Assignment # 1(Set USB to "Read-Only" Mode When Inserted into a System, 2 DD Image Creation and Forensic Analysis Using Autopsy, Forensic Analysis of the DD Image Using Autopsy

Syed Abdul Basit

ID: 24109120

TASK # 1:

Set USB to "Read-Only" Mode When Inserted into a System

To prevent any accidental modifications or data tampering, the goal is to configure the USB drive so that it becomes read-only when connected to a system. This ensures that the data on the USB can only be viewed and not altered.

1.Open the Registry Editor:

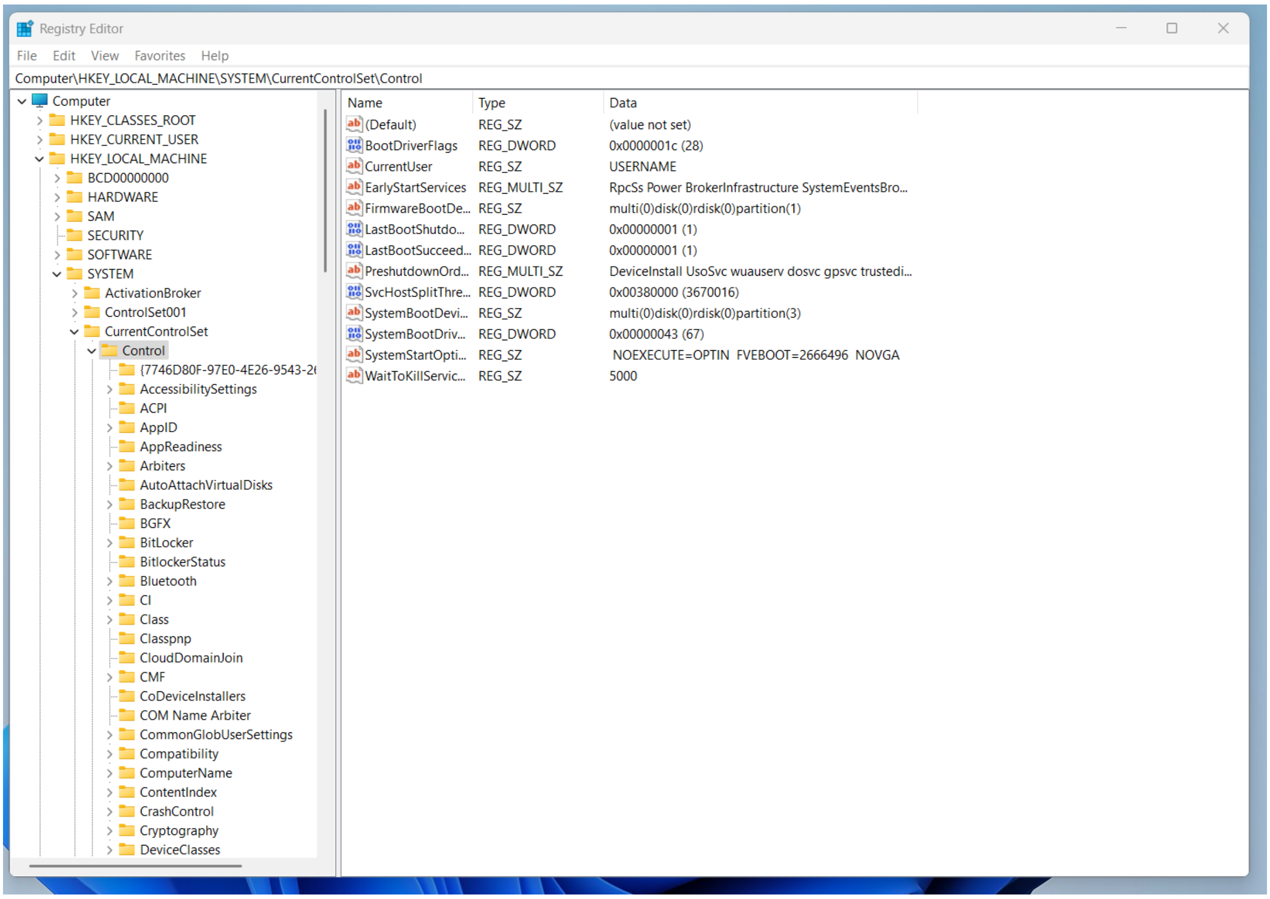
- Press **Win** + **R** to open the **Run** dialog box.
- Type regedit and press **Enter**.

2. Navigate to the USB Storage Key:

- In the Registry Editor, go to the following path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

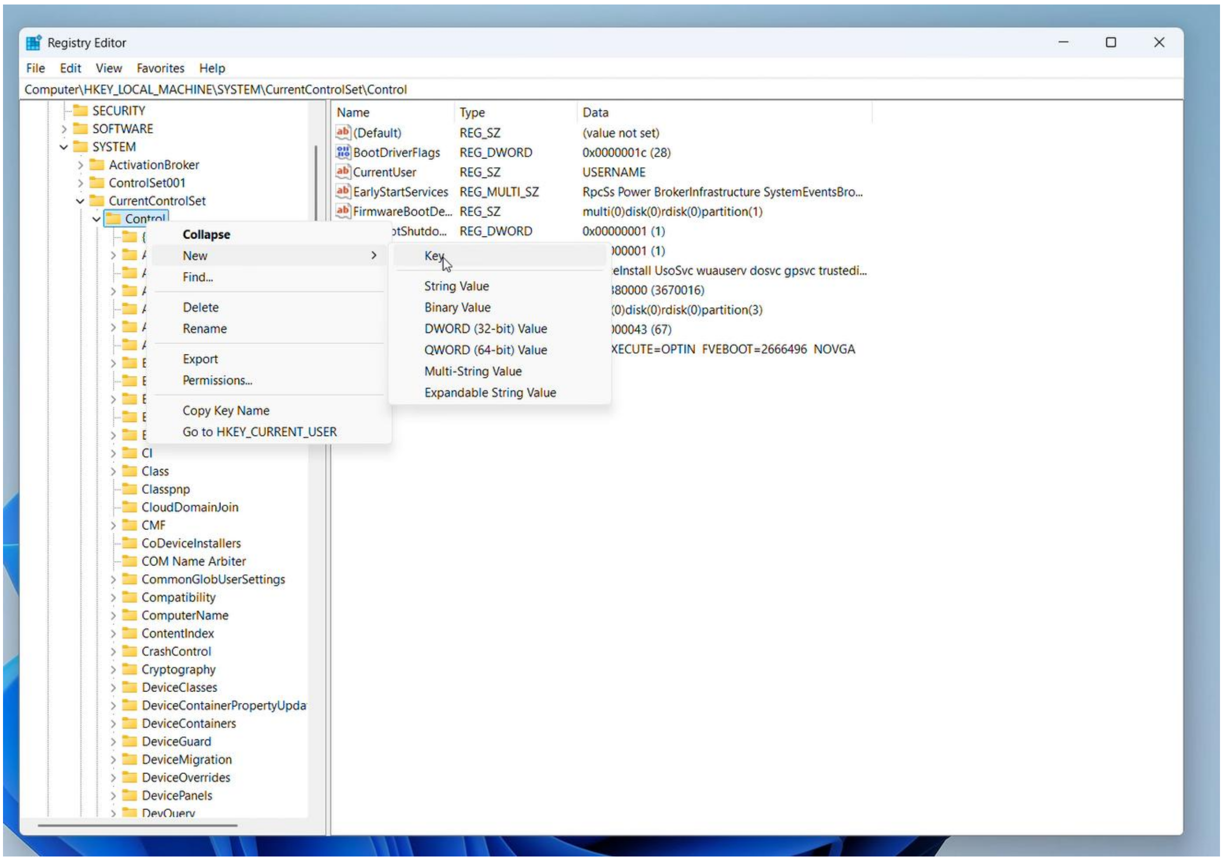
3. Scroll down and look for the **"StorageDevicePolicies"** key. If you don't see it, you may need to create it (right-click on **Control** → **New** → **Key**, and name it **StorageDevicePolicies**).



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ActivationBroker
      ControlSet001
      CurrentControlSet
        Control
          {7746D80F-97E0-4E26-9543-2(
          AccessibilitySettings
          ACPI
          AppID
          AppReadiness
          Arbiters
          AutoAttachVirtualDisks
          BackupRestore
          BGFX
          BitLocker
          BitlockerStatus
          Bluetooth
          CI
          Class
          Classpnp
          CloudDomainJoin
          CMF
          CoDeviceInstallers
          COM Name Arbiter
          CommonGlobUserSettings
          Compatibility
          ComputerName
          ContentIndex
          CrashControl
          Cryptography
          DeviceClasses
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
BootDriverFlags	REG_DWORD	0x0000001c (28)
CurrentUser	REG_SZ	USERNAME
EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure SystemEventsBro...
FirmwareBootDe...	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)
LastBootShutdo...	REG_DWORD	0x00000001 (1)
LastBootSucceed...	REG_DWORD	0x00000001 (1)
PreshutdownOrd...	REG_MULTI_SZ	DeviceInstall UsoSvc wuauserv dosvc gpsvc trustedi...
SvcHostSplitThre...	REG_DWORD	0x00380000 (3670016)
SystemBootDevi...	REG_SZ	multi(0)disk(0)rdisk(0)partition(3)
SystemBootDriv...	REG_DWORD	0x00000043 (67)
SystemStartOpti...	REG_SZ	NOEXECUTE=OPTIN FVEBOOT=2666496 NOVGA
WaitToKillServic...	REG_SZ	5000



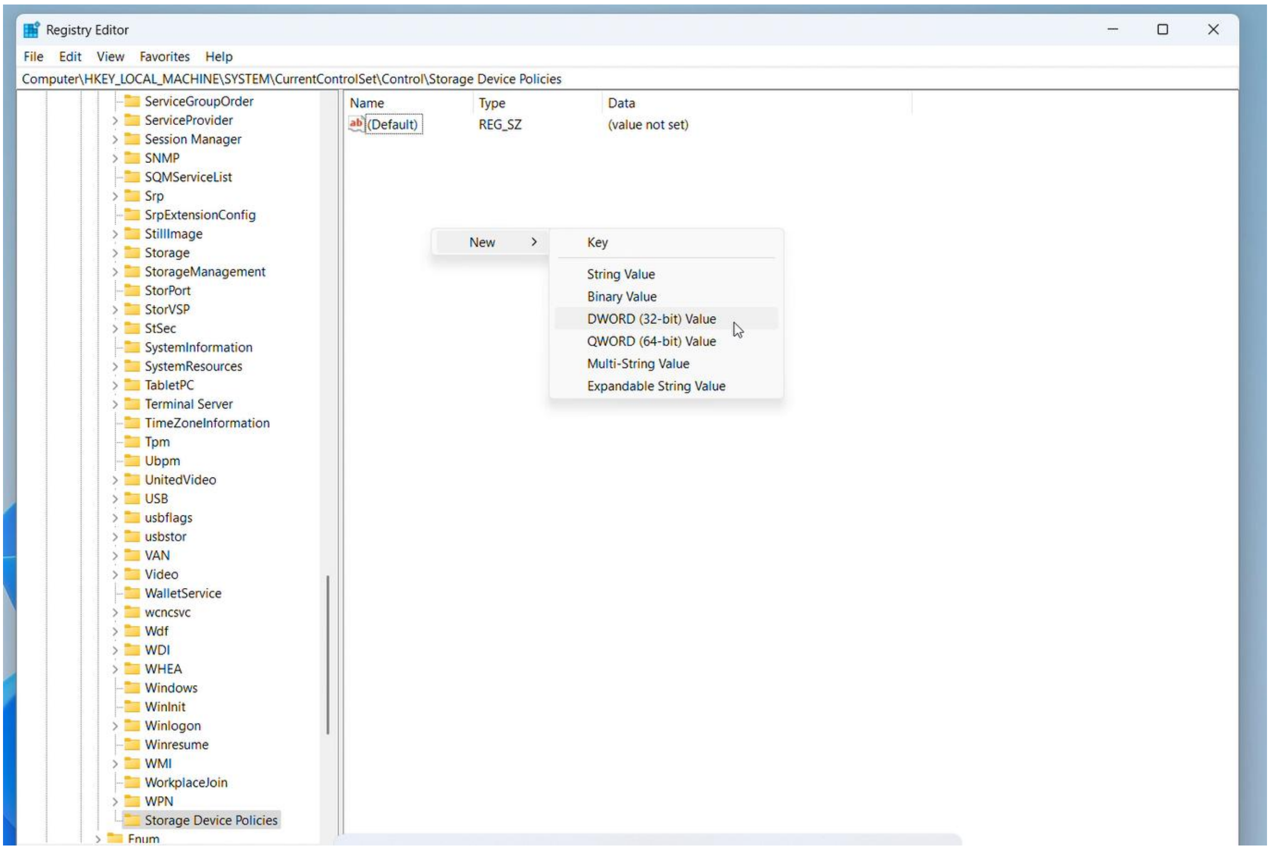
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

Name	Type	Data
(Default)	REG_SZ	(value not set)
BootDriverFlags	REG_DWORD	0x0000001c (28)
CurrentUser	REG_SZ	USERNAME
EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure SystemEventsBro...
FirmwareBootDe...	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)
...otShutdo...	REG_DWORD	0x00000001 (1)
		...)00001 (1)
		...eInstall UsoSvc wuauserv dosvc gpsvc trustedi...
		...380000 (3670016)
		...(0)disk(0)rdisk(0)partition(3)
		...)00043 (67)
		...XECUTE=OPTIN FVEBOOT=2666496 NOVGA

4.Create the WriteProtect Value:

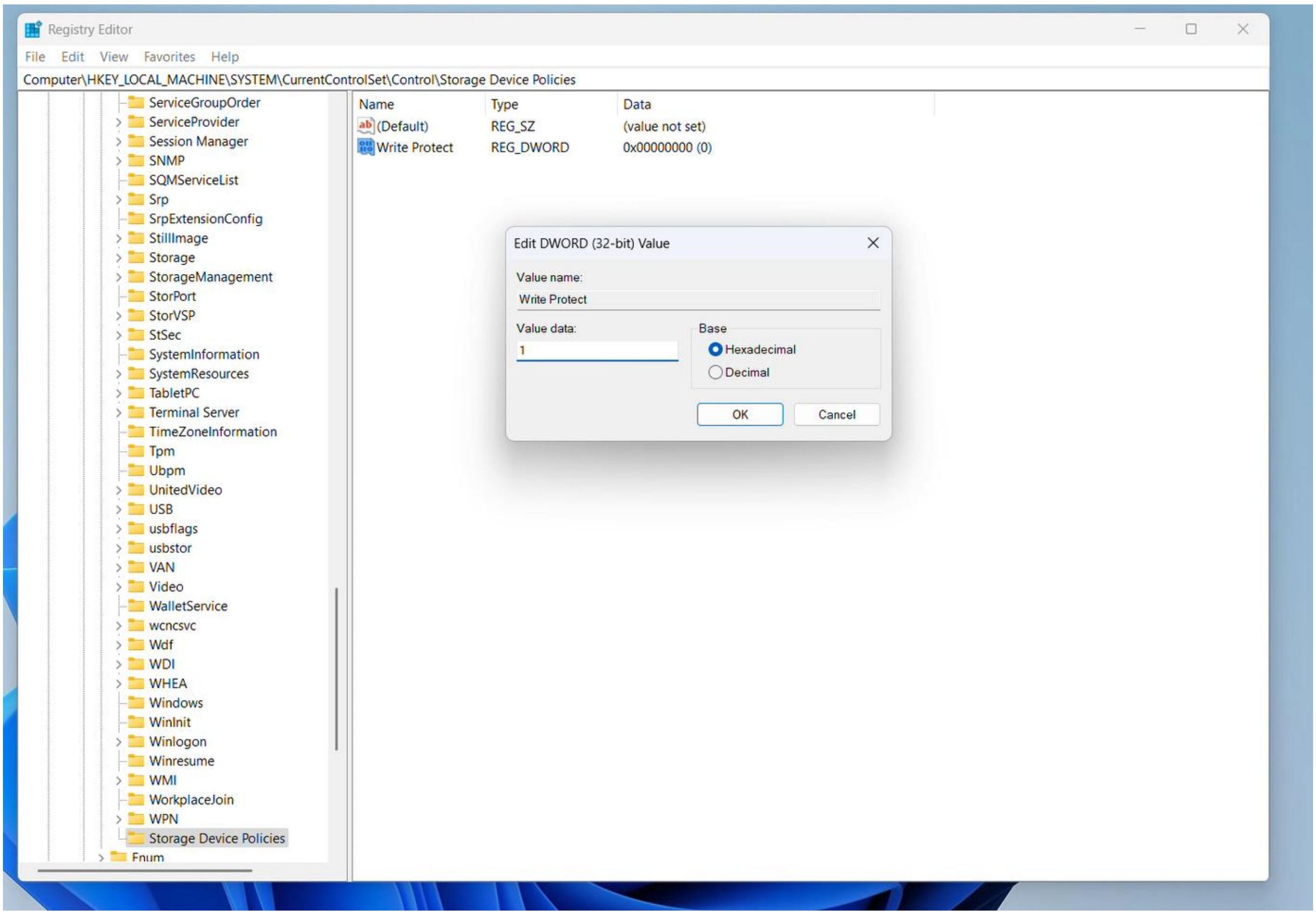
Once inside the StorageDevicePolicies key, right-click in the right pane and choose New → DWORD (32-bit) Value.Name the new value WriteProtect.

5.**Set WriteProtect to 1**: Double-click on **WriteProtect** and change the **Value data** to 1 to enable read-only mode then click **OK**.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Storage Device Policies

Name	Type	Data
(Default)	REG_SZ	(value not set)



Registry Editor

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Storage Device Policies

Name	Type	Data
(Default)	REG_SZ	(value not set)
Write Protect	REG_DWORD	0x00000000 (0)

Edit DWORD (32-bit) Value

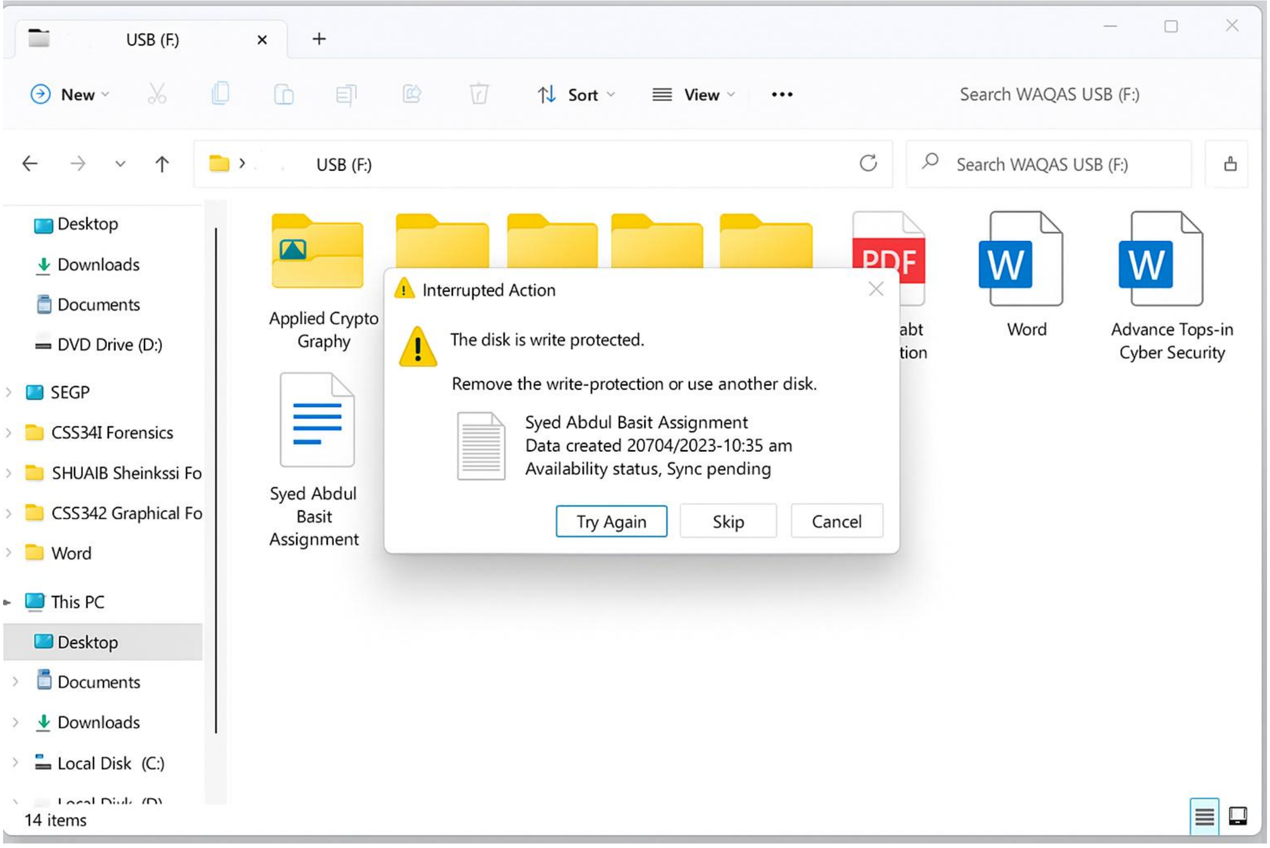
Value name: Write Protect

Value data: 1

Base: ● Hexadecimal ○ Decimal

Conclusion:

In this task, we successfully created a **read-only environment for the USB device** to ensure the integrity of digital evidence. By modifying the Windows Registry and/or using diskpart, we prevented any accidental write operations. A **system restart** was required for the changes to take effect. This setup is crucial in digital forensics to maintain evidence in its original state.



Interrupted Action

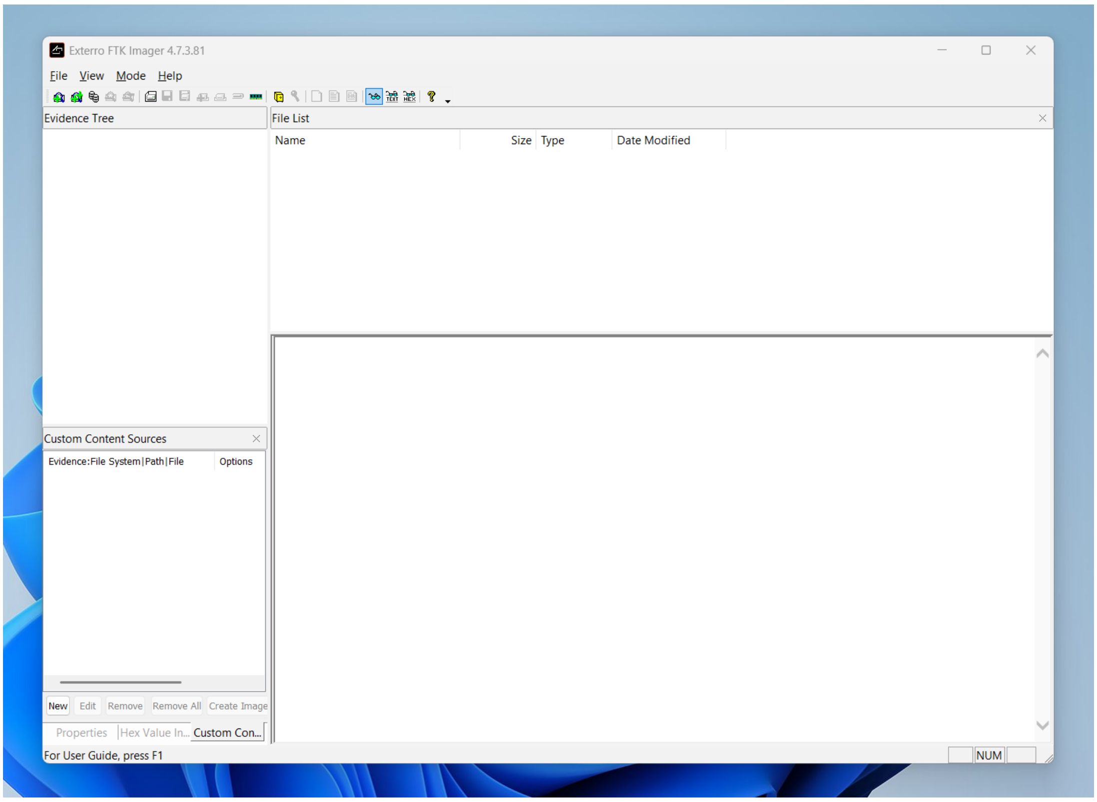
The disk is write protected.

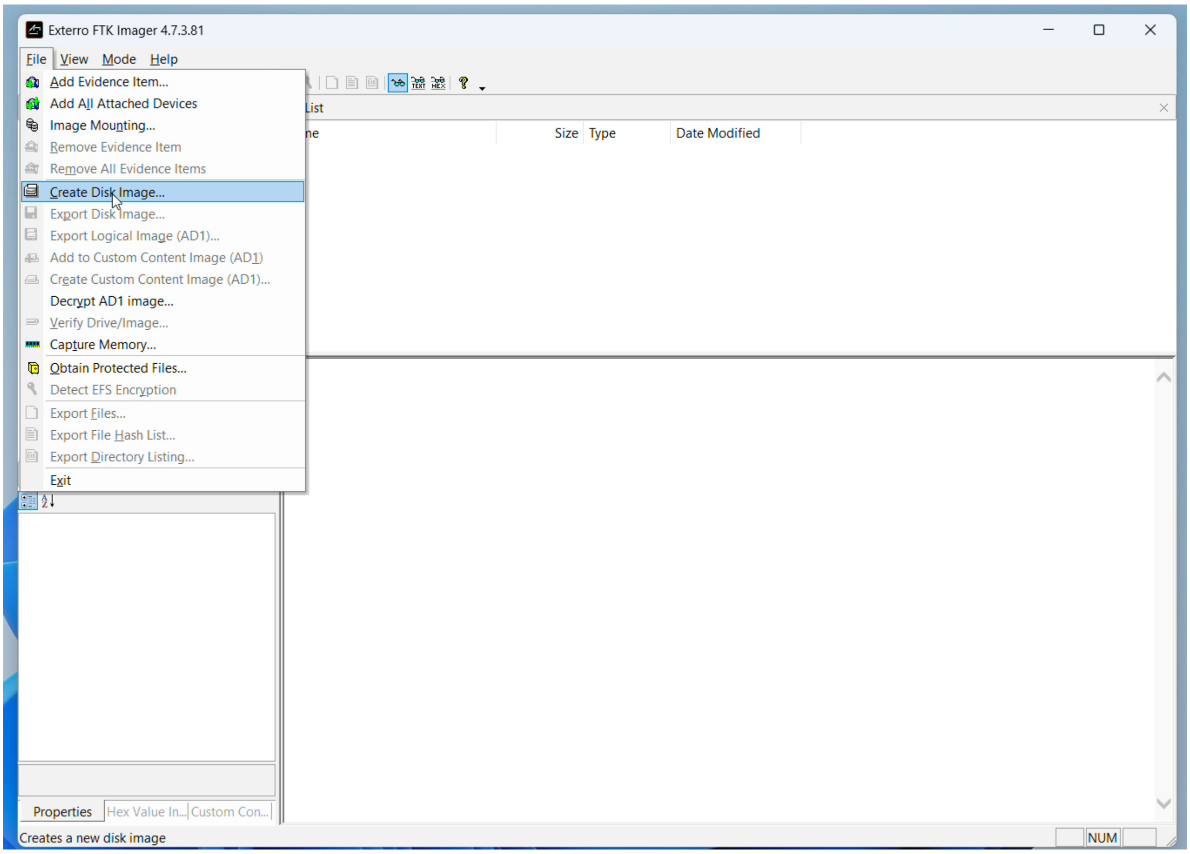
Remove the write-protection or use another disk.

Syed Abdul Basit Assignment
Data created 20704/2023-10:35 am
Availability status, Sync pending

TASK # 2 DD Image Creation and Forensic Analysis Using Autopsy

Step 1: I began by launching FTK Imager, a forensic tool used to create disk images of storage devices. Using this tool, I generated a bit-by-bit duplicate (DD image) of the target USB drive. This raw image format is crucial in digital forensics, as it ensures an exact replica of the original data is captured without making any modifications.

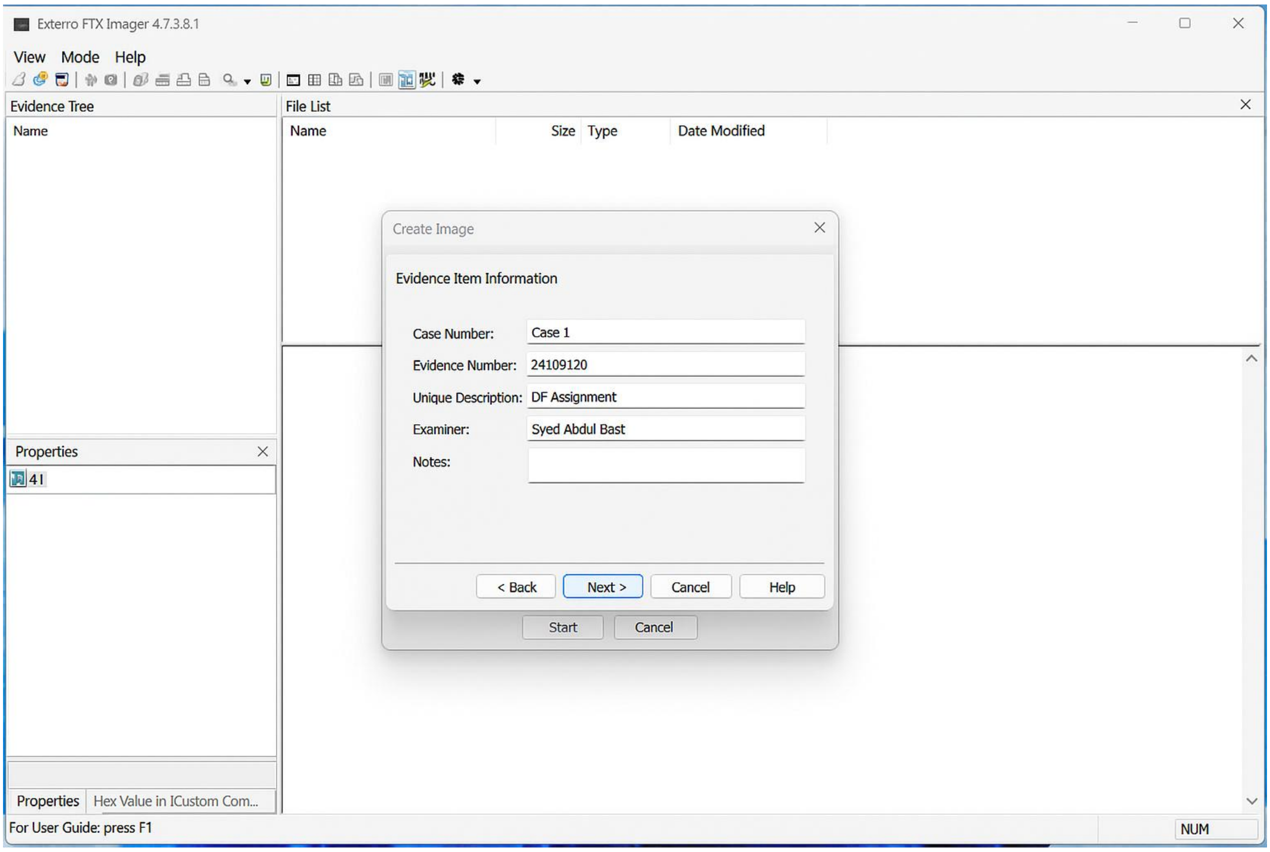




Creates a new disk image

Step 2: After launching FTK Imager, I clicked on "File" in the top menu and selected "Create Disk Image" to begin the forensic imaging process.

1. In the dialog box, I selected the appropriate source type (such as Physical Drive or Logical Drive) based on the target device.



Exterro FTX Imager 4.7.3.8.1

Create Image

Evidence Item Information

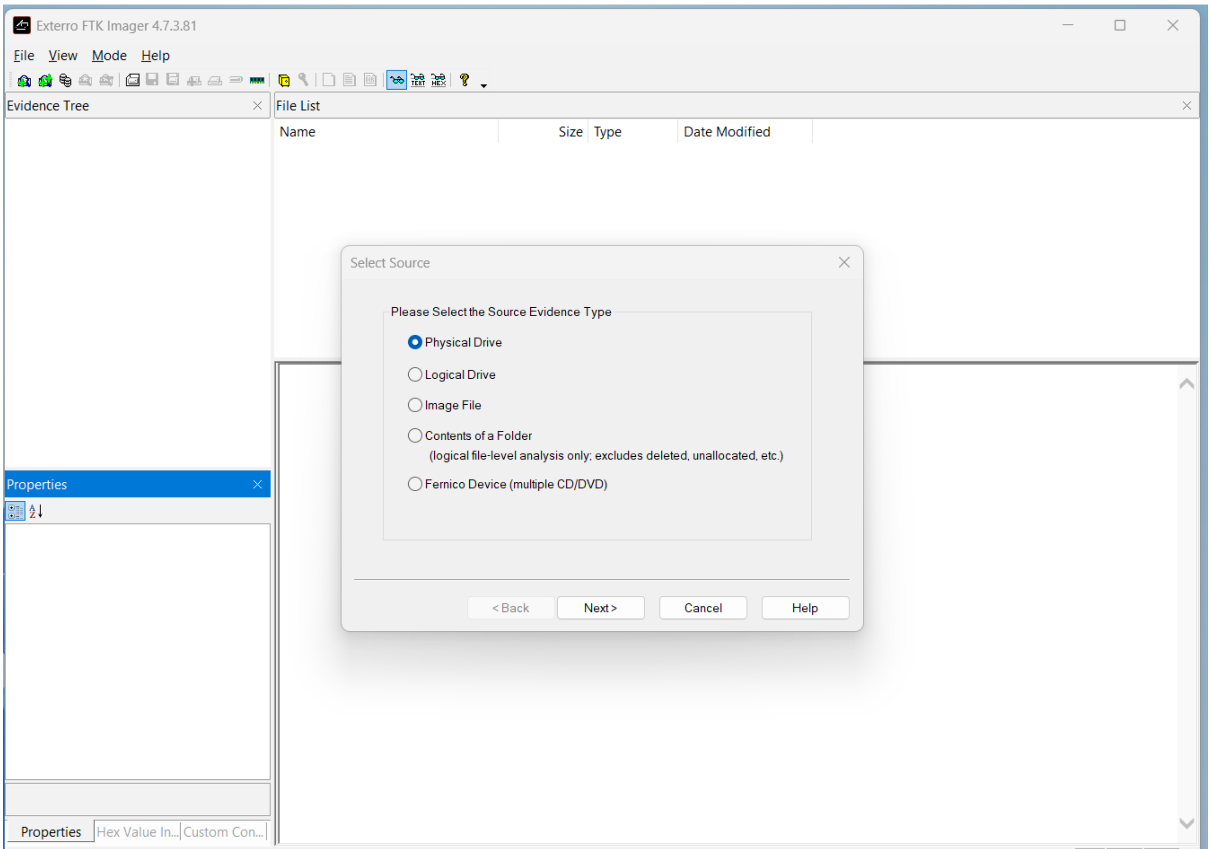
Case Number: Case 1

Evidence Number: 24109120

Unique Description: DF Assignment

Examiner: Syed Abdul Bast

Notes:



Exterro FTK Imager 4.7.3.81

Select Source

Please Select the Source Evidence Type

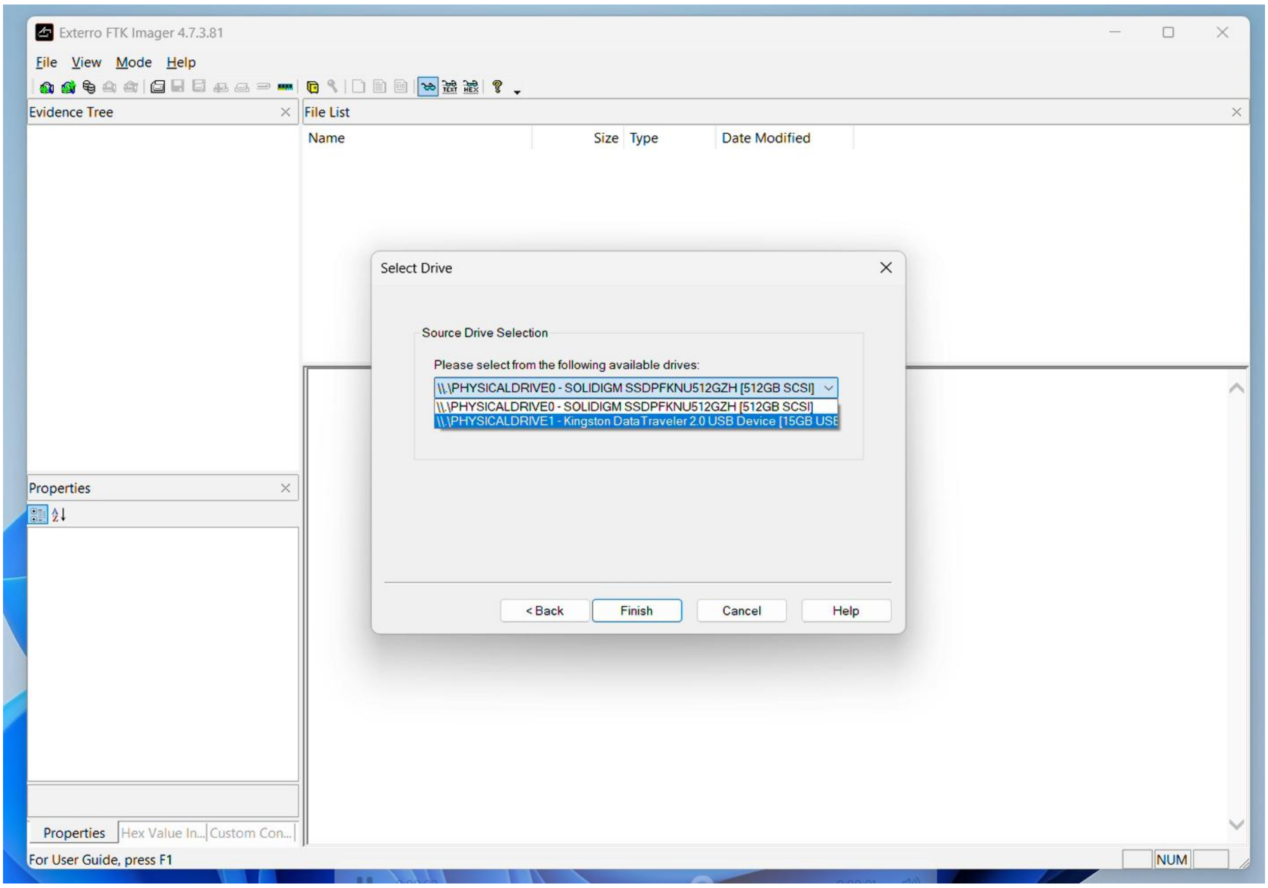
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)



Select Drive

Source Drive Selection

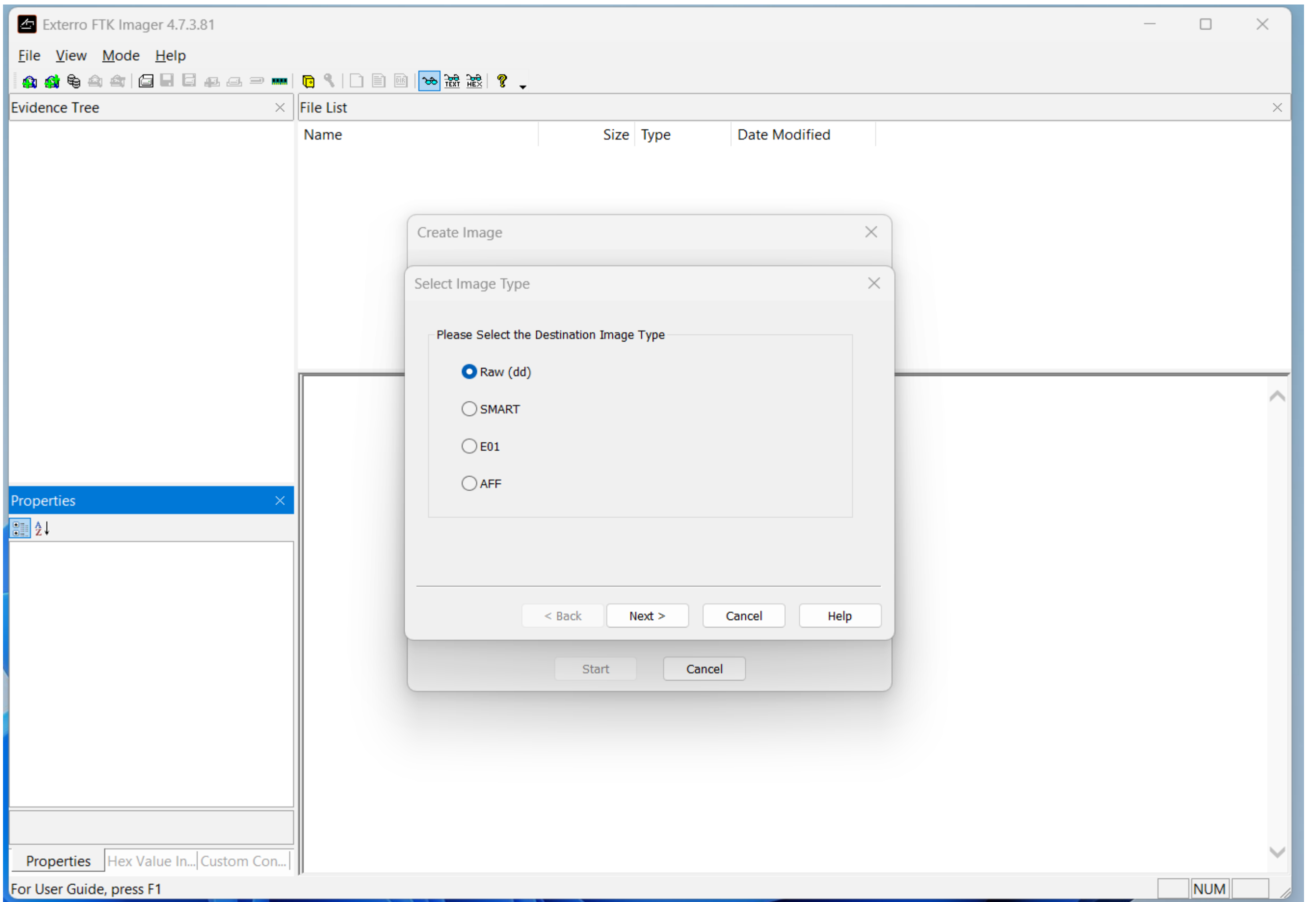
Please select from the following available drives:

\\.\PHYSICALDRIVE0 - SOLIDIGM SSDPFKNU512GZH [512GB SCSI]

\\.\PHYSICALDRIVE0 - SOLIDIGM SSDPFKNU512GZH [512GB SCSI]
\\.\PHYSICALDRIVE1 - Kingston DataTraveler 2.0 USB Device [15GB USE

2. I selected the correct drive to image by choosing my USB drive from the available list.

3. I chose **"Raw (dd)"** as the image type to obtain an exact bit-by-bit copy of the USB drive.



Exterro FTK Imager 4.7.3.81

Create Image

Select Image Type

Please Select the Destination Image Type

● Raw (dd)

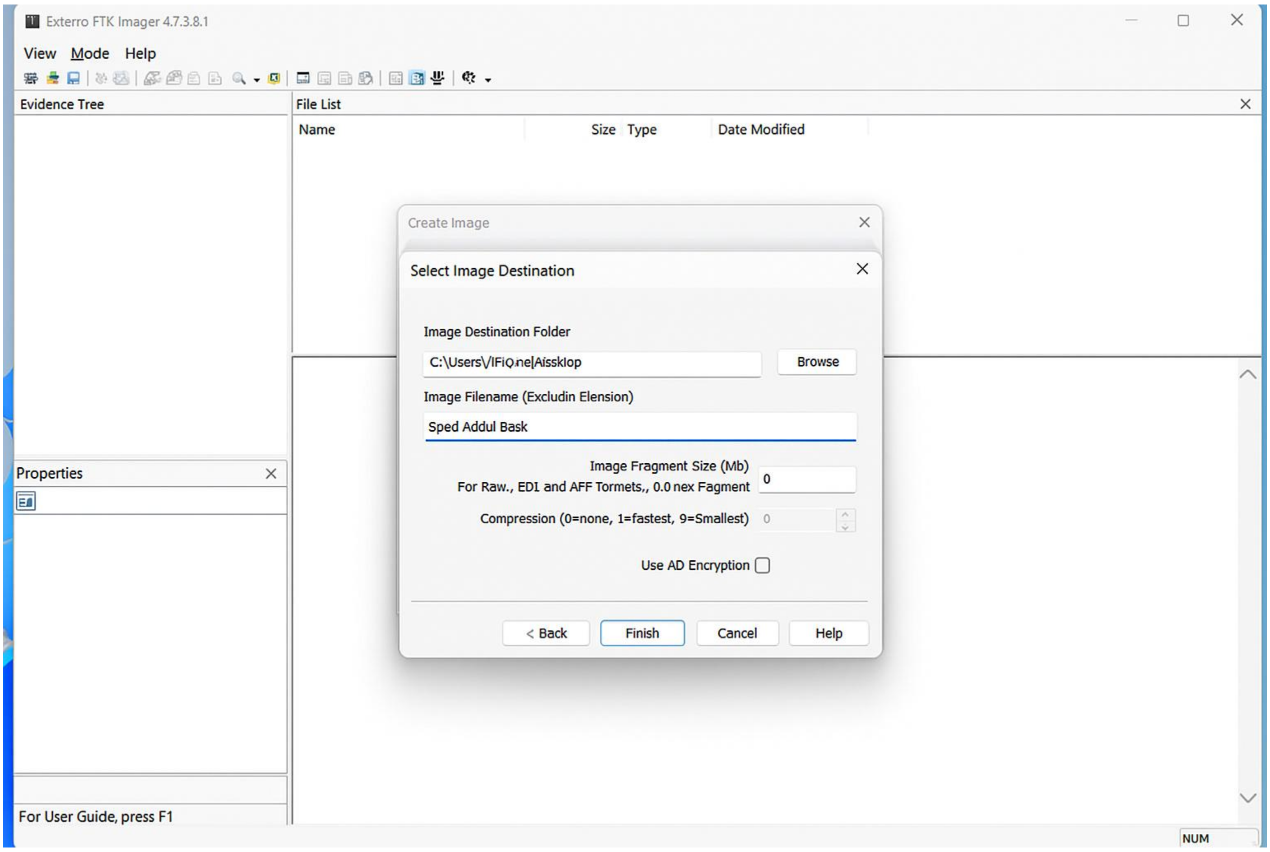
○ SMART

○ E01

○ AFF

4.Entered optional case information for documentation, such as case number and examiner name.

5. Set the image fragment size to 0, which means the image will not be split and will be saved as a single .dd file. Chose the destination folder and named the file "Shuaib DF." Clicked "Finish" to start creating the image.



Select Image Destination

Image Destination Folder

C:\Users\/IFiQ.ne|Aissklop

Image Filename (Excludin Elension)

Sped Addul Bask

Image Fragment Size (Mb)
For Raw., EDI and AFF Tormets,, 0.0 nex Fagment: 0

Compression (0=none, 1=fastest, 9=Smallest): 0

Use AD Encryption □

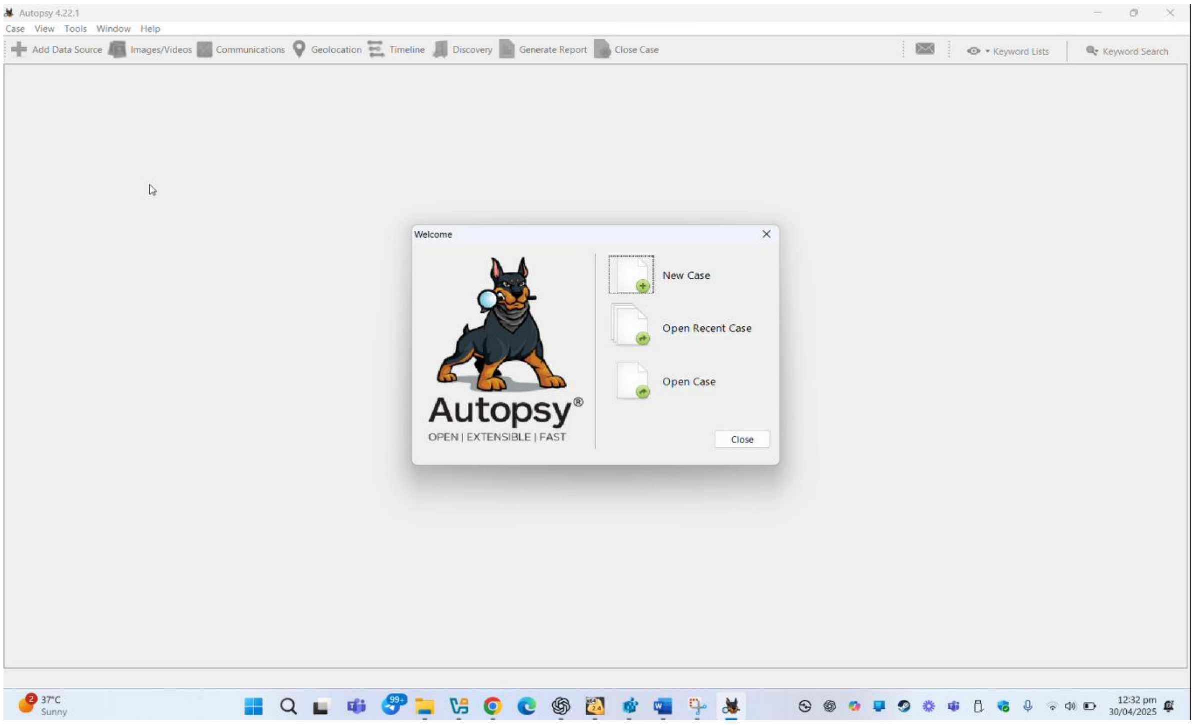
6. Once I clicked **"Finish"**, FTK Imager began creating the DD image of the USB drive. The **progress bar** displayed the status of the imaging process in real-time.

This completed the creation of a verified and hash-checked DD image of your USB drive, which is now ready for forensic analysis in Autopsy.

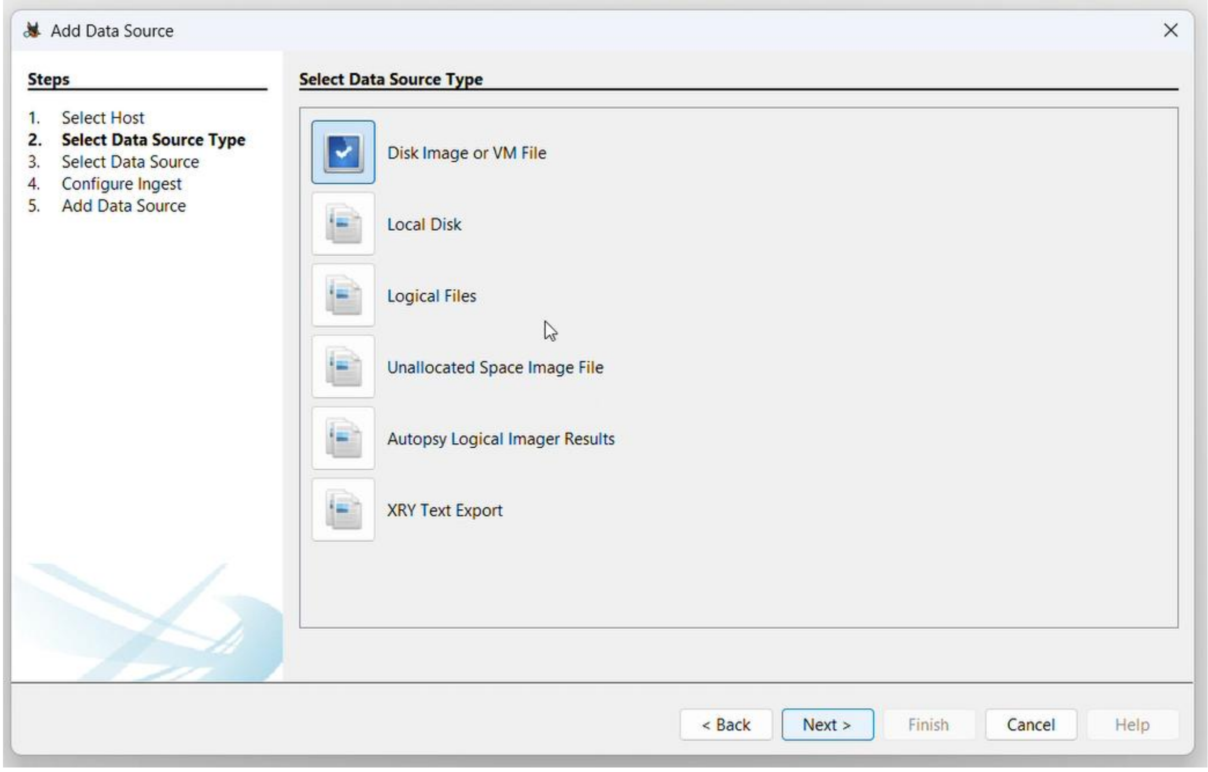
Task # 3: Forensic Analysis of the DD Image Using Autopsy

Once the .dd image was created, I utilized Autopsy, a digital forensics tool, to investigate the image's contents. Here are the steps I took:

1: Opened Autopsy and selected "Create New Case" to start the investigation



2: Entered the case name, base directory, and optional case details, such as the examiner's name, to set up the case.



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

Logical Files

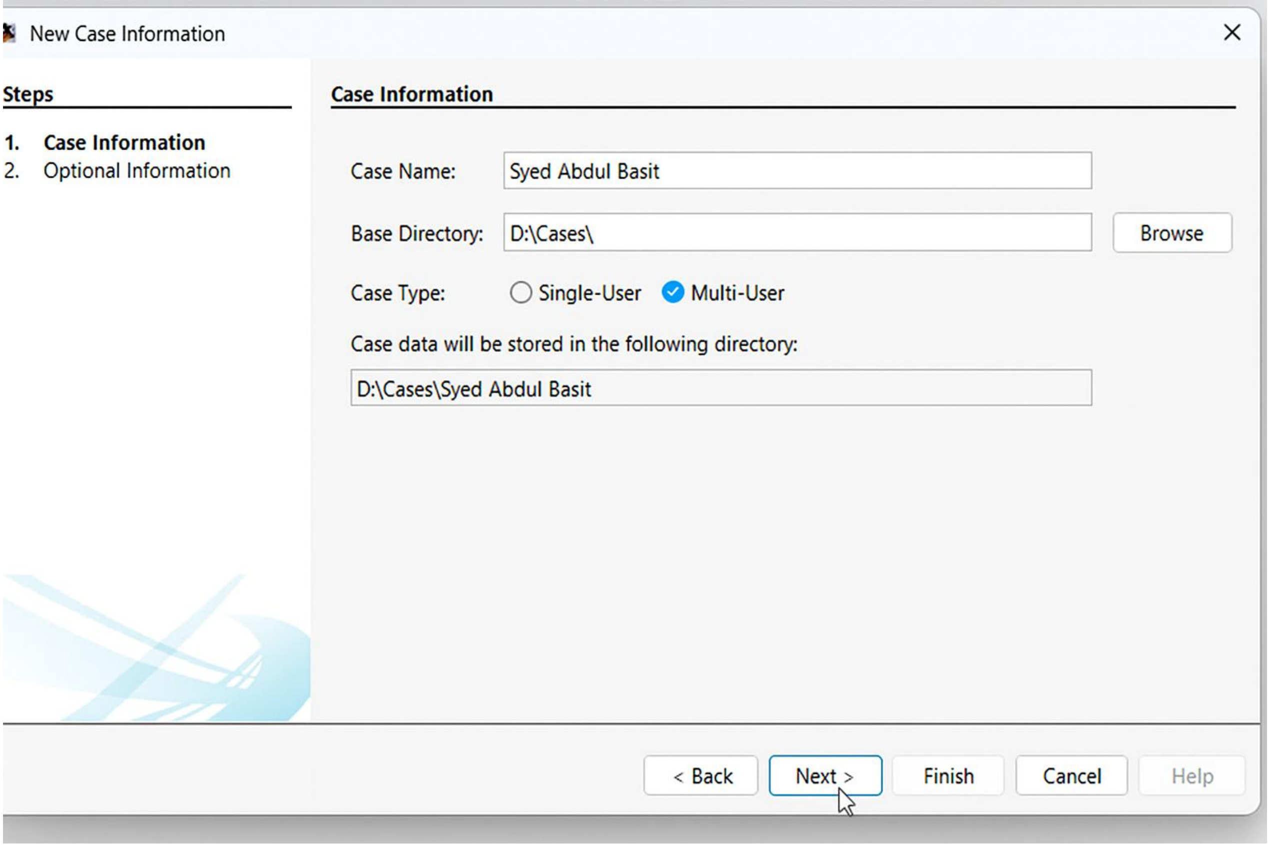
Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

3: Clicked "Next" to proceed, then chose "Add Data Source" to include the DD image for analysis.

4: In the Ingest Module Configuration screen, I selected the essential modules required for analyzing files, web activity, deleted data, and keywords, then clicked "Next."



New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

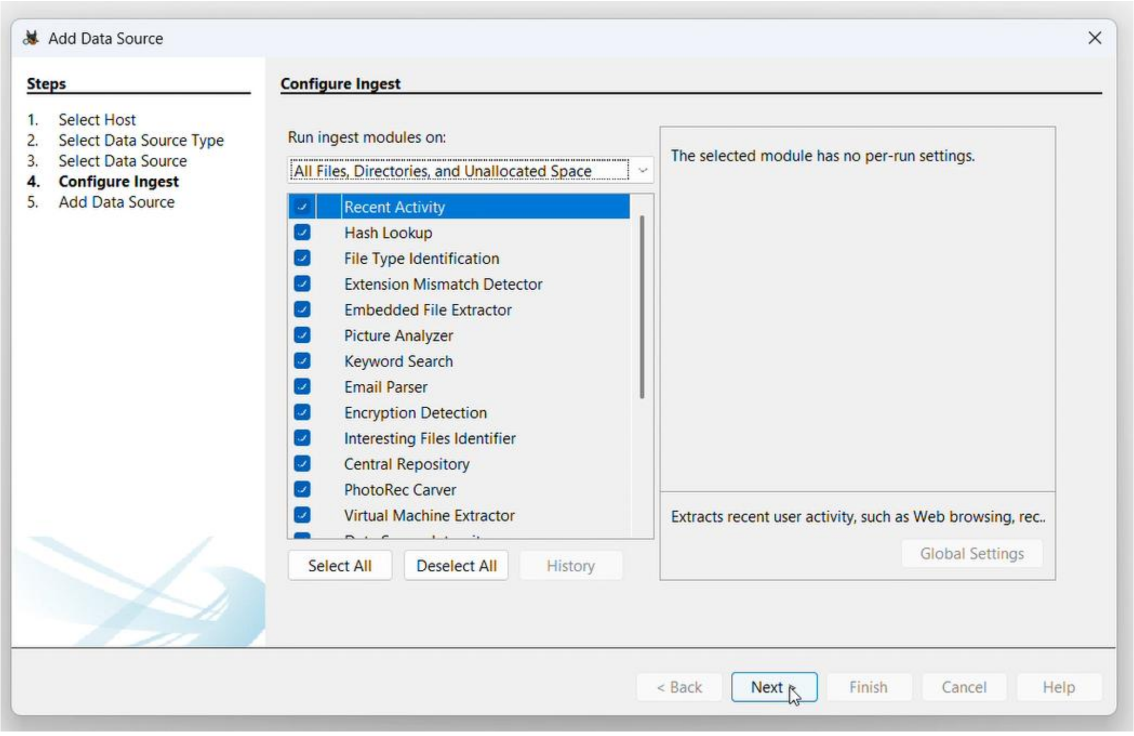
Case Name: Syed Abdul Basit

Base Directory: D:\Cases\

Case Type: ○ Single-User ● Multi-User

Case data will be stored in the following directory:

D:\Cases\Syed Abdul Basit



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

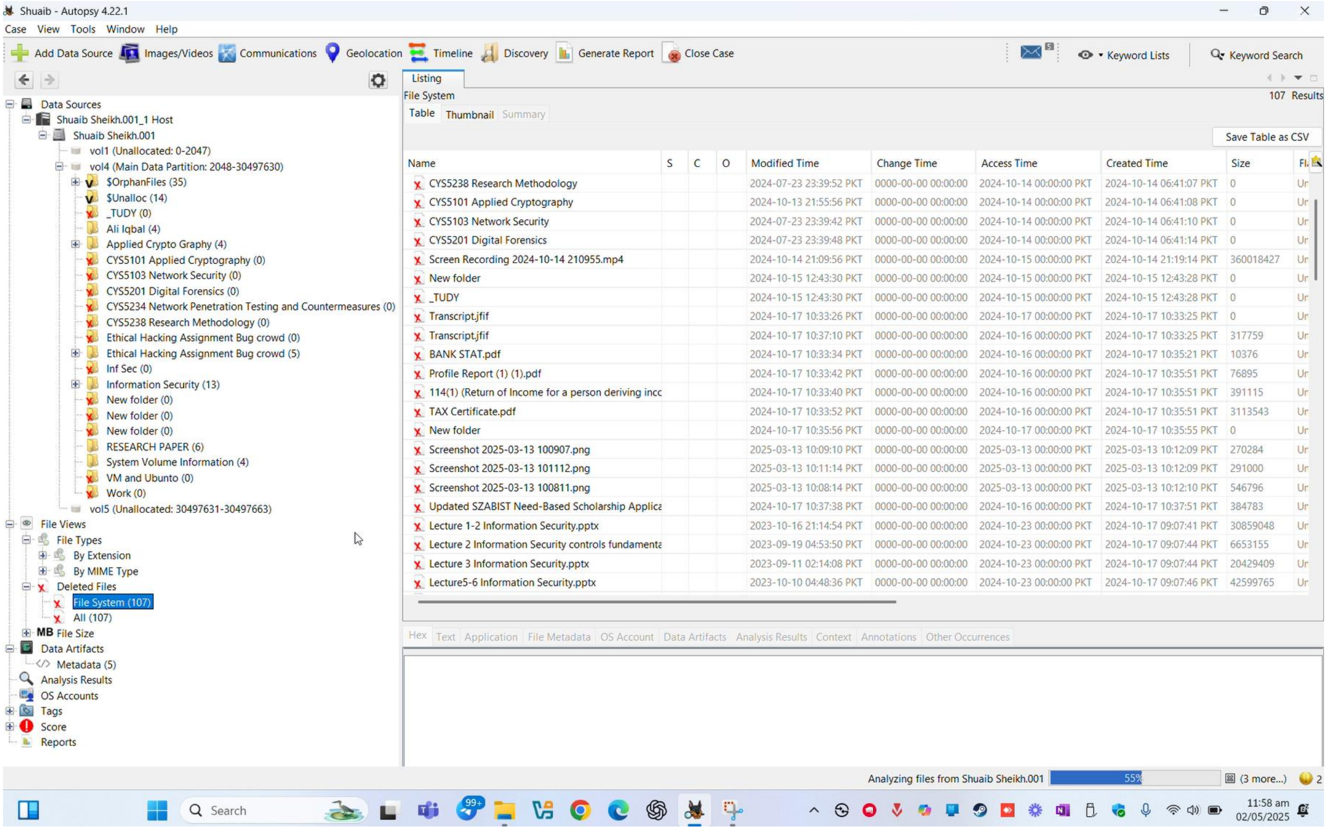
All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rec..

STEP 5: Autopsy began analyzing the image using the selected modules. Shortly after, results started to appear, including active files, deleted files, browsing history, and user activity. All findings were organized and displayed in the left panel under the Tree View.



- Data Sources
  - Shuaib Sheikh.001_1 Host
    - Shuaib Sheikh.001
      - vol1 (Unallocated: 0-2047)
      - vol4 (Main Data Partition: 2048-30497630)
        - $OrphanFiles (35)
        - $Unalloc (14)
        - _TUDY (0)
        - Ali Iqbal (4)
        - Applied Crypto Graphy (4)
        - CYS5101 Applied Cryptography (0)
        - CYS5103 Network Security (0)
        - CYS5201 Digital Forensics (0)
        - CYS5234 Network Penetration Testing and Countermeasures (0)
        - CYS5238 Research Methodology (0)
        - Ethical Hacking Assignment Bug crowd (0)
        - Ethical Hacking Assignment Bug crowd (5)
        - Inf Sec (0)
        - Information Security (13)
        - New folder (0)
        - New folder (0)
        - New folder (0)
        - RESEARCH PAPER (6)
        - System Volume Information (4)
        - VM and Ubuntu (0)
        - Work (0)
      - vol5 (Unallocated: 30497631-30497663)
- File Views
  - File Types
    - By Extension
    - By MIME Type
  - Deleted Files
    - File System (107)
    - All (107)
  - MB File Size
- Data Artifacts
  - Metadata (5)
- Analysis Results
- OS Accounts
- Tags
- Score
- Reports

File System

107 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Fl
CYS5238 Research Methodology				2024-07-23 23:39:52 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:07 PKT	0	Ur
CYS5101 Applied Cryptography				2024-10-13 21:55:56 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:08 PKT	0	Ur
CYS5103 Network Security				2024-07-23 23:39:42 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:10 PKT	0	Ur
CYS5201 Digital Forensics				2024-07-23 23:39:48 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:14 PKT	0	Ur
Screen Recording 2024-10-14 210955.mp4				2024-10-14 21:09:56 PKT	0000-00-00 00:00:00	2024-10-15 00:00:00 PKT	2024-10-14 21:19:14 PKT	360018427	Ur
New folder				2024-10-15 12:43:30 PKT	0000-00-00 00:00:00	2024-10-15 00:00:00 PKT	2024-10-15 12:43:28 PKT	0	Ur
_TUDY				2024-10-15 12:43:30 PKT	0000-00-00 00:00:00	2024-10-15 00:00:00 PKT	2024-10-15 12:43:28 PKT	0	Ur
Transcript.jfif				2024-10-17 10:33:26 PKT	0000-00-00 00:00:00	2024-10-17 00:00:00 PKT	2024-10-17 10:33:25 PKT	0	Ur
Transcript.jfif				2024-10-17 10:37:10 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:33:25 PKT	317759	Ur
BANK STAT.pdf				2024-10-17 10:33:34 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:35:21 PKT	10376	Ur
Profile Report (1) (1).pdf				2024-10-17 10:33:42 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:35:51 PKT	76895	Ur
114(1) (Return of Income for a person deriving incc				2024-10-17 10:33:40 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:35:51 PKT	391115	Ur
TAX Certificate.pdf				2024-10-17 10:33:52 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:35:51 PKT	3113543	Ur
New folder				2024-10-17 10:35:56 PKT	0000-00-00 00:00:00	2024-10-17 00:00:00 PKT	2024-10-17 10:35:55 PKT	0	Ur
Screenshot 2025-03-13 100907.png				2025-03-13 10:09:10 PKT	0000-00-00 00:00:00	2025-03-13 00:00:00 PKT	2025-03-13 10:12:09 PKT	270284	Ur
Screenshot 2025-03-13 101112.png				2025-03-13 10:11:14 PKT	0000-00-00 00:00:00	2025-03-13 00:00:00 PKT	2025-03-13 10:12:09 PKT	291000	Ur
Screenshot 2025-03-13 100811.png				2025-03-13 10:08:14 PKT	0000-00-00 00:00:00	2025-03-13 00:00:00 PKT	2025-03-13 10:12:10 PKT	546796	Ur
Updated SZABIST Need-Based Scholarship Applica				2024-10-17 10:37:38 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:37:51 PKT	384783	Ur
Lecture 1-2 Information Security.pptx				2023-10-16 21:14:54 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:41 PKT	30859048	Ur
Lecture 2 Information Security controls fundamenta				2023-09-19 04:53:50 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:44 PKT	6653155	Ur
Lecture 3 Information Security.pptx				2023-09-11 02:14:08 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:44 PKT	20429409	Ur
Lecture5-6 Information Security.pptx				2023-10-10 04:48:36 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:46 PKT	42599765	Ur

Analyzing files from Shuaib Sheikh.001 55% (3 more...)

11:58 am
02/05/2025

USB Image Analysis Summary:

After imaging the USB with FTK Imager and analyzing it in Autopsy, key findings emerged:

- **Existing Files:** Documents, images, and executables, some manually copied.
- **Recovered Deleted Files:** Personal documents, login-related texts, and setup files—possible signs of data exfiltration.
- **Sensitive Data:** Cached passwords, credentials, and notes indicate private information storage.
- **Web Activity:** Limited browser cache suggests file downloads.
- **Hidden Files:** Some files marked as system-related, hinting at concealment or malware.
- **File Timeline:** Usage patterns reveal suspicious deletions close to imaging time.

Conclusion:

This investigation highlights how USBs can hold crucial evidence, with recovered deleted files—especially sensitive data—being a critical aspect.