Browsing History and Notepad Parser – User Guide

By Muhammad Musaab (22i1560), Syed Arham Ahmed (22i1552), Muhammad Azan (22i1668), and Muhammad (22i1612)
CY22-B
FAST-NUCES ISB
Digital Forensics under **Sir Mehmood ul Hassan**

Introduction

In the world of Digital Forensics, it is known that there are multiple ways through which evidence may be hidden or abstracted away, one of which is to *not* save content made in a text-editor such as Notepad, so as to avoid creating a file that may be searched and viewed. It is also known that there are often remnant traces of activity that can point to some incriminatory evidence, e.g. the browsing history of a defendant.
Our tool is handy for fetching, compiling, and viewing the **unsaved Notepad content** as well as **Edge and Chrome browsing data** on Windows 11 machines.

Getting Started

Installation

Requirements:

- Windows 11
- Python 3
- pywin32 (python library)
- cryptography (python library)
- sqlite3 (python library for SQL)

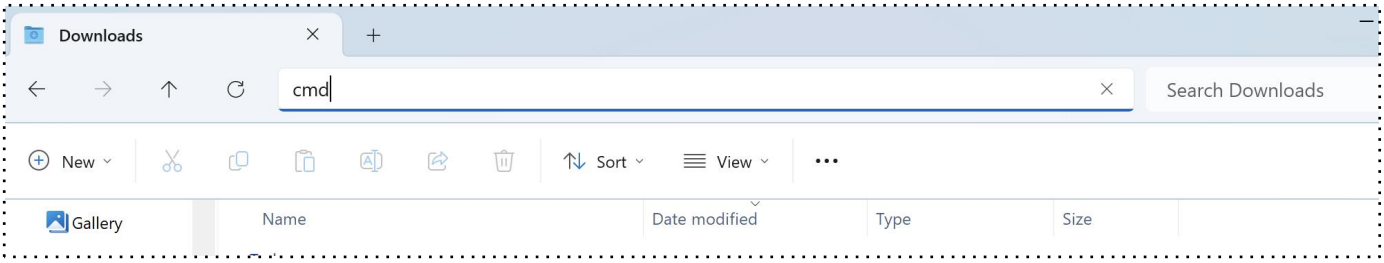
To install the python libraries, open Command Prompt, and enter:

```
pip install cryptography
pip install pywin32
pip install sqlite3
```

For the respective libraries.

Setup

1. Open *File Explorer*
2. Move "**HistoryParser.py**" to a directory of your choice.
3. Go to that directory, click on the **directory-path field** at the top, and enter "cmd" (this should open Command Prompt in that directory)



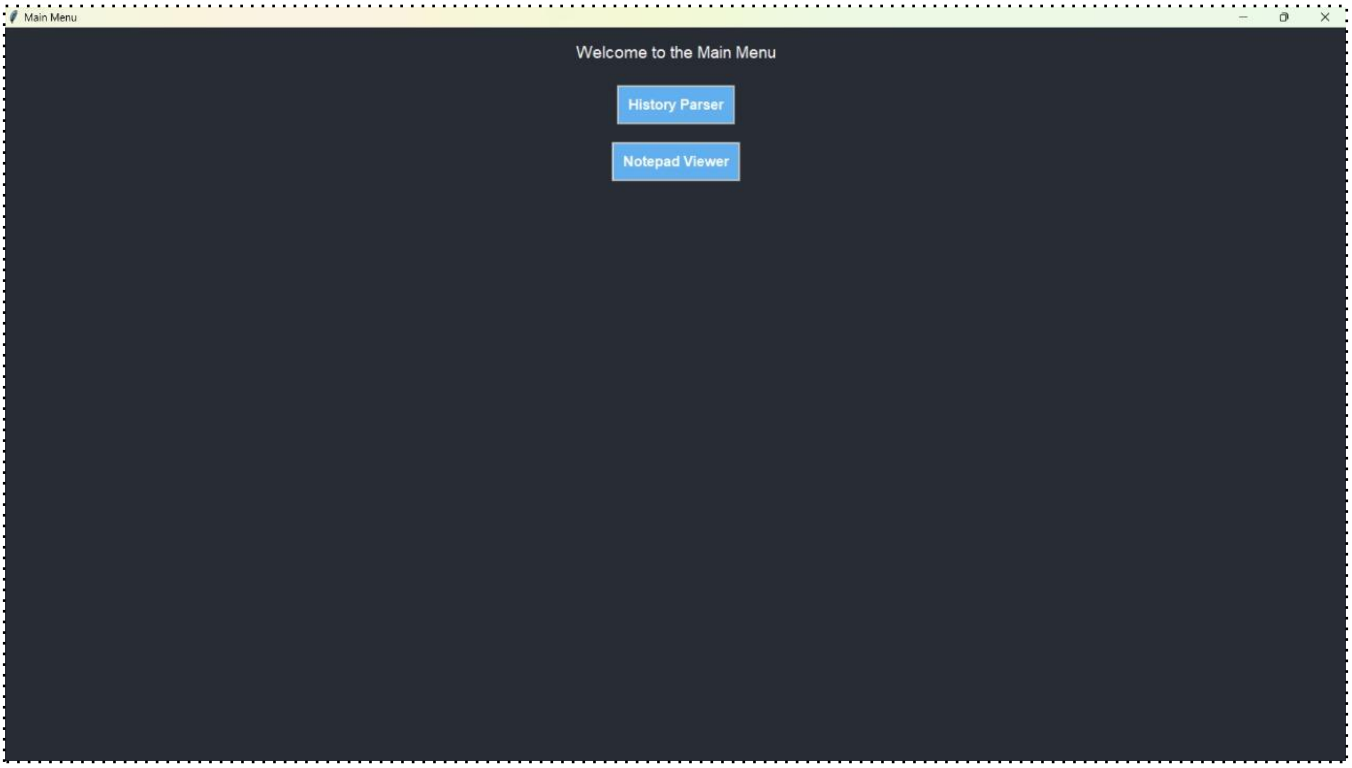
4. Enter "`.\HistoryParser.py`"

A window should open– the tool is now running!

Usage

Main Menu

Upon opening, you will see the main menu with 2 buttons.

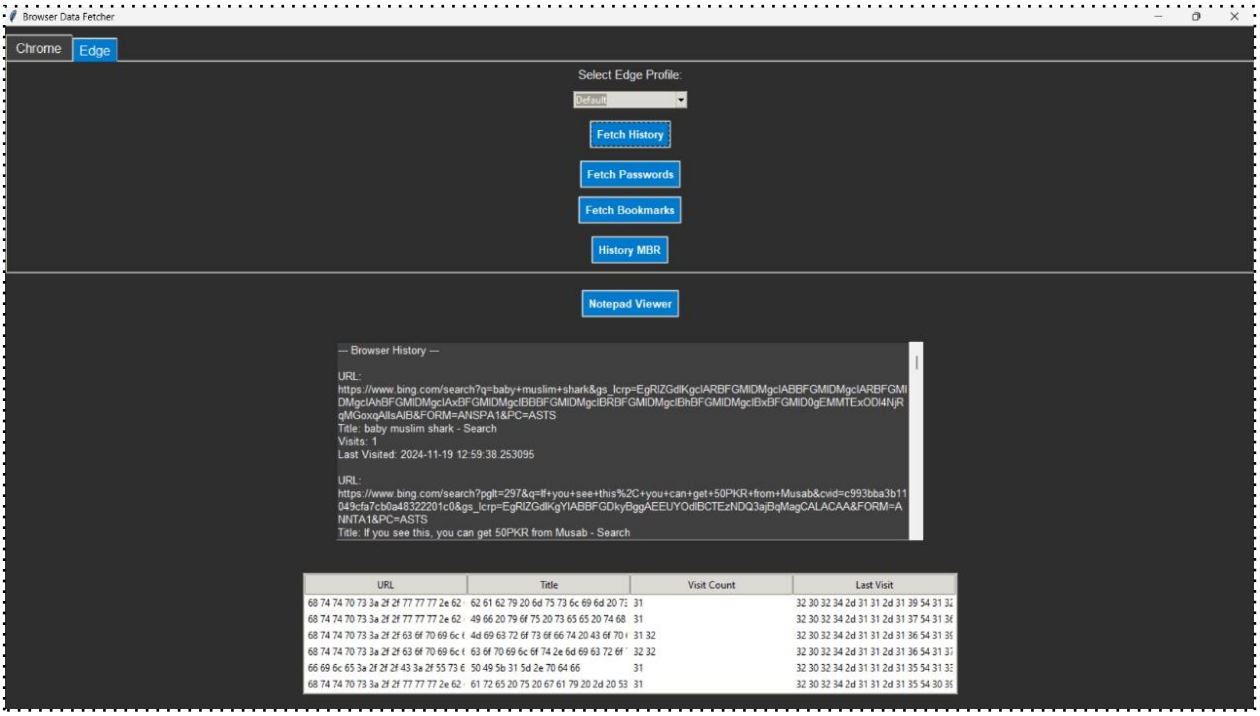


You may click on either “**History Parser**” or “**Notepad Viewer**”.

```
Note: You may safely exit the application at any point by clicking the X at
              the top-right corner of the application window.
```

History Parser

Upon clicking “**History Parser**”, you shall see a window similar to the one shown below:



At the top, there are two tab selectors ("**Chrome**" and "**Edge**") for you to choose the browser to fetch the data of.

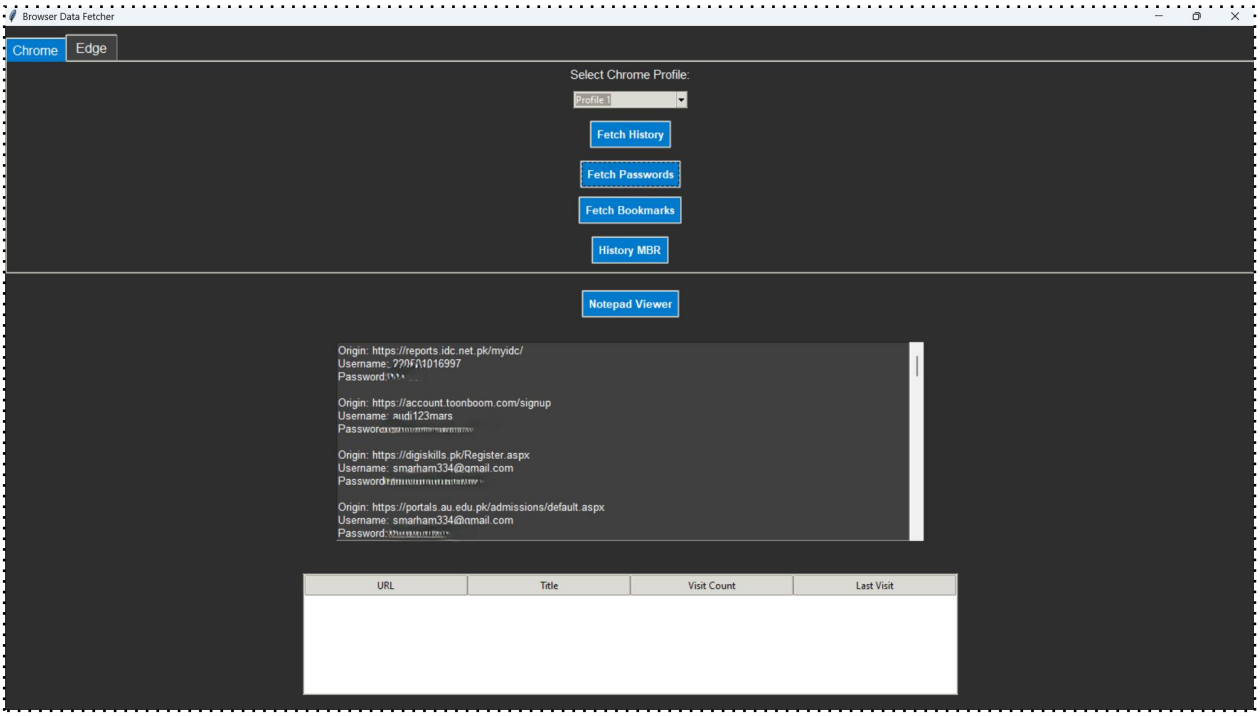
Inside the tabs, there is first a dropdown menu that lets you choose *which user profile*'s data to fetch.

Then there are the following (5) buttons:

1. **Fetch History** - Fetch, process, and display ALL the entries in the browsing history database's URL table. In the dark window immediately below the buttons, the following attributes are displayed (with the **Last Visited** URL entry being first i.e. sorted by newest-first):
    a. *URL*
    b. *Title*
    c. *Visit Count*
    d. *Last Visit Time*

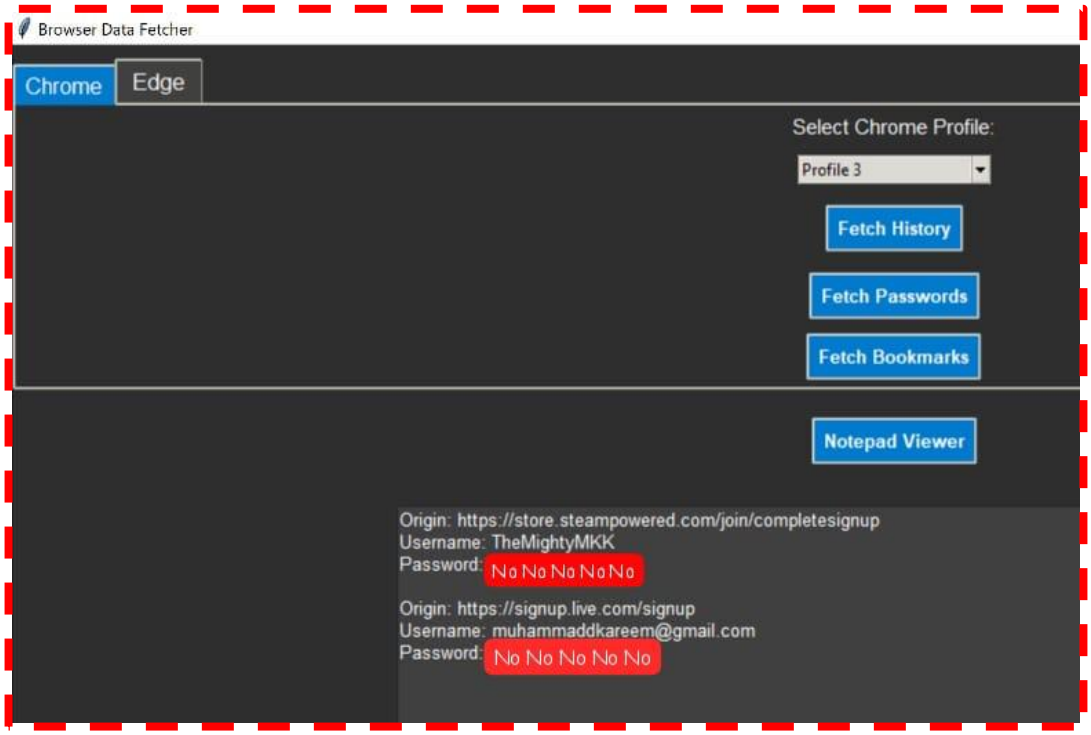
    The hexadecimal equivalents for each of those attributes are also given in the white table at the bottom.

2. **Fetch Passwords** - Fetch and display the login data saved on the browser.

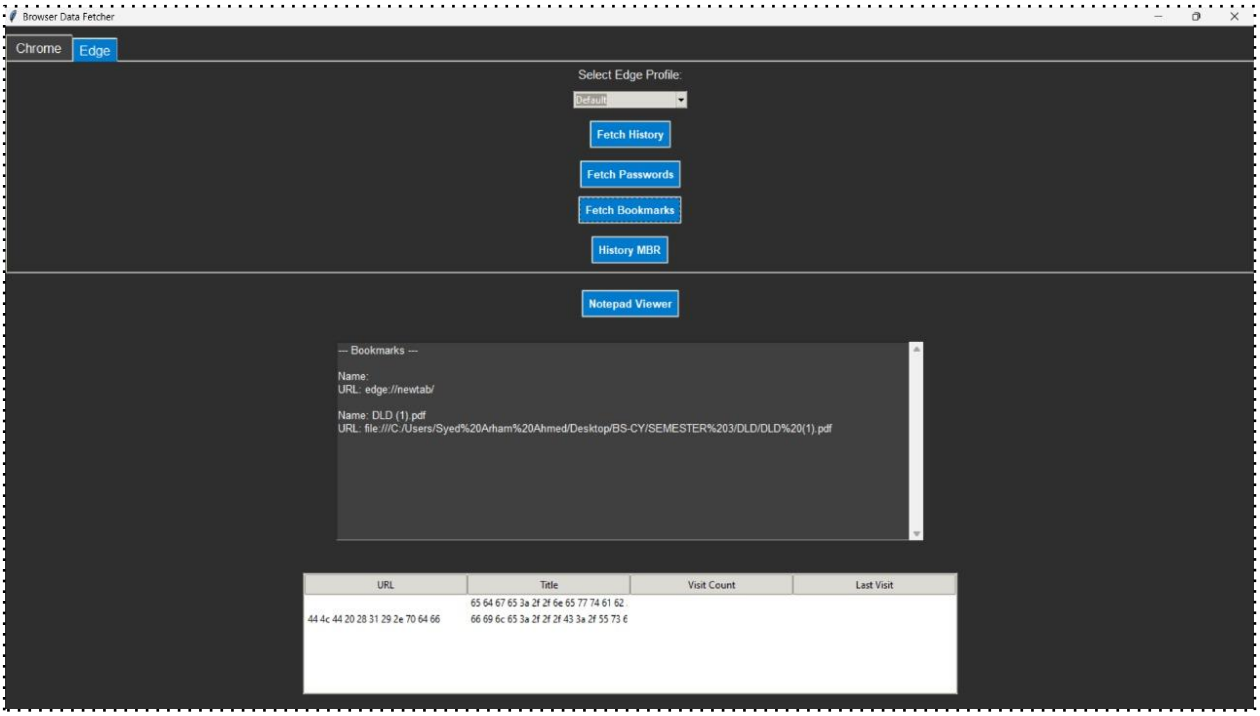


Caution

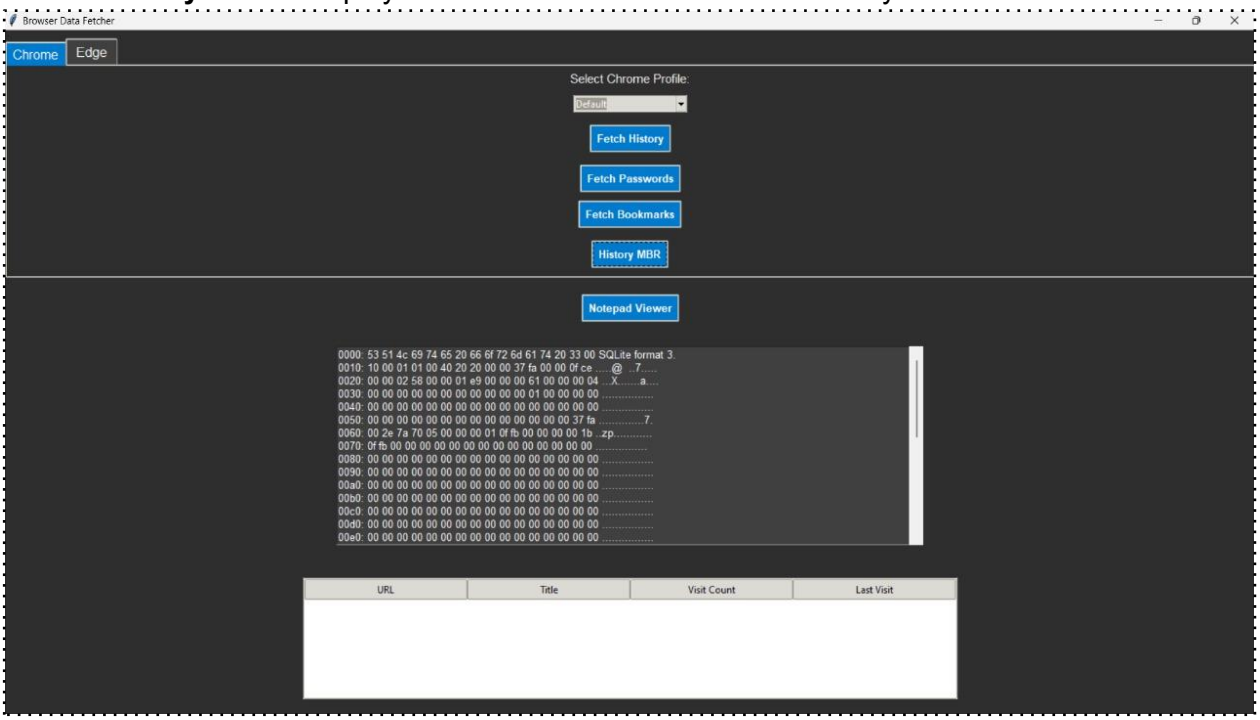
Be careful not to freely share screenshots/copy-pastes of the tools' outputs, as they may contain sensitive information, the sharing of which may be illegal or harmful (to you or to others).



3. **Fetch Bookmarks** - Fetch and display the stored bookmarks.



4. **History MBR** - Display the Master Boot Record of the History database file



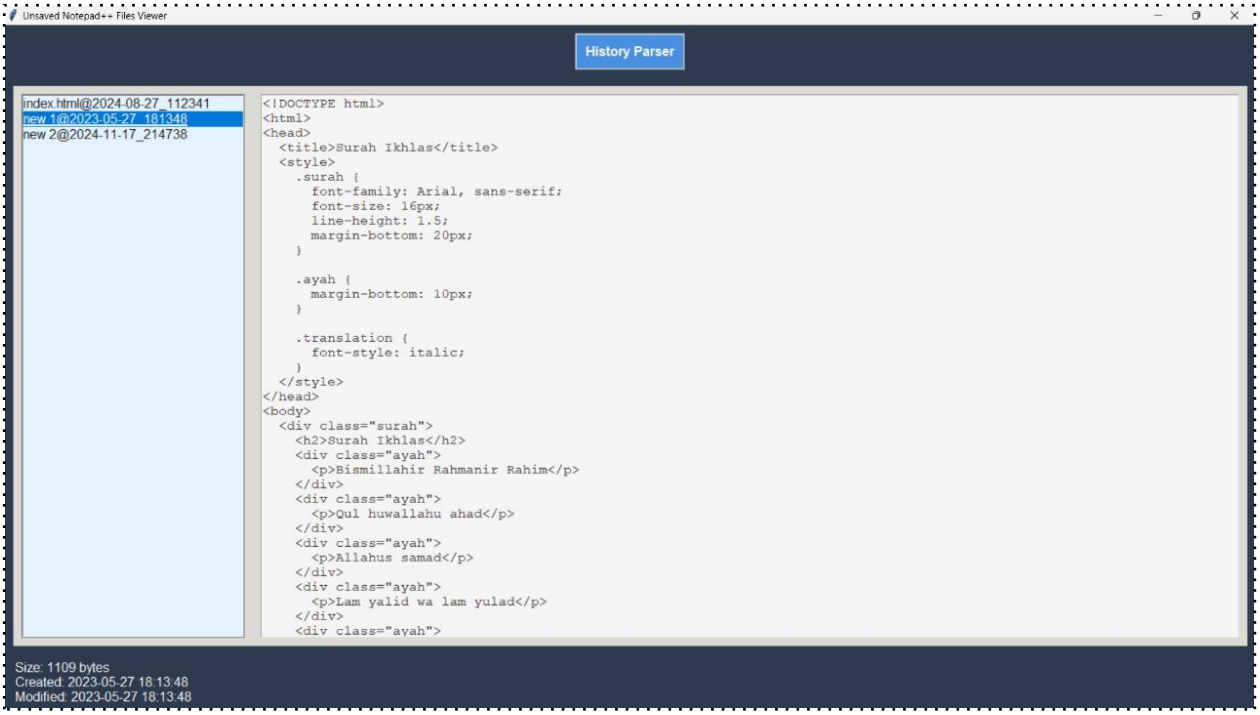
All of these tools for the browser data are *semi-live* — though the window content does not change as the corresponding browsing data changes, you can simply click the button again to *re-fetch* the data.

In other words, the tool **doesn't** {fetch and store ALL data at once when “History Parser” is clicked, then just change according to the user's button-pressing which data is displayed in the window} — it simply fetches *the specific* data new *each time* a button is clicked.

5. **Notepad Viewer** - Switch to the **Notepad Viewer**

Notepad Viewer

Upon clicking “**Notepad Viewer**” a new window will appear, and all the tabs of *Notepad++* will automatically be fetched.



In the **left** sub-window, you can see the **list of the opened tabs**.
Click on the items (i.e. fetched tabs) in the list to open them, then the contents will be displayed in the **right** sub-window.
At the bottom left corner of the window, you will also see the *Content size*, *Created time*, and *Modified time* of the selected tab.

At the top in the window is a “**History Parser**” button that you may use to switch to **History Parser**.
As this tool fetches data automatically upon being opened, it does not update/refresh on its own with changes in *Notepad++*’s content.
To update/re-fetch the Notepad++ tab content: Switch to **History Parser** (click the top button) and then **switch back** (click on “**Notepad Viewer**”).

Troubleshooting

Don't worry, we faced plenty of trouble too. Contact i221552@nu.edu.pk, i221560@nu.edu.pk, or ChatGPT.

FAQ

Q: Does this work on Android?
A: No.

Q: Isn’t this very limited in possible use-cases?
A: Sure, but it can be very, very helpful in the “few” cases it applies.

Q: Is there an easter-egg in this guide?
A: Yes