

CUSTOM PAYLOAD ENCODER & OBFUSCATION FRAMEWORK

(Linux Style Project Report – Detection & Research Only)

**Project Report submitted in partial fulfillment of the requirements
of**
UNIFIED INTERNSHIP PROGRAM
(Cyber Security / Ethical Hacking)

Submitted By
Name: Aquib Ahmad Khan
Intern ID: UMID27112571911
Domain: Cyber Security

Operating System Used
Windows 11 (Linux-style methodology)

Project Duration
January 2026 – February 2026

1. Introduction

This project focuses on designing a custom payload encoder and obfuscation framework. The objective is to demonstrate how encoding and obfuscation techniques are used in malware research and detection environments for educational and defensive security purposes.

2. Project Objectives

- Understand payload encoding techniques
- Implement Base64, XOR, and Multi-layer encoders
- Generate encoded payload outputs
- Maintain structured project workflow

3. Tools & Environment

Operating System: Windows 11

Programming Language: Python 3.14.2

Editor: VS Code / Notepad

Execution Environment: PowerShell

4. Project Directory Structure

```
encoders/  
payloads/  
output/  
reports/  
screenshots/
```

5. Encoding Modules Implemented

Base64 Encoder: Converts payload into Base64 format.

XOR Encoder: Applies XOR-based obfuscation.

Multi-layer Encoder: Combines Base64 and XOR for layered obfuscation.

6. Execution & Output

Each encoder script was executed successfully using PowerShell. Encoded payloads were generated and saved in the output directory as text files.

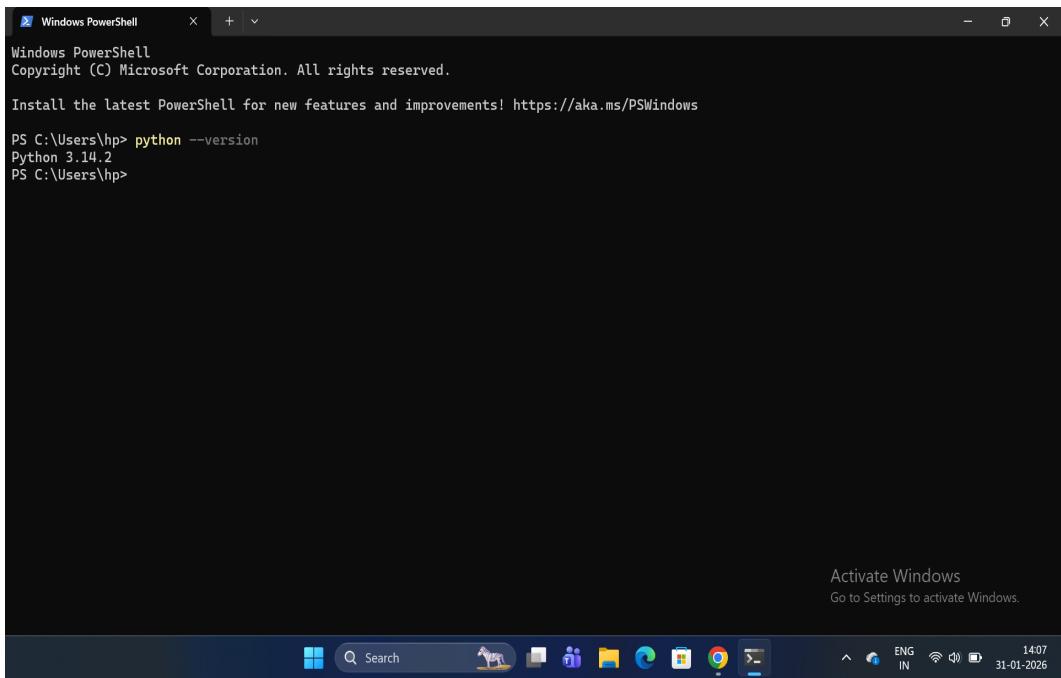
7. Screenshots & Results

The following pages contain step-by-step screenshots showing execution, directory structure, encoded outputs, and report generation.

8. Conclusion

This project successfully demonstrates payload encoding and obfuscation techniques. It helps in understanding how attackers hide payloads and how defenders analyze such techniques in a controlled, ethical environment.

Execution Screenshot



A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the following text:

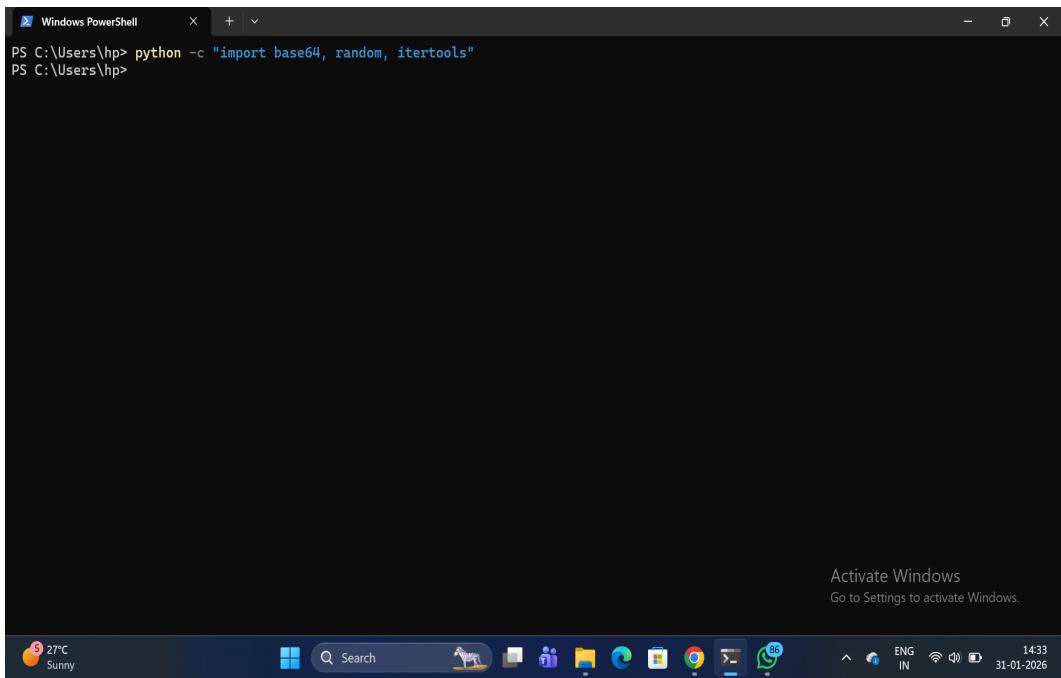
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\hp> python --version
Python 3.14.2
PS C:\Users\hp>
```

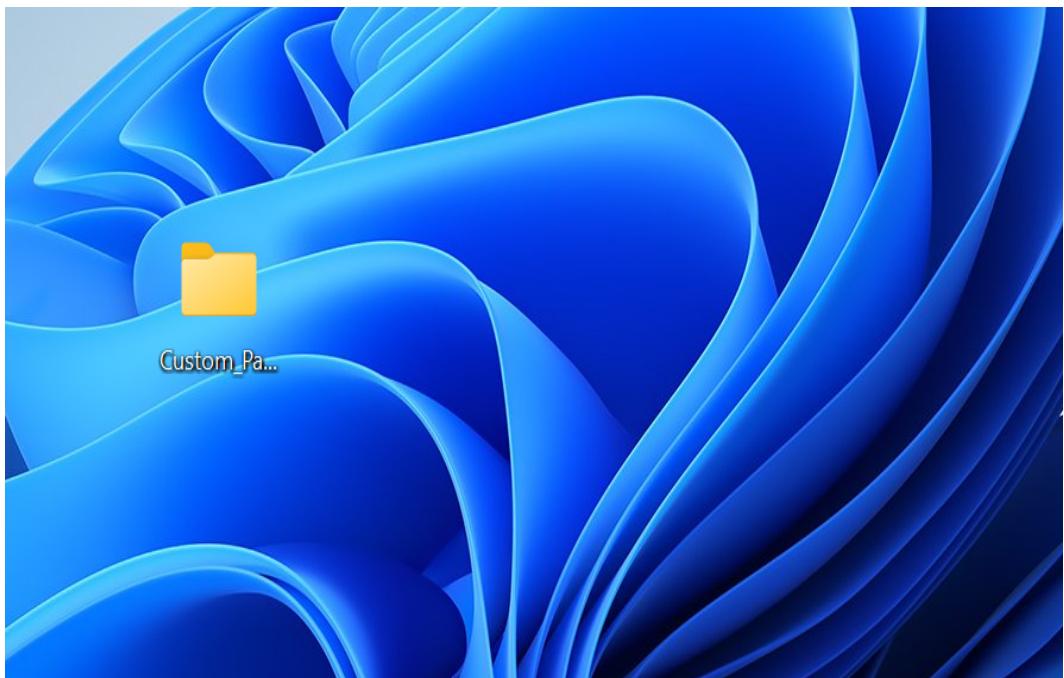
The window has a dark theme. In the bottom right corner, there is a watermark that says "Activate Windows" and "Go to Settings to activate Windows." At the very bottom of the screen, the Windows taskbar is visible, showing icons for various apps like File Explorer, Edge, and Google Chrome, along with system status indicators.

Execution Screenshot

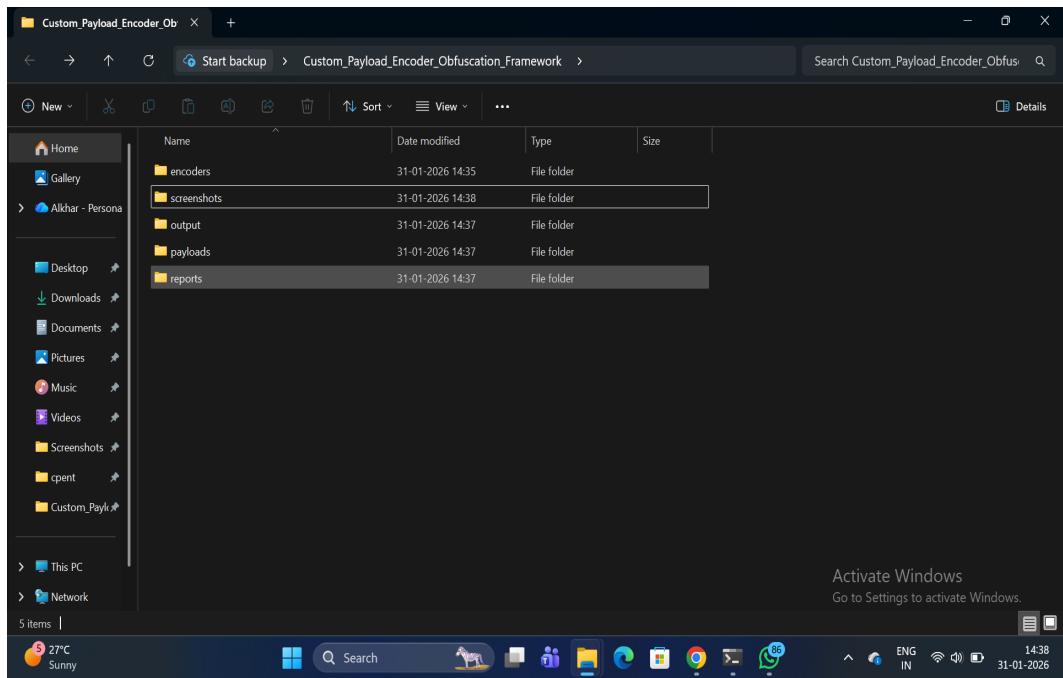


A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command entered is "python -c \"import base64, random, itertools\"". The PowerShell interface includes a title bar, a menu bar with options like File, Edit, View, Insert, Tools, Help, and Exit, and a status bar at the bottom displaying system information such as weather (27°C Sunny), date (31-01-2026), and time (14:33). The main area of the window is black, indicating no output has been displayed yet.

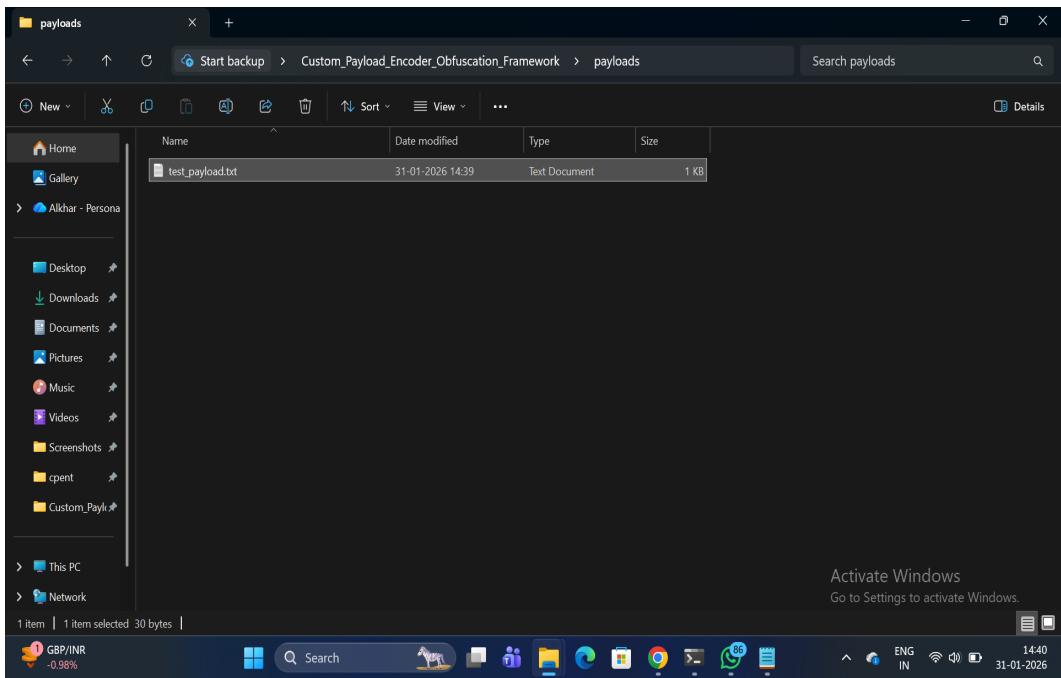
Execution Screenshot



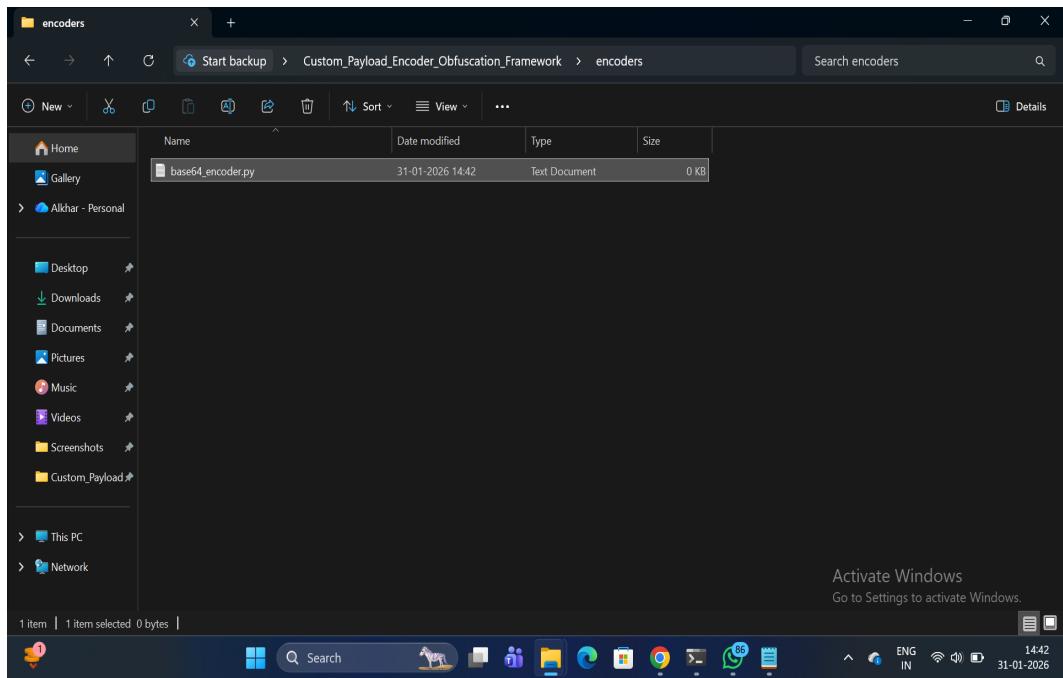
Execution Screenshot



Execution Screenshot



Execution Screenshot



Execution Screenshot

A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command `dir` is run to list files in the directory C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework\payloads, showing a single file named "test_payload.txt" with a length of 30 bytes. The date is 31-01-2026 and the time is 14:39. The command `cd ..` is run to move up one directory level. Then, the directory "encoders" is changed using `cd encoders`. Finally, the Python script `base64_encoder.py` is executed with the command `python base64_encoder.py`, resulting in a base64 encoded payload being saved to the file "base64_encoded_payload.txt". The PowerShell window has a dark theme and is running on a Windows 10 desktop.

```
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework\payloads> dir

Directory: C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework\payloads

Mode                LastWriteTime         Length Name
----                - - - - - - - - - - - - - - - - -
-a----   31-01-2026     14:39            30 test_payload.txt

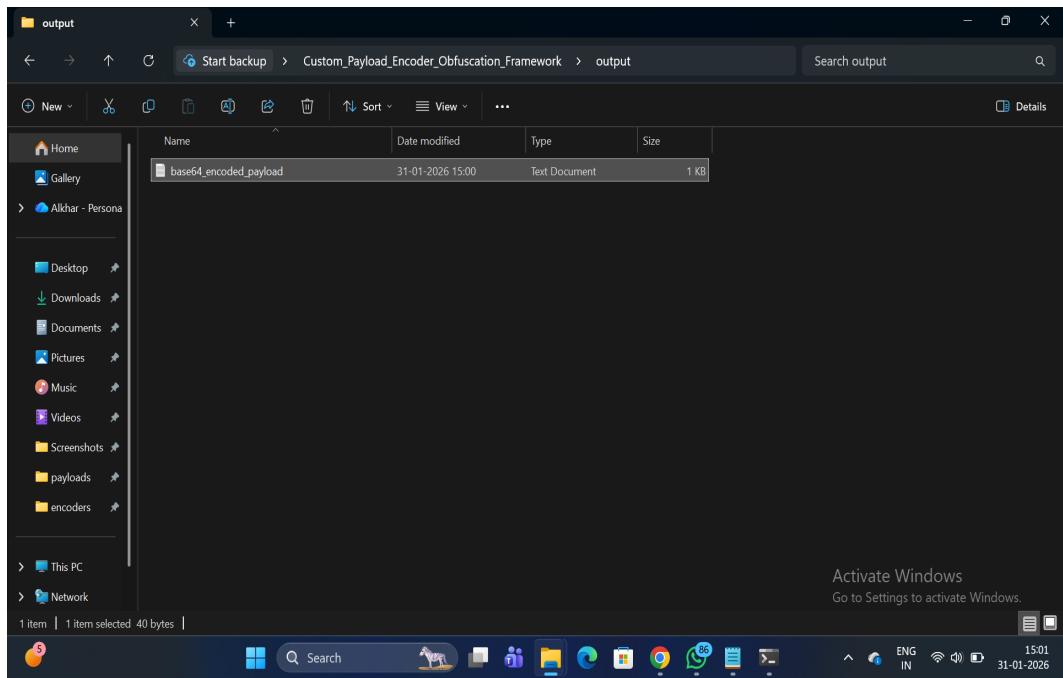
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework\payloads> cd ..

PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework> cd encoders
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework\encoders> python base64_encoder.py
[+] Base64 Encoding Completed
[+] Encoded payload saved to: ./output/base64_encoded_payload.txt
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscati0n_Framework\encoders> |
```

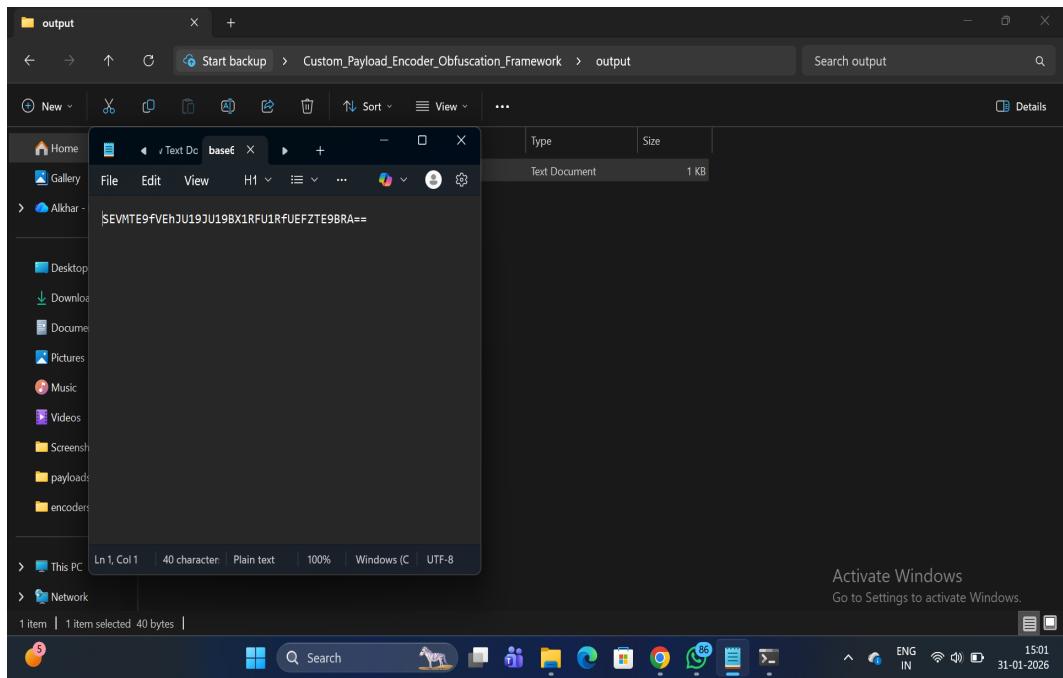
Activate Windows
Go to Settings to activate Windows.

15:00
ENG IN 31-01-2026

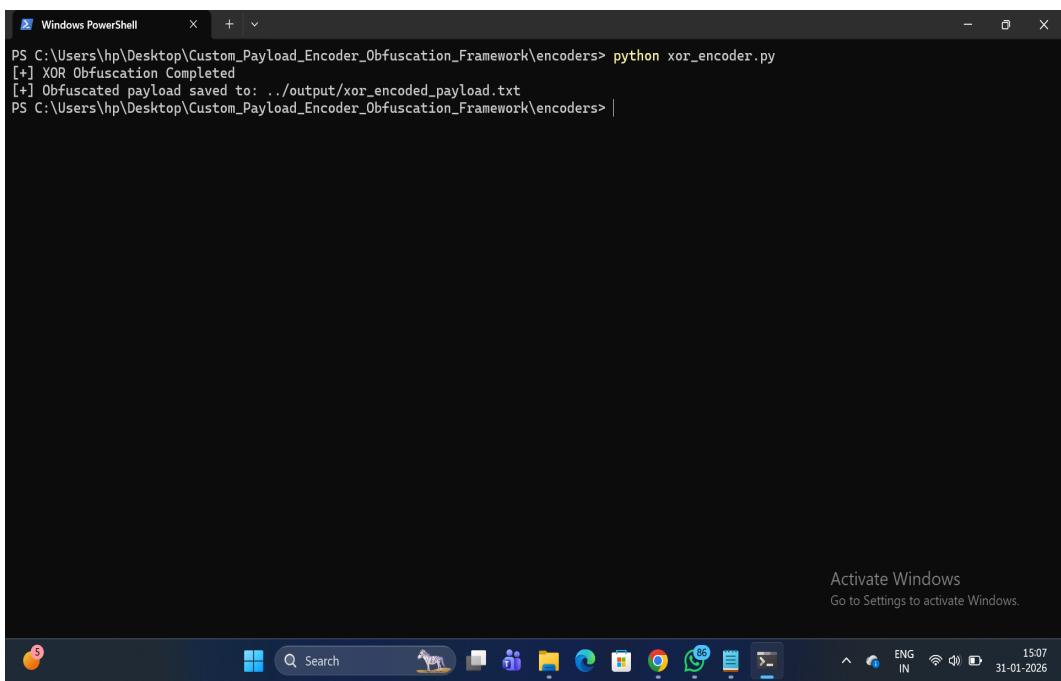
Execution Screenshot



Execution Screenshot



Execution Screenshot

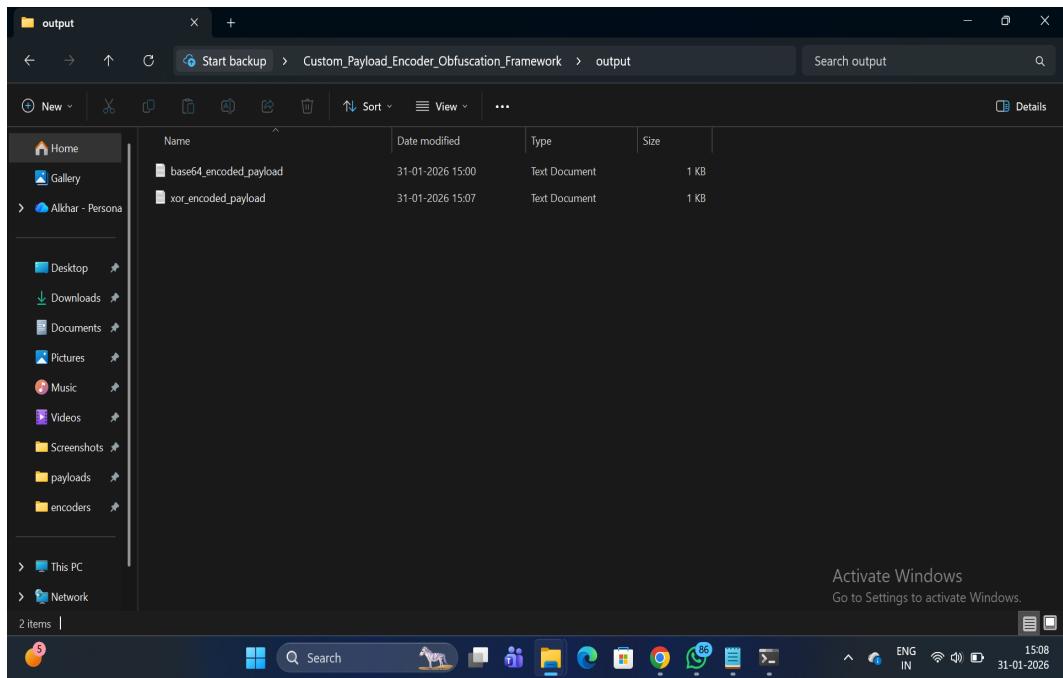


```
Windows PowerShell      + - 
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscation_Framework\encoders> python xor_encoder.py
[+] XOR Obfuscation Completed
[+] Obfuscated payload saved to: ../output/xor_encoded_payload.txt
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscation_Framework\encoders> |
```

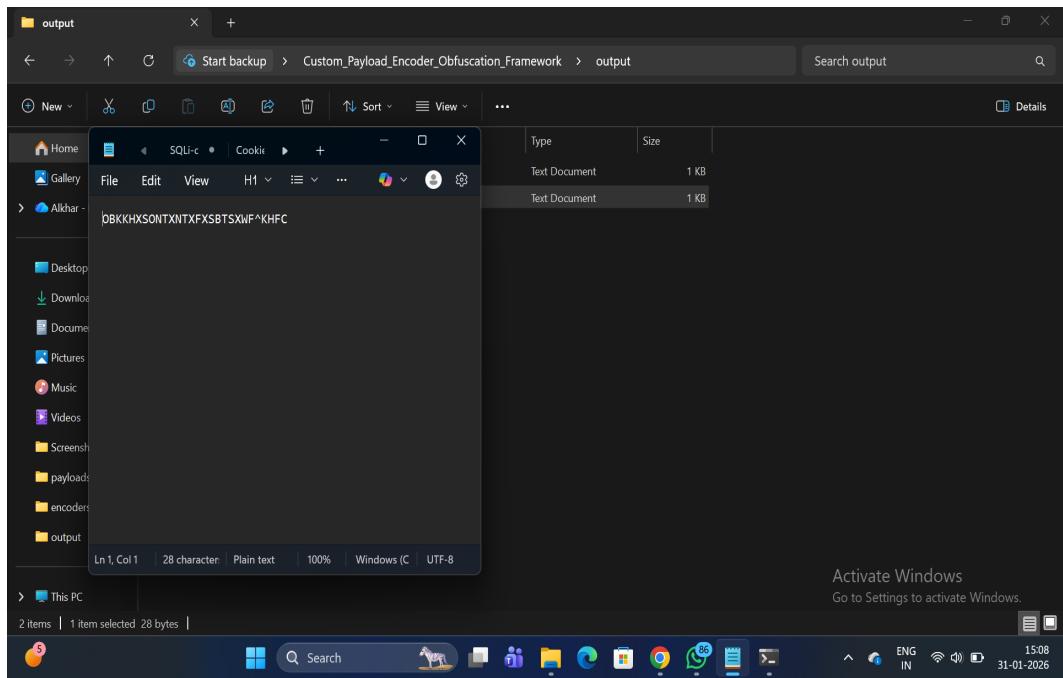
Activate Windows
Go to Settings to activate Windows.

15:07
31-01-2026

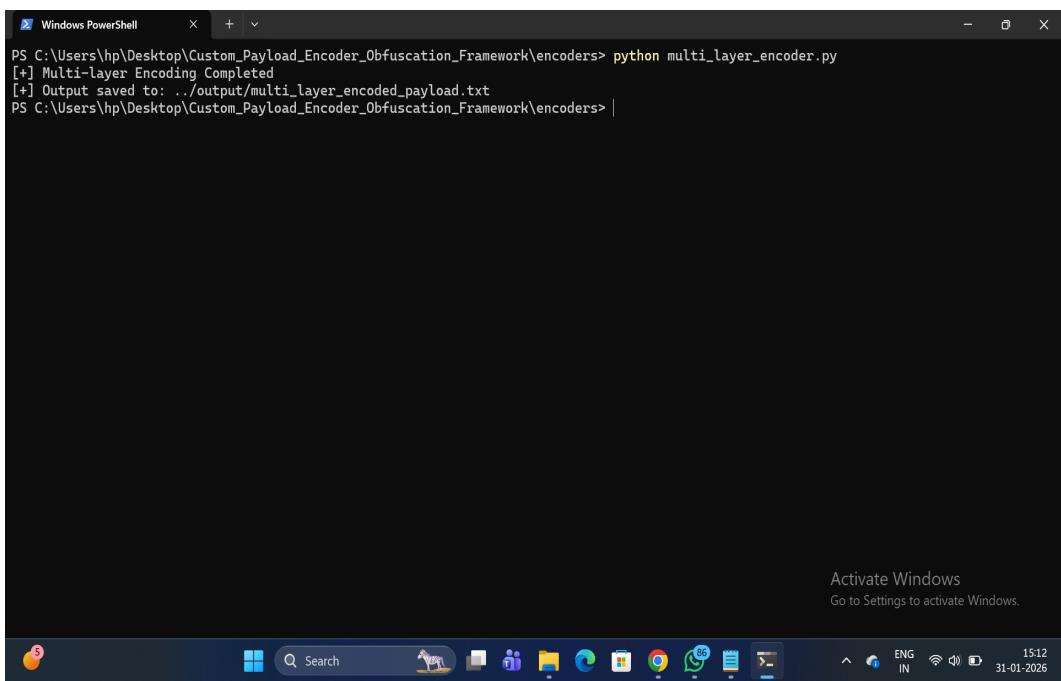
Execution Screenshot



Execution Screenshot



Execution Screenshot



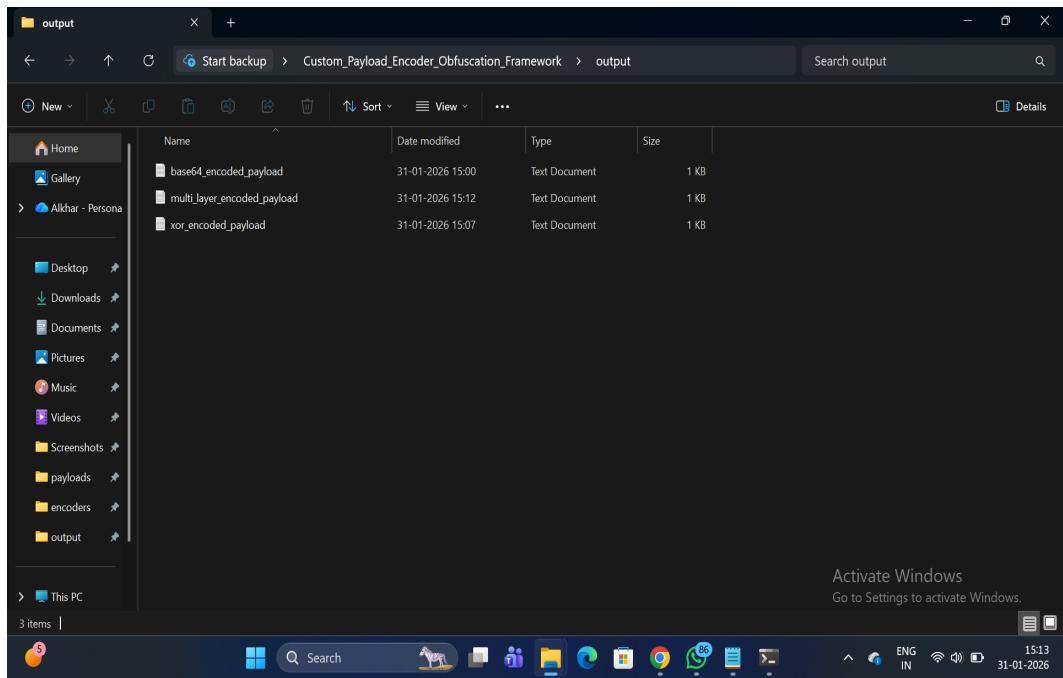
A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command executed was `python multi_layer_encoder.py`. The output indicates that "Multi-layer Encoding Completed" and the "Output saved to: ./output/multi_layer_encoded_payload.txt". The PowerShell window is set against a dark background, and the taskbar at the bottom shows various pinned icons and the system tray.

```
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscation_Framework\encoders> python multi_layer_encoder.py
[+] Multi-layer Encoding Completed
[+] Output saved to: ./output/multi_layer_encoded_payload.txt
PS C:\Users\hp\Desktop\Custom_Payload_Encoder_0bfuscation_Framework\encoders> |
```

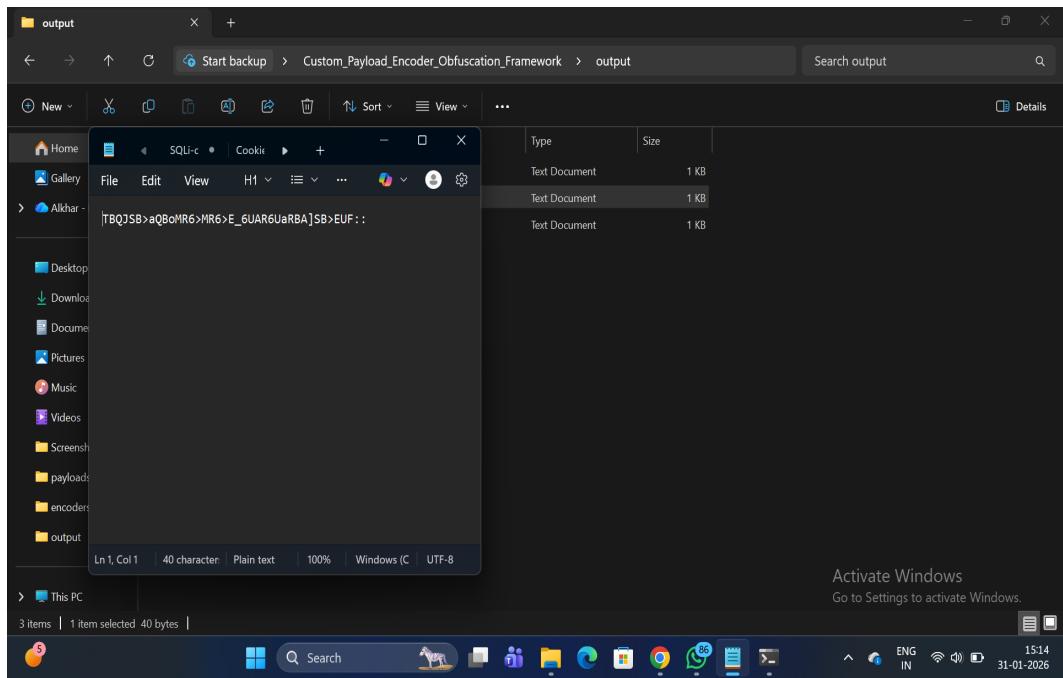
Activate Windows
Go to Settings to activate Windows.

5 Search 🐾 ⏺ ENG IN 15:12 31-01-2026

Execution Screenshot



Execution Screenshot



Execution Screenshot

