

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

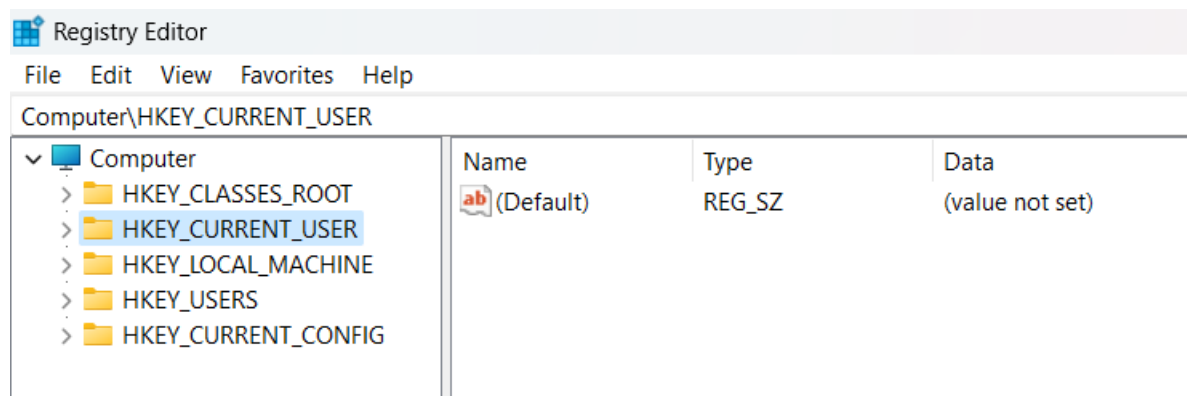
- **Structure:**

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:**

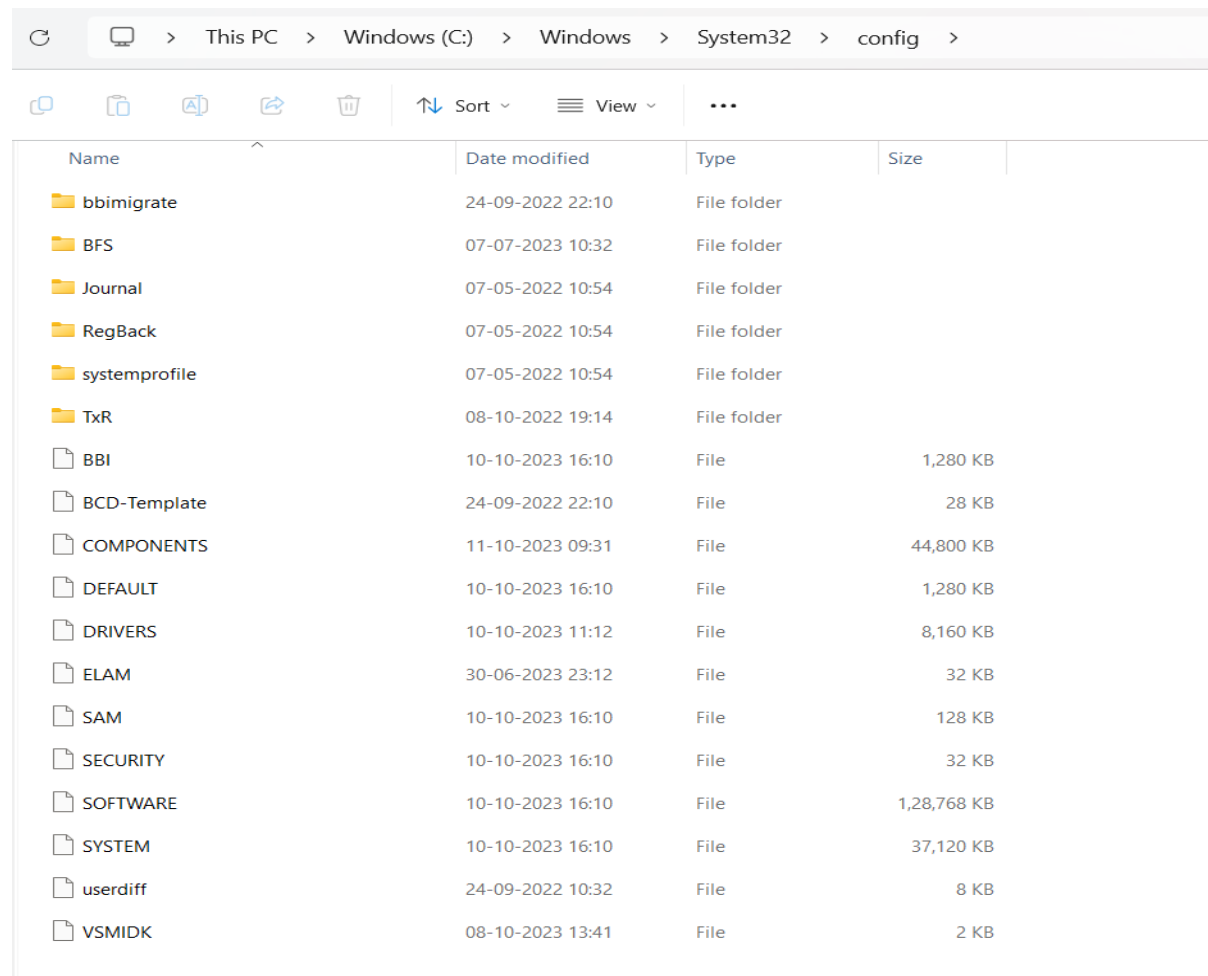
The five primary hives are:

➤ 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.



Name	Date modified	Type	Size
bbimigrate	24-09-2022 22:10	File folder	
BFS	07-07-2023 10:32	File folder	
Journal	07-05-2022 10:54	File folder	
RegBack	07-05-2022 10:54	File folder	
systemprofile	07-05-2022 10:54	File folder	
TxR	08-10-2022 19:14	File folder	
BBI	10-10-2023 16:10	File	1,280 KB
BCD-Template	24-09-2022 22:10	File	28 KB
COMPONENTS	11-10-2023 09:31	File	44,800 KB
DEFAULT	10-10-2023 16:10	File	1,280 KB
DRIVERS	10-10-2023 11:12	File	8,160 KB
ELAM	30-06-2023 23:12	File	32 KB
SAM	10-10-2023 16:10	File	128 KB
SECURITY	10-10-2023 16:10	File	32 KB
SOFTWARE	10-10-2023 16:10	File	1,28,768 KB
SYSTEM	10-10-2023 16:10	File	37,120 KB
userdiff	24-09-2022 10:32	File	8 KB
VSMIDK	08-10-2023 13:41	File	2 KB

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.

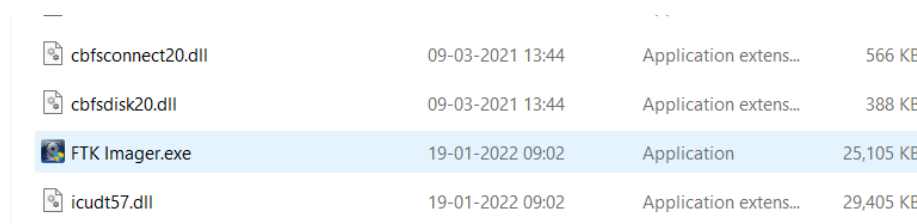
Information that can be found in the registry includes:

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 from flash drive and run the FTK Imager.exe file



cbfsconnect20.dll	09-03-2021 13:44	Application extens...	566 KB
cbfsdisk20.dll	09-03-2021 13:44	Application extens...	388 KB
FTK Imager.exe	19-01-2022 09:02	Application	25,105 KB
icudt57.dll	19-01-2022 09:02	Application extens...	29,405 KB

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..

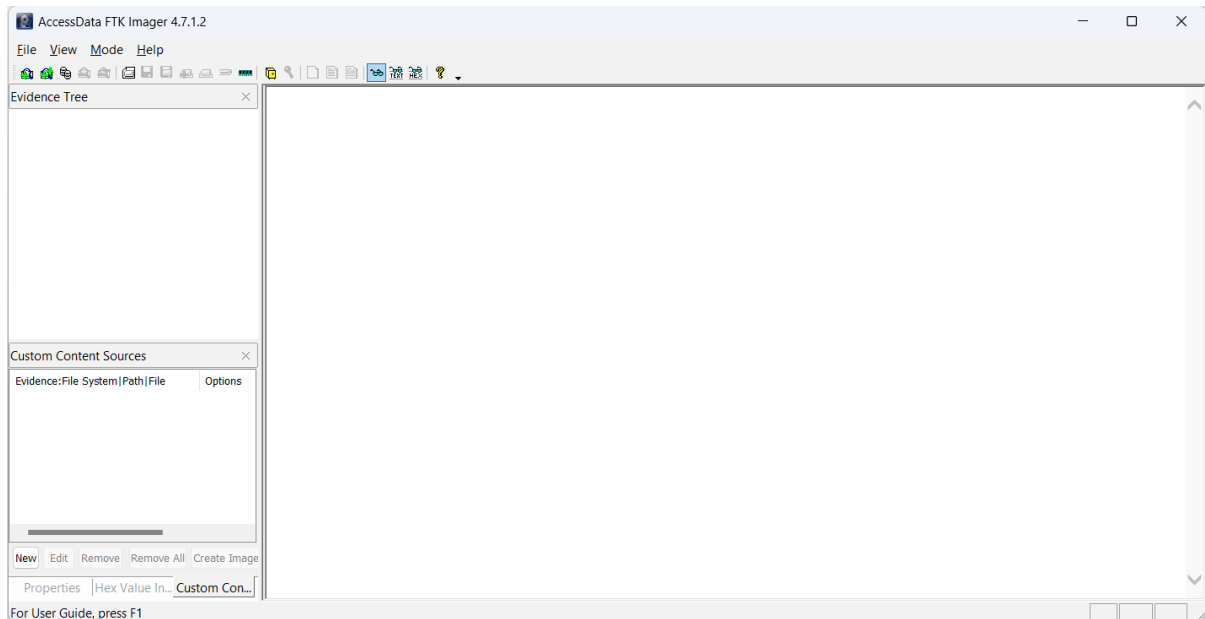


Fig. 3: The FTK Imager's home page

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

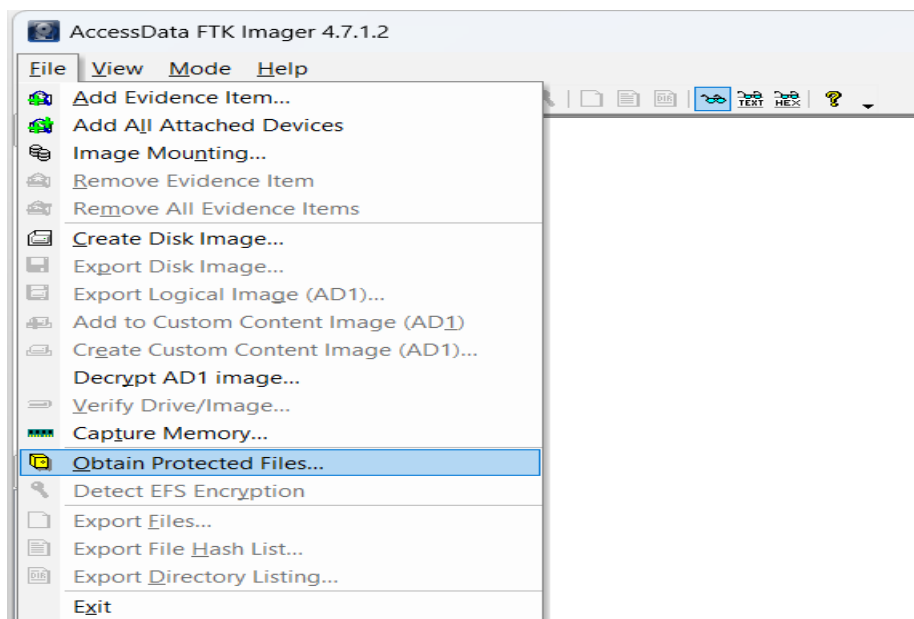
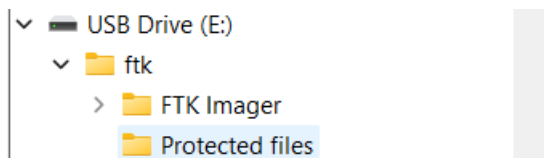


Fig. 4: Image of choosing the option to gather data

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



Step 3: Select the registry 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.

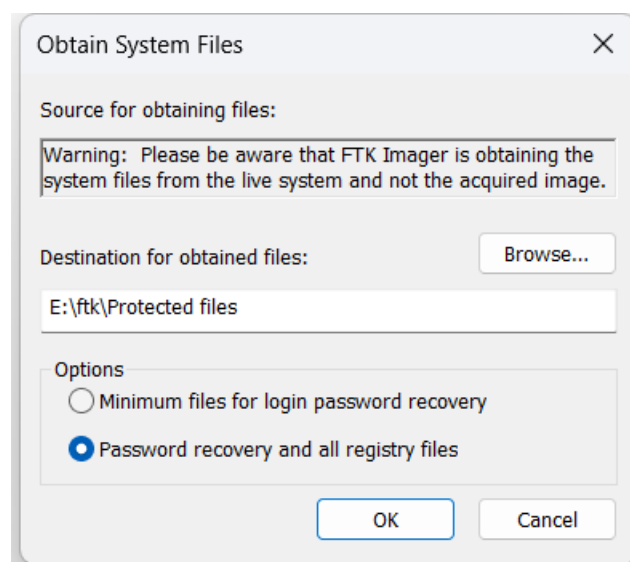
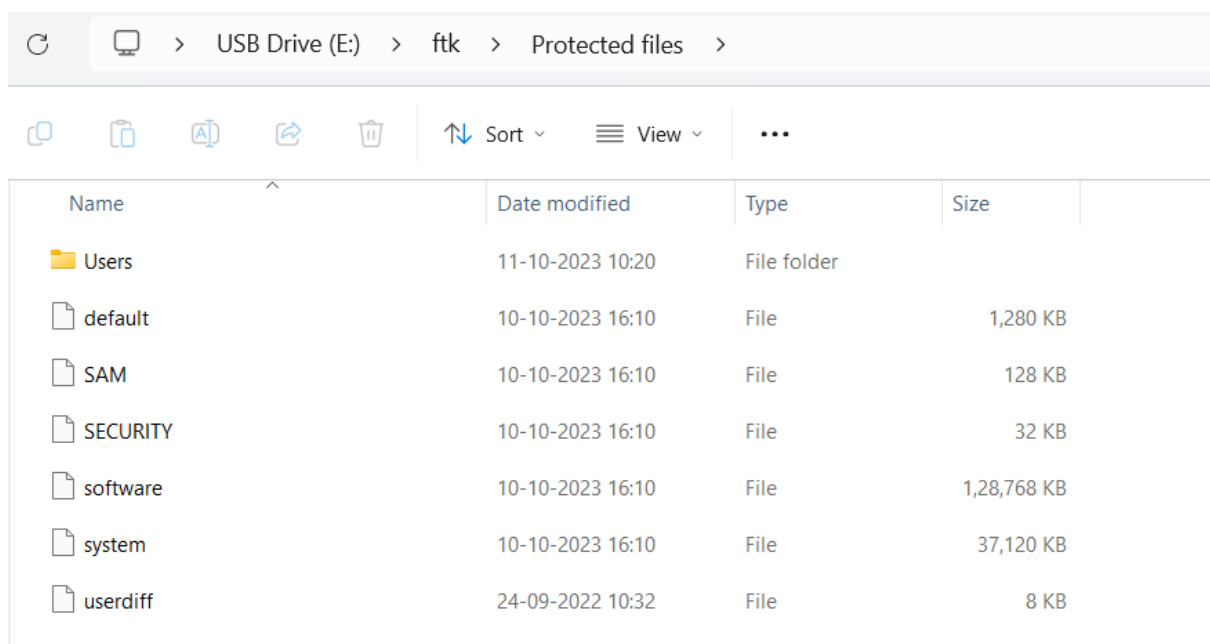


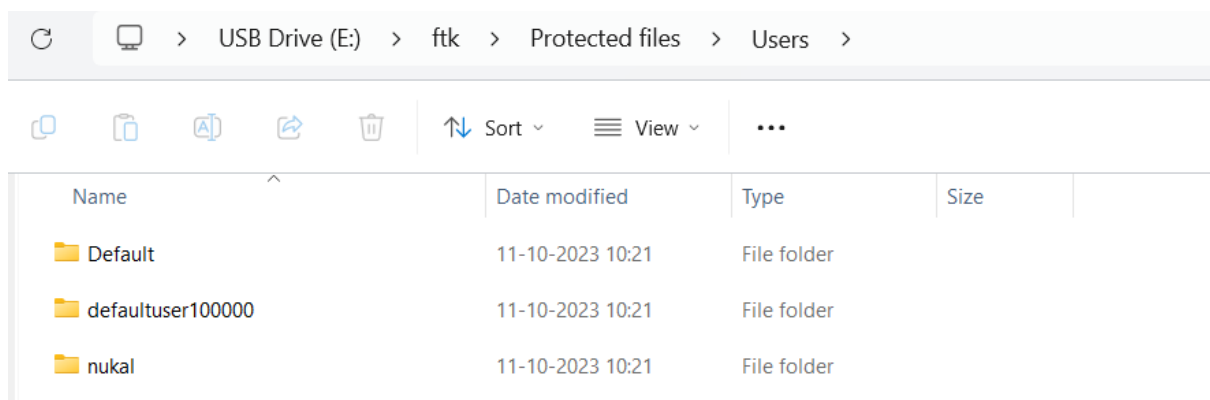
Fig 5: System Files selection

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



Name	Date modified	Type	Size
Users	11-10-2023 10:20	File folder	
default	10-10-2023 16:10	File	1,280 KB
SAM	10-10-2023 16:10	File	128 KB
SECURITY	10-10-2023 16:10	File	32 KB
software	10-10-2023 16:10	File	1,28,768 KB
system	10-10-2023 16:10	File	37,120 KB
userdiff	24-09-2022 10:32	File	8 KB

Fig. 6 shows the mounted files in the folder



Name	Date modified	Type	Size
Default	11-10-2023 10:21	File folder	
defaultuser100000	11-10-2023 10:21	File folder	
nukal	11-10-2023 10:21	File 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

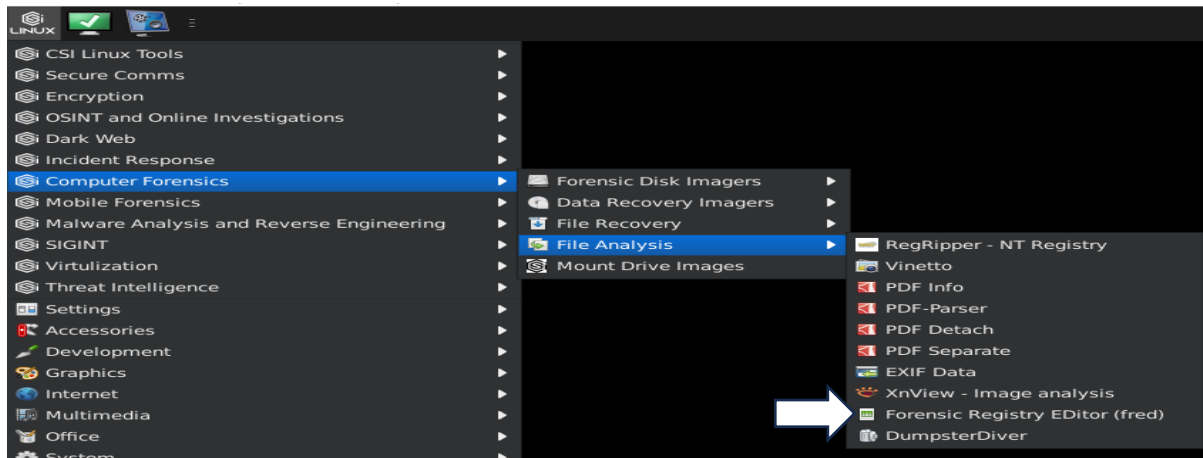


Figure 8: shows the route to the Registry Analysis tool.

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

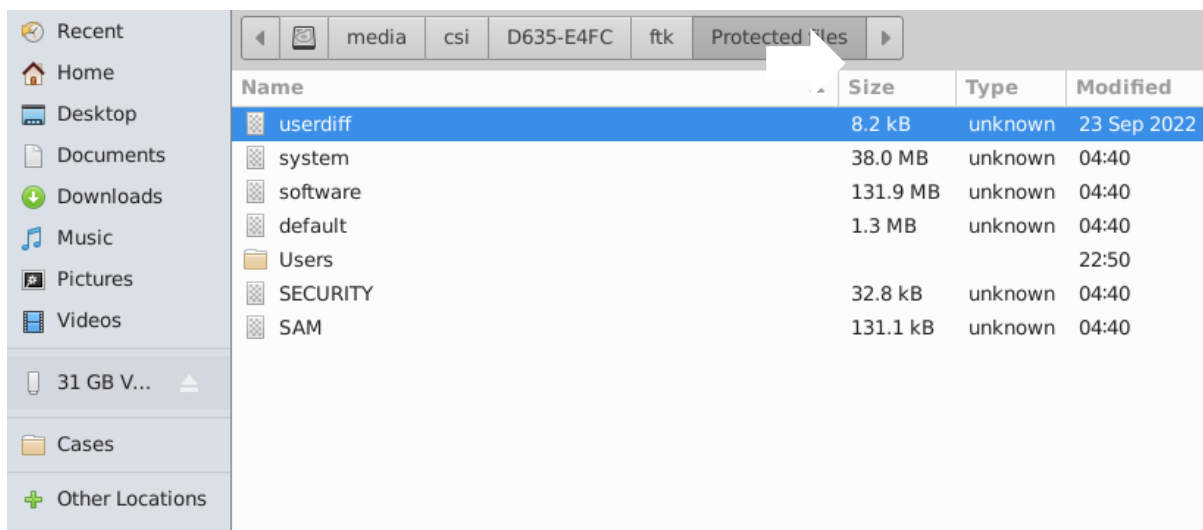


Fig 9: List of HIVES in the folder.

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

- HIVE: Users
- Path: Microsoft>windows NT>current version>networklist>profiles

▼ ProfileList	2023/10/08 08:22:46
S-1-5-18	2022/05/07 05:28:05
S-1-5-19	2022/05/07 05:28:05
S-1-5-20	2022/05/07 05:28:05
S-1-5-21-186879529-4066553570-1488168359-1001	2023/10/11 03:57:09
S-1-5-21-186879529-4066553570-1488168359-1003	2023/01/29 03:42:54
S-1-5-21-186879529-4066553570-1488168359-1005	2023/02/19 04:34:01
S-1-5-21-186879529-4066553570-1488168359-1009	2023/09/25 16:04:38

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

Name	Size	Type	Modified
NTUSER.DAT	262.1 kB	unknown	Fri

Fig 12: File used to investigate.

[illegible]

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

116	REG_BINARY	65 00 6c 00 6b 00 2e 00 64 00 6f 00 63 00 78 00 00 00 66 00 32
117	REG_BINARY	69 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e
118	REG_BINARY	76 00 68 00 65 00 73 00 3f 00 75 00 73 00 70 00 3d 00 73 00 69

Hex viewer		
0000	65 00 6c 00 6b 00 2e 00 64 00 6f 00 63 00 78 00	e.l.k...d.o.c.x.
0010	00 00 66 00 32 00 00 00 00 00 00 00 00 00 00 00	..f.2.....
0020	65 6c 6b 2e 64 6f 63 78 2e 6c 6e 6b 00 00 4a 00	elk.docx.lnk..J.
0030	09 00 04 00 ef be 00 00 00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00 00 00 00 00 00 65 00 6c 00e.l.
0060	6b 00 2e 00 64 00 6f 00 63 00 78 00 2e 00 6c 00	k...d.o.c.x...l.
0070	6e 00 6b 00 00 00 1c 00 00 00	n.k.....

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

15	REG_BINARY	45 00 6d 00 70 00 6c 00 6f 00 79 00 65 00 65 00 53 00 61 00 6d 00
16	REG_BINARY	45 00 6d 00 70 00 6c 00 6f 00 79 00 65 00 65 00 53 00 61 00 6d 00

Hex viewer		
0000	45 00 6d 00 70 00 6c 00 6f 00 79 00 65 00 65 00	E.m.p.l.o.y.e.e.
0010	53 00 61 00 6d 00 70 00 6c 00 65 00 44 00 61 00	S.a.m.p.l.e.D.a.
0020	74 00 61 00 00 00 84 00 32 00 00 00 00 00 00 00	t.a.....2.....
0030	00 00 00 00 45 6d 70 6c 6f 79 65 65 53 61 6d 70EmployeeSamp
0040	6c 65 44 61 74 61 2e 6c 6e 6b 00 00 5e 00 09 00	leData.lnk..^...
0050	04 00 ef be 00 00 00 00 00 00 00 00 00 00 2e 00 00 00
0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00 00 00 00 45 00 6d 00 70 00E.m.p.
0080	6c 00 6f 00 79 00 65 00 65 00 53 00 61 00 6d 00	l.o.y.e.e.S.a.m.
0090	70 00 6c 00 65 00 44 00 61 00 74 00 61 00 2e 00	p.l.e.D.a.t.a...
00a0	6c 00 6e 00 6b 00 00 00 26 00 00 00	l.n.k...&...

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 explorer> typed url

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

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

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

▼ Interfaces	2023/09/16 05:25:10
{12b38ffe-aa12-4145-a792-f2c179a2b78a}	2022/11/29 09:43:08
{155bf64c-8f80-11ea-a50f-806e6f6e6963}	2022/11/30 15:38:13
{181ef3a7-f6fa-4499-b871-de7464665202}	2022/11/29 09:43:08
▶ {32b5d256-6885-40ae-a31a-e4e05e62567b}	2023/10/11 04:31:27
{46f91e9b-731a-47c6-9795-face872c372d}	2023/10/10 07:55:40
{691e9ea9-ef40-4447-b9a7-4e63c9e0a4db}	2022/11/29 09:43:08
{6aa70ea2-83bc-44e4-981e-6b5e4b409706}	2023/03/18 07:43:29
{6b0e23b9-24ef-4434-b42a-4b0b06c05bc4}	2023/10/11 04:40:32
{78007ad6-3ac6-4f38-aa9a-055a94ec366a}	2023/10/10 10:41:24
{95f58b6c-86d2-42b3-915f-4449292512d1}	2022/11/29 09:43:08
{b59f3564-0ecc-4988-993a-d08ceeaadca3}	2023/10/10 10:41:24
{ba0205ae-ea37-4bd4-8b2f-cfa2cb6c8a4c}	2022/11/29 09:43:08
{c3467c78-0002-4112-ba32-f7933829fada}	2023/10/11 03:55:04
{d63055e5-1f52-4f51-8479-6777dd1bcbe}	2023/09/15 06:59:05
{da63f254-d233-4b38-9369-49a0f923f373}	2023/10/11 03:55:04
{dafcf77c-5acb-46a8-b1eb-bdb291f6a768}	2023/10/11 04:40:32
{e7cb8835-1cba-4ee5-b344-456693e6fb44}	2023/09/15 06:59:05

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

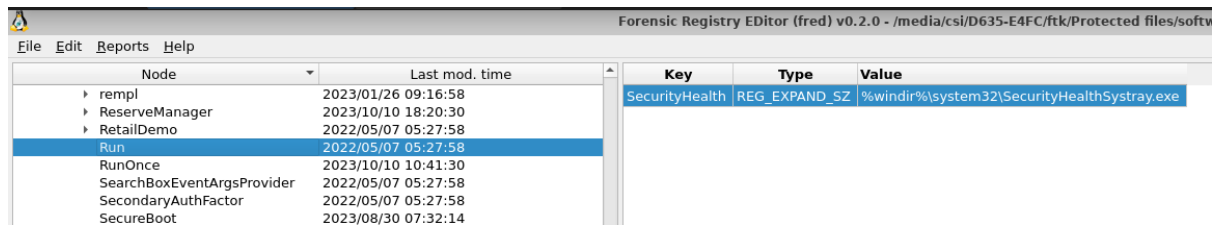


Fig 19: Programs that System automatically launches.

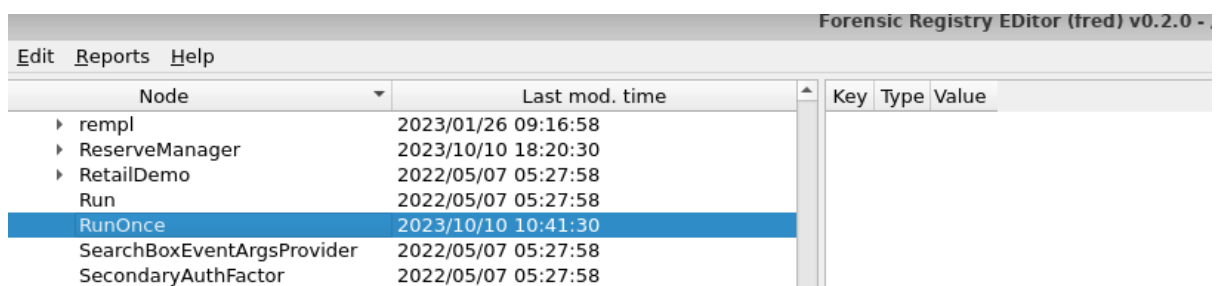


Fig 20: Programs that System launches once.

Note: Seems that hacker not installed any malware

Step 8: programs that System automatically launches.

- HIVE: SYSTEM
- system>CurrentControlSet>Services

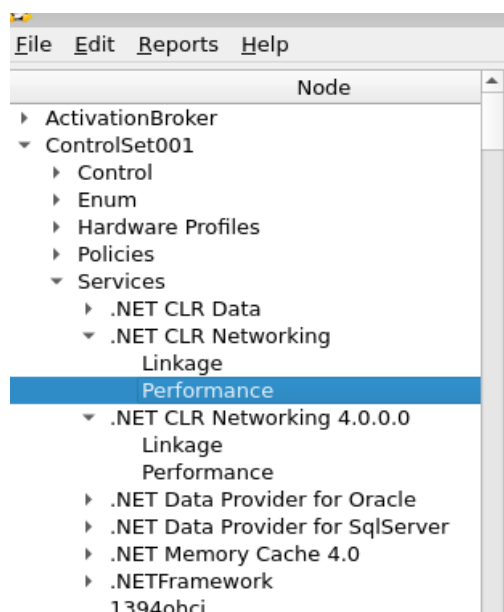


Fig 21: Services list

- 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.

Handwritten signature