UNIVERSITY OF CALICUT

CENTRE FOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Dr. JOHN MATTHAI CENTRE

ARANATTUKARA, THRISSUR

PIN-680618

TERM PAPER REPORT

ON

RETRIVAL OF DELETED FILE IN DIGITAL FORENSIC

MASTER OF COMPUTER APPLICATIONS(MCA)

Second Semester

TERM PAPER REPORT

ON

RETRIVAL OF DELETED FILE IN DIGITAL FORENSIC

Submitted in partial fulfillment of Second semester

MASTER OF COMPUTER APPLICATIONS

Submitted by

ABHIRAMI K.V

(JMAWMCA002)

UNIVERSITY OF CALICUT
CENTRE FOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

DR. JOHN MATTHAI CENTRE, ARANATTUKARA

THRISSUR-680618

MAY 2023

UNIVERSITY OF CALICUT

CENTRE FOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Dr. JOHN MATTHAI CENTRE

MASTER OF COMPUTER APPLICATIONS

CERTIFICATE

This is to certify that the seminar report entitled **"RETRIVAL OF DELETED FILE IN DIGITAL FORENSIC"** is a bonafide record of the work done by **ABHIRAMI K.V (JMAVMCA002)** during the academic year 2022 – 2023 towards the partial fulfillment of the requirements for the award of the degree of **MASTER OF COMPUTER APPLICATIONS (MCA)** of University of Calicut.

Mrs. REEMA K.R.
Guide
CCSIT, Dr. John Matthai Centre

Mrs. BINI P.B
Associate Coordinator
CCSIT, Dr. John Matthai Centre

DECLARATION

I, Abhirami K.V hereby declare that the seminar report entitled "RETRIVAL DELETED FILE IN DIGITAL FORENSIC" submitted to University of Calicut in partial fulfillment of the requirement for the award of the degree of Master of Computer Applications is an original work done by me under the guidance of Mrs. REEMA K.R., Assistant Professor of CCSIT, Dr. John Matthai Centre, Aranattukara, Thrissur.

Date: …. /…./……

ABHIRAMI K.V

RETRIVAL OF DELETED FILE IN DIGITAL FORENSIC

Abhirami KV

Second Semester MCA

Dr.John Mathai centre Aranattukara, Thrissur

abhiramikv05@gmail.com

ABSTRACT: **Retrieving deleted files is a common task in digital forensic, and forensic toolkit offer a variety of methods for accomplishing this. The recovery is performed on files that have been deleted from a file system. FTK Imager is a tool that allows investigators to create forensic images of digital storage devices and analyze the contents of those images. When it comes to retrieving deleted files, FTK Imager can be used to search for deleted files within the forensic image and recover them. The tool has a user-friendly interface and supports a wide range of file systems, making it a powerful tool for forensic investigations. Autopsy, on the other hand, is an open-source digital forensic tool that allows investigators to conduct a wide range of forensic analyses, including file recovery. Autopsy's file recovery feature uses file carving to search for and extract deleted files from the image. The tool can recover a variety of file types, including images, videos, and documents.**

Keywords: **Digital forensic, FTK, Autopsy, Cyber crim*e***

I. INTRODUCTION

Digital forensic is the process of collecting, analyzing, and preserving digital evidence in order to investigate and solve crimes or other legal matters. This can include recovering data from computers, mobile devices, and other digital storage media, as well as analyzing network traffic and other digital communications.The goal of digital forensics is to gather and analyze evidence in a way that preserves its integrity, so that it can be presented in court or other legal proceedings. Digital forensics can be used in a variety of legal matters, including criminal investigations, civil litigation, and internal corporate investigations.The process of digital forensics

typically involves several steps, including acquiring a forensic image of the digital storage media, analyzing the data using specialized software and techniques, and presenting the results in a clear and concise manner. Digital forensic experts must also follow proper chain-of-custody procedures to ensure that the evidence is admissible in court. Digital forensics can be a complex and rapidly-evolving field, as new technologies and threats emerge. Digital forensic experts must be skilled in computer science, data analysis, and legal procedures, as well as staying up-to-date with the latest developments in technology and digital forensics techniques.

II. WHAT IS A DELETED FILE

In digital forensic, a deleted file refers to a file that has been intentionally or unintentionally removed from the file system of a digital device. When a file is deleted, it is not completely erased from the device's storage media. Instead, the space previously occupied by the file is marked as available for new data to be written over it.

However, until new data is written over the space, it may be possible for a forensic examiner to recover the deleted file using specialized tools and techniques. This is because the data comprising the file may still exist on the device, although the file system is no longer aware of its existence.

In some cases, a deleted file may be recoverable in its entirety, while in other cases only fragments of the file may be recoverable. Recovering deleted files can be an important part of a digital forensic investigation, as it may provide evidence that can be used to reconstruct events, identify suspects, or establish motives.

III. TECHNIQUES

FTK Imager and Autopsy are two commonly used tools that can be used for deleted file recovery.

FTK Imager is a forensic imaging tool that can be used to create a forensic image of a hard drive or other storage device. It can also be used to analyze and recover deleted files, as well as to view and analyze the content of the disk image. FTK Imager has a user-friendly interface and offers a wide range of features, including keyword searching, hash value calculation, and the ability to preview file.

Autopsy is an open-source digital forensic tool that offers a range of features for analyzing and investigating digital devices. Like FTK Imager, Autopsy can be used to recover deleted files and analyze disk images. It offers advanced features such as timeline analysis, keyword searching, and the ability to recover files from unallocated space.

Both FTK Imager and Autopsy are powerful tools that can be used for deleted file recovery, but they differ in terms of their features, ease of use, and compatibility with different file systems and operating systems. It is recommended to use both tools in conjunction with each other to increase the chances of recovering deleted files and to perform a thorough analysis of digital devices during a digital forensic investigation.

IV. WORKING PRINCIPLE OF FTK IMAGER

The steps involved in FTK (Forensic Toolkit) file recovery can vary depending on the specific scenario and the file system being analyzed. However, here are some general steps that are typically followed when using FTK for file recovery:

1) *Acquire the evidence*: Before attempting any file recovery, it's important to acquire a forensic image of the storage device. This image will be used for analysis and file recovery, and it must be an exact copy of the original storage device to ensure the integrity of the evidence.

2) *Launch FTK*: Once the forensic image has been acquired, launch FTK and create a new case to begin the analysis.

3) *Add evidence to the case*: Add the forensic image to the case in FTK, and select the file system of the storage device being analyzed.

4) *Conduct a search for deleted files*: Use the FTK search functionality to look for deleted files on the storage device. FTK can search for deleted files based on various criteria, such as file type, file name, and file extension.

5) *Examine the search results*: After conducting the search, examine the search results to identify any deleted files that have been found. FTK will typically display information about each file,such as its name, size, and location.

6) *Recover the files*: Select the deleted files that need to be recovered and use the FTK recovery functionality to recover them. FTK will typically prompt the user to specify a location for the recovered files.

7) *Validate the recovered files*: Once the files have been recovered, validate their integrity to ensure that they can be used as evidence. This can involve comparing the recovered files to the original forensic image, checking file signatures, and examining metadata.

V. ADVANTAGES OF FTK IMAGER

1. FTK Imager is a powerful tool for digital forensic investigations, offering a range of features that can help investigators to quickly and easily acquire disk images and analyze them for evidence of digital crime.
2. Easy to use: FTK Imager has a user-friendly interface that makes it easy for even non-technical users to use. It also provides step-by-step guidance to help users through the forensic imaging process.
3. Versatile: FTK Imager can be used to acquire images from a wide range of devices and file systems, including hard drives, USB drives, CDs, and DVDs. It can also acquire images from virtual machines and cloud storage
4. Fast acquisition: FTK Imager can acquire images of a device or storage media very quickly. It has the ability to create images of just the allocated space or of the entire disk, depending on the requirements of the investigation.
5. Advanced features: FTK Imager includes a number of advanced features that can be useful in forensic investigations, such as hash verification, keyword searching, and the ability to mount disk images as read-only to perform further analysis.
6. Widely used: FTK Imager is a widely used tool in the digital forensics community and is supported by a large community of forensic professionals. This means that it is regularly updated with new features and improvements, and users can find support and guidance when needed.

VI. APPLICATION OF FTK IMAGER

FTK Imager is a forensic tool that is commonly used for imaging, analyzing, and recovering data from computer systems. One of its main applications is in deleted file recovery. Here are some ways FTK Imager can be used for deleted file recovery:

1. *Imaging the hard drive*: FTK Imager can be used to create a bit-by-bit copy of the entire hard drive or a specific partition. This image can be used for offline analysis, which is helpful in deleted file recovery since it avoids the risk of overwriting data. The image can be mounted as a read-only drive, allowing for analysis of deleted files and data recovery
2. *Recovering deleted files*: FTK Imager can recover deleted files using its "Deleted File Recovery" feature. This feature allows users to search for deleted files based on specific file types, keywords, or other attributes. The tool can recover both active and deleted files from the hard drive, making it useful in situations where data may have been lost due to corruption, accidental deletion, or other reasons.
3. *Analyzing file metadata*: FTK Imager can also analyze file metadata, such as creation and modification dates, to help determine if a file has been deleted. This can be useful in identifying files that were deleted intentionally or unintentionally
4. *Identifying file fragments*: When a file is deleted, it may leave behind fragments on the hard drive that can be recovered. FTK Imager can identify these fragments and attempt to recover the full file.

FTK Imager is a powerful tool for deleted file recovery, particularly in cases where data loss may have occurred due to accidental deletion or corruption. Its ability to recover both active and deleted files, and its analysis of file metadata and fragments, make it a valuable resource for forensic investigators and IT professionals alike

VII. WORKING PRINCPLE OF AUTOPSY

Acquisition: Autopsy acquires a disk image of the device or storage media to be analyzed. The disk image is a bit-for-bit copy of the original device or media and contains all the data, including deleted files.

Parsing: Autopsy parses the disk image to extract information about the file system, partitions, and file metadata, such as timestamps, file names, and file paths.

Carving: Autopsy uses a technique called file carving to recover deleted files. File carving involves searching the disk image for patterns that match known file types, such as JPEG images or PDF documents, and then extracting the data associated with those patterns

Reconstruction: Autopsy reconstructs the recovered files by combining the carved data with the file metadata extracted during parsing. This allows the recovered files to be viewed and analyzed within the context of the original file system and folder structure.

Reporting: Autopsy generates a report that summarizes the findings of the analysis, including details of any recovered files, their file type, and their location on the disk image.

VIII. ADVANTAGE OF AUTOPSY

An autopsy is a forensic method of analyzing a computer system or device to uncover evidence of digital crimes or recover deleted files. There are several advantages of performing an autopsy for deleted file recovery, including:

1. *Uncover hidden data*: When a file is deleted, it is not completely erased from the hard drive. Instead, the operating system marks the space where the file was located as available for new data. By analyzing the hard drive using specialized forensic tools, an autopsy can uncover hidden data that is not accessible through normal means..
2. *Recover deleted files*: An autopsy can recover deleted files that have not yet been overwritten by new data. By analyzing the hard drive and identifying the location of the deleted file, an autopsy can restore the file to its original state.
3. *Identify potential evidence*: An autopsy can uncover evidence of digital crimes or suspicious activity on a computer system. By analyzing the hard drive, an autopsy can identify deleted files that may be relevant to an investigation, such as deleted emails, chat logs, or documents.
4. Provide a comprehensive report: An autopsy provides a detailed report of the findings, including any deleted files that were recovered.

IX. APPLICATION OF AUTOPSY

1. *Searching for deleted files*: Autopsy has a powerful search function that can be used to search for deleted files based on file type, keyword, or other attributes. This feature can help identify deleted files that may be relevant to an

investigation or data recovery effort.

2. Carving for deleted files: Autopsy can also use file carving techniques to recover deleted files that may not be located through normal search functions. File carving involves searching for file signatures or headers on the hard drive to identify and recover deleted files.
3. Timeline analysis: Autopsy can create a timeline of system activity, which can be useful in identifying when files were created, modified, or deleted. This timeline can be used to identify when a file was deleted and potentially recover it.
4. Analyzing file metadata: Autopsy can also analyze file metadata, such as creation and modification dates, to help determine if a file has been deleted. This can be useful in identifying files that were deleted intentionally or unintentionally.
5. Reporting: Autopsy provides a comprehensive report of its findings, including any deleted files that were recovered. This report can be used in legal proceedings or investigations to support a case or uncover new leads.

STARTING COMPUTER FORENSIC USING FTK:

Forensic Tool Kit (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 case can be quickly accessed, dramatically reducing the time of perform the analysis.

Digital investigation include following processes:

- Preparation
- Acquisition and preservation
- Analysis
- Reports and presentations

The computer forensic tool need to keep updated to address issues such as an increasing size of hard drives and the use of encryption in order to reduce the time to perform the data acquisition and analysis.

Access Data has two versions of the platforms:

- FTK forensic: this version of FTK has the ability to perform the acquisition and analysis of digital devices such As computer hard drives, USB drives, flash memory devices, smartphones, Tablets, and other digital media. Its approach is related to a process called Post-mortem computer forensics, which happens when the computer has Been powered down.
- AD Enterprise: In general, AD Enterprise has the same features as the FTK Forensics version plus the ability to analyze multiple computers across your Company simultaneously. Another important feature of this version is the Ability to acquire and analyze volatile data, such as RAM. The investigation Process is totally confidential, and the investigated user will not be aware of the analysis, even if it is done through the network and with the target Equipment in use.

A. Downloading FTK:

Once the FTK platform has been acquired, Access Data usually sends the DVDs for product installation and the hardware dongle codemeter with the license of the product. if not, then it is possible to download the FTK directly from the Access Data website.

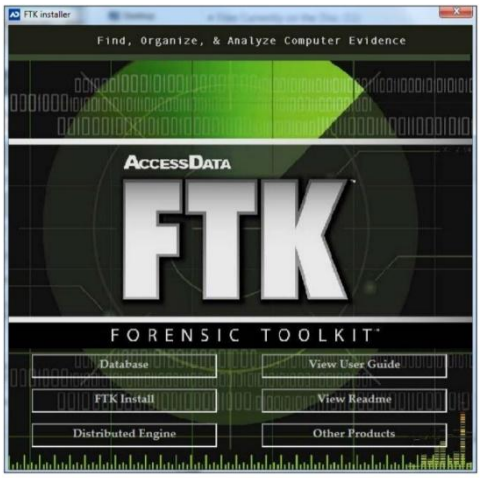
B. Prerequisites for FTK:

There are two different settings (configuration options) for FTK installation:

- One machine: FTK + database
- Two machines: FTK + database on separate machine.

C. Installing FTK and the database:

FTK installation is quite simple, although the components' installation sequence must be respected. Access Data has created a menu to provide support for the correct Installation, as can be seen in the following



(fig i)

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

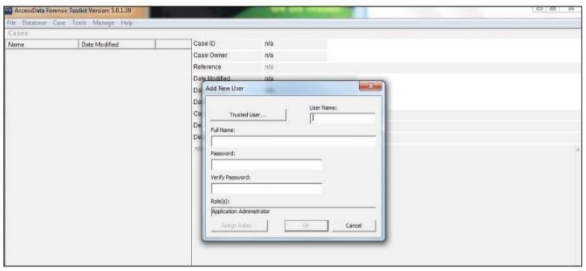
Button and select the components listed as follows:

- 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
- CodeMeter: This is the USB CodeMeter hardware driver and Management component
- Imager: This is the FTK Imager product

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 PostgresSQL

D. Running FTK for the first time:

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



(fig ii)

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, who will manage the FTK tool

E. Working with FTK Forensic:

The FTK is a complete platform for digital investigations, and although it has a friendly interface, its use requires attention, especially during the preanalysis phase. A wrong setting of the case can generate negative impacts on the project and may require more time than planned.

F. Acquisition and preservation:

Acquisition and preservation are considered as the most critical steps of the process since errors are not

allowed at the time of evidence acquisition. The basic principle of computer forensics is preservation of the digital evidence integrity. The acquisition can be done using the following tools:

Write blockers (hardware or software)
• Forensic duplicators
• Boot disks
• Remote acquisition (through network)

G. Analysis:

Analysis is the part of the investigation process that involves the most amount of technical aspects. Some of the reasons are listed as follows:

- Necessary technical knowledge about operation system, file system, network, and applications
- Specialized software is required
- Skill for creating filters and searching evidence in operational system artifacts

H. Reports and presentation :

This is the last step of the process. After we have found results and arrived at conclusions about the investigation, we need to perform the following steps:

- Adapt the report language for the target audience use technical language for the technical team or more formal and appropriate language for lawyers or judges
- Take care that the reports and presentations are clear and conclusive and avoid opinions
- Provide the presentation in different kinds of file formats such as PDF,HTML, DOC, and so on.

I. Managing groups and users :

The FTK allows you to create multiple users and assign roles to them, providing a more collaborative solution. To add a new user, we have to perform the following steps:

1. Click on Database and select Administer Users
2. Click on the Create Use button
3. Fill in the presented fields as follows:

- **User Name**: In this field, enter the name that will be recognized by the FTK
- **Full Name**: In this field, enter the full name that should appear on case reports
- **Password**: In this field, enter the password for the user
- **Verify Password:** In this field, enter the same password for verification

4. After entering the required information into the fields, click on **Assign Roles**.
5. To assign rights to this user, use one of the roles presented as follows

- Application Administrator: This performs all tasks, including adding and managing users
- Case Administrator: This performs all tasks that an application administrator can perform, except creating and managing users
- Case Reviewer: This cannot create cases; it only processes cases

6. After choosing the correct profile, click on OK to apply the role, and then click on OK again to create the user.

The user's passwords can be changed at any time. Just click on Change Password to enter the new password.

J. Creating a new investigation case :

The FTK allows you to manage your investigations by assigning a case for each of them. The case information is stored in a database.

1. Click on Newand select New Case. The New Case Options dialog opens.
2. Fill in the fields that appear in the following manner:

a. *Case Name*: In this field, enter the name of the case.
b. *Description*: This field is optional and text free.
c. *Reference*: This field is also optional and text free.
d. Description File: In this field, you can attach a file to the case.
e. *Case Folder Directory*: This holds the path where case files will be stored.
f. *Database Directory*: This is the path where case database will be stored. Select the In the case folder checkbox to set the same folder of the case.
g. *Processing Profile*: Configure the default processing options for the case by either using a processing profile or custom settings. This item will be detailed in the next topic.
h. *Open the case*: Check this option if you wish to open the case as soon as it is created. After the fields are filled, click on OK to create the new case.

3. The next step is to add the evidence file

4. Click on Add and select one of the following:
   - Acquired Image(s): Select this type to add an image file (dd, e01, AD1, and so on)
   - All Images in Directory: Select this to add all images in a specific folder
   - Contents of a Directory: Select this type to add all files in a specific folder
   - Individual File(s): Select this to add a single file (docx, pdf, jpg, and so on)
   - Physical Drive: Select this to add a physical device (a full hard disk)
   - Logical Drive: Select this to add a logical volume or partition, for example, the C or D drive

5. Click on OK set the following items:
   - Time Zone: Select the correct time zone of the location where the evidence was collected.
   - Refinement Options: Select which items will be processed in evidence. This item will be detailed in the next topic.
   - Language Settings: Select the correct language that corresponds to the alphabet used in the collected evidence.

6. Once all the parameters are configured, click on OK and wait for the evidence processing.

K. Case processing options:

To work better with your investigation case, the evidence data should be processed. When evidence is processed, data about the evidence is created and stored in the database. The processed data can be viewed at any time.
If you want to process the evidence as quickly as possible, you can use a predefined field mode that deselects almost all processing options. If you need an item for later, an additional analysis can be performed to enable additional processing options. Or, if you have time to categorize and index files, more options can be enabled. This step will take a significant amount of time for a large evidence set.

L. Refining the case evidence :

The evidence refinement process allows the specification of how the evidence is sorted and displayed, by adding or removing data according to date filters, file types, and status.
To set case evidence refining options, perform the following steps:
1. Click on the Evidence Refinement (Advanced) icon in the left-hand side pane. The following two dialog tabs will be seen:
   - Refine Evidence by File Status/Type
   - Refine Evidence by File Date/Size

2. Click on the corresponding tab.
   - This first tab allows you to focus on specific files needed for a case, including or removing files by type or status. For example, if you only search for evidence in Word files, it is much more effective if you apply the filters and only select the Documents checkbox in the File Types.
   - The second tab refines evidence by the date range or file size. In a scenario where you already know some information about the data you are seeking, it is recommended to apply this filter. A lot of processing time is saved.

X. How to use Autopsy for digital investigation?

Now, we will see how we can use Autopsy for investigating a hard drive. For that, we will go through a popular scenario most of us come across while studying digital forensics, and that is the scenario of *Greg Schardt.*

Step 1: Run Autopsy and select *New Case*.

Step 2: Provide the *Case Name* and the *directory* to store the case file. Click on *Next.*

Step 3: Add *Case Number* and Examiner's details, then click on *Finish*.

Step 4: Choose the required data source type, in this case *Disk Image* and click on *Next*

Step 5: Give path of the data source and click on *Next*

Step 6: Select the required modules and click on *Next*

Step 7: After the data source has been added, click on *Finish*

Step 8: You reach here once all the modules have been ingested. You can begin investigating.

XI. CONCLUSION

FTK (Forensic Toolkit) and Autopsy are both popular digital forensics tools used for deleted file recovery. Here is an overall review of both tools:
FTK:
FTK is a powerful digital forensics tool that is widely used by law enforcement agencies and digital forensic professionals. It has a user-friendly interface and is known for its speed and accuracy in searching for and recovering deleted files. FTK can recover files from a wide range of devices, including hard drives, memory cards, and USB drives. It also has advanced search and analysis features, making it a popular choice for complex investigations.
Autopsy:
Autopsy is an open-source digital forensics tool that is also used for deleted file recovery. It has a user-friendly interface and is popular among both beginner and advanced users. One of the key features of Autopsy is its ability to recover deleted files from various file systems,

including NTFS, FAT, and EXT. It also has built-in keyword search functionality, which allows users to search for specific keywords within files. Additionally, Autopsy has a plugin architecture, which allows users to extend its functionality.

Overall, both FTK and Autopsy are excellent tools for deleted file recovery. FTK is known for its speed and accuracy, while Autopsy is popular among both beginner and advanced users and has a robust plugin architecture. Ultimately, the choice between these two tools will depend on the specific needs of the investigation and the expertise of the user.

ACKNOWLEDGEMENT

FTK Imager and autopsy are the two tools which is widely used by the forensic investigators to retrieve the file for further investigation in the field of digital forensic. It is very essential to understand that the success of the recovery of deleted file is mainly depending on various factors such as condition of the storage media, file system that is used and action that is taken after the deletion the file. Final outcome of the process is the recovery of deleted file from the system.

Overall, both FTK and Autopsy are excellent tools for deleted file recovery. FTK is known for its speed and accuracy, while Autopsy is popular among both beginner and advanced users and has a robust plugin architecture. Ultimately, the choice between these two tools will depend on the specific needs of the investigation and the expertise of the user.

REFERENCES

[1]. Osho, O., & Ohida, S. O. (2016). Comparative evaluation of mobile forensic tools. *IJ Inf. Technol. Comput. Sci*, *1*, 74-83.

[2]. Carbone, F. (2014). *Computer forensics with FTK*. Packt Pub..

[3]. Wahyudi, E., Riadi, I., & Prayudi, Y. (2018). Virtual machine forensic analysis and recovery method for recovery and analysis digital evidence. *International Journal of Computer Science and Information Security*, *16*.

[4]. Bennett, D. J., & Stephens, P. (2008). A Usability Analysis of the Autopsy Forensic Browser. *HAISA*, 105-1