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.

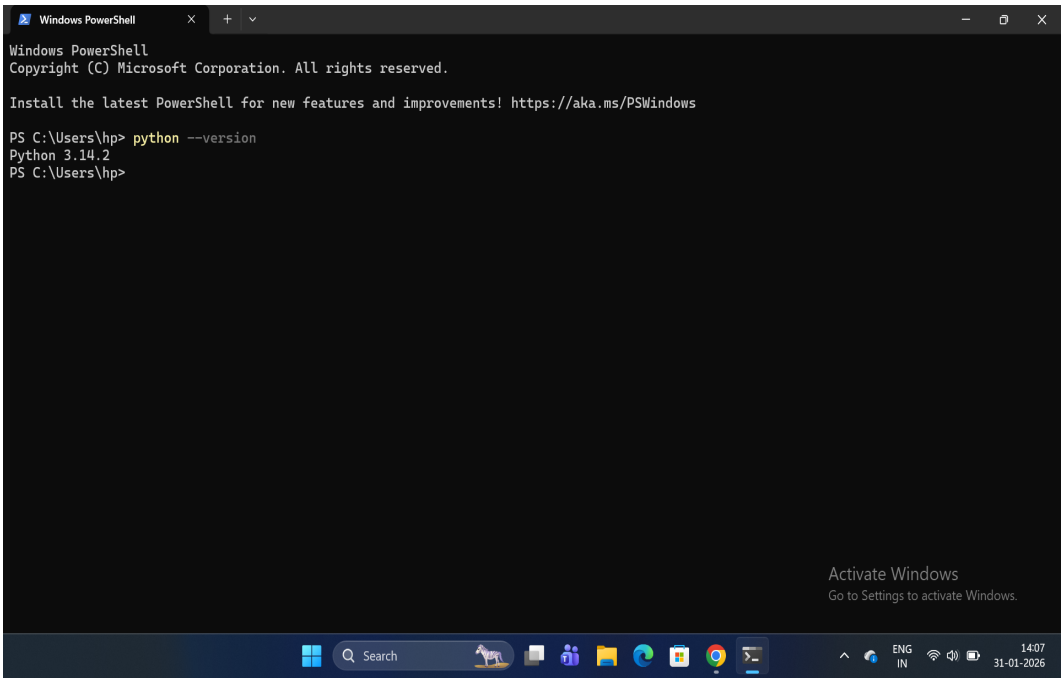
7. Screenshots & Results

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

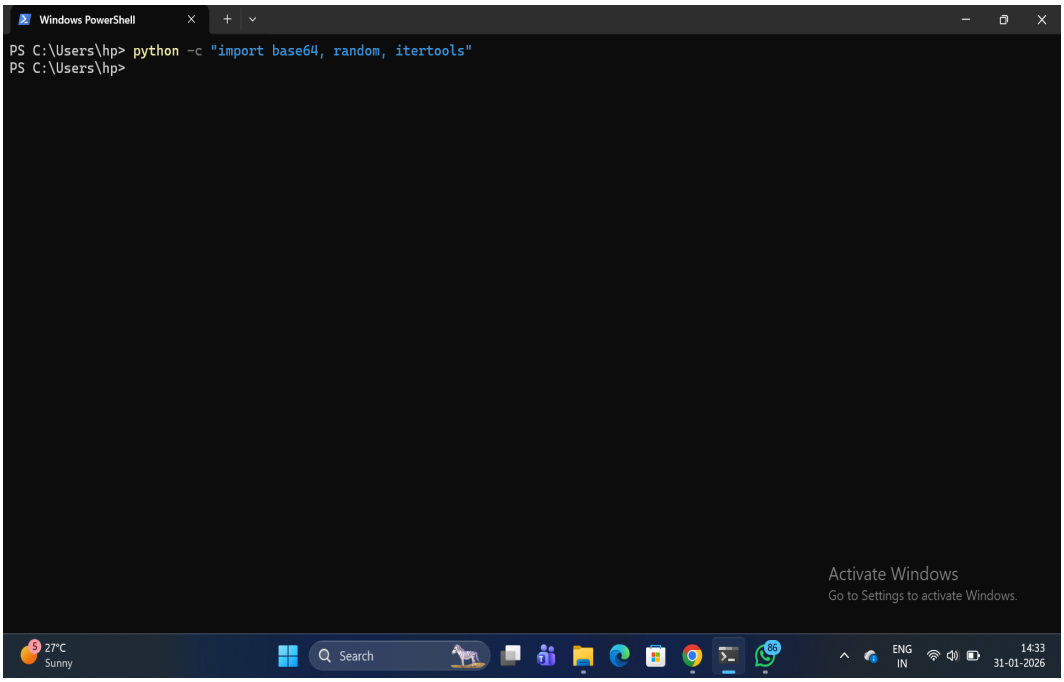
8. Conclusion

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.

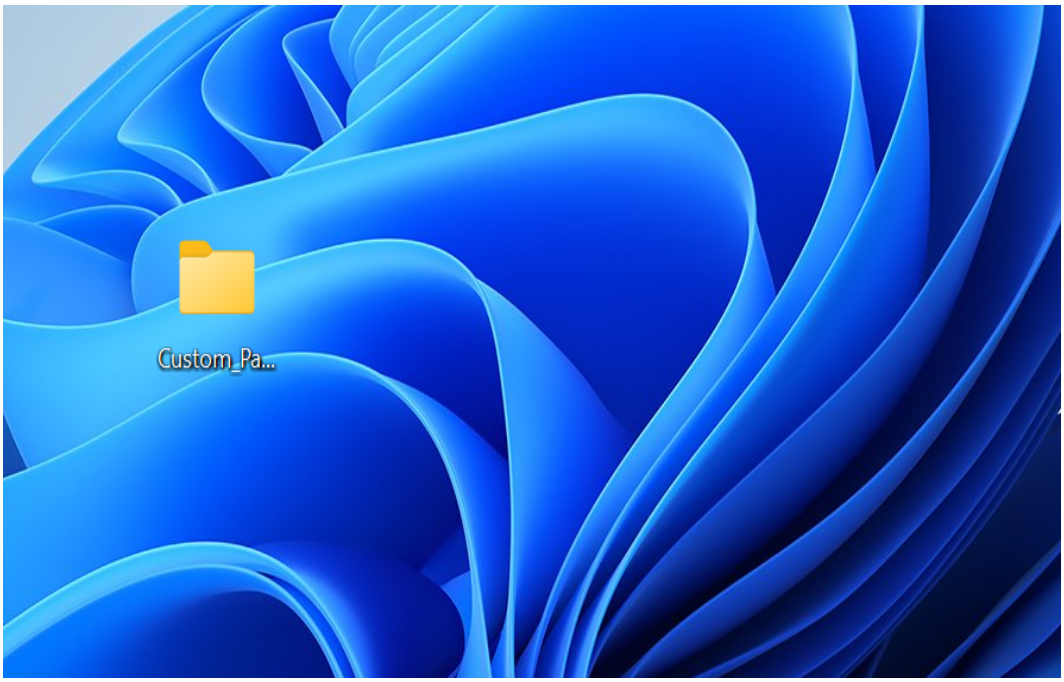
Execution Screenshot



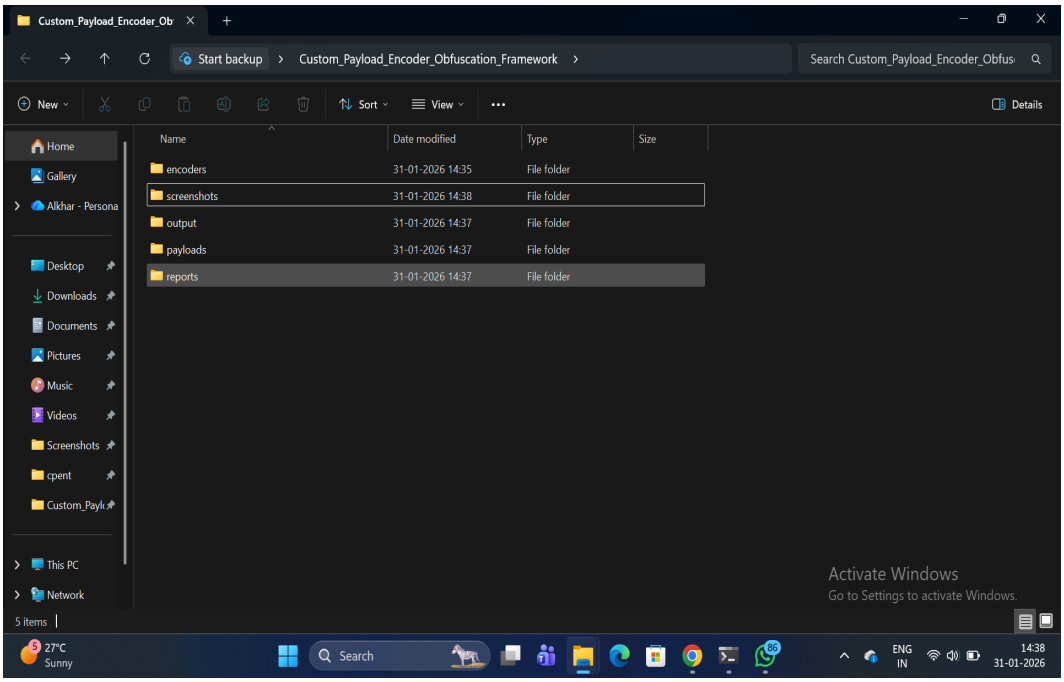
Execution Screenshot



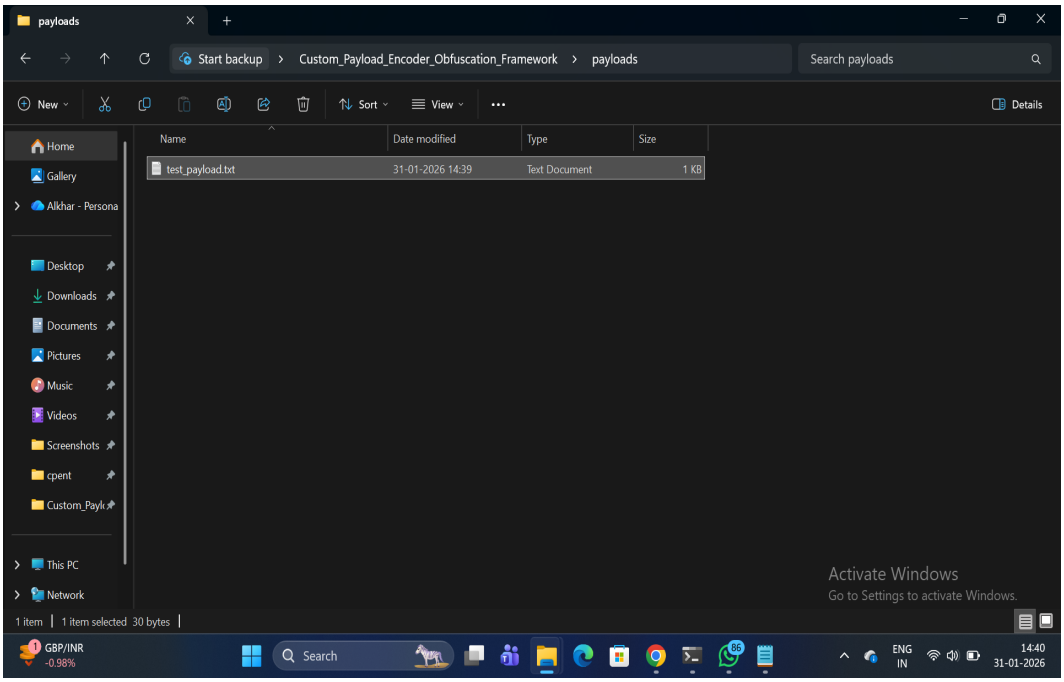
Execution Screenshot



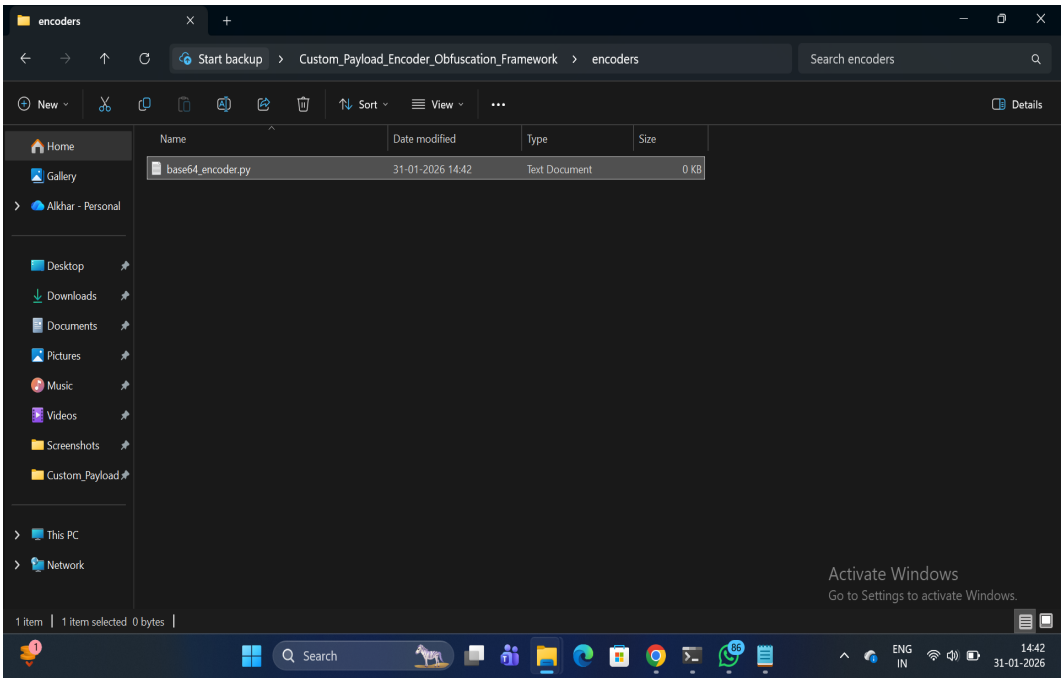
Execution Screenshot



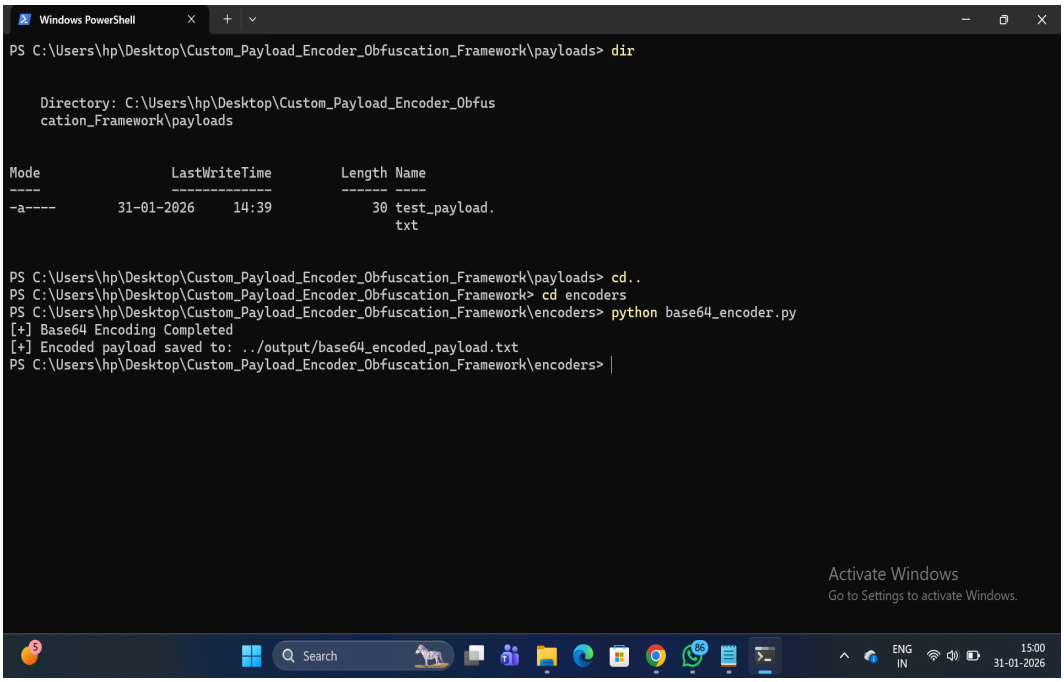
Execution Screenshot



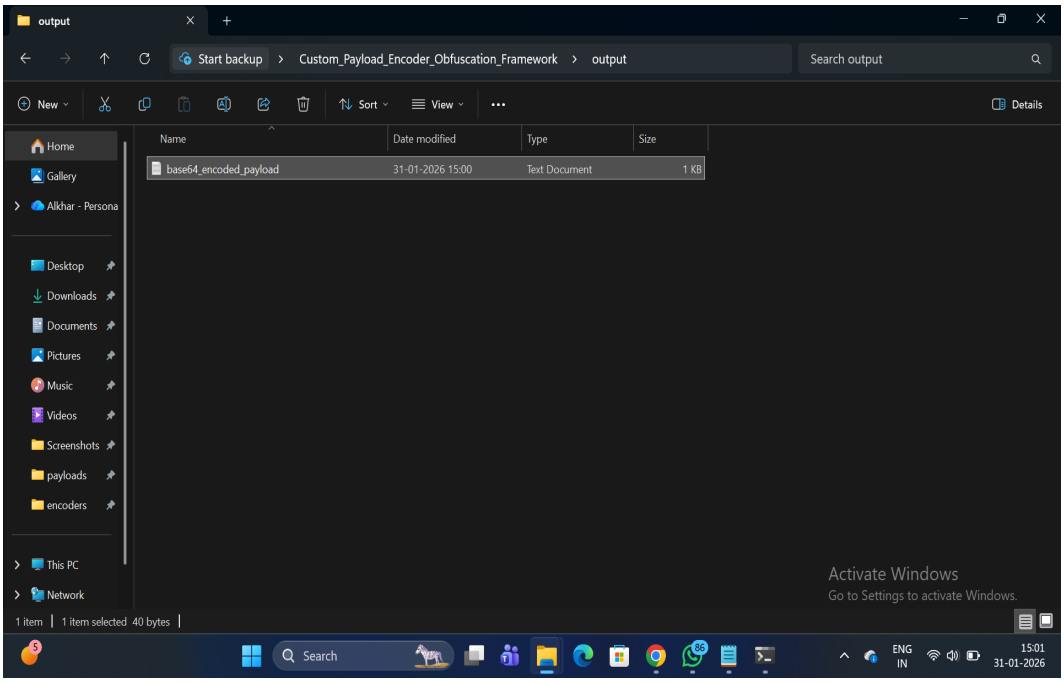
Execution Screenshot



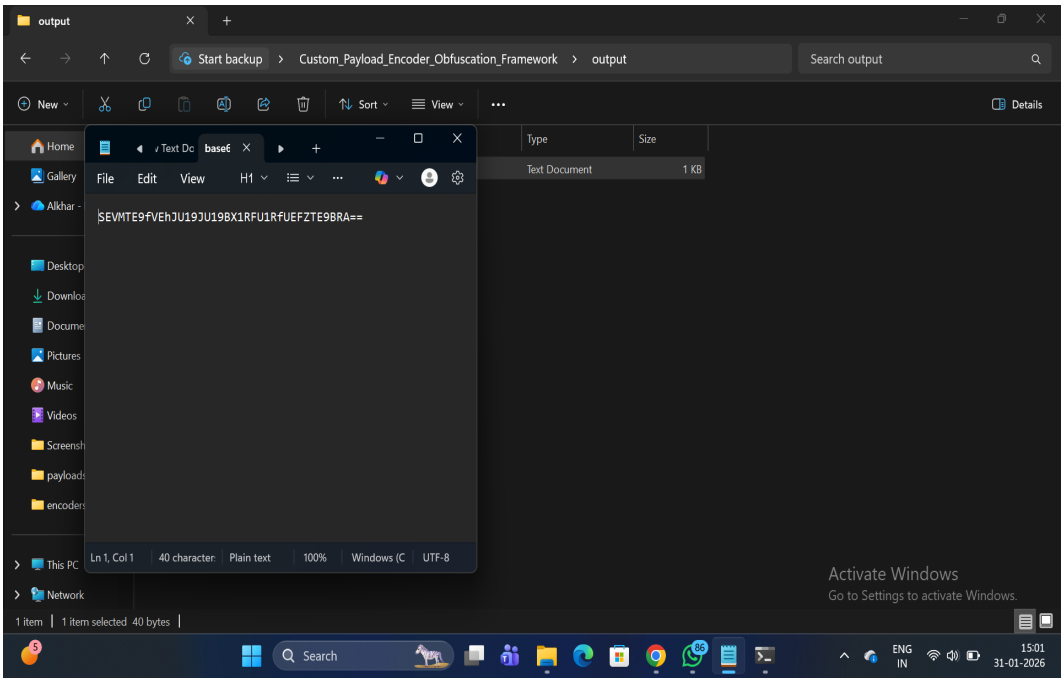
Execution Screenshot



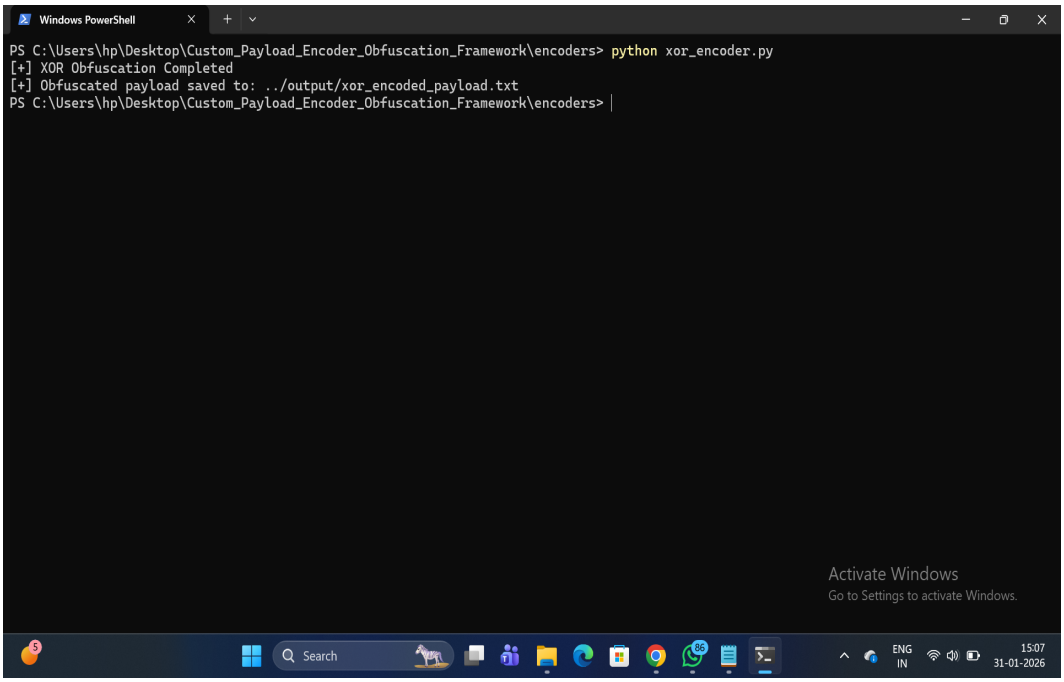
Execution Screenshot



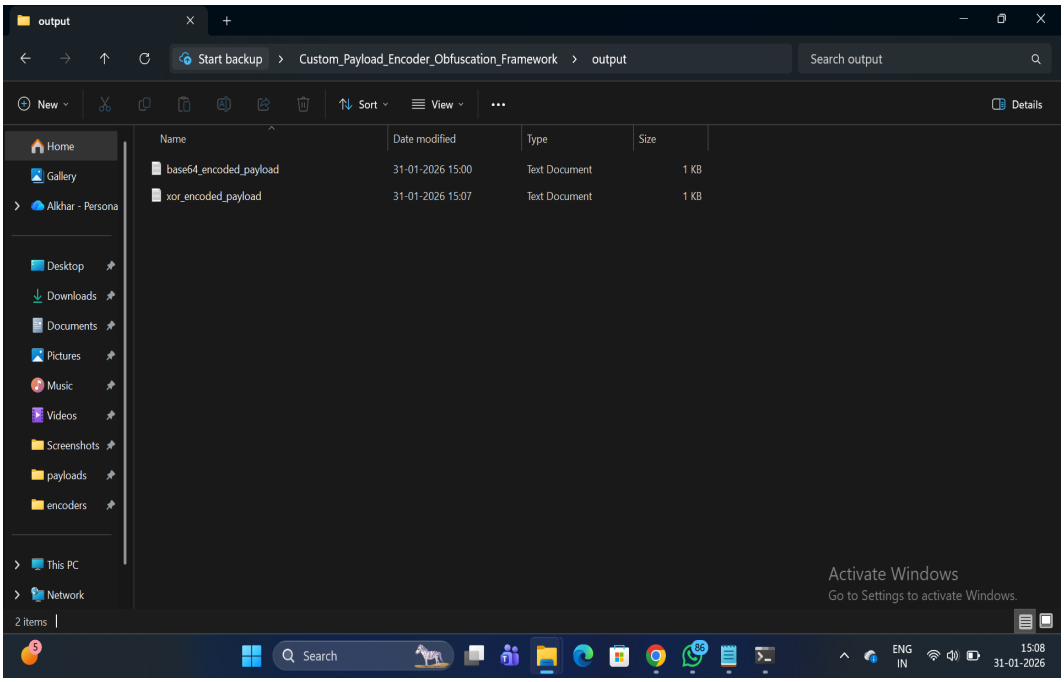
Execution Screenshot



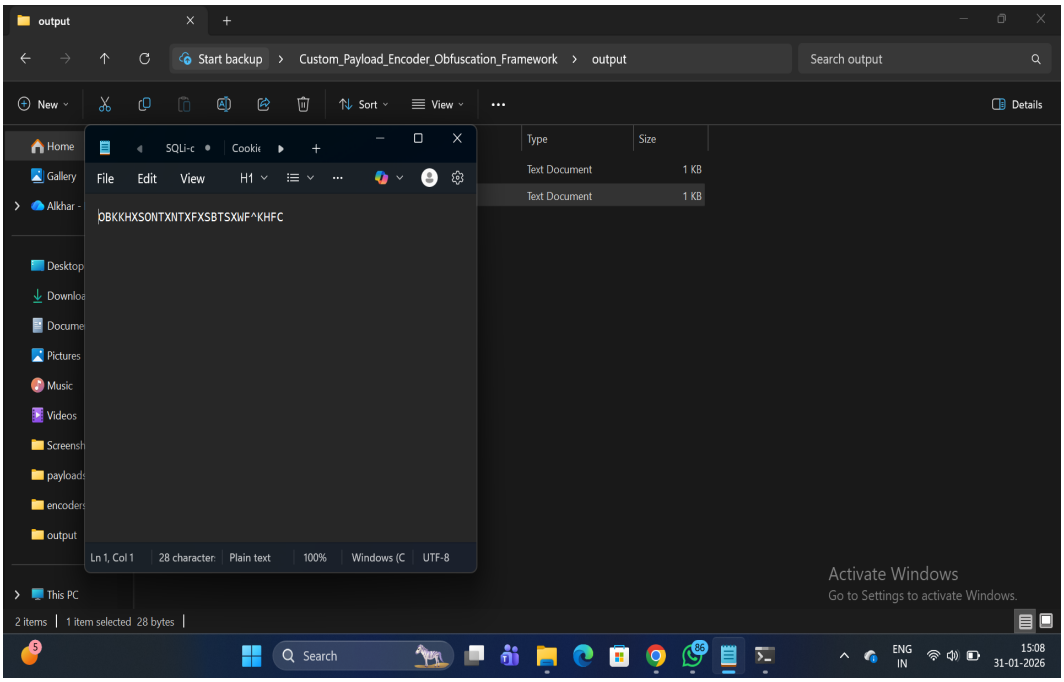
Execution Screenshot



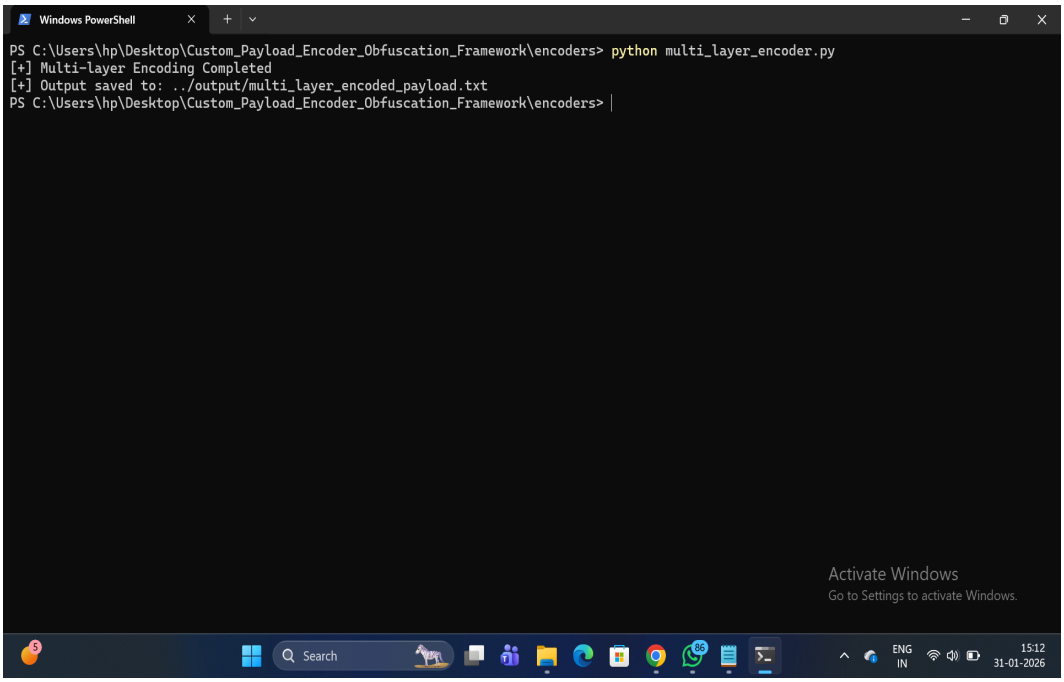
Execution Screenshot



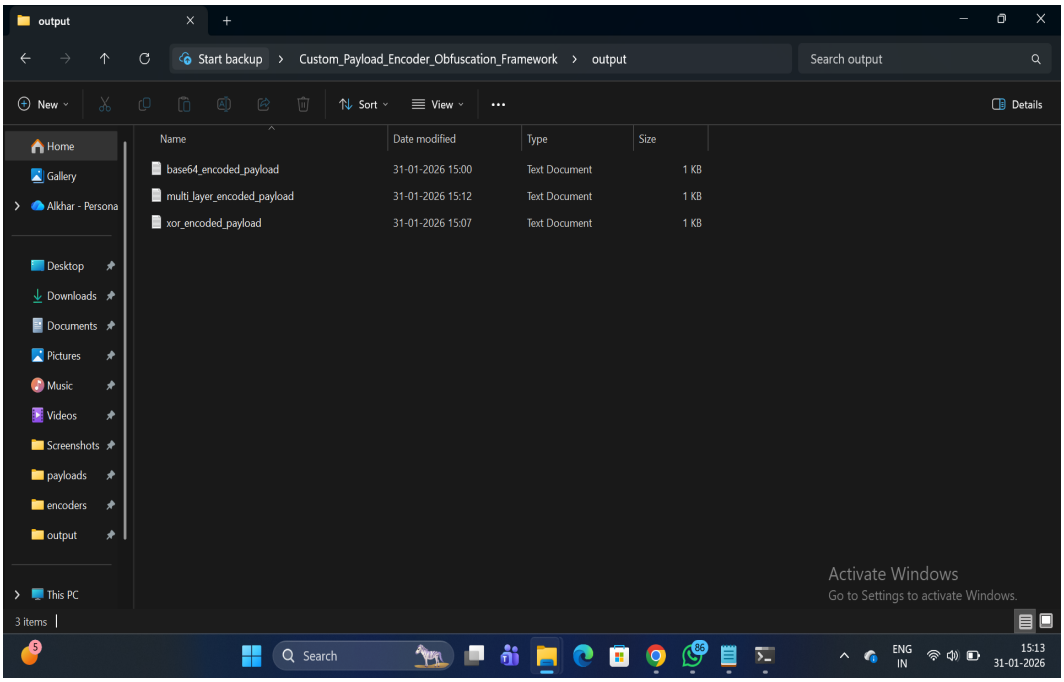
Execution Screenshot



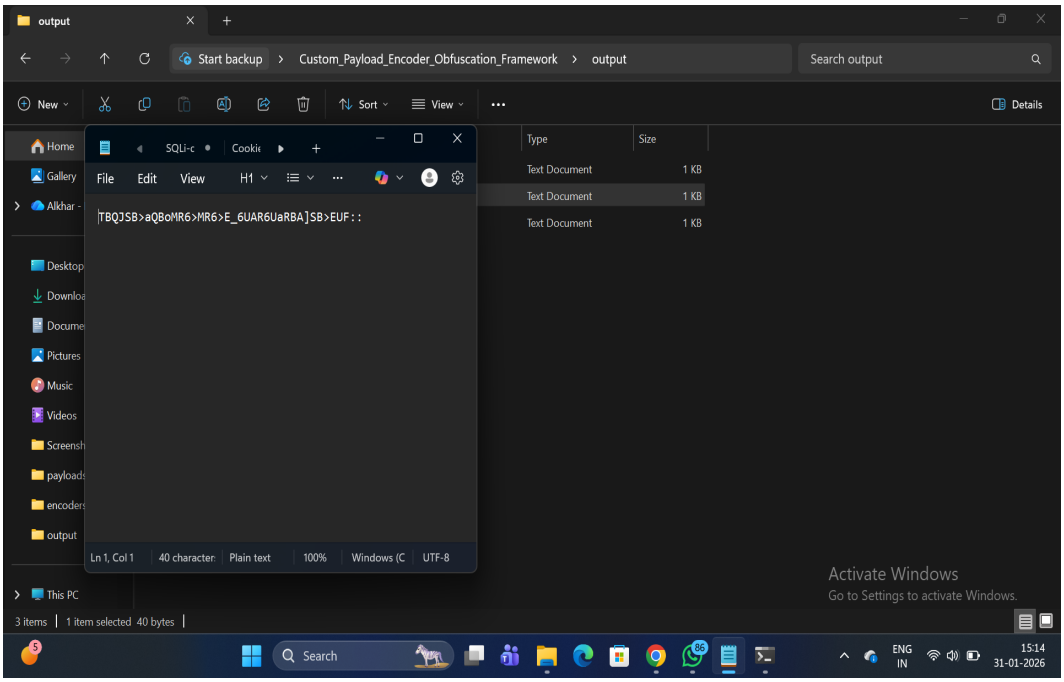
Execution Screenshot



Execution Screenshot



Execution Screenshot



Execution Screenshot