

LAB 07

Thầy Mai Hoàng Đình
Trường đại học FPT

Người thực hiện

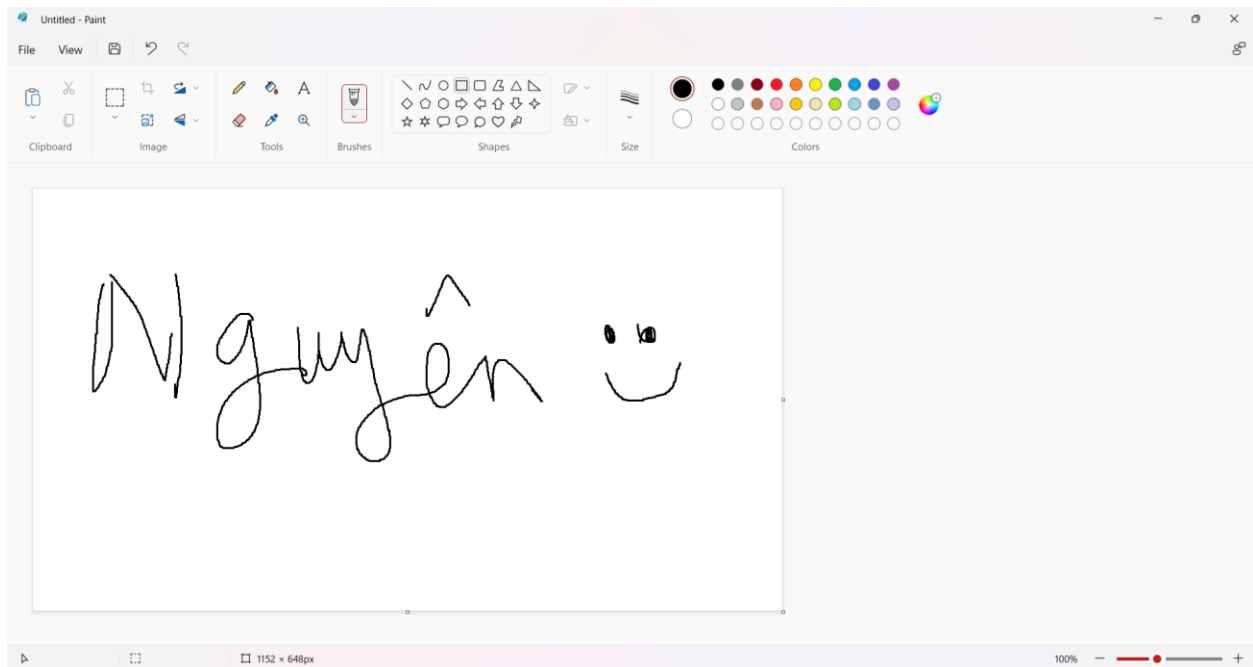
Đặng Hoàng Nguyên

Lab-Project 7: Thumbnail cache

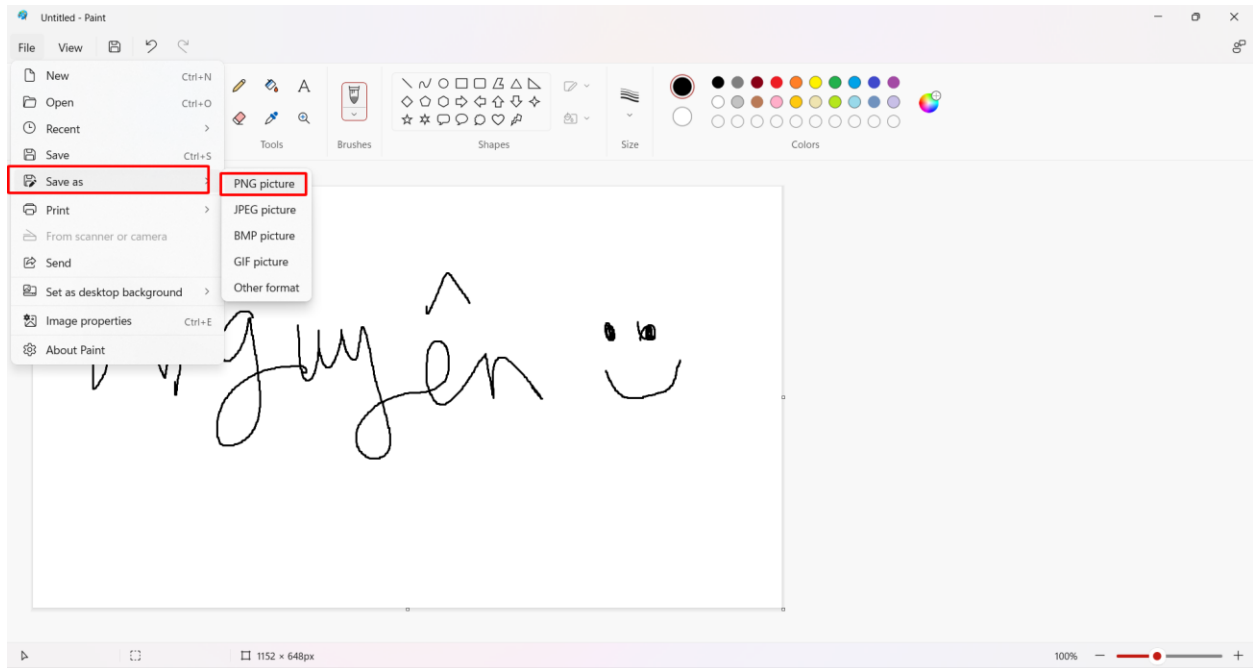
Trong bài lab này, chúng ta sẽ dùng các một trong những máy được list sau đây: Window7, Window Vista, Window2008 server, Windows 10,11. Khuyến khích sử dụng máy Window 7 và Window 2008 server,10,11 , còn thực hiện trên Windows XP thì sẽ không thực hiện được bởi vì file thumbnail của WinXP rất khác so với những máy được nêu trên

Creating Two Test Images

Bây giờ chúng ta sẽ recover ảnh thông qua file bị xóa. Bắt đầu tạo hai file hình sử dụng công cụ **Paint** và ghi tên mình vào trong đó.

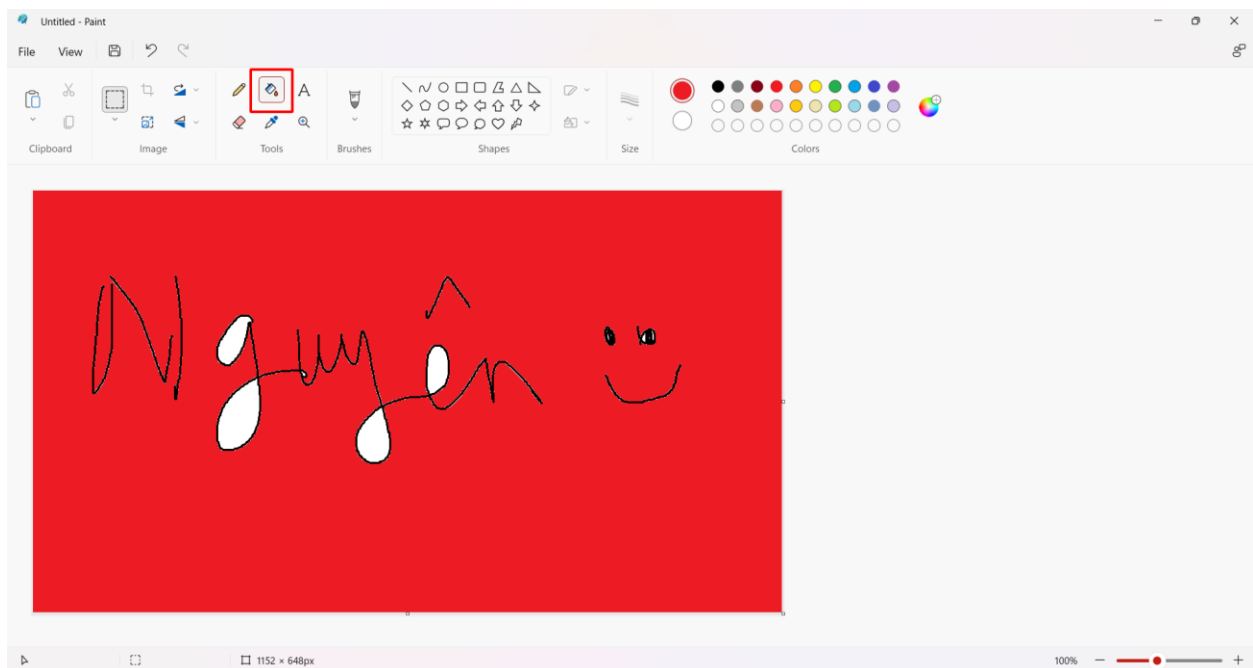


Sau khi ghi tên mình xong vào trong paint, ta tiến hành save file lại với tên **nguyen** ở dưới dạng là một file **png** bằng cách nhấn **File** → **Save As** → **PNG Picture**

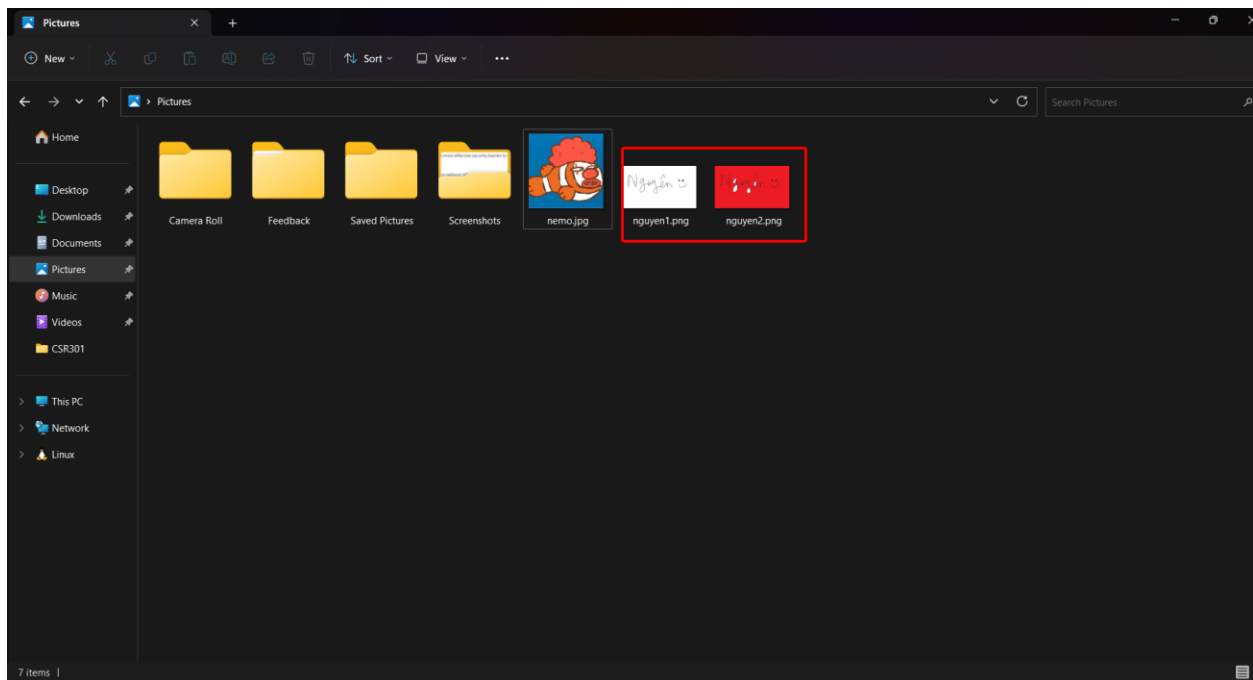


Sau đó chúng ta sẽ nhập thư mục mà chúng ta muốn. Theo trường hợp này, chúng ta sẽ lưu ở thư mục **Downloads** với tên là **nguyen.png**

Tiếp theo sau đó, sử dụng công cụ Fill with Color hỗ trợ trên paint để tạo ra một file khác

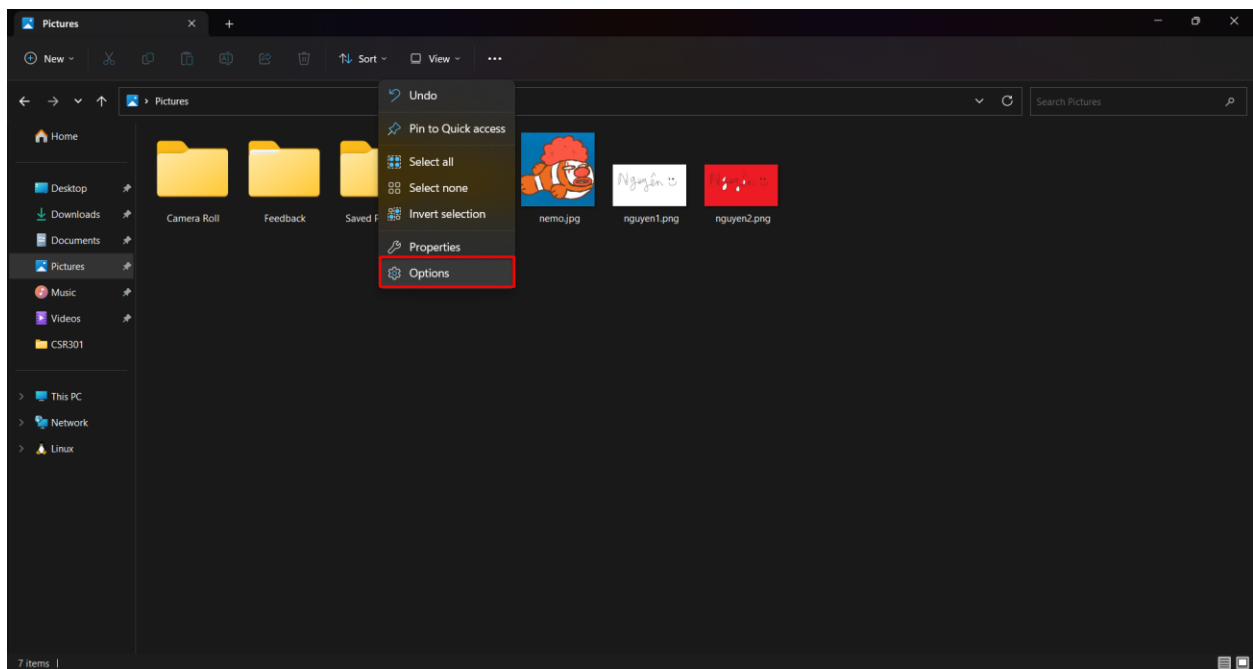


Sau khi tạo xong thì chúng ta cũng sẽ phải save nó dưới dạng png theo như các thao tác hồi nãy. Sau khi lưu xong vào Folder để kiểm tra xem đã lưu chưa. Trong trường hợp này chúng ta sẽ kiểm tra tại thư mục Pictures của user hiện tại



Viewing the Thumbcache Files

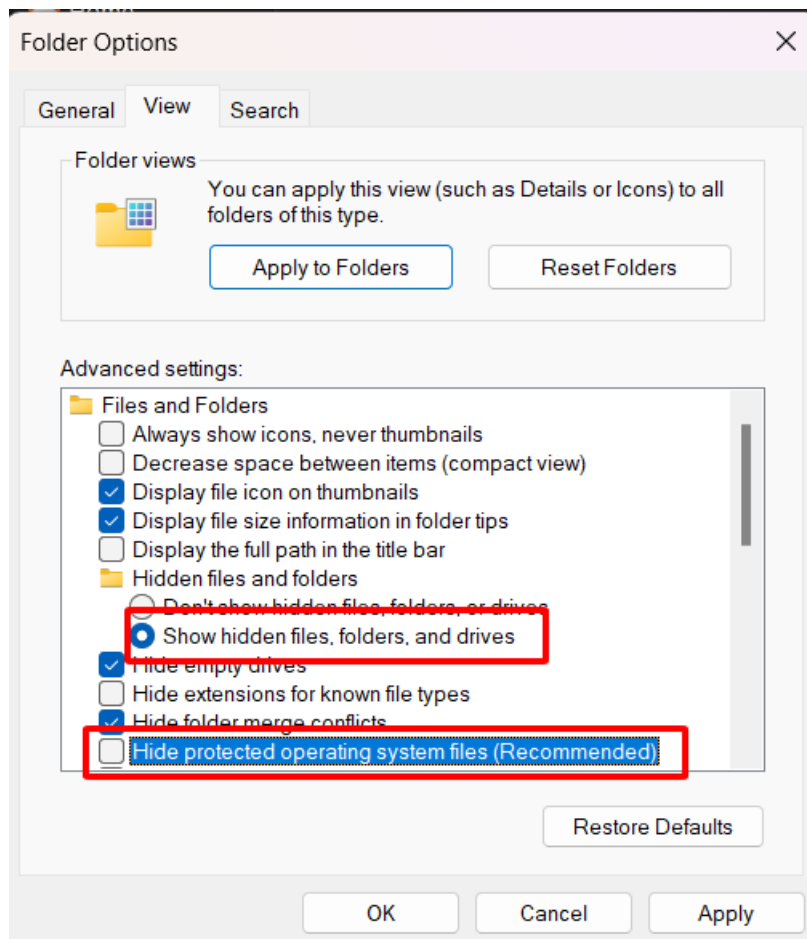
Trong phần My computer của máy, ta vào “...” → Options



Nhấn vào View tab

Chỉnh các thông số sau:

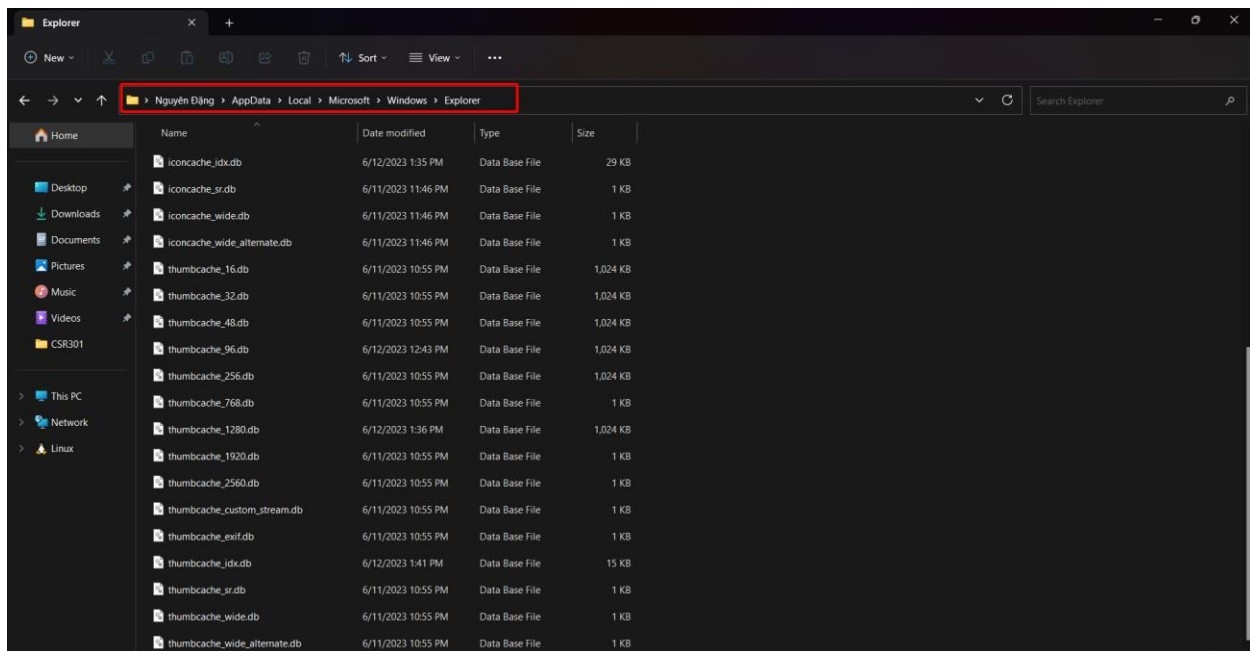
- Nhấn chọn **"Show hidden files, folders, or drives"**
- Bỏ chọn **"Hide protected operating system files (Recommended)"**



Sau đó chúng ta sẽ đổi đường dẫn như sau:

- C:\Users\<your-user>\AppData\Local\Microsoft\Windows\Explorer

Trong trường hợp này là C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer



Getting Thumbcache Viewer

Chúng ta sẽ tải Thumbcach Viewer thoogn qua đường dẫn sau đây:

- <https://thumbcacheviewer.github.io/>

THUMBCACHE VIEWER

[Download Thumbcache Viewer 32-bit](#)

[Download Thumbcache Viewer 64-bit](#)

Version 1.0.3.7
Released on 8/25/2021

[Make A Donation](#)

Please consider making a donation.
Your support is greatly appreciated.

[View project on GitHub](#)

[Check out my other projects](#)

About

Thumbcache Viewer allows you to extract thumbnail images from the thumbcache_*.db and iconcache_*.db database files found on Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, and Windows 11. The program comes in two flavors: a graphical user interface and command-line interface.

Looking to open Thumbs.db files? Try my [Thumbs Viewer](#) instead.

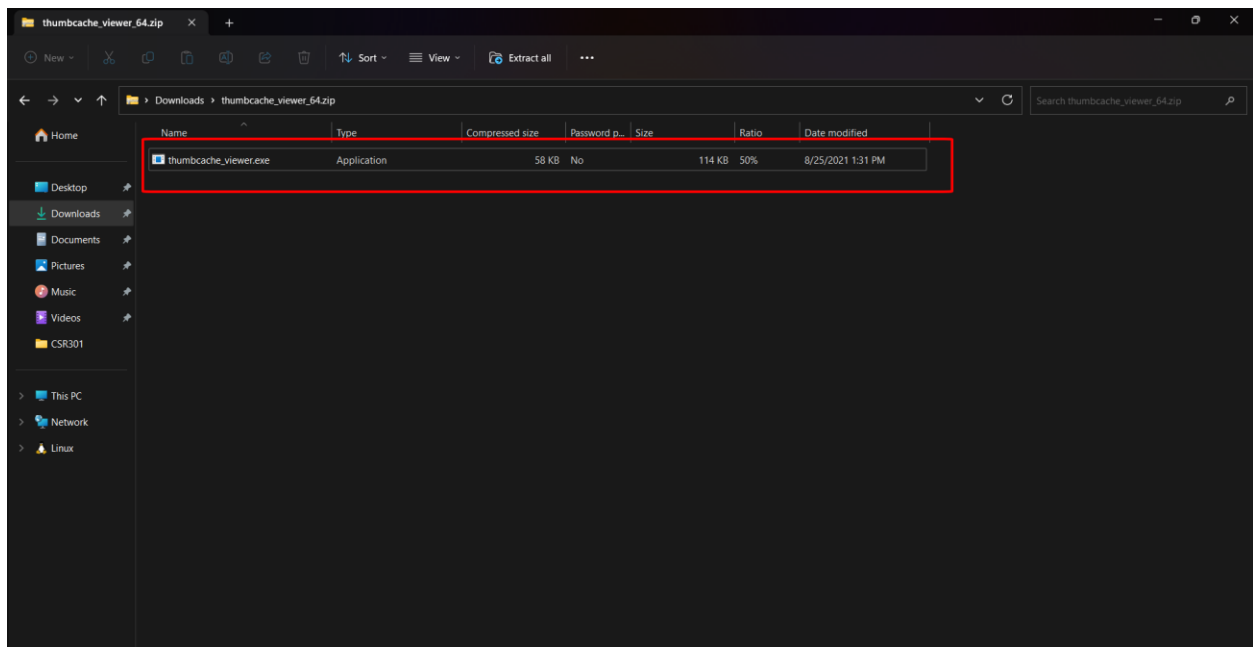
GUI Usage

The main menu will allow you to save entries, export entries to a CSV (comma-separated values) file, remove entries from the list (the database is not modified), hide 0 byte entries, verify CRC-64 header and data checksums, and map files to entry hashes.

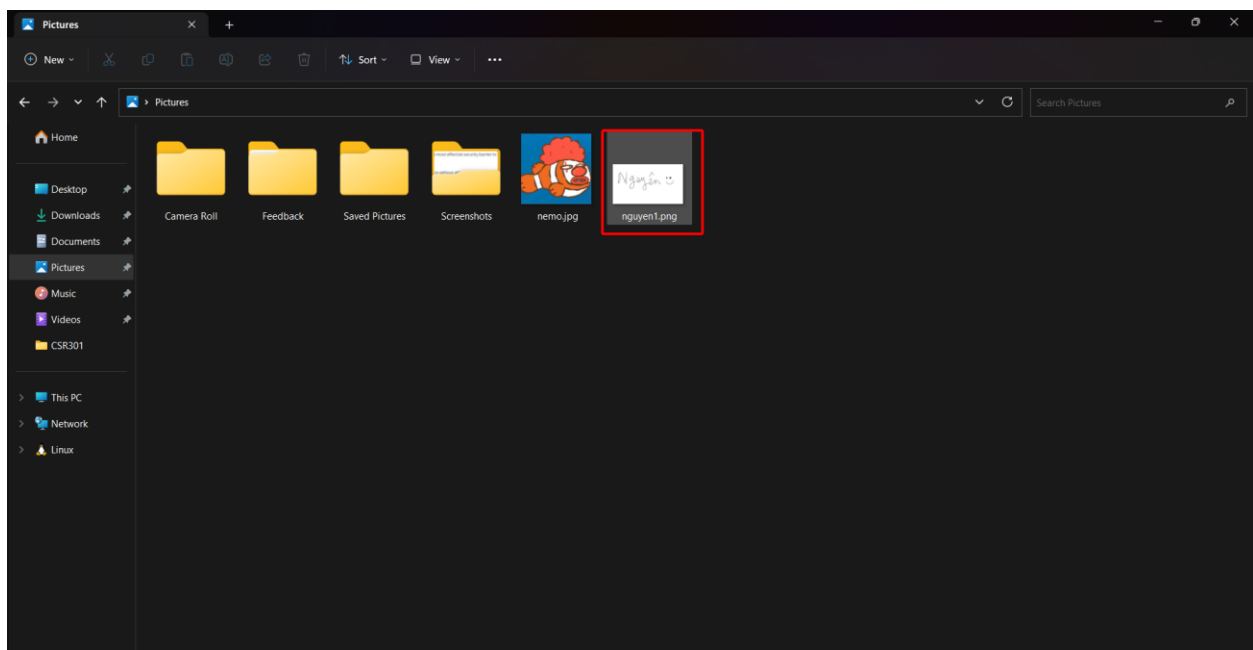
When verifying entries, mismatched checksums will be displayed in red along with the correct value. It's not that common to see unless the database has been overwritten or truncated. Another thing to note is that mapping files by scanning directories must be done on the same computer system in which the database was generated. This ensures that the correct inputs can be hashed to compare against the entry hash in the database. Mapping files using Windows.edb (ESE database) should be done on an operating system that shares the same or newer operating system version in which the Windows.edb was generated. Mapped entries that included extended

Sau khi tải xong chúng ta sẽ vào trong thư mục đã tải nó. Tại đây là Downloads. Sau khi tải xong, unzip nó bằng cách **nhấn chuột phải → Unzip**.

Sau khi unzip xong, double click chọn vào file thumbcache viewer.exe



Sau đó vào bên trong thư mục lưu hai file png ban này, tiến hành xóa hẳn 1 trong 2 file với tổ hợp Shift + delete để xóa hoàn toàn mà không thông qua recycle bin. Như ta thấy ở đây chỉ còn mỗi `nguyen1.png`



Trong `thumbcache_viewer.exe` ta sẽ chọn **File** → **Open** và chọn đường dẫn tới nơi chứa các `thumbcachefile`, sau đó nhấn chọn vào **thumbcache_256.db**

Sau khi hoàn tất sẽ có các file với tên được hiển thị bằng số hexa. Như thế là chúng ta thấy file đã được xem trên `thumbcache`

Thumbnails Viewer

File Edit View Tools Help

#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum
1	738a8addf61713e3.png	105666 B	30 KB	105754 B	30 KB	3d5fc708aff4b1d	a029dde62ef
2	bff4d8387373ac8d.png	68420 B	27 KB	68508 B	27 KB	715f6807627c3fd7	2c57d549a4c
3	1cb4f3608cb50d9f.jpg	161106 B	17 KB	161194 B	16 KB	0bccf30568621840	1926bf2ab9c
4	Windows77cba95647300...	12312 B	16 KB	12428 B	16 KB	b631a58f24417758	4a64885954c
5	df5cb8f3fd1ae6e.jpg	136910 B	14 KB	136998 B	14 KB	e3476533f8deb079	4a59286bf9c
6	285de3c86fa21a0e.jpg	58414 B	9 KB	58502 B	9 KB	a24b7e13d4f661a2	e65c7902c14
7	3b6eac98a5087f.png	96672 B	8 KB	96758 B	8 KB	3cb7c514346103e7	207026a130e
8	23d720cb2eae7e.jpg	24 B	8 KB	112 B	8 KB	53ffcfb910ef37e9	00cf6d1e0e6
9	717ecc356e8e802b.jpg	29016 B	7 KB	29104 B	7 KB	b5768bdeb6ab147fe	879427ea751
10	41efad561a782c51.jpg	37074 B	7 KB	37162 B	7 KB	79da89ea284f81c4	353057ed0b1
11	9e0a66d74e7adaf8.jpg	51182 B	7 KB	51270 B	6 KB	7585e11e1a3facab	13e6926cc7c
12	Windows77cba95647100...	178966 B	7 KB	179082 B	6 KB	8b82af0c9691392d	0e653827ba1
13	3c0296fdd73f6f06.jpg	44622 B	6 KB	44710 B	6 KB	a760c42cc0611684	ebd366c2dc
14	98e14927f78f432b.jpg	156094 B	4 KB	156182 B	4 KB	e7bcb72e9997e2b9	3a03c73712c
15	73d45d0c9109d31d.jpg	151404 B	4 KB	151492 B	4 KB	b0dd391294448bfa	c7efcc7456ef
16	906b6d8ae2794efb.png	186778 B	0 KB	186866 B	0 KB	6429481a3a2546d7	e2c121ed62c
17	a3308f1582d5cfc4	8612 B	0 KB	8700 B	0 KB	0000000000000000	4adaf18dc43
18	66e82c3256dc2b50	8700 B	0 KB	8788 B	0 KB	0000000000000000	3e2ece68a55
19	92b0748b577de47e	8788 B	0 KB	8876 B	0 KB	0000000000000000	10beae94c8c
20	:(645FF040-5081-101B-...	8876 B	0 KB	9012 B	0 KB	0000000000000000	10eaf598cd6f
21	77b52b32c6419519	9012 B	0 KB	9100 B	0 KB	0000000000000000	f345c469d18
22	c52140f93f9fef43	9100 B	0 KB	9188 B	0 KB	0000000000000000	eedc73b1dd
23	6de444de5e0e251	9188 B	0 KB	9276 B	0 KB	0000000000000000	ee62e1f923
24	:(20D04FE0-3A6A-1069-...	9276 B	0 KB	9412 B	0 KB	0000000000000000	c7cb3b353a1f
25	:(F02C1A0D-BE21-4350-...	9412 B	0 KB	9548 B	0 KB	0000000000000000	e75a92d3fa5
26	13aff69035d92ea2	9548 B	0 KB	9636 B	0 KB	0000000000000000	e0e805d263c
27	e8bfcfd9243e34680	9636 B	0 KB	9724 B	0 KB	0000000000000000	9fcacf2a88b
28	7d61eb6902c06163	9724 B	0 KB	9812 B	0 KB	0000000000000000	e514d230c3v
29	51b936996da64625	9812 B	0 KB	9900 B	0 KB	0000000000000000	55701c9f9af
30	d191388e76207b08	9900 B	0 KB	9988 B	0 KB	0000000000000000	96ded62fdeu
31	dbd3b1c7e413705a	9988 B	0 KB	10076 B	0 KB	0000000000000000	d92cf115aa7
32	4602949ef6d83cb0	10076 B	0 KB	10164 B	0 KB	0000000000000000	afdde5df8e05
33	6229f9eae0633717b	10164 B	0 KB	10252 B	0 KB	0000000000000000	23f521eeae1
34	af615b653a527e7f	10252 B	0 KB	10340 B	0 KB	0000000000000000	62e561b77b
35	4e7b6c42c869945	10340 B	0 KB	10428 B	0 KB	0000000000000000	e0e616215v
36	e775449efc95b05	10428 B	0 KB	10516 B	0 KB	0000000000000000	894724b457

98e14927f78f432b.jpg - 256x144