DISK FORENSICS

Disk Image Creation and Analysis

TOOLS WE USED IN THIS PROJECT:

- **DISK EXPLORER NTFS.**
- **R DRIVE**
- **WINHEX**
- **ACCESS DATA FTK**

ABSTRACT:

Disk Explorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery. FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Access Data Forensic Toolkit (FTK) is warranted.

File Recovery using EASEUS Data Recovery Wizard EASEUS Data Recovery Wizard is recovery software for windows that supports file, partition, and complete recovery of data. Partition Recovery Using MiniTool Power Data Recovery Tool MiniTool Power Data recovers deleted data from Windows Recycle Bin and restores data from a corrupted hard drive, virus infection, unexpected system shutdown, or software failure.

Forensic Toolkit (FTK) computer forensics software that can be used to acquire, preserve, analyze, and present computer evidence. FTK presents computer evidence by creating a case report and case log to document the evidence and investigation results. This uses the Report Wizard to create and modify reports. In the report, you can add bookmarks, customize graphics references, select file listings, and include supplementary files and the case log. The report is generated in HTML.

DELIVERABLES:

1.September-Data Acquisition and Duplication (Disk Explorer & FTK Imager Tool).

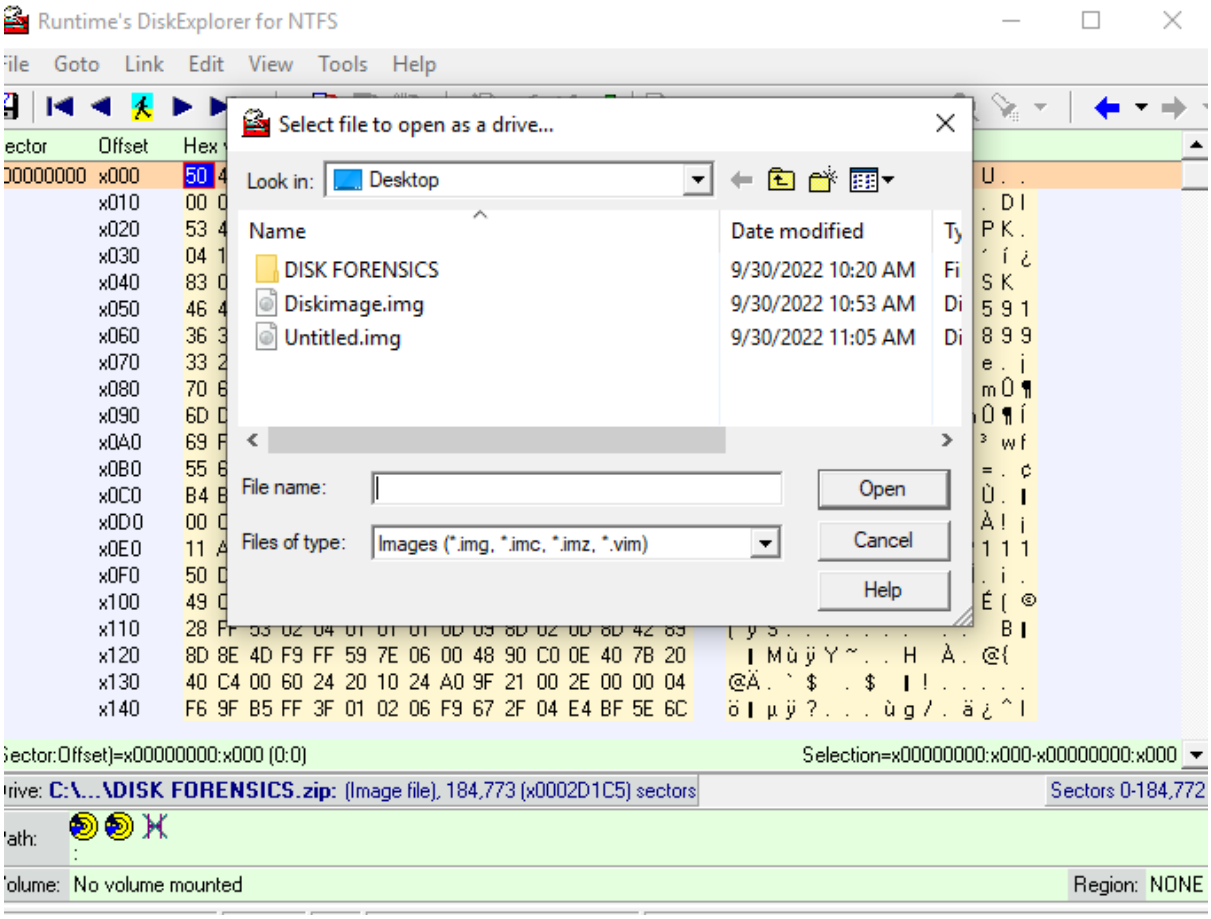
2.October- Recovering Deleted Files and Deleted Partitions.

3.November- Investigating a Case Using Access Data FTK.

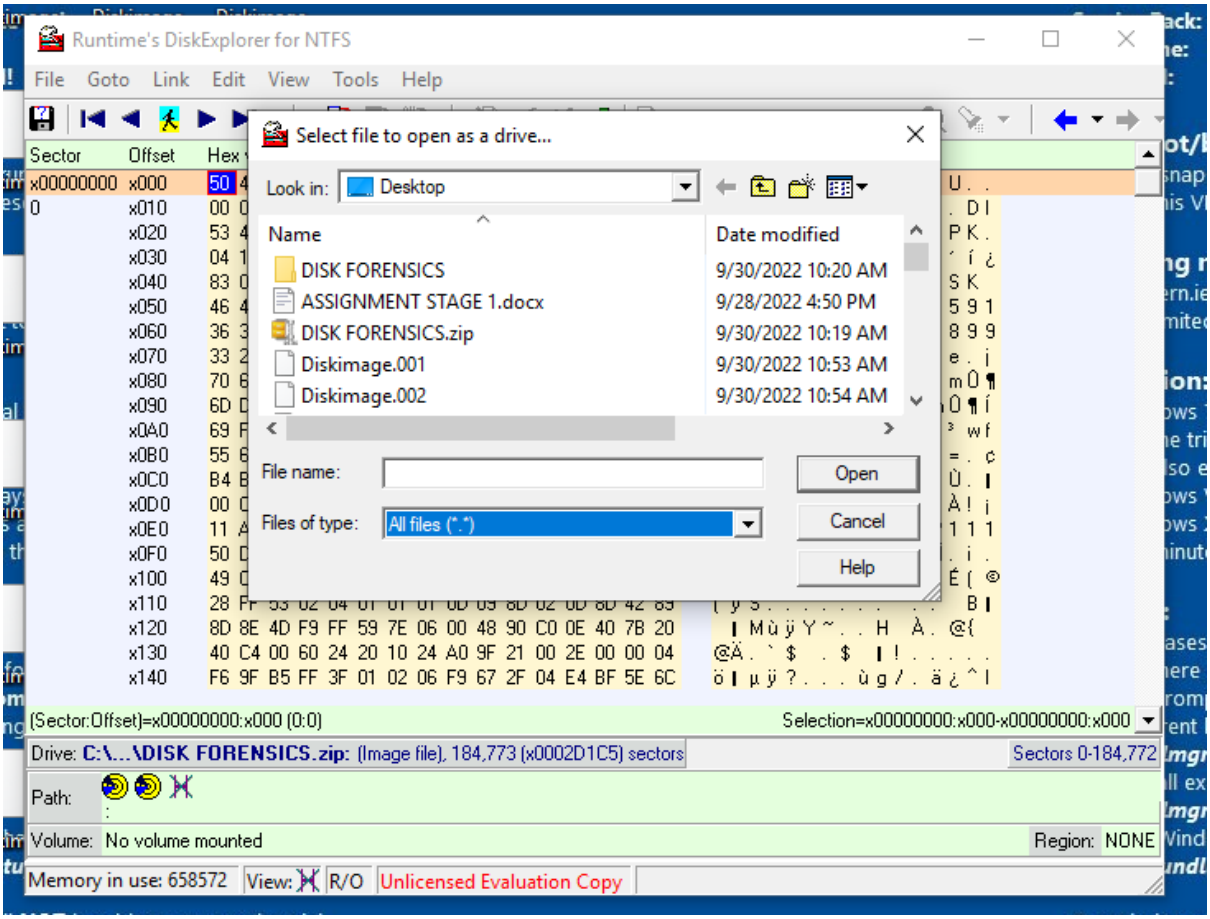
DISK FORENSICS FIRST DELIVERIABLE

Data Acquisition and Duplication (Disk Explorer & FTK Imager Tool).

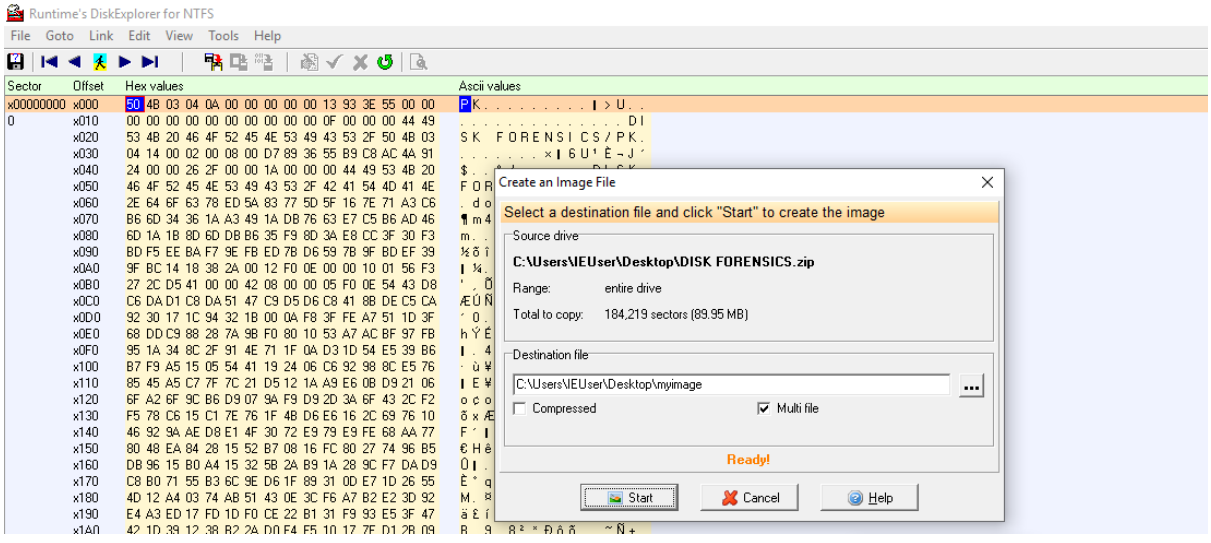
1. Disk Explorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery. Disk Explorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery. It navigates your NTFS drive by jumping to the partition table, boot record, Master file table, or the root directory. It also inspects the file entry details, NT attributes, etc
   Using Disk Explorer we can create disk image, in the below screenshot we have took 100MB data consisting folder. And uploaded in the tool as a drive to create a disk image.



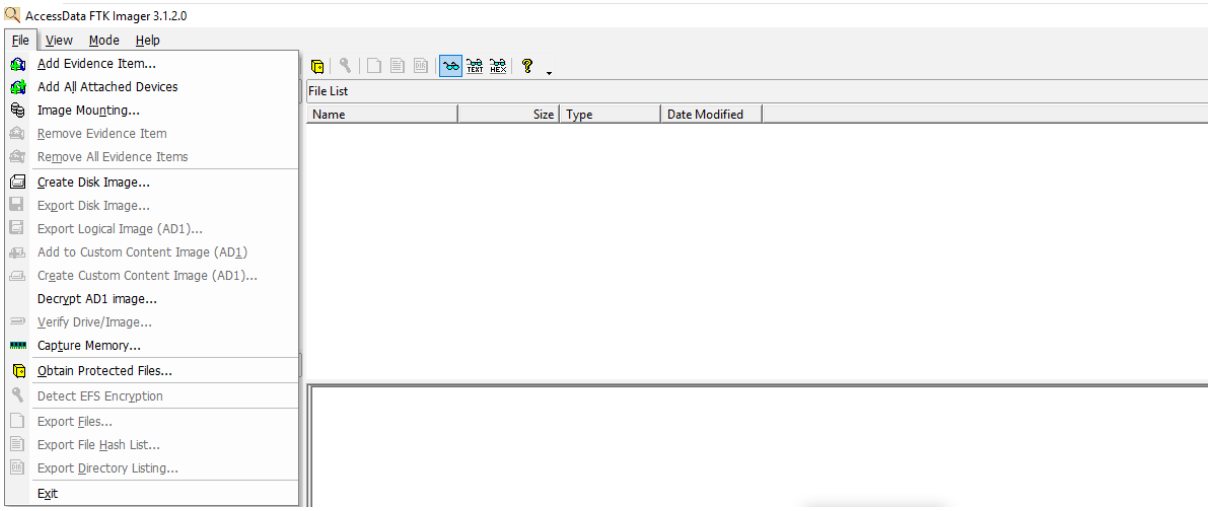
2. In this we have took the folder DISK FORENSICS as the drive for loading in the tool.



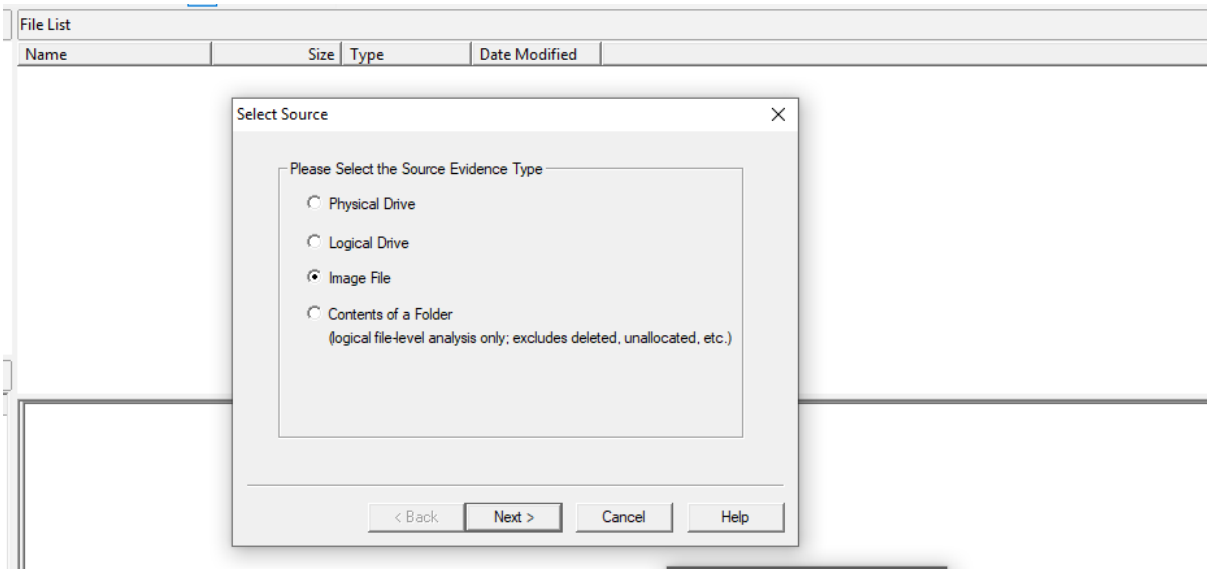
3. Below we are selecting the destination path for the disk image and named it as myimage



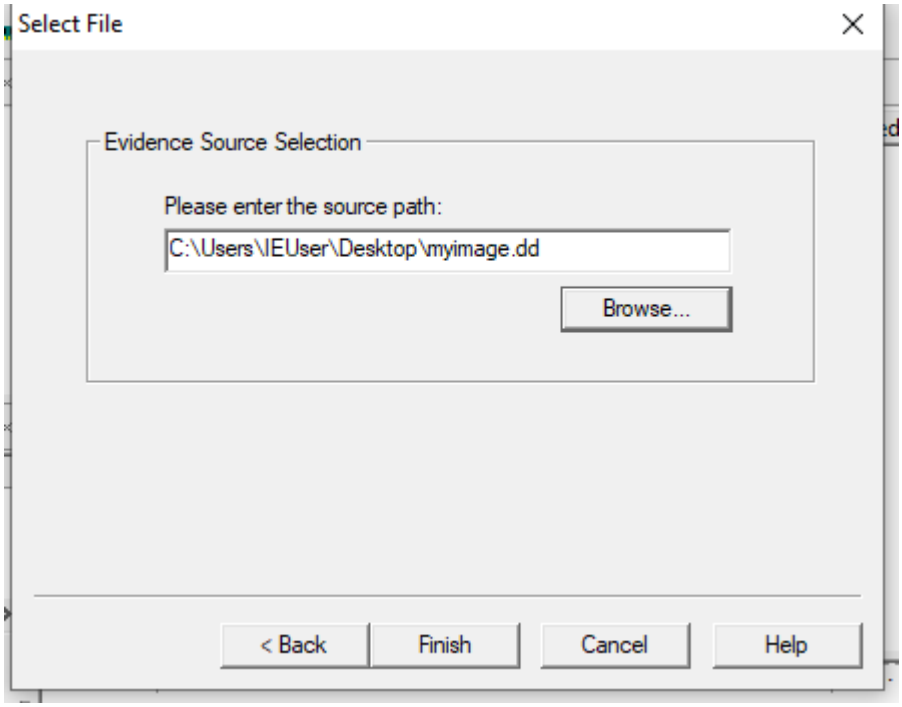
4. FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as AccessData Forensic Toolkit (FTK) is warranted.
   Using this tool we can investigate the data present in the disk image.



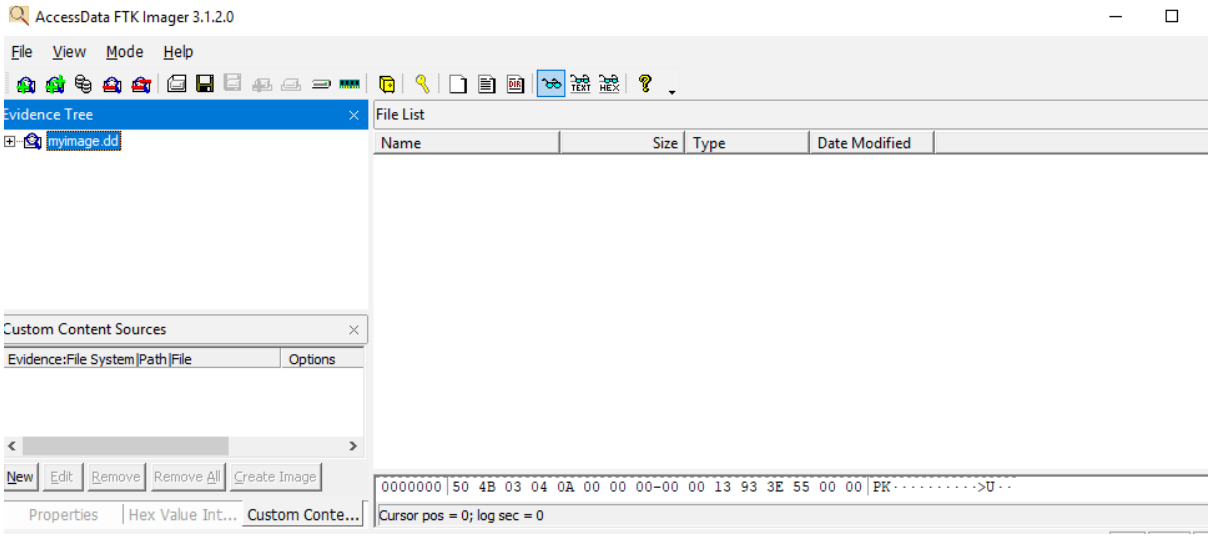
5. Here we are selecting the source which we have to investigate.

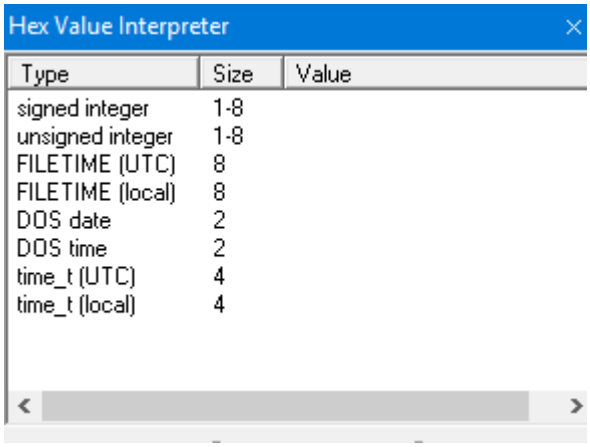


6. In the below screen shot, we are loading the disk image.



7. Below we can view the data present in the disk image in the hex format.





8. In the below screenshot, we can view the type of folders and data present in the image .

```
Created By AccessData® FTK® Imager 3.1.2.0

Case Information:
Acquired using: ADI3.1.2.0
Case Number: 01
Evidence Number: 01
Unique description: DISK IMG
Examiner: KIRAN ALEKHYA MADHURI
Notes: HI

------------------------------------------------------------

Information for C:\Users\IEUser\Desktop\EVIDENCE\myimage.dd:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 184,219
[Image]
 Image Type: Raw (dd)
 Source data size: 89 MB
 Sector count:    184219
[Computed Hashes]
 MD5 checksum:    f42d6878e7a19550a023b0b9e6527688
 SHA1 checksum:   0097fcd4bb986347df58580269cfe7ab3fadafee

Image Information:
 Acquisition started:   Fri Sep 30 18:47:09 2022
 Acquisition finished:  Fri Sep 30 18:47:10 2022
```

```
Information for C:\Users\IEUser\Desktop\EVIDENCE\myimage.dd:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 184,219
[Image]
 Image Type: Raw (dd)
 Source data size: 89 MB
 Sector count:    184219
[Computed Hashes]
 MD5 checksum:    f42d6878e7a19550a023b0b9e6527688
 SHA1 checksum:   0097fcd4bb986347df58580269cfe7ab3fadafee

Image Information:
 Acquisition started:   Fri Sep 30 18:47:09 2022
 Acquisition finished:  Fri Sep 30 18:47:10 2022
 Segment list:
  C:\Users\IEUser\Desktop\EVIDENCE\myimage.dd.001

Image Verification Results:
 Verification started:  Fri Sep 30 18:47:10 2022
 Verification finished: Fri Sep 30 18:47:11 2022
 MD5 checksum:    f42d6878e7a19550a023b0b9e6527688 : verified
 SHA1 checksum:   0097fcd4bb986347df58580269cfe7ab3fadafee : verified
```

Second Deliverable – (October) Recovering Deleted Files and Deleted Partitions

File Recovery using EASEUS Data Recovery Wizard EASEUS Data Recovery Wizard is recovery software for windows that supports file, partition, and complete recovery of data. Partition Recovery Using MiniTool Power Data Recovery Tool MiniTool Power Data recovers deleted data from Windows Recycle Bin and restores data from a corrupted hard drive, virus infection, unexpected system shutdown, or software failure. The recovery of data for the system consisting virus and using the MiniTool Power Data Recovery for getting the data as it is present in the original format without changing the format. Using this tool we can restore the data in the short period of time .

R Drive:

Drive Image and Backup for Windows

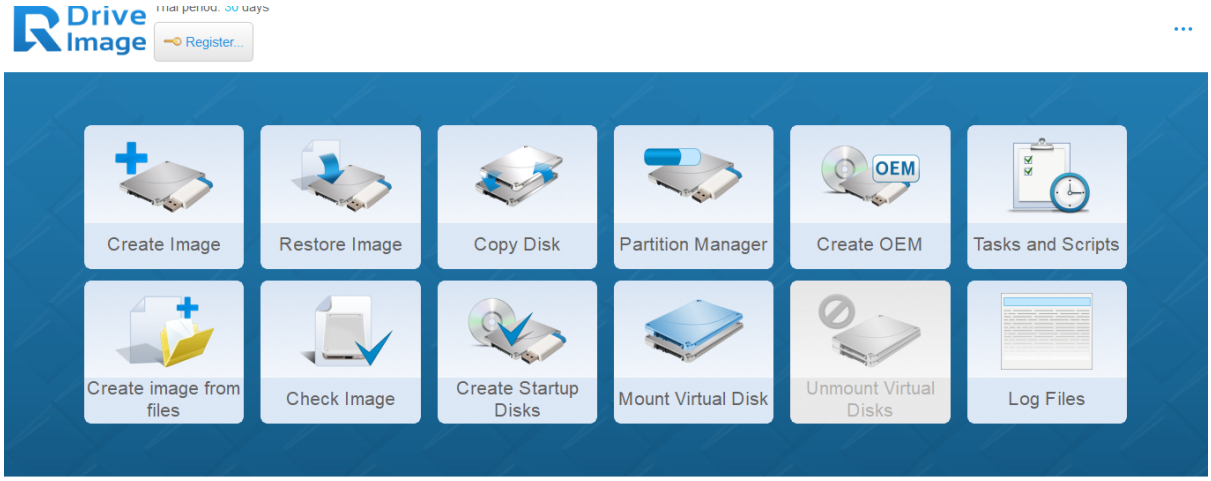
R-Drive Image is a potent utility providing disk image files creation for backup or duplication purposes. A disk image file contains the exact, byte-by-byte copy of a hard drive, partition or logical disk and can be created with various compression levels on the fly without stopping Windows OS and therefore without interrupting your business. These drive image files can then be stored

in a variety of places, including various removable media such as CD-R(W)/DVD, Iomega Zip or Jazz dis, etc.

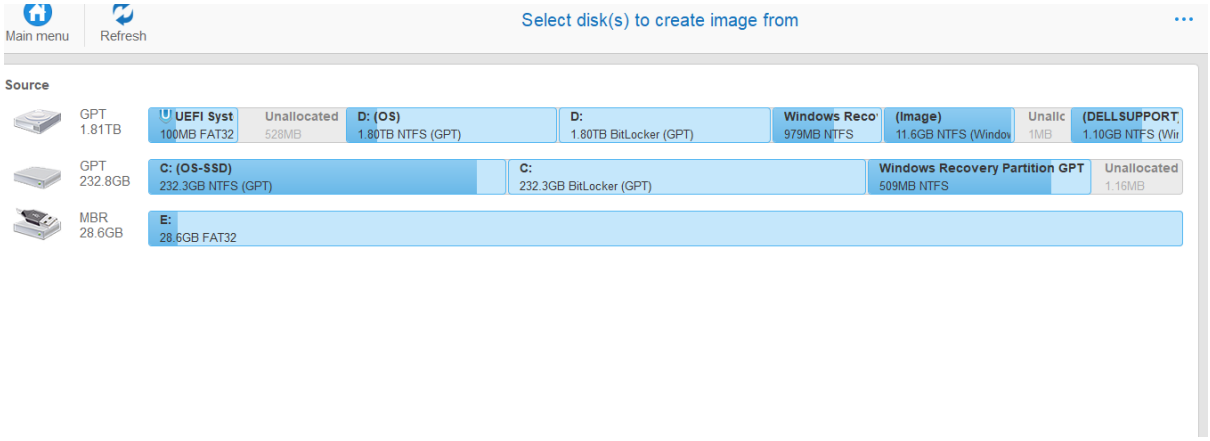
Using R-Drive Image, you can completely and rapidly restore your system after heavy data loss caused by an operating system crash, virus attack or hardware failure.

R-Drive Image is one of the best backup and disaster recovery solutions to prevent losing your data after a fatal system failure.

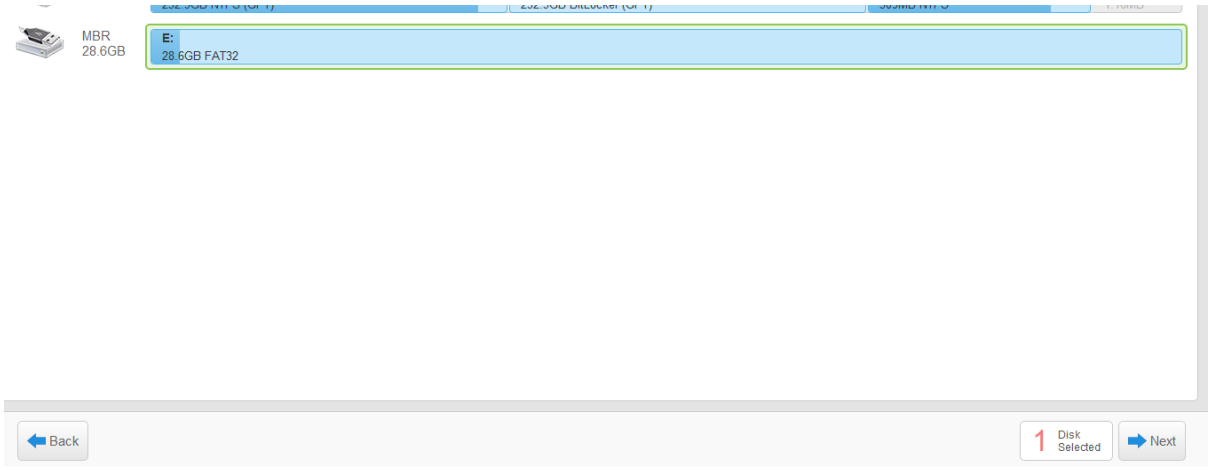
Step 1: Creating Disk image using R-Drive Image tool



Step 2: Selecting drive to create disk image

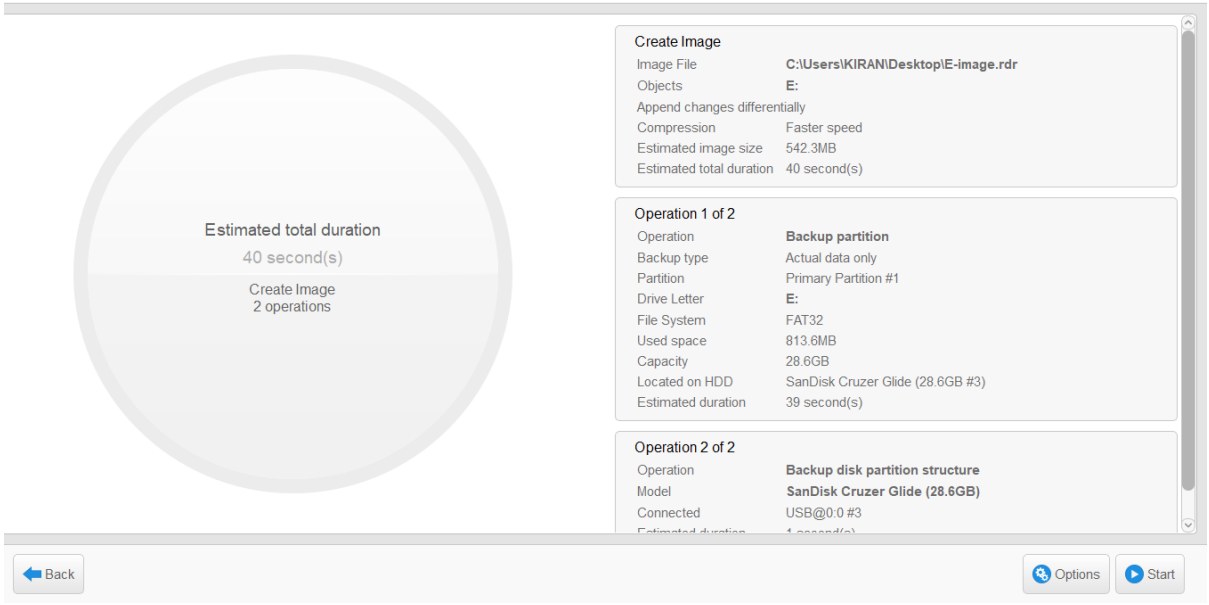


Step 3: Selected the disk and started the operation

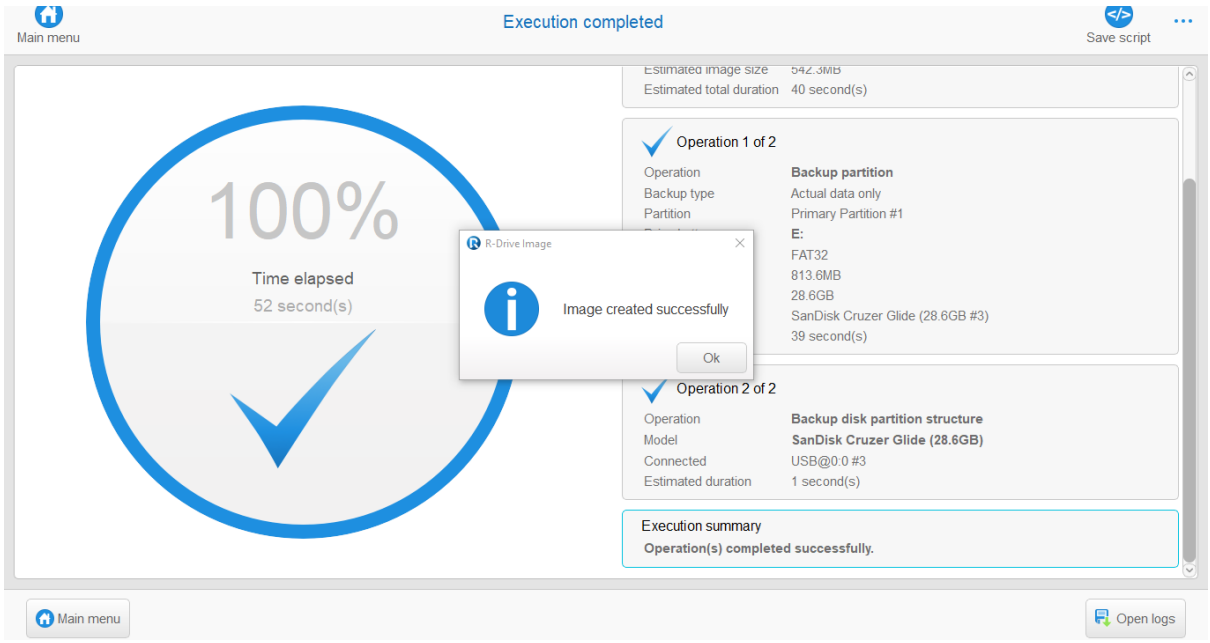


Step 4: Selected the destination to save the disk image

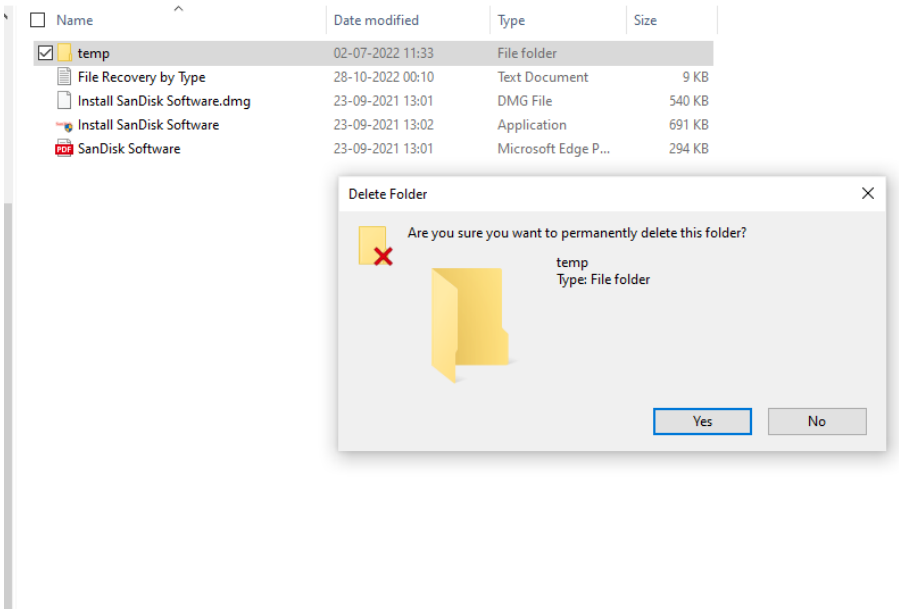
Step 5: Created the disk image



After creating the disk image, the pop message notifies the completion

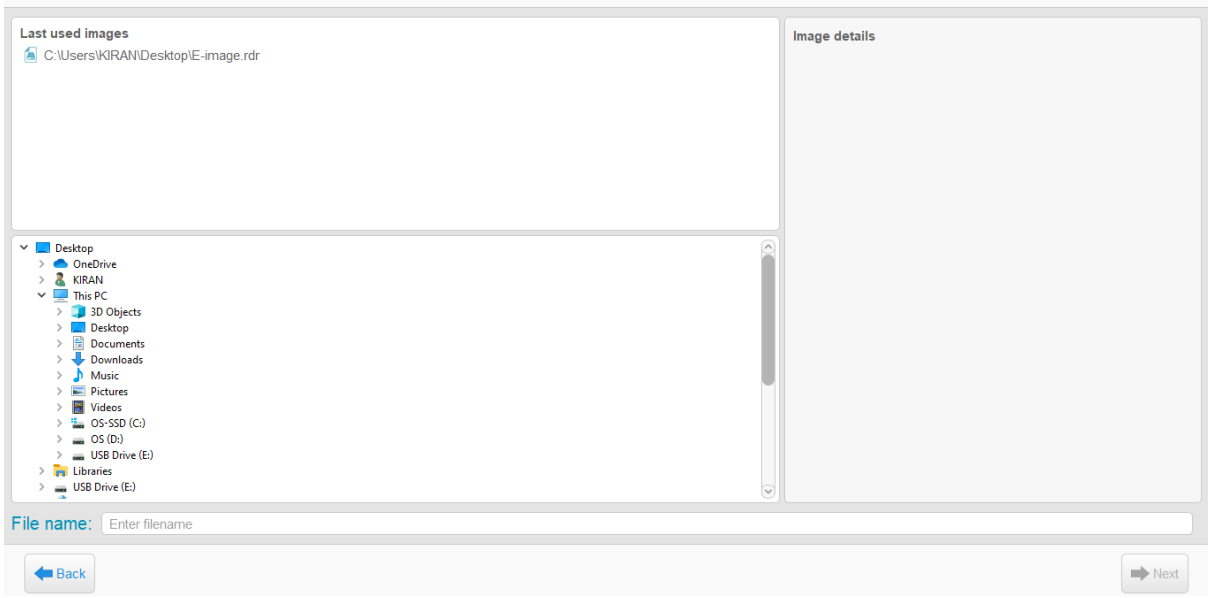


Step 6: Deleting the folder permanently from the drive

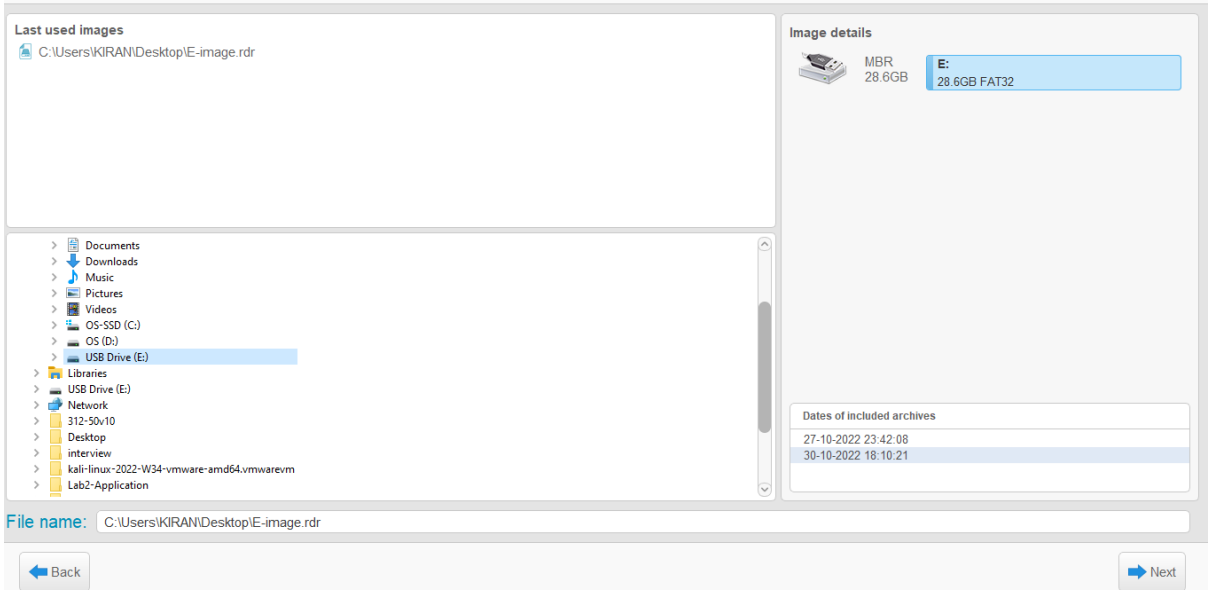


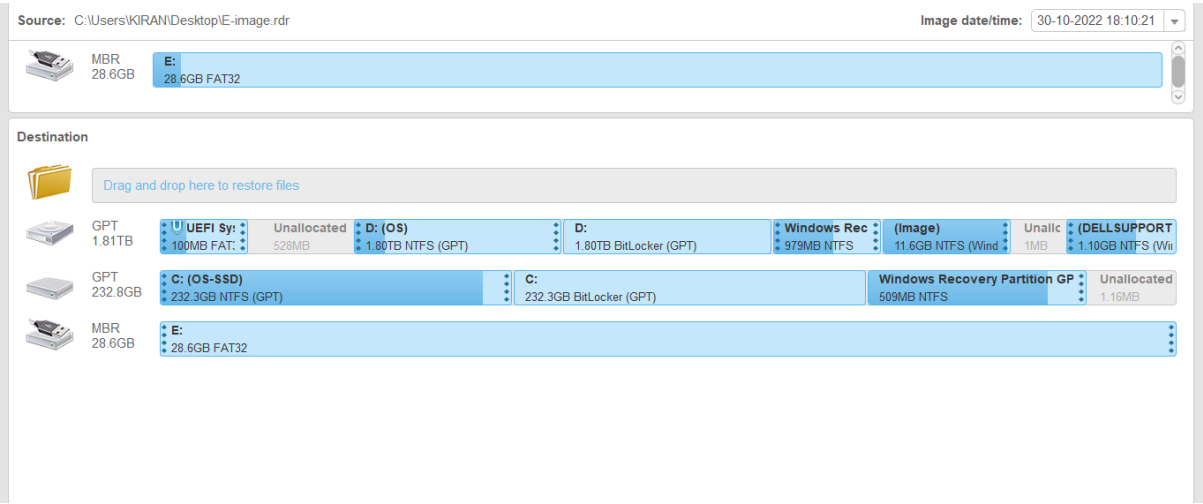
RECOVERING THE DELETED DATA

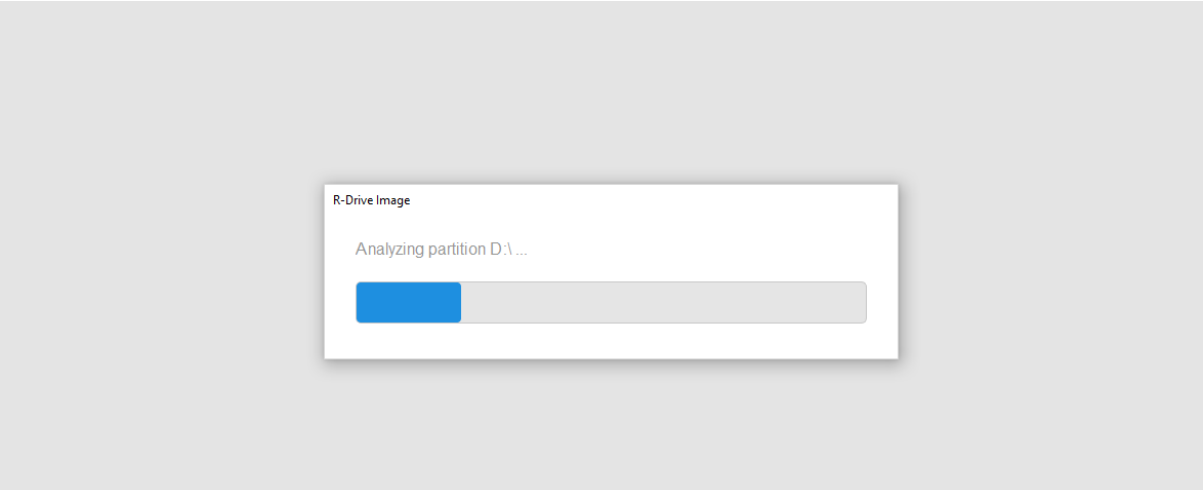
Step 1: Selecting the disk image to recover the data

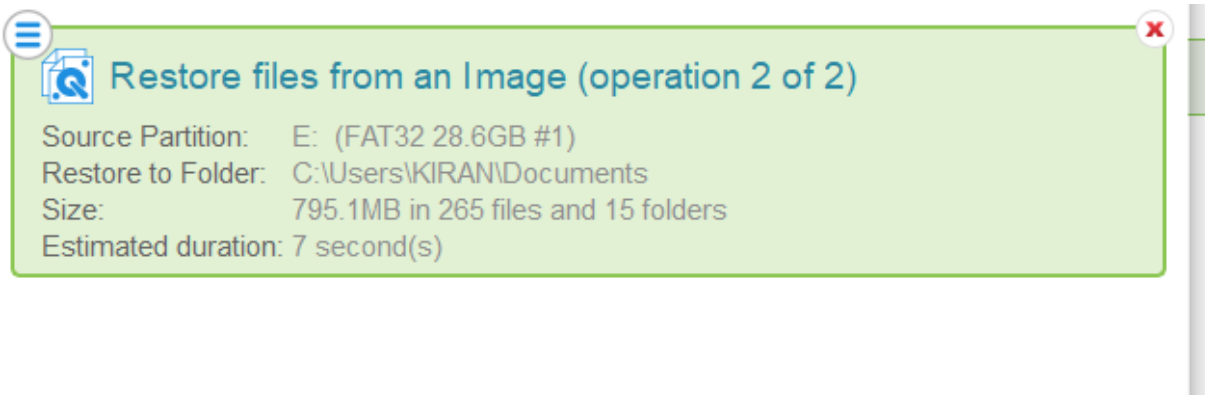


Step 2: Specifying the destination to recover the data

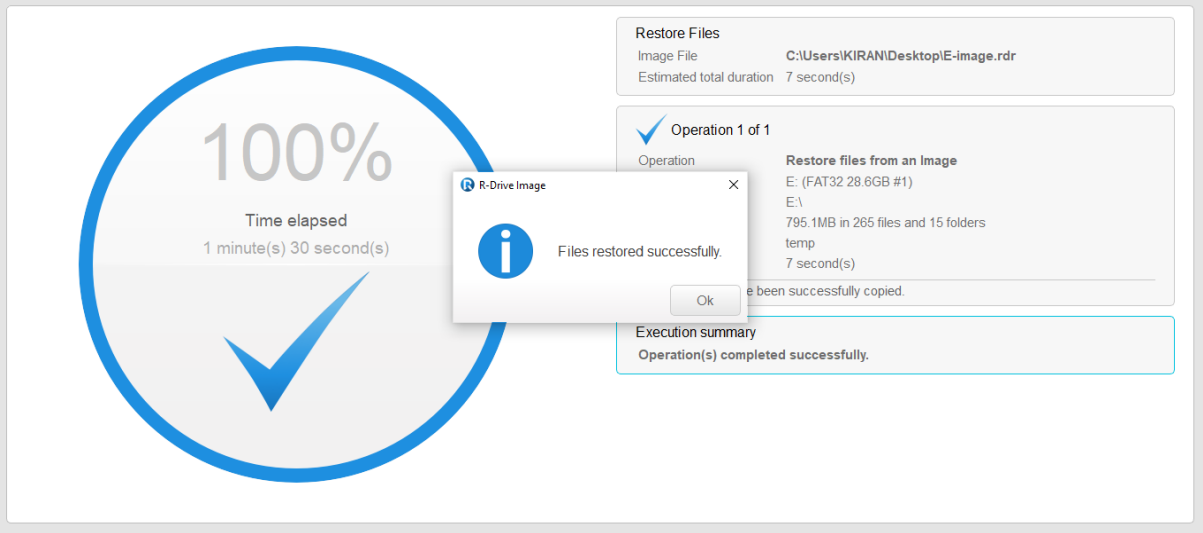


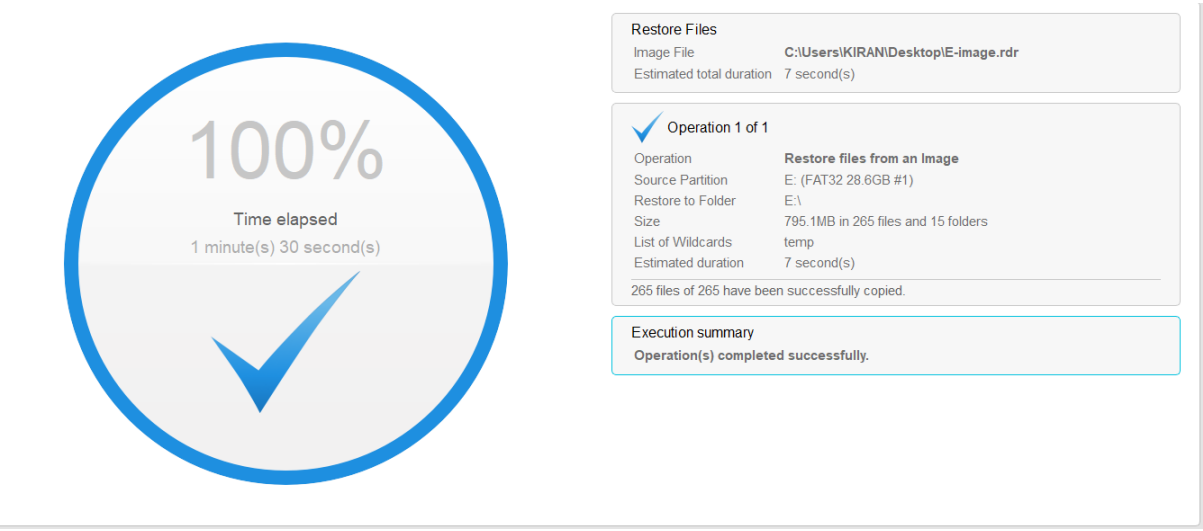

Source: C:\Users\KIRAN\Desktop\E-image.rdr
Image date/time: 30-10-2022 18:10:21
MBR
28.6GB
E:
28.6GB FAT32
Destination
Drag and drop here to restore files
GPT
1.81TB
UEFI Sy
100MB FAT
Unallocated
528MB
D: (OS)
1.80TB NTFS (GPT)
D:
1.80TB BitLocker (GPT)
Windows Rec
979MB NTFS
(Image)
11.6GB NTFS (Wind
Unallc
1MB
(DELLSUPPORT
1.10GB NTFS (Wi
GPT
232.8GB
C: (OS-SSD)
232.3GB NTFS (GPT)
C:
232.3GB BitLocker (GPT)
Windows Recovery Partition GP
509MB NTFS
Unallocated
1.16MB
MBR
28.6GB
E:
28.6GB FAT32


R-Drive Image
Analyzing partition D:\ ...

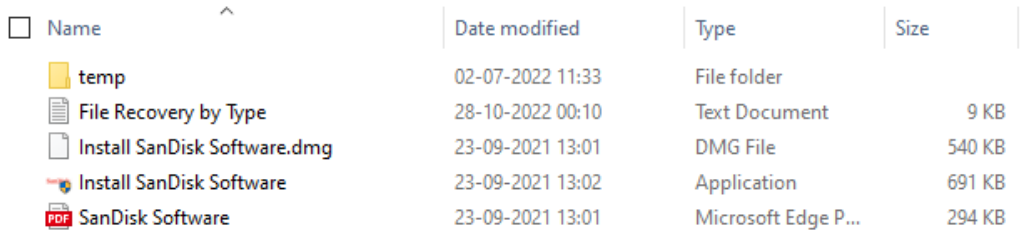

Restore files from an Image (operation 2 of 2)
Source Partition: E: (FAT32 28.6GB #1)
Restore to Folder: C:\Users\KIRAN\Documents
Size: 795.1MB in 265 files and 15 folders
Estimated duration: 7 second(s)

Step 3: The deleted files are recovered successfully





Step 4: The recovered folder(temp) using the disk image

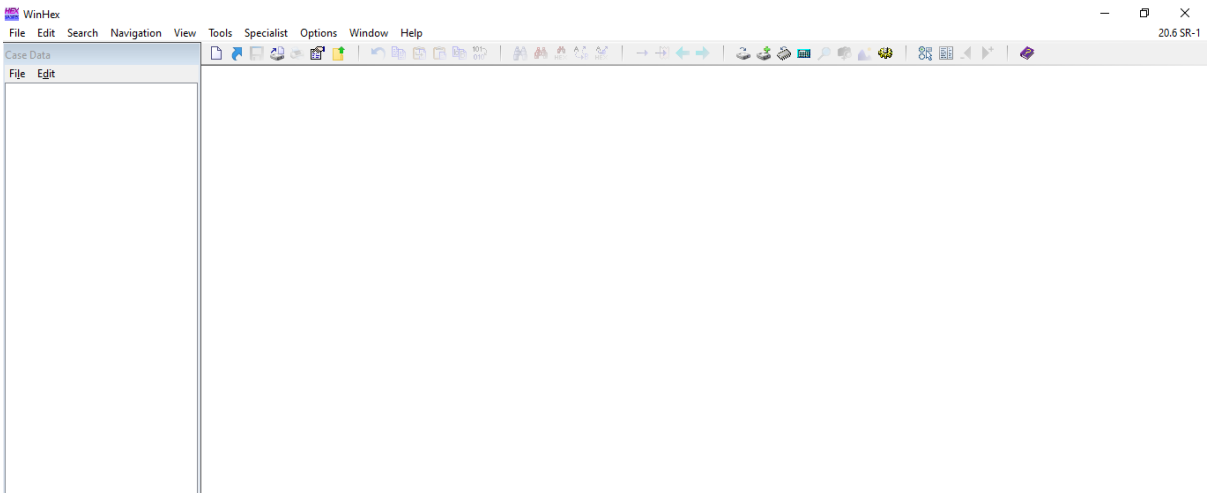


Name	Date modified	Type	Size
temp	02-07-2022 11:33	File folder	
File Recovery by Type	28-10-2022 00:10	Text Document	9 KB
Install SanDisk Software.dmg	23-09-2021 13:01	DMG File	540 KB
Install SanDisk Software	23-09-2021 13:02	Application	691 KB
SanDisk Software	23-09-2021 13:01	Microsoft Edge P...	294 KB

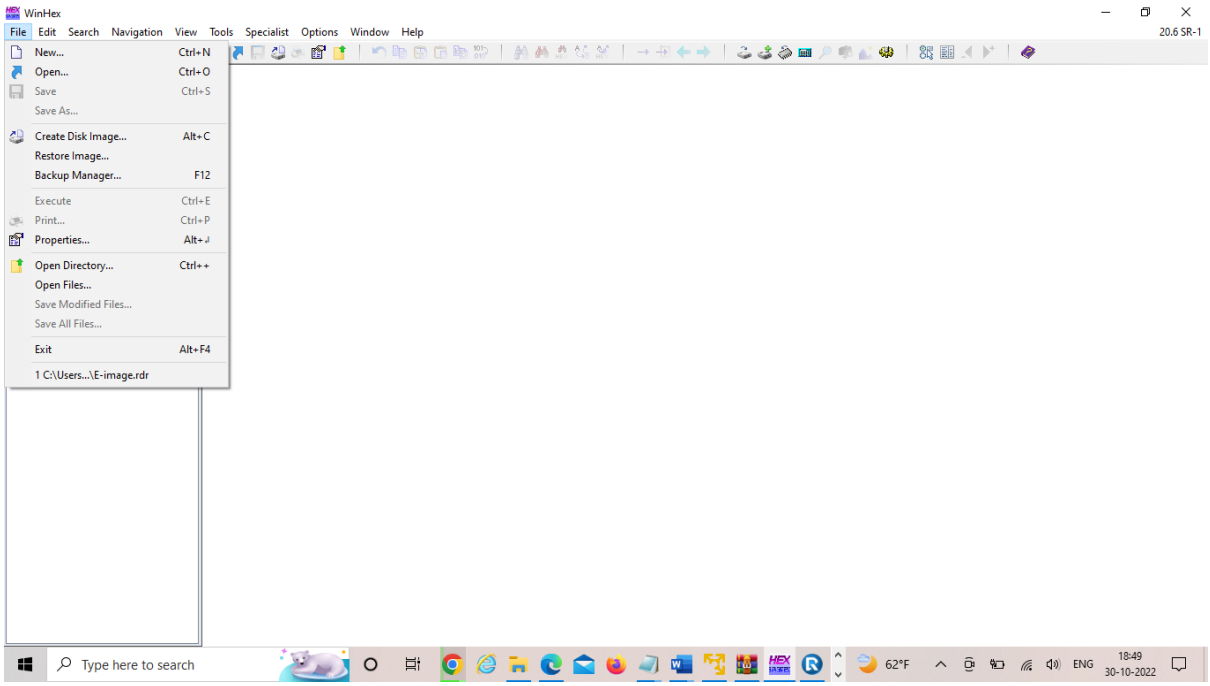
WINHEX:

- WinHex is in its core a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security.
- An advanced tool for everyday and emergency use: inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.

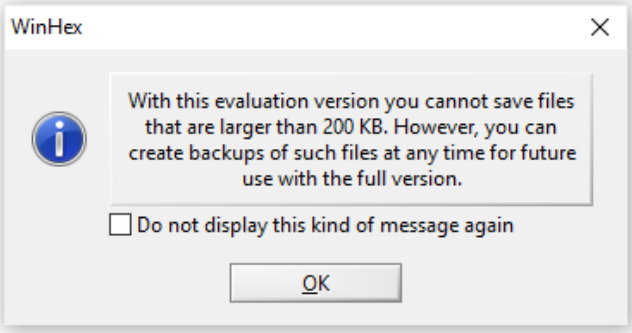
STEP1: install WINHEX tool, and start the application.



Step 2: Using WINHEX we can recover a particular file. In here we are selecting the disk image

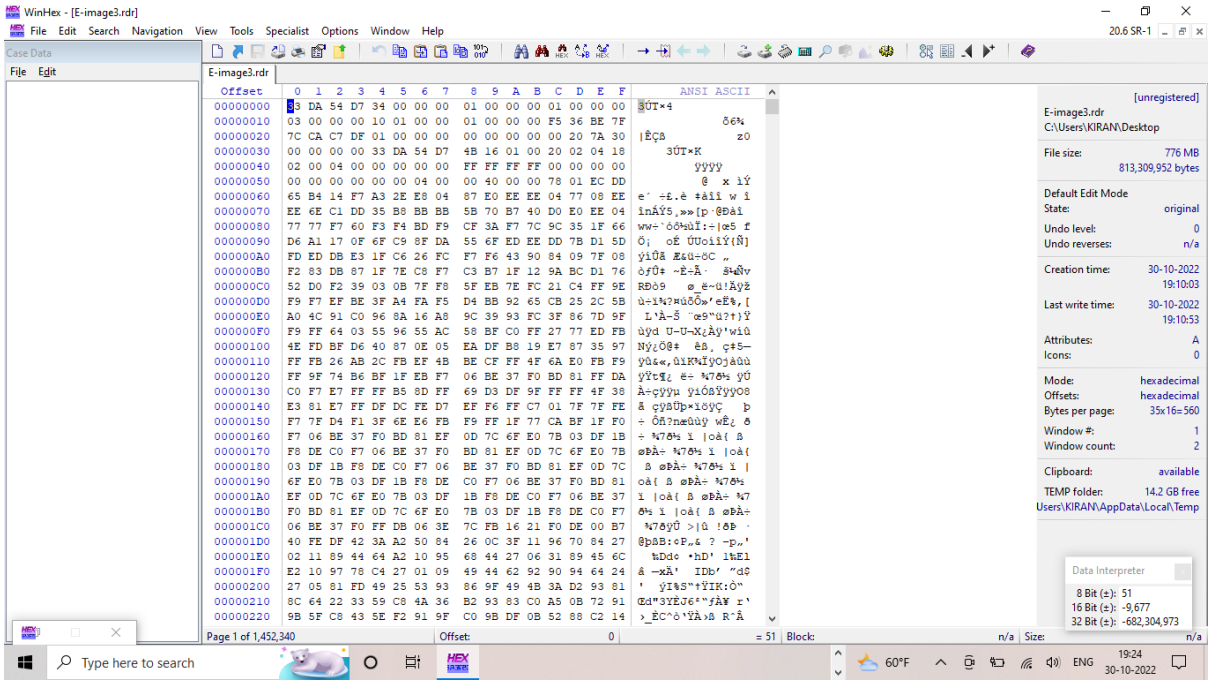


Step 3: popup message will be displayed on monitor

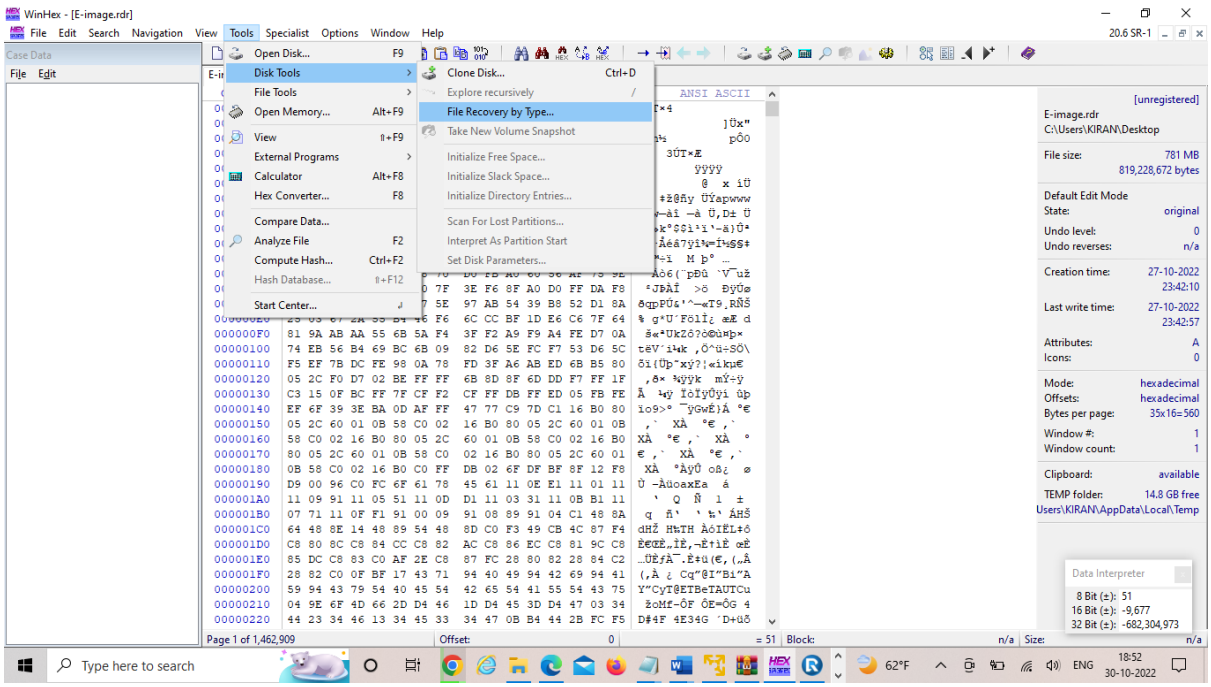


Step 4:

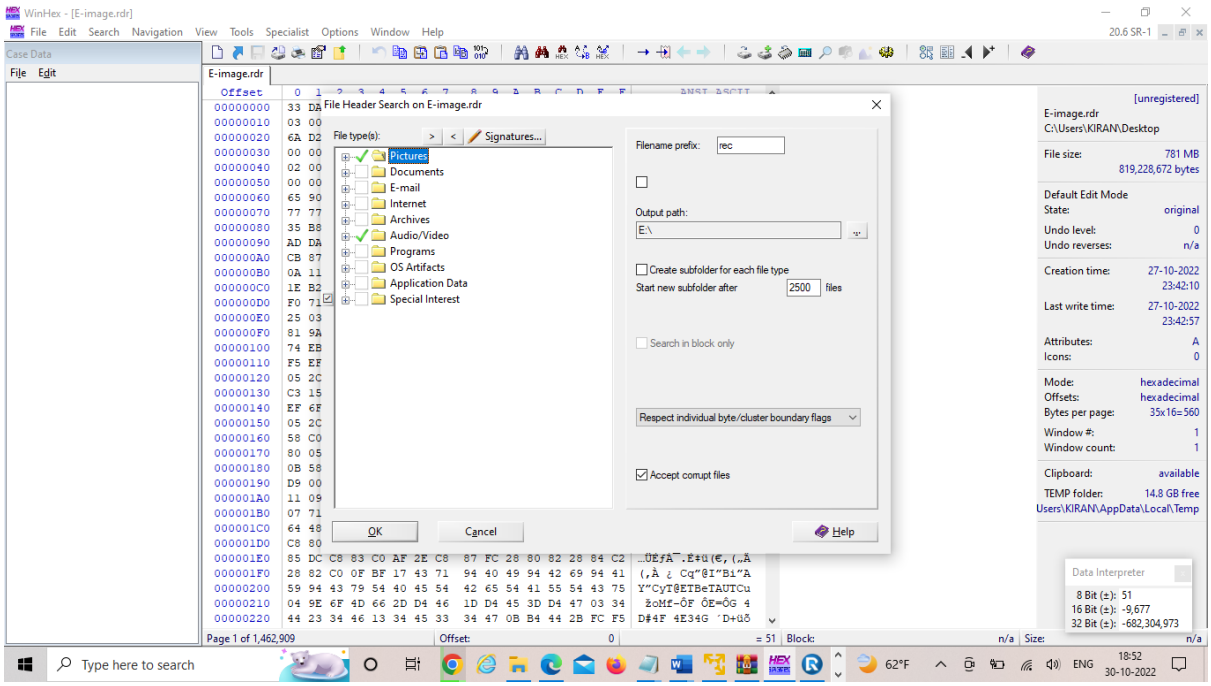
We can view the disk image data hexadecimal

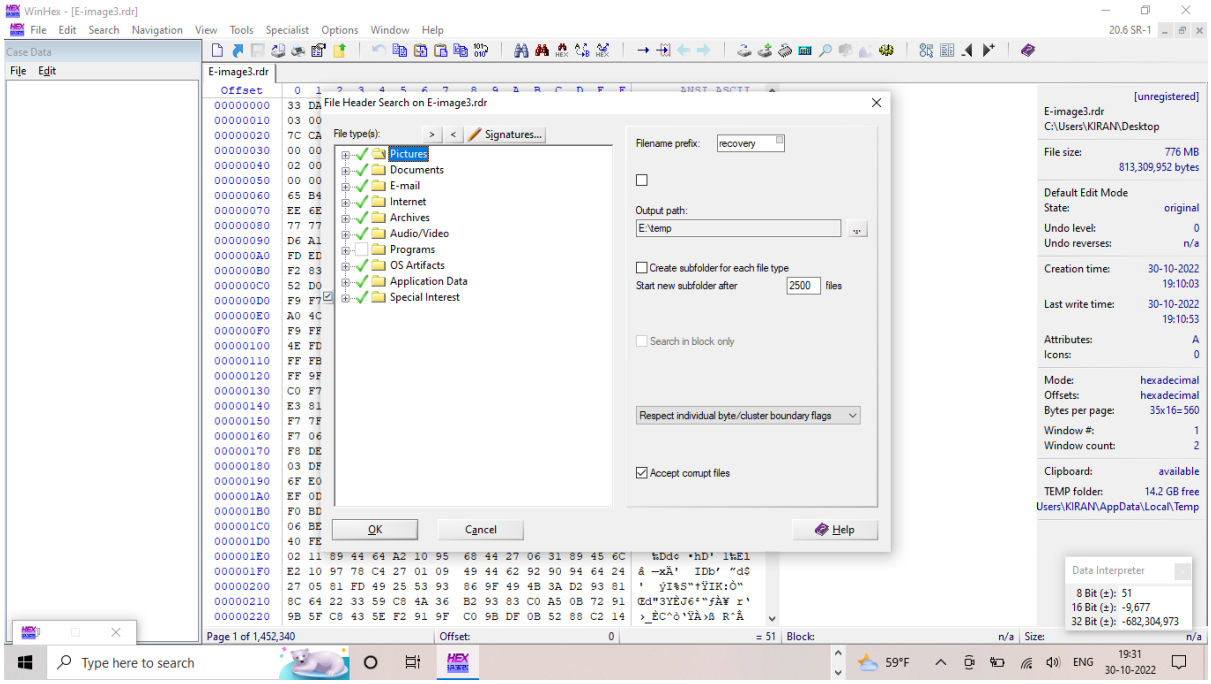


Step 5: We can select the type of the data to be recovered using the disk image

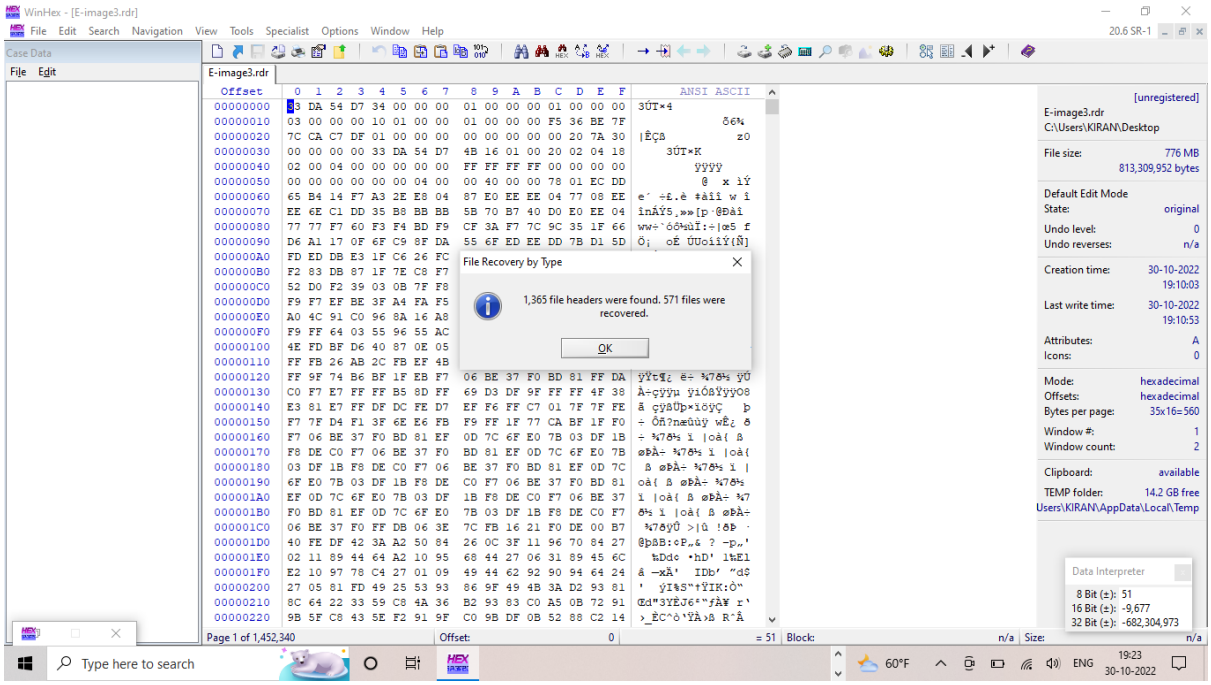


Step 6: Here we are selecting the type pictures to be recovered after permanently deleting the files from the drive



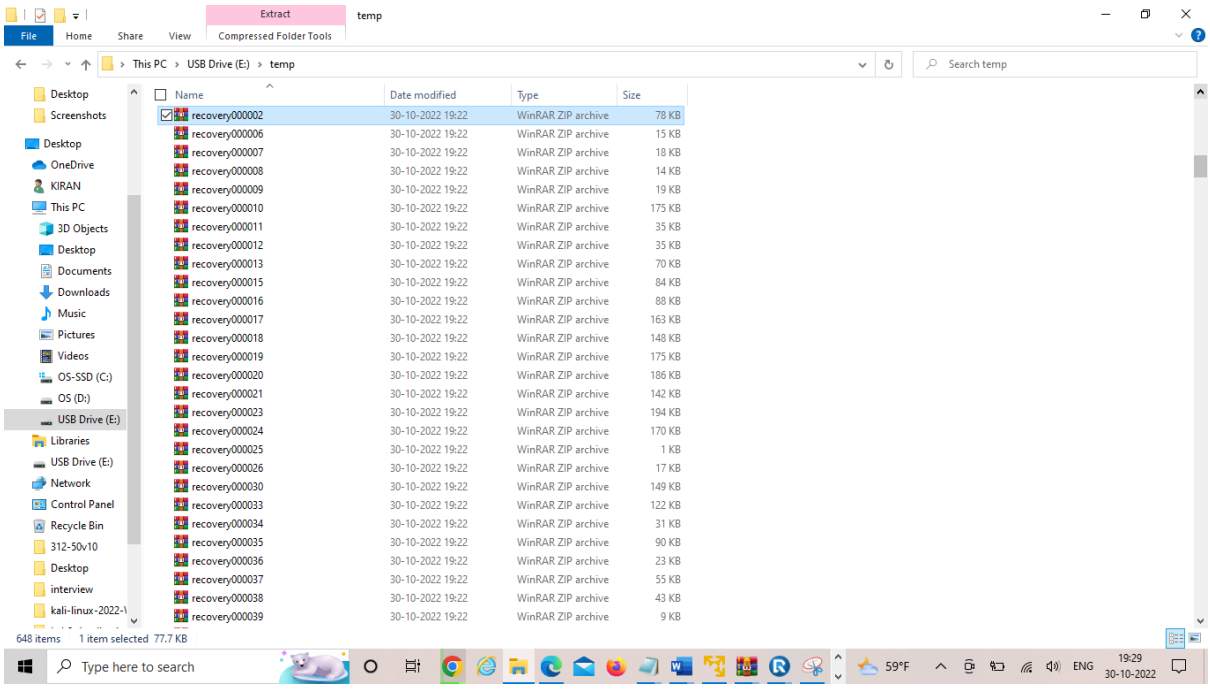


Step 7: The picture type files are recovered using Disk image

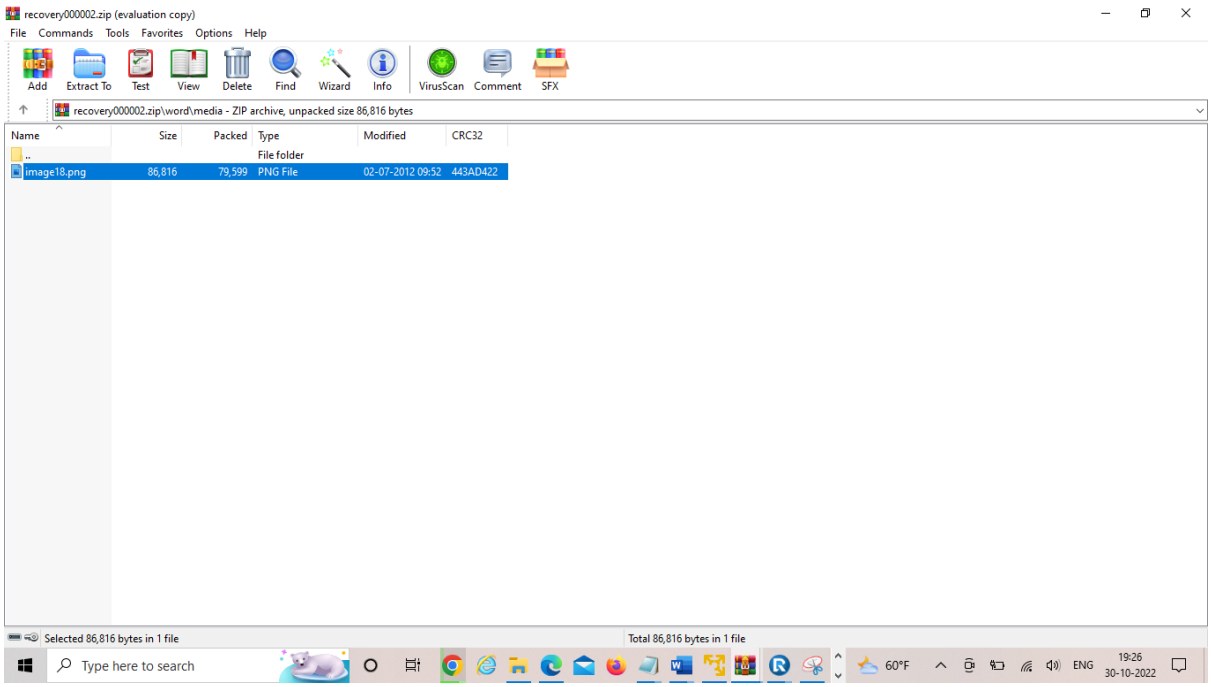


Step 8:

The recovered pictures from winhex tool in PC



The recovered file will come in the form of zip, where we need to extract from the zip folder



3rd Deliverable: (November)

Forensic Toolkit (FTK) computer forensics software that can be used to acquire, preserve, analyze, and present computer evidence. FTK presents computer evidence by creating a case report and case log to document the evidence and investigation results. This uses the Report Wizard to create and modify reports. In the report, you can add bookmarks, customize graphics references, select file listings, and include supplementary files and the case log. The report is generated in HTML.

Forensic Toolkit (FTK) is a complete platform for digital investigations, developed to assist the work of professionals working in the information security, technology, and law enforcement sectors.

Through innovative technologies used in filters and the indexing engine, the relevant evidence of investigation cases can be quickly accessed, dramatically reducing the time to perform the analysis

Forensic digital investigations include the following processes:

1.Preparation
2.Acquisition and preservation
3.Analysis
4.Reports and presentation

provide support for the correct installation, as can be seen in the following screenshot:

Perform the following steps for installing FTK:

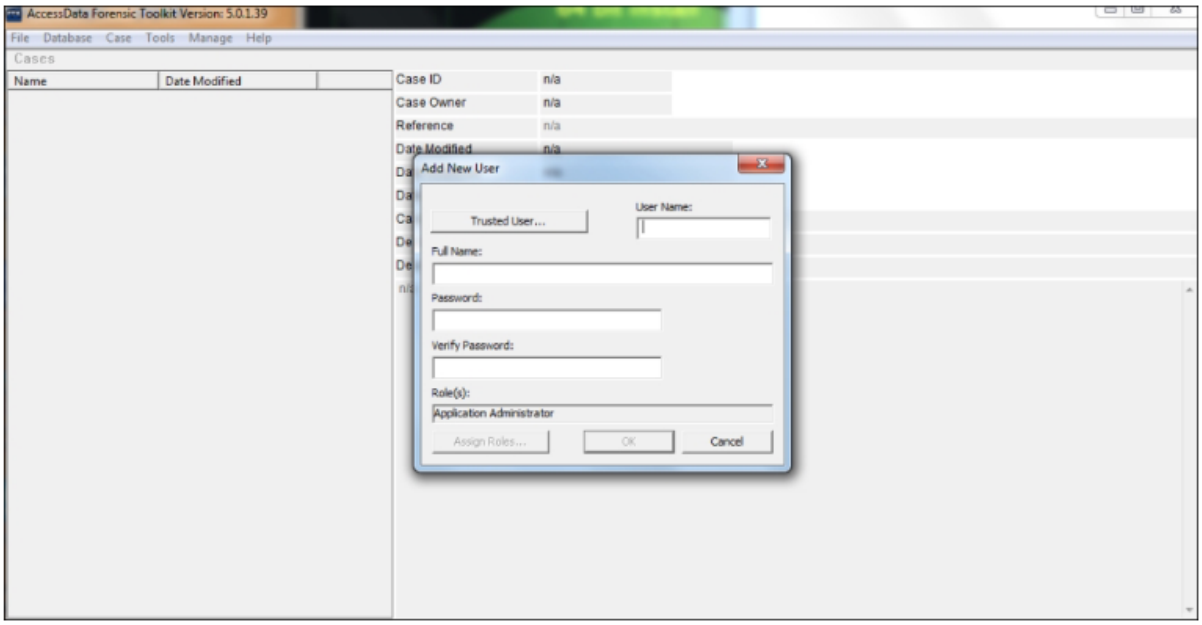
1. Start the installation process by using the Database component. You can then enter a password to create the PostgreSQL database admin user.
2. Once the database installation is done, install FTK.
3. Install the Distributed Engine component, as it is necessary for the correct operation of FTK.
4. The View User Guide installation is optional, but high recommended.
5. To finish the FTK platform installation process, click on the Other Products button and select the components listed as follows:

License Manager: This is the product's license control component.
Registry Viewer: This is the Windows registry analysis component.
PRTK: This is the password recovery component.
Code Meter: This is the USB Code Meter hardware driver and management component.
Imager: This is the FTK Imager product.

Tip:

Make sure that you select the correct platform, which can be either 32- or 64-bits, and in case the Unable to connect to the database requested error message appears, just change the RDBMS option to Postgres SQL.

Running FTK for the first time



If the installation has been done correctly, the first step would be to create a user:

Next, you can complete the fields in the form and then click on OK to create the first user. This user will be the application administrator.

Data storage media:

It is important to realize that data acquisition may be performed not only on hard disks, but also across other devices that have the storage capacity, few of which are listed as follows:

Magnetic media:

1. Floppy disks
2. Hard drives
3. USB/PC cards
4. ZIP and tape drives

Optical media:

1. CDs
2. CD-Rs and CD-RWs
3. DVDs
4. Alternative media:
5. MP3 players
6. Tablets
7. Smartphones
8. Video games, TVs, and so on

FTK Imager has the ability to collect and analyze each of these devices.

During an investigative process, we must look at these items because they may have relevant evidence, not often found in hard disks.

Overview of Access Data FTK:

Forensic Toolkit (FTK) computer forensics software that can be used to acquire, preserve, analyze, and present computer evidence. FTK presents computer evidence by creating a case report and case log to document the evidence and investigation results. This uses the Report Wizard to create and modify reports. In the report, you can add bookmarks, customize graphics references, select file listings, and include supplementary files and the case log. The report is generated in HTML

You can use FTK Imager to preview a piece of evidence prior to

creating the image file(s). You can then choose to image the entire

evidence object or choose specific items by selecting Add to

Custom Content (AD1) image.

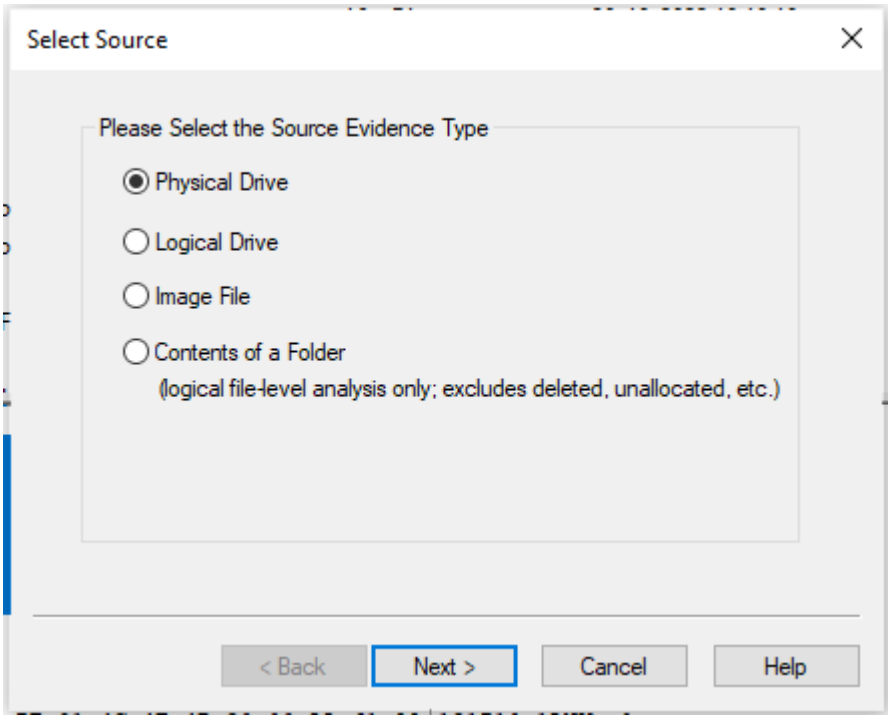
Adding and previewing an evidence Item

You can either add a single evidence item or several items at one time. The following screenshot shows the procedure in a step-by-step format:

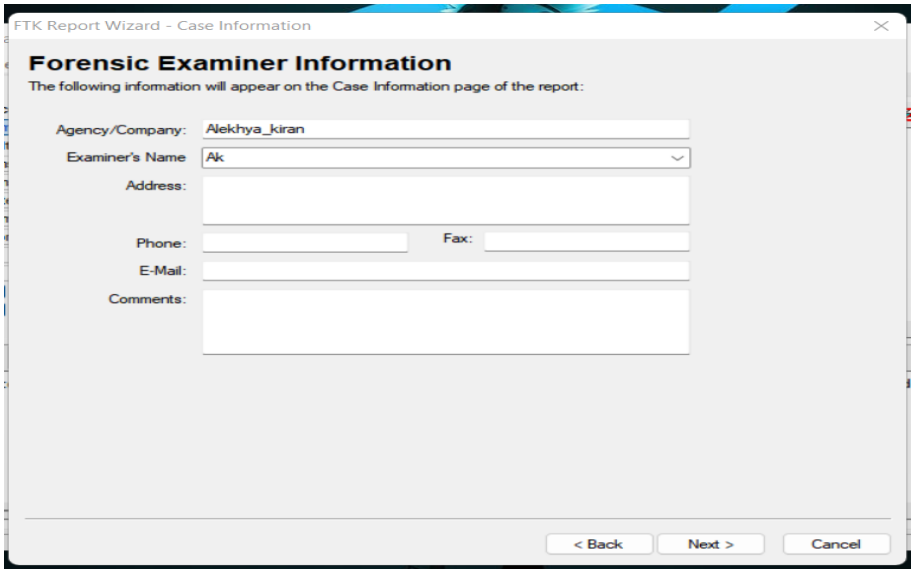
1. Click on the Add Evidence Item button on the toolbar.

2. Select the source type you want to preview and then click on

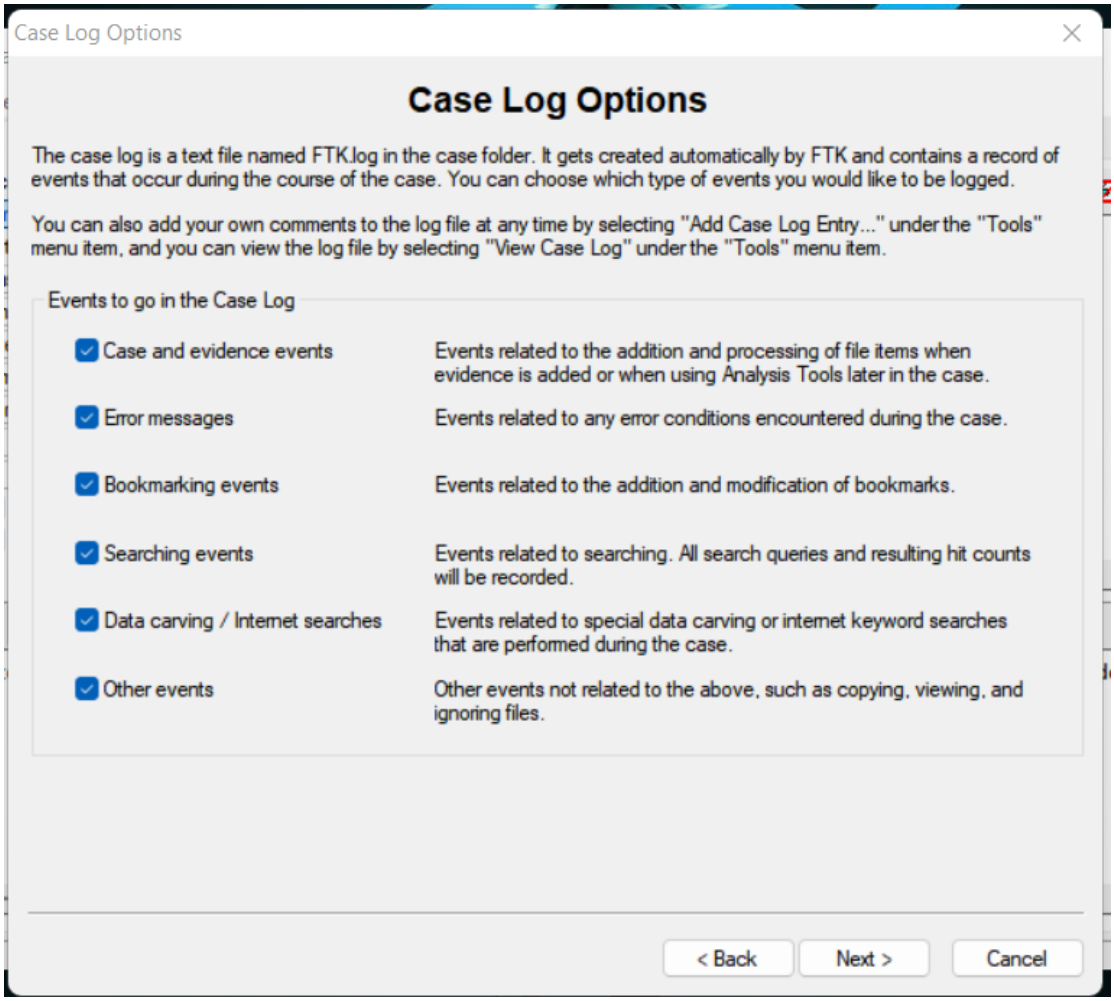
Next.

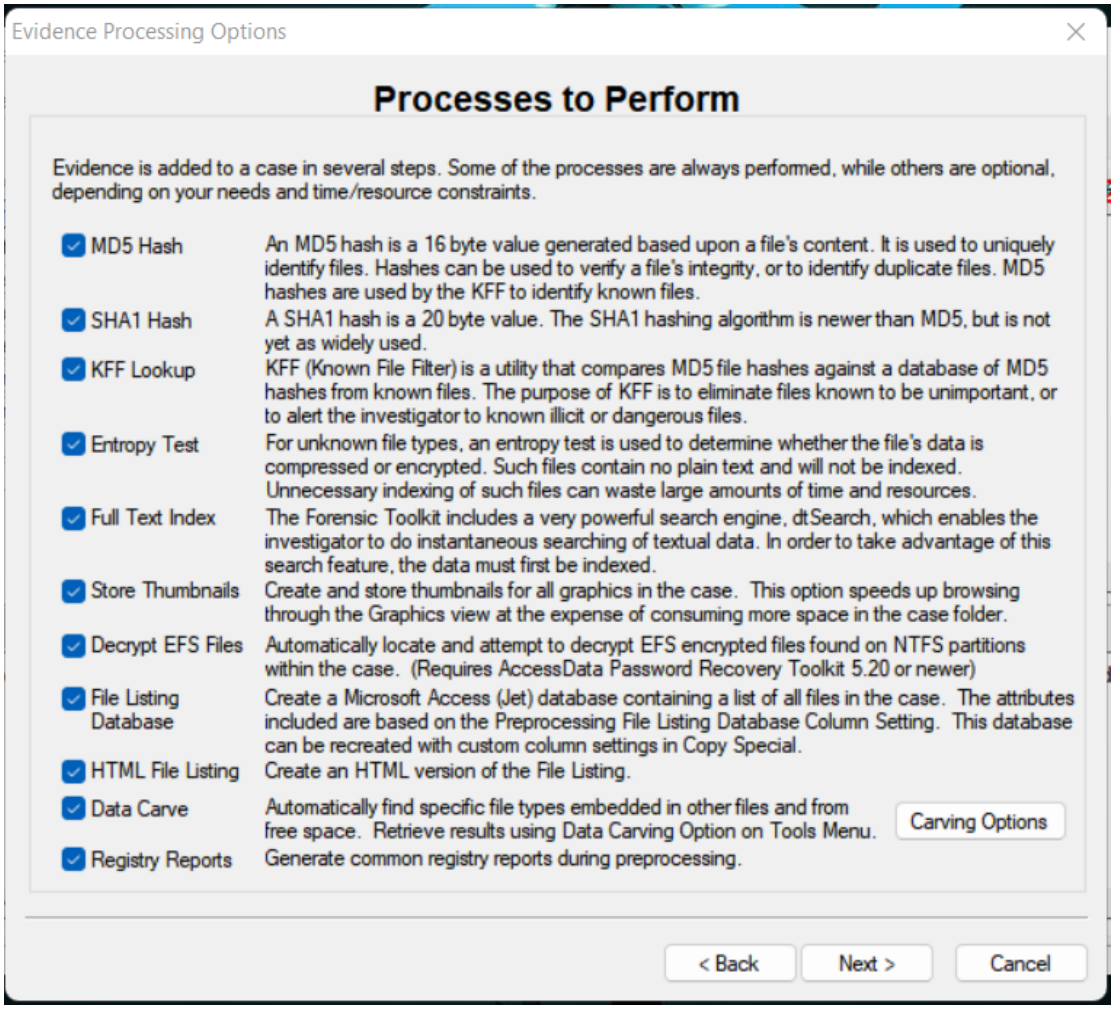


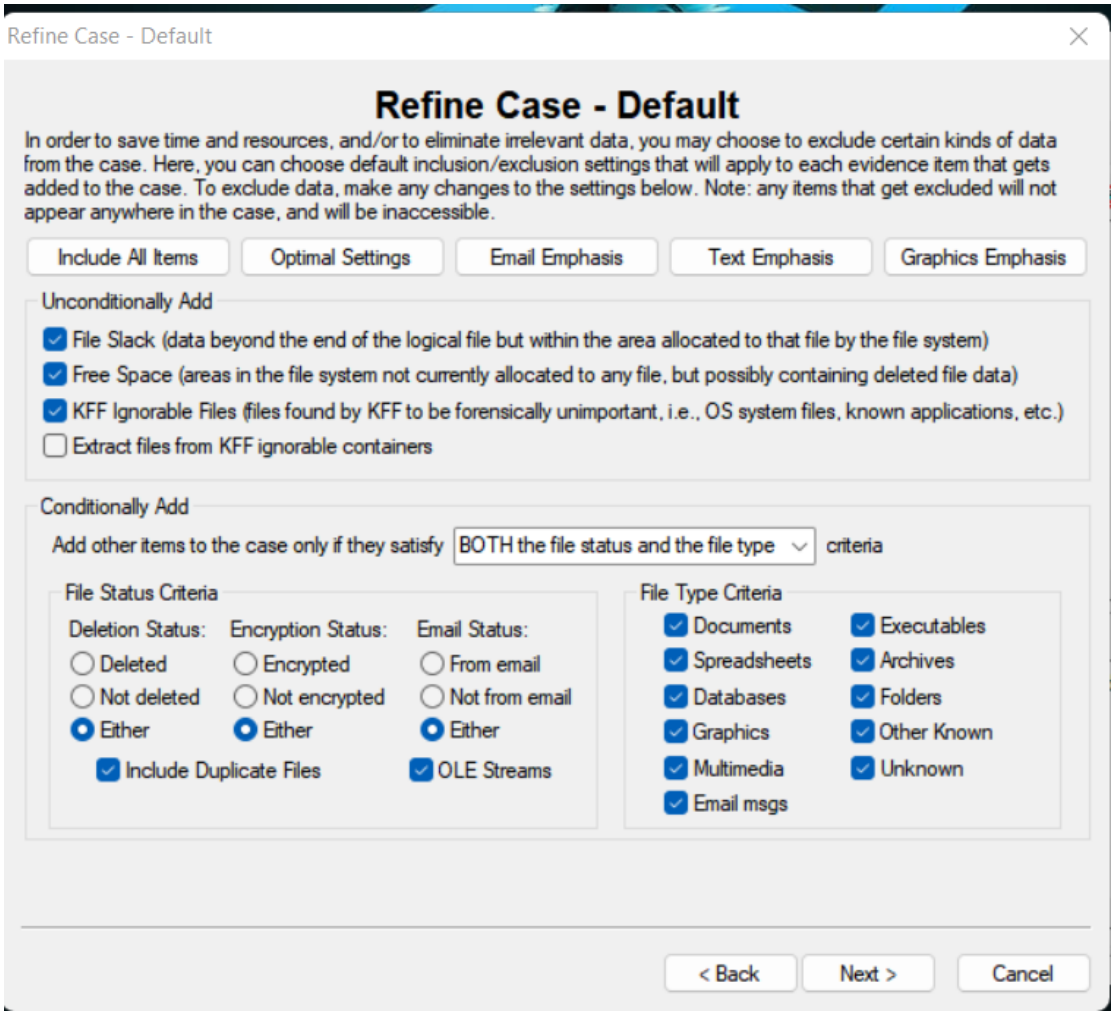
Creating New Case By giving Information of Investigator :

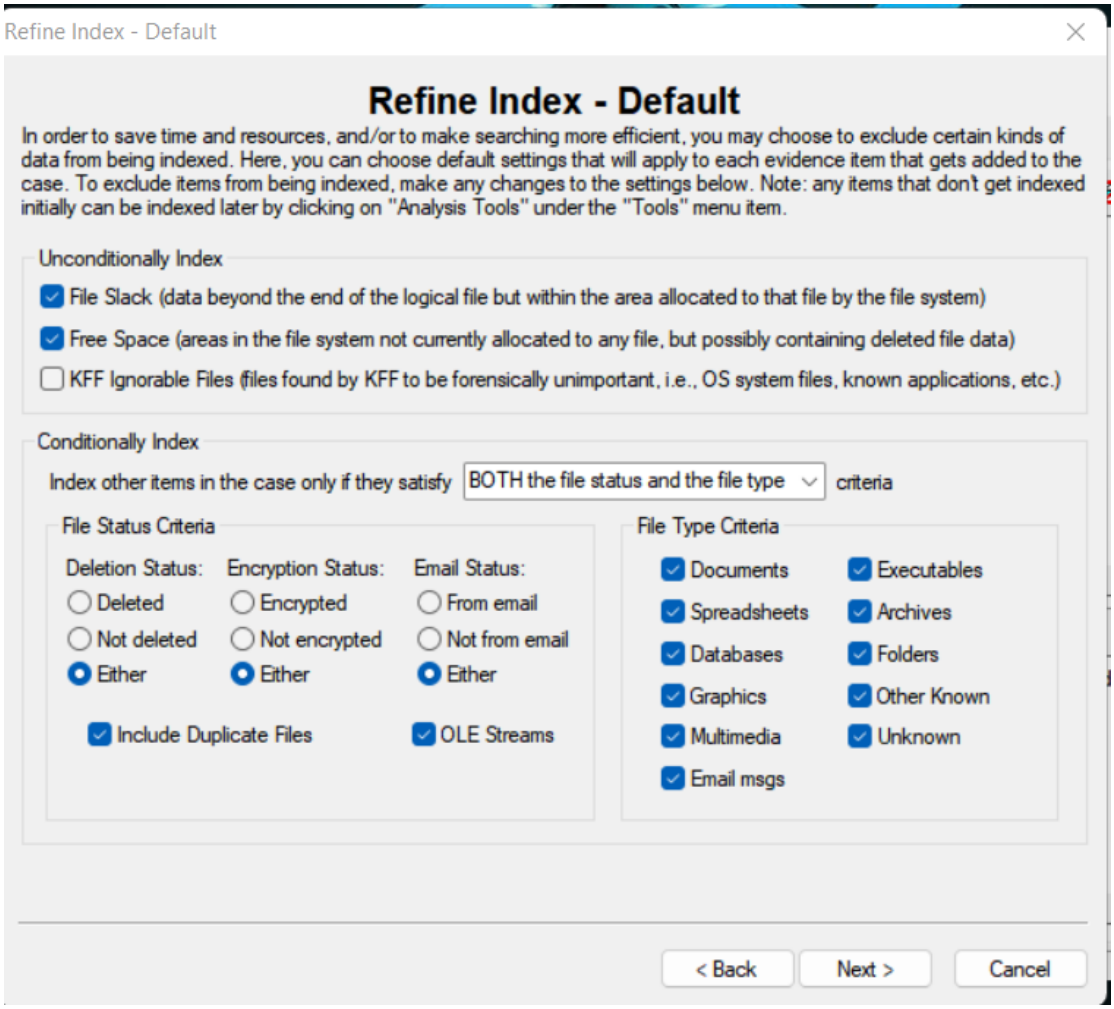


Selecting different case logs option for examining a case:


Case Log Options
Case Log Options
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.
Events to go in the Case Log
Case and evidence events
Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Error messages
Events related to any error conditions encountered during the case.
Bookmarking events
Events related to the addition and modification of bookmarks.
Searching events
Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches
Events related to special data carving or internet keyword searches that are performed during the case.
Other events
Other events not related to the above, such as copying, viewing, and ignoring files.
< Back
Next >
Cancel


Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel


Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy
BOTH the file status and the file type
criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel



ADD EVIDENCE:

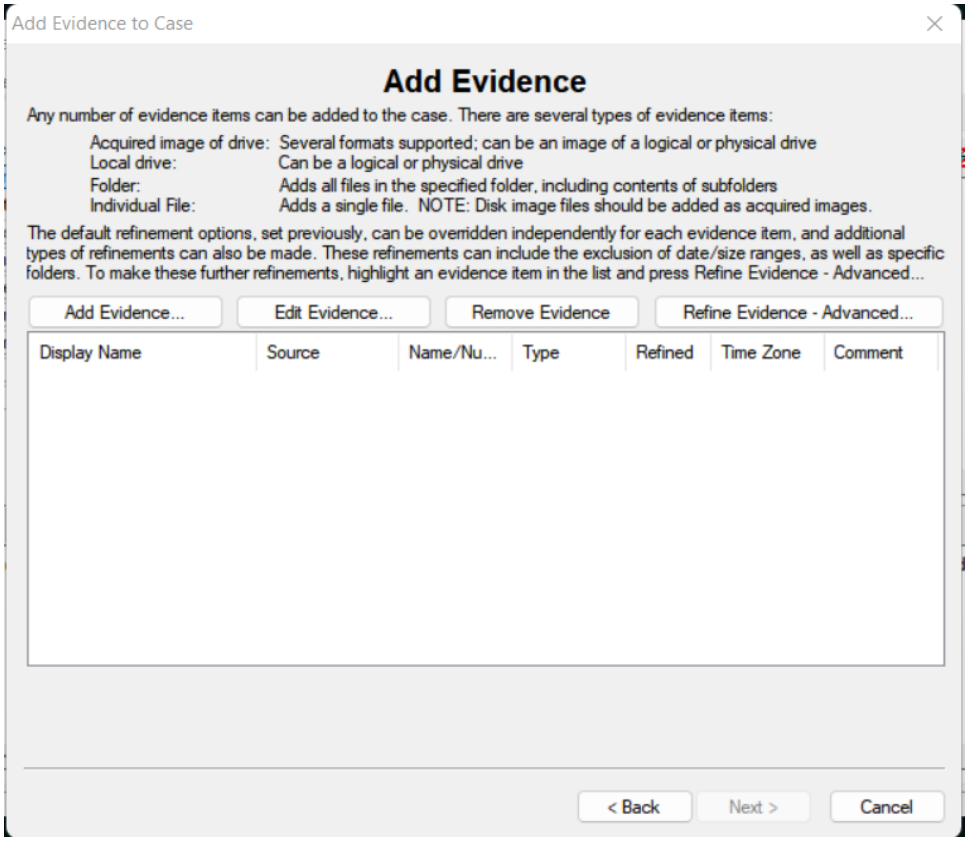
BY SELECTING OPTIONS LIKE :

1.ACQUIRED IMAGE OF DRIVE.

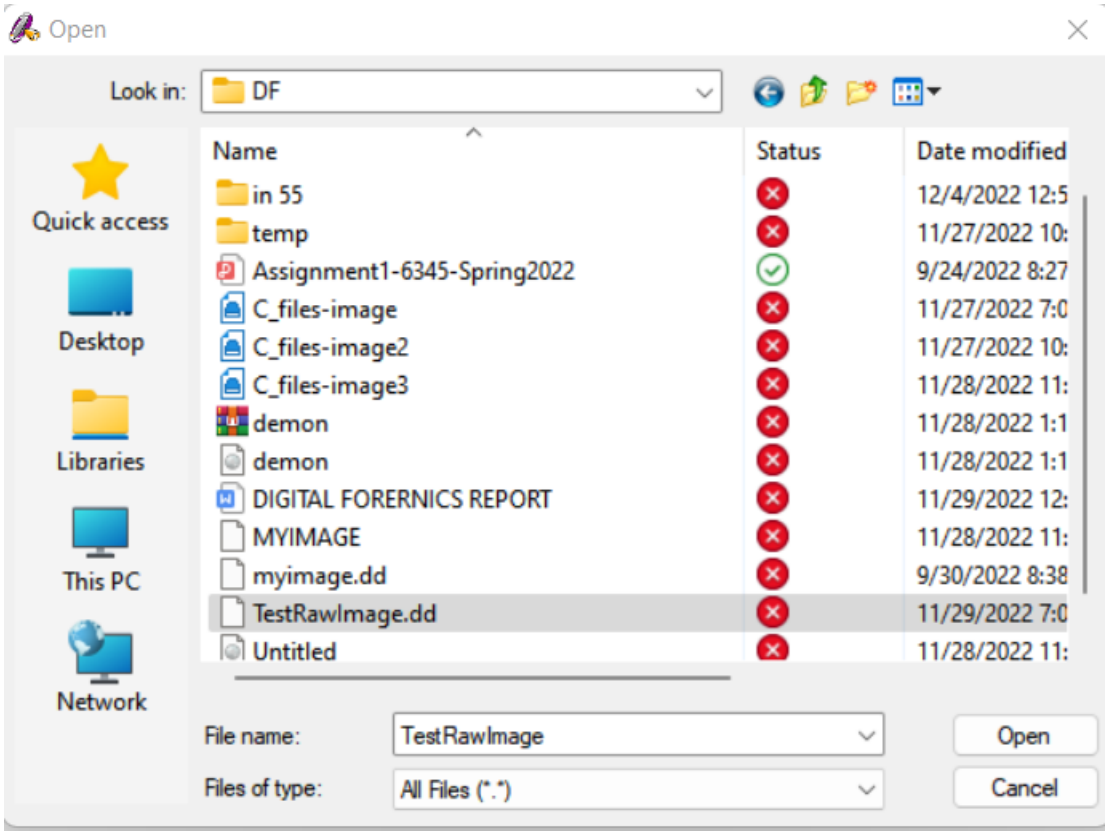
2.LOCAL DRIVE.

3.CONTENTIAL OF A FOLDER

4.INDIVIDUAL FILE

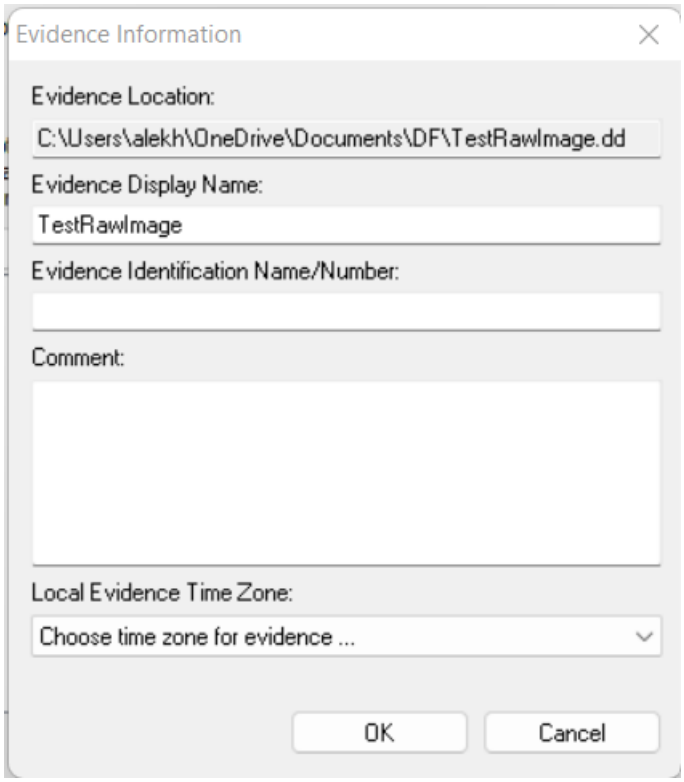


SELECTING FILE (myimage.dd):

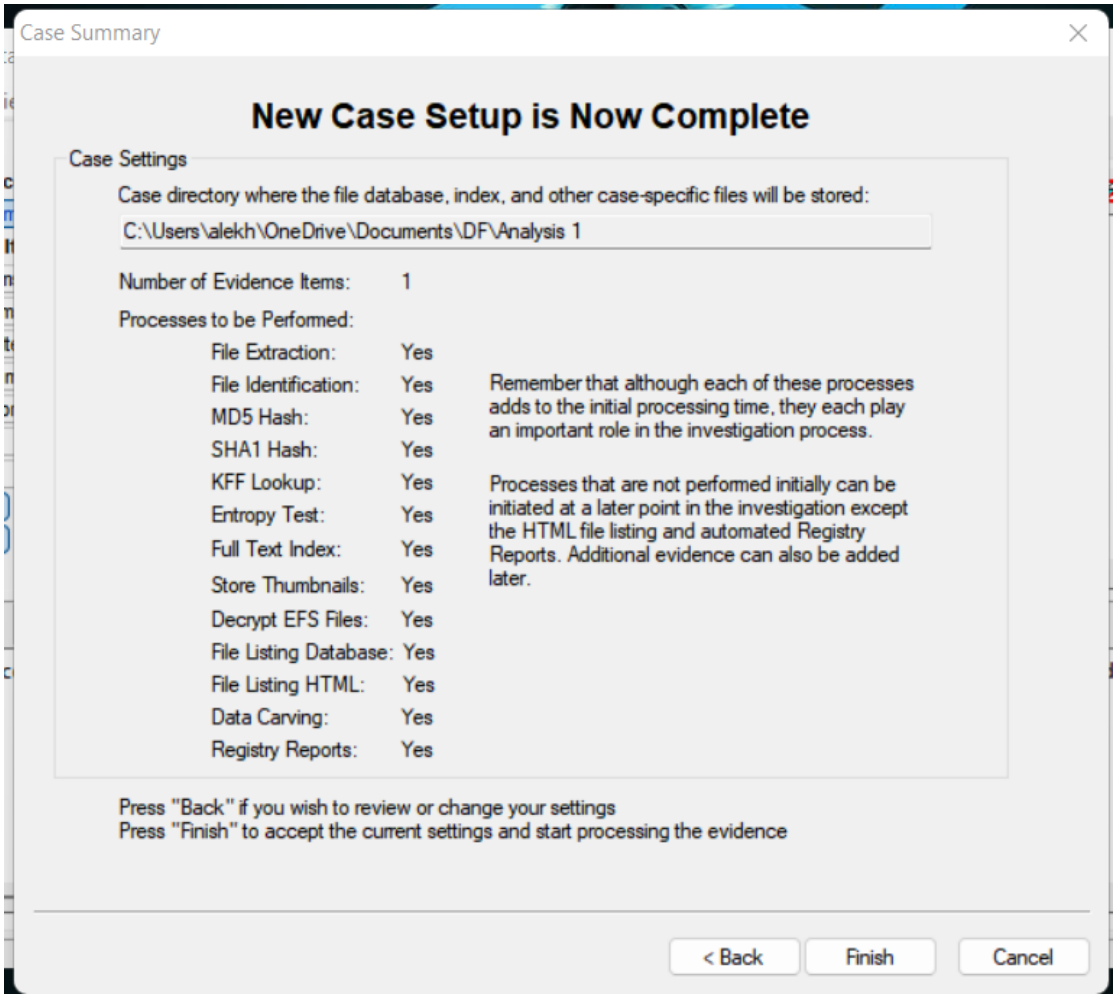


CAN ADD LOCAL EVIDENCE TIME ZONE:

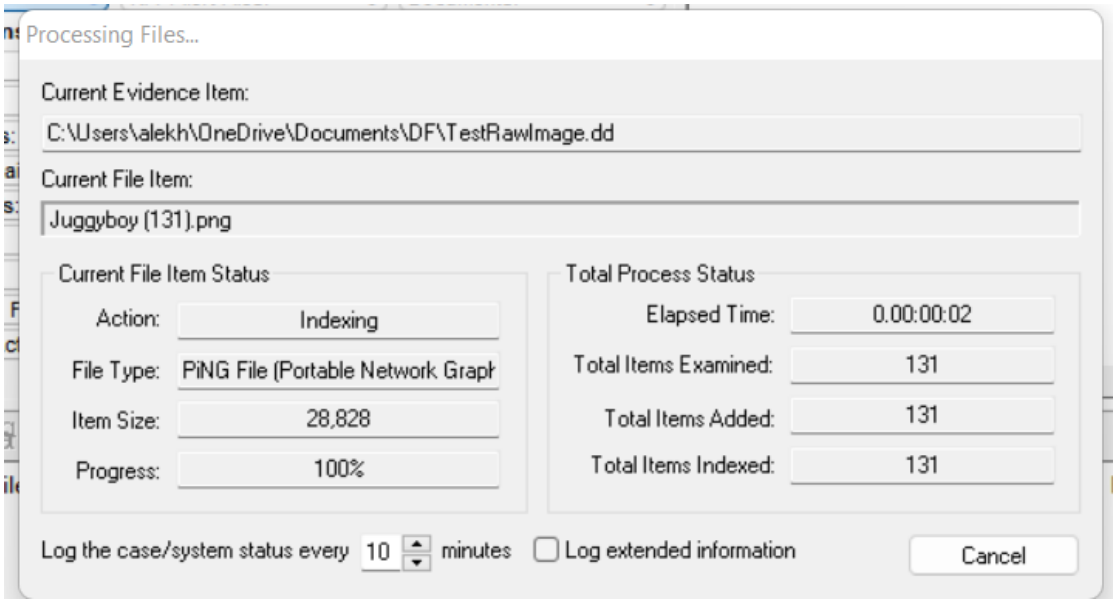
The correct use of the Time Zone feature is of the utmost importance for computer forensics because it might reflect the wrong
MAC time of files contained in the evidence, making a professional use the wrong information in an investigation report.
Based on this, you must configure the time zone to reflect the location where the evidence was acquired. For example, if you conducted the acquisition of a computer that was located in Los Angeles, US, and bring the evidence to Sao Paulo, Brazil, where your lab is situated, you should adjust the time zone to Los Angeles
so that the MAC time of files can reflect the actual moment of its modification, alteration, or creation.
The FTK allows you to make that time zone change at the same time that you add a newevidence to the case. Select the time zone of the evidence where it was seized from the drop-down list in the Time Zone field. This is required to add evidence in the case.



NEW CASE SETUP IS NOW COMPLETED:



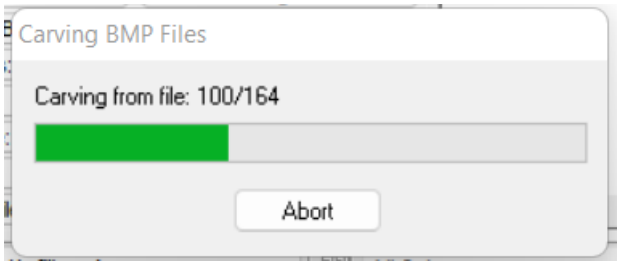
ANALYZE ALL THE FILES IN THE TestRawImage.dd

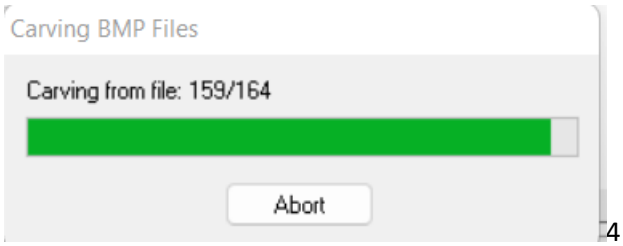


DATA CRAVING:

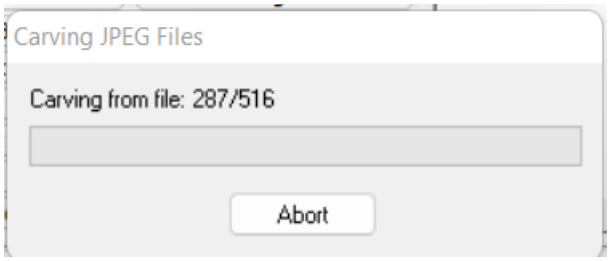
Data carving is the process of searching for data in destroyed disk evidence. To accomplish this, identify the file.

primarily unallocated clusters for headers and footers. When adding evidence to a case, the FTK offers a number of predetermined carvers from which you can choose. To satisfy your precise requirements, you can even design your own unique carvings.

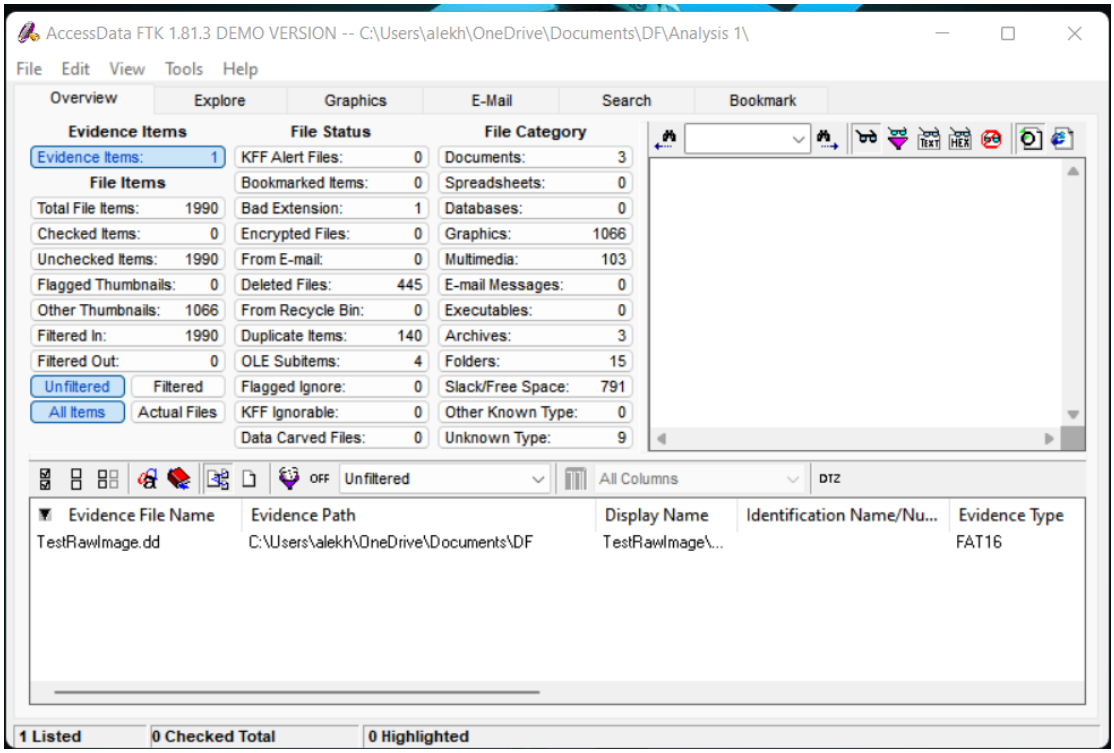


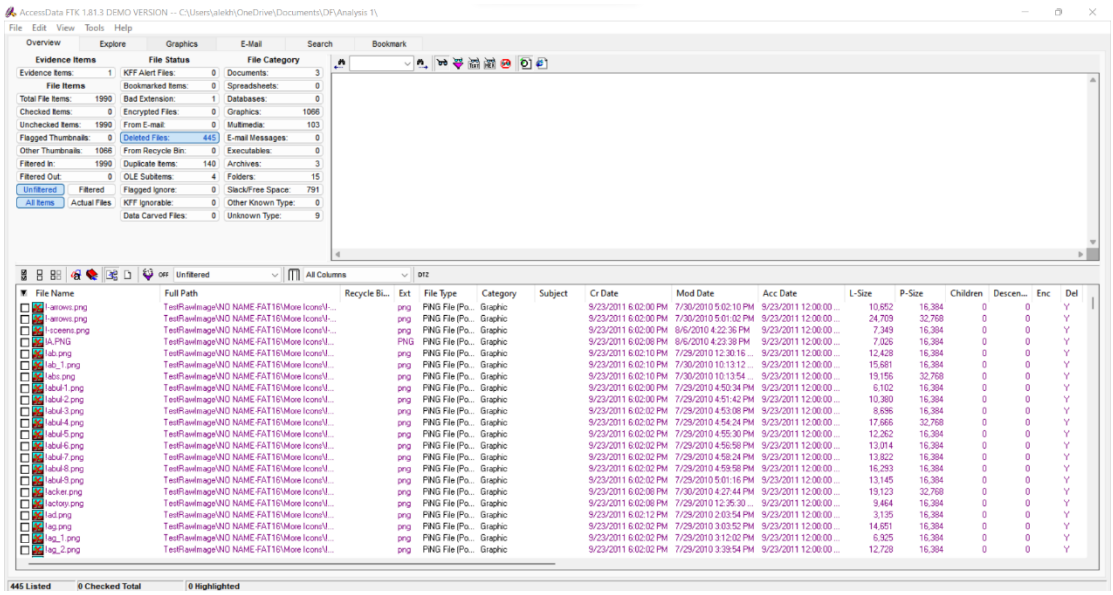


4

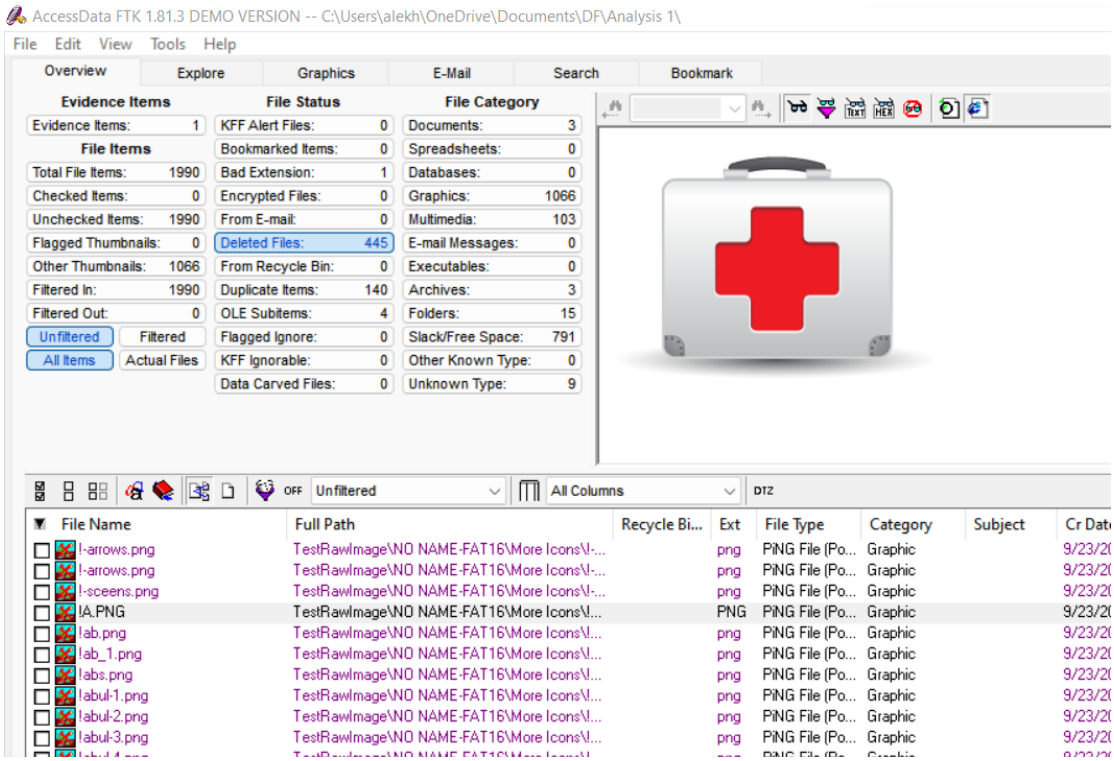


After analysis you can see the number of deleted items and duplicate items in folder:

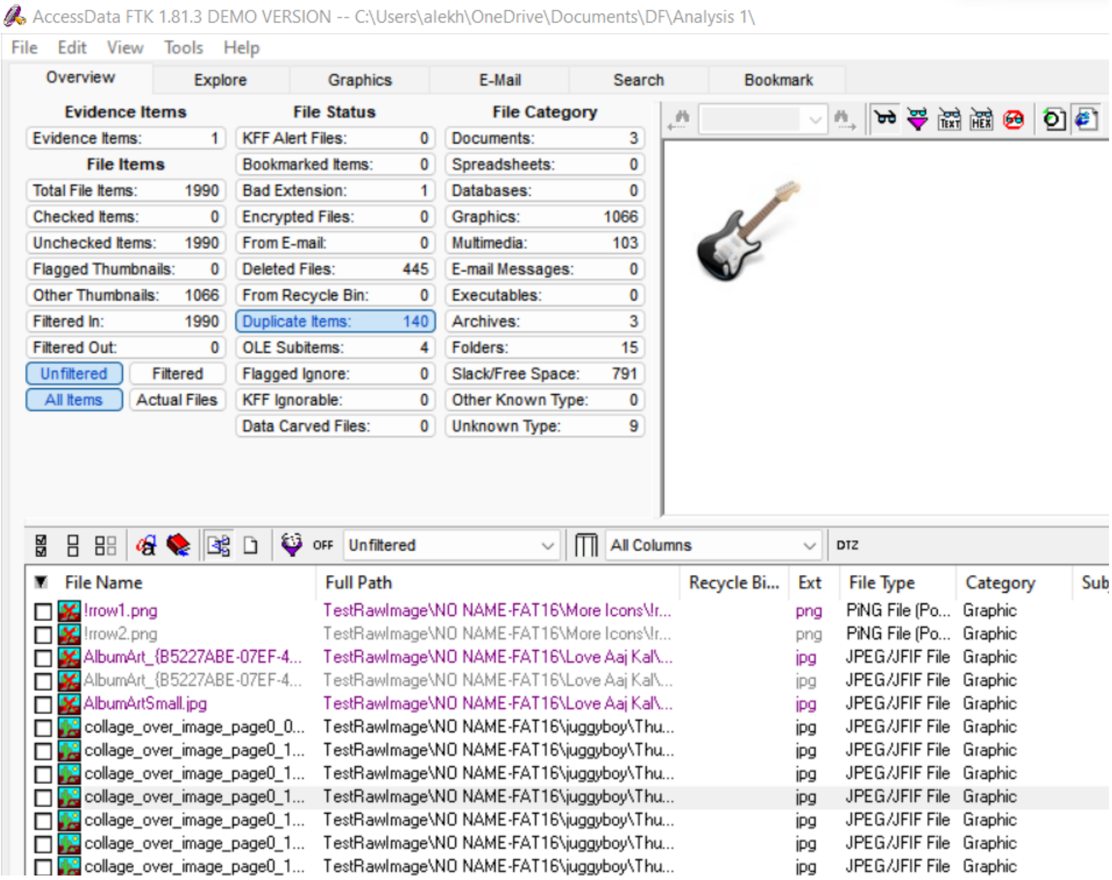




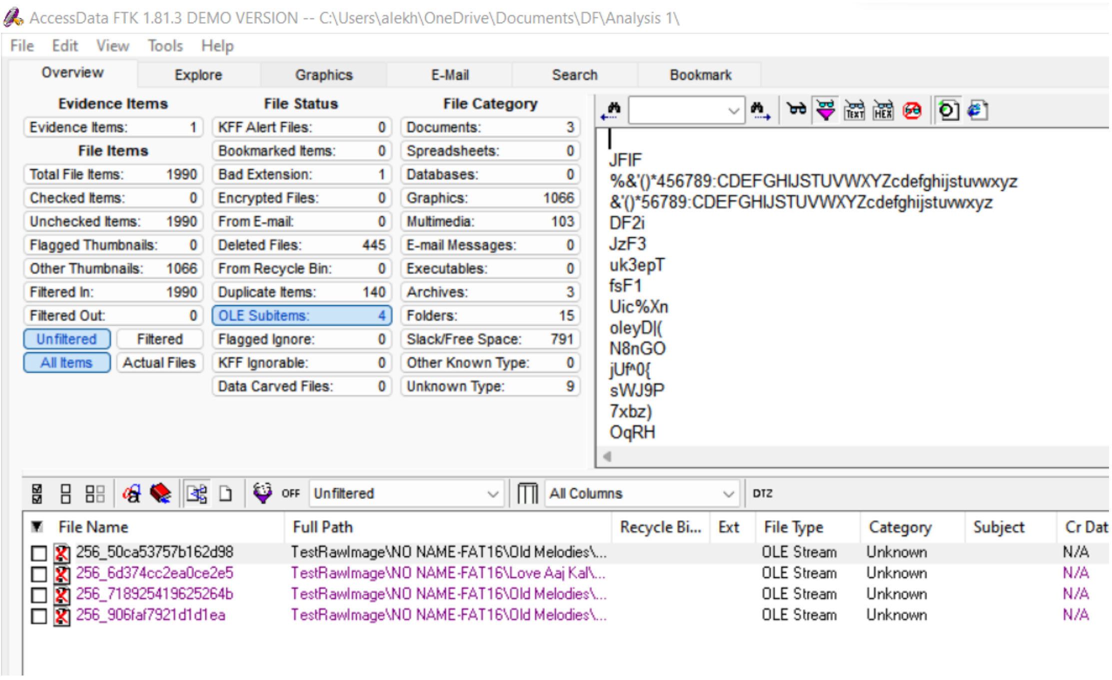
By selecting deleted file you can see preview of IA.PNG :



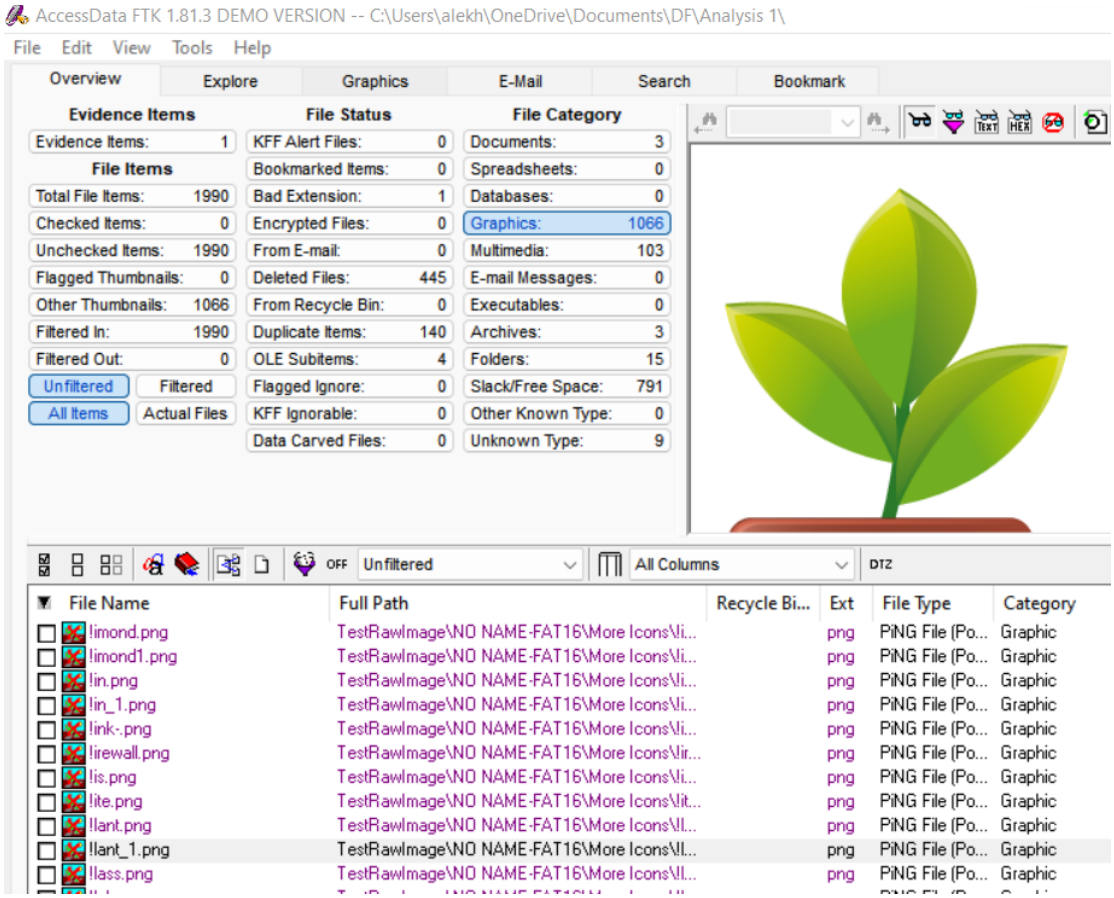
By selecting Duplicate items you can preview the filesby click on any file :

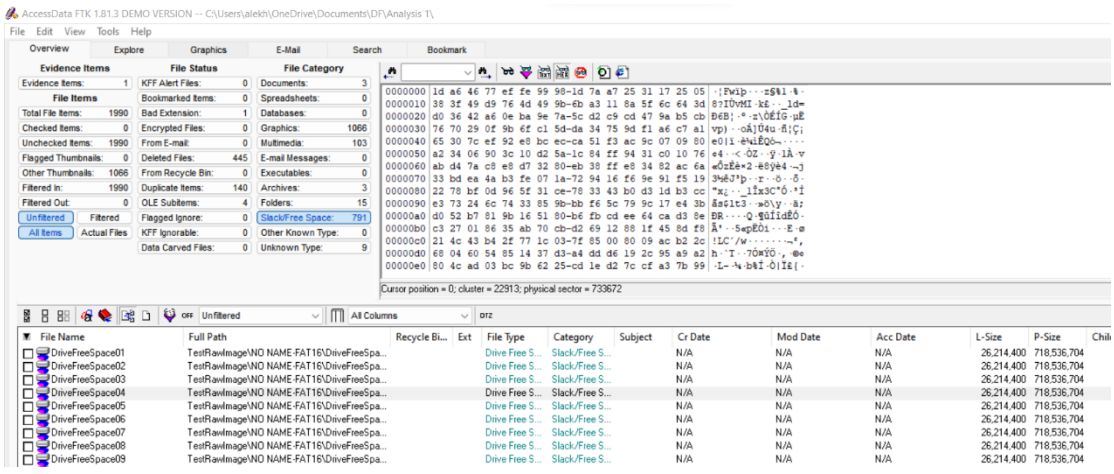


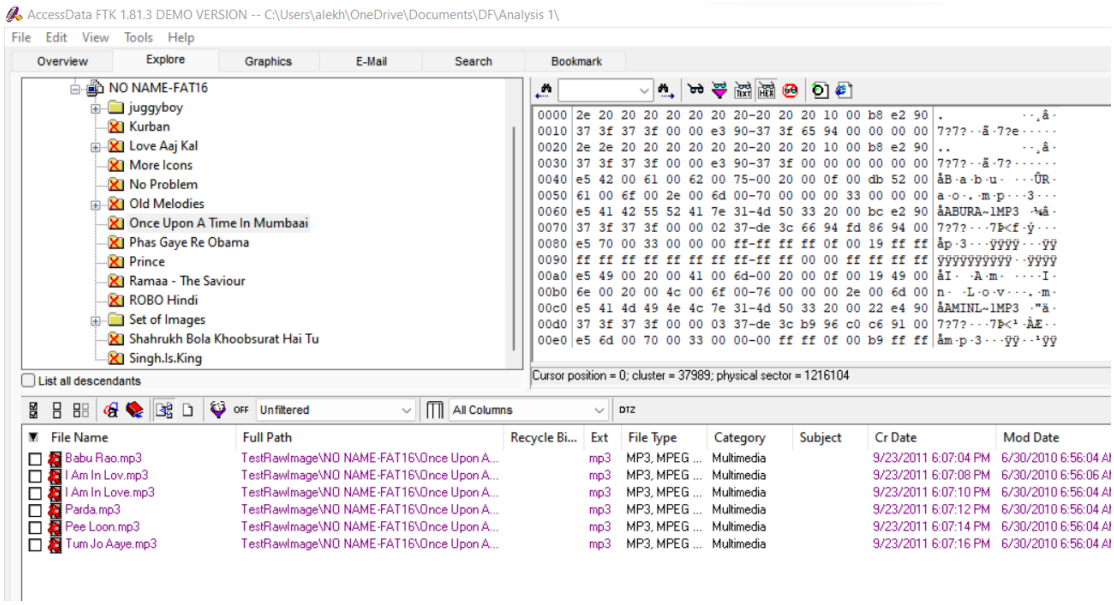
BY SELECTING OLE SUBTERMS U CAN PREVIEW ALL THE DATA PRESENT IN THE FILE:



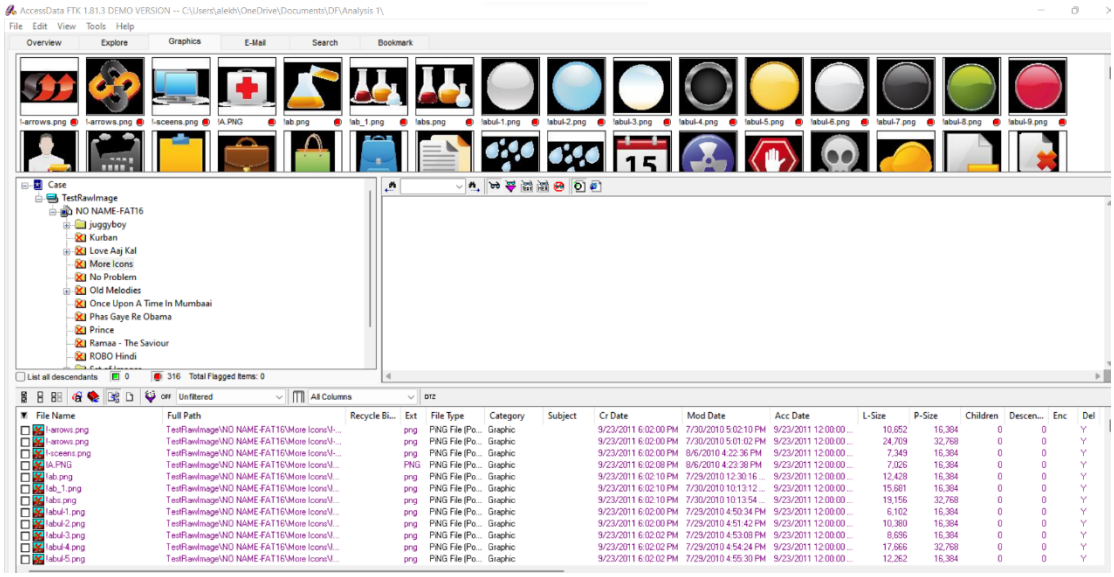
BY SELECTING GRAPHICS U CAN PREVIEW ALL THE FILES PRESENT IN GRAPHICS(1066):



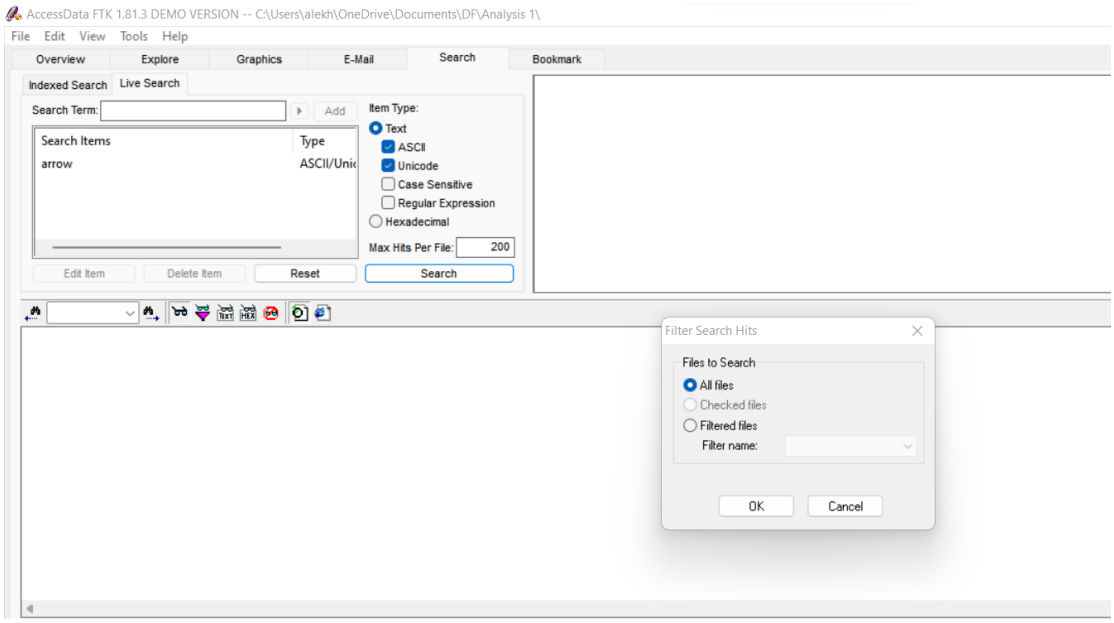




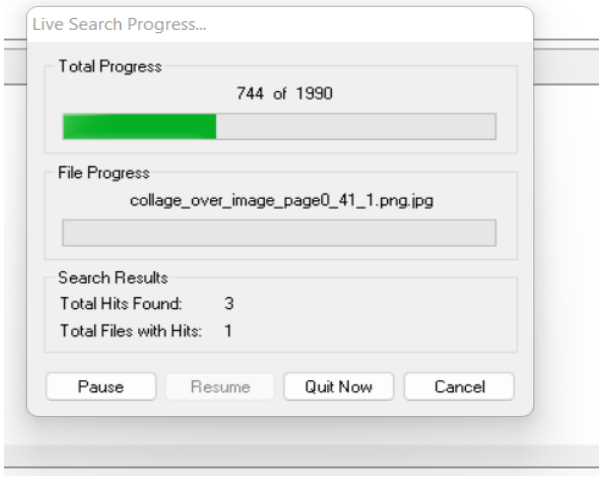
SET OF IMAGES ARE DISPLAYED IN GRAPHICS



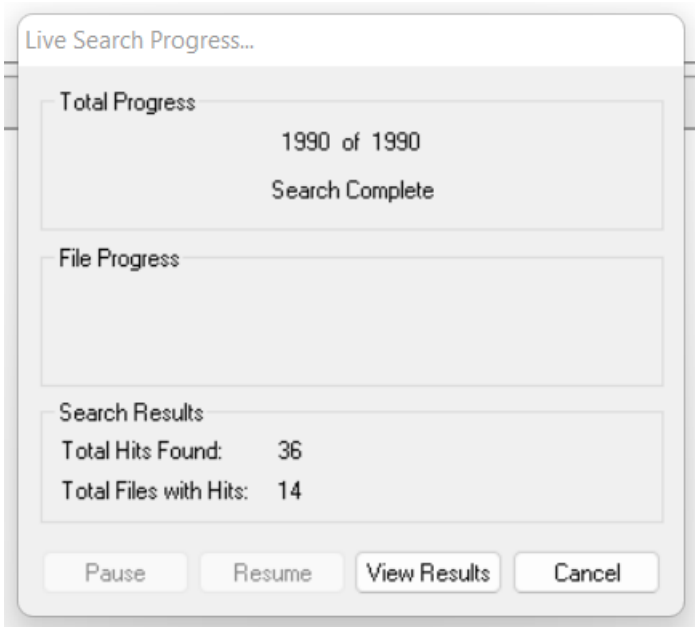
WE CAN SEARCH ITEMS BY WRITING SEARCH TERMS (WE CAN SELECT THE ITEM TYPE ALSO)



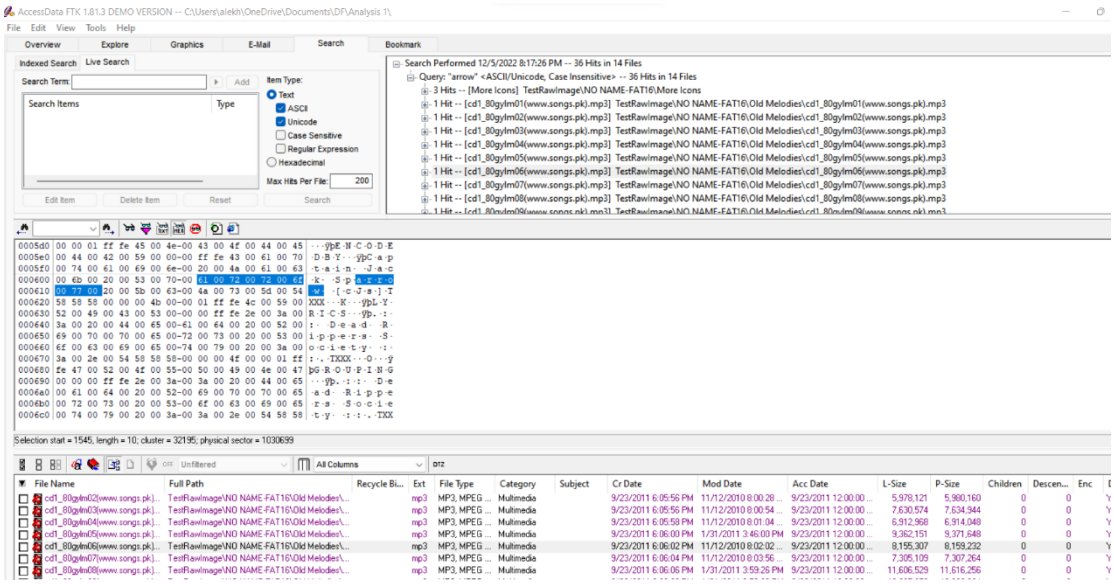
ANALYZING ALL THE FILES (FOR LIVE SEARCH PROGRESS)



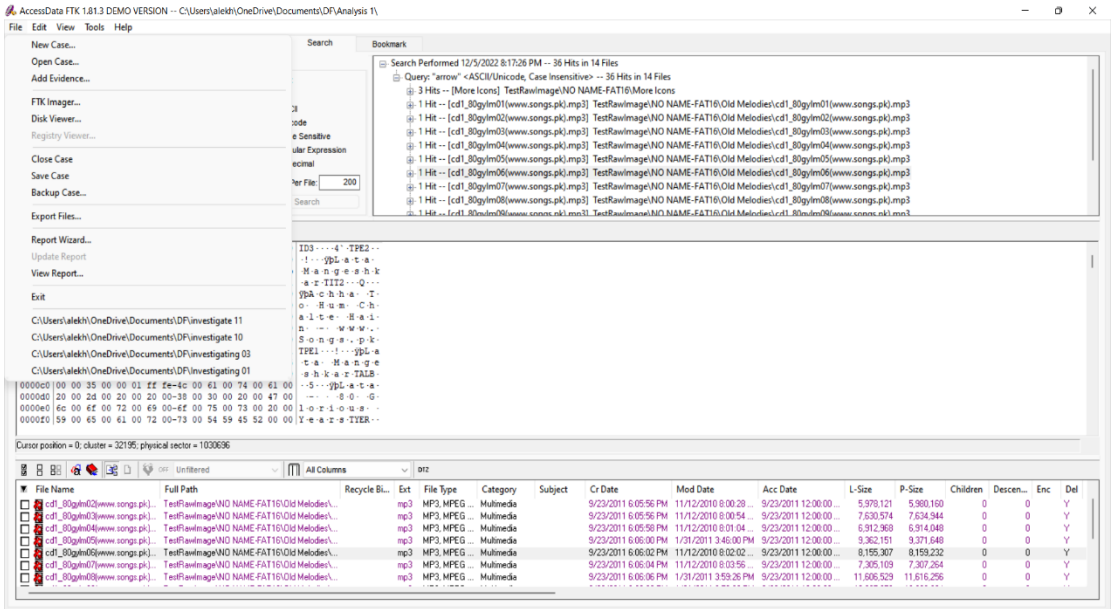
TOTAL COUNT OF THE FILES:



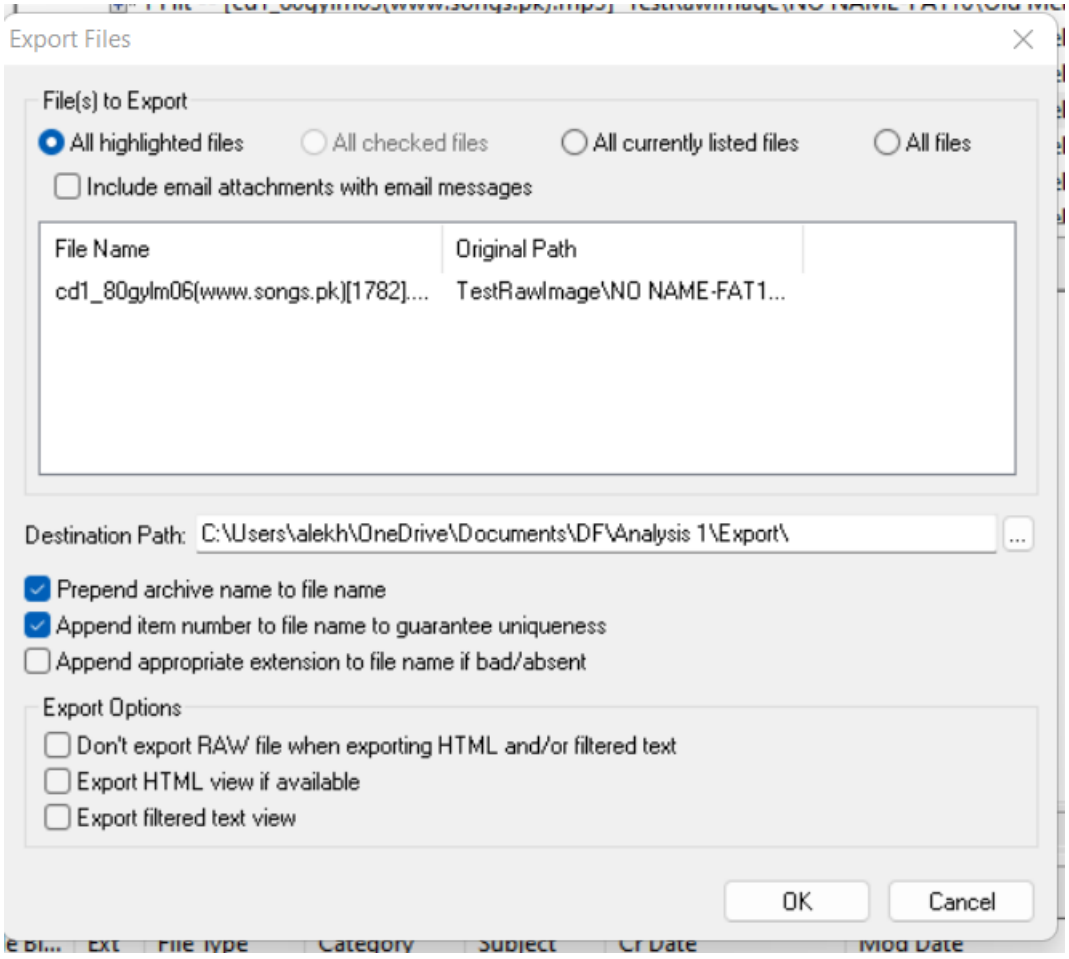
RESULTS FOR LIVE SEARCH :

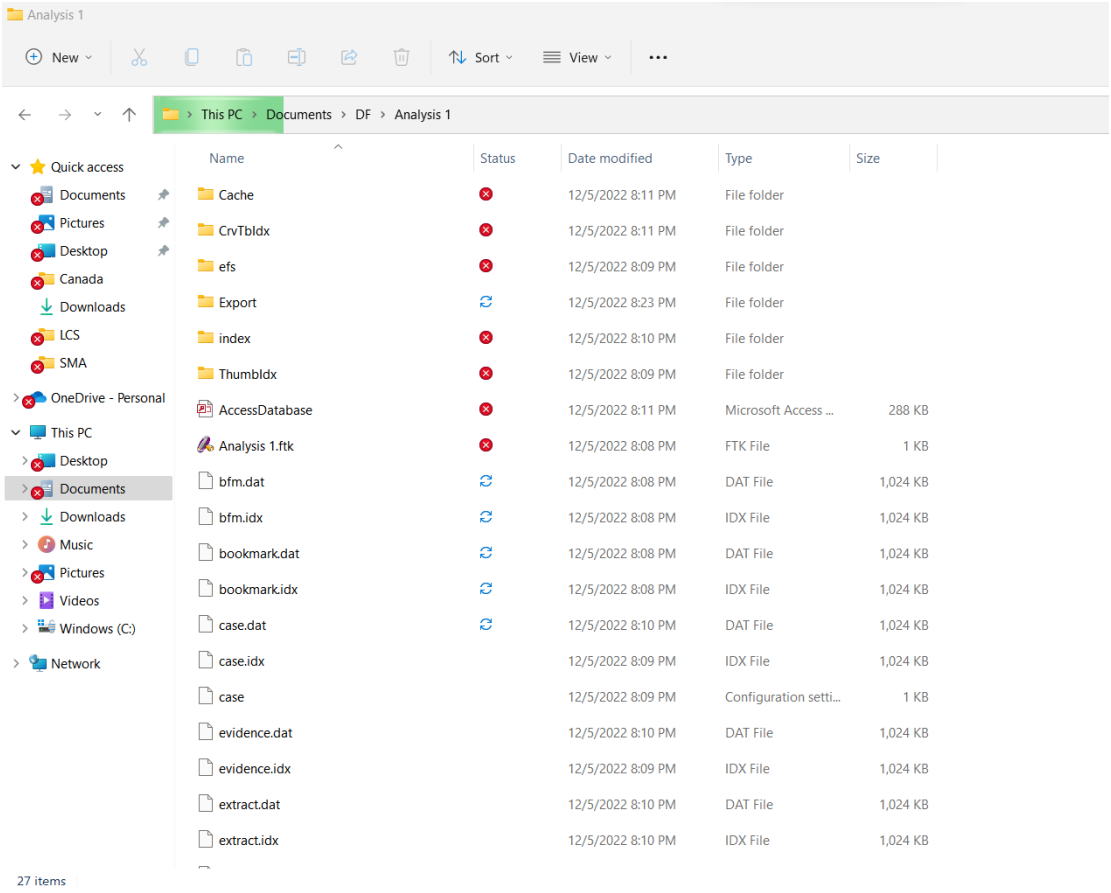


BY SELECTING EXPORT FILE OF SEARCH RESULT:



WE CAN SELECT THE OPTION (ALL HIGHLIGHTED FILES)

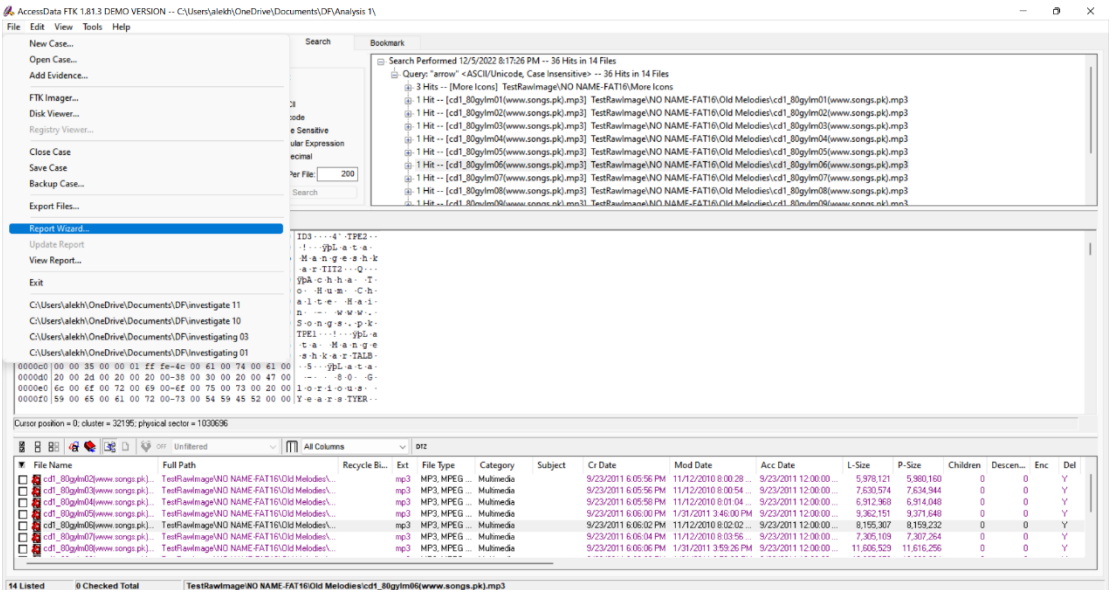


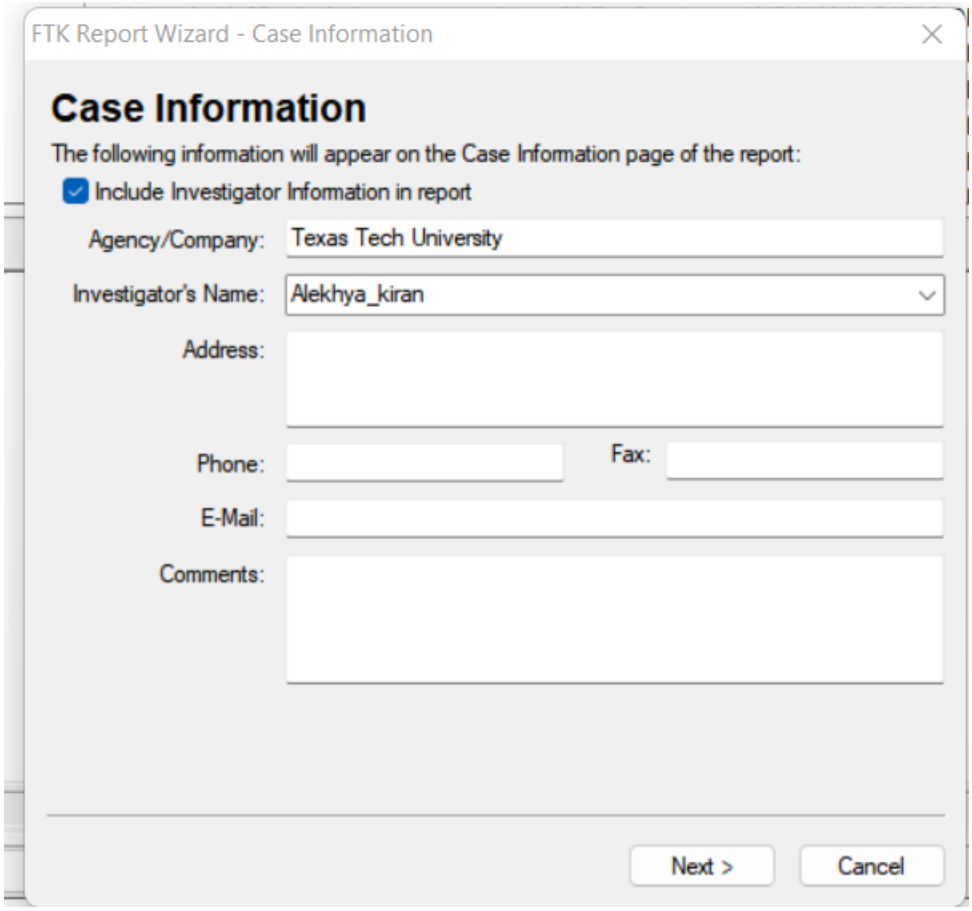


FOR REPORT WIZARD:

STEP TP STEP SNAPSHOTS ARE ATTACHED :

SELECTING REPORT WIZARD:





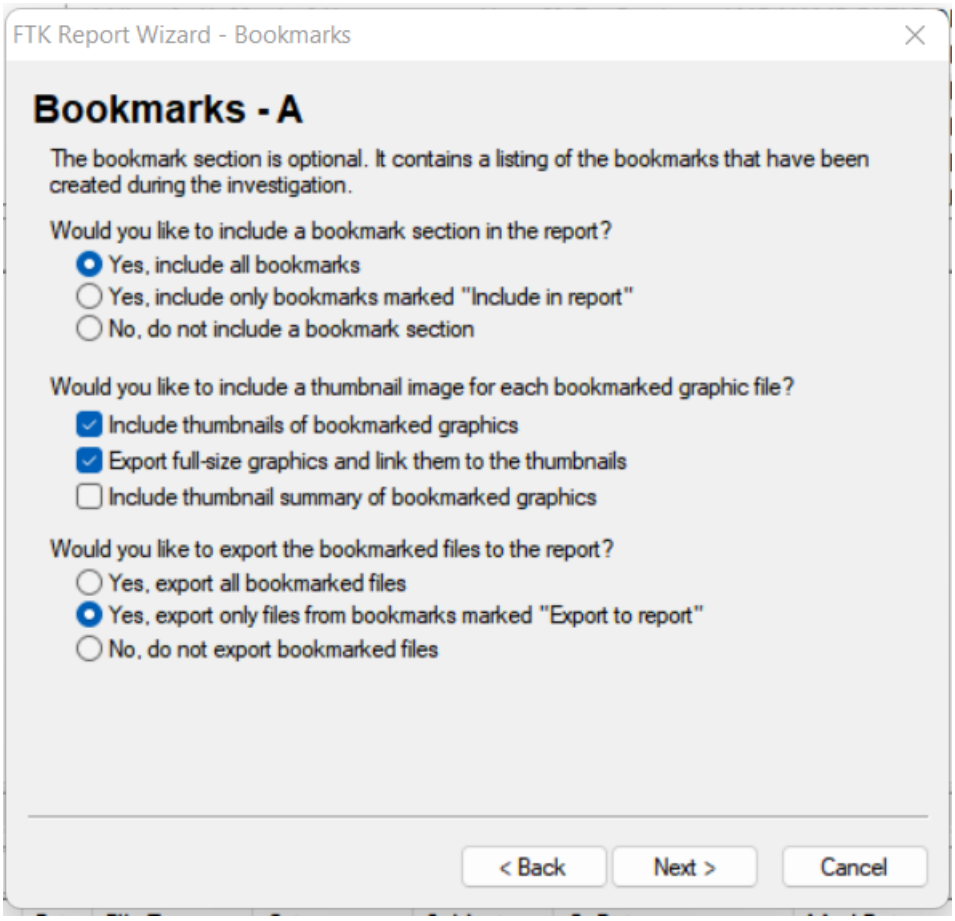
BOOKMARK FOR THE REPORT:

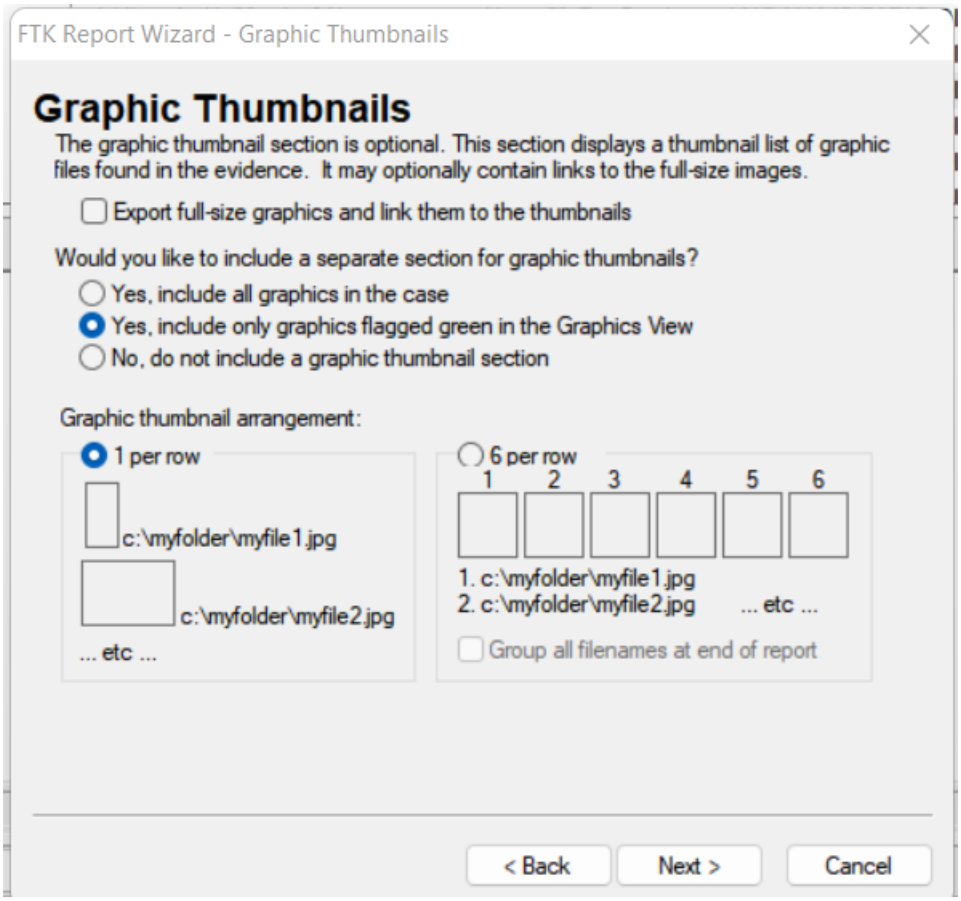
A bookmark is a group of files that you want to reference in your case. These are user-created groups and the list is stored for later reference and for use in the report output. You can create as many bookmarks as needed in a case. Bookmarks can be nested within other bookmarks for convenience and categorization purposes.

Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar or related graphic images. The Bookmarks tab lists all bookmarks that have been created in the current case.

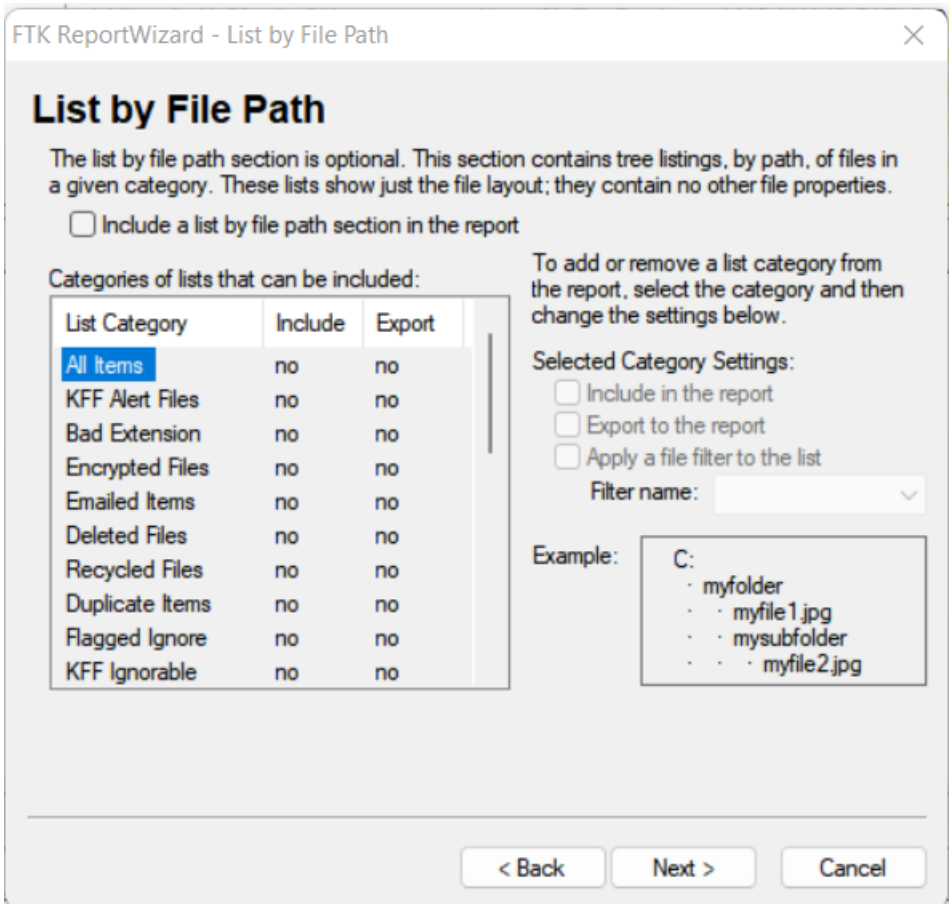
To create a bookmark, perform the following steps:

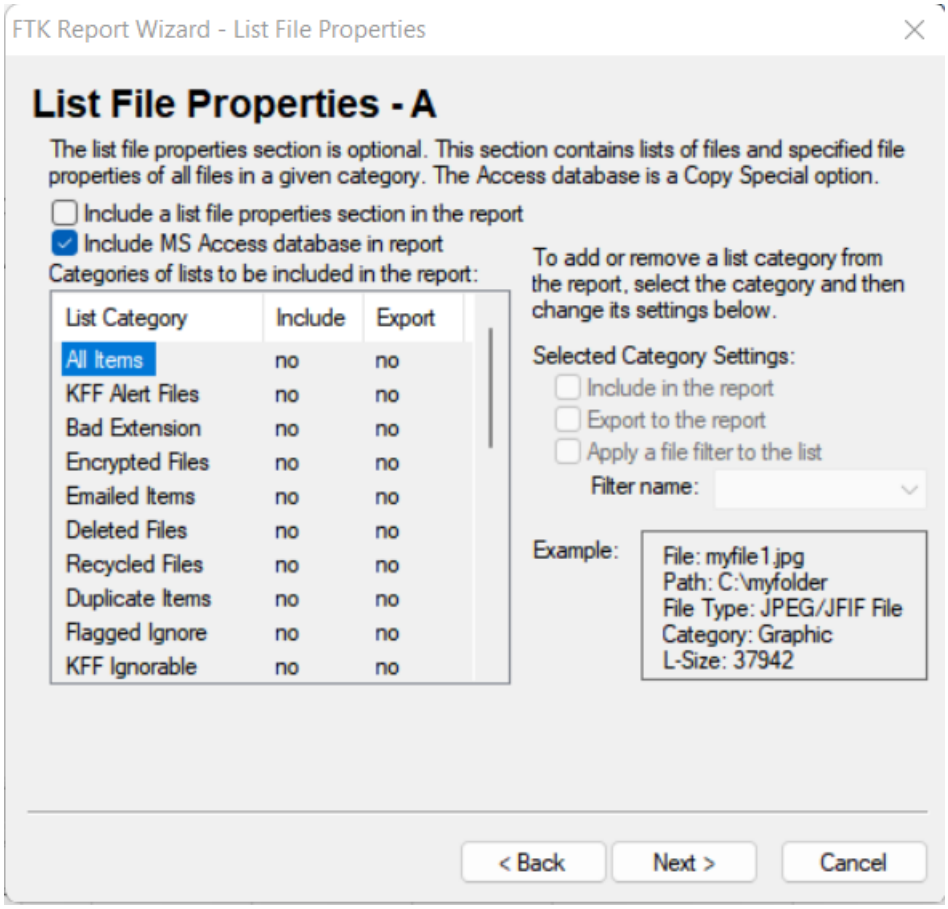
1. In the File List view, select the files that you want to add to the bookmark.
2. Right-click on selected files and click on Create Bookmark.
3. Enter the information about the bookmark.
4. Click on OK:


FTK Report Wizard - Bookmarks
Bookmarks - A
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.
Would you like to include a bookmark section in the report?
Yes, include all bookmarks
Yes, include only bookmarks marked "Include in report"
No, do not include a bookmark section
Would you like to include a thumbnail image for each bookmarked graphic file?
Include thumbnails of bookmarked graphics
Export full-size graphics and link them to the thumbnails
Include thumbnail summary of bookmarked graphics
Would you like to export the bookmarked files to the report?
Yes, export all bookmarked files
Yes, export only files from bookmarks marked "Export to report"
No, do not export bookmarked files
< Back
Next >
Cancel

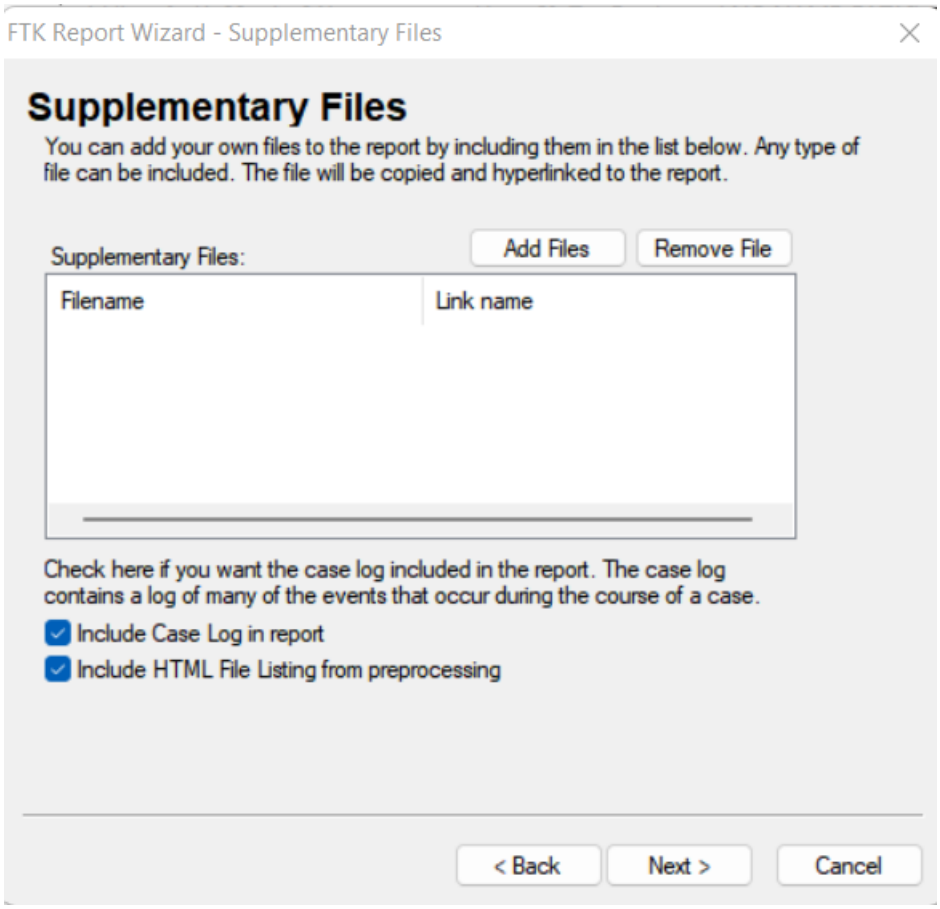

FTK Report Wizard - Graphic Thumbnails
Graphic Thumbnails
The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.
Export full-size graphics and link them to the thumbnails
Would you like to include a separate section for graphic thumbnails?
Yes, include all graphics in the case
Yes, include only graphics flagged green in the Graphics View
No, do not include a graphic thumbnail section
Graphic thumbnail arrangement:
1 per row
c:\myfolder\myfile1.jpg
c:\myfolder\myfile2.jpg
... etc ...
6 per row
1 2 3 4 5 6
1. c:\myfolder\myfile1.jpg
2. c:\myfolder\myfile2.jpg ... etc ...
Group all filenames at end of report
< Back
Next >
Cancel

LISTING BY FILE PATH:

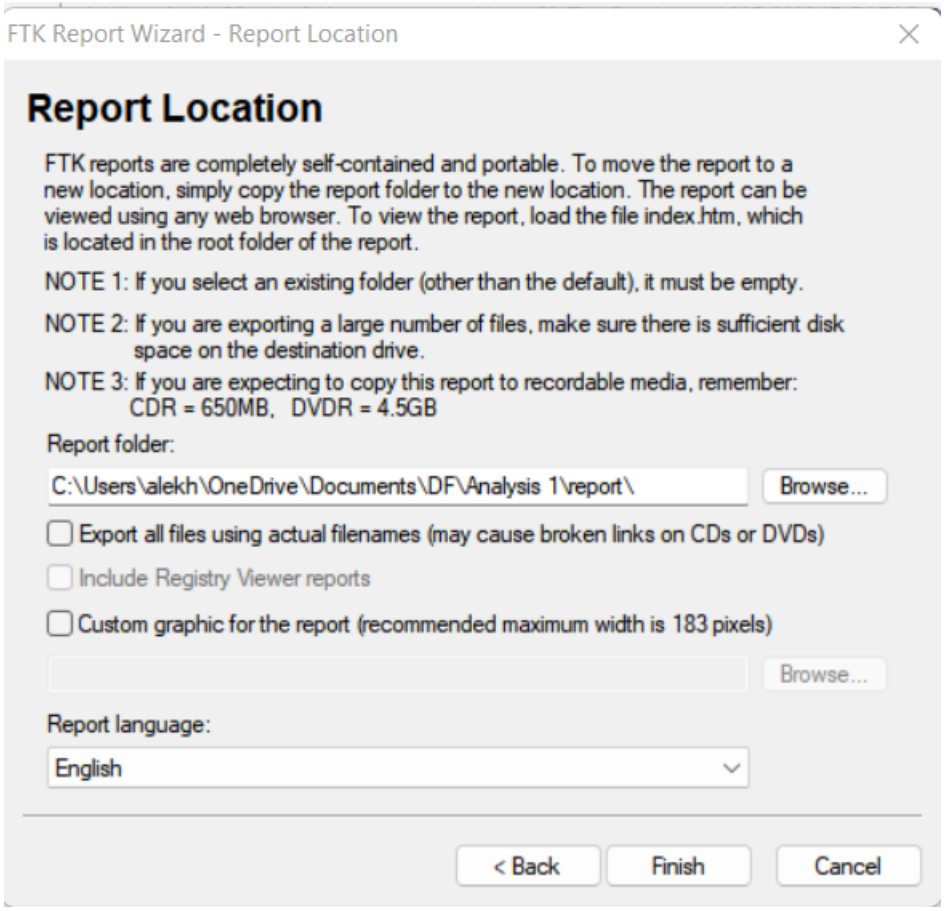




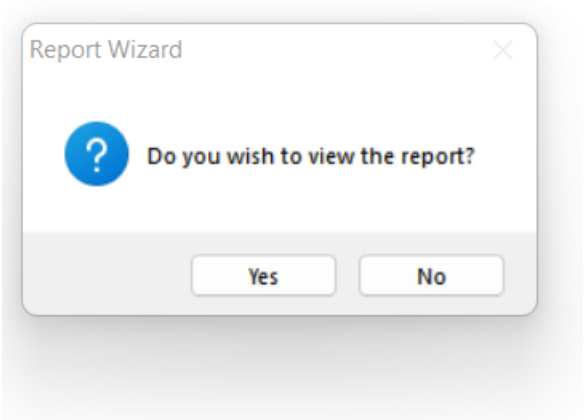
INCLUDING ALL CASE LOG AND HTML FILE LISTING



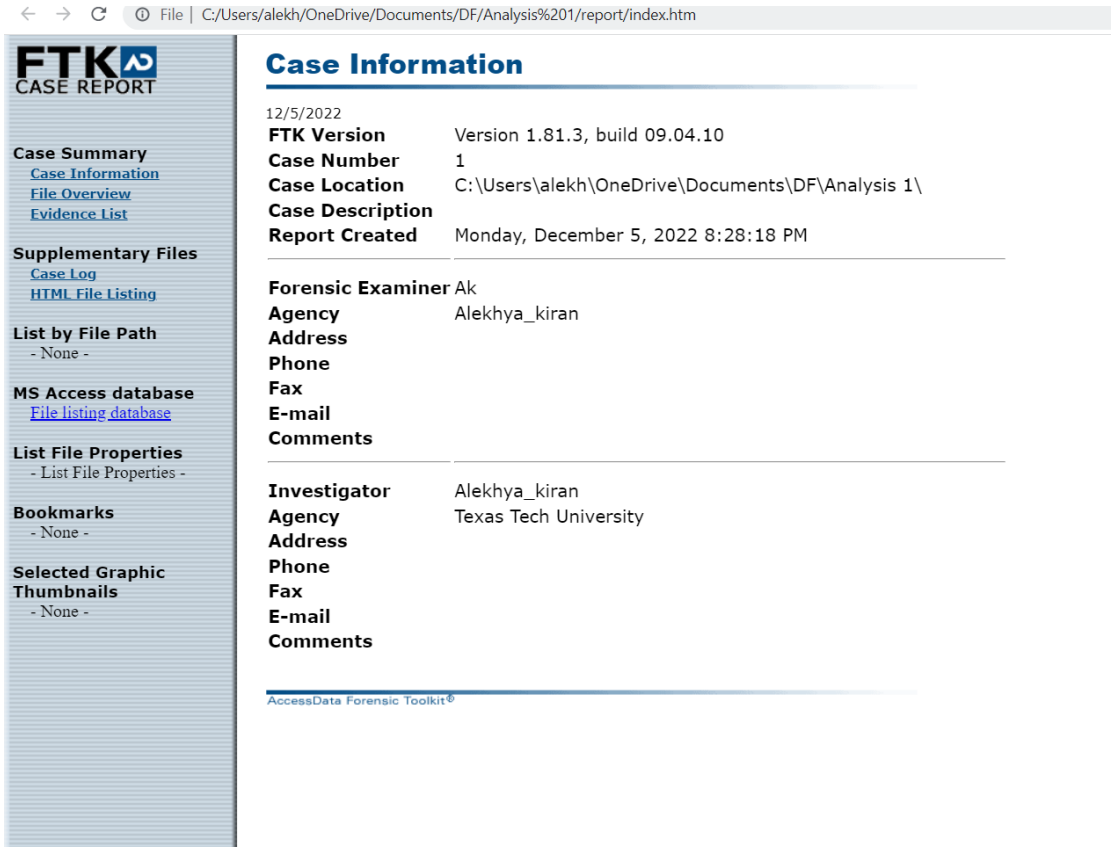
REPORT LOCATION :



SELECTING TO VIEW THE REPORT:



CASE INFORMATION OF DISK IMAGE:



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log
HTML File Listing

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Bookmarks
- None -

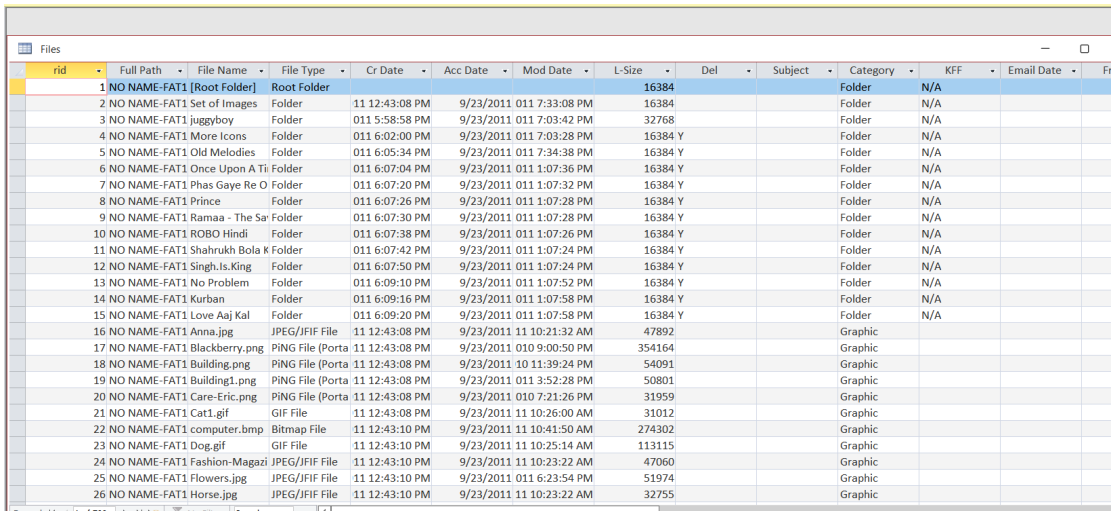
Selected Graphic Thumbnails
- None -

Case Information

12/5/2022

FTK Version	Version 1.81.3, build 09.04.10
Case Number	1
Case Location	C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\
Case Description	
Report Created	Monday, December 5, 2022 8:28:18 PM
Forensic Examiner	Ak
Agency	Alekhya_kiran
Address	
Phone	
Fax	
E-mail	
Comments	
Investigator	Alekhya_kiran
Agency	Texas Tech University
Address	
Phone	
Fax	
E-mail	
Comments	

AccessData Forensic Toolkit®



Files

rid	Full Path	File Name	File Type	Cr Date	Acc Date	Mod Date	L-Size	Del	Subject	Category	KFF	Email Date
1	NO NAME-FAT1	[Root Folder]	Root Folder				16384			Folder	N/A	
2	NO NAME-FAT1	Set of Images	Folder	11 12:43:08 PM	9/23/2011	011 7:33:08 PM	16384			Folder	N/A	
3	NO NAME-FAT1	juggyboy	Folder	011 5:58:58 PM	9/23/2011	011 7:03:42 PM	32768			Folder	N/A	
4	NO NAME-FAT1	More Icons	Folder	011 6:02:00 PM	9/23/2011	011 7:03:28 PM	16384	Y		Folder	N/A	
5	NO NAME-FAT1	Old Melodies	Folder	011 6:05:34 PM	9/23/2011	011 7:34:38 PM	16384	Y		Folder	N/A	
6	NO NAME-FAT1	Once Upon A Ti	Folder	011 6:07:04 PM	9/23/2011	011 1:07:36 PM	16384	Y		Folder	N/A	
7	NO NAME-FAT1	Phas Gaye Re O	Folder	011 6:07:20 PM	9/23/2011	011 1:07:32 PM	16384	Y		Folder	N/A	
8	NO NAME-FAT1	Prince	Folder	011 6:07:26 PM	9/23/2011	011 1:07:28 PM	16384	Y		Folder	N/A	
9	NO NAME-FAT1	Ramaa - The Sa	Folder	011 6:07:30 PM	9/23/2011	011 1:07:28 PM	16384	Y		Folder	N/A	
10	NO NAME-FAT1	ROBO Hindi	Folder	011 6:07:38 PM	9/23/2011	011 1:07:26 PM	16384	Y		Folder	N/A	
11	NO NAME-FAT1	Shahrukh Bola K	Folder	011 6:07:42 PM	9/23/2011	011 1:07:24 PM	16384	Y		Folder	N/A	
12	NO NAME-FAT1	Singh.Is.King	Folder	011 6:07:50 PM	9/23/2011	011 1:07:24 PM	16384	Y		Folder	N/A	
13	NO NAME-FAT1	No Problem	Folder	011 6:09:10 PM	9/23/2011	011 1:07:52 PM	16384	Y		Folder	N/A	
14	NO NAME-FAT1	Kurban	Folder	011 6:09:16 PM	9/23/2011	011 1:07:58 PM	16384	Y		Folder	N/A	
15	NO NAME-FAT1	Love Aaj Kal	Folder	011 6:09:20 PM	9/23/2011	011 1:07:58 PM	16384	Y		Folder	N/A	
16	NO NAME-FAT1	Anna.jpg	JPEG/JFIF File	11 12:43:08 PM	9/23/2011	11 10:21:32 AM	47892			Graphic		
17	NO NAME-FAT1	Blackberry.png	PiNG File (Porta	11 12:43:08 PM	9/23/2011	010 9:00:50 PM	354164			Graphic		
18	NO NAME-FAT1	Building.png	PiNG File (Porta	11 12:43:08 PM	9/23/2011	10 11:39:24 PM	54091			Graphic		
19	NO NAME-FAT1	Building1.png	PiNG File (Porta	11 12:43:08 PM	9/23/2011	011 3:52:28 PM	50801			Graphic		
20	NO NAME-FAT1	Care-Eric.png	PiNG File (Porta	11 12:43:08 PM	9/23/2011	010 7:21:26 PM	31959			Graphic		
21	NO NAME-FAT1	Cat1.gif	GIF File	11 12:43:08 PM	9/23/2011	11 10:26:00 AM	31012			Graphic		
22	NO NAME-FAT1	computer.bmp	Bitmap File	11 12:43:10 PM	9/23/2011	11 10:41:50 AM	274302			Graphic		
23	NO NAME-FAT1	Dog.gif	GIF File	11 12:43:10 PM	9/23/2011	11 10:25:14 AM	113115			Graphic		
24	NO NAME-FAT1	Fashion-Magazi	JPEG/JFIF File	11 12:43:10 PM	9/23/2011	11 10:23:22 AM	47060			Graphic		
25	NO NAME-FAT1	Flowers.jpg	JPEG/JFIF File	11 12:43:10 PM	9/23/2011	011 6:23:54 PM	51974			Graphic		
26	NO NAME-FAT1	Horse.jpg	JPEG/JFIF File	11 12:43:10 PM	9/23/2011	11 10:23:22 AM	32755			Graphic		

FINAL REPORT OF THE IMAGE:

FTK CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log
- HTML File Listing

List by File Path
- None -

MS Access database
- File listing database

List File Properties
- List File Properties -

Bookmarks
- None -

Selected Graphic Thumbnails
- None -

File Overview

12/5/2022

Evidence Items
Evidence Items: 1

File Items
Total File Items: 1,990
Flagged Thumbnails: 0
Other Thumbnails: 1,066

File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 1
Encrypted Files: 0
From E-mail: 0
Deleted Files: 445
From Recycle Bin: 0
Duplicate Items: 140
OLE Subitems: 4
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0

File Category
Documents: 3
Spreadsheets: 0
Databases: 0
Graphics: 1,066
Multimedia: 103
E-mail Messages: 0
Executables: 0
Archives: 3
Folders: 15
Slack/Free Space: 791
Other Known Type: 0
Unknown Type: 9

FTK CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log
- HTML File Listing

List by File Path
- None -

MS Access database
- File listing database

List File Properties
- List File Properties -

Bookmarks
- None -

Selected Graphic Thumbnails
- None -

Evidence List

12/5/2022
Display Name: TestRawImage\NO NAME-FAT16
Evidence File Name: TestRawImage.dd
Evidence Path: C:\Users\alekh\OneDrive\Documents\DF
Identification Name/Number:
Evidence Type: FAT16
Added: 12/5/2022 8:09:00 PM
Children: 1,589
Descendants: 1,990

AccessData Forensic Toolkit®

FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log
HTML File Listing

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Bookmarks
- None -

Selected Graphic Thumbnails
- None -

```
12/5/2022 8:09:00 PM -- FTK Version 1.81.3 build 09.04.10
        FTK Exe Path:  C:\Program Files (x86)\AccessData\AccessData Forensic Toolkit 1.81.3\Program\ftk.exe
        Examiner's Machine:
        Phys Mem:  Total: 4,294,967,295  Available: 3,834,355,712  Used: 460,611,583
        Virt Mem:  Total: 4,294,836,224  Available: 3,467,272,192  Used: 827,564,032
        Page File Available: 4,294,967,295
        ----------------------------------------------------
12/5/2022 8:09:00 PM -- KFF database being used:  none
12/5/2022 8:09:00 PM -- Examiner's Local Machine Setting is time zone used for file times (create, modify, accessed) in file display and reports.
12/5/2022 8:09:00 PM -- New case started by examiner Ak using FTK version 1.81.3 build 09.04.10
        Investigator: Alekhya_kiran
        Case Name: Analysis 1
        Case Number: 1
        Case Folder: C:\Users\alekh\OneDrive\Documents\DF\Analysis 1
        Description:
        Case Log Options (NOT Case Reviewer Logging Options):
          Log case and evidence events: Yes
          Log error messages: Yes
          Log bookmarking events: Yes
          Log searching events: Yes
          Log special searching events: Yes
          Log other events: Yes
          Log extended information: No
        Processes to be performed:
          File Extraction: Yes
          File Identification: Yes
          MD5 Hash: Yes
          SHA1 Hash: Yes
          KFF (Known File Filter): Yes
          Entropy Test: Yes
          Full Text Index: Yes
          Prerender Thumbnails: Yes
          File Listing Database: Yes
          HTML File Listing: Yes
          Data Carving: Yes
          Preprocess Registry Files: Yes
          Decrypt EFS Files: Yes
        Default Case Refinement Settings:
          Add files only if they satisfy BOTH the file status and the file type criteria as follows:
            File Status Criteria:
              Deletion status: any
              Encryption status: any
              From email status: any
              Duplicate status: any
              OLE stream status: any
            File Type Criteria:
              documents: yes
              spreadsheets: yes
```