DAY 5 - TASK 5

Objective: Capture live network packets and identify basic protocols and traffic types.
Tools: Wireshark (free).
Deliverables: A packet capture (.pcap) file and a short report of protocols identified

Wireshark Protocol Analysis Report

Date of Capture: 11th Aug, 2025
Capture File: `packet_capture.pcap`
Duration: 1 minute
Interface Used: eth0

1. Overview

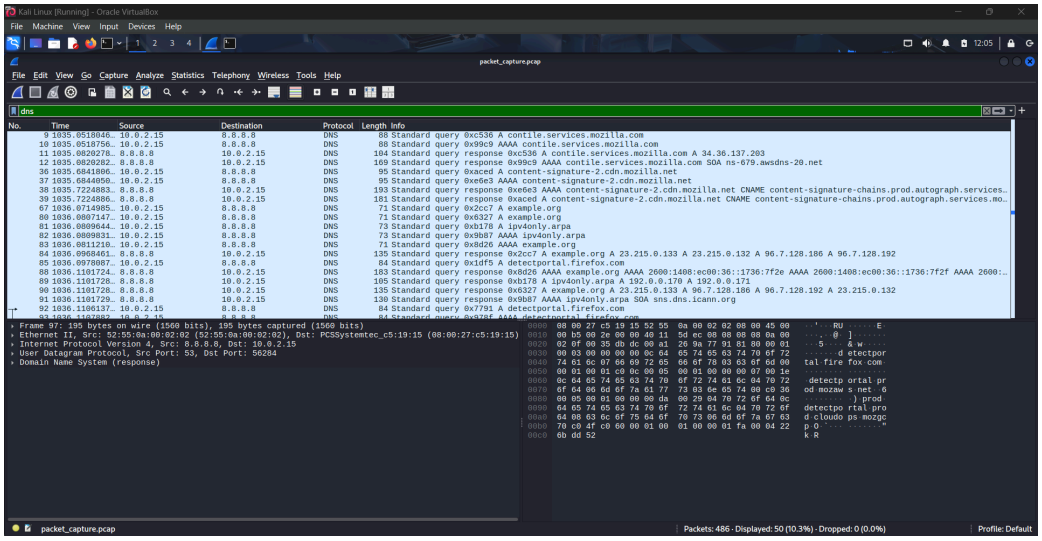
A network packet capture was performed using Wireshark to observe real-time network activity on the Kali Linux VM. The objective was to identify and analyze different network protocols involved in typical browsing activity.

---

2. Protocols Identified

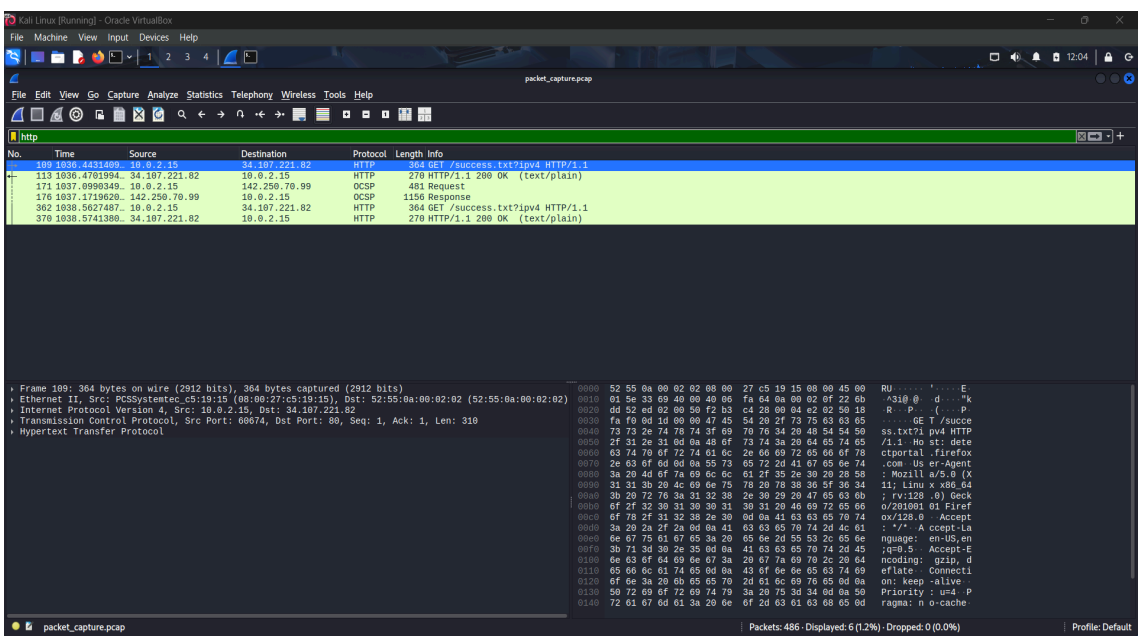
A. DNS (Domain Name System)

- **Purpose:** DNS translates human-readable domain names (e.g., `google.com`) into IP addresses for routing over the Internet.
- **Observation in Capture:**
  - Multiple DNS **Query (Standard Query A)** packets were sent from the local machine to the DNS server.
  - **Response packets** contained resolved IP addresses.
- **Port Used:** UDP 53 (sometimes TCP 53 for large responses).



B. HTTP (HyperText Transfer Protocol)

- **Purpose:** HTTP is used for transferring web pages and other web resources.
- **Observation in Capture:**
  - GET requests from the client to the server for HTML content.
  - Response headers visible in the payload.
- **Port Used:** TCP 80



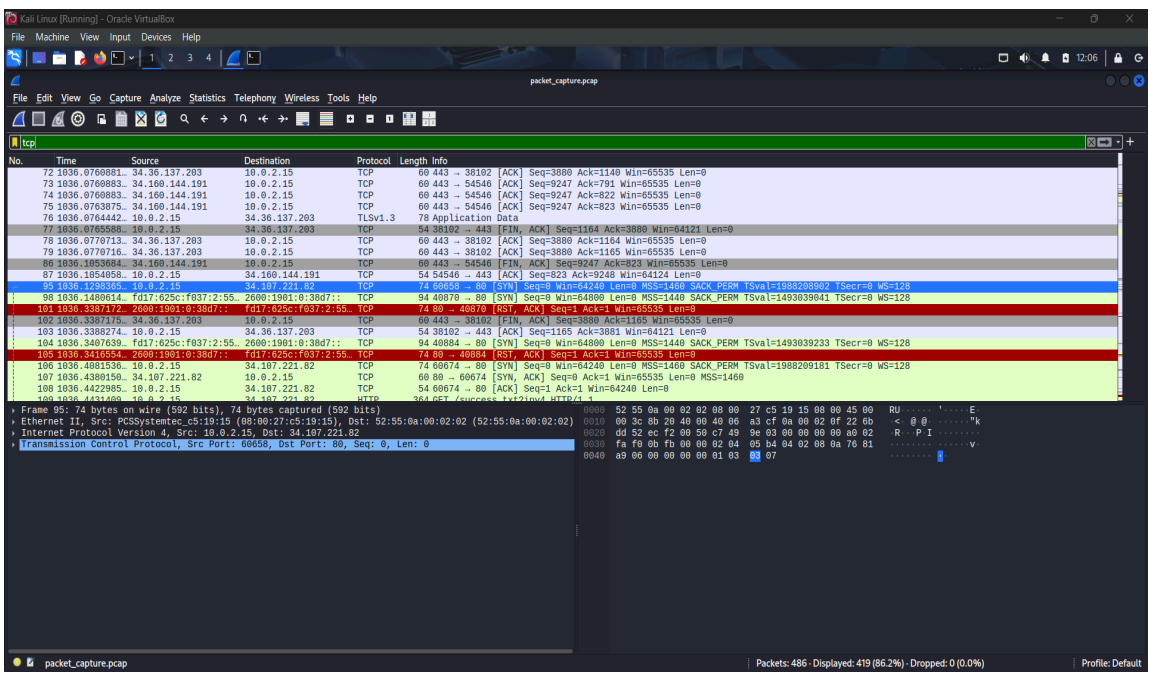
C. TCP (Transmission Control Protocol)

- **Purpose:** TCP provides reliable, ordered, and error-checked delivery of data. It underlies many application protocols like HTTP, HTTPS, and FTP.

- **Observation in Capture:**

    - Multiple TCP 3-way handshakes (`SYN`, `SYN-ACK`, `ACK`).
    - Data segments carrying HTTP and DNS traffic.
    - Connection termination packets (`FIN`, `ACK`).

- **Ports Used:** Varies depending on the application protocol (e.g., 80 for HTTP, 53 for DNS if using TCP).

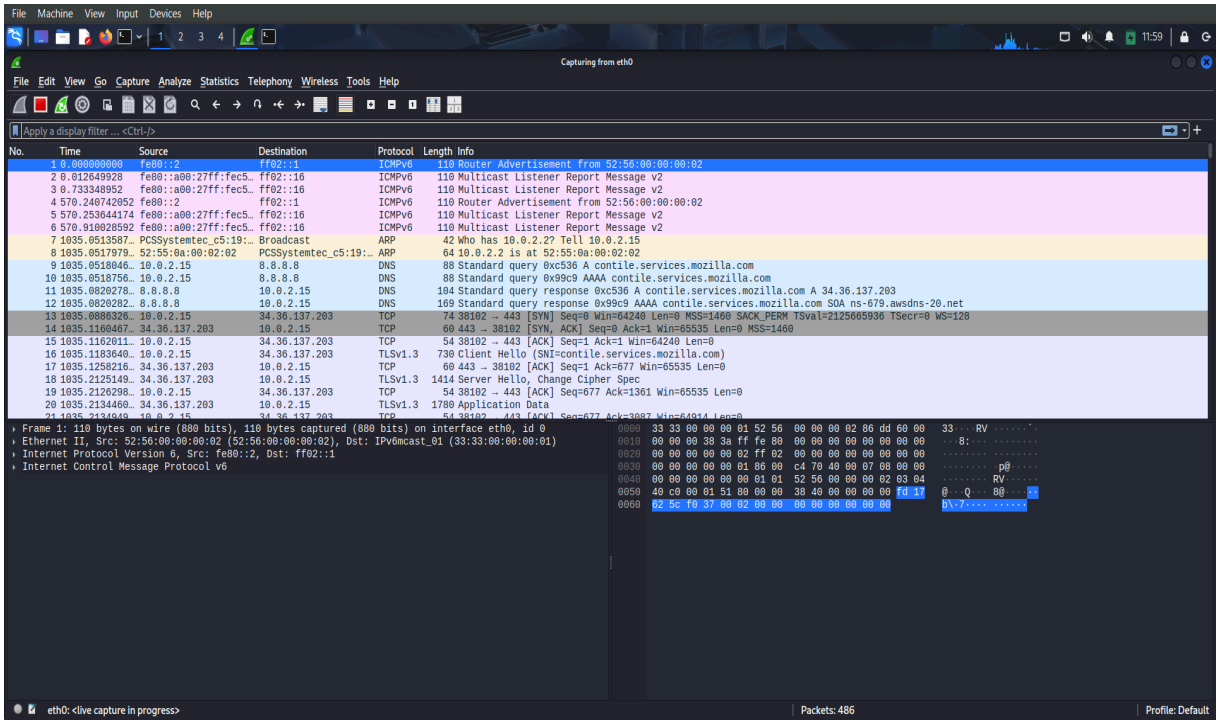


---

3. Additional Protocols (if observed)

- **ARP (Address Resolution Protocol):** Resolves IP addresses to MAC addresses within the local network.

- **ICMP (Internet Control Message Protocol):** Used for ping requests and network diagnostics.



---

4. Summary of Findings

The captured traffic primarily consisted of DNS lookups, HTTP requests, and TCP segments. The presence of these protocols confirms typical web browsing behavior, starting from DNS resolution to establishing a TCP connection and retrieving web resources over HTTP.