

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.

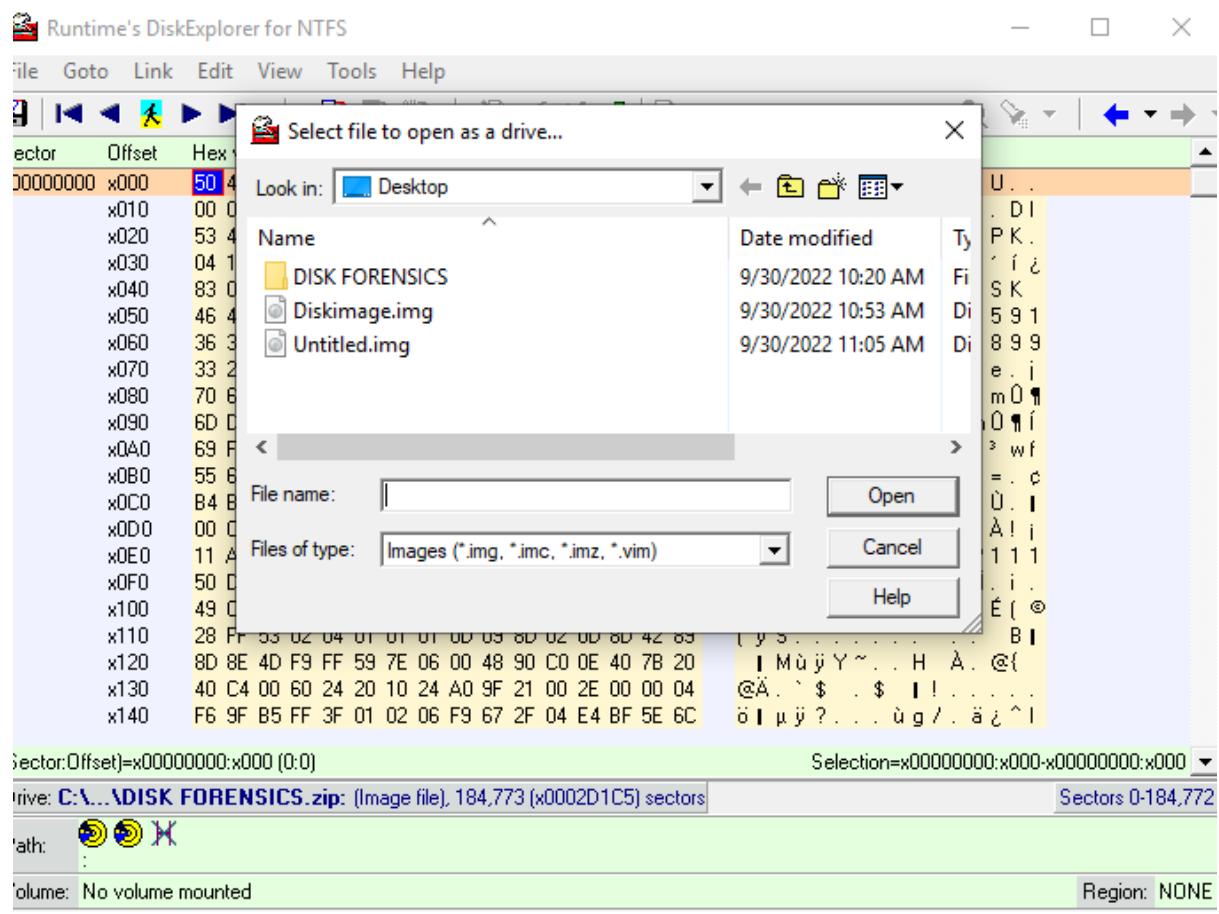
DELIVERABLES:

- 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.

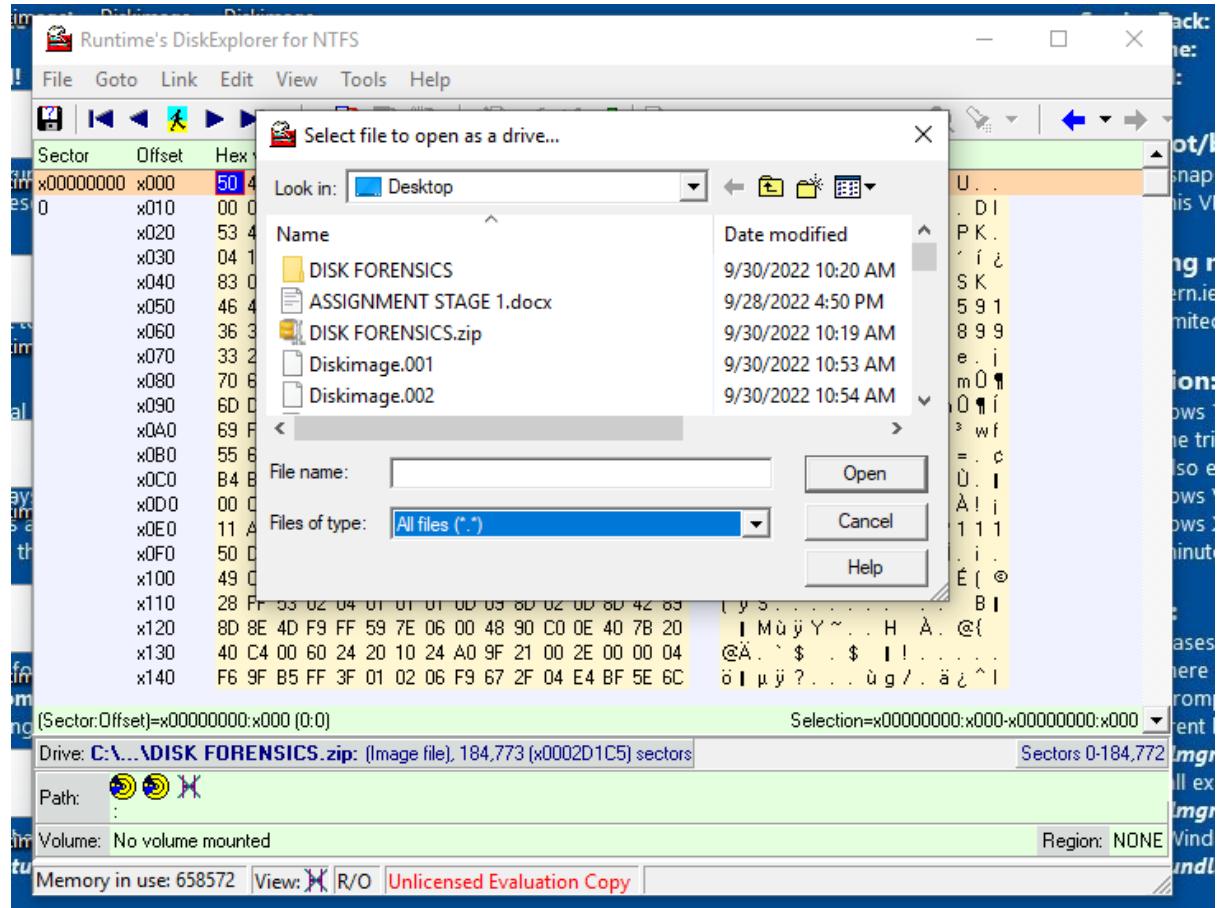
DISK FORENSICS FIRST DELIVERABLE

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

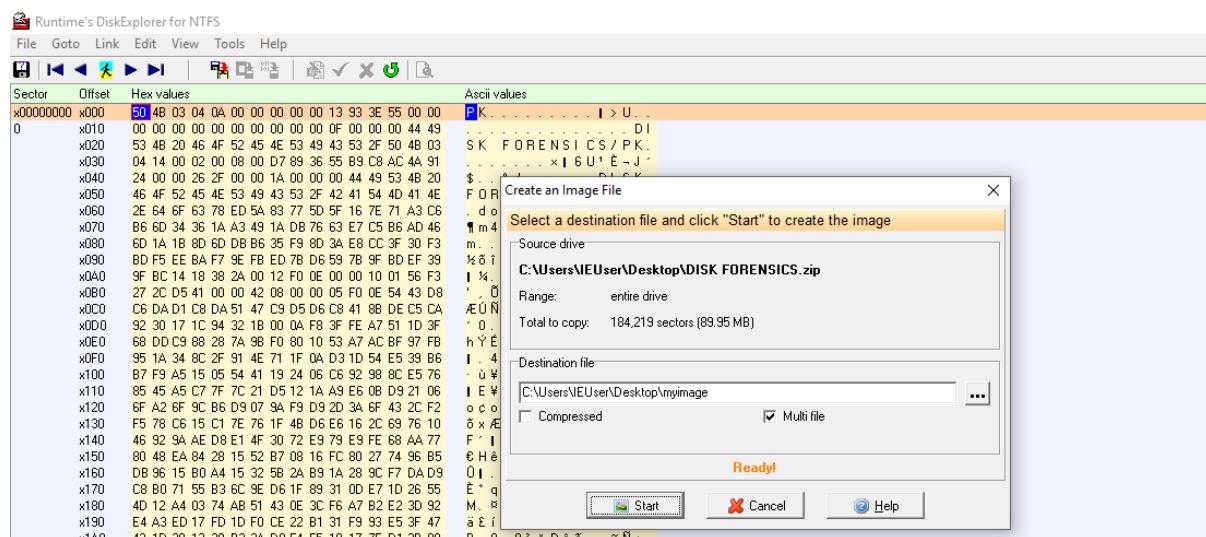
1. Disk Explorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery. Disk Explorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery. It navigates your NTFS drive by jumping to the partition table, boot record, 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.

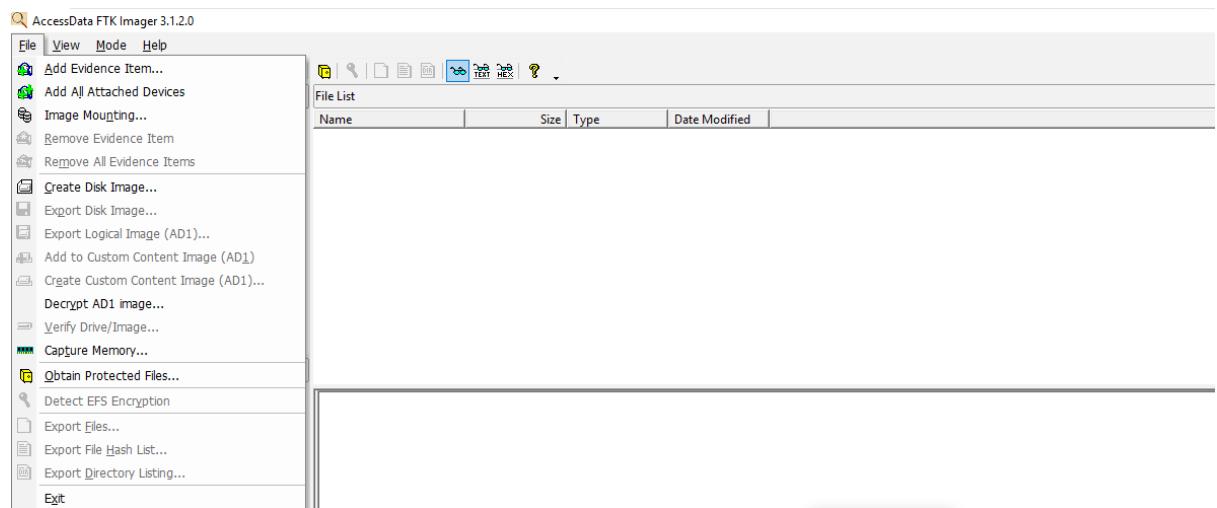


3. Below we are selecting the destination path for the disk image and named it as myimage

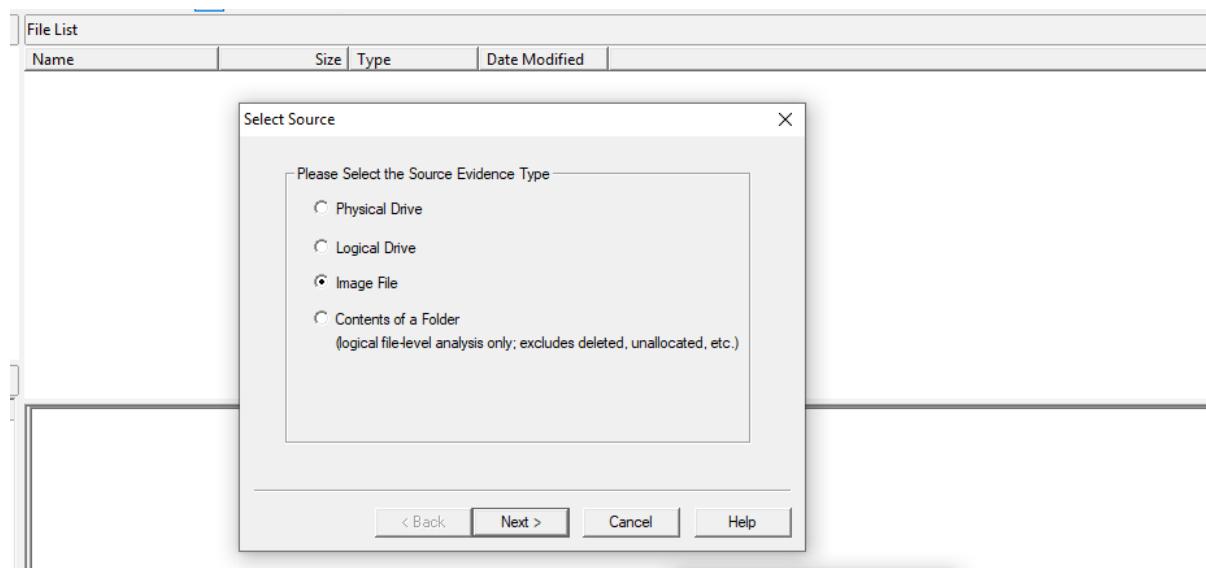


4. FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as AccessData Forensic Toolkit (FTK) is warranted.

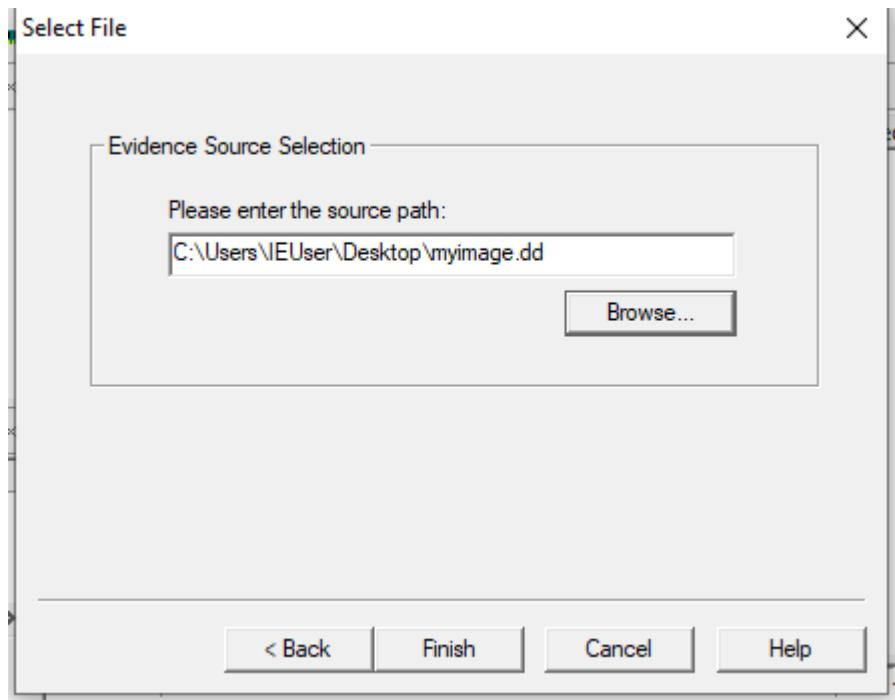
Using this tool we can investigate the data present in the disk image.



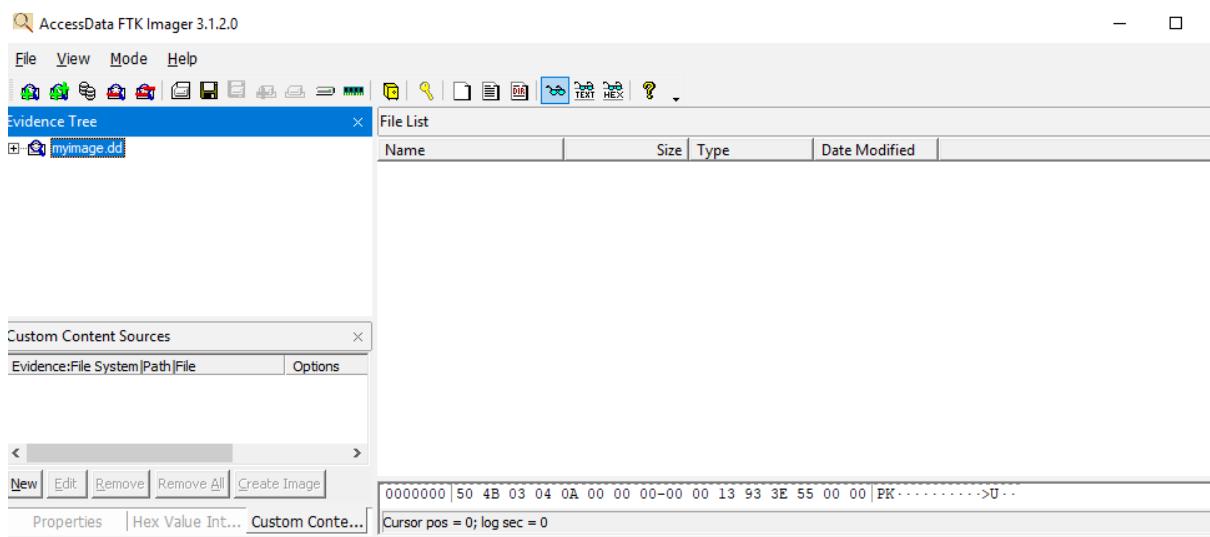
5. Here we are selecting the source which we have to investigate.



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.



Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

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: 0097fcd4bb986347df58580269cf7ab3fadafef

Image Information:
 Acquisition started: Fri Sep 30 18:47:09 2022
 Acquisition finished: Fri Sep 30 19:47:10 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: 0097fc4bb986347df58580269cf7ab3fadafee
```

```
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: 0097fc4bb986347df58580269cf7ab3fadafee : 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

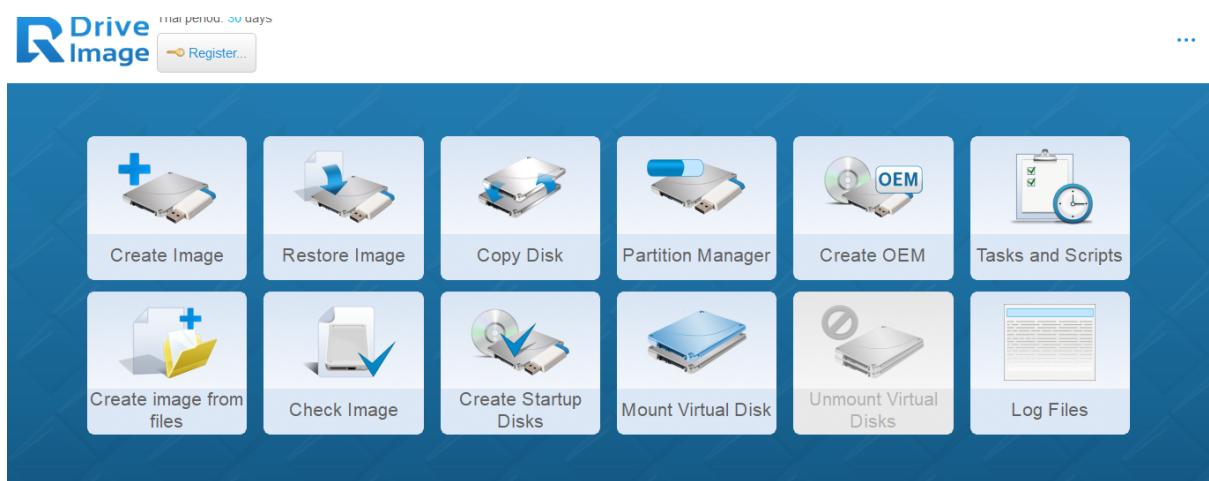
R-Drive Image is a potent utility providing disk image files creation for backup or duplication purposes. A disk image file contains the exact, byte-by-byte copy of a hard drive, partition or logical disk and can be created with various compression levels on the fly without stopping Windows OS and therefore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

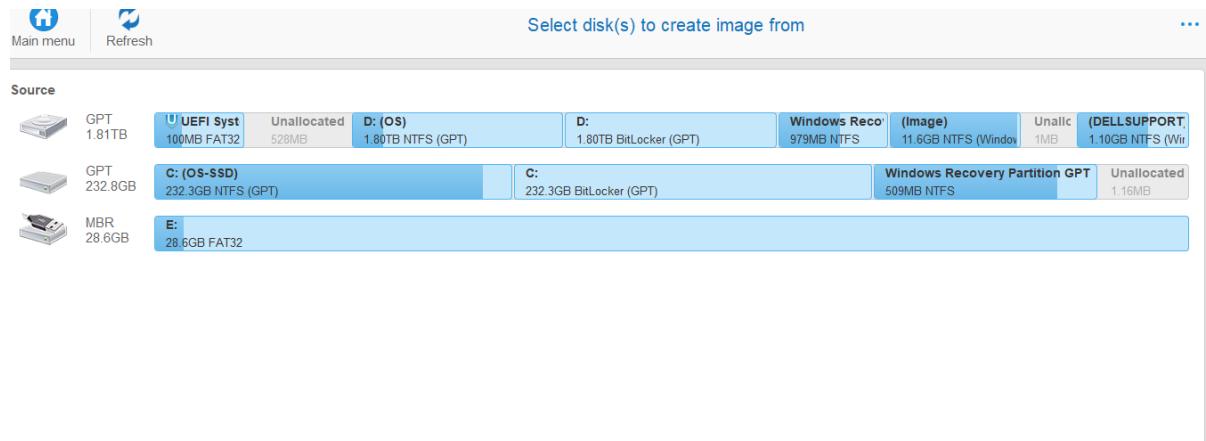
Using R-Drive Image, you can completely and rapidly restore your system after heavy data loss caused by an operating system crash, virus attack or hardware failure.

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

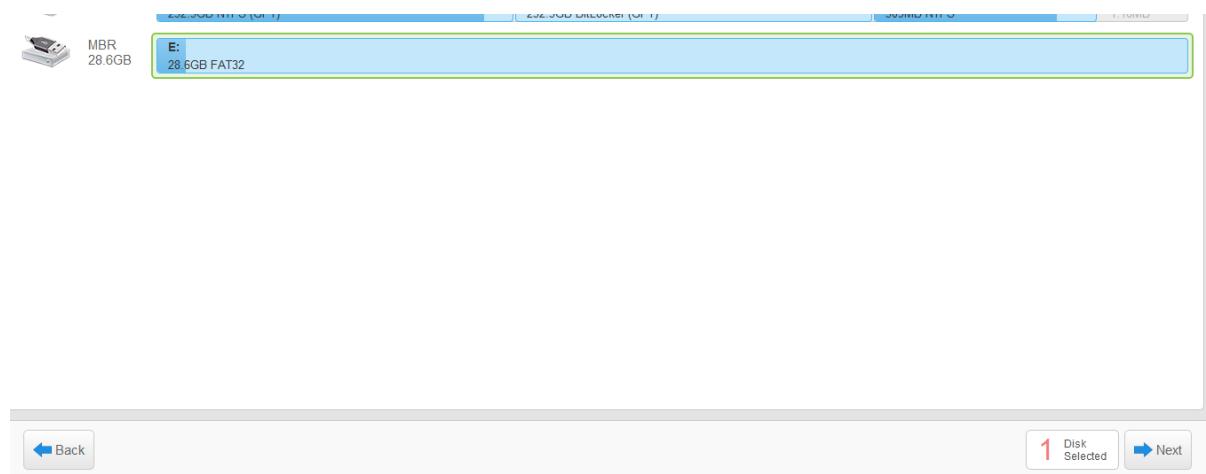
Step 1: Creating Disk image using R-Drive Image tool



Step 2: Selecting drive to create disk image



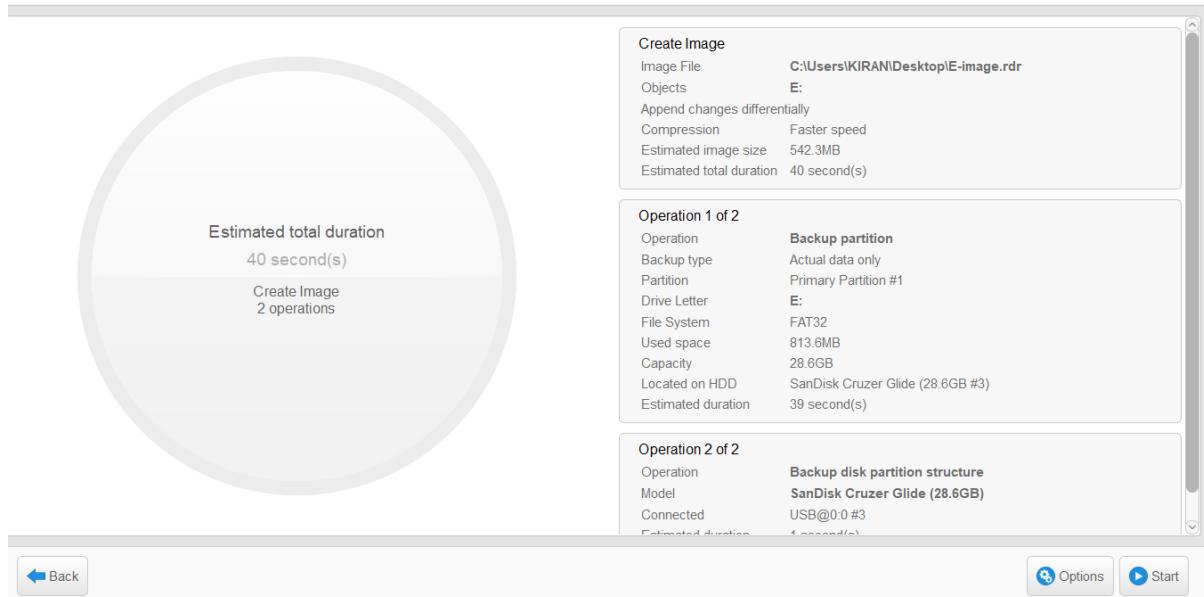
Step 3: Selected the disk and started the operation



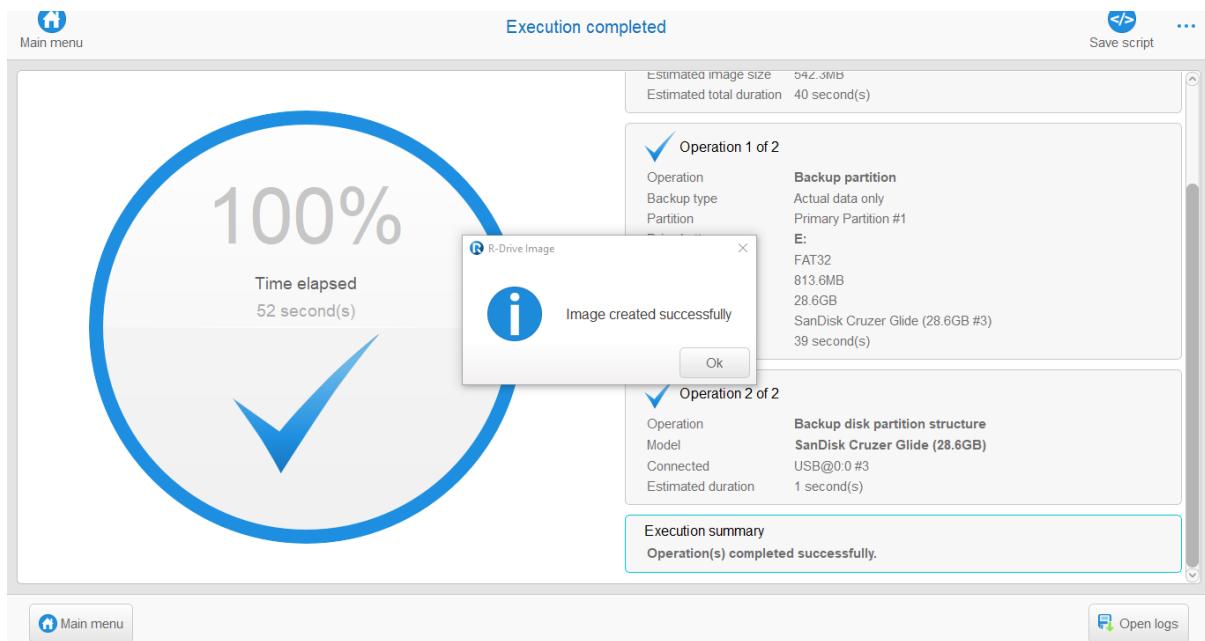
Step 4: Selected the destination to save the disk image



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

A file manager window displays a list of files and folders. The "temp" folder is selected and highlighted with a yellow icon. The table columns are Name, Date modified, Type, and Size. The "temp" folder was created on 02-07-2022 11:33 and is a File folder. Other items listed include "File Recovery by Type", "Install SanDisk Software.dmg", "Install SanDisk Software", and "SanDisk Software".

Delete Folder

Are you sure you want to permanently delete this folder?

temp
Type: File folder

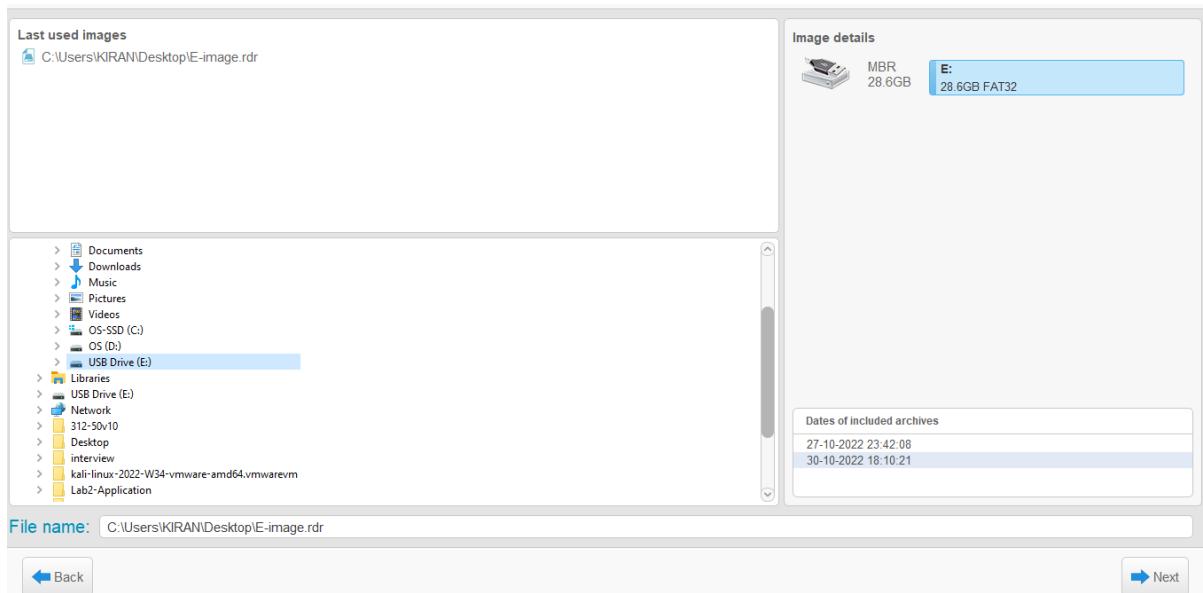
Yes No

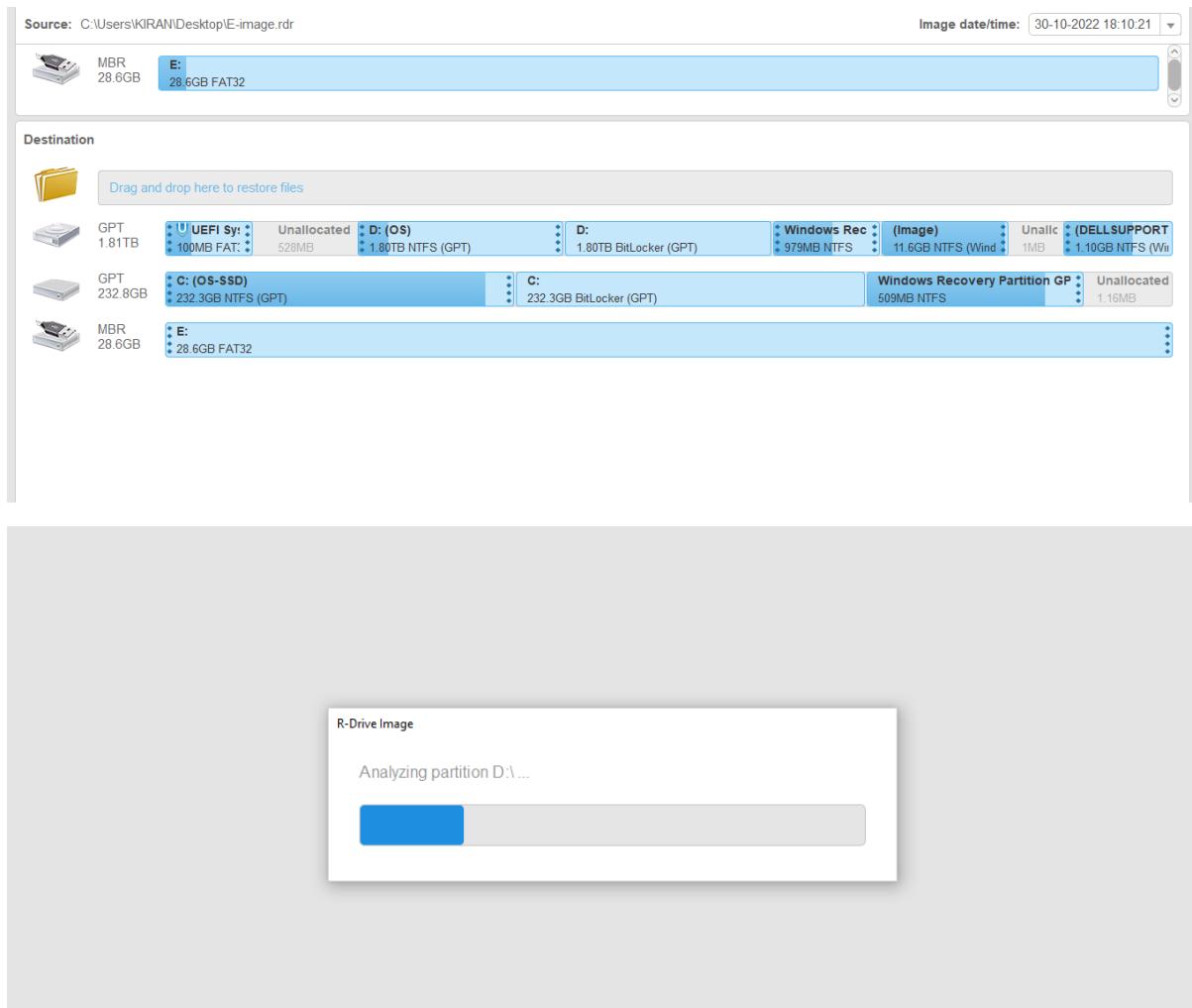
RECOVERING THE DELETED DATA

Step 1: Selecting the disk image to recover the data

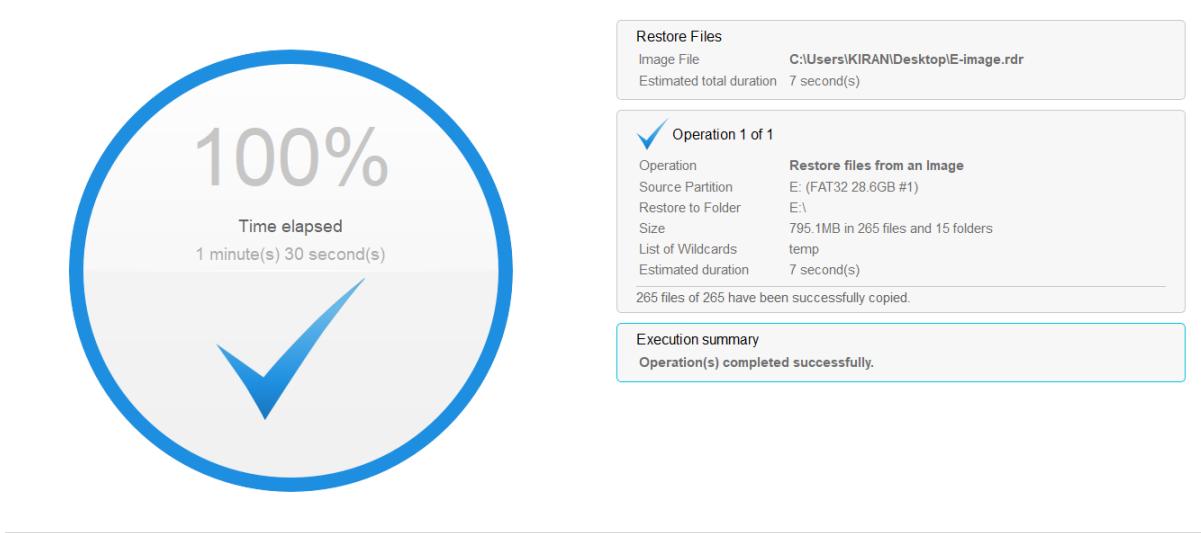
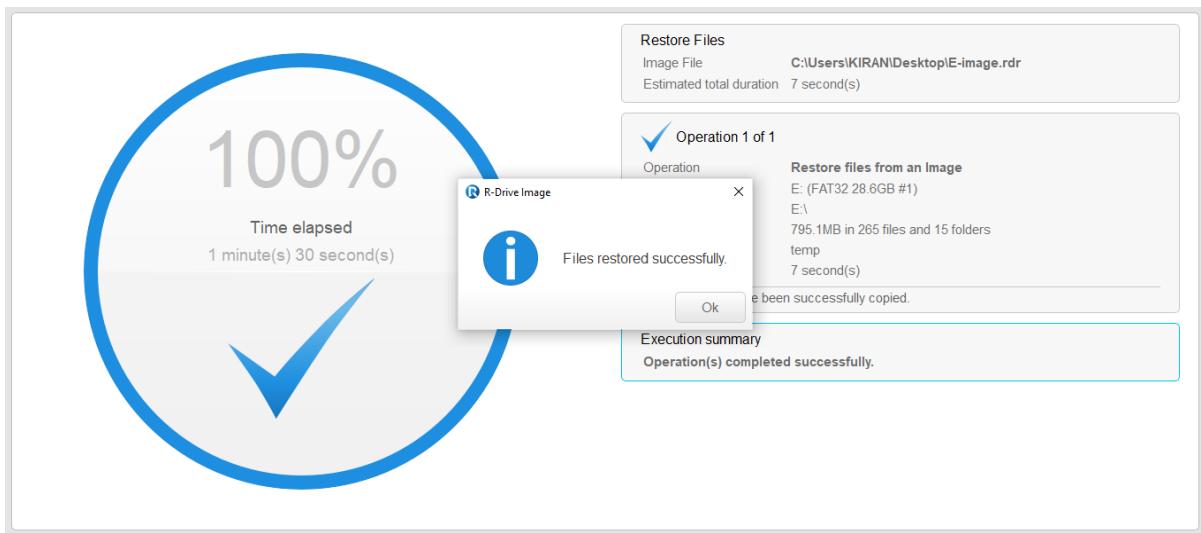


Step 2: Specifying the destination to recover the data





Step 3: The deleted files are recovered successfully



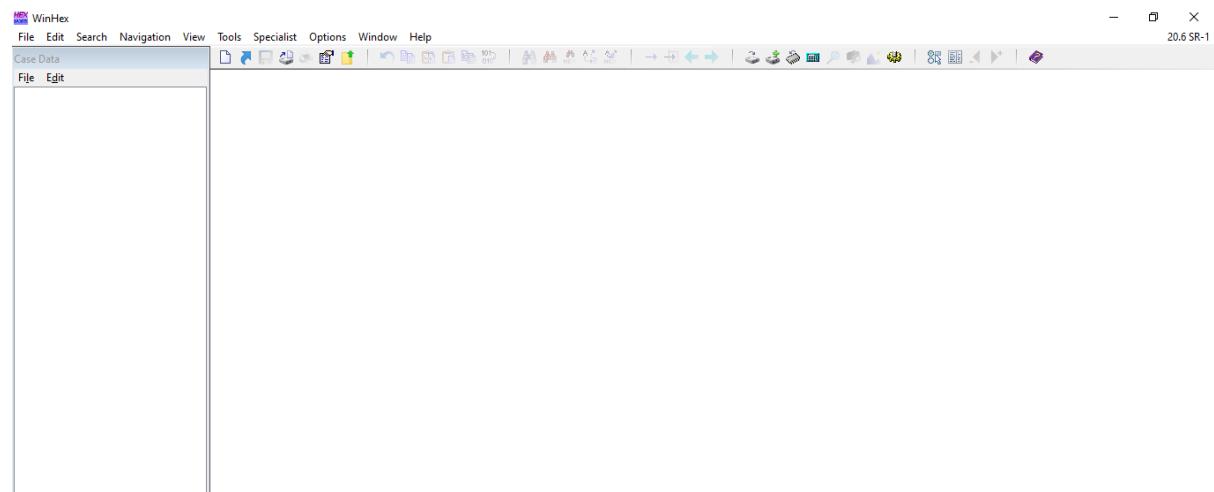
Step 4: The recovered folder(temp) using the disk image

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

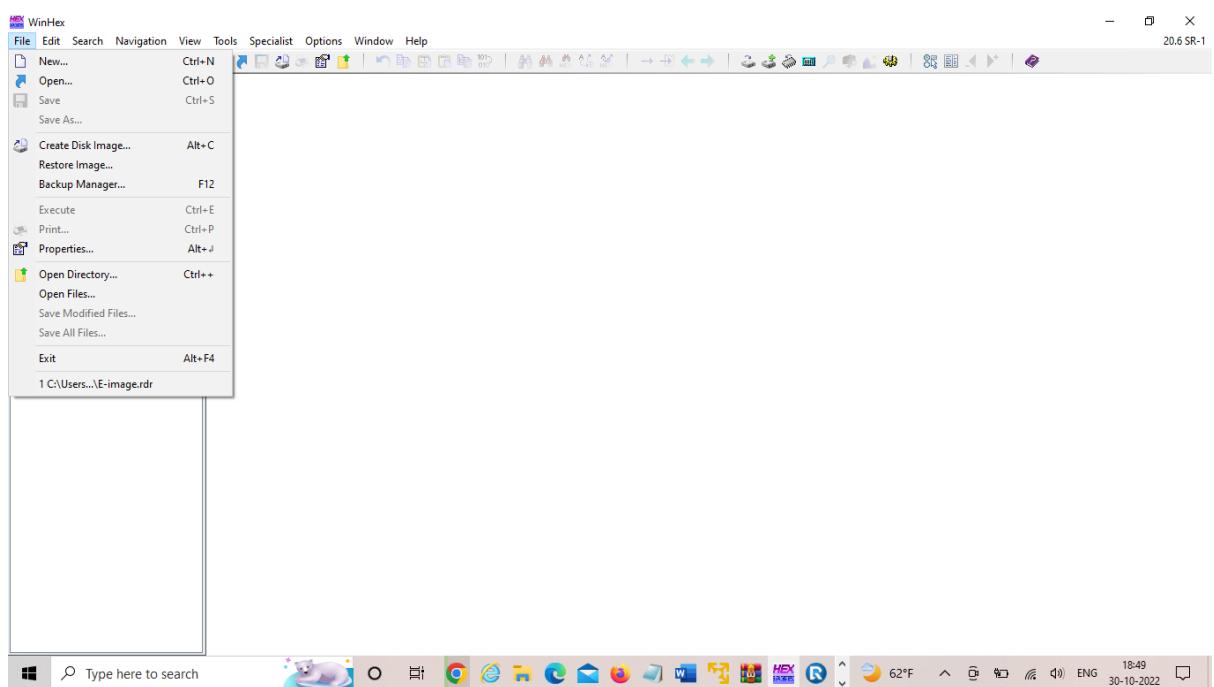
WINHEX:

- 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.

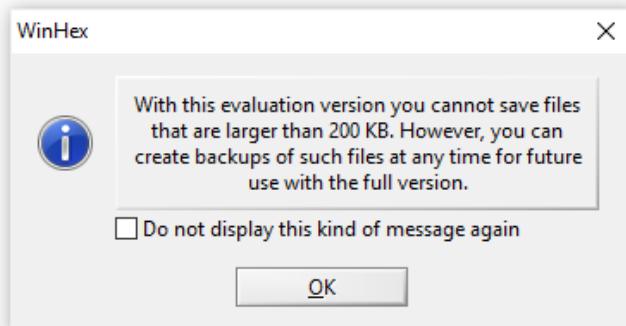
STEP1: install WINHEX tool, and start the application.



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

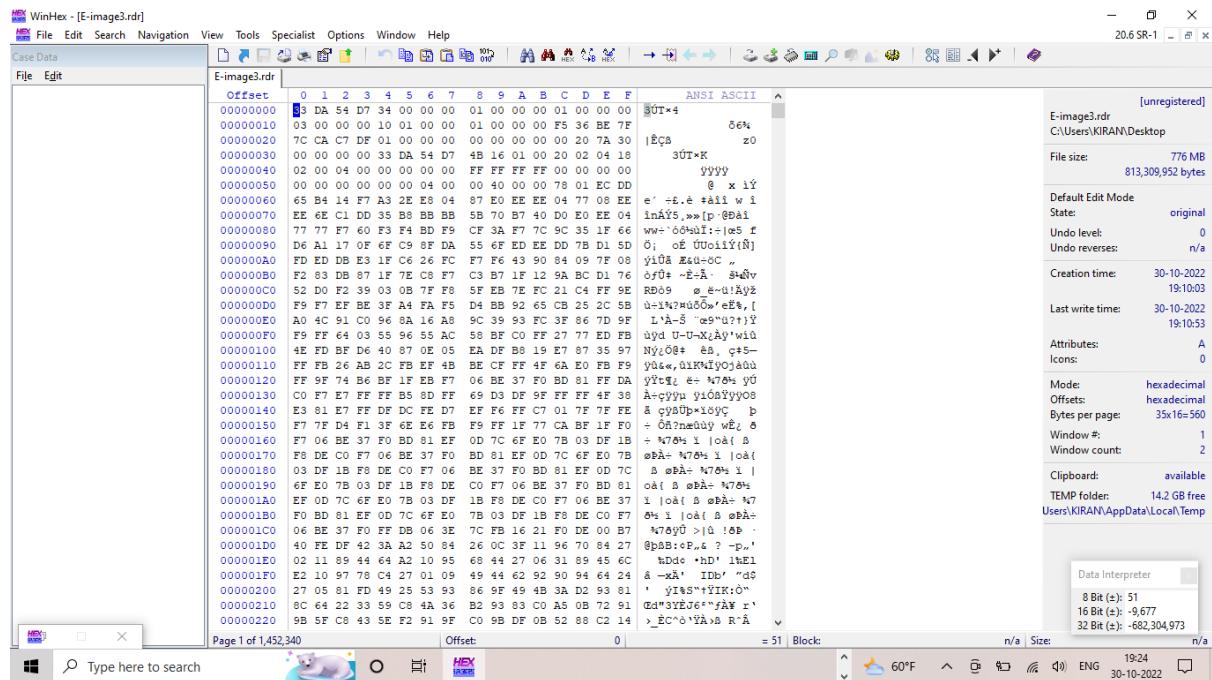


Step 3: popup message will be displayed on monitor

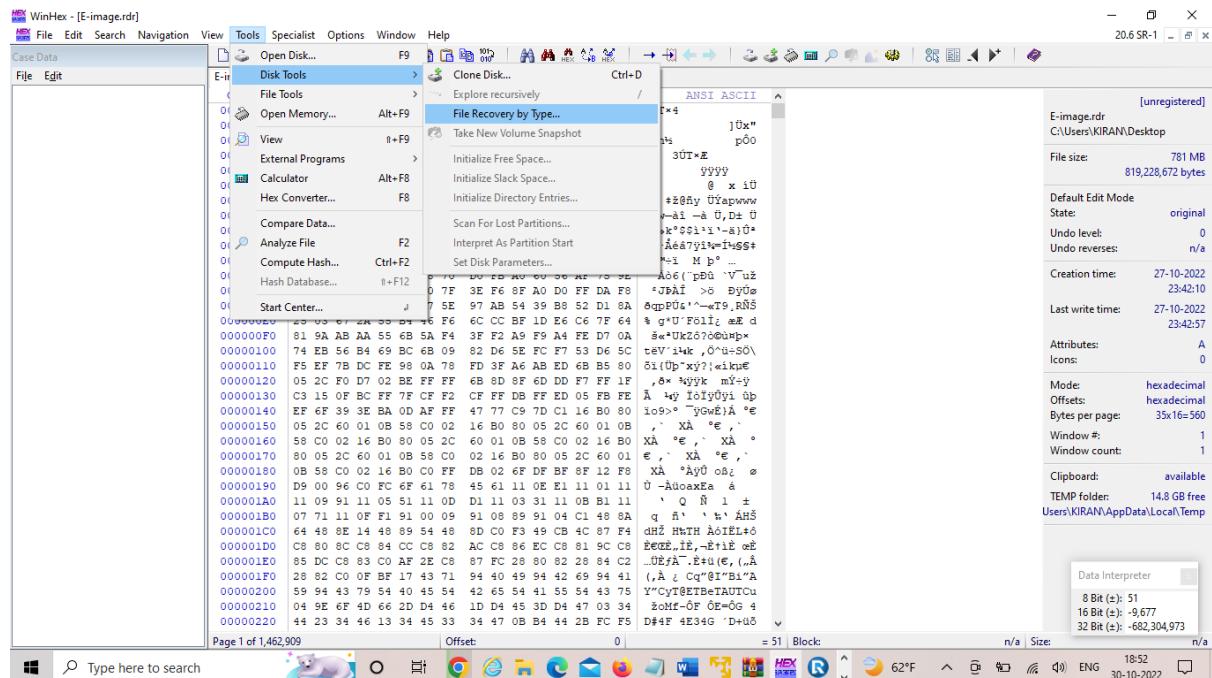


Step 4:

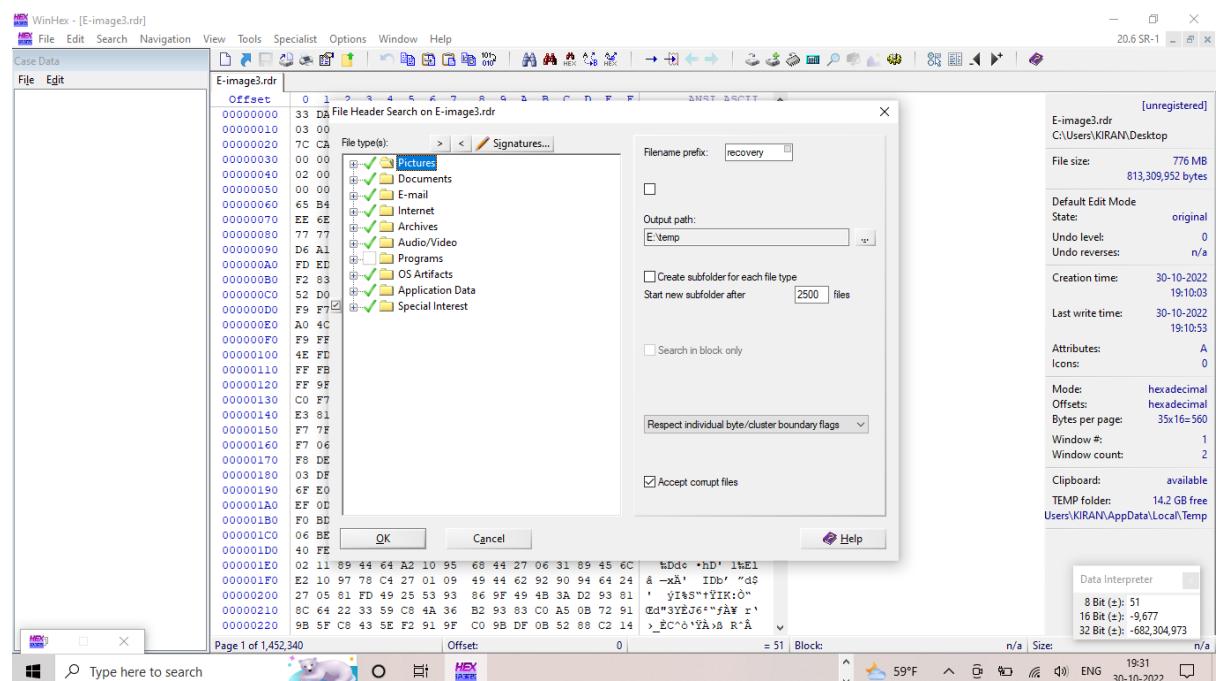
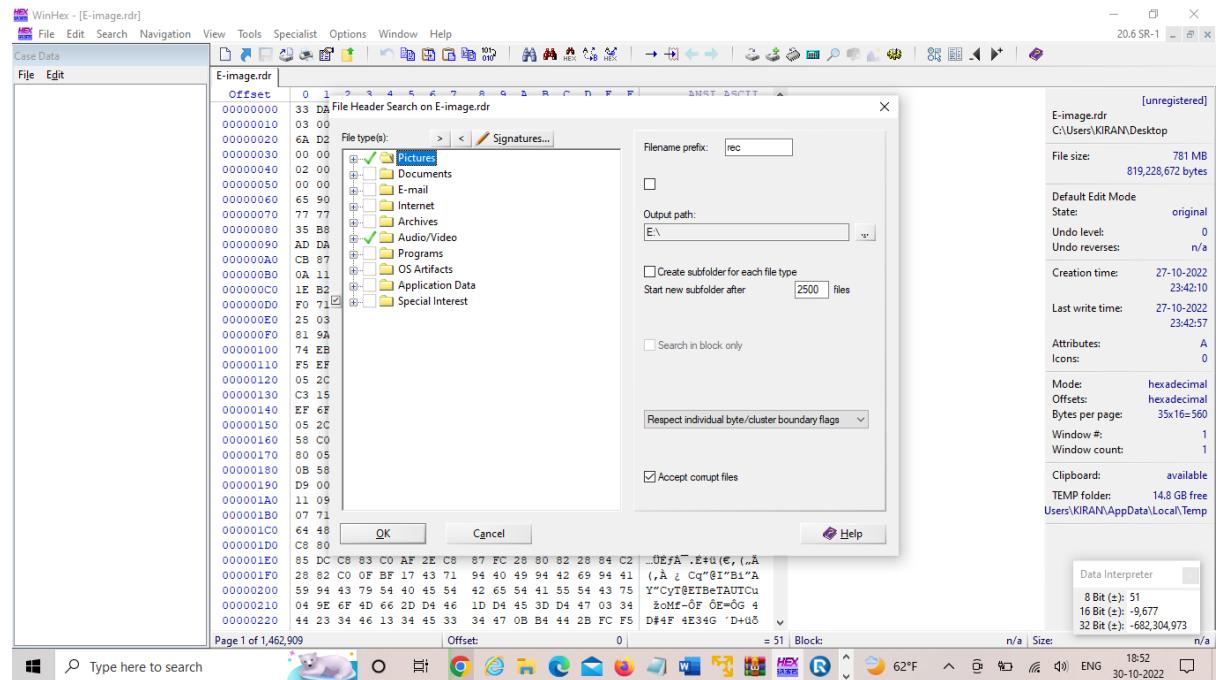
We can view the disk image data hexadecimal



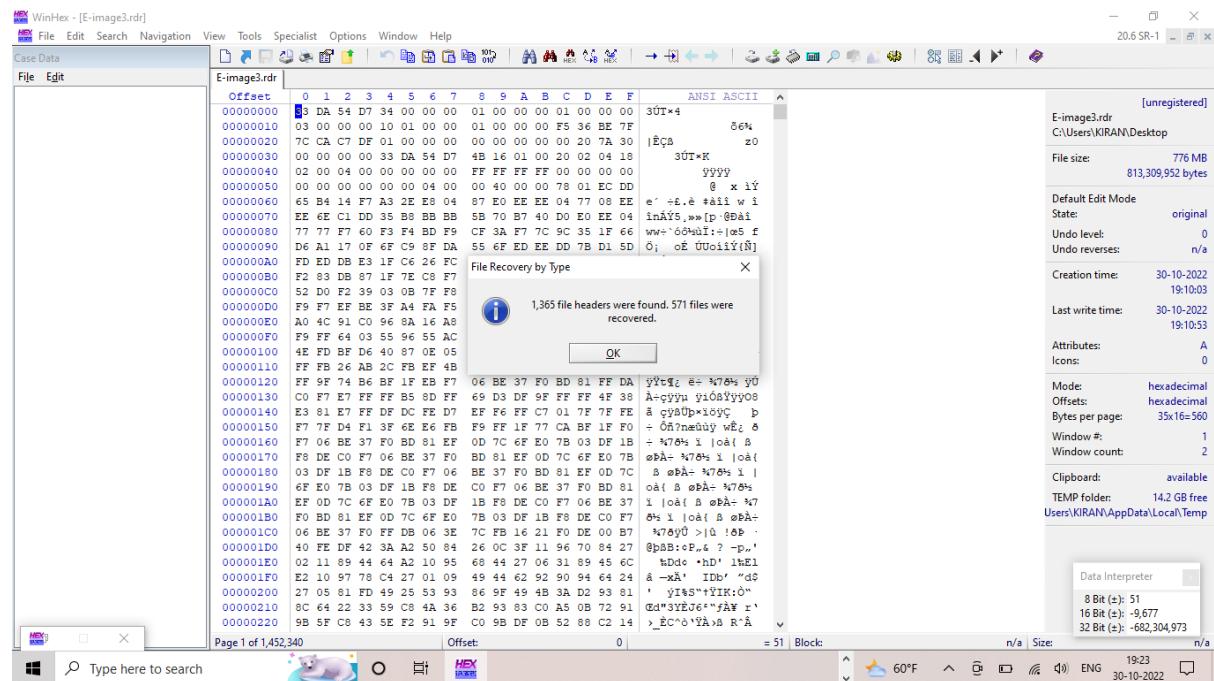
Step 5: We can select the type of the data to be recovered using the disk image



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

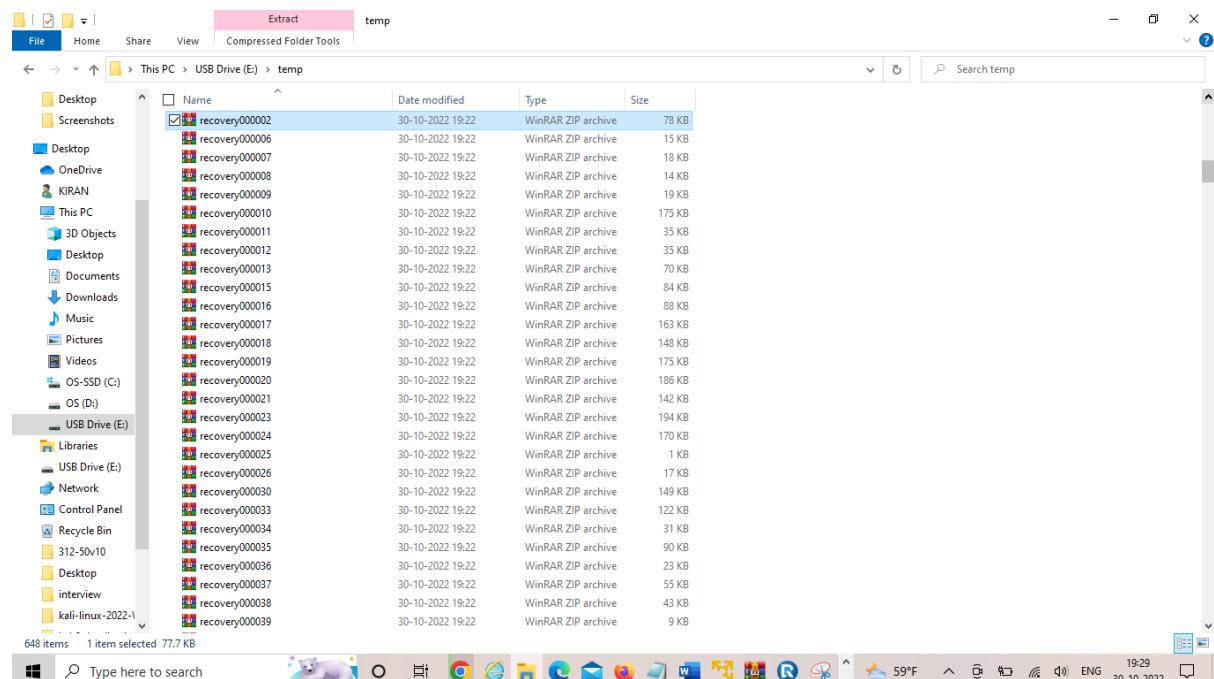


Step 7: The picture type files are recovered using Disk image

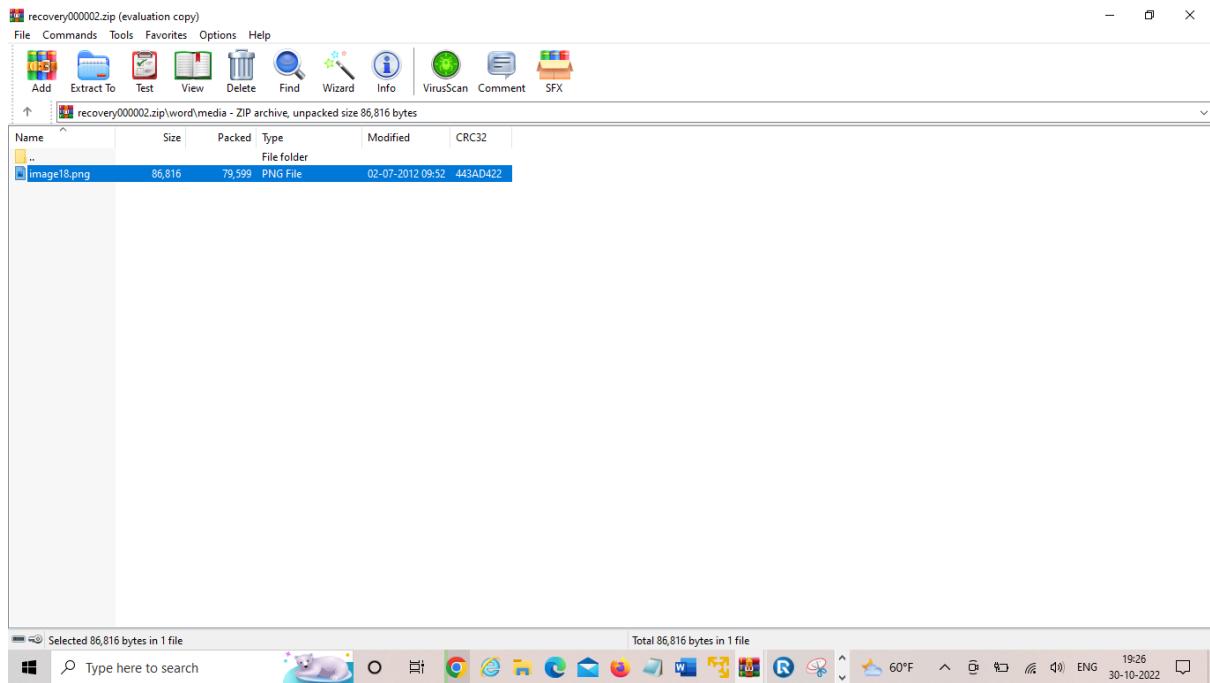


Step 8:

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 highly 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.

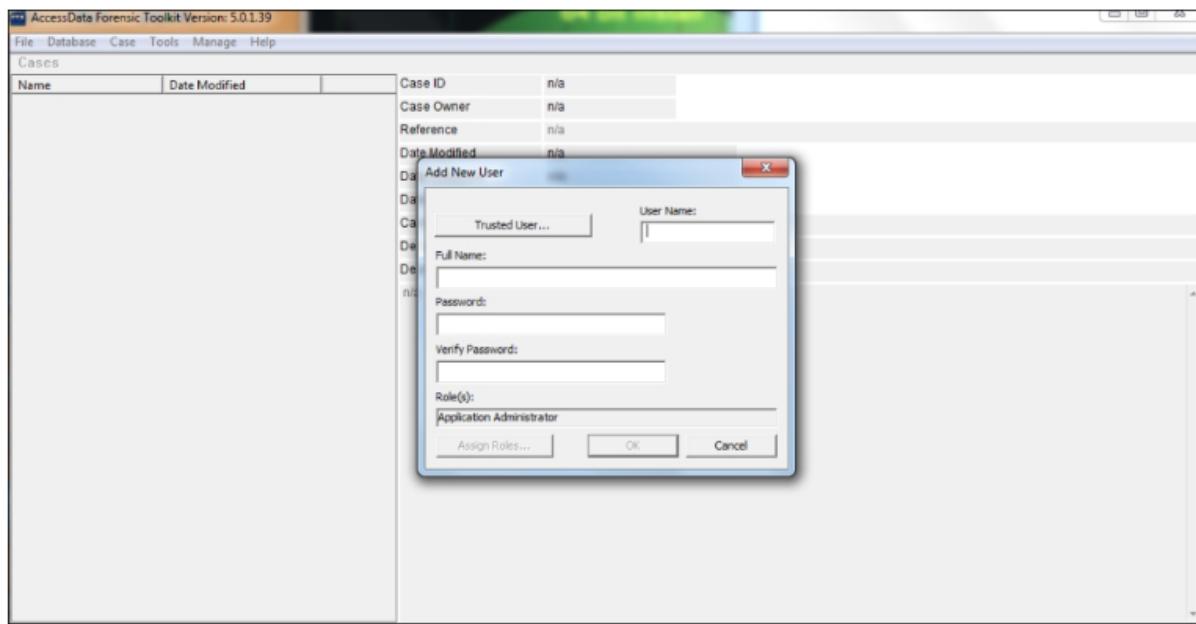
Code Meter: This is the USB Code Meter hardware driver and management component.

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:

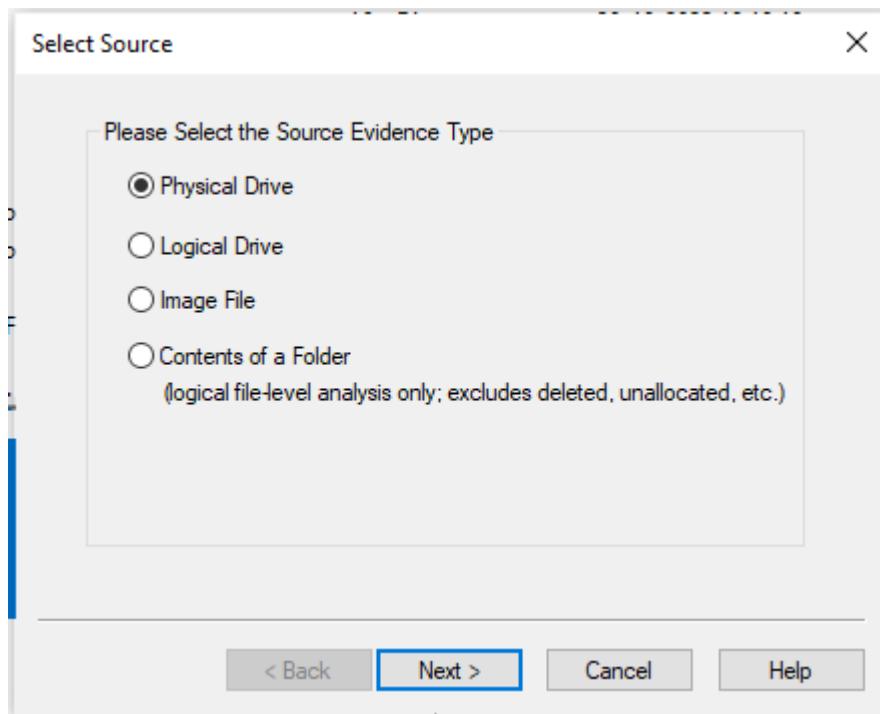
Forensic Toolkit (FTK) computer forensics software that can be used to acquire, preserve, analyze, and present computer evidence. FTK presents computer evidence by creating a case report and case log to document the evidence and investigation results. This uses the Report Wizard to create and modify 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.

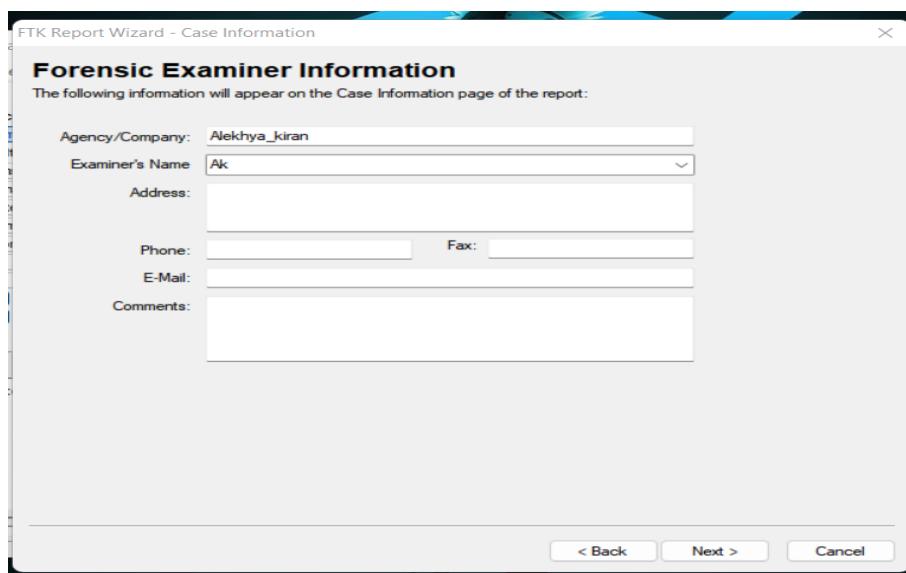
Adding and previewing an evidence Item

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 FTKlog 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

- | | |
|--|--|
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> Error messages | Events related to any error conditions encountered during the case. |
| <input checked="" type="checkbox"/> Bookmarking events | Events related to the addition and modification of bookmarks. |
| <input checked="" type="checkbox"/> Searching events | Events related to searching. All search queries and resulting hit counts will be recorded. |
| <input checked="" type="checkbox"/> Data carving / Internet searches | Events related to special data carving or internet keyword searches that are performed during the case. |
| <input checked="" type="checkbox"/> 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.

- | | |
|---|---|
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> 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) |
| <input checked="" type="checkbox"/> 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. |
| <input checked="" type="checkbox"/> HTML File Listing | Create an HTML version of the File Listing. |
| <input checked="" type="checkbox"/> 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 |
| <input checked="" type="checkbox"/> 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: | Encryption Status: | Email Status: |
| <input type="radio"/> Deleted | <input type="radio"/> Encrypted | <input type="radio"/> From email |
| <input type="radio"/> Not deleted | <input type="radio"/> Not encrypted | <input type="radio"/> Not from email |
| <input checked="" type="radio"/> Either | <input checked="" type="radio"/> Either | <input checked="" type="radio"/> Either |
| <input checked="" type="checkbox"/> Include Duplicate Files | | <input checked="" type="checkbox"/> OLE Streams |

File Type Criteria

- | | |
|--|---|
| <input checked="" type="checkbox"/> Documents | <input checked="" type="checkbox"/> Executables |
| <input checked="" type="checkbox"/> Spreadsheets | <input checked="" type="checkbox"/> Archives |
| <input checked="" type="checkbox"/> Databases | <input checked="" type="checkbox"/> Folders |
| <input checked="" type="checkbox"/> Graphics | <input checked="" type="checkbox"/> Other Known |
| <input checked="" type="checkbox"/> Multimedia | <input checked="" type="checkbox"/> Unknown |
| <input checked="" type="checkbox"/> Email msgs | |

 < Back Next > Cancel

Refine Index - Default

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

- 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.)

Conditionally Index

Index other items in the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

- | | | |
|---|---|---|
| Deletion Status: | Encryption Status: | Email Status: |
| <input type="radio"/> Deleted | <input type="radio"/> Encrypted | <input type="radio"/> From email |
| <input type="radio"/> Not deleted | <input type="radio"/> Not encrypted | <input type="radio"/> Not from email |
| <input checked="" type="radio"/> Either | <input checked="" type="radio"/> Either | <input checked="" type="radio"/> Either |
- Include Duplicate Files OLE Streams

File Type Criteria

- | | |
|--|---|
| <input checked="" type="checkbox"/> Documents | <input checked="" type="checkbox"/> Executables |
| <input checked="" type="checkbox"/> Spreadsheets | <input checked="" type="checkbox"/> Archives |
| <input checked="" type="checkbox"/> Databases | <input checked="" type="checkbox"/> Folders |
| <input checked="" type="checkbox"/> Graphics | <input checked="" type="checkbox"/> Other Known |
| <input checked="" type="checkbox"/> Multimedia | <input checked="" type="checkbox"/> Unknown |
| <input checked="" type="checkbox"/> Email msgs | |

< Back

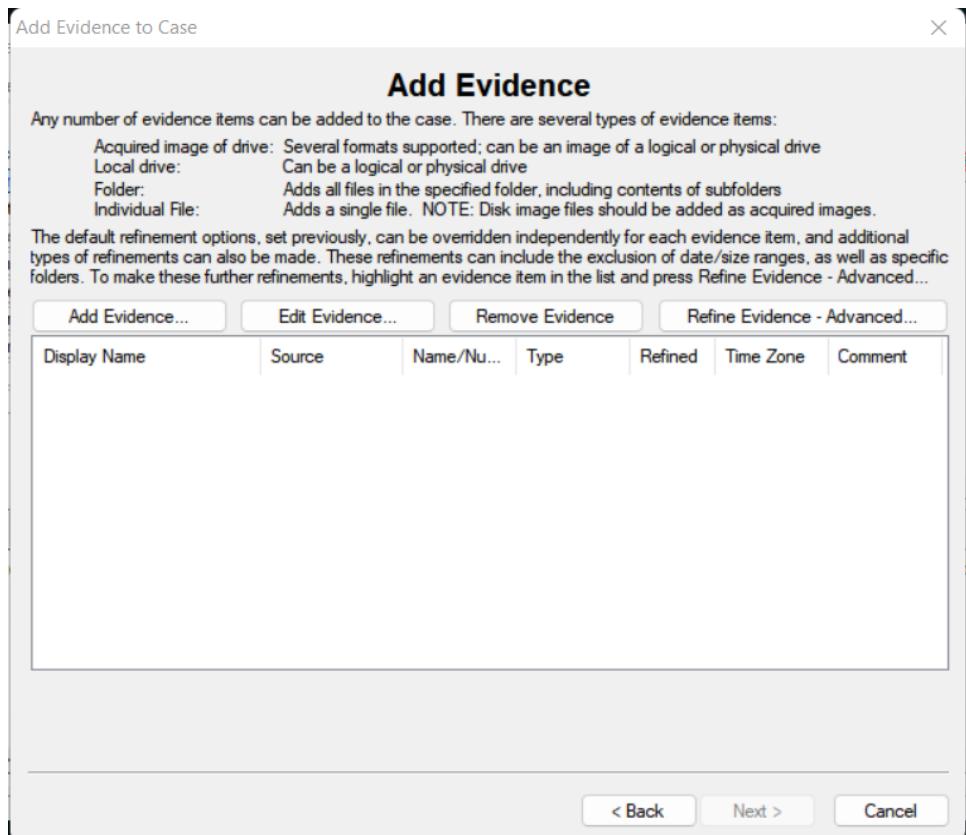
Next >

Cancel

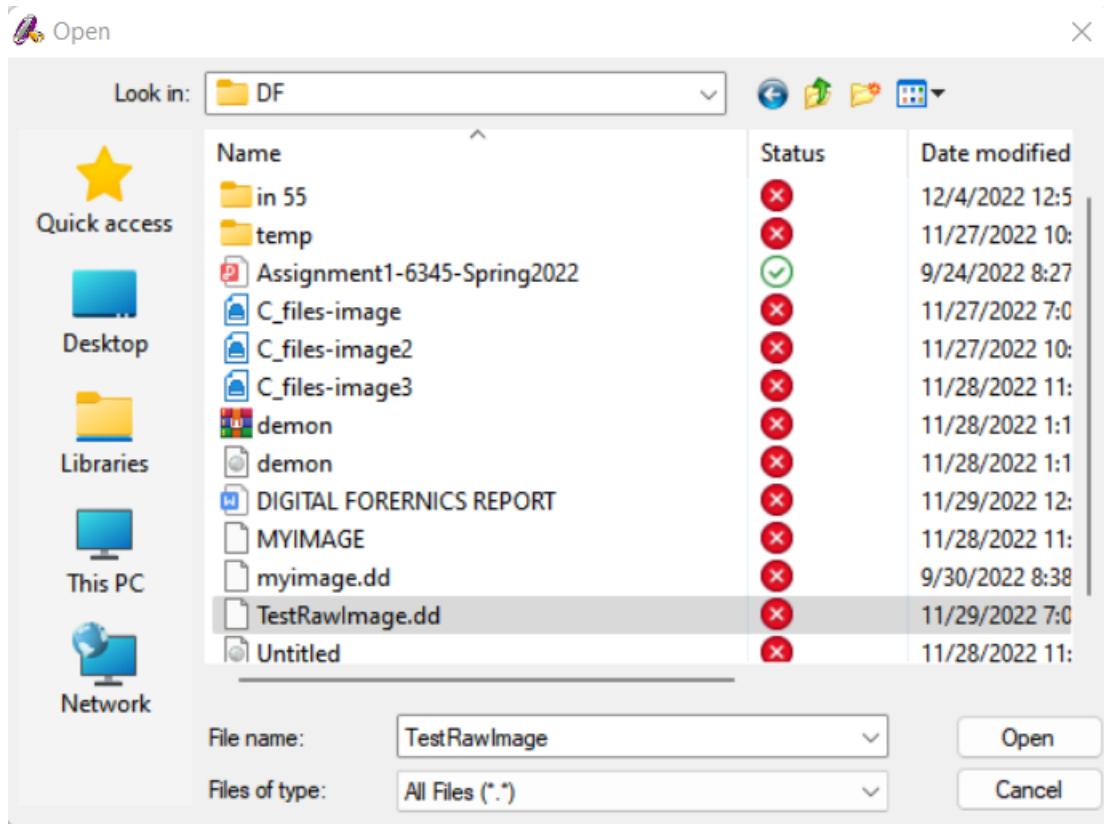
ADD EVIDENCE:

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:

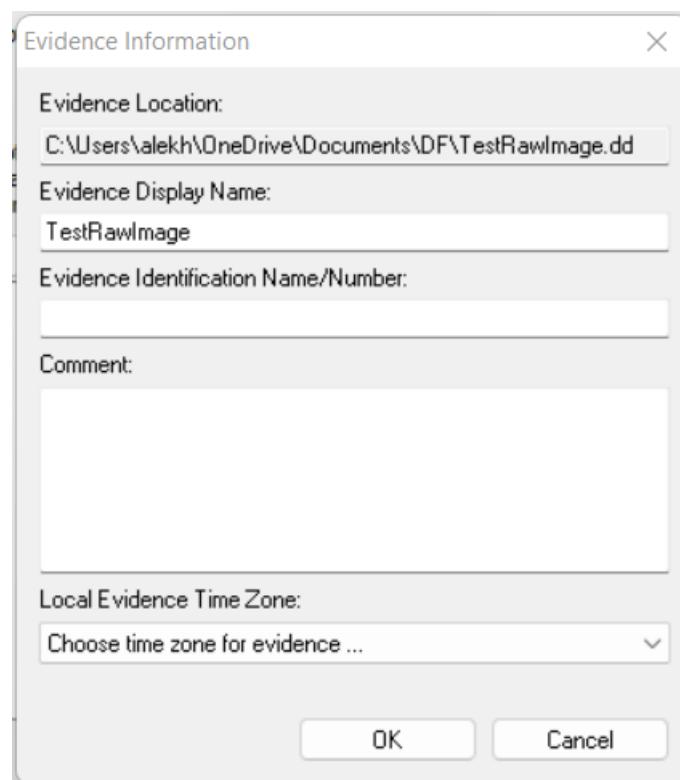
The correct use of the Time Zone feature is of the utmost importance for computer forensics because it might reflect the wrong

MAC time of files contained in the evidence, making a professional use the wrong information in an investigation report.

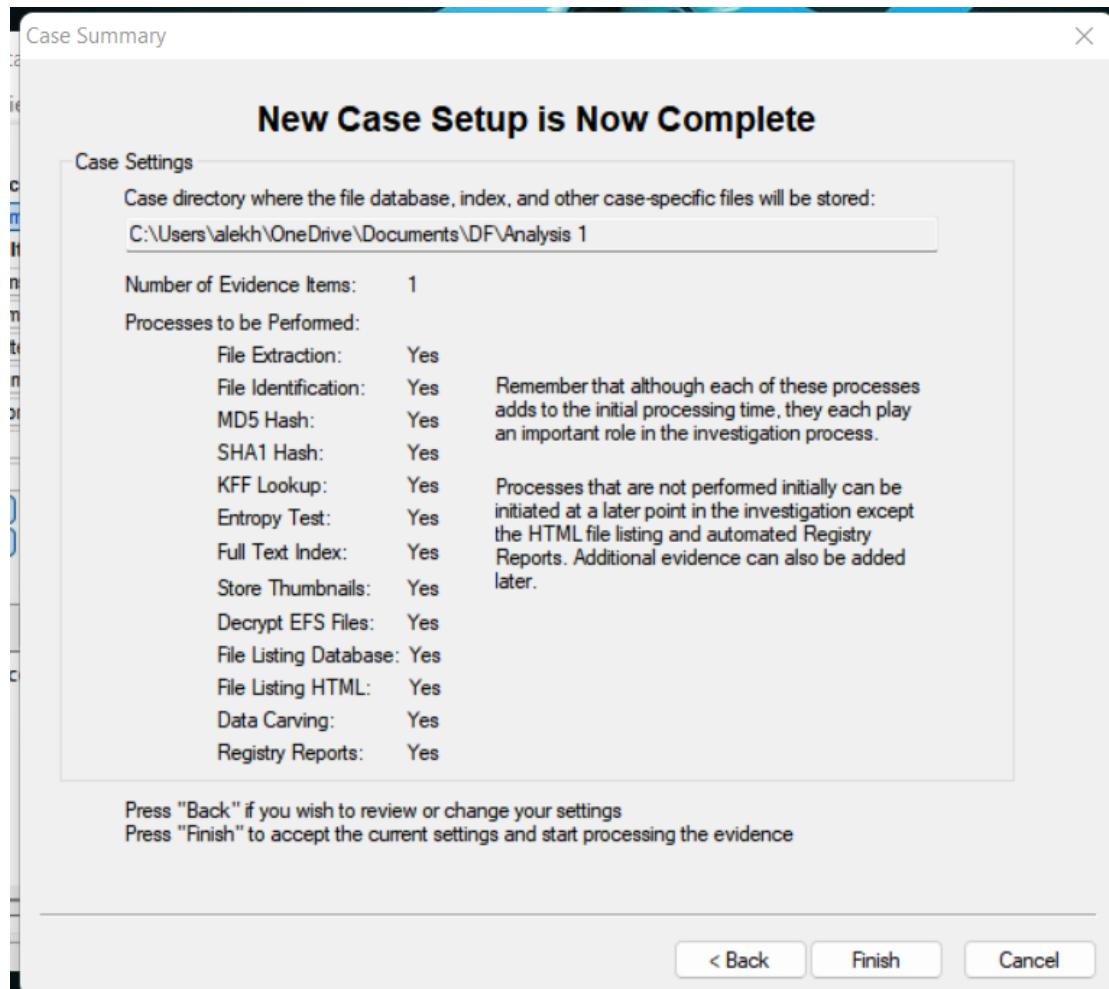
Based on this, you must configure the time zone to reflect the location where the evidence was acquired. For example, if you conducted the acquisition of a computer that was located in Los Angeles, US, and bring the evidence to Sao Paulo, Brazil, where your lab is situated, you should adjust the time zone to Los Angeles

so that the MAC time of files can reflect the actual moment of its modification, alteration, or creation.

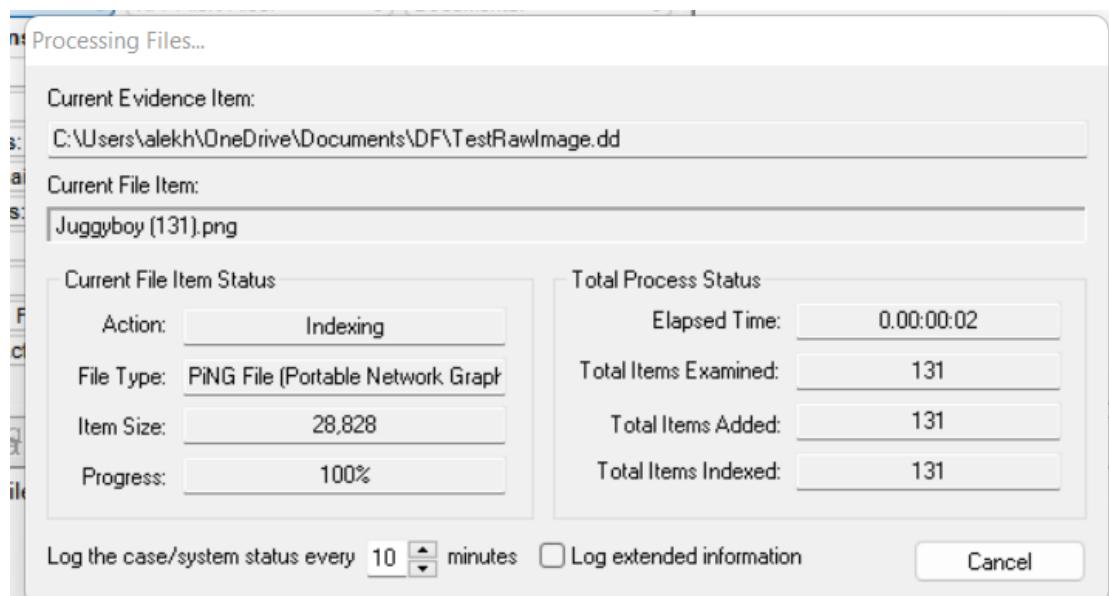
The FTK allows you to make that time zone change at the same time that you add a new evidence to the case. Select the time zone of the evidence where it was seized from the drop-down list in the Time Zone field. This is required to add evidence in the case.



NEW CASE SETUP IS NOW COMPLETED:



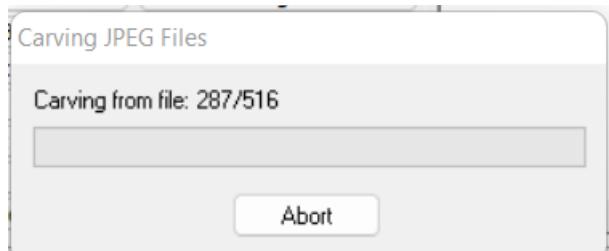
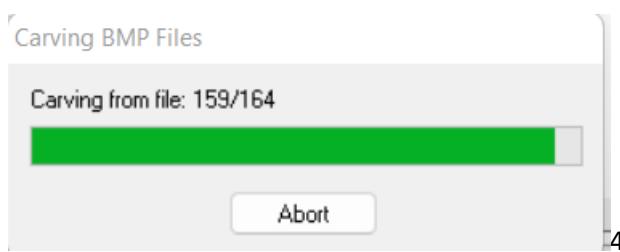
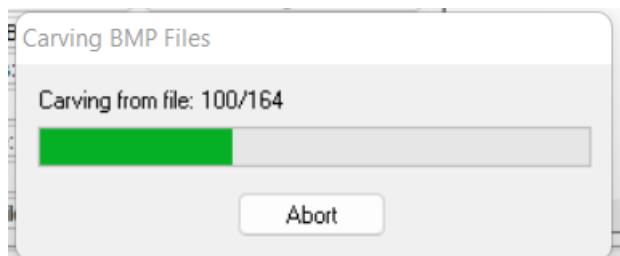
ANALYZE ALL THE FILES IN THE TestRawImage.dd



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.



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

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE Subitems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9

File Icons: OFF Unfiltered All Columns dtz

Evidence File Name	Evidence Path	Display Name	Identification Name/Number	Evidence Type
TestRawImage.dd	C:\Users\alekh\OneDrive\Documents\DF	TestRawImage\...		FAT16

1 Listed 0 Checked Total 0 Highlighted

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE Subitems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9

File Icons: OFF Unfiltered All Columns dtz

File Name	Full Path	Recycle Blk.	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children	Descre...	Enc	Del
ab1.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:00 PM	7/29/2010 6:02:10 PM	9/23/2011 12:00:00	10,862	16,384	0	0	Y	0	Y
ab2.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:00 PM	7/29/2010 6:01:02 PM	9/23/2011 12:00:00	24,709	32,768	0	0	Y	0	Y
ab3.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:00 PM	8/6/2010 4:22:35 PM	9/23/2011 12:00:00	7,349	16,384	0	0	Y	0	Y
ab4.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:08 PM	8/6/2010 4:23:38 PM	9/23/2011 12:00:00	7,026	16,384	0	0	Y	0	Y
ab5.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:10 PM	7/29/2010 12:30:16	9/23/2011 12:00:00	12,428	16,384	0	0	Y	0	Y
ab6.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:10 PM	7/29/2010 12:30:16	9/23/2011 12:00:00	15,561	16,384	0	0	Y	0	Y
ab7.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:10 PM	7/29/2010 10:13:54	9/23/2011 12:00:00	18,155	32,768	0	0	Y	0	Y
ab8.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:00 PM	7/29/2010 4:59:34 PM	9/23/2011 12:00:00	5,102	16,384	0	0	Y	0	Y
ab9.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:00 PM	7/29/2010 4:51:42 PM	9/23/2011 12:00:00	10,380	16,384	0	0	Y	0	Y
ab10.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 4:53:08 PM	9/23/2011 12:00:00	8,896	16,384	0	0	Y	0	Y
ab11.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 4:54:24 PM	9/23/2011 12:00:00	17,666	32,768	0	0	Y	0	Y
ab12.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 4:55:00 PM	9/23/2011 12:00:00	12,362	16,384	0	0	Y	0	Y
ab13.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 4:58:09 PM	9/23/2011 12:00:00	13,931	16,384	0	0	Y	0	Y
ab14.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 4:58:24 PM	9/23/2011 12:00:00	13,822	16,384	0	0	Y	0	Y
ab15.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 4:59:58 PM	9/23/2011 12:00:00	16,293	16,384	0	0	Y	0	Y
ab16.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 5:01:16 PM	9/23/2011 12:00:00	13,145	16,384	0	0	Y	0	Y
ab17.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 5:27:44 PM	9/23/2011 12:00:00	19,123	32,768	0	0	Y	0	Y
ab18.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 5:30:01 PM	9/23/2011 12:00:00	9,400	16,384	0	0	Y	0	Y
ab19.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:12 PM	7/29/2010 2:02:54 PM	9/23/2011 12:00:00	3,125	16,384	0	0	Y	0	Y
ab20.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 3:03:52 PM	9/23/2011 12:00:00	14,851	16,384	0	0	Y	0	Y
ab21.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 3:12:02 PM	9/23/2011 12:00:00	6,925	16,384	0	0	Y	0	Y
ab22.png	TestRawImage\DD NAME FAT16\Move\Icon\...		png	PNG File (P...)	Graphic	9/23/2011 6:02:02 PM	7/29/2010 3:39:54 PM	9/23/2011 12:00:00	12,728	16,384	0	0	Y	0	Y

445 Listed 0 Checked Total 0 Highlighted

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

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE Subitems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
I-arrows.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
I-arrows.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
I-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!A.PNG	TestRawImage\NO NAME-FAT16\More Icons\...		PNG	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!ab.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!ab_1.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!abs.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!abul-1.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!abul-2.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM
!abul-3.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PING File (Po...	Graphic		9/23/2023 10:20:00 AM

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

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items					
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE Subitems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9



File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Sub
!rrow1.png	TestRawImage\NO NAME-FAT16\More Icons\!r...		png	PING File (Po...	Graphic	
!rrow2.png	TestRawImage\NO NAME-FAT16\More Icons\!r...		png	PING File (Po...	Graphic	
AlbumArt_{B5227ABE-07EF-4...	TestRawImage\NO NAME-FAT16\Love Aaj Kal\...		jpg	JPEG/JFIF File	Graphic	
AlbumArt_{B5227ABE-07EF-4...	TestRawImage\NO NAME-FAT16\Love Aaj Kal\...		jpg	JPEG/JFIF File	Graphic	
AlbumArtSmall.jpg	TestRawImage\NO NAME-FAT16\Love Aaj Kal\...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_0...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	
collage_over_image_page0_1...	TestRawImage\NO NAME-FAT16\juggyboy\Thu...		jpg	JPEG/JFIF File	Graphic	

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

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items					
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE Subitems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9

```
JFIF
%&()*456789:CDEFIGHIJSTUVWXYZcdefghijstuvwxyz
&(*56789:CDEFIGHIJSTUVWXYZcdefghijstuvwxyz
DF2i
JzF3
uk3epT
fsF1
Uic%Xn
oleyDl(
N8nGO
jUP0{
sWJ9P
7xbz)
OqRH
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Dat
256_50ca53757b162d98	TestRawImage\NO NAME-FAT16\Old Melodies\...			OLE Stream	Unknown	N/A	
256_6d374cc2ea0ce2e5	TestRawImage\NO NAME-FAT16\Love Aaj Kal\...			OLE Stream	Unknown	N/A	
256_718925419625264b	TestRawImage\NO NAME-FAT16\Old Melodies\...			OLE Stream	Unknown	N/A	
256_906faf7921d1d1ea	TestRawImage\NO NAME-FAT16\Old Melodies\...			OLE Stream	Unknown	N/A	

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

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE SubItems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9



File Name	Full Path	Recycle Bi...	Ext	File Type	Category
limond.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
limond1.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
lin.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
lin_1.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
link_.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
lirewall.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
lis.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
lite.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
llant.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
llant_1.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic
llass.png	TestRawImage\NO NAME-FAT16\More Icons\li...		png	PNG File (Po...	Graphic

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1990	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1066
Unchecked Items:	1990	From E-mail:	0	Multimedia:	103
Flagged Thumbnails:	0	Deleted Files:	445	E-mail Messages:	0
Other Thumbnails:	1066	From Recycle Bin:	0	Executables:	0
Filtered In:	1990	Duplicate Items:	140	Archives:	3
Filtered Out:	0	OLE SubItems:	4	Folders:	15
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	791
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	9

Cursor position = 0; cluster = 22913; physical sector = 733672

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Chk
DriveFreeSpace01	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace02	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace03	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace04	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace05	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace06	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace07	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace08	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	
DriveFreeSpace09	TestRawImage\NO NAME-FAT16\DriveFreeSpa...		Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	N/A	26.214.400	718.536.704	

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

NO NAME-FAT16

- juggyboy
- Kurban
- Love Aaj Kal
- More Icons
- No Problem
- Old Melodies
- Once Upon A Time In Mumbai
- Phas Gaye Re Obama
- Prince
- Ramaa - The Saviour
- ROBO Hindi
- Set of Images
- Shahrukh Bola Khoobsurat Hai Tu
- Singh Is King

Cursor position = 0; cluster = 37989; physical sector = 1216104

All Columns

File Name	FullPath	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
Babu Rao.mp3	TestRawImage\NO NAME-FAT16\Once Upon A...		mp3	MP3, MPEG ...	Multimedia		9/23/2011 6:07:04 PM	6/30/2010 6:56:04 AI
I Am In Lov.mp3	TestRawImage\NO NAME-FAT16\Once Upon A...		mp3	MP3, MPEG ...	Multimedia		9/23/2011 6:07:08 PM	6/30/2010 6:56:06 AI
I In Love.mp3	TestRawImage\NO NAME-FAT16\Once Upon A...		mp3	MP3, MPEG ...	Multimedia		9/23/2011 6:07:10 PM	6/30/2010 6:56:04 AI
Parda.mp3	TestRawImage\NO NAME-FAT16\Once Upon A...		mp3	MP3, MPEG ...	Multimedia		9/23/2011 6:07:12 PM	6/30/2010 6:56:04 AI
Pee Loon.mp3	TestRawImage\NO NAME-FAT16\Once Upon A...		mp3	MP3, MPEG ...	Multimedia		9/23/2011 6:07:14 PM	6/30/2010 6:56:04 AI
Tum Jo Aaye.mp3	TestRawImage\NO NAME-FAT16\Once Upon A...		mp3	MP3, MPEG ...	Multimedia		9/23/2011 6:07:16 PM	6/30/2010 6:56:04 AI

SET OF IMAGES ARE DISPLAYED IN GRAPHICS

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Case TestRawImage

NO NAME-FAT16

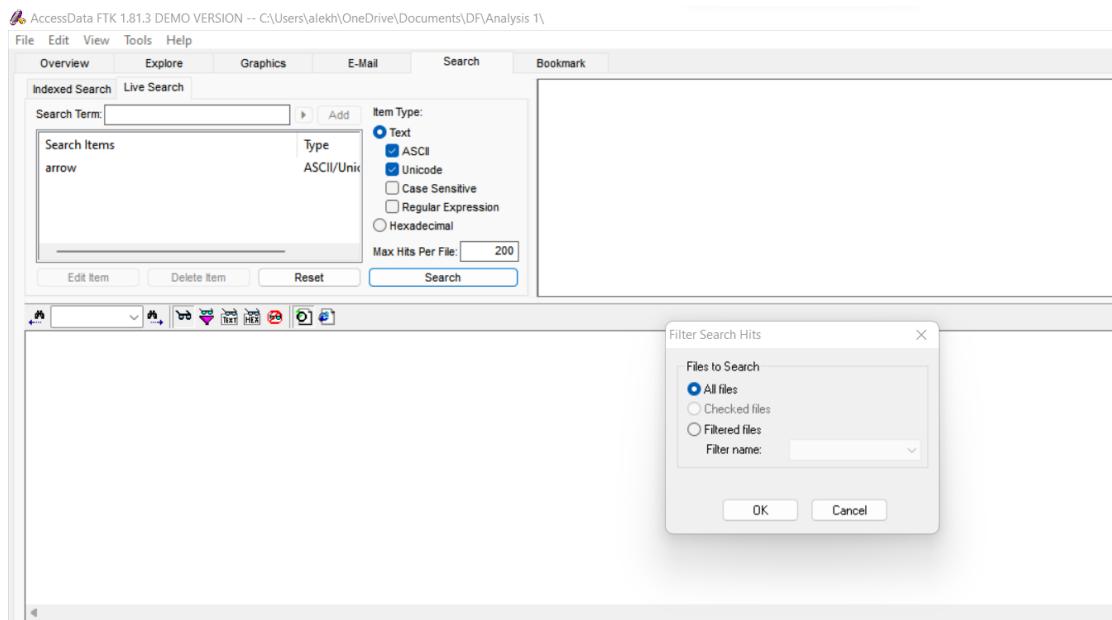
- juggyboy
- Kurban
- Love Aaj Kal
- More Icons
- No Problem
- Old Melodies
- Once Upon A Time In Mumbai
- Phas Gaye Re Obama
- Prince
- Ramaa - The Saviour
- ROBO Hindi

1 316 Total Flagged items: 0

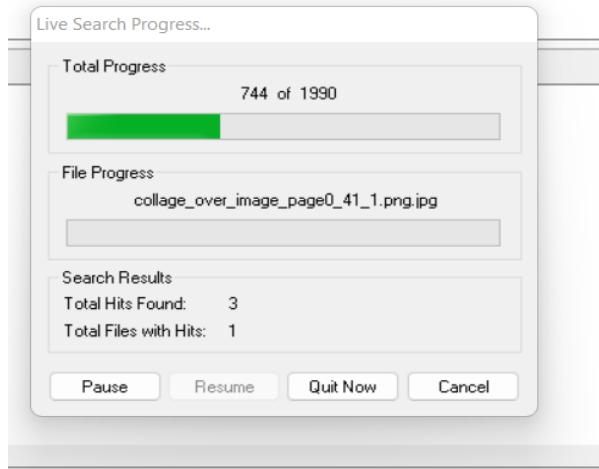
All Columns

File Name	FullPath	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children	Descen...	Enc	Del
arrows.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/30/2010 5:02:10 PM	9/23/2011 12:00:00...	10,952	16,394	0	0	Y	
arrows.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/30/2010 5:01:02 PM	9/23/2011 12:00:00...	24,709	32,768	0	0	Y	
arrows.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	8/6/2010 4:22:36 PM	9/23/2011 12:00:00...	7,349	16,394	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	8/6/2010 4:22:36 PM	9/23/2011 12:00:00...	7,326	16,384	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/29/2010 10:26:16...	9/23/2011 12:00:00...	12,429	16,394	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:10 PM	7/29/2010 10:13:12...	9/23/2011 12:00:00...	15,881	16,394	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:10 PM	7/30/2010 10:13:54...	9/23/2011 12:00:00...	19,156	32,768	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/29/2010 4:50:34 PM	9/23/2011 12:00:00...	6,102	16,394	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/29/2010 4:47:42 PM	9/23/2011 12:00:00...	10,389	16,384	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/29/2010 4:45:30 PM	9/23/2011 12:00:00...	8,936	16,384	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/29/2010 4:54:24 PM	9/23/2011 12:00:00...	17,985	32,768	0	0	Y	
l-screens.png	TestRawImage\NO NAME-FAT16\More Icons\...		png	PNG File [Po...	Graphic		9/23/2011 6:02:00 PM	7/29/2010 4:55:30 PM	9/23/2011 12:00:00...	12,252	16,384	0	0	Y	

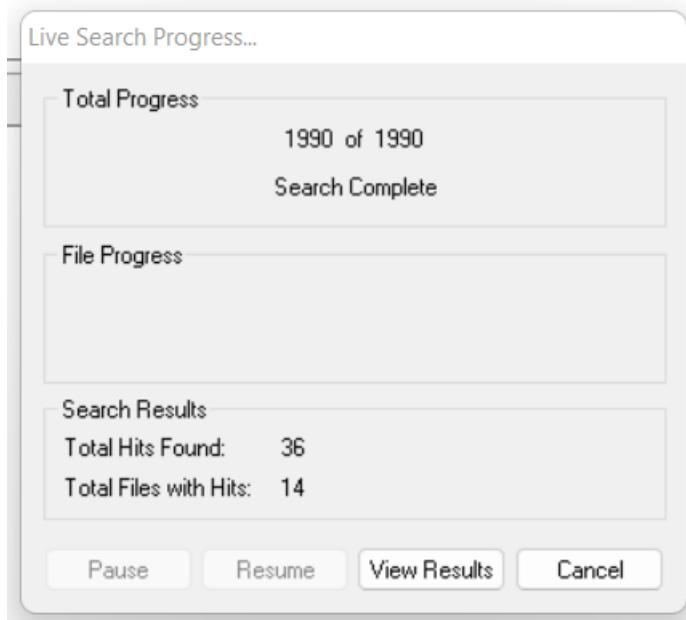
WE CAN SEARCH ITEMS BY WRITING SEARCH TERMS (WE CAN SELECT THE ITEM TYPE ALSO)



ANALYZING ALL THE FILES (FOR LIVE SEARCH PROGRESS)



TOTAL COUNT OF THE FILES:



RESULTS FOR LIVE SEARCH :

AccessData FTK 1.8.1.3 DEMO VERSION -- C:\Users\alekh\OneDrive\Documents\DF\Analysis 1\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search: Live Search

Search Term: Add Item Type: Text ASCII Unicode Case Sensitive Regular Expression Hexadecimal

Max Hits Per File:

Search

Search Performed 12/5/2022 8:17:26 PM -- 36 Hits in 14 Files

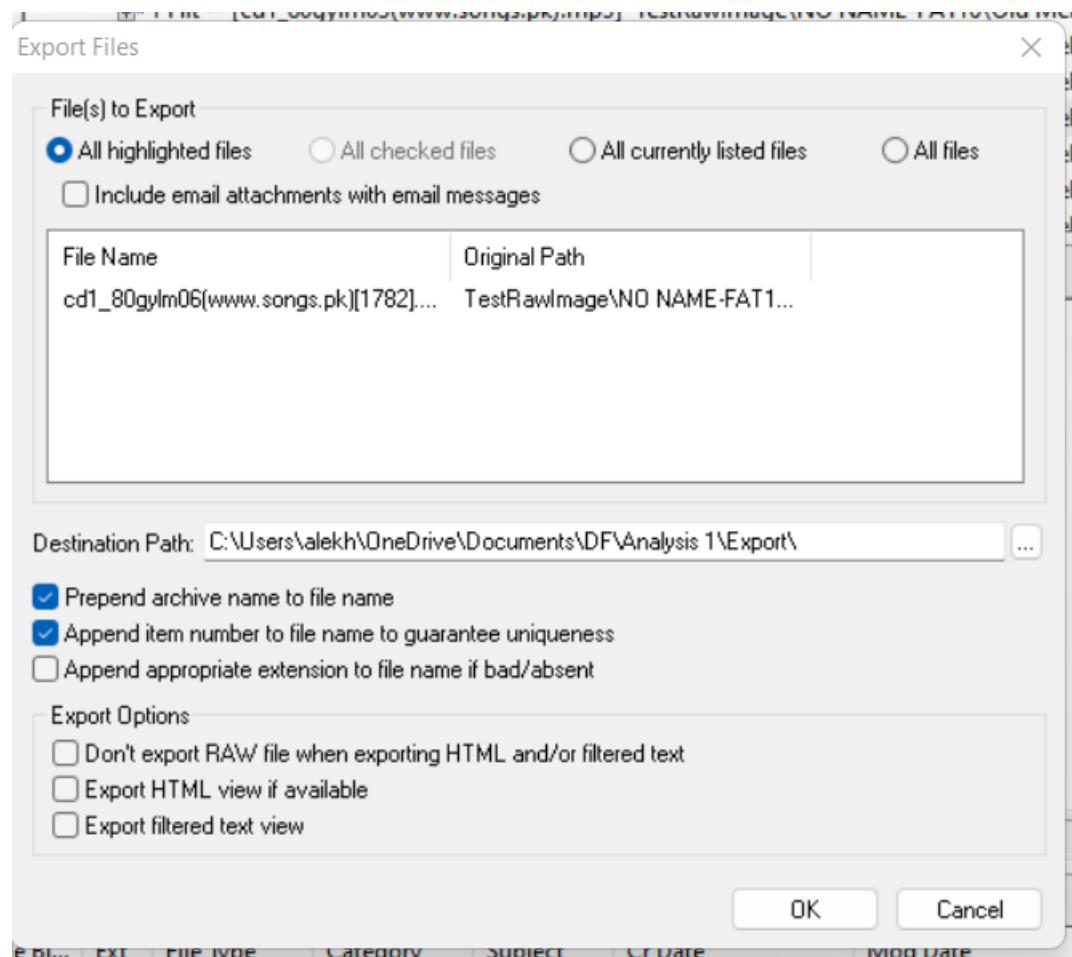
Query: "arrow" <ASCII/Unicode, Case Insensitive> -- 36 Hits in 14 Files

- ④ 3 Hits -- [More icons] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym01\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym02\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym03\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym03\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym04\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym04\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym05\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym05\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym06\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym06\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym07\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym07\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym08\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym08\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym09\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym09\www.songs.pk\mp3
- ④ 1 Hit -- [cd1_80gym09\www.songs.pk.mp3] TestRawImage\NO NAME=FAT16\Old Melodies\cd1_80gym09\www.songs.pk\mp3

File Name	Full Path	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children	Descen...	Enc
cd1_80gym01\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/22/2011 6:05:55 PM	1/17/2010 8:00:28	9/22/2011 12:00:00	5,800,112	5,800,112	0	0	Y
cd1_80gym02\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/22/2011 6:05:55 PM	1/17/2010 8:00:24	9/22/2011 12:00:00	5,634,844	5,634,844	0	0	Y
cd1_80gym03\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/22/2011 6:05:55 PM	1/17/2010 8:01:04	9/22/2011 12:00:00	6,912,988	6,914,048	0	0	Y
cd1_80gym04\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/22/2011 6:06:00 PM	1/17/2011 3:46:00 PM	9/22/2011 12:00:00	9,362,151	9,371,648	0	0	Y
cd1_80gym05\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/22/2011 6:06:02 PM	1/17/2010 8:02:02	9/23/2011 12:00:00	8,195,307	8,195,222	0	0	Y
cd1_80gym06\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/23/2011 6:06:04 PM	1/17/2010 8:02:56	9/23/2011 12:00:00	7,305,109	7,307,264	0	0	Y
cd1_80gym07\www.songs.pk...	TestRawImage\NO NAME=FAT16\Old Melodie...	mp3	MP3, MPEG ...	Multimed...		9/23/2011 6:06:06 PM	1/31/2011 3:59:26 PM	9/23/2011 12:00:00	11,606,529	11,616,256	0	0	Y

BY SELECTING EXPORT FILE OF SEARCH RESULT:

WE CAN SELECT THE OPTION (ALL HIGHLIGHTED FILES)



The screenshot shows a Windows File Explorer interface. The left sidebar displays a navigation tree with categories like 'Quick access', 'OneDrive - Personal', 'This PC', and 'Network'. The 'Documents' folder under 'This PC' is currently selected. The main pane shows a list of files and folders within the 'Analysis 1' folder. The columns are 'Name', 'Status', 'Date modified', 'Type', and 'Size'. The 'Status' column contains red circular icons with white minus signs. The 'Type' column indicates file types such as 'File folder', 'Microsoft Access ...', 'FTK File', 'DAT File', 'IDX File', and 'Configuration setti...'. The 'Size' column shows file sizes like 288 KB, 1 KB, and 1,024 KB.

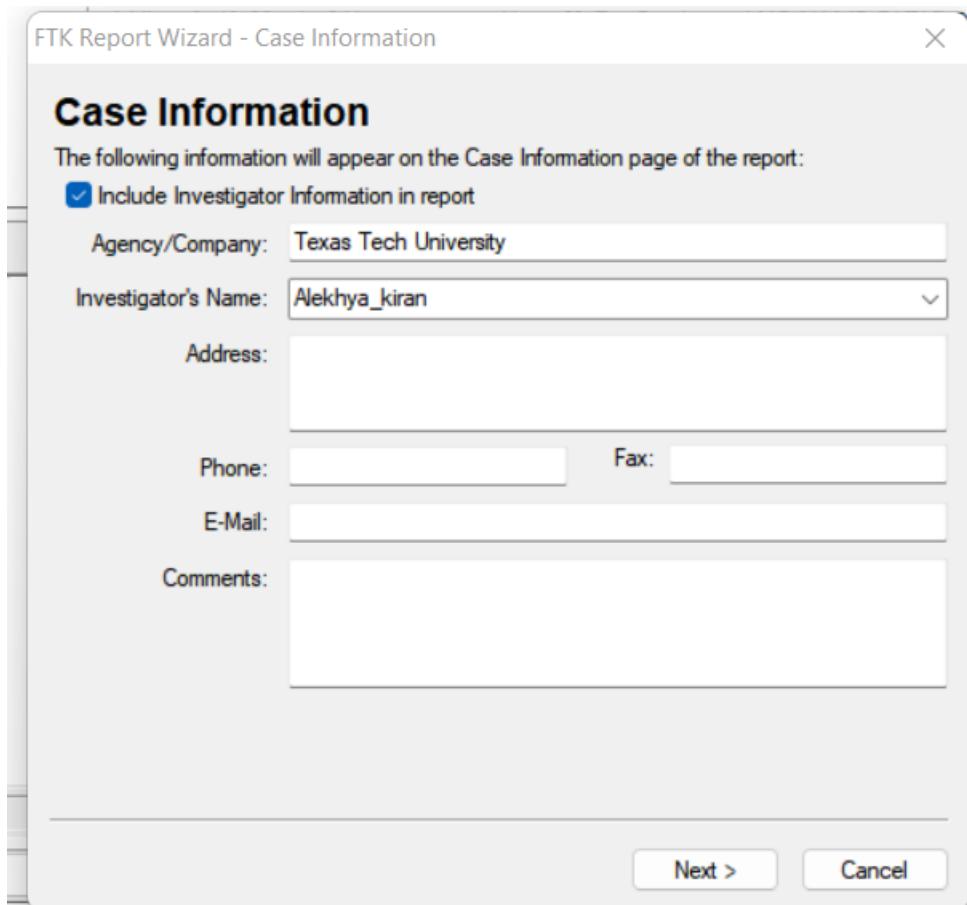
Name	Status	Date modified	Type	Size
Cache	✖	12/5/2022 8:11 PM	File folder	
CrvTbldx	✖	12/5/2022 8:11 PM	File folder	
efs	✖	12/5/2022 8:09 PM	File folder	
Export	⟳	12/5/2022 8:23 PM	File folder	
index	✖	12/5/2022 8:10 PM	File folder	
Thumbldx	✖	12/5/2022 8:09 PM	File folder	
AccessDatabase	✖	12/5/2022 8:11 PM	Microsoft Access ...	288 KB
Analysis 1.ftk	✖	12/5/2022 8:08 PM	FTK File	1 KB
bfm.dat	⟳	12/5/2022 8:08 PM	DAT File	1,024 KB
bfm.idx	⟳	12/5/2022 8:08 PM	IDX File	1,024 KB
bookmark.dat	⟳	12/5/2022 8:08 PM	DAT File	1,024 KB
bookmark.idx	⟳	12/5/2022 8:08 PM	IDX File	1,024 KB
case.dat	⟳	12/5/2022 8:10 PM	DAT File	1,024 KB
case.idx	⟳	12/5/2022 8:09 PM	IDX File	1,024 KB
case		12/5/2022 8:09 PM	Configuration setti...	1 KB
evidence.dat		12/5/2022 8:10 PM	DAT File	1,024 KB
evidence.idx		12/5/2022 8:09 PM	IDX File	1,024 KB
extract.dat		12/5/2022 8:10 PM	DAT File	1,024 KB
extract.idx		12/5/2022 8:10 PM	IDX File	1,024 KB

FOR REPORT WIZARD:

STEP TP STEP SNAPSHOTS ARE ATTACHED :

SELECTING REPORT WIZARD:

File	Edit	View	Tools	Help	Search	Bookmark									
New Case...					Search										
Open Case...						Search Performed 12/5/2022 8:17:26 PM -- 36 Hits in 14 Files									
Add Evidence...						Query: "arrow" < ASCII/Unicode, Case Insensitive > 36 Hits in 14 Files									
FTK Imager...						↳ 3 Hits -- [More icons] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym01\www.songs.pk.mp3									
Disk Viewer...						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym02\www.songpk.mp3									
Registry Viewer...						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym03\www.songpk.mp3									
Close Case						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym04\www.songpk.mp3									
Save Case						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym05\www.songpk.mp3									
Backup Case...						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym06\www.songpk.mp3									
Export Files...						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym07\www.songpk.mp3									
Report Wizard...						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym08\www.songpk.mp3									
Update Report						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym09\www.songpk.mp3									
View Report...						↳ 1 Hit -- [cd1_80gym01\www.songs.pk.mp3] TestRawImage\NO NAME-FAT10\Old Melodies\cd1_80gym10\www.songpk.mp3									
Exit															
C:\Users\alekh\OneDrive\Documents\DF\investigate11															
C:\Users\alekh\OneDrive\Documents\DF\investigate10															
C:\Users\alekh\OneDrive\Documents\DF\investigating03															
C:\Users\alekh\OneDrive\Documents\DF\investigating01															
00000d 00 00 35 00 00 01 ff fe=fc 00 01 7d 00 74 00 61 00															
00000d 20 00 20 00 20 00 20-38 00 30 00 20 00 47 00															
00000d 60 00 44 ff 72 00 69 ee=ff 02 00 71 00 70 00 20 00 1-e-0-1-0-0															
00001d 59 00 65 00 61 00 72 00-73 00 54 59 45 52 00 00 Y=e-a-z TYER -															
Current position = 0, cluster = 32195, physical sector = 103096															
					All Columns	b72									
File Name	Full Path	Recycle Bl...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children	Descen...	Enc	Del
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		11/2/2010 6:05 PM	11/2/2010 8:00 ...	11/2/2011 12:00:00	5,978,121	5,980,160	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		3/2/2011 6:05 PM	11/7/2010 8:00 ...	9/22/2011 12:00:00	7,650,574	7,653,444	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		3/2/2011 6:05 PM	11/7/2010 8:00 ...	9/22/2011 12:00:00	5,912,151	5,917,648	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		9/22/2011 6:06 PM	1/3/2011 3:45:00 PM	9/22/2011 12:00:00	3,362,151	3,371,648	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		9/22/2011 6:06 PM	1/3/2011 3:45:00 PM	9/22/2011 12:00:00	8,195,307	8,159,232	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		9/22/2011 6:06 PM	1/12/2010 8:02:00	9/22/2011 12:00:00	7,305,109	7,307,264	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		9/22/2011 6:06 PM	11/12/2010 8:03:55	9/23/2011 12:00:00	0	0	0	0	Y	
	TestRawImage\NO NAME-FAT10\Old Melodie...		mp3	MPEG-3	Multimedia		9/23/2011 6:06 PM	1/31/2011 3:59:26 PM	9/23/2011 12:00:00	11,605,529	11,616,256	0	0	Y	



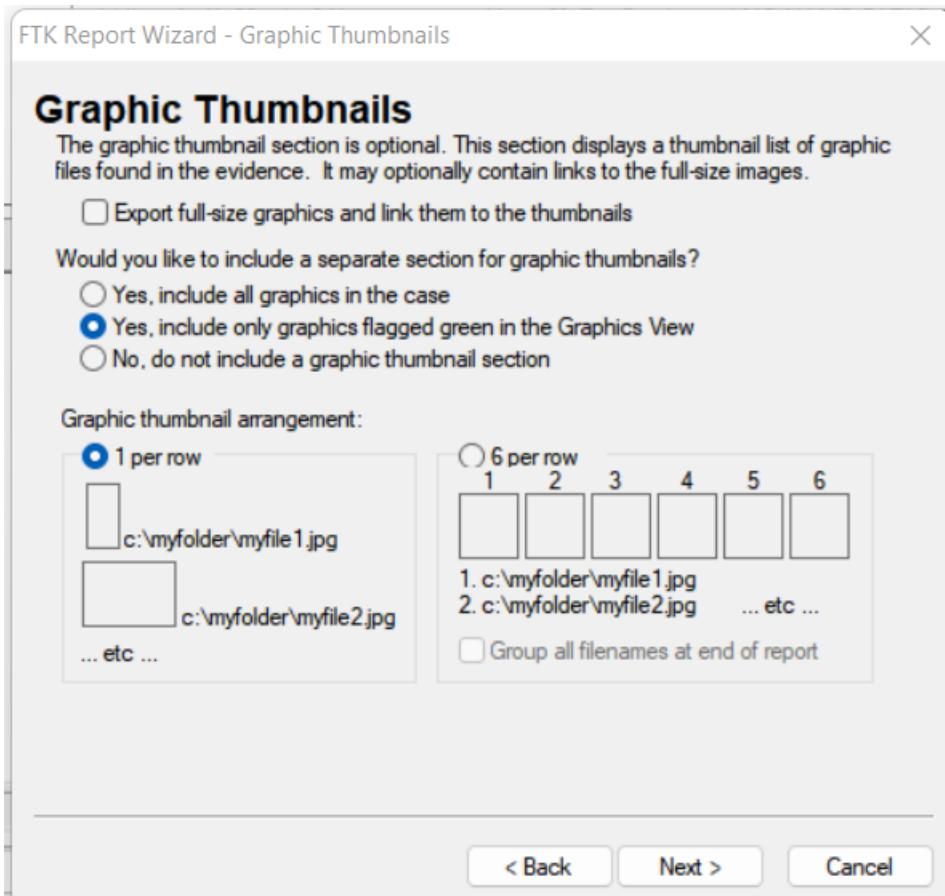
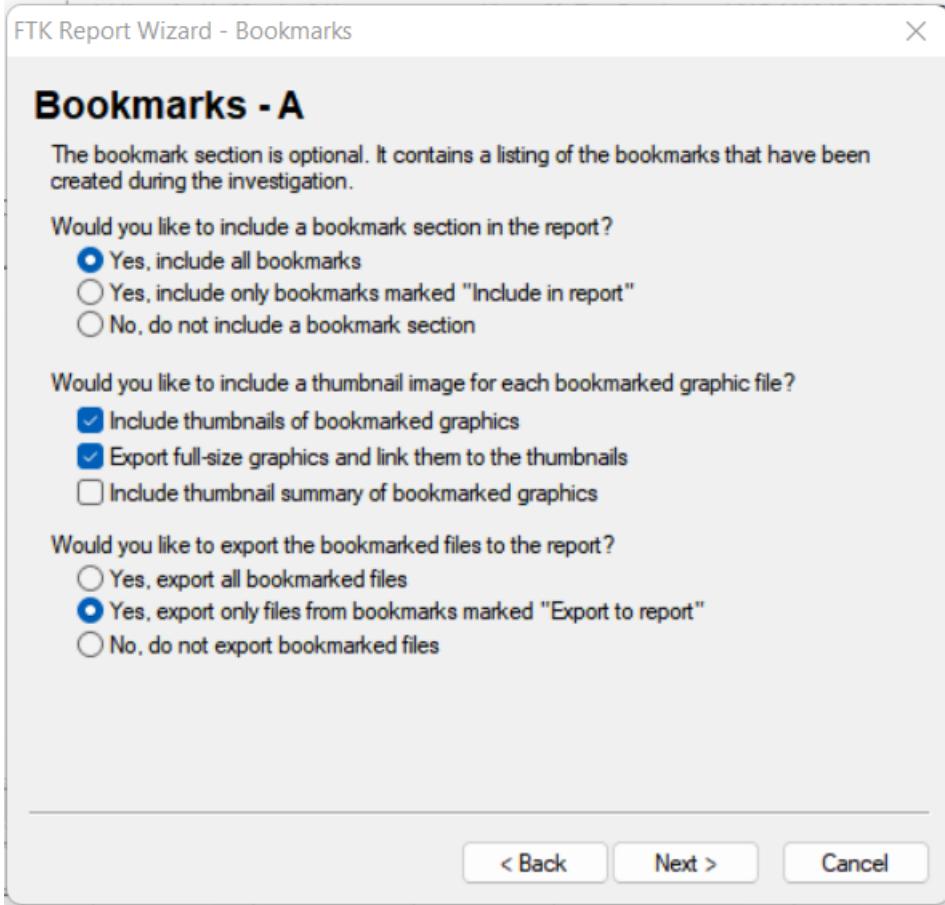
BOOKMARK FOR THE REPORT:

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:



LISTING BY FILE PATH:

FTK ReportWizard - List by File Path

List by File Path

The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.

Include a list by file path section in the report

Categories of lists that can be included:

List Category	Include	Export
All Items	no	no
KFF Alert Files	no	no
Bad Extension	no	no
Encrypted Files	no	no
Emailed Items	no	no
Deleted Files	no	no
Recycled Files	no	no
Duplicate Items	no	no
Flagged Ignore	no	no
KFF Ignorable	no	no

To add or remove a list category from the report, select the category and then change the settings below.

Selected Category Settings:

Include in the report
 Export to the report
 Apply a file filter to the list

Filter name:

Example:

```
C:
· myfolder
· · myfile1.jpg
· · mysubfolder
· · · myfile2.jpg
```

< Back Next > Cancel

List File Properties - A

The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.

Include a list file properties section in the report

Include MS Access database in report

Categories of lists to be included in the report:

List Category	Include	Export
All Items	no	no
KFF Alert Files	no	no
Bad Extension	no	no
Encrypted Files	no	no
Emailed Items	no	no
Deleted Files	no	no
Recycled Files	no	no
Duplicate Items	no	no
Flagged Ignore	no	no
KFF Ignorable	no	no

To add or remove a list category from the report, select the category and then change its settings below.

Selected Category Settings:

Include in the report

Export to the report

Apply a file filter to the list

Filter name:

Example:

File: myfile1.jpg
Path: C:\myfolder
File Type: JPEG/JFIF File
Category: Graphic
L-Size: 37942

< Back

Next >

Cancel

INCLUDING ALL CASE LOG AND HTML FILE LISTING

Supplementary Files

You can add your own files to the report by including them in the list below. Any type of file can be included. The file will be copied and hyperlinked to the report.

Supplementary Files:

[Add Files](#)[Remove File](#)

Filename

Link name

Check here if you want the case log included in the report. The case log contains a log of many of the events that occur during the course of a case.

- Include Case Log in report
- Include HTML File Listing from preprocessing

[< Back](#)[Next >](#)[Cancel](#)

REPORT LOCATION :

Report Location

FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.

NOTE 1: If you select an existing folder (other than the default), it must be empty.

NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.

NOTE 3: If you are expecting to copy this report to recordable media, remember:
CDR = 650MB, DVDR = 4.5GB

Report folder:

C:\Users\alekh\OneDrive\Documents\DFV\Analysis 1\report\

Export all files using actual filenames (may cause broken links on CDs or DVDs)

Include Registry Viewer reports

Custom graphic for the report (recommended maximum width is 183 pixels)

Report language:

English

< Back

Finish

Cancel

SELECTING TO VIEW THE REPORT:



Do you wish to view the report?

Yes

No

CASE INFORMATION OF DISK IMAGE:

← → ⌂ File | C:/Users/alekh/OneDrive/Documents/DF/Analysis%201/report/index.htm

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 Alekhyakiran
Address
Phone
Fax
E-mail
Comments

Investigator Alekhyakiran
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	Fr
	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 juggboy		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.ls.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/JIF 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/JIF File	11 12:43:10 PM	9/23/2011 11 10:23:22 AM		47060			Graphic			
	25	NO NAME-FAT1 Flowers.jpg		JPEG/JIF File	11 12:43:10 PM	9/23/2011 011 6:23:54 PM		51974			Graphic			
	26	NO NAME-FAT1 Horse.jpg		JPEG/JIF 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

AccessData Forensic Toolkit®



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®

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 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 Exec Path: C:\Program Files (x86)\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 -- FTK 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
Prerendered Thumbnails: Yes
File Listing Database: Yes
HTML File Listing: Yes
Data Carving: Yes
Preprocess Registry Files: Yes
Decompile EPL 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
```

