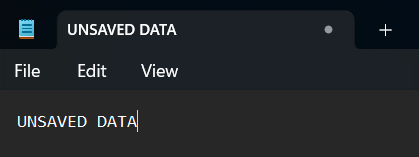
**4/3/2024**

In Windows, Notepad application cache is stored as “<GUID>.bin” files

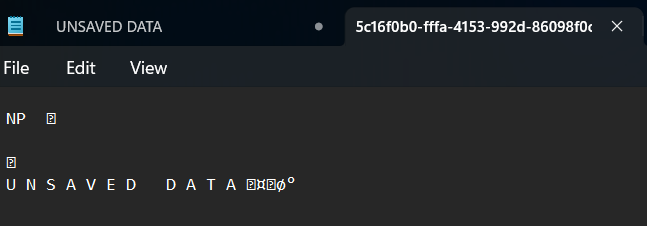
* Directory : C:\Users\josep\AppData\Local\Packages\Microsoft.WindowsNotepad\_8wekyb3d8bbwe\LocalState\TabState
* Even if the file isn’t saved - Data is still displayed (with other odd-ball data)

**Context –** Data just entered into notepad and not saved to any file can be extracted through from cache

Below is an image of data in notepad not saved to any file

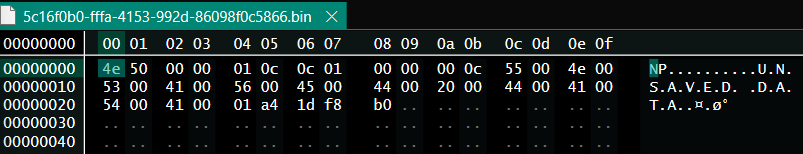


Opening - "C:\Users\josep\AppData\Local\Packages\Microsoft.WindowsNotepad\_8wekyb3d8bbwe\LocalState\TabState\5c16f0b0-fffa-4153-992d-86098f0c5866.bin"

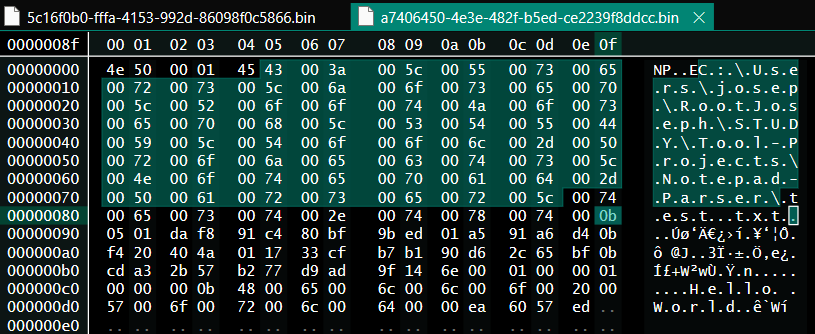
O

**Objective –** Build a script to extract cached data and file information

HEX EDITOR OUTPUT FOR AN UNSAVED FILE ABOVE



HEX EDITOR OUTPUT FOR SAVED FILE



**Length** of actual filename stored in the byte at index 04 (In above image -> hex(45) -> 69

To extract filename -> index 05 + length of filename (divided by 2 -> to account for the alternating null byte

====================================================================================================================================================================

**Extracting data from SAVED&UNSAVED file after closing notepad application**

* There seems to be a starting delimiter after the random bytes “\x00\x01”
* The ending delimiter is of the format “\x01\x00\x00\x00”

NOTE – this is common for both saved and unsaved files

* Between both these delimiters, there is a data marker that is half the length of the text data marker.
  + The text data marker is present at after the “.txt” extension and right before the first byte of text data
* NOTE – The length of the marker varies from one bin file to another, it might differ by file size
  + - To find index of starting delimiter
      * content[0:].index(“\x00\x01”)
    - To find index of ending delimiter
      * content[0:].index(“\x01\x00\x00\x00”)
    - To get file marker contents
      * content[startDelimit+2:endDelimit]
  + To get the starting index of the actual file data
    - content[endDelimit+4+len(fileMarker)]