Forensic analysis using

Open-source technology.

By Abhinav Adarsh

11908522

Rollno.49 INT301

CA3

Index

Chapter 1

Introduction

What is disk forensics?

Disk forensics, also known as computer forensics or digital forensics, is the practice of collecting, analyzing, and preserving digital evidence from computer storage devices, such as hard drives, solid-state drives, flash drives, and memory cards. The goal of disk forensics is to identify, preserve, and analyze data in a way that maintains its integrity and authenticity, and to use the information obtained to support legal or investigative purposes.

Why is disk forensics important?

Disk forensics is important because it enables investigators to recover and analyze data that may be crucial to solving crimes or resolving disputes. In many cases, digital evidence can provide more comprehensive and accurate information than traditional forms of evidence, such as witness testimony or physical artifacts.

Types of disk forensics

There are several types of disk forensic analysis, including:

- **Live analysis:** This involves analyzing data on a computer while it is still running, which can be useful in situations where investigators need to quickly gather information without disrupting the normal functioning of the system.
- **Post-mortem analysis:** This involves analyzing data on a computer that has been shut down or seized and can provide a more thorough and detailed examination of the system.
- **Network forensics:** This involves analyzing data from network traffic to identify evidence of criminal activity, such as hacking or data theft.
- **Memory forensics:** This involves analyzing data from a computer's RAM (random access memory), which can provide valuable information about running processes, open files, and other system activity.
- **Mobile device forensics:** This involves analyzing data from smartphones, tablets, and other mobile devices, which can contain valuable evidence in cases involving cybercrime, fraud, or other digit offenses.

Disk Forensics

Disk forensics is a vital component of digital forensics that focuses on the investigation of data stored on physical storage media, such as hard drives and solid-state drives. Disk forensics involves examining the contents of the disk to identify evidence of digital activity.

When a crime is suspected, a forensic examiner may seize the suspect's computer or storage devices and conduct an analysis of the data stored on the disk. Disk forensics can help investigators identify the source of digital evidence and reconstruct events that took place on the disk.

To conduct a disk forensic examination, the examiner must use specialized tools and techniques to identify, preserve, and analyze data on the disk. This may involve making a bit-by-bit copy of the disk to preserve the original evidence, searching for hidden or deleted files, and analyzing the file system to determine how data was stored and accessed.

Disk forensics is often used in criminal investigations, such as cases involving fraud, cybercrime, and intellectual property theft. It can also be used in civil litigation to gather evidence in cases involving electronic discovery, trade secret theft, and breach of contract.

To be an expert in disk forensics, one must have in-depth knowledge of computer hardware, operating systems, file systems, and data recovery techniques. The examiner must also be proficient in the use of specialized tools and software to analyze disk images and recover deleted or hidden data.

1.1 Objective of the project

The objective of this project is to use open-source software to generate a report that can extract deleted data from a hard disk drive. Specifically, the software tool that will be used in this project is Autopsy, which is a powerful digital forensic investigation tool that can analyze disk images and recover data from them.

1.2 Description of the project

The project involves using Autopsy to generate a report that can extract deleted data from a hard disk drive. Autopsy is a free and open-source digital forensics tool that is widely used by law enforcement agencies, government organizations, and digital forensics professionals to analyze and recover data from digital devices.

To use Autopsy for this project, we will need to obtain a disk image of the hard drive that contains the deleted data. This can be done using a disk imaging tool such as dd or FTK Imager. Once we have the disk image, we can load it into Autopsy and run a search for deleted files.

Autopsy has a built-in search functionality that can identify deleted files based on various criteria such as file type, file size, and file name. Once the deleted files have been identified, we can generate a report that lists the recovered files along with their metadata such as the date and time they were deleted, the file path, and the file size.

The report generated by Autopsy can be exported in various formats such as HTML, PDF, or CSV. This report can then be used by digital forensics investigators to analyze the recovered data and determine whether any malicious activity occurred on the hard drive.

1.3 Scope of the project

The scope of this project is limited to using Autopsy to generate a report that can extract deleted data from a hard disk drive. The project does not involve analyzing the recovered data or determining the cause of the data loss. The project also assumes that a disk image of the hard drive is available for analysis. If a disk image is not available, the project may require additional steps to create-one.

Chapter 2

System Description

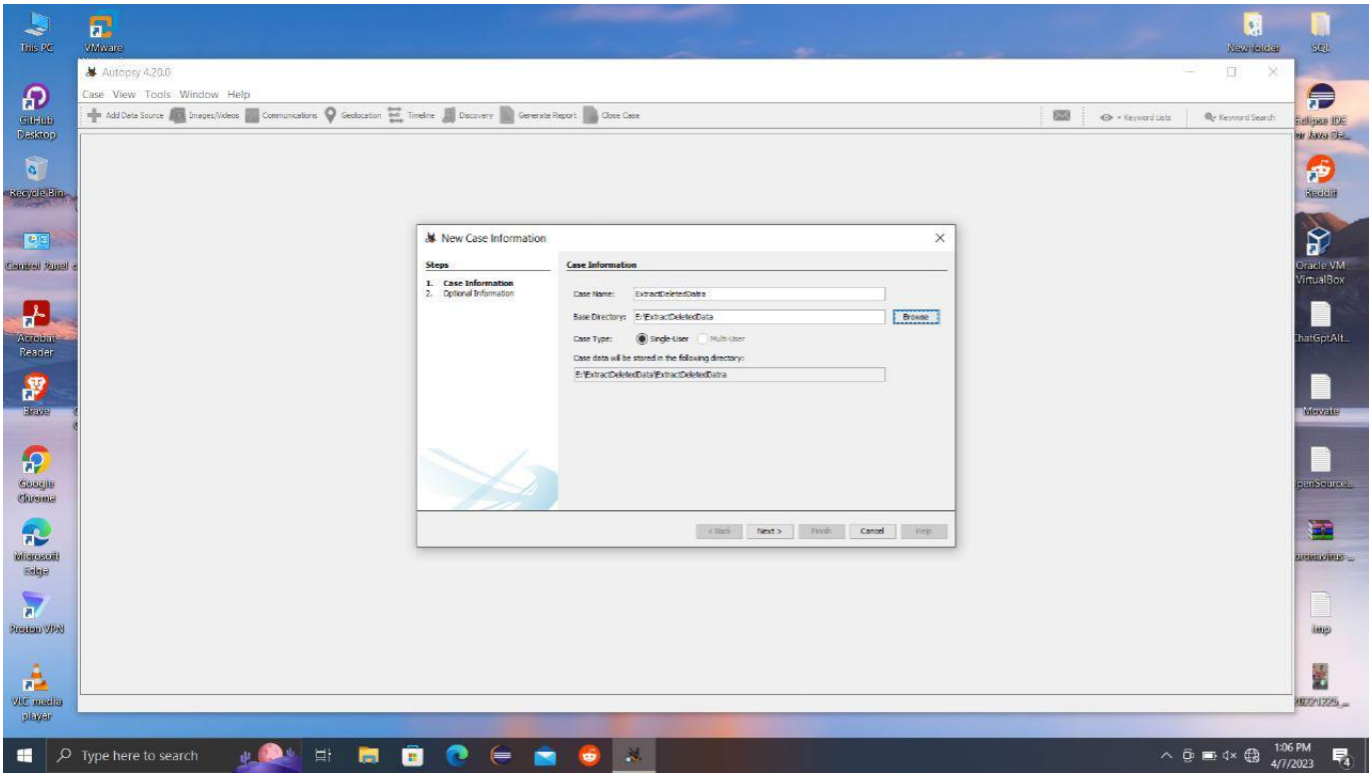
1.4 Target system description

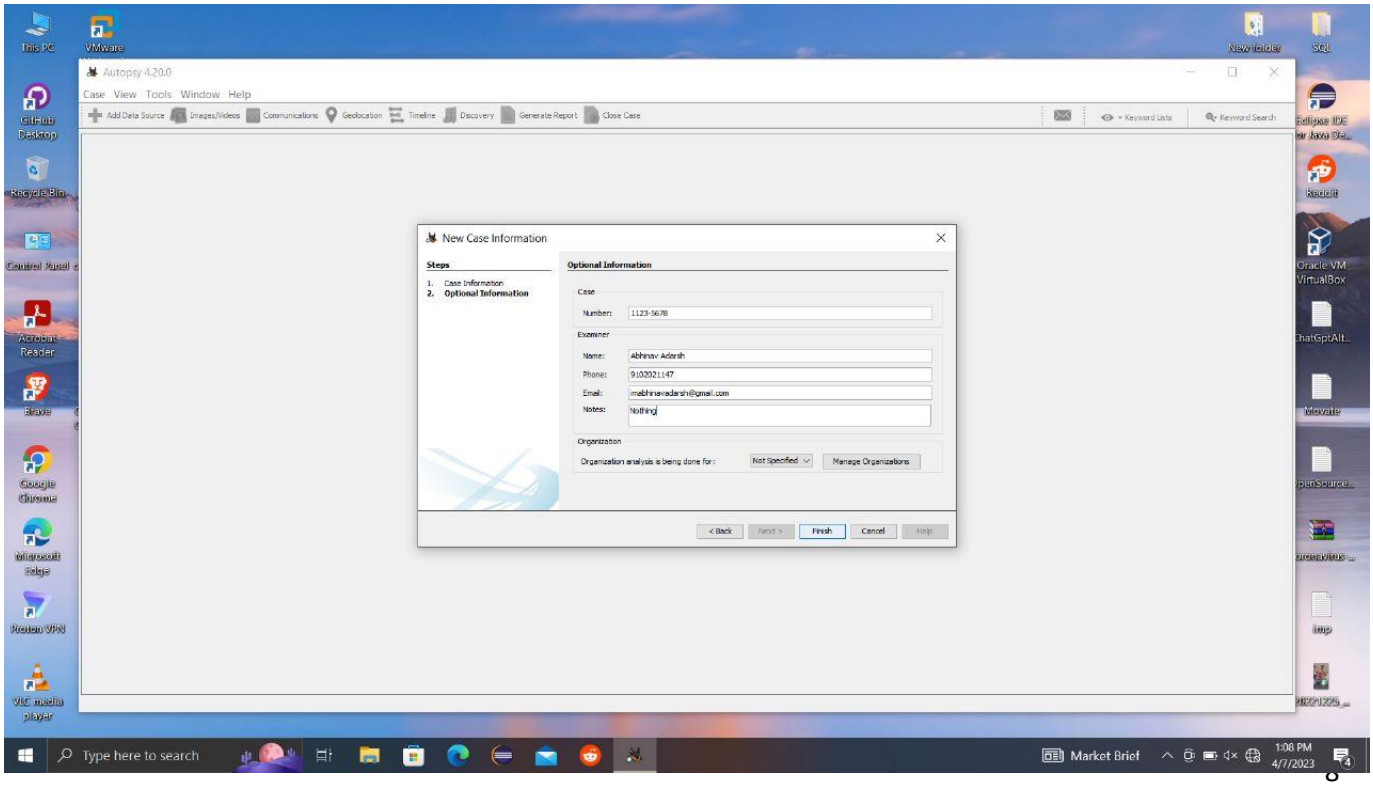
- A digital forensics system capable of extracting deleted data from a hard disk drive.
- The system will use open-source software Autopsy to generate a report that can identify and recover deleted files from a disk image of the hard drive.
- The system should have the processing power and memory to run Autopsy.
- A write-blocker device or hardware write-blocking capability is required to ensure that the data on the storage devices is not altered during the extraction process.
- The system should understand the file system on the storage device and how the data is organized, such as NTFS, FAT32, or ext4.
- A secure location to store the extracted data, such as an encrypted hard drive or other secure storage device, is necessary.
- The system should have the necessary permissions or legal authority to extract and analyze the data on the storage devices.
- Proper documentation of the extraction process and any findings is important to ensure that the extracted data can be used as evidence in legal proceedings if necessary.

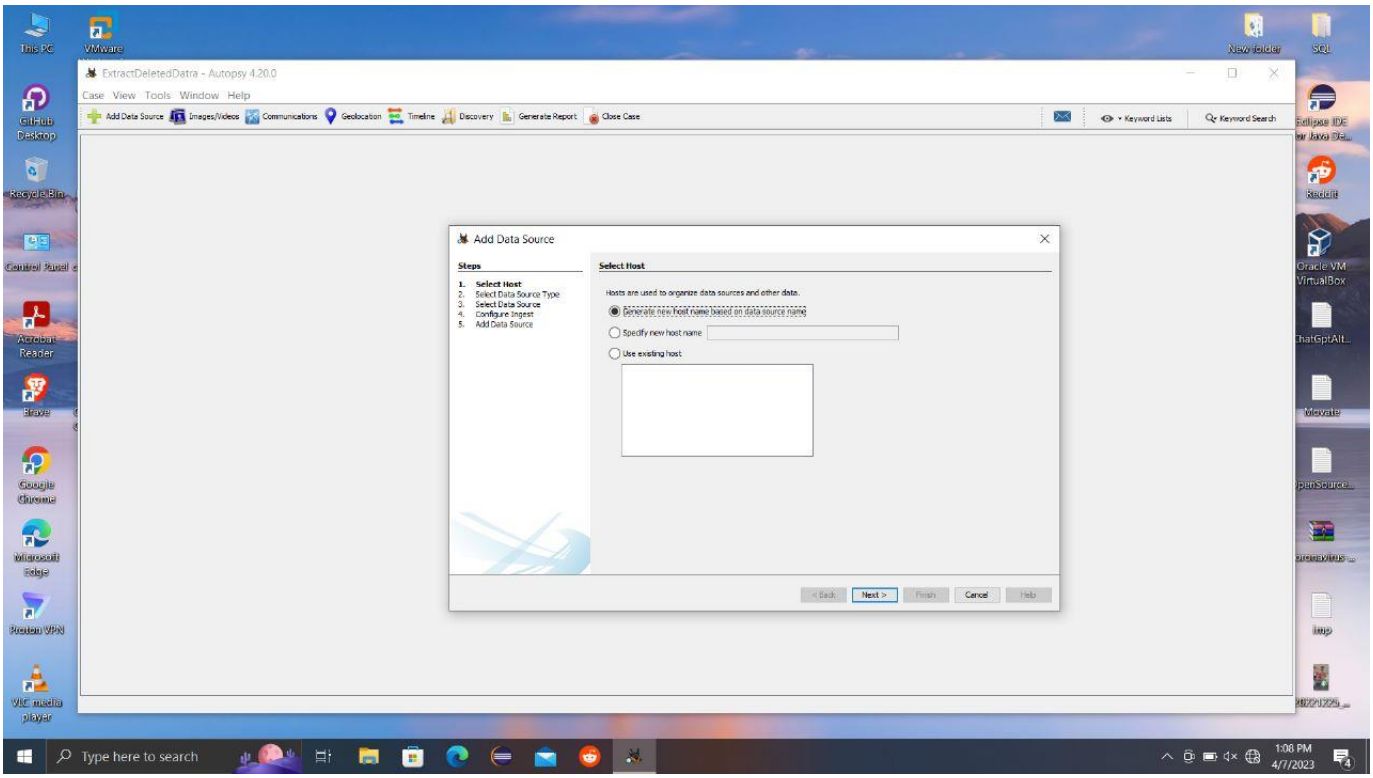
1.5 Assumptions and Dependencies (If applicable)

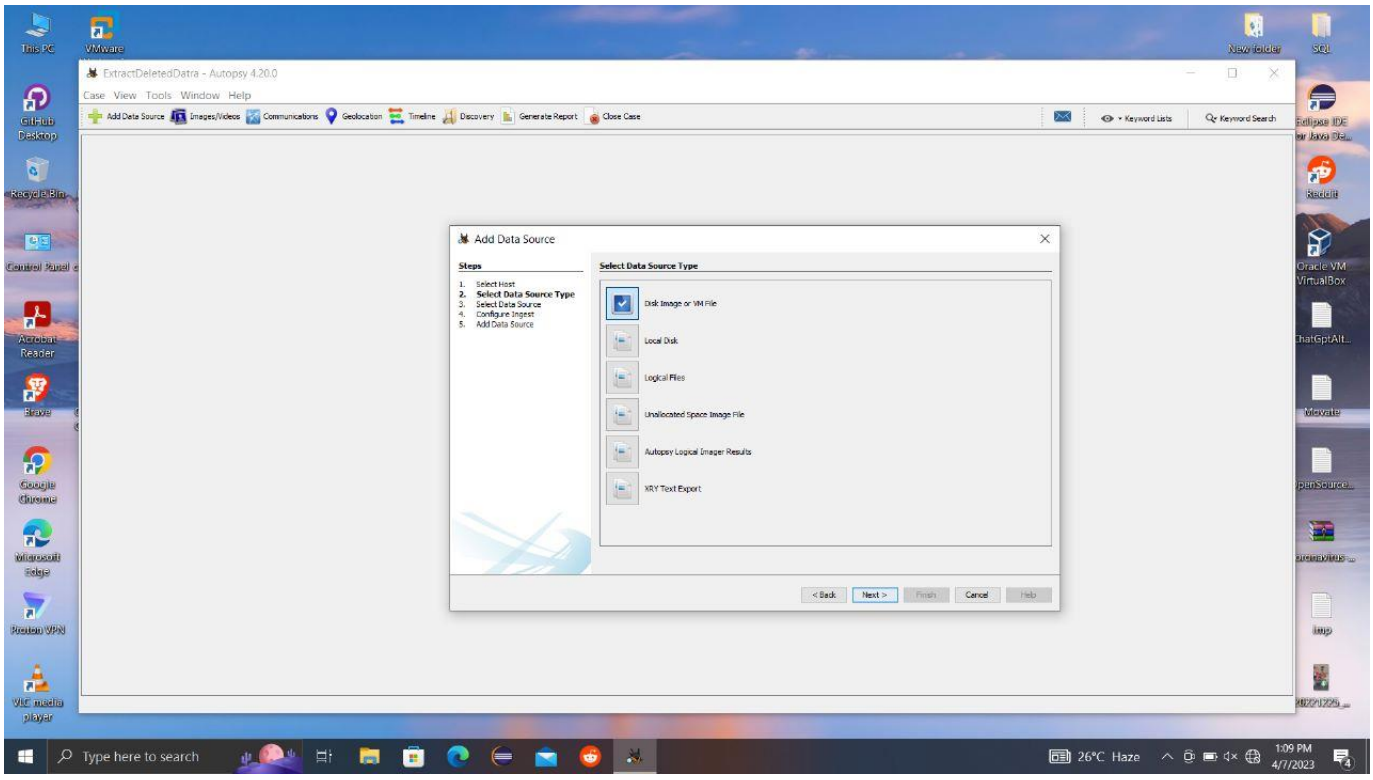
- The hard disk drive is available for analysis and has not been physically damaged.
- Autopsy is installed and properly configured on the digital forensics system.
- The storage device is accessible to the digital forensics system.
- The file system of the storage device is supported by Autopsy.
- The extracted data may need to be further analyzed or processed using other software.

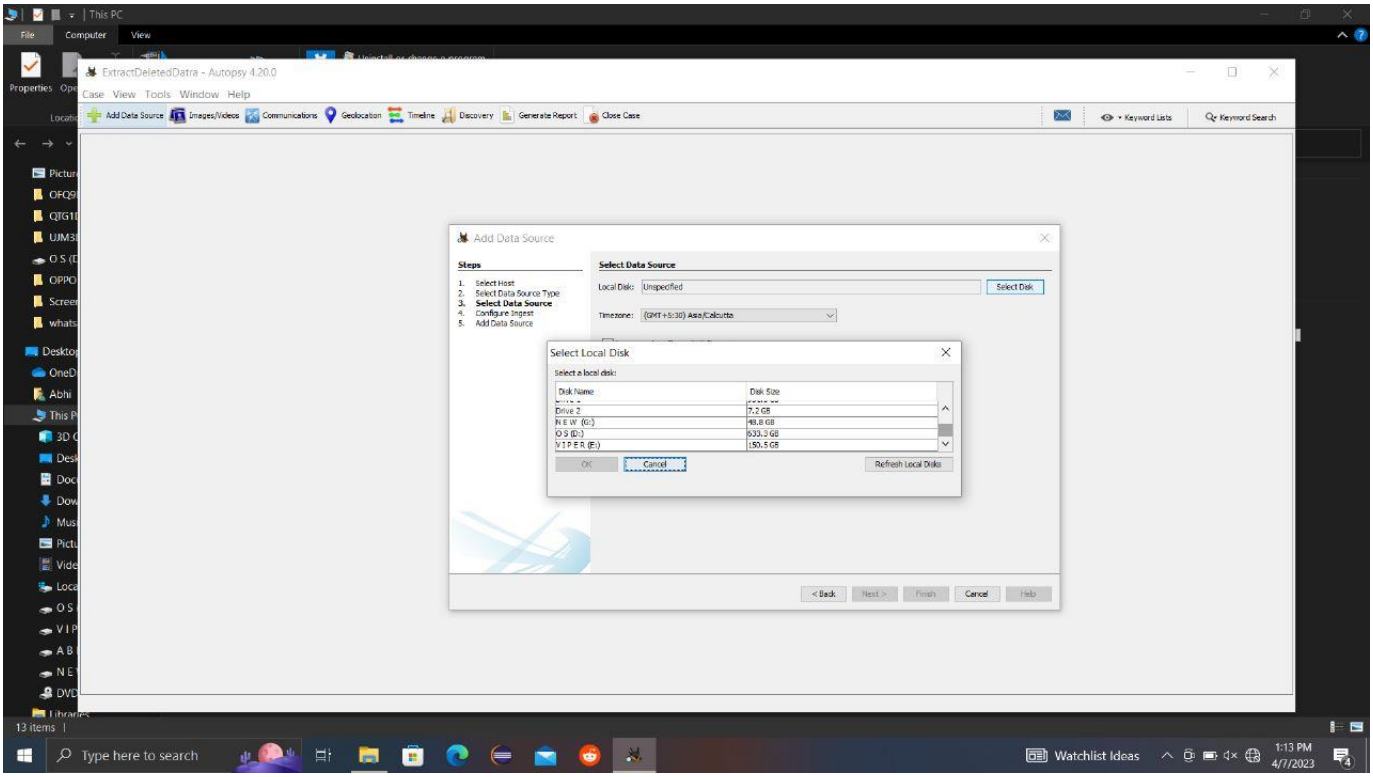
2. Analysis Screenshot

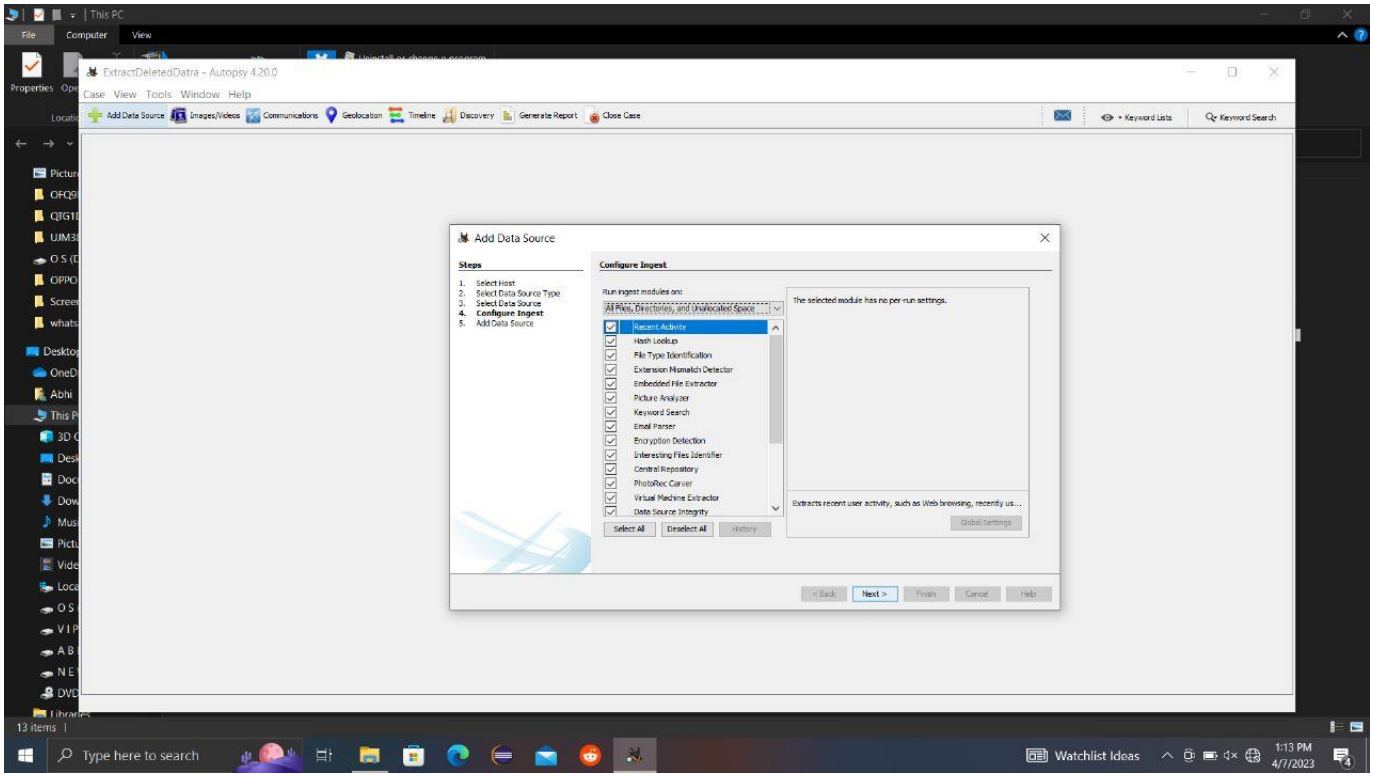


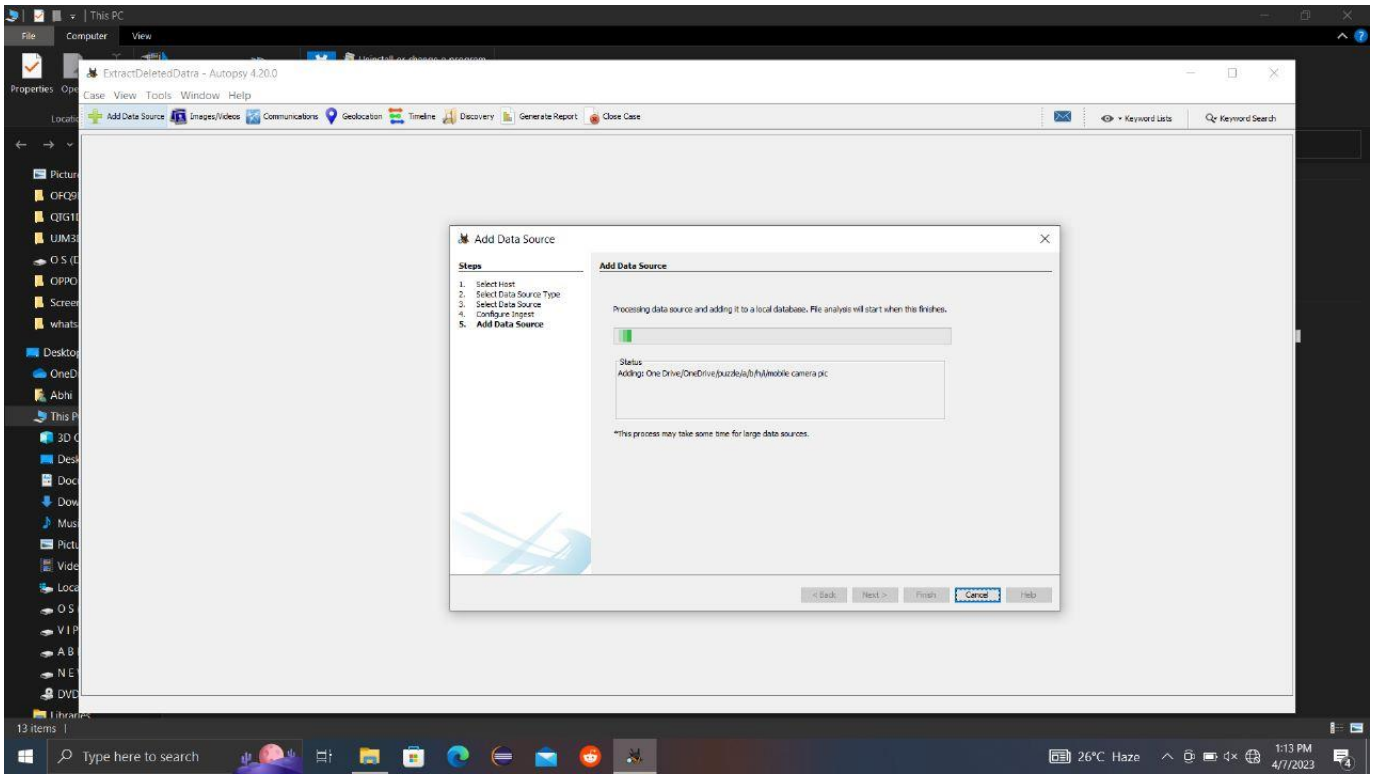


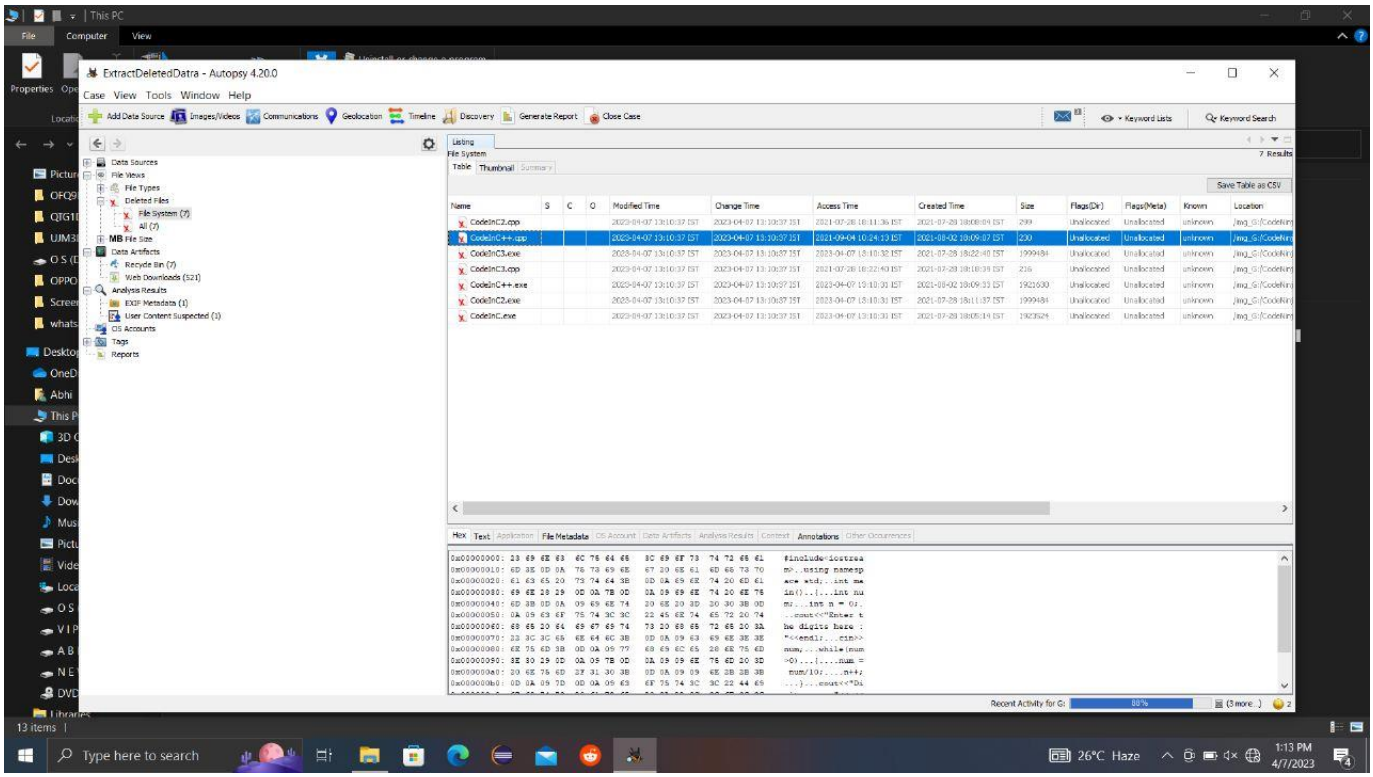

ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help
Type here to search
1:08 PM
4/7/2023

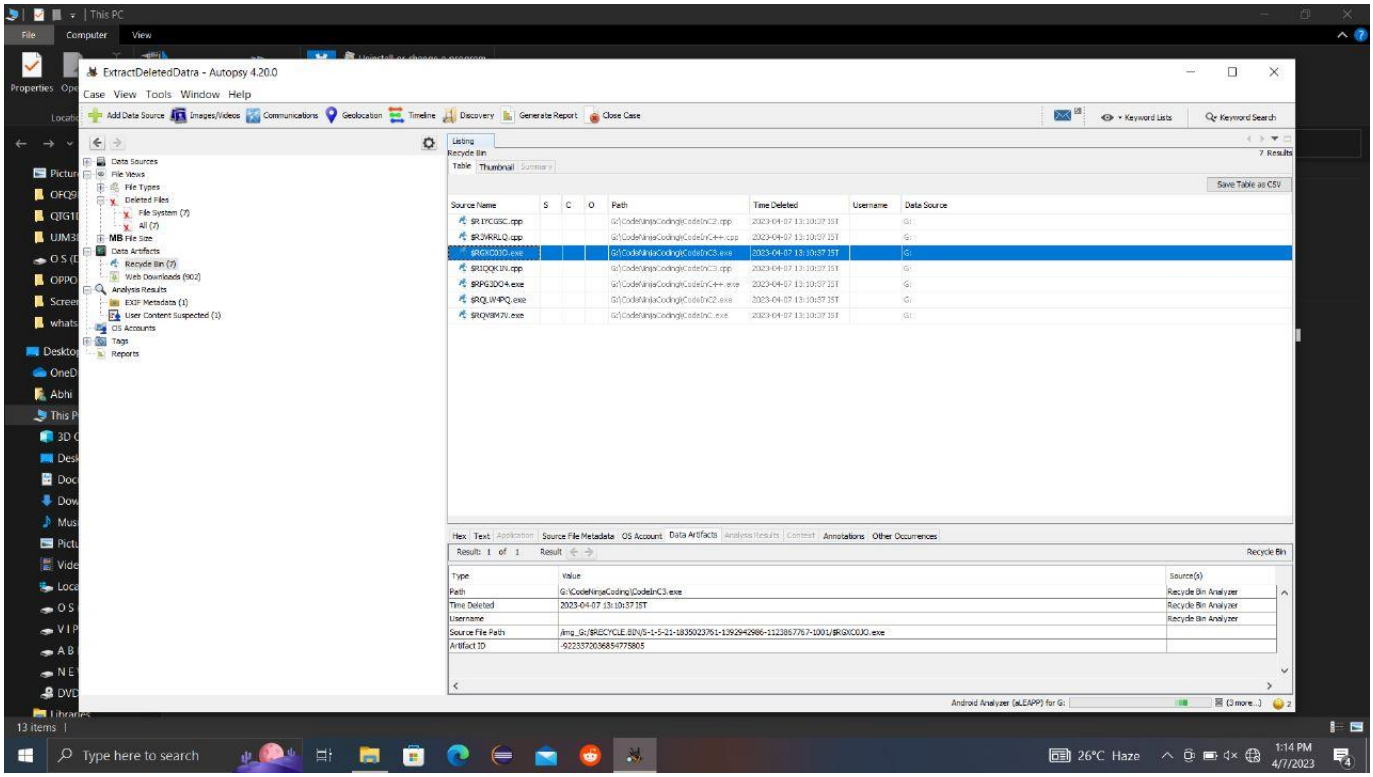

ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help
Type here to search
26°C Haze
1:09 PM
4/7/2023

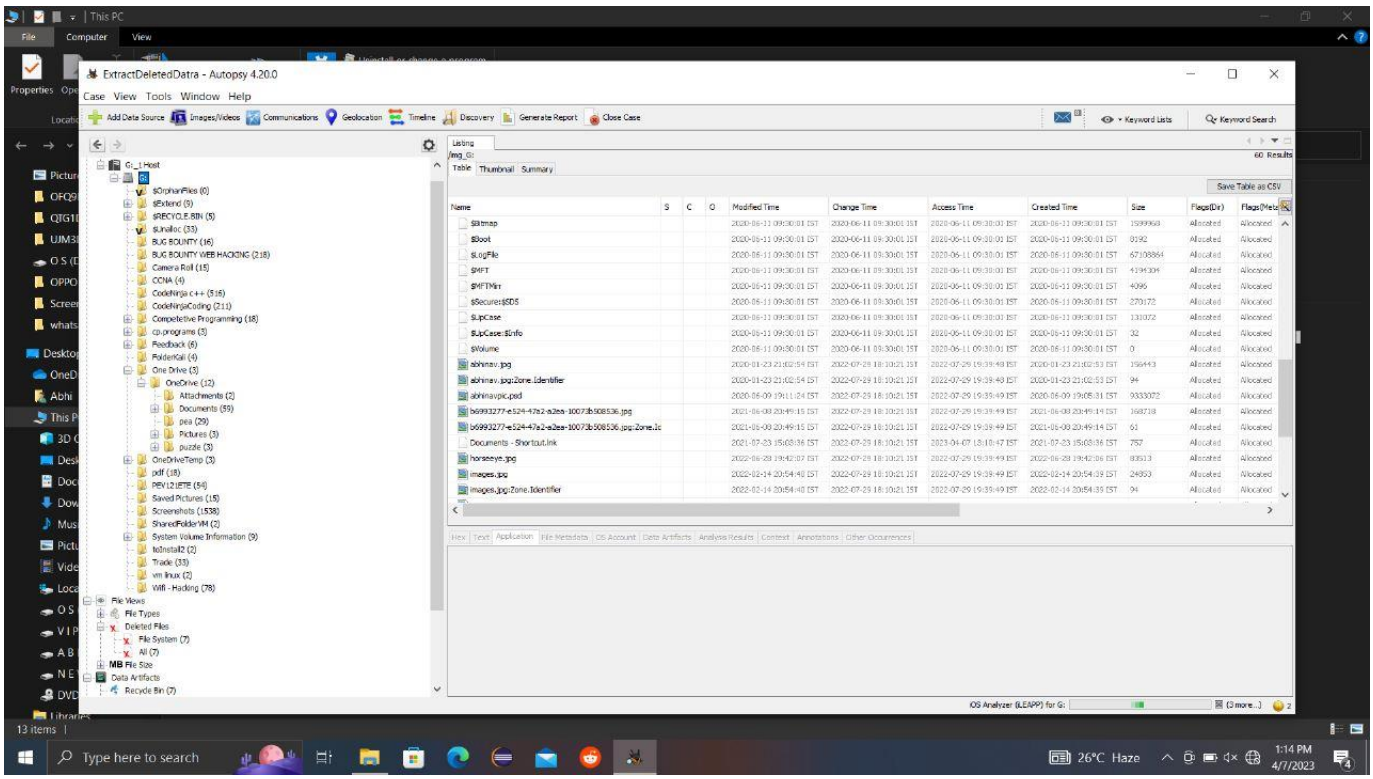

This PC
ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Steps
Select Data Source
Select Local Disk
Disk Name
Disk Size
Drive 2
7.2 GB
N E W (G:)
48.8 GB
O S (D:)
633.3 GB
V I P E R (E:)
150.5 GB
OK
Cancel
Refresh Local Disks
< Back
Next >
Finish
Cancel
Help
13 items
Type here to search
Watchlist Ideas
1:13 PM
4/7/2023

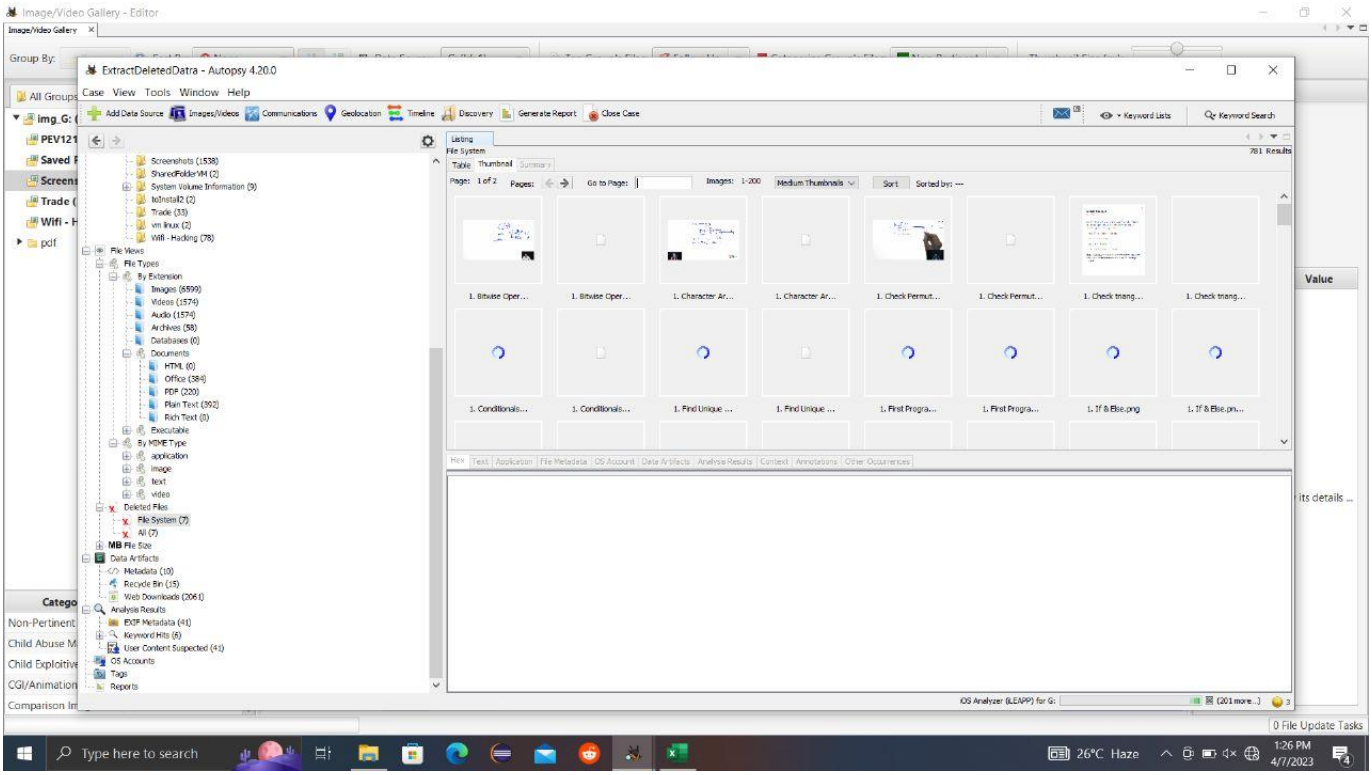

This PC
ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
The selected module has no per-run settings.
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
Data Source Integrity
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
Select All
Deselect All
History
< Back
Next >
Finish
Cancel
Help
13 items
Type here to search
Watchlist Ideas
1:13 PM
4/7/2023

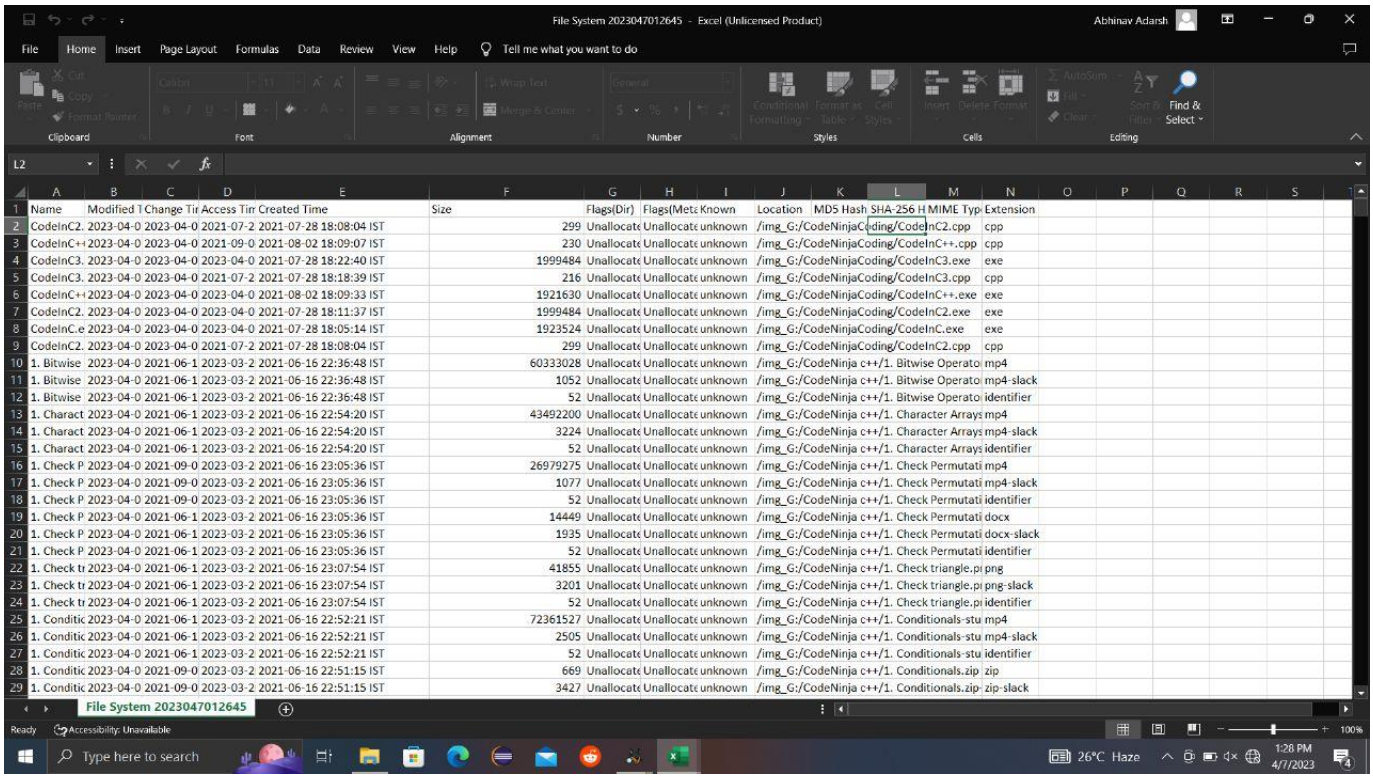

ExtractDeletedDatra - Autopsy 4.20.0
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
Adding: One Drive/OneDrive/puzzleja/b/fvl/mobile camera pic
*This process may take some time for large data sources.
Cancel

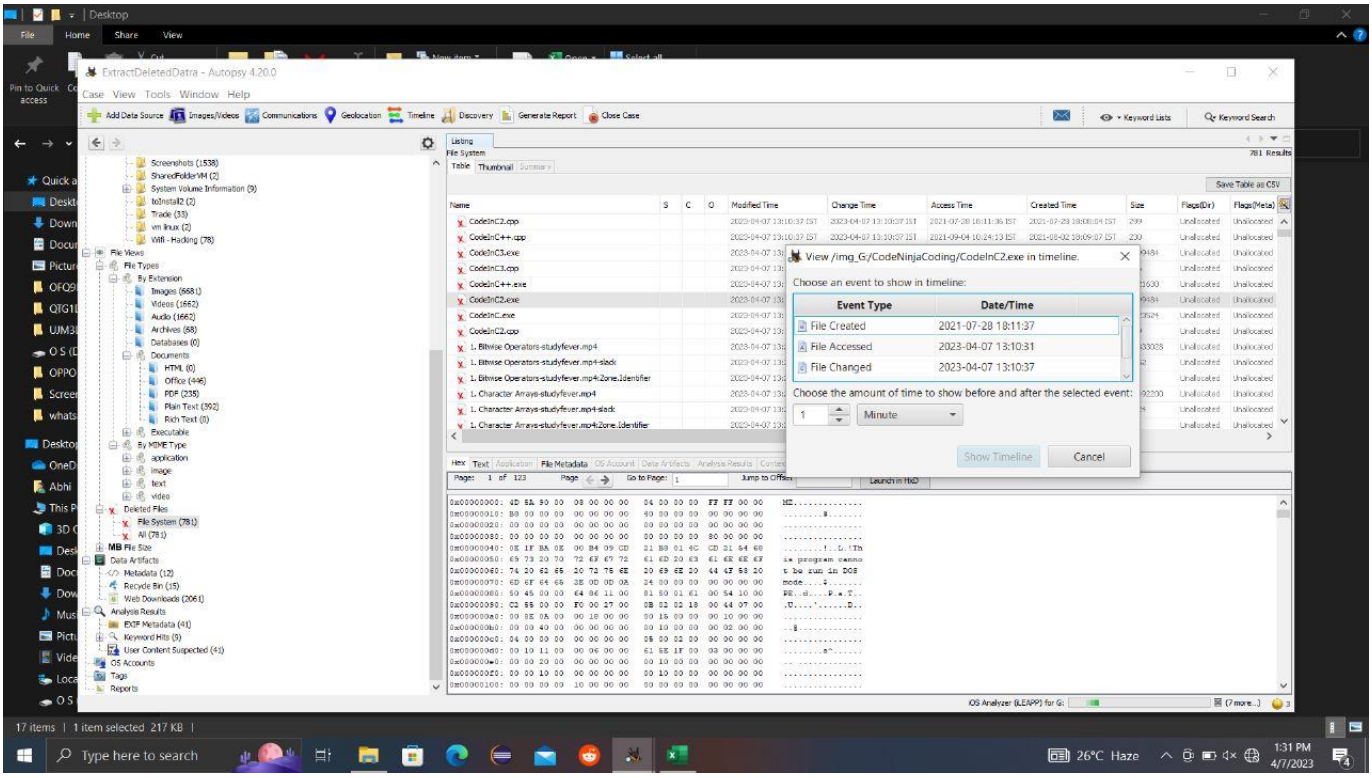

ExtractDeletedDatra - Autopsy 4.20.0
CodeInC2.cpp
CodeInC++.cpp
CodeInC3.exe
CodeInC3.cpp
CodeInC++.exe
CodeInC2.exe
CodeInC.exe


ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File System (7)
All (7)
MB File Size
Data Artifacts
Recycle Bin (7)
Web Downloads (902)
Analysis Results
EXIF Metadata (1)
User Content Suspected (1)
OS Accounts
Tags
Reports
Recycle Bin
7 Results
Save Table as CSV
Source Name
Path
Time Deleted
Username
Data Source
$R1YCGSC.cpp
$RJVRRLQ.cpp
$RGXC0JO.exe
$RQQK1N.cpp
$RPG3DO4.exe
$RQLWPQ.exe
$RQV8M7V.exe
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 1 of 1
Type
Value
Source(s)
Path
G:\CodeNinjaCoding\CodeInC3.exe
Recycle Bin Analyzer
Time Deleted
2023-04-07 13:10:37 IST
Username
Source File Path
/img_G:/$RECYCLE.BIN/S-1-5-21-1835023751-1392942986-1123857767-1001/$RGXC0JO.exe
Artifact ID
-9223372036854775805
Android Analyzer (aLEAPP) for G:
13 items
Type here to search
26°C Haze
1:14 PM
4/7/2023

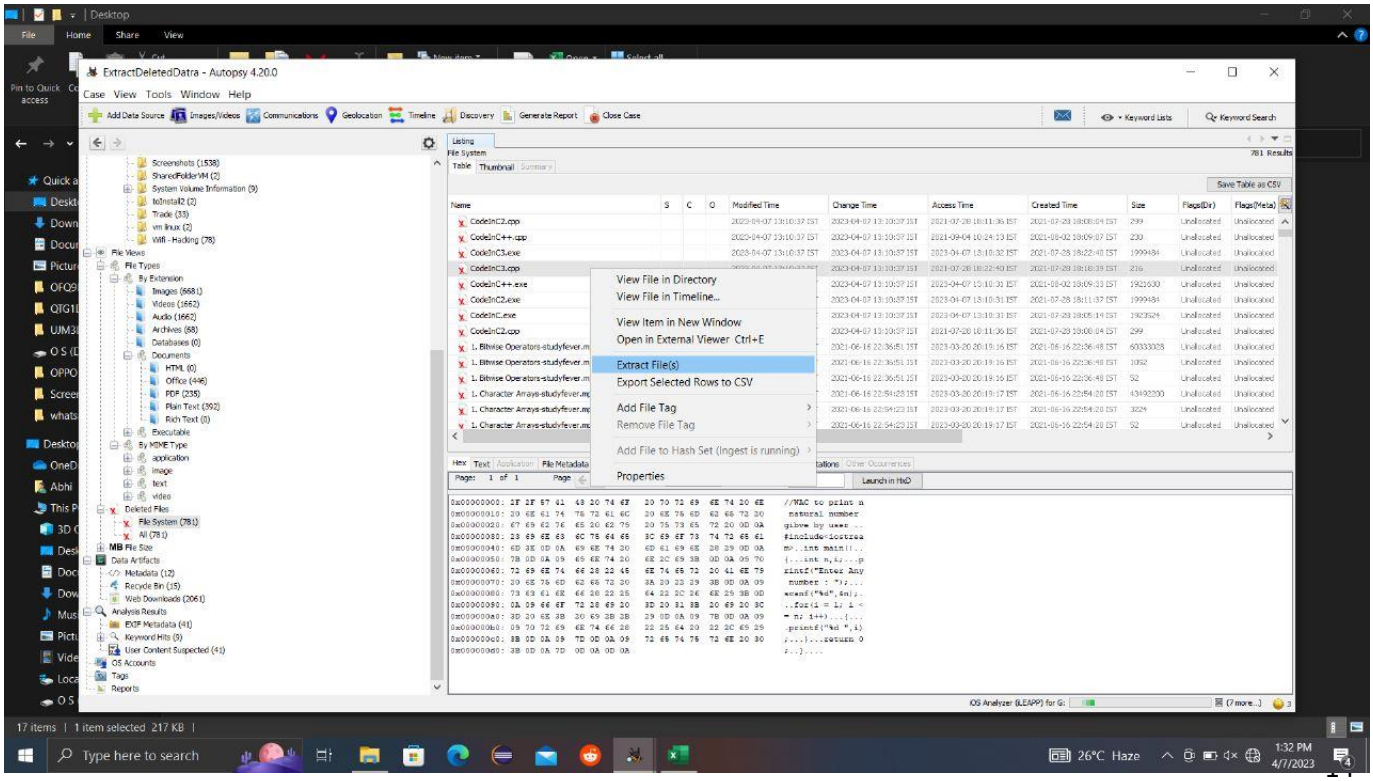

ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
G:_1 Host
$OrphanFiles (0)
$Extend (5)
$RECYCLE.BIN (5)
$Unalloc (35)
BUG BOUNTY (16)
BUG BOUNTY WEB HACKING (218)
Camera Roll (15)
CCNA (4)
CodeNinja c++ (516)
CodeNinjaCoding (211)
Competetive Programming (18)
cp-programs (3)
Feedback (6)
FolderKali (4)
One Drive (3)
OneDrive (12)
Attachments (2)
Documents (59)
pea (29)
Pictures (3)
puzzle (3)
OneDriveTemp (3)
pdf (18)
PEV12 LETTE (56)
Saved Pictures (15)
Screenshots (1,538)
SharedFolderVM (2)
System Volume Information (9)
tshirts2 (2)
Trade (33)
vm linux (2)
Wifi - Hacking (78)
File Views
File Types
Deleted Files
File System (7)
All (7)
MB File Size
Data Artifacts
Recycle Bin (7)
/img_G:
60 Results
Save Table as CSV
Name
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
$Bitmap
$Boot
$LogFile
$MFT
$MFTMirr
$Secure:$SDS
$UpCase
$UpCase:$Info
$Volume
abhinav.jpg
abhinav.jpg:Zone.Identifier
abhinavpic.psd
b6993277-e524-47a2-a2ea-1007db508536.jpg
b6993277-e524-47a2-a2ea-1007db508536.jpg:Zone.Id
Documents - Shortcut.lnk
horseeye.jpg
images.jpg
images.jpg:Zone.Identifier
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
iOS Analyzer (iLEAPP) for G:
13 items
Type here to search
26°C Haze
1:14 PM
4/7/2023

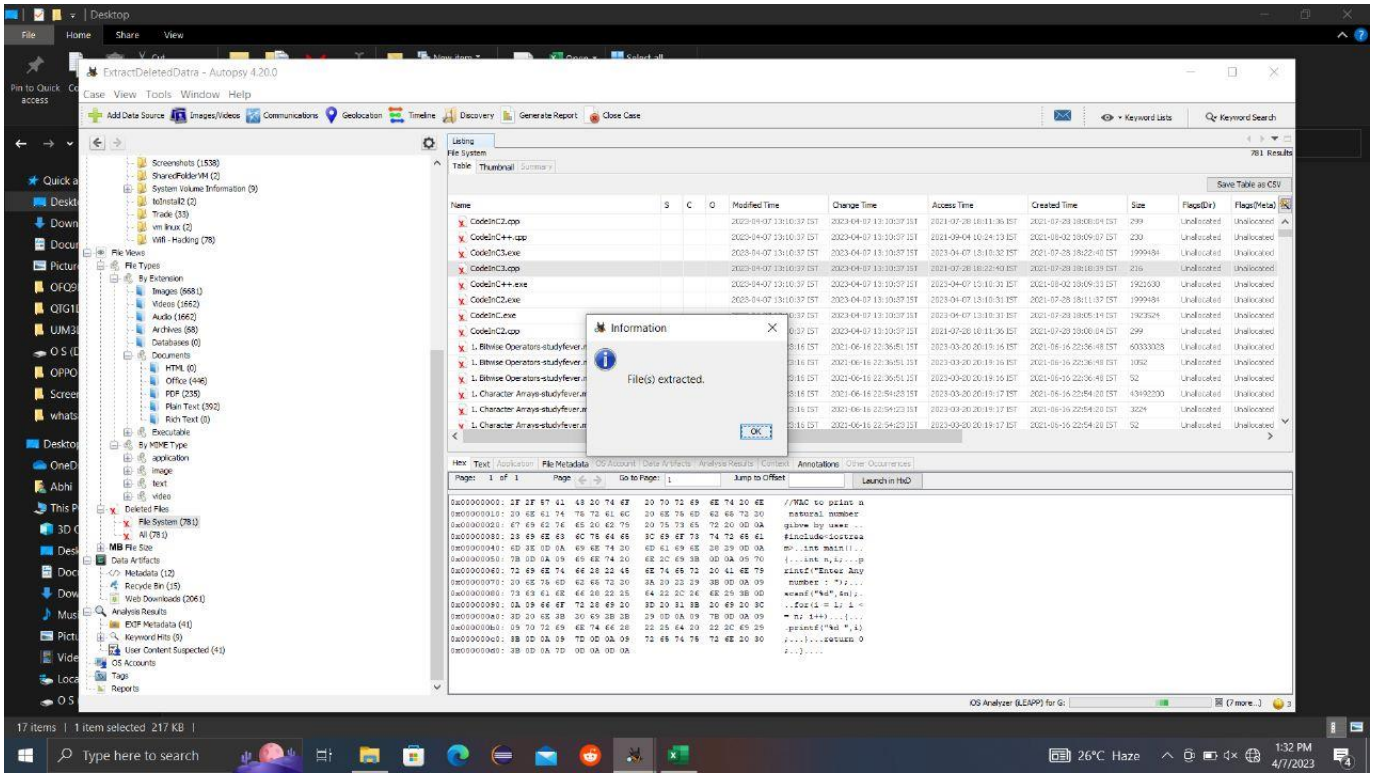

Image/Video Gallery - Editor
ExtractDeletedDatra - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Value
0 File Update Tasks
Type here to search
26°C Haze
1:26 PM
4/7/2023


File System 2023047012645 - Excel (Unlicensed Product)
Abhinav Adarsh
File Home Insert Page Layout Formulas Data Review View Help
Tell me what you want to do
Clipboard Font Alignment Number Styles Cells Editing
Name Modified T Change Tir Access Tim Created Time Size Flags(Dir) Flags(Meta Known Location MD5 Hash SHA-256 H MIME Typ Extension
CodeInC2. 2023-04-0 2023-04-0 2021-07-2 2021-07-28 18:08:04 IST 299 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC2.cpp cpp
CodeInC++ 2023-04-0 2023-04-0 2021-09-0 2021-08-02 18:09:07 IST 230 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC++.cpp cpp
CodeInC3. 2023-04-0 2023-04-0 2023-04-0 2021-07-28 18:22:40 IST 1999484 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC3.exe exe
CodeInC3. 2023-04-0 2023-04-0 2021-07-2 2021-07-28 18:18:39 IST 216 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC3.cpp cpp
CodeInC++ 2023-04-0 2023-04-0 2023-04-0 2021-08-02 18:09:33 IST 1921630 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC++.exe exe
CodeInC2. 2023-04-0 2023-04-0 2023-04-0 2021-07-28 18:11:37 IST 1999484 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC2.exe exe
CodeInC.e 2023-04-0 2023-04-0 2023-04-0 2021-07-28 18:05:14 IST 1923524 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC.exe exe
CodeInC2. 2023-04-0 2023-04-0 2021-07-2 2021-07-28 18:08:04 IST 299 Unallocate Unallocate unknown /img_G:/CodeNinjaCoding/CodeInC2.cpp cpp
1. Bitwise 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:36:48 IST 60333028 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Bitwise Operato mp4
1. Bitwise 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:36:48 IST 1052 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Bitwise Operato mp4-slack
1. Bitwise 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:36:48 IST 52 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Bitwise Operato identifier
1. Charact 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:54:20 IST 43492200 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Character Arrays mp4
1. Charact 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:54:20 IST 3224 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Character Arrays mp4-slack
1. Charact 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:54:20 IST 52 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Character Arrays identifier
1. Check P 2023-04-0 2021-09-0 2023-03-2 2021-06-16 23:05:36 IST 26979275 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check Permutati mp4
1. Check P 2023-04-0 2021-09-0 2023-03-2 2021-06-16 23:05:36 IST 1077 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check Permutati mp4-slack
1. Check P 2023-04-0 2021-09-0 2023-03-2 2021-06-16 23:05:36 IST 52 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check Permutati identifier
1. Check P 2023-04-0 2021-06-1 2023-03-2 2021-06-16 23:05:36 IST 14449 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check Permutati docx
1. Check P 2023-04-0 2021-06-1 2023-03-2 2021-06-16 23:05:36 IST 1935 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check Permutati docx-slack
1. Check P 2023-04-0 2021-06-1 2023-03-2 2021-06-16 23:05:36 IST 52 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check Permutati identifier
1. Check tr 2023-04-0 2021-06-1 2023-03-2 2021-06-16 23:07:54 IST 41855 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check triangle.pi png
1. Check tr 2023-04-0 2021-06-1 2023-03-2 2021-06-16 23:07:54 IST 3201 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check triangle.pi png-slack
1. Check tr 2023-04-0 2021-06-1 2023-03-2 2021-06-16 23:07:54 IST 52 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Check triangle.pi identifier
1. Conditic 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:52:21 IST 72361527 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Conditionals-stu mp4
1. Conditic 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:52:21 IST 2505 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Conditionals-stu mp4-slack
1. Conditic 2023-04-0 2021-06-1 2023-03-2 2021-06-16 22:52:21 IST 52 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Conditionals-stu identifier
1. Conditic 2023-04-0 2021-09-0 2023-03-2 2021-06-16 22:51:15 IST 669 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Conditionals.zip zip
1. Conditic 2023-04-0 2021-09-0 2023-03-2 2021-06-16 22:51:15 IST 3427 Unallocate Unallocate unknown /img_G:/CodeNinja c++/1. Conditionals.zip zip-slack
File System 2023047012645
Ready
Accessibility: Unavailable
Type here to search
26°C Haze
1:28 PM
4/7/2023


ExtractDeletedDatra - Autopsy 4.20.0
View /img_G:/CodeNinjaCoding/CodeInC2.exe in timeline.
Choose an event to show in timeline:
Event Type
Date/Time
File Created
2021-07-28 18:11:37
File Accessed
2023-04-07 13:10:31
File Changed
2023-04-07 13:10:37
Choose the amount of time to show before and after the selected event:
Minute
Show Timeline
Cancel

•


ExtractDeletedDatra - Autopsy 4.20.0
View File in Directory
View File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)
Export Selected Rows to CSV
Add File Tag
Remove File Tag
Add File to Hash Set (Ingest is running)
Properties


ExtractDeletedDatra - Autopsy 4.20.0
Information
File(s) extracted.
OK

•

3. Reference/ Bibliography

1. Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
2. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press.
3. Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations. Cengage Learning.
4. Quick, D., Chakraborty, S., & Martini, B. (2019). Digital Forensics Basics: A Practical Guide Using Windows OS. Apress.
5. Autopsy User Documentation: https://sleuthkit.org/autopsy/docs/user-docs/3