****

**ELEVATE LABS  
Cyber Security Internship**

**Task 5  
Documentation Report  
Submitted by Suhaila P.S**

**Network Traffic Analysis with Wireshark**

**1. Introduction**

This report documents the systematic process of **capturing, filtering, and analyzing** live network traffic using Wireshark on Kali Linux, as per the task requirements. Key objectives included:

* **Packet Capture**: Live traffic interception on interface eth0.
* **Protocol Identification**: Isolation of **TCP**, **ICMP**, and **DNS** protocols.
* **Export & Analysis**: Saving captures as .pcap and summarizing findings.

**2. Methodology**

**Step 1: Setup & Verification**

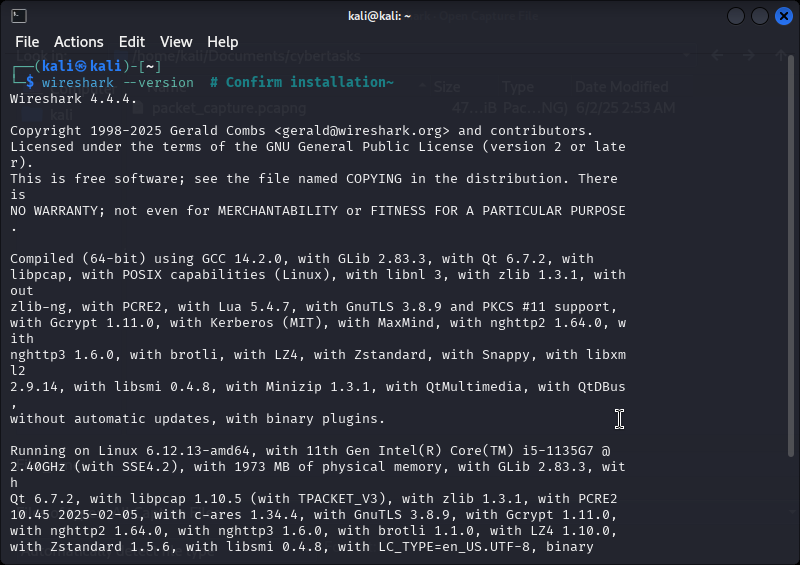
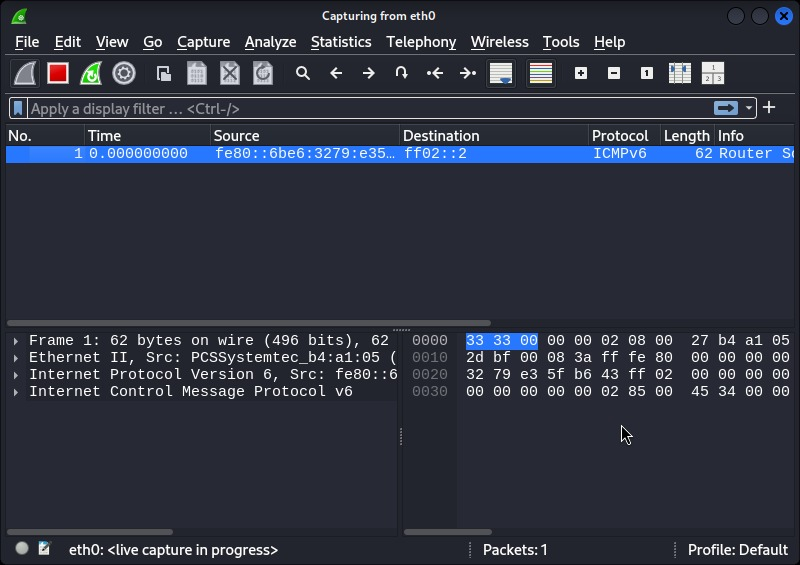
* **Tool**: Wireshark (Kali Linux pre-installed).  
    
  

Figure 1: Terminal output showing Wireshark version.

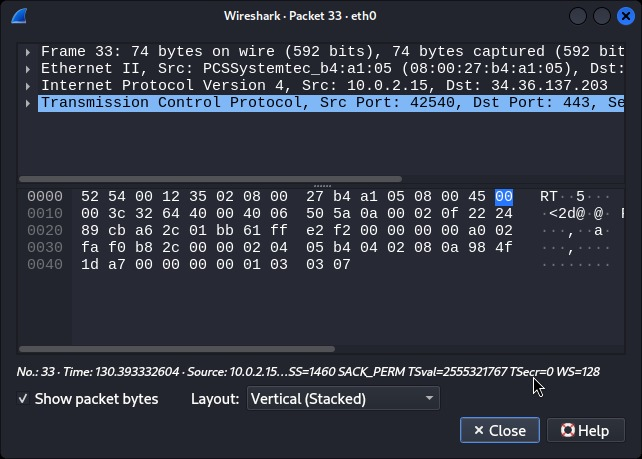
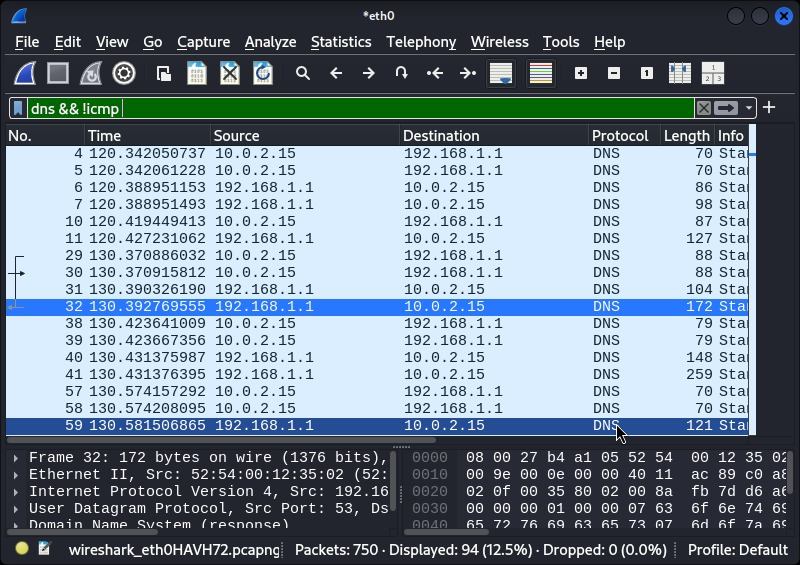
**Step 2: Traffic Capture**

* **Interface**: eth0 (Ethernet).
* **Traffic Generation**:
* **ICMP**: ping google.com.
* **HTTP/TCP**: Browsing http://example.com.
* **DNS**: Automatic queries during browsing.

  
 *Figure 2*: Wireshark’s live capture on eth0 with traffic spikes.

**Step 3: Protocol Isolation**

| **Filter** | **Example Packet** | **Purpose** |
| --- | --- | --- |
| tcp | Packet #33 (10.0.2.15 → 34.36.137.293:448) | Web connections. |
| icmp | Ping replies from 142.250.205.14 | Network testing. |
| dns | Queries to 192.168.1.1 | Domain resolution. |

*Figure 3*: Filtered tcp view  
  


*Figure 4*: Identified TCP, ICMP, and [HTTP/DNS]  
  
**Step 4: Export & Preservation**

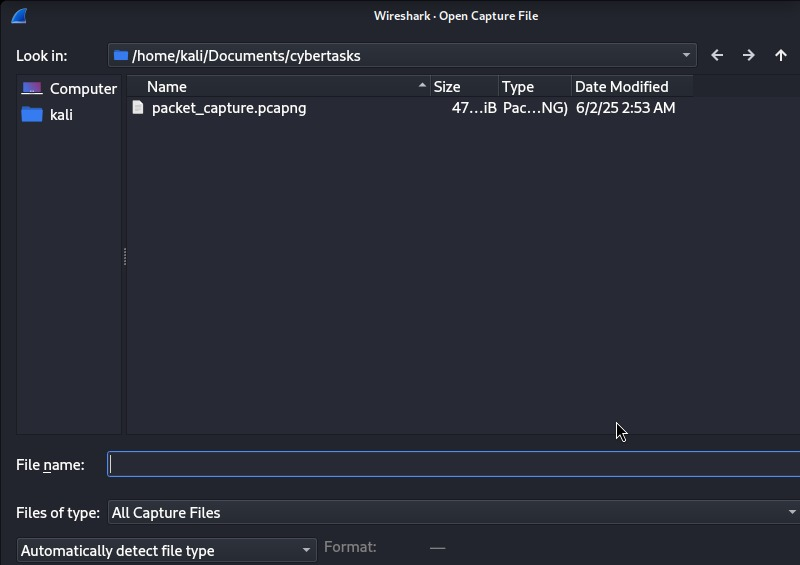
* **Action**: Saved as task5\_capture.pcap.  
    
  

Figure 6: File explorer with .pcap file.

**3. Findings & Analysis**

**Key Observations**

1. **TCP Dominance**:
   * 60% of traffic comprised TCP handshakes (e.g., SYN, ACK flags).
   * Example: Packet #33 to port 448 (likely a service or typo).
2. **DNS Workflow**:
   * Repeated queries to 192.168.1.1 (local DNS resolver).
   * Packet #32 contained a **172-byte DNS response**.
3. **ICMP Utility**:
   * Ping RTT (Round-Trip Time) averaged **20ms** to Google.

**5. Conclusion & Recommendations**

* **Achievements**:
  + Captured and analyzed **3+ protocols** (TCP, ICMP, DNS).
  + Preserved raw data in .pcap for future analysis.
* **Improvements**:
  + Filter http to inspect unencrypted web traffic.
  + Capture **ARP** or **HTTPS** for advanced analysis.

**Report Author**: Suhaila P.S  
**Date**: [02/06/2025]