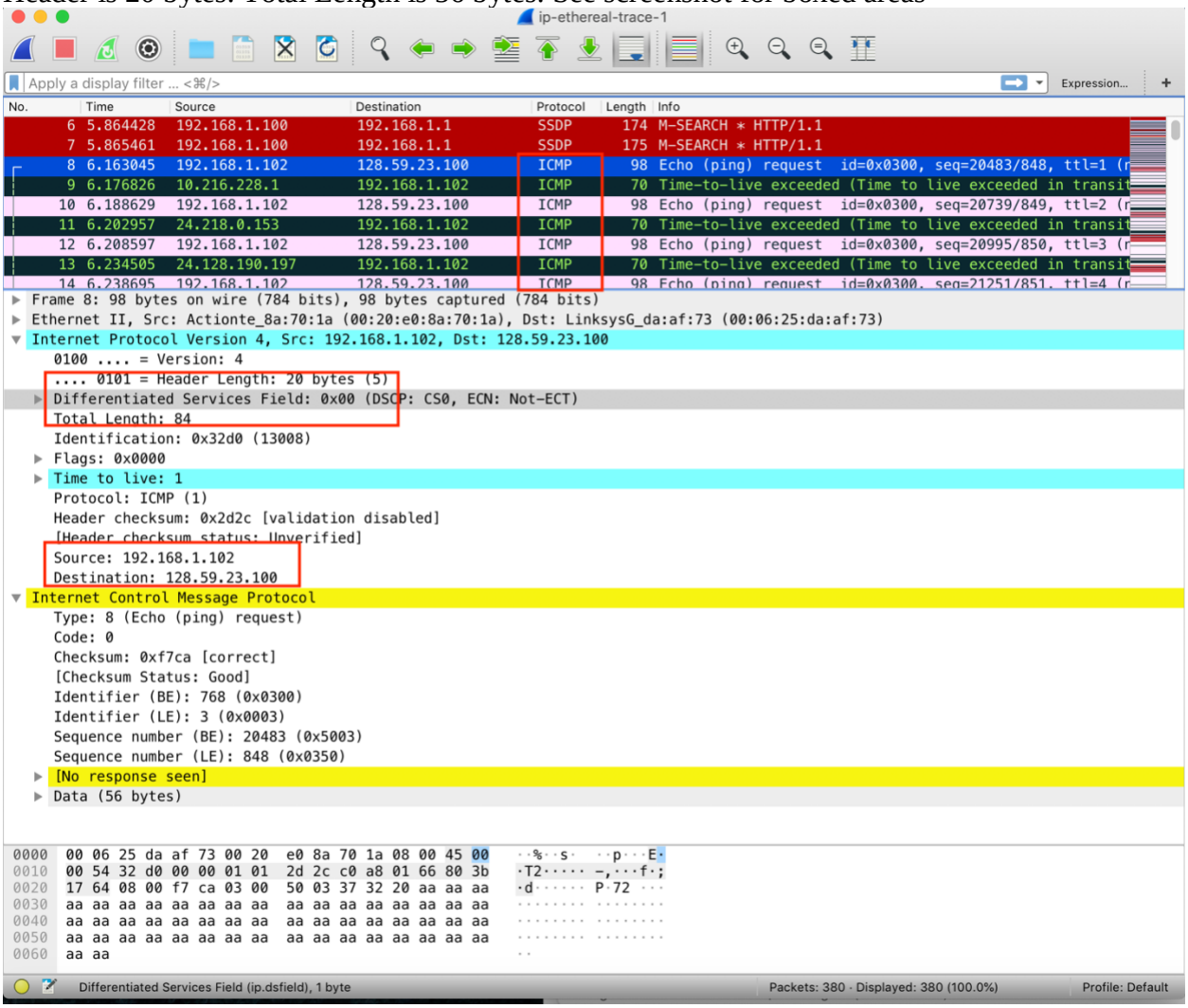
Arthur Liou
CS372
Lab 4

*Notes: I've attached my screenshots and boxed in red where I annotated my output.*
Using ip-ethereal-trace-1

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?
192.168.102
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.
Header is 20 bytes. Total Length is 56 bytes. See screenshot for boxed areas



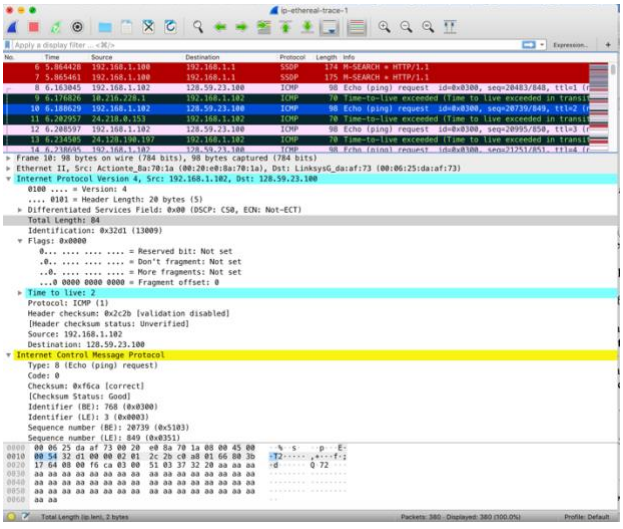
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
No, the fragments flag is not set.

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?
ID, time to live, and header checksum

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

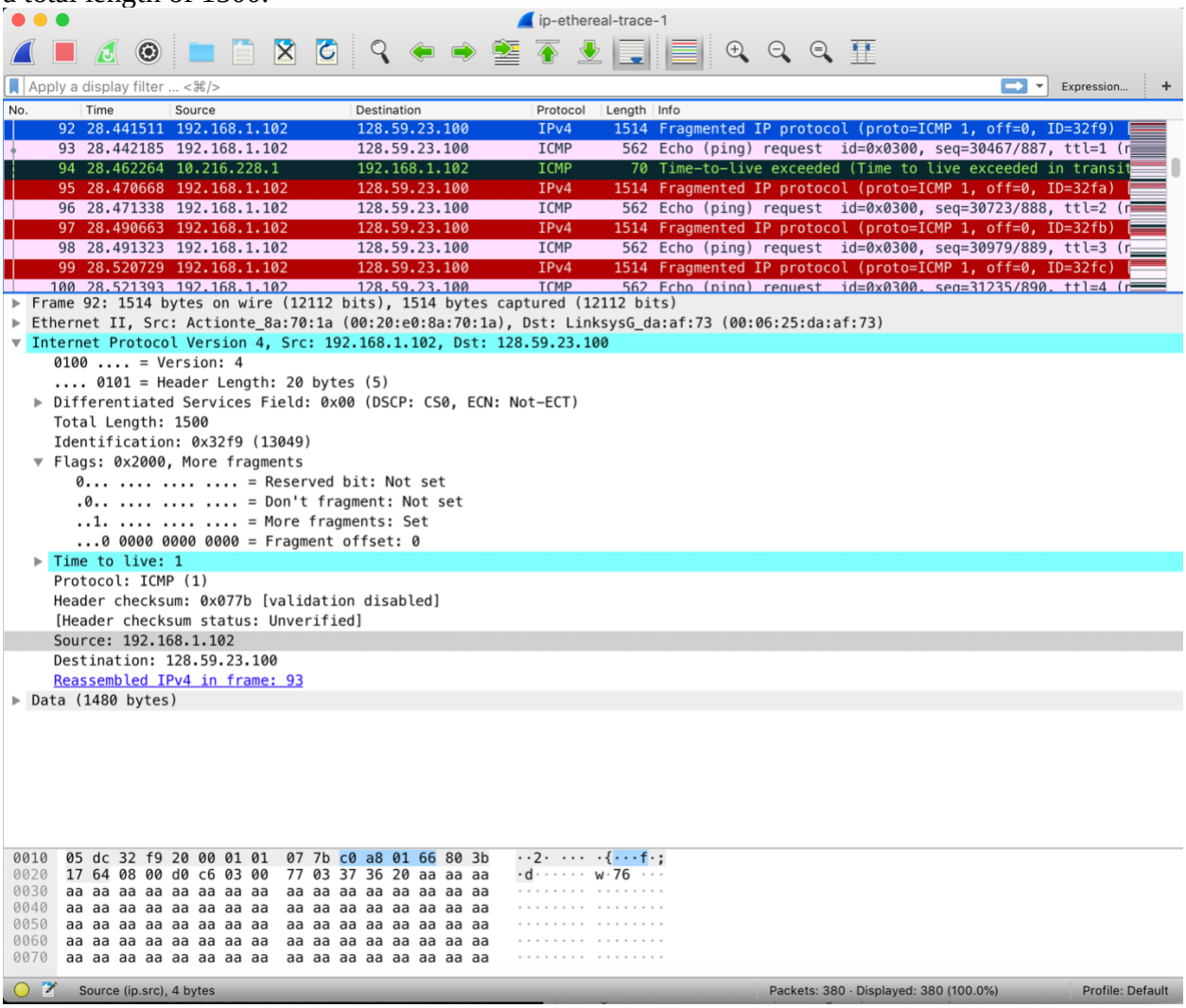
Constant: Version, header length, total length, flag, fragment offset, protocol, source, and destination.
Change: All else, header checksum, sequence number, frame #
The protocol, source, destination, and flag must stay constant since the same data is being transmitted from one device to another. The ID and time-to-live would change since they are attached to unique packets and not the data transmission. The header checksum changes since the header changes. Thus, the checksum would be different each time.

7. Describe the pattern you see in the values in the Identification field of the IP datagram
It will increment with each new call
8. What is the value in the Identification field and the TTL field?
ID: 0x32d1 or 13009
TLL: 2
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, the ID and TTL will change. The ID field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. 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, the message was fragmented. We can see the “fragmented IP protocol”

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?
The Flags bit for more fragments is set “More fragments: Set”, indicating that the datagram has been fragmented. Since the fragment offset is 0, this is the first fragment. This first datagram has a total length of 1500.




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 fragment offset is not zero. No, more fragments flag is not set

13. What fields change in the IP header between the first and second fragment?
Fields that changed are: total length, flags, fragment offset, and check sum.

14. How many fragments were created from the original datagram?
From the given lab file (ip-ethereal-trace-1), I found 7 fragments. However, if we act in according to the Lab instrcutions, we'd have 3.

15. What fields change in the IP header among the fragments?
Fields changed: total length, flags, fragment offset, and checksum