

# Network Traffic Analysis & Incident Investigation Using PCAP



Presented by

Nikhil Kumar, ERP ID: [6606652]

1

## 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: \_\_\_\_\_

2

## Declaration of Originality

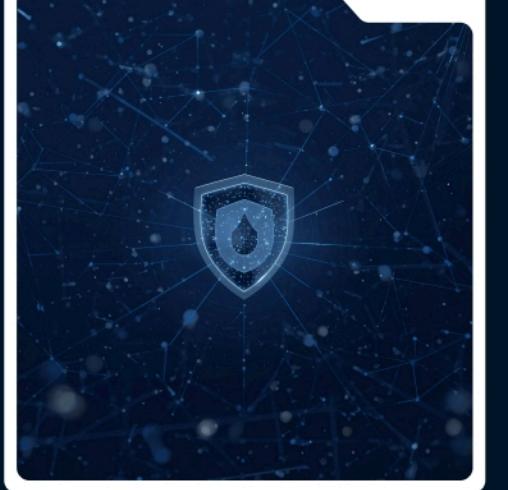
I hereby declare that this project report titled "Network Traffic Analysis & Incident Investigation Using PCAP (SOC Analyst Simulation)" is my original work. I have conducted the research, analysis, and writing independently, adhering to the ethical guidelines of academic integrity.

- 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.

3

# 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.



4

# 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.

5

# Table of Contents

## Overview of Project Sections

1. Introduction
2. Tools & Technologies Used
3. Methodology / Investigation Process
4. Results and Discussion
5. Conclusion

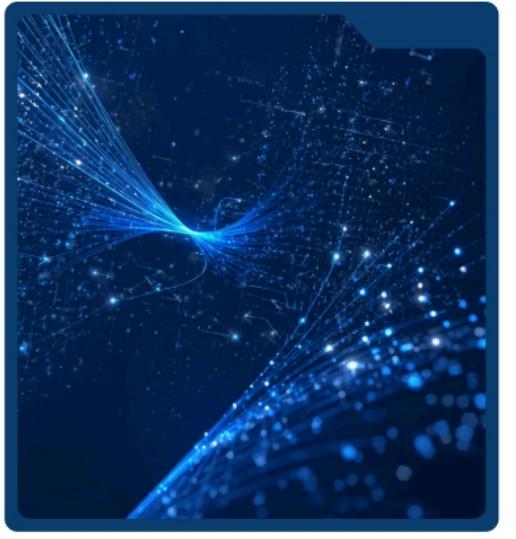


# Introduction

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



7

# 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.



8

# 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.*

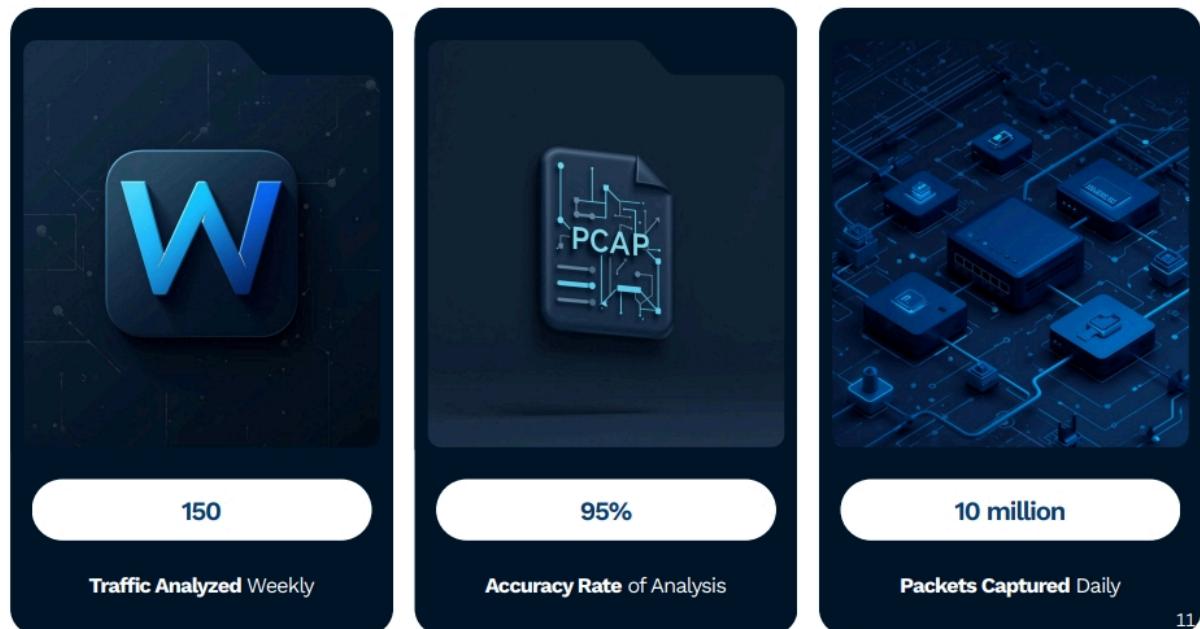
9

# 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.*

10



11

## Methodology Overview

**2024**

Initial network setup completed

**2025**

Traffic data collection initiated

**2025**

Incident analysis performed thoroughly

**2026**

Final report generated successfully

12

## 📁 STEP 1: Download Required Files

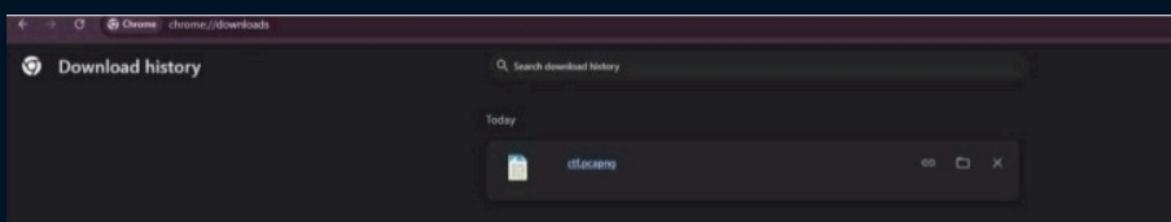
### 1. Download PCAP file

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

13

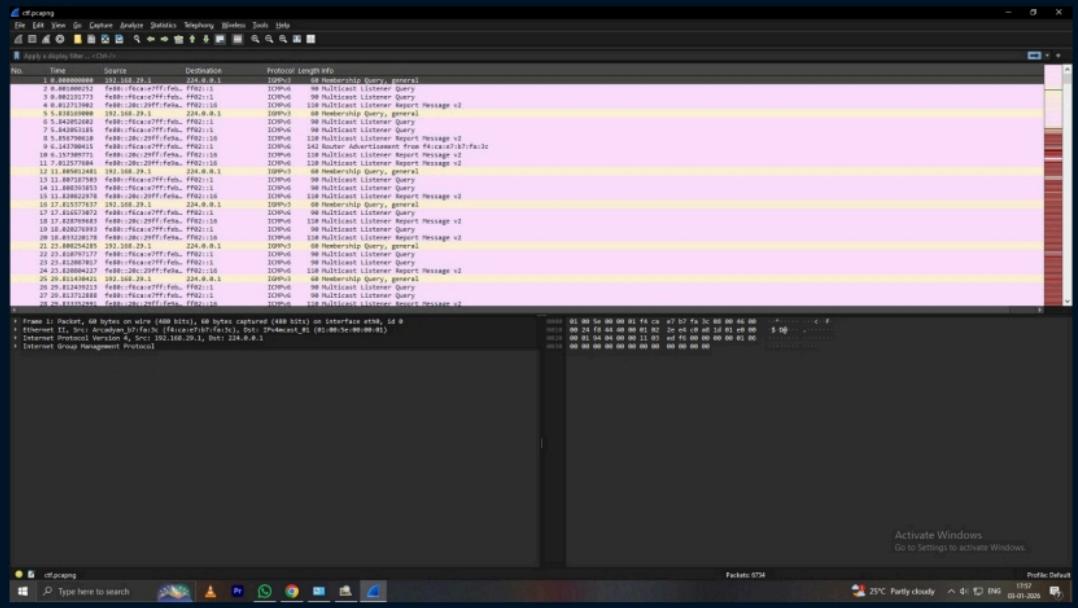


14

## 📁 STEP 2: Open PCAP File in Wireshark

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

15



16

## 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

17

Protocol	Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
Ethernet - 8	54.36.137.205	96	23 kB	27	15 kB	29	8 kB						
	54.37.27.271.82	17	2 kB	8	752 bytes	9	910 bytes						
	192.168.28.1	39	1 kB	24	1 kB	15	1 kB						
	192.168.28.1	77	7 kB	53	3 kB	28	2 kB						
	192.168.28.10	5,936	573 kB	3,015	472 kB	2,971	181 kB						
	192.168.25.15	6,090	614 kB	3,000	177 kB	3,098	437 kB						
	224.0.1.1	20	2 kB	0	0 bytes	20	2 kB						

18

Wireshark - Conversations (cf-pcapng)																		
Conversation Settings		Browser_E	IPv4_E	IPv6_E	NCP	TCP_2810	UDP_15											
		Address A - B	Port A - B	Address B - A	Port B	Bytes	Packets	Bytes	Stream ID	Packets A - B	Bytes A - B	Packets B - A	Bytes B - A	Abs Start	Duration	Bytes A - B	Bytes B - A	Rows
<input type="checkbox"/> Name resolution		192.168.20.159	4549	192.168.20.155	1025	2	132 bytes	422	1	78 bytes	1	54 bytes	0	09:21:12.2596	0.000000			0
<input checked="" type="checkbox"/> Absolute start time		192.168.20.159	45500	192.168.20.155	1042	2	132 bytes	423	1	78 bytes	1	54 bytes	0	09:21:12.2599	0.000007			0
<input type="checkbox"/> Display raw data		192.168.20.159	45502	192.168.20.155	1044	2	132 bytes	425	1	78 bytes	1	54 bytes	0	09:21:12.2600	0.000003			0
<input type="checkbox"/> Limit to display filter		192.168.20.159	45502	192.168.20.155	1045	2	132 bytes	426	1	78 bytes	1	54 bytes	0	09:21:12.2609	0.000003			0
<input type="checkbox"/> Copy		192.168.20.159	45502	192.168.20.155	1047	2	132 bytes	427	1	78 bytes	1	54 bytes	0	09:21:12.2609	0.000003			0
<input type="checkbox"/> Follow Stream...		192.168.20.159	45506	192.168.20.155	1087	2	132 bytes	428	1	78 bytes	1	54 bytes	0	09:21:12.141	0.000007			0
<input type="checkbox"/> Graph...		192.168.20.159	45508	192.168.20.155	1089	2	132 bytes	429	1	78 bytes	1	54 bytes	0	09:21:12.1411	0.000005			0
<input type="checkbox"/> I/O Graphs		192.168.20.159	45509	192.168.20.155	1087	2	132 bytes	431	1	78 bytes	1	54 bytes	0	09:21:12.242	0.000019			0
<input type="checkbox"/> Protocol		192.168.20.159	45510	192.168.20.155	1089	2	132 bytes	432	1	78 bytes	1	54 bytes	0	09:21:12.242	0.000009			0
Bluetooth		192.168.20.159	45511	192.168.20.155	1090	2	132 bytes	433	1	78 bytes	1	54 bytes	0	09:21:12.242	0.000008			0
BTLE		192.168.20.159	45511	192.168.20.155	1091	2	132 bytes	434	1	78 bytes	1	54 bytes	0	09:21:12.244	0.000012			0
DCCP		192.168.20.159	45518	192.168.20.155	1093	2	132 bytes	441	1	78 bytes	1	54 bytes	0	09:21:12.547	0.000011			0
DSDP		192.168.20.159	45519	192.168.20.155	1093	2	132 bytes	442	1	78 bytes	1	54 bytes	0	09:21:12.5471	0.000011			0
FC		192.168.20.159	45520	192.168.20.155	1093	2	132 bytes	443	1	78 bytes	1	54 bytes	0	09:21:12.5482	0.000011			0
FDDI		192.168.20.159	45521	192.168.20.155	1090	2	132 bytes	444	1	78 bytes	1	54 bytes	0	09:21:12.452	0.000007			0
IEEE 802.11		192.168.20.159	45522	192.168.20.155	1090	2	132 bytes	445	1	78 bytes	1	54 bytes	0	09:21:12.452	0.000008			0
IEEE 802.15.4		192.168.20.159	45524	192.168.20.155	7901	2	132 bytes	446	1	78 bytes	1	54 bytes	0	09:21:12.557	0.000044			0
IEEE 802.15.4S		192.168.20.159	45525	192.168.20.155	7901	2	132 bytes	447	1	78 bytes	1	54 bytes	0	09:21:12.5571	0.000044			0
ILNP		192.168.20.159	45526	192.168.20.155	34737	2	132 bytes	448	1	78 bytes	1	54 bytes	0	09:21:12.5588	0.000014			0
IP		192.168.20.159	45527	192.168.20.155	50199	2	132 bytes	450	1	78 bytes	1	54 bytes	0	09:21:12.559	0.000090			0
IP		192.168.20.159	45528	192.168.20.155	50200	2	132 bytes	451	1	78 bytes	1	54 bytes	0	09:21:12.5591	0.000090			0
DCCP		192.168.20.159	45529	192.168.20.155	10630	2	132 bytes	452	1	78 bytes	1	54 bytes	0	09:21:12.5664	0.000045			0
DSDP		192.168.20.159	45530	192.168.20.155	10630	2	132 bytes	453	1	78 bytes	1	54 bytes	0	09:21:12.666	0.000003			0
FC		192.168.20.159	45531	192.168.20.155	10717	2	132 bytes	454	1	78 bytes	1	54 bytes	0	09:21:12.671	0.000007			0
FDDI		192.168.20.159	45532	192.168.20.155	10702	2	132 bytes	455	1	78 bytes	1	54 bytes	0	09:21:12.674	0.000018			0
IEEE 802.11		192.168.20.159	45533	192.168.20.155	7901	2	132 bytes	456	1	78 bytes	1	54 bytes	0	09:21:12.674	0.000009			0
IEEE 802.15.4		192.168.20.159	45535	192.168.20.155	32509	2	132 bytes	458	1	78 bytes	1	54 bytes	0	09:21:12.769	0.000013			0
ILNP		192.168.20.159	45578	192.168.20.155	445	25	9 bytes	825	12	9 bytes	11	6 bytes	0	09:21:20.280	0.554524	60 Mbps	122 kbps	5
IP		192.168.20.159	45579	192.168.20.155	445	25	9 bytes	826	12	9 bytes	8	752 bytes	0	09:21:20.281	0.554524	542 bytes	1174 bytes	0
IP		192.168.20.159	45580	192.168.20.155	445	18	7 bytes	824	9	7 bytes	8	752 bytes	0	09:21:20.2811	0.554524	204 bytes	542 bytes	3
IP		192.168.20.159	45584	192.168.20.155	445	18	7 bytes	824	9	7 bytes	8	752 bytes	0	09:21:20.282	0.554524	21 bytes	6 bytes	8
IP		192.168.20.159	45584	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2821	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45584	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2822	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45586	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2823	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45587	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2824	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45588	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2825	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45589	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2826	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45590	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2827	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45591	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2828	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45592	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2829	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45593	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2830	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45594	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2831	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45595	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2832	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45596	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2833	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45597	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2834	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45598	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2835	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45599	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2836	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45600	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2837	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45601	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2838	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45602	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2839	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45603	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2840	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45604	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2841	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45605	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2842	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45606	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2843	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45607	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2844	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45608	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2845	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45609	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2846	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45610	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2847	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45611	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2848	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45612	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2849	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45613	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2850	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45614	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2851	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45615	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2852	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45616	192.168.20.155	445	18	7 bytes	825	9	7 bytes	8	752 bytes	0	09:21:20.2853	0.554524	11 bytes	11 bytes	0
IP		192.168.20.159	45617	192.														

19

20

Profile Details 18:54 21

# ⌚ STEP 4: Find First Attack Packet Timestamp

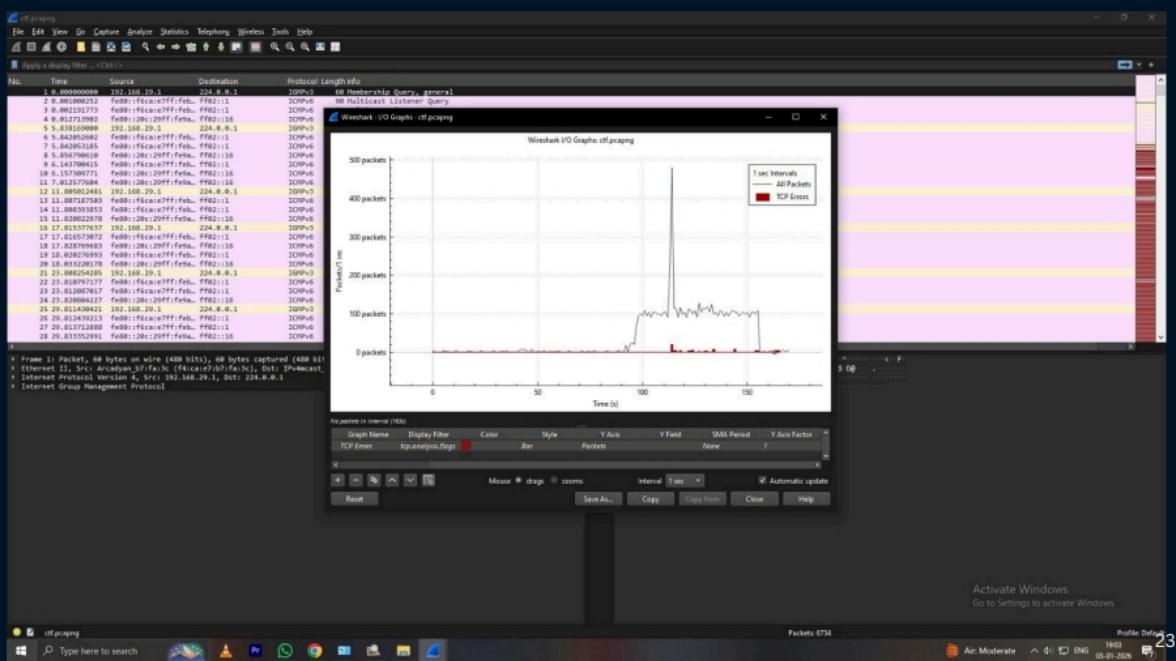
1. Use display filter:

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

2. First SYN packet = start of attack

3. Note Time column

22



# 🕵️ STEP 5: Detect Reconnaissance (Port Scanning)

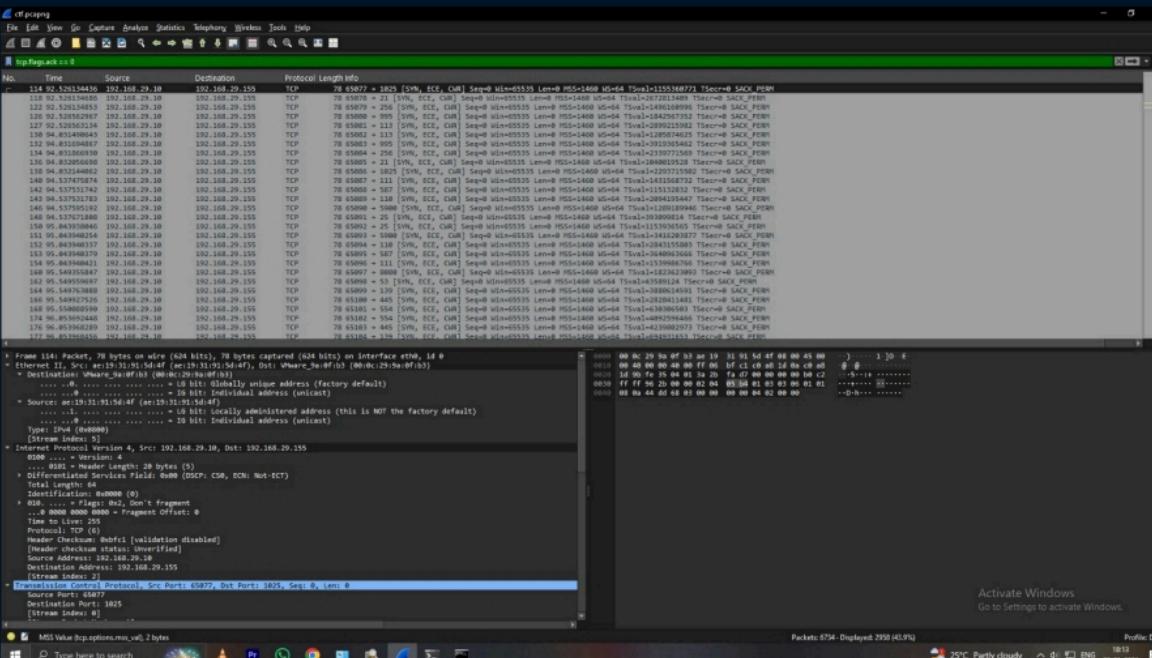
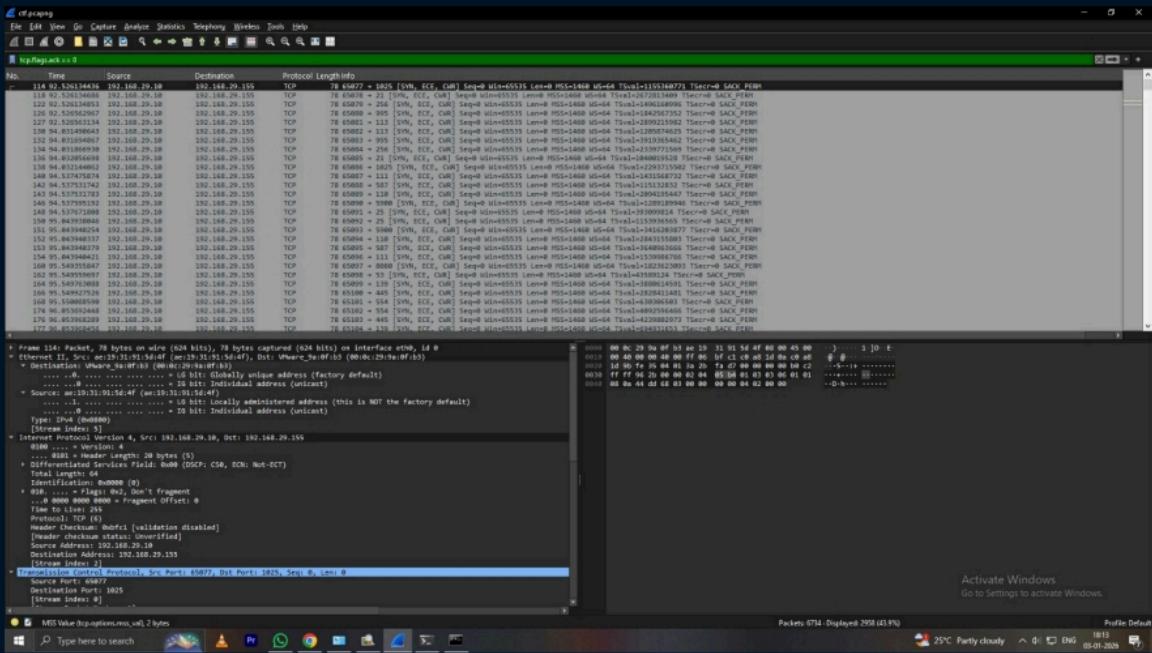
## Evidence of scanning:

- ◆ Multiple SYN packets
- ◆ Different destination ports
- ◆ Same source IP

Filter to show scan:

```
tcp.flags.syn == 1
```

24



## STEP 6: Analyze HTTP Traffic

### 1. Apply filter:

Copy code

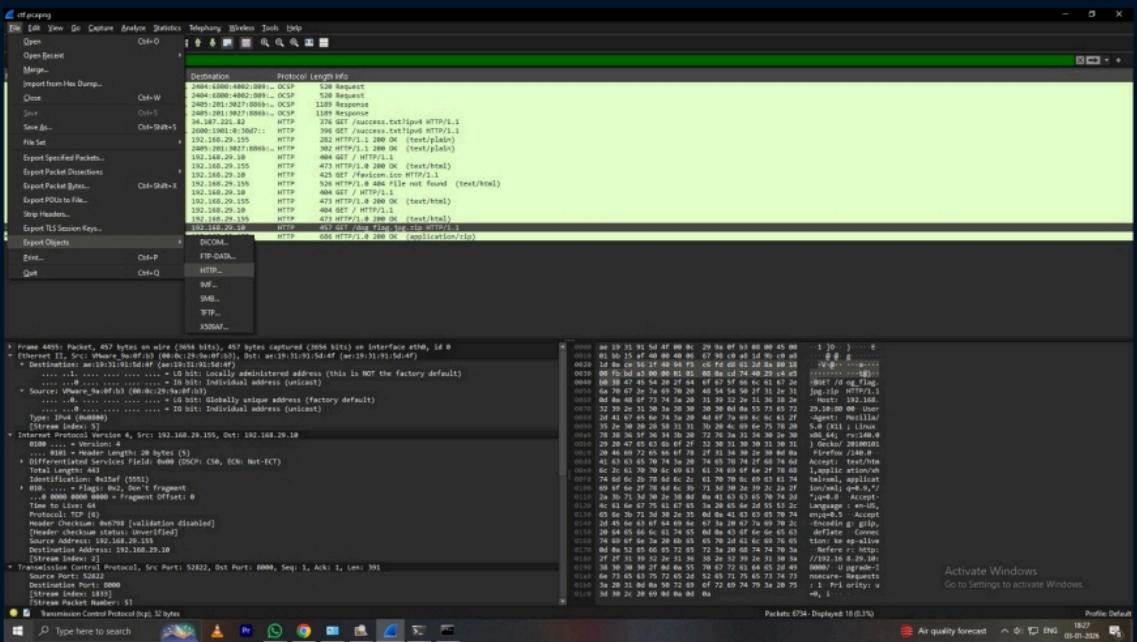
http

### 2. Look for:

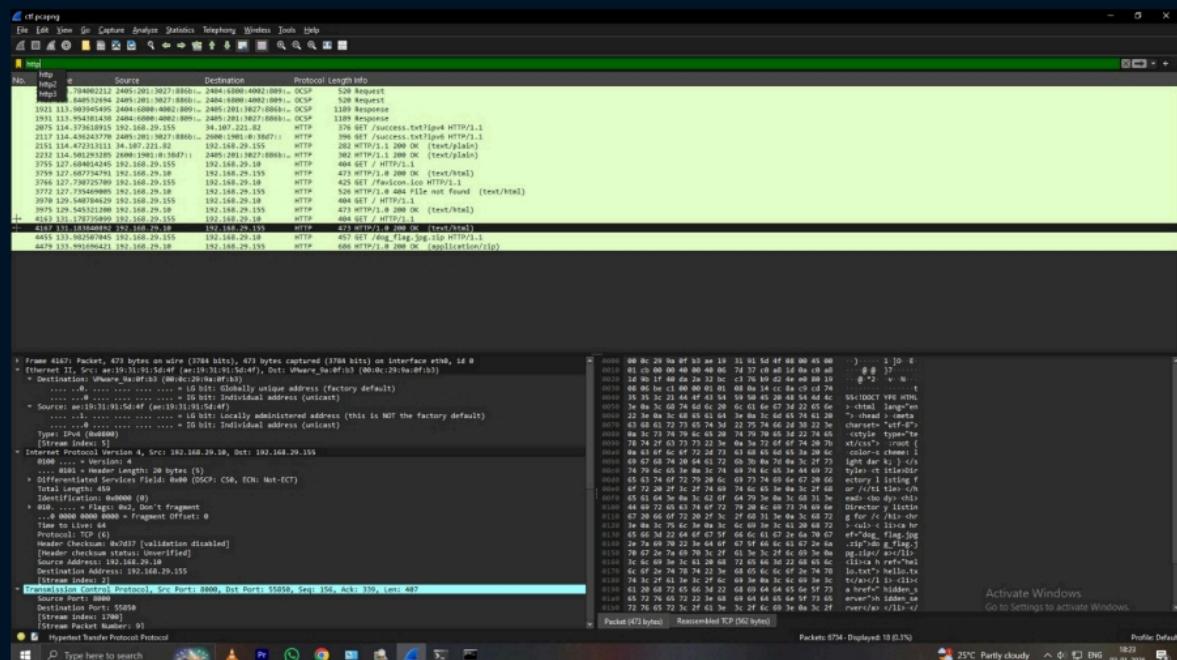
- GET requests
- File download (.zip)

### 3. Select suspicious packet

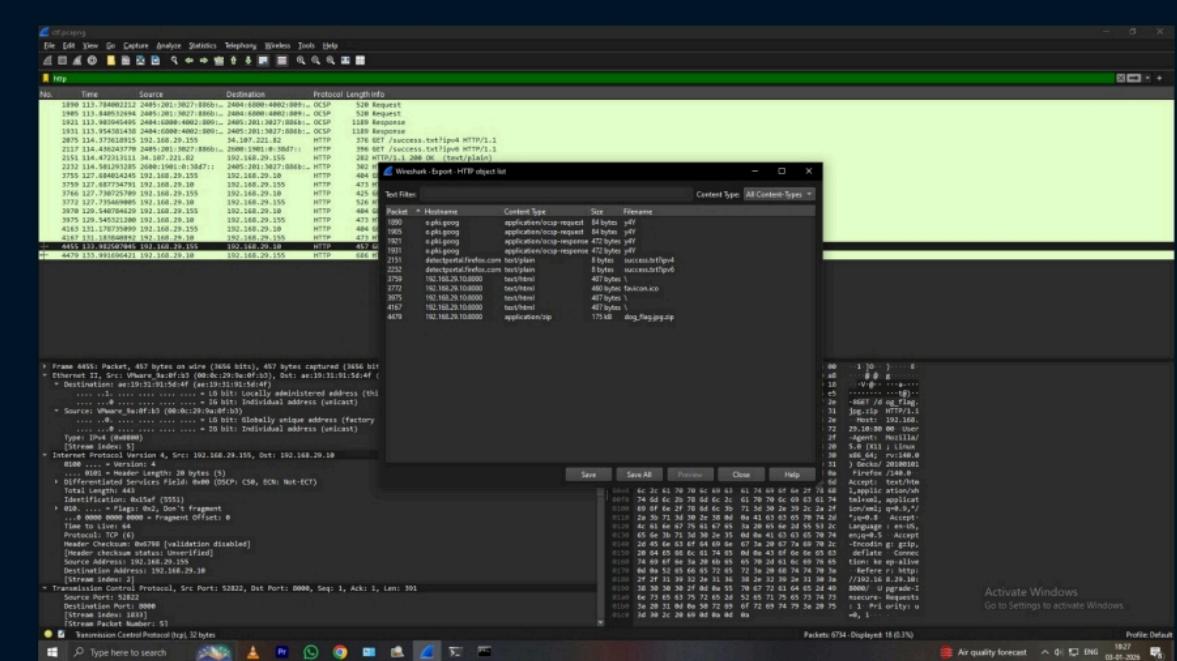
### 4. Right-click → Follow → HTTP Stream



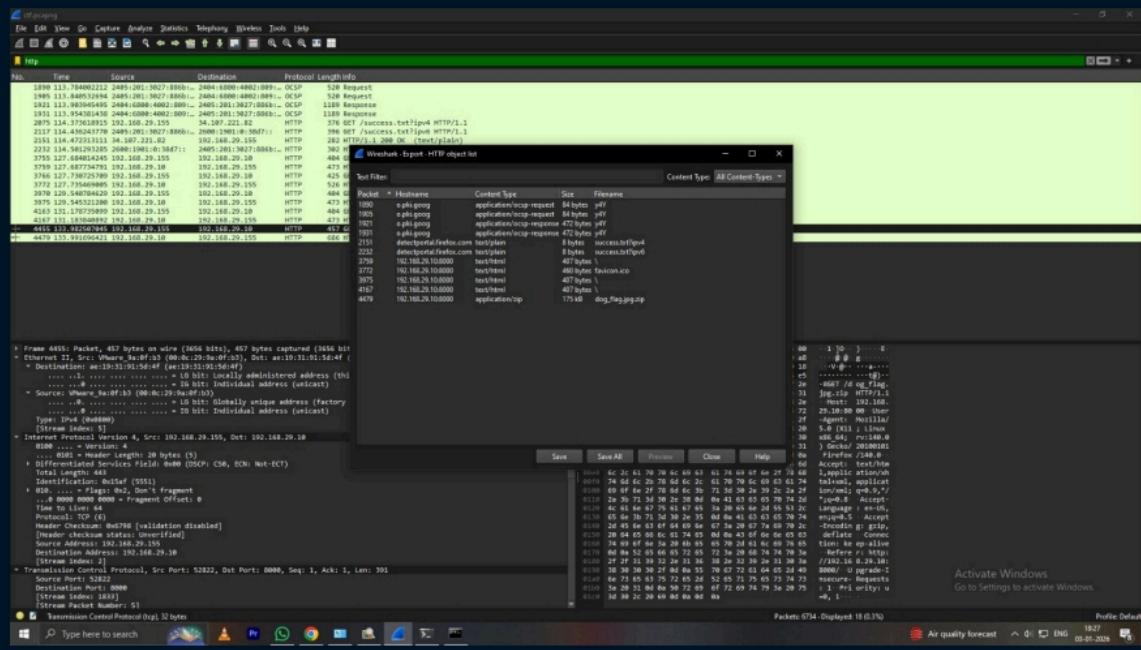
28



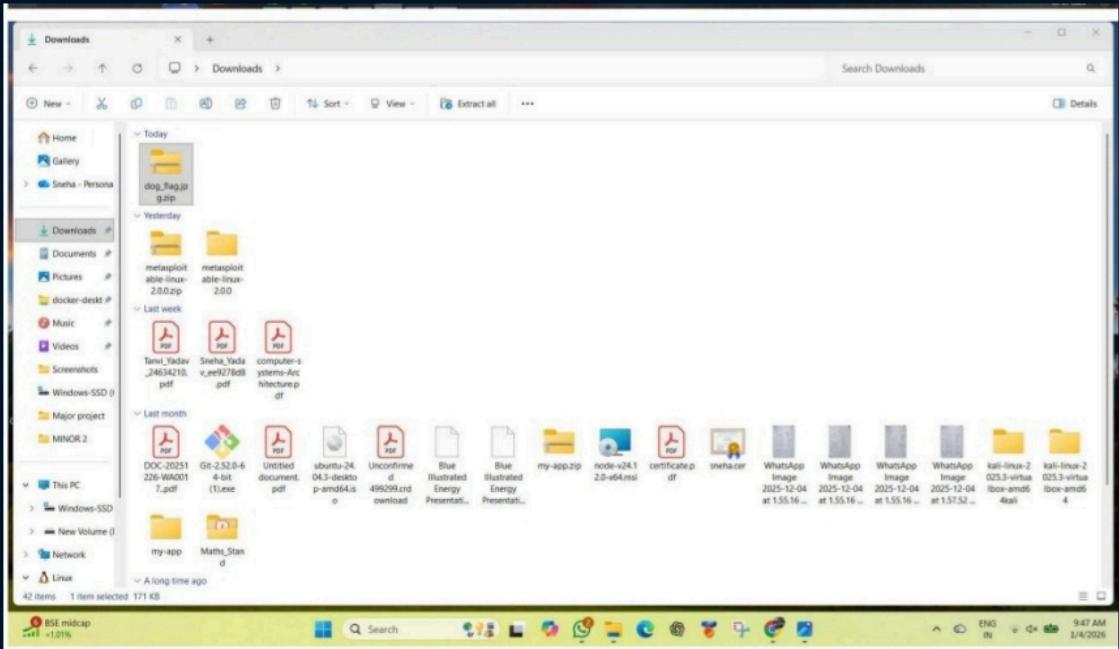
29



30



30



31

## STEP 7: Extract ZIP File from PCAP

1. Go to:

Copy code

File → Export Objects → HTTP

2. Find .zip file

3. Click Save

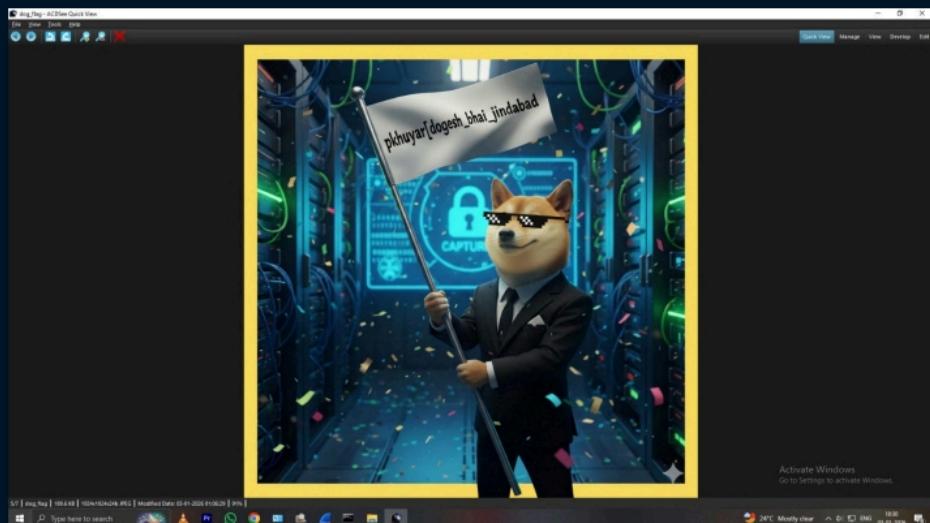
4. Save it to a folder

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

34



35

## ! ? 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?  
pkhuyarf[dogesh\_bhai\_jindabad]
- ◆ What evidence suggests reconnaissance activity?

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

36

# 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.*

37

# THANK YOU

38