⏭ MINOR–2PROJECT REPORT ⏮

PCAP FILE ANALYSIS USING WIRESHARK

Name: SWAPNIL GUPTA

Semester: 3rd Semester

Subject: Cyber Security / Network Security

Project Title: Analysis of Network Traffic Using PCAP

Tool Used: Wireshark

PCAP File: `ctf.pcapng`

1 Introduction

Cybersecurity is a vital area of computer engineering that focuses on protecting systems and networks from cyber threats. One of the key methods used in cybersecurity analysis is monitoring and examining network traffic to detect suspicious or malicious activities. A PCAP (Packet Capture) file contains detailed records of network communications, including packet data, source and destination IP addresses, ports, and protocols. These files are widely used in digital forensics and incident response to investigate security incidents.

In this project, a PCAP file was analyzed using the Wireshark network protocol analyzer. The analysis began with identifying the attacker and victim systems by examining IP addresses and communication patterns. Port scanning activity was detected by observing multiple connection attempts to different ports, indicating reconnaissance behavior by the attacker. HTTP traffic was then analyzed to inspect web-based communications and identify any suspicious file transfers. During this process, a ZIP file transmitted over the network was extracted and examined.

2 objectives of the Project

The main objectives of this project are:

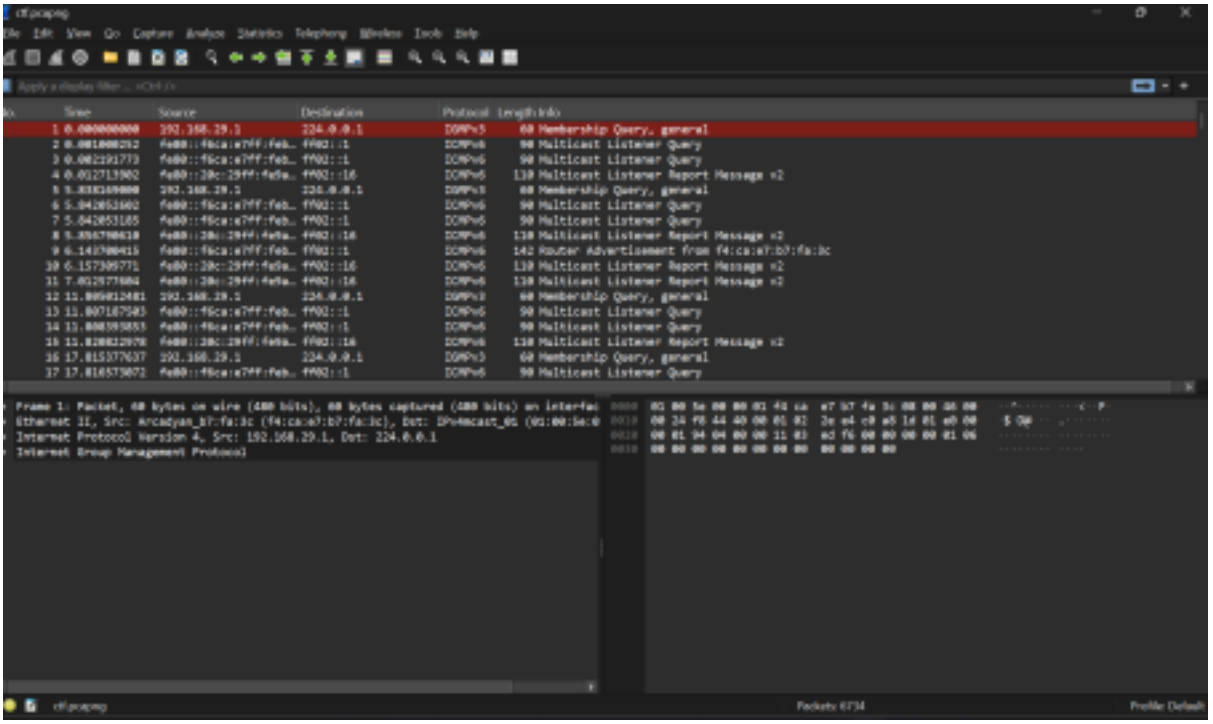
- To understand PCAP file analysis
- To identify attacker and victim IP addresses
- To detect reconnaissance activity (port scanning)
- To analyze HTTP traffic
- To extract files from network traffic
- To retrieve a flag from the extracted file
- To document the findings in a report

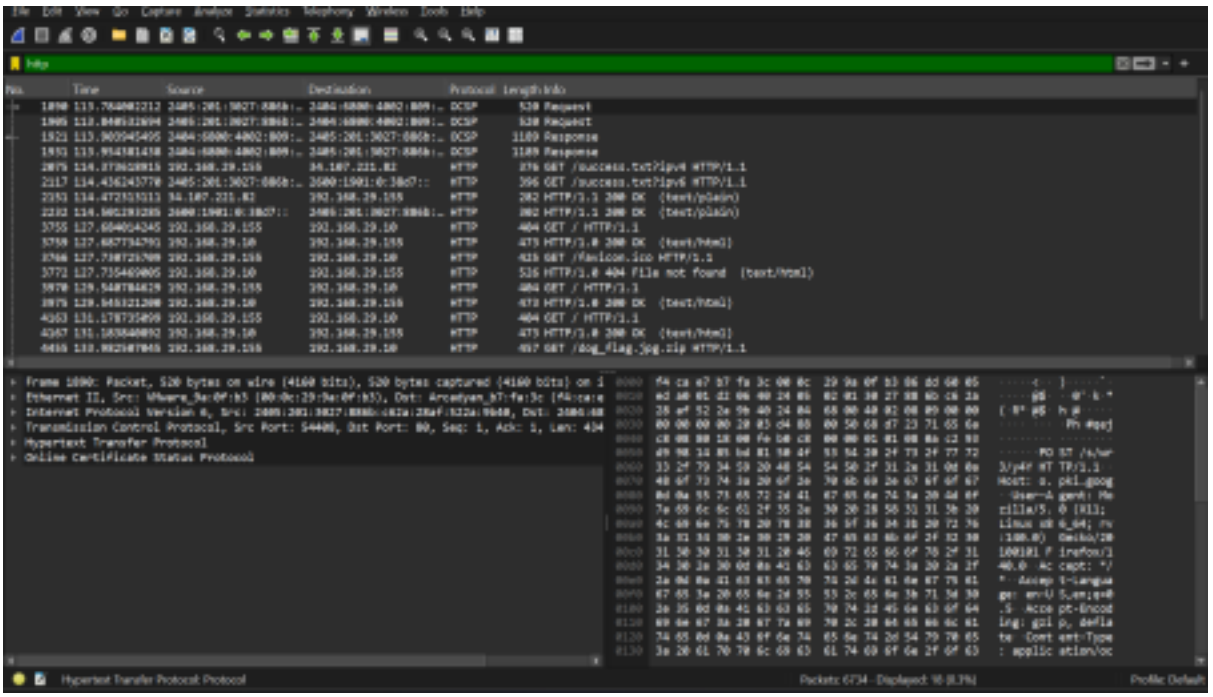
3 Tools Used

Tool	Description
Google Docs	To Prepare the report
Zip Extractor	To unzip downloaded files
Windows OS	System used for analysis
Wireshark	Network packet analyzer

4 Methodology

The PCAP file was loaded into Wireshark and various display filters were used to examine network traffic, including TCP SYN packets and HTTP requests. Traffic statistics and conversation analysis helped in identifying the attacker and victim systems. Files transferred over the network were extracted using Wireshark's Export Objects → HTTP feature.





5 Analysis and Observations

ﷺ 5.1 Victim IP Address

Victim IP:

192.168.29.155

Reason:

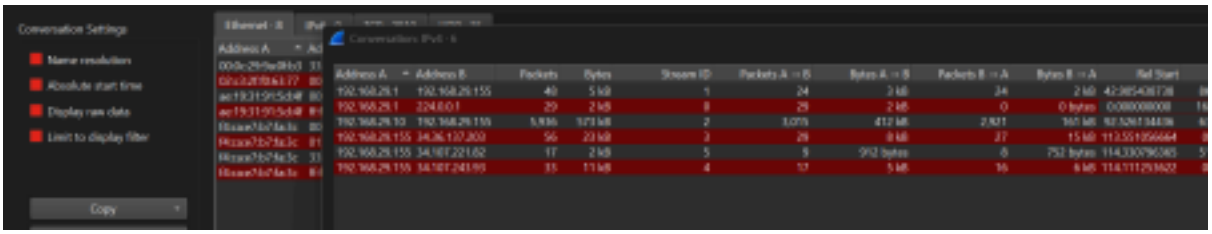
- It is a private IP address
- It receives traffic from multiple ports
- It is the target of scanning and file requests

ﷺ 5.2 Attacker IP Address

Attacker IP;192.168.29.10

Reason:

- Sends multiple TCP SYN packets
- Scans many ports of the victim
- Hosts the ZIP file on HTTP server

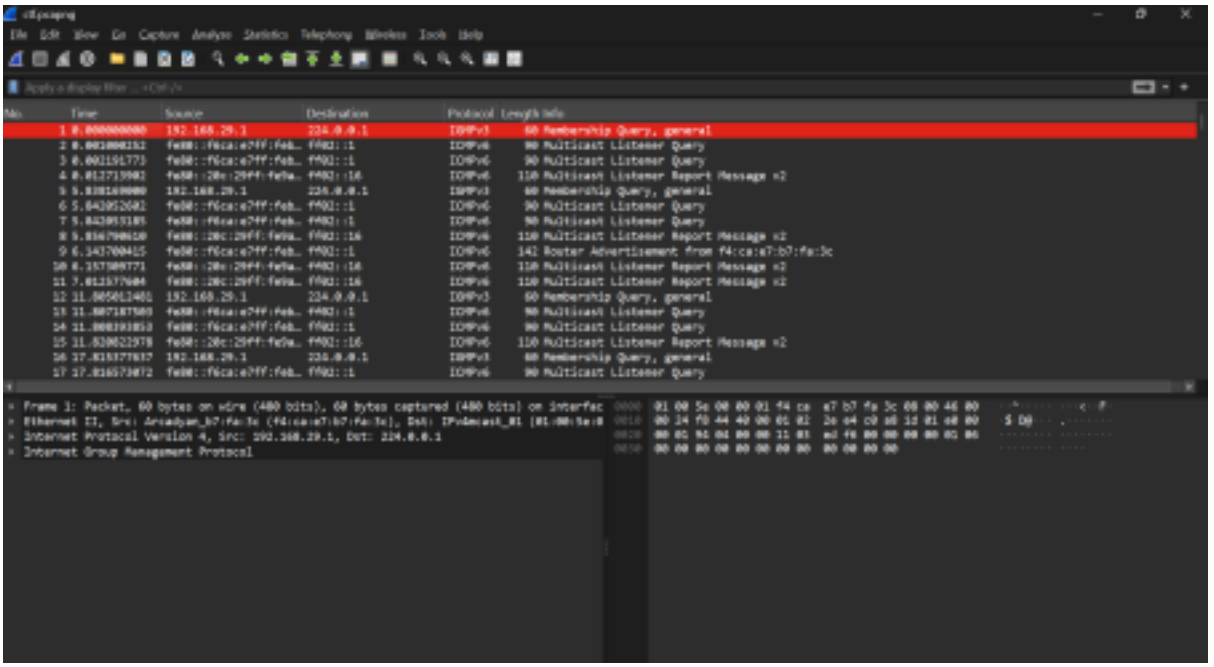


ﷺ 5.3 First Packet Timestamp

The first suspicious packet was observed at:

0.0000000000 seconds

This indicates the beginning of attack-related activity.



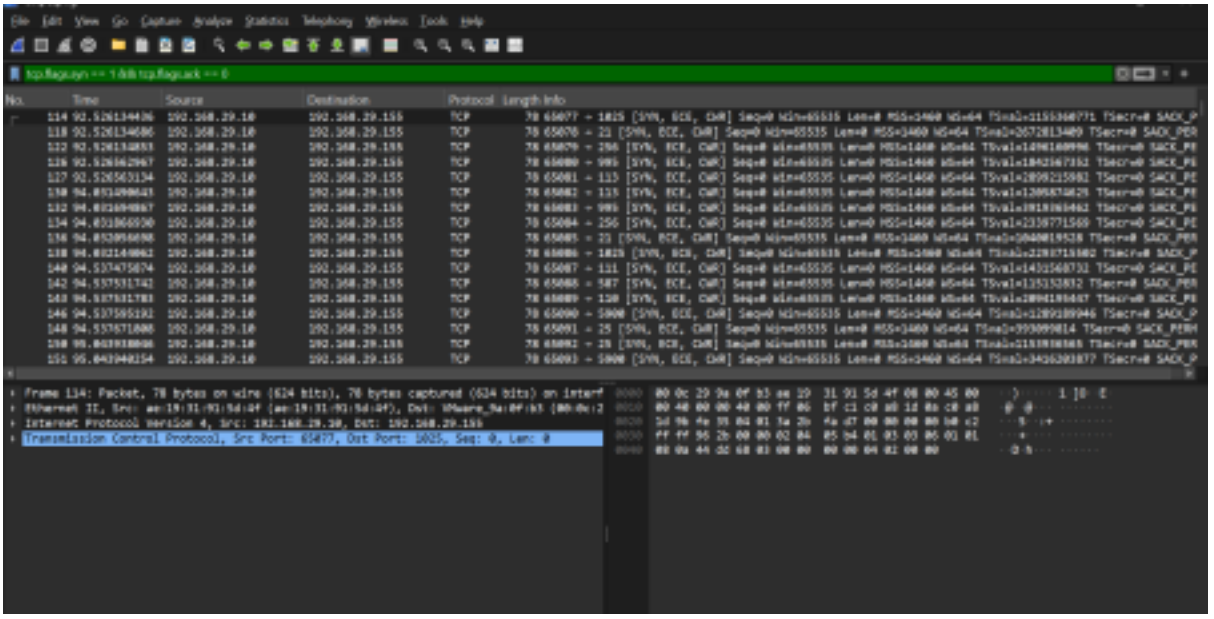
⏩⏪ 5.4 Evidence of Port Scanning

Using the filter:

tcp.flags.syn == 1 && tcp.flags.ack == 0
The following was observed:

- Multiple SYN packets
- Different destination ports
- Same source and destination IPs

This behavior indicates **port scanning**.

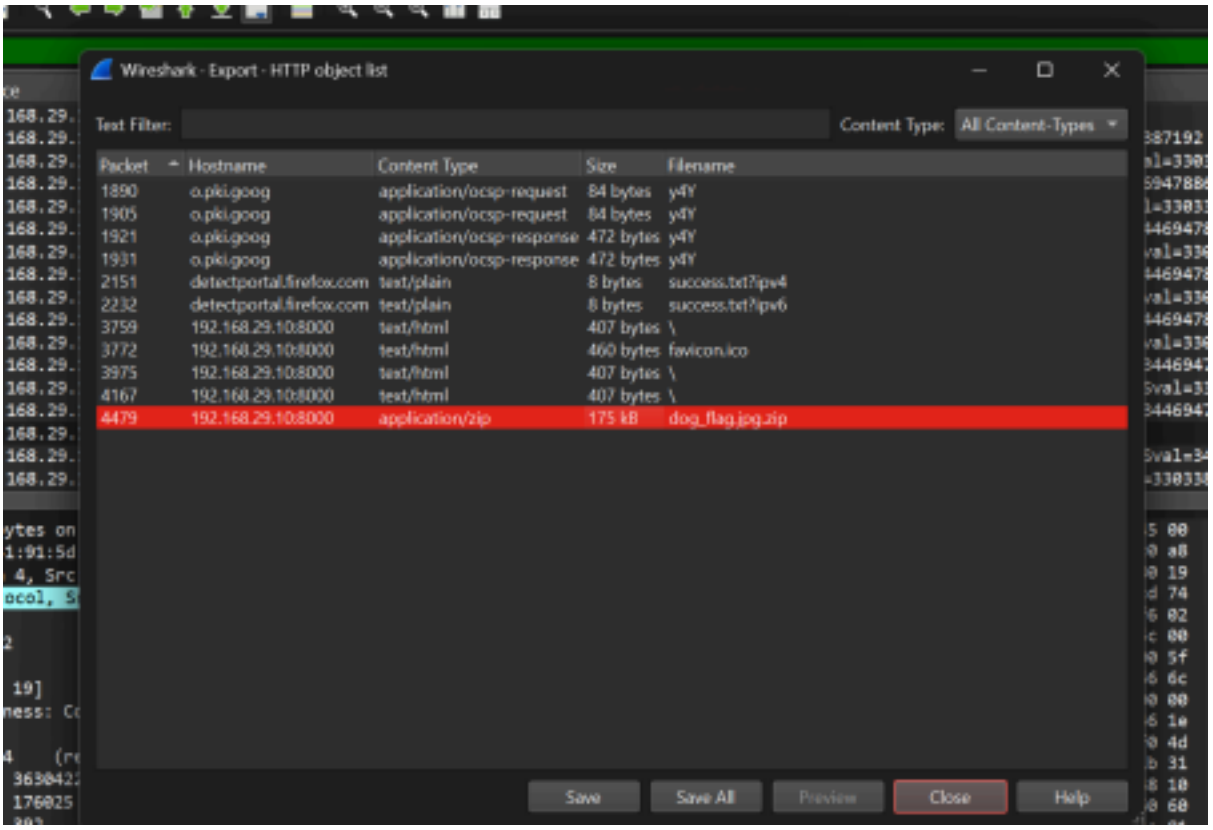


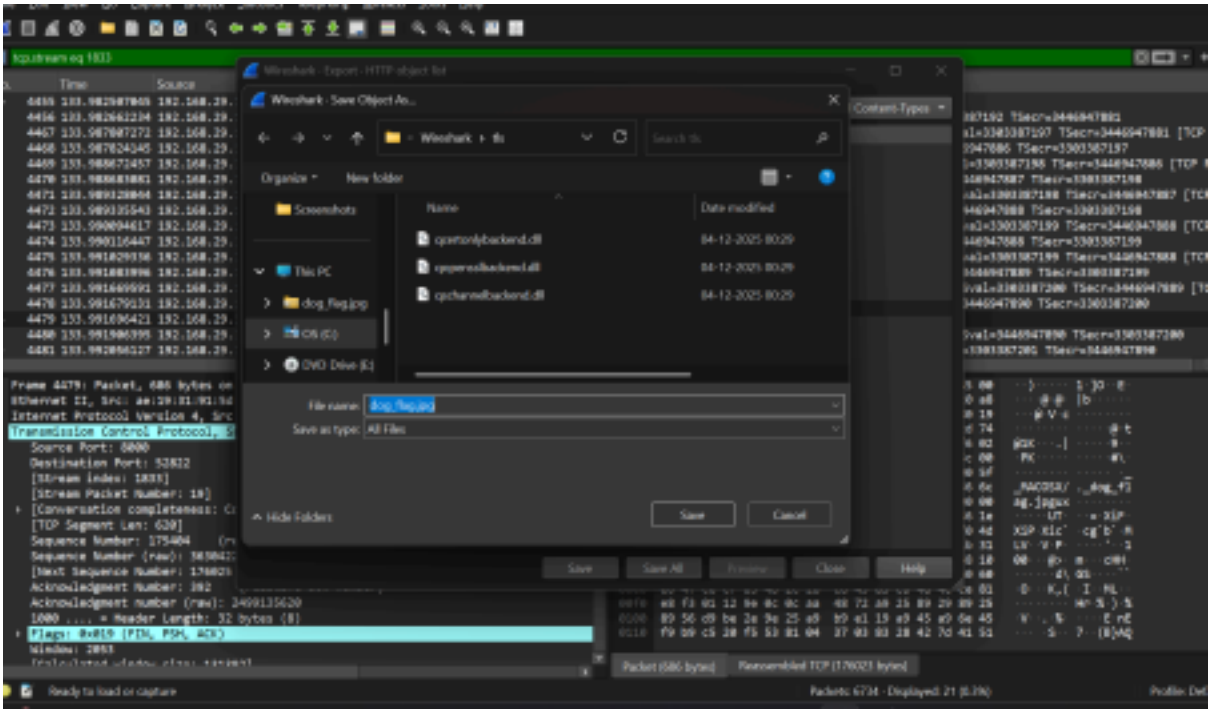
5.5 HTTP Traffic Analysis

Applying the filter:http

A suspicious file download request was found:

GET /dog_flag.jpg.zip HTTP/1.1
This confirms a ZIP file download using HTTP.





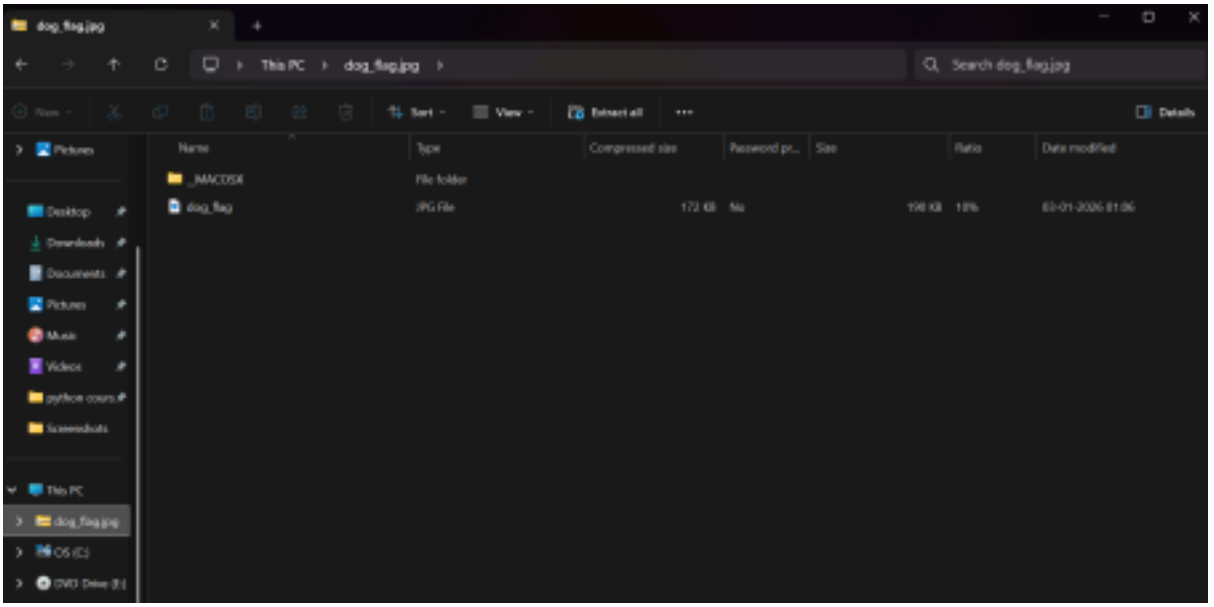
5.6 ZIP File Extraction

The ZIP file was extracted using:

File → Export Objects → HTTP

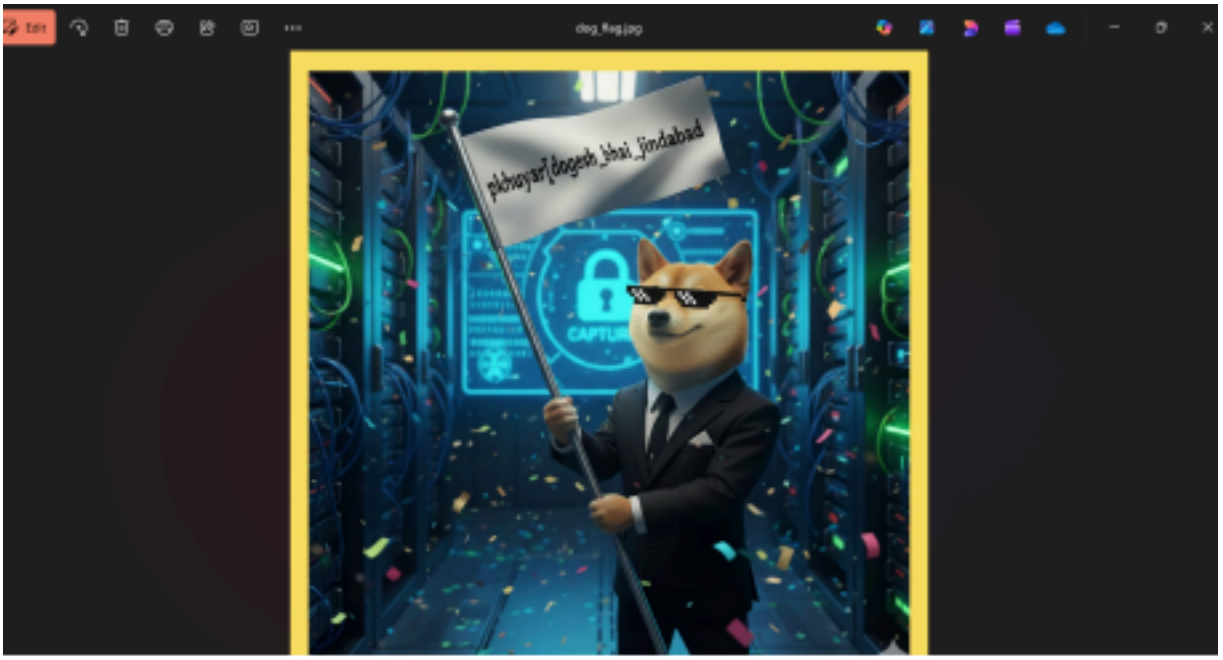
Extracted ZIP file:

dog_flag.jpg.zip



◆◆ 5.7 Flag Retrieval

After extracting the ZIP file, an image file named `dog_flag.jpg` was obtained.
The image contained the following flag:
pkhuyr{dogesh_bhai_jindabad}



6 Answers to Given Questions

Question	Answer
Attacker IP address	192.168.29.10
Victim IP address	192.168.29.155
First packet timestamp	92.526134436 seconds
Evidence of reconnaissance	TCP SYN packets to multiple ports
ZIP file name	dog_flag.jpg.zip

Flag **pkhuyr{dogesh_bhai_jin dabad}**

7 Conclusion

This project offered an in-depth understanding of network traffic analysis using the Wireshark tool. By carefully examining the PCAP file, it was possible to identify the attacker and victim systems based on IP addresses and communication patterns. Reconnaissance activity, such as port scanning, was detected by analyzing repeated connection attempts and TCP SYN packets.

Further analysis of HTTP traffic revealed the transfer of files over the network. Using Wireshark's HTTP Export Objects feature, a ZIP file was successfully extracted from the captured traffic. The contents of the ZIP file were examined, and a hidden flag was retrieved from the extracted image. Overall, this project significantly improved practical knowledge of cybersecurity by providing hands-on experience in traffic analysis, attack detection, and digital forensics.

GUIDED BY — PRASHANT SIR

THANK YOU !