National College of Ireland

Configuration Manual

MSc Research Project
M.Sc. Cyber Security

Aryan Kedare
Student ID: x23290323

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Aryan Kedare

Student ID: X23290323

Programme: M. Sc Cyber Security **Year:** 2024-25

Module: MSc (Research) Practicum

Lecturer: Joel Aleburu

Submission Due Date: 11th August 2025

Project Title: Developing Proactive Measures Against Increasingly Sophisticated Ransomware-as-a-Service (RaaS) Attacks

Word Count: ..... **Page Count:** .....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Aryan Kedare

Date: 11 August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project	□

is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual
Developing Proactive Measures Against Increasingly Sophisticated Ransomware-as-a-Service (RaaS) Attacks

Aryan Kedare
X23290323

1 Introduction

This configuration manual provides step-by-step instructions for deploying and running the AI-Based Ransomware Detection and Response System. The project intends to proactively detect and mitigate Ransomware-as-a-Service threats, using machine learning, behaviour heuristics and lightweight file protection.
The system works in a controlled, virtualized environment using a Windows 11 guest VM hosted on a Linux-based machine which is kali linux using VirtualBox. The monitoring application monitor.py is using a trained Random Forest model to evaluate system activity in real time and classify behaviour as benign or ransomware-related based on features such as file access, registry edits, entropy changes and API usage.
When suspicious behaviour is detected, the system classifies the likely ransomware type like Encryption, Shadow Wiper, CryptoAPI-based or Generic and depending on severity, takes automated protective actions. These include encrypting sensitive files using hash_conceal() function, simulating access lockdown by triggering zero_trust_enforce() and logging all relevant details to ai_detection_log.txt.
This manual helps developers, testers, cybersecurity researchers or system administrators who wish to test the tool and make a progress in the field.

2 System Specification

2.1 The following is the hardware configurations of the machine.

Host Machine Specification

	Specification
Operating System	Kali Linux
Virtualization Tool	VirtualBox 6.x or higher
Python Version	Python 3.10 or above
RAM	16 GB
Disk Space	250 GB

Virtual Isolated Environment Specification

	Specification
Operating System	Windows 11 – Latest Updated
RAM	16 GB
Disk Space	250 GB

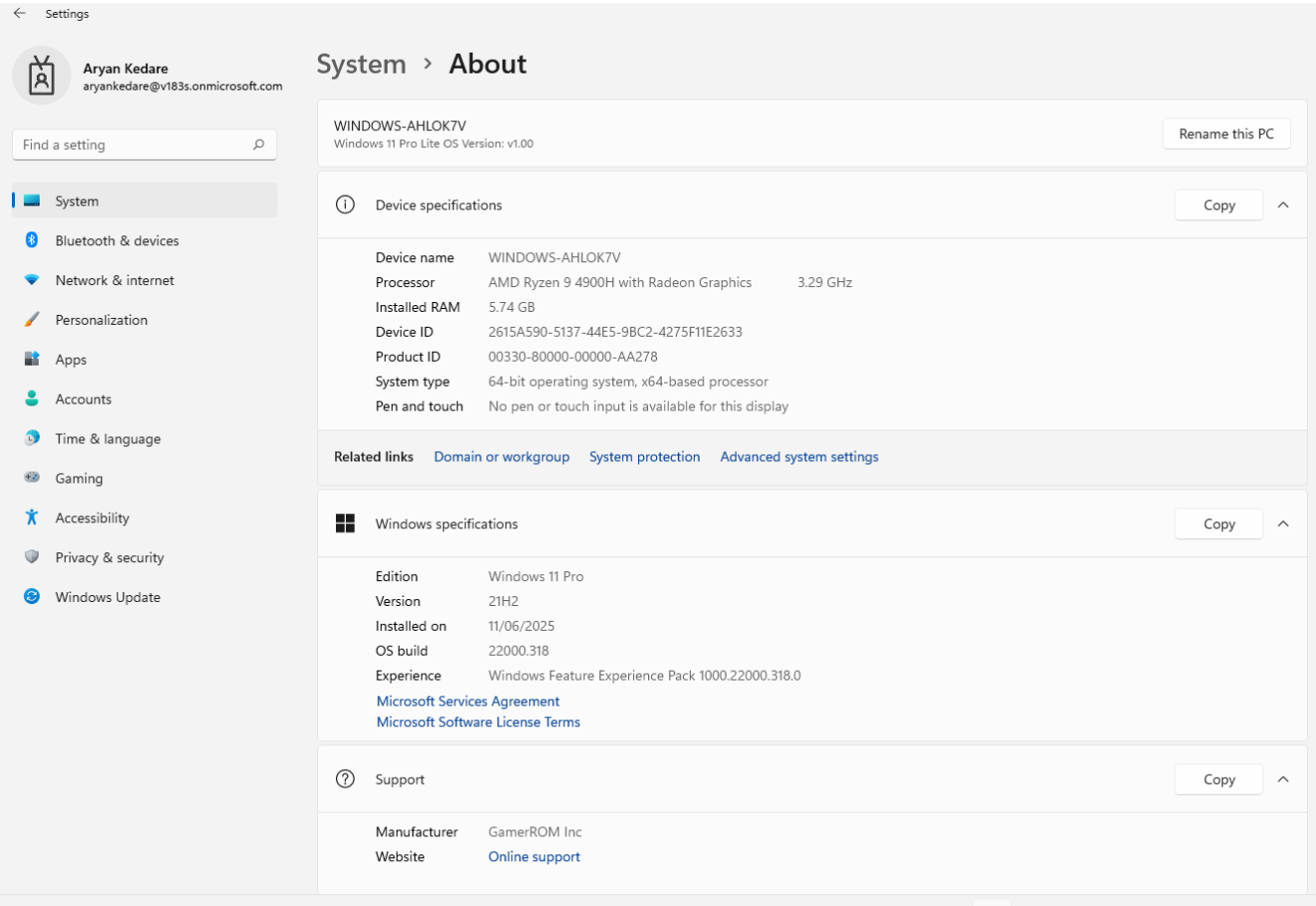

Figure 1: Virtual Machine Specs

3 Required Tools and Libraries

- Inside Windows VM following tools needs to be installed

  1. Visual Code Studio: https://code.visualstudio.com/
  2. Python Latest Version: https://www.python.org/downloads/
  3. Notepad++: https://notepad-plus-plus.org/

- Installing required python libraries

pip install pandas scikit-learn joblib psutil

```
PS C:\Users\AryanKedare\Downloads> pip install pandas scikit-learn joblib psutil
Requirement already satisfied: pandas in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (2.3.0)
Requirement already satisfied: scikit-learn in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (1.7.0)
Requirement already satisfied: joblib in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (1.5.1)
Requirement already satisfied: psutil in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (7.0.0)
Requirement already satisfied: numpy>=1.26.0 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from pandas) (2.3.0)
Requirement already satisfied: python-dateutil>=2.8.2 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from pandas) (2.9.0.post0)
Requirement already satisfied: pytz>=2020.1 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from pandas) (2025.2)
Requirement already satisfied: tzdata>=2022.7 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from pandas) (2025.2)
Requirement already satisfied: scipy>=1.8.0 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from scikit-learn) (1.15.3)
Requirement already satisfied: threadpoolctl>=3.1.0 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from scikit-learn) (3.6.0)
Requirement already satisfied: six>=1.5 in c:\users\aryankedare\appdata\local\programs\python\python313\lib\site-packages (from python-dateutil>=2.8.2->pandas) (1.17.0)
```

Figure 2: pip installation

4 Project Structure

```
RansomwareDetection/
├── monitor.py
├── conceal_module.py
├── ransomware_rf_model.pkl
├── decrypt_file.py
├── simulate_api_trace.bat
├── simulate_system_load.py
├── ai_detection_log.txt
├── C:\SensitiveData\important.pdf
```

Figure 3: Project Stucture

5 Initial Setup

Step 1: Creating Virtual Machine

- Using Kali Linux as the host machine and using VirtualBox to install Windows 11.

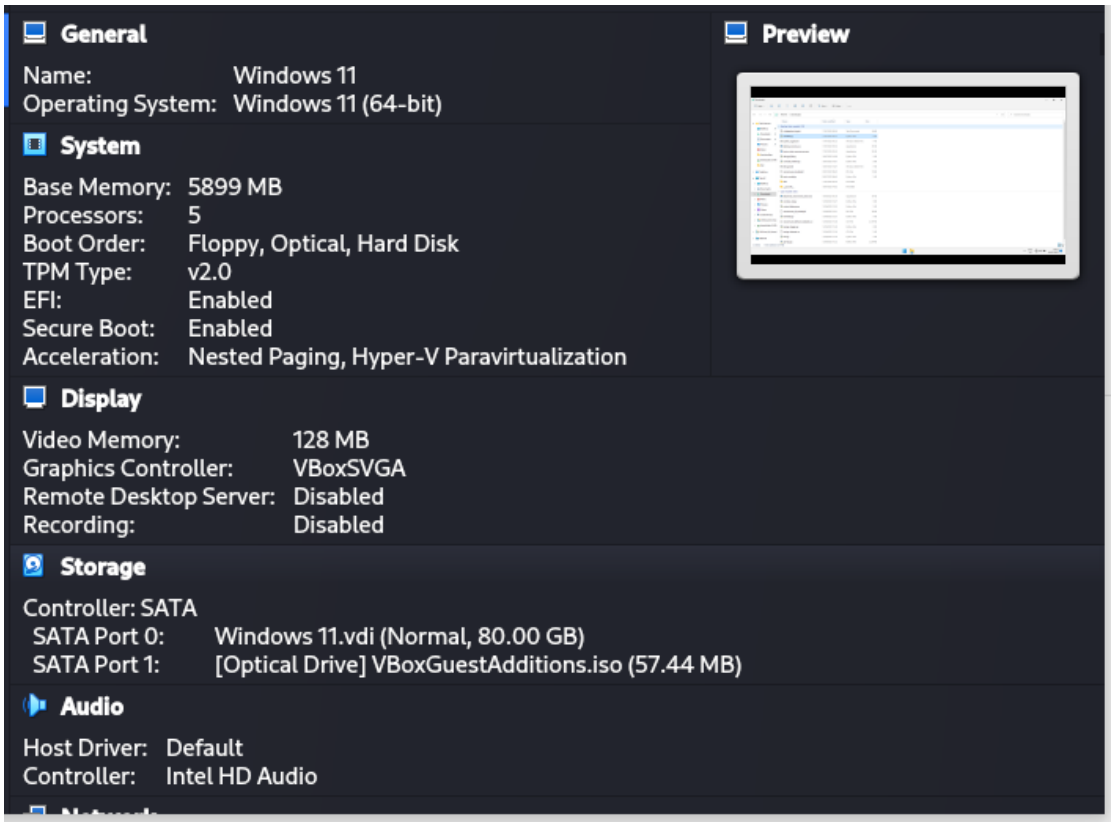

Figure 4: VirtualBox Configuration

Step 2: Since we are handling the ransomware here, its important to disable the internet connection to prevent the leaking of malicious code from our isolated environment.

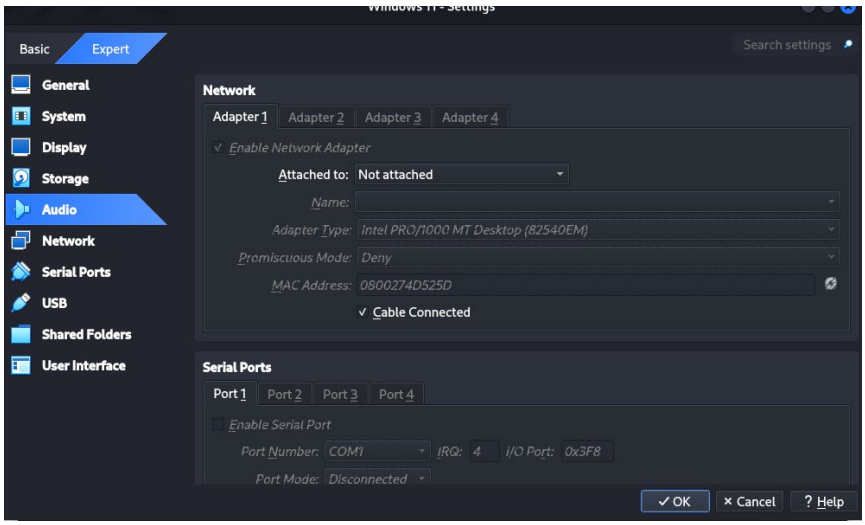

Figure 5: disabling the internet connection

Step 3: Transfer the project source code to the virtual environment using external usb.

Step 4: Make do the basic installations of the tools and allow VS code through firewall since we are **tracking network activities** while detecting the ransomware

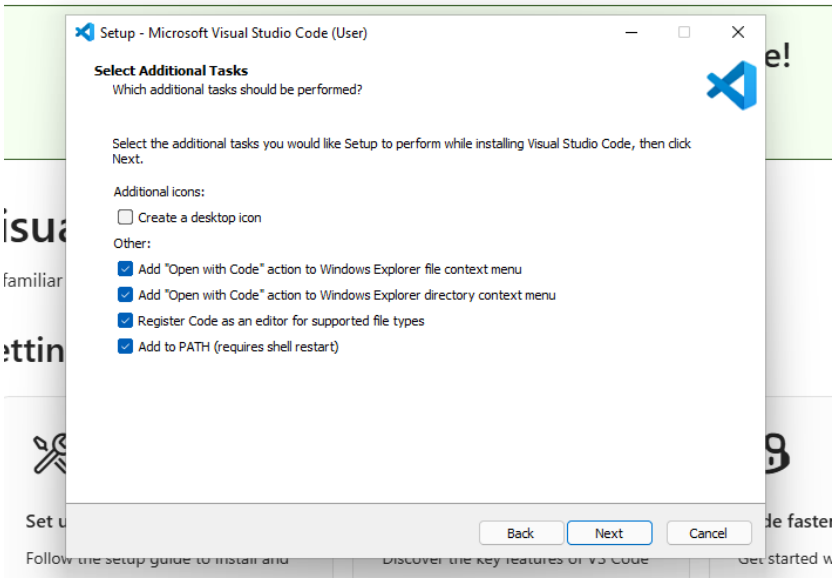

Figure 6: VS code installation Config

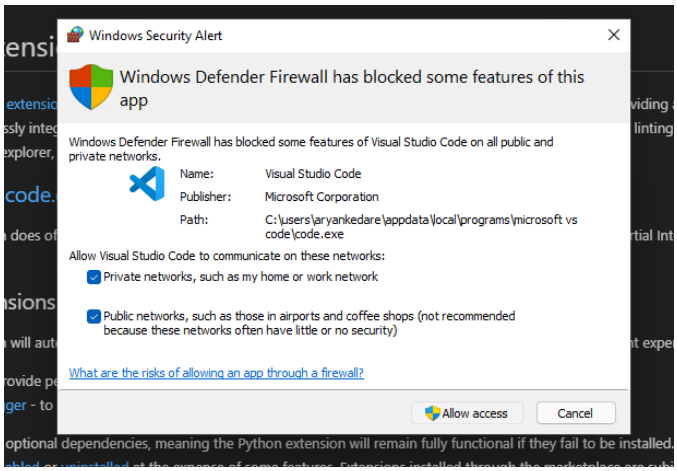

Figure 7: Allowing VS code through firewall

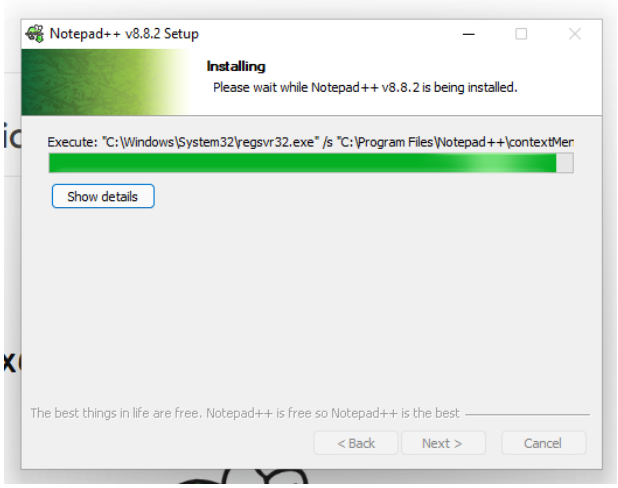

Figure 8: Notepad++ installation

Step 4: Once all the installations are done, create a place any document in C:\SensitiveData\important.pdf to make sure our hash concel feature works.

Step 5: Run monitor.py script as **administrator** and start executing the deactivated strains downloaded from malwarebazar.

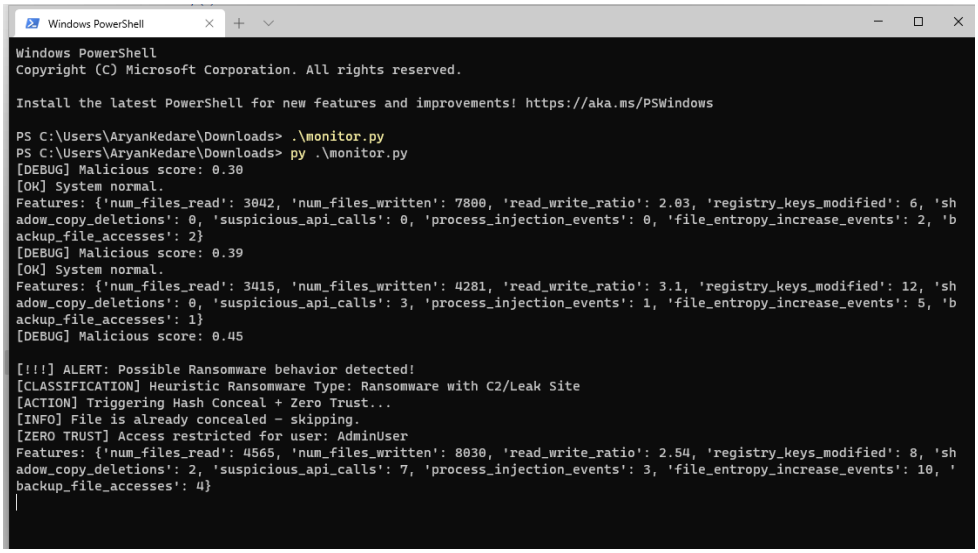

Figure 9: monitor.py in action

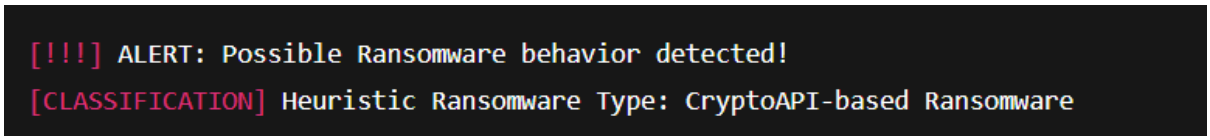

Figure 10: ransomware alert

Step 6: Checking the logs regarding what type of ransomware was used, when did it happen.

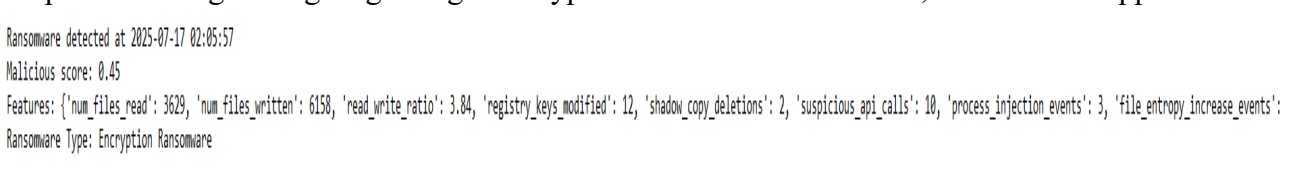

Figure 11: Monitor.py logs

The logs can be filtered by TimeStamp, Ransomware Type and file actions.

Step 6: Since our important file was encrypted, its important to get back of file once the ransomware attack is over, to decrypt the file run python decrypt_file.py

Figure 12: file encrypted to base64 to prevent from ransomware

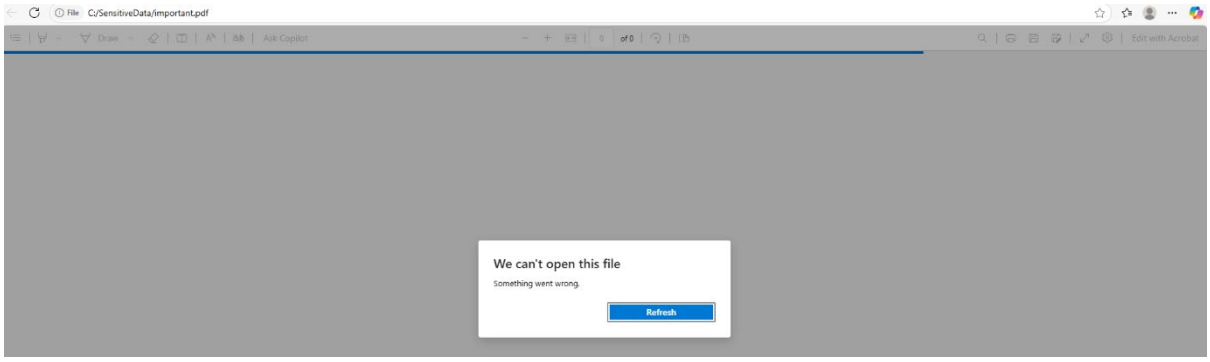

Figure 13: file oprning error

Figure 14: Decrypting the file

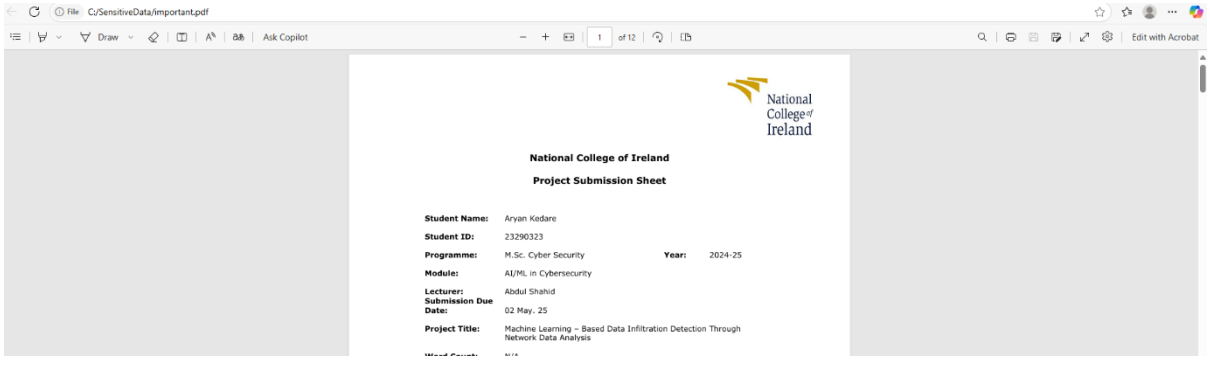

Figure 15: File opening

- Optional Customizations

Feature	How to Modify
Detection Threshold	Edit THRESHOLD = 0.4 in monitor.py
Sensitive File Path	Update path in hash_conceal() call
Decryption Target	Modify path in decrypt_file.py