Assignment no 1

Muhammad Farrukh - 24109124

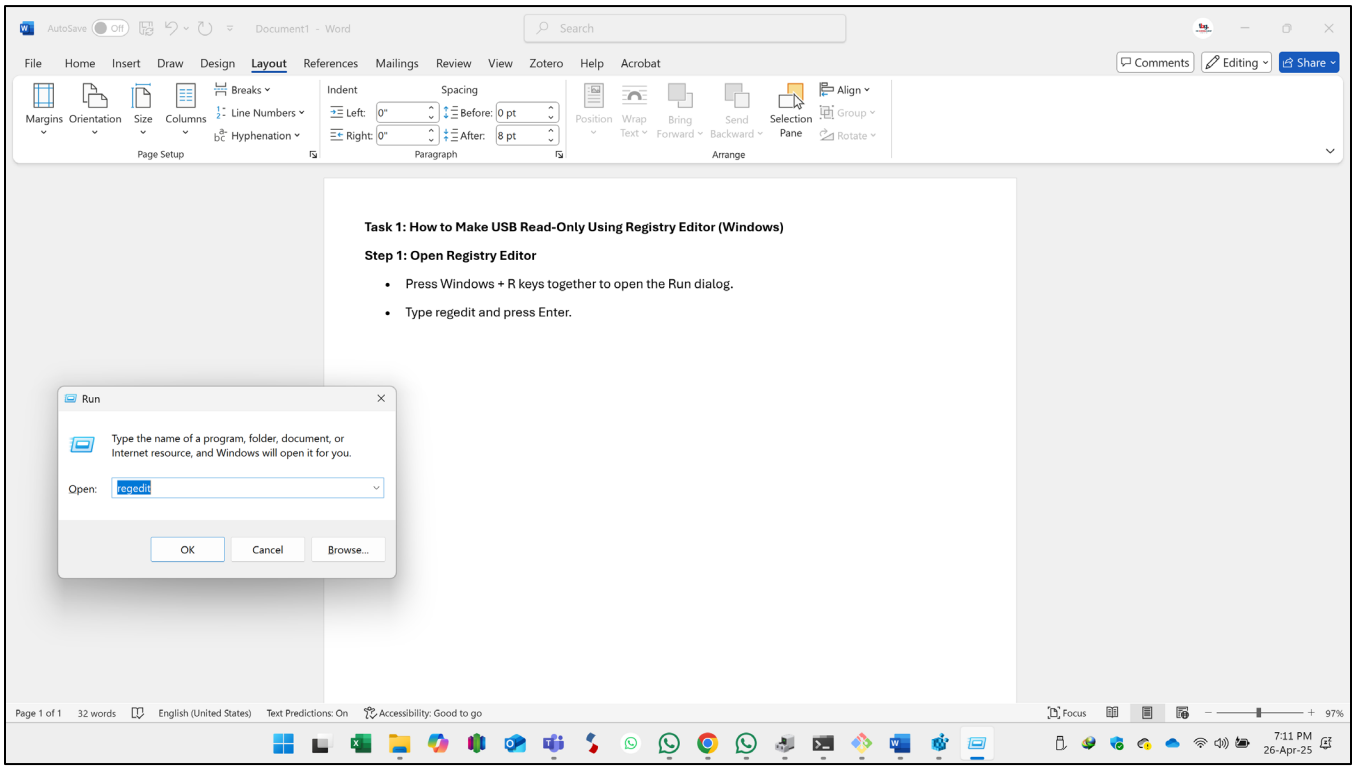
Digital Forensics

Submitted to Mr. Muhammad Waqar

Task 1: How to Make USB Read-Only Using Registry Editor (Windows)

Step 1: Open Registry Editor

- Press Windows + R keys together to open the Run dialog.
- Type regedit and press Enter.

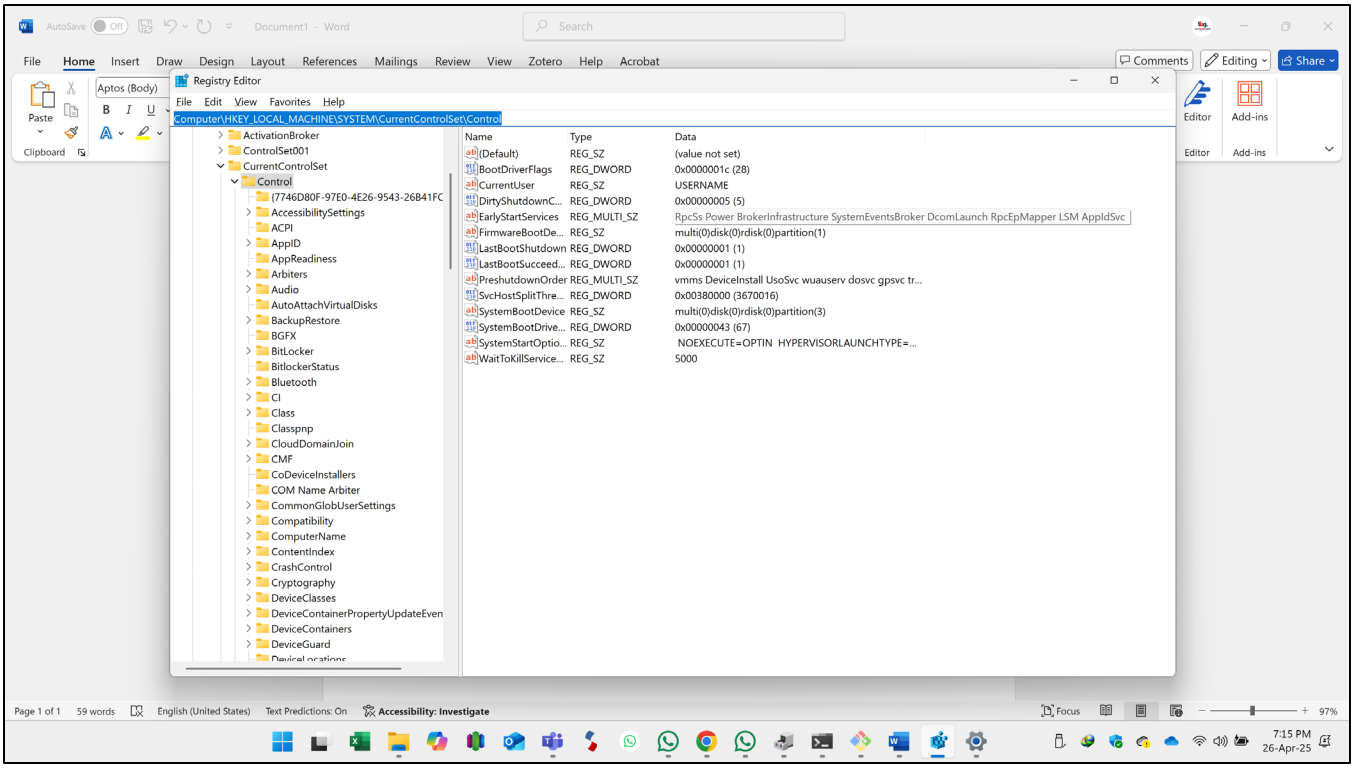


Step 2: Navigate to the Correct Registry Path

In Registry Editor, go to the following path:

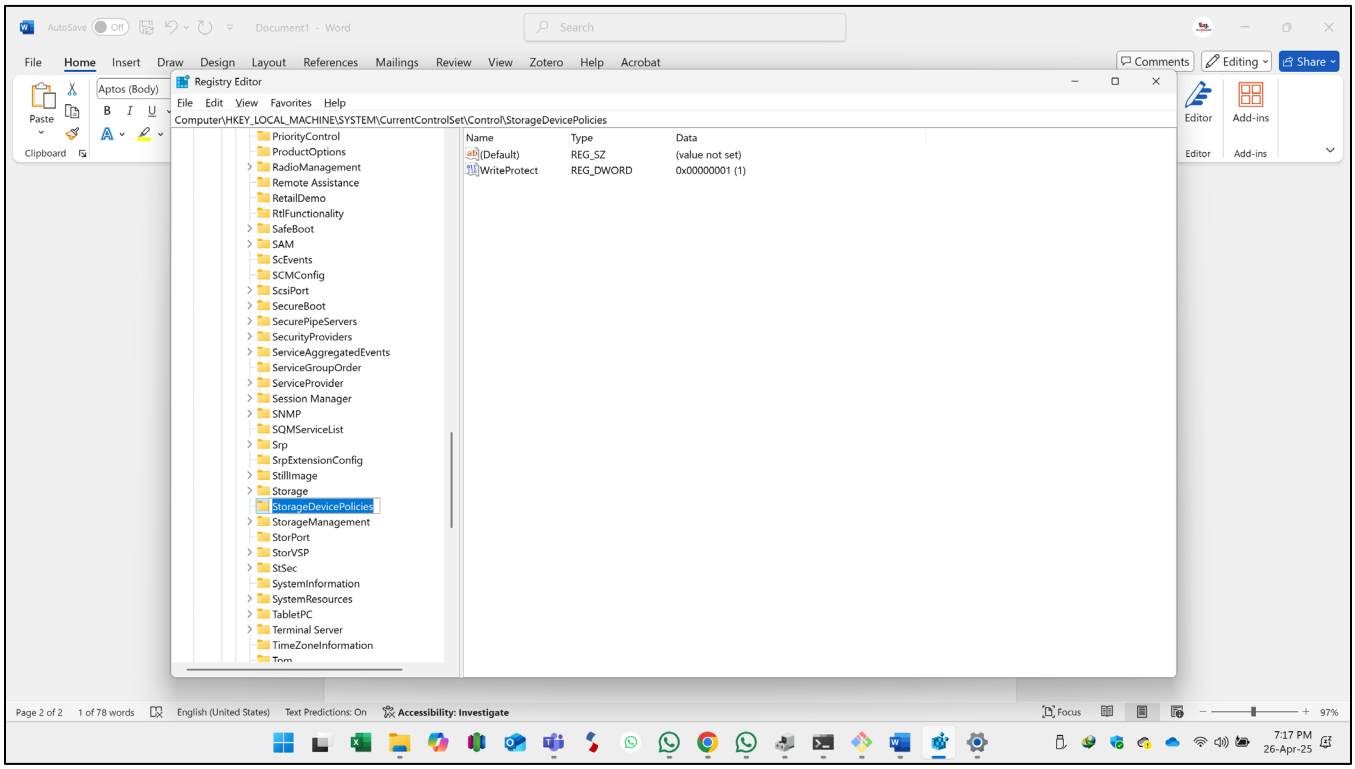
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

- Expand the folders (HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control).



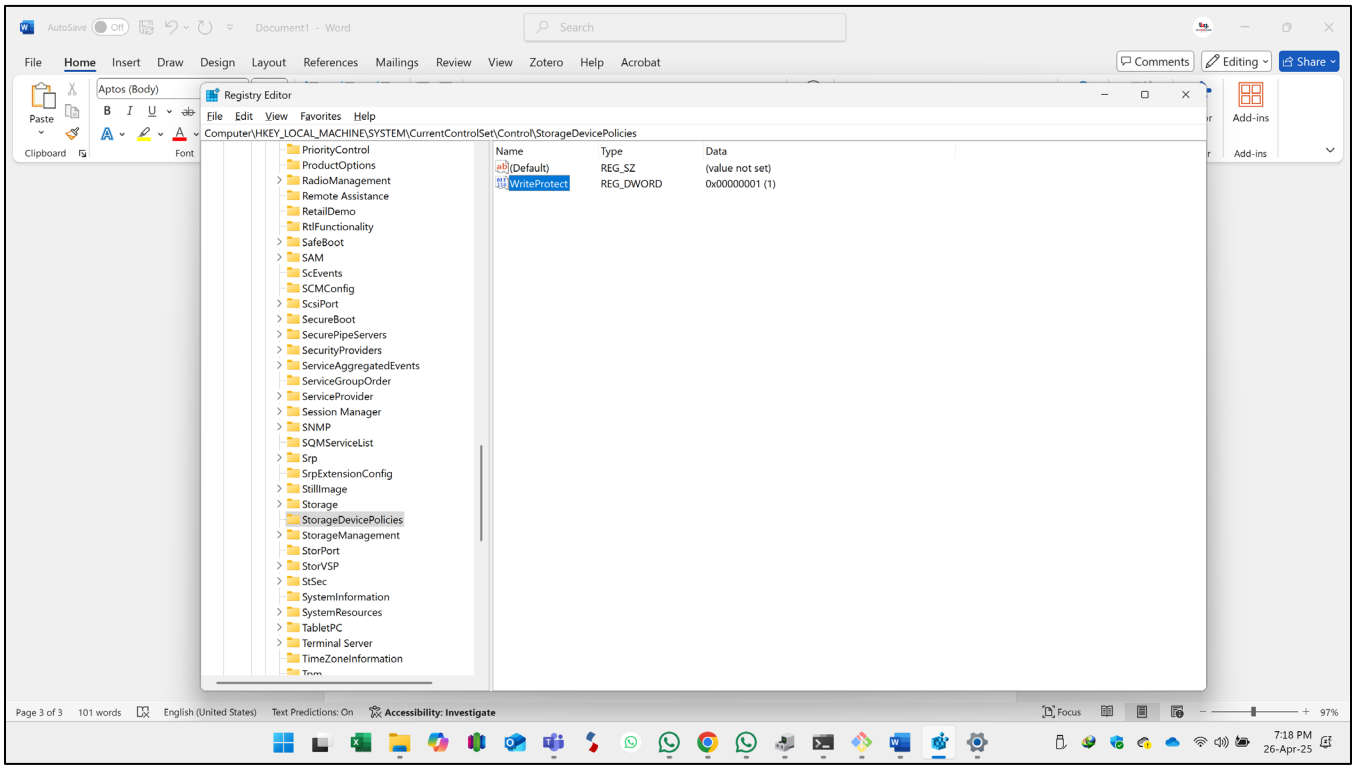
Step 3: Create "StorageDevicePolicies" Key

- Right-click on the **Control** folder.
- Click **New → Key**.
- Name the new key **StorageDevicePolicies**.



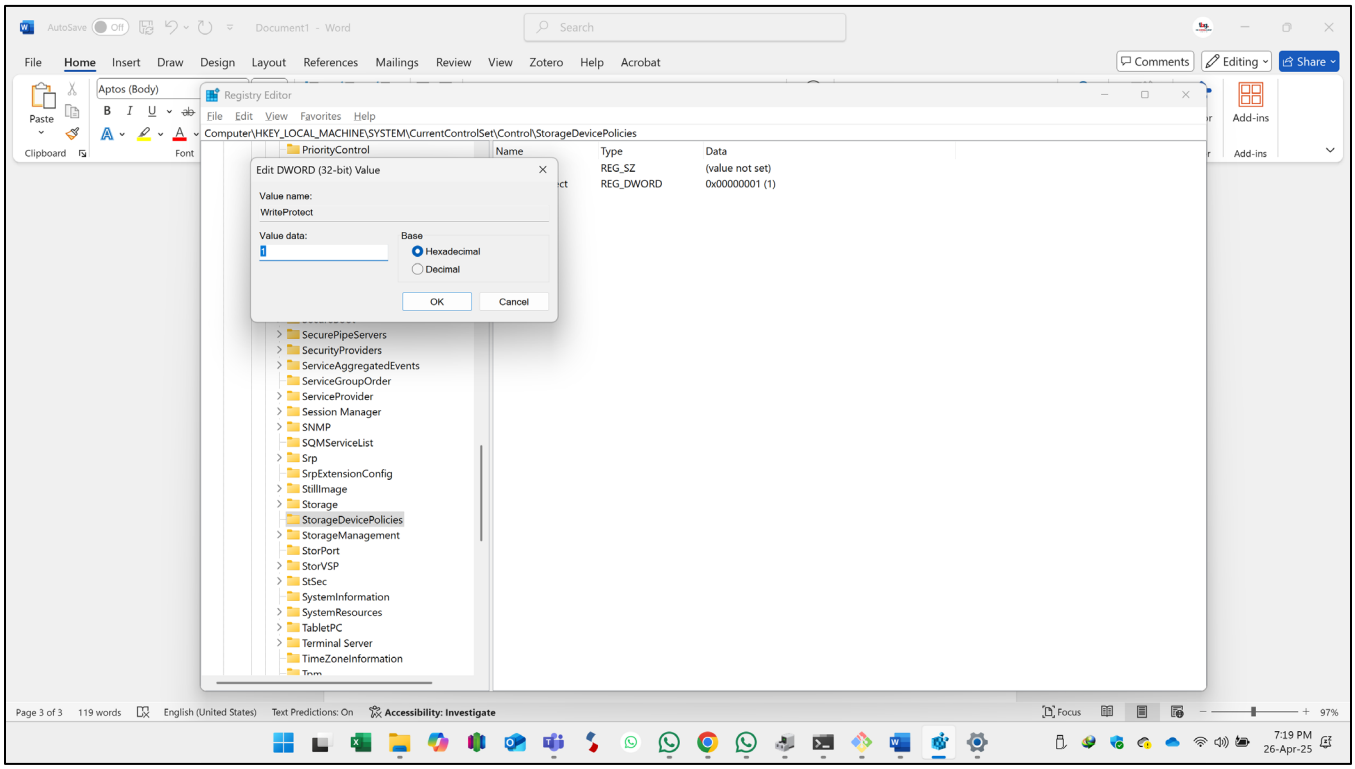
Step 4: Create "WriteProtect" Value

- Right-click on the **StorageDevicePolicies** key (folder) you just created.
- Select **New → DWORD (32-bit) Value**.
- Name it **WriteProtect**.



Step 5: Set Value to 1

- Double-click the **WriteProtect** value.
- Set the **Value Data** to 1.
- Click **OK**.



Step 6: Restart Your Computer

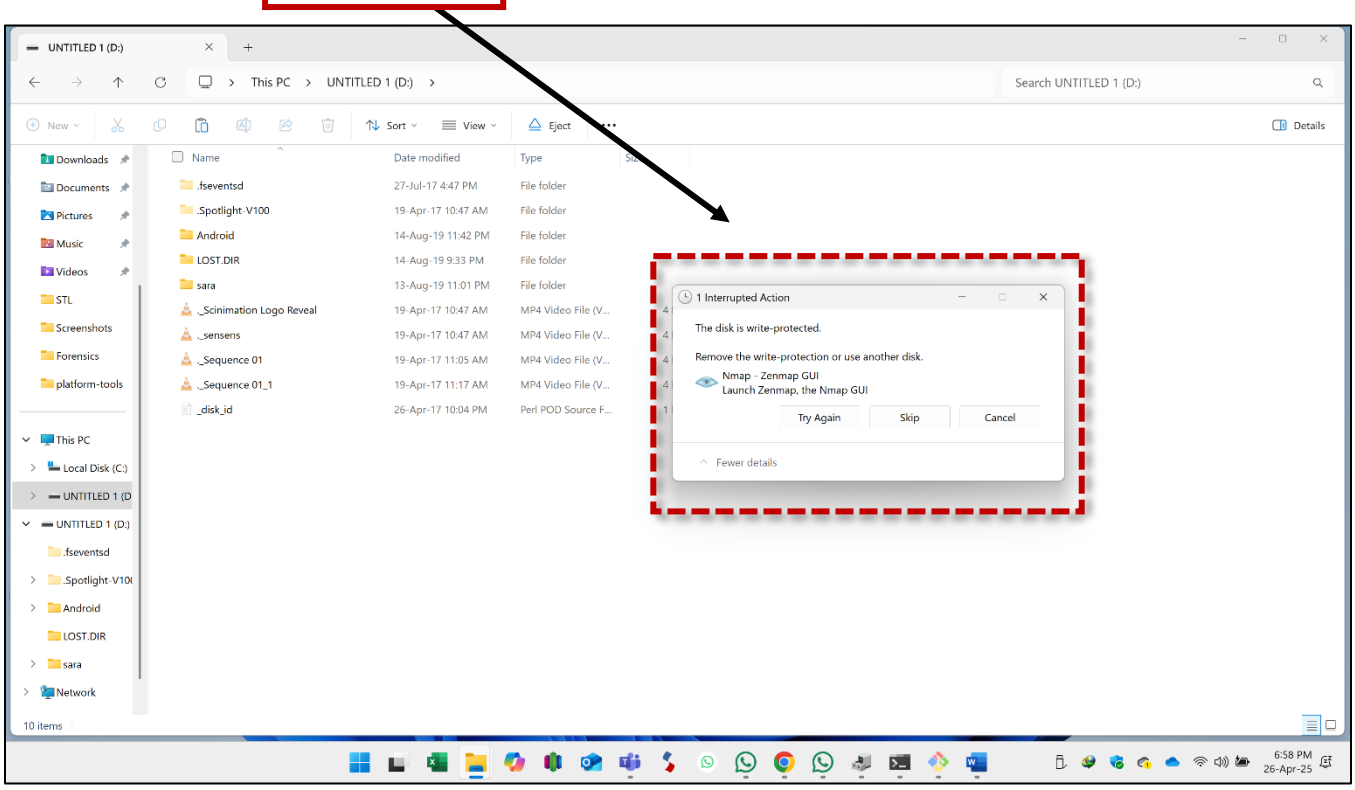
After making these changes, **restart** your computer for them to take effect.

Result:

Now, whenever someone connects a USB flash drive:

- They can **view** or **read** files.
- But they **cannot** copy new files, delete, or modify anything on the USB.

Your USB ports are **write-protected** now!

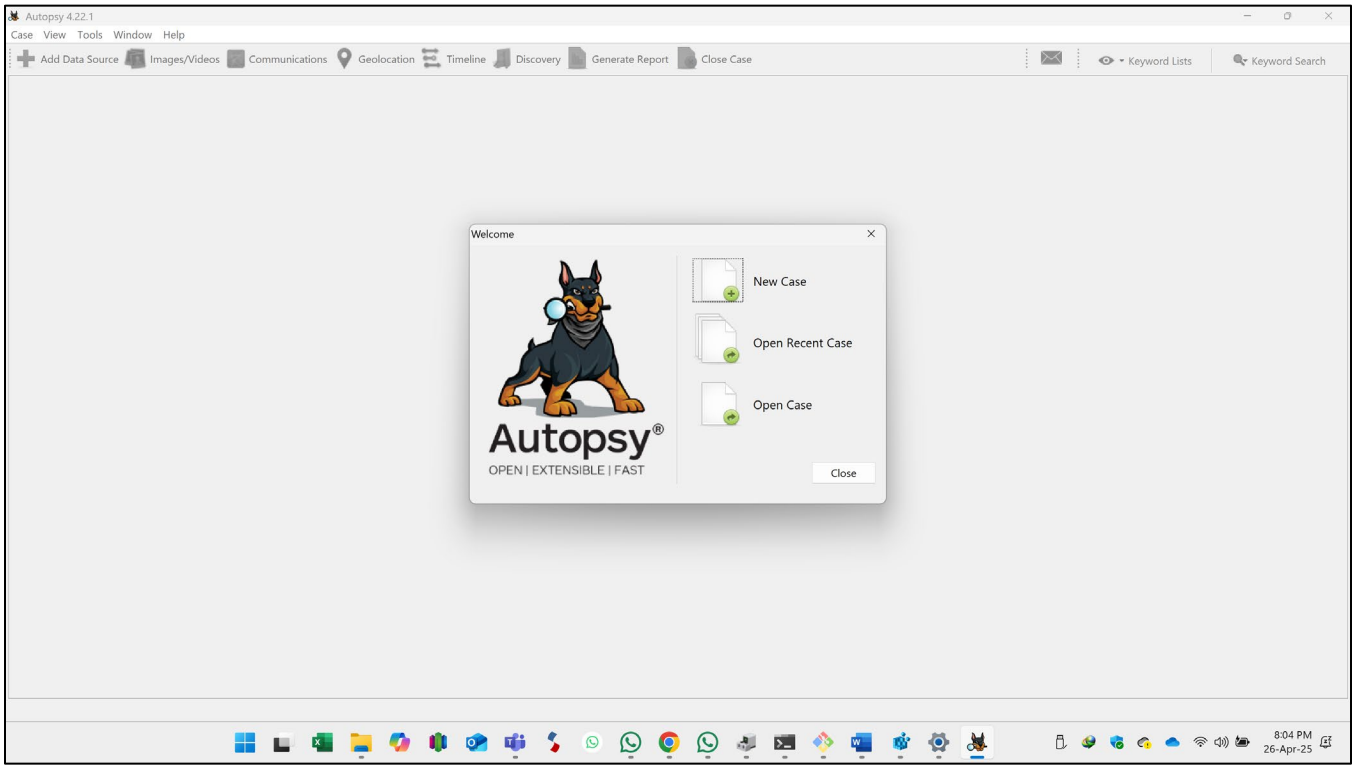


Task 2: Forensic Imaging and Analysis of USB Devices Using dd and Autopsy

Extract and Analyze the USB Image in Autopsy

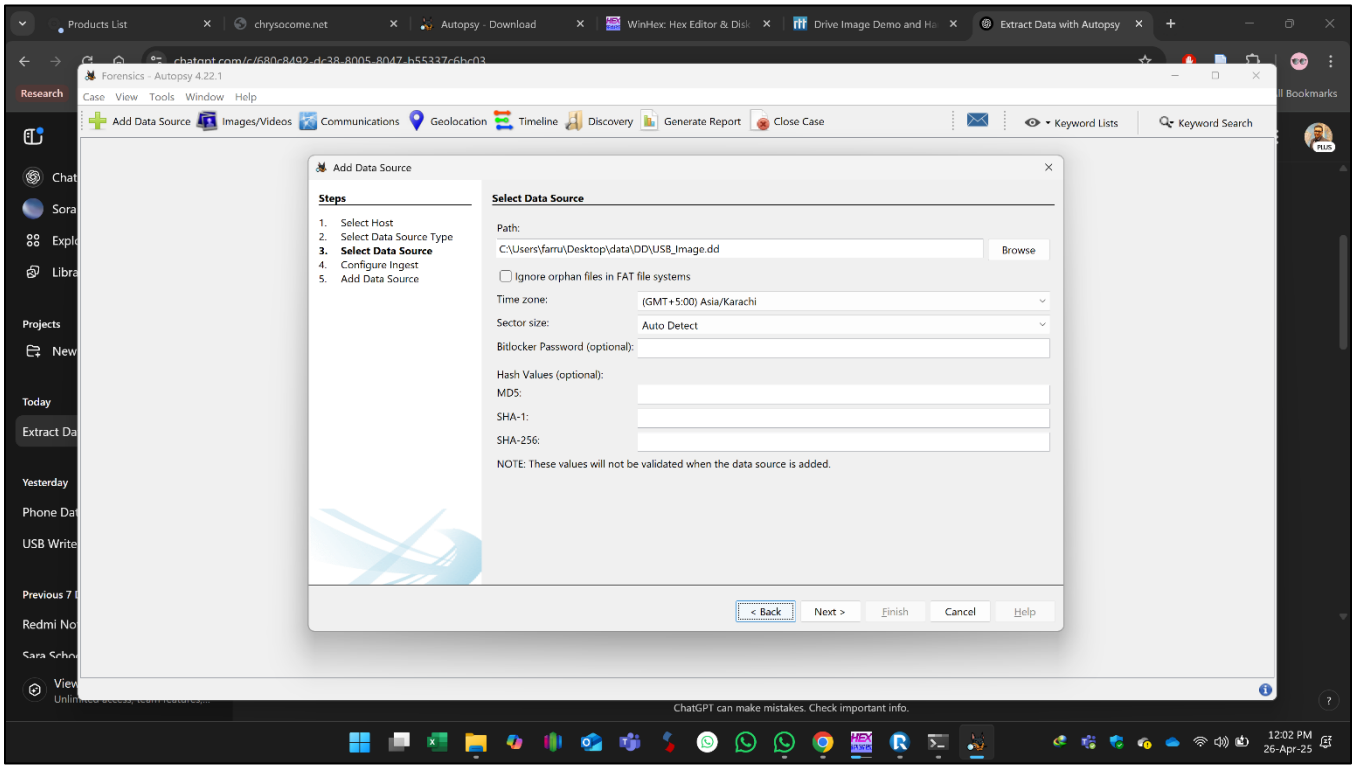
Create a New Case

- Click Create New Case.
- Enter Case Name and Case Directory.
- Click Next and finish setup.



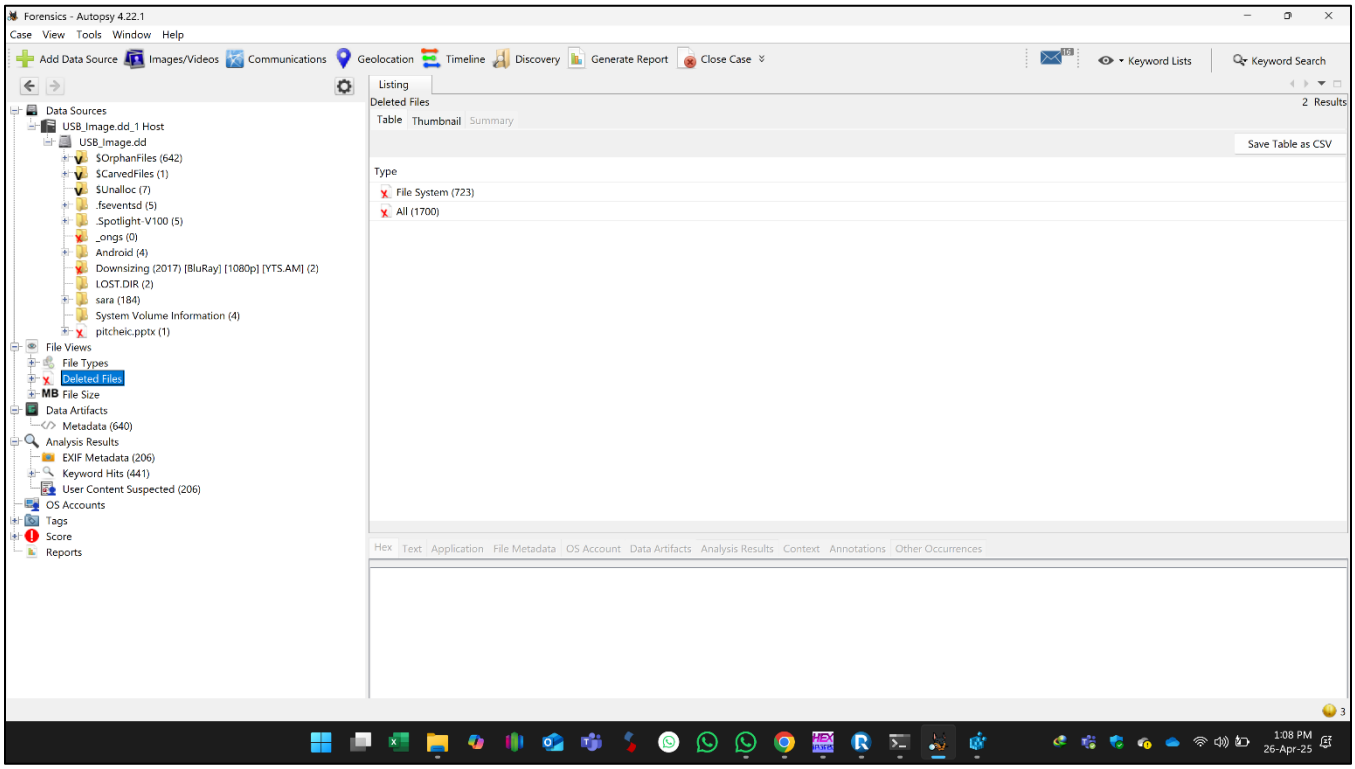
Add USB Image as Data Source

- Click Add Data Source.
- Select Disk Image or VM file.
- Browse and select your usb_image.dd file you created earlier.
- Click Next.



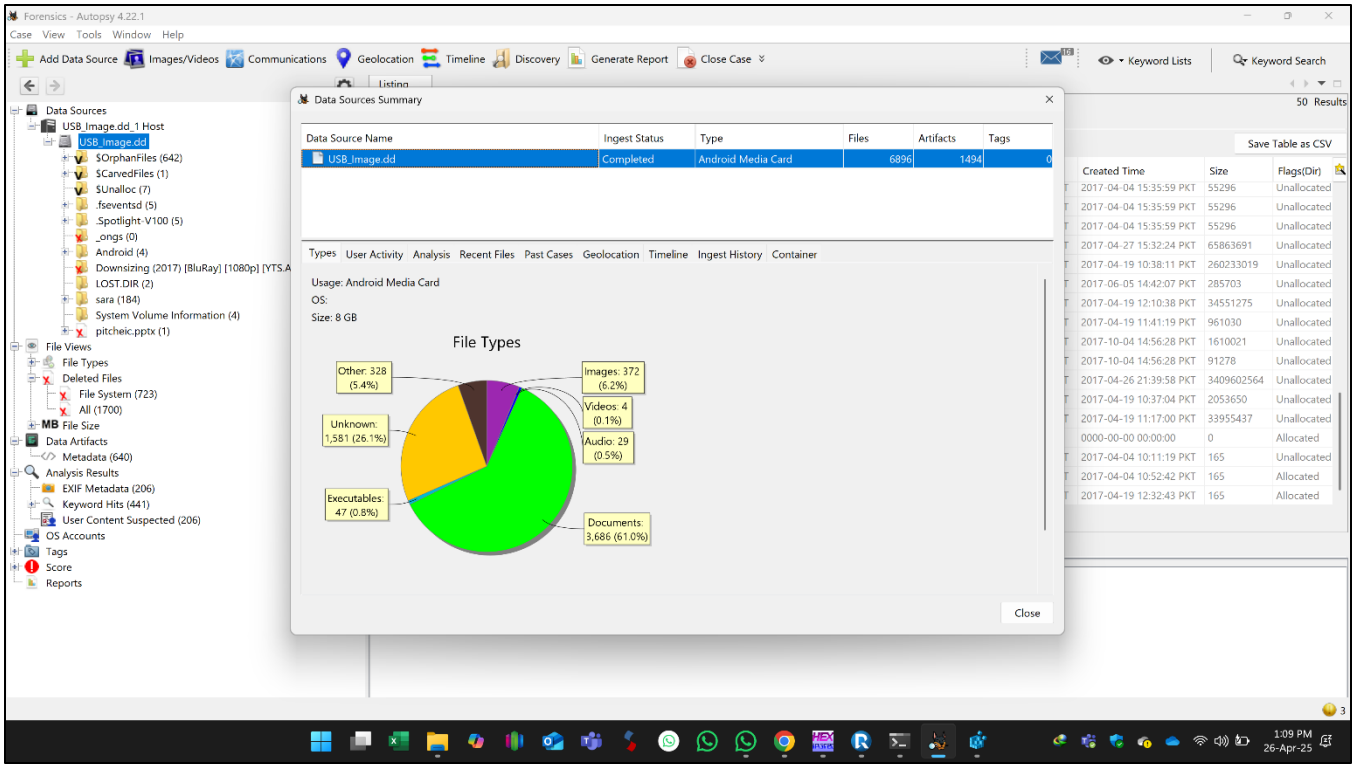
Start Analysis

- Autopsy will process the .dd image.

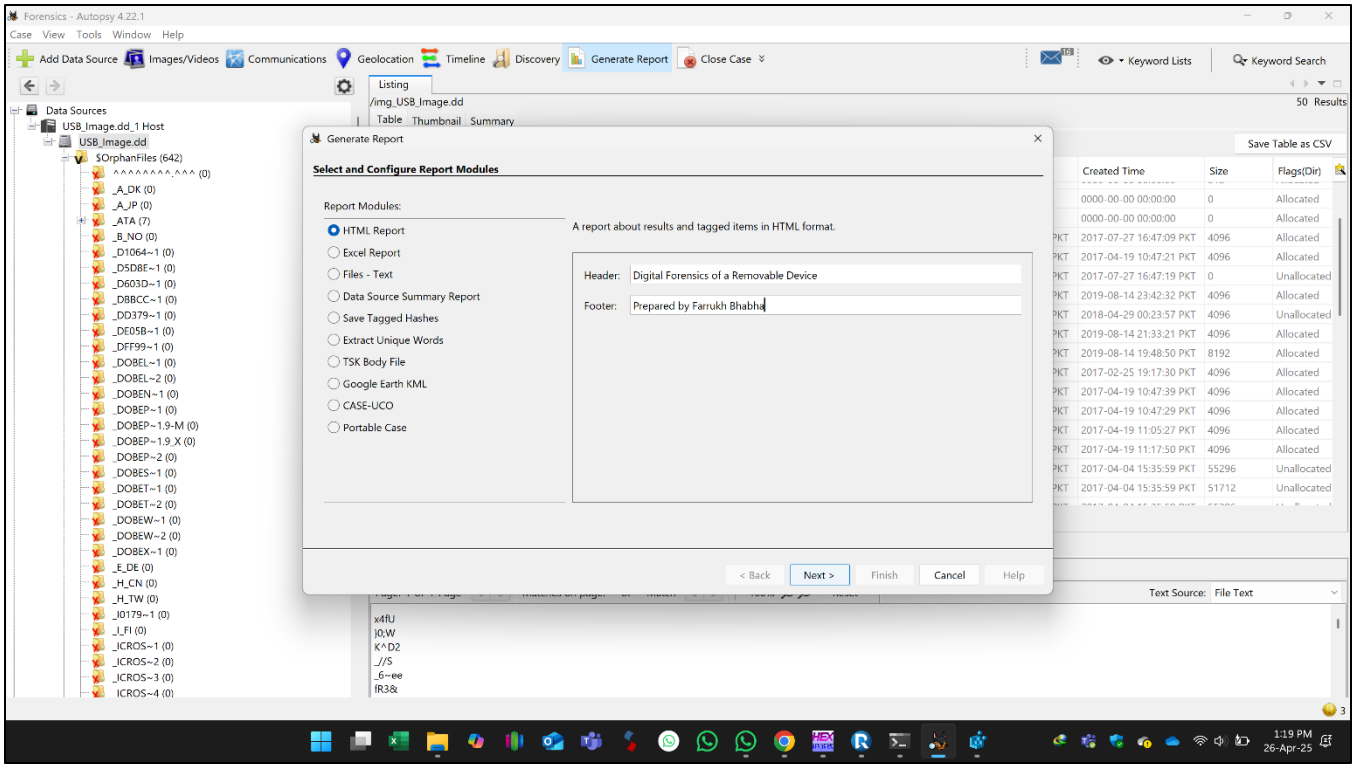


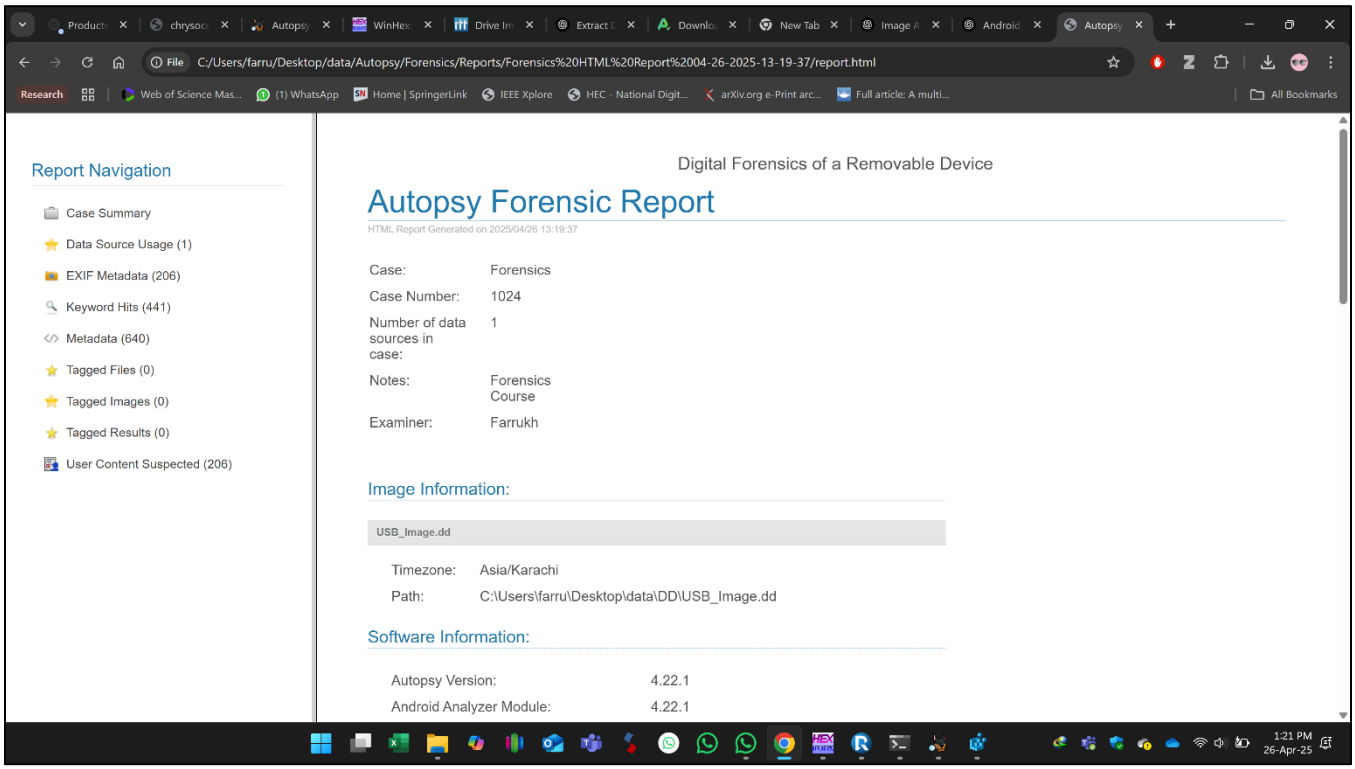
Once scanning is done, you can:

- Browse the full file system.
- View deleted files.
- Search documents, images, etc.
- Create detailed forensic reports.



Go to Generate Report to get a detailed report of Files Found, Deleted Files, Metadata, Keyword Hits etc


Forensics - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
USB_Image.dd_1 Host
USB_Image.dd
$OrphanFiles (642)
Listing
/img_USB_Image.dd
Table Thumbnail Summary
50 Results
Save Table as CSV
Created Time
Size
Flags(Dir)
Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Data Source Summary Report
Save Tagged Hashes
Extract Unique Words
TSK Body File
Google Earth KML
CASE-UCO
Portable Case
A report about results and tagged items in HTML format.
Header: Digital Forensics of a Removable Device
Footer: Prepared by Farrukh Bhabha
< Back
Next >
Finish
Cancel
Help
Text Source: File Text
1:19 PM
26-Apr-25


C:/Users/farru/Desktop/data/Autopsy/Forensics/Reports/Forensics%20HTML%20Report%2004-26-2025-13-19-37/report.html
Report Navigation
Case Summary
Data Source Usage (1)
EXIF Metadata (206)
Keyword Hits (441)
Metadata (640)
Tagged Files (0)
Tagged Images (0)
Tagged Results (0)
User Content Suspected (206)
Digital Forensics of a Removable Device
Autopsy Forensic Report
HTML Report Generated on 2025/04/26 13:19:37
Case: Forensics
Case Number: 1024
Number of data sources in case: 1
Notes: Forensics Course
Examiner: Farrukh
Image Information:
USB_Image.dd
Timezone: Asia/Karachi
Path: C:\Users\farru\Desktop\data\DD\USB_Image.dd
Software Information:
Autopsy Version: 4.22.1
Android Analyzer Module: 4.22.1
1:21 PM
26-Apr-25

Conclusion

In this project, we successfully demonstrated the complete process of forensic imaging and analysis of a USB device using open-source tools.

First, the USB drive was imaged using the dd utility in a Windows environment. The dd tool allowed us to create a bit-by-bit forensic copy of the entire USB device, preserving all active, deleted, and hidden data without altering the original evidence.

Next, the created .dd image file was analyzed using Autopsy, a digital forensics platform.
By adding the USB image into Autopsy, we were able to:

- Recover and browse through the complete file system of the USB.
- Identify deleted files and recover hidden data.
- Extract metadata such as file creation dates, last accessed times, and modification timestamps.
- Detect and examine system artifacts, if any.

Finally, a Forensic Report was generated using Autopsy's "Generate Report" feature.
This report provided:

- A detailed listing of all files found on the USB.
- Separate sections for deleted files, extracted documents, images, and other artifacts.
- Complete metadata and timeline information.
- A clear, structured HTML-based summary for presenting the forensic findings professionally.

The report generated serves as documented digital evidence that can be used for legal, investigative, or academic purposes while maintaining the chain of custody principles.

Overall, the project demonstrated that using dd and Autopsy, investigators can efficiently perform reliable USB imaging, analysis, and reporting without expensive commercial tools — ensuring cost-effectiveness, evidence integrity, and professional investigation standards.