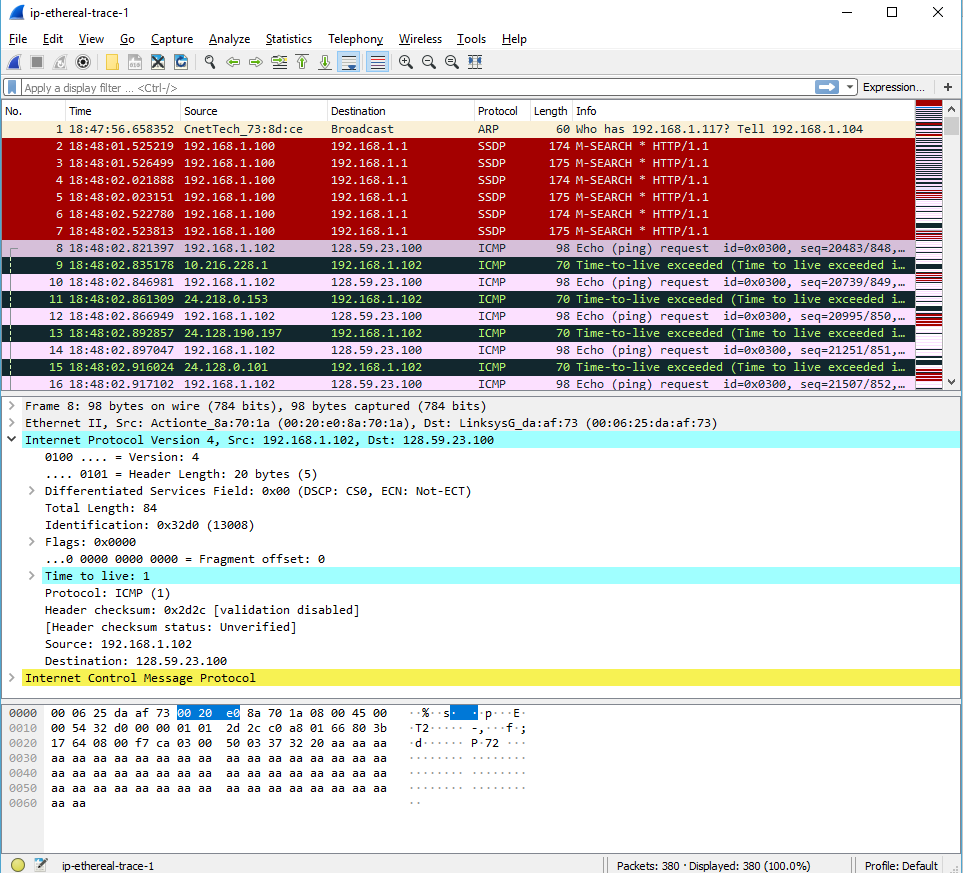
CS 372 – Lab 4

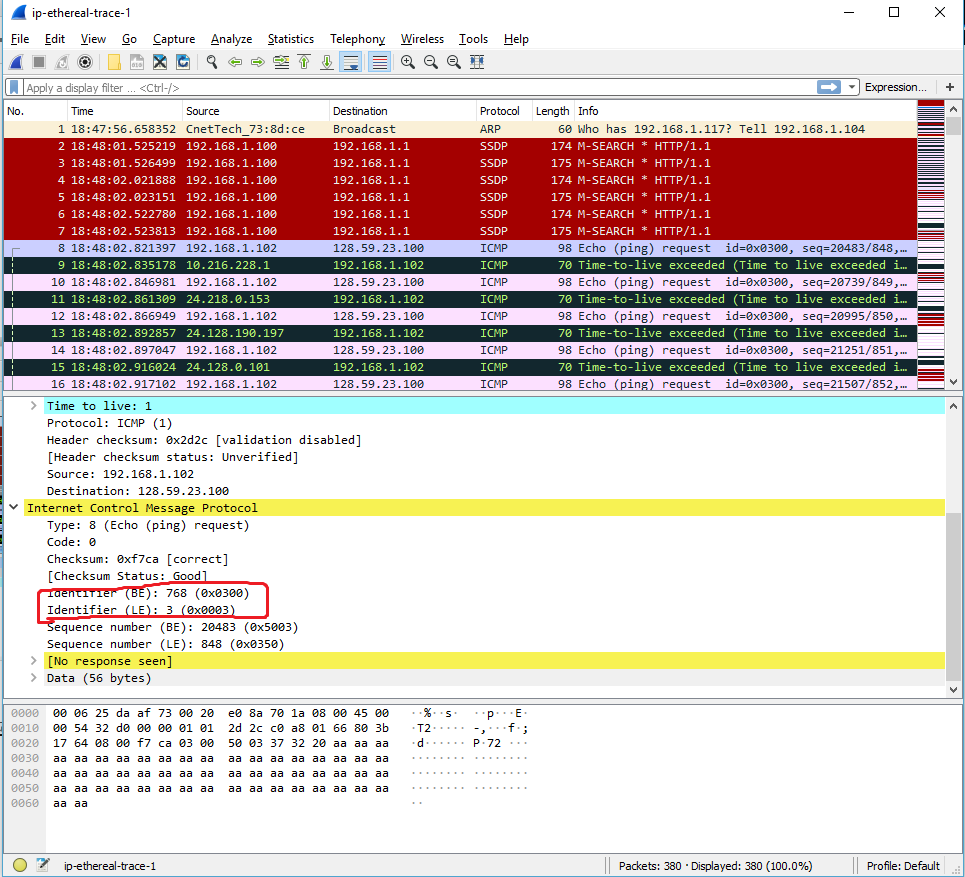
1. Select the first ICMP Echo Request message sent by your computer and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

**My IP address is 192.168.1.102**

****

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

**The value of the upper layer protocol field is ICMP (0X03)**

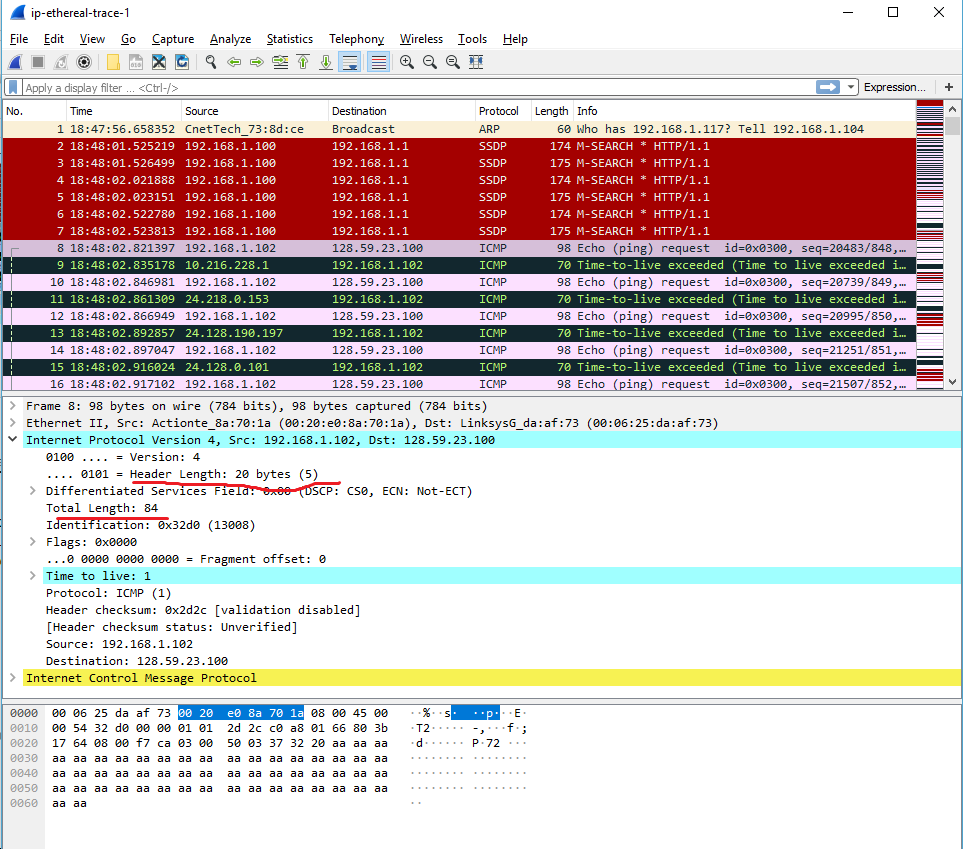
****

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.

**There are 20 bytes in IP header as shown in the screenshot, and the total length of the packet is 84 bytes.**

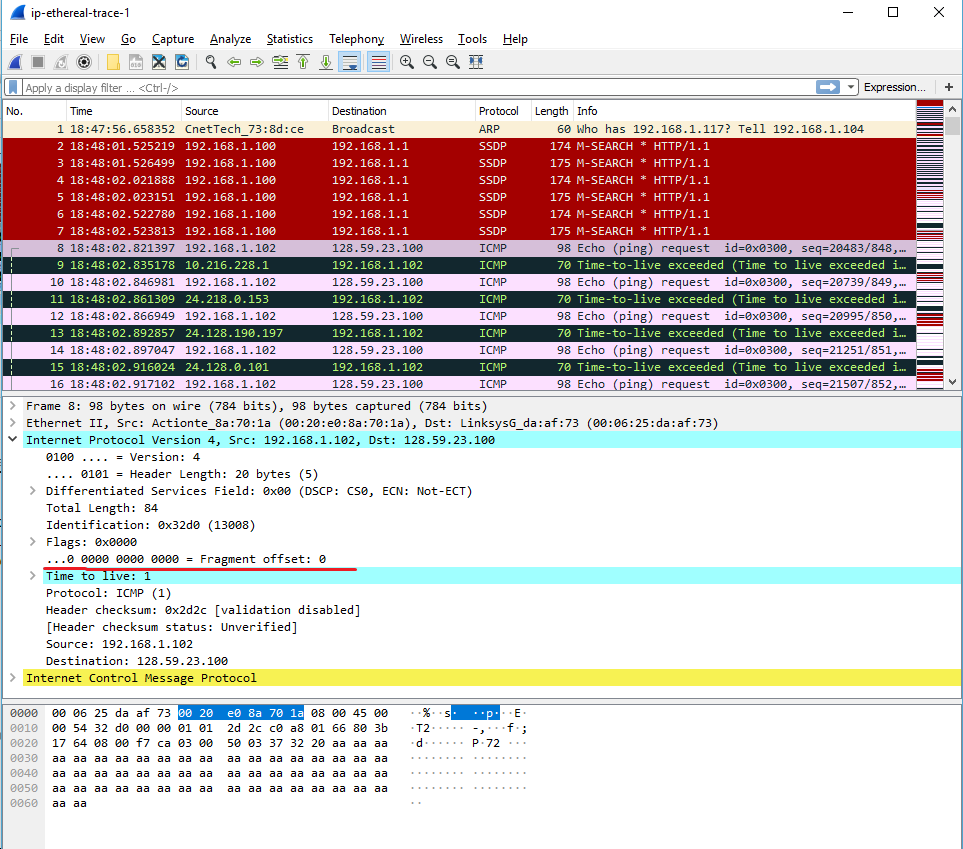
**(84-20=64).**

**That leaves 64 bytes for the payload of the IP datagram.**

****

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

**The fragment offset is set to 0, therefore, the packet has not been fragmented.**

****

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?

**The header checksum, time to live, and the Identification section change from each datagram to the next.**

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

**The following fields stay and must stay constant:**

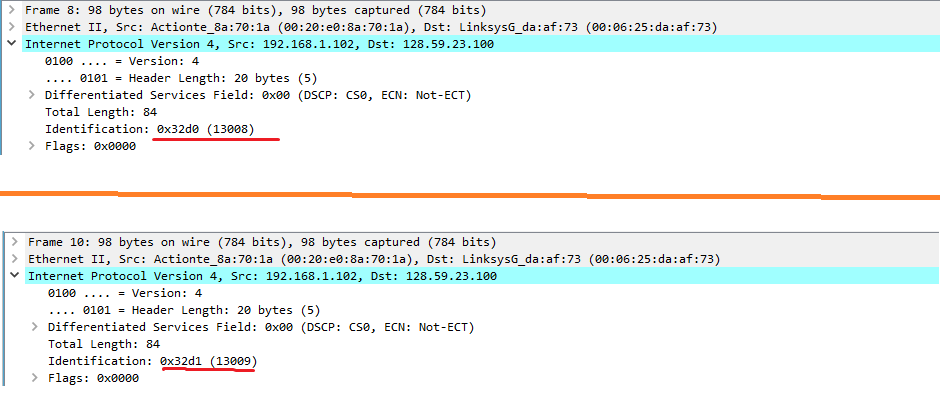
* **Version (IPv4 always used)**
* **Header length (doesn’t change since we are always using IPv4)**
* **Source IP (my computer’s IP address doesn’t change)**
* **Destination IP (gaia.cs.umass.edu’s IP address doesn’t change)**
* **Differentiated services (same protocol every time)**
* **Upper layer protocol (always use ICMP)**

**The following fields must change:**

* **The header checksum (header changes from each datagram to next)**
* **Identification (incrementing, each IP datagram has a different ID)**
* **Time to live (incrementing, as this is how trace route works)**

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

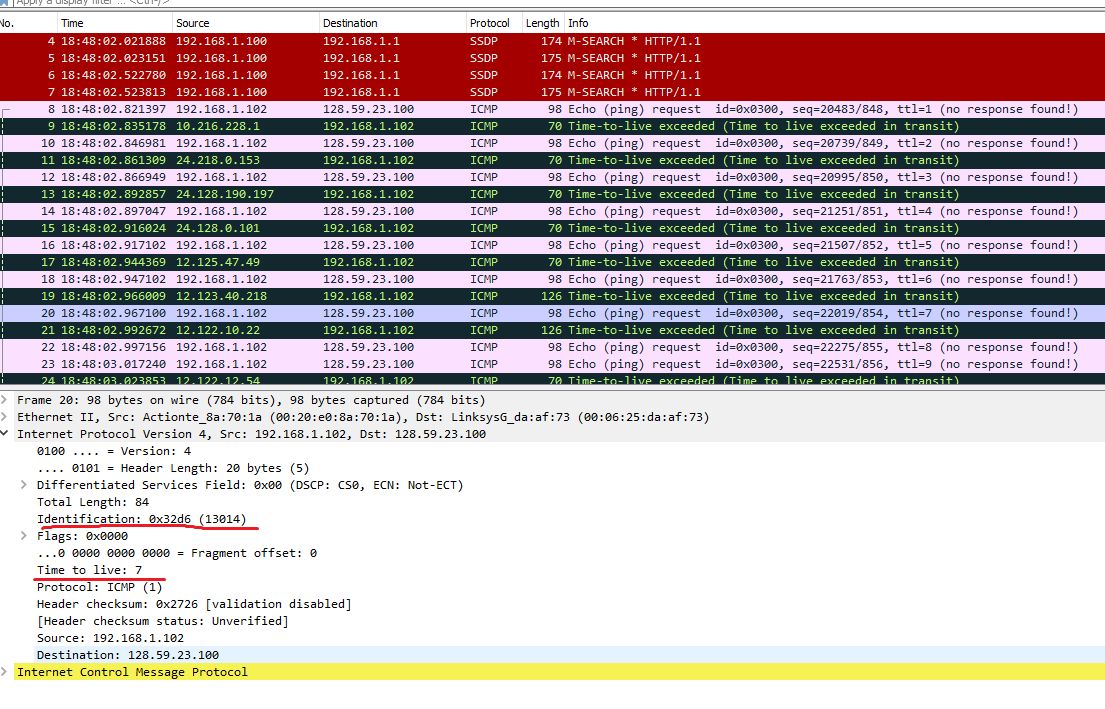
**The pattern in the identification field is that the field increases by 1 in each strand of echo requests.**

****

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

**Identification: 13014**

**TTL: 7**



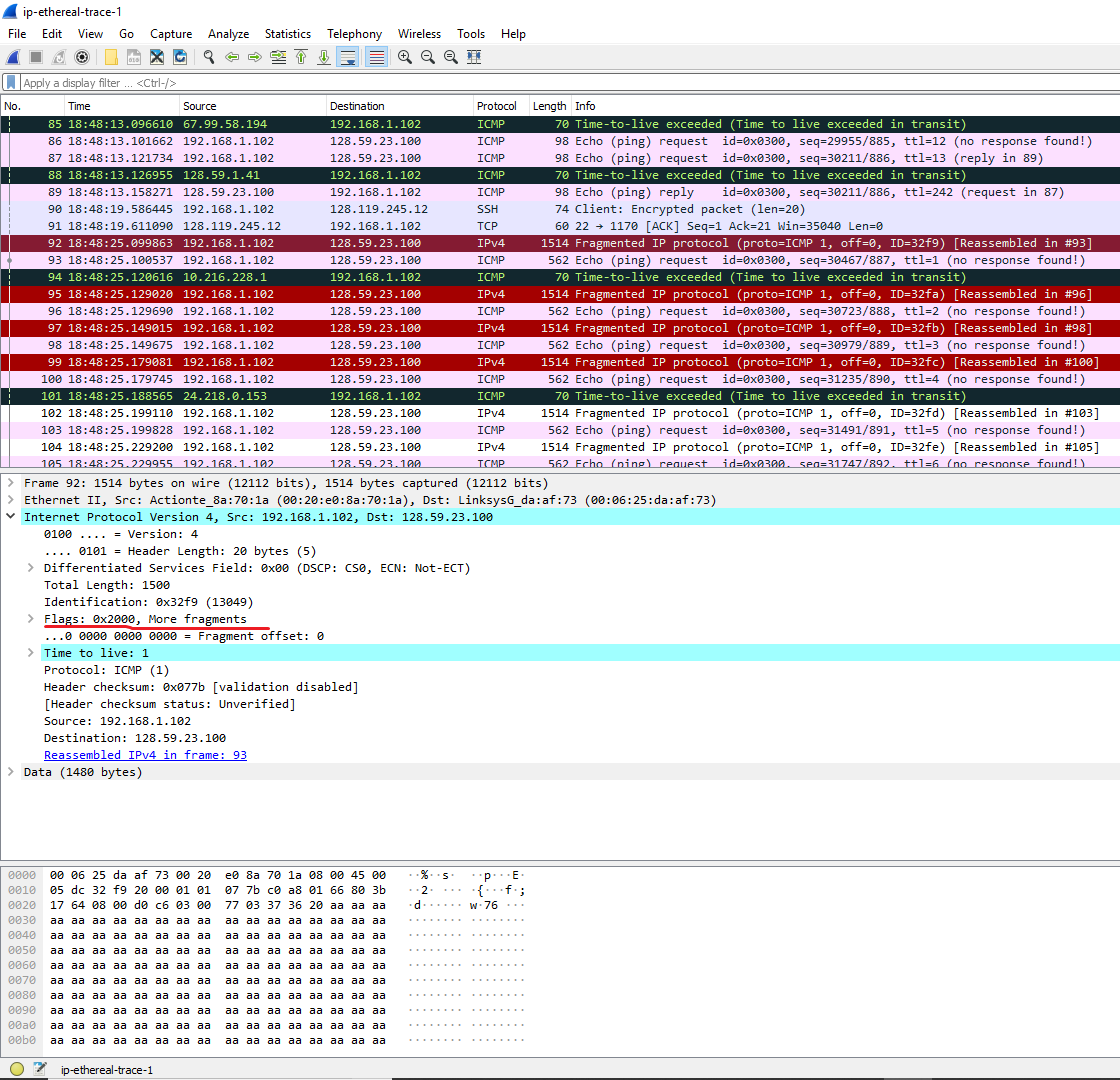
1. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

**The Identification field changes from all the replies because this field must have a unique value. If they (2 or more replies) have the same value, then the replies must be fragments of a bigger packet.**

**The TLL field does not change because the time to live to the first hop router is always the same.**

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?

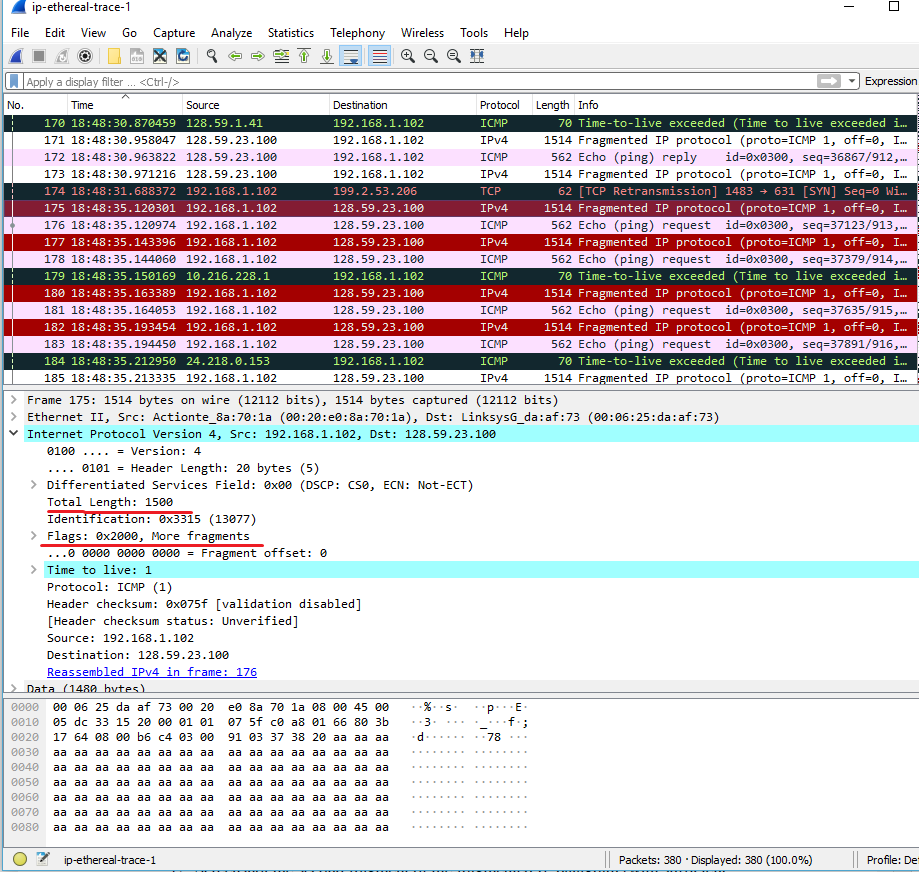
**Yes, that message has been fragmented across more than one IP datagram.**

****

1. 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?

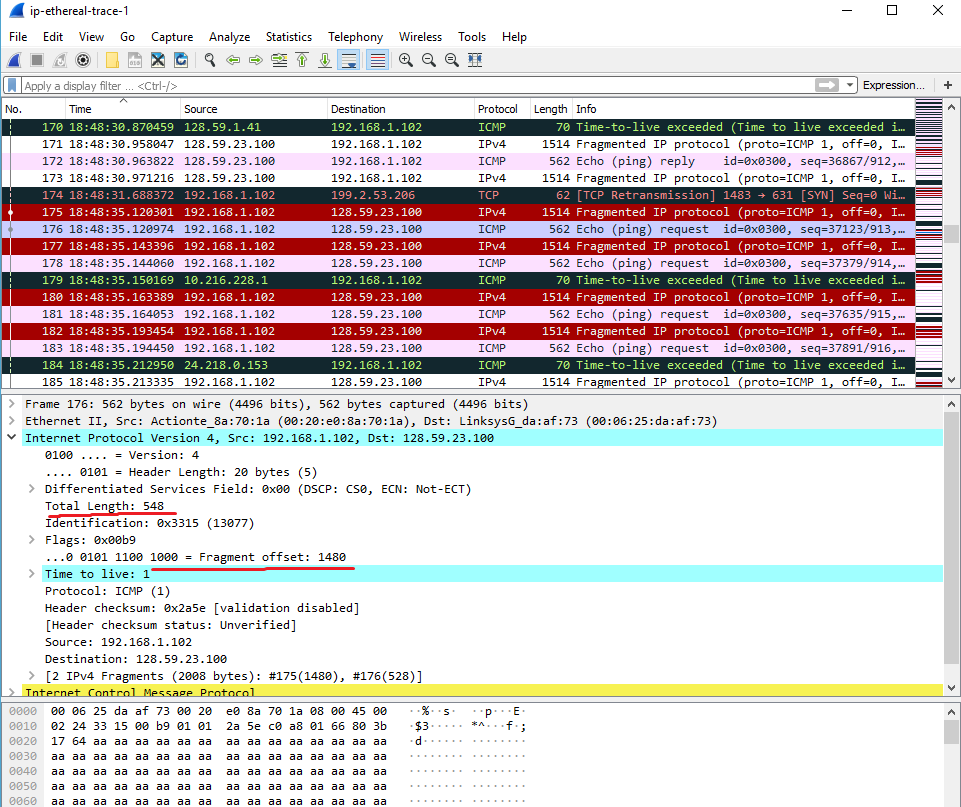
**The fact that the flag is set for more segments shows that the datagram has been fragmented. The fragment offset is set to 0 indicates that this is the first fragment rather than a latter fragment where that value is set to (1480).**

**The datagram has a total length of 1500.**



1. 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 second fragment is obvious because it now has a fragment offset of 1480. There are no more fragments because it no longer has a flag set for more fragments.**



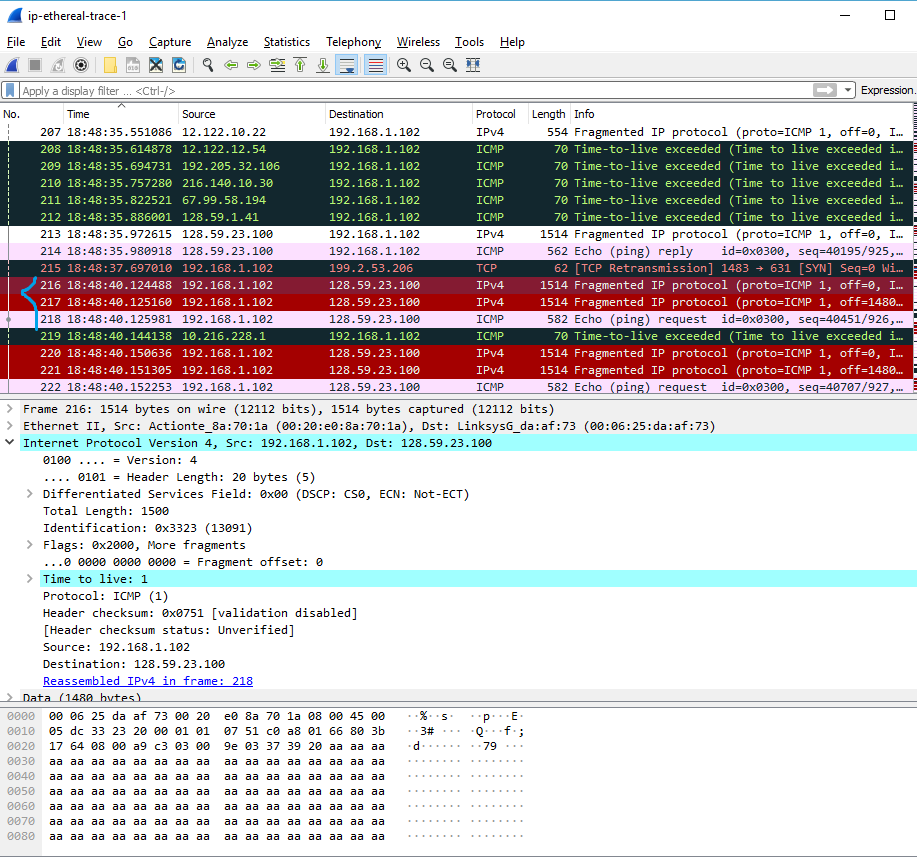
1. What fields change in the IP header between the first and second fragment?

**The fields that changed were:**

* **Length**
* **Flag set**
* **Fragment Offset**
* **Header checksum**

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

**3 fragments were created.**



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

**The fields that change are the fragment offset (0, 1480, 2960) and checksum. The first 2 packets also have lengths of 1500 and more fragment flags set, while the last fragment is shorter and does not have a flag set.**