National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Project

User Guide for Password Extractor Tool

Submitted by: Muazam Ali | Mustansir Hussain,
Abdul Muhaiman | Eman Fatima
Roll number: 22I-1734 | 22I-1764 | 22I-1694 | 22I-1675
Date: 17/11/2024

Table of Contents

• Introduction

The **Password Extractor** is a tool designed for Windows users who need to extract and analyze saved credentials from Google Chrome and Microsoft Edge or search for sensitive information within temporary files. It also extract account info and extract SAM file. This application requires administrative privileges and supports exporting results in CSV format.

• Installation and Setup

1. **Ensure Requirements are Met**:

   - The tool is Windows-only, so make sure you're on a Windows OS.
   - Google Chrome and Microsoft Edge should be installed on the system.
   - Run the program as an administrator to access all necessary resources.
   - Any IDE installed on the system to run program Application.

2. **Install Required Libraries**:

   - Open a Command Prompt or Terminal and install the necessary libraries with the following commands:

     - pip install pycryptodome # For AES decryption
     - pip install pypiwin32 # For Windows encryption
     - pip install pycryptodomex # For cryptography functions

3. **Download or Clone the Project Files**:

   - If you have a ZIP file, extract it to a folder on your Desktop or another directory.
   - Ensure that all Python files are in the same directory for the program to run successfully.

• Running the Application

1. **Run as Administrator**:

    - Right-click the main program files (usually DF_Project.py) and select **Run as Administrator**. This allows the application to access restricted system files and decrypt passwords from browser databases.

2. **Launch the Program**:

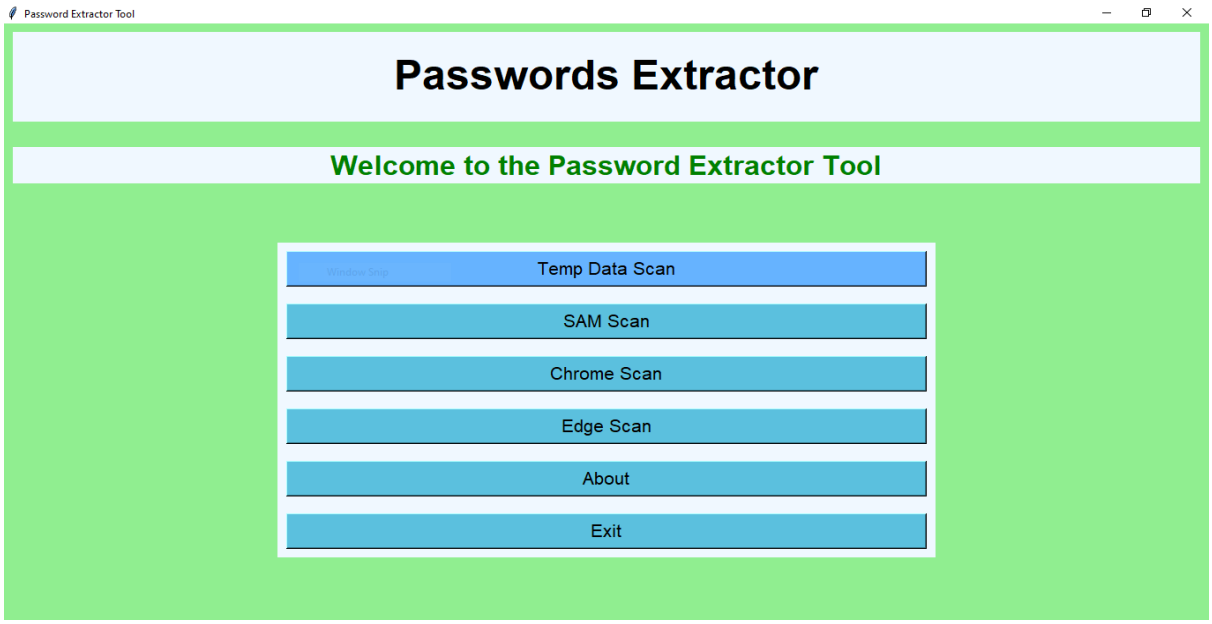
    - **Python3 DF_Project.py**
    - The application will open with a Graphical User Interface (GUI) created using **tkinter**. The main page provides buttons for each feature and options to navigate through the functionalities.

• Navigating the Application

1. Main Page

The main page serves as the central control hub. From here, you can access the core functionalities of the tool:

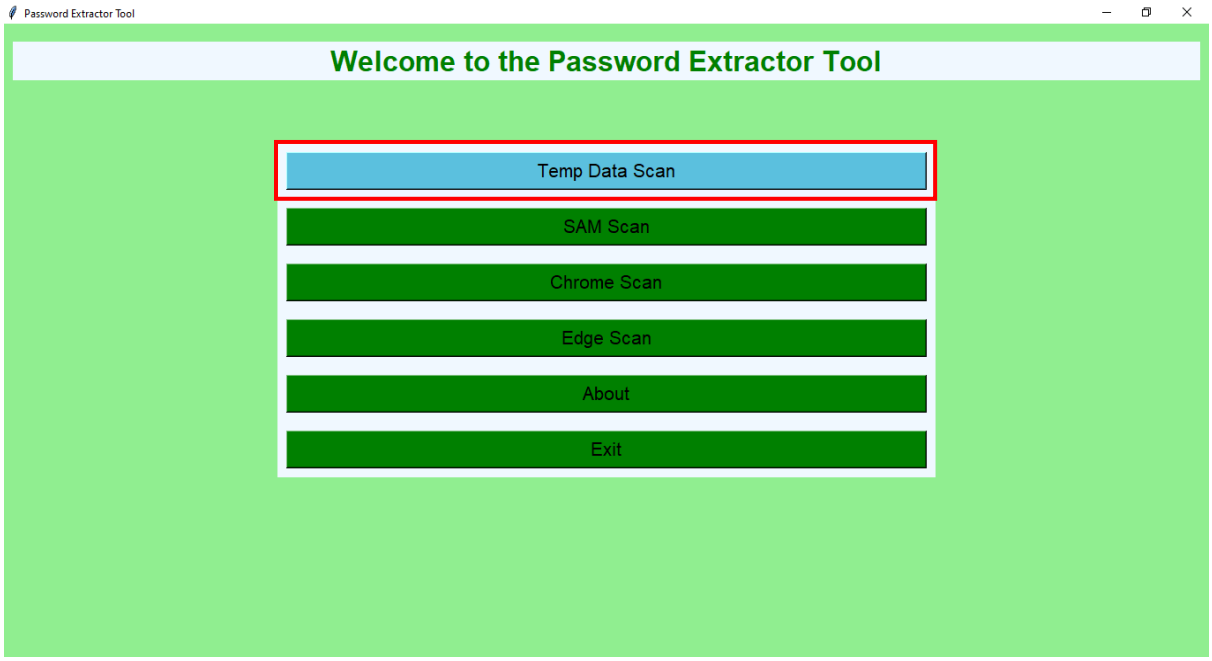
- **Temp Data Scan**: Scans temporary folders for specific keywords related to sensitive data.
- **SAM Scan**: Scans system and extract SAM file and show Account info.
- **Chrome Scan**: Extracts saved passwords from the Google Chrome browser.
- **Edge Scan**: Extracts saved passwords from the Microsoft Edge browser.
- **About**: Displays program details, purpose, version, and developer information.
- **Exit**: Closes the application.

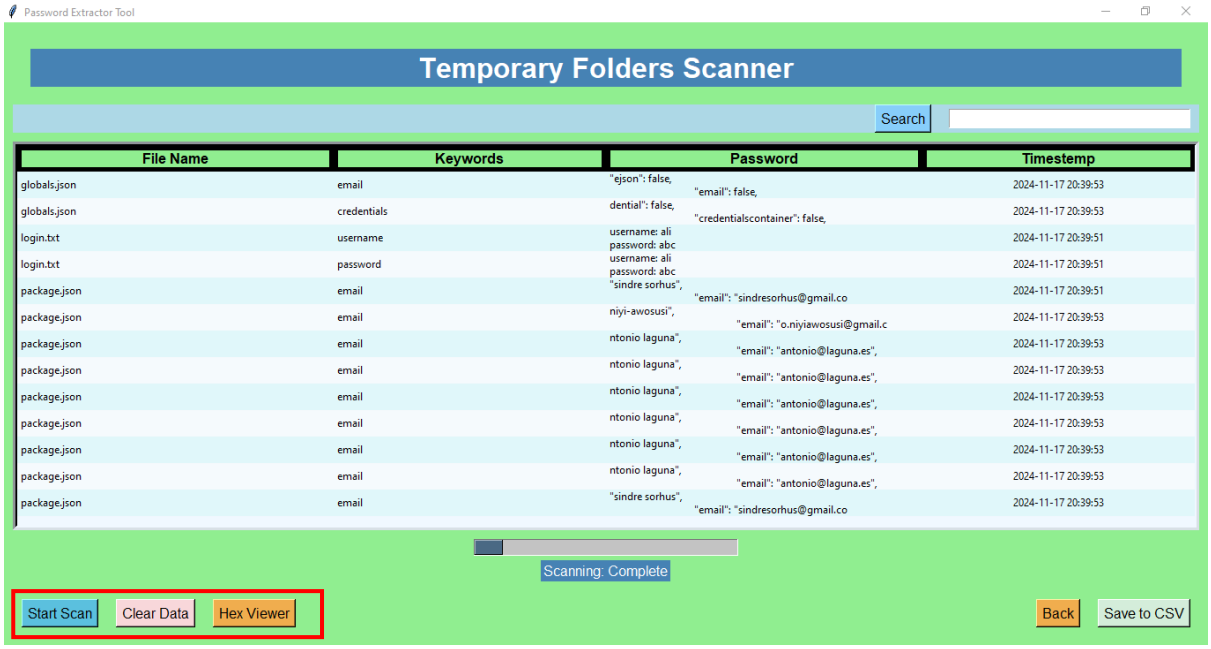


2. Temp Data Scan

1. **Select "Temp Data Scan"**:
    - This feature scans system folders (e.g., Desktop, Downloads, Documents) and temporary files (e.g., Sticky Notes, Notepad) for sensitive keywords such as "username," "email," "password," or "credential."

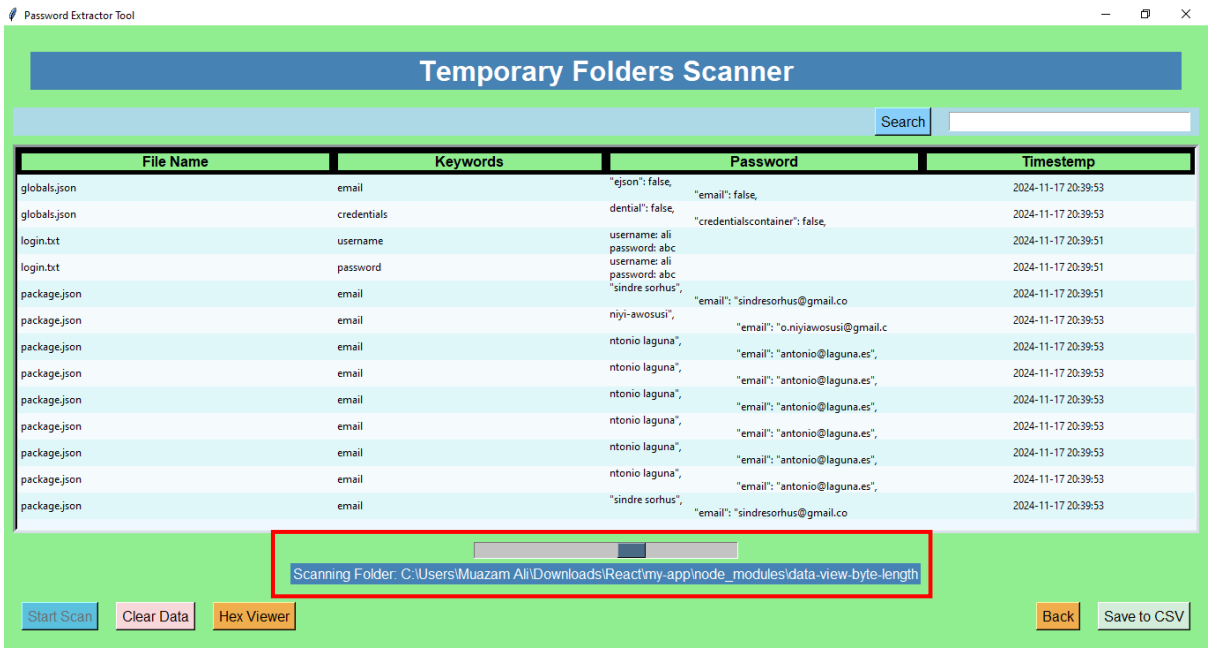
- Click **start scan** button





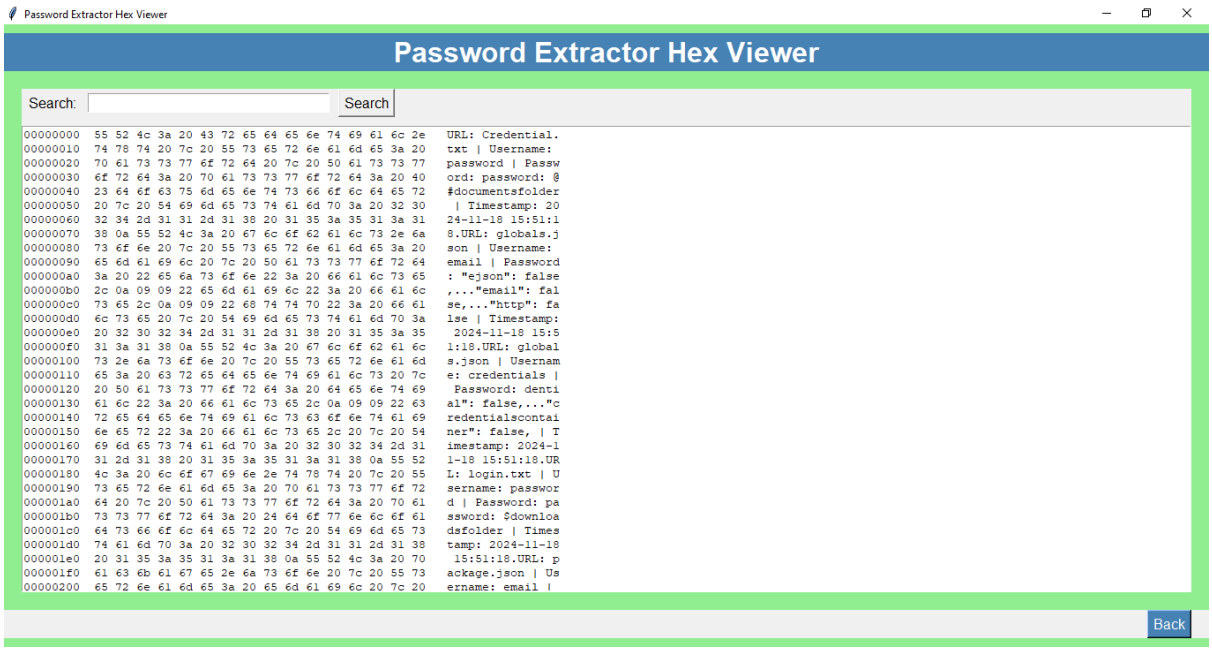
2. **Review Results**:

- If any matching files or content is found, the file path and content snippet are displayed. This enables easy identification of files containing sensitive information.

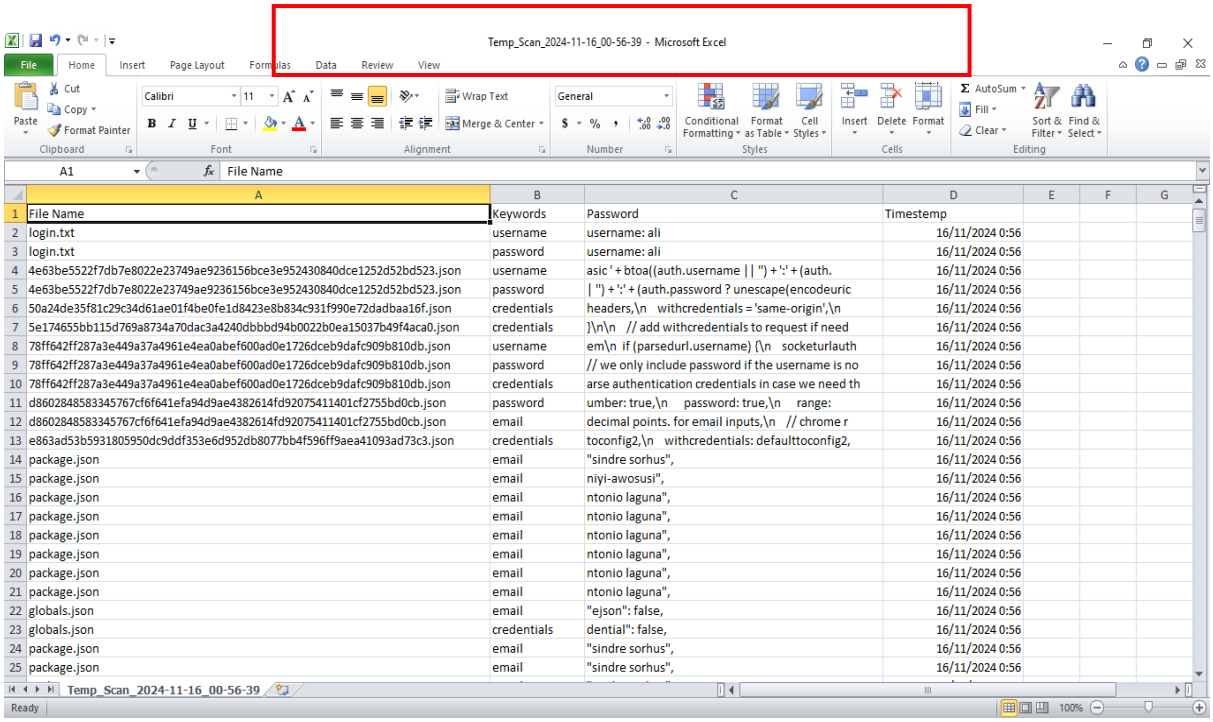


3. **Hex Viewer:**

- Hex viewer displays all the output in the hex form with search box functionality.

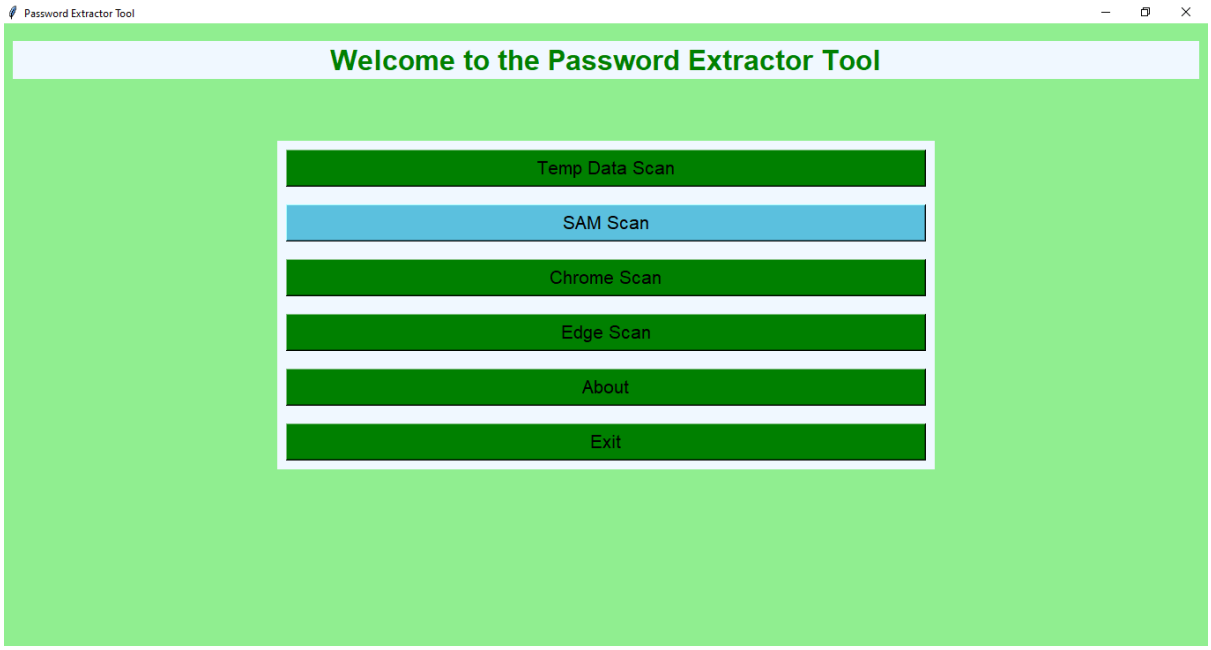


4. **Save Results (Optional)**:
   - Results can be saved to a CSV file on the Desktop. This CSV file includes details such as file paths and matching content for later review.

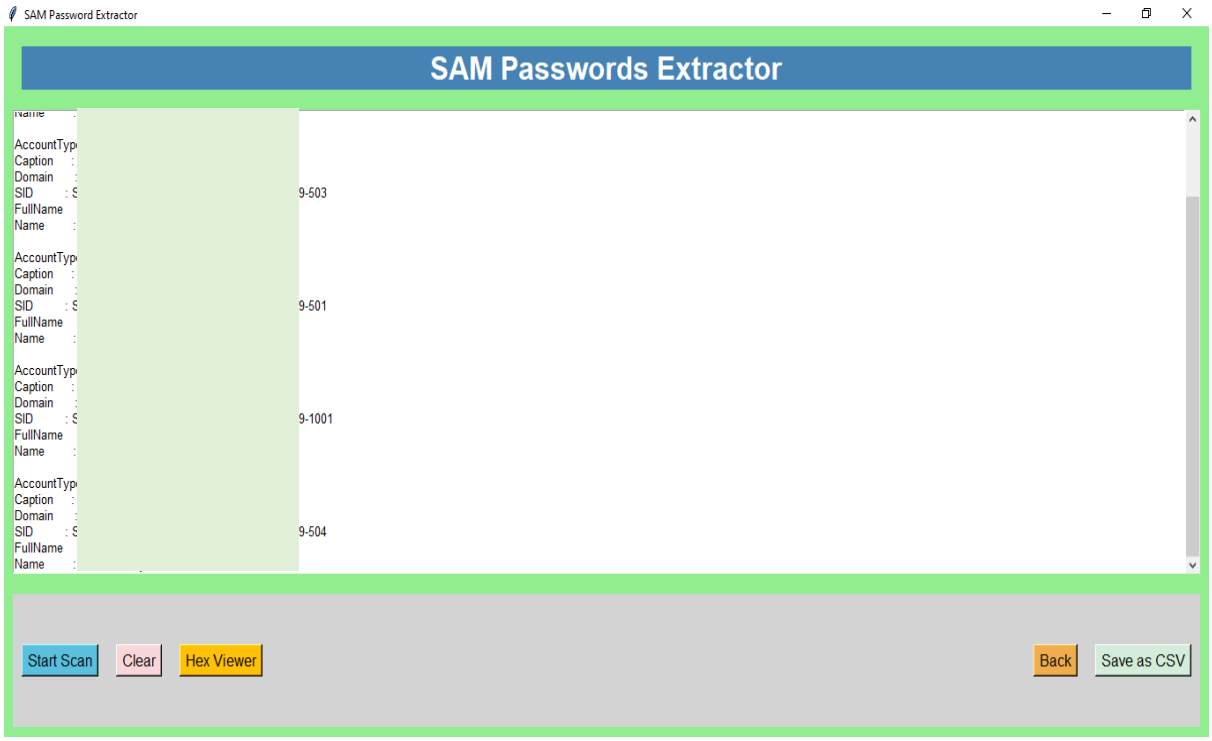


3. SAM Scan

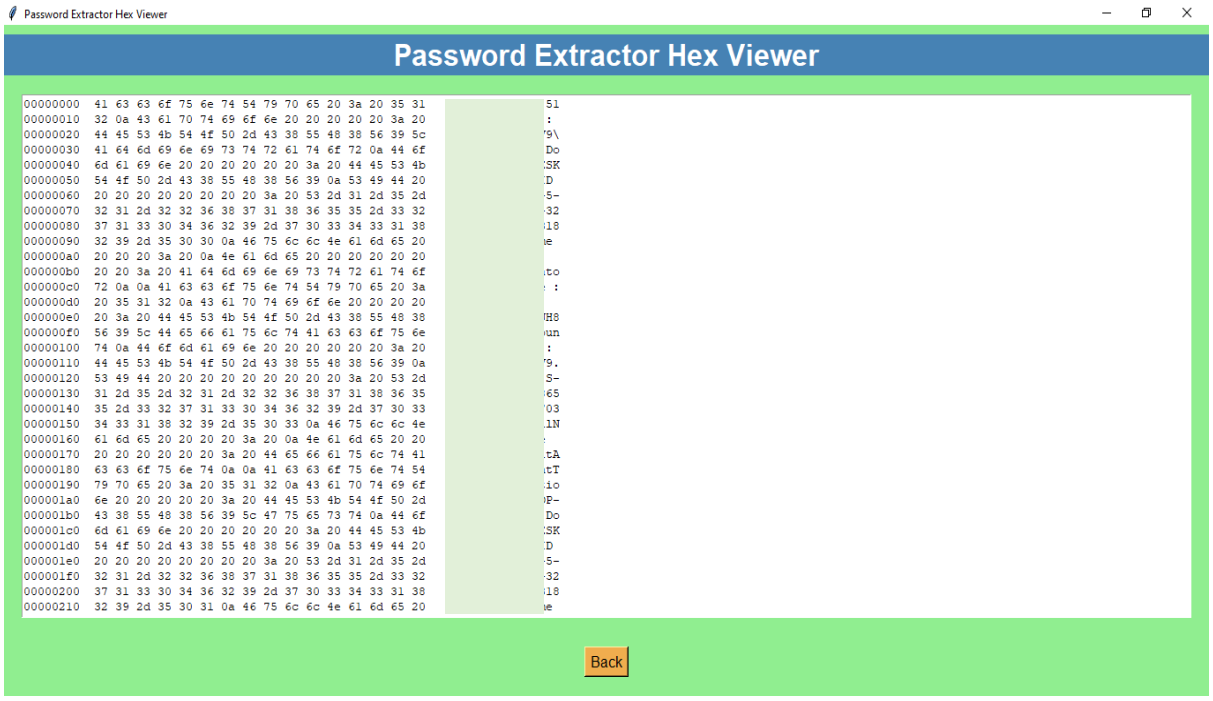
1. Select SAM Scan



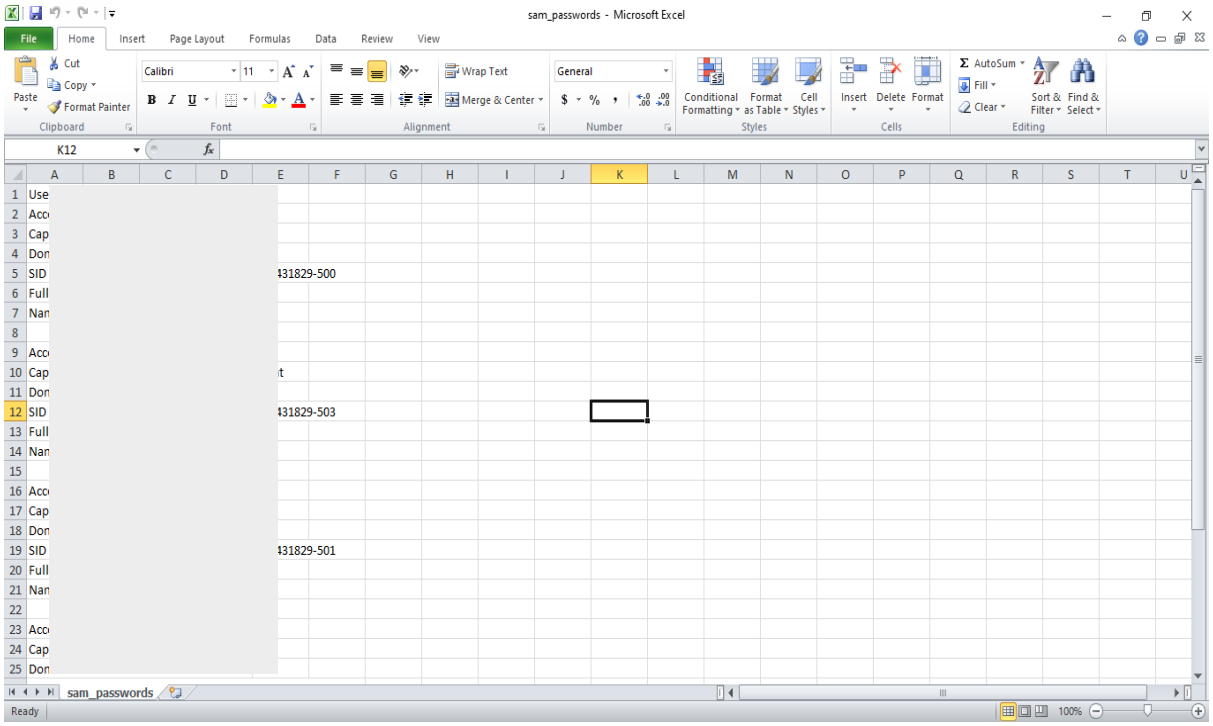
2. Account info



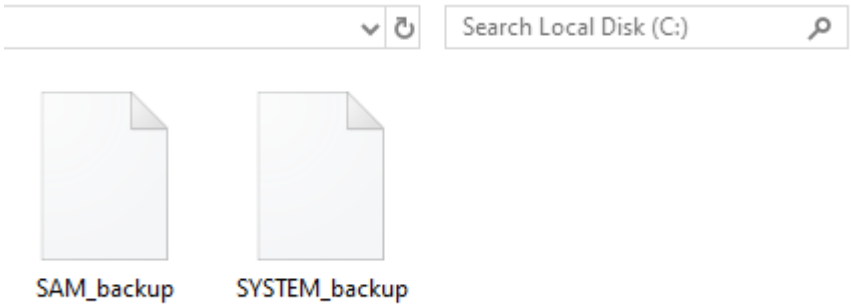
3. Hex Viewer



4. Review Results

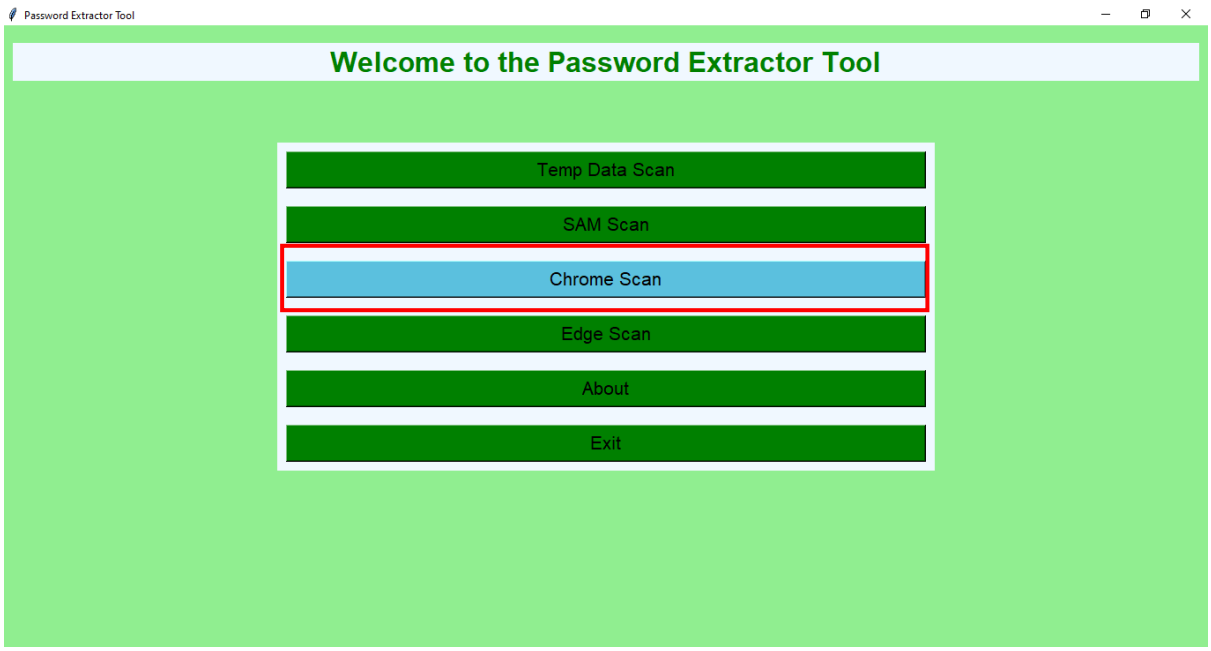


5. **Extracted SAM File**

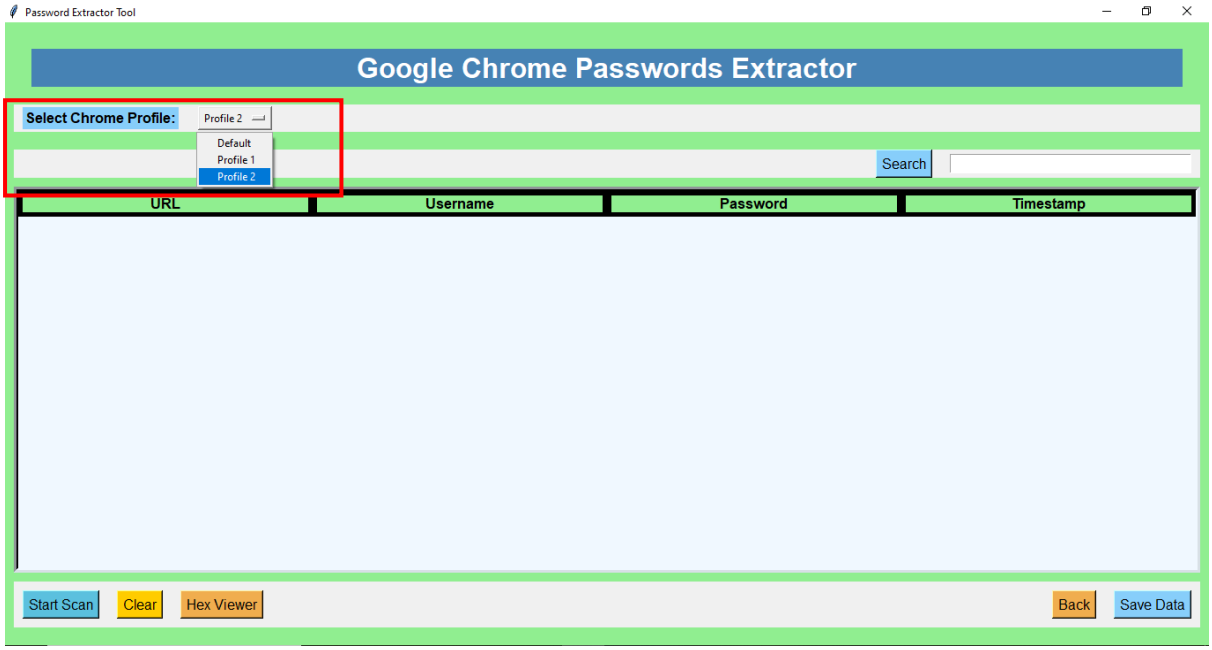


4. Chrome Scan

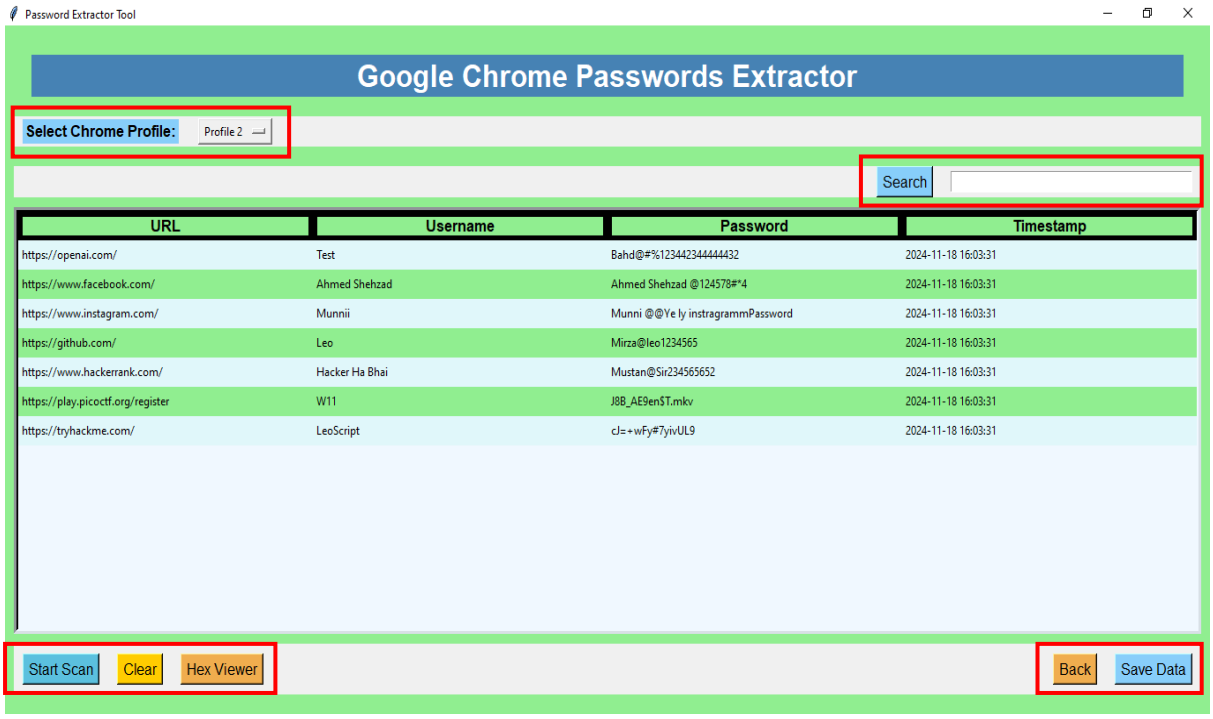
1. **Select "Chrome Scan"**:
    - This feature locates and decrypts saved passwords from Google Chrome's SQLite database file, Login Data.



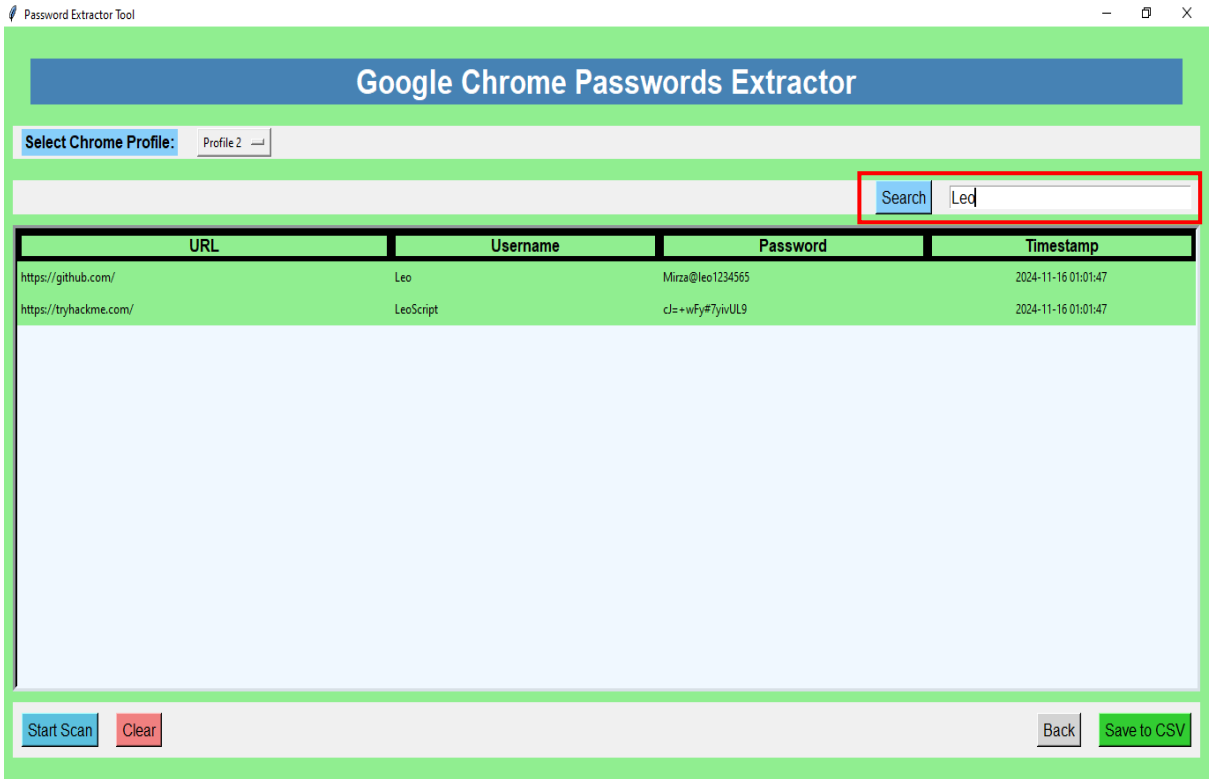
- **Profile Selection:**



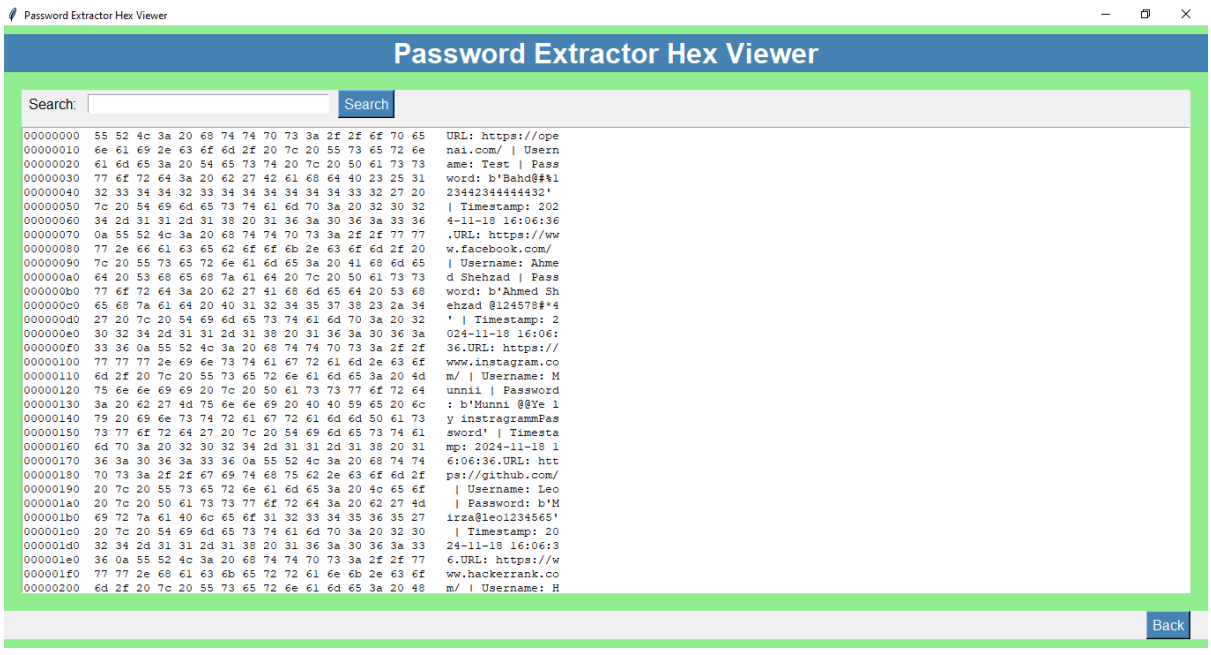
2. **Password Extraction**:
    - The application uses AES decryption and win32crypt to decrypt saved passwords and displays them in a readable format (username, URL, password).



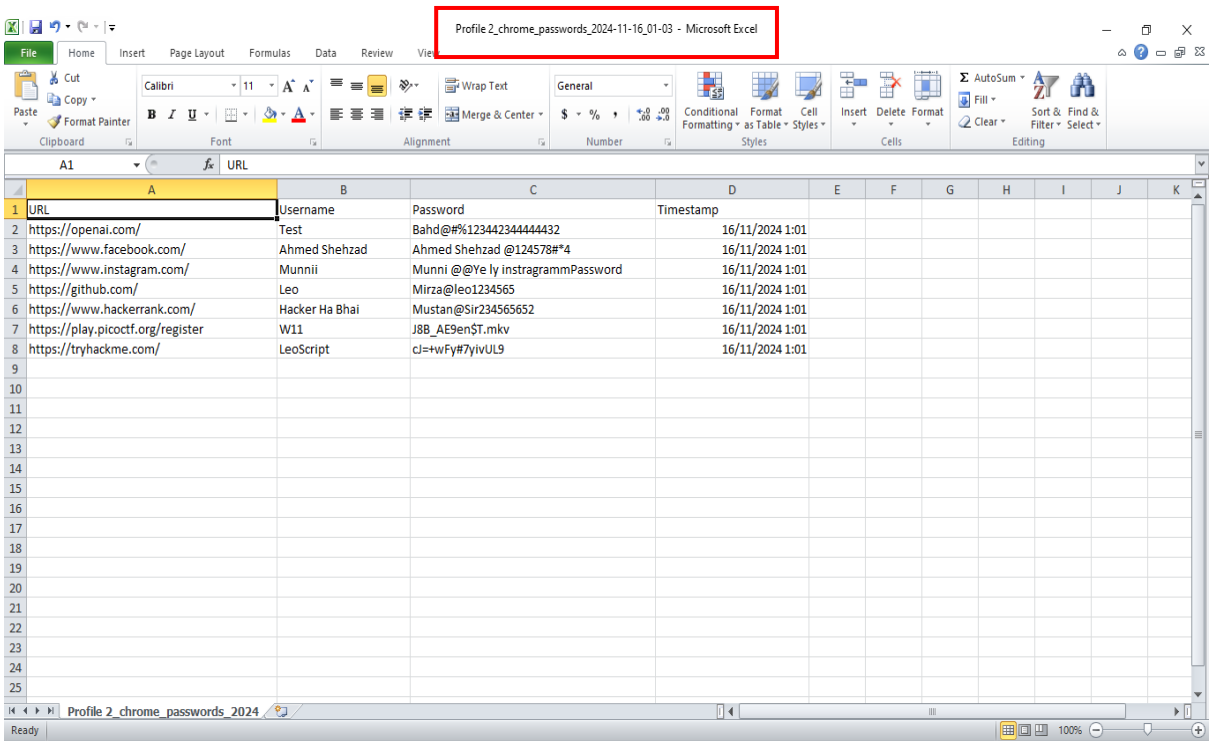
- **Search String:**



- **Hex Viewer:**



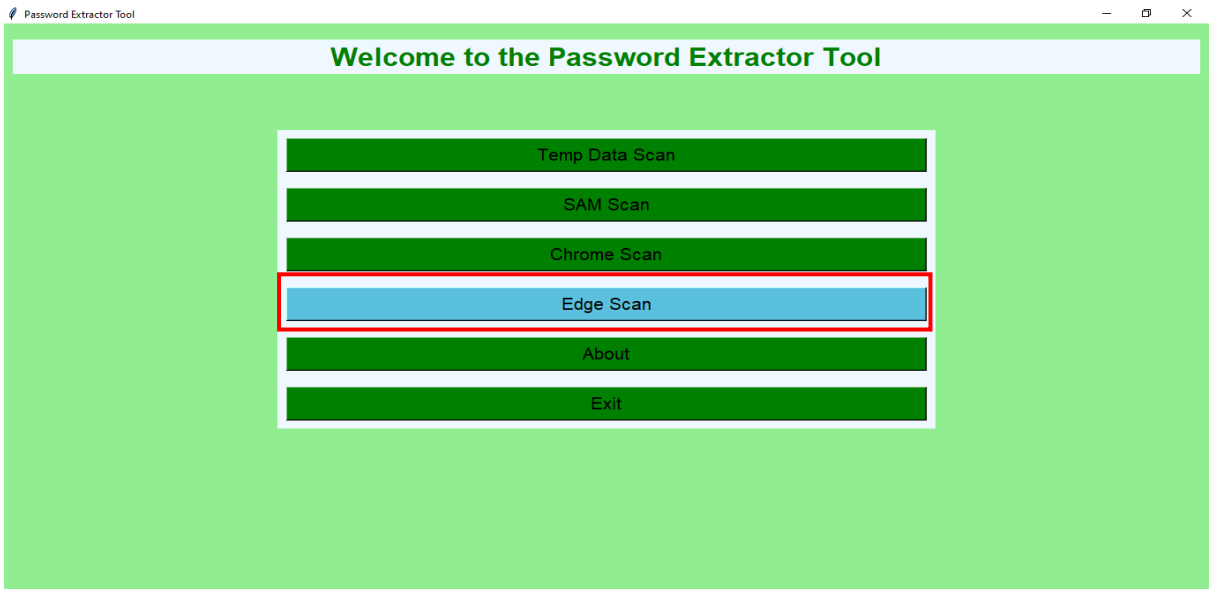
3. **Review Results**:
   - Extracted passwords are displayed in the interface and can be exported to a CSV file for analysis.



URL	Username	Password	Timestamp
https://openai.com/	Test	Bahd@#%123442344444432	16/11/2024 1:01
https://www.facebook.com/	Ahmed Shehzad	Ahmed Shehzad @124578#*4	16/11/2024 1:01
https://www.instagram.com/	Munnii	Munni @@Ye ly instragrammPassword	16/11/2024 1:01
https://github.com/	Leo	Mirza@leo1234565	16/11/2024 1:01
https://www.hackerrank.com/	Hacker Ha Bhai	Mustan@Sir234565652	16/11/2024 1:01
https://play.picoctf.org/register	W11	J8B_AE9en$T.mkv	16/11/2024 1:01
https://tryhackme.com/	LeoScript	cJ=+wFy#7yivUL9	16/11/2024 1:01

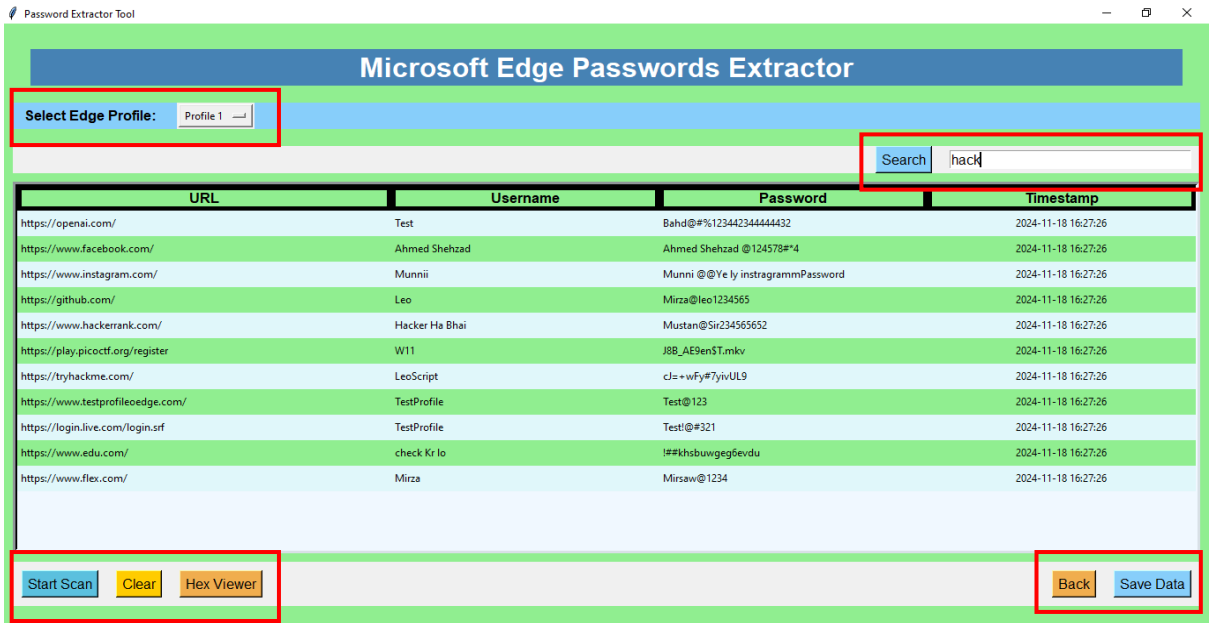
5. Edge Scan

1. **Select "Edge Scan"**:
    - Similar to the Chrome Scan, this feature decrypts saved passwords from Microsoft Edge's database file.

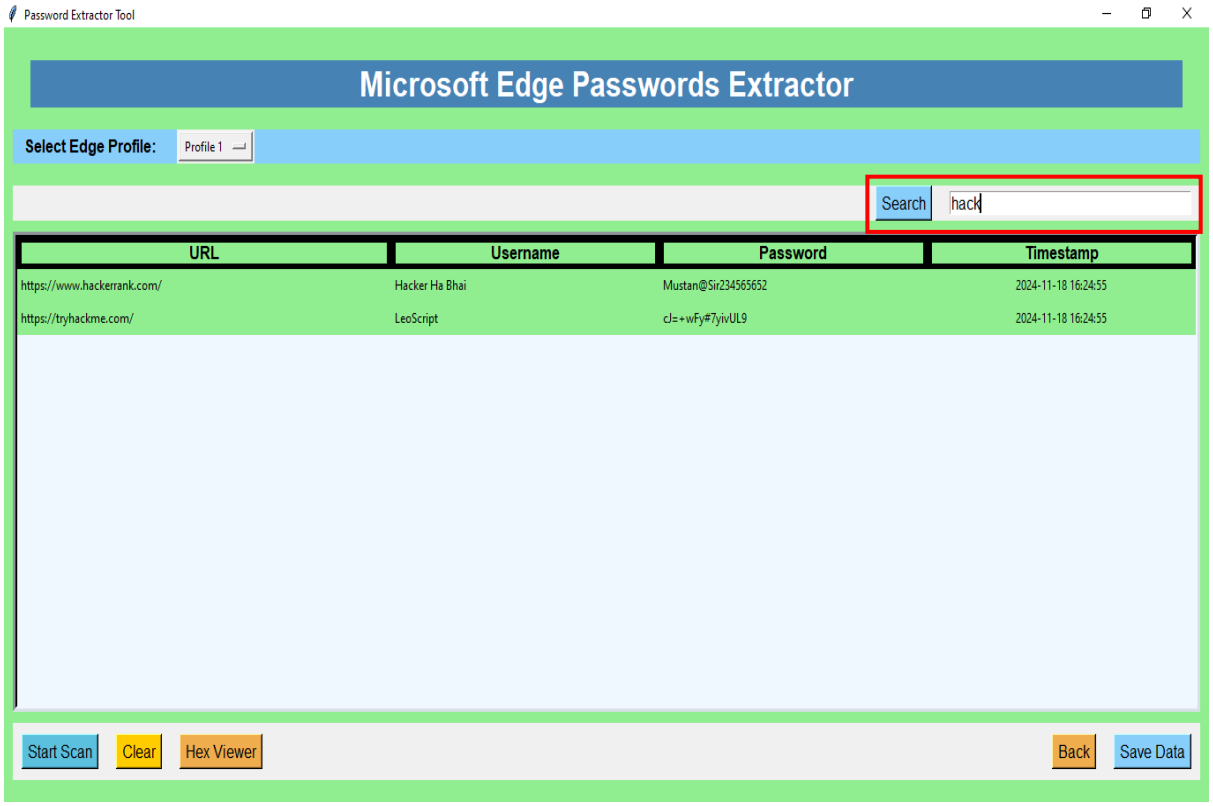


2. **Password Extraction**:

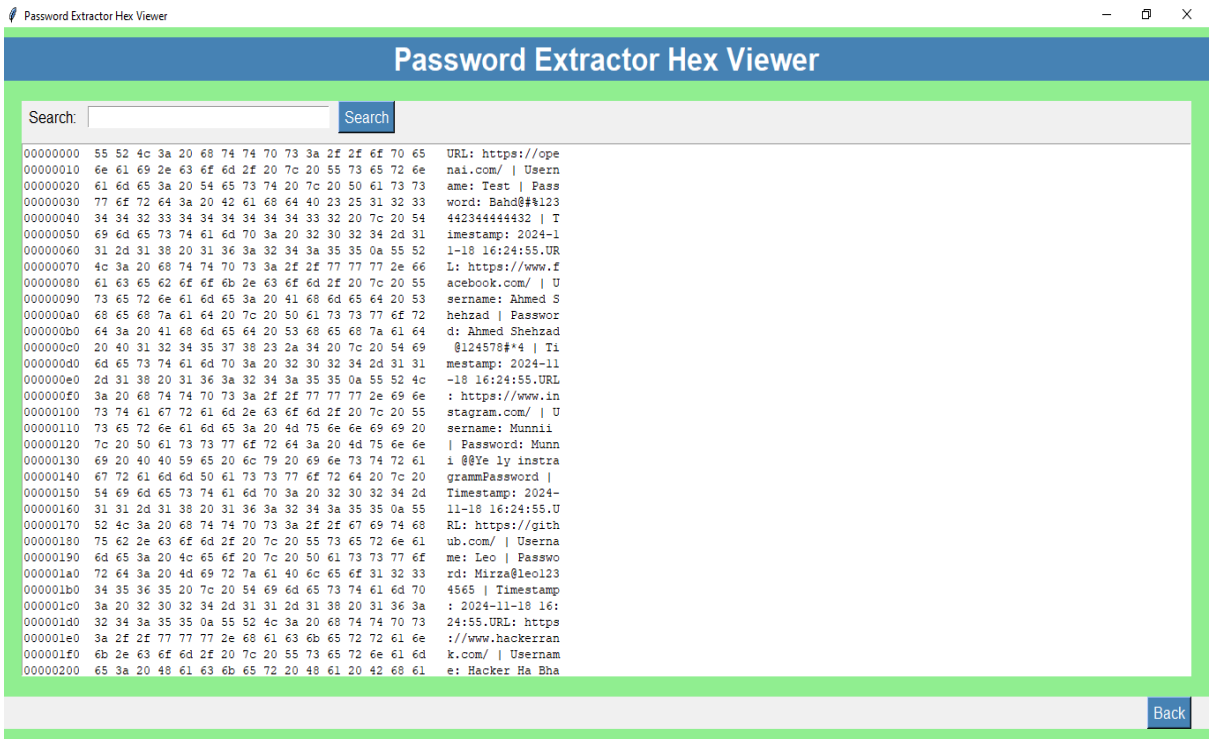
- The tool accesses Edge's SQLite database, decrypts saved credentials, and displays the data.



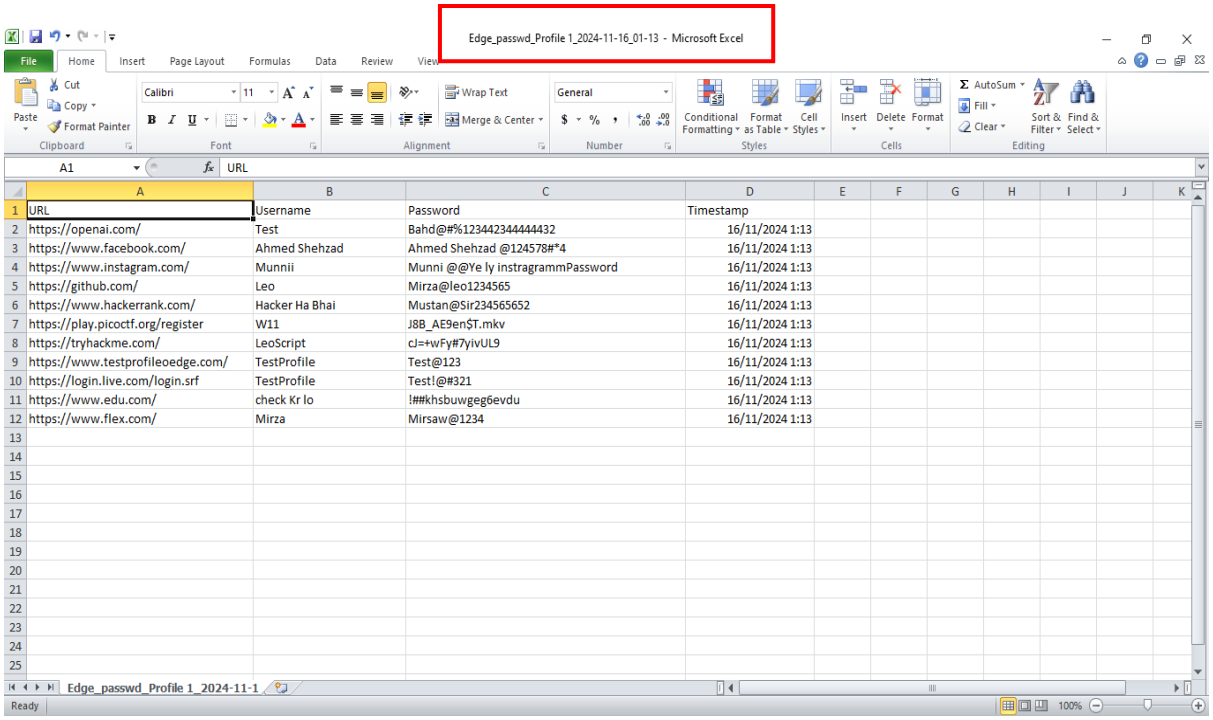
- **Search Bar:**



- **Hex Viewer**

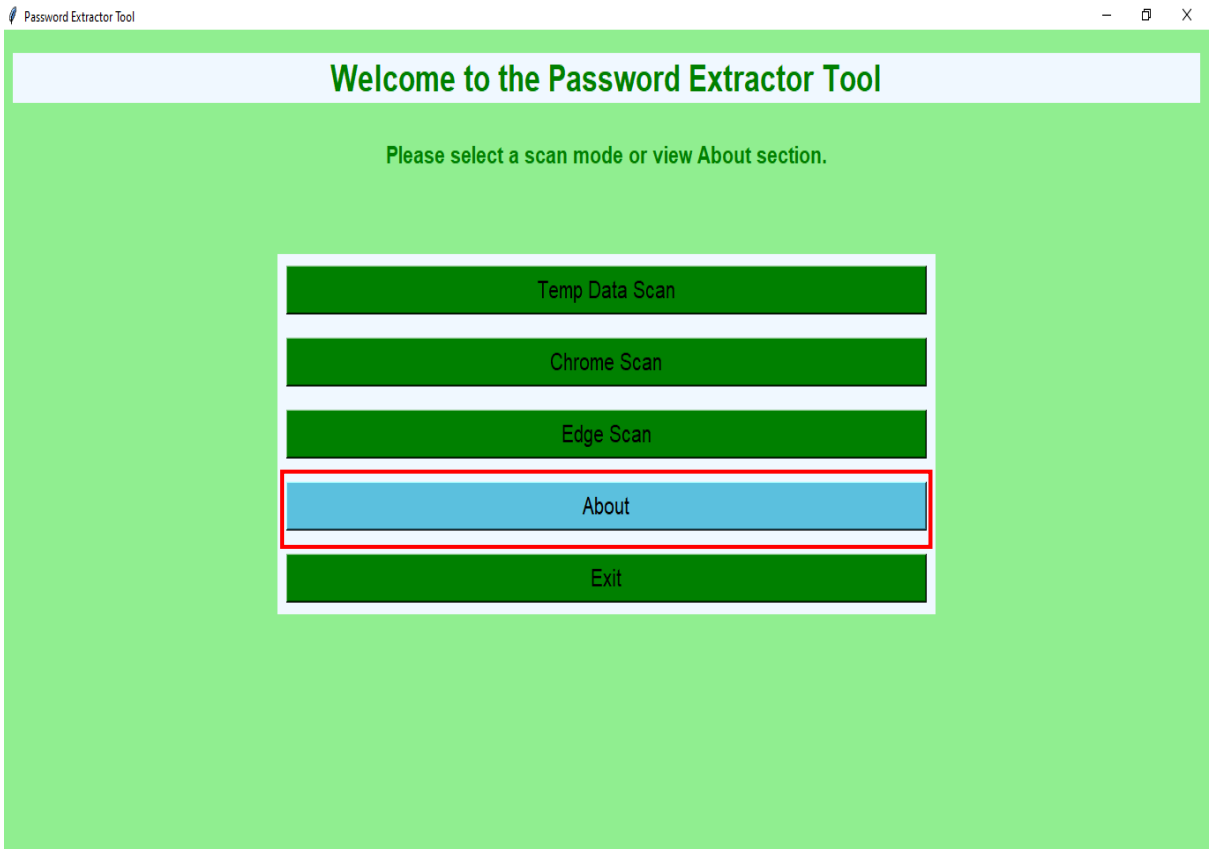


3. **Review Results**:
    - Like Chrome, the extracted passwords are displayed within the interface, with an option to save them to a CSV file for further review.

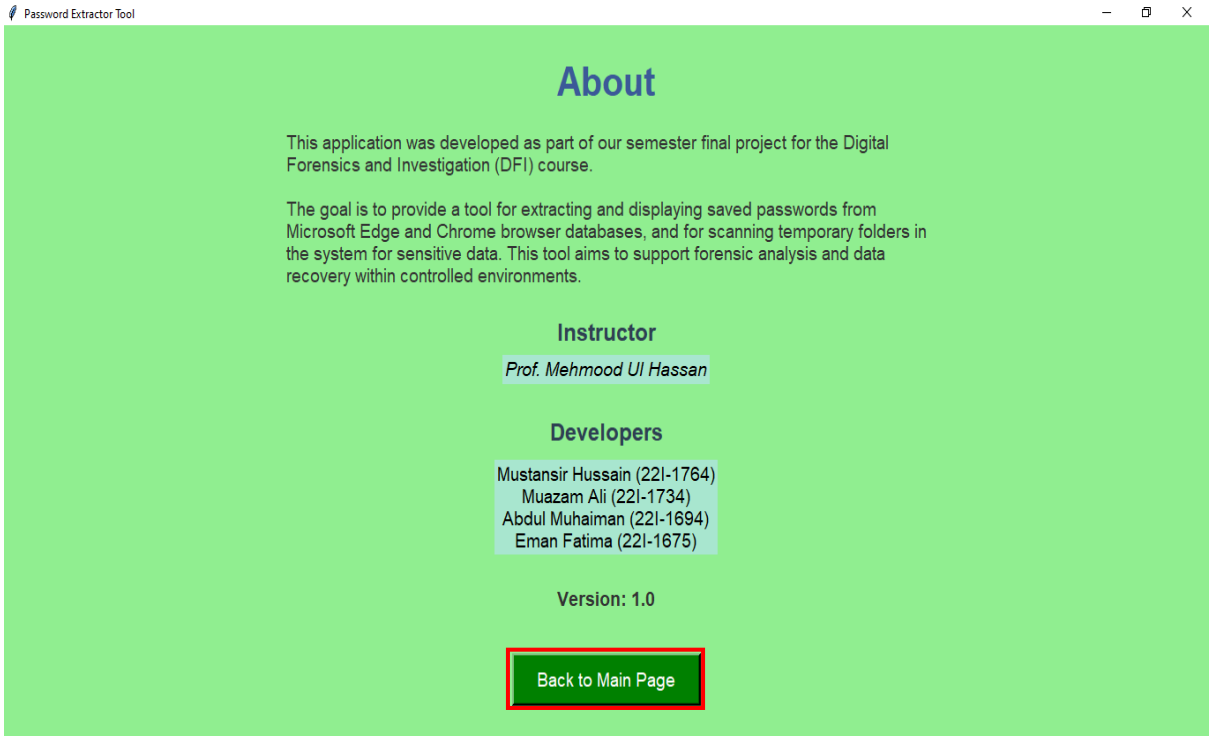


6. About

1. **Select "About"**:
    - The About page provides details about the tool, including:
        - Purpose of the tool
        - Developer names and contact information
        - Version of the tool

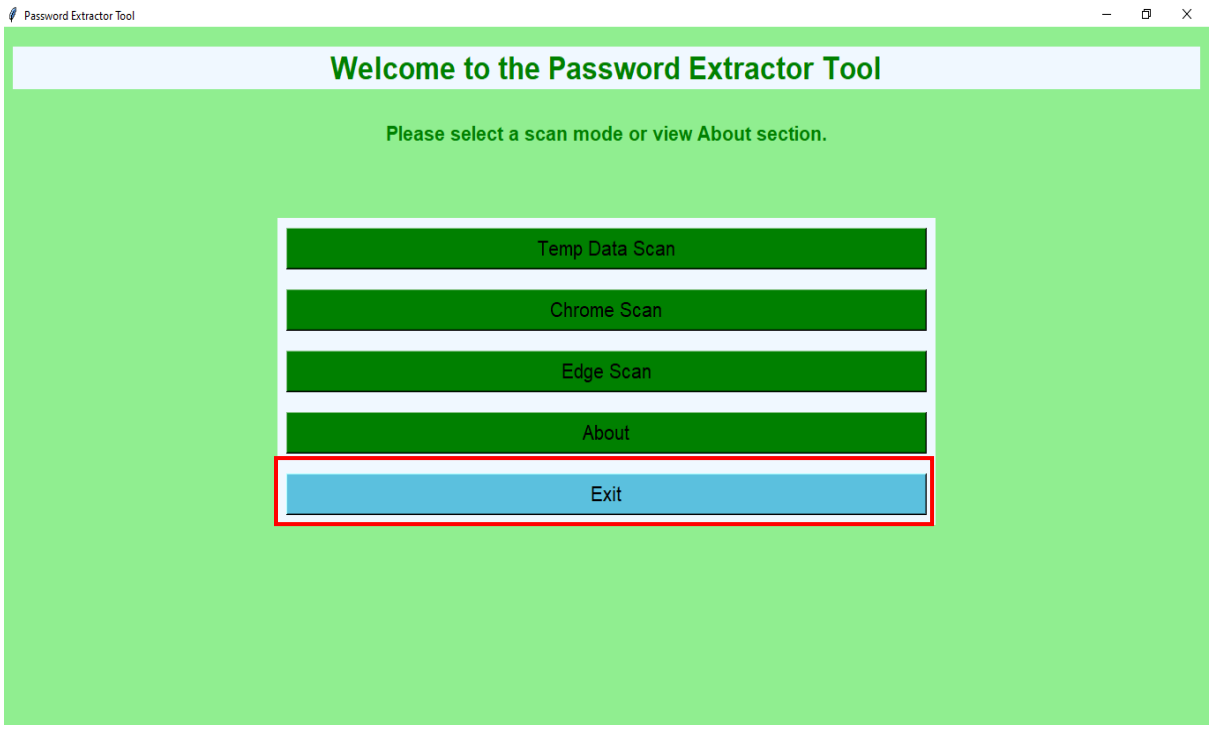


2. **Return to Main Page**:
    - Click the button to go back to the main menu after viewing the information.



7. Exit

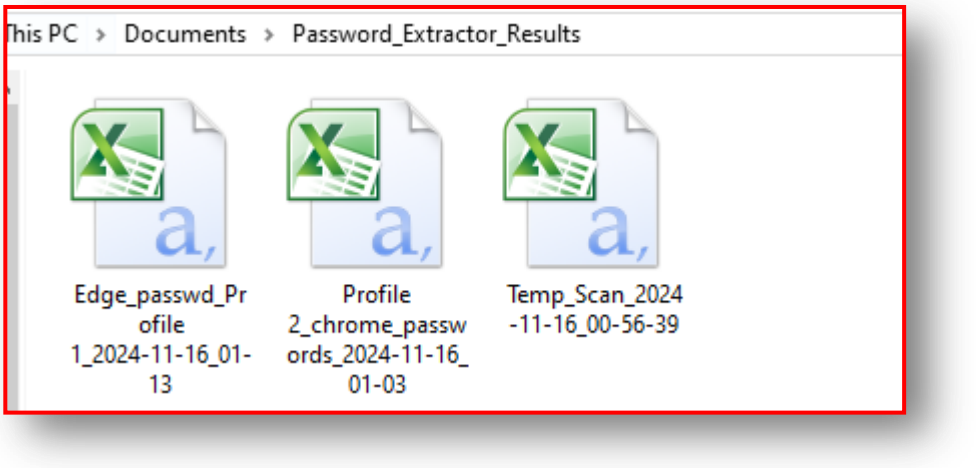
1. **Select "Exit"**:
    - This closes the application. Be sure to save any necessary data before exiting.



• Saving Results

1. **Saving as CSV**:

    - For each functionality (Temp Data Scan, Chrome Scan, Edge Scan), you have the option to save the results to a CSV file on your **Documents Folder** by default.
    - The CSV file includes:
        - **For Chrome and Edge**: URLs, usernames, and decrypted passwords.
        - **For Temp Data Scan**: File paths, keywords found, and relevant content snippets.



2. **Location**:

    - By default, saved CSV files are stored in the **Documents\Password_Extractor_Results** for easy access.

- Troubleshooting

Common Issues

1. **Permission Errors**:
    - Ensure the program is run as an administrator. Right-click on DF_Project.py and select **Run as Administrator**.
2. **Missing Libraries**:
    - Verify that required libraries are installed by running:
        - **pip install pycryptodome pypiwin32 pycryptodomex**
3. **Chrome or Edge Not Installed**:
    - Install both browsers on your system to fully use the Chrome and Edge scanning functionalities.
4. **CSV File Not Saving**:
    - Confirm that your Documents folder is accessible, and you have write permissions. The program attempts to save results on the Desktop by default.
5. **SAM File Hash Extraction**
    - The Security Account Manager (SAM) file is a sensitive Windows file that stores hashed passwords for user accounts. Extracting SAM file hashes can be challenging due to system protections and antivirus interference.
6. **Antivirus Interference**:
    - **Problem**: Antivirus software detects hash extraction tools as malicious and blocks them.
    - **Solution**:
        - Temporarily disable the antivirus or add the tool to the antivirus exception list.
        - Use trusted tools (e.g., *Mimikatz* or *Impacket*) to avoid unnecessary detection.
7. **File Access Restrictions**:

- **Problem**: SAM file is locked by the operating system and cannot be directly accessed.
- **Solution**:
  - Boot into an alternate OS (e.g., Linux live USB) and mount the drive to access the SAM file.
  - Use tools like *Offline NT Password & Registry Editor* or *Windows PE* to bypass access restrictions.

8. **System Protections (e.g., UAC)**:
   - **Problem**: User Account Control (UAC) and other mechanisms block unauthorized access.
   - **Solution**:
     - Run the program as an administrator.
     - Exploit Volume Shadow Copy Service (VSS) to access SAM file
9. **Library Import Issue**
   - Sometimes libraries in Python or other programming environments can cause errors during import. These issues often stem from missing dependencies, incorrect versions, or environment conflicts.

This user guide should help you navigate and use the **Password Extractor tool** effectively. Make sure to run the application responsibly, as it extracts sensitive information that should be handled securely.