Analyzing the Windows Registry for Forensic Evidence

❖ Windows Registry

The Microsoft Windows operating system stores configuration settings and choices in the Windows Registry, a hierarchical database. Because it stores details on the hardware, software, user preferences, and system settings, it is essential to the operation of Windows.

Key aspects of Windows Registry

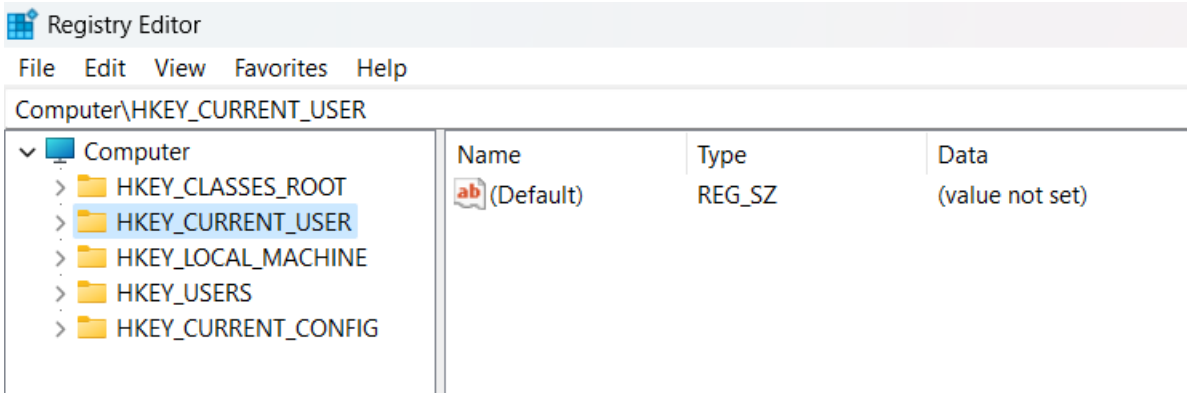
- **Structure:**

The Registry is organized into keys and subkeys like a tree. Values and subkeys may be included in each key. The structure resembles a file system, with keys representing directories and values representing files.

- **Hives:**

The five primary hives are:

➢ Path: Windows Home > Registry Editor



➢ **HKEY_CLASSES_ROOT (HKCR):** This key contains information about file associations and OLE (Object Linking and Embedding) object classes. It is used to associate file extensions with the applications that should open them.

➢ **HKEY_CURRENT_USER (HKCU):** This key contains configuration settings for the user currently logged into the system. It stores user-specific preferences, settings, and application data.

➢ **HKEY_LOCAL_MACHINE (HKLM):** This key contains configuration settings for the local computer. It stores system-wide settings and information about installed software and hardware.

➢ **HKEY_USERS (HKU):** This key contains configuration settings for all user profiles on the computer. Each user's settings are stored in a subkey under HKEY_USERS.

➢ **HKEY_CURRENT_CONFIG (HKCC):** This key contains information about the current hardware configuration of the system. It is used by the Plug and Play system to configure hardware devices.

Each hive is a separate file or group of files that is loaded into memory when the computer starts up. Hives are typically stored in the %SystemRoot%\System32\Config folder.

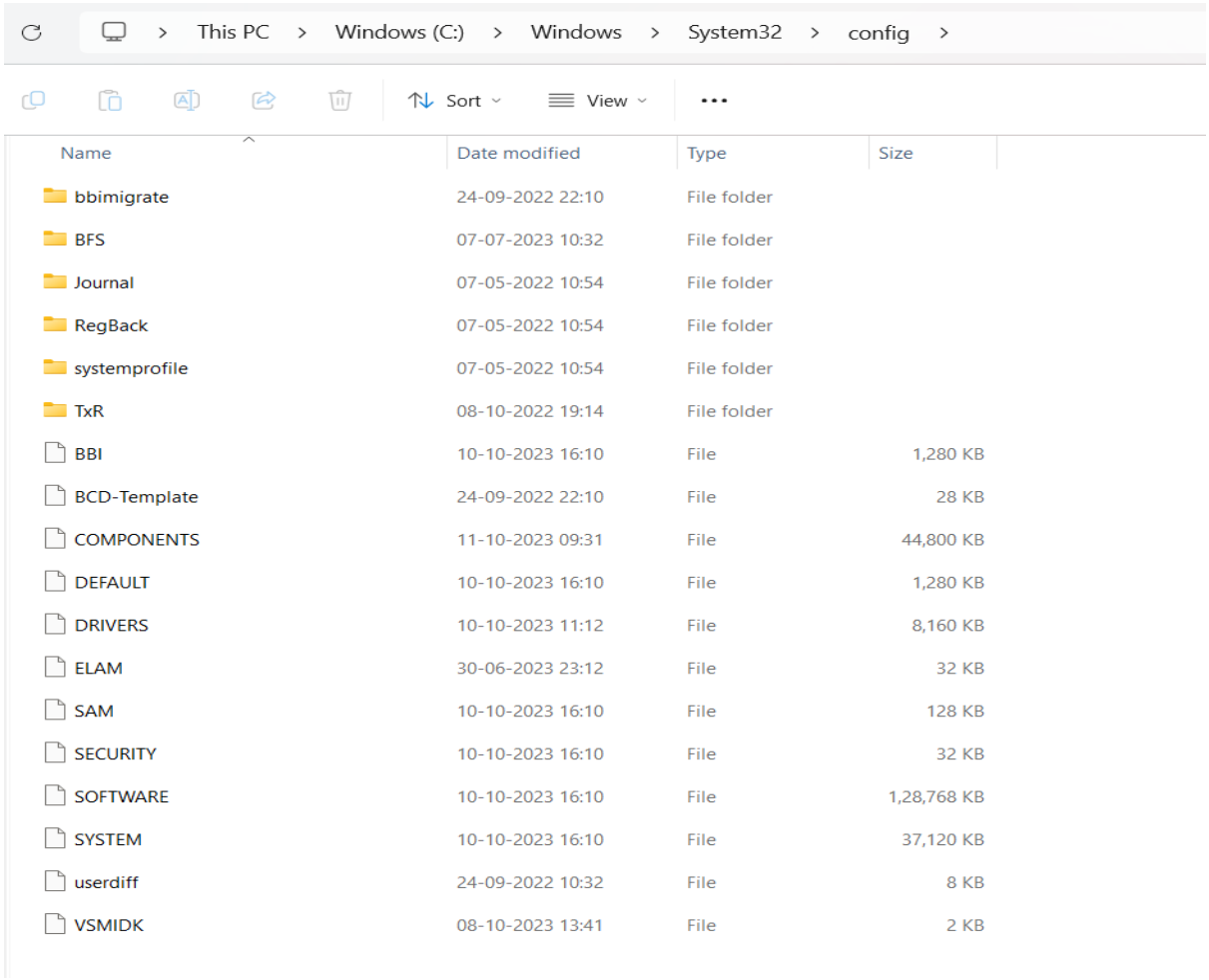


Fig 1: Windows registry files' location

Here are some ways in which registers can be useful in forensic analysis of a computer:

- **Program Execution Analysis:** Registers hold information about the program or process that is presently running. To ascertain the condition of the CPU at a certain point in time, forensic investigators can look at the contents of registers. This can assist in reconstructing the order in which instructions were executed, which is essential for comprehending the operations performed by a computer.

- **Memory Access Patterns:** Memory addresses and data that is being read from or written to memory are stored in registers. Register value analysis may shed light on a program's memory access patterns, which is helpful for tracing data flows and spotting instances of data tampering or illegal access.

- **System Call Analysis:** The parameters and return values for system calls that a program makes to the operating system are frequently stored in registers. Register contents can be used by forensic investigators to determine which system calls were performed, what

arguments were supplied, and what actions those calls produced. This can make it easier to determine the steps the software has made.

- **Time Analysis:** Timestamps and other information pertaining to time can be stored in registers. This may be utilized to construct timelines during a forensic inquiry by figuring out when various events took place.

- **Memory Analysis:** Examining the register contents during memory forensics can shed light on how a process was functioning when memory was captured. This can aid in retrieving passwords, sensitive data saved in memory, and cryptographic keys.

- **Malware Analysis:** Malware often uses registers for various purposes, including code execution, process injection, and data theft. Analyzing register values can help in identifying and understanding the behavior of malicious software.

- **Root Cause Analysis:** When investigating a system breach or an incident, examining register values during the time of compromise can help in identifying the root cause of the incident. For instance, registers may contain information about the exploit used to compromise the system.

- **Digital Signature Verification**: Registers may hold information related to digital signatures. Forensic experts can analyze these registers to verify the authenticity and integrity of files or software.

TOOL: FTK Imager

- FTK Imager is a forensic imaging tool that is used to create forensic images of hard drives, partitions, and logical files. It is a powerful tool that can be used to collect evidence from a variety of devices, including computers, smartphones, and tablets.

- FTK Imager can be used to create forensic images of live systems, which means that it can be used to image a device without shutting it down. This is particularly useful in situations where shutting down the device could destroy evidence.

- FTK Imager also supports a variety of forensic image formats, including E01, AFF, and DD. This makes it easy to share forensic images with other investigators or to use them in other forensic tools.

Here are some of the key roles of FTK Imager in digital forensics:

- **Collecting evidence:** FTK Imager can be used to collect evidence from a variety of devices, including computers, smartphones, and tablets. This evidence can be used to investigate crimes, such as cybercrime and fraud.

- **Preserving evidence:** FTK Imager creates forensic images of devices, which are bit-for-bit copies of the original device. This ensures that the evidence is preserved and cannot be altered.

- **Analyzing evidence:** FTK Imager can be used to analyze forensic images to identify evidence of crimes or other incidents. For example, FTK Imager can be used to identify deleted files, malware infections, and network activity.

- **Reporting evidence:** FTK Imager can be used to generate reports that document the findings of a forensic investigation. These reports can be used to prosecute criminals or to protect systems from future attacks.

Information that can be found in the registry includes:

1. Users and the time they last used the system Most recently used software
2. Any devices mounted to the system, including unique identifiers of flash drives, hard
3. Drives, phones, tablets, etc. When the system connected to a specific wireless access point
4. What and when files were accessed A list of any searches done on the system

Creating a forensic copy

Step 1: Copy the entire "FTK Imager" installation folder (typically "C:\Program Files AccessData FTK Imager" or "C:\Program Files (x86)\AccessData\FTK Imager") to your flash drive

Open the folder form flash drive and run the FTk Imager.exe file

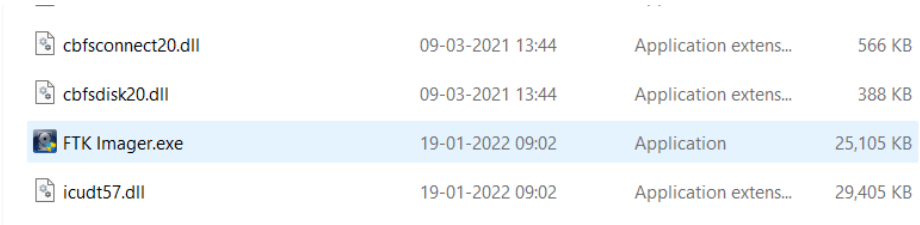


Fig 2: The program is located in the drive's FTK Imager subdirectory.

- FTK is using the USB drive to run independently so that it won't affect the system registers..

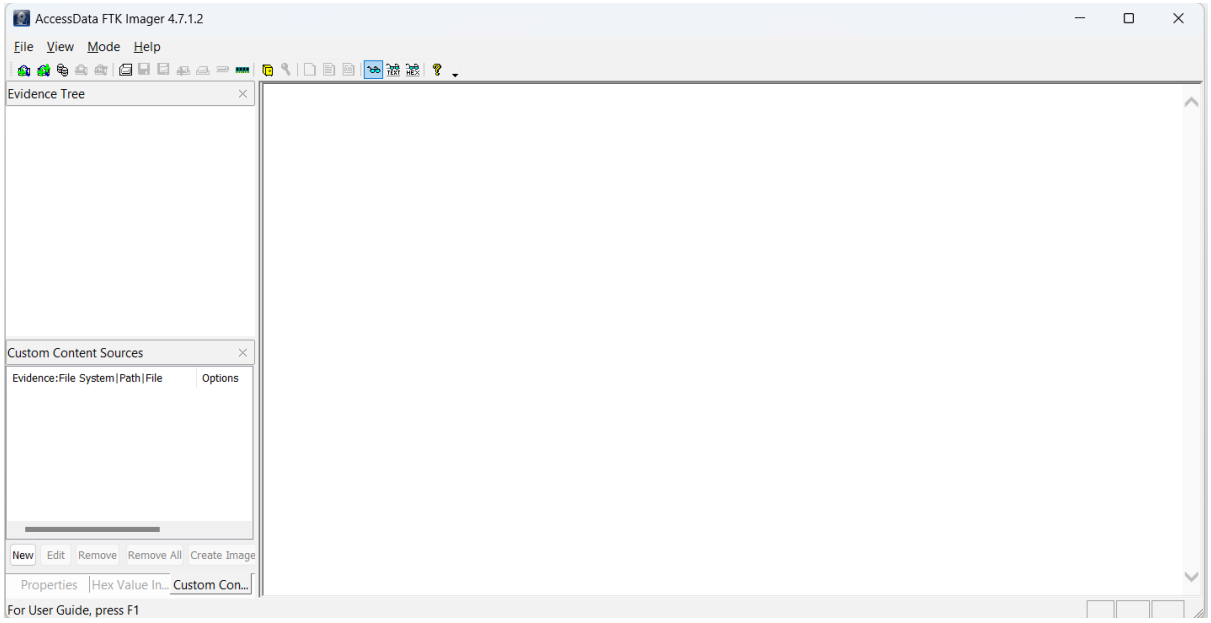


Fig. 3: The FTK Imager's home page

Step 2: Make a new folder on the disk to house the system register files (for instance, protected files).

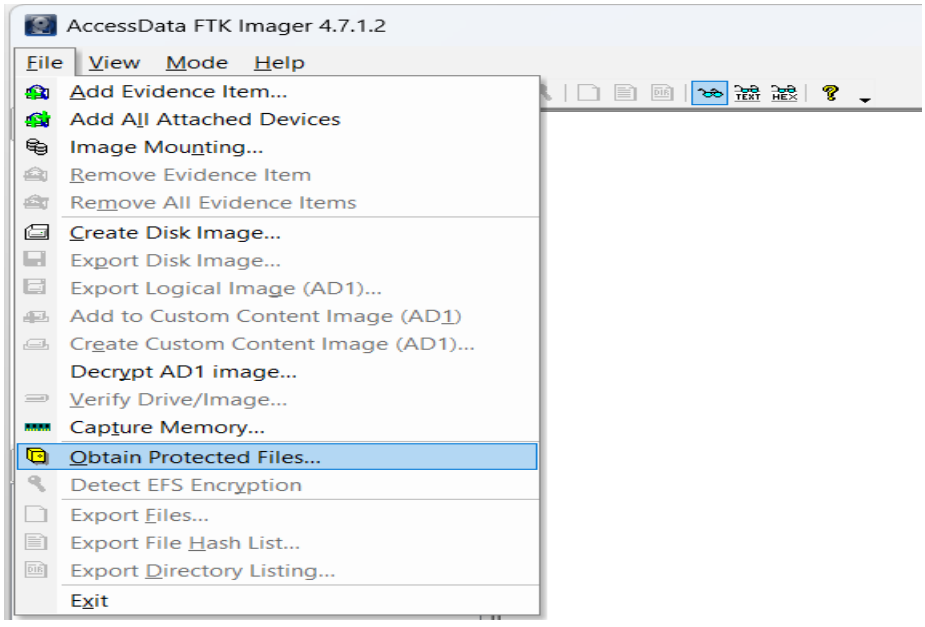
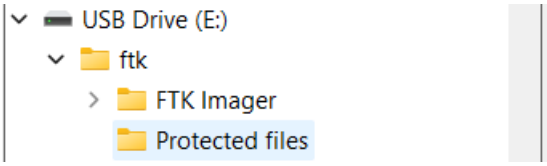


Fig. 4: Image of choosing the option to gather data

Select the location of the Protected folder to copy the data there.



Step 3: Select the registery files and password recovery options.

Note: The minimum files for login password recovery and password recovery and register values are two different sets of files that can be used to recover a user's password.

The minimum files for login password recovery are the files that are absolutely necessary to recover a user's password. These files include the SAM file and the SYSTEM hive of the registry. The SAM file contains the user accounts and their passwords, while the SYSTEM hive contains the settings for the operating system.

The password recovery and register values are a more comprehensive set of files that can be used to recover a user's password. These files include the SAM file, the SYSTEM hive, and the SECURITY hive of the registry. The SECURITY hive contains the security settings for the operating system, including the passwords for the administrator accounts.

The main difference between the minimum files for login password recovery and the password recovery and register values is that the password recovery and register values include the SECURITY hive of the registry. This gives investigators more options for recovering a user's password.

Set of files	Files	Description
Minimum files for login password recovery	SAM file, SYSTEM hive	The absolute minimum files needed to recover a user's password.
Password recovery and register values	SAM file, SYSTEM hive, SECURITY hive	A more comprehensive set of files that can be used to recover a user's password.

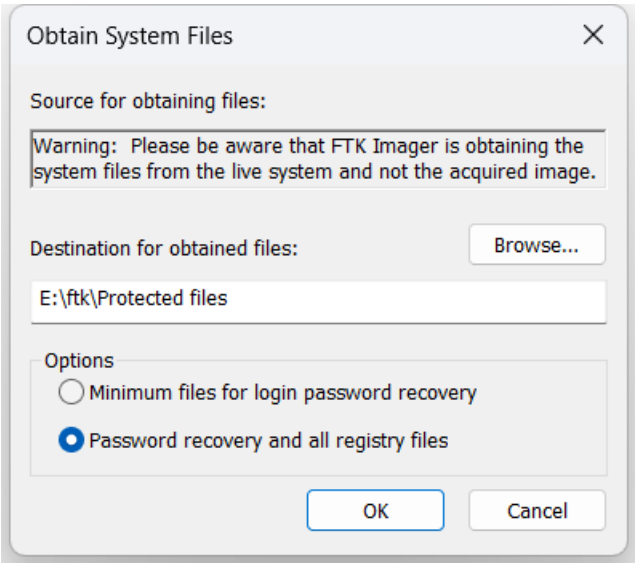


Fig 5: System Files selection

Step 4: Check to make sure that every file has been returned to the folder.

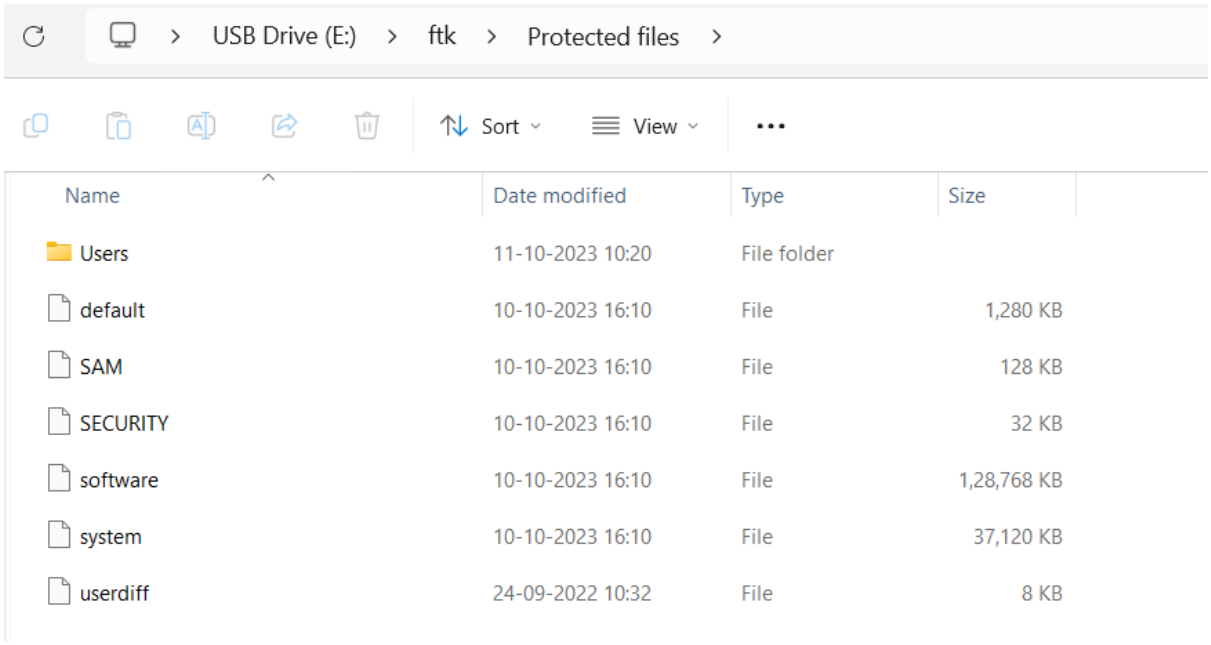


Fig. 6 shows the mounted files in the folder

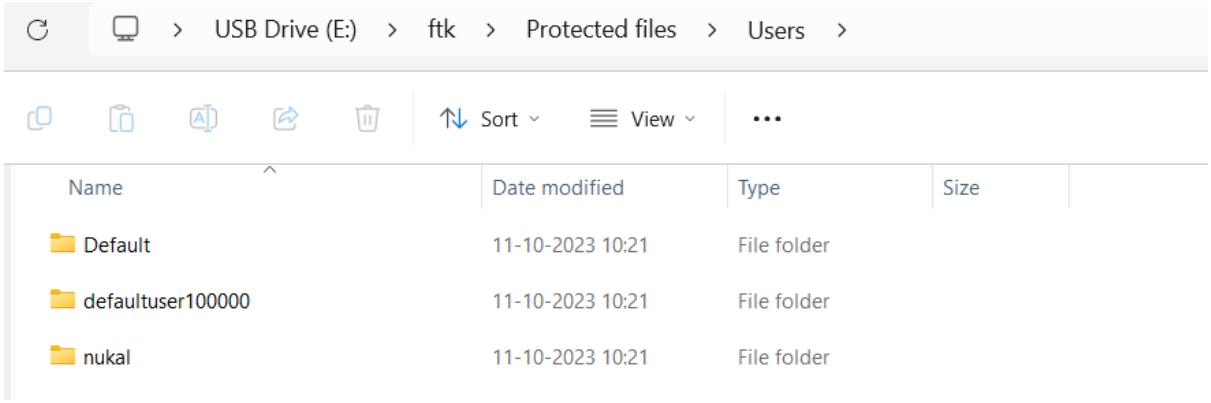


Fig 7: Files in the User Windows registry

Step 1: Open the Forensic registry editor(fred)

- Path: Files > computer Forensic > File Analysis > Forensic Registry eDitor

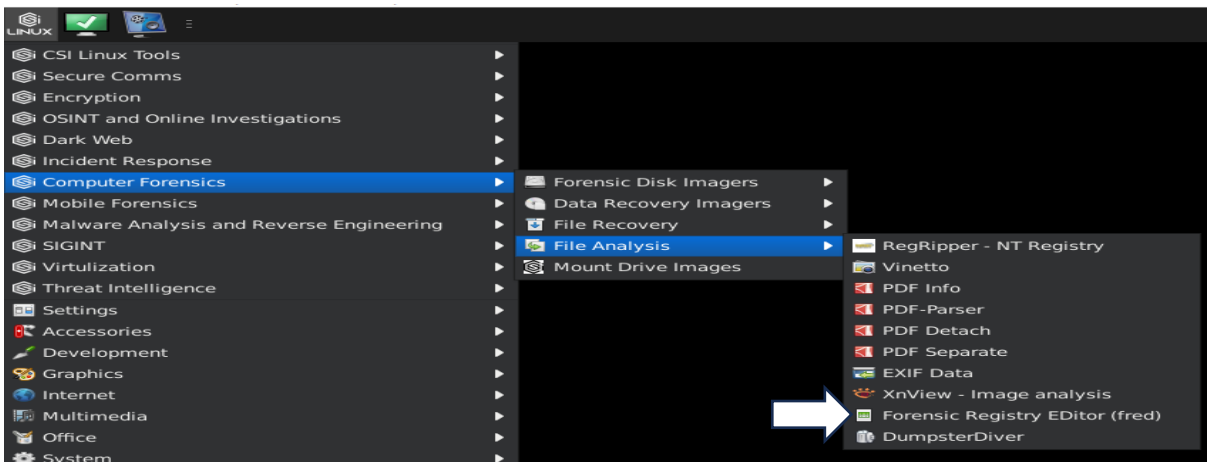


Figure 8: shows the route to the Registry Analysis tool.

Step 2: Pick the HIVE to investigate in accordance with the requirements for the investigation.

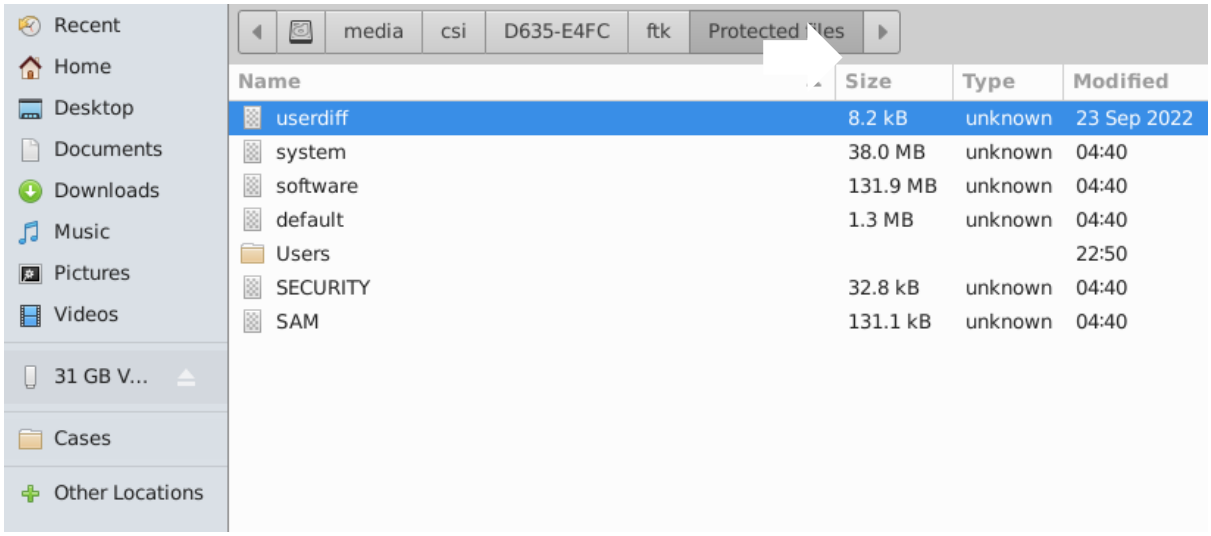


Fig 9: List of HIVES in the folder.

Step 3: The system's user profiles should be examined.

- HIVE: Users

- Path: Miscrosoft>windows NT>current version>networklist>profiles

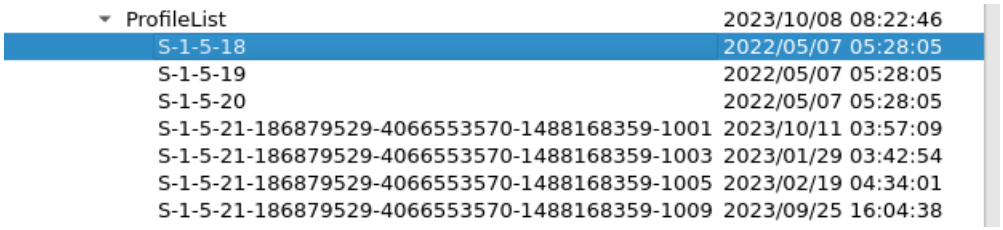


Fig 10: User profile list.

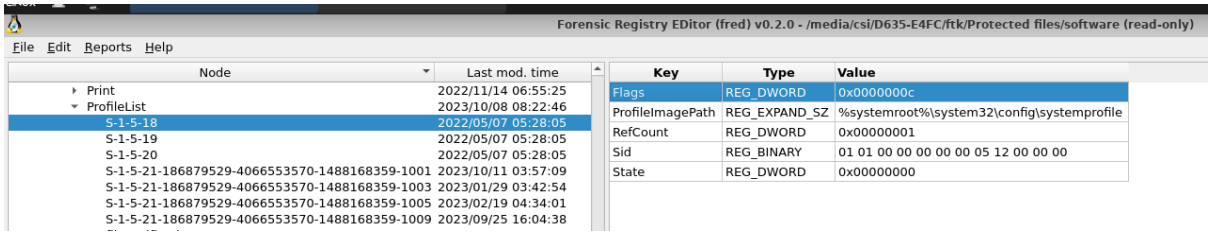


Fig 11: Detailed analysis of the User info.

Step 4: Investigate the Documents that the user/Hacker accessed in the system

- HIVE: System
- Path: Software>Microsoft>windows>current version> expoler> recent docs

To check what are the documents that the hacker is accessed

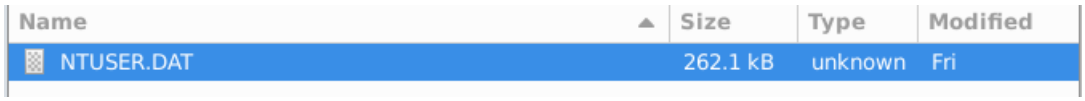


Fig 12: File used to investigate.

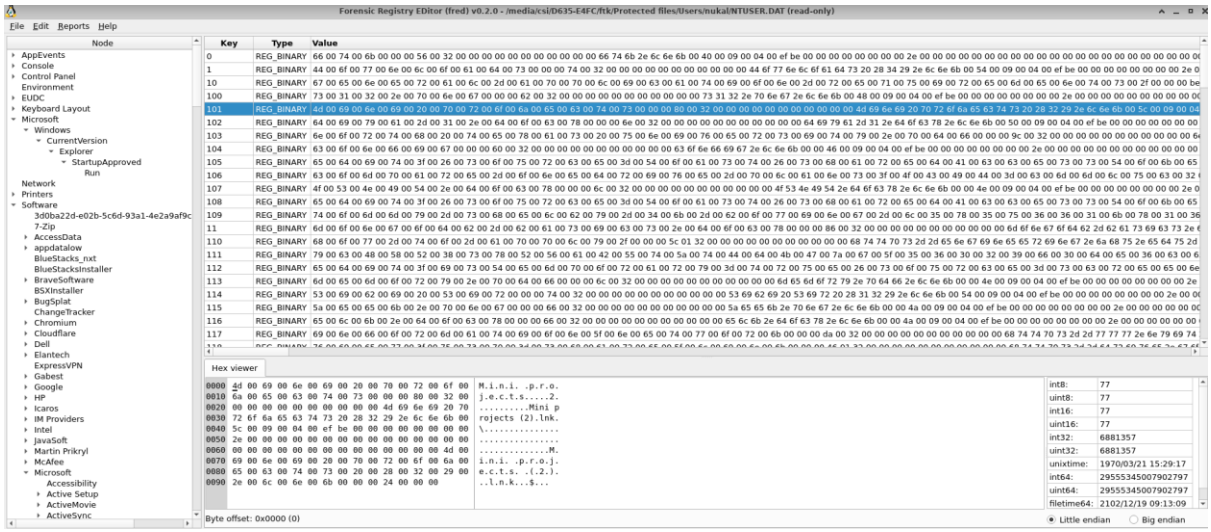


Fig 13: A list of the documents that the user has access to.

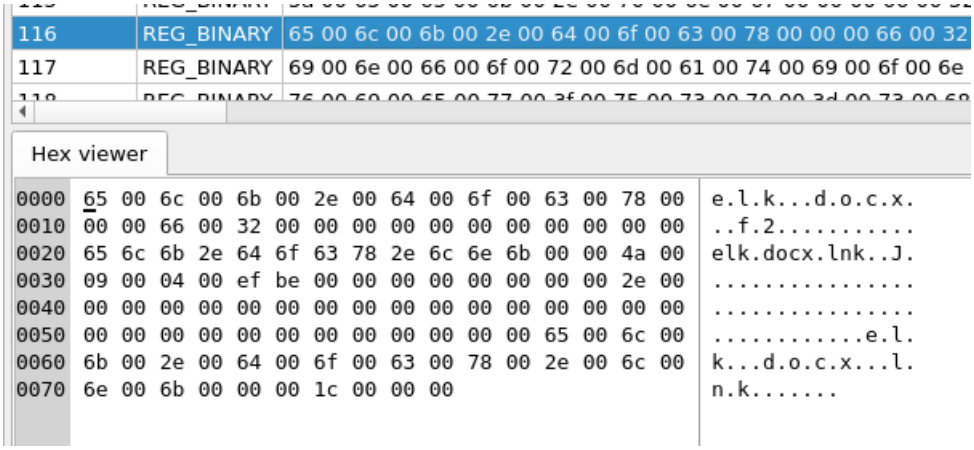


Fig. 14: Close examination of the name-containing document.

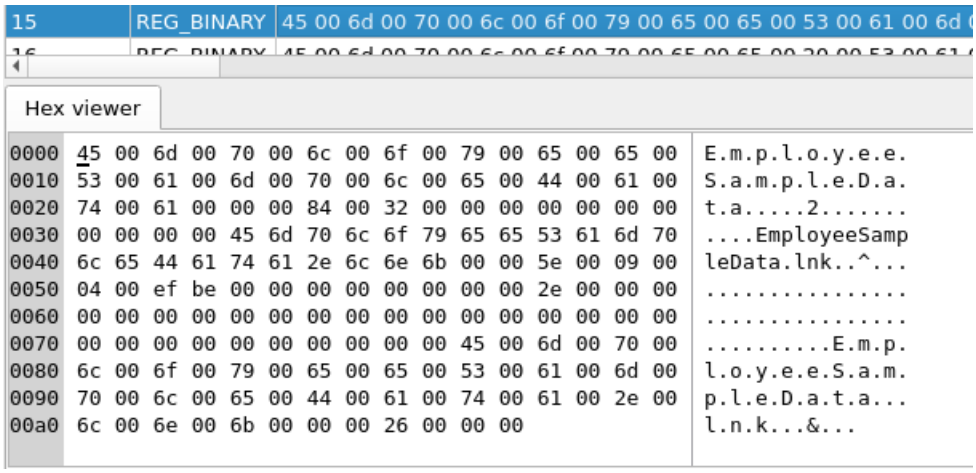


Fig. 15: Close examination of the name-containing document(2).

Step 5: search into or search up the URL that the user or hacker has visited.

- HIVE: System
- Path: Microsoft> Internet exploler> typed url

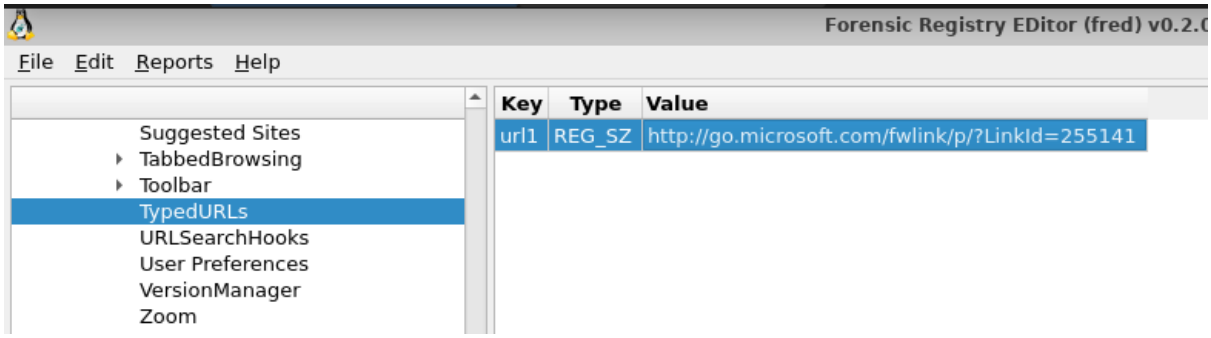


Fig 16: List of URL's that user visisted.

Step 6: explore the Network services of the User/attacker used in the connection

- HIVE: System
- Path: ControlSet001>Services>Tcp Ip> Parameters> Interfaces

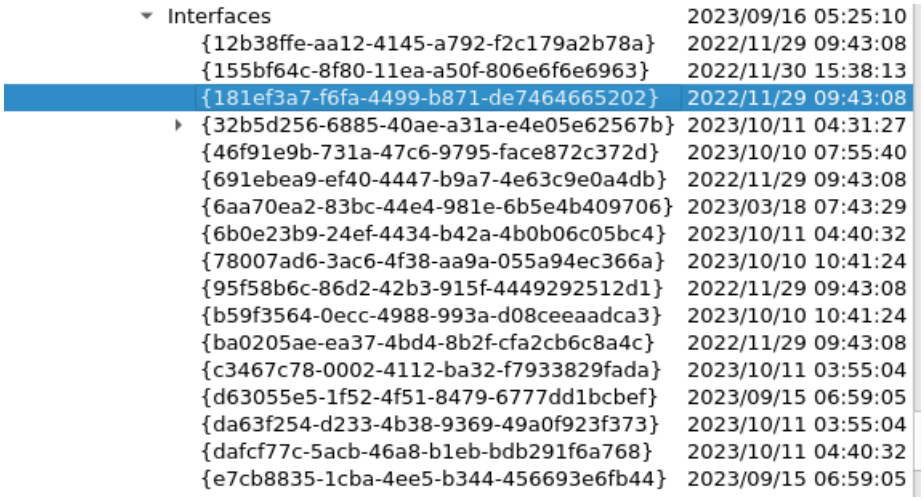


Fig 17: list of the system interfaces that are currently in use.

- We are able to list the machine's IP address.

Key	Type	Value
DefaultGateway	REG_MULTI_SZ	
DefaultGatewayMetric	REG_MULTI_SZ	
DhcpConnForceBroadcastFlag	REG_DWORD	0x000
DhcpDefaultGateway	REG_MULTI_SZ	172.18
DhcpGatewayHardware	REG_BINARY	ac 12 (
DhcpGatewayHardwareCount	REG_DWORD	0x000
DhcpIPAddress	REG_SZ	172.18
DhcpInterfaceOptions	REG_BINARY	fc 00 (
DhcpNameServer	REG_SZ	172.18
DhcpNetworkHint	REG_SZ	65944
DhcpServer	REG_SZ	172.18
DhcpSubnetMask	REG_SZ	255.25
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.25
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000001
IPAddress	REG_MULTI_SZ	
IsServerNapAware	REG_DWORD	0x00000000
Lease	REG_DWORD	0x00000e10
LeaseObtainedTime	REG_DWORD	0x6526251f
LeaseTerminatesTime	REG_DWORD	0x6526332f
NameServer	REG_SZ	
RegisterAdapterName	REG_DWORD	0x00000000
RegistrationEnabled	REG_DWORD	0x00000001

Fig 18: In detailed of the Network

Step 7: What are the services set to start when the system starts.

- HIVE: SYSTEM
- Software>Microsoft>windows>current version>run

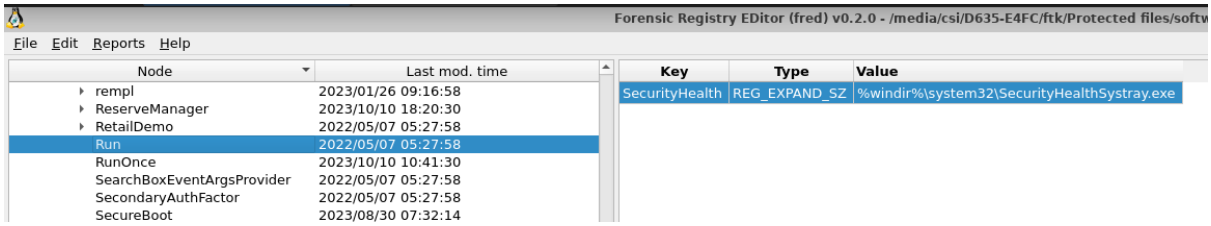


Fig 19: Programs that System automatically launches.

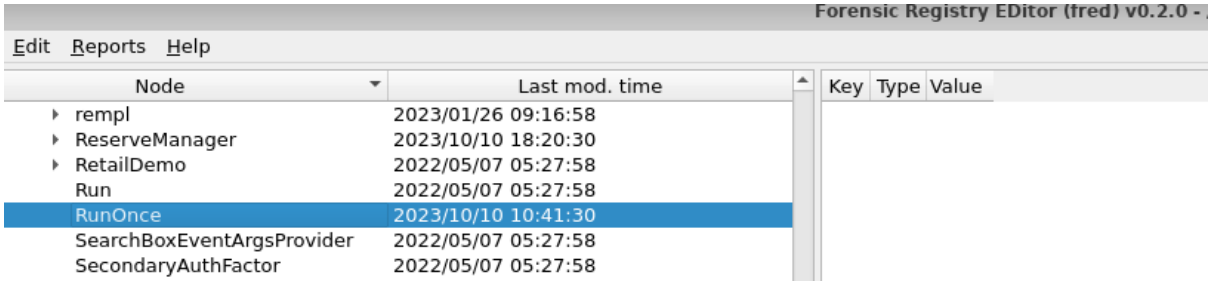


Fig 20: Programs that System launches once.

Note: Seems that hacker not installed any malware

Step 8: programs that System automatically launches.

- HIVE: SYSTEM
- system>CurrentControlSet>Services

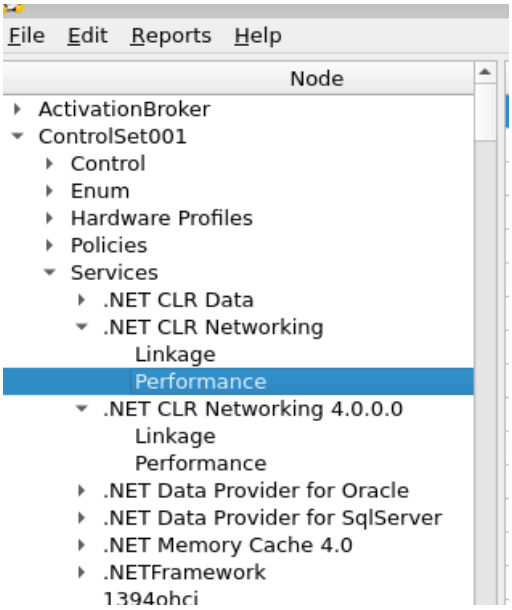
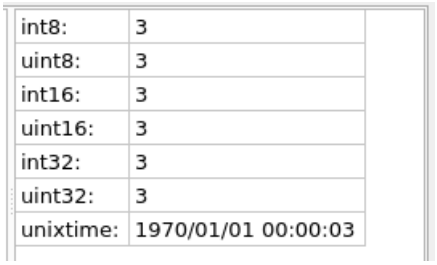


Fig 21: Services list

- 2 means automatically,
- 3 means manually
- 4 means disabled



int8:	3
uint8:	3
int16:	3
uint16:	3
int32:	3
uint32:	3
unixtime:	1970/01/01 00:00:03

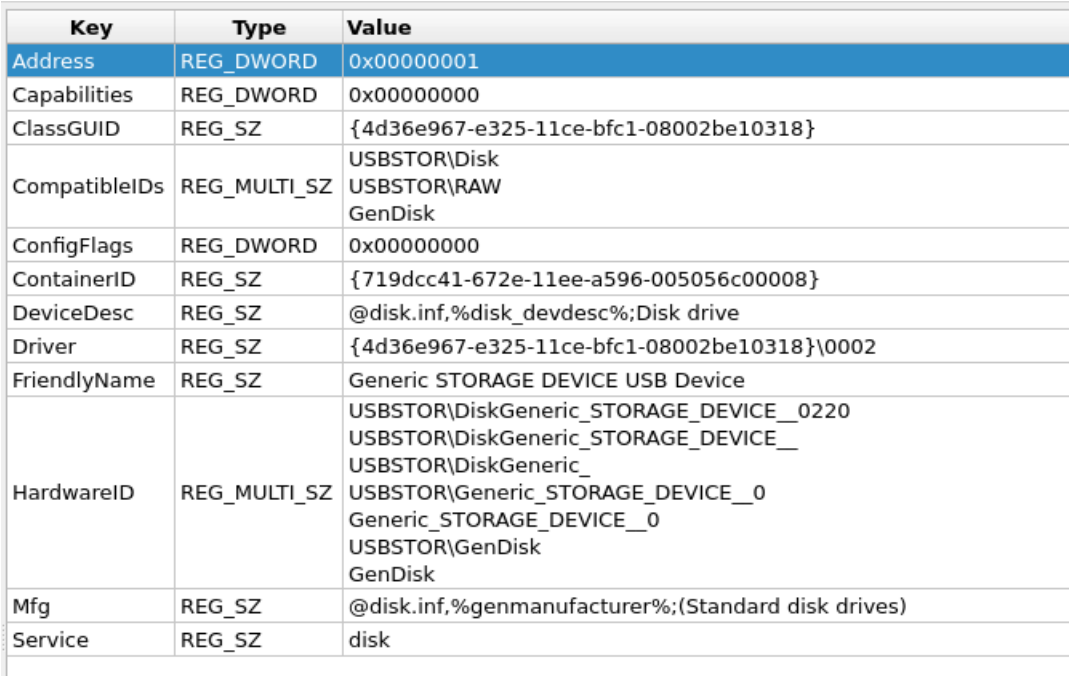
Fig 22: System int code (specific service)

Step 9: To check what are the external drivers have been attached to the system

- Hive:SYSTEM
- Path: System>controlSer>Enum>USBSTOR

USBSTOR	2023/10/10 05:35:17
Disk&Ven_Generic&Prod_STORAGE_DEVICE&Rev_0220	2023/10/10 05:35:17
Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00	2023/09/25 13:57:21
{5d624f94-8850-40c3-a3fa-a4fd2080baf3}	2022/09/24 16:40:19
{8e7bd593-6e6c-4c52-86a6-77175494dd8e}	2022/09/30 10:42:56
{DD8E82AE-334B-49A2-AEAE-AEB0FD5C40DD}	2022/09/24 16:40:08

Fig 23: List of Drivers connected to the system.



Key	Type	Value
Address	REG_DWORD	0x00000001
Capabilities	REG_DWORD	0x00000000
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000
ContainerID	REG_SZ	{719dcc41-672e-11ee-a596-005056c00008}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0002
FriendlyName	REG_SZ	Generic STORAGE DEVICE USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskGeneric_STORAGE_DEVICE__0220 USBSTOR\DiskGeneric_STORAGE_DEVICE__ USBSTOR\DiskGeneric_ USBSTOR\Generic_STORAGE_DEVICE__0 Generic_STORAGE_DEVICE__0 USBSTOR\GenDisk GenDisk
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

Fig 24: In detailed of the driver.