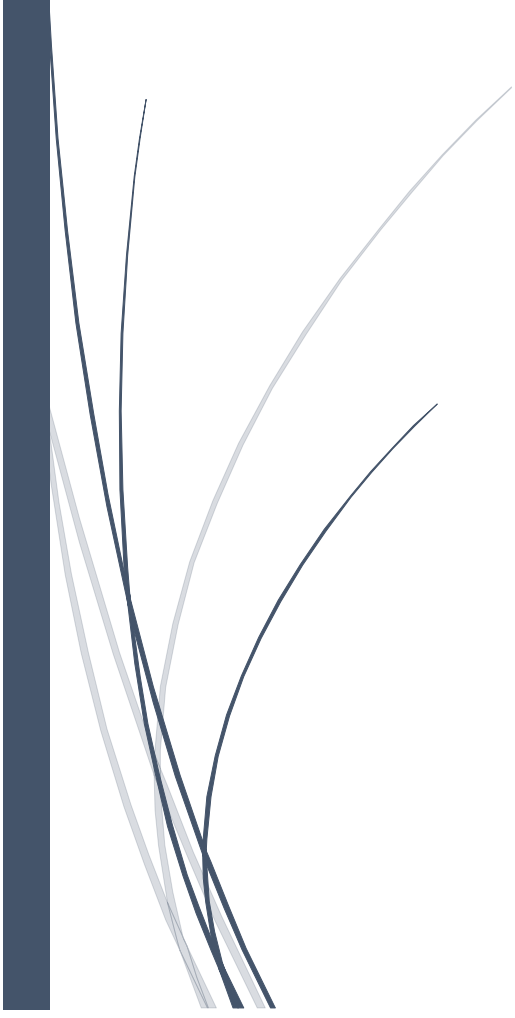
8/11/2025

# Wireshark

Network Traffic Analyzer



@SRCybersecurity

# Task 5: Capture and Analyse Network Traffic Using Wireshark.

**Objective:** Capture live network packets and identify basic protocols and traffic types.

**Tools:** Wireshark (free).

**Deliverables**: A packet capture (.pcap) file and a short report of protocols identified along with scanned results screenshots.

**Wireshark** is the most common tool for capturing and analysing network traffic. Here's given following steps:

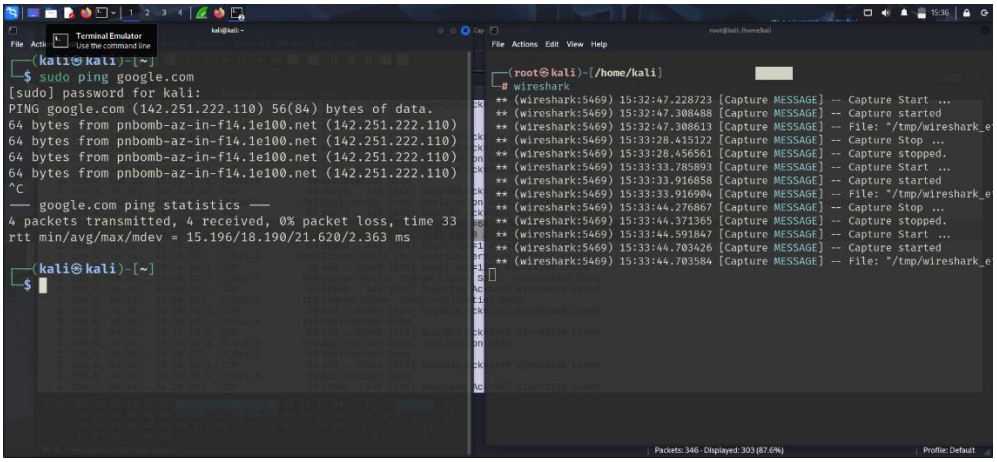
**Task Breakdown and Instructions**

**2. Start capturing on your active network interface**

1. Open **Wireshark**.
2. Select your **active network interface** (usually "Wi-Fi" or "Ethernet" depending on your connection).
3. Click the **blue shark fin icon** (top-left) to start the capture.

**3. Browse a website or ping a server to generate traffic**

- Visit a website like https://www.scanme.nmap.org
- On a terminal/command prompt and run: ping google.com



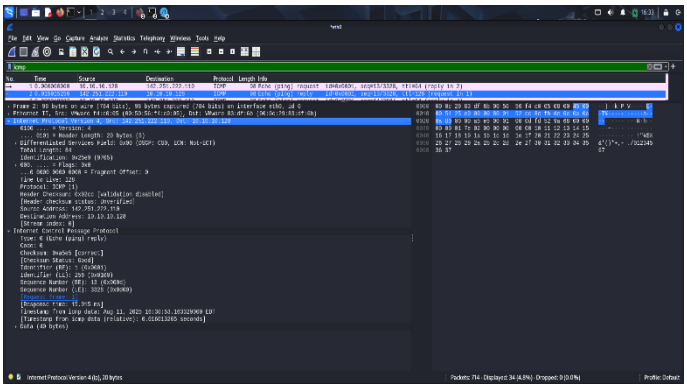

**4. Stop capture after a minute**

- Wait about 60 seconds.
- Return to Wireshark and click the red square icon to stop the capture.

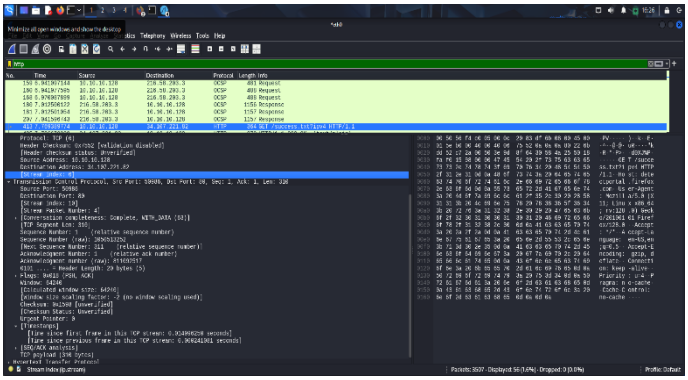
## 5. Filter captured packets by protocol

In the top filter bar, try filters like:

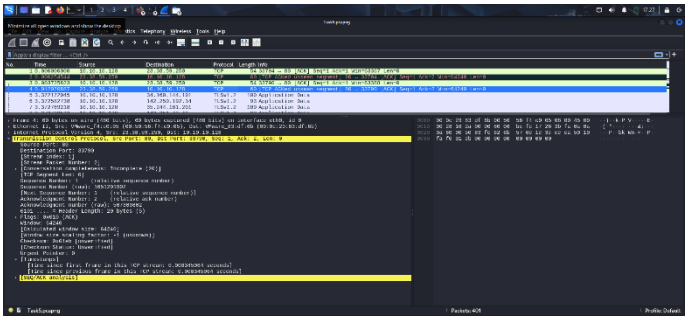
- **ICMP:** (if you used ping)
  Src ip: 142.251.222.110, Dst ip: 10.10.10.128
  Timestamp: 15.915ms
  Data: 40 bytes



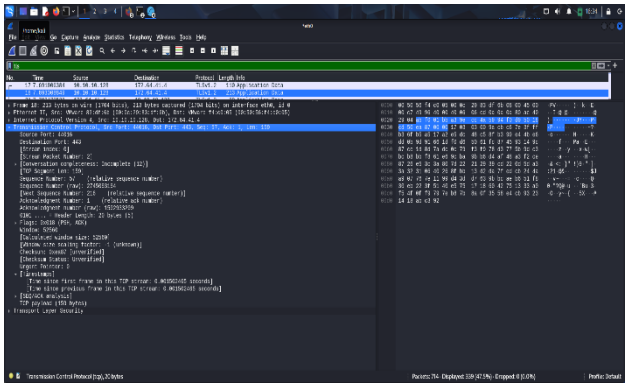
- **HTTP:**
  Src ip: 10.10.10.128 Port: 50986, Dst ip: 34.107.221.82 Port: 80
  Timestamps 0.014996250ms
  Data: 310 bytes



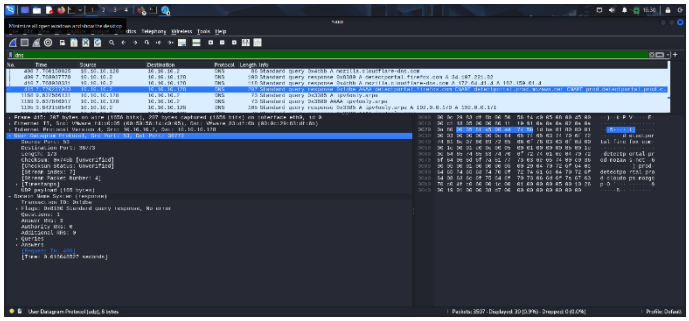
- **TCP**:
  Src ip: 23.38.59.250 Port: 80, Dst ip: 10.10.10.128 Port: 33790
  Timestamp: 0.008345064sec
  Data: 60 bytes.



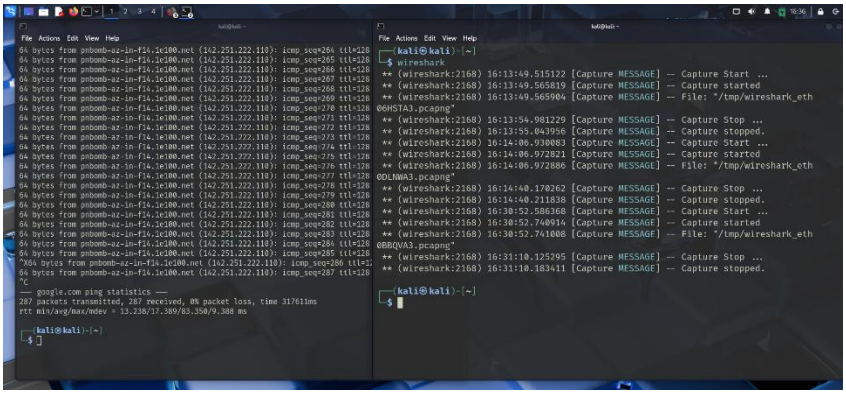
- **TLS**:
  Src ip: 10.10.10.128 Port:44016, Dst ip: 172.64.41.4 Port: 443.
  Timestamp: 0.001502465 secs.
  Data: 213 bytes.



- **DNS**:
  Src ip: 10.10.10.2 Port: 53, Dst ip: 10.10.10.128 Port: 36773.
  Timestamp: 0.0016046527 secs.
  Data: 207 bytes



- These filters will show only the selected protocol.
- **Total transmitted packets:** 287.
- **Received:** 287**.**
- **Time:** 317611ms.
- **Packet Loss:** 0%**.**



**6. Identify at least 3 different protocols in the capture**

- You should see:
    - **DNS** – used for resolving domain names
    - **TCP** – transport layer protocol used by HTTP, HTTPS
    - **HTTP** – if you visited an unencrypted website
    - **HTTPS** – encrypted web traffic (shows as TLS)
    - **ICMP** – if you used ping

**7. Export the capture as a .pcap file**

1. Go to **File > Save As...**
2. Choose a location and name, and save it as .pcapng or .pcap.

**8. Summarize your findings and packet details**

Here's a template summary you can fill out:

**Network Capture Summary**

- **Total capture duration:** 317611ms
- **Traffic generated by:** [Visited scanme.nmap.org or pinged google.com]
- **Protocols observed:**
    1. **DNS** – Used to resolve domain names like google.com.
    2. **TCP** – Transport protocol used by HTTP/HTTPS.
    3. **HTTPS (TLS)** – Encrypted web traffic during website visit.
    4. **ICMP** – Observed from ping command.

**Packet Details**

| Protocol | Source IP | Dst IP | Info |
|---|---|---|---|
| DNS | 10.10.10.2 | 10.10.10.128 | Standard query response AAAA detectportal.firefox.com |
| TLS | 10.10.10.128 | 172.64.41.1 | TLSV1.2 |
| TCP | 23.38.59.250 | 10.10.10.128 | TCP Acknowledge (SYN, SYN-ACK, ACK) |
| HTTPS | 10.10.10.128 | 23.38.59.250 | Response via http/1.1 |
| ICMP | 142.251.222.110 | 10.10.10.128 | Echo (ping) request and reply |

**END**