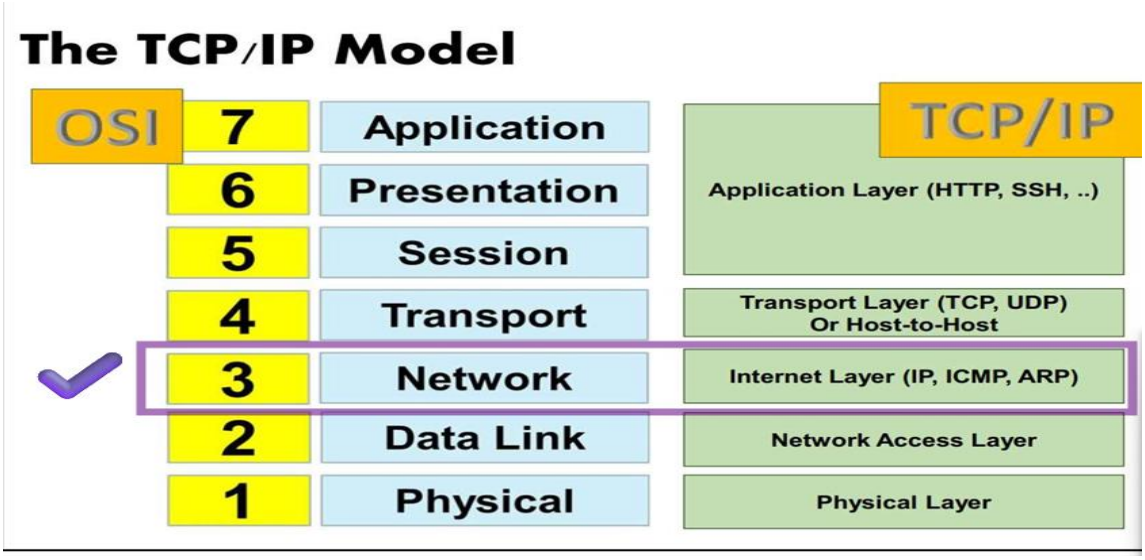
by SOUFIANE ZAFZOUF

zafzoufsoufiane@gmail.com

● IPv4 Packet Analysis Project Report



1. Introduction

This project is about analyzing IPv4 packets using Wireshark. We look inside real packets to understand how MTU, fragmentation, and TTL work. The goal is to learn how these parts of the network affect how packets travel across the internet.

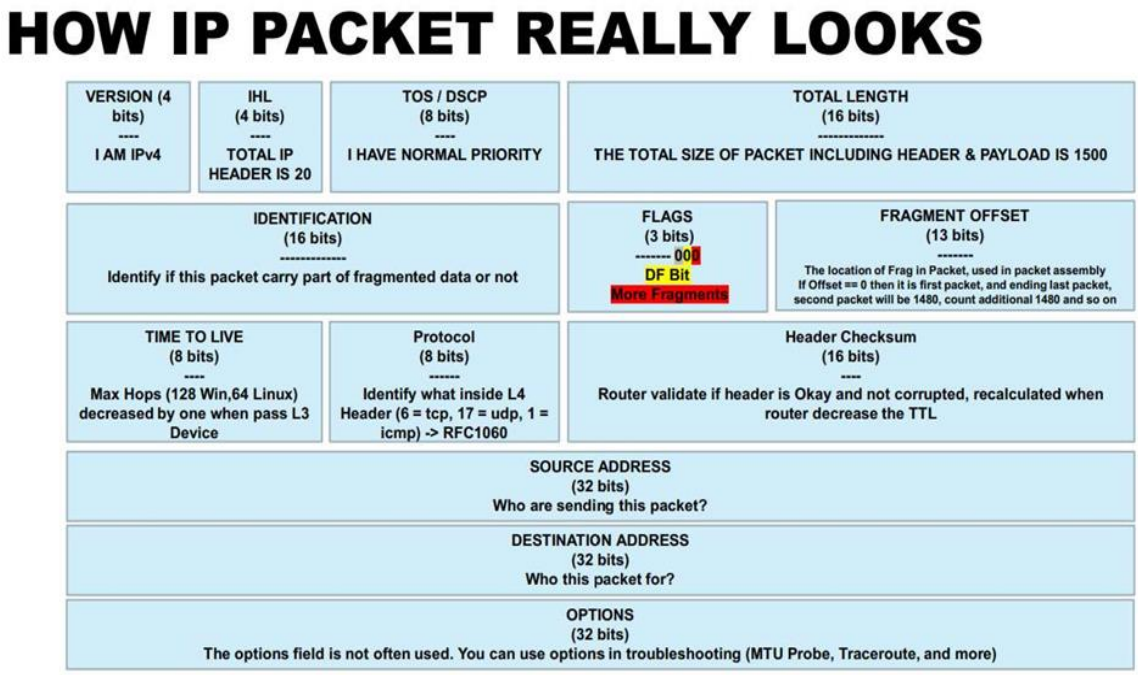
2. Tools & Environment

- Kali Linux (VMware)
- Wireshark
- Command line tools: ping, traceroute, hping3

3. IPv4 Header Fields Explained

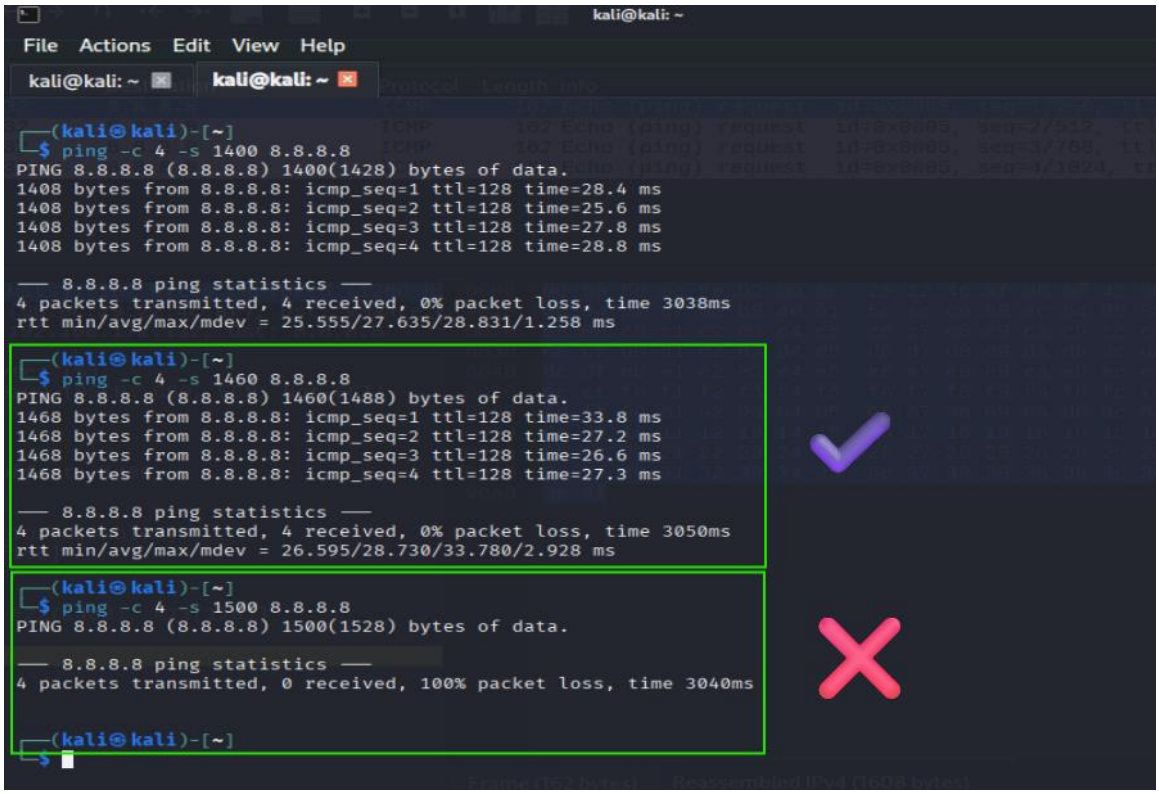
Here are the important fields we studied:

- Version: Always 4 for IPv4
- Header Length: Size of the header, normally 20 bytes
- Total Length: Full size of the packet (header + data)
- Identification: ID for reassembling fragments
- Flags: Tells if packet can be fragmented
- Fragment Offset: Position of fragment in the original data
- TTL (Time To Live): Maximum number of hops before packet is dropped
- Protocol: Type of payload (like ICMP, TCP, etc)
- Source and Destination IP: Who sent it and where it's going

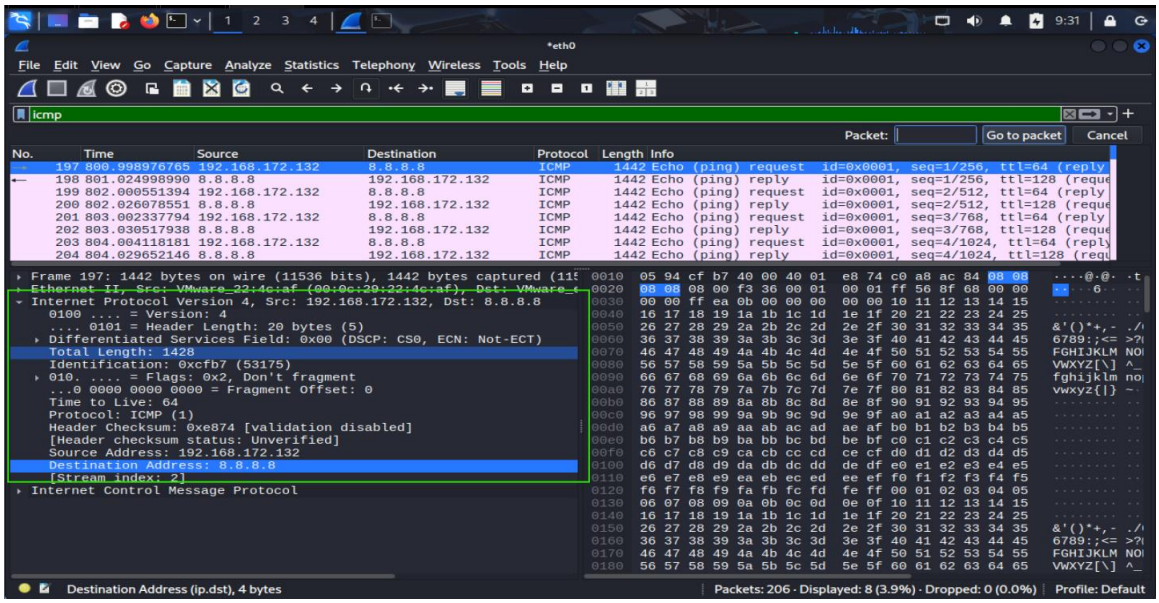


4. Testing MTU and Fragmentation

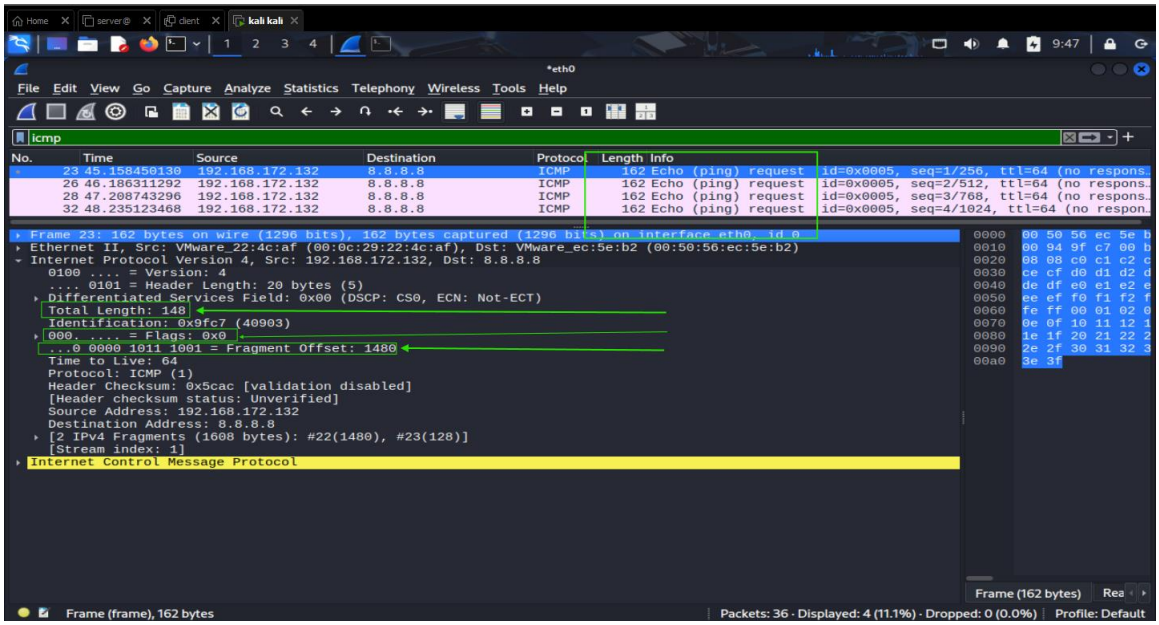
We used the ping command with a large packet size to test the MTU:
`ping -c 4 -s 1400 8.8.8.8`
This showed how packets can be too big and may need to be fragmented. Fragmented packets have the same ID but different Fragment Offset values.



And analyses packet normal (the package is not fragmented) :



And analyses packet not normal (the package is fragmented) :

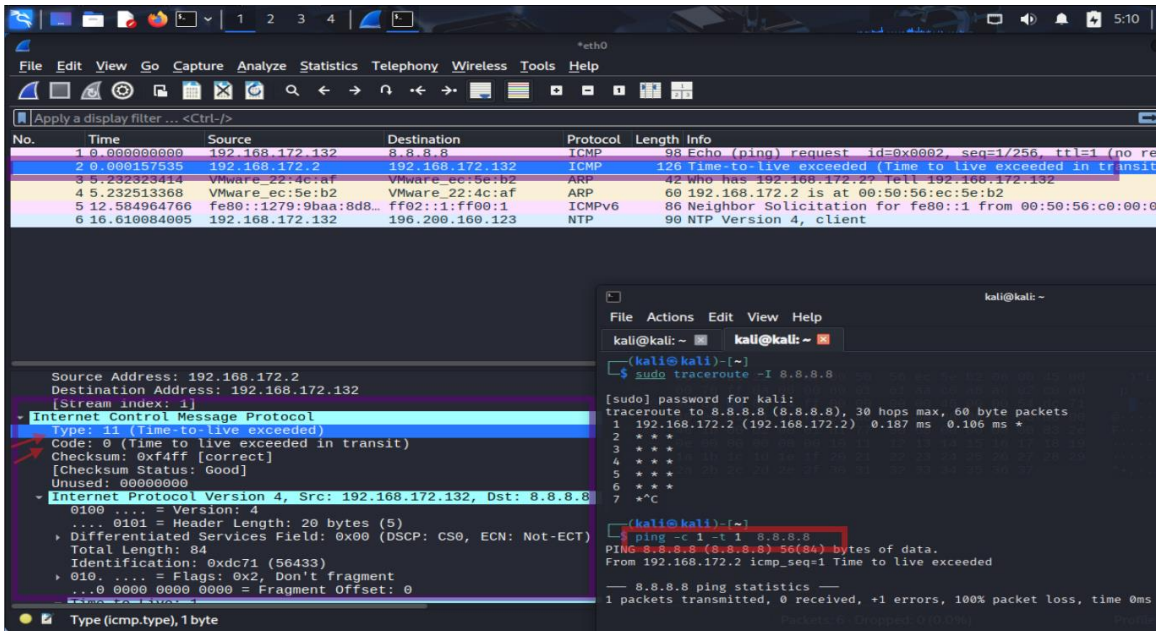


5. TTL and ICMP Time Exceeded

We used:

`ping -c 1 -t 1 8.8.8.8`

This sets the TTL to 1. When the router sees TTL=1, it drops the packet and replies with ICMP Time Exceeded. This shows how routers help stop infinite loops.



6. Screenshots & Real Packet Analysis

We used Wireshark to capture real traffic and look at each field in the header. We included screenshots in the `screenshots/` folder to show how these values look in real packets.

7. Conclusion

From this project, we learned how IPv4 headers work. We also learned how MTU, fragmentation, and TTL can affect how packets move in a network. These concepts are important for network engineers and cybersecurity students.