Wireshark Lab: IP v7.0

Supplement to Computer Networking: A Top-Down

Approach, 7th ed., J.F. Kurose and K.W. Ross

Using PingPlotter, visit gaia.cs.umass.edu.

1. The IP address of my computer is 129.8.217.48, but in the zip file with traces I used, the IP is 128.59.23.100
2. The value in the upper layer protocol field is ICMP (1).
3. There were 20 bytes in the IP header. The total length was 84 bytes, so 84-20 is 64 bytes as total payload length.
4. No, the datagram has not been fragmented. This is because the fragment offset value is 0 and the fragmented flags are not set.
5. The identification, Time To Live, and Header Checksum fields are always changing.
6. The fields that stay the same are source IP, destination IP, length, and IP version. These fields must stay constant because they are directing the datagram, setting a length, and needing to use the same IP version for all interaction. The identification, TTL, and header checksum must always change because they are the identifiers for the packets.
7. The pattern is that the identification field value increments by 1 each packet.
8. The value of the identification field was 0xa60 and the TTL field value was 244.
9. Identification would change from packet to packet, but the TTL field value stays the same throughout.
10. Yes, there were 2 fragmentations.
11. The first fragment has its fragmentation flag set, meaning that there Is another fragmented part somewhere. The datagram is 1500-20 = 1480 bytes long.
12. The fragmentation flag is set to 0x0, so the flag is not set, showing that this segment was not fragmented, meaning that this packet is the last fragment, not the first.
13. The total length, fragmentation flags, more fragments field, and fragment offset field will all change between the first and second fragment.
14. There are 3 fragments created from the original datagram.
15. The total length field, fragmentation field, more fragments field, and fragment offset field all change between the first, second, and third fragments.