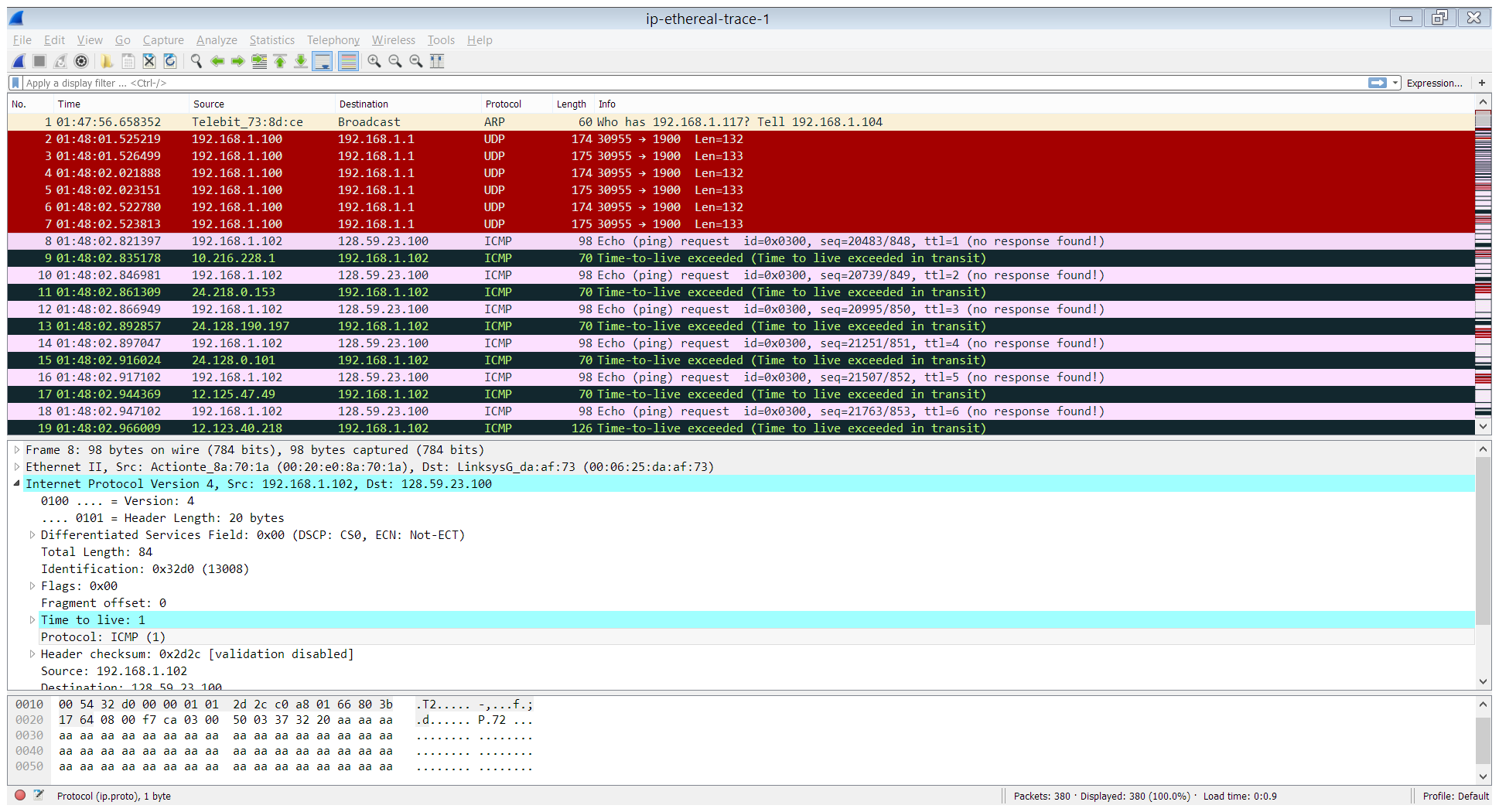
**Tevin Jeffrey**

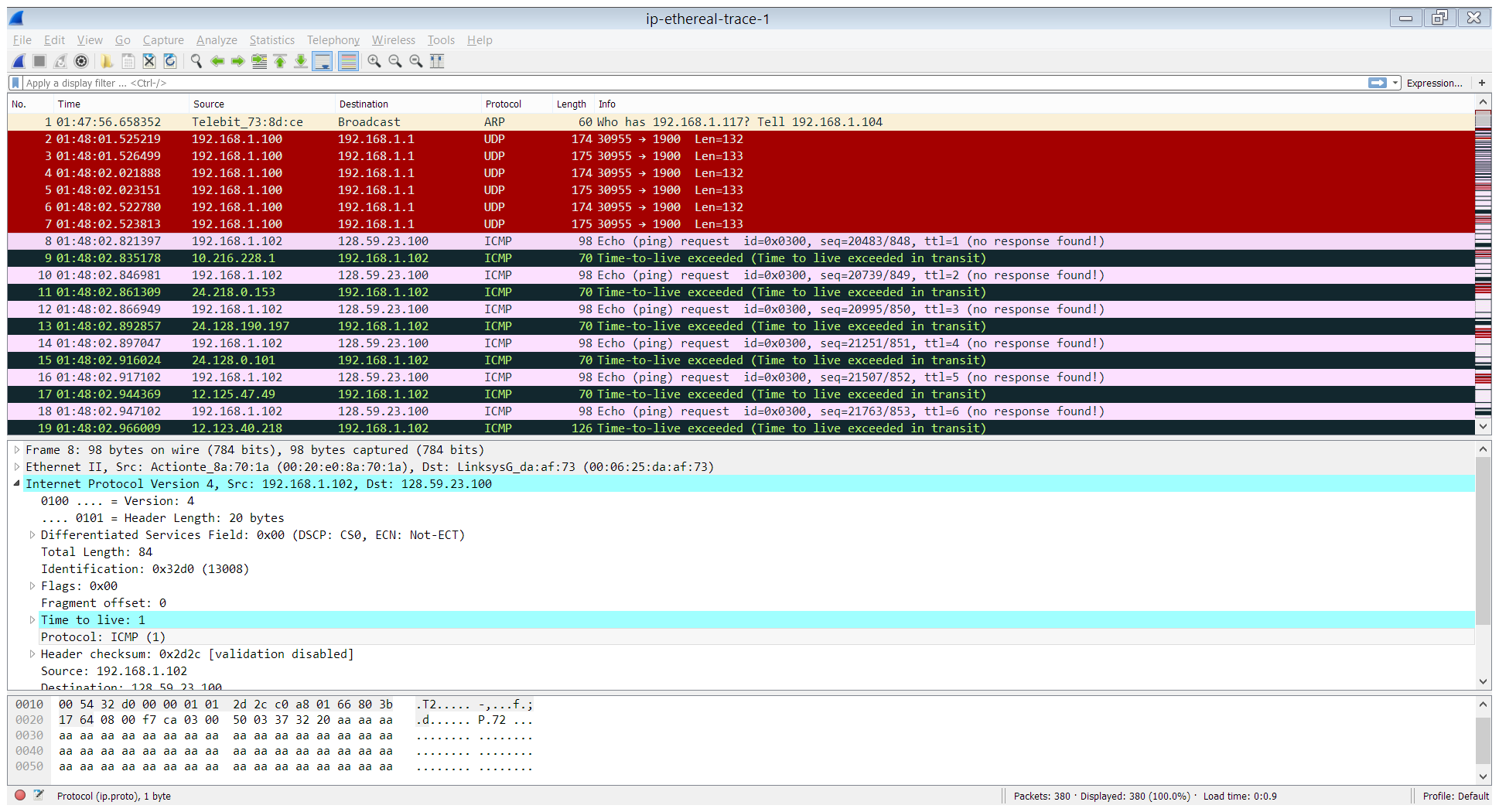
**Wireshark Lab 6**

**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?**

****

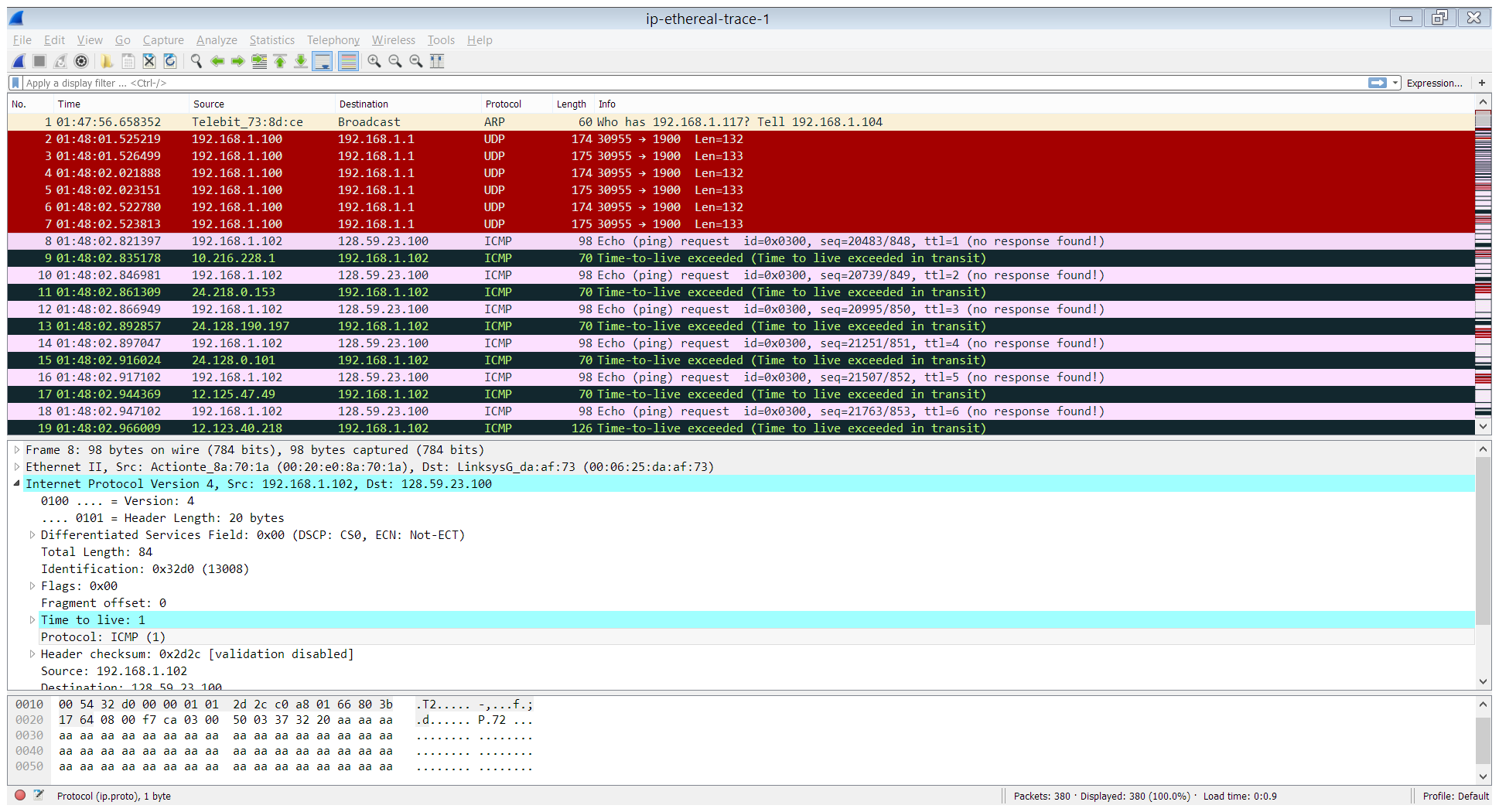
The IP address of my computer is 192.168.1.102

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

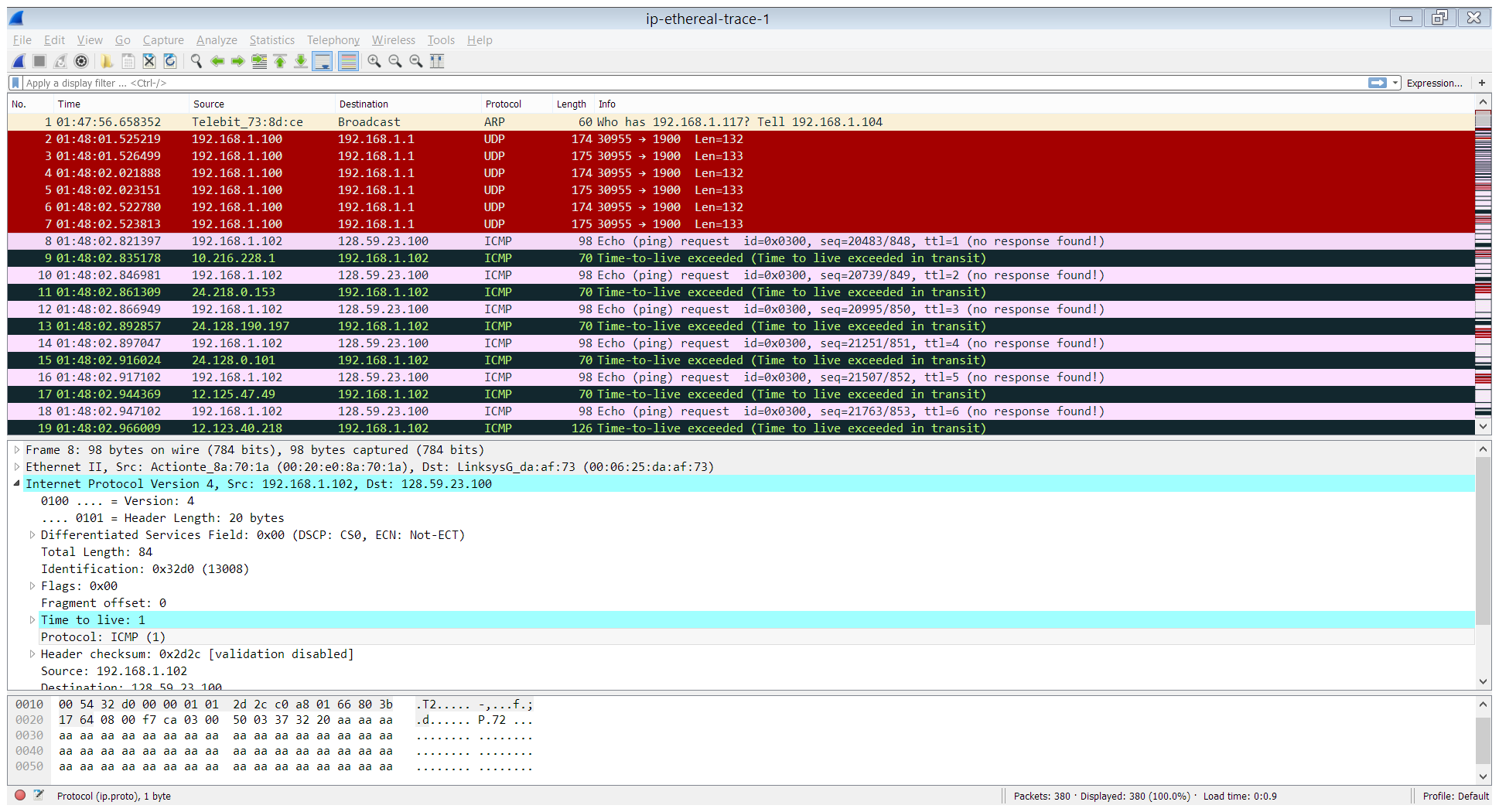
****

The upper layer protocol is ICMP

**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.**

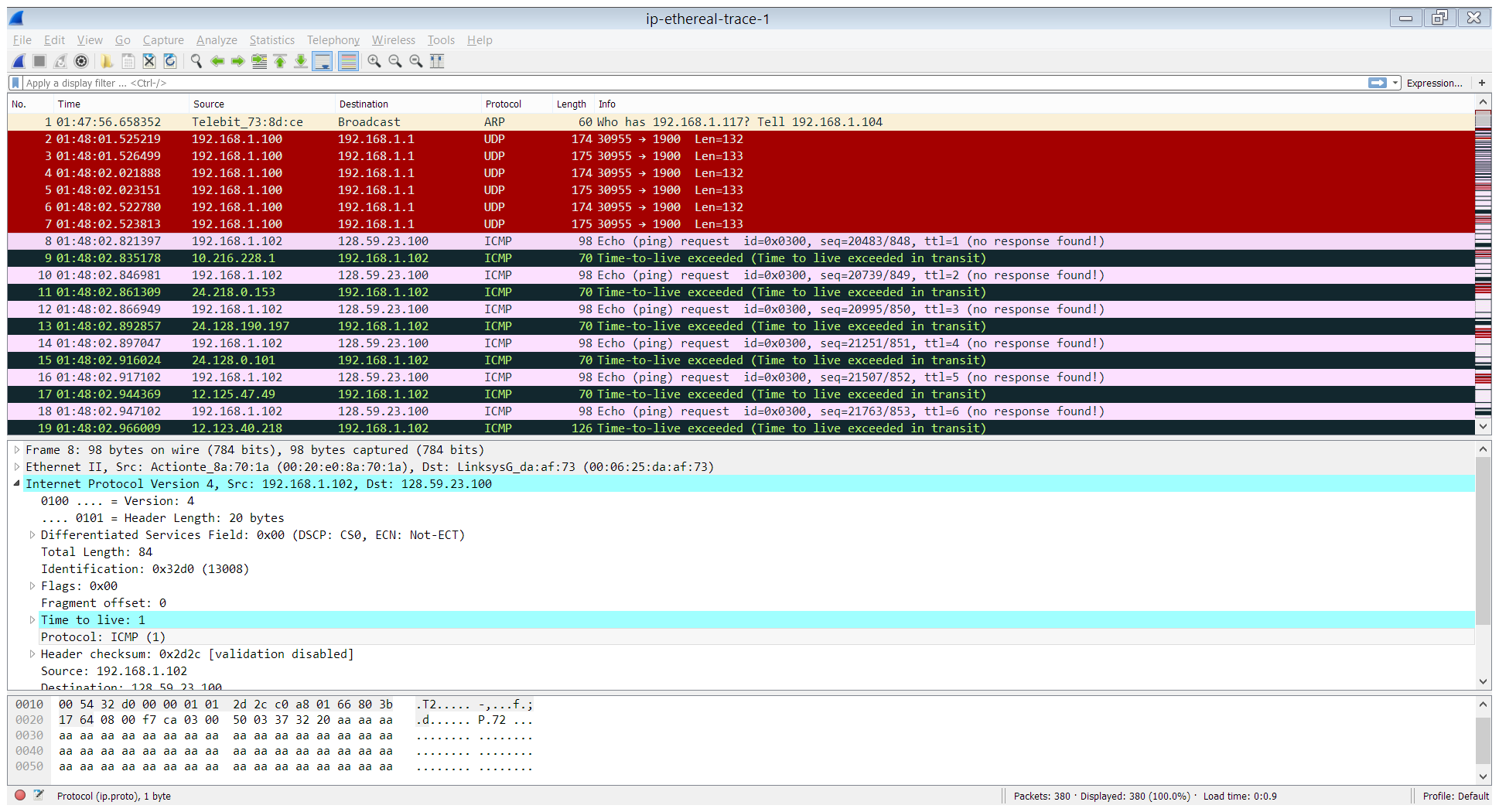
****

There are 20 bytes in the header.

****

If the total length is 84 bytes then the payload byes should be 64 bytes.

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

****

No, none of the fragment bits are set.

**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 field changes every time.

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

Src and Dest ip addresses, header and payload length, are all constant. TTL must obviously change, so must the checksum, since it is calculated based on the bytes in the IP layer, since TTL changes, so must the checksum.

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

The identification field seems to be in sequential order.

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

0x0000

And TTL is 22

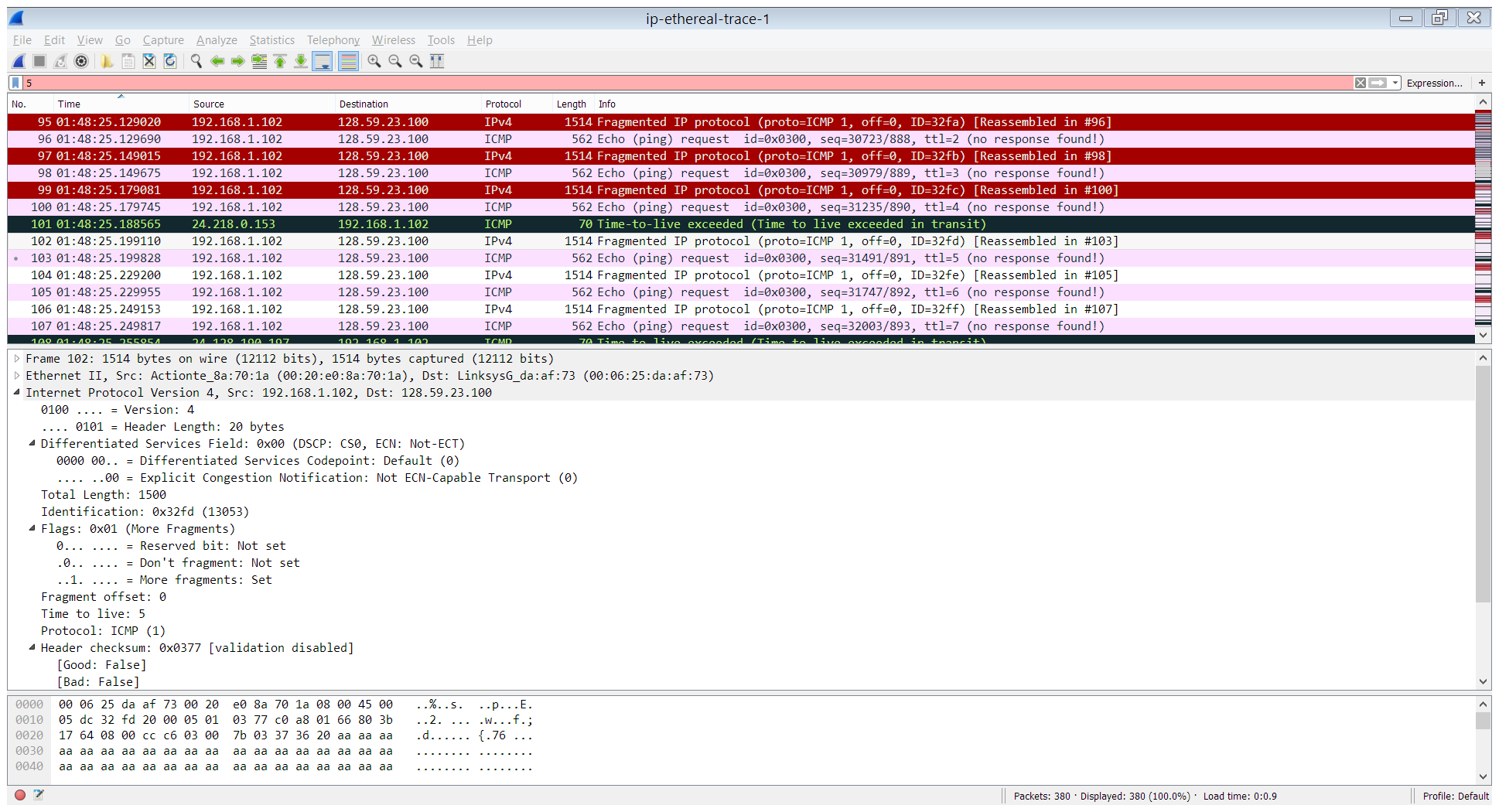
**9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?**

No, they sometimes change and I have no idea why.

**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

**11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented?**



The more fragment bit is set.

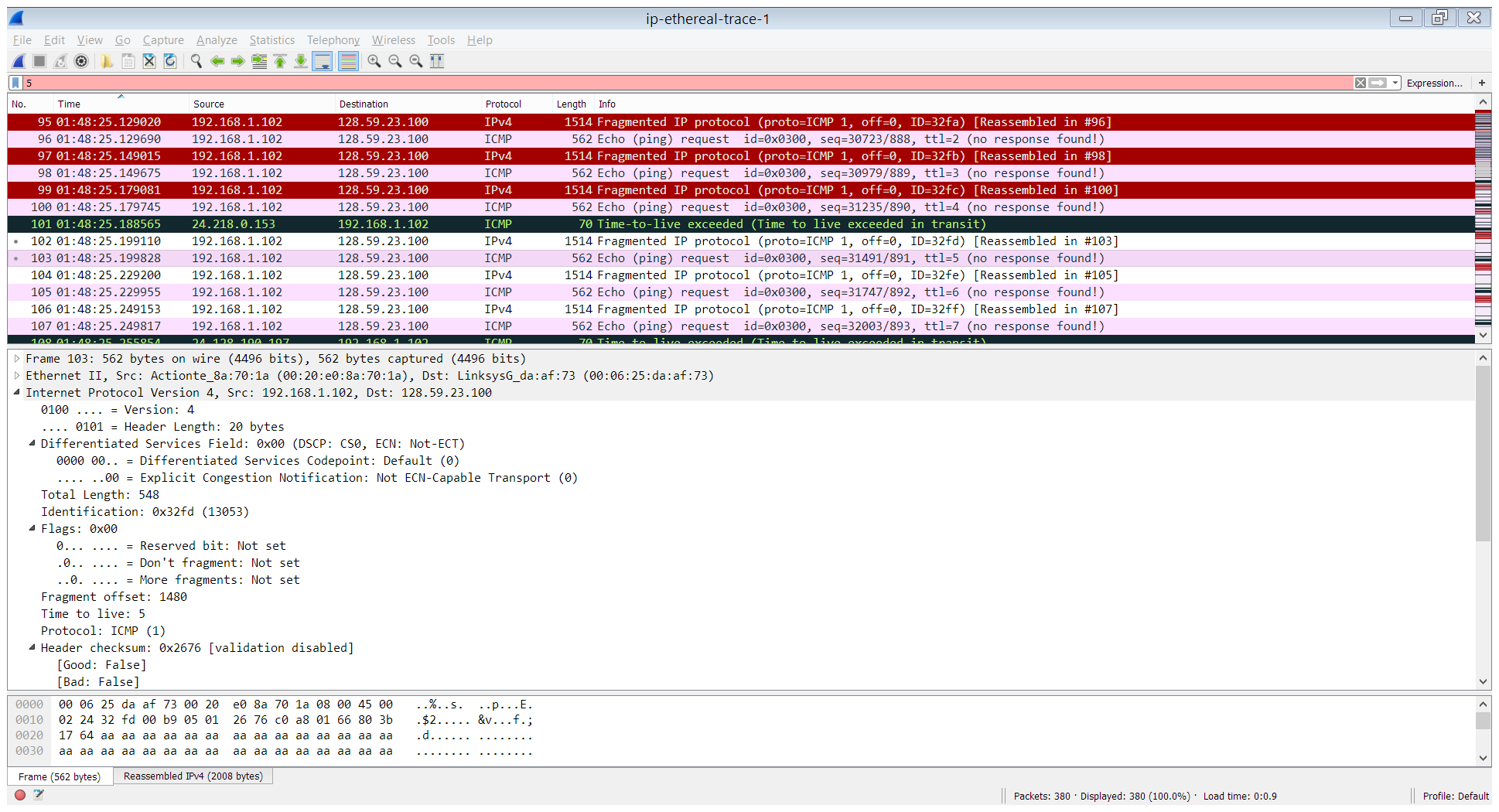
**What information in the IP header indicates whether this is the first fragment versus a latter fragment?**

The fragment offset is at 0

**How long is this IP datagram?**

The total length of this datagram is 1500 bytes.

**12. 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?**



**What information in the IP header indicates that this is not the first datagram fragment?**

The fragment offset is not 0, meaning this datagram is just part of a whole.

**Are the more fragments? How can you tell?**

There are no more fragments because the *More Fragments* bit is not set.

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

The checksum, total length as well as the fragment bit was changed in the second fragment compared to the first.

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

There is not 3 fragments.

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

The checksum, total length as well as the fragment bit was changed in the fragments.