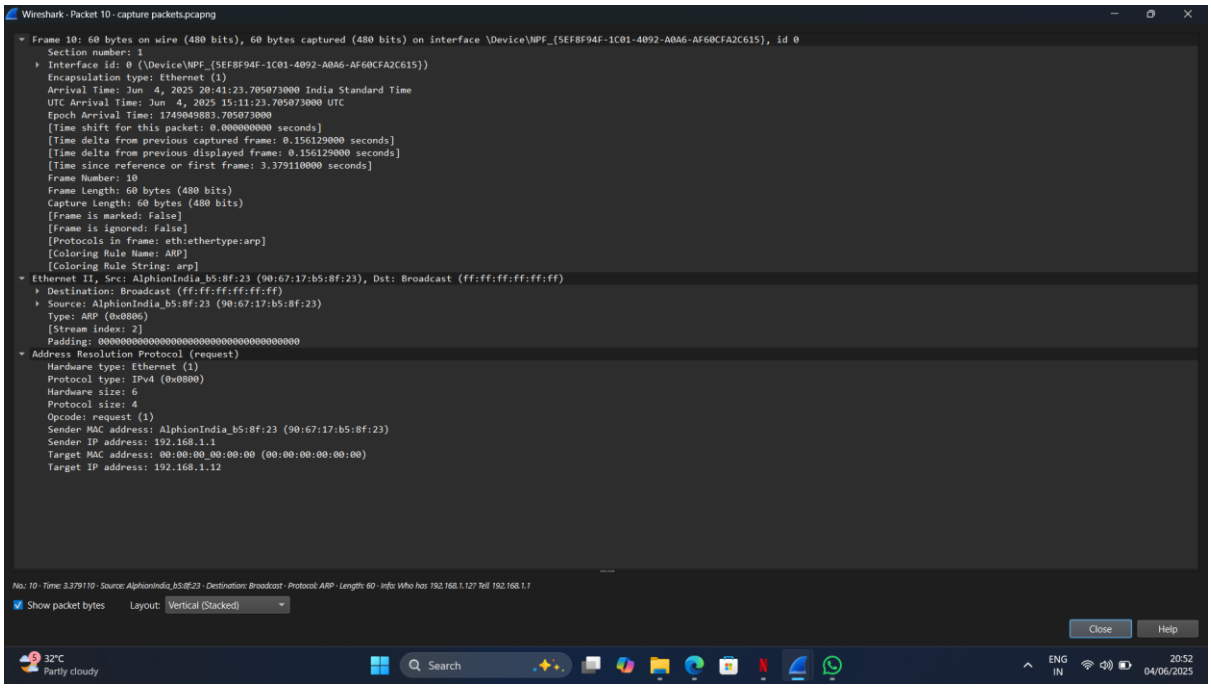
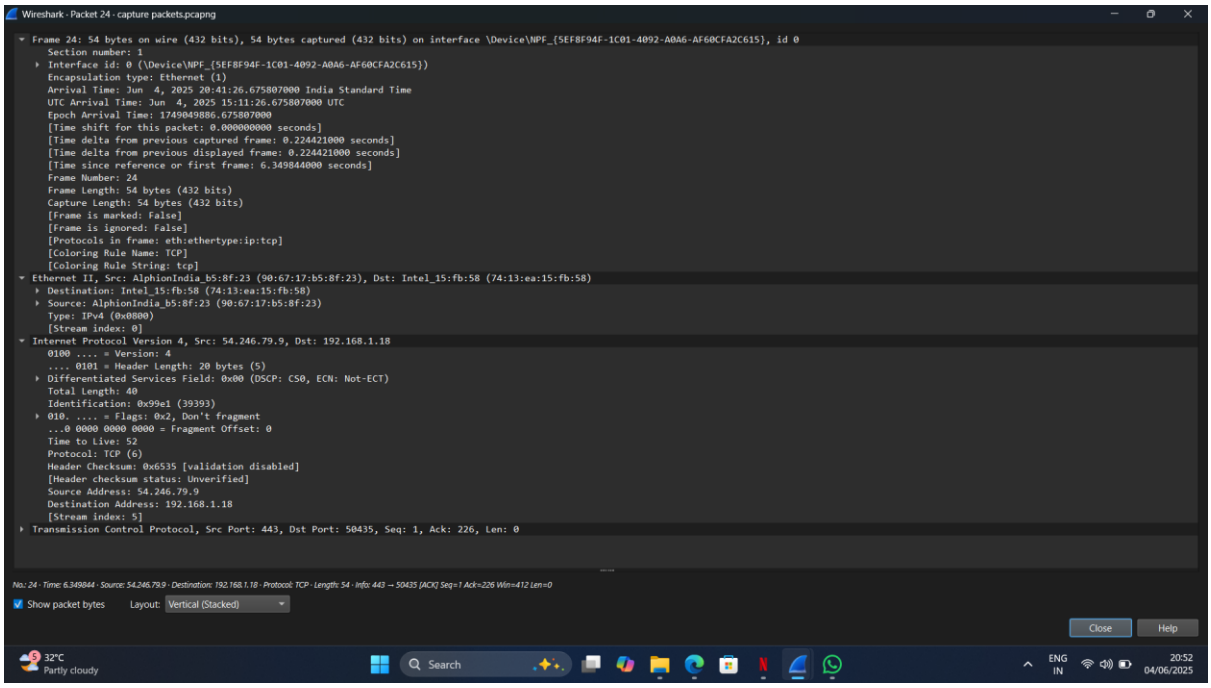
TASK-5

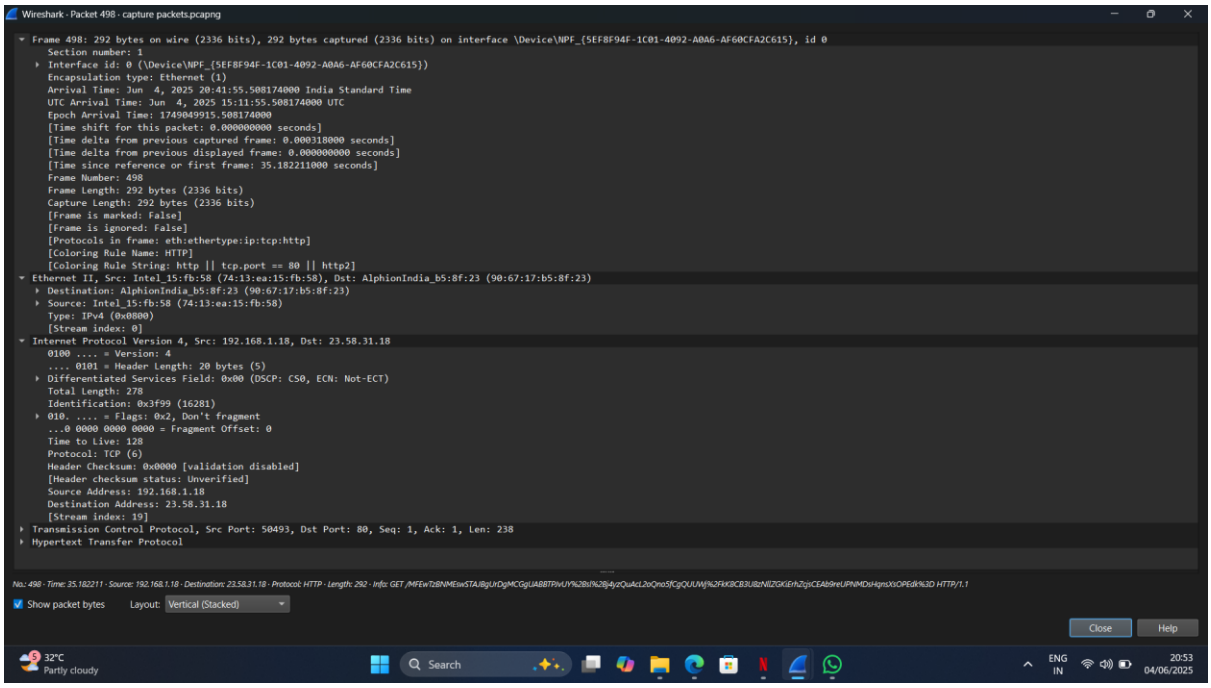
Address resolution protocol (ARP)



Transmission control protocol (TCP)



Hypertext transfer protocol (HTTP)



OFFICIAL REPORT ON NETWORK PACKET CAPTURE ANALYSIS

Report Title: Packet Capture Analysis – ARP, TCP, and HTTP Protocols
Tool Used: Wireshark
Capture File: capture packets.pcapng
Date of Analysis: June 4, 2025
Captured Interface: Ethernet (Wi-Fi)

---

1. Address Resolution Protocol (ARP) Packet Analysis

Frame Number: 10
Timestamp: 20:41:23.705
Packet Length: 60 bytes
Source MAC Address: 90:67:17:b5:8f:23 (AlphionIndia)
Destination MAC Address: ff:ff:ff:ff:ff:ff (Broadcast)
ARP Opcode: Request
Sender IP Address: 192.168.1.1
Target IP Address: 192.168.1.12

Summary:
This is a standard **ARP request**, where the host at 192.168.1.1 is asking "Who has IP address 192.168.1.12?". It is sent to all devices on the local network using the broadcast address.

---

2. Transmission Control Protocol (TCP) Packet Analysis

Frame Number: 24
Timestamp: 20:41:26.678
Packet Length: 54 bytes
Source MAC Address: 90:67:17:b5:8f:23 (AlphionIndia)
Destination MAC Address: 74:13:ea:15:fb:58 (Intel_15)
Source IP Address: 54.246.79.9
Destination IP Address: 192.168.1.18
Source Port: 443 (HTTPS)
Destination Port: 50435
TCP Flags: ACK
Sequence Number: 1
Acknowledgment Number: 226

Summary:
This packet is part of a **TCP handshake or communication** between a remote HTTPS server and a local host. The acknowledgment number indicates an active session or handshake in progress.

---

3. Hypertext Transfer Protocol (HTTP) Packet Analysis

Frame Number: 498
Timestamp: 20:41:55.508
Packet Length: 292 bytes
Source MAC Address: 74:13:ea:15:fb:58
Destination MAC Address: 90:67:17:b5:8f:23
Source IP Address: 192.168.1.18
Destination IP Address: 23.58.31.18
Source Port: 50493
Destination Port: 80 (HTTP)
HTTP Method: GET
Payload: URL-encoded request string

Summary:
This is an **HTTP GET request** from the internal host (192.168.1.18) to an external server (23.58.31.18). It contains encoded URL parameters, indicating that the user is retrieving web content over an unencrypted connection.

Conclusion & Recommendations

1. **Normal Activity:**
    - The ARP packet is typical for local IP-to-MAC resolution.
    - The TCP and HTTP packets show expected traffic types in a browsing session.
2. **Security Note:**
    - The use of HTTP (unencrypted) rather than HTTPS exposes data to potential interception. Recommend redirecting all web traffic to HTTPS to ensure confidentiality.
    - ARP requests, while normal, can be spoofed; monitor for ARP poisoning attacks.
3. **Best Practices:**
    - Use network segmentation to reduce exposure.
    - Enable ARP inspection features on managed switches.
    - Inspect and log HTTP requests for unusual patterns.