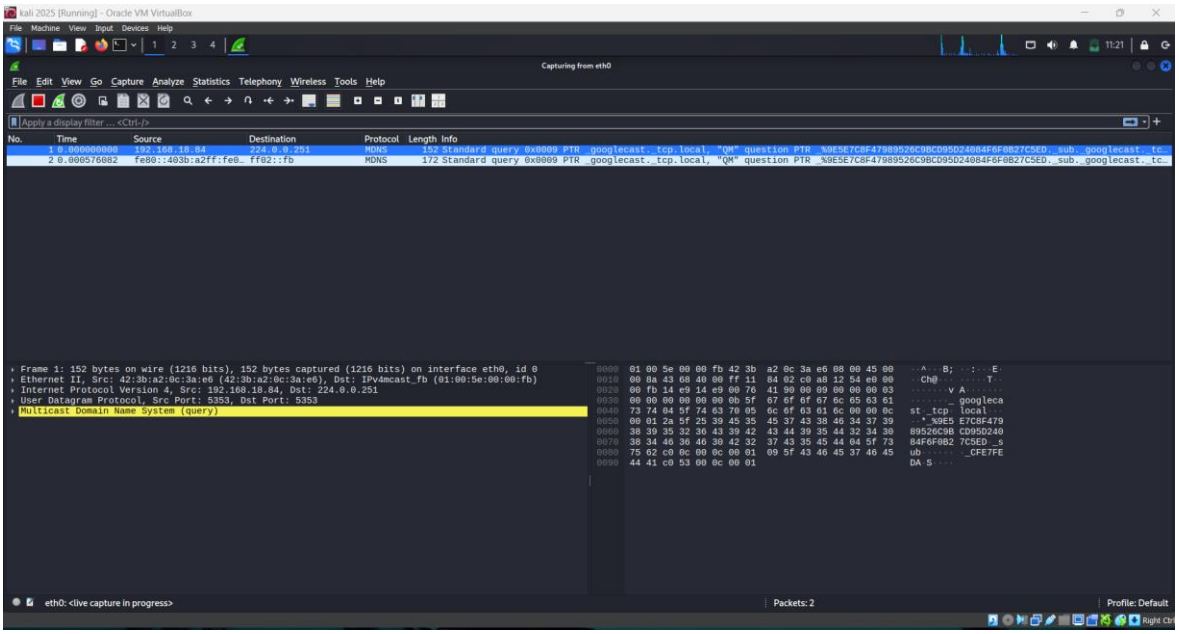
Wireshark Packet Capture Report

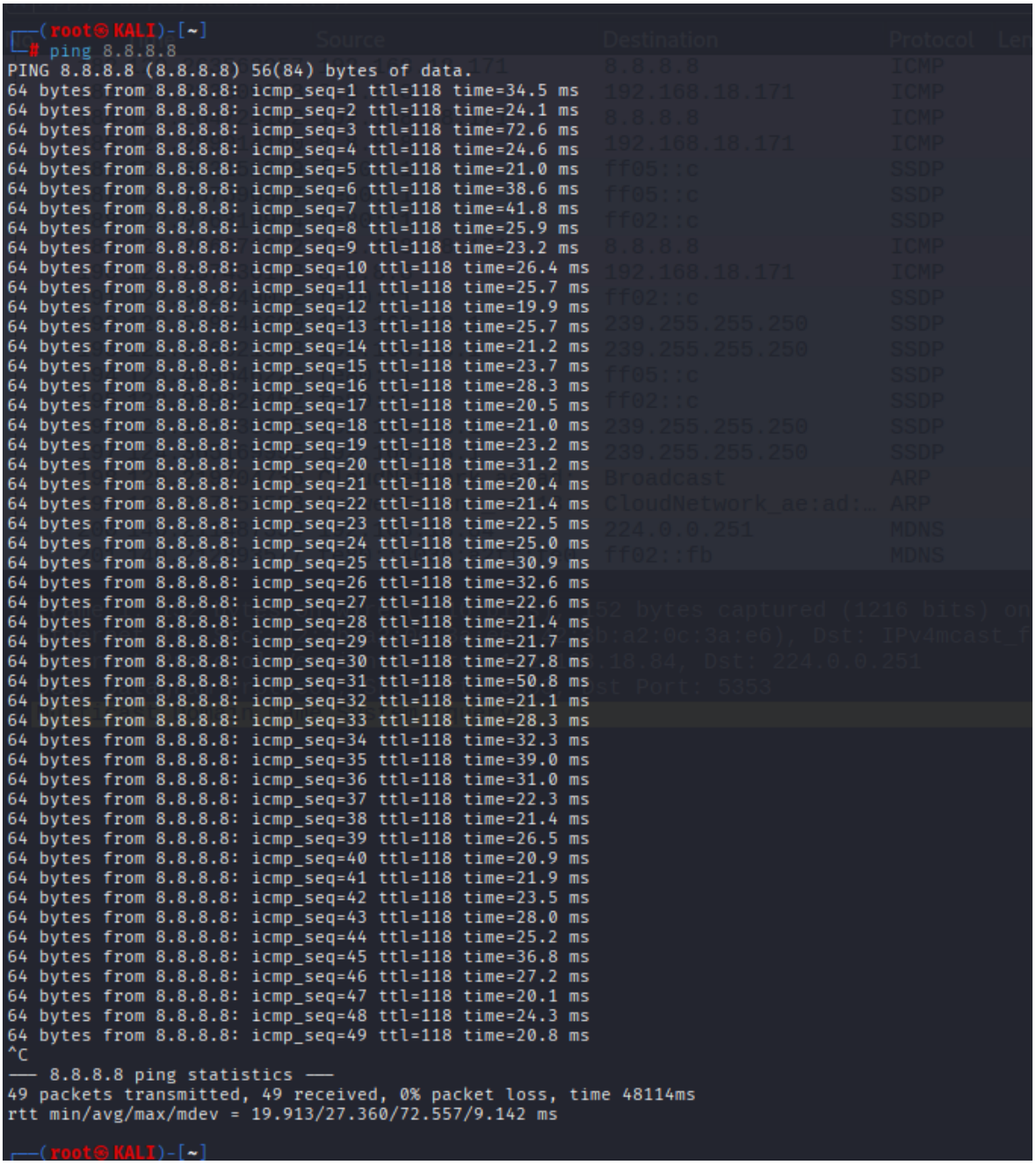
This report documents the process of capturing and analyzing network traffic using Wireshark on Kali Linux. Each step includes a screenshot and explanation for better understanding.

Step 1: Opening Wireshark

In this step, Wireshark is launched on Kali Linux. The main interface shows the available network interfaces that can be monitored.

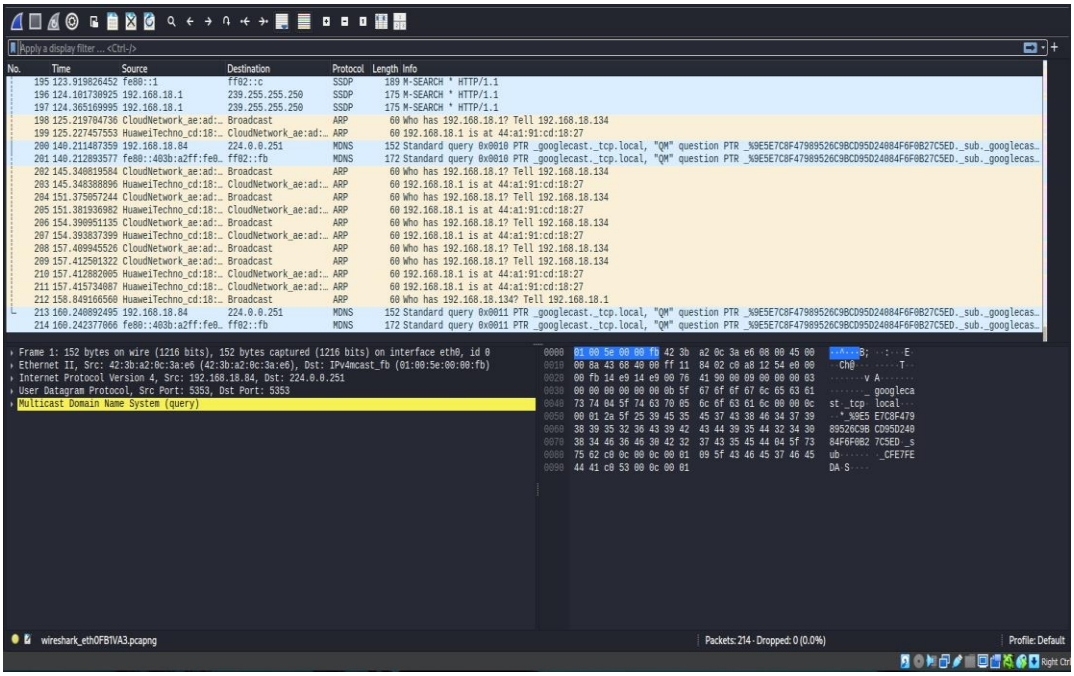


After that I ping to ping 8.8.8.8 (Google)



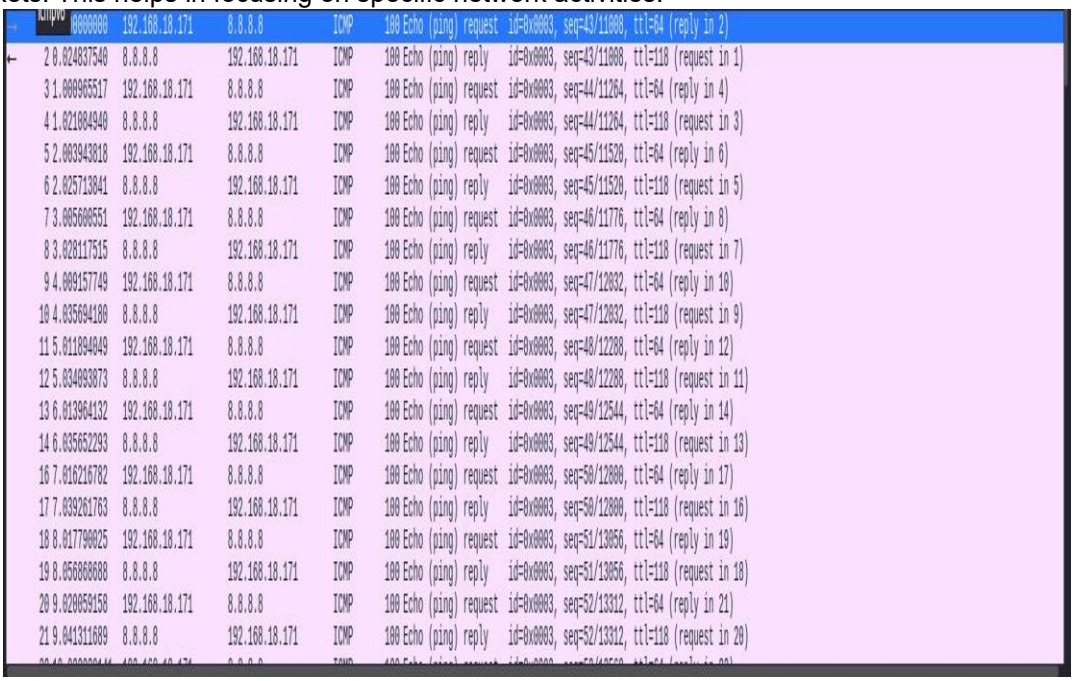
Step 2: Starting Packet Capture

The active network interface (such as eth0 or wlan0) is selected, and the 'Start Capturing Packets' button is clicked to begin capturing live network traffic.



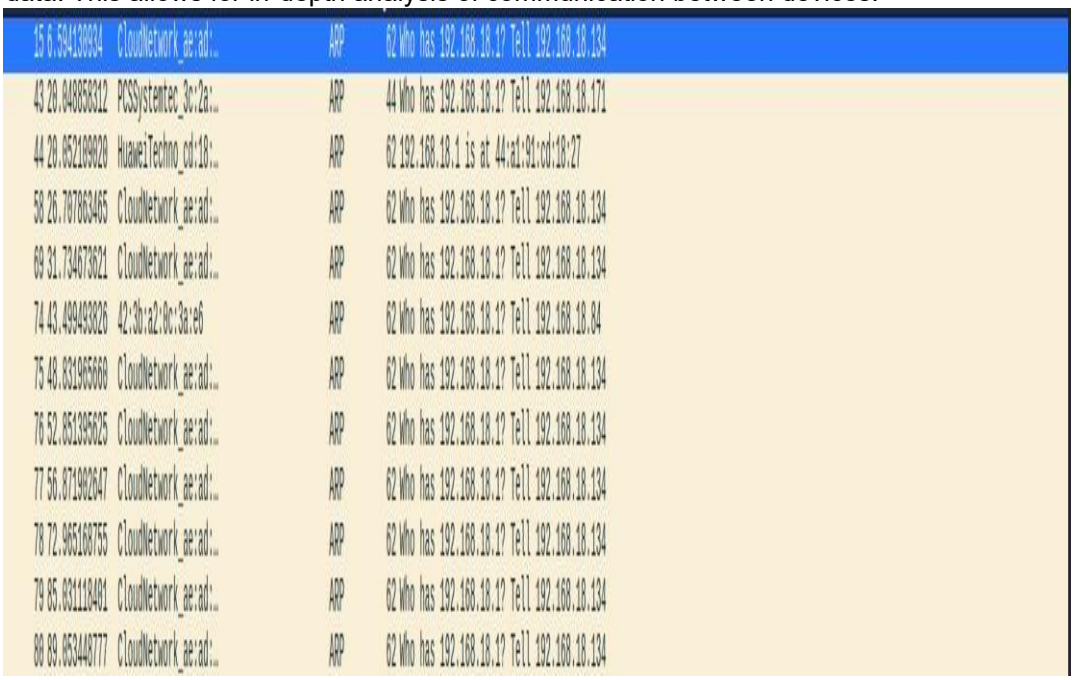
Step 3: Filtering Traffic by Protocol

After capturing data, filters such as 'HTTP', 'DNS', or ICMP' are applied to view only relevant packets. This helps in focusing on specific network activities.



Step 4: Viewing Packet Details

A selected packet is expanded to show detailed protocol layers (Ethernet, IP, TCP/UDP, etc.) along with data. This allows for in-depth analysis of communication between devices.



Conclusion

The above steps demonstrate how to use Wireshark for basic packet capturing and protocol analysis. Through this exercise, we identified different types of traffic and learned to filter and inspect packets in detail.