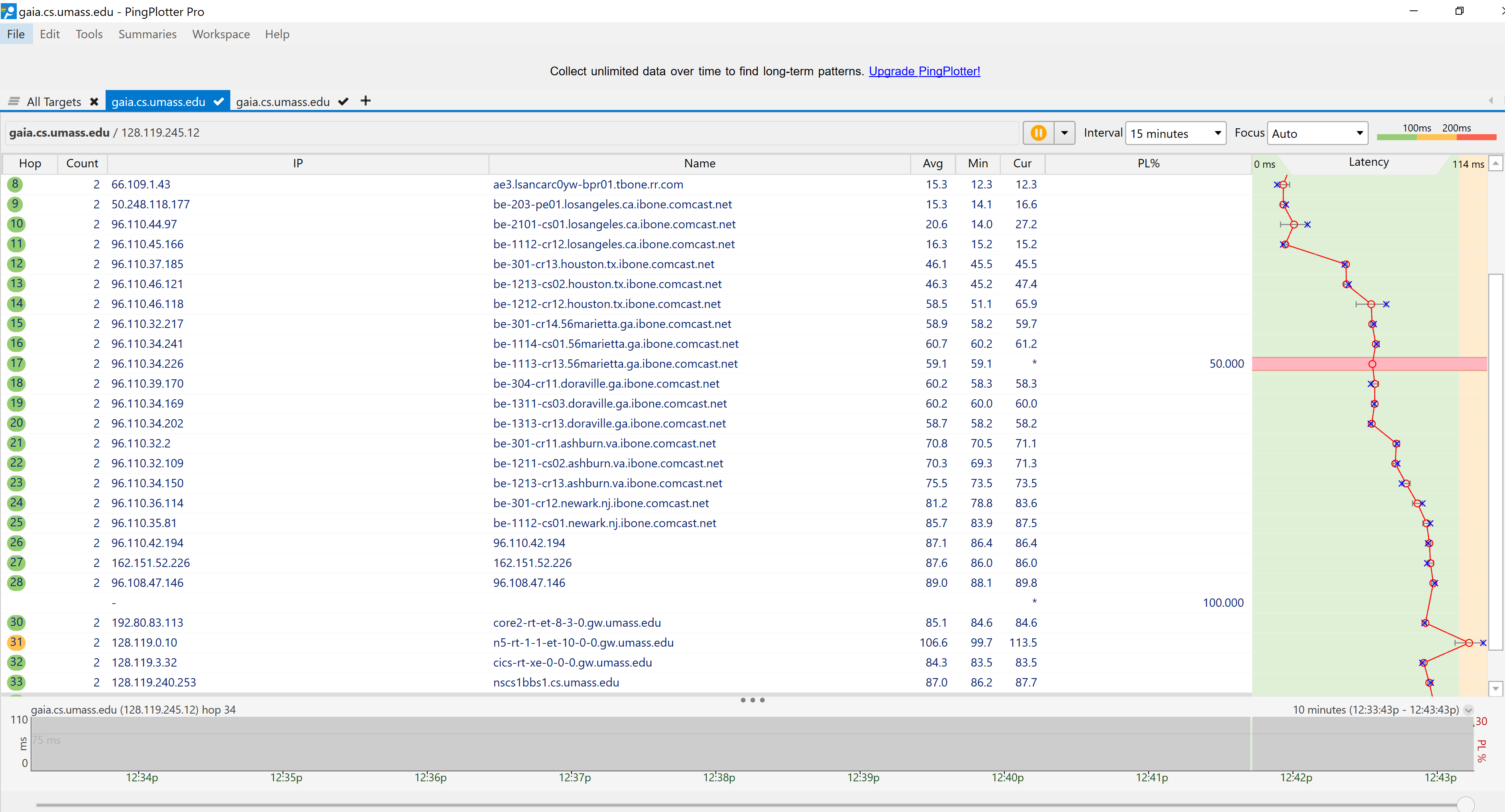
**QUESTIONS**

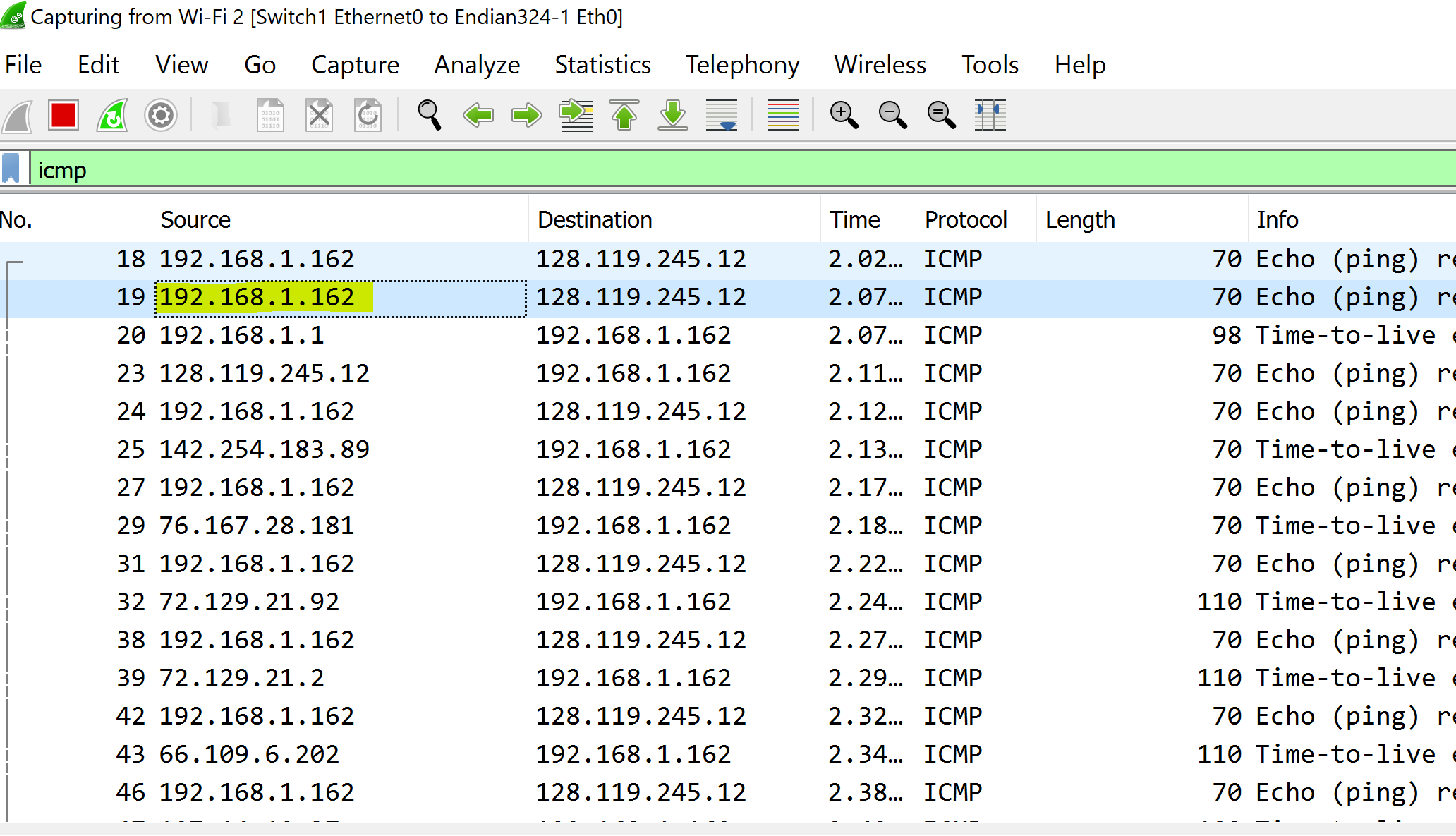
**USING THE 56-BYTE PACKET-SIZE PING CAPTURE DATA**

Open the Wireshark 56-byte packet size capture file and sort the packet listing according to time by clicking on the Time column.

1. Provide a screenshot of pingplotter result for 56-byte packet size. In Wireshark, 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? Provide screenshot(s) to illustrate and support your answer.

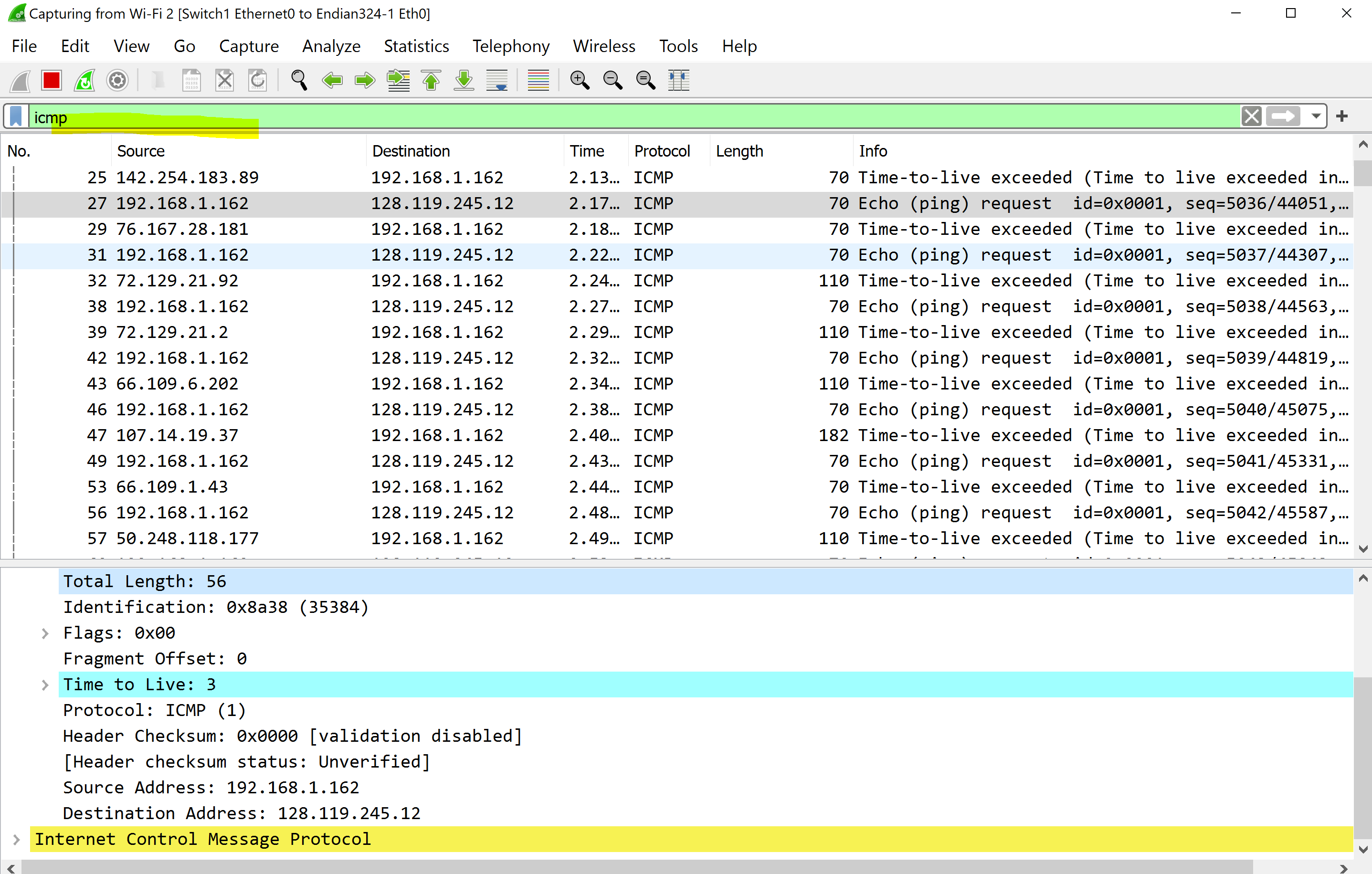


MY IP Address is 192.168.1.162



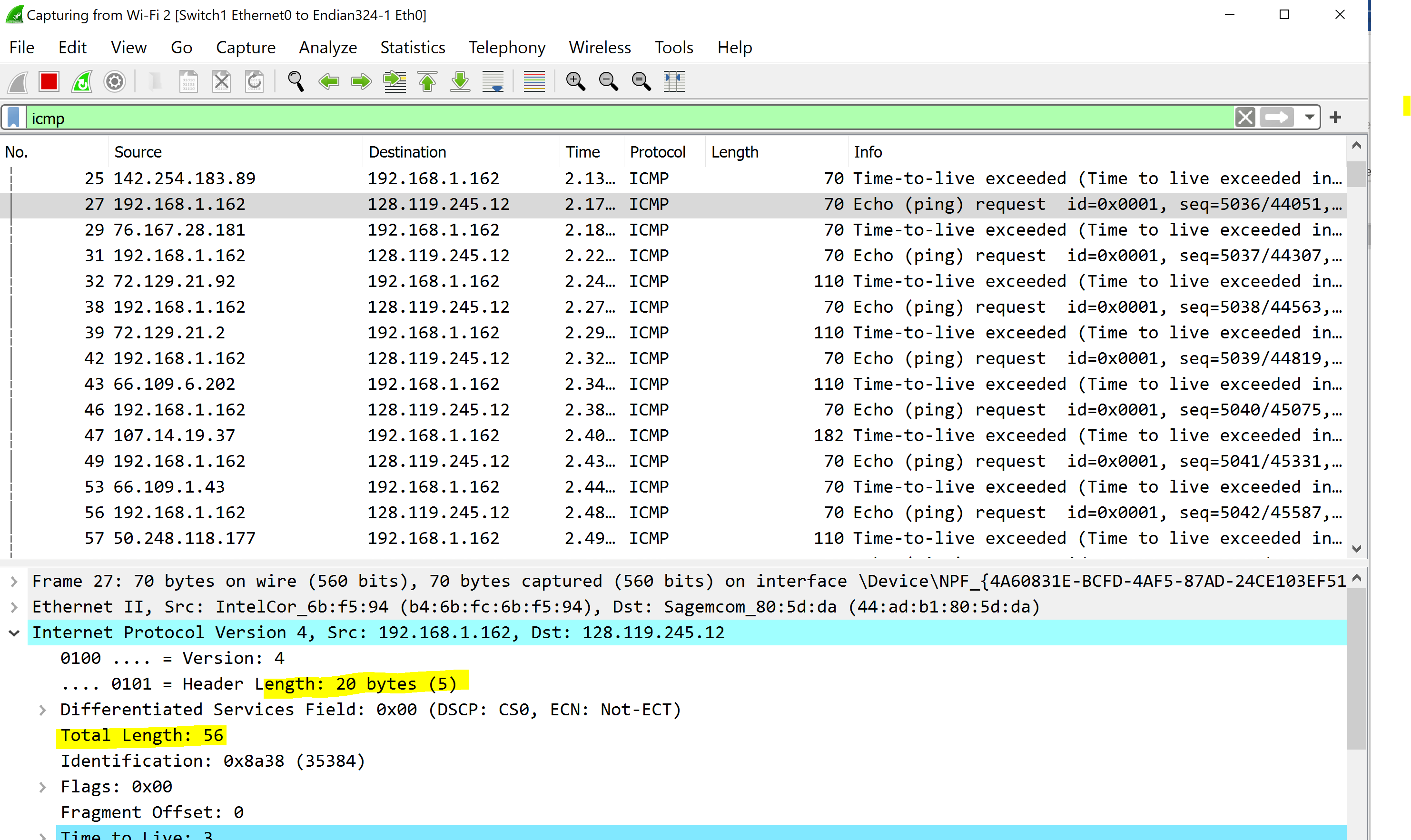
1. Within the IP packet header, what is the value in the upper layer protocol field? Provide screenshot(s) to illustrate and support your answer.

Within the header the upper layer protocol field is ICMP (1)



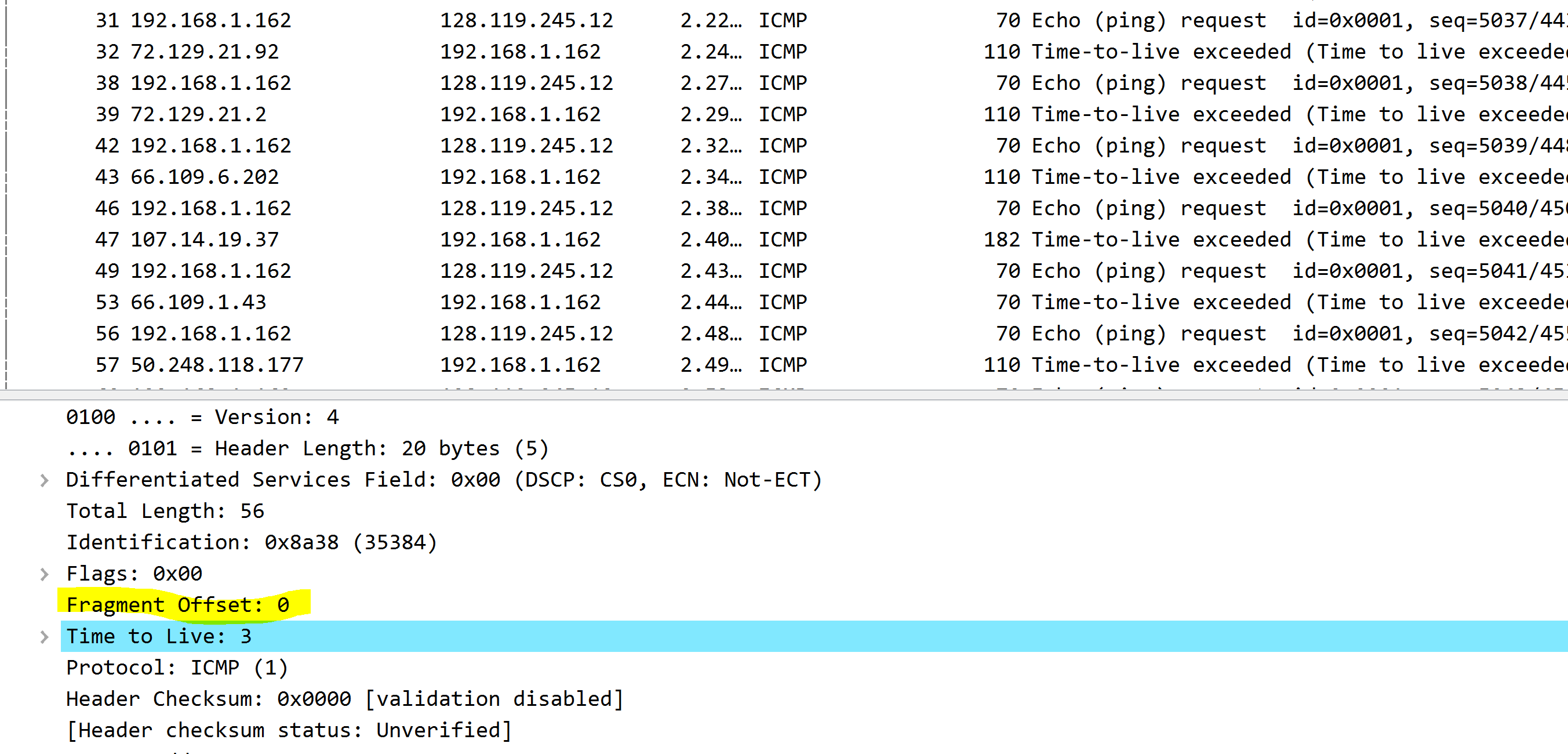
1. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes. Provide screenshot(s) to illustrate and support your answer.

The IP header is 20 bytes since the total length is 56 and 56-20 bytes = 36 byes would be the payload of the datagram.



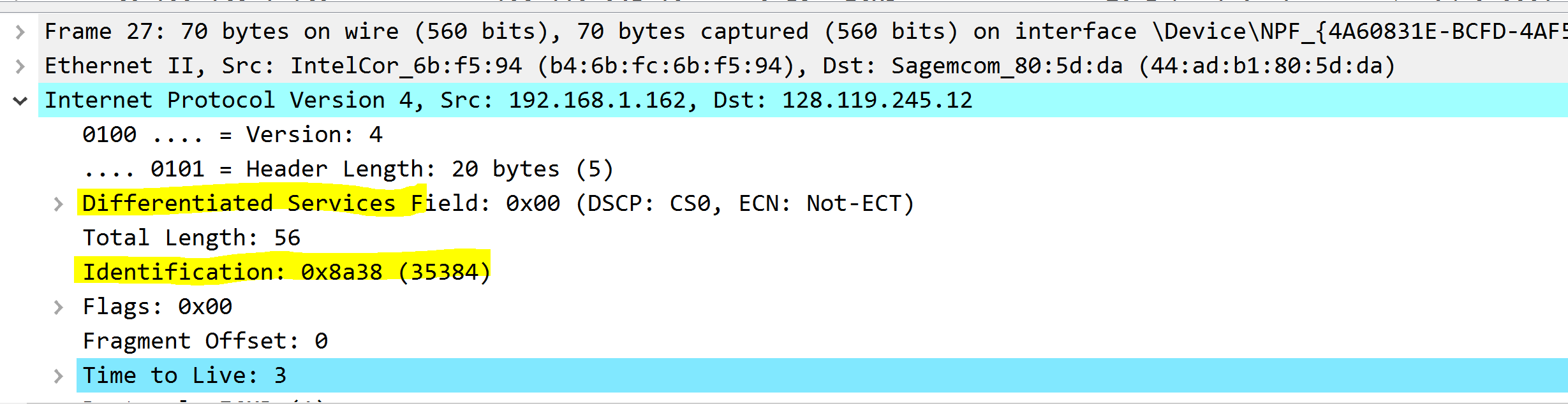
1. as this IP datagram been fragmented. Explain how you determined whether the datagram has been fragmented. Provide screenshot(s) to illustrate and support your answer.

The fragments offset is 0 which mean indicates the starting position of the data



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? Provide screenshot(s) to illustrate and support your answer.

The TTL, checksum, and Identification



1. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why? Provide screenshot(s) to illustrate and support your answer.

* IPv4 is always in use, which means it stays constant.
* Source IP is from the same source every time.
* The destination IP since we’re sending to gaia.cs.umass.edu every time.
* Header length is from the ICMP packets.
* Upper layer protocol is also part of the IMCP packets

**fields must stay Constant**

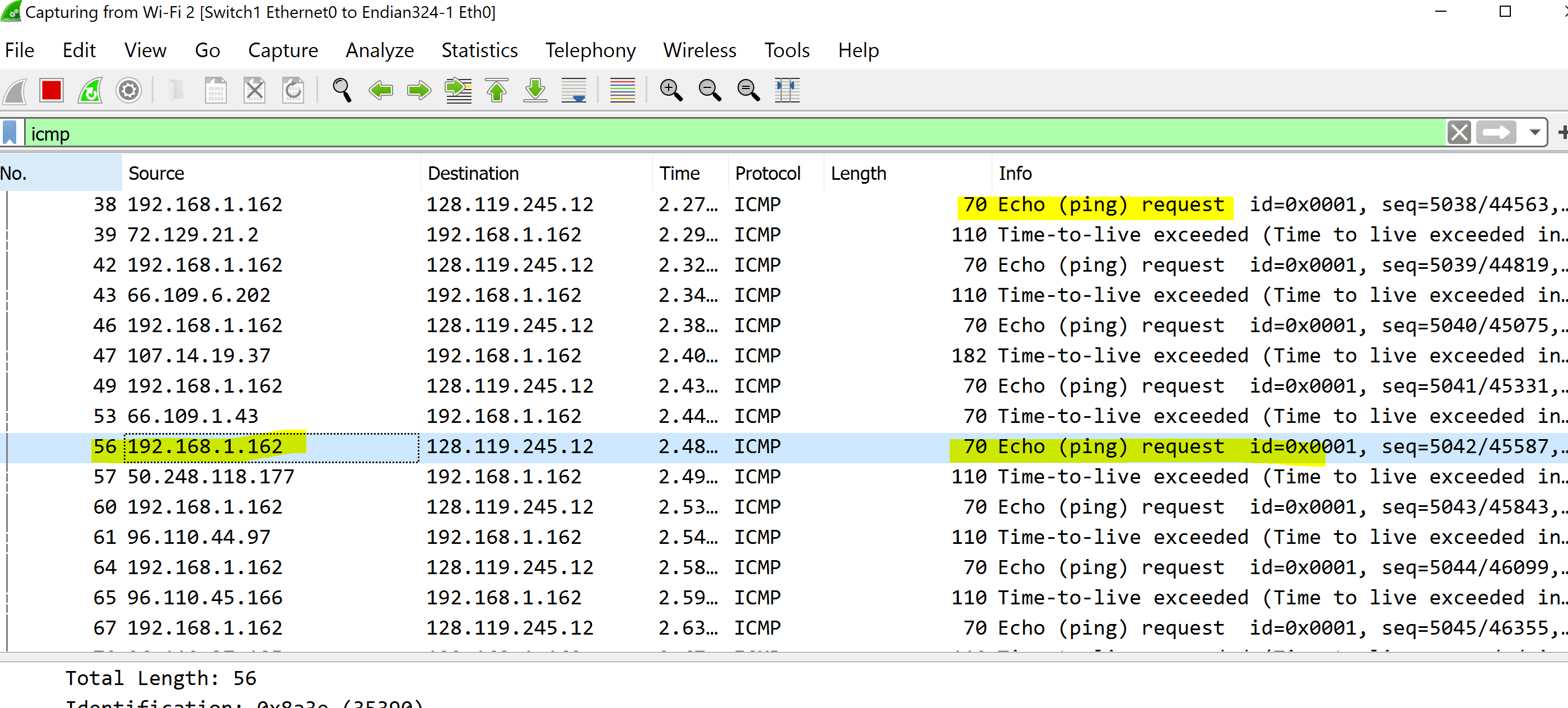
* Vserion(IPv4)
* Source IP
* Destination
* Upper Layer

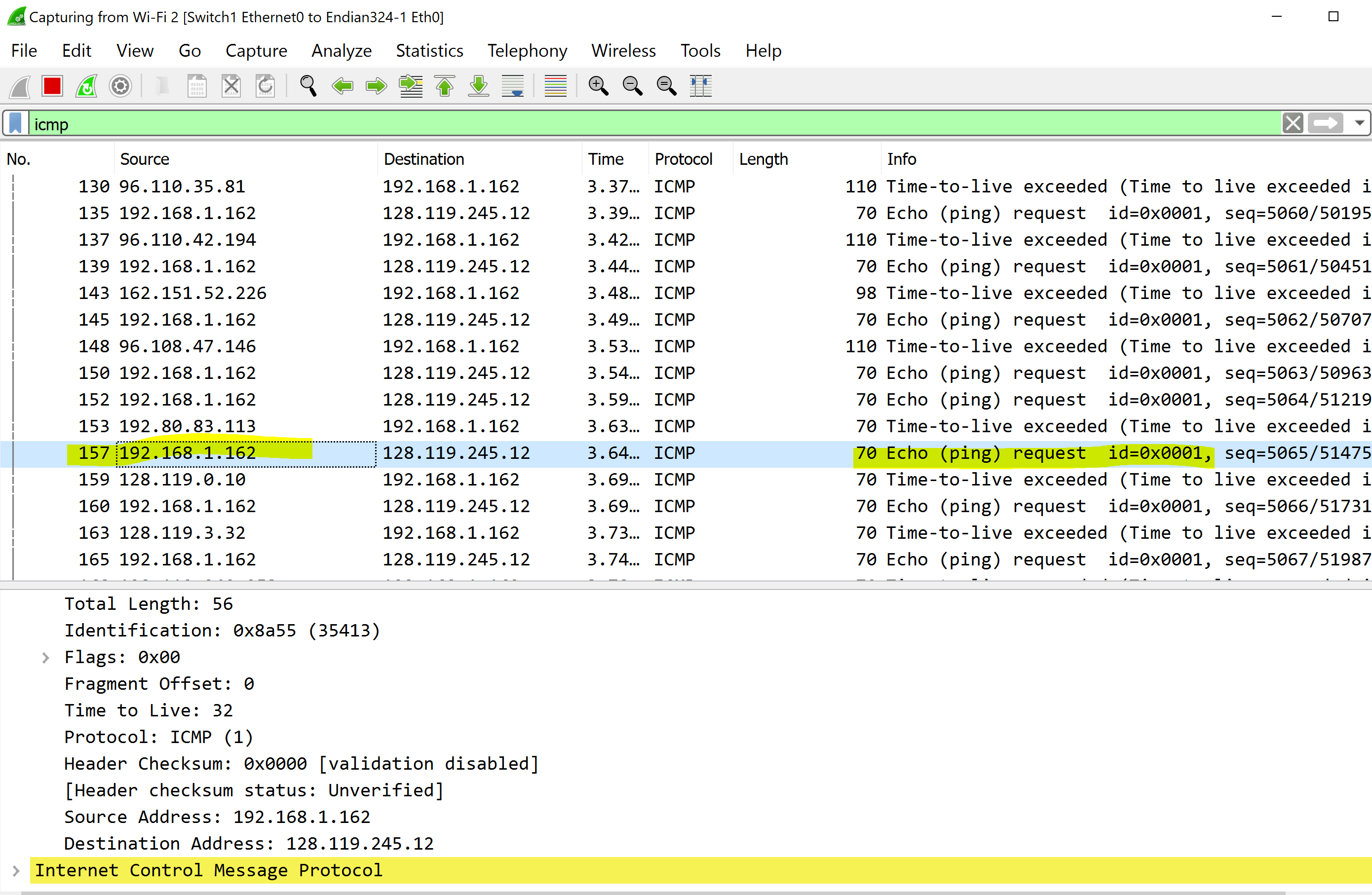
**fields must change**

* The header checksum
* Identifications
* Time to live

1. Describe the pattern you see in the values in the Identification field of the IP datagram. Provide screenshot(s) to illustrate and support your answer.

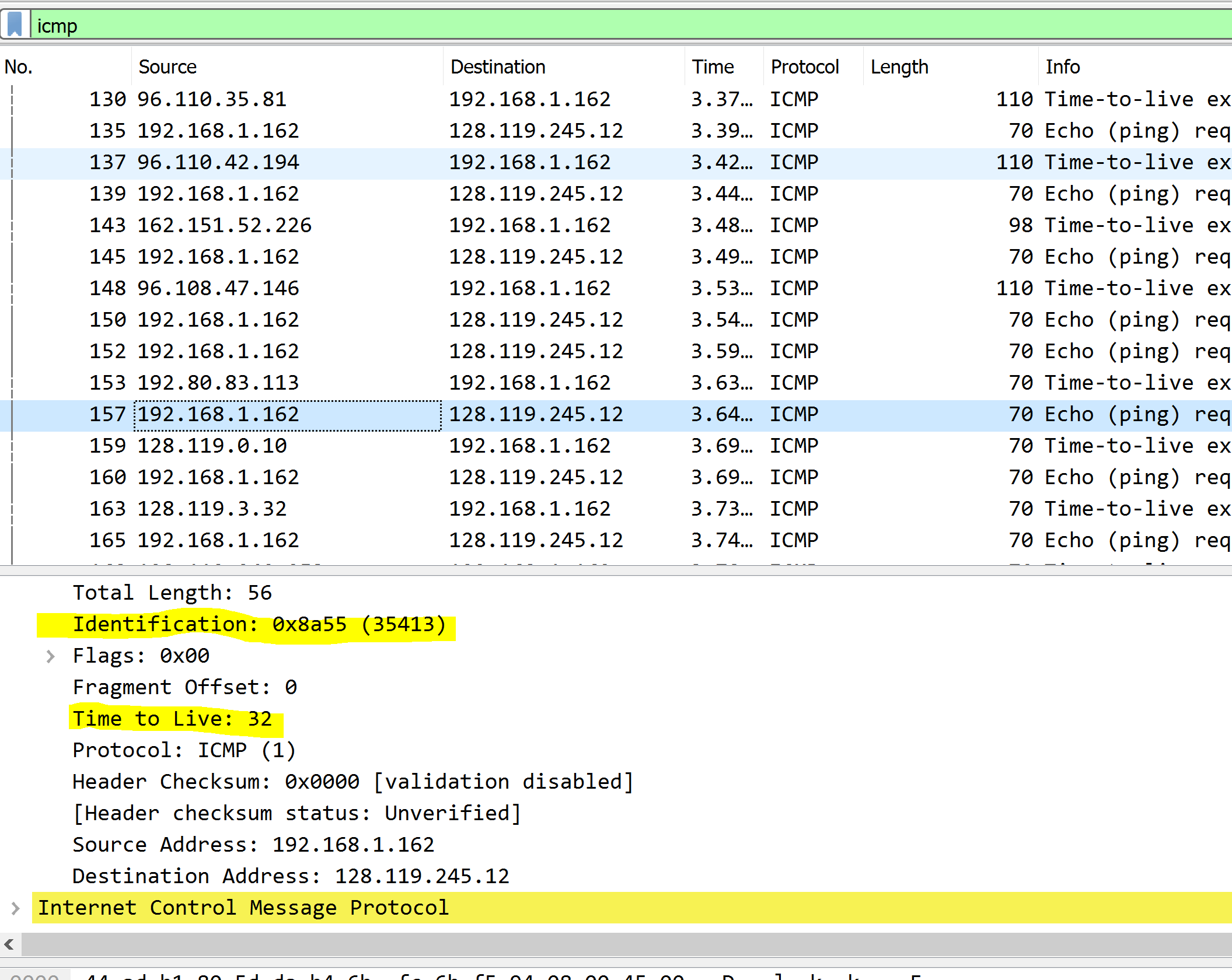
The pattern that the ip header identification field increments with each ICMP Echo request





1. hat is the value in the Identification field and the TTL field? Provide screenshot(s) to illustrate and support your answer.

The Identification field is 35413 and the TTL field is 32

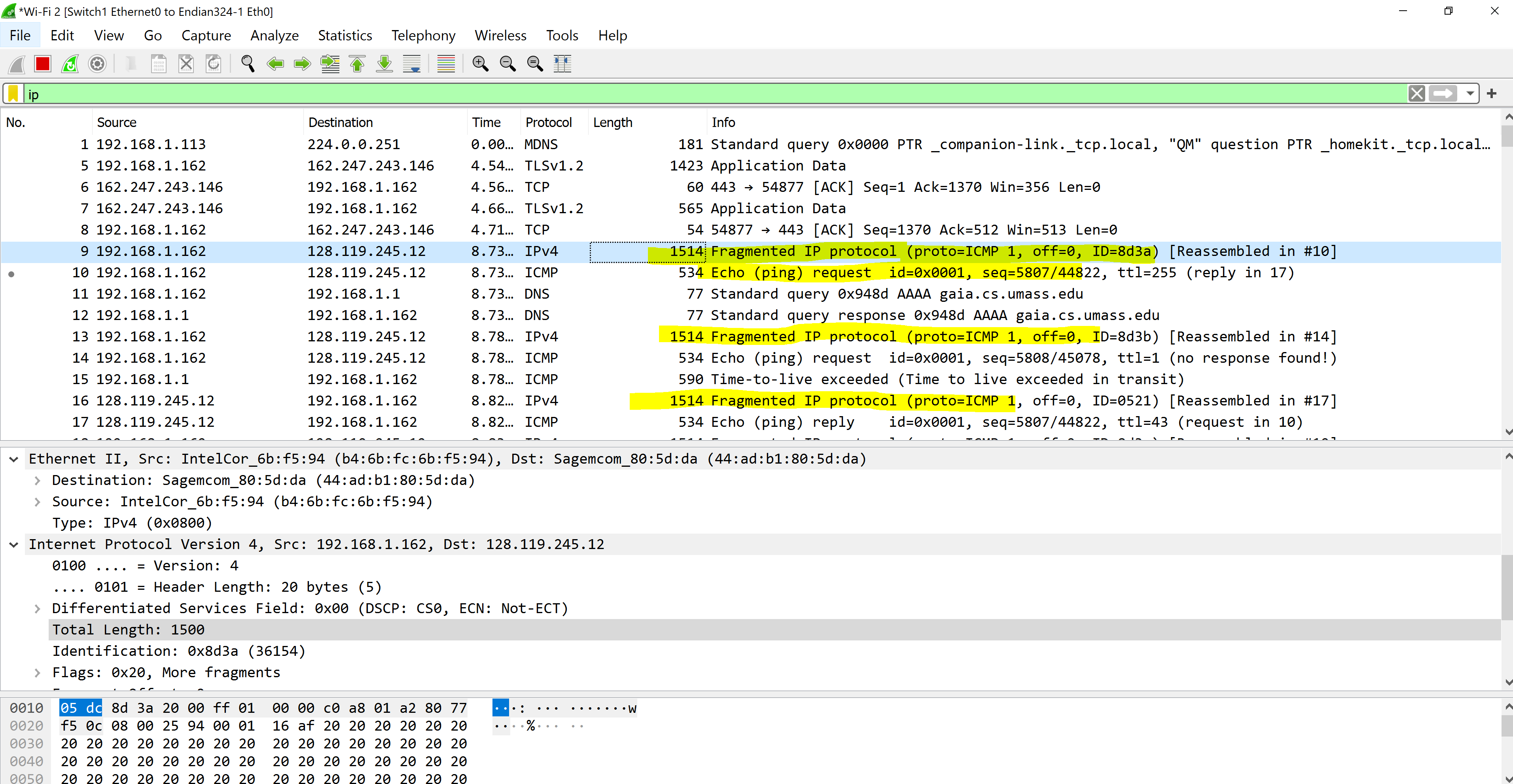


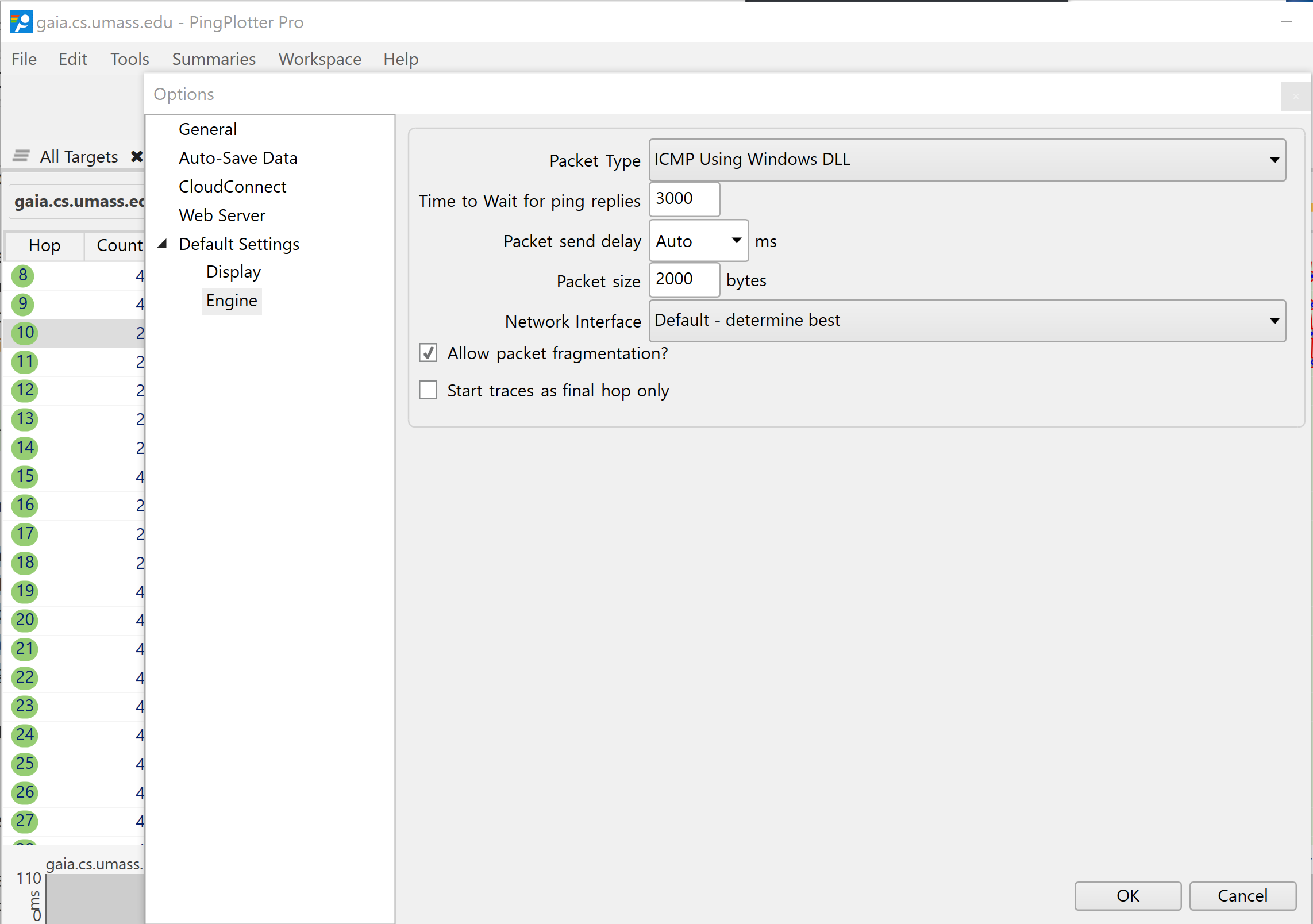
1. Do these values remain unchanged for all the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why? Provide screenshot(s) to illustrate and support your answer.

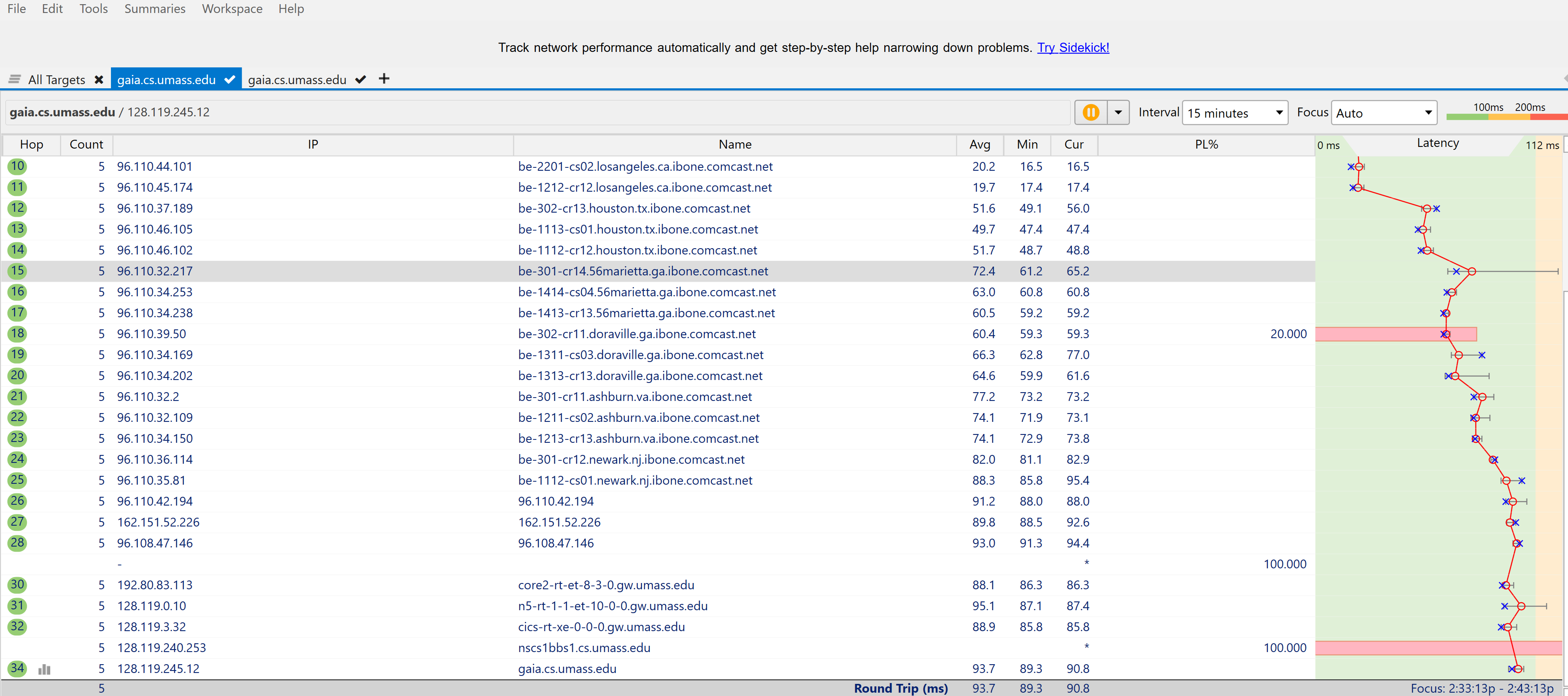
The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram. The TTL field remains unchanged because the TTL for the first hop router is always the same.

1. Provide a screenshot of pingplotter result for 2000-byte packet size. In Wireshark, 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? Explain how you determined whether the datagram has been fragmented. Provide screenshot(s) to illustrate and support your answer.

Yes the message been Fragmented across more than one IP Datagram

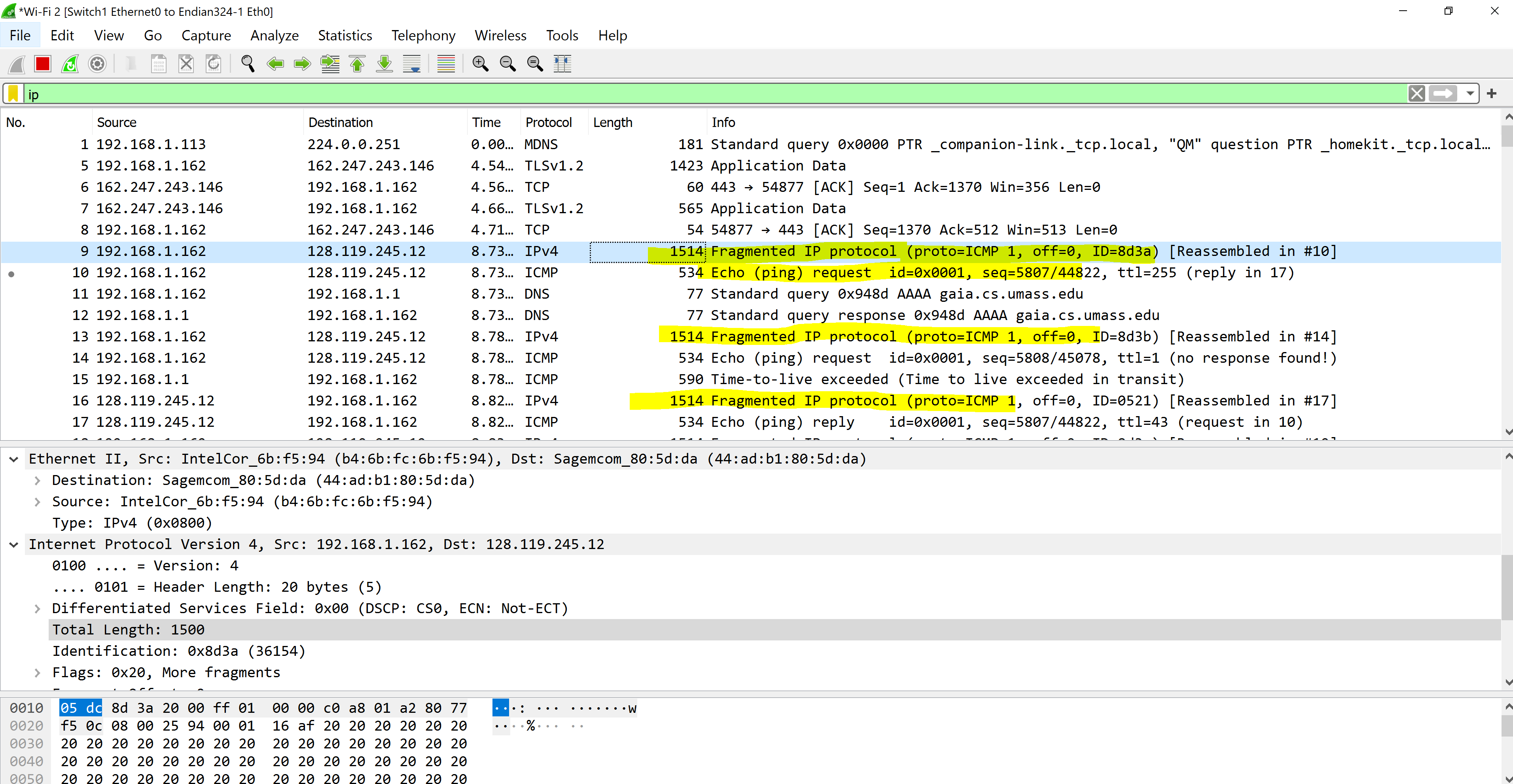






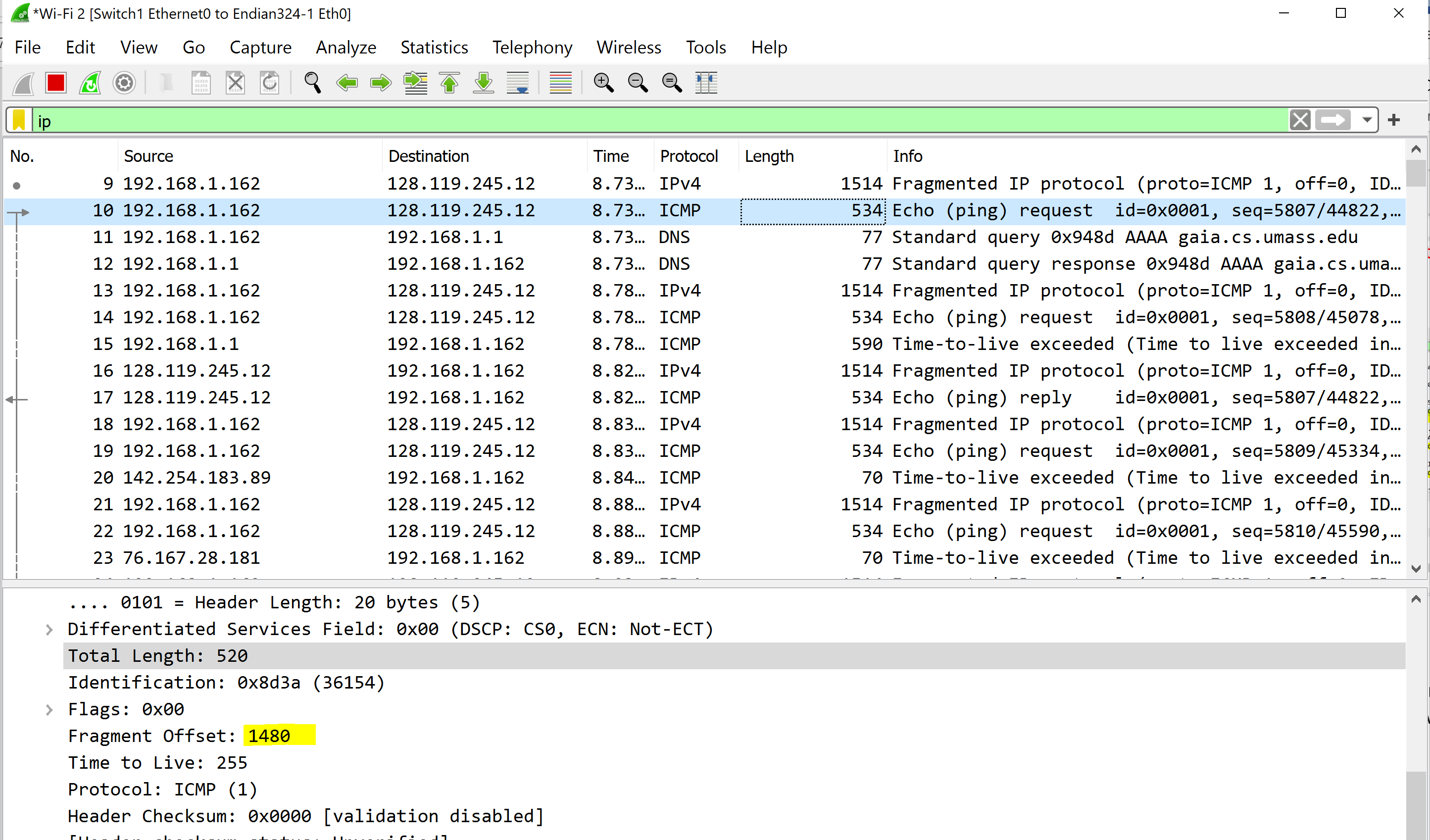
1. . From the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram? Provide screenshot(s) to illustrate and support your answer.

From the first fragment of the Ip datagram looks like it has been fragmented where we can see the total length of 1514 which includes the header and since the fragment offset is 0 that conforms the first fragment.



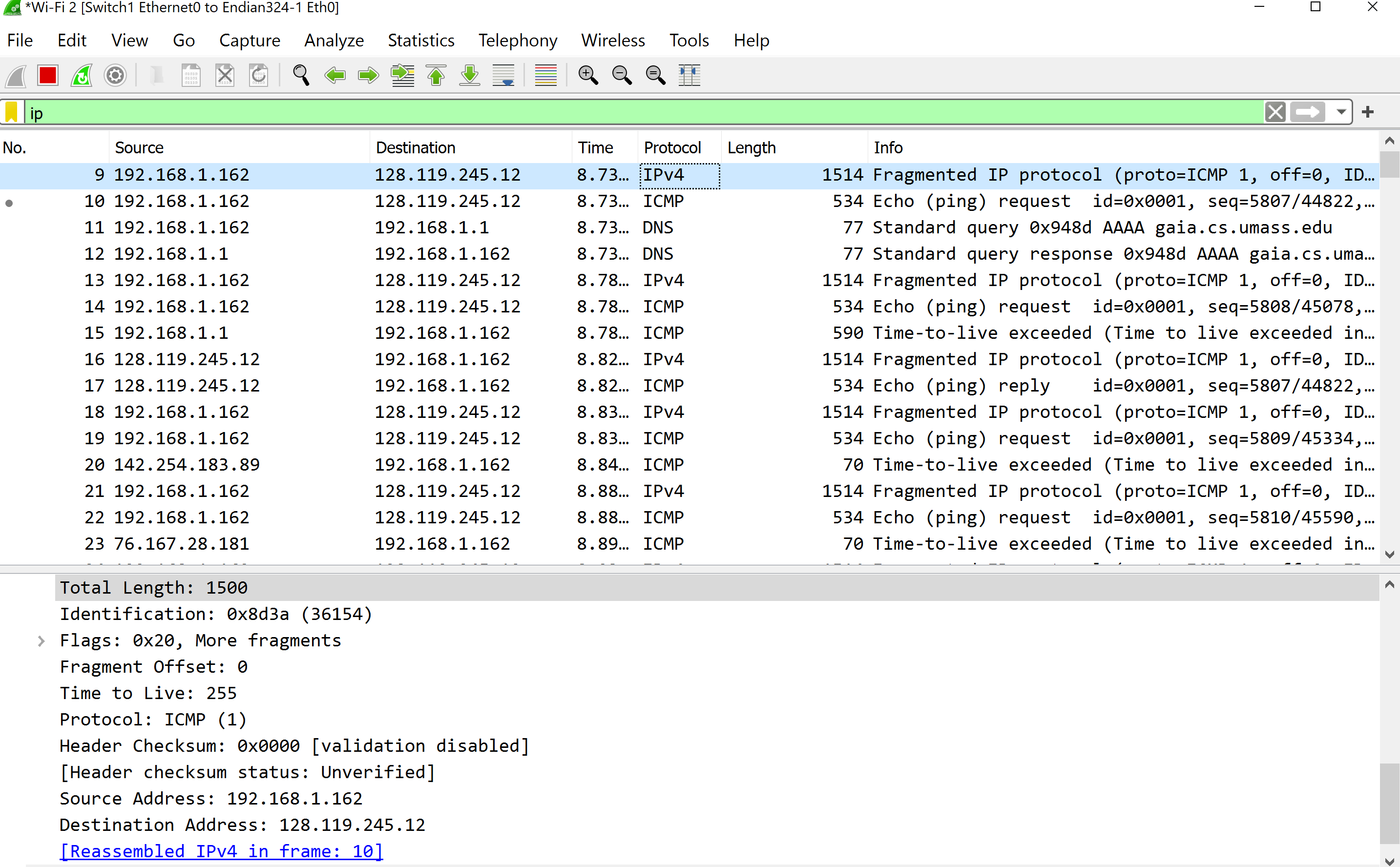
1. From the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell? Provide screenshot(s) to illustrate and support your answer.

Since the fragment offset is 1480 that means it was the last fragment and we do not see any more fragment flag is not set.



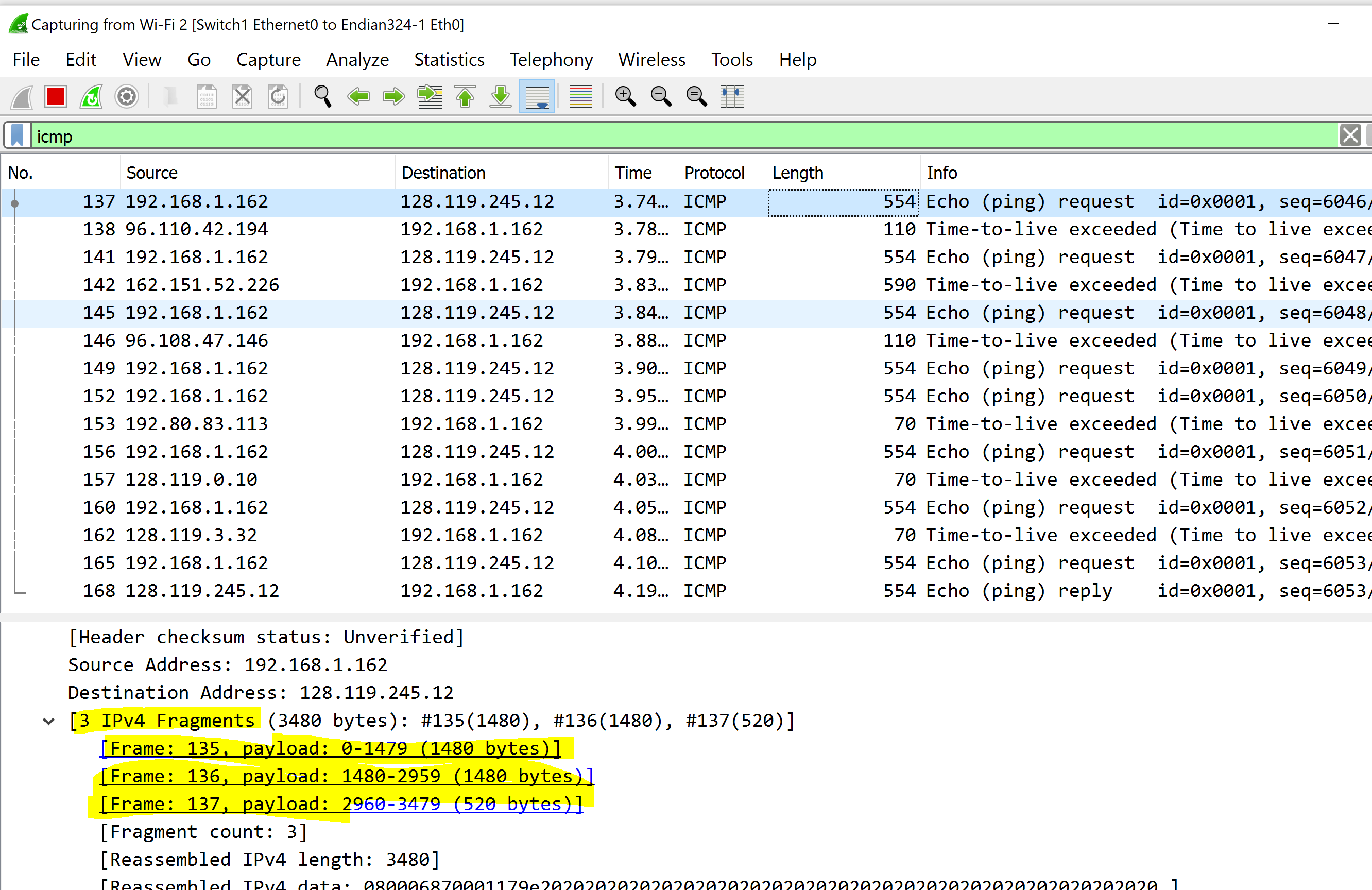
1. What fields change in the IP header between the first and second fragment? Provide screenshot(s) to illustrate and support your answer.

The changes are in the fragment offset number, the total length, flags, and checksum



1. Provide a screenshot of pingplotter result for 3500-byte packet size. In Wireshark, how many fragments were created from the original datagram? Provide screenshot(s) to illustrate and support your answer.





**I see 3 fragments are being created**

1. what fields change in the IP header among the fragments? Provide screenshot(s) to illustrate and support your answer.