COMP-3670 Lab 3- Wireshark Lab: IP v7.0 Questions 8-15

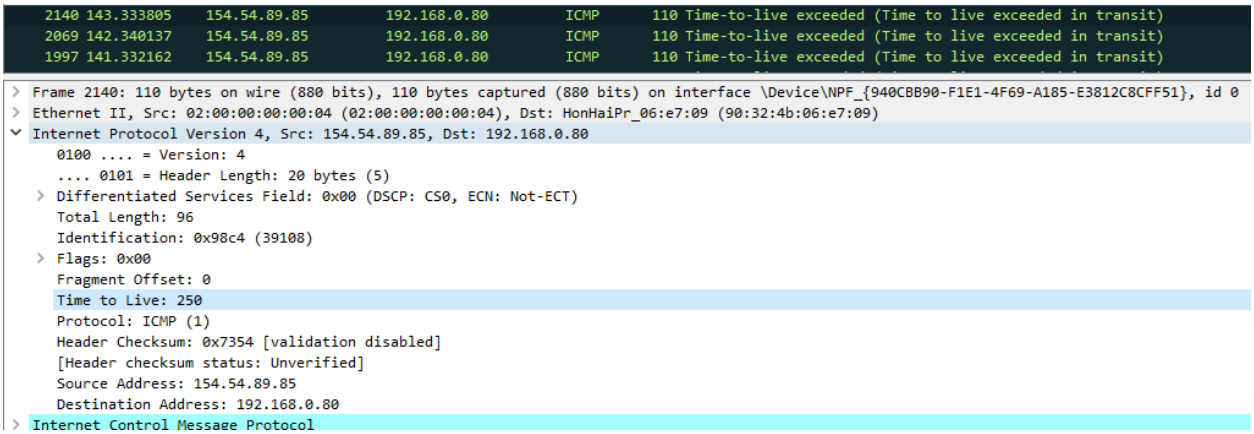
Donovan Longo

105011200

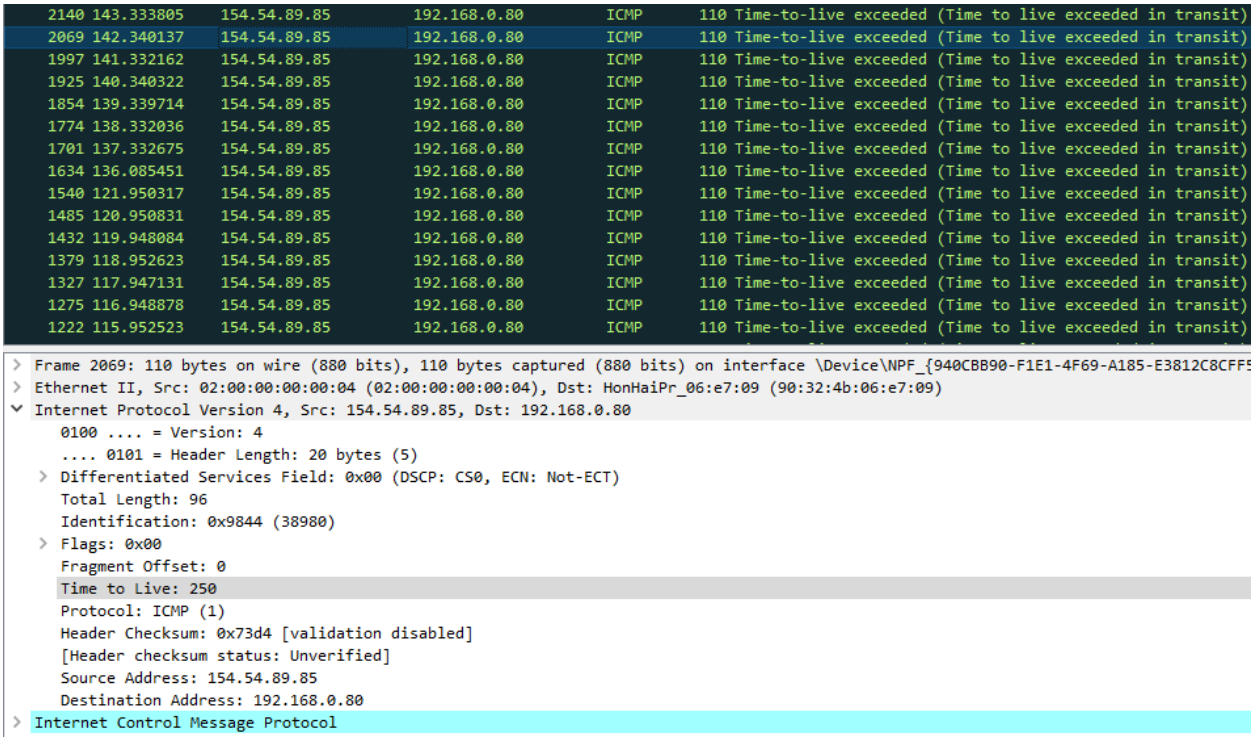
---

8. The identification field has a value of: 39108

The TTL field has a value of: 250

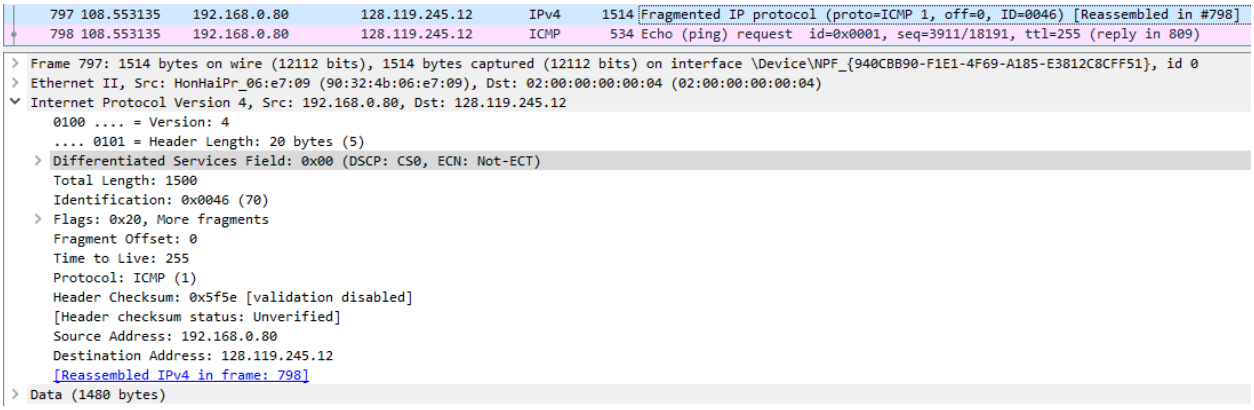


9. The identification field does not remain unchanged for all the ICMP TTL-exceeded replies to sent to our computer. This is because the identification field is a unique value given to all datagrams. The only time an IP datagram has the same identification value is when the datagram has been fragmented. The Time to Live field does remain unchanged, keeping the value of 250 for all the TTL-exceeded replies to the computer. Below is a screenshot of another ICMP TTL-exceeded reply to prove my answer. TTL is still 250 but the identification field has the value of 38980.



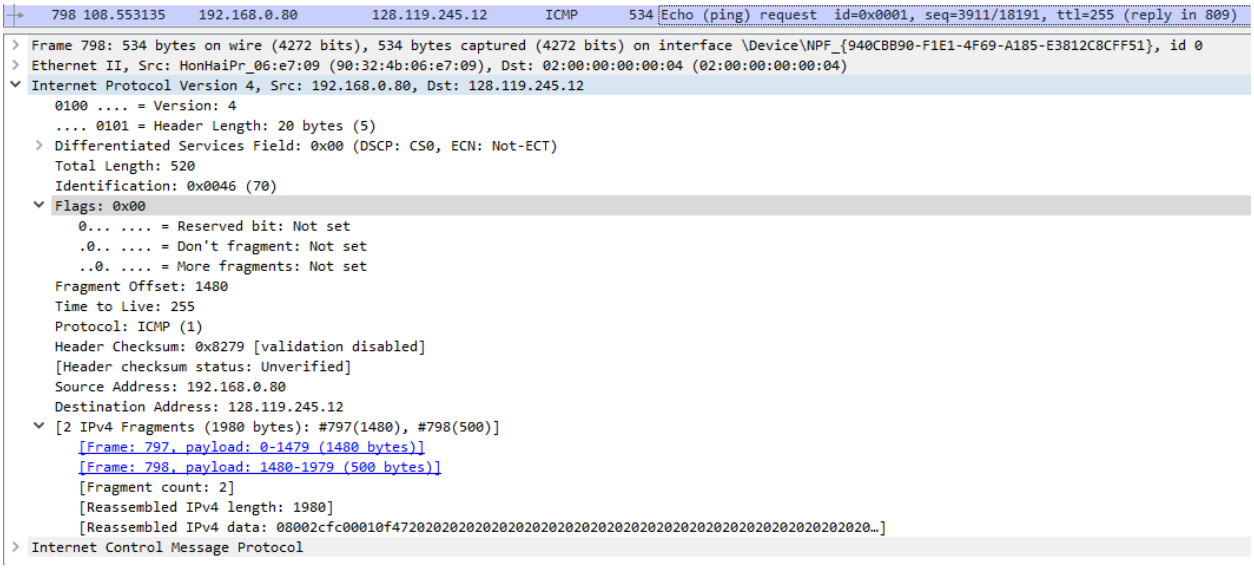
Fragmentation

10. Yes, the first ICMP Echo request sent from our computer with a large size was fragmented across more than one IP datagram.



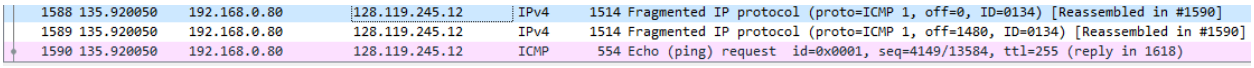
11. Using the screenshot above we can tell this datagram has been fragmented since the Flags field is set for more fragments. To determine whether this is the first fragment versus a latter fragment we can use the Fragment Offset field which the value is 0. This indicates this is the first fragment. Lastly the IP datagram has a length of 1480 bytes from the data and 20 bytes from the header totaling to 1500 bytes.

12. The Fragment Offset field in the IP deafer indicates that it is not the first fragment. This is because the value of fragment offset is 1480, not zero resulting this fragment is not the first datagram fragment. Since the Flags value is not set to more fragments, we can conclude this is the last fragment. Screenshot included below.



13. The fields that changed in the IP header include; total length to 520, flags to 0x00, fragment offset to 0 and checksum value.

14. 3 fragments were created from the original datagram after changing the packet size to 3500.



15. The fields that changed in the IP header among all the fragments include fragment offset, and checksum. The last fragment's total length is 540 and flags not set to more fragments which differ from the first two packets where their total lengths are 1500 and flags are set to more fragments. A screenshot of the last fragment to prove these fields is included below