Network Traffic Analysis & Incident Investigation Using PCAP

Presented by
Nikhil Kumar, ERP ID: [6606652]

Certificate of Completion

This is to certify that
Nikhil Kumar ,ERP ID: [6606652]
has successfully completed the project titled
"Network Traffic Analysis & Incident Investigation Using PCAP (SOC Analyst Simulation)"
during the semester of **3rd Semester** under the subject of **Cyber Security Minor2.**
This project demonstrates a comprehensive understanding of network security protocols and incident analysis techniques, adhering to academic standards set forth by Rungta college of engineering and technology at **CSVTU.**
Date: January 6, 2026
Signature: _____

Declaration of Originality

I hereby declare that this project report titled "Network Traffic Analysis & Incident Investigation Using PCAP (SOC Analyst Simulation)" is my original work. I have conducted the research, analysis, and writing independently, adhering to the ethical guidelines of academic integrity.

- All sources of information and data used in this report are properly cited.
- No part of this work has been submitted for any other academic purpose.
- I understand the importance of plagiarism-free submissions and have ensured that this report complies with the standards set by my institution.

Acknowledgement

I would like to express my sincere gratitude to my project guide and mentors for their invaluable support and guidance throughout this project. Their insights helped shape the direction of my work, enabling me to successfully navigate the complexities of network traffic analysis.

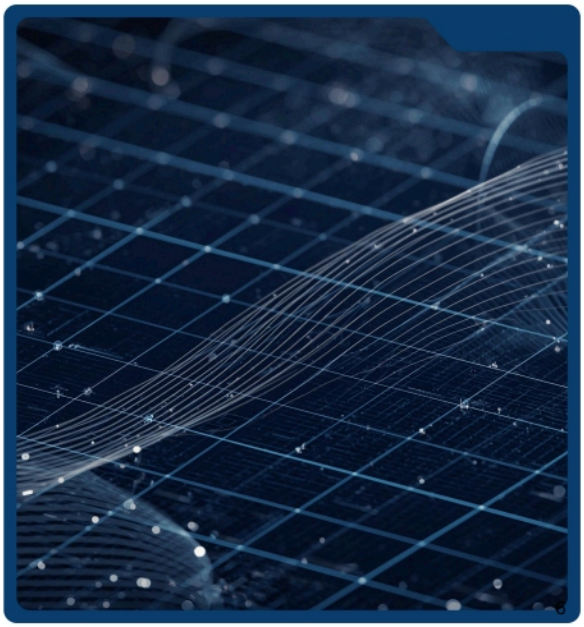
Abstract

Summary of Project Findings and Objectives

This project focuses on **network traffic analysis** and incident investigation utilizing PCAP files, simulating a SOC analyst's role to enhance cybersecurity knowledge and practical skills.

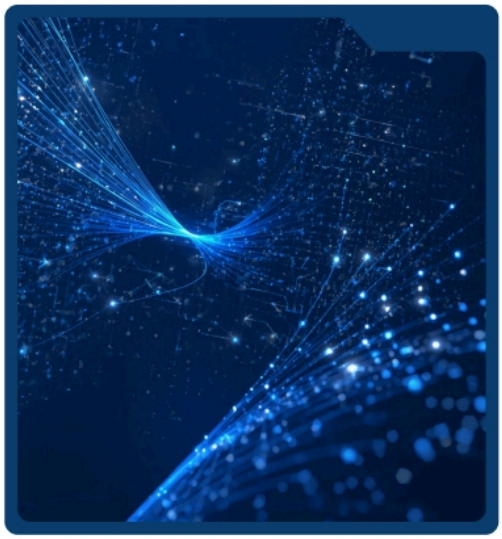
Table of Contents

Overview of Project Sections



Introduction

This section delves into **network traffic analysis** and the importance of incident investigation in cybersecurity. By analyzing packet data and traffic patterns, organizations can enhance their security posture, detect anomalies, and efficiently respond to potential threats, ensuring robust network defense mechanisms.



📌 Tools Required

1.Wireshark (latest version)
2.PCAP file
3.7-zip/WinRAR
4.Windows/Linux system

What is SOC?

A Security Operations Center (SOC) is a centralized team responsible for monitoring, detecting, and responding to cybersecurity threats within an organization. It continuously analyzes network traffic, system logs, and security alerts to identify and prevent cyber attacks.

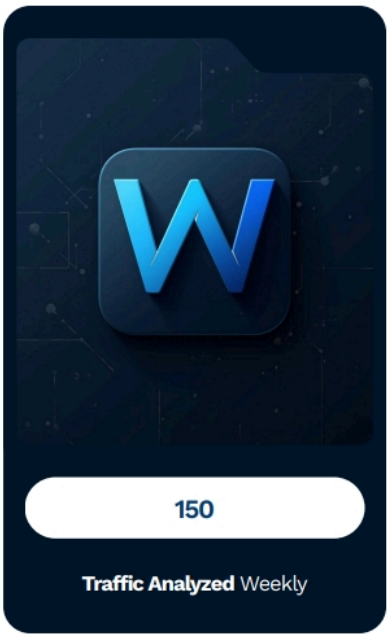
What is PCAP?

PCAP (Packet Capture) is a file format used to store captured network traffic. It contains detailed information about data packets such as source IP, destination IP, protocol, ports, and payload.

Objectives of investigation..

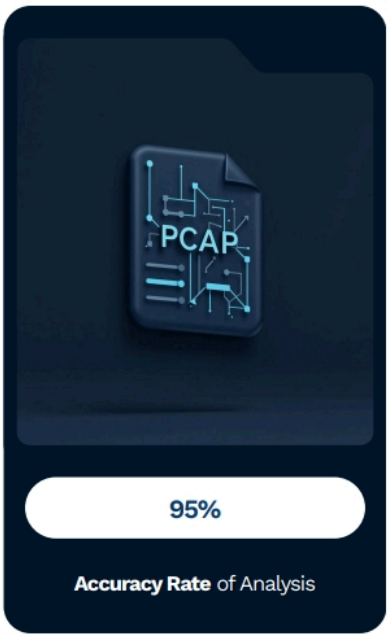
The main objectives of this investigation are:

- *To analyze network traffic using a PCAP file.*
- *To identify the attacker and victim systems involved in the incident.*
- *To detect reconnaissance activities such as port scanning.*
- *To analyze suspicious HTTP traffic and file transfers.*
- *To extract the transferred ZIP file and retrieve the flag.*
- *To document the findings in a structured SOC analyst report.*



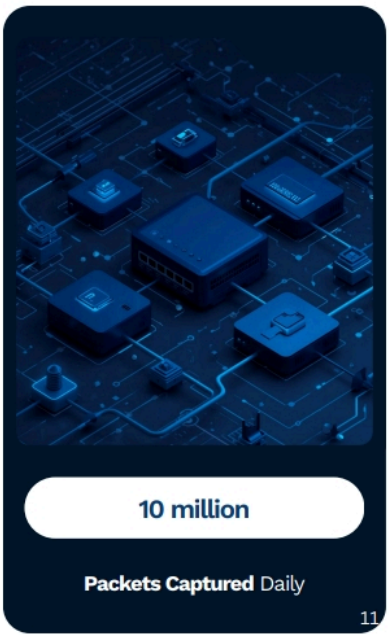
150

Traffic Analyzed Weekly



95%

Accuracy Rate of Analysis



10 million

Packets Captured Daily

Methodology Overview

2024

Initial network setup completed

2025

Traffic data collection initiated

2025

Incident analysis performed thoroughly

2026

Final report generated successfully

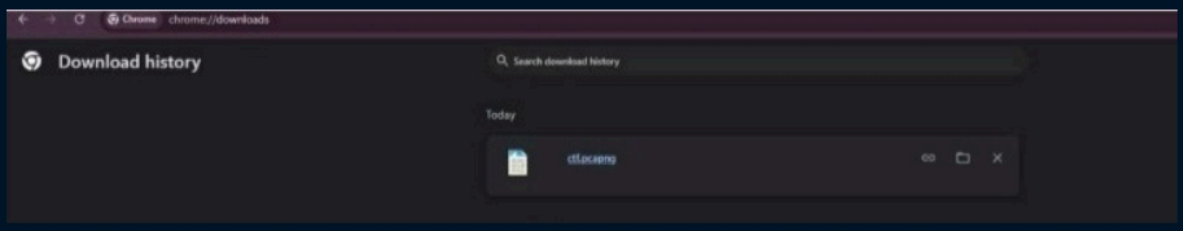
📁 STEP 1: Download Required Files

1.Download PCAP file

→https://drive.google.com/file/d/1XlqKcBkLO4NWVJKZUYnEnLTvwoGe8tHN/view usp=sharing

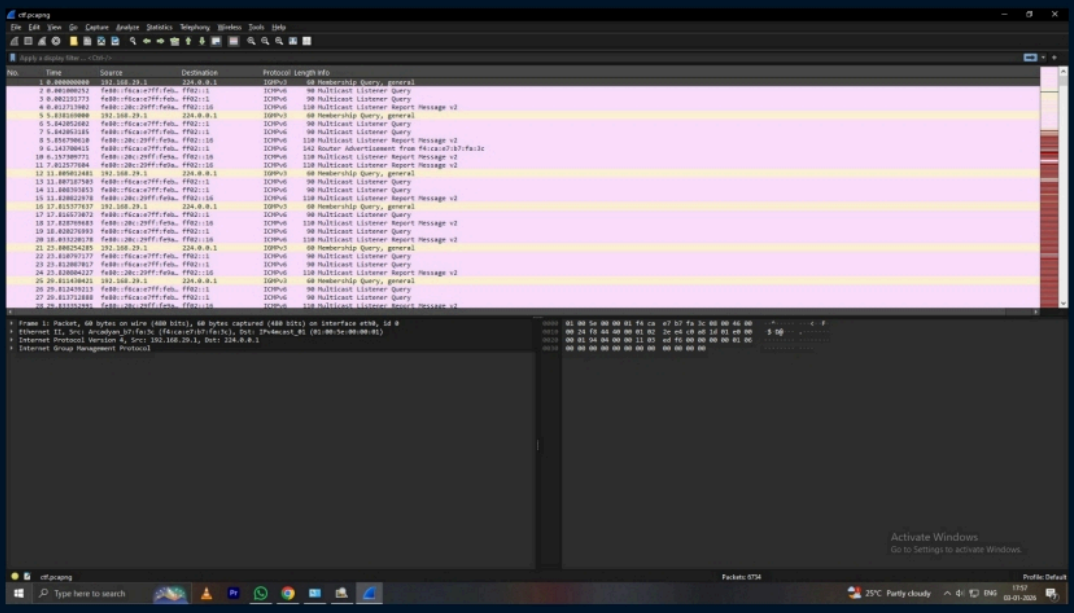
2.Download Wireshark

- Download from: https://www.wireshark.org
- Install with default settings
- Allow Npcap during installation



📁 STEP 2: Open PCAP File in Wireshark

1.Open Wireshark
2.Click File → Open
3.Select the downloaded .pcap file
4.Click Open



🔍 STEP 3: Identify Attacker & Victim IP

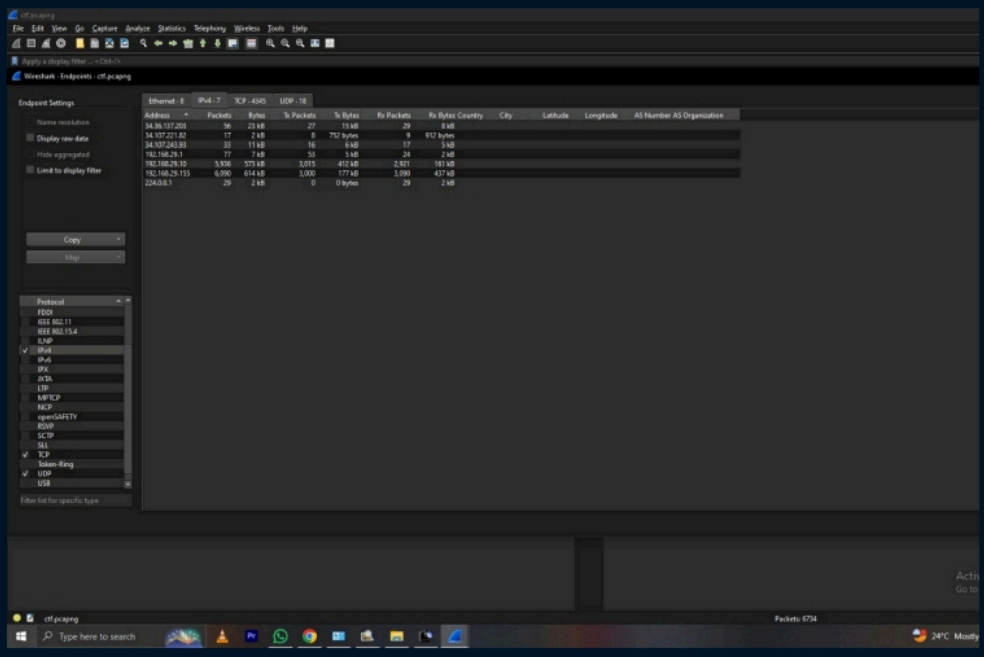
1. Go to:
   Statistics → Conversations → IPv4
2. Observe:
   - One IP sending packets to many ports
   - One IP receiving most traffic

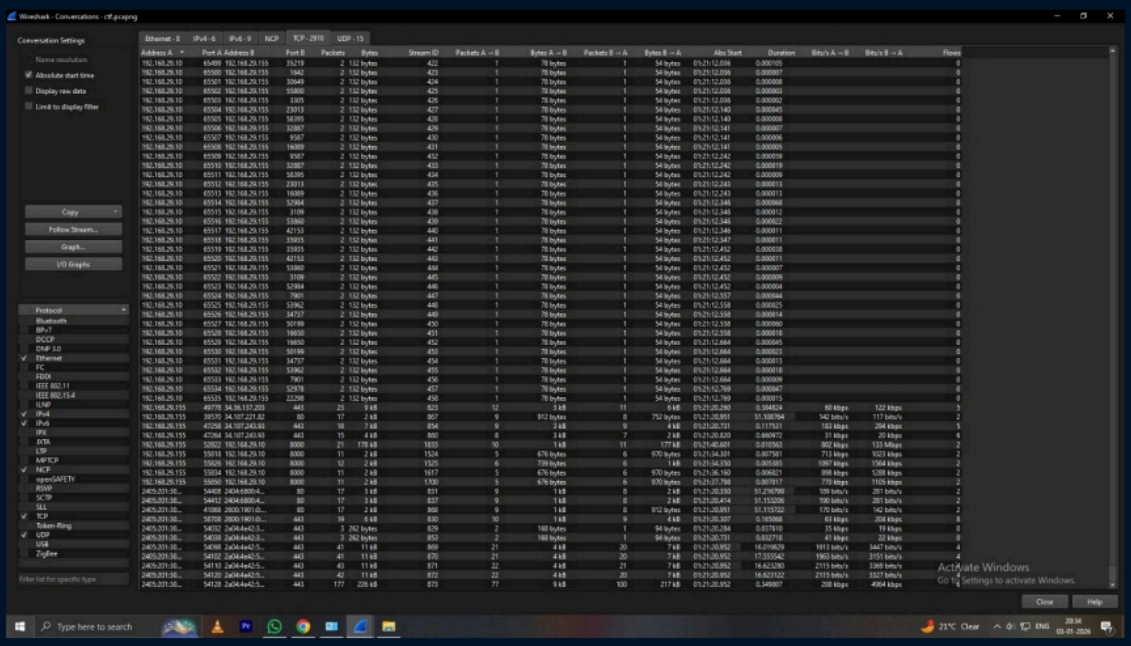
➡️ Attacker IP:

- Sends SYN packets to multiple ports

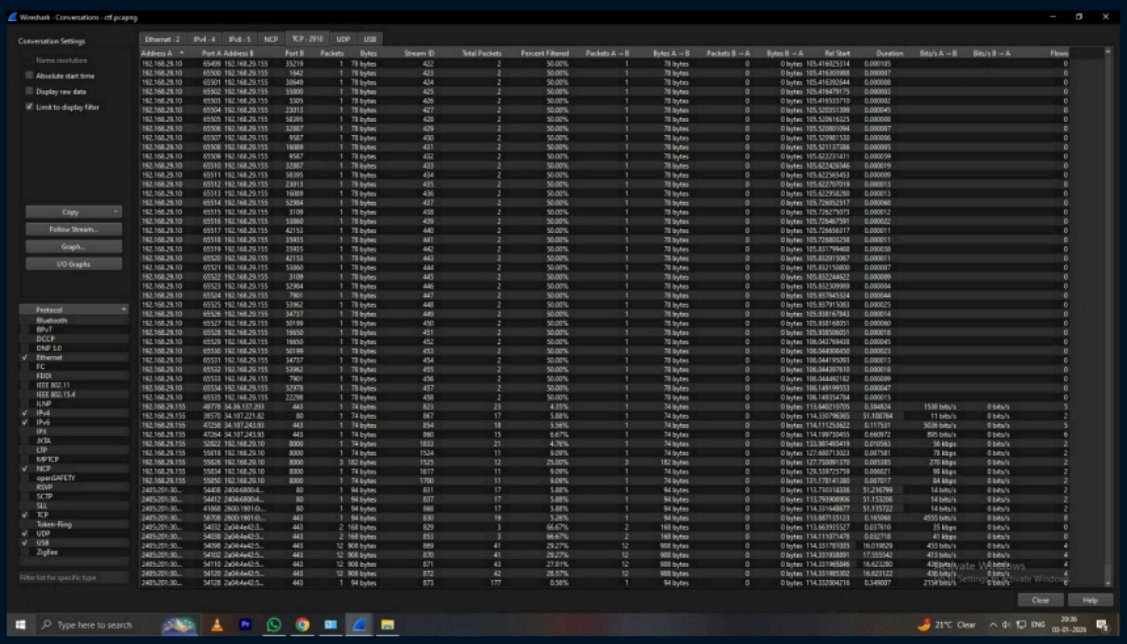
➡️ Victim IP:

- Target of scanning + HTTP communication

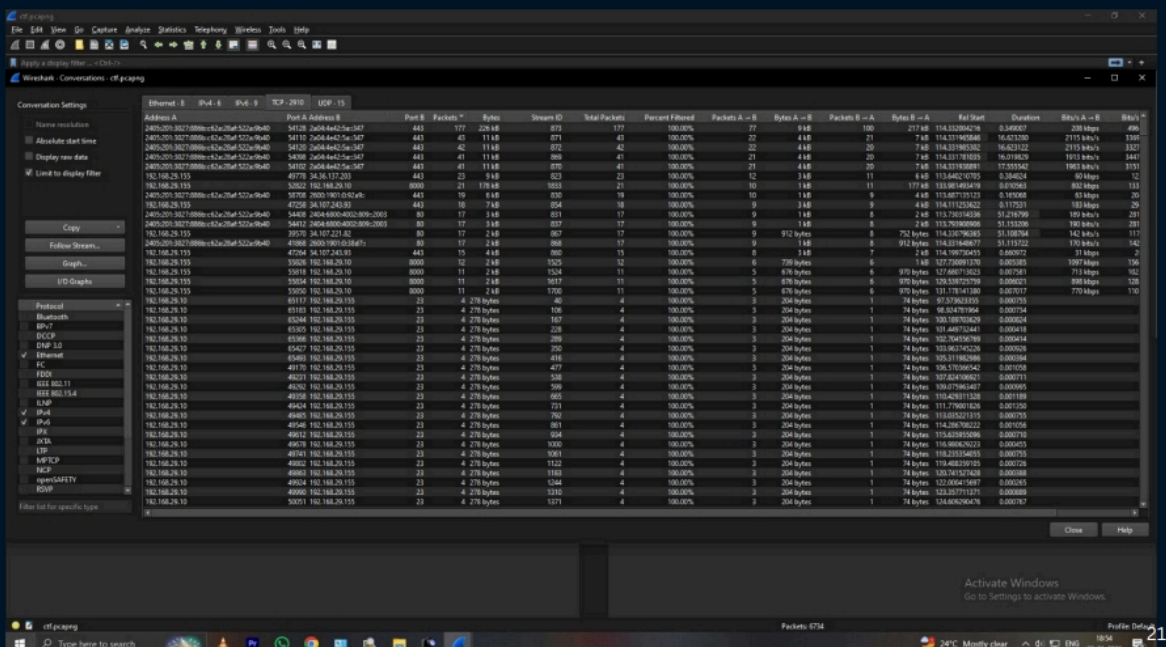




19



20



21

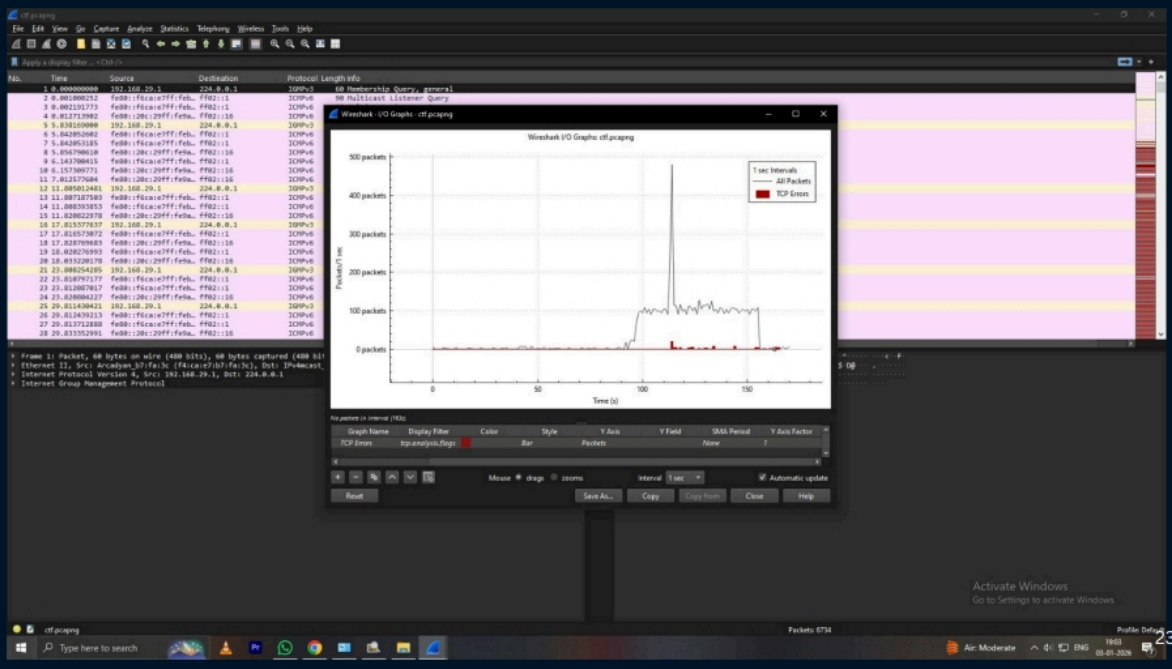
⏱️ STEP 4: Find First Attack Packet Timestamp

1.Use display filter:

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

2.First SYN packet = start of attack

3.Note Time column



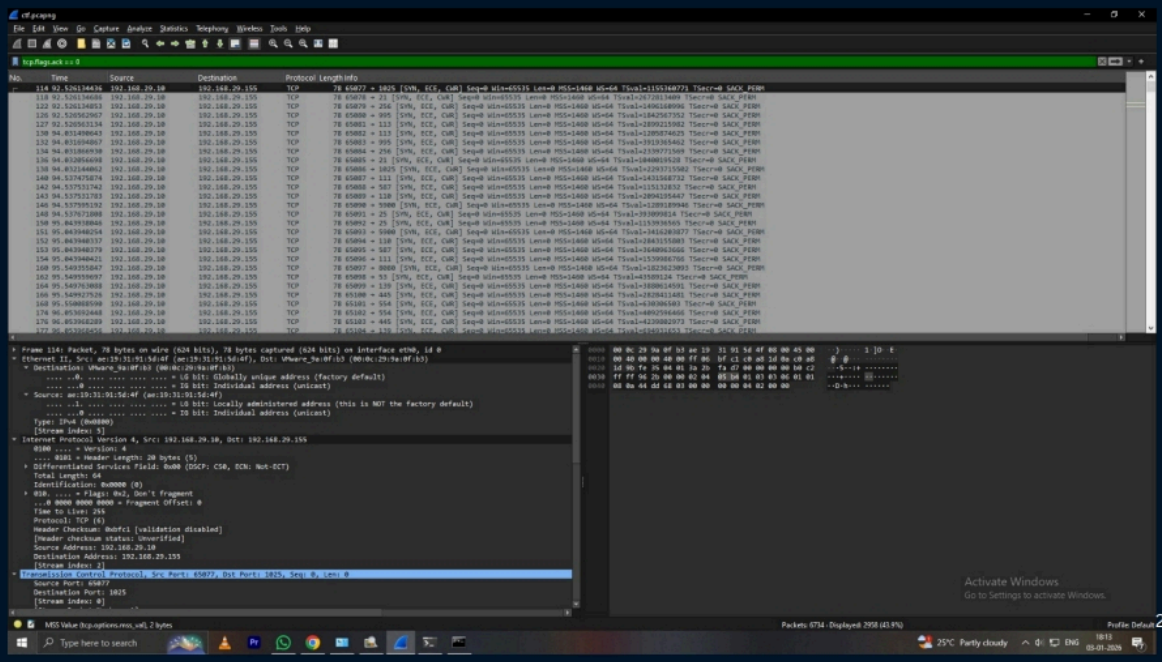
🥷 STEP 5: Detect Reconnaissance (Port Scanning)

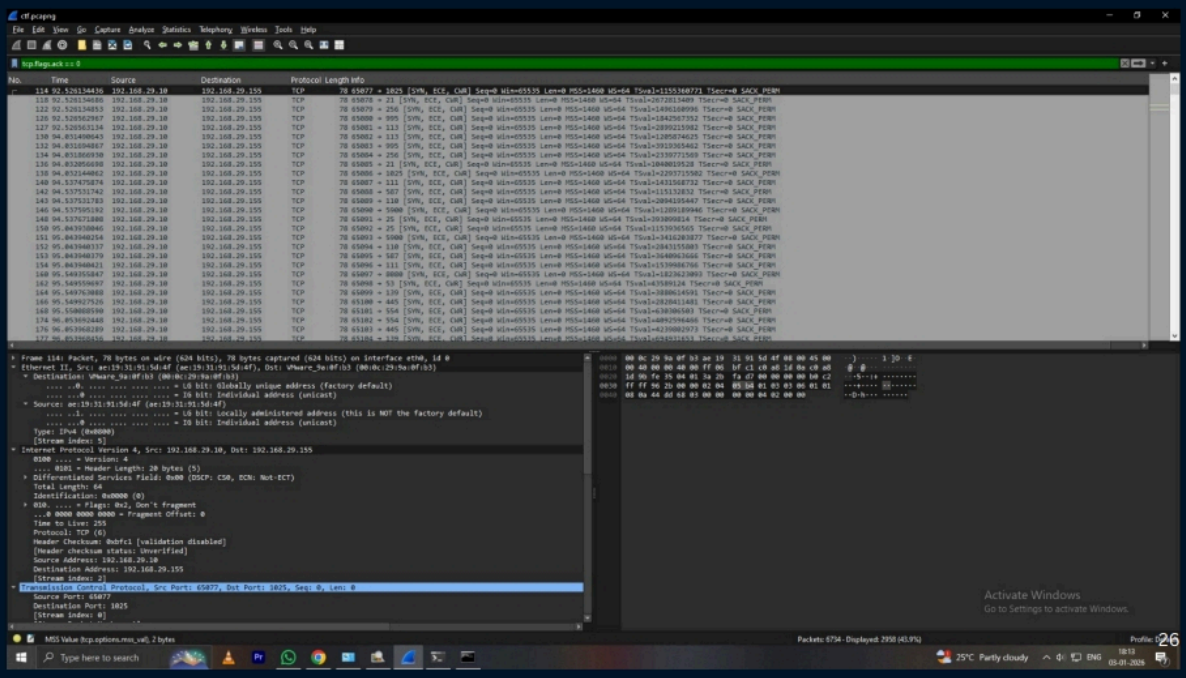
Evidence of scanning:

- 🔹 **Multiple SYN packets**
- 🔹 **Different destination ports**
- 🔹 **Same source IP**

Filter to show scan:

tcp.flags.syn == 1





🌐 STEP 6: Analyze HTTP Traffic

1. Apply filter:

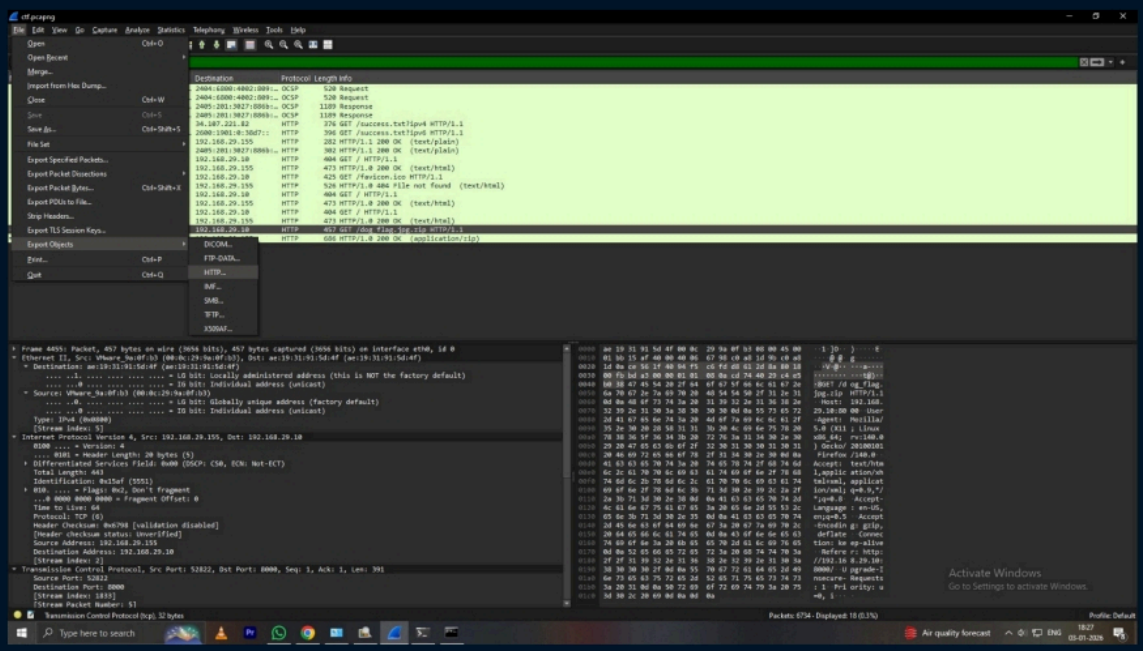
```
http
```

Copy code

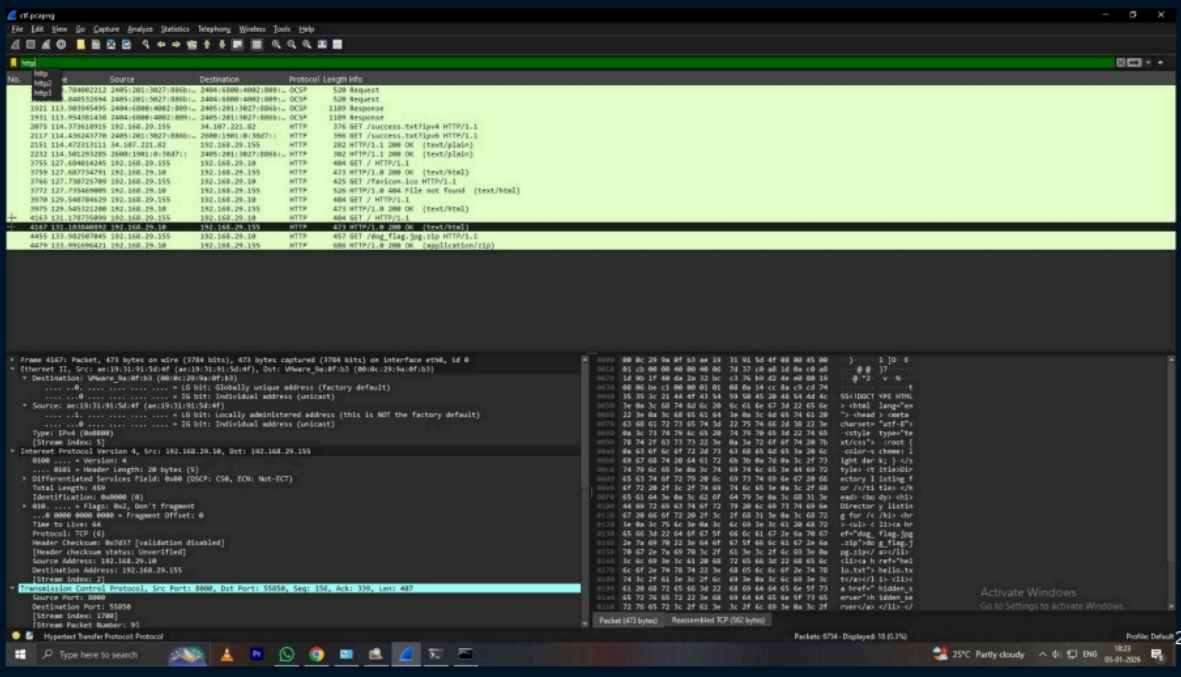
2. Look for:

- `GET` requests
- File download (`.zip`)

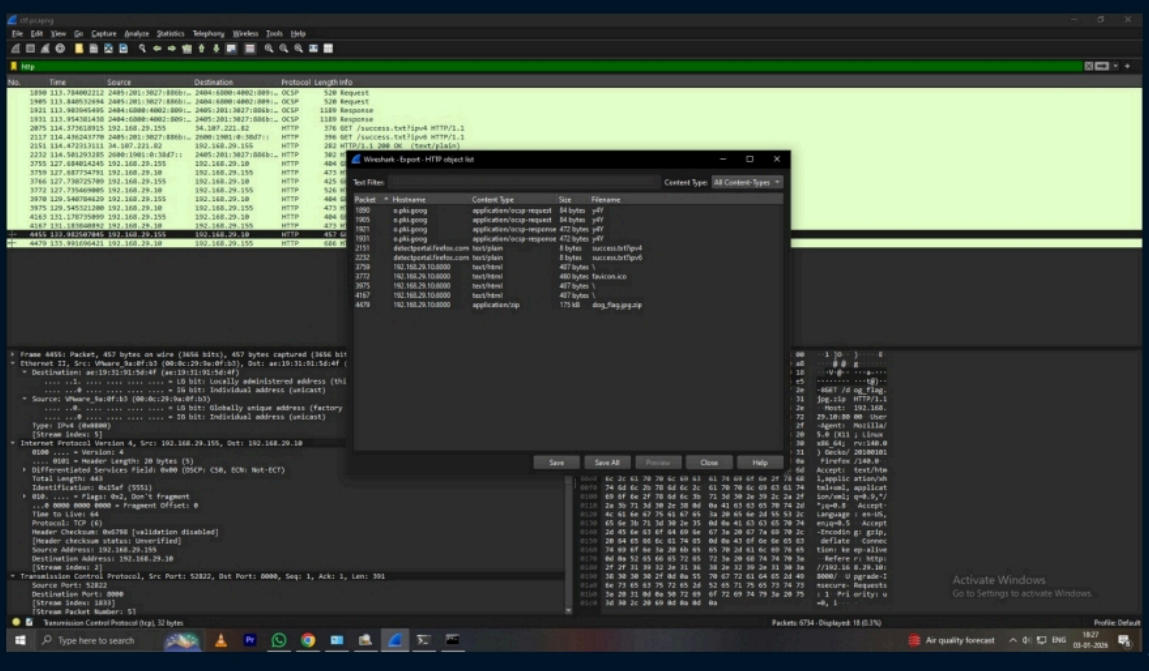
3. Select suspicious packet
4. Right-click → **Follow** → **HTTP Stream**



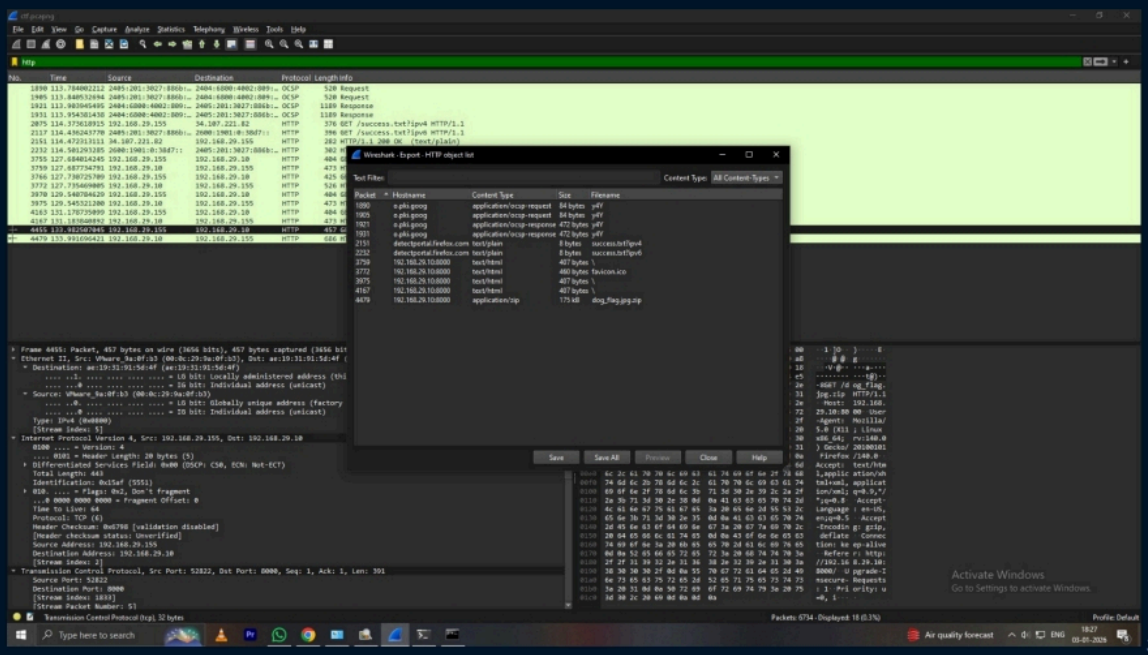
28



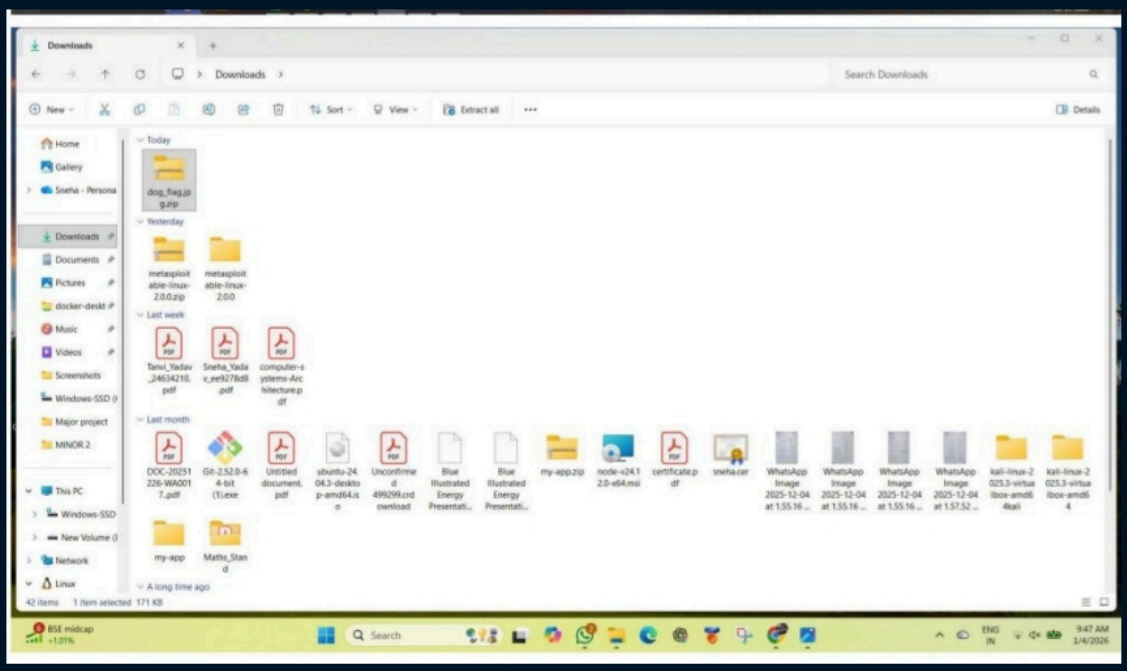
29



30



30



31

📦 STEP 7: Extract ZIP File from PCAP

1. Go to:

```
File → Export Objects → HTTP
```

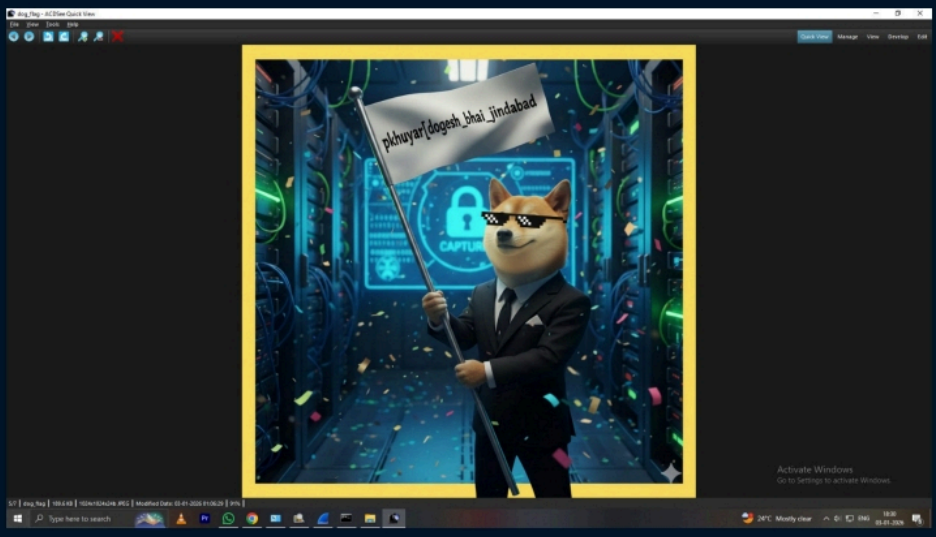
Copy code

2. Find `.zip` file
3. Click **Save**
4. Save it to a folder

32

STEP 8: Unzip the File

1. Right-click ZIP → **Extract Here**
2. Open extracted file
3. Locate **flag.txt** or similar file
4. Open it



!? QUESTIONS AND ANSWERS

- **What is attackers ip address?**
  192.168.29.10
- What is the name of the downloaded ZIP file?
  dog_flag.jpg
- What is the flag obtained after unzipping the file?
  pkhuyar[dogesh_bhai_jindabad]
- What evidence suggests reconnaissance activity?

The attacker dends multiple SYN packets to different port numbers on the victim machine

Result And Conclusion

Result:

The PCAP analysis helped identify the attacker and victim, detect port scanning, and analyze HTTP-based ZIP file transfer. The ZIP file was extracted successfully and the flag was obtained.

Conclusion:

This project shows how PCAP analysis is used in SOC investigations to detect attacks and data theft. It highlights the importance of network monitoring and timely incident response.

THANK YOU