🔍 Task 5: Network Traffic Capture & Analysis with Wireshark

🎯 Objective

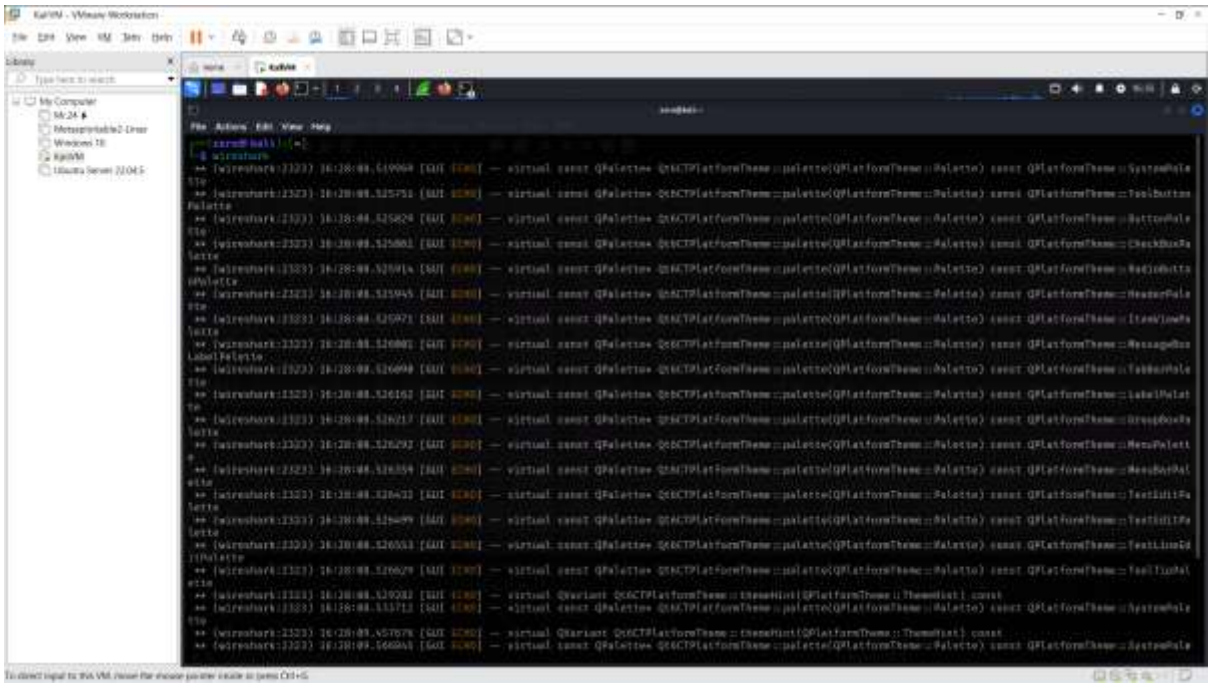
Capture live network traffic, apply filters to isolate specific protocols or hosts, and analyze packets to understand communication patterns and detect anomalies.

🛠 Environment

- **Operating System:** Kali Linux
- **Tool Used:** Wireshark

🧪 Steps Performed

1. **Opened Wireshark**



2. sudo wireshark

Selected the active interface (eth0 for wired / wlan0 for wireless).

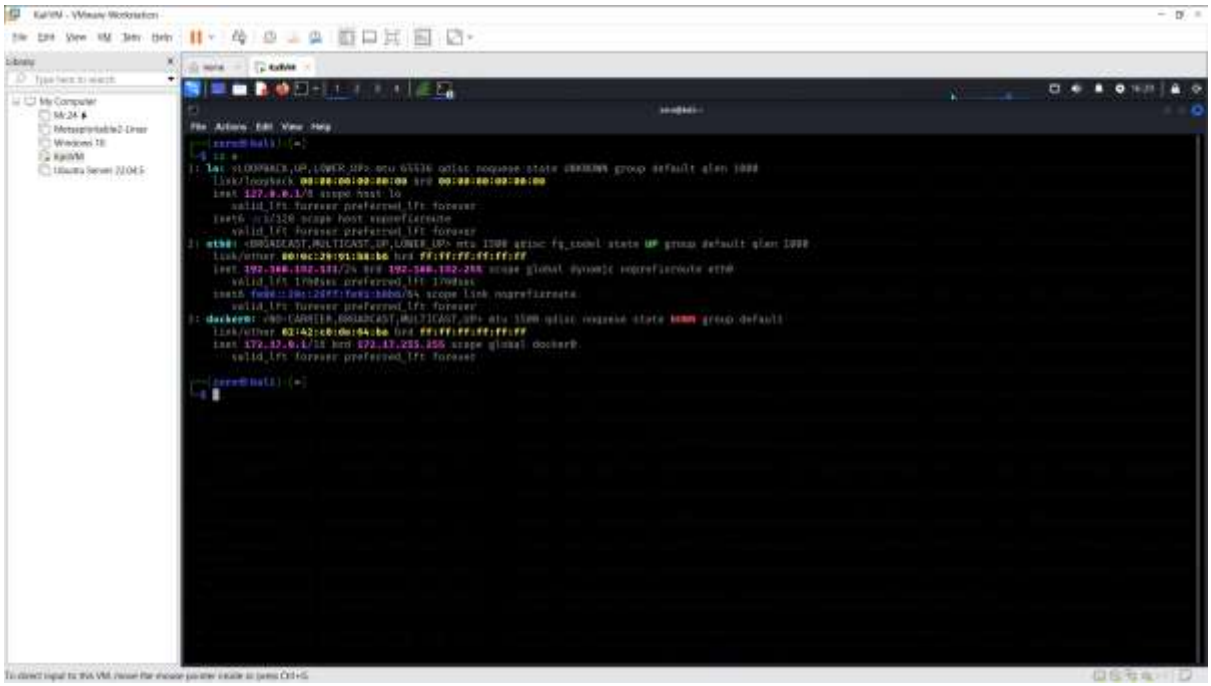
Choose the Right Network Interface

- In Wireshark's home screen, select your **active network interface**:

- **eth0** → wired
- **wlan0** → Wi-Fi

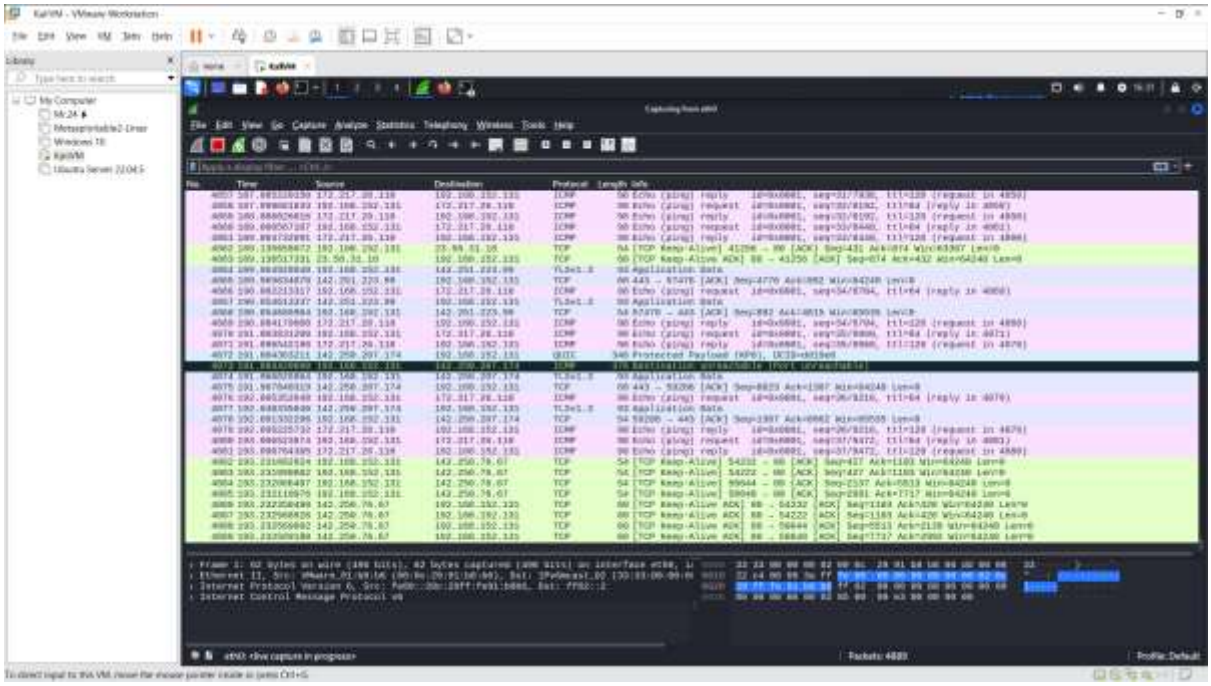
- You can confirm your active interface with:

ip a



3. **Started Packet Capture**
   Began capturing live network packets.
4. **Generated Network Traffic**
   - Visited multiple websites
   - Ran:

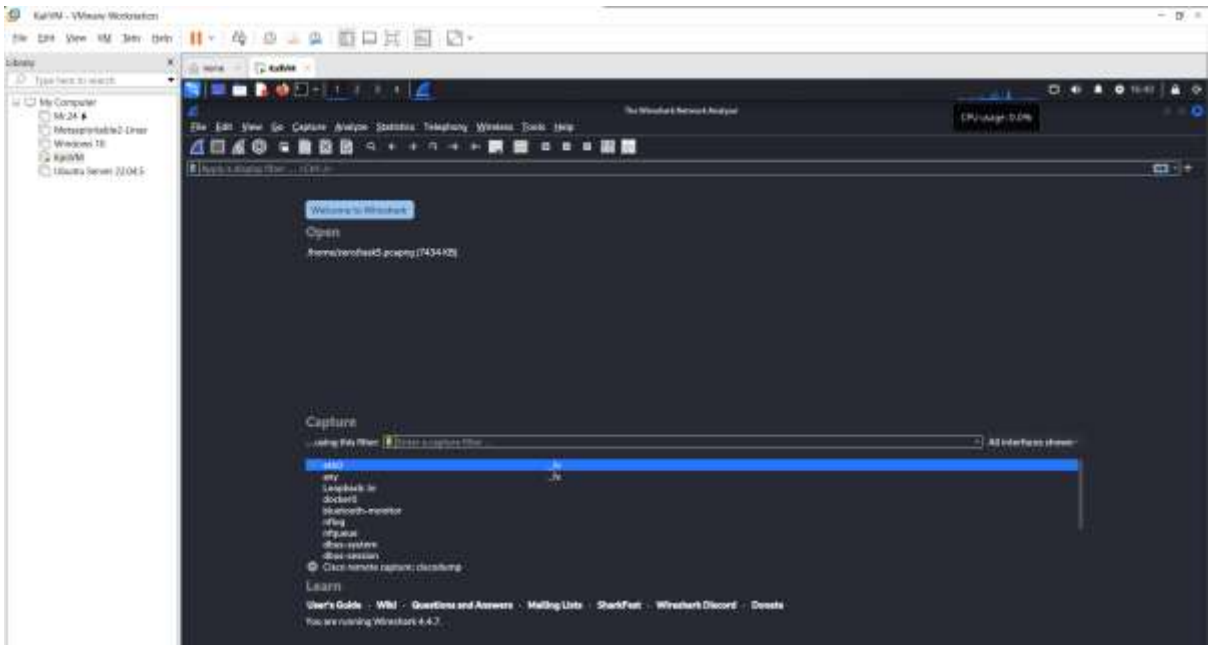
     ping google.com

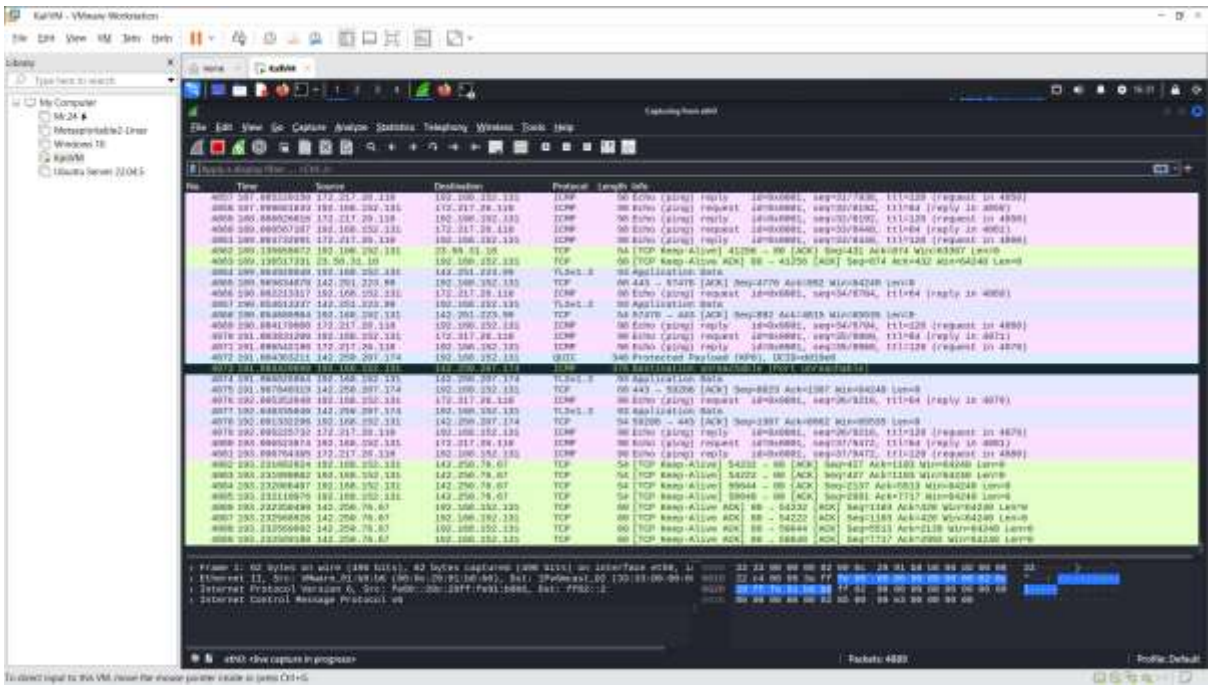


5. **Stopped and Saved Capture**
    - Saved the file as task5.pcapng for analysis.
6. **Applied Filters for Analysis**
    - **HTTP traffic**:
    - http
    - **TCP traffic**:
    - tcp
    - **Filter by IP**:
    - ip.addr == <target-ip>
7. **Analyzed Captured Data**
    - Checked **Source** and **Destination** IPs
    - Identified protocols used: HTTP, HTTPS, DNS, ICMP
    - Used **Statistics → Protocol Hierarchy** for protocol breakdown
    - Viewed **Conversations** and **Endpoints** to track communication flows

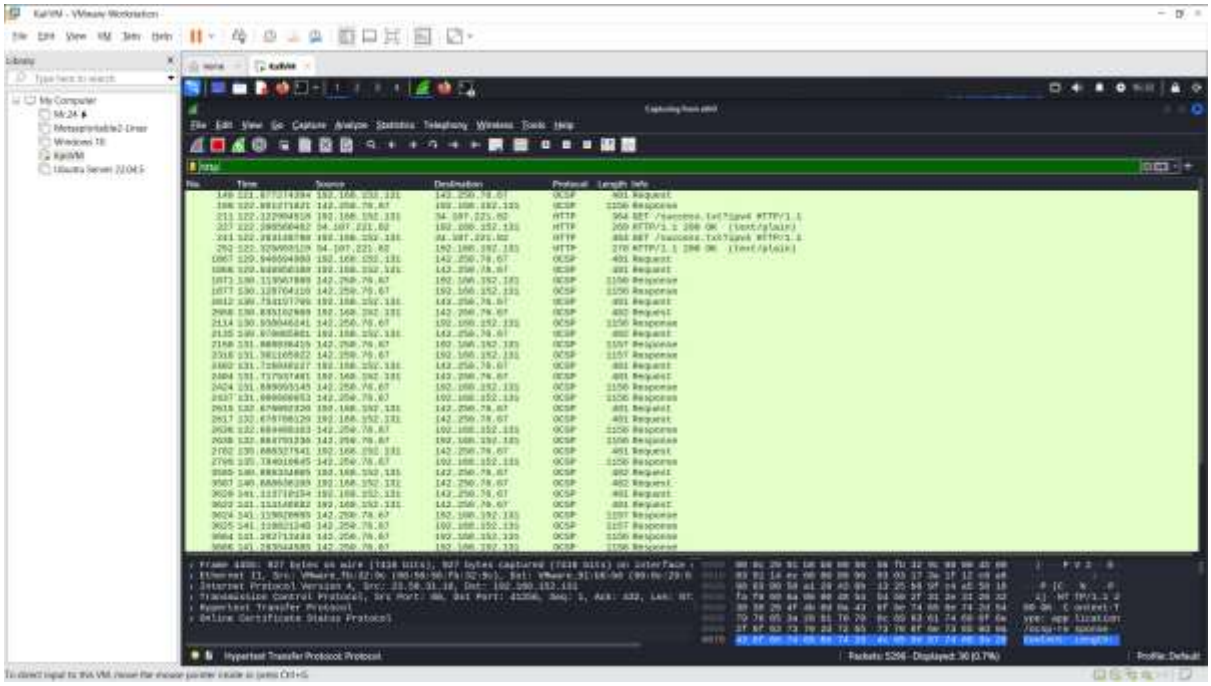
Screenshots Included

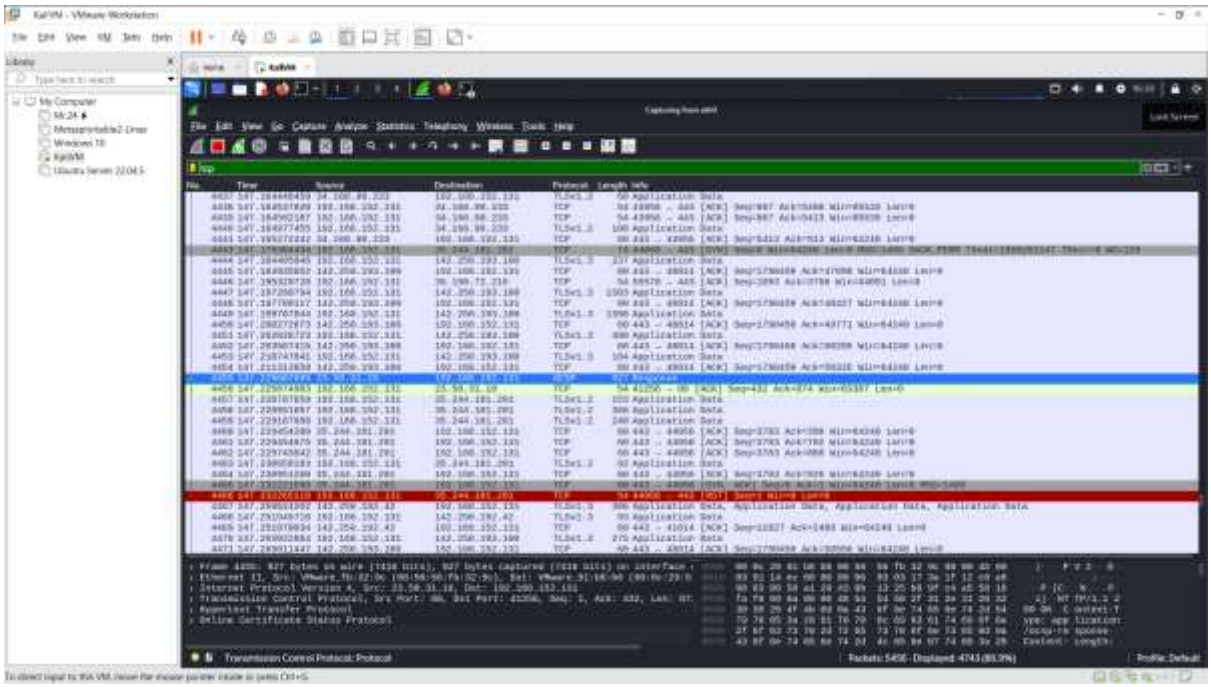
- Full capture window

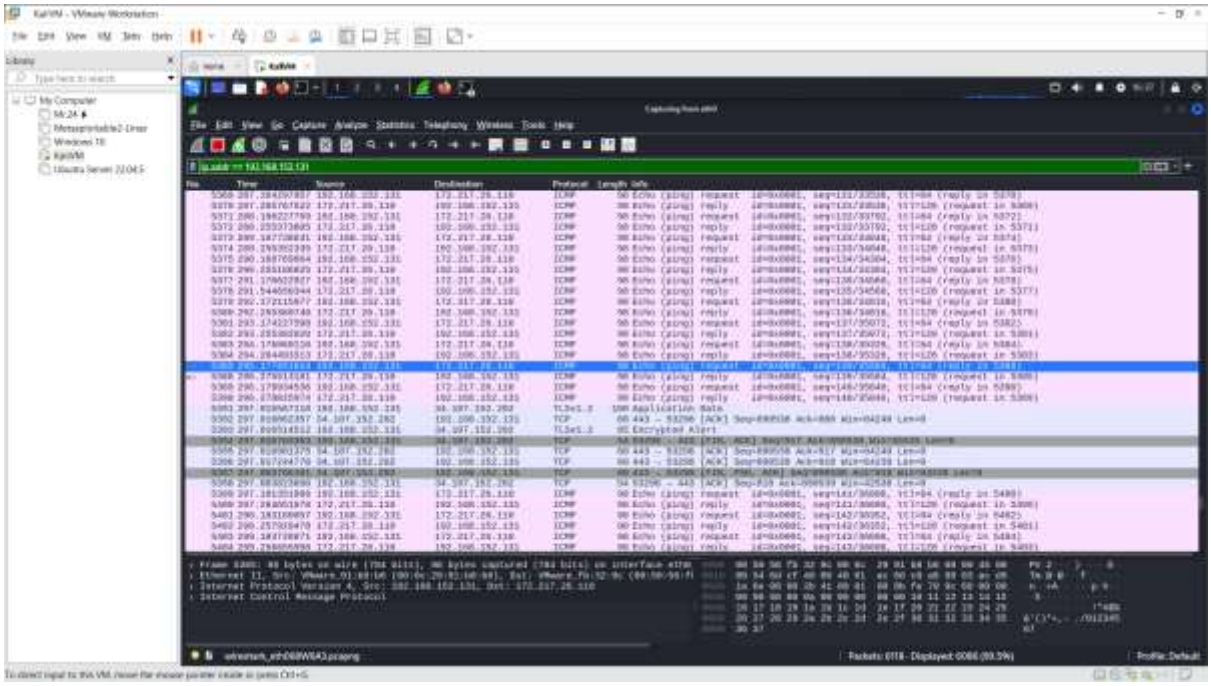




- Filtered view (HTTP/TCP)







- Protocol statistics
- Conversations & Endpoints summaries

✅ Outcome

- Successfully captured and analyzed live network traffic
- Applied protocol and IP filters for targeted inspection
- Observed different network protocols in action
- Gained insight into how data travels across the network