**Task 5: Capture and Analyze Network Traffic Using Wireshark.**

**Objective:**

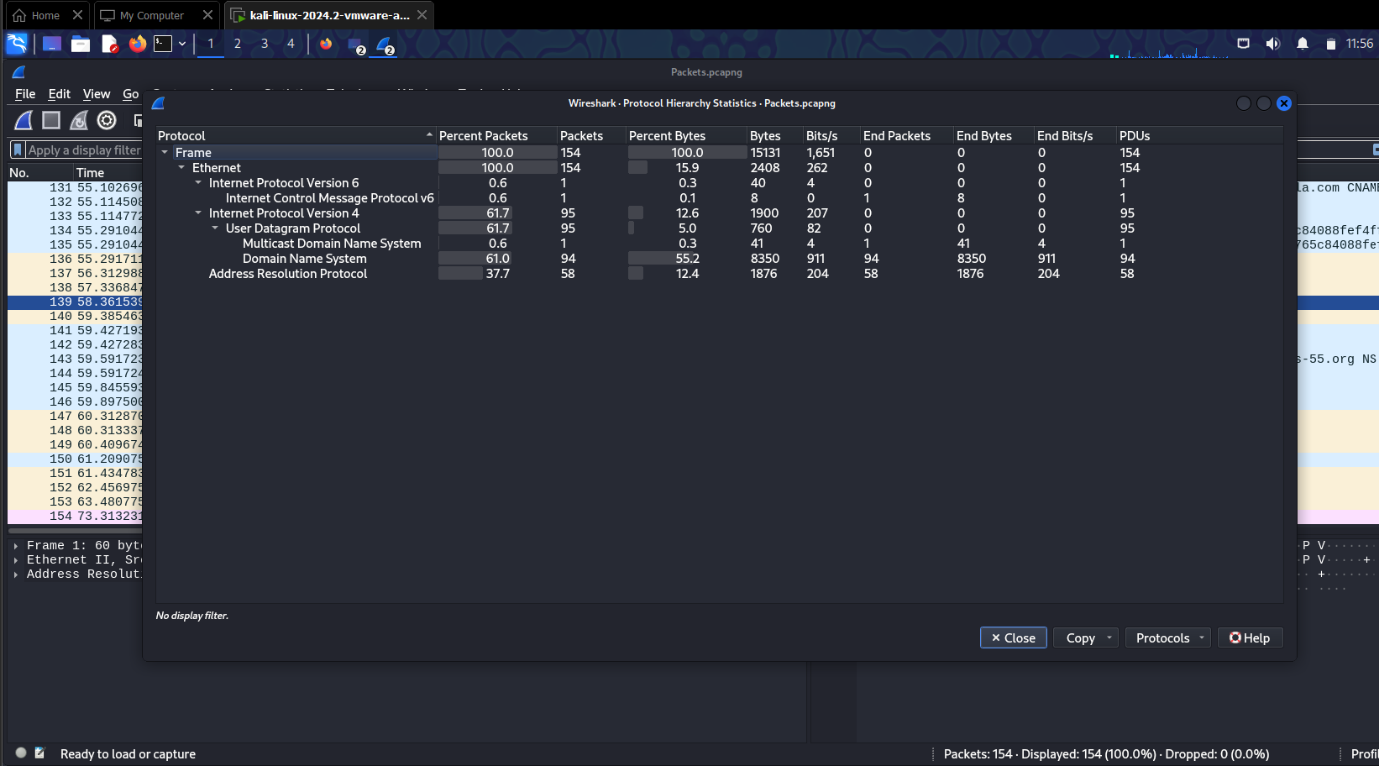
Capture live network packets using **Wireshark** and identify basic protocols and traffic types.

**Tools:**

* **Wireshark**
* **Operating System**: Kali Linux

**Procedure:**

1. **Launch Wireshark**
   * Open terminal
   * Run: sudo wireshark
   * Select network interface (e.g., wlan0)
   * Start the live capture.
2. **Generate Traffic**  
   While capturing:
   * Open Firefox
   * Browse several websites (e.g., google.com, kali.org, youtube.com).
3. **Stop and Save the Capture**
   * Stop the capture after 3–5 minutes.
   * Save as: network\_capture.pcap
4. **Analyze Packets**
   * Use **Protocol Hierarchy**:  
     Statistics → Protocol Hierarchy
   * Use filters.



**Conclusion:**

The analysis of live packet capture on Kali Linux using Wireshark showed active use of encrypted protocols like HTTPS, frequent DNS lookups, and foundational network communications such as ARP and ICMP. This reflects normal browsing behavior and demonstrates how protocol layers interact in real-time.