Minor 2 Project

Project 2: Network Traffic Analysis & Incident Investigation Using PCAP (SOC Analyst Simulation)

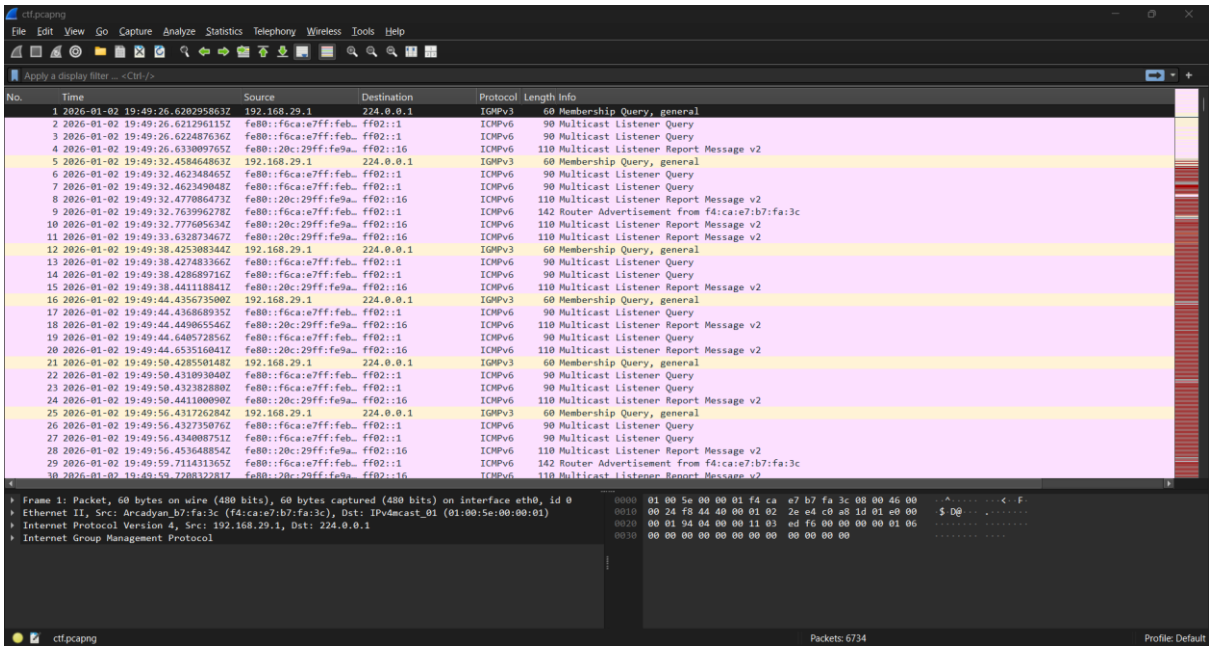
I am working as a Junior SOC Analyst in the Security Operations Centre of my organisation. During routine monitoring, one of the internal systems was suspected to be compromised. As part of the incident response process, the SOC team captured the network traffic (PCAP file) during the suspected incident window and provided it to me for detailed analysis.

My task was to analyse the PCAP file using Wireshark, following real-world SOC investigation methodologies. During the analysis, I focused on identifying the attacker's IP address, determining which internal system was the victim, and understanding the nature of the suspicious activities observed in the network traffic.

I examined the traffic patterns to identify reconnaissance activity, such as port scanning, and further analysed the HTTP traffic to determine how sensitive data was transferred over the network. During this investigation, I identified that a ZIP file containing sensitive data was downloaded using unencrypted HTTP communication.

Using Wireshark's file reconstruction features, I successfully extracted the ZIP file from the PCAP, analysed its contents, and retrieved the hidden flag. All findings were documented with appropriate screenshots and evidence, replicating the workflow of a real SOC analyst during a network-based incident investigation.

1.Open the PCAP file in Wireshark

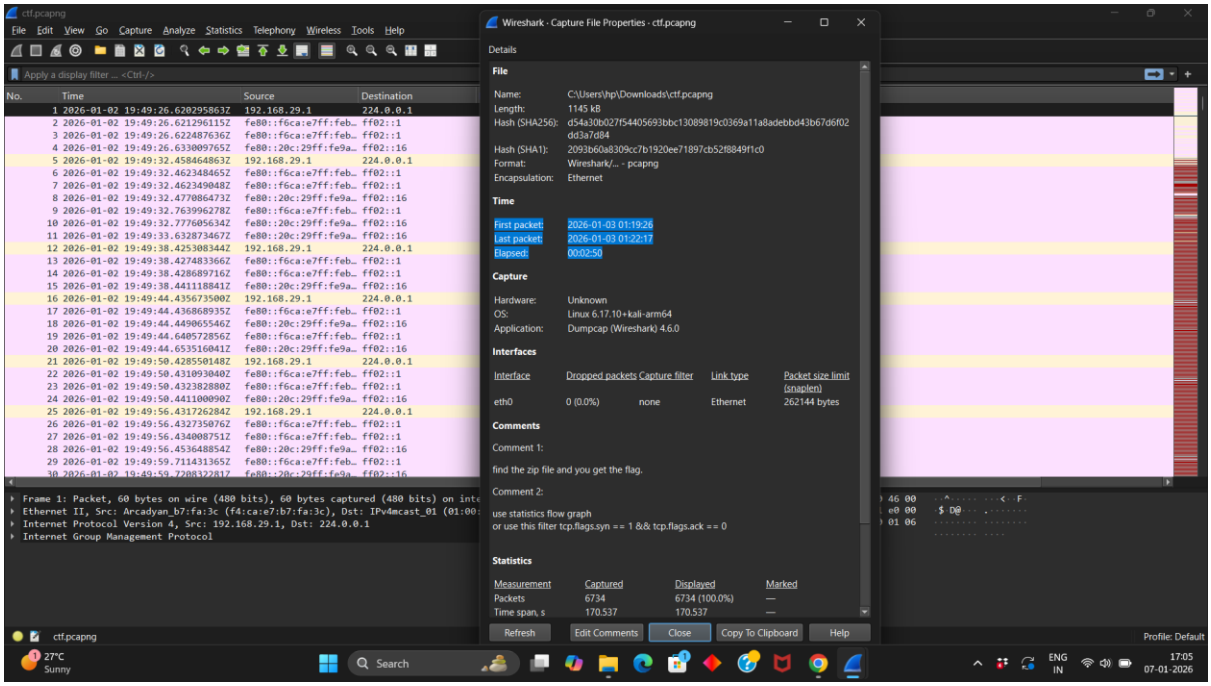


Statistics → Time

When the traffic started – 03 Jan 2026 (01:19:26)

When suspicious activity End – 03 Jan 2026 (01:22:17)

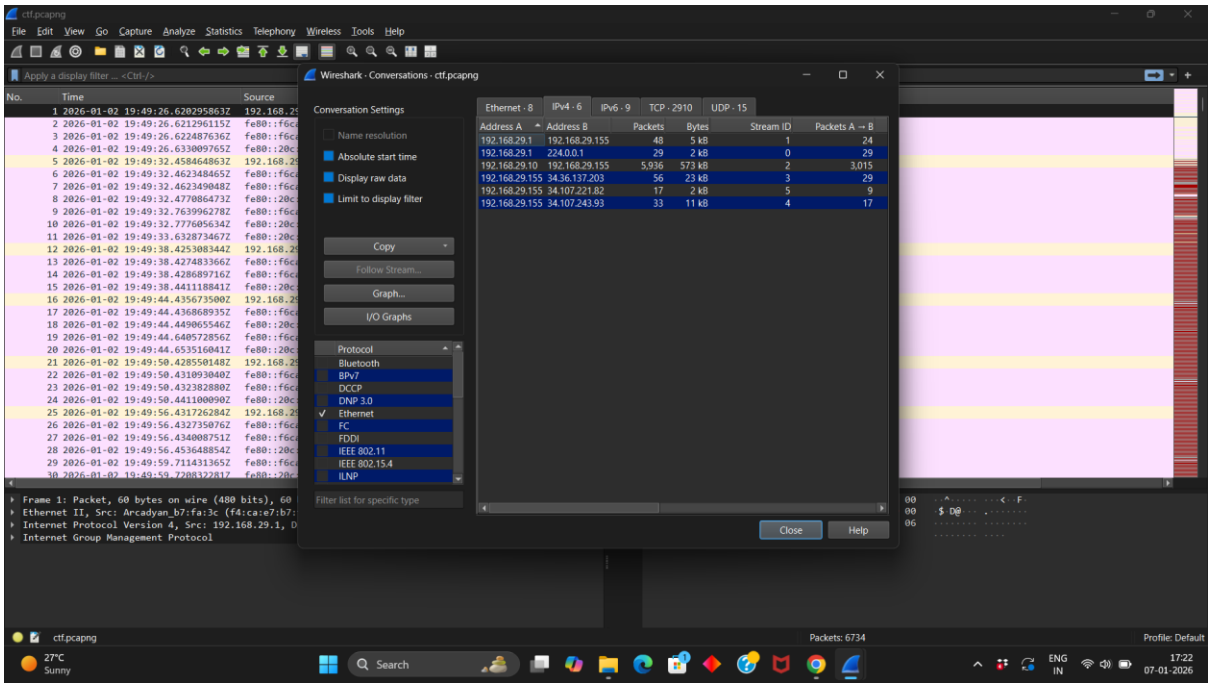
How long the activity Lasted - 02 min 50 sec



2. Analyse network traffic patterns

Conversation → IPv4

- section of Wireshark, the third row shows communication between Address A (192.168.29.10) and Address B (192.168.29.155). This conversation contains a significantly high number of packets compared to other entries, which indicates abnormal traffic and is considered suspicious.

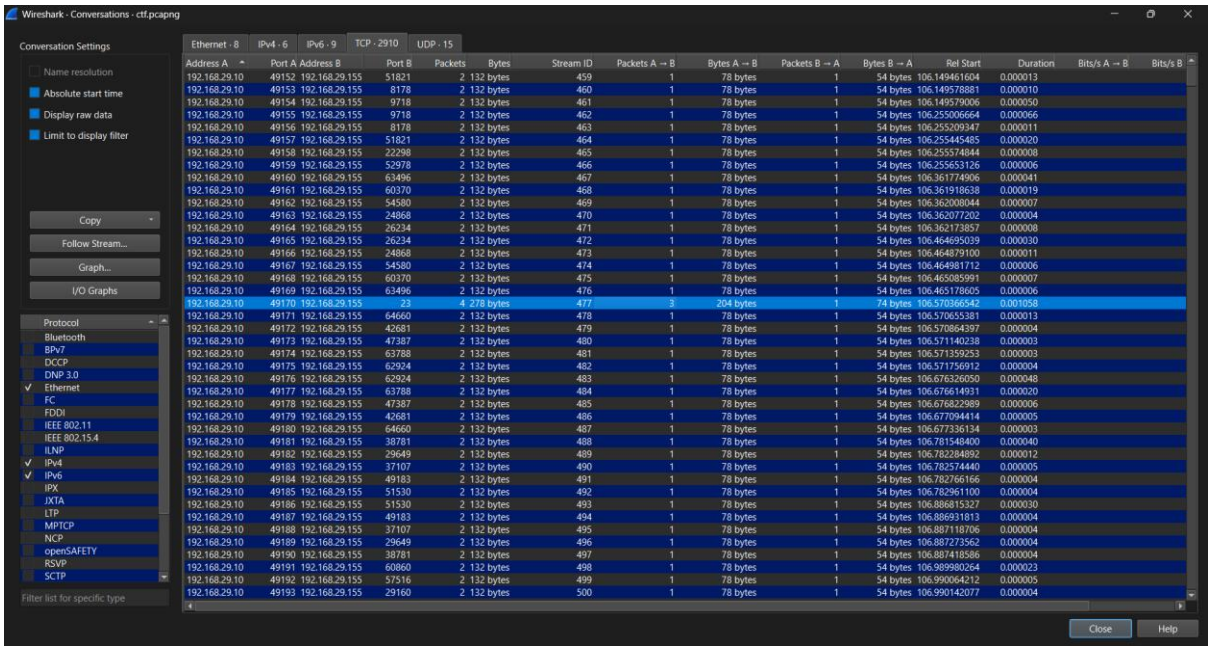


3. Identify the attacker and victim

Conversation → TCP

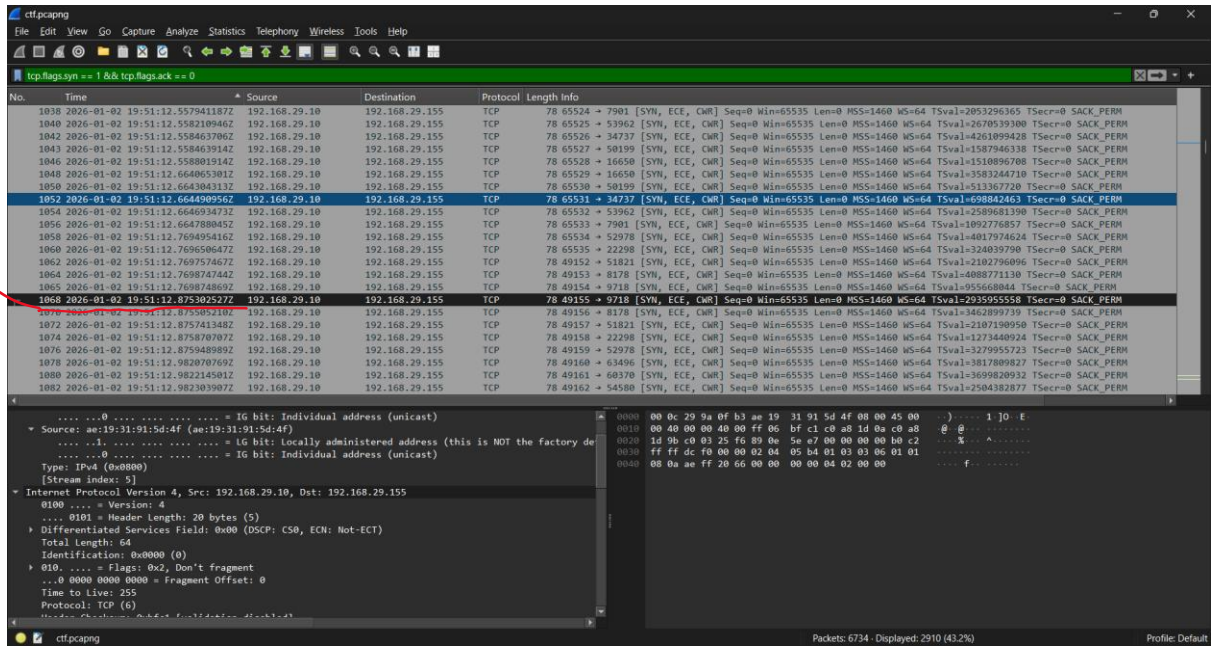
In this image IP (192.168.29.10) it's appears to be hitting a lot of ports towards IP (192.168.29.155).

- Victim → 192.168.29.155
- Attacker → 192.168.29.10



4.Determine when the attack started

5.Identify reconnaissance activity (port scanning)



Command: tcp.flags.syn == 1 && tcp.flags.ack == 0

TCP Three-Way Handshake

TCP establishes a connection using a three-step handshake process:

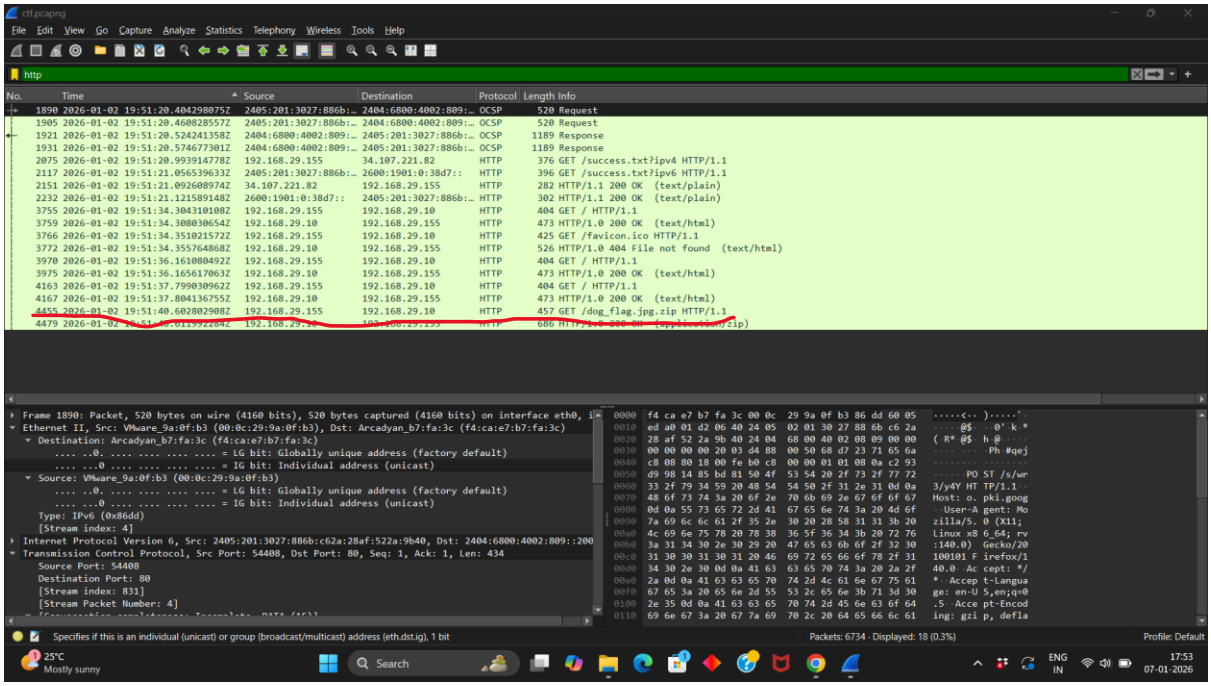
- **SYN** → The client sends a request to initiate a connection.
- **SYN-ACK** → The server responds to the client's request.
- **ACK** → The client acknowledges the server's response and the connection is established.

Explanation of the Command:

1. **tcp.flags.syn == 1**
   This condition selects packets where the **SYN (Synchronize)** flag is set. It indicates an attempt to initiate a TCP connection and is typically used when a client tries to connect to a specific port on a server.

2. **tcp.flags.ack == 0**
   This condition selects packets where the **ACK (Acknowledgment)** flag is not set. This means the packet is not acknowledging any previous communication.

6.Find the HTTP file download



After finding the HTTP

dog_flag.jpg.zip

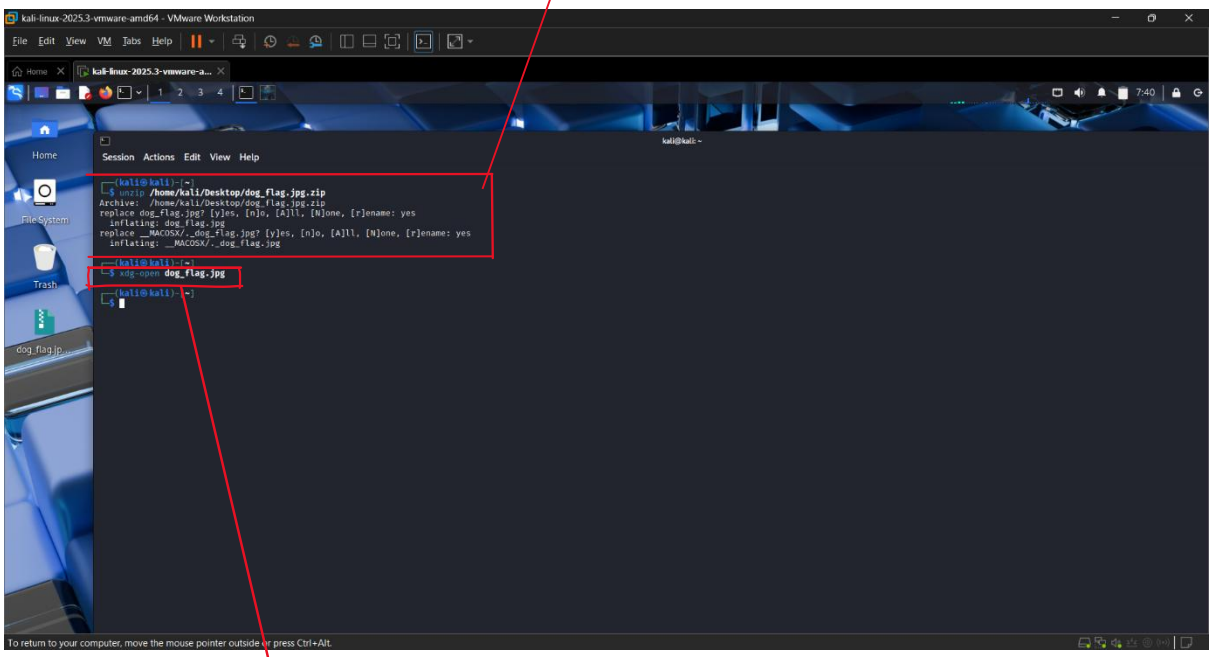
7. Extract the ZIP file from the PCAP

1. Go to file
2. Extract object
3. Choose the fiel (dog_flag.jpg.zip)
4. Save

8. Unzip the file

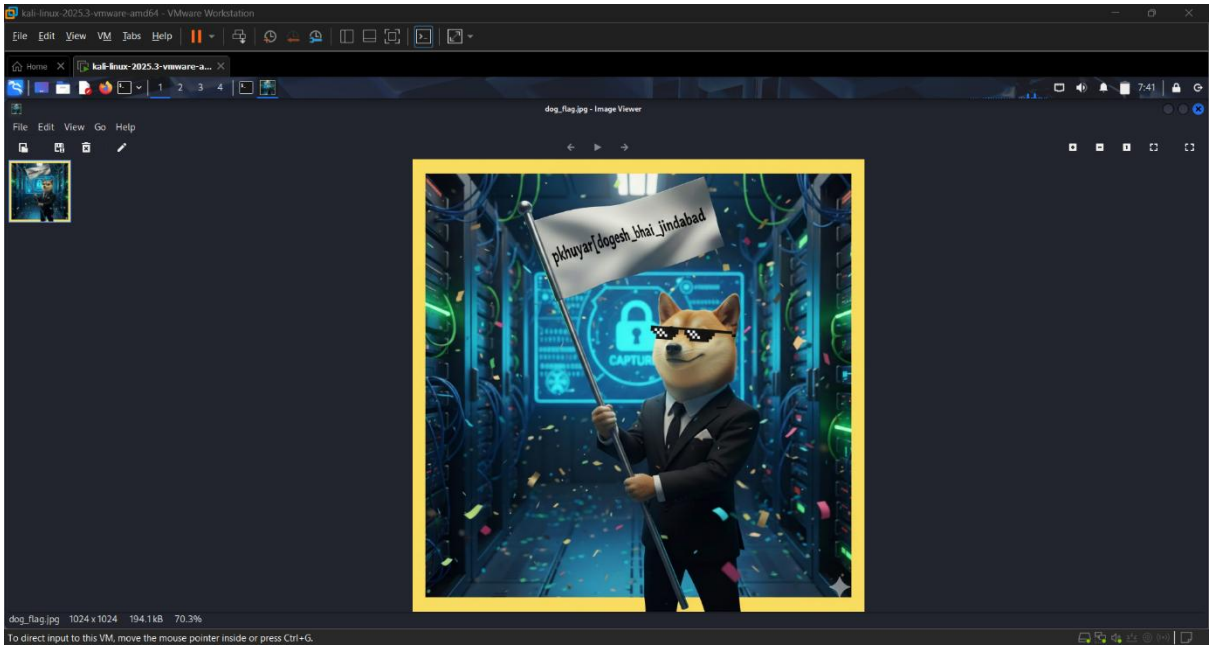
1. Go to Linux
2. Drag or copy the zip file in Linux OS
3. Open terminal
4. Run command to unzip

Command to unzip



The command **xdg-open** dog_flag.jpg is used in Linux to open a file using the system's default application. It will open the file in default image viewer.

Retrieve the flag



Questions to Answer

Answer the following questions one by one in your report:

1. What is the attacker IP address?

Ans→ 192.168.29.10

2. What is the first packet timestamp related to the attack?

Ans→ 2026-01-02 19:51:12.875302527Z

3. What evidence suggests that port scanning (reconnaissance) was performed?

Ans→ TCP 3-way handshake

4. What is the name of the downloaded ZIP file?

Ans → dog_flag.jpg.zip

5. What is the flag obtained after unzipping the file?

FLAG{pkhuyar_[doges_bhai_jindabad}