

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

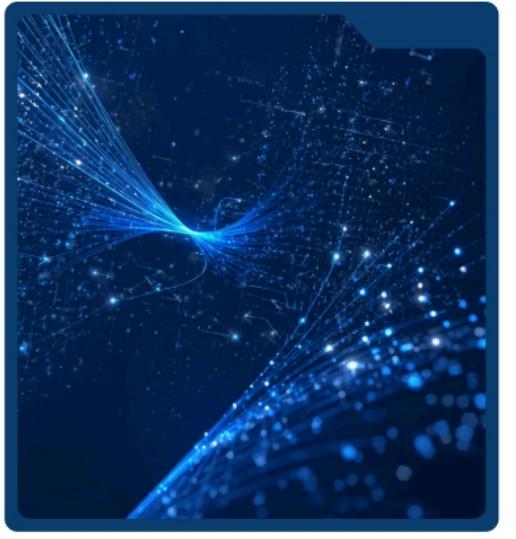


Introduction

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.

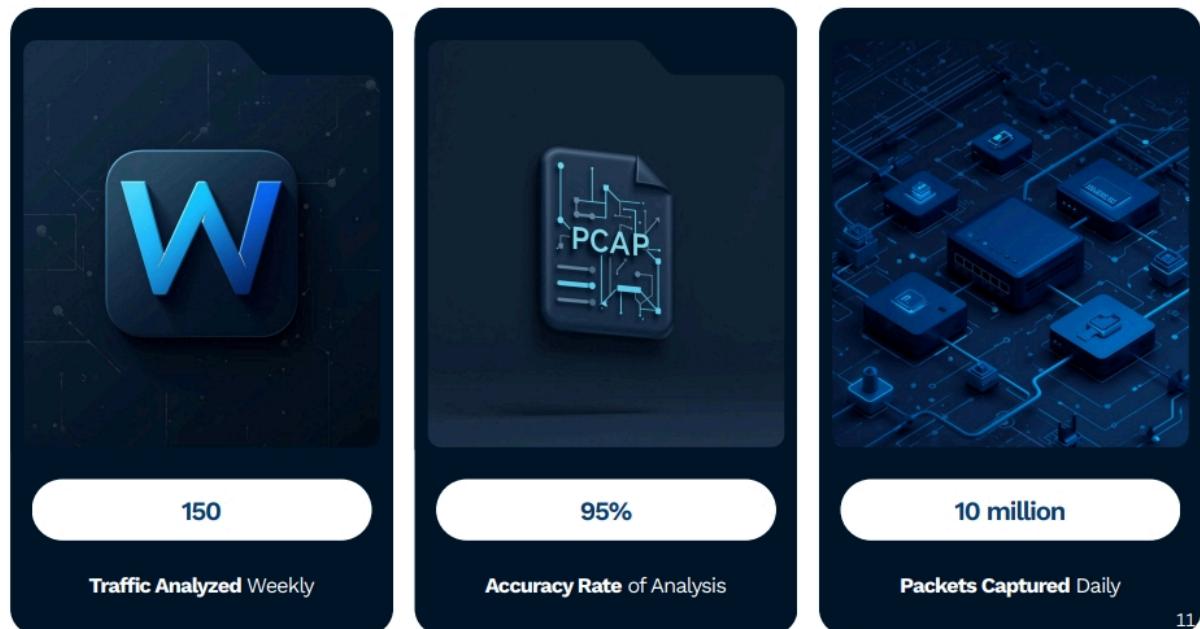
9

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

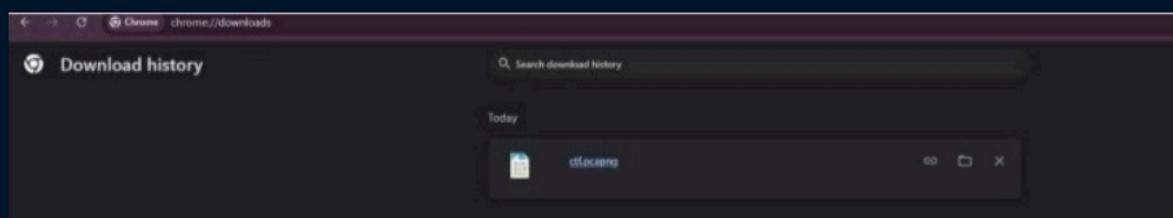
1. Download PCAP file

→[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

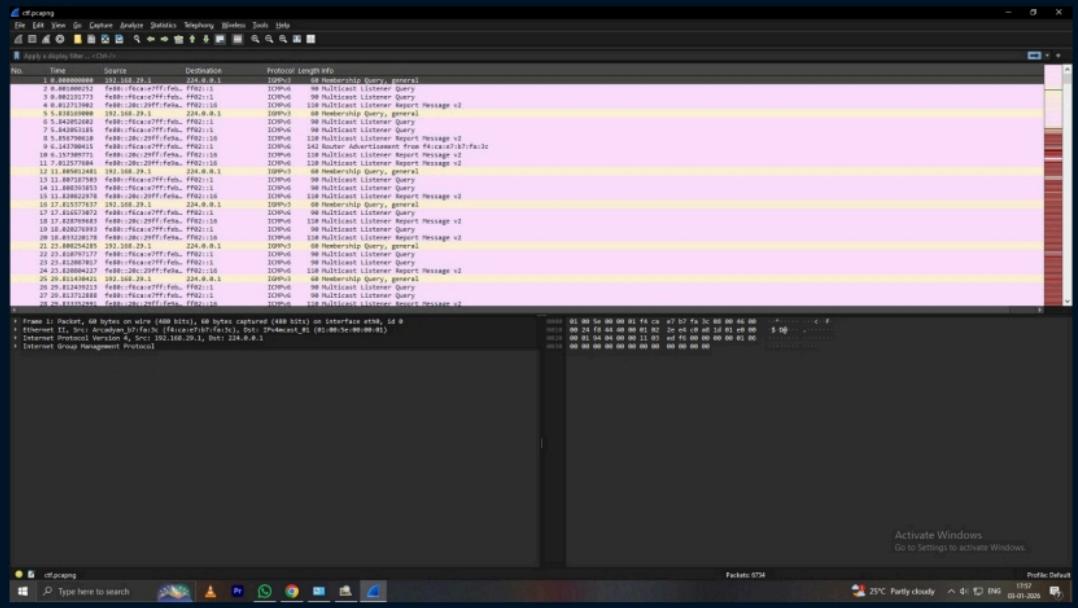


14

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						
	54.37.27.271.80	17	2 kB	8	750 bytes	9	910 bytes						
	192.168.28.10	30	3 kB	24	1 kB	11	2 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	Port A	Address B	Port B	Protocol	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bytes A → B	Bytes B → A	Flags	
192.168.20.15	65499	192.168.20.155	1	HTTP	422	1	78 bytes		1	54 bytes	09:21:12.2596	0.000000			0	
192.168.20.15	65500	192.168.20.155	1642	2	132 bytes	423	1	78 bytes		1	54 bytes	09:21:12.2599	0.000007			0
192.168.20.15	65501	192.168.20.155	1643	2	132 bytes	424	1	78 bytes		1	54 bytes	09:21:12.2600	0.000003			0
192.168.20.15	65502	192.168.20.155	53800	2	132 bytes	425	1	78 bytes		1	54 bytes	09:21:12.2601	0.000003			0
192.168.20.15	65503	192.168.20.155	3105	2	132 bytes	426	1	78 bytes		1	54 bytes	09:21:12.2609	0.000003			0
192.168.20.15	65504	192.168.20.155	7719	2	132 bytes	427	1	78 bytes		1	54 bytes	09:21:12.2610	0.000003			0
192.168.20.15	65505	192.168.20.155	58995	2	132 bytes	428	1	78 bytes		1	54 bytes	09:21:12.2640	0.000008			0
192.168.20.15	65506	192.168.20.155	53887	2	132 bytes	429	1	78 bytes		1	54 bytes	09:21:12.2641	0.000007			0
192.168.20.15	65507	192.168.20.155	5957	2	132 bytes	430	1	78 bytes		1	54 bytes	09:21:12.2642	0.000005			0
192.168.20.15	65508	192.168.20.155	53889	2	132 bytes	431	1	78 bytes		1	54 bytes	09:21:12.2643	0.000005			0
192.168.20.15	65509	192.168.20.155	9587	2	132 bytes	432	1	78 bytes		1	54 bytes	09:21:12.2644	0.000019			0
192.168.20.15	65510	192.168.20.155	53890	2	132 bytes	433	1	78 bytes		1	54 bytes	09:21:12.2645	0.000019			0
192.168.20.15	65511	192.168.20.155	23013	2	132 bytes	434	1	78 bytes		1	54 bytes	09:21:12.2646	0.000013			0
192.168.20.15	65512	192.168.20.155	53891	2	132 bytes	435	1	78 bytes		1	54 bytes	09:21:12.2647	0.000013			0
192.168.20.15	65513	192.168.20.155	53892	2	132 bytes	436	1	78 bytes		1	54 bytes	09:21:12.2648	0.000008			0
192.168.20.15	65514	192.168.20.155	52864	2	132 bytes	437	1	78 bytes		1	54 bytes	09:21:12.2649	0.000008			0
192.168.20.15	65515	192.168.20.155	3109	2	132 bytes	438	1	78 bytes		1	54 bytes	09:21:12.2649	0.000012			0
192.168.20.15	65516	192.168.20.155	53893	2	132 bytes	439	1	78 bytes		1	54 bytes	09:21:12.2650	0.000012			0
192.168.20.15	65517	192.168.20.155	42153	2	132 bytes	440	1	78 bytes		1	54 bytes	09:21:12.2649	0.000011			0
192.168.20.15	65518	192.168.20.155	35915	2	132 bytes	441	1	78 bytes		1	54 bytes	09:21:12.2649	0.000011			0
192.168.20.15	65519	192.168.20.155	39175	2	132 bytes	442	1	78 bytes		1	54 bytes	09:21:12.2649	0.000011			0
192.168.20.15	65520	192.168.20.155	53733	2	132 bytes	443	1	78 bytes		1	54 bytes	09:21:12.2642	0.000011			0
192.168.20.15	65521	192.168.20.155	53860	2	132 bytes	444	1	78 bytes		1	54 bytes	09:21:12.2643	0.000007			0
192.168.20.15	65522	192.168.20.155	53861	2	132 bytes	445	1	78 bytes		1	54 bytes	09:21:12.2643	0.000007			0
192.168.20.15	65523	192.168.20.155	53862	2	132 bytes	446	1	78 bytes		1	54 bytes	09:21:12.2643	0.000004			0
192.168.20.15	65524	192.168.20.155	7901	2	132 bytes	447	1	78 bytes		1	54 bytes	09:21:12.2644	0.000004			0
192.168.20.15	65525	192.168.20.155	53863	2	132 bytes	448	1	78 bytes		1	54 bytes	09:21:12.2644	0.000008			0
192.168.20.15	65526	192.168.20.155	34737	2	132 bytes	449	1	78 bytes		1	54 bytes	09:21:12.2644	0.000008			0
192.168.20.15	65527	192.168.20.155	50199	2	132 bytes	450	1	78 bytes		1	54 bytes	09:21:12.2645	0.000008			0
192.168.20.15	65528	192.168.20.155	53864	2	132 bytes	451	1	78 bytes		1	54 bytes	09:21:12.2645	0.000008			0
192.168.20.15	65529	192.168.20.155	18630	2	132 bytes	452	1	78 bytes		1	54 bytes	09:21:12.2646	0.000045			0
192.168.20.15	65530	192.168.20.155	50198	2	132 bytes	453	1	78 bytes		1	54 bytes	09:21:12.2646	0.000003			0
192.168.20.15	65531	192.168.20.155	53734	2	132 bytes	454	1	78 bytes		1	54 bytes	09:21:12.2646	0.000003			0
192.168.20.15	65532	192.168.20.155	34727	2	132 bytes	455	1	78 bytes		1	54 bytes	09:21:12.2646	0.000018			0
192.168.20.15	65533	192.168.20.155	7901	2	132 bytes	456	1	78 bytes		1	54 bytes	09:21:12.2646	0.000009			0
192.168.20.15	65534	192.168.20.155	53735	2	132 bytes	457	1	78 bytes		1	54 bytes	09:21:12.2646	0.000013			0
192.168.20.15	65535	192.168.20.155	53736	2	132 bytes	458	1	78 bytes		1	54 bytes	09:21:12.2646	0.000013			0
192.168.20.15	65536	192.168.20.155	49778	23	9 98	825	12	5 88	11	6 88	09:21:12.2620	0.554524	60 Mbps	122 kbps	5	
192.168.20.15	65537	192.168.20.155	157203	443	25	9 98	826	8	512 bytes	09:21:12.2621	0.554524	542 bytes	1174 kbps	5		
192.168.20.15	65538	192.168.20.155	53737	443	18	7 98	824	9	512 bytes	09:21:12.2621	0.554524	512 bytes	1244 kbps	3		
192.168.20.15	65539	192.168.20.155	53738	443	18	7 98	824	8	512 bytes	09:21:12.2620	0.554524	512 bytes	1244 kbps	3		
192.168.20.15	65540	192.168.20.155	53739	443	15	4 98	850	8	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65541	192.168.20.155	53740	443	15	4 98	851	9	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65542	192.168.20.155	53741	443	15	4 98	852	9	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65543	192.168.20.155	53742	443	15	4 98	853	10	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65544	192.168.20.155	53743	443	15	4 98	854	11	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65545	192.168.20.155	53744	443	15	4 98	855	12	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65546	192.168.20.155	53745	443	15	4 98	856	13	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65547	192.168.20.155	53746	443	15	4 98	857	14	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65548	192.168.20.155	53747	443	15	4 98	858	15	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65549	192.168.20.155	53748	443	15	4 98	859	16	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65550	192.168.20.155	53749	443	15	4 98	860	17	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65551	192.168.20.155	53750	443	15	4 98	861	18	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65552	192.168.20.155	53751	443	15	4 98	862	19	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65553	192.168.20.155	53752	443	15	4 98	863	20	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65554	192.168.20.155	53753	443	15	4 98	864	21	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65555	192.168.20.155	53754	443	15	4 98	865	22	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65556	192.168.20.155	53755	443	15	4 98	866	23	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65557	192.168.20.155	53756	443	15	4 98	867	24	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65558	192.168.20.155	53757	443	15	4 98	868	25	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65559	192.168.20.155	53758	443	15	4 98	869	26	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65560	192.168.20.155	53759	443	15	4 98	870	27	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65561	192.168.20.155	53760	443	15	4 98	871	28	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65562	192.168.20.155	53761	443	15	4 98	872	29	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65563	192.168.20.155	53762	443	15	4 98	873	30	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65564	192.168.20.155	53763	443	15	4 98	874	31	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65565	192.168.20.155	53764	443	15	4 98	875	32	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65566	192.168.20.155	53765	443	15	4 98	876	33	3 88	7	2 18	09:21:12.2620	0.569972	31 bytes	656 kbps	6
192.168.20.15	65567	192.168.20.155	53766	443												

19

20

Profile Details

⌚ STEP 4: Find First Attack Packet Timestamp

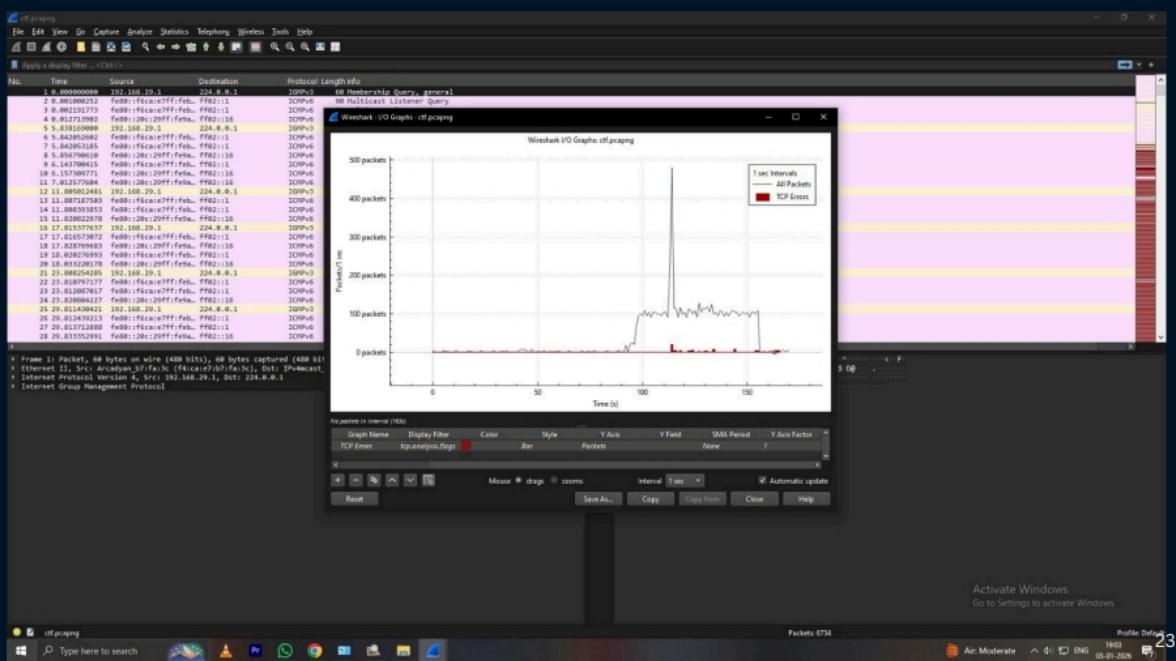
1. Use display filter:

```
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)

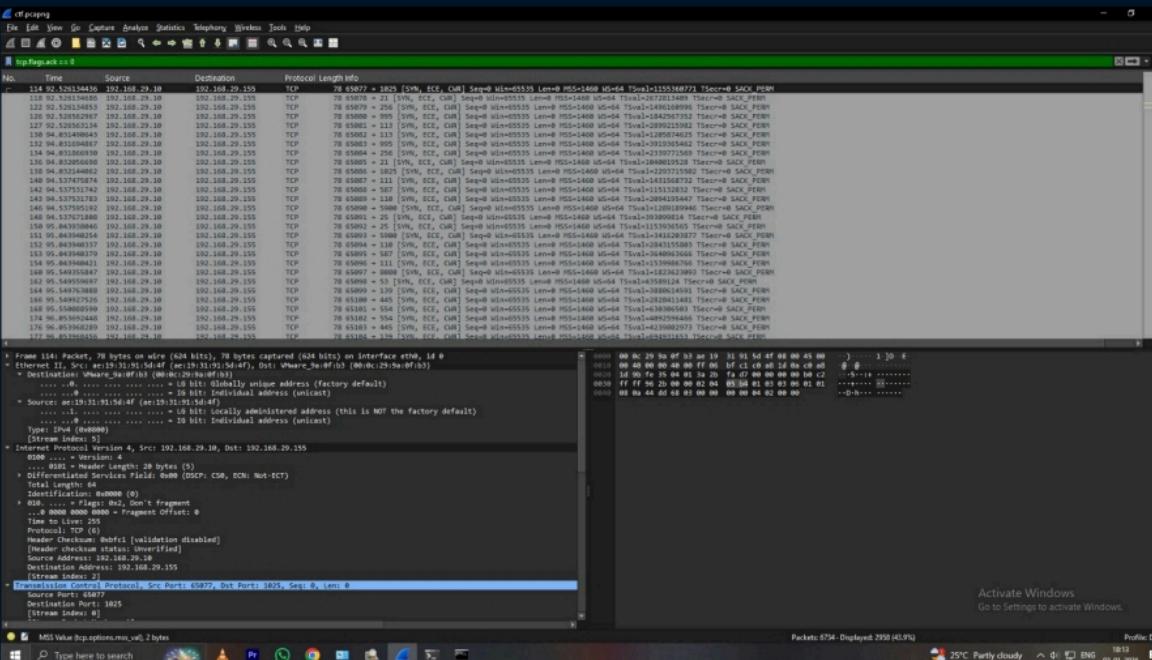
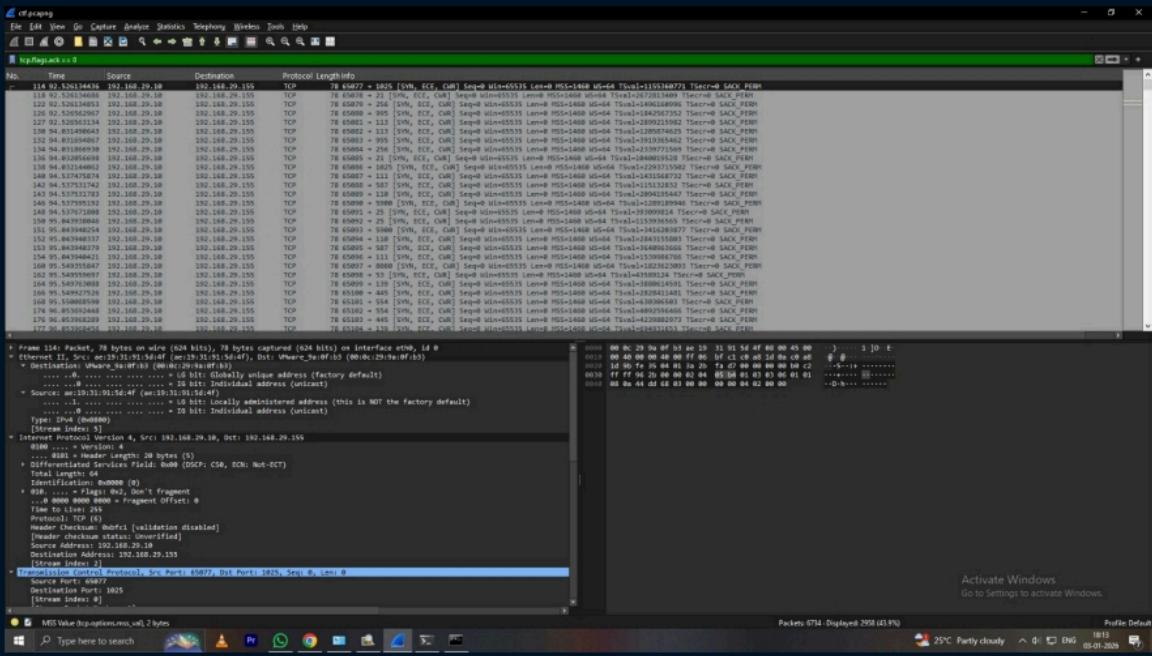
Evidence of scanning:

- ◆ 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

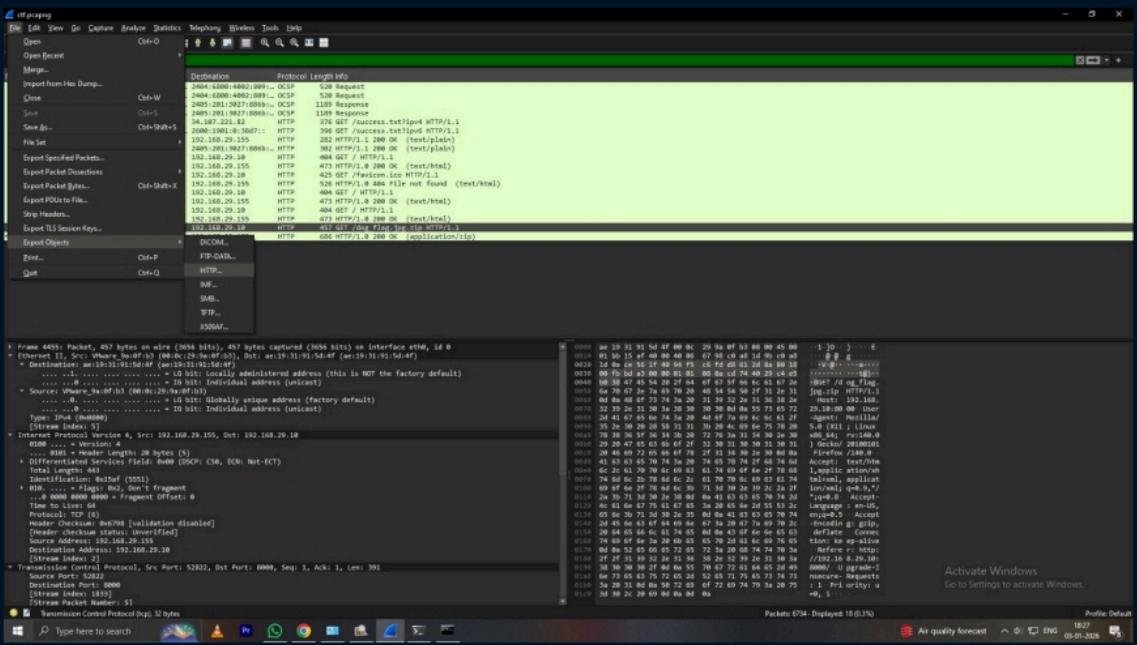
http

2. Look for:

- GET requests
- File download (.zip)

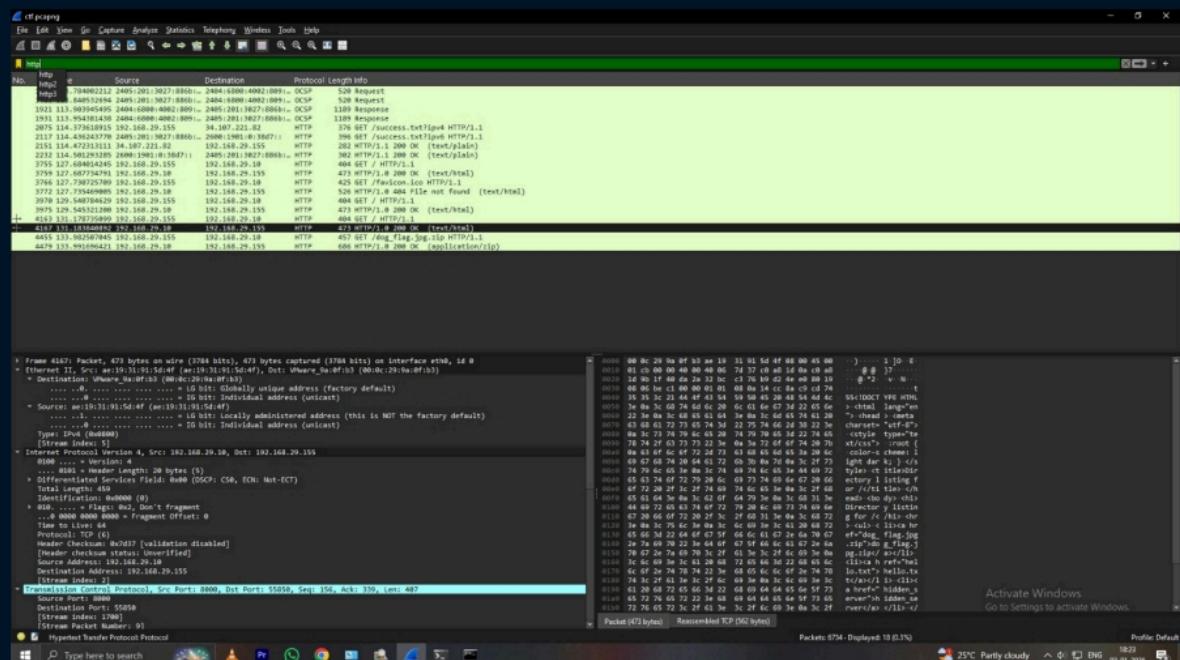
3. Select suspicious packet

4. Right-click → Follow → HTTP Stream



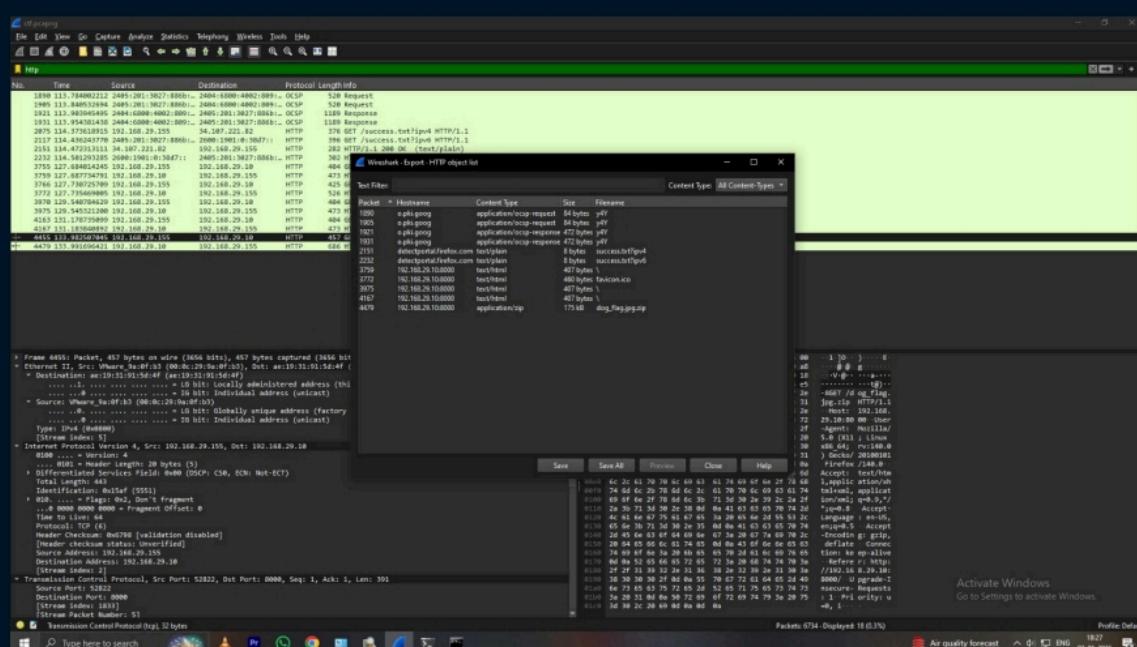
Activate Windows
Go to Settings to activate Windows.

28



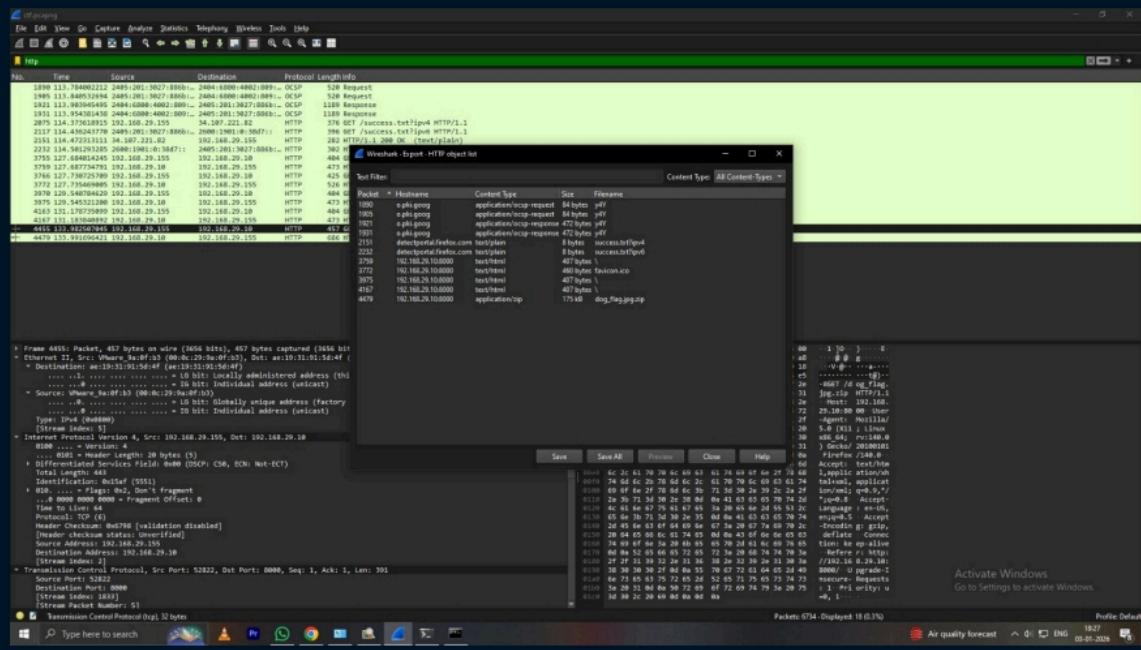
Activate Windows
Go to Settings to activate Windows.

29

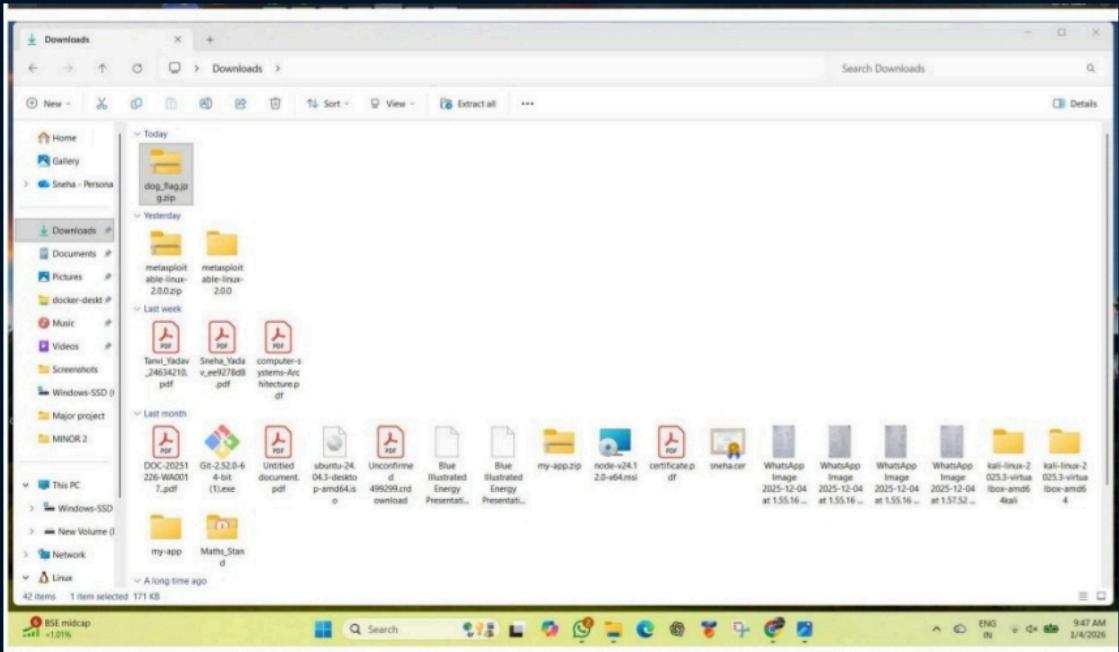


Activate Windows
Go to Settings to activate Windows.

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

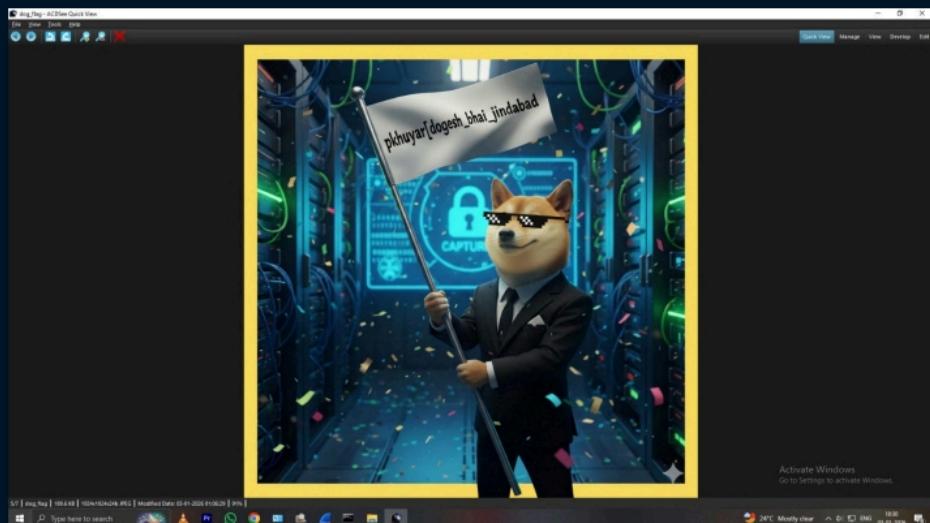
4. Save it to a folder

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