Task - 5

Network Traffic Analysis Report – Wireshark

Title: Capture and Analysis of Network Traffic using Wireshark
Date: 11/08/2025
Name: Abinash I
Tool Used: Wireshark v4.x
System Used: Linux

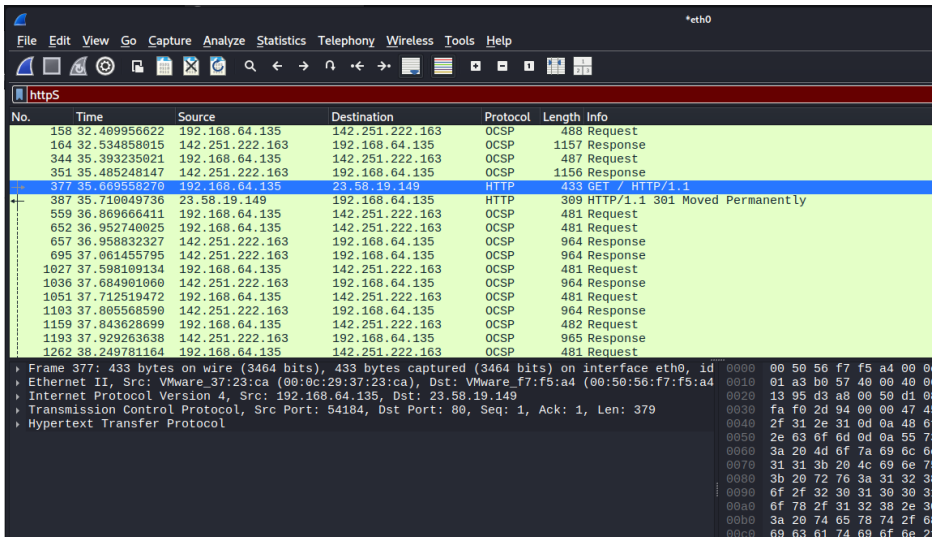
Objective

To capture live network traffic and identify common internet protocols such as HTTP, DNS, and TCP using Wireshark.

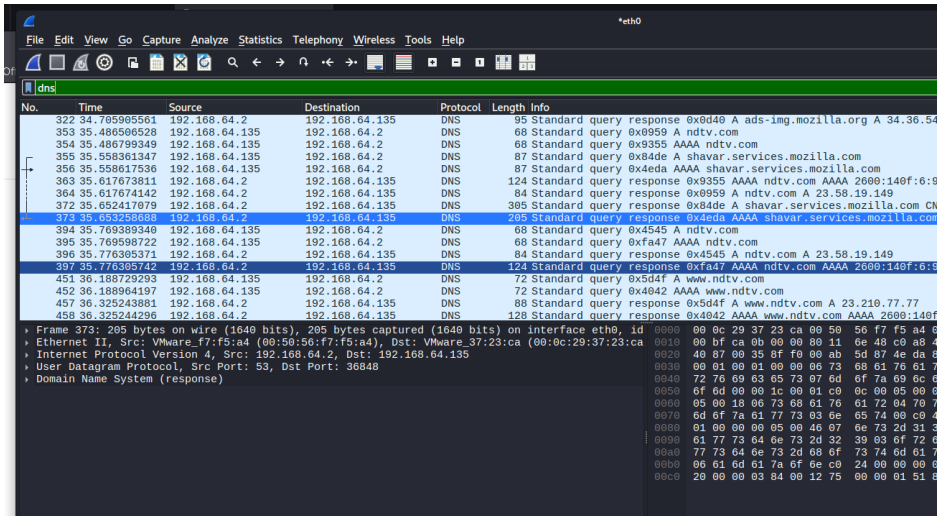
Procedure

1. Installed **Wireshark** and selected the active network interface (Wi-Fi).
2. Started a live packet capture for about 1 minute.
3. Generated traffic by:
   - Visiting a website in a browser.
   - Performing a `ping` command to an external server.
4. Applied protocol filters in Wireshark:
   - `http` → to view HTTP requests and responses.
   - `dns` → to see DNS queries and responses.
   - `tcp` → to observe TCP handshake and communication.
5. Took screenshots for each filtered protocol.
6. Saved the packet capture as **network_capture.pcap**.

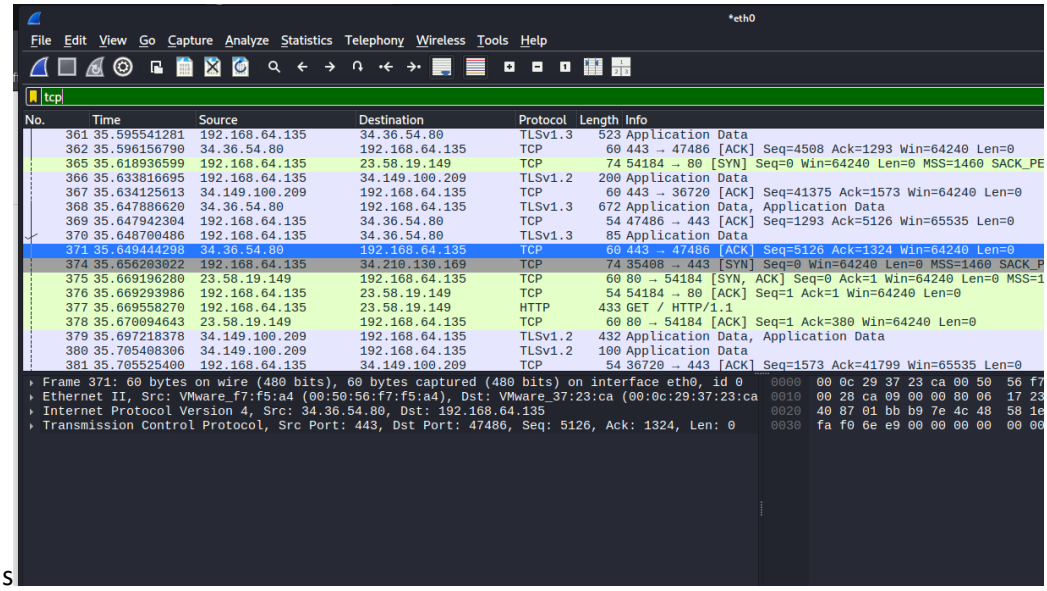
HTTP filtered packets



DNS filtered packets



TCP filtered packets



S

Conclusion

The network capture confirmed the presence of HTTP, DNS, and TCP traffic. Each protocol serves a distinct role in enabling web browsing:

- **DNS** translates domain names into IP addresses.
- **TCP** ensures reliable data delivery.
- **HTTP** enables content retrieval from web servers.