Forensics Information Extractor – User Guide

Introduction

The Forensic System Extractor is a comprehensive tool for both live and static forensic data acquisition from Windows systems. The application provides two modes of operation: **Live System Acquisition** and **Static Acquisition**. Users can choose the mode they wish to explore at the start of the application.

Steps to Use the Application

1. Launch the Application

- Open the application. The main menu appears with the following options:

In case of the executable file run the application as Administration and in case of having scripts:

1. Launch cmd.exe as **admin** from the search bar.
2. Locate to the folder containing the script
3. Run the following command '*python main.py*' and....
    - **Live System Info**: Extract forensic information from the live system.
    - **Static System Info**: Extract forensic information from static files such as NTUSER.dat, SAM, and SYSTEM.

2. Choose the Mode

- **Live System Info**:
    - Click the **Live System Info** button to proceed.
    - Use the provided buttons to extract various types of live forensic data:
        - **System Info**: Fetch system configuration details.
        - **User Info**: Retrieve active user accounts and profile information.
        - **Hardware Info**: Extract details about hardware components like CPU, RAM, and disk drives.
        - **USB Devices**: List previously connected USB devices.
        - **Browser History**: Retrieve browsing history from supported browsers.
        - **Recent Files**: View a list of recently accessed files.

    - Extracted information is displayed in the scrollable output box.
- **Static System Info**:
    - Click the **Static System Info** button to proceed.
    - Options provided:
        - **NTUSER.dat File**: Extract data from the NTUSER.dat file to retrieve software installation information.
        - **SAM and SYSTEM Files**: Process the SAM and SYSTEM registry hives to retrieve user account information.
        - **User Account Info**: View details of extracted user accounts.
    - Extracted information is displayed in the scrollable output box.
    - Use the **Close** button on the static interface to terminate the static mode and return to the main menu.

Supported Features

Live System Acquisition

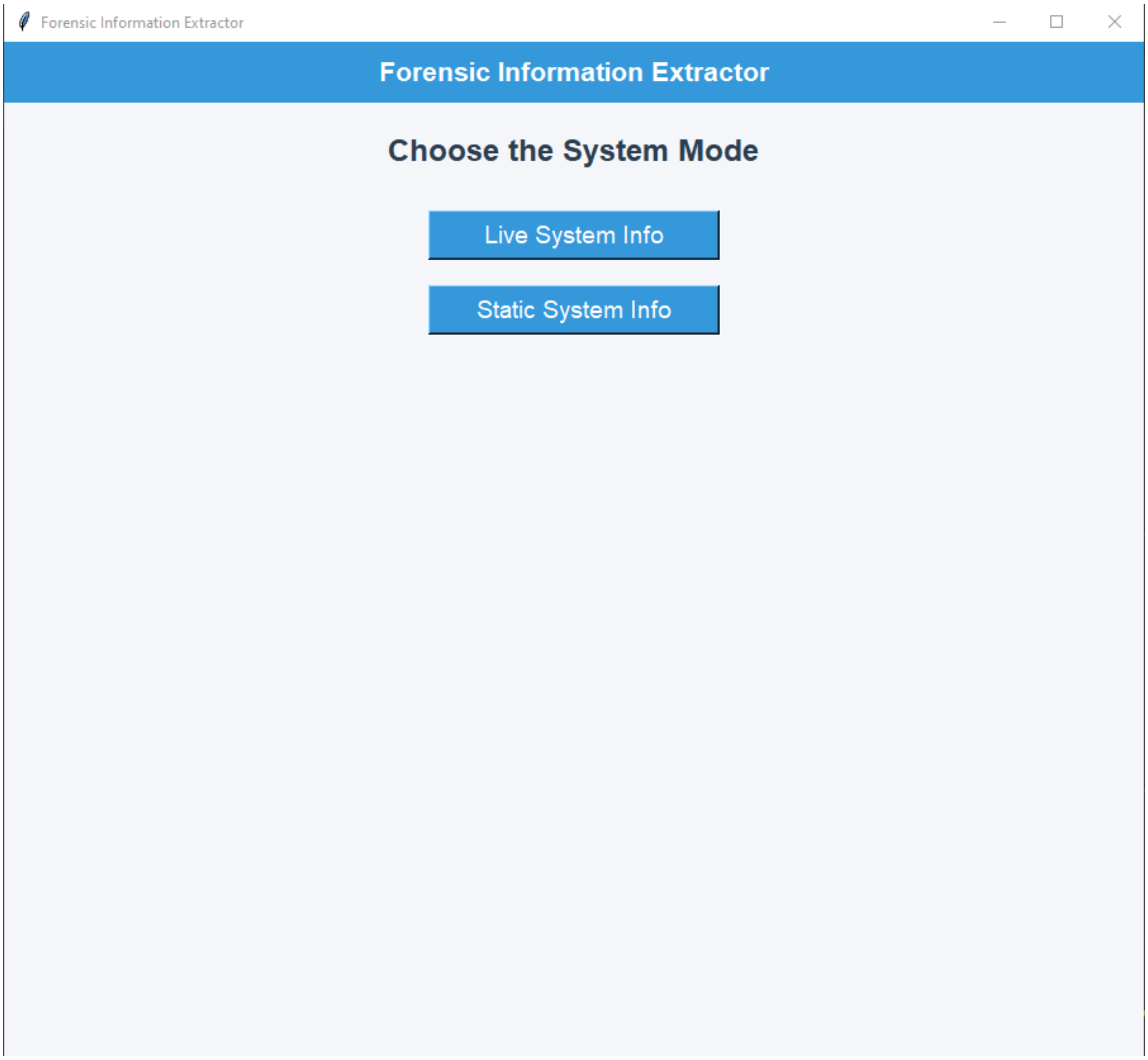
- **System Info**: Fetches operating system details, installation date, and BIOS information.
- **User Info**: Retrieves local user accounts and profile creation/access dates.
- **Hardware Info**: Extracts details about CPUs, RAM, and disk drives/partitions.
- **USB Devices**: Lists previously connected USB storage devices.
- **Browser History**: Retrieves browsing history from supported browsers:
    - Google Chrome
    - Mozilla Firefox
    - Microsoft Edge
    - Brave
    - Opera GX
- **Recent Files**: Displays a list of recently accessed files.

Static Acquisition

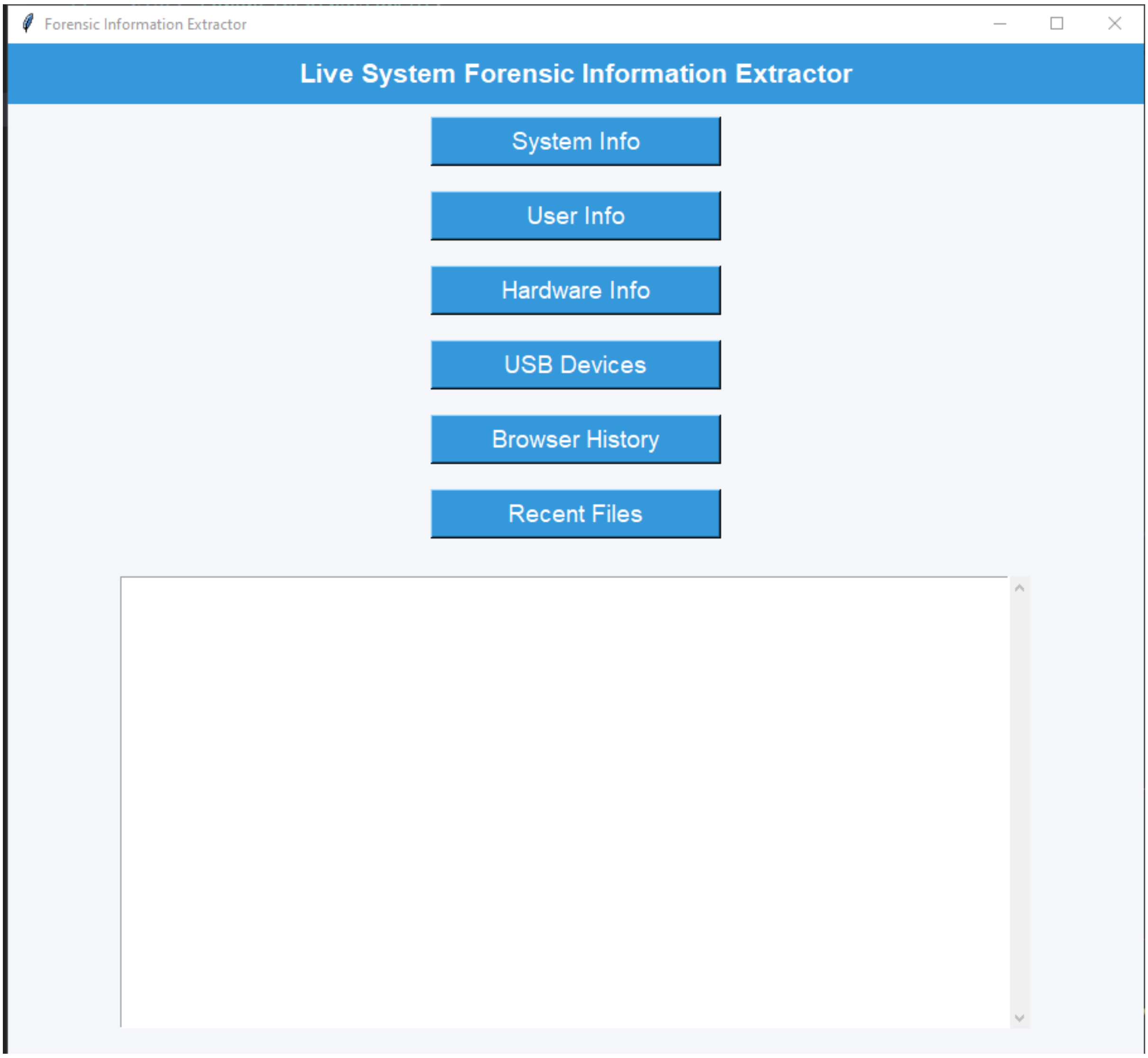
- **NTUSER.dat File**: Extracts software information from the NTUSER.dat registry hive.
- **SAM and SYSTEM Files:** Processes the SAM and SYSTEM registry hives to retrieve user account details and NTLM hashes.
- **User Account Info**: Displays user account information in a tabular format with an option to export data as CSV.

Example Screenshots

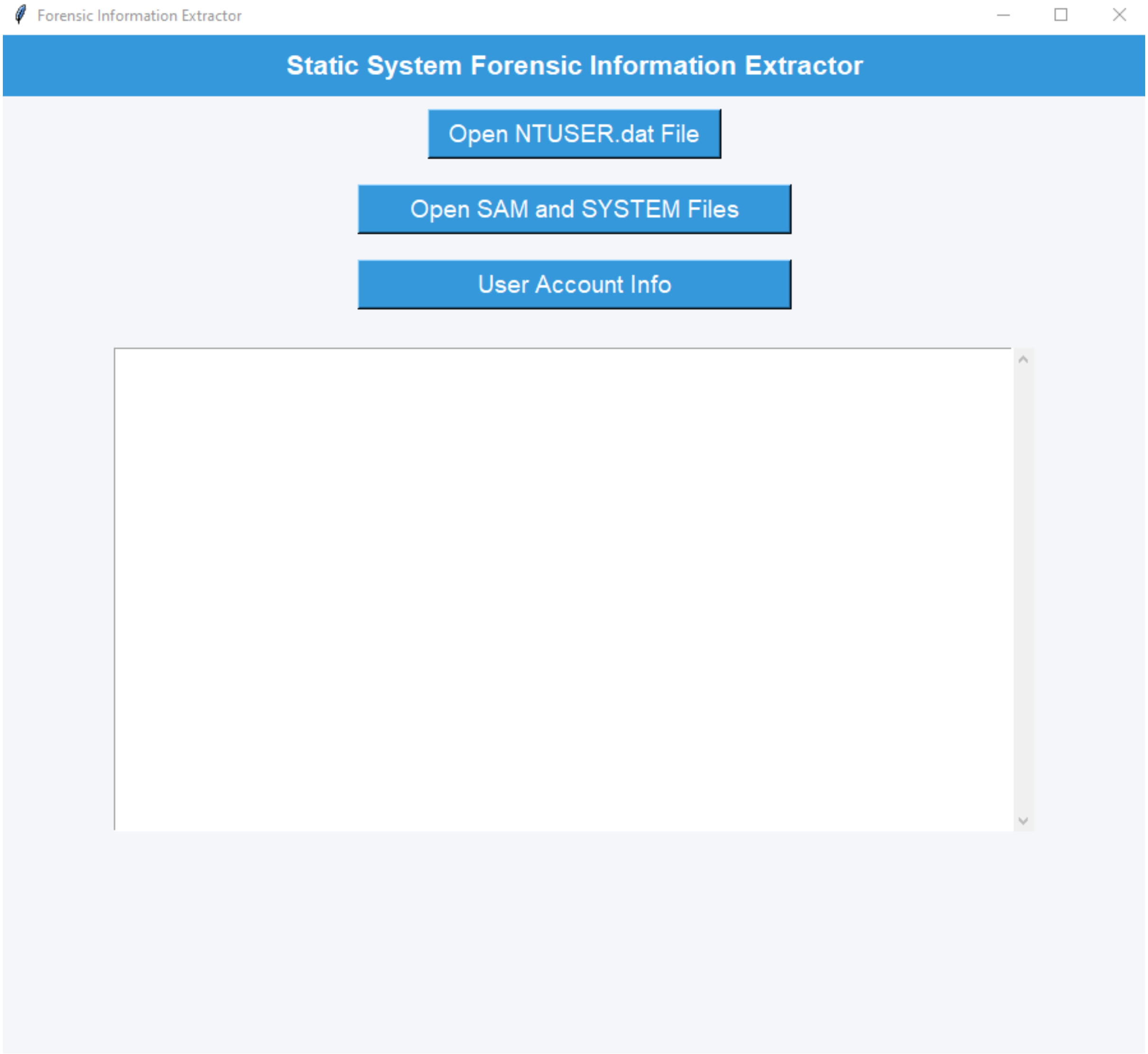
Main Menu


Forensic Information Extractor
Forensic Information Extractor
Choose the System Mode
Live System Info
Static System Info

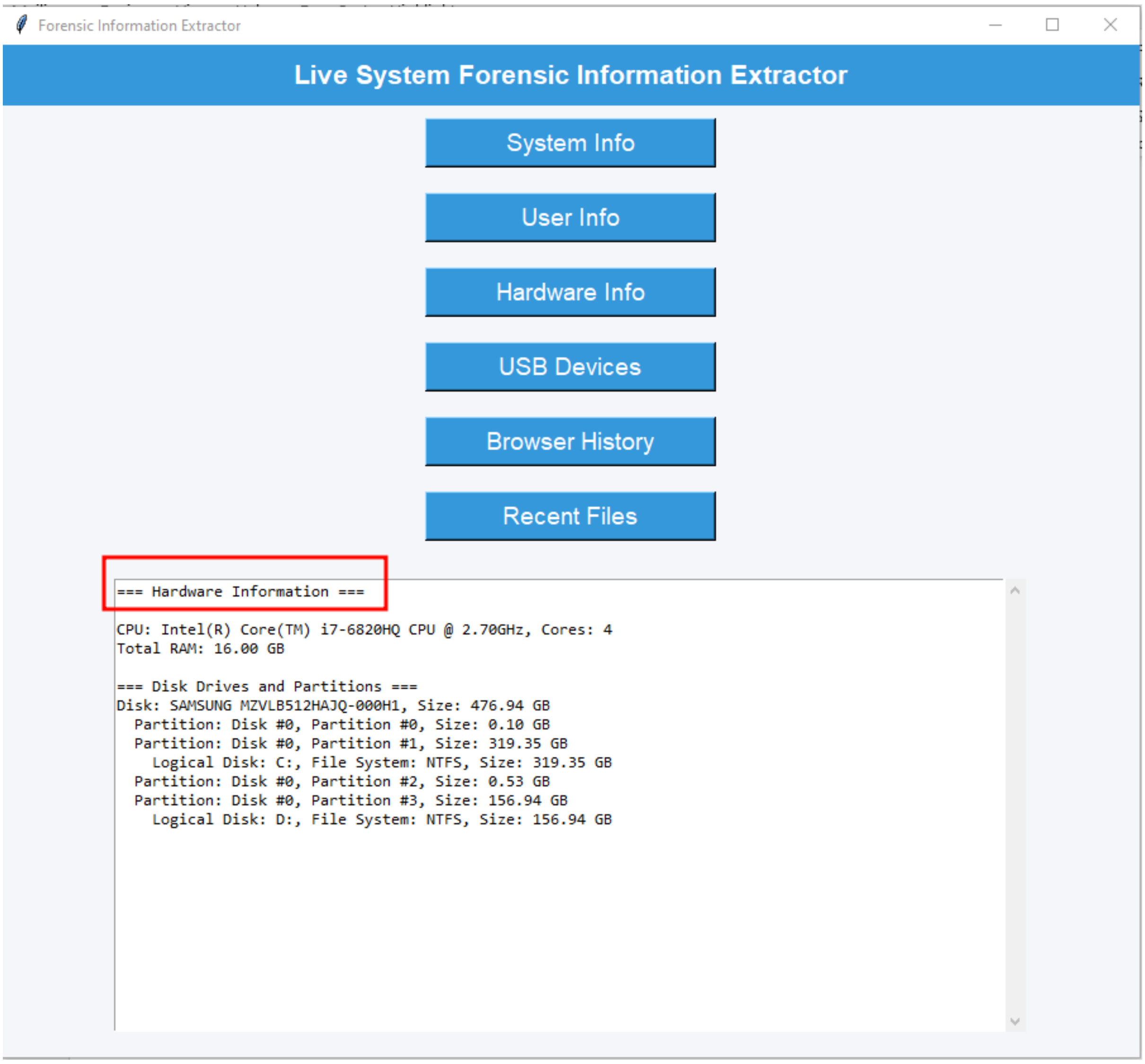
Live System Info Interface


Forensic Information Extractor
Live System Forensic Information Extractor
System Info
User Info
Hardware Info
USB Devices
Browser History
Recent Files

Static System Info Interface


Forensic Information Extractor
Static System Forensic Information Extractor
Open NTUSER.dat File
Open SAM and SYSTEM Files
User Account Info

Extracted Data Example


Forensic Information Extractor
Live System Forensic Information Extractor
System Info
User Info
Hardware Info
USB Devices
Browser History
Recent Files

```
=== Hardware Information ===

CPU: Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz, Cores: 4
Total RAM: 16.00 GB

=== Disk Drives and Partitions ===
Disk: SAMSUNG MZVLB512HAJQ-000H1, Size: 476.94 GB
  Partition: Disk #0, Partition #0, Size: 0.10 GB
  Partition: Disk #0, Partition #1, Size: 319.35 GB
    Logical Disk: C:, File System: NTFS, Size: 319.35 GB
  Partition: Disk #0, Partition #2, Size: 0.53 GB
  Partition: Disk #0, Partition #3, Size: 156.94 GB
    Logical Disk: D:, File System: NTFS, Size: 156.94 GB
```