Wireshark Packet Capture & Analysis Report

Task: Network Traffic Analysis with Wireshark
Date: 2025-08-11
Author: Kondiba Gangadhar Jogdand

Objective

The objective of this task was to capture network traffic using Wireshark, apply various protocol filters such as HTTP, DNS, TCP, UDP, and ICMP, and analyze the captured packets to understand communication patterns between hosts. The task demonstrates basic to intermediate packet analysis skills.

Procedure

1. Launched Wireshark and selected the appropriate network interface for capturing packets.
2. Started packet capture and generated network traffic using the browser and other network tools.
3. Applied display filters to isolate traffic for specific protocols:
   - HTTP
   - DNS
   - TCP
   - UDP
   - ICMP
4. Observed resolved addresses and packet details for each filter.
5. Stopped the capture and saved the results in a .pcapng file.

Results

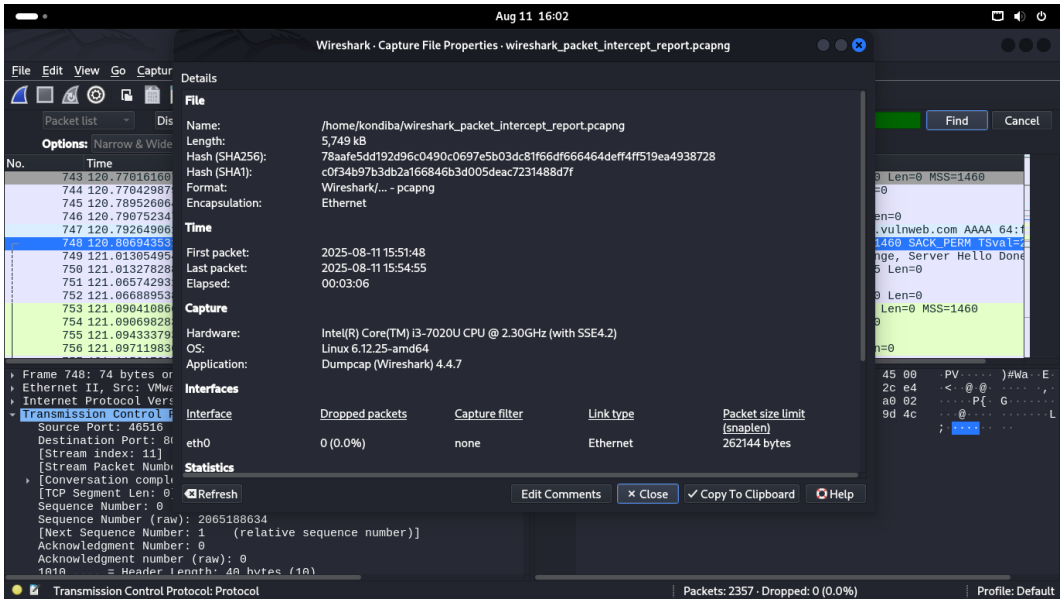

Figure: Initial packet capturing process.

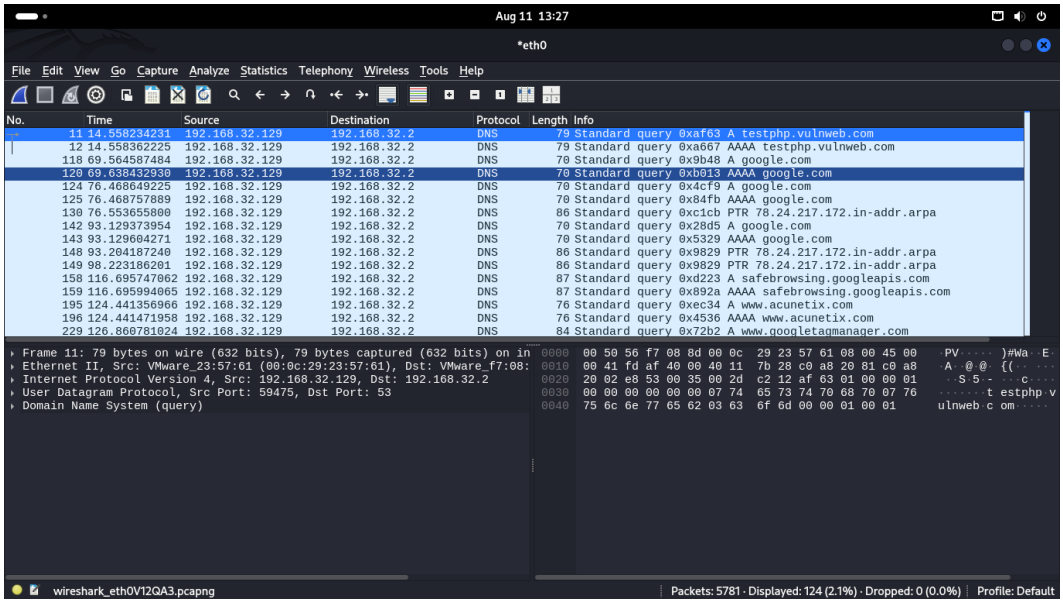

Figure: Captured packets overview.

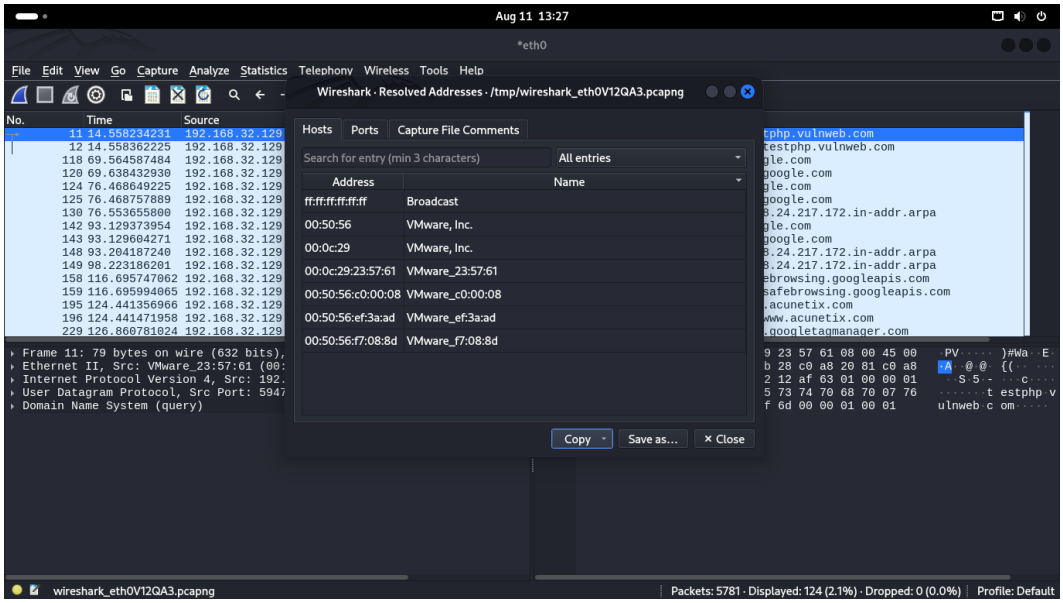

Figure: Resolved network addresses.

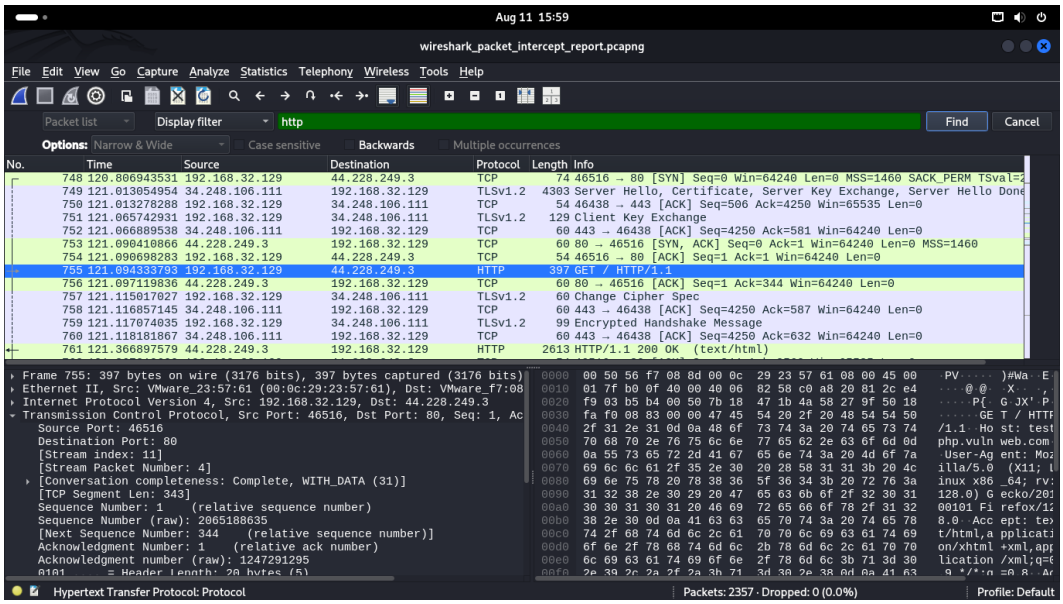

Figure: HTTP traffic filtered view.

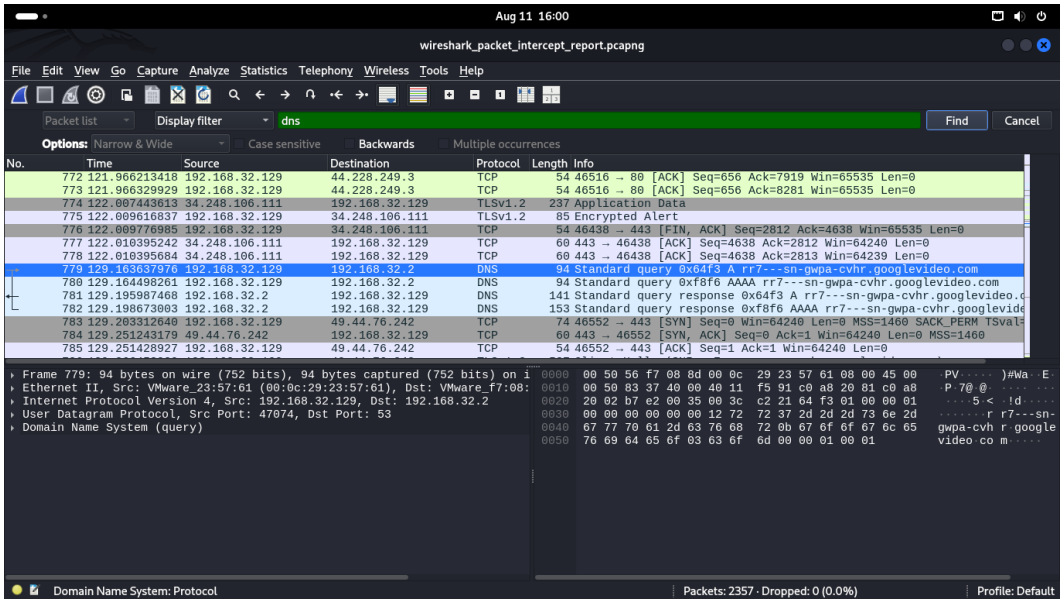

Figure: DNS traffic filtered view.

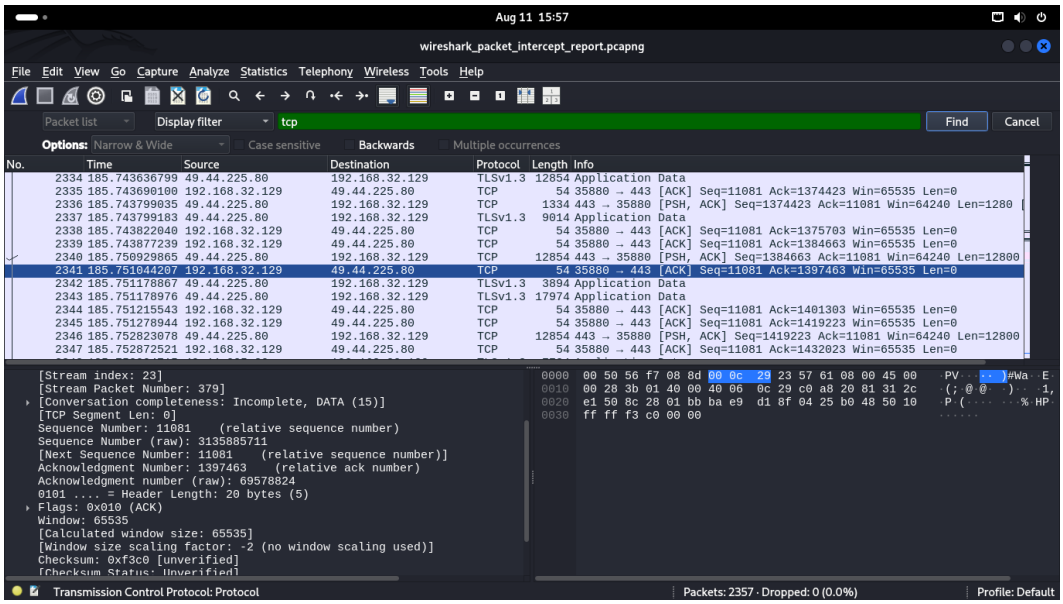

Figure: TCP traffic filtered view.

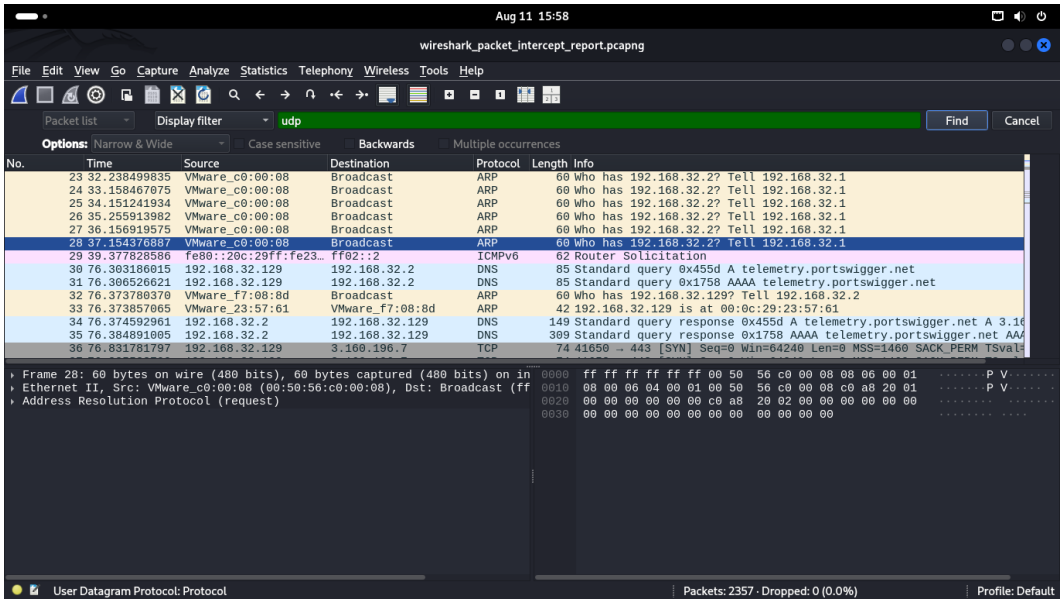

Figure: UDP traffic filtered view.

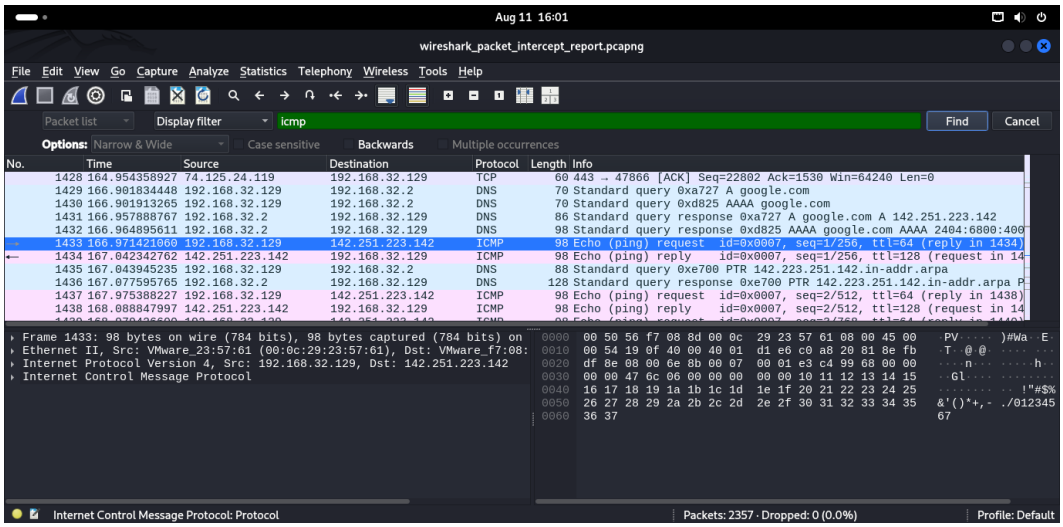

Figure: ICMP traffic filtered view.

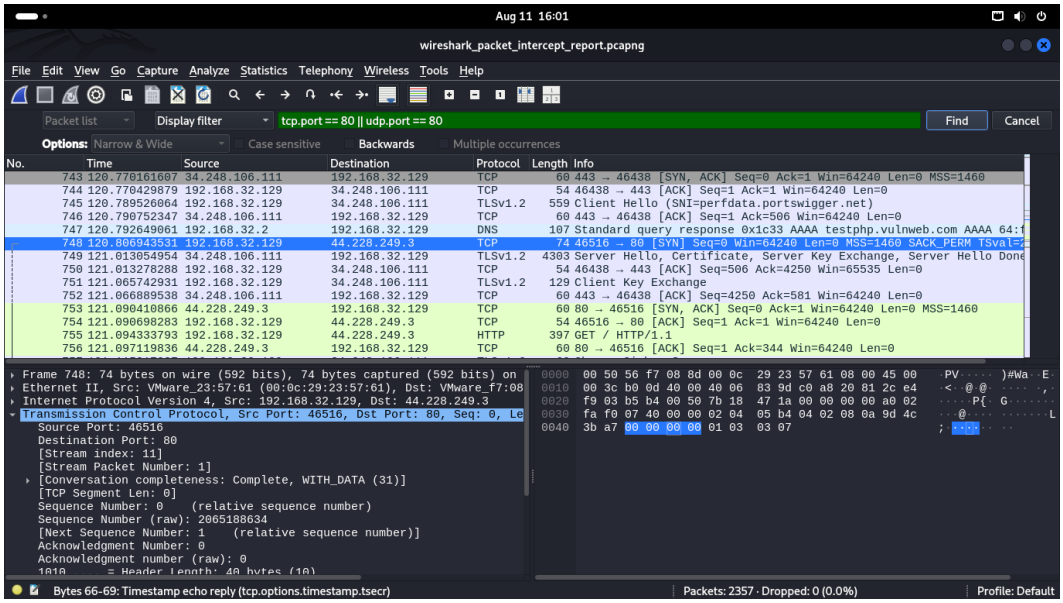

Figure: Filtered TCP and UDP ports display.

Conclusion

This exercise provided hands-on experience with Wireshark for network packet capture and analysis. By applying specific protocol filters, it was possible to focus on relevant traffic types and gain a better understanding of how different protocols operate on the network.

Appendix

Captured packet file: wireshark_packet_intercept_report.pcapng