International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Undoit: Data Recovery Application

Prof. Shobha Lolge[1], Mahesh Vishwakarma[2], Saurabhkumar Yadav[3],Vishal Gupta[4]
[1]*Asst. Professor, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra* [2]*Dept. of Computer, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra* [3]*Dept. of Computer, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra*
[4]*Dept. of Computer, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra*

Abstract—Data recovery software for mobile phones is engineered to retrieve lost, deleted, or corrupted images from internal storage, SD cards, and cloud backups. These tools utilize advanced scanning algorithms, deep file search, and AI-based reconstruction techniques to restore photos in formats such as JPEG, PNG, HEIF, and RAW. The success of data recovery is influenced by factors including file overwriting, storage fragmentation, and the extent of data corruption. To maximize recovery chances, users are advised to cease device usage immediately after accidental deletion and avoid saving new files, while regular backups and cloud synchronization remain the most effective preventative strategies against permanent data loss.

This research paper presents a comparative analysis of three prominent forensic data recovery tools—FTK Imager, Test Disk, and Foremost—evaluating their effectiveness in retrieving lost files from various storage media. FTK Imager, a proprietary tool, is recognized for its structured imaging and high recovery success rates, supporting multiple file systems and forensic image formats. Test Disk, an open-source solution, excels in partition recovery and repairing non-bootable disks, though its undelete

feature is limited to specific file systems. Foremost, a command-line tool, specializes in file carving, making it effective for recovering deleted files even when file system metadata is compromised, but it may struggle with complete file restoration in cases of fragmentation

Keywords – Data Recovery, Digital Forensics, FTK Imager, Test disk, Foremost, File Recovery

1. INTRODUCTION

In the modern digital era, data recovery has emerged as a critical component of forensic investigations, enabling the retrieval of lost, deleted, or corrupted files that are essential for uncovering vital information. This capability is indispensable for law enforcement agencies, cybersecurity professionals, and corporate investigators, all of whom depend on accurate data reconstruction to solve crimes, prevent security breaches, and resolve internal disputes. Data loss can occur due to a variety of reasons, including accidental deletions, hardware failures, system formatting errors, and malicious cyberattacks. The widespread adoption of digital storage solutions in both personal and professional environments has heightened the need for proficient forensic data recovery methods.

As individuals and organizations increasingly rely on digital platforms to store sensitive information, the risk of data loss incidents grows, making the ability to recover such data not just advantageous but essential. Effective data recovery requires the use of specialized tools and methodologies designed to extract, reconstruct, and preserve digital evidence without compromising its integrity. This research paper explores a range of forensic tools used in data recovery, providing a comparative analysis of their functionalities and success rates. It also examines the significant impact that data recovery has on legal proceedings and cybercrime investigations, where digital evidence often plays a pivotal role in establishing

facts and supporting judicial outcomes.

In legal contexts, the ability to recover and present digital evidence can significantly influence the direction and outcome of a case, with courts increasingly recognizing digital evidence as credible when obtained and handled according to strict forensic protocols. Similarly, in cybercrime investigations, timely and effective data recovery can be the deciding factor between thwarting a security threat and suffering its consequences. By analyzing the tools and techniques employed in forensic data recovery, this paper aims to highlight best practices and recommend strategies to enhance the effectiveness of digital investigations.

2. Literature Survey

The significance of data recovery in forensic investigations has been underscored by various studies. Abdillah and Prayudi (2022) conducted a comparative analysis of open-source forensic tools, focusing on Foremost and Test Disk, and found them effective for file recovery on Linux systems. Their research highlighted that while tools like FTK Imager and TSK Recover are widely used, they may not fully restore certain corrupted files, whereas Foremost and Test Disk demonstrated a higher success rate in complete data recovery. Bharti et al. (2020) examined the capabilities of various mobile forensic tools, including UFED, in extracting data from Android devices. Their study provided benchmarks for researchers comparing new tools with existing ones, emphasizing the importance of selecting appropriate software based on specific forensic requirements. Varayogula et al. (2022) compared multiple forensic tools, emphasizing FTK Imager's reliability in structured data recovery. Their findings suggest that while FTK Imager offers structured and reliable data recovery, open-source tools like Test Disk provide cost-effective solutions adaptable to various forensic scenarios. Researchers have also explored challenges in digital data recovery, including software limitations and real-world applicability. Understanding the capabilities and shortcomings of these tools aids forensic analysts in making informed decisions when selecting software for data recovery tasks. Emerging technologies, such as artificial intelligence and machine learning, present promising advancements that could enhance accuracy and efficiency in forensic investigations. In summary, the literature indicates that both proprietary and open-source forensic tools have distinct advantages and limitations. The choice of tool should align with the specific needs of the investigation, considering factors such as cost, data type, and required recovery depth. Ongoing research into integrating advanced technologies holds potential for significant improvements in the field of forensic data recovery.

3. PROPOSED SYSTEM

Based on the "UndoIt" document, the proposed system offers innovative solutions for data recovery in various data applications, particularly digital forensic investigations and cybercrime scenarios. The system, named "UndoIt," leverages a combination of well-established forensic tools, namely FTK Imager, Test Disk, and Foremost, to maximize data recovery success while adhering to forensic best practices. FTK Imager is utilized for its structured imaging and data retrieval capabilities, Test Disk for partition recovery and file restoration, and Foremost for file carving. "UndoIt" employs a multi-faceted approach, starting with initial assessment and forensic imaging, followed by partition recovery and file carving as needed, and concluding with data reconstruction, verification, and reporting. By adhering to strict forensic procedures like write-blocking and hash verification, "UndoIt" aims to ensure data integrity and admissibility in legal proceedings, making it suitable for law enforcement agencies, cybersecurity experts, and corporate investigators seeking reliable and comprehensive data recovery solutions. Overall, "UndoIt"

balances the strengths of proprietary and open-source tools, integrating a range of data recovery techniques to enhance accuracy, efficiency, and adaptability in forensic investigations.

"UndoIt" focuses on the retrieval of lost, deleted, or corrupted data resulting from a range of incidents, including accidental deletions, hardware malfunctions, system formatting errors, and malicious cyberattacks. The system aims to provide end-to-end data recovery services, from initial assessment and imaging to file carving and reconstruction.

FTK Imager: This proprietary tool forms a cornerstone of the system, utilized for its robust structured imaging and data retrieval capabilities. "UndoIt" uses FTK Imager for forensic imaging, creating exact copies of storage media in various formats (RAW, E01, DD, SMART). Its ability to support multiple file systems (NTFS, FAT, HFS+, EXT) ensures compatibility with a wide range of storage devices. Its user-friendly interface will be used in structured data recovery for legal cases.

Test Disk: As an open-source partition and file recovery tool, Test Disk provides "UndoIt" with the ability to restore lost partitions and repair non-bootable disks. It is used particularly when dealing with partition corruption or accidental formatting. "UndoIt" uses it's undelete feature (compatible with FAT, exFAT, NTFS, and ext2) to help recover accidently deleted files.

Foremost: Specializing in file carving, Foremost is integrated into "UndoIt" to recover deleted files based on their headers, footers, and internal data structures. Foremost is applied in scenarios where file system metadata is compromised or when dealing with fragmented data. It extracts file fragments based on headers, footers, and internal data structures, effectively recovering files without relying on file system metadata.

4. Methodology:

This study evaluates the effectiveness of three forensic data recovery tools—FTK Imager, Test Disk, and Foremost—in retrieving lost files from various storage media.

4.1 Tools Selected for Comparison

- FTK Imager: A proprietary forensic tool renowned for creating forensic images and facilitating structured data retrieval. It supports multiple file systems, including NTFS, FAT, HFS+, and EXT, and can generate forensic images in formats such as RAW, E01, DD, and SMART .
- Test Disk: An open-source recovery tool designed primarily for partition recovery and file restoration. It is effective in repairing disks that are no longer bootable and includes an undelete feature for specific file systems.
- Foremost: A command-line tool specializing in file carving, which involves extracting file fragments based on headers, footers, and internal data structures. Developed to replicate the functionality of DOS carving software on the Linux platform, Foremost is effective in recovering files without relying on file system metadata.

4.2 Experimental Setup

Hardware: The experiments were conducted on a Windows 11 laptop equipped with a 512GB SSD and an 8GB USB flash drive.

Software: FTK Imager, Test Disk, and Foremost were installed on a forensic workstation running a Linux environment to utilize the full capabilities of each tool.

Procedure: The evaluation involved deleting files of various formats, including JPG, PNG, and MP4, from the storage devices. Each tool was then employed to attempt recovery of these files.

The scenarios tested included:

- Retrieving files from formatted drives.
- Recovering lost or deleted partitions.
- Extracting deleted file fragments through file carving techniques.

Standard forensic procedures were adhered to throughout the experiments to maintain data integrity and ensure reproducibility of results. This included the use of write-blocking techniques to prevent any modification of the original data and hash verification methods to confirm the authenticity and integrity of the recovered files.

By systematically comparing the performance of FTK Imager, Test Disk, and Foremost across these scenarios, this study aims to provide insights into their respective strengths and limitations, thereby guiding forensic professionals in selecting appropriate tools for specific data recovery tasks.

5. RESULT

In digital forensic investigations, selecting the appropriate data recovery tool is crucial for effective evidence retrieval. A comparative analysis of FTK Imager, Test Disk, and Foremost reveals distinct strengths and limitations for each tool.

FTK Imager is a proprietary forensic tool renowned for its structured imaging and data retrieval capabilities. It supports various imaging formats, including Raw (DD), SMART, Expert Witness/EnCase, and Advanced Forensic Format (AFF). Studies have highlighted its reliability in structured data recovery, making it ideal for forensic professionals handling legal cases.

Test Disk is an open-source recovery tool designed primarily for partition recovery and file restoration. It is particularly effective in restoring lost partitions and repairing disks that are no longer bootable. However, its undelete feature is limited to specific file systems, such as FAT, ex FAT, NTFS, and ext2, which may restrict its applicability in certain scenarios.

Foremost is a command-line tool specializing in file carving and retrieving file fragments. It is beneficial for recovering deleted files, especially when file headers and metadata are partially lost. Despite its utility, Foremost may struggle with complete file restoration, particularly in cases involving fragmented data.

Comparative Performance:

Evaluations of these tools have considered factors such as recovery success rate, integrity of recovered files, usability, and processing time. While specific numerical metrics may vary across studies, general findings suggest:

- FTK Imager: Demonstrates a high success rate in recovering structured file systems efficiently, with a user-friendly interface that enhances usability.
- Test Disk: Effectively restores partitions but may have limitations with fragmented data; it requires a moderate level of technical expertise to operate.
- Foremost: Useful for deleted file carving but may face challenges in complete file restoration; as a command-line tool, it has a steeper learning curve, impacting usability.

6. OVERVIEW

Data recovery is a process of acquiring lost, corrupted or damaged data from different storage medium. Data recovery plays an important role when the data is unable to access by regular procedures. For instance, the data in an electronic device is corrupted or formatted completely, and also when the storage medium is damaged data recovery method is used to acquire the data. In certain digital crimes criminals tries to delete logs, files and other useful data to erase their traces of evidence in crime. In such situations investigation officer requires certain data recovery software to acquire the essential data, which helps in further investigation procedures. Data recovery

software or the techniques of data recovery are also required in situations where the loss of data is due to virus, accidental deletion and system failure . Data losses may be caused by both computer and physical issues, while we can recover data by means of software and hardware ways. This study gives a brief knowledge of different types of data recovery software in forensic aspects. The information restoration process varies depending on the circumstances of the information recovery, the data restoration tool used to create the restore, and the standby destinations material. Many backup software solutions for desktops and laptops, for example, allow consumers to restore lost data easily, but recovering a broken databases from a tape back is a time consuming process that necessitates IT support. Information restoration solutions might also be utilized to retrieve data that originally not authorized and was accidentally erased from a desktops file systems, but is still strewn over the hard disk. Because a file and its associated information are kept in separate locations, data recovery possible. The Windows operating system, for example, keeps track of which documents are on the hard drive and where they are kept using a file allocation table.

7. DISCUSSION

The results indicate that FTK Imager is the most reliable tool for comprehensive data recovery in forensic investigations. It offers structured recovery with high accuracy, making it particularly effective for cases requiring the retrieval of large volumes of data while maintaining file integrity. Additionally, FTK Imager's compatibility with various storage media and forensic imaging capabilities further enhance its reliability in digital investigations. However, its proprietary nature presents a financial challenge for forensic teams with limited budgets .On the other hand, open-source tools like Test disk and Foremost remain valuable alternatives due to their accessibility and adaptability. Test disk excels in partition recovery and is a recovering fragmented or incomplete data. Challenges such as file corruption, partial recovery, and compatibility with different operating systems were noted across all tools. Selecting the appropriate forensic data recovery tool depends on the specific needs of an investigation, balancing factors such as recovery success rate, usability, and cost considerations. The need for improvements in open-source forensic tools remains evident, particularly in enhancing user experience and improving data reconstruction accuracy. Further development in this area could make open-source solutions more competitive against proprietary forensic software, increasing their adoption in forensic investigations worldwide. option when dealing with lost or corrupted partitions. However, it requires users to have a strong understanding of disk structures and command-line operations, making it less user-friendly for beginners. Foremost, a tool specializing in file carving, is particularly useful for retrieving deleted files from digital storage media. Despite its strengths, Foremost struggles with full file restoration, often**.**

8. CONCLUSION

This comparative analysis of data recovery tools highlights FTK Imager as the most effective for structured forensic investigations due to its robust imaging capabilities, high recovery success rates, and user-friendly interface. Its ability to create forensic images while preserving file integrity makes it an essential tool for digital forensic professionals. However, its proprietary nature and associated costs may limit accessibility for some forensic teams. Test disk is highly recommended for partition recovery, particularly in cases where data loss occurs due to accidental formatting or partition corruption. Its open-source nature makes it an attractive option for budget-conscious forensic teams, though its

command-line interface may present a learning curve for inexperienced users. Despite these challenges, Test disk remains a powerful tool for restoring lost partitions and file structures. Foremost serves as a valuable secondary tool for file carving, making it especially useful for recovering deleted files from damaged storage media. Unlike FTK Imager and Test disk, Foremost focuses on identifying and extracting files based on predefined headers and footers, which allows it to recover data even in cases where file system structures are compromised. However, its reliance on signature-based recovery can lead to partial or fragmented file restoration, which may limit its overall effectiveness.

9. REFERENCE

- Abdillah, M. F., & Prayudi, Y. (2022). Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux. *International Journal of Advanced Computer Science and Applications*, 13(9).
- Bharti, P., Vyas, N., & Dave, M. (2020). Comparison of Mobile Forensic Tools to Extract Data from Various Android Devices. *International Journal of Computer Sciences and Engineering*, 8(5).
- Varayogula, S., & Nandhini, M. (2022). Comparative Analysis of Data Extraction for Qualcomm Based Android Devices. *2022 International Conference on Computer Communication and Informatics (ICCCI)*.