International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Recovery of Deleted Files: Challenges and Techniques

Naveen R[1] Vijayarajan M[2] Archana K P[3] Nidhin S S[4]

[1,2,3]BSc Forensic Science, Dept of Criminology and Forensic Science, Nehru Arts and Science College, Coimbatore
[4]Assistant Professor, Dept of Criminology and Forensic Science Nehru Arts and Science College

ABSTRACT
In digital forensics, recovering deleted files is crucial for investigations related to cybercrimes, corporate espionage, financial fraud, and personal data recovery. When a file is deleted from a storage device, it is not immediately removed; instead, the system marks its space as available for new data. Until overwritten, this data can often be recovered using specialized forensic techniques. However, modern storage technologies, encryption, and anti-forensic tools pose significant challenges to successful data retrieval. This research explores the mechanisms of file deletion across various storage systems, including Hard Disk Drives (HDDs), Solid-State Drives (SSDs), USB flash drives, and cloud storage. It highlights challenges such as data overwriting, SSD TRIM operations, encrypted storage, and the deliberate use of data-wiping tools. The study also examines different file systems (NTFS, FAT, EXT, HFS+) and their impact on data recovery. To address these challenges, forensic experts employ recovery techniques such as metadata analysis, file carving, and data imaging. Advanced forensic tools, including Autopsy, FTK Imager, EnCase, and Test Disk, aid in identifying, extracting, and reconstructing deleted files. This study emphasizes the importance of digital forensics in modern investigations, showcasing how deleted file recovery can provide critical evidence in criminal cases, cybersecurity incidents, and civil disputes. The findings contribute to improving forensic methodologies, ensuring more effective and reliable data retrieval in forensic science.

Keywords: Digital forensics, File recovery, Deleted data, Metadata analysis, Cyber security, File carving, Storage devices

INTRODUCTION

Cyber forensics, sometimes referred to as digital forensics, is a subfield of forensic science that focuses on locating, gathering, preserving, analyzing, and presenting digital evidence associated with cybercrimes. It is essential for looking into illegal activity involving networks, digital storage systems, mobile devices, and PCs. Cyber forensics has become crucial for law enforcement organizations, cybersecurity specialists, and legal experts because of the growing dependence on technology in the private, business, and governmental spheres.

Computer forensics, which deals with recovering and analyzing data from computers and storage devices; network forensics, which tracks and analyzes network traffic to identify cyber threats and breaches; mobile forensics, which concentrates on recovering data from smartphones and tablets; malware forensics, which

investigates malicious software to determine its origin and functionality; and cloud forensics, which deals with looking into data stored on cloud platforms, are some of the subfields that fall under this umbrella.

Definition and Importance of Data Recovery

The act of recovering lost, damaged, or unusable data from a variety of storage media, such as hard drives, solid-state drives (SSDs), CDs, DVDs, or cloud storage, is known as data recovery. In order to recover files, documents, photos, or entire databases that have been lost as a result of problems like hardware failure, virus assaults, file corruption, natural disasters, or inadvertent deletion, this process usually entails the use of specialist tools, techniques, and knowledge. It is impossible to overestimate the significance of data recovery, particularly when considering business continuity. Data is essential to daily operations, communication, and decision-making in enterprises. Downtime, monetary loss, and reputational harm are just a few of the serious consequences that can result from losing important data, such as client information, bank records, or project files.

Overview of Data Recovery

Retrieving lost, erased, or inaccessible files from digital storage devices such hard disks, solid-state drives (SSDs), USB drives, and cloud storage is known as data recovery. It is essential to cybersecurity, digital forensics, and personal data management because it makes sure that important data can be recovered following unintentional loss, system failures, or cyberattacks. The capacity of data recovery to recover important files for individuals, companies, and law enforcement is what makes it so important; it keeps data loss from having negative financial or legal effects.

Numerous factors, such as user error, software corruption, hardware malfunctions, malware infections, and storage device formatting, can cause files to be erased. Deleted files can sometimes be recovered until they are overwritten by fresh data, which enables recovery tools and forensic specialists to restore the lost data.

Role of Digital Forensics in Data Recovery

With a collection of specialized methods and procedures intended to examine, preserve, and recover digital evidence from a range of platforms, storage systems, and devices, digital forensics plays a crucial and complex role in data recovery. The first step in the procedure is to identify and evaluate all possible sources of data, which may include network devices, mobile phones, tablets, cloud storage, hard drives, solid-state drives (SSDs), and even virtual environments. Important files that have been erased, corrupted, or damaged may be stored in each of these data sources. Experts in digital forensics emphasize data preservation to maintain data integrity throughout the recovery process after these sources have been discovered. In order to ensure that the recovered data may be used in legal or investigative contexts without running the risk of contamination or evidence tampering, this is accomplished by employing technologies such as write-blockers, which prevent any alteration or modification of the original data.

Factors Affecting File Recovery

Overwriting, data fragmentation, storage medium type, and the use of encryption or compression are some of the critical aspects that affect the success of file recovery. Until fresh data overwrites its storage location, a deleted file can still be recovered. The original data is irreversibly destroyed by overwriting, making recovery all but impossible. Furthermore, because missing fragments might cause a file to become corrupted or incomplete, data fragmentation—where files are kept in non-contiguous sectors and complicate recovery.

File Deletion Process in Different Storage Systems

A file is written into sectors on a storage medium when it is stored on a digital device, and the file system

records the file's location and metadata. The operating system marks the space as open for new data when a file is removed rather than deleting the data right away.

Until they are overwritten, erased files on conventional Hard Disk Drives (HDDs) frequently stay intact, allowing for forensic tool recovery. However, the TRIM command, which aggressively deletes erased data to maximize speed, causes Solid-State Drives (SSDs) to operate differently, making file recovery much more challenging.

Techniques for Recovering Deleted Files

Several software-based techniques that examine storage devices to recover lost data are used to recover erased files. Signature-based recovery is one of the most used methods, in which forensic tools search a storage media for distinct file signatures or headers that show the beginning of a file. Even if the files' original directory entries have been deleted, this technique aids in finding and rebuilding them. File carving is an additional method that looks for file fragments using specified structures while avoiding the file system. When metadata is lost or corrupted, file carving is very helpful since it enables the recovery of full or partial files through the analysis of raw data sectors.

Data scraping and hex analysis are more sophisticated recovery techniques in which forensic specialists look at the unprocessed hexadecimal representation of data on a device. They can locate file remains, retrieve pertinent data, and restore deleted files by manually examining the hex code.

Challenges in Deleted File Recovery

There are a number of difficulties in recovering deleted files, especially because of deliberate data-hiding techniques and improvements in storage technology. The TRIM command in SSDs, which permanently deletes removed data to maximize performance, is one significant barrier. SSDs actively remove storage blocks, making file recovery all but impossible after TRIM has been run, in contrast to HDDs, where deleted files can be recovered until they are overwritten.

The adoption of anti-forensic methods by criminals to thwart data recovery is another difficulty. These tactics include file manipulation techniques like steganography, which conceals data within other files, encryption to make recovered data unusable, and secure deletion tools that repeatedly overwrite files. Disk-wiping software is another tool used by criminals to totally destroy storage media, leaving little to no trace.

OBJECTIVE

1. Identify the challenges: Investigate the common challenges and obstacles faced during deleted file recovery, including file fragmentation, overwriting, and corruption.
2. Understand file system structures: Examine the underlying file system structures and storage media to understand how data is stored and retrieved.
3. Evaluate data recovery techniques: Assess various data recovery techniques, including software-based methods, algorithmic approaches, and hardware-based solutions.

METHODOLOGY

Particulars	Methods
Signification of Study	This study to comprehensively explore the complexities and methods involved in restoring deleted data, with the ultimate goal of developing effective strategies for successful file recovery, while also identifying potential challenges and understanding the underlying file system structures and storage media.

Universe of the study	Cyber Police station, Malappuram
Data Collection	Data is collected by conducting interviews with cyber experts and analyzing case studies.
Research Design	Explorative and Descriptive
Tools of the Study	Tools used are forensic software's such as Autopsy, FTK imager, enCase, Recuva and R- studio.
Limitations	Limited data collected; have to collect data from many experts to get accurate result.

RESULT

This study explores key aspects of cybercrime investigations through a combination of conducted interviews, analyzed case studies, and practical experiments. Interviews with cyber security experts provide valuable perspectives on the challenges faced in digital forensics, particularly in recovering deleted evidence. Case studies examine real-world cybercrime incidents, demonstrating how forensic tools are applied in tracking digital threats and analyzing electronic evidence. Practical experiments with tools like Autopsy, FTK, and Magnet Axiom offer insights into their functionalities, strengths, and limitations in data recovery and forensic investigations.

Thematic Findings

Theme 1: Common cyber crimes

Interviews with cybersecurity experts revealed varying perspectives on the prevalence and impact of common cybercrimes, particularly fraud, insider threats, and cyber harassment. One expert emphasized that fraud including phishing scams and identity theft remains the most frequently reported cybercrime, with criminals using increasingly sophisticated social engineering tactics. Another interviewee, specializing in corporate cybersecurity, highlighted the growing risk of insider threats, explaining that employees with privileged access often misuse their credentials for financial gain or sabotage, making it difficult to detect malicious activity before significant damage occurs. Regarding cyber harassment, a digital forensics investigator noted that online stalking and cyberbullying cases have surged, particularly on social media platforms and messaging apps. However, challenges in evidence collection arise as perpetrators delete messages or use encrypted communication channels. Experts agreed that cybercriminals often erase their digital traces, making deleted file recovery a critical aspect of forensic investigations. One interviewee pointed out that while forensic tools like Autopsy and EnCase are effective in retrieving deleted data, encrypted or overwritten files pose significant challenges. Example: " Insider threats and employee misconduct employees deleting sensitive company files before resignation or termination" (Interviewee 1)

Theme 2 : Challenges in deleted file recovery

Interviews with cybersecurity experts highlighted significant challenges in deleted file recovery, including data overwriting, encryption, and variations in file systems. While forensic tools like FTK and EnCase aid recovery, their effectiveness is limited when files are overwritten or encrypted without decryption keys. Experts also noted that cloud storage complexities make digital evidence retrieval difficult, as data is often fragmented across multiple servers and restricted by provider policies. Legal professionals emphasized jurisdictional constraints that delay or prevent access to crucial evidence. Overall, the findings stress the need for advanced AI driven forensic tools and standardized legal frameworks to

improve cybercrime investigations Example: "Encryption and secure deletion make recovery harder"(Interviewee 2).

Theme 3: Digital Forensic Tools and Techniques

Interviews with cybersecurity experts emphasized the critical role of forensic tools in cybercrime investigations. Experts highlighted that Autopsy, FTK, X-Ways, EnCase, and R-Studio are widely used for data recovery and digital evidence analysis, with each tool offering specific advantages depending on the case. A mobile forensics specialist noted that UFED and Magnet Axiom are particularly valuable for extracting data from smartphones, including deleted messages and encrypted files. However, experts agreed that these tools have limitations, especially when dealing with advanced encryption or anti-forensic techniques used by cybercriminals. Comparing perspectives, forensic analysts stressed the need for continuous updates in forensic tools, while legal professionals highlighted challenges in ensuring digital evidence admissibility in court. Overall, the findings underscore the importance of advancing forensic technologies and integrating AI-driven analysis to enhance digital investigations . Example: "For investigations, file recovery tools (e.g., Autopsy, FTK, EnCase, R-Studio) and techniques (e.g., carving, MFT analysis, volume shadow copy recovery) are commonly used" (Interviewee 1)

Theme 4 : Advanced cyber investigation areas

Interviews with cybersecurity experts highlighted the growing importance of OSINT (Open-Source Intelligence), Dark Web investigations, and cloud forensics in modern cybercrime investigations. One expert emphasized that OSINT is crucial for gathering publicly available data to track cybercriminal activities, while another specialist noted that Dark Web investigations play a key role in uncovering illegal marketplaces and hidden communication channels. A cloud forensics investigator pointed out that cybercriminals increasingly exploit cloud infrastructure, making cloud forensics essential for retrieving evidence stored across multiple servers. Experts also discussed the sophisticated malware tactics used by cybercriminals, such as fileless malware and obfuscation techniques, which make traditional forensic methods less effective. Forensic analysts stressed the need for advanced investigative techniques, including AI-driven analysis and behavioral forensics, to uncover hidden evidence. Legal professionals in the interviews highlighted the jurisdictional and privacy challenges in accessing data from cloud providers and encrypted communication platforms. Overall, the findings emphasize the need for continuous advancements in cyber investigation methodologies to keep pace with evolving digital threats Example: "OSINT techniques helped track a cybercriminal by analyzing leaked credentials and transaction patterns on the Dark Web, despite challenges posed by encryption and anonymity tools" (Interviewee 1)

Theme 5: Essential Skills and Certifications for Cybercrime Investigators

Interviews with cybersecurity experts highlighted those digital forensics expertise, evidence handling, and knowledge of cyber laws are critical for effective cybercrime investigations. A forensic analyst emphasized that proper evidence handling ensures data integrity and admissibility in court, while a legal expert noted that understanding cyber laws helps Investigators navigate jurisdictional challenges. Experts agreed that certifications like CEH (Certified Ethical Hacker), EnCE (EnCase Certified Examiner), and CFCE (Certified Forensic Computer Examiner) validate an investigator's technical skills and credibility. However, some interviewees pointed out that certifications alone are not enough, stressing the importance of hands-on experience and continuous training to keep up with evolving cyber threats. Overall, the findings highlight the need for a combination of certifications, practical expertise, and legal awareness to enhance the effectiveness of cybercrime investigations . Example: "Hands on experience with recovery

tools or proper evidence collection and handling" (Interviewee 2).

DISCUSSION

The study highlights the critical role of digital forensics in cybercrime investigations, particularly in recovering deleted files, analyzing digital evidence, and overcoming challenges posed by encryption, cloud storage, and legal constraints. The findings, supported by expert interviews, case studies, and practical experiments, demonstrate that forensic tools like FTK, EnCase, and Magnet Axiom are essential for data recovery and analysis. Additionally, expertise in OSINT, Dark Web investigations, and cyber laws is crucial for tracking digital threats and ensuring evidence admissibility in court.

The significance of this study lies in its contribution to understanding modern cybercrime challenges and the evolving role of forensic techniques in combating digital threats. By identifying gaps in forensic methodologies and legal frameworks, the study provides insights into improving investigative approaches and enhancing cybersecurity measures.

The research also emphasizes the importance of certifications like CEH, EnCE, and CFCE, which validate investigators' skills and strengthen their ability to handle digital evidence effectively.

However, the study has limitations, including the rapid evolution of cyber threats, which may render some forensic techniques outdated. Additionally, legal and jurisdictional constraints make cross-border investigations difficult, limiting access to crucial digital evidence stored in cloud environments. To overcome these challenges, continuous updates in forensic tools, advancements in AI-driven analysis, and the establishment of standardized international legal frameworks are necessary. Future research should focus on emerging cyber threats, such as deep fake fraud and AI-powered cybercrimes, to develop more resilient forensic methodologies and investigative strategies.

CONCLUSION

Cybercrime investigations involve complex challenges, requiring expertise in digital forensics, specialized tools, and legal knowledge. The key themes common cyber crimes, challenges in deleted file recovery, forensic tools and techniques, advanced investigative areas, and essential investigator skills highlight the need for robust forensic methodologies to track and analyze cyber threats. The analysis underscores the significance of digital evidence in solving cybercrimes and the obstacles investigators face, such as encryption, data overwriting, and jurisdictional restrictions. Existing theories, such as Routine Activity Theory and General Strain Theory, provide a framework for understanding cybercriminal behavior, while forensic science models emphasize structured investigative approaches. However, the field is constantly evolving, with new threats emerging that challenge traditional forensic methods. Strengthening legal frameworks, integrating AI into forensic tools, and enhancing investigator training are crucial steps toward improving cybercrime investigations. Looking ahead, the fight against cybercrime requires continuous adaptation, collaboration between law enforcement and cybersecurity experts, and the development of innovative solutions to stay ahead of increasingly sophisticated digital threats.

REFERENCES

1. Zhao, P., & Zhang, L. (2020). Deleted file recovery method, apparatus and device, and readable storage medium.
2. Bansal, A., Agrawal, A., Singh Sankhla, M., & Kumar, R. (2016). Computer Forensic Investigation

on Hard Drive Data Recovery: A Review Study. IOSR Journal of Computer Engineering, 18(05), 39–42.
3. Ahn, J.-H., Park, J., & Lee, S. (2014). The Research on the Recovery Techniques of Deleted Files in the XFS Filesystem. 24(5), 885–896.
4. Knight, B. (2013). Techniques to recover files in a storage network.
5. Ranade, D. M., Shah, A. S., Bellari, N., & Agrawal, M. (2007). Techniques for file system recovery.
6. Nikkel, Bruce. "Data Deletion Challenges and Risks of Recovery." (2019).
7. Venkatesh, K., et al. "Recovery of Deleted Files in the NTFS File System using Python and PyTSK3." 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS). IEEE, 2024.
8. Conner, Tyler. A Review of the Challenges Anti-Forensics Present to the Viability of File Recovery. MS thesis. Utica College, 2020.
9. Nodler, Joshua. Deleted File Recovery in Ext4 File Systems. MS thesis. Bowling Green State University, 2024.
10. Deshpande, Bhagyashri P. "The Advanced Way Of Data Recovery." International Journal Of Computer Science And Applications 6.2 (2013).
11. Yulianto, Semi, and Benfano Soewito. "Investigating the impact on data recovery in computer forensics." 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs). IEEE, 2023.
12. Kuts, Dmitry, et al. "The Peculiarities of Deleted Files Recovery in FAT32 File System." 2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radio electronics and Information Technology (USBEREIT). IEEE, 2023.
13. Tomer, Shashank, et al. "Data recovery in Forensics." 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN). IEEE, 2017.
14. Suthar, Hepi. "How to Recover Deleted Data from SSD Drives after TRIM." Advanced Techniques and Applications of Cybersecurity and Forensics. Chapman and Hall/CRC, 2025. 248-263.
15. Duisburg, Sarah M., and An-I. Andy Wang. "A survey of confidential data storage and deletion methods." ACM Computing Surveys (CSUR) 43.1 (2010): 1-37.
16. Geiger, Matthew. "Counter-forensic tools: Analysis and data recovery." 18th FIRST Conference. Vol. 65. 2006.
17. Bhardwaj, Akas deep, et al. "Forensic Investigations of Permanently Deleted Data from Recycle Bin." 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2023.
18. Chervenak, Ann, Vivekenand Vellanki, and Zachary Kurmas. "Protecting file systems: A survey of backup techniques." Joint NASA and IEEE Mass Storage Conference. Vol. 99. 1998.
19. Oestreicher, L. (2019). Analysis of deleted data remnants on SSDs. IEEE Transactions on Digital Forensics, 15(4), 456-470.
20. Aljaedi, A., Furnell, S., Clarke, N., & Reich, C. (2011). Forensic analysis of cloud computing systems. Network Security, 2011(11), 4-10.
21. Aljaedi, A., Furnell, S., Clarke, N., & Reich, C. (2011). Forensic analysis of cloud computing systems. Network Security, 2011(11), 4-10.
22. Reardon, Joel, David Basin, and Srdjan Capkun. "On secure data deletion." IEEE security & privacy 12.3 (2014): 37-44.

23. Abdillah, Muhammad Fahmi, and Yudi Prayudi. "Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux." International Journal of Advanced Computer Science and Applications 13.9 (2022): 633-639.
24. Ogazi-Onyemaechi, Bernard Chukwuemeka, Ali Dehghantanha, and K-KR Choo. "Performance of android forensics data recovery tools." Contemporary digital forensic investigations of cloud and mobile applications. Syngress, 2017. 91-110.
25. Surbiryala, Jayachander, and Chunming Rong. "Data recovery and security in cloud." 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA). IEEE, 2018.
26. Pisaric, Milana. "Challenges of recovering and analyzing volatile data." DANI ARČIBALDA RAJSA ""ARCHIBALD REISS DAYS.
27. Alhussein, Mohammed, and Duminda Wijesekera. "A highly recoverable and efficient filesystem." Procedia Technology 16 (2014): 491-498.
28. Ravi, Akshara, T. Raj Kumar, and Angelo Renju Mathew. "A method for carving fragmented document and image files." 2016 International Conference on Advances in Human Machine Interaction (HMI). IEEE, 2016.
29. Roux, Brian, and Michael Falgoust. "Ethical issues raised by data acquisition methods in digital forensics research." Journal of Information Ethics 21.1 (2012): 40.
30. Barton, T., and M. H. B. Azhar. "Forensic analysis of the recovery of Wickr's ephemeral data on Android platforms." The First International Conference on Cyber-Technologies and Cyber-Systems. IARIA, 2016.