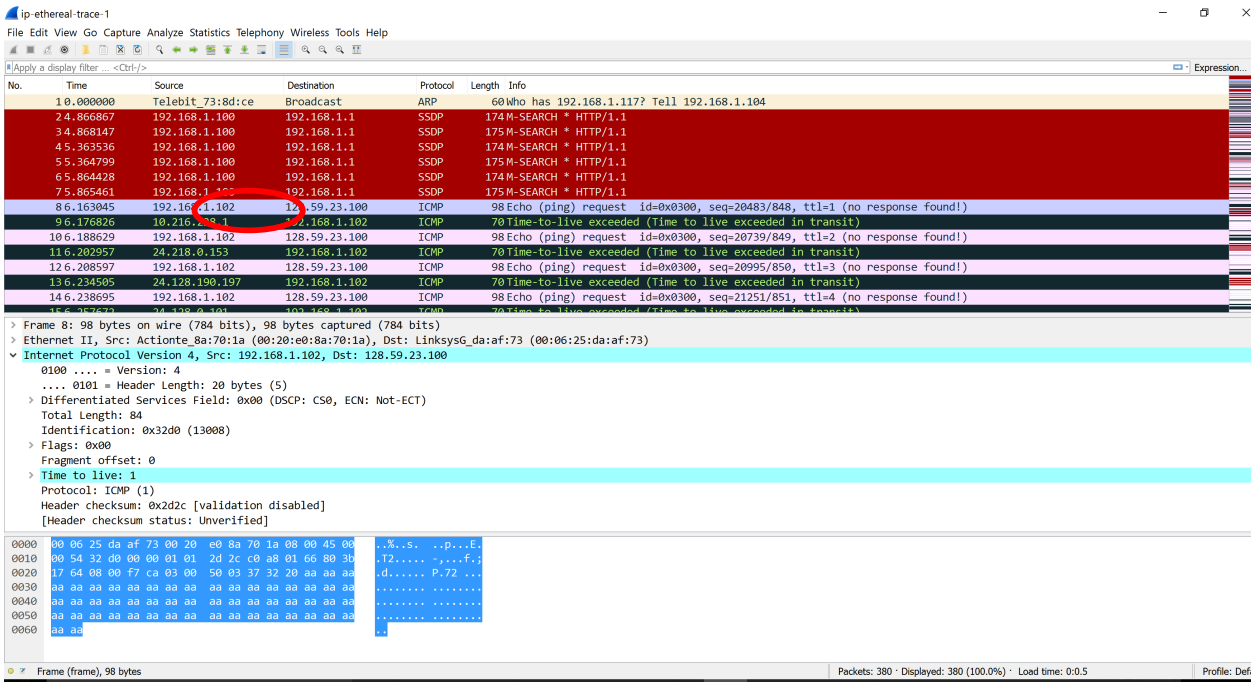
Wireshark IP



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?**

   192.168.1.102

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

   ICMP (1)

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.**

   `.... 0101 = Header Length: 20 bytes (5)`

   Header length: 20 bytes. There are 20 bytes in the IP header which leaves 36 bytes for the payload of the IP datagram because we were sending a packet of length 56 bytes.

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

   ```
   Identification: 0x32d0 (13008)
   Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
   Fragment offset: 0
   .... 0101 = Header Length: 20 bytes (5)
   ```

   No. Fragment offset: 0

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 header checksum, time to live and the identification changes from each datagram to the next.

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

   Fields that stay constant are the same as fields must stay constant: Version (Ipv4…), length of the header (ICMP packets), source IP(sending the same place), destination IP(contacting the same

place), upper layer protocol (because of ICMP), Differentiated Services (since all packets are ICMP they use the same Type of Service class).

Fields that must change: Header checksum (Header changes), identification (Each packets must have different IP), time to live (traceroute increments each subsequent packet)

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

   The pattern is that the IP header Identification fields increment with each ICMP Echo request.

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

```
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
```

Identification: 0x32d0 (13008)
TTL: 1

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?**

   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.

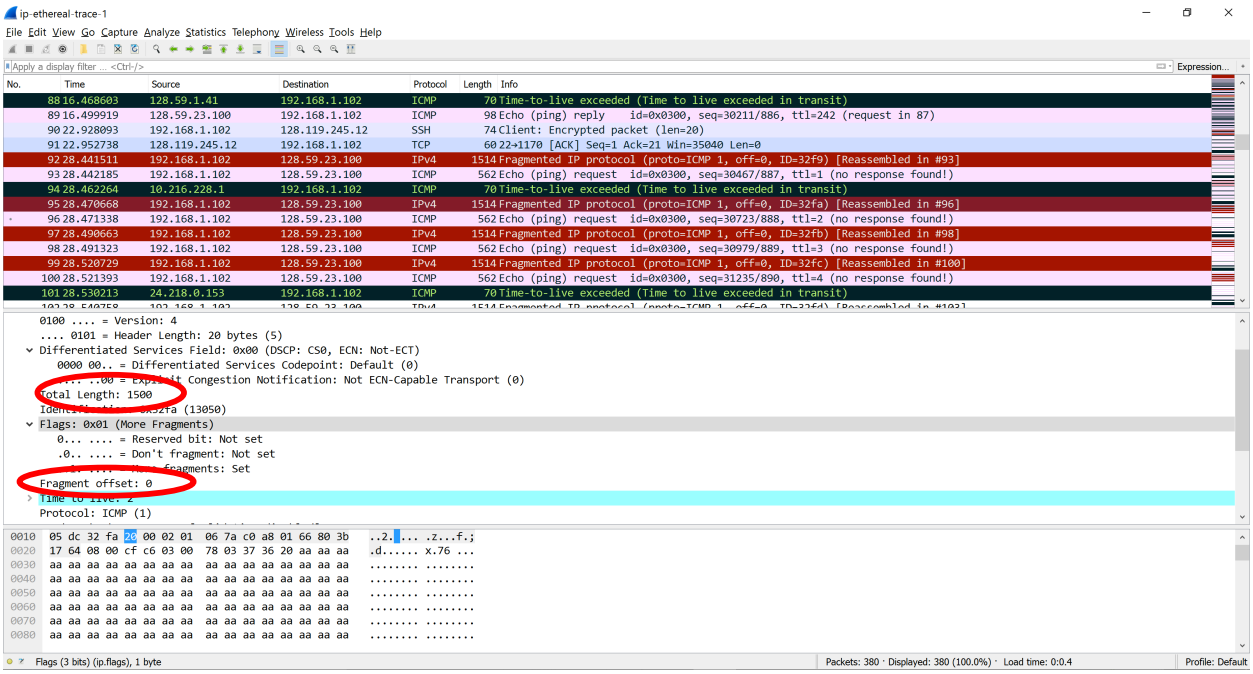
10. **Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?**

    Yes

11. **Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?**

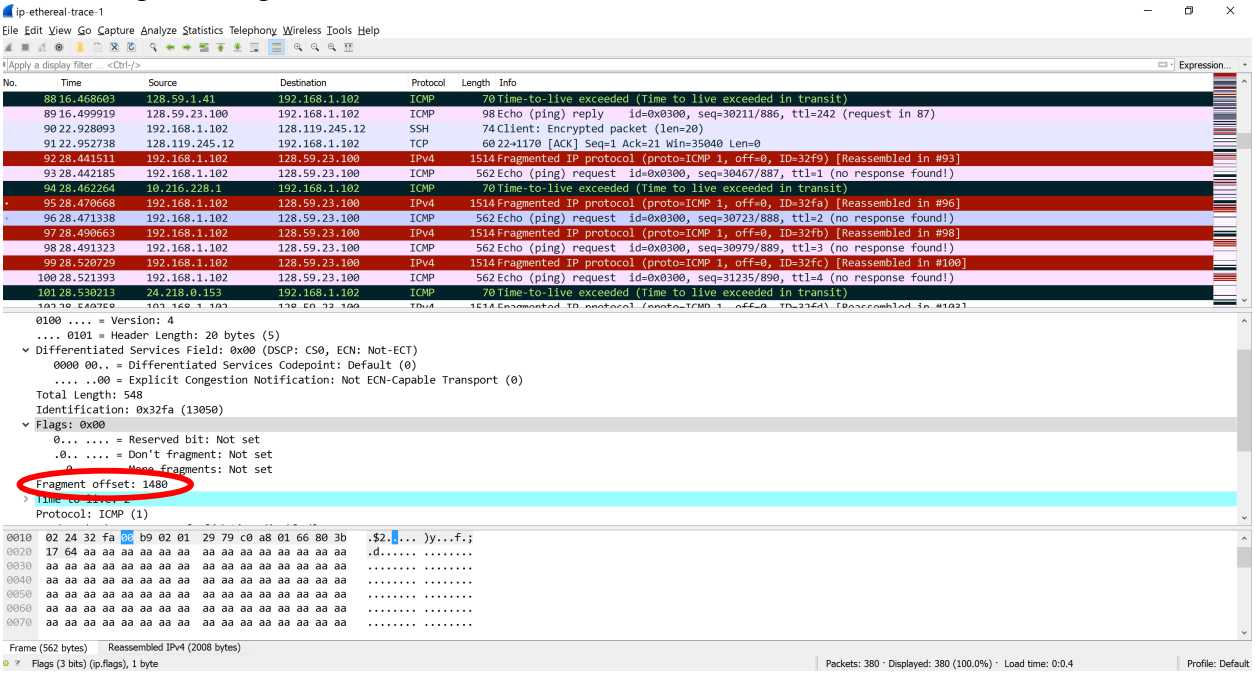
    The datagram has been fragmented because the flags bit for more fragment is set. The fragment offset is 0 so that this is the first fragment.

    The first datagram has the length of 1500.



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?**

    This is not the frist fragment because fragmet offset is 1480. This is the last fragment because fragment flags is not set.



13. **What fields change in the IP header between the first and second fragment?**
    The length, Flags set, Fragment offset, Header checksum
14. **How many fragments were created from the original datagram?**
    After switching to 3500, 3 fragments are created.
15. **What fields change in the IP header among the fragments?**
    The IP header fields that changed between all of the packets are: fragment offset, and checksum. The first two packets have the length of 1500 and more fragments set to 1, the last packet has the length of 540 and more fragments bit set to 0.