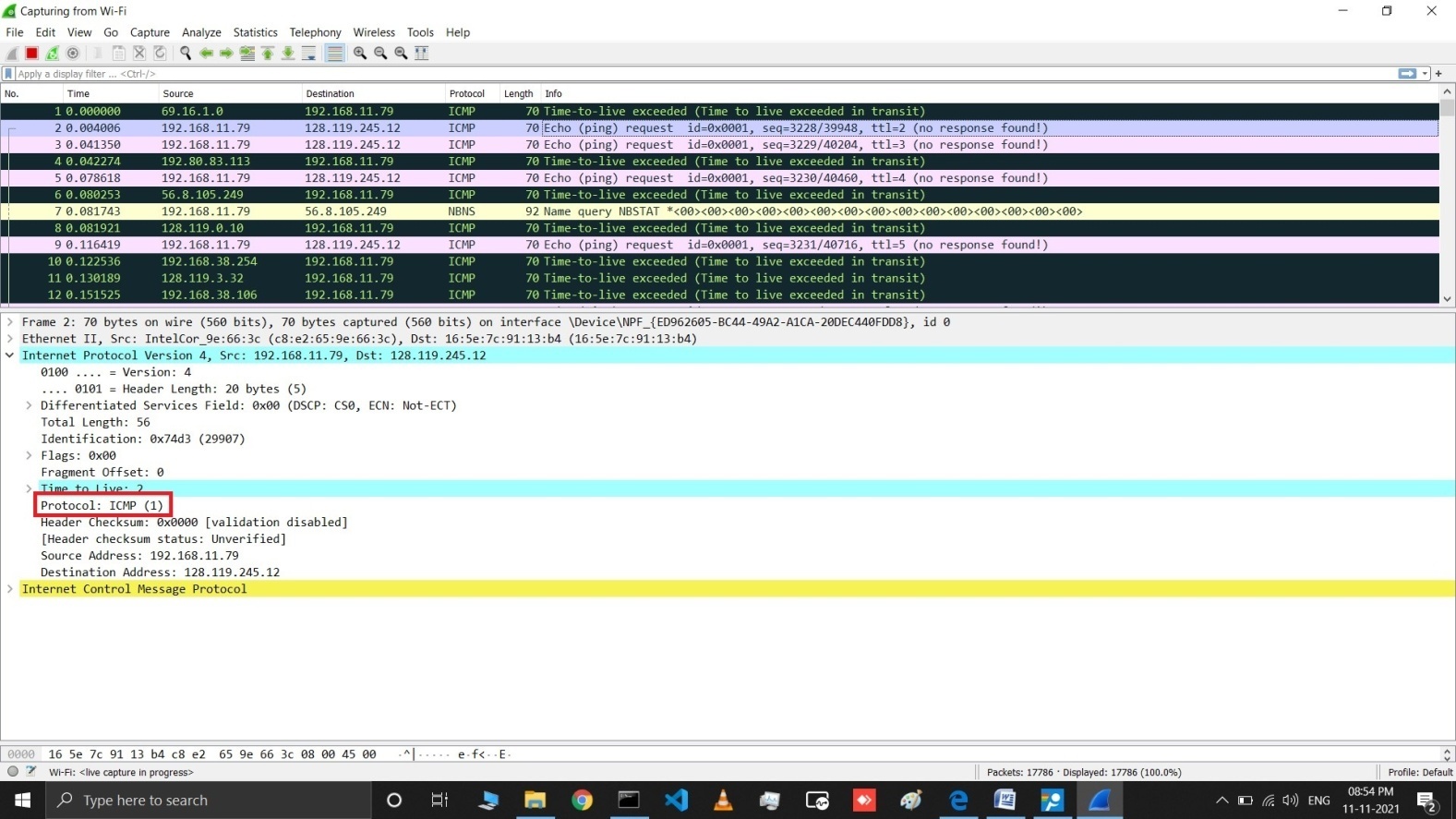
What is the IP address of your computer?

## Answer: The IP address of my computer is 192.168.11.79



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

## Answer: The value of the upper layer protocol field is ICMP (0X01)

****

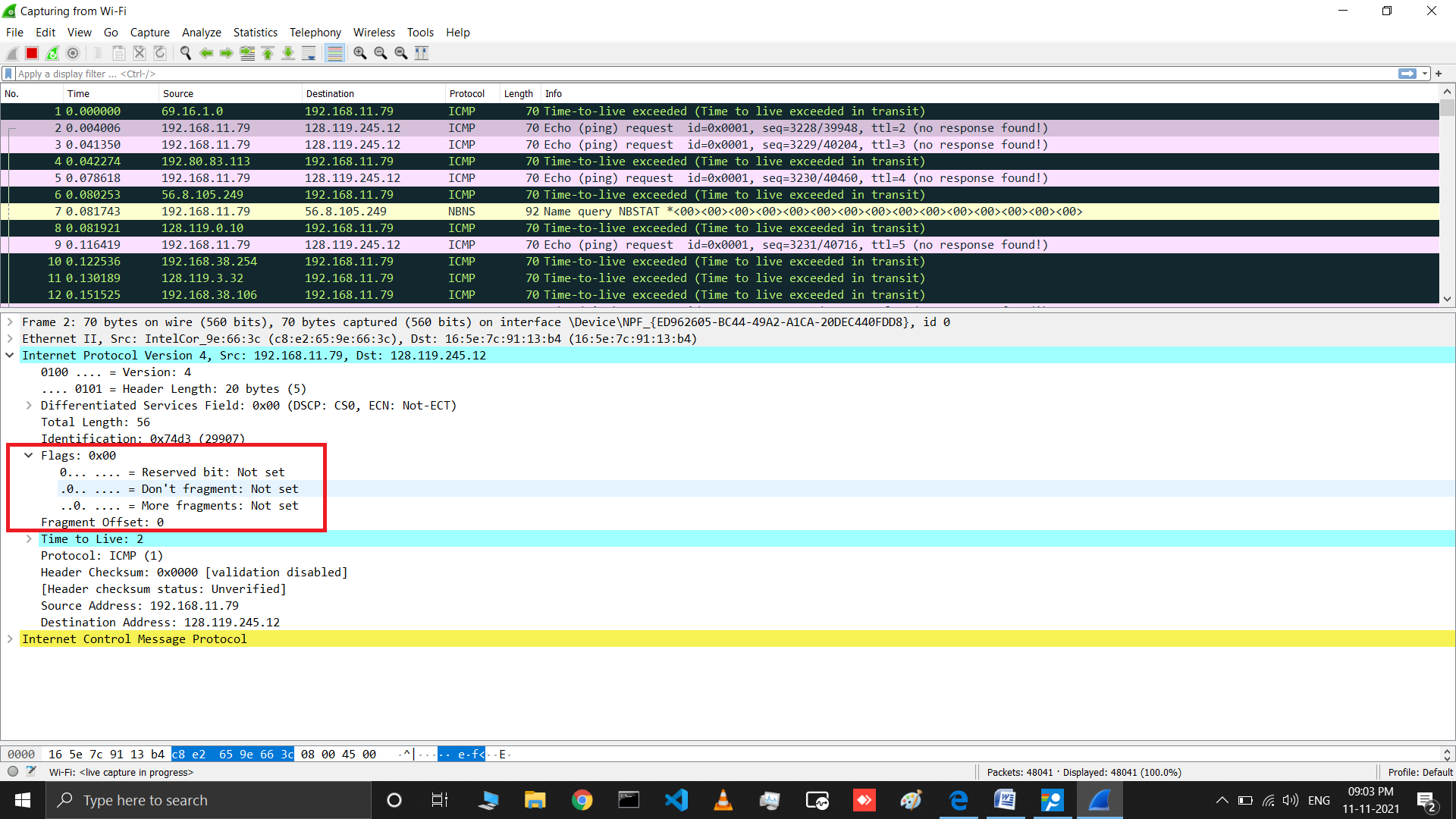
1. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payloadbytes.

## Answer: 20 bytes, 56 bytes, Total Length –Header Length

## 4.jpg

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

## Answer: No, Flags : 0x00(More frags not set)



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

## Answer: Identification field is incrementing. Time to live is also incrementing.

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

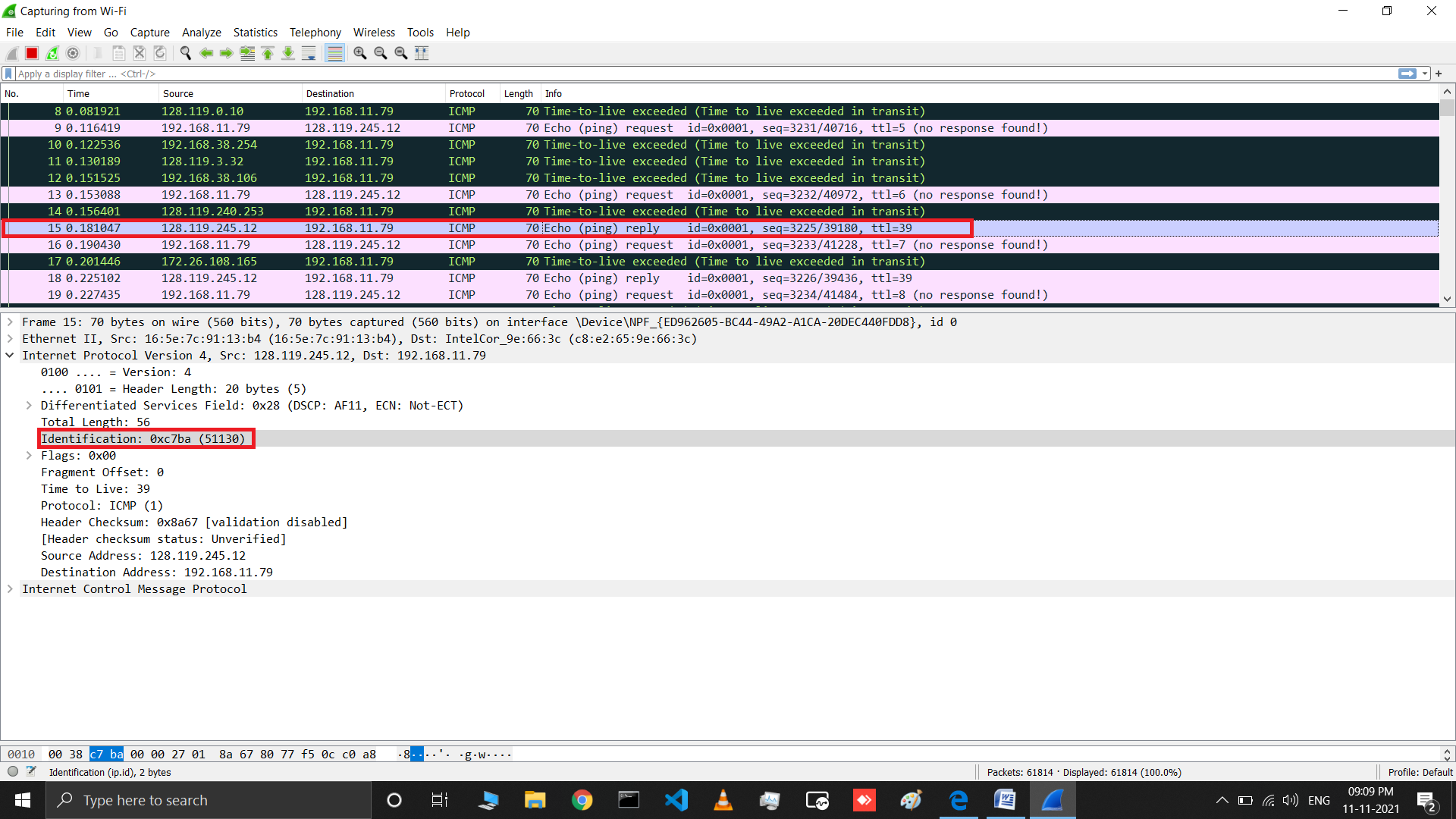
## Answer: version (IPv4 always used) , header length (doesn’t change since we are always using IPv4) , source IP (my computer’s IP address doesn’t change) , destination IP (usc.edu’s IP address doesn’t change) , differentiated services (same protocol every time) , upper layer protocol (same protocol every time) , header checksum (verification disabled in my tests) The following fields change: , Identification field is incrementing (each IP datagram has a different ID) , Time to live is also incrementing (this is how trace route works, as discussed in the assignment)

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

## Answer: They are incrementing with each datagram.

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

## Answer: Identification: 51130 TTL: 39

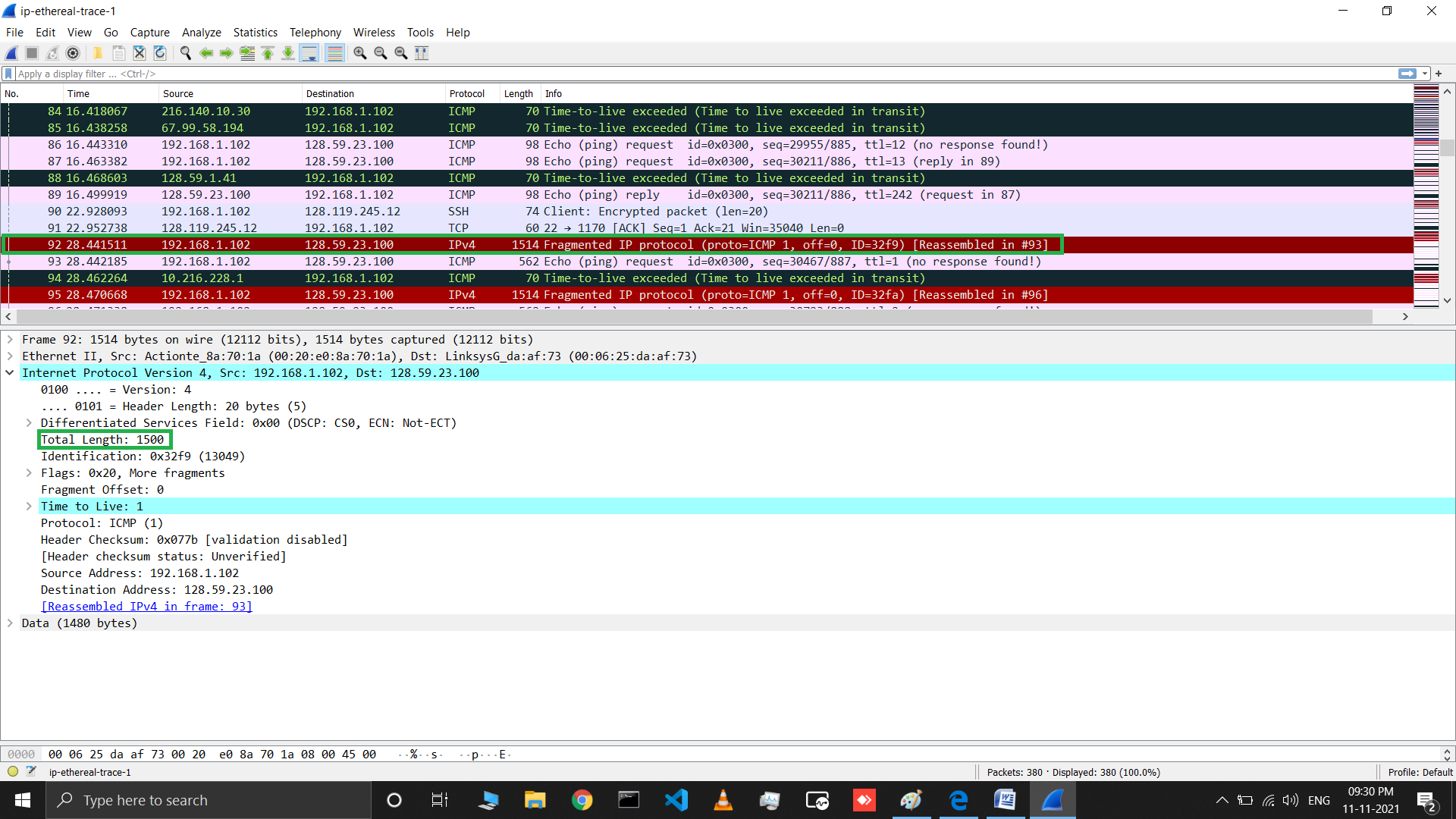


1. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router?Why?

## Answer: The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When 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 remains unchanged because the TTL for the first hop router is always thesame.

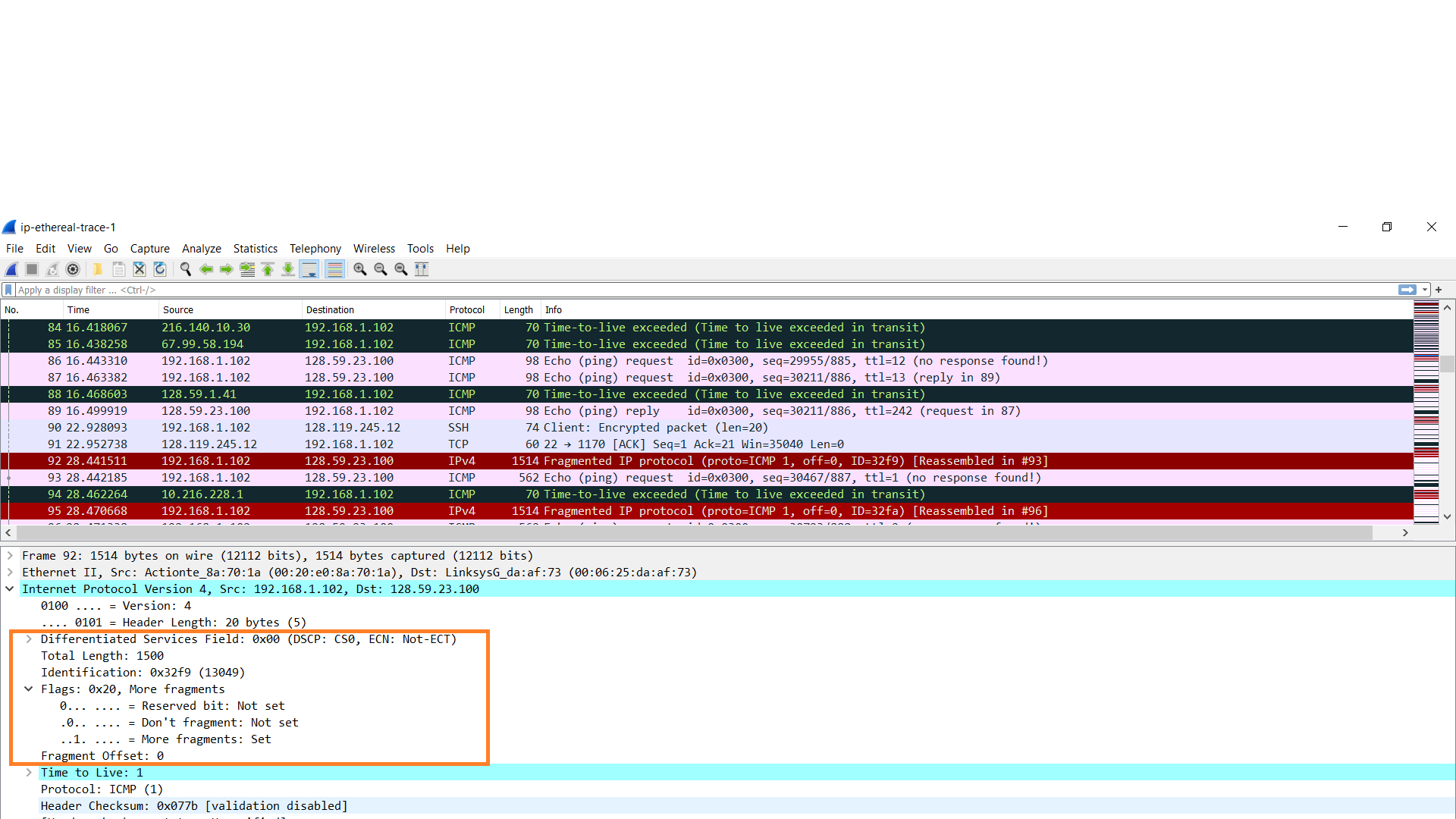
1. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *ping plotter* to be 2000. Has that message been fragmented across more than one IP datagram?

**Answer: Yes, fragmented into two packets (1500 and 548) .**



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?

## Answer: Flags:0x20(More frags set), Fragment offset = 0, 1500 bytes.



1. Print out the second fragment of the fragmented IP datagram. What informationin the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

## Answer: Fragment Offset = 1480, No, flags = 0x00(More frags Not set)

## 9.png

1. What fields change in the IP header between the first and second fragment? **Answer: The IP header fields that changed between the fragments are: total length,flags, fragment offset, and checksum.**
2. How many fragments were created from the original datagram?( *Packet Size* in *ping plotter* to be 2000)

## Answer: After switching to 3500, there are 3 packets created from the original datagram.

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

## Answer: The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0.