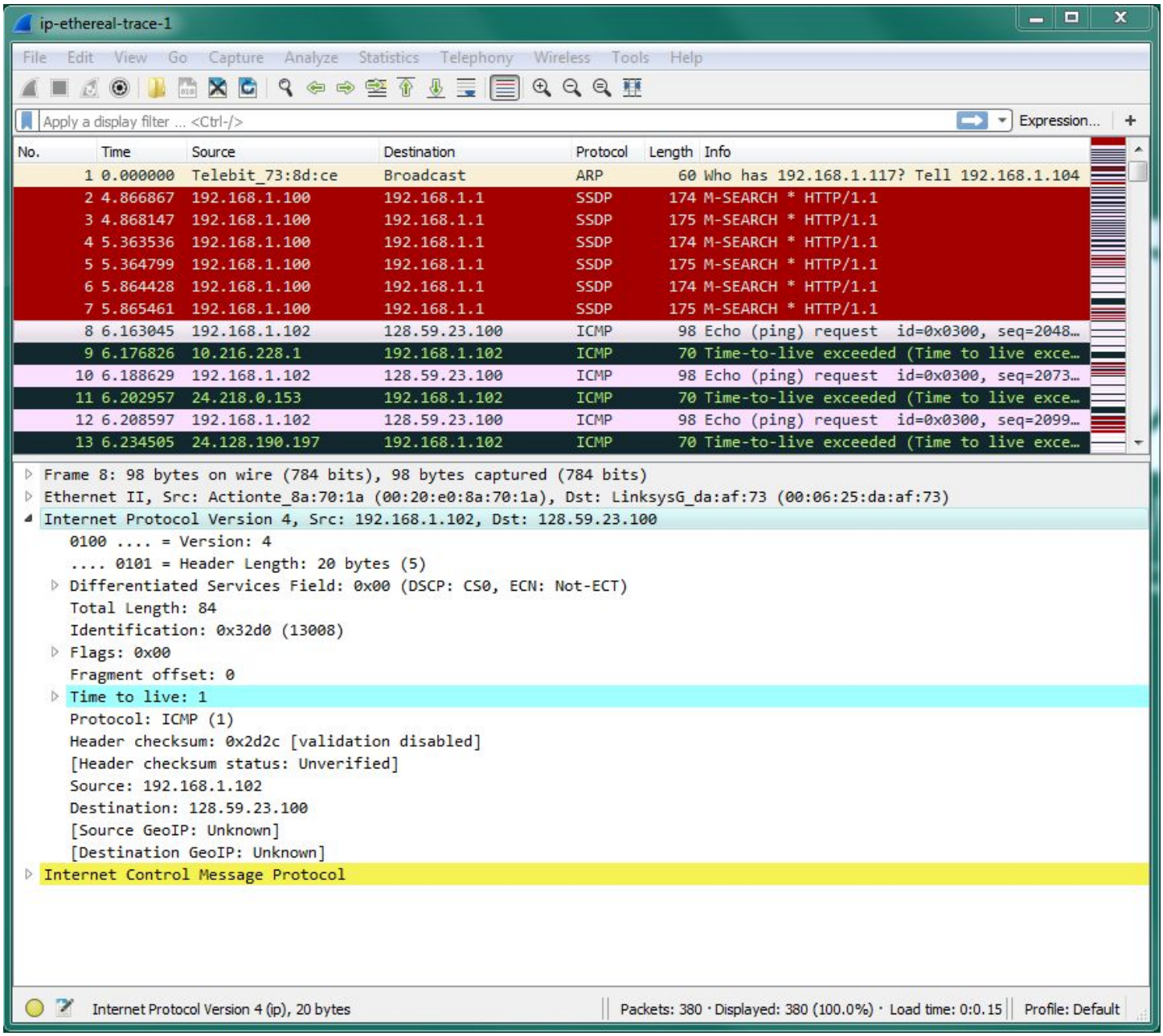
Sterling Price - U49743231
Matthew Kramer - U20891900
CNT 4004.001 - Wireshark Lab 3



1. What is the IP address of your computer?

The IP address of our computer is **192.168.1.102** according to the source field of the packet.

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

The upper layer protocol is **ICMP (1)**, or Internet Control Message Protocol.

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.

The IP header is **20** bytes long, according to the header length field. Since the total length of the packet is **84** bytes, and **20** of those bytes are the header, **84 - 20 = 64** bytes are in the payload.

Sterling Price - U49743231
Matthew Kramer - U20891900
CNT 4004.001 - Wireshark Lab 3

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

Since the fragment offset field is **`0`**, no fragmentation has occurred.

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, header checksum, and identification fields always change from one datagram to the next.

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

The fields that stay constant across IP datagrams are:

1. Source IP
   - because we are always sending from the same IP address.
2. Destination IP
   - since we are always sending to the same IP address.
3. Differentiated Services
   - as a result of all packets using ICMP, all packets must use the same type of service.
4. Header Length
   - as we are always using IPv4.
5. Upper Layer Protocol
   - because all packets use Internet Control Message Protocol.
6. Version
   - since IPv4 is consistent from packet to packet.

The fields the **must** stay constant are the same as above.

The fields that **must** change are:

1. Header Checksum
   - since the header changes in each packet.
2. Identification
   - because each packet must be uniquely identifiable.
3. Time to Live
   - Incremented by **`traceroute`** for each packet.

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

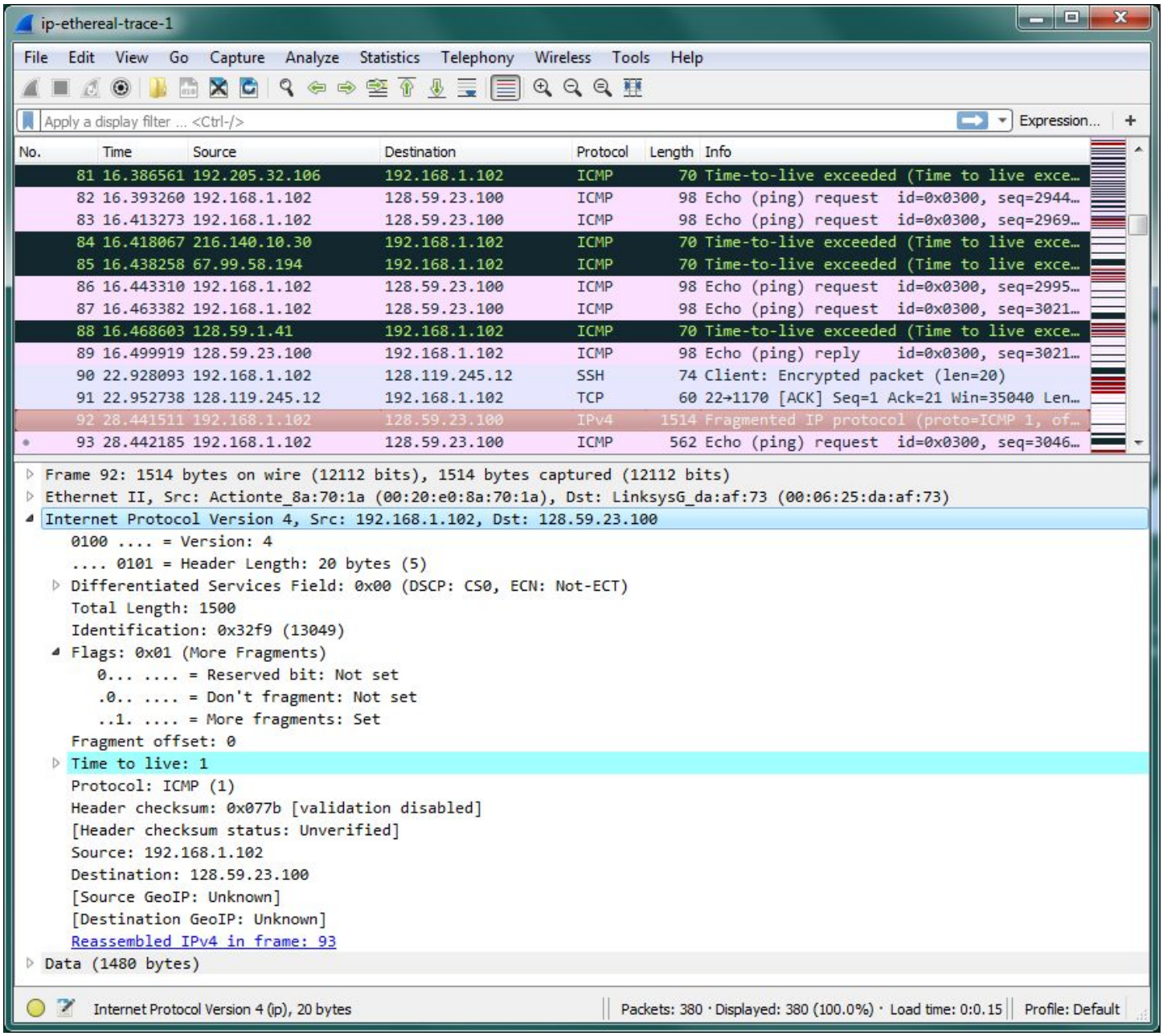
For every ICMP echo request that is sent, the IP header's identification field is incremented

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

The identification value is **`13000`** and the value in the time to live field is **`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?

For all ICMP TTL-exceeded replies, the identification field changes because it **must** be a unique value. Otherwise, if two datagrams have the same value within the identification field, then they can be considered as fragments of an encompassing datagram. On the other hand, the TTL field remains unchanged since the TTL for the nearest router stays the same.



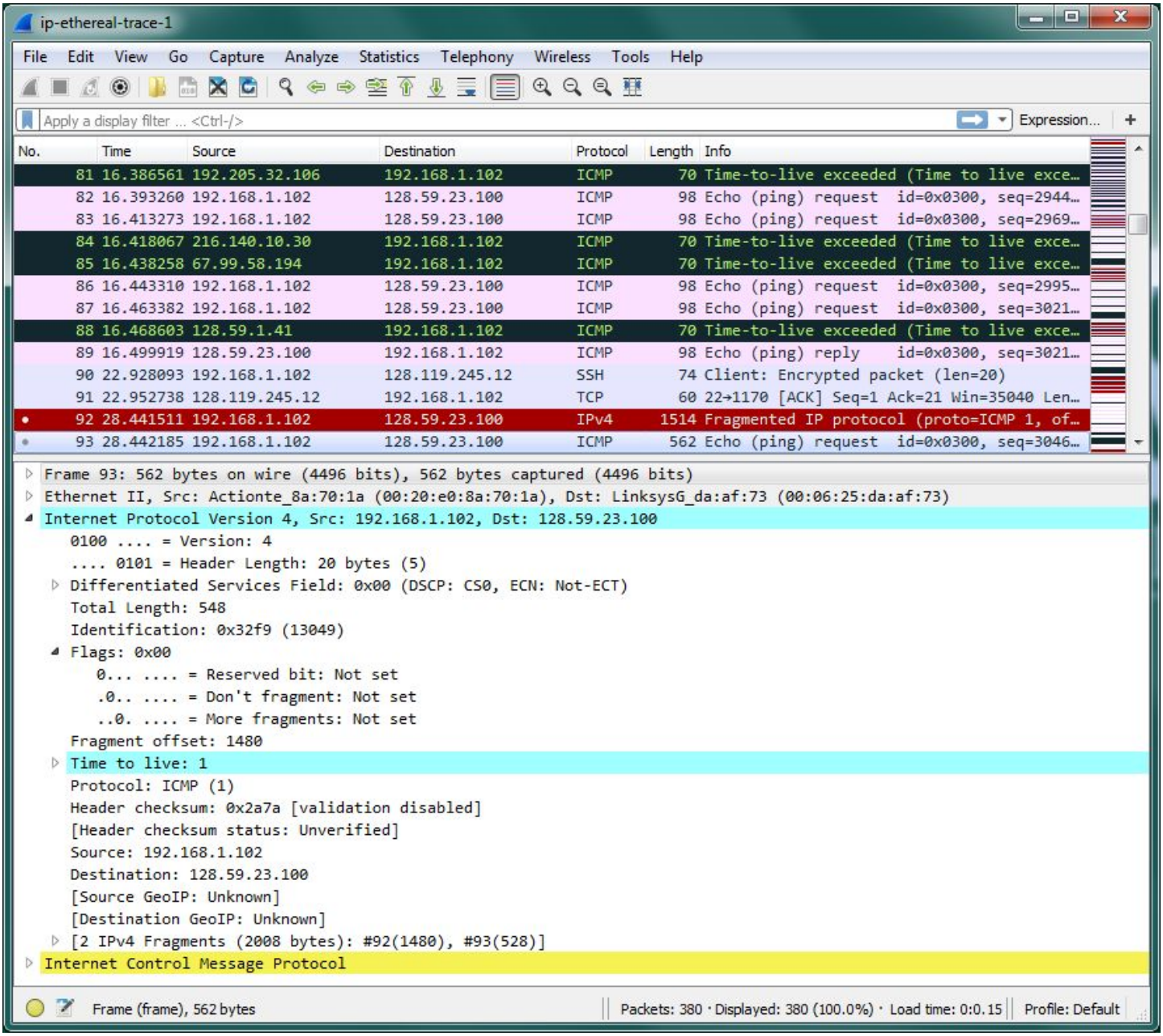
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Yes, it has.

Sterling Price - U49743231
Matthew Kramer - U20891900
CNT 4004.001 - Wireshark Lab 3

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?

We can tell that the datagram has been fragmented because the **`More Fragments`** flag has been set. Further, we can confirm that this is the first fragment because the **`Fragment Offset`** value is **`0`**. This IP datagram has a length of **`1500`**, according to the **`Total Length`** field.



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?

We can determine that this is not the first datagram fragment by the **`Fragment Offset`** field whose value is **`1480`**. Since the **More Fragments** flag is not set, this is the last fragment of the datagram.

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

    The fields that changed between the two fragments are: **`Header Checksum`**, **`Fragment Offset`**, **`Flags`**, and **`Total Length`**.

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

    With a packet size of **`3500`**, 3 fragments were created from the original datagram.

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

    The fields that change are the **`Fragment Offset`** and **`Header Checksum`**. The first two packets have **`Total Length`** values of 1500 and the **More Fragments** flag is set, while the third fragment has a shorter **`Total Length`** value of 540 and no flags set.