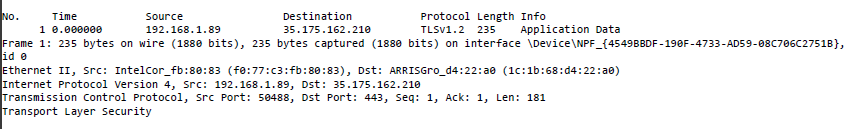
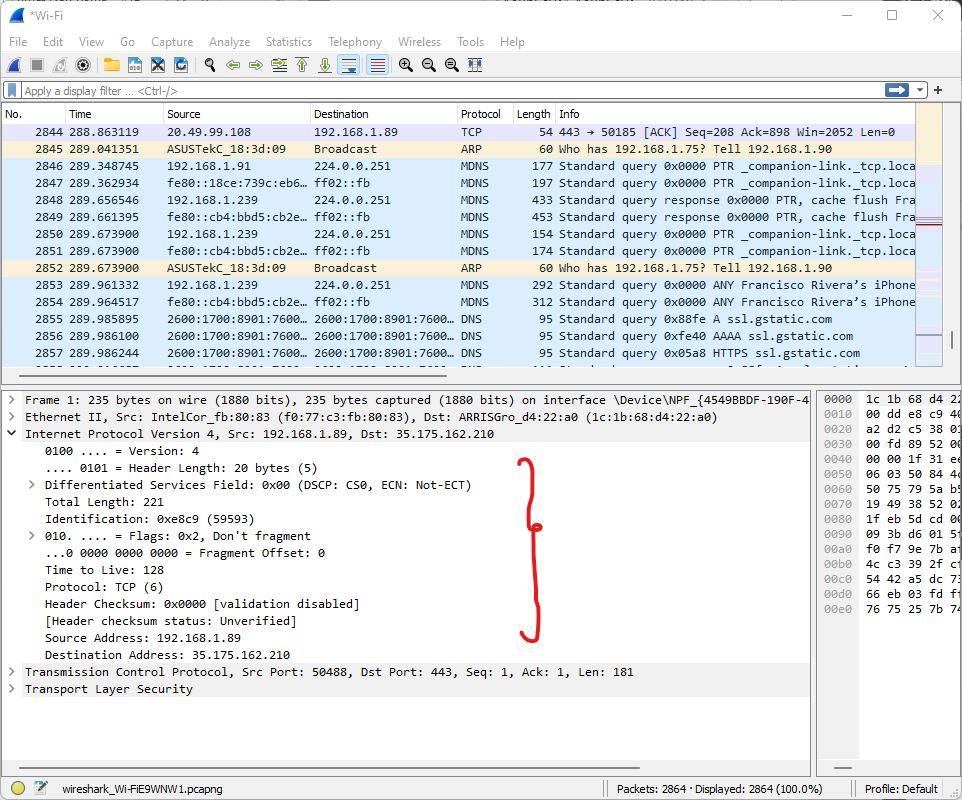
Lab 3: IP

1. **Capturing packets from an execution of traceroute**
2. **A look at the captured trace**

1. My computer: 192.168.0.26



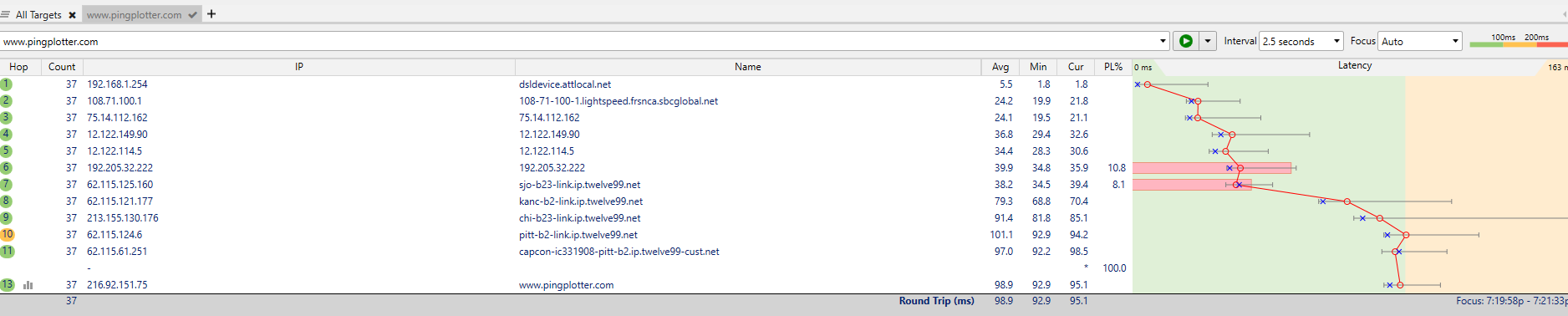
2. Within the header, the value in the upper layer protocol field is ICMP (0x00).



3. There are 20 bytes in the IP header, and 56 bytes total length, this gives 36 bytes in the payload of the IP datagram.

4. The more fragments bit = 0, so the data is not fragmented.

5. Identification, Time to live and Header checksum always change.



6. The fields that stay constant across the IP datagrams are:

• Version (since we are using IPv4 for all packets)

• header length (since these are ICMP packets)

• source IP (since we are sending from the same source)

• destination IP (since we are sending to the same destination)

• Differentiated Services (since all packets are ICMP they use the same

Type of Service class)

• Upper Layer Protocol (since these are ICMP packets)

The fields that must stay constant are:

• Version (since we are using IPv4 for all packets)

• header length (since these are ICMP packets)

• source IP (since we are sending from the same source)

• destination IP (since we are sending to the same destination)

• Differentiated Services (since all packets are ICMP they use the same

Type of Service class)

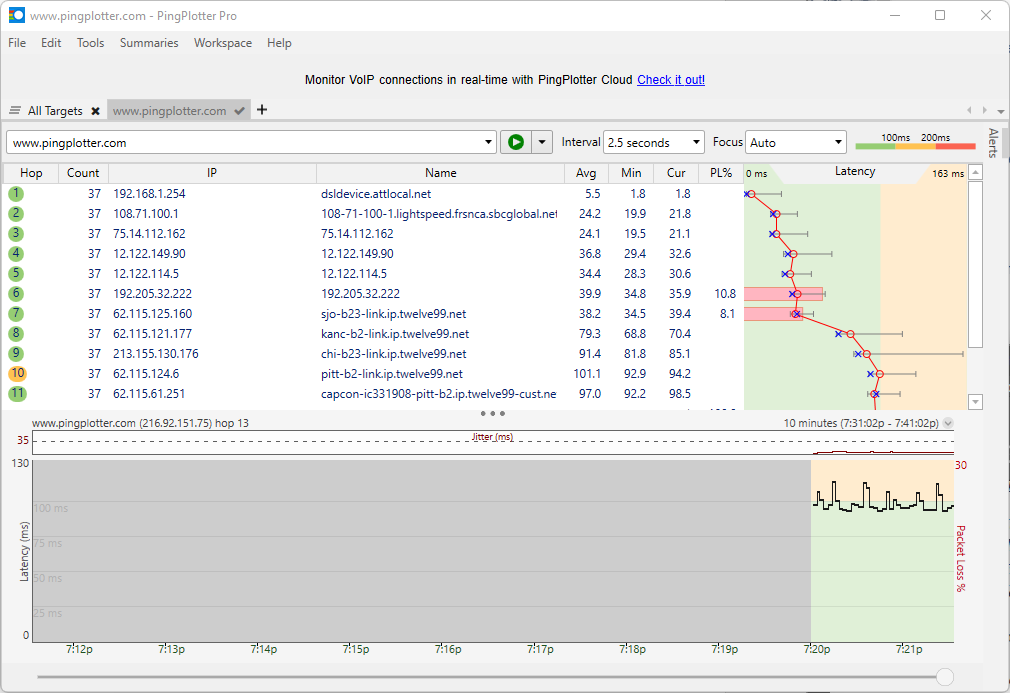
• Upper Layer Protocol (since these are ICMP packets)

The fields that must change are:

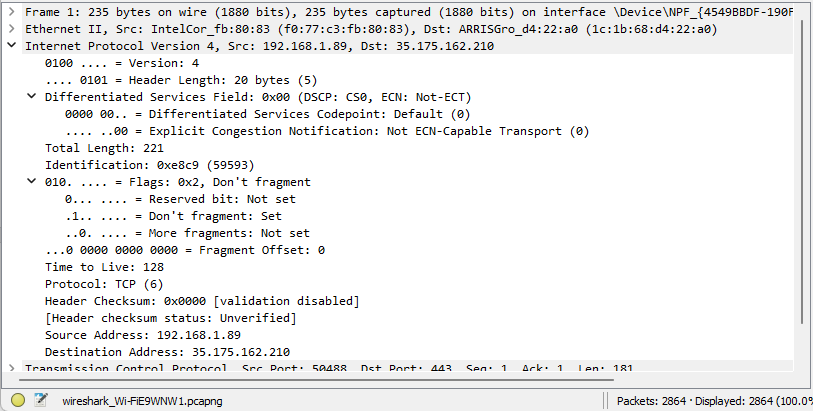
• Identification (IP packets must have different ids)

• Time to live (traceroute increments each subsequent packet)

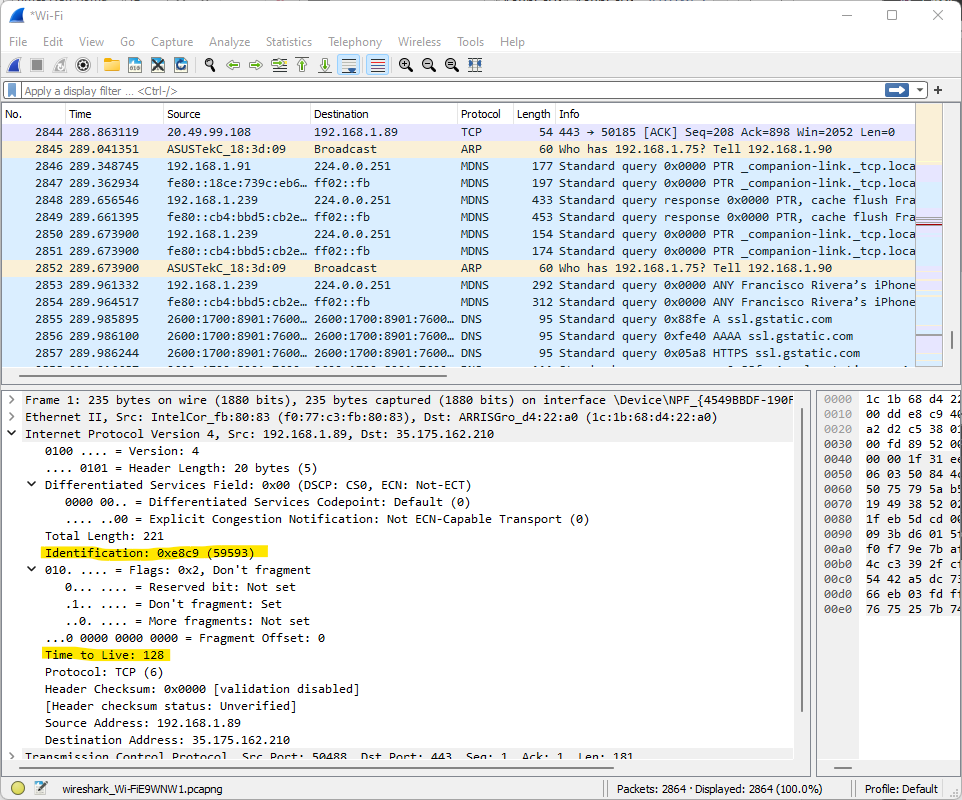
• Header checksum (since header changes, so must checksum)



7. The pattern is that the IP header Identification fields increment with each ICMP Echo (ping) request.



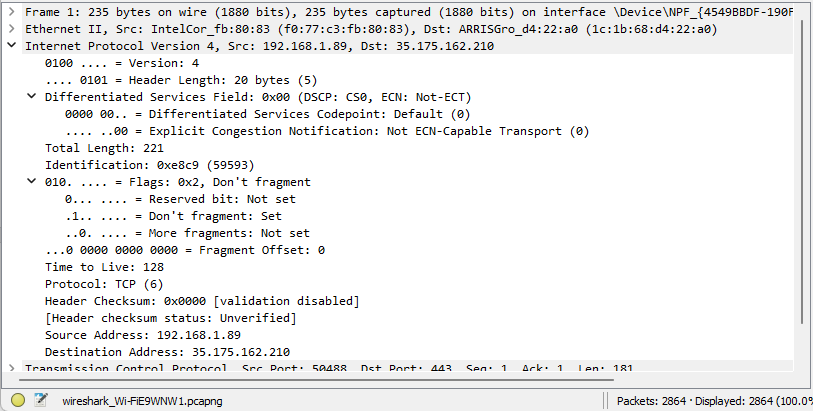
8. Identification: 59593 and Time to Live: 128



9. The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram. The TTL field remains unchanged because the TTL for the first hop router is always the same.

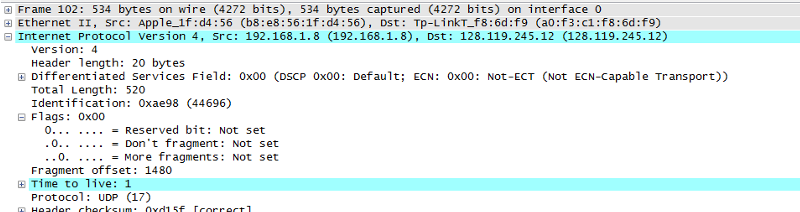
1. **Fragmentation**

10. No, this packet has not been fragmented across more than one IP datagram.



11. The Flags bit for more fragments is not set, indicating that the datagram has not been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 221, including the header.

12. We can tell that this is not the first fragment, since the fragment offset is 1480. It is the last fragment, since the more fragments flag is not set.



13. The IP header fields that changed between the fragments are: total length, flags, fragment offset, and checksum.

14. After switching to 3500, there are 3 packets created from the original datagram.

15. The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0.