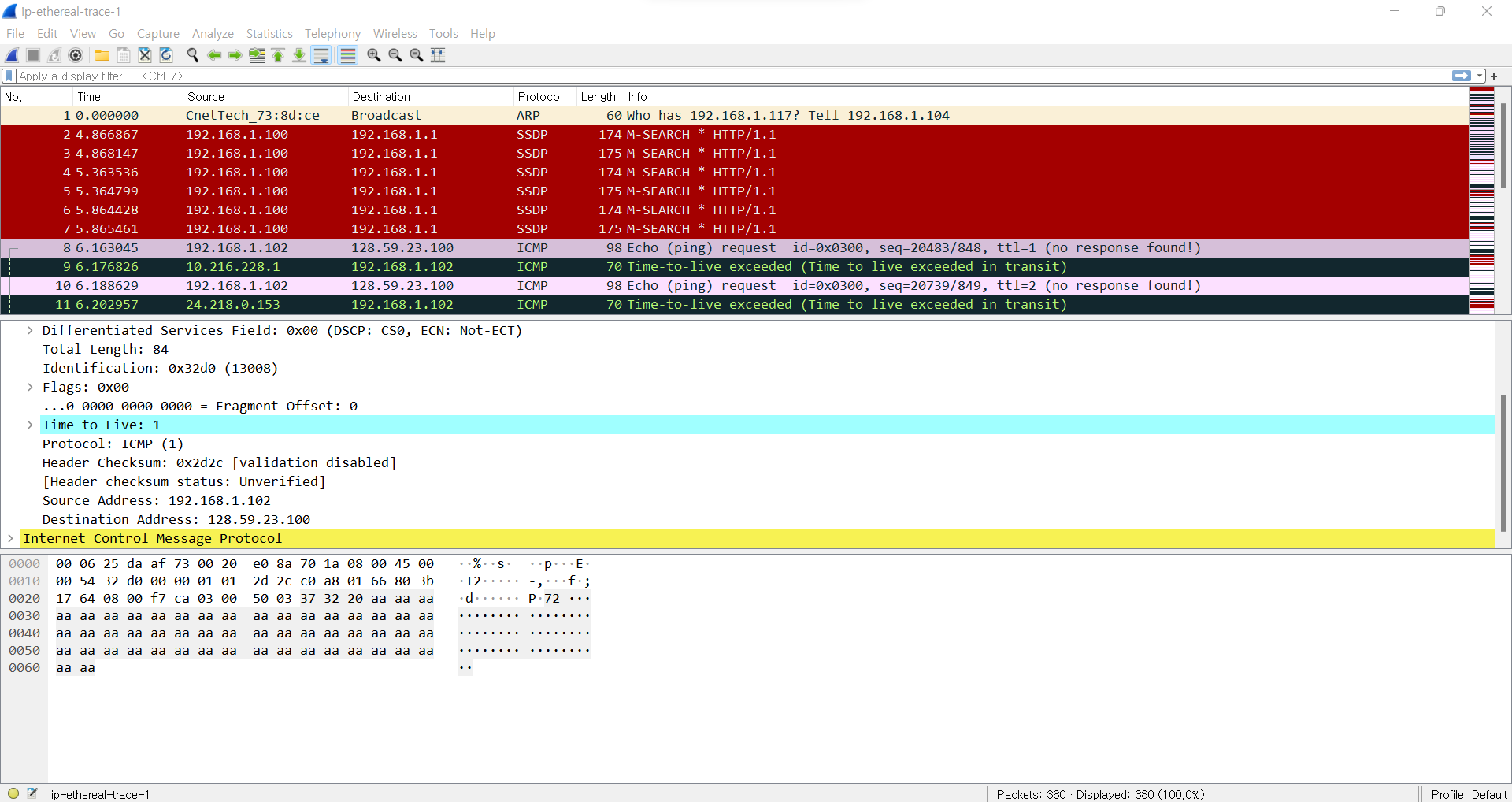
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

192.169.1.102

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

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.

IP header: 20 bytes

The Payload of IP datagram: 56 bytes (=84(total length)-20(header)-8(ICMP))

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

The data gram is not fragmented because ‘More fragments’ flag is not set.

텍스트이(가) 표시된 사진

자동 생성된 설명

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?

Identification field, Header Checksum, TTL, and sequence number always change.

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

Flags, Fragment offset, and Identifier stayed constant. “More Fragments” Field, Fragment offset, and Identifier must be constant. The reason is that ICMP message sent by my computer is not fragmented, and router has to know where the ICMP message came from. Identification field, Header Checksum, TTL, and sequence number must change. The reason is that router needs to distinguish multiple ICMP messages, and then send appropriate corresponding responds to my computer.

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

The higher byte of 16-bit value of the Identification field is 32 in hexadecimal e.g., 0x32\_\_ .

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

Identification Field: 0x9d73

TTL Field: 255

텍스트이(가) 표시된 사진

자동 생성된 설명

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?

Only the TTL field remained for all ICMP TTL-exceeded replies sent to my computer by the first hop.

The reason is to define the router where TTL is exceeded.

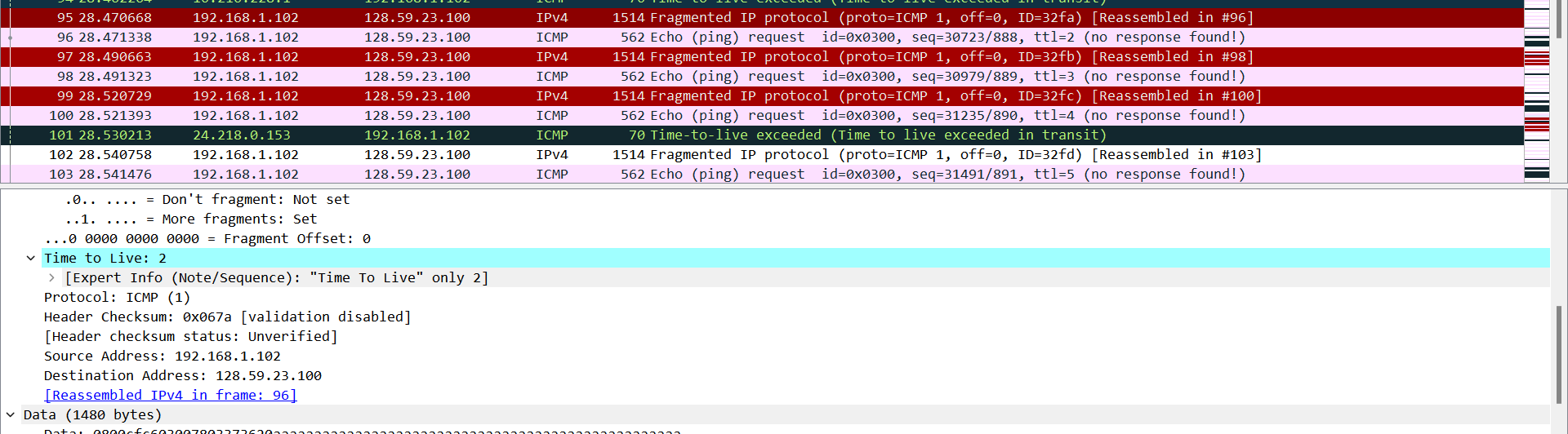
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.

Yes, the message had been fragmented into two IP datagram



11. 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?

IP header indicates that the datagram been fragmented by setting ‘More fragments’ flag. Moreover, IP header indicates the first fragment by writing ‘fragment offset’ as 0, and then the latter fragment by writing the byte where latter fragment should be placed. This IP datagram is 1514 byte long. (The payload is 1480bytes long)

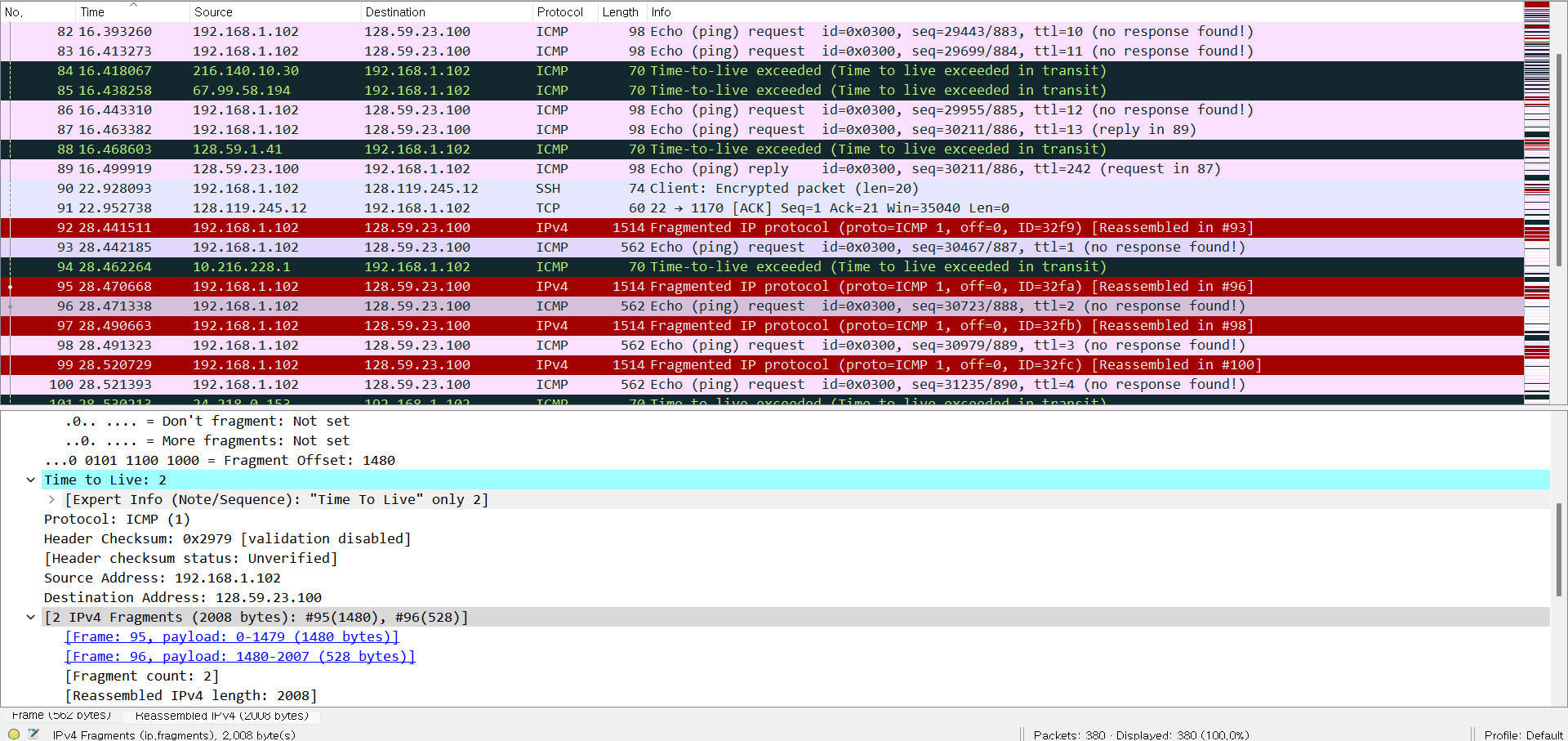


(Frame: 95)

12. 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 IP header indicates that this is not the first datagram fragment by writing a location after the first fragment(e.x.1480) in ‘Fragment Offset’, and IP header indicates there are more fragments by setting “More fragments” flag.

(If ‘More Fragments’ flag is cleared, then there is no more fragment after this fragment.)



(Frame: 96)

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

Flag, “Fragment Offset”, and Checksum changed in the IP header between the first and second fragment.

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

Three fragments were created from the original datagram.

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

Flag, “Fragment Offset”, and Checksum changed in the IP header among the fragments.