

**CY2002**

**Digital Forensics**

**History Parser**

**Hands-On Projects**

**Table of Contents**

[**1.** **Introduction:** 2](#_Toc182417332)

[**2.** **Setup and prerequisites:** 2](#_Toc182417333)

[**3.** **Main Application window:** 3](#_Toc182417334)

[**4.** **Browser History Analysis:** 3](#_Toc182417335)

[**5.** **Notepad Data Extraction:** 13](#_Toc182417336)

[**6.** **Directory Listing:** 16](#_Toc182417337)

[**7.** **Metadata Viewer:** 18](#_Toc182417338)

[**8.** **File Hashing:** 22](#_Toc182417339)

[**9.** **File Encryption and Compression:** 24](#_Toc182417340)

[**10.** **Network Activity Monitoring:** 25](#_Toc182417341)

[**11.** **Process Activity Monitoring:** 26](#_Toc182417342)

[**12.** **File System Scanner:** 27](#_Toc182417343)

[**13.** **System Event Logs Viewer:** 27](#_Toc182417344)

[**14.** **Conclusion :** 28](#_Toc182417345)

# **Introduction:**

The **"History Parser Tool"** is a comprehensive forensic software application designed using Python and PyQt5. The tool aims to provide an easy-to-use graphical interface for digital forensic analysis, offering a variety of features such as parsing browser history, extracting metadata, computing file hashes, encrypting files, and viewing system logs. This report covers the detailed implementation, setup, and execution of the tool, complete with screenshots and explanations.

# **Setup and prerequisites:**

To run the "History Parser Tool," the following Python libraries must be installed:

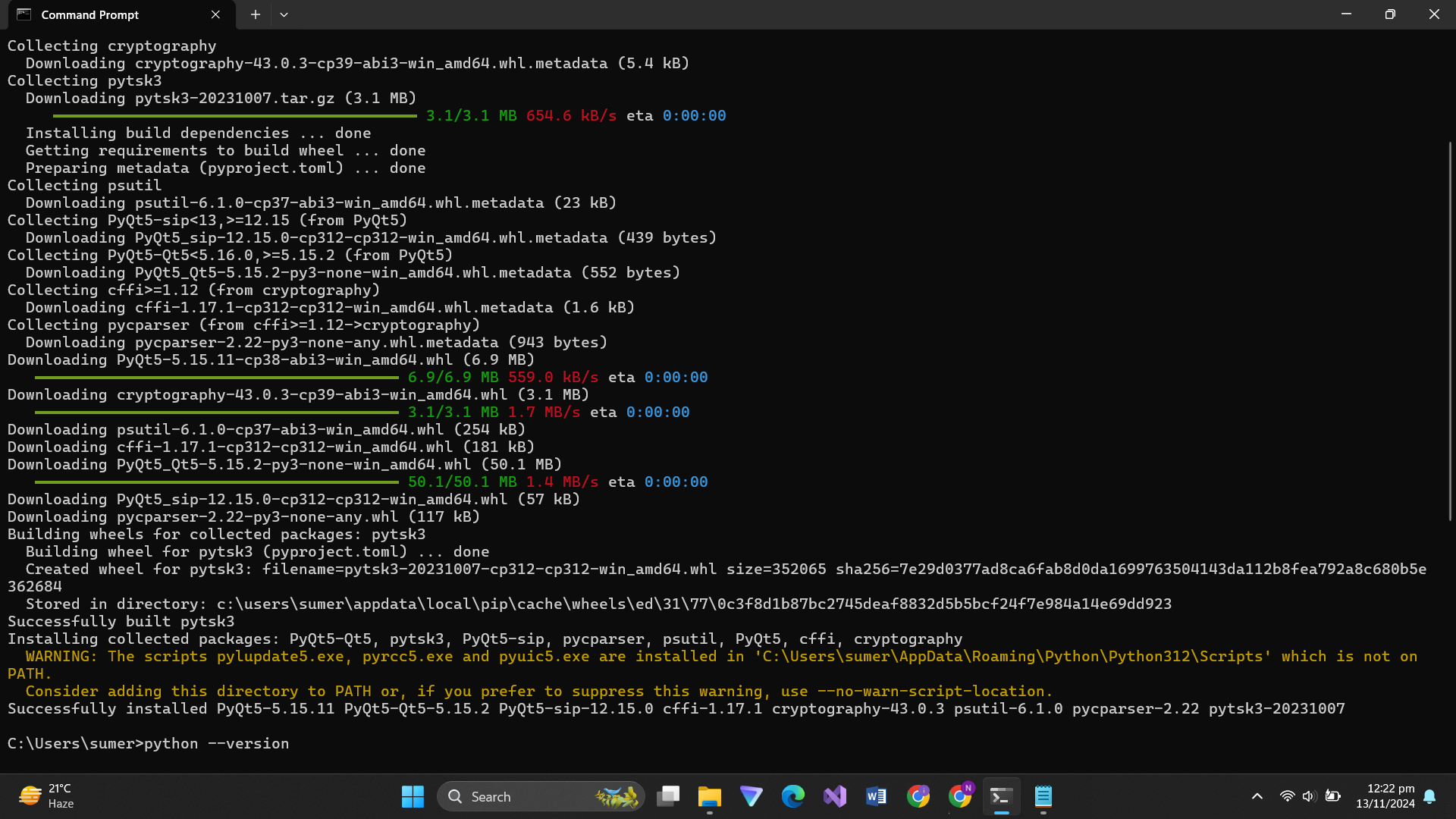
* **PyQt5**: For building the graphical user interface.
* **Cryptography**: For file encryption and decryption.
* **PyTSK3**: For forensic analysis of disk images.
* **Psutil**: For monitoring system processes and network activity.
* **SQLite3**: For parsing browser history databases.
* **Ctypes**: For accessing Windows API functions.

**Installation Command:**

pip install PyQt5 cryptography pytsk3 psutil

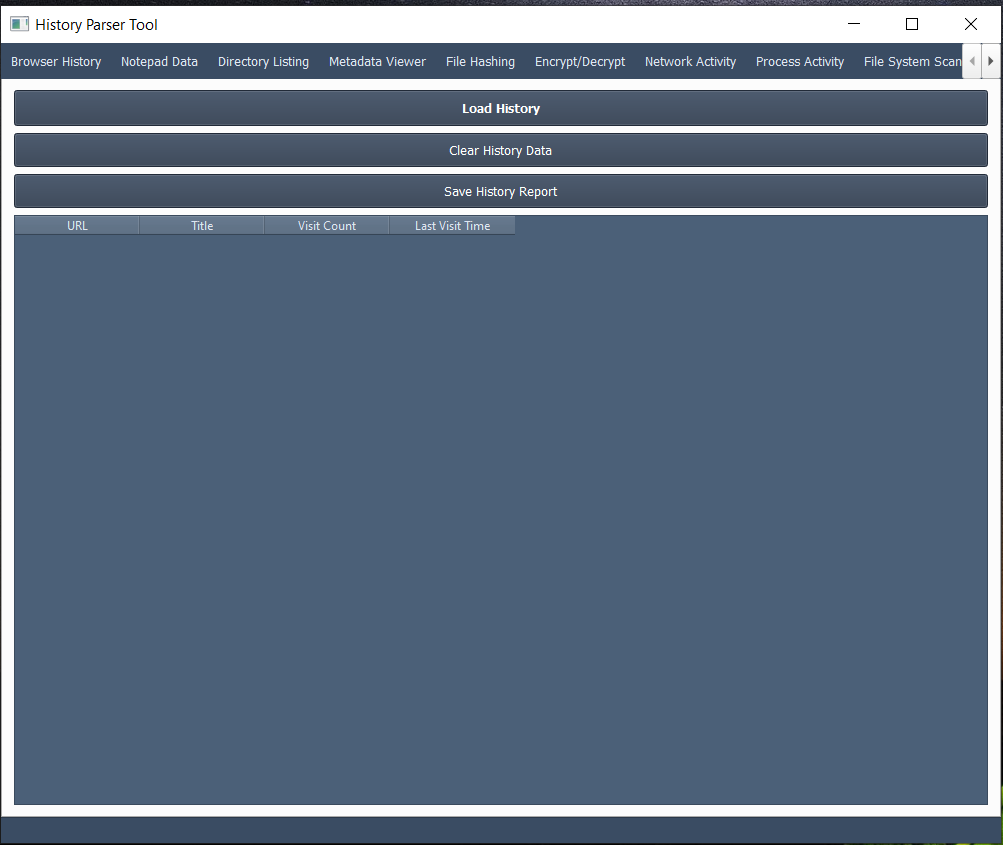
Ensure that Python 3.8 or higher is installed. You can verify the Python version with:

python –version



# **Main Application window:**

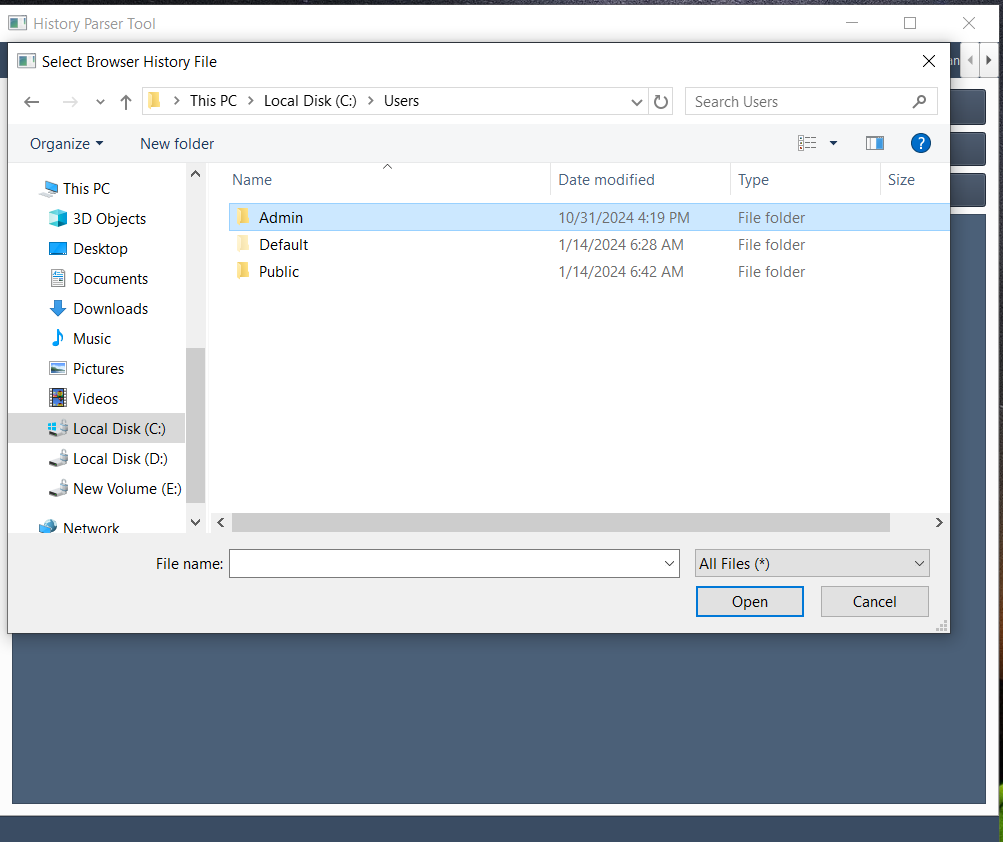
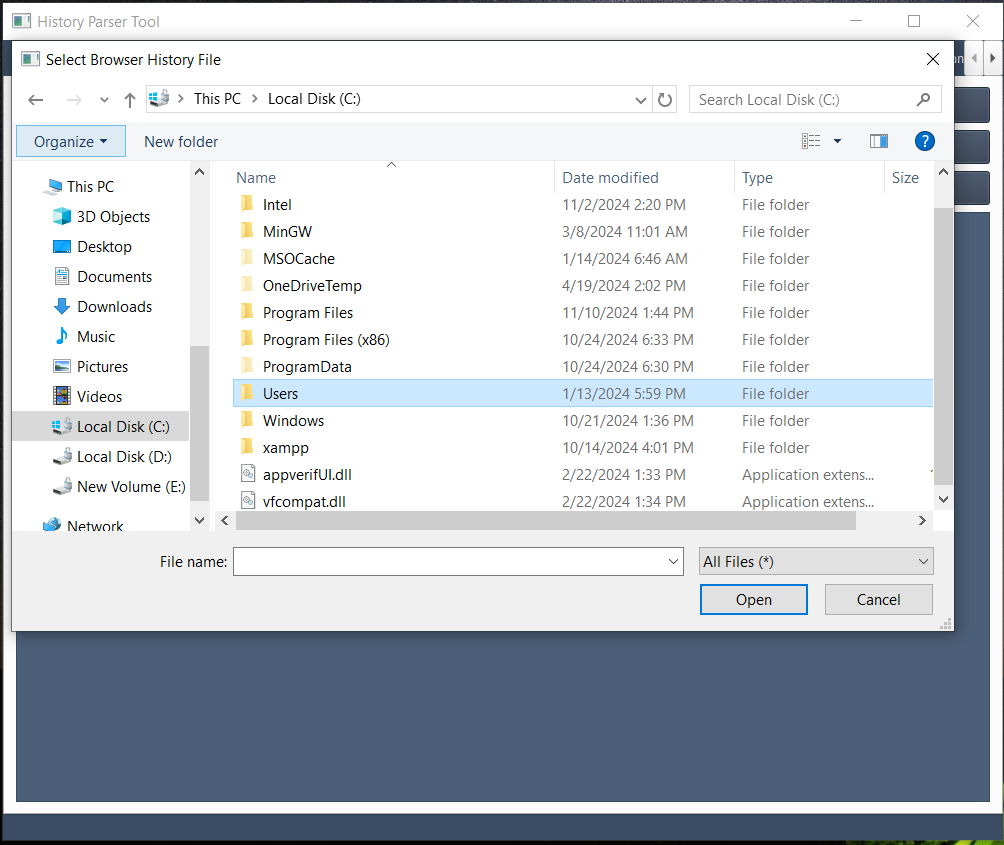
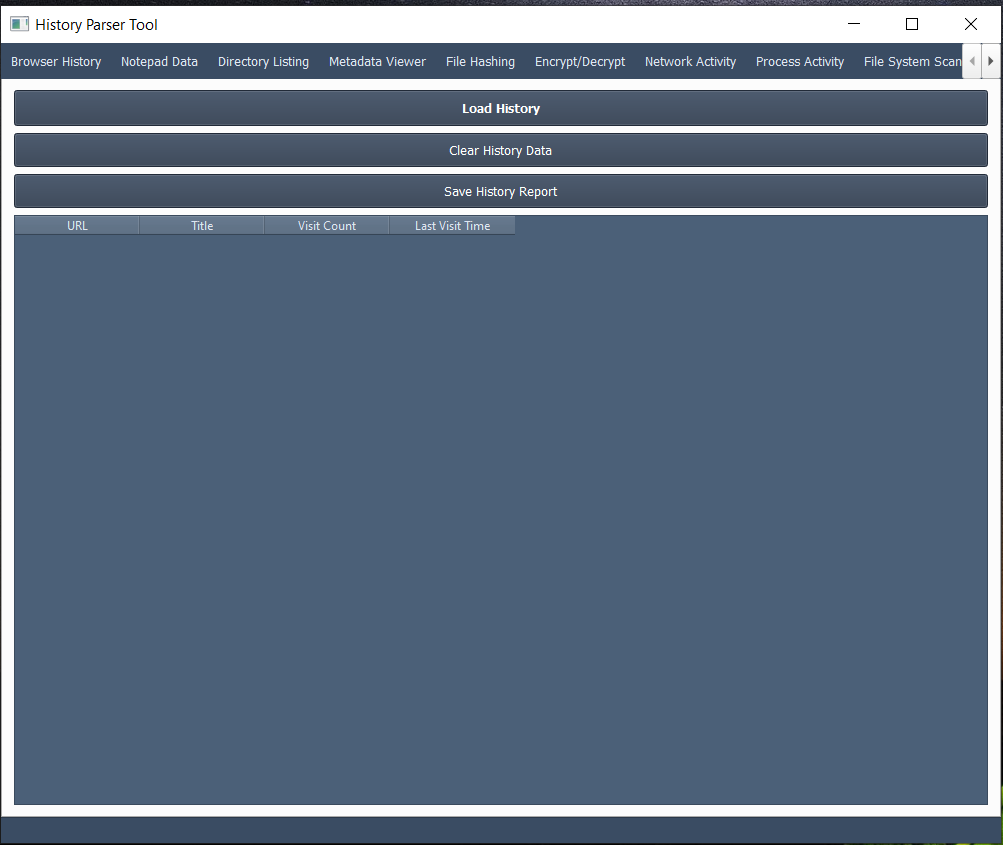
The main window of the application is divided into several tabs, each focusing on a specific forensic task. The UI uses a grey-blue color scheme for a modern, professional look, with clear labels and well-organized components.

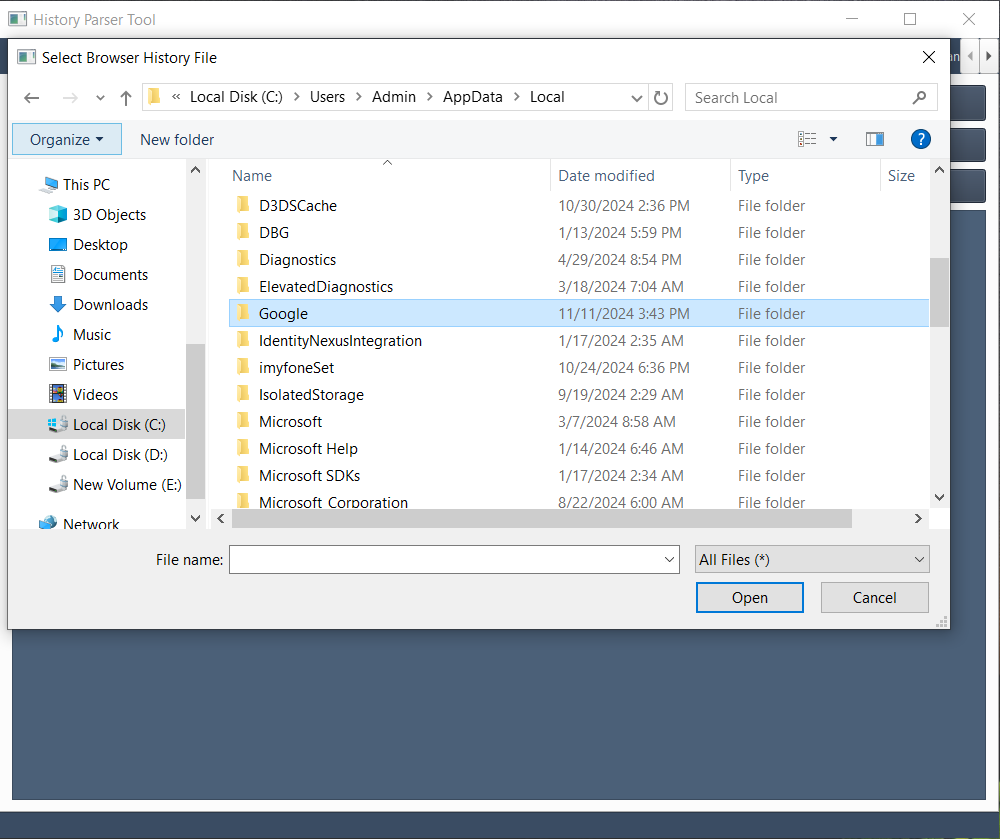
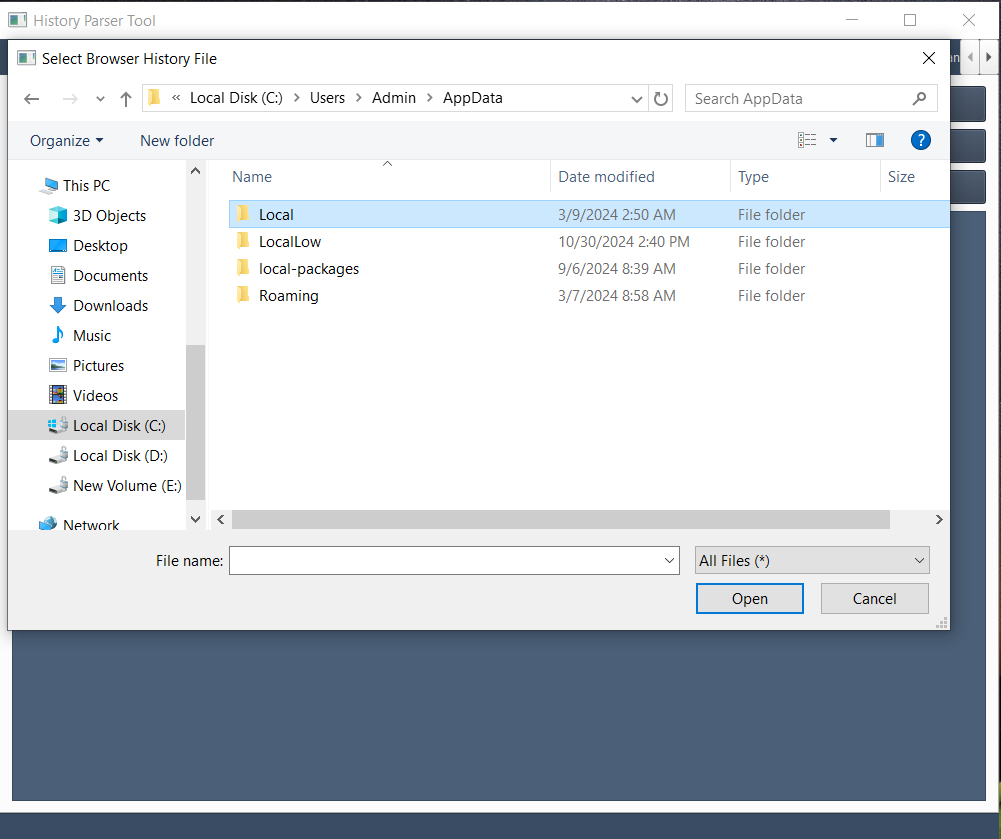
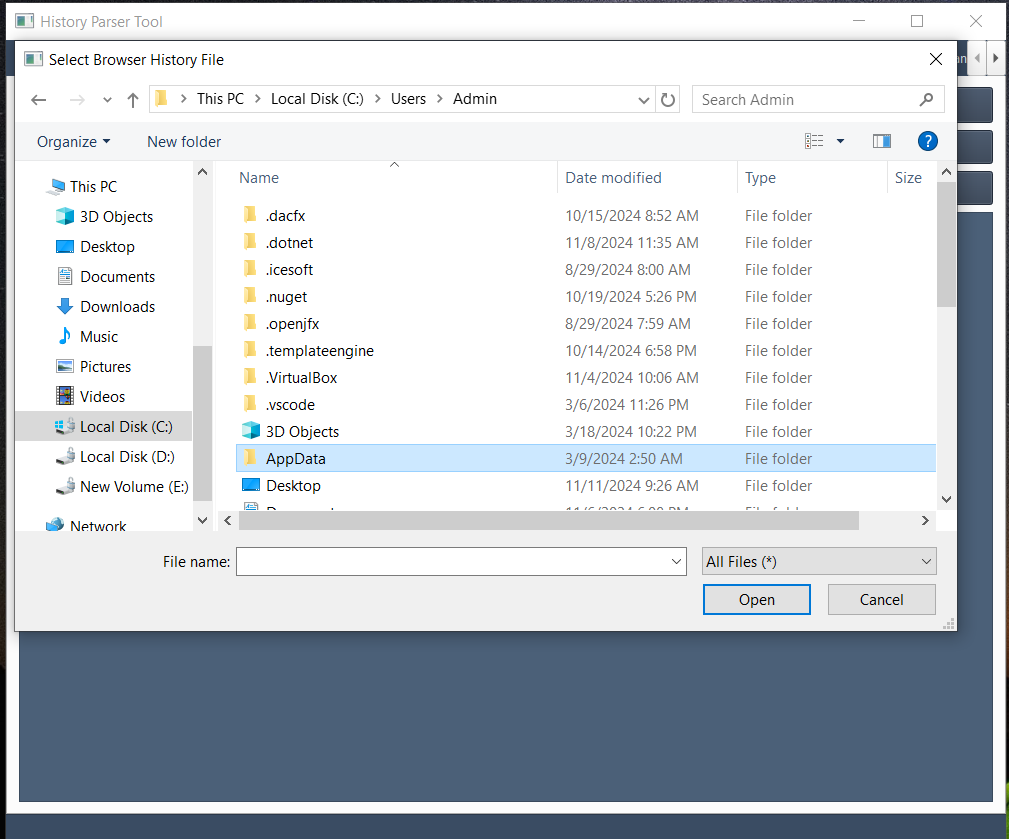


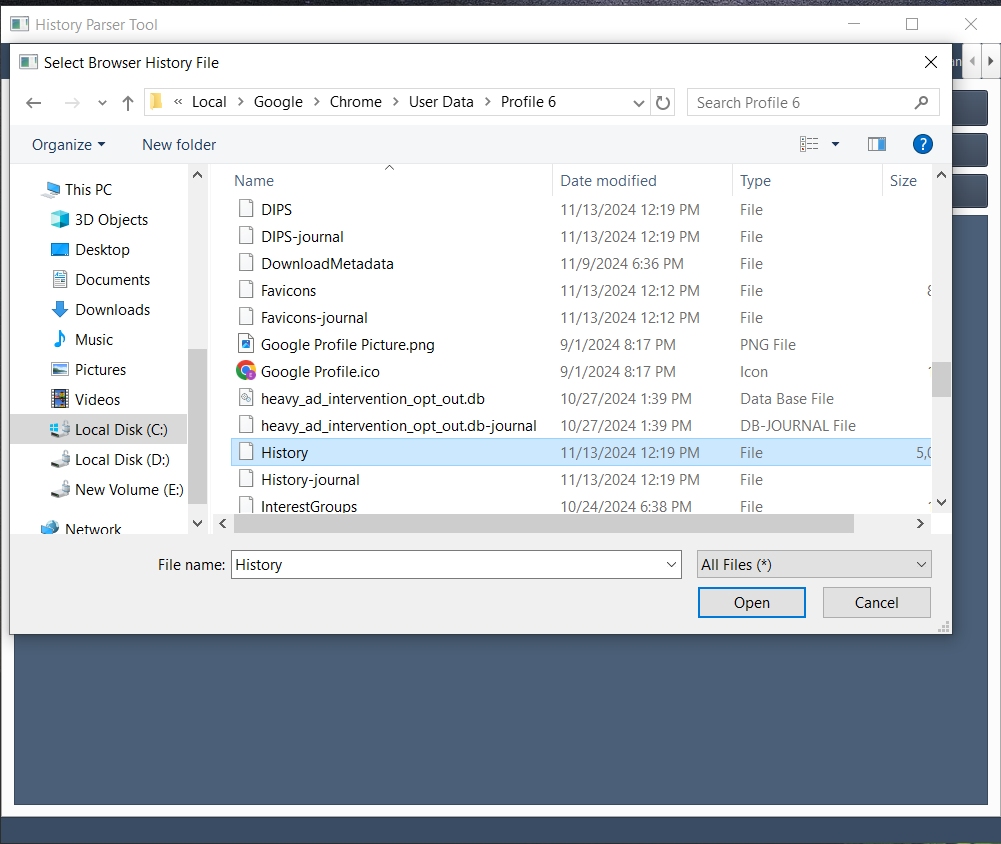
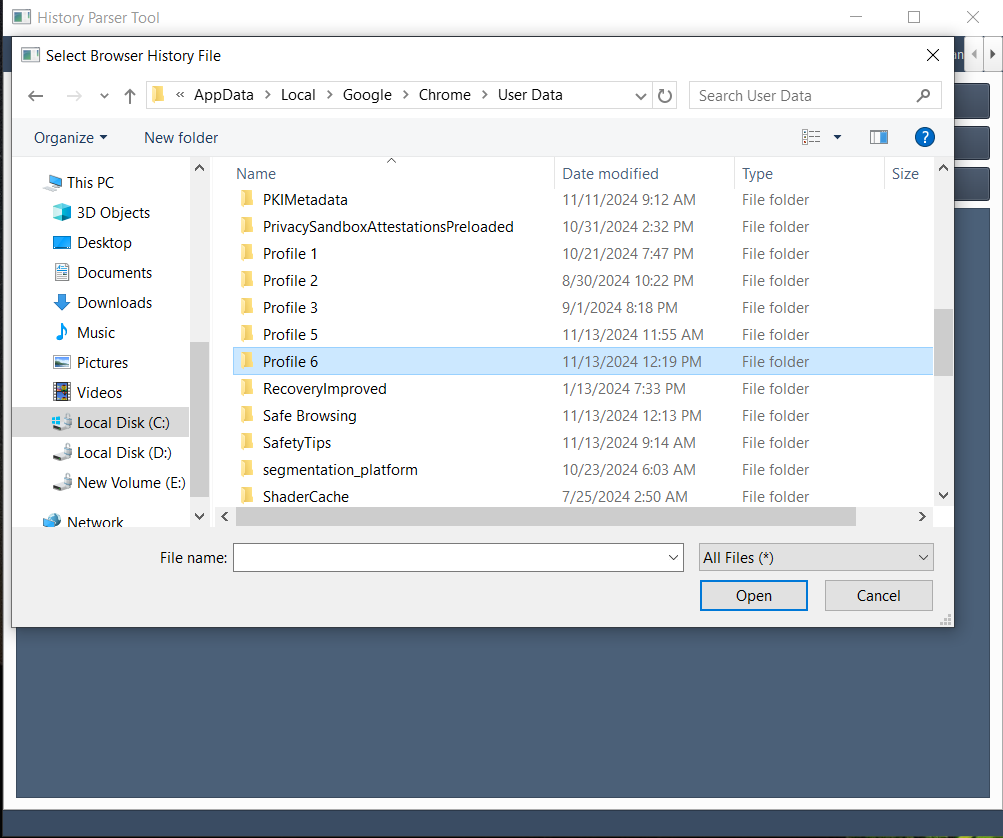
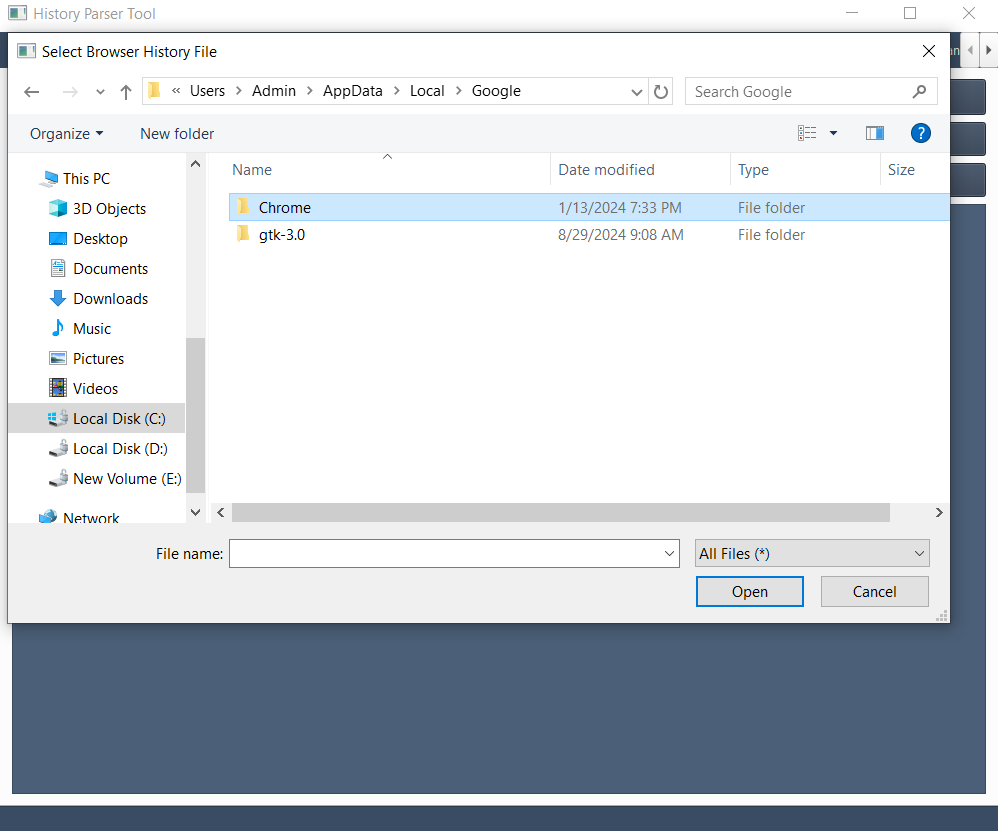
# **Browser History Analysis:**

The **Browser History** tab allows users to load browser history files (SQLite databases) from popular browsers like Google Chrome and Microsoft Edge. The application parses the history database and displays columns such as URL, title, visit count, and last visit time.

* **Steps to Use:**
  1. Click **Load History** and select the history database file.
  2. The table will populate with the parsed history data.
  3. Click **Save History Report** to export the data to a text file.







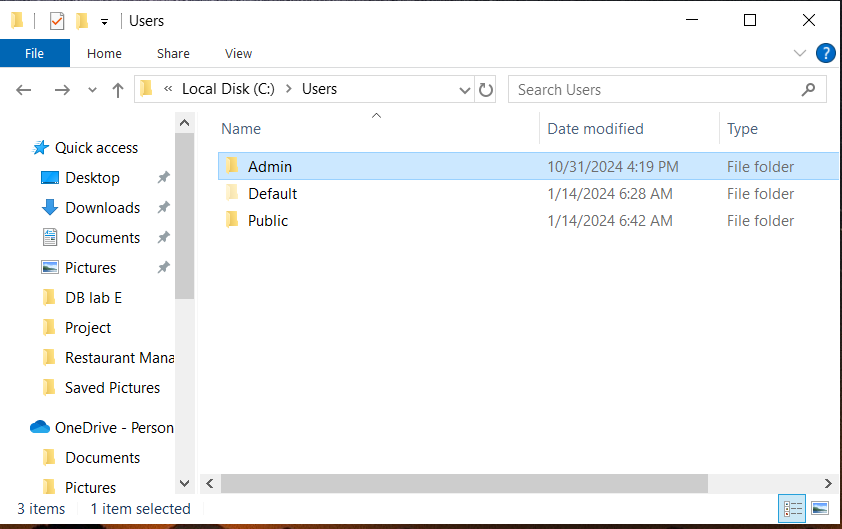


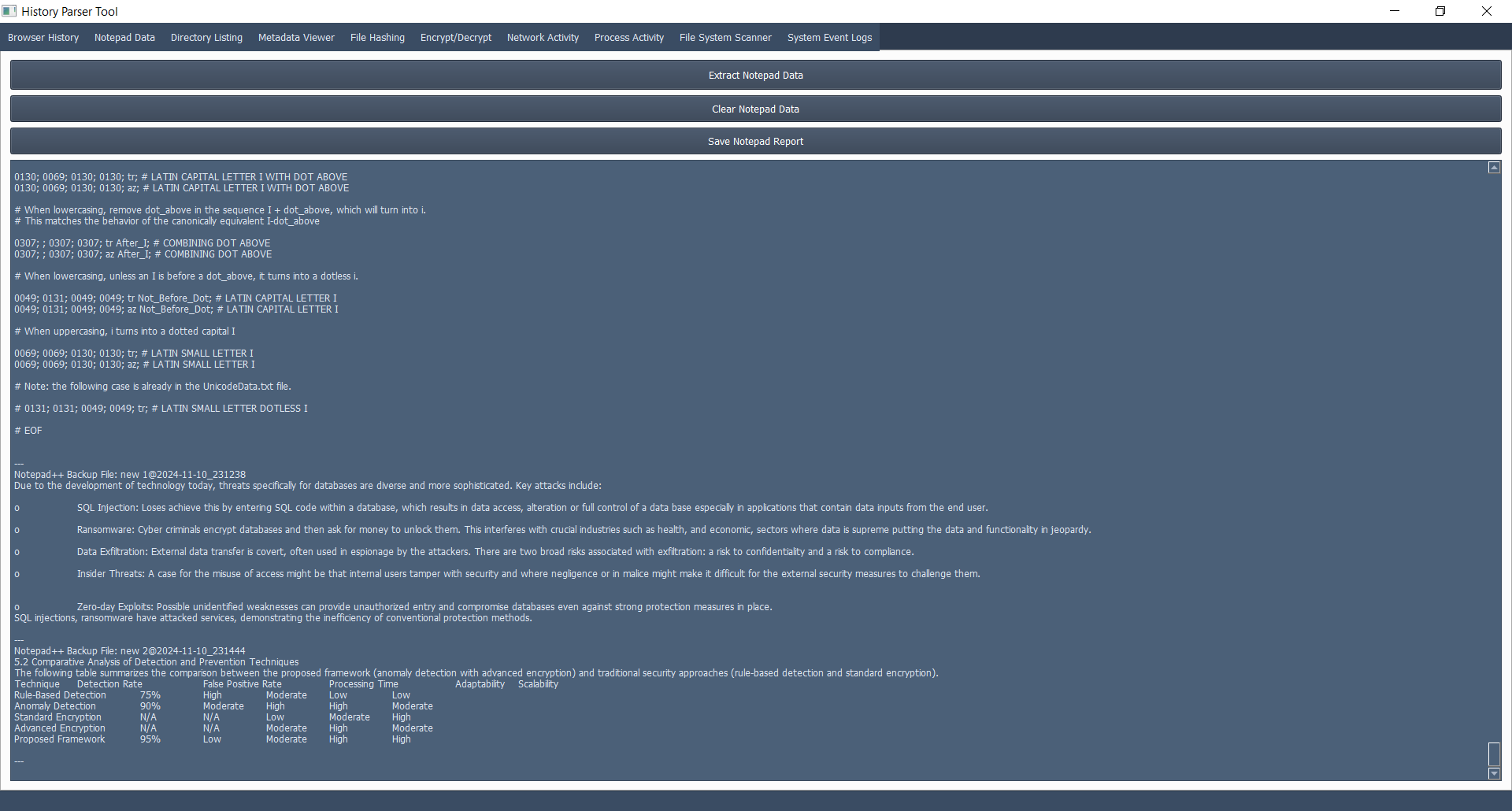
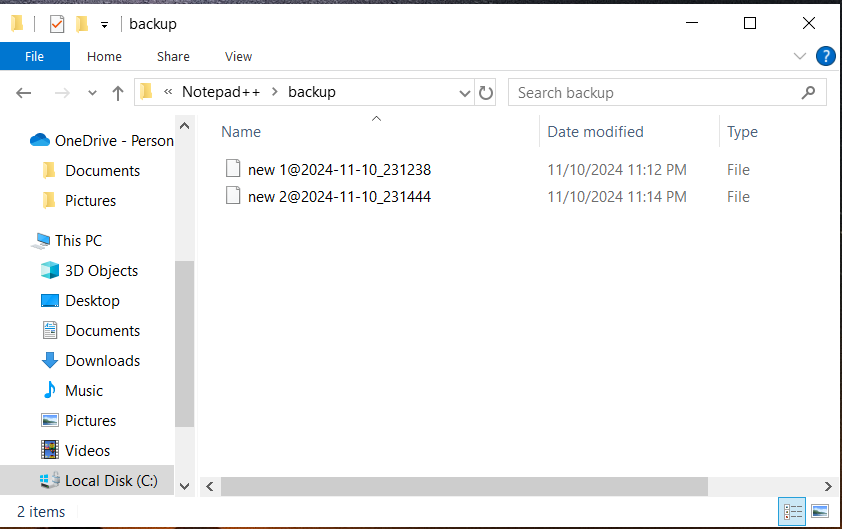
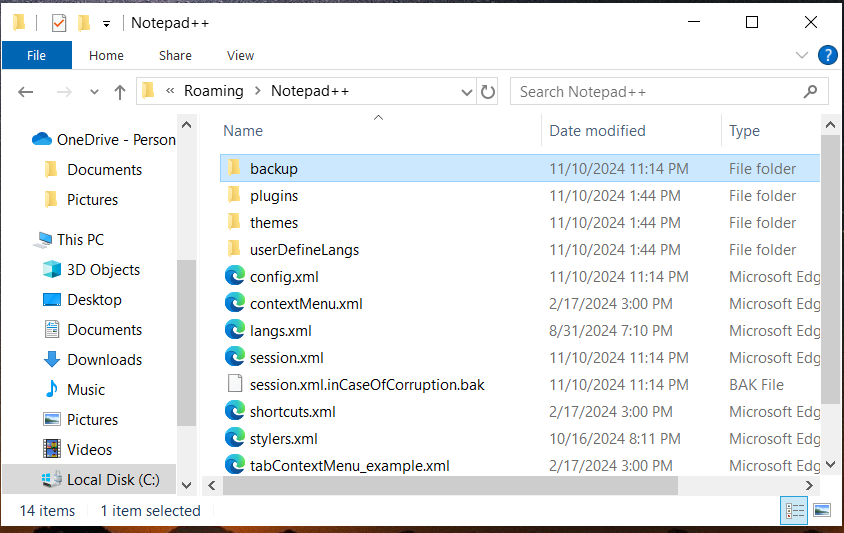
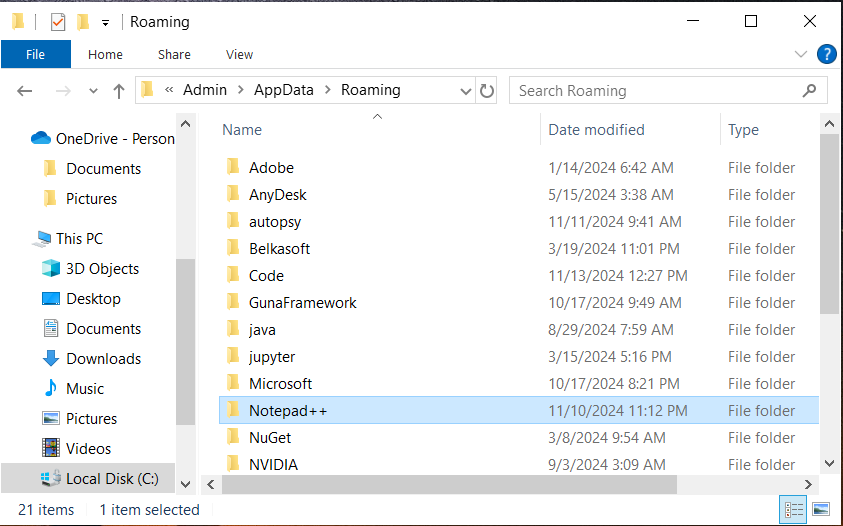
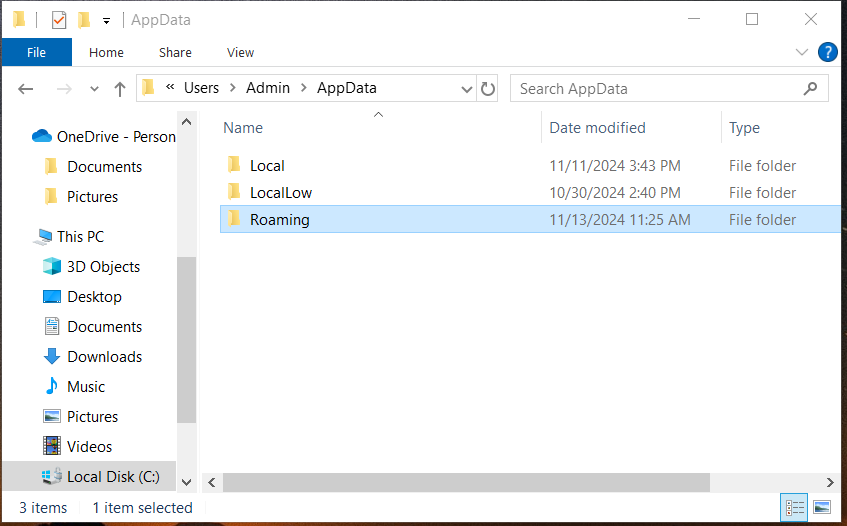
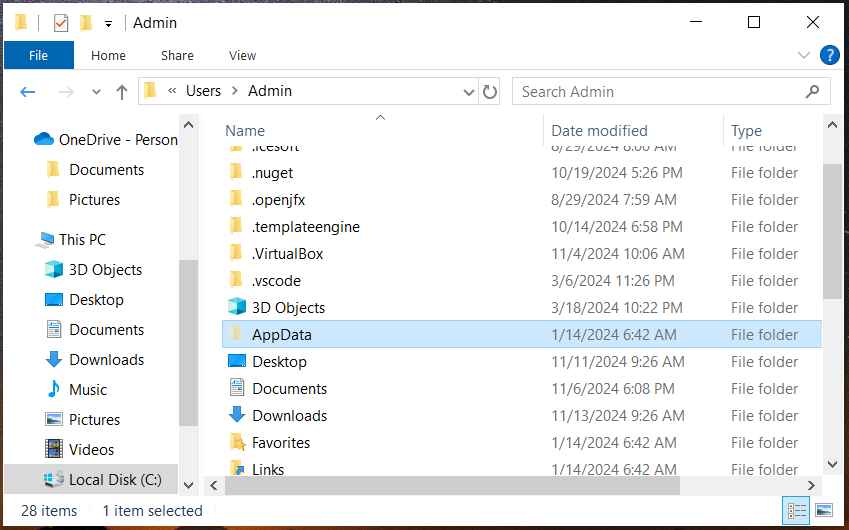
# **Notepad Data Extraction:**

The **Notepad Data** tab extracts unsaved text files from temporary directories, including Notepad and Notepad++ backup locations.

* **Steps to Use:**
  1. Click **Extract Notepad Data**.
  2. The tool searches predefined paths for unsaved or backup text files.
  3. Extracted text is displayed in a text box for review and can be saved.

**Screenshot: Notepad Data Extraction**



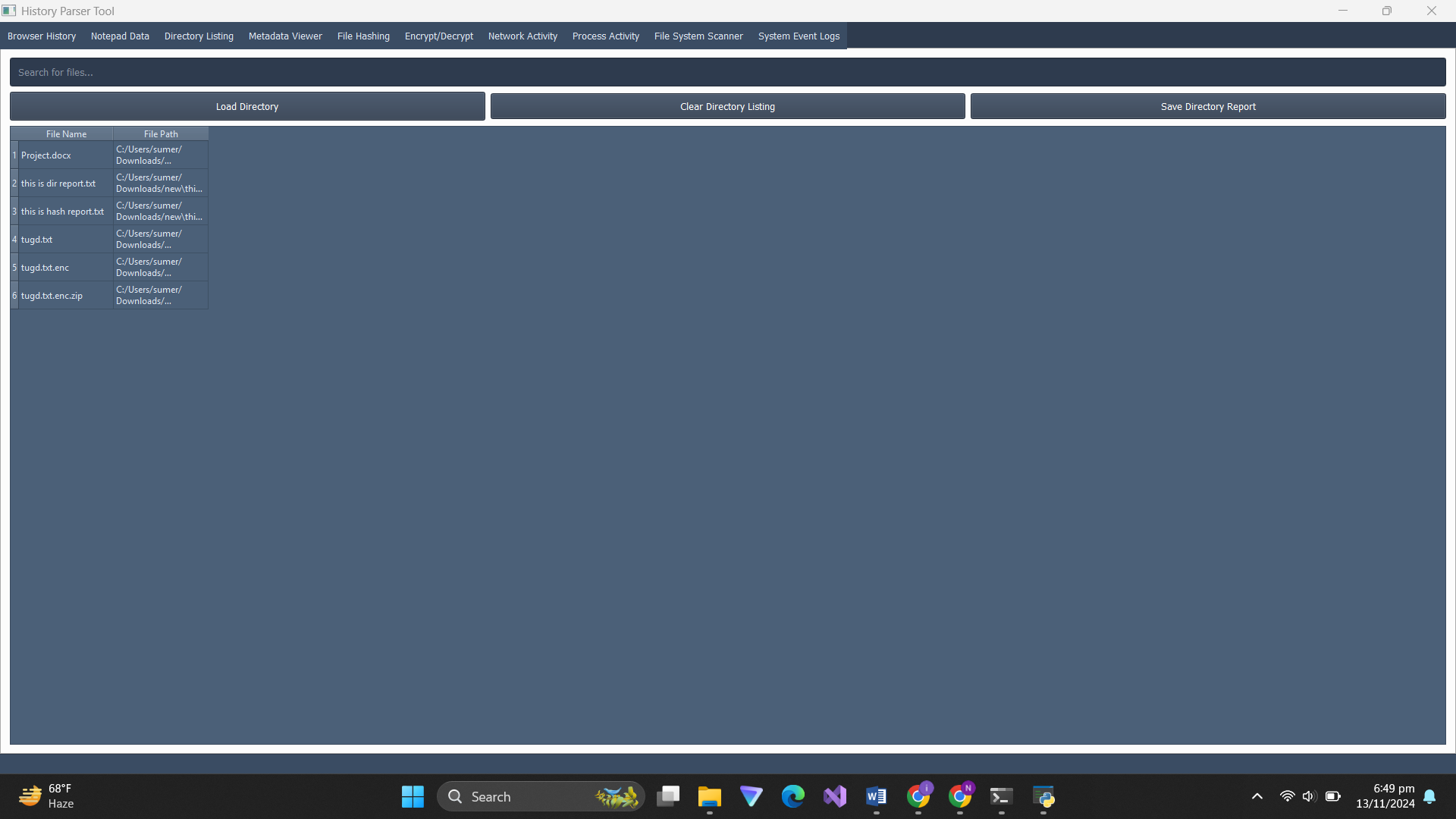


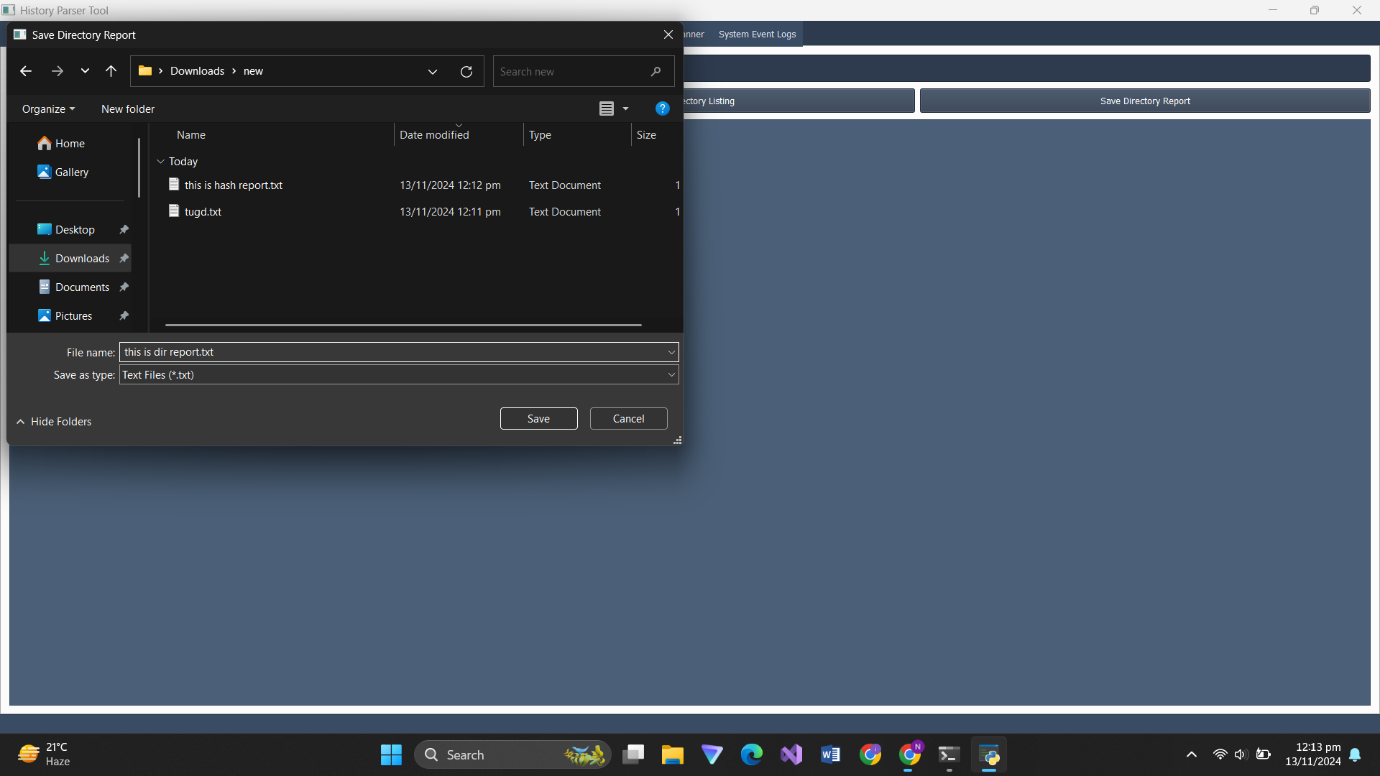
# **Directory Listing:**

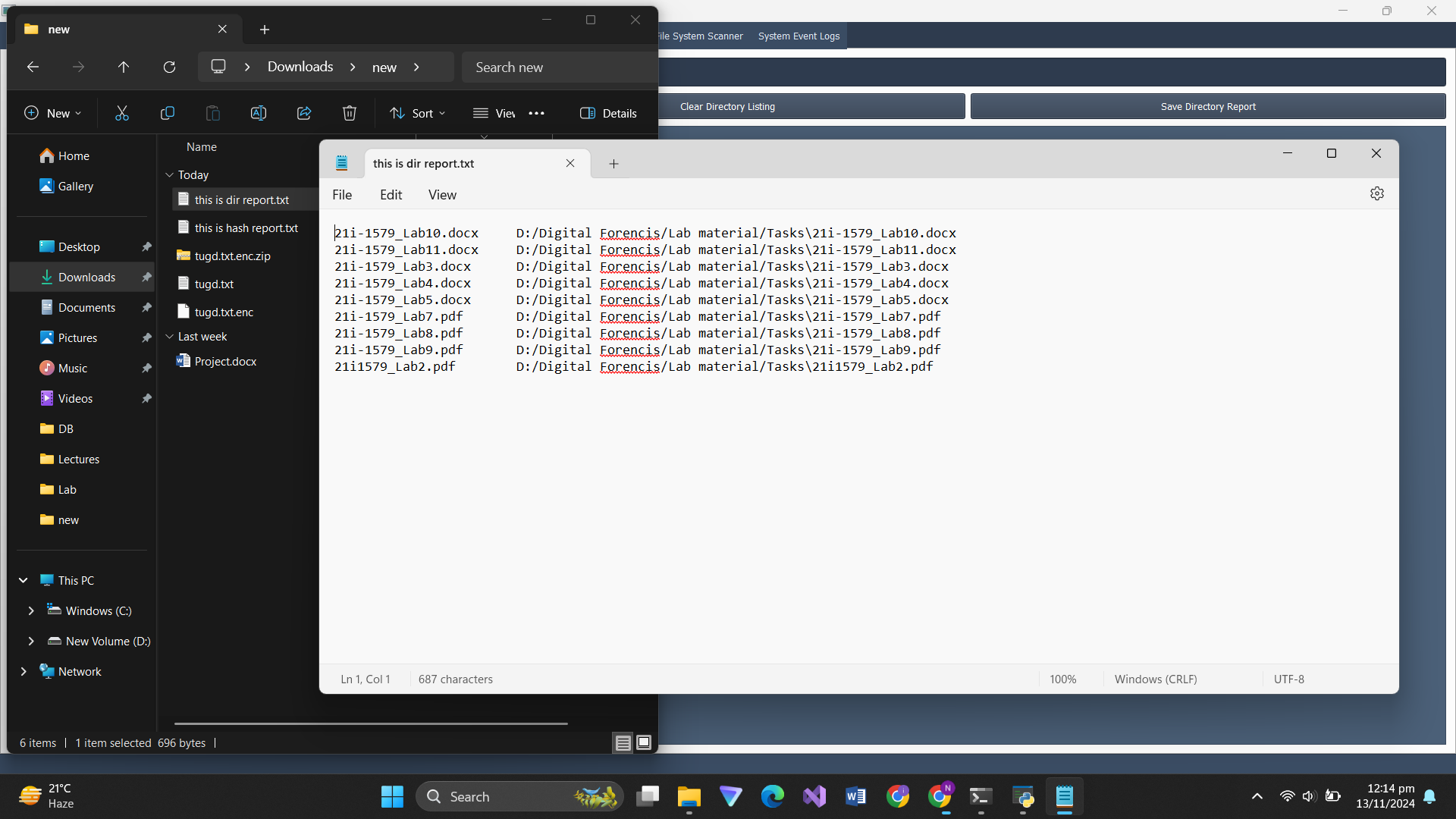
The **Directory Listing** tab scans a selected folder and displays all files along with their paths. Users can filter the files using the search bar.

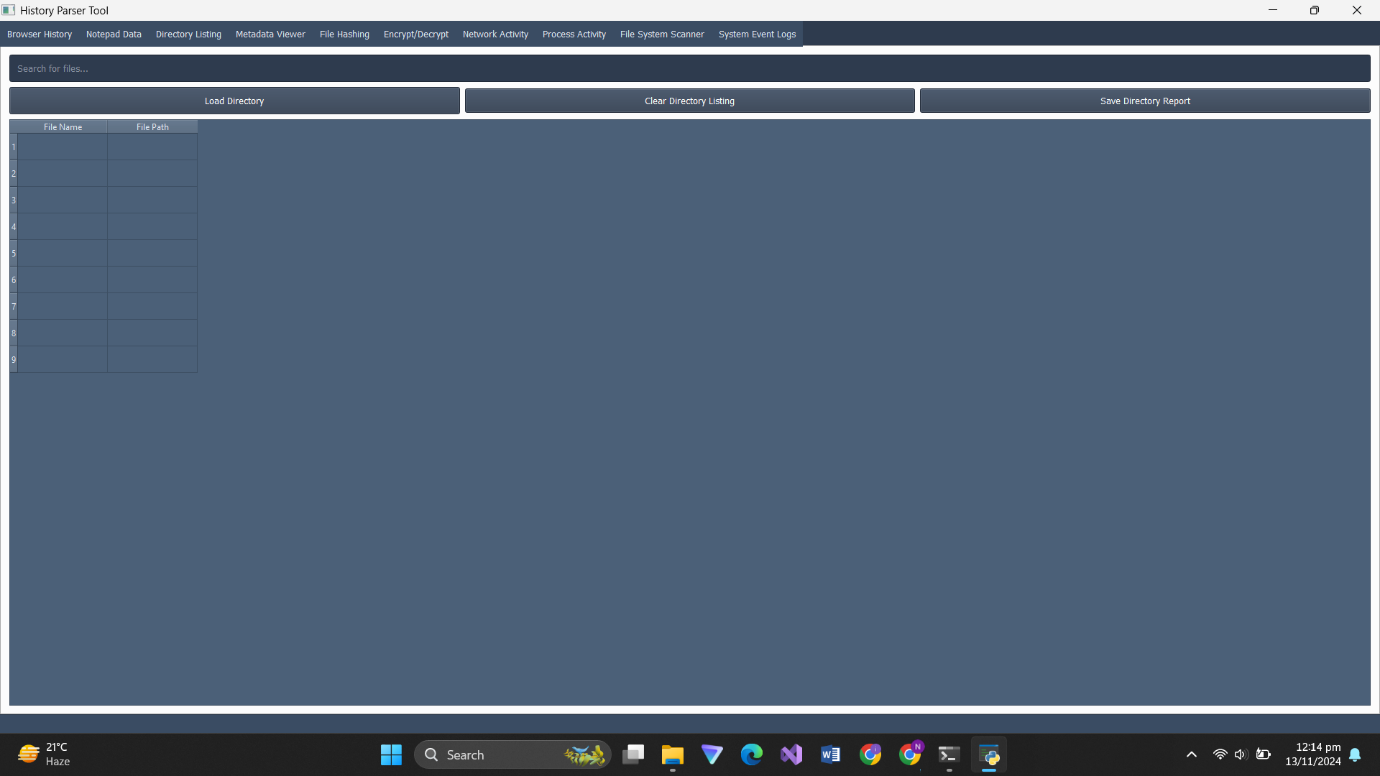
* **Steps to Use:**
  1. Click **Load Directory** and choose a folder.
  2. The tool lists all files in the directory.
  3. Use the search input to filter results.
  4. Click **Save Directory Report** to export the list.

**Screenshot: Directory Listing Tab**







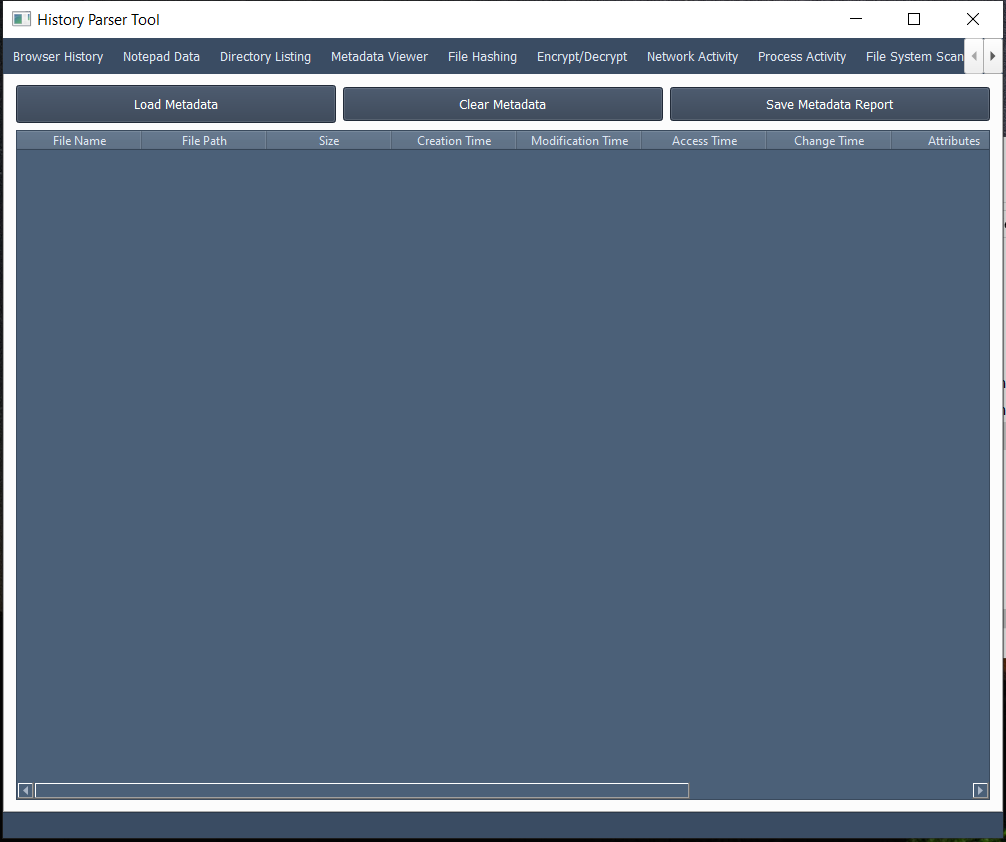


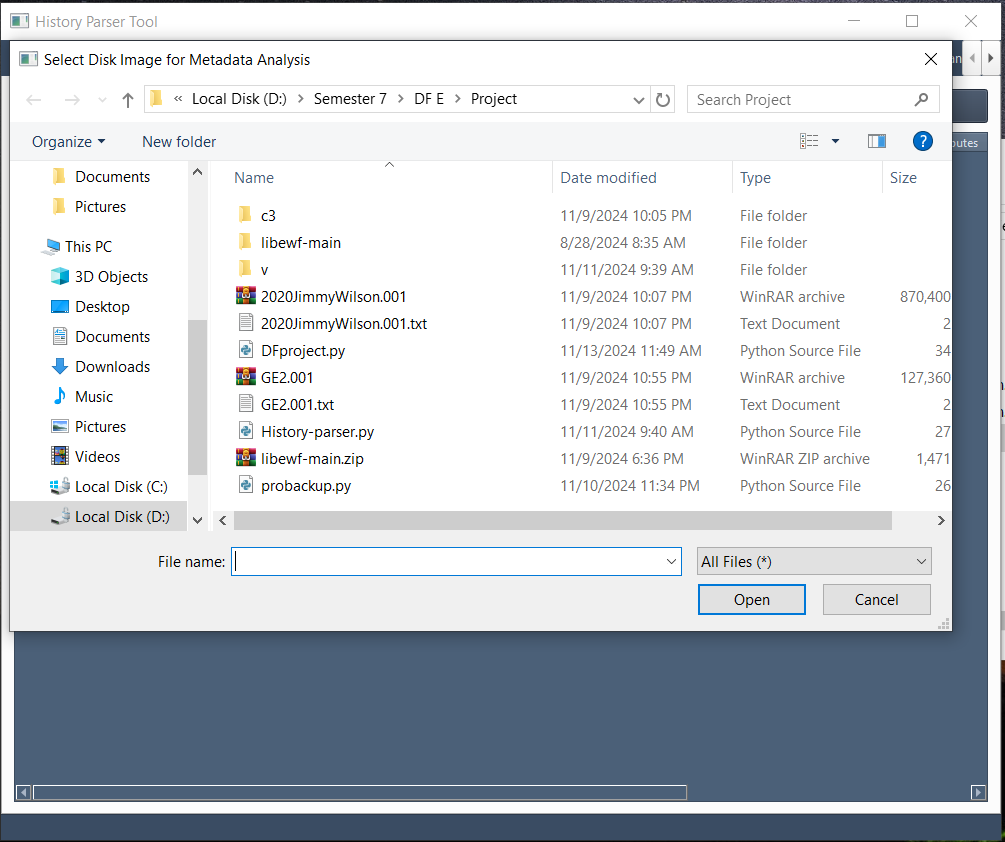
# **Metadata Viewer:**

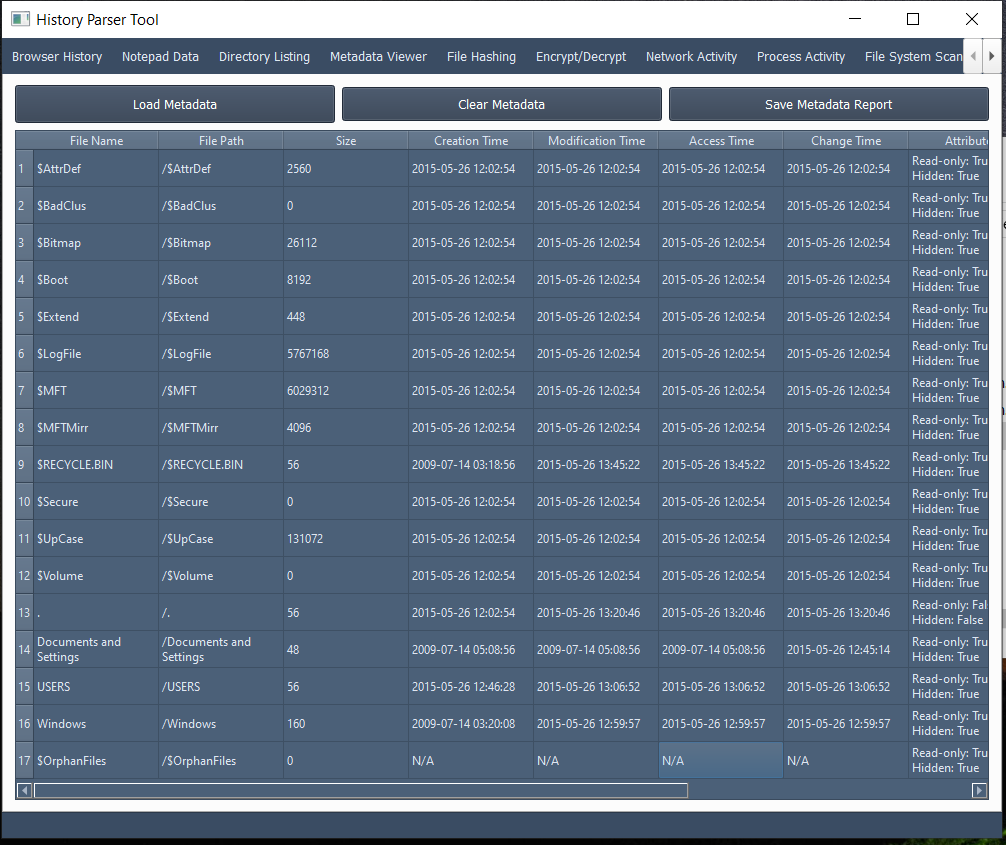
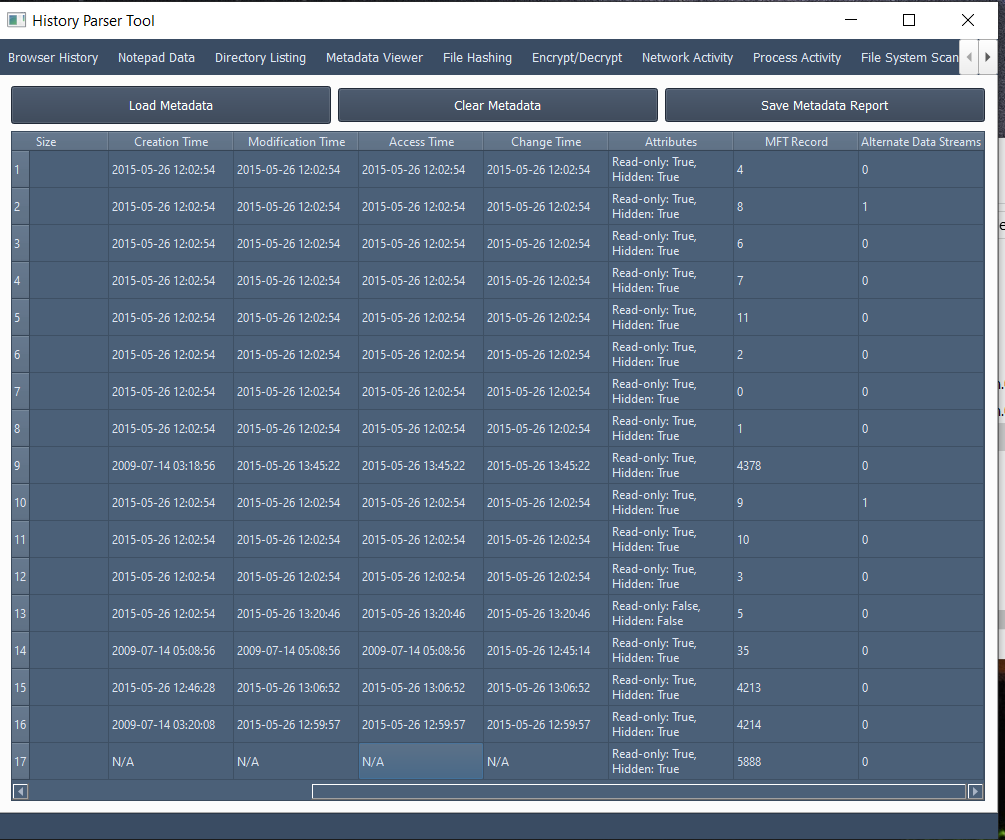
The **Metadata Viewer** tab uses pytsk3 to analyze disk images and extract file metadata, including timestamps, NTFS attributes, MFT records, and alternate data streams.

* **Steps to Use:**
  1. Click **Load Metadata** and select a disk image file.
  2. The tool extracts metadata from the root directory.
  3. Metadata is displayed in a table format and can be saved.

**Screenshot: Metadata Viewer Tab**





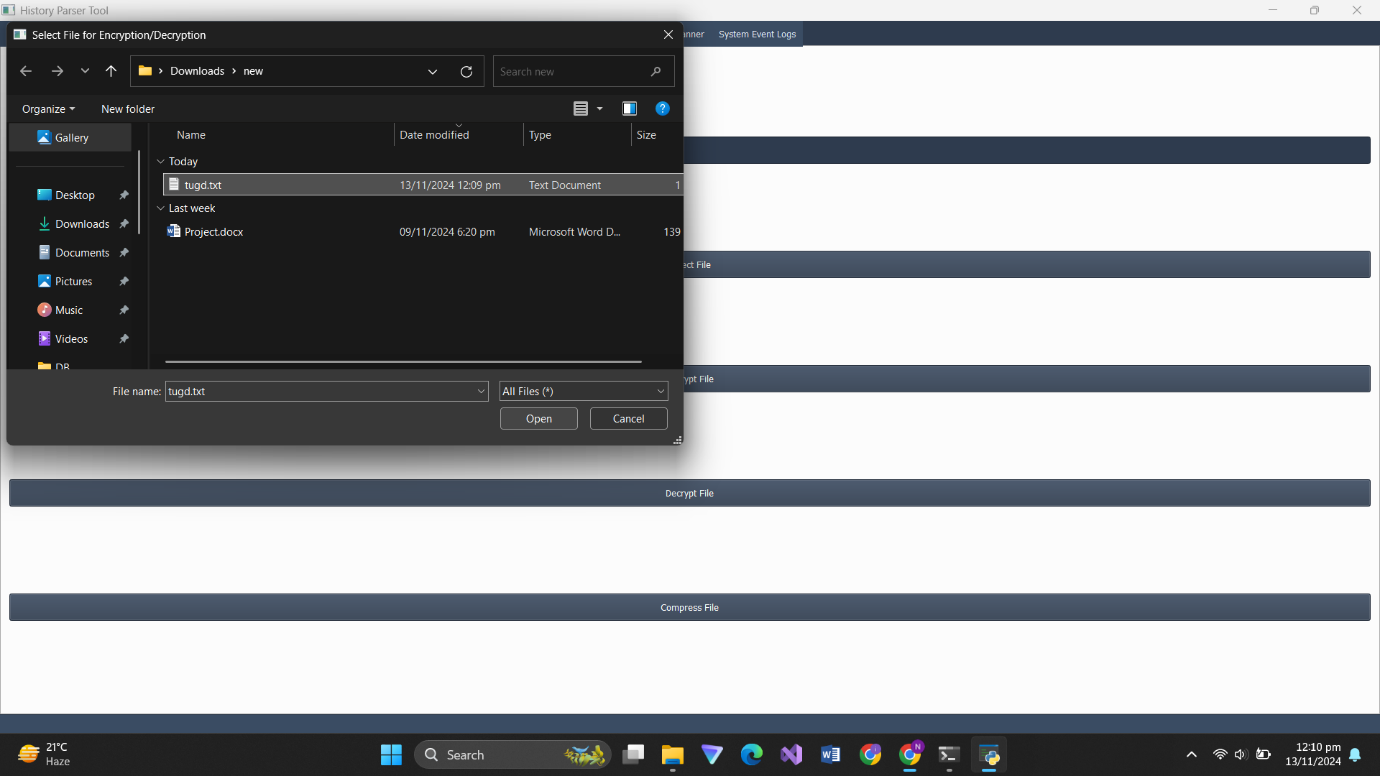


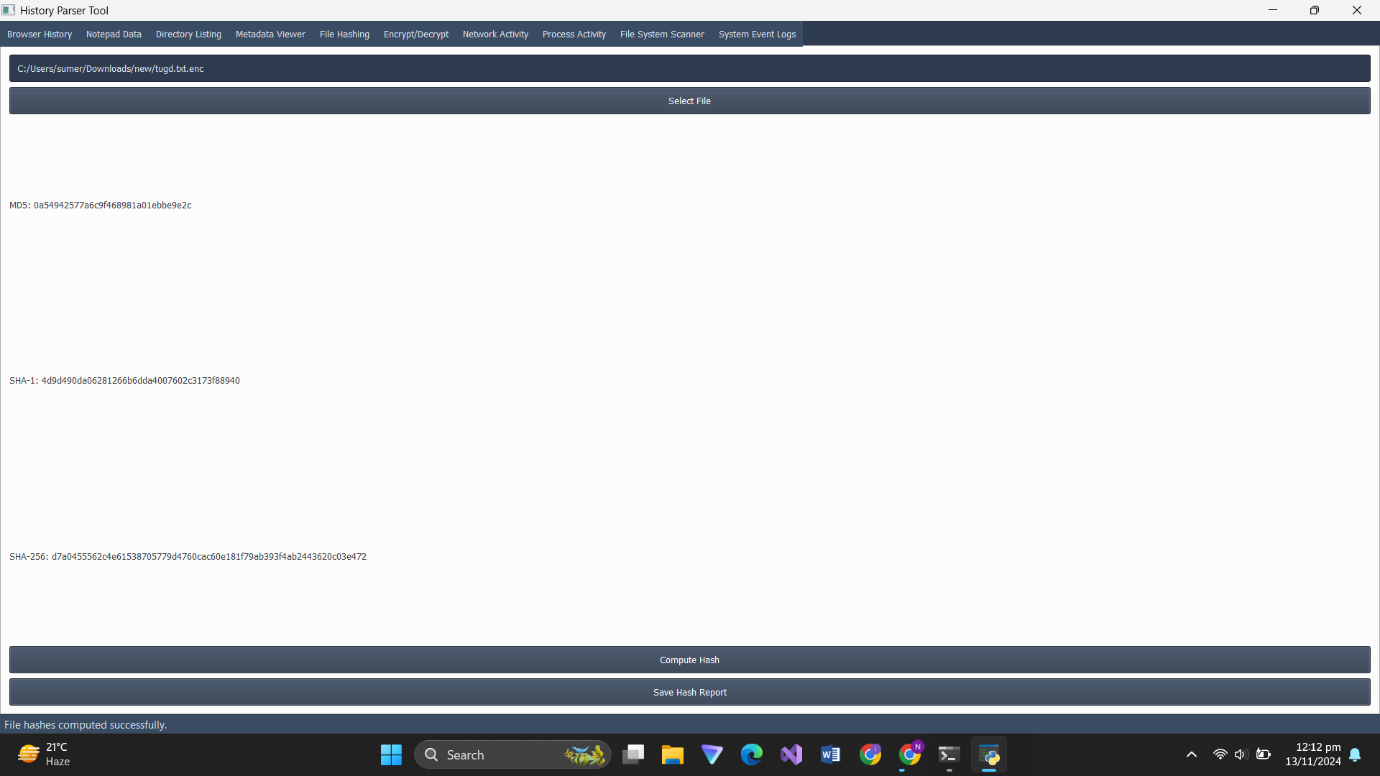
# **File Hashing:**

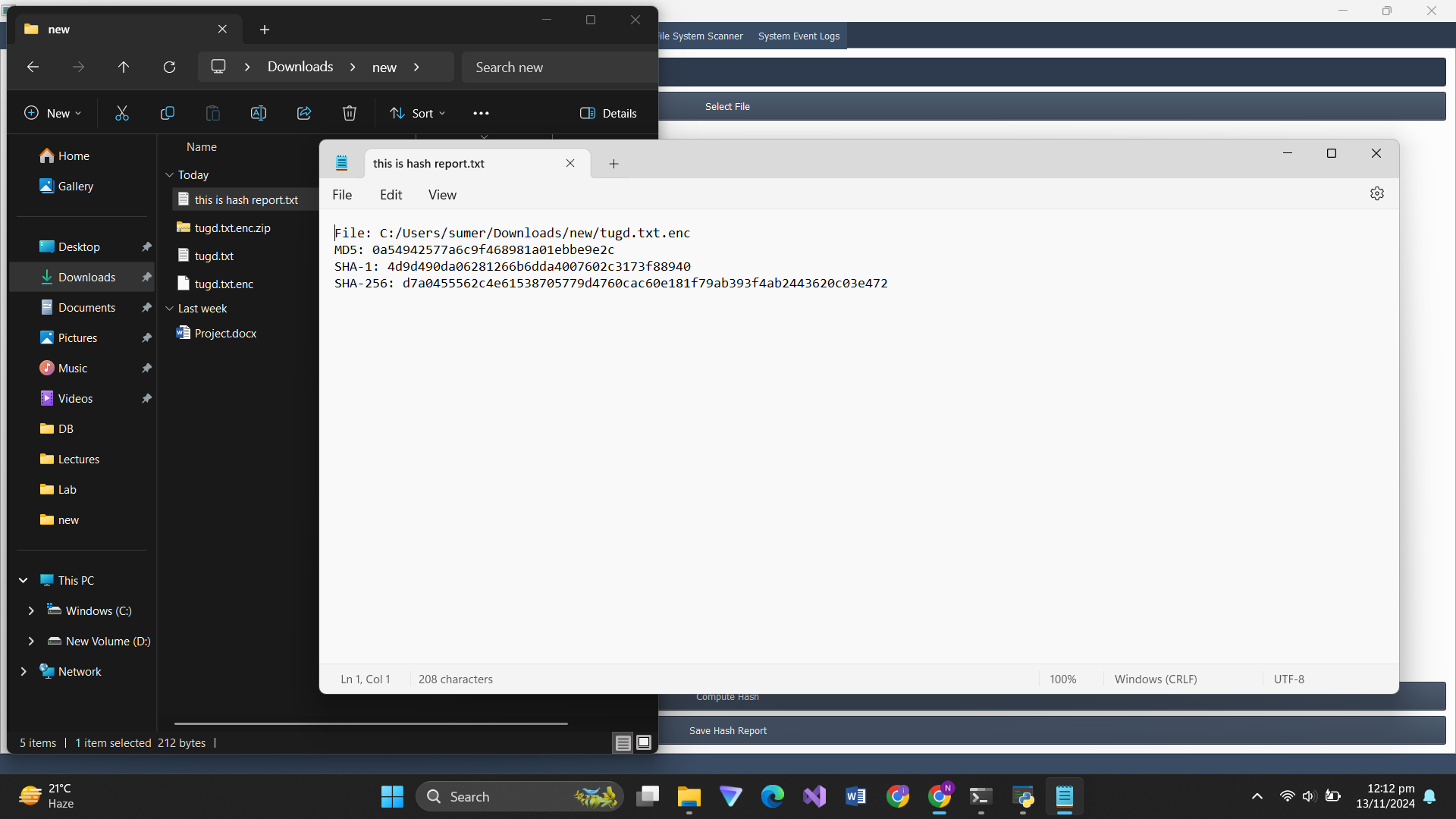
The **File Hashing** tab computes MD5, SHA-1, and SHA-256 hashes for selected files, providing an essential tool for data integrity verification.

* **Steps to Use:**
  1. Click **Select File** and choose a file.
  2. Click **Compute Hash** to generate hashes.
  3. Click **Save Hash Report** to export the hash values.

**Screenshot: File Hashing Tab**





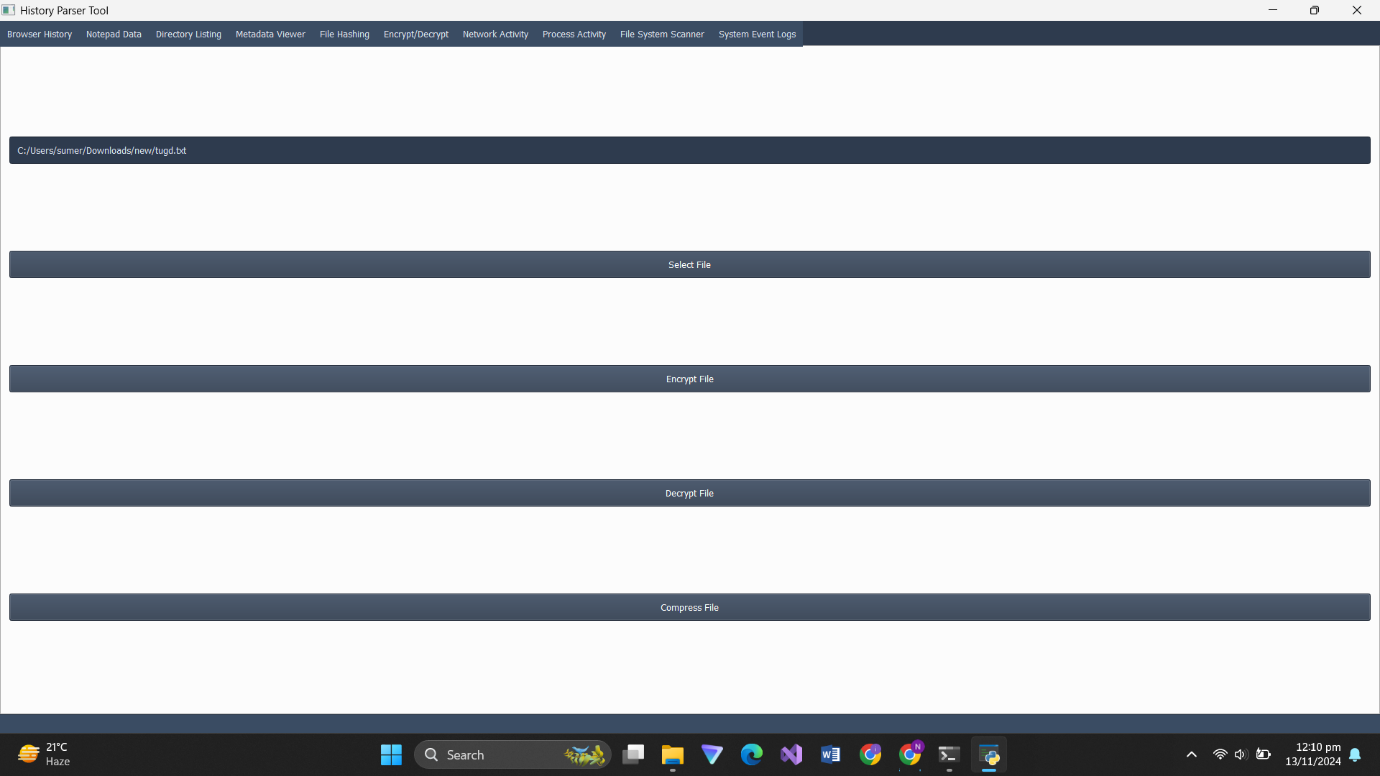


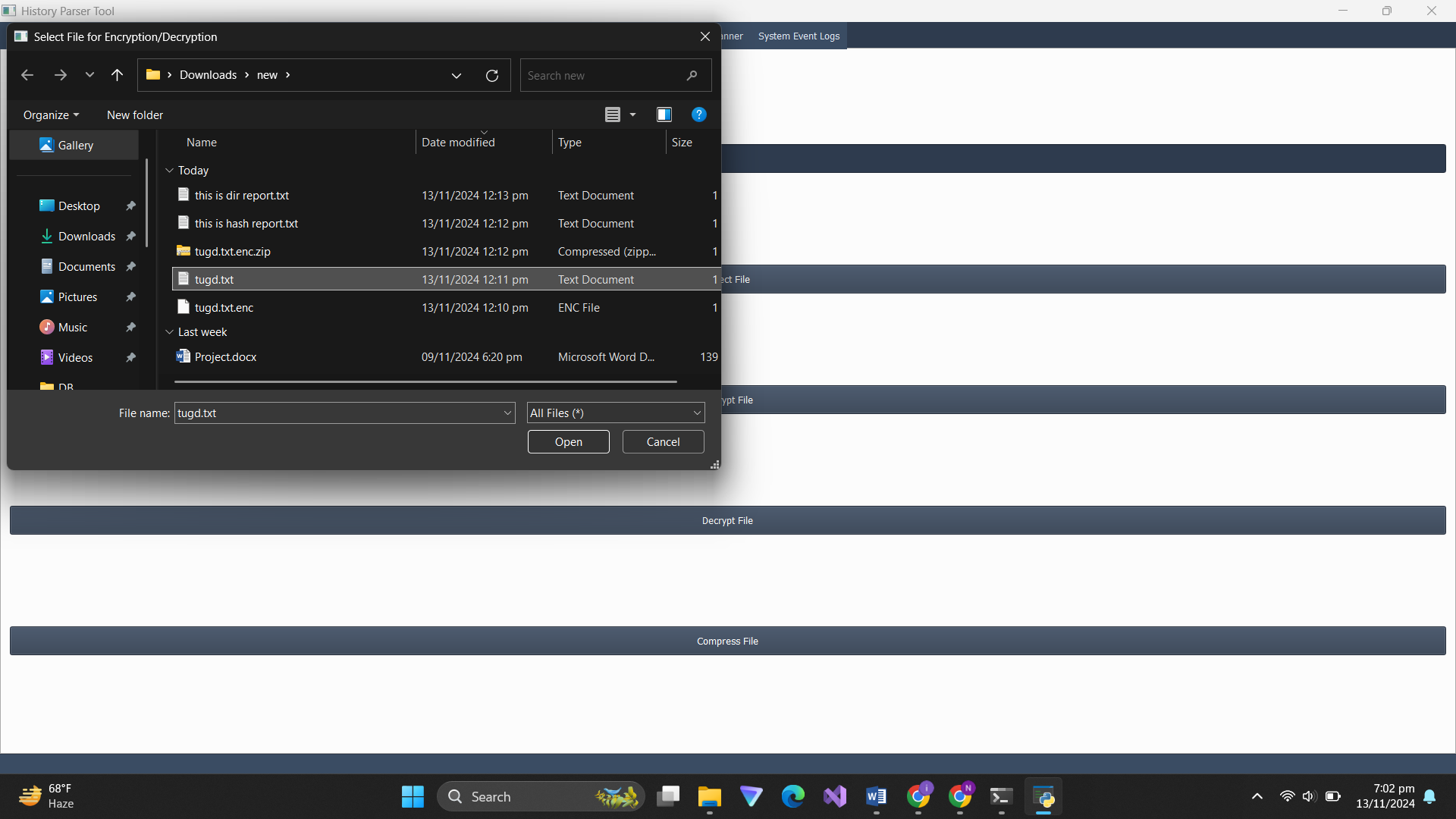
# **File Encryption and Compression:**

The **Encrypt/Decrypt** tab allows users to encrypt files using the **Fernet** symmetric encryption method. Users can also compress files into a ZIP archive.

* **Steps to Use:**
  1. Click **Select File** to choose a file.
  2. Click **Encrypt File** or **Decrypt File** as needed.
  3. Click **Compress File** to create a ZIP archive.

**Screenshot: Encryption Tab**



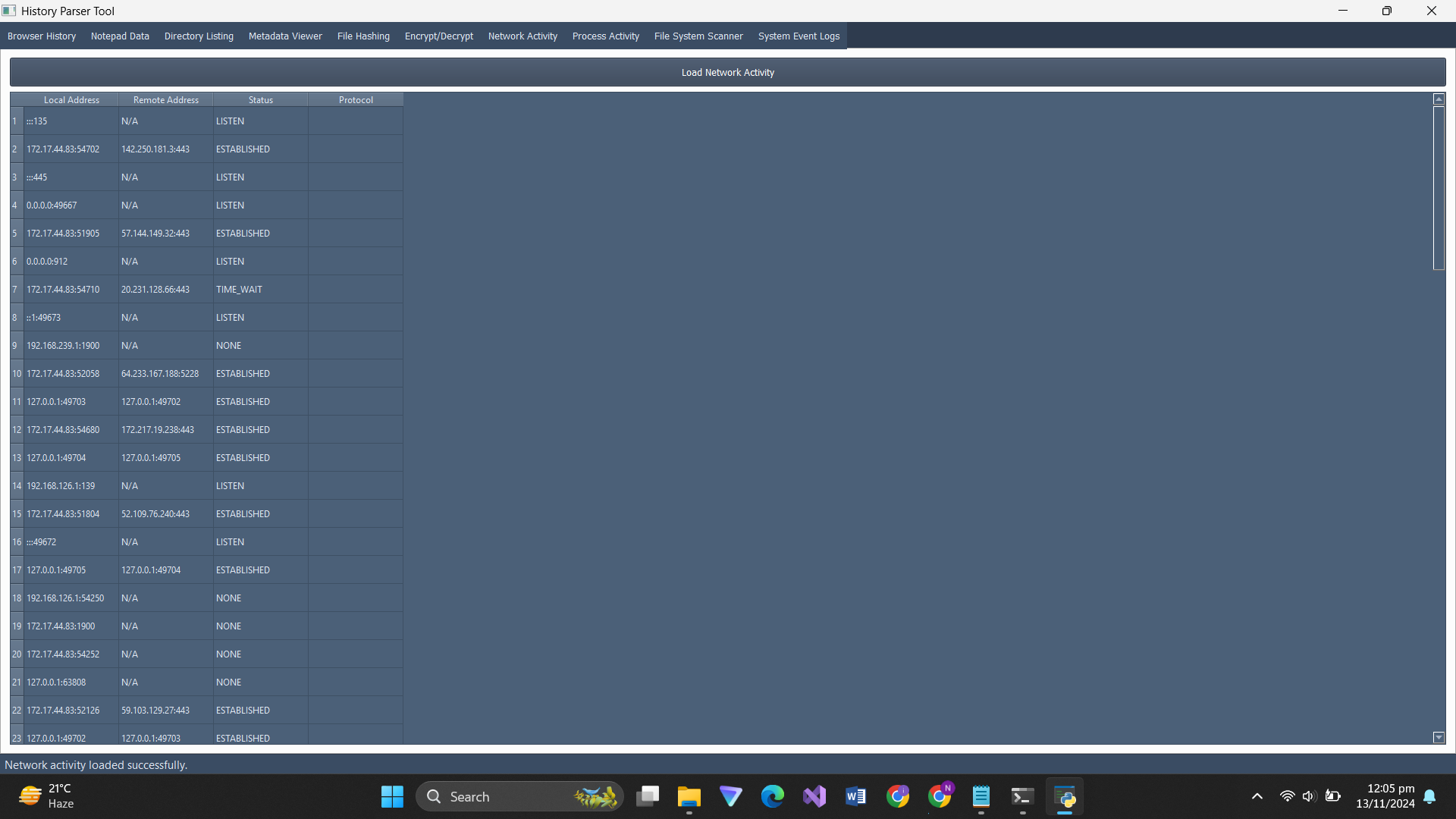


# **Network Activity Monitoring:**

The **Network Activity** tab uses psutil to display active network connections, including local and remote addresses, connection status, and protocol type.

* **Steps to Use:**
  1. Click **Load Network Activity**.
  2. The table populates with information on current network connections.

**Screenshot: Network Activity Tab**

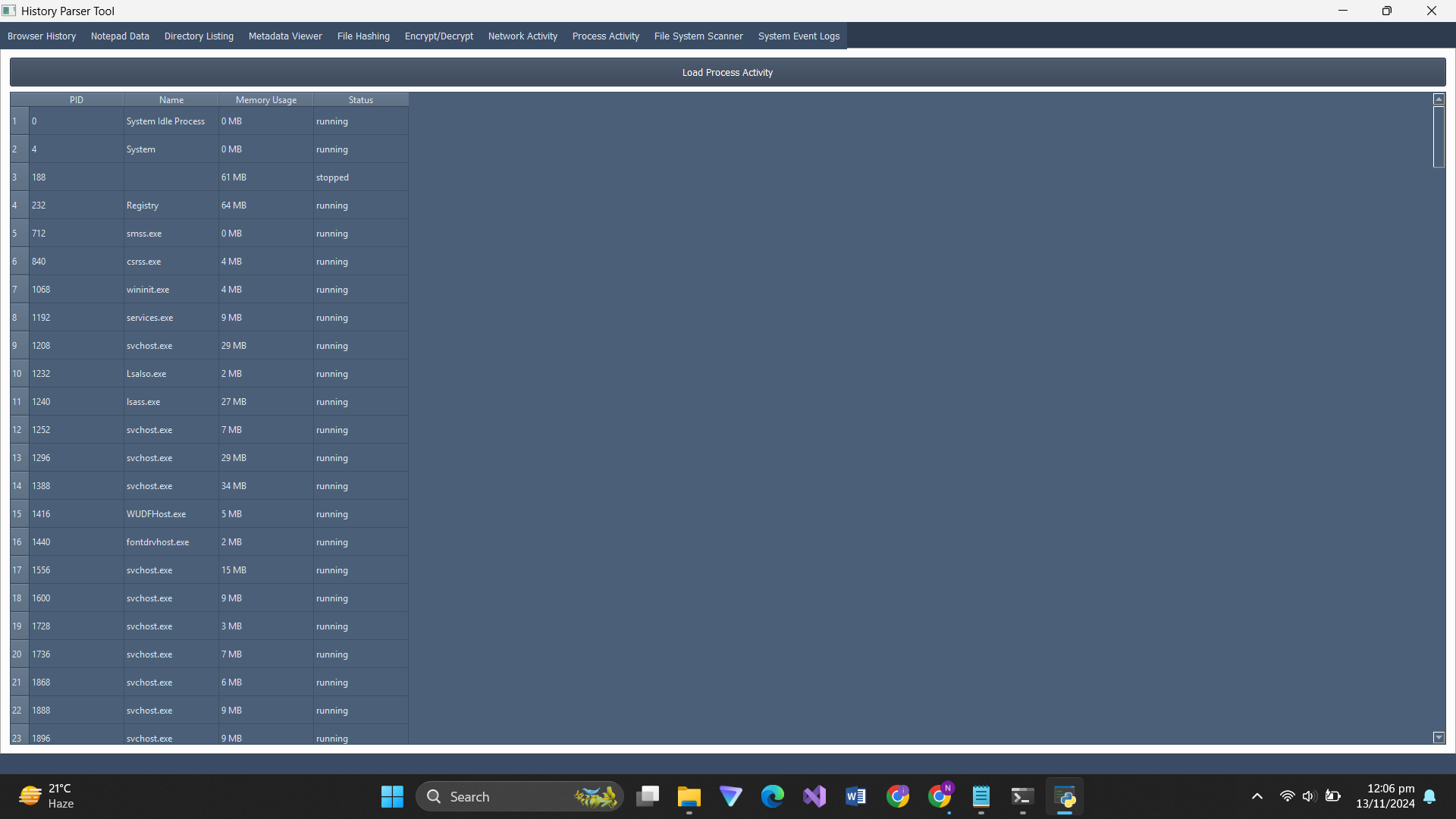


# **Process Activity Monitoring:**

The **Process Activity** tab lists all running processes, showing the process ID (PID), process name, memory usage, and status.

* **Steps to Use:**
  1. Click **Load Process Activity**.
  2. The table displays detailed information about each running process.

**Screenshot: Process Activity Tab**

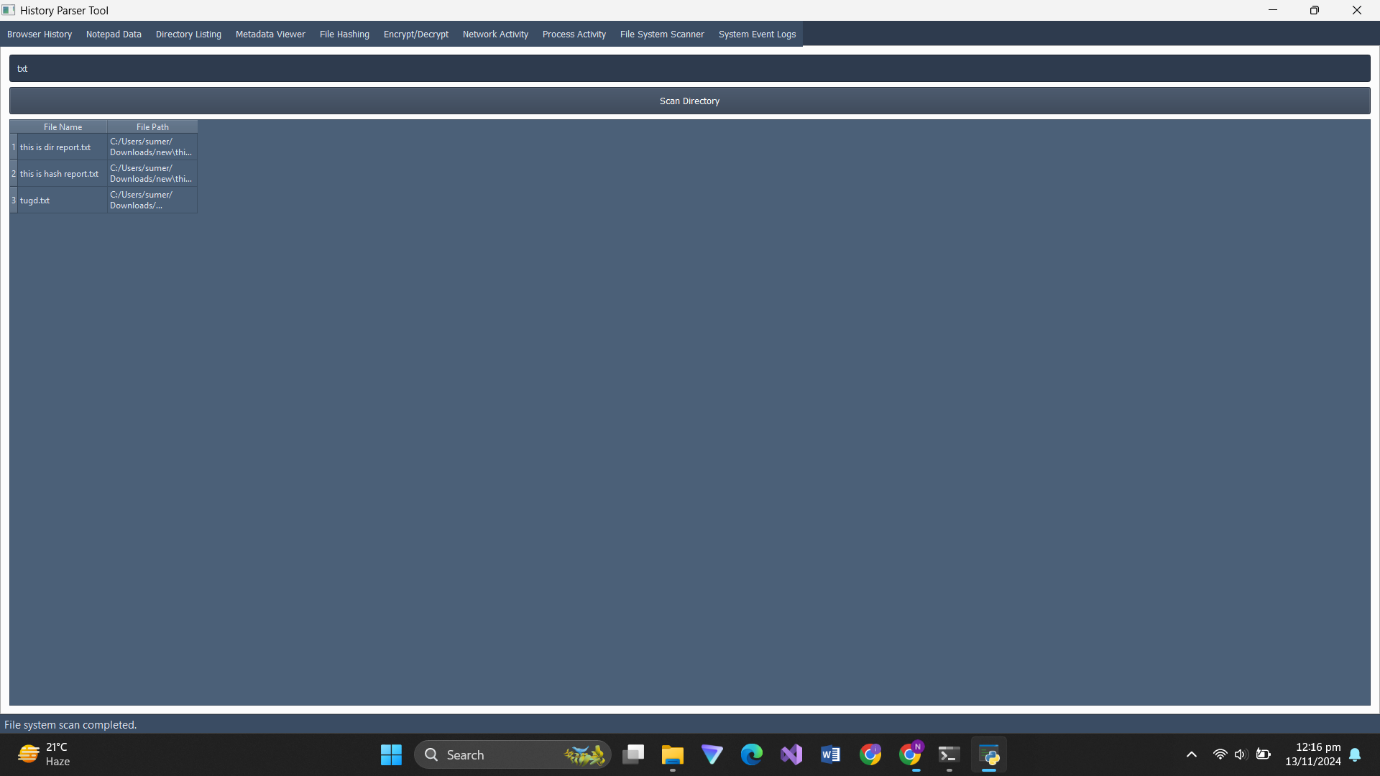


# **File System Scanner:**

The **File System Scanner** tab allows users to search for files with specific extensions in a selected directory.

* **Steps to Use:**
  1. Enter the file extension (e.g., .txt).
  2. Click **Scan Directory** and choose a folder.
  3. The table displays matching files.

**Screenshot: File System Scanner Tab**

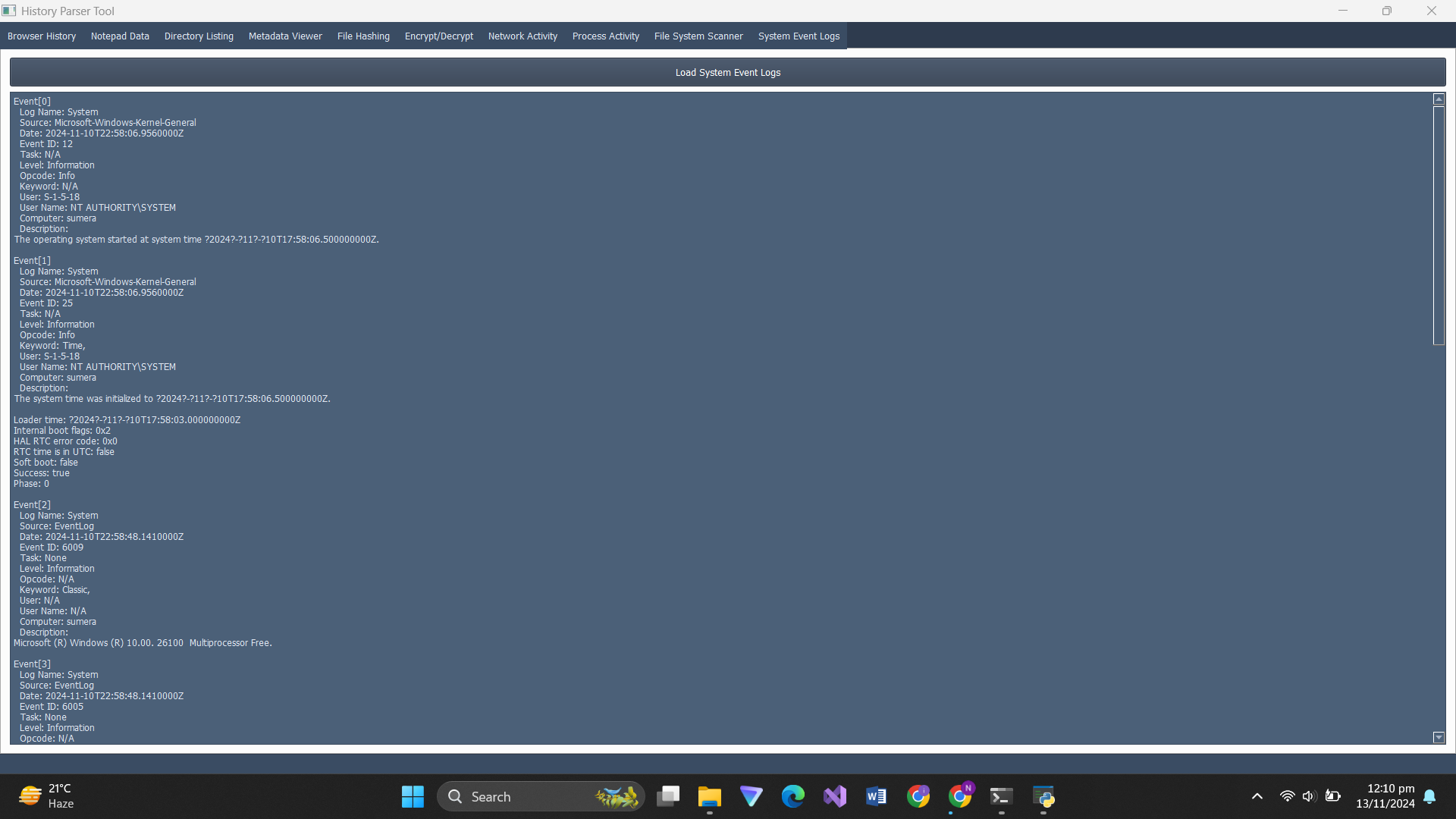


# **System Event Logs Viewer:**

The **System Event Logs** tab retrieves recent system logs using the wevtutil command on Windows. It displays logs in a text box for review.

* **Steps to Use:**
  1. Click **Load System Event Logs**.
  2. Recent system logs are displayed in the text box.

**Screenshot: System Event Logs Tab**



# **Conclusion :**

The **"History Parser Tool"** is a powerful and versatile application for forensic analysis, combining multiple utilities into a single user-friendly interface. Its features facilitate quick and efficient analysis of browser history, metadata, file integrity, and system activity, making it an invaluable tool for digital forensic investigators.

**Future Enhancements:**

* Integration with additional forensic tools.
* Support for parsing additional browser history formats.
* Improved error handling and user feedback mechanisms.