# LAB 05

Thầy Mai Hoàng Đỉnh
Trường đại học FPT

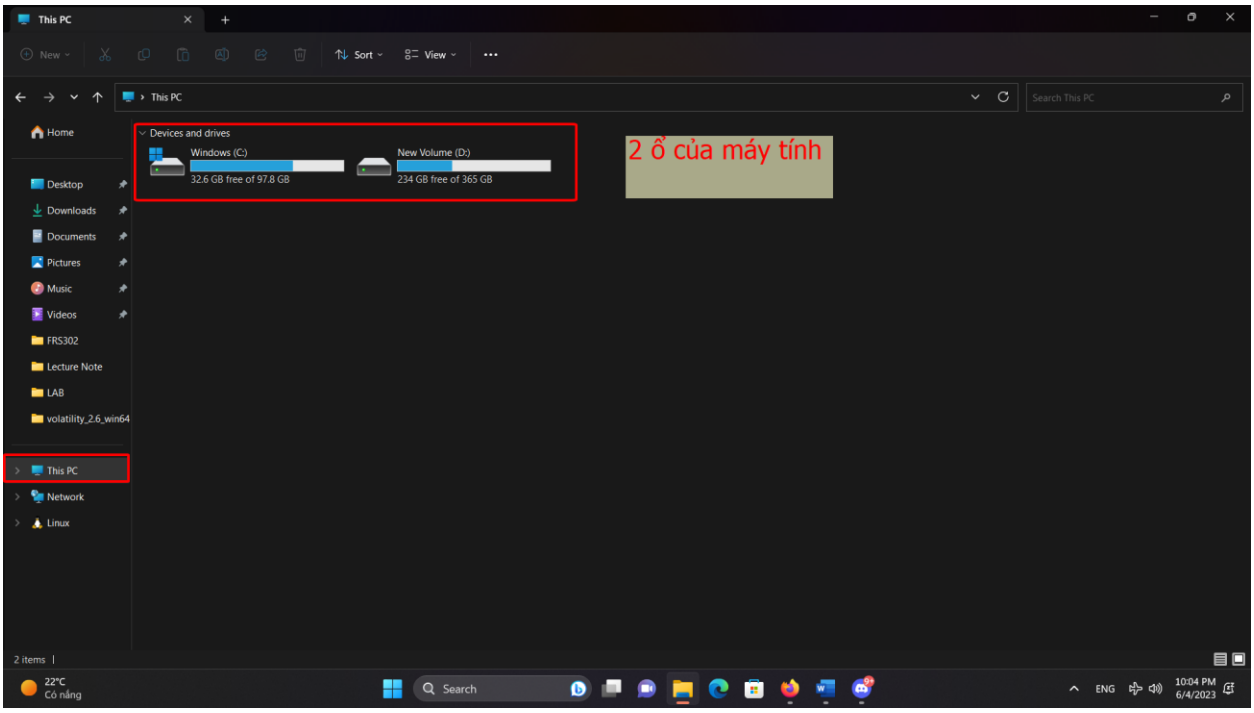
Người thực hiện

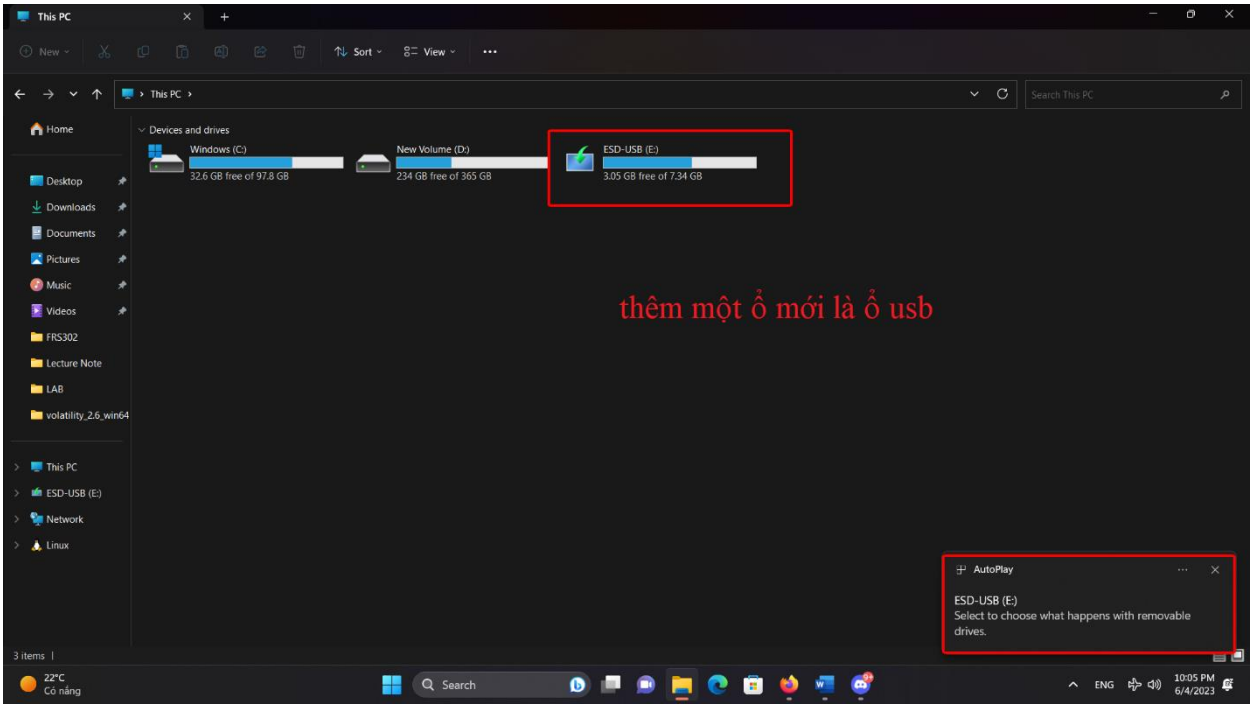
Đặng Hoàng Nguyên

# Capturing and Examining the Registry

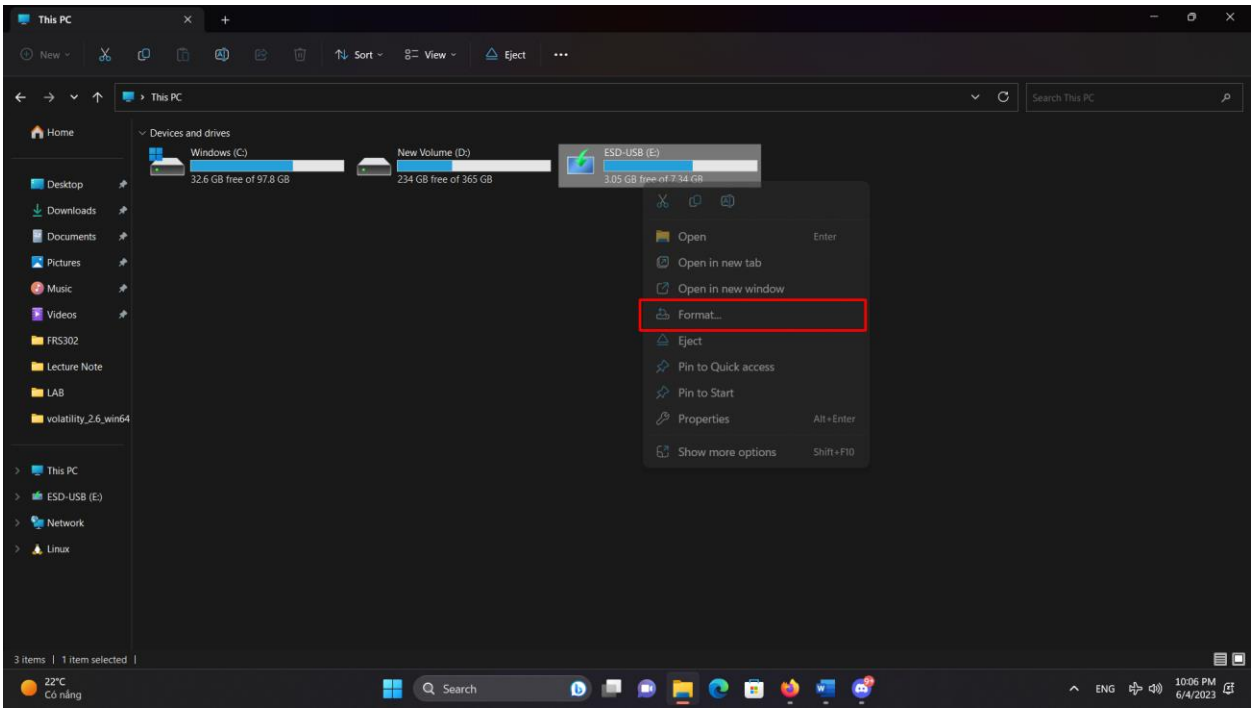
## Connect a USB Device

Bước đầu ta sẽ cắm một cái USB vào bên trong máy, chúng ta có thể check usb cắm chưa qua thông báo hiện trong phần notification hoặc vào bên trong phần Th của máy, nếu hiện ra ổ mới thì đã kết nối thành công.



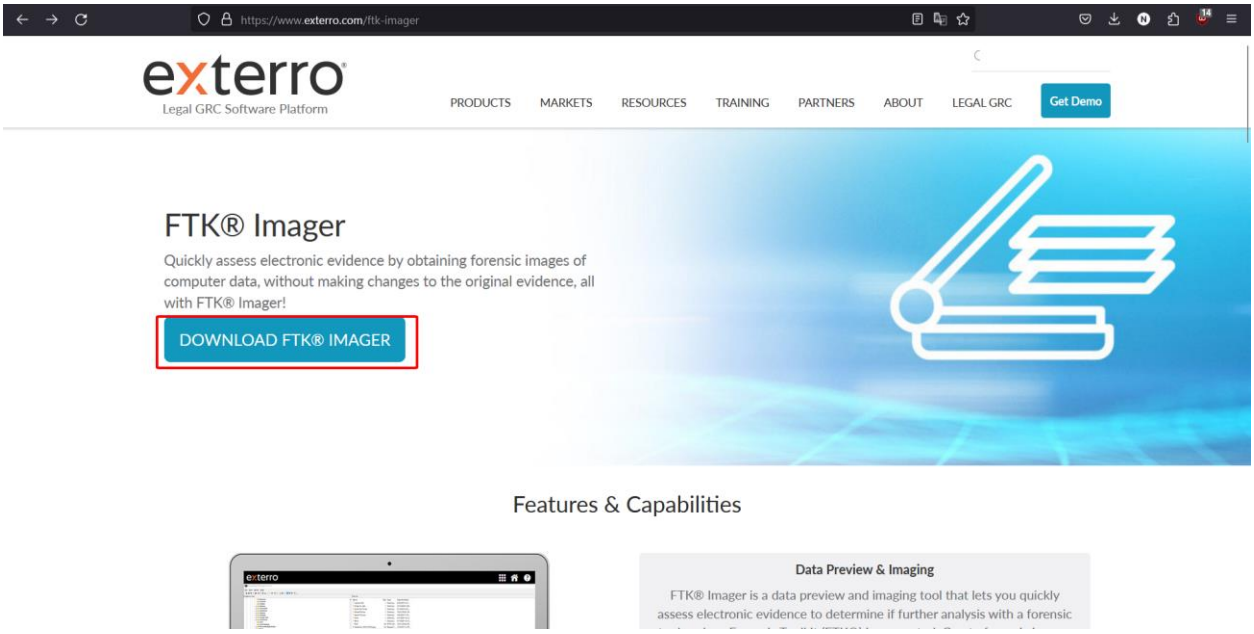



Sau khi kết nối thành công thì chúng ta sẽ eject usb đó ra khỏi máy bằng cách nhấn chuột phải vào phân vùng usb → Eject

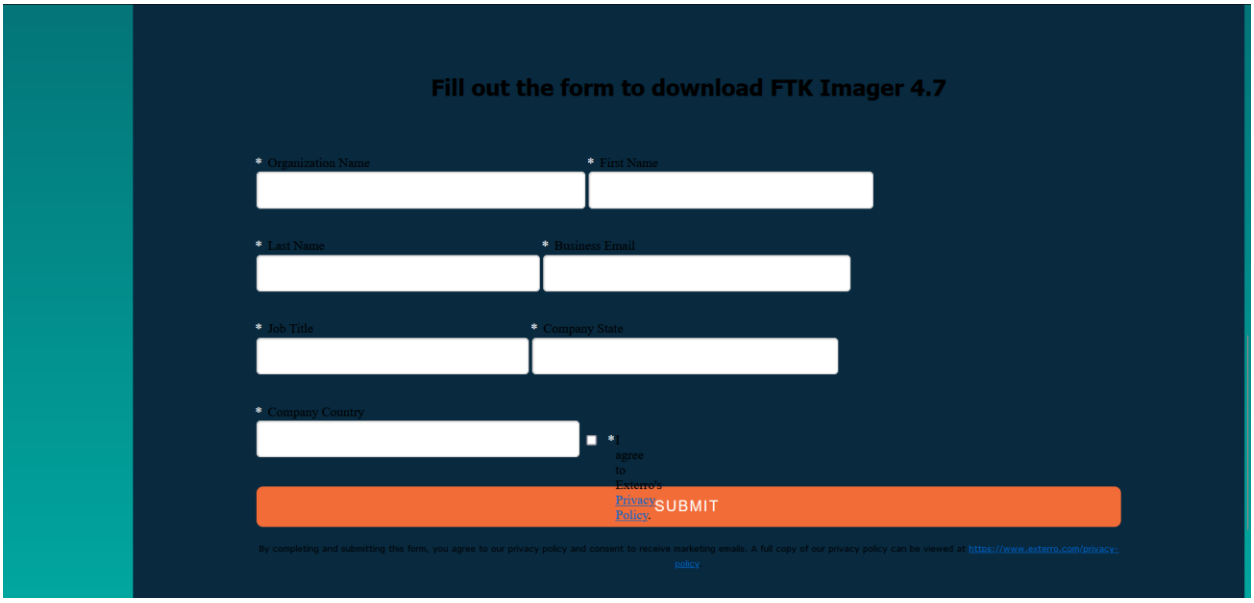



**Downloading FTK Imager Lite**

Sau khi chúng ta đã làm xong các bước trên, chúng ta sẽ tiến hành cài FTK Imager. Link tải tại đây: https://www.exterro.com/ftk-imager



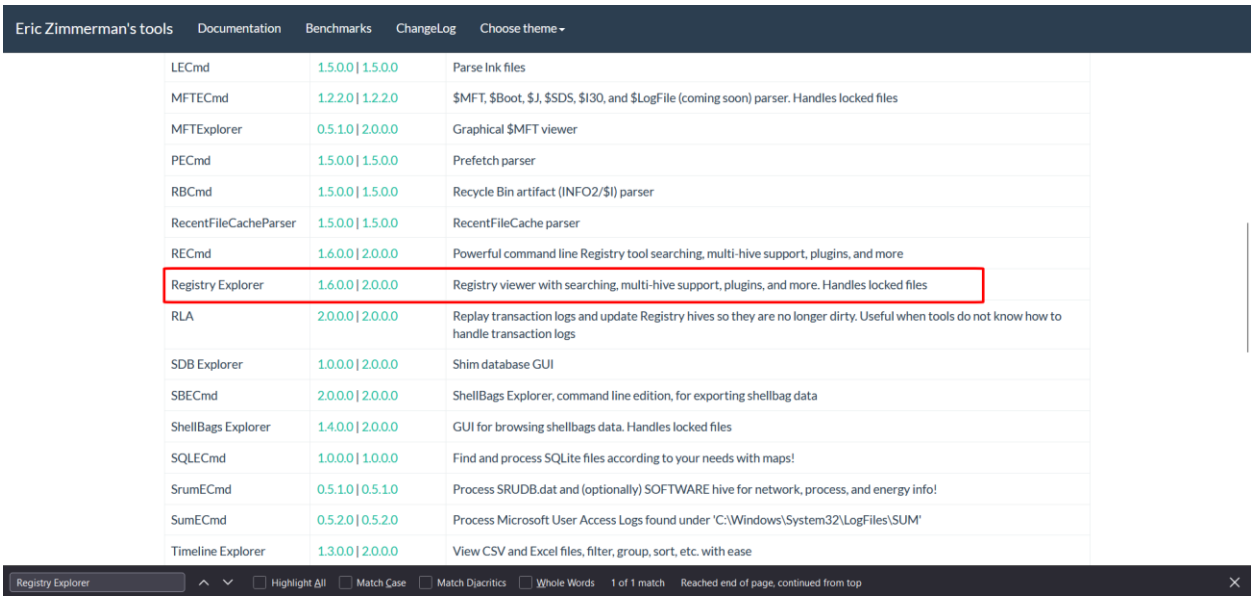

Sau khi nhấn xong, chúng ta sẽ điền những thông tin cơ bản của chúng ta vào để có thể download được FTK Imager




## Downloading Registry Explorer

Bây gwof chúng ta sẽ tiến hành download registry Explorer thông qua trang web sau: **https://ericzimmerman.github.io/#!index.md**

Kéo xuống và tải **Registry Explorer**. Chúng ta có thể tải 1 trong 2 bảng 1.6 hoặc 2.0. Trong trường hợp này em sẽ tải banr 2.0 cho mới.

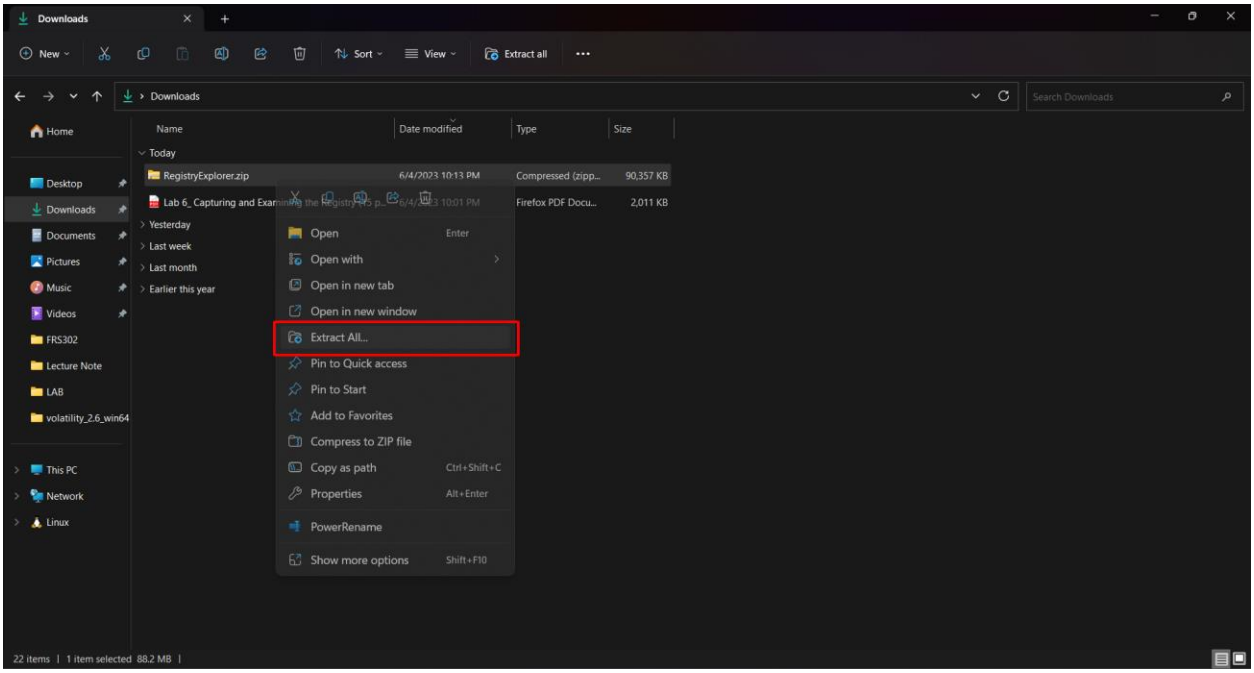



## Unzipping Registry Explorer

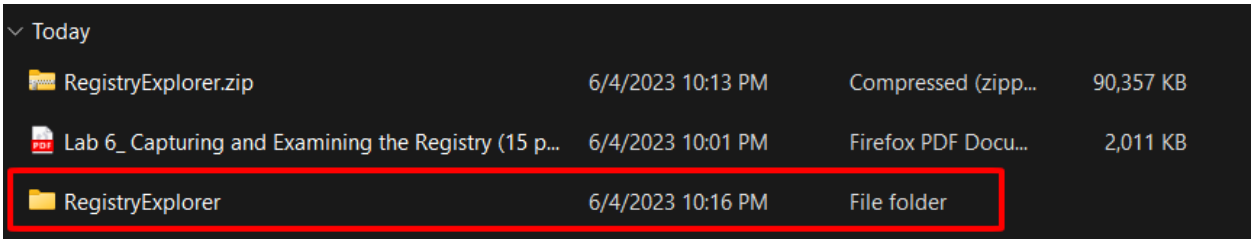
Sau khi tải xong, nó sẽ là một file zip, ta sẽ tiến hành unzip chúng, có thể dung công cụ hỗ trợ của Windows là File Explorer để có thể unzip hoặc chỉ cần dung Winrar là có thể unzip được

Vào trong thư mục mà ta download file zip

Chuột phải rồi nhấn **Extract All..**

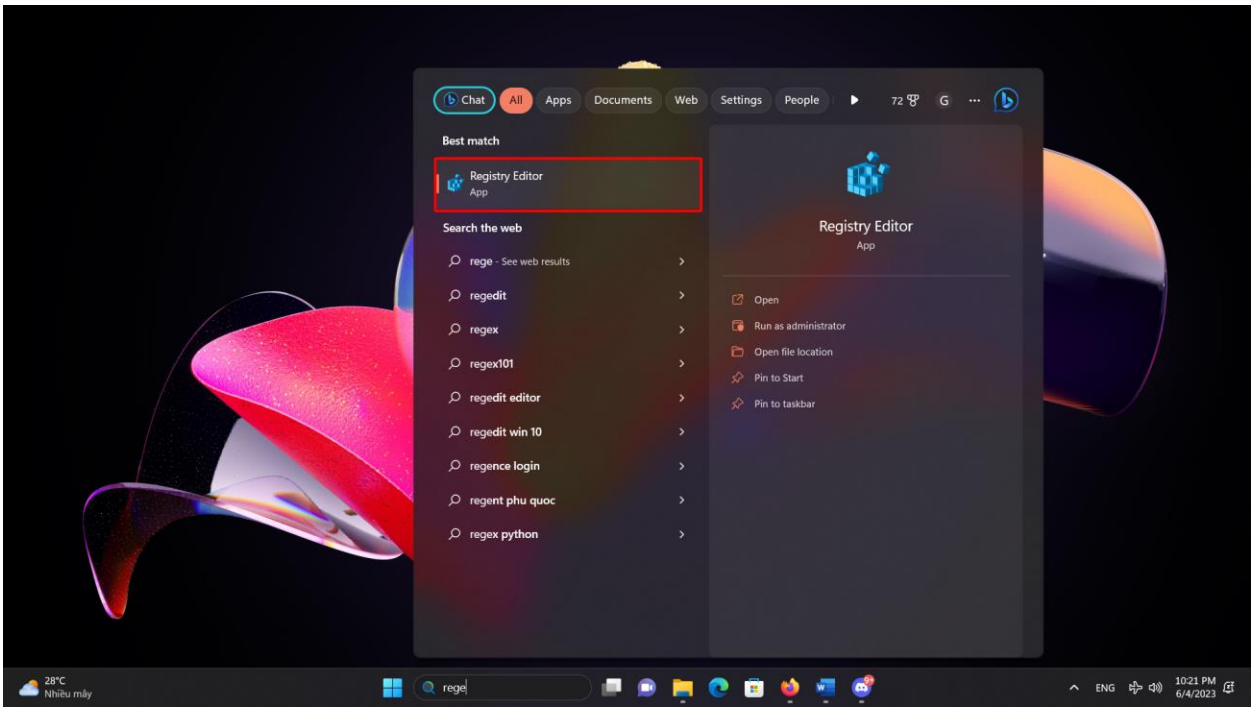



Sau khi giải nén thành công thì chúng ta có một file được gọi là RegistryExplorer

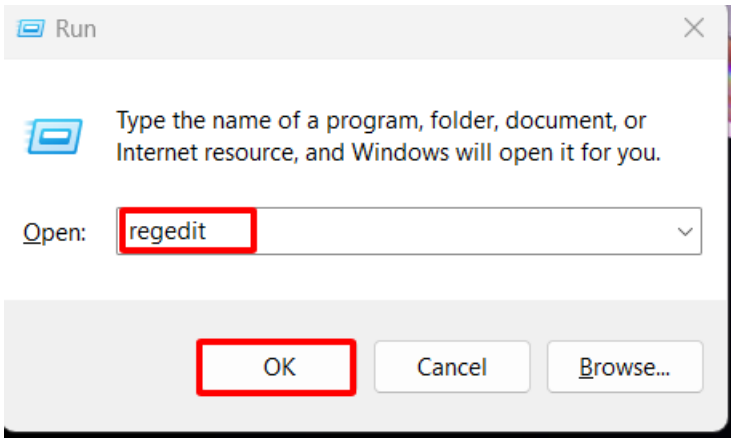



## Viewing the Hive Files

Nhấn biểu tượng **Windows** trên bàn phím hoặc trên màn hình window để hiện ra thanh Search. Sau đó search từ sau: **Regedit editor** sẽ hiện kết quả như sau

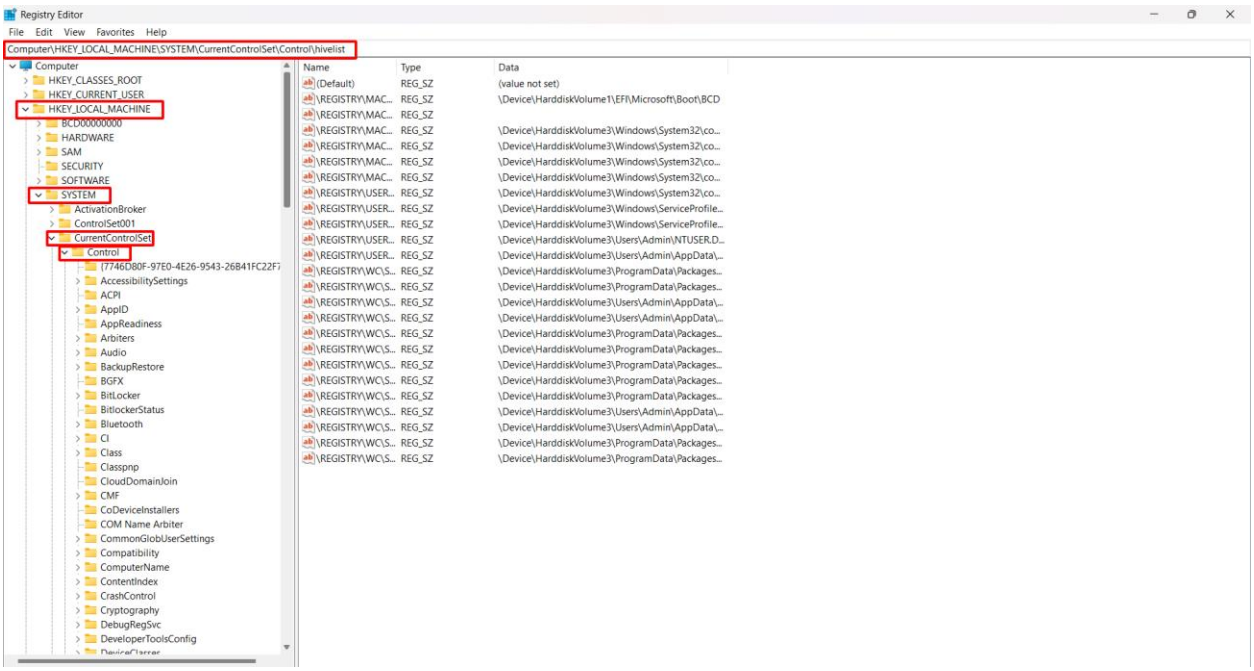



Hoặc đơn giản hơn nhấn tổ hợp phím **Ctrl R** để hiện ra hộp Run, sau đó nhập vào **regedit** rồi nhấn ok




Trong **RegistryEditor** bên thanh bên trái, chúng ta sẽ chuyển tới Folder sau đây:

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\HiveList**

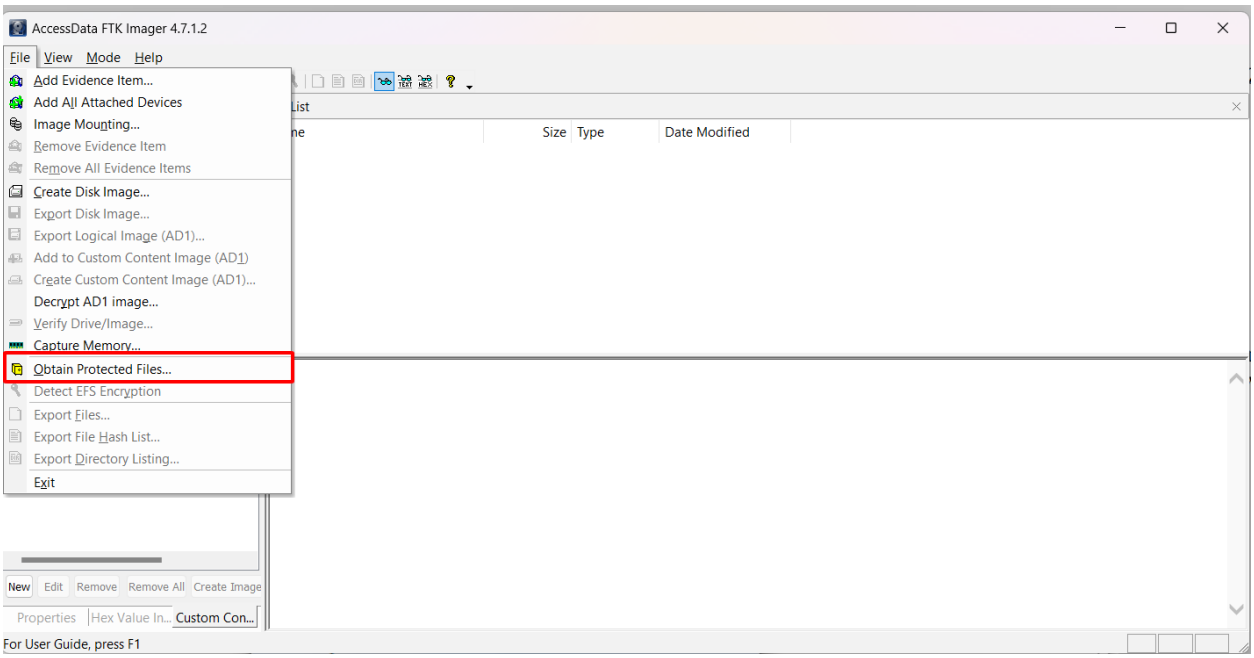



Sau khi vào chúng ta sẽ thấy có rất nhiều registry khác nhau. HiveList duy trì một danh sách của tất cả các tập tin hive trong registry đang được tải, bao gồm cả Master Boot Record (MBR), mã boot loader và control set được sử dụng trong lần khởi động cuối cùng. Thông tin trong khóa này giúp Windows theo dõi các tập tin hive và đảm bảo chúng được tải đúng cách khi khởi động

**Creating a Registry Image with FTK Imager Lite**

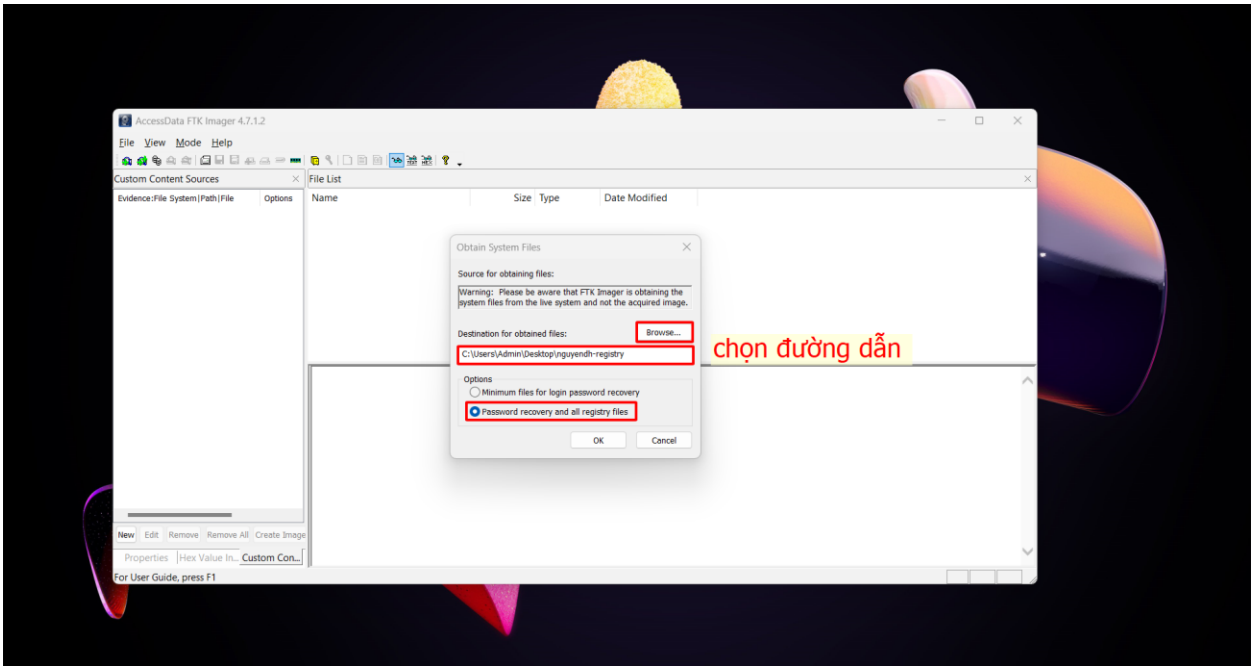
Sau khi đã có FTK Imager thông qua việc cài đặt từ những bài lab trước, chúng ta sẽ bắt đầu mở FTK Imager lên và bắt đầu quá trình tạo registry

Trên toolbar chọn **File → "Obtain Protected Files"**



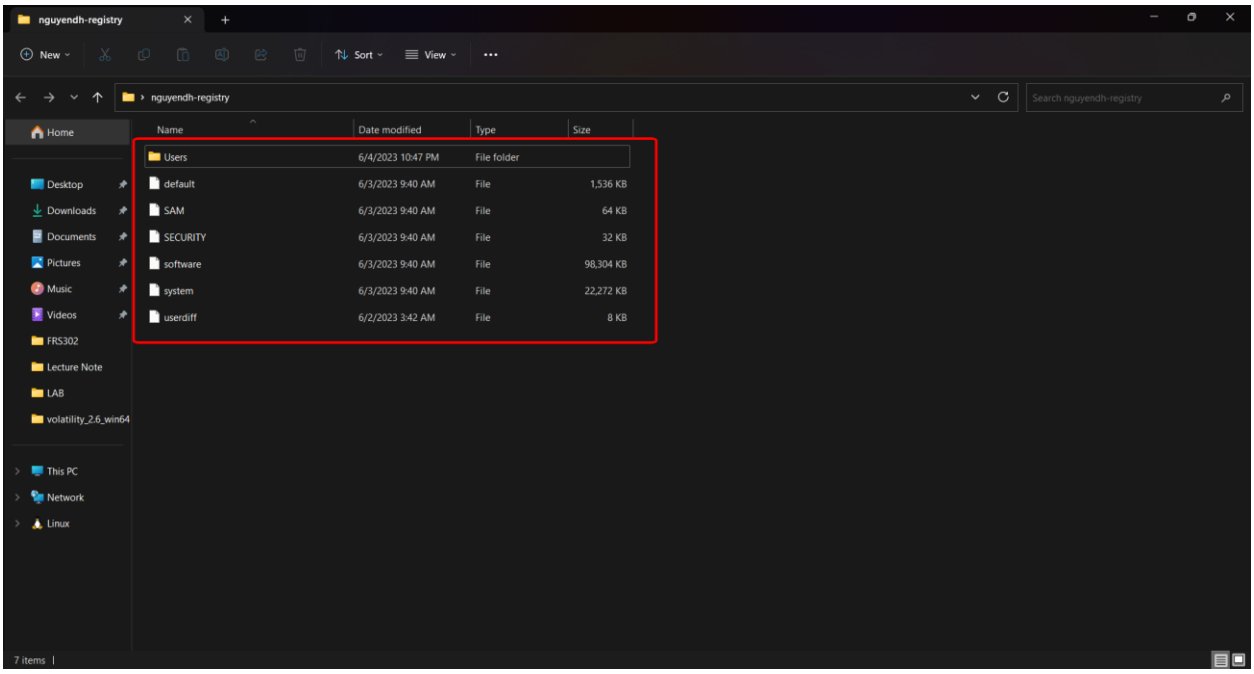

Sẽ có một pop up hiện ra thông báo rằng đây là registry trên máy của chúng ta, chứ không phải là máy nạn nhân, sau đó chúng ta sẽ tạo một folder để chứa tất cả các registry sau khi lấy ra. Trong trường hợp này sẽ đặt tất cả registry được dump ra bên trong thư mục nguyendh-registry bên trong Desktop.

Sau đó nhấn chọn **“Password recovery and all registry files”** sau đó chọn **OK**



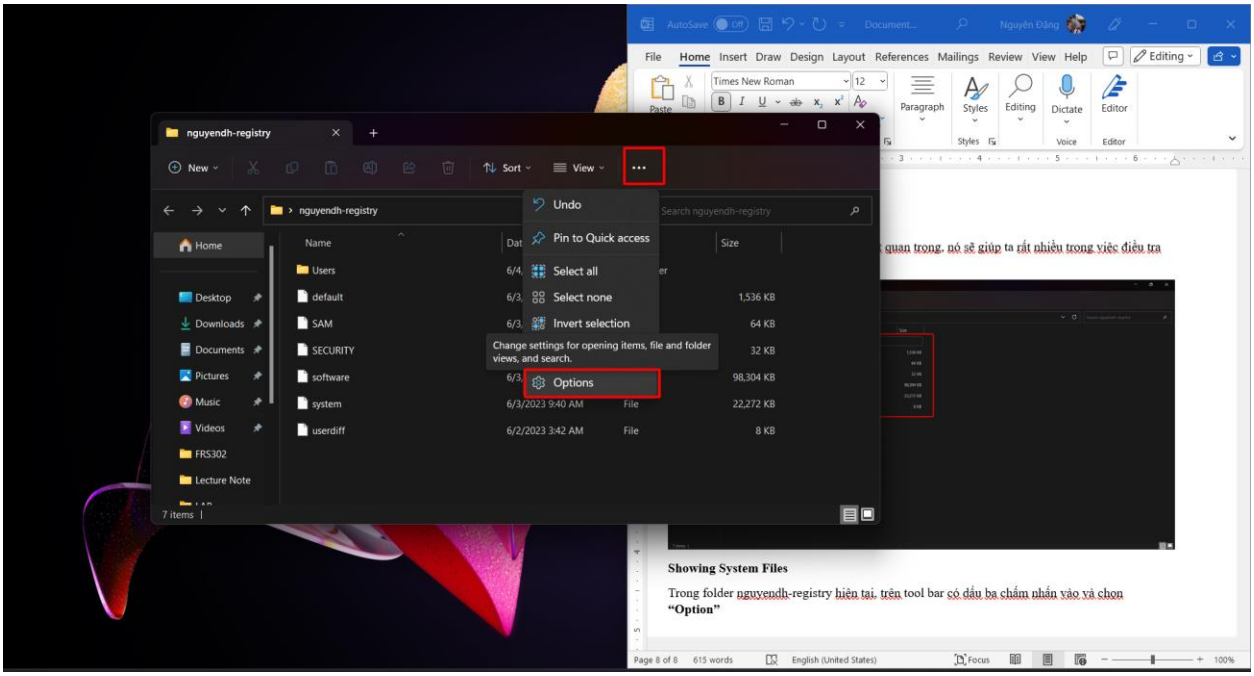

Đợi trong một khoảng thời gian để chương trình có thể chạy. Sau khi chạy hoàn tất, chúng ta sẽ thấy rằng bên trong folder mà chúng ta muốn nó dump ra, hiện tại là nguyendh-registry đã có các

file. Đây là những file cơ bản và cũng rất quan trọng, nó sẽ giúp ta rất nhiều trong việc điều tra pháp y số




**Showing System Files**

Trong folder nguyendh-registry hiện tại, trên tool bar có dấu ba chấm nhấn vào và chọn **"Option"**

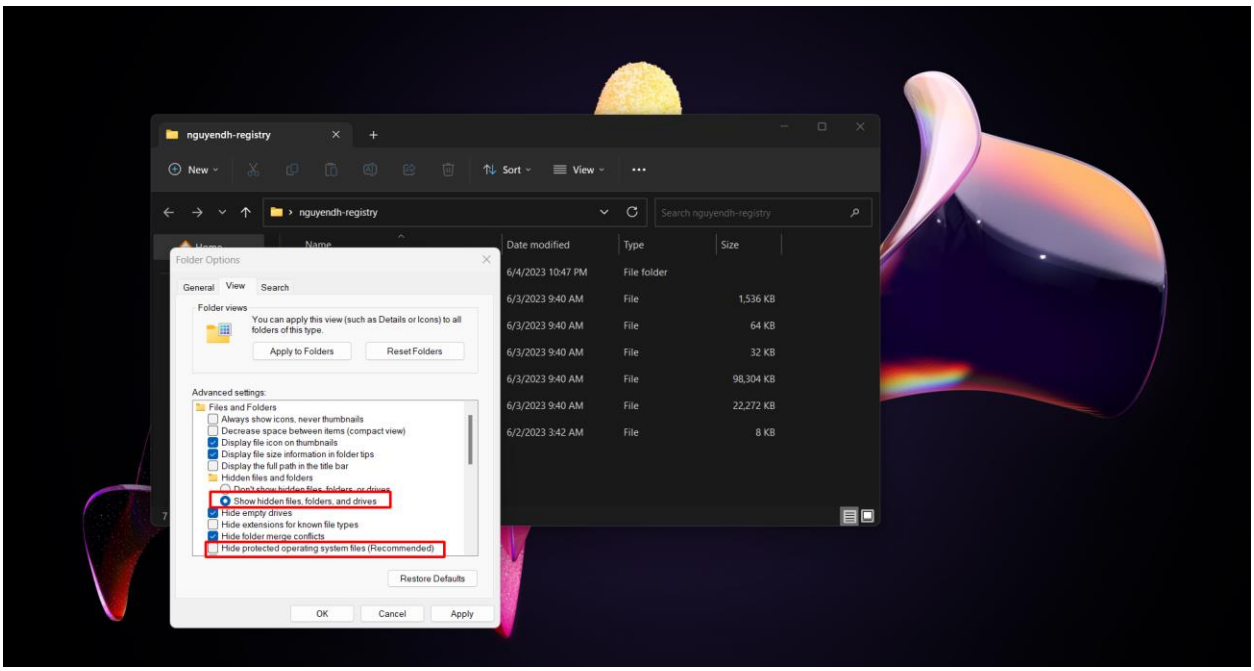



Trong Folder Options, di chuyển qua tab **"View"** chỉnh các phần sau:

- Bật cái này lên **"Show hidden files, folders, and drives”**
- Tắt đi phần **“Hide protected operating system files (Recommended)"**

Lưu ý: Nếu có một pop up thông báo cảnh báo, chúng ta chỉ việc nhấn **Yes**

Sau khi đã thực hiện xong mọi việc nhấn **“Apply”** và sau đó **“OK”**

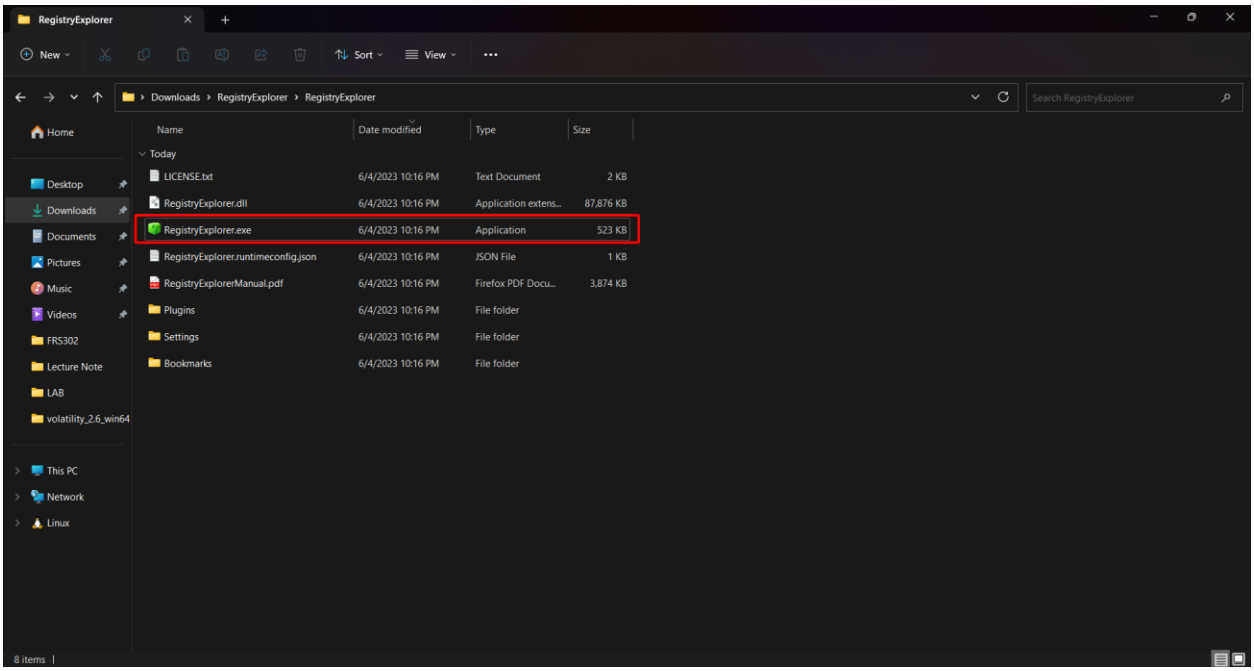



**Viewing TypedURLs with Registry Explorer**

TypedURLs là những trang url mà người dung hay sử dụng

Vào bên trong thư mục giải nén RegistryExplorer. Trong trường hợp này sẽ vào bên trong đường dẫn sau: C:\Users\Admin\Downloads\RegistryExplorer\RegistryExplorer

Và sau đó chọn mở Registry Explorer.exe




Trong Registry Explorer, nhấp vào File, " Load Offline Hive".

Sau đó vào bên trong thư mục đã dump registry, trong trường hợp này là nguyendh-registry và vào đường dẫn sau đây:

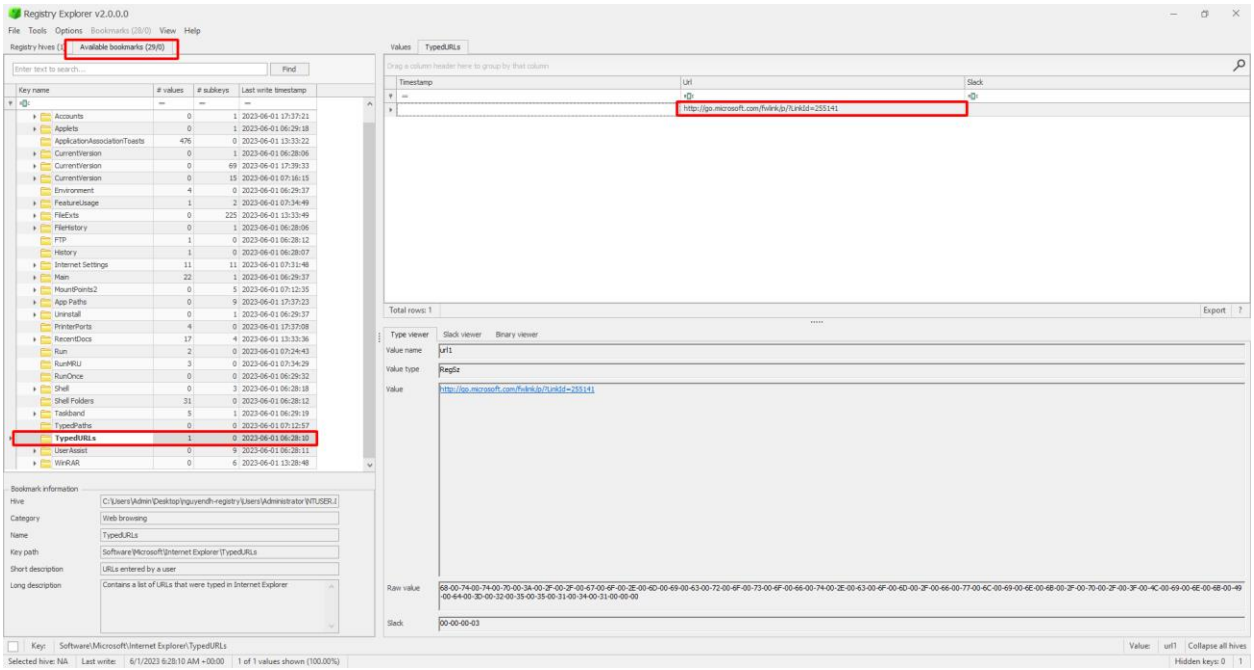
- Users\Administrator\NTUSER.DAT

Nếu một hộp bật lên có tiêu đề "Dirty hive detected!" hãy nhấp vào No.

Nếu một hộp bật lên có tiêu đề "Load dirty hive?", hãy nhấp vào Yes.

Trong Registry Explorer, ở ngăn trên cùng bên trái, nhấp vào tab " Available bookmark". Cuộn xuống và nhấp vào TypedURLs.

Khung trên cùng bên phải hiển thị các URL đã được truy cập, như hình bên dưới:

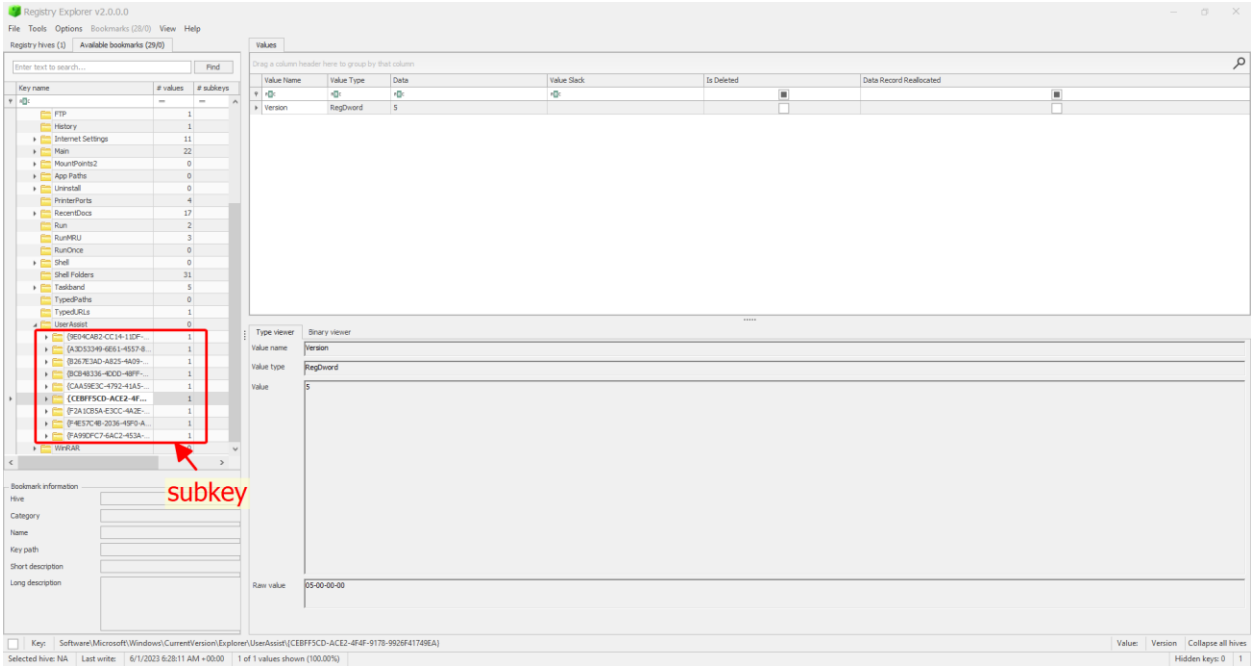


**Viewing UserAssist with Registry Explorer**

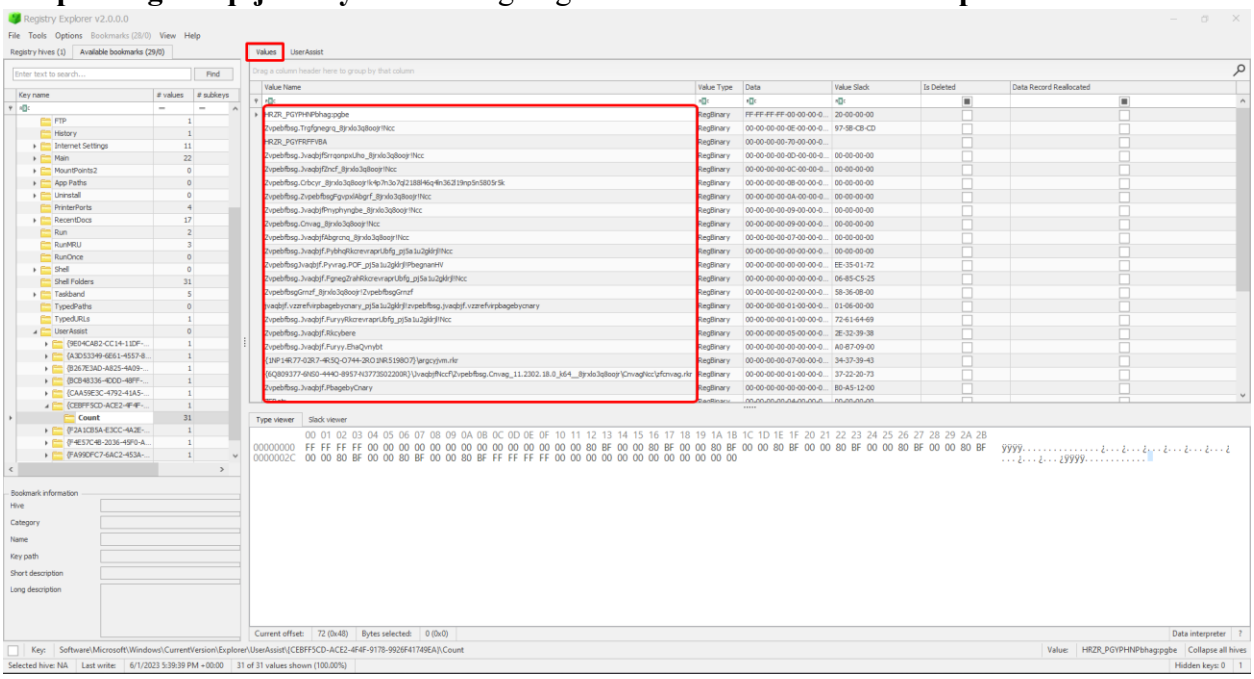
UserAssist là nơi khi một user chạy chương trình lên, theo e hiểu là nó sẽ tính xem là chương trình đó được chạy mấy lần bởi người dùng

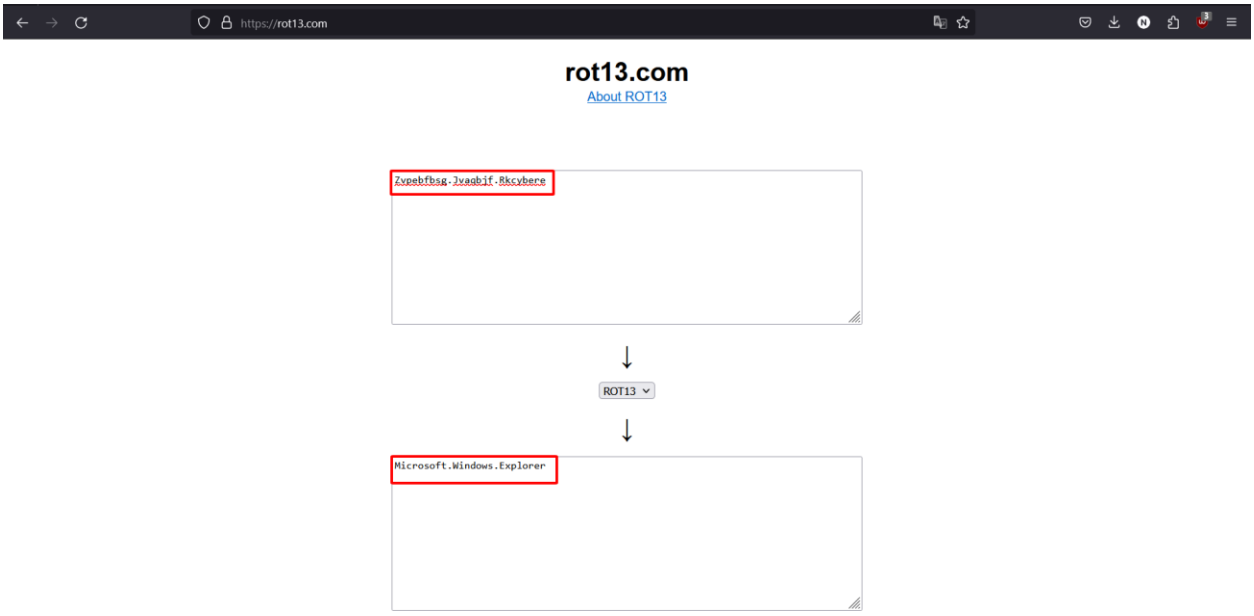
Trong vẫn trong phần **Available bookmark**, ta sẽ kéo xuống và chọn tới phần **UserAssist.**

Trong đaya sẽ có khá nhiều **subkey**, mỗi subkey sẽ có một folder con được gọi là **count**, nếu nhấn vào folder count đó mà bên phải không xuất hiện cái gì, chúng ta có thể kéo xuống phần subkey khác cho tới khi nào xuất hiện thông tin thì thôi

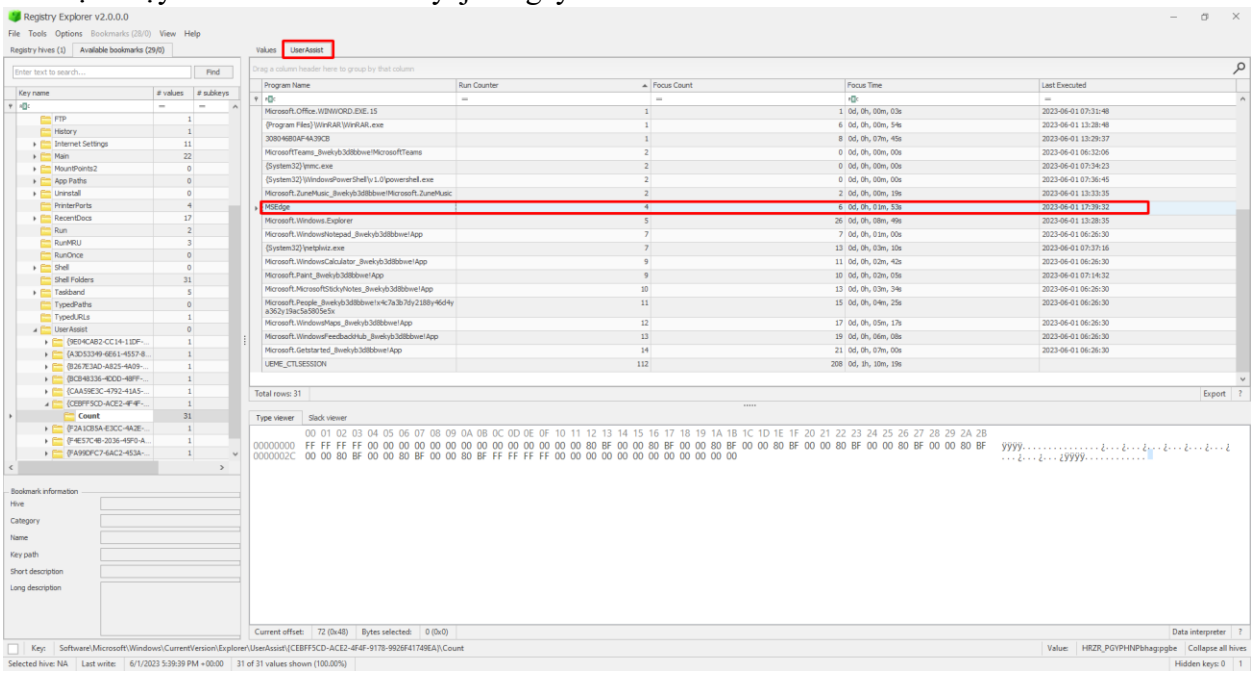



Bên trong phần value, ta sẽ thấy có những thông tin về program, thoạt đầu nhìn khá là vô tri về tên nhưng thật chất ra nó đã được mã hóa rot13, một thuật toán khá dễ đoán và dễ break. Thử lấy một tên bên Value name và decode rot13 xem nó sẽ ra cái gì và ta có:
**“Zvpebfbsg.Jvaqbjf.Rkcybere”** tương ứng với **“Microsoft.Windows.Explorer “**






Qua bên phần UserAssists kế bên phần Values ta có thể thấy rằng các file đã được hiển thị xem đã chạy được bao nhiêu lần, lần cuối chạy là khi nào. Như trong trường hợp này Microsoft edge đã được chạy 4 lần và lần cuối chyaj là ngày 1/6/2023 lúc 17:39:32



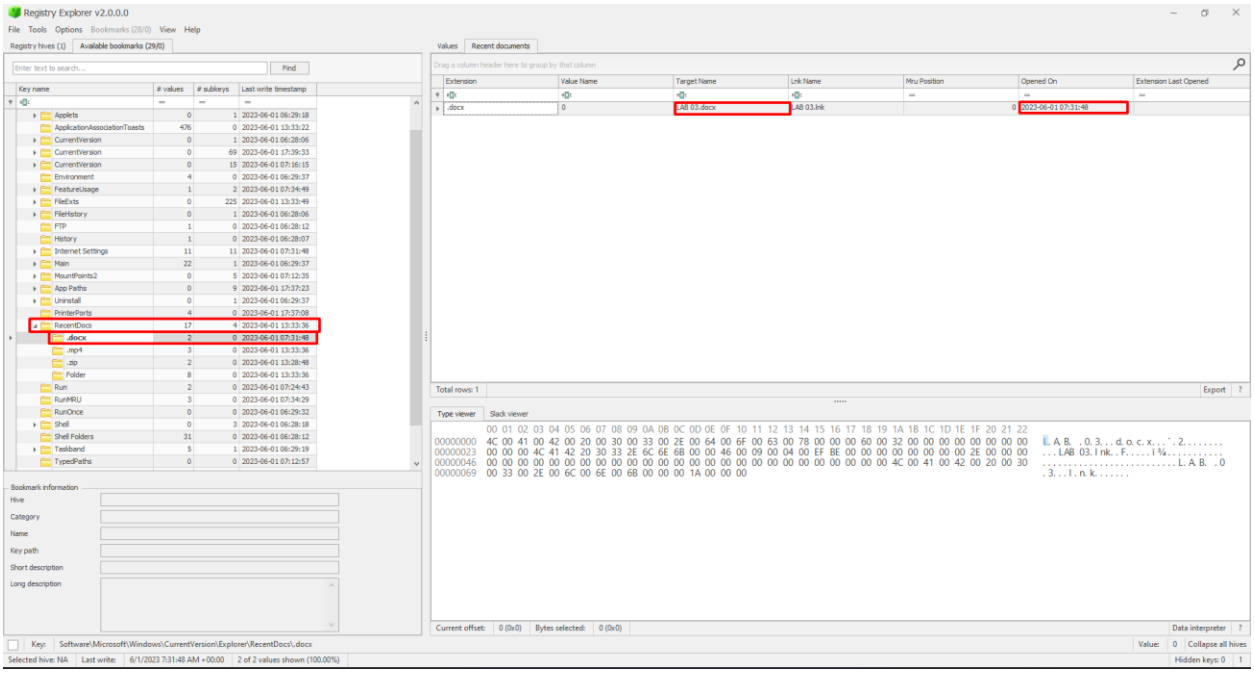

## Viewing RecentDocs

RecentDocs hiển thị các tài liệu mà người dùng đã mở gần đây.

Trong Registry Explorer trên cùng bên trái, mở rộng RecentDocs. Một danh sách các phần mở rộng tên tệp xuất hiện. Nhấp vào .txt.

Khung trên cùng bên phải hiển thị các tệp .txt được sử dụng gần đây, như minh họa bên dưới. Nhưng vì không có mở một file txt nào trước đó, chỉ mở bằng word nên thay vì .txt, trong trường hợp này sẽ dung word thay.

Ở đây ta thấy rằng máy nhận được một file có tên là Lab03.docx được mở vào ngày 1/6/2023 lúc 7:31:48



**Finding the Current Control Set**

"CurrentControlSet" là một registry key trong các hệ điều hành Microsoft Windows, nó lưu trữ các dữ liệu cấu hình cho phần cứng và phần mềm của hệ thống. Đây là một trong những subkey được đặt dưới registry key "HKEY_LOCAL_MACHINE\SYSTEM".

Trong Registry Explorer, nhấp vào Tệp, " Load Offline Hive ". Điều hướng đến Màn hình của bạn và mở tệp này:

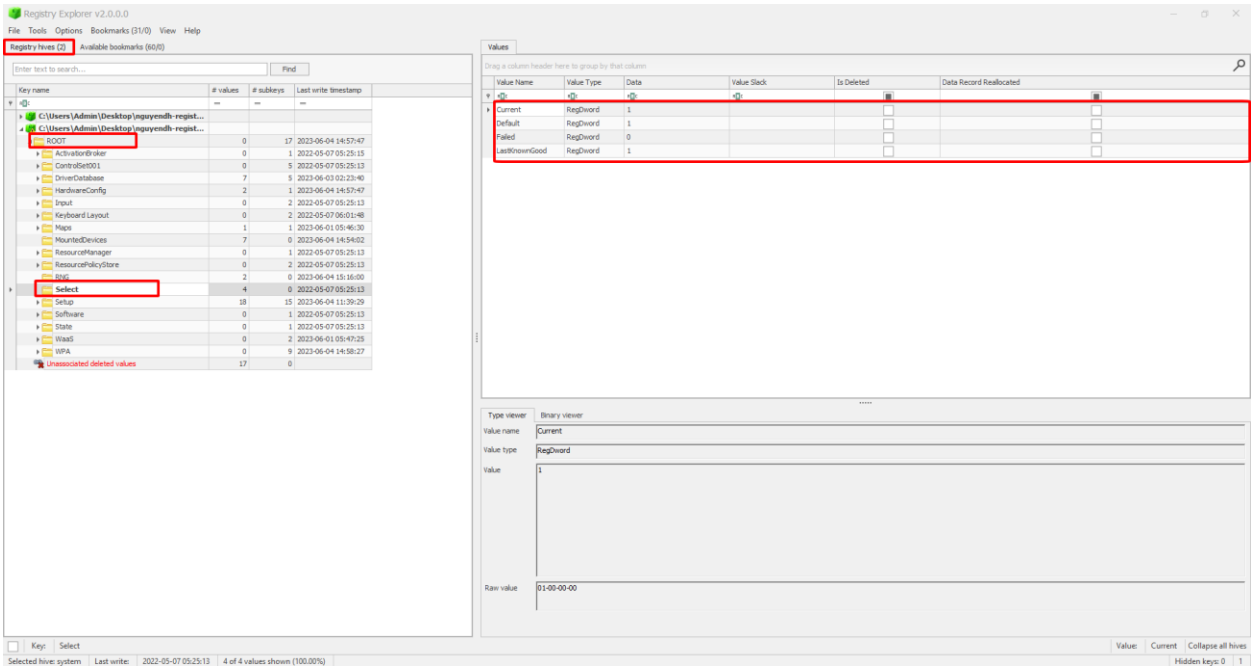
- nguyendh-registry\system

Nếu một hộp bật lên có tiêu đề " Dirty hive detected! ", hãy nhấp vào No.

Nếu một hộp bật lên có tiêu đề "Load dirty hive?", hãy nhấp vào Yes.

Trong bên trái của Registry Explorer, nhấp vào tab "Registry hives".

Sau đó mở rộng **ROOT** và nhấp vào **Select**, như hình bên dưới:



Bên phải sẽ hiển thị một số thông tin cho chúng ta thấy:

- Current – lần cuối cùng đăng nhập vào
- Default – Số sẽ đa số sẽ giống như current
- Failed – sẽ là số 0 nếu chưa có lỗi nào xảy ra
- LastKnownGood -- là bộ điều khiển cuối cùng mà hệ thống khởi động thành công được sử dụng để phục hồi lỗi của hệ thống trong trường hợp khởi động gặp sự cố.

**Viewing USBSTOR with Registry Explorer**

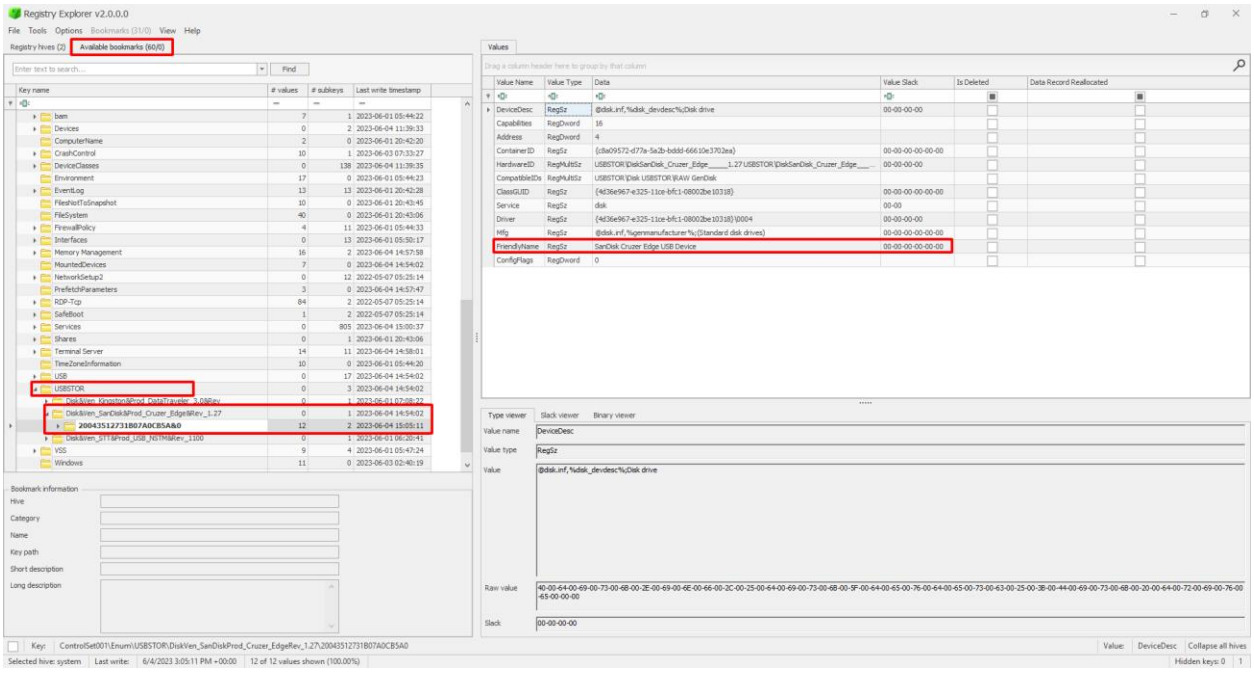
USBSTOR hiển thị danh sách mọi thiết bị USB đã được kết nối với máy tính. Điều này rất quan trọng đối với nhiều cuộc điều tra, bởi vì những thiết bị có thể chứa bằng chứng bổ sung.

Chuyển sang “Available bookmarks”

Sau đó nhấn mở roognj **USBTOR**. Sẽ hiện ra những key của những USB mà đã gắn vào bên trong máy.

Sẽ có các subkey, ta chỉ việc click chọn vào những subkey bên trong đó, sẽ có thanh hiện ra bên phải. Trong phần value, ta tìm tới phần **FriendlyName** nơi đây sẽ hiện tên đúng của USB

Như hình dưới đây, ta có thể thấy rằng registry này đã lưu lại được tên của USB mà ta đã cắm ở bên trong máy lúc ban đầu bài lab


Registry Explorer v2.0.0.0
File Tools Options Bookmarks (31/0) View Help
Registry hives (2) Available bookmarks (60/0)
Enter text to search... Find
Key name # values # subkeys Last write timestamp
bam 7 1 2023-06-01 05:44:22
Devices 0 2 2023-06-04 11:39:33
ComputerName 2 0 2023-06-01 20:42:20
CrashControl 10 1 2023-06-03 07:33:27
DeviceClasses 0 138 2023-06-04 11:39:35
Environment 17 0 2023-06-01 05:44:23
EventLog 13 13 2023-06-01 20:42:28
FileshotToSnapshot 10 0 2023-06-01 20:43:45
FileSystem 40 0 2023-06-01 20:43:06
FirewallPolicy 4 11 2023-06-01 05:44:33
Interfaces 0 13 2023-06-01 05:50:17
Memory Management 16 2 2023-06-04 14:57:58
MountedDevices 7 0 2023-06-04 14:54:02
NetworkSetup2 0 12 2022-05-07 05:25:14
PrefetchParameters 3 0 2023-06-04 14:57:47
RDP-Tcp 84 2 2022-05-07 05:25:14
SafeBoot 1 2 2022-05-07 05:25:14
Services 0 805 2023-06-04 15:00:37
Shares 0 1 2023-06-01 20:43:06
Terminal Server 14 11 2023-06-04 14:58:01
TimeZoneInformation 10 0 2023-06-01 05:44:20
USB 0 17 2023-06-04 14:54:02
USBSTOR 0 3 2023-06-04 14:54:02
Disk&Ven_SanDisk&Prod_Cruzer_Edge&Rev_1.27 0 1 2023-06-04 14:54:02
2004351273 1B07A0CB5A&0 12 2 2023-06-04 15:05:11
VSS 9 4 2023-06-01 05:47:24
Windows 11 0 2023-06-03 02:40:19
Bookmark information
Hive
Category
Name
Key path
Short description
Long description
Values
Drag a column header here to group by that column
Value Name Value Type Data Value Slack Is Deleted Data Record Reallocated
DeviceDesc RegSz @disk.inf,%disk_devdesc%;Disk drive 00-00-00-00
Capabilities RegDword 16
Address RegDword 4
ContainerID RegSz {c8a09572-d77a-5a2b-bddd-66610e370 2ea}
HardwareID RegMultiSz USBSTOR\DiskSanDisk_Cruzer_Edge____1.27 USBSTOR\DiskSanDisk_Cruzer_Edge___
CompatibleIDs RegMultiSz USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID RegSz {4d36e967-e325-11ce-bfc1-08002be10318}
Service RegSz disk
Driver RegSz {4d36e967-e325-11ce-bfc1-08002be10318}\0004
Mfg RegSz @disk.inf,%genmanufacturer%;(Standard disk drives)
FriendlyName RegSz SanDisk Cruzer Edge USB Device
ConfigFlags RegDword 0
Type viewer Slack viewer Binary viewer
Value name DeviceDesc
Value type RegSz
Value @disk.inf,%disk_devdesc%;Disk drive
Raw value 40-00-64-00-69-00-73-00-6B-00-2E-00-69-00-6E-00-66-00-2C-00-25-00-64-00-69-00-73-00-6B-00-5F-00-64-00-65-00-76-00-64-00-65-00-73-00-63-00-25-00-3B-00-44-00-69-00-73-00-6B-00-20-00-64-00-72-00-69-00-76-00-65-00-00-00
Slack 00-00-00-00
Key: ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Edge&Rev_1.27\2004351273 1B07A0CB5A&0
Value: DeviceDesc Collapse all hives
Selected hive: system Last write: 6/4/2023 3:05:11 PM +00:00 12 of 12 values shown (100.00%)
Hidden keys: 0 1