Vlad Predovic

CS 372  
Summer 2016

Lab 3: IP

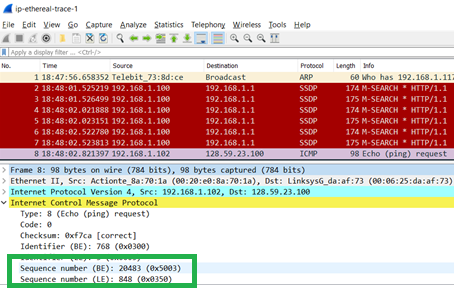
*NOTE: USED IP-ETHEREAL-TRACE-1 for homework*

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?

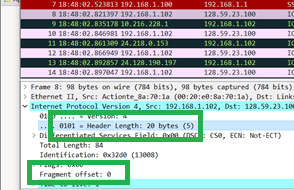
My computer: 192.168.1.102

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

The value in the upper layer protocol field is ICMP 0x5003



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.

There are 20 bytes in the IP header. In the instructions it said to initially send packets of length 56 bytes. Therefore, the payload must be 36 bytes.

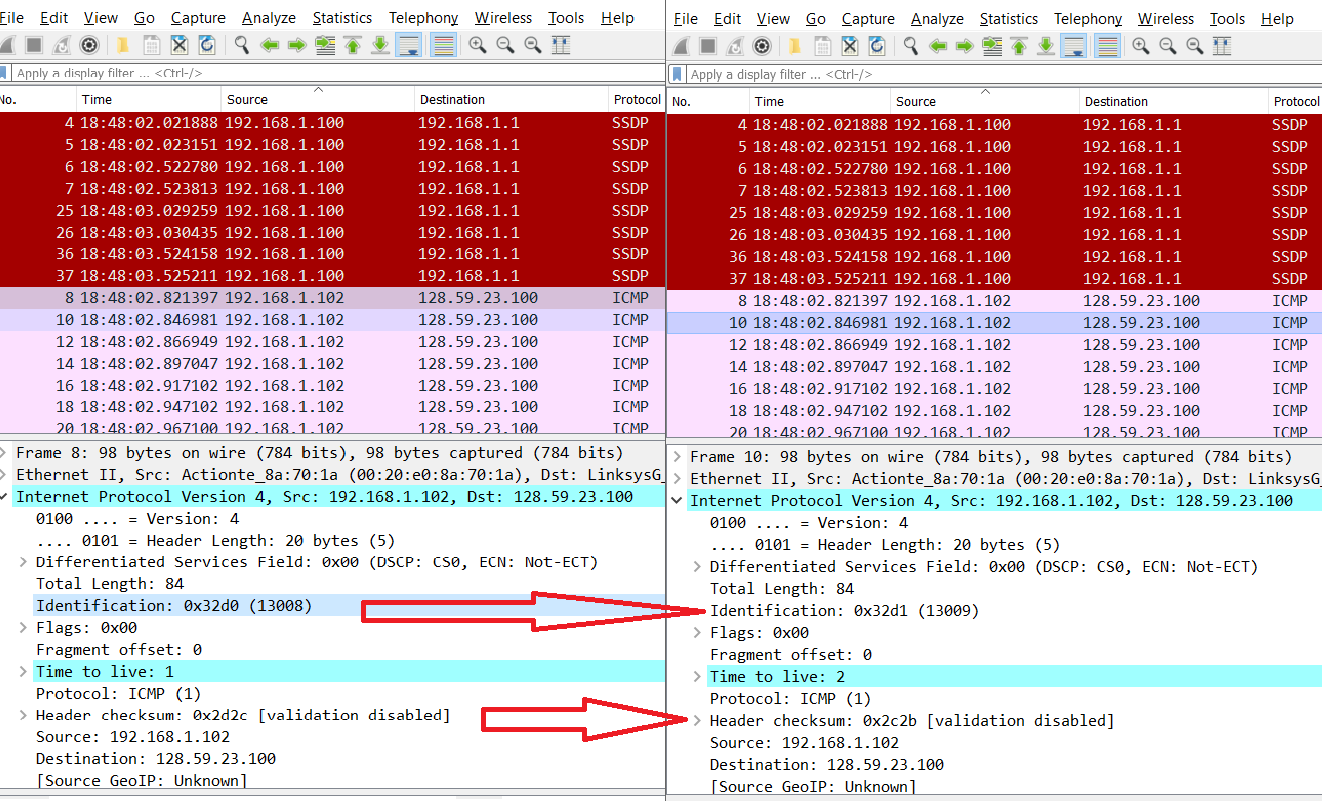
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

The IP datagram has not been fragmented. You can tell because the flag is not set 0x00 and the fragment offset 0.

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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?

Frame number, header checksum, Time to live, and Identification



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

Constant fields: Version, Header length, source IP(same source), Destination IP(same place), Upper layer protocol,

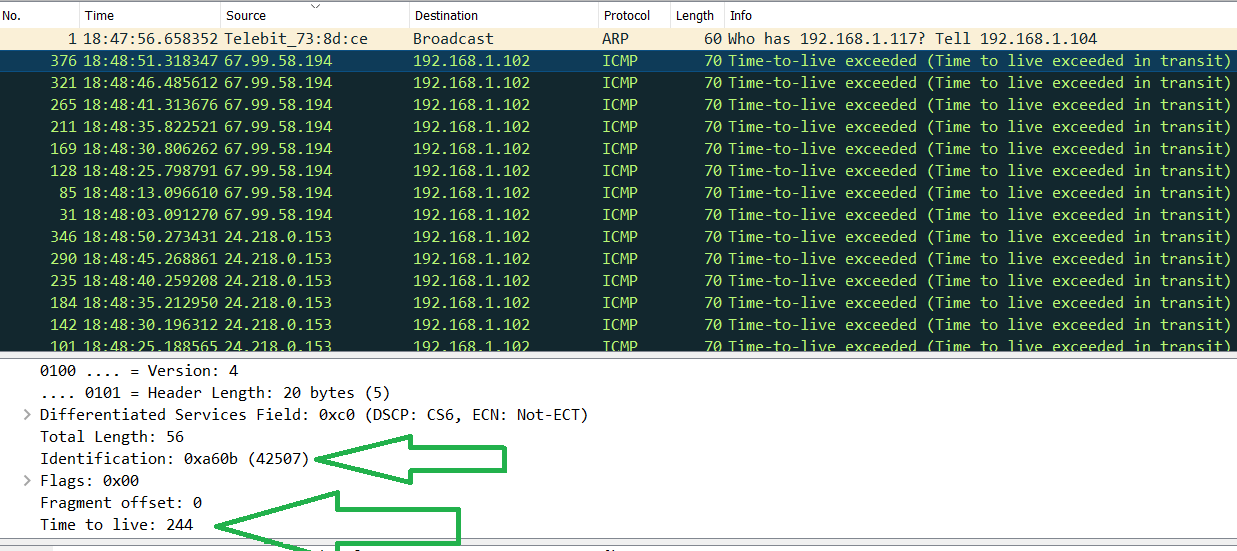
Fields that change are the checksum because the header changes with each different packet and the Identification which is used to verify each individual packet.

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

It goes up by one each time in the echo frames. (As can be seen in the picture above question 6)

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

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

Identification: 0xa60b (42507  
Time to live: 244

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?

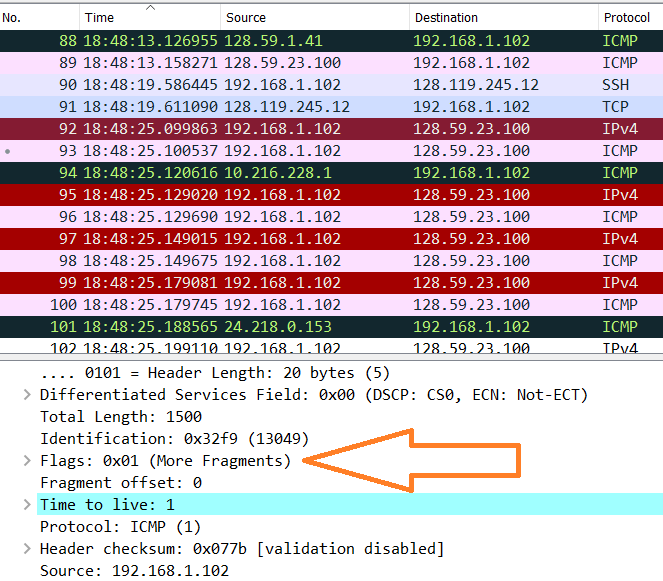
The identification field is used to separate unique packets. If two were to have the same one, it would suggest they were fragments of the same packet. Therefore, this field continually changes.

However, the TTL field will not change because regardless of the packet number, it will always have to go the same number of steps to reach its destination.

Fragmentation

Sort the packet listing according to time again by clicking on the *Time* column.

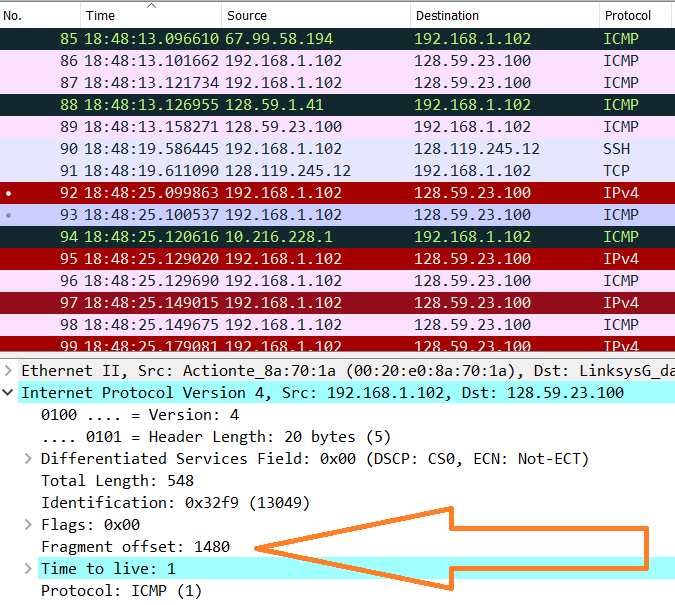
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the *ipethereal-trace-1*packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.3]

Yes, that message has been fragmented as noted by the orange arrow.

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?

First fragment is printed out above (under question 10). You can tell it is the first fragment because the flag is set to 0x01 and the offset is set to 0 (which happens when it is the first fragment)

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?



Fragment offset is set to 1480. Thi suggests that it is the second part of the fragment. Since the packets were 2000 bytes long and the flag is not set (0x00), This is the second and last fragment.

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

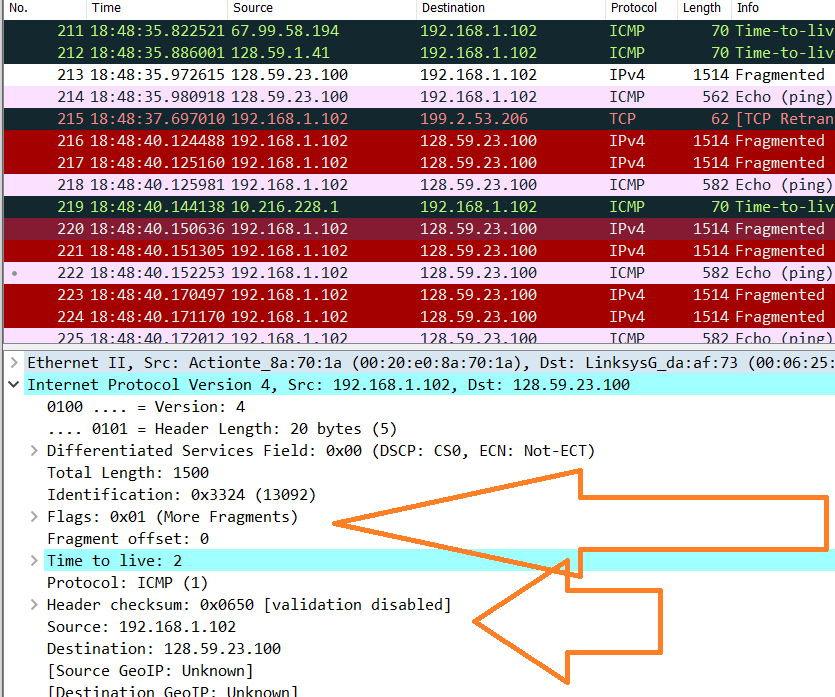
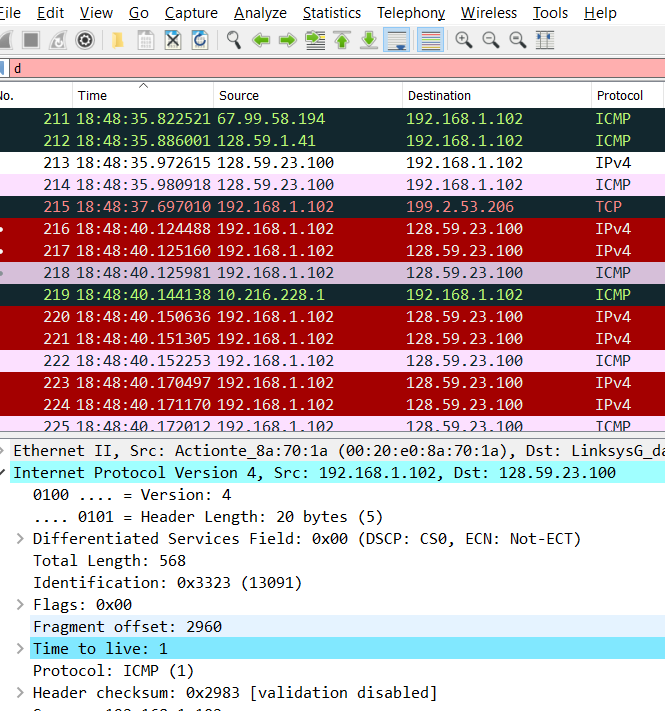
The header checksum, the fragment offset, the flag field, and the legth of the transmitted packet.

Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.

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

3 fragments with offsets 0, 1480, and 2060

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

The header checksum, the fragment offset, the flag field, and the legth of the transmitted packet.