Wireshark Lab: IP v6.0

Vandré Leal Cândido

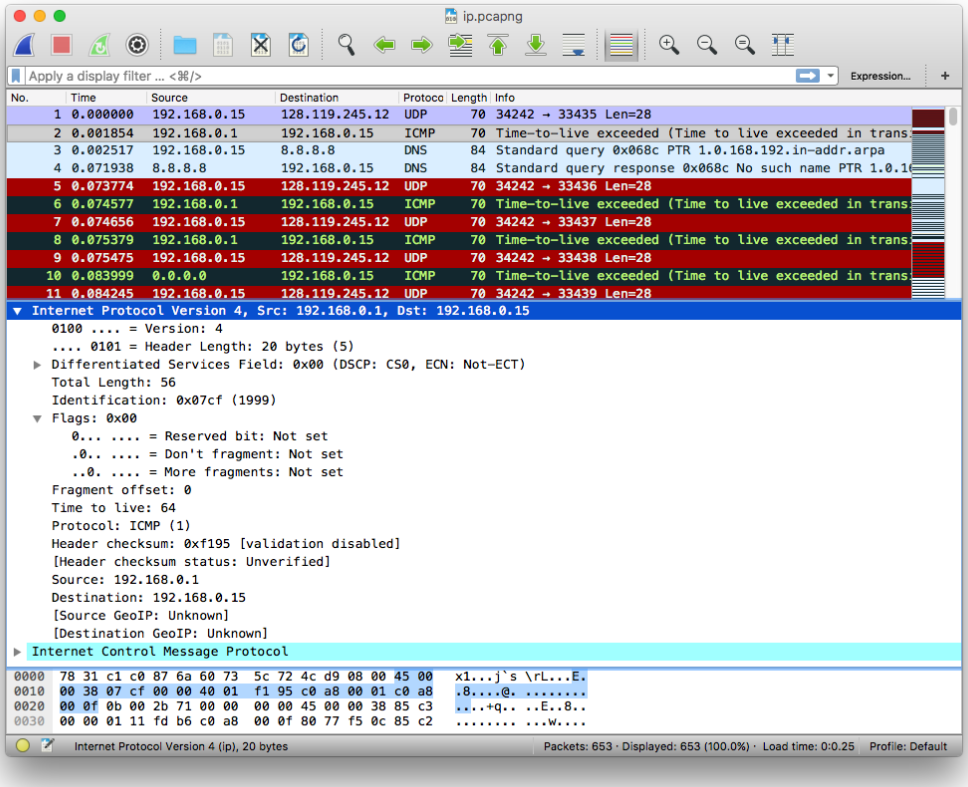
September 1, 2017

1 A look at the captured trace

- *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?*

  The IP address of my computer is 192.168.0.1.

Figure 1: Local IP address



The previous screenshot is also used to answer the following questions.

- *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 (1).

- *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 header. The payload is 36 bytes since it is the length of the datagram subtracted by the number of header bytes (56 - 20 = 36).

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

  This datagram hasn't been fragmented since the **More fragments** flag is not set.

- *Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?*

  Three fields always change from one ICMP message to another: **Identification**, **Time to live** and **Header checksum**.

- *Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?*

  The following fields stay constant and must stay constant:

  - Version: IPv4.
  - Header length: constant value (20 bytes) for all ICMP packets.
  - Source: sending from the same source.
  - Destination: sending to the same destination.
  - Differentiated Services: all ICMP packets use the same service class.
  - Upper Layer Protocol: IMCP(1) for all ICMP packets.

  The fields that must change are the ones mentioned in the previous question:

  - Identification: IP packets must have different identification numbers.
  - Time to live: traceroute increments the value.
  - Header checksum: since the header changes the checksum must change as well.

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

  The Identification field value is incremented on every new ICMP message.

- *What is the value in the Identification field and the TTL field?*

  Identification: 0x07cf (1999).
  TTL: 64.

- *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 value changes for all of the ICMP TTL-exceeded replies since it's an unique value. Two or more datagrams only have the same identification value in case they are fragments of a single large datagram. The TTL value remains unchanged because the TTL for the first router has always the same value.

2 Fragmentation

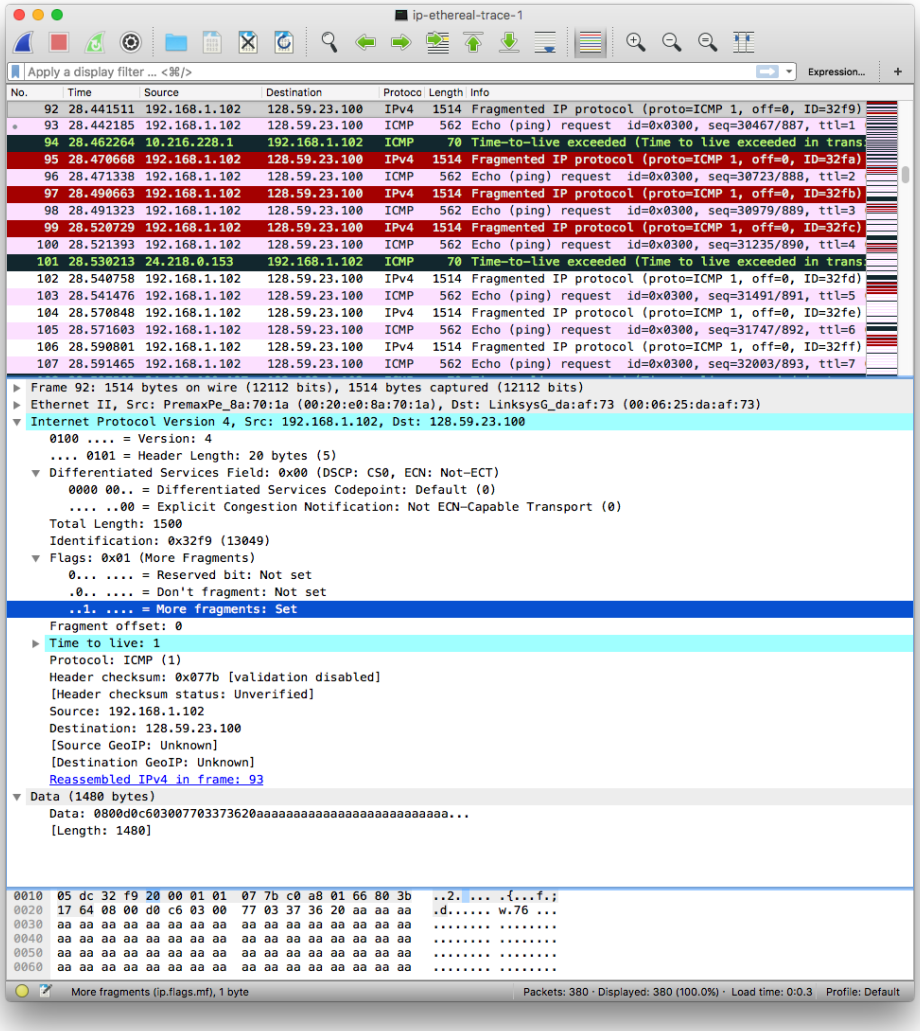
- *Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip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

  The file suggested was downloaded and will be used in this section since the message hasn't been fragmented on my tests.

- *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 flag **More fragments** set to 1 indicates that the datagram has been fragmented. The field **Fragment offset** set to 0 indicates that this is the first fragment, otherwise the value of this field would be greater than 0. The datagram has a total length of 1500 bytes, including the header.

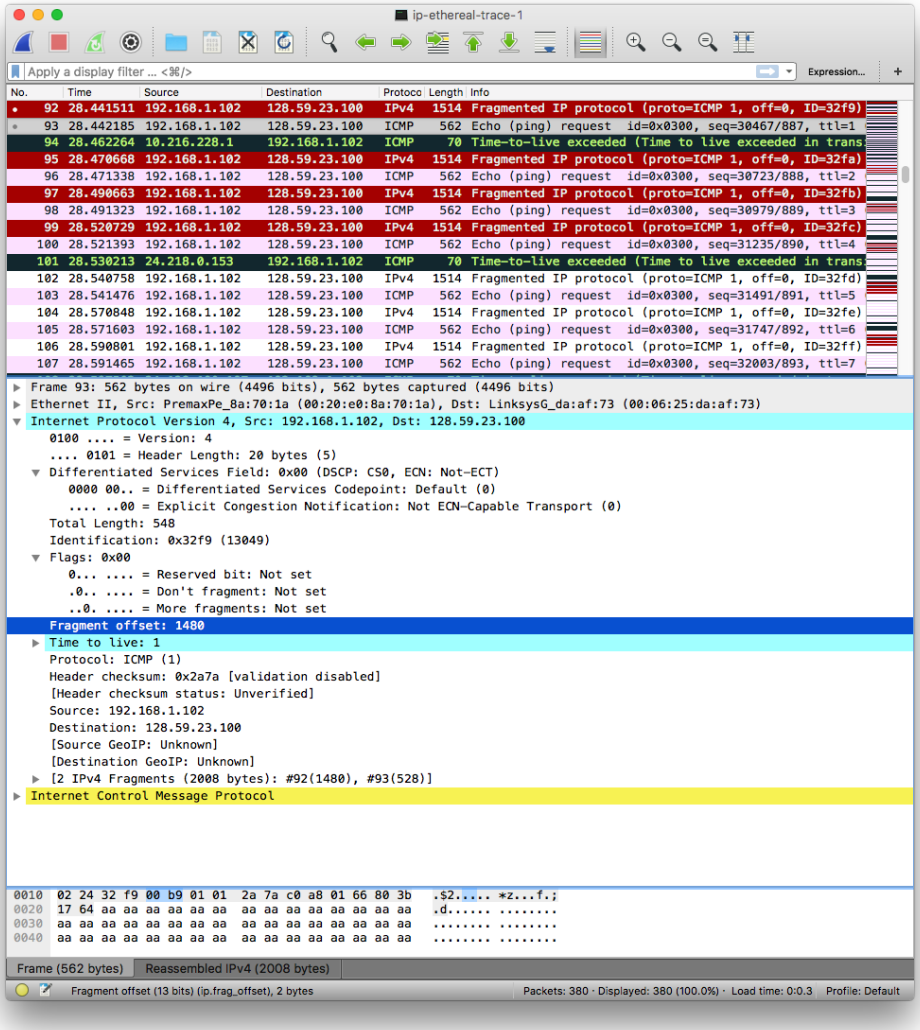
Figure 2: First datagram (packet size=2000)



- *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?*

  The value of the field **Fragment offset** is 1480 and indicates that this is the second and last fragment since the flag **More fragments** is not set.

Figure 3: Second datagram (packet size=2000)



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.

- *What fields change in the IP header between the first and second fragment?*

  The fields that changed between the first and second fragment are: **Total Length**, **Flags**, **Fragment offset** and **Header checksum**

- *How many fragments were created from the original datagram?*

  Three fragments were created after switching the packet size to 3500.

- *What fields change in the IP header among the fragments?*

  The fields that changed between all the fragments are: **Fragment offset** and **Header checksum**. **Total Length** and **Flags** are only changed between the first two packets and the last one since both the first and the second fragments have a total length of 1500 with the flag **More fragments** set to 1, whereas the last packet has a total length of 540 with the flag **More fragments** not set.

Figure 4: First datagram (packet size=3500)

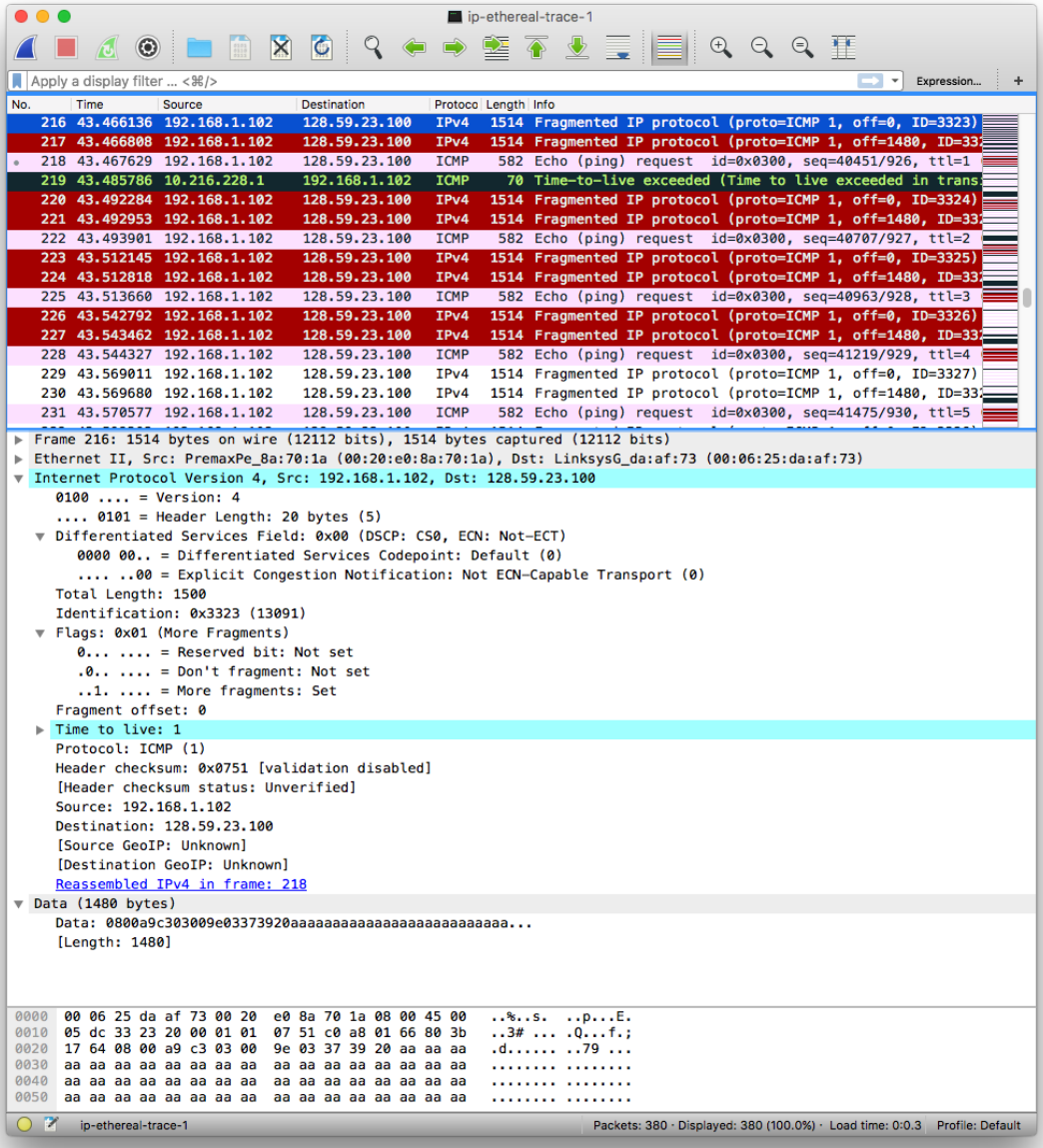


Figure 5: Second datagram (packet size=3500)

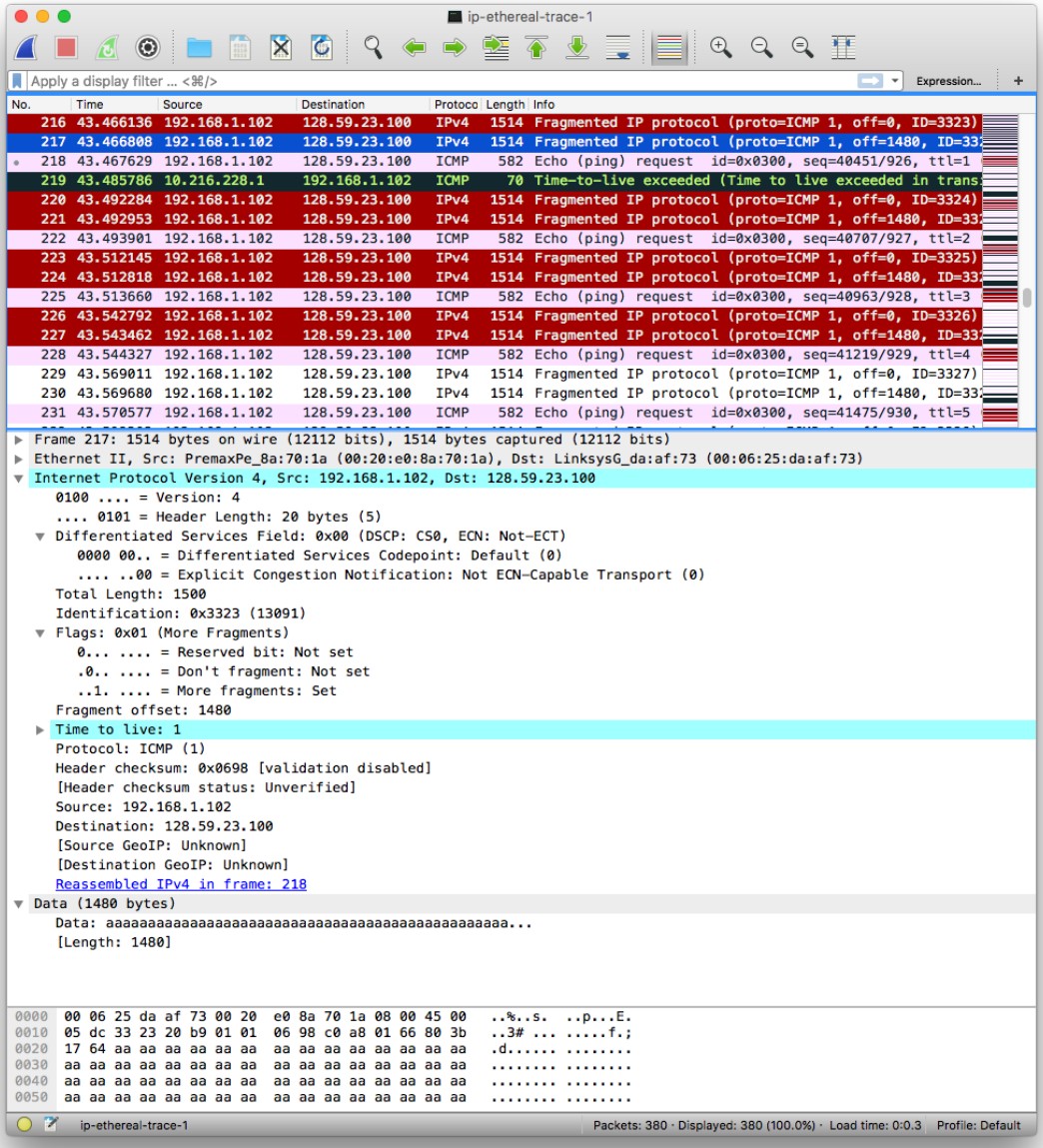


Figure 6: Third datagram (packet size=3500)