Network Analysis Report
Date: March 10, 2025

1. Network Scan Findings
- **Host Discovery (Nmap -sn 10.138.16.0/24):**
  - 100 hosts are active on the subnet `10.138.16.0/24`. Key live hosts include:
    - `10.138.16.1` (Likely gateway)
    - `10.138.16.48` (Highly active in packet captures)
    - `10.138.16.50`, `10.138.16.241`, `10.138.16.247`, `10.138.16.252`

- **Port & Service Scans:**
  - **10.138.16.50:** Host appears down or blocking probes (use `-Pn` for forced scan).
  - **10.138.16.241:** All 65,535 ports filtered or closed, suggesting strict firewall rules or host isolation.

2. Host Analysis (10.138.16.48)
- **Observed Activity in Wireshark:**
  - **TCP Port 143 (IMAP):** Repeated SYN packets to external IPs (`142.251.179.109/108`), indicating connection attempts to IMAP servers. Retransmissions suggest blocked traffic or no response.
  - **TCP Port 7000:**
    - Active communication with internal hosts (e.g., `10.138.16.141`, `10.138.16.77`).
    - Data exchange followed by orderly connection termination (FIN/ACK). Likely a custom service or application.
  - **RST Packets:** Host sends frequent TCP RST responses to incoming SYN/PSH packets (e.g., from `10.138.16.139`), suggesting:
    - Firewall rules blocking unauthorized connections.
    - Intrusion Prevention System (IPS) resetting suspicious sessions.

3. Wireless Monitoring Attempts
- **Interface `enp0s1`:**
  - Wired Ethernet interface with IP `10.138.16.194`. No wireless capabilities (`iwconfig` shows no extensions).
- **Failed Monitor Mode:**
  - `airmon-ng` errors due to attempts on a non-wireless interface (`enp0s1`).
  - Processes `NetworkManager` and `wpa_supplicant` were running but irrelevant for wired monitoring.

4. Key Observations
1. **Host 10.138.16.48:**
   - Acts as a critical node with both inbound and outbound traffic.
   - Aggressively resets unauthorized connections (e.g., TCP RST to port 51859).
   - May host a service on port 7000 (data exchange observed).
2. **External IMAP Traffic:**

  - Outbound SYN packets to `142.251.179.109/108` (likely Google IPs) suggest email client activity but no successful connections.
3. **Network Security:**
  - Evidence of active filtering (e.g., closed ports on `10.138.16.241`, RST responses from `10.138.16.48`).

5. Recommendations
- **Further Investigation:**
  - Scan `10.138.16.48` with `-Pn -p 7000` to confirm service details.
  - Analyze firewall rules on `10.138.16.48` to understand RST behavior.
- **Wireless Analysis:**
  - Use a wireless adapter for monitor mode; `enp0s1` is wired.
- **Traffic Decryption:**
  - Inspect TLS/SSL on port 7000 (if encrypted) to identify application protocols.

Conclusion: The network shows signs of robust security measures (filtering, RST responses). Host `10.138.16.48` is critical, with unusual activity on port 7000 and aggressive connection resets. Further targeted scans and protocol analysis are recommended.