Mobile Forensics: Recovery of Deleted Data from Android and iOS Devices

***Omraj Gautam**

Abstract

Mobile phones have become indispensable in both personal and professional domains, serving as primary devices for communication, data storage, and online interaction. As their usage increases, these devices also emerge as critical sources of evidence in digital investigations. One of the most significant challenges in mobile forensics is the recovery of deleted data, particularly from encrypted applications and secure operating systems like Android and iOS. This paper investigates methods and tools used in recovering deleted artifacts, including messages, call logs, multimedia files, and application data, from smartphones running Android and iOS. Through practical analysis and comparison, this study highlights the extent to which deleted data can be retrieved, evaluates the role of forensic tools such as Cellebrite UFED, Oxygen Forensic Detective, and Magnet AXIOM, and explores the impact of operating system security features on forensic recovery. The findings suggest that while Android devices offer broader opportunities for artifact recovery due to their open architecture, iOS devices pose significant challenges, often requiring advanced exploits or jailbreaking techniques. The study emphasizes the importance of deleted data recovery in cybercrime investigations and suggests future directions for research in mobile forensics.

I. Introduction

In today's digital age, smartphones have become central to human communication, entertainment, and business activities. With the availability of high-speed internet, cloud integration, and advanced applications, mobile phones are no longer simple communication devices but powerful computing platforms that store and transmit vast amounts of personal and professional information. Consequently, they have become prime targets for cybercriminals as well as vital sources of digital evidence in criminal, civil, and corporate investigations.

Mobile forensics, a branch of digital forensics, focuses on the identification, acquisition, analysis, and preservation of data stored on mobile devices. Unlike traditional computer forensics, mobile forensics presents unique challenges due to the diversity of operating systems, frequent updates, proprietary hardware, and sophisticated security features. Among these challenges, the recovery of deleted data is particularly significant. Deleted artifacts, such as text messages, instant messenger chats, call records, images, and browsing history, often contain crucial information that can determine the

outcome of an investigation.

Both Android and iOS, the two dominant mobile operating systems, implement strong security mechanisms including full-disk encryption, sandboxing, and secure deletion protocols. While these measures enhance user privacy, they also complicate forensic investigations. Applications such as WhatsApp, Telegram, and Signal further increase complexity by using end-to-end encryption and secure deletion techniques, making the recovery of deleted communications difficult.

The importance of deleted data recovery in mobile forensics is evident in cases involving cybercrime, fraud, terrorism, harassment, and financial disputes. Even partial recovery of deleted artifacts can provide investigators with valuable leads. This paper aims to examine the methodologies, tools, and limitations of recovering deleted data from Android and iOS devices. By comparing both platforms, the study identifies key challenges faced by forensic practitioners and evaluates strategies to overcome them.

II. Aim & Objectives

The primary aim of this research is to investigate and compare the processes of recovering deleted data from Android and iOS devices, focusing on the effectiveness of forensic tools and techniques in retrieving crucial digital evidence. Since smartphones have become essential tools in daily life and are often involved in cybercrime or civil disputes, understanding the scope and limitations of deleted data recovery is critical for digital forensic practitioners.

Based on this aim, the following objectives are formulated:

- **To identify and categorize the types of deleted artifacts** (such as text messages, multimedia files, call logs, browsing history, and instant messaging chats) that can be recovered from Android and iOS devices.
- **To evaluate the effectiveness of commonly used forensic tools** such as Cellebrite UFED, Oxygen Forensic Detective, Magnet AXIOM, and Autopsy in the recovery of deleted data.
- **To compare the recovery processes and outcomes between Android and iOS platforms**, highlighting the differences in operating system architecture, file systems, and security mechanisms.
- **To analyze the challenges posed by encryption and secure deletion mechanisms** implemented in modern smartphones and applications.
- **To provide forensic significance of deleted data recovery** in supporting investigations related to cybercrime, fraud, and other digital offenses.

III. Forensic Significance

- Mobile forensics plays a crucial role in modern digital investigations, as smartphones often hold information that is highly relevant in legal, corporate, and personal disputes. The ability to recover deleted data significantly increases the evidentiary value of these devices, making forensic analysis indispensable in the fight against cybercrime and other unlawful activities.
- Deleted data recovery is particularly significant because criminals and wrongdoers frequently attempt to erase evidence of their activities. Whether it is a deleted text message, a removed image, or a wiped call log, such artifacts may contain critical leads that can establish intent, timeline, or association in an investigation. Even fragments of deleted information can provide vital clues when corroborated with other sources of digital evidence.
- From a legal perspective, mobile forensics supports law enforcement agencies and judicial bodies by ensuring that evidence is retrieved in a forensically sound manner. Properly recovered and preserved artifacts can be presented in court as admissible evidence, provided that chain-of-custody protocols and integrity checks are maintained. This underscores the importance of reliable forensic tools and methodologies.
- Moreover, deleted data recovery has applications beyond criminal justice. In corporate environments, mobile forensics is used to investigate data leakage, insider threats, and employee misconduct. In civil cases, such as family disputes or harassment claims, recovered mobile data can support or challenge testimonies.
- Thus, the forensic significance of deleted data recovery lies in its ability to:
- Reveal concealed or intentionally destroyed information.
- Strengthen the credibility of investigations with corroborative digital evidence.
- Assist in reconstructing timelines of events.
- Provide leads for further investigative actions, such as network forensics or cloud data acquisition.
- In summary, deleted data recovery enhances the depth, accuracy, and reliability of digital forensic investigations, making it a cornerstone of mobile forensics.

IV. Challenges

Recovering deleted data from mobile devices is a complex task due to the dynamic nature of mobile operating systems, rapid advancements in device hardware, and increasingly sophisticated security mechanisms. Unlike traditional desktop forensics, where file systems and recovery techniques are relatively stable, mobile platforms introduce unique challenges that complicate the forensic process. The key challenges include:

1. Operating System Security Mechanisms

- **Android** employs multiple file systems (EXT4, F2FS) and allows a variety of hardware vendors, leading to differences in data storage structures.
- **iOS** utilizes the APFS (Apple File System) and advanced sandboxing, making it difficult to access application-level data without jailbreaking.
- Both systems implement **full-disk encryption**, requiring access to device-specific encryption keys that may not be easily obtainable.

2. Frequent Updates and Device Diversity

- The constant release of new versions of Android and iOS introduces changes in encryption, storage structures, and app data handling.
- The diversity of Android devices (Samsung, Xiaomi, OnePlus, etc.) further complicates forensic analysis as each vendor customizes the OS differently.

3. End-to-End Encryption in Applications

- Popular messaging applications such as WhatsApp, Telegram, and Signal employ end-to-end encryption, preventing network-based data interception.
- Deleted messages from such apps are often overwritten quickly, making their recovery challenging without exploiting memory or cached files.

4. Rooting and Jailbreaking Requirements

- Forensic tools often require **root access (Android)** or **jailbreaking (iOS)** to bypass system restrictions and access protected areas of the device.
- However, these procedures may alter the integrity of evidence and are sometimes restricted in forensic best practices.

5. Volatile and Overwritten Data

- Mobile devices frequently overwrite deleted data due to limited storage space. Once overwritten, recovery becomes nearly impossible.
- Volatile memory (RAM) can contain valuable forensic artifacts but is lost once the device is powered down.

6. Legal and Ethical Constraints

- Laws regulating privacy and digital evidence acquisition vary across jurisdictions. Investigators must ensure compliance with legal frameworks while attempting to recover deleted data.

- Unauthorized bypassing of encryption or accessing cloud backups may raise ethical and admissibility concerns in court.

7. Cloud Synchronization

- Many mobile applications sync with cloud services (Google Drive, iCloud). This makes deleted local data difficult to interpret, as copies may still exist remotely. However, accessing cloud data requires separate legal authorization and technical capabilities.
- In conclusion, while technological advancements have enabled significant progress in mobile forensics, the above challenges continue to restrict the completeness and reliability of deleted data recovery. Overcoming these issues requires continuous development of forensic tools, innovative methodologies, and adherence to legal standards.

V. Literature Review

Mobile forensics has emerged as one of the most dynamic areas of digital forensics due to the rapid growth of smartphones and their extensive use in personal, business, and criminal activities. A large body of research has focused on data acquisition, recovery of deleted files, and forensic analysis of mobile applications, especially on Android and iOS platforms.

1. Early Research in Mobile Forensics

Simon and Slay (2010) examined the recovery of application activity data from memory, highlighting the role of volatile memory analysis in identifying user activity. Their work emphasized that deleted artifacts often persist in memory long after deletion, offering opportunities for forensic recovery. Similarly, Chin et al. (2011) analyzed inter-application communication in Android devices, identifying vulnerabilities that could be leveraged for forensic extraction of data.

2. Forensic Analysis of Social Media and Messaging Applications

Anglano (2014) conducted one of the most comprehensive forensic analyses of WhatsApp Messenger on Android smartphones, detailing the structure of recovered artifacts such as message histories, timestamps, and contact lists. The study demonstrated that even deleted conversations could often be reconstructed through database remnants.

Ovens and Morison (2016) extended this approach by focusing on iOS devices, particularly analyzing instant messaging apps like Kik. Their research highlighted the challenges of iOS sandboxing and encryption, while showing that certain artifacts remain recoverable with advanced forensic tools.

Norouzizadeh Dezfouli et al. (2016) investigated multiple social networking applications, including Facebook, Twitter, and LinkedIn, on both Android and iOS. They concluded that despite increasing security measures, metadata and deleted traces could still be extracted from device memory and backups.

3. Deleted Data Recovery Techniques

Majeed and Saleem (2017) studied forensic analysis of social media applications on Windows 10 but extended their insights to highlight how similar challenges exist in mobile platforms. Their findings on data remnants in unallocated storage are directly applicable to deleted data recovery in smartphones.

Cahyani et al. (2017) emphasized the role of mobile forensics in counter-terrorism, particularly focusing on cloud-synchronized communication applications. They identified that even if local data is deleted, forensic investigators can often retrieve deleted messages from linked cloud accounts.

Sudozai et al. (2018) provided an in-depth study on the IMO chat application across Android and iOS. Their analysis of encrypted traffic and deleted records highlighted the complexity of recovering deleted data in applications that employ strong cryptography.

4. Advancements in Tools and Techniques

Kitsaki et al. (2018) investigated Android applications with a forensic focus, pointing out that deleted artifacts can be retrieved through both logical and physical acquisition methods, though the latter is more intrusive.

Ghafarian and Wood (2018) concentrated on Skype communications, showing that memory forensics can uncover deleted chat fragments, call records, and even hidden processes that persist in volatile memory.

Recent studies (2020–2024) have increasingly emphasized AI-driven approaches to automate artifact recovery. For instance, Zhang et al. (2021) applied machine learning techniques to identify deleted traces in large mobile datasets, significantly improving recovery efficiency. Similarly, Kumar and Meena (2022) explored blockchain-integrated forensic methods to ensure integrity and traceability of recovered mobile artifacts.

5. Comparative Studies: Android vs. iOS

Multiple researchers have compared the forensic opportunities and limitations between Android and iOS.

- Android devices are generally considered more accessible for forensic recovery due to open file systems and wider tool support.
- iOS devices, with APFS and strong encryption, present greater challenges; however, jailbreaking techniques and iTunes backups have provided alternative avenues for recovery (Walnycky et al., 2015).
- Recent works (Sharma & Patel, 2023) highlight that while Android permits recovery of deleted messages and multimedia files even after partial overwriting, iOS recovery is often limited to metadata unless advanced exploits are employed.

6. Forensic Relevance of Deleted Data

Al Mutawa et al. (2011, 2012) demonstrated how deleted instant messaging artifacts could be

essential in identifying criminal activity, especially in social media–related cases. Their findings remain relevant as more modern applications adopt similar storage structures.

Sgaras et al. (2012) argued that deleted data recovery is vital for reconstructing timelines of events, especially when user activity is intentionally erased to conceal evidence.

Summary of Literature Review

The reviewed studies reveal a consistent emphasis on the importance of deleted data recovery in mobile forensics. While significant progress has been made in developing tools and techniques, the literature also shows that:

- Android offers broader opportunities for deleted data recovery due to its architecture.
- iOS continues to challenge forensic investigators, with deleted artifacts often retrievable only through jailbreaking or backup analysis.
- Encrypted applications pose a persistent obstacle, requiring innovative techniques like memory forensics or AI-based analysis.

  This literature forms the foundation for the present research, which compares Android and iOS deleted data recovery in practical scenarios using established forensic tools.

VI. Tools & Technologies

Recovering deleted data from mobile devices requires the use of specialized forensic tools and supporting technologies. These tools are designed to extract, analyze, and preserve data in a forensically sound manner while overcoming the security mechanisms of Android and iOS. The following are the key tools and technologies relevant to this study:

1. Cellebrite UFED (Universal Forensic Extraction Device)

Cellebrite UFED is one of the most widely used commercial forensic solutions for mobile devices. It supports logical, file system, and physical extractions of both Android and iOS devices.

- **Capabilities:** Recovery of deleted SMS, call logs, images, and instant messaging data.
- **Strengths:** Broad device compatibility, ability to bypass lock screens on certain devices, and comprehensive reporting.
- **Limitations:** Advanced encryption in newer iOS versions limits full recovery unless a jailbreak or exploit is available.

2. Oxygen Forensic Detective

Oxygen Forensic Detective provides in-depth analysis of mobile applications and cloud services.

- **Capabilities:** Access to over 25,000 application artifacts, including WhatsApp, Telegram, Facebook, and Signal.

- **Strengths:** Cloud data acquisition (Google Drive, iCloud) and recovery of partially deleted artifacts from app databases.
- **Limitations:** Requires device access credentials or tokens for cloud acquisition.

3. Magnet AXIOM

Magnet AXIOM is a comprehensive forensic suite that supports mobile, computer, and cloud data acquisition.

- **Capabilities:** Logical and physical extractions, keyword searching, timeline reconstruction, and deleted artifact recovery.
- **Strengths:** Strong analytical features, including visualization of chat history and recovery of media files from unallocated space.
- **Limitations:** iOS extractions are limited without jailbreaks, and newer Android security models restrict full access.

4. Autopsy (with Mobile Modules)

Autopsy is an open-source forensic platform primarily used for computer forensics, but with mobile forensic modules it can analyze Android and iOS data images.

- **Capabilities:** File carving, recovery of deleted media, and timeline analysis.
- **Strengths:** Open-source and extensible, suitable for academic and experimental research.
- **Limitations:** Lacks some advanced decryption capabilities found in commercial tools.

5. Android Debug Bridge (ADB)

ADB is a command-line tool provided by Google for Android device management.

- **Capabilities:** Allows access to device files, log data, and backup creation for forensic analysis.
- **Strengths:** Useful for extracting app-related files without rooting, depending on OS version.
- **Limitations:** Deleted data recovery is limited; more powerful when combined with forensic tools.

6. i Tunes and iCloud Backups (for iOS)

Apple devices create encrypted or unencrypted backups, which may retain deleted artifacts.

- **Capabilities:** Recovery of deleted messages, app data, and call history from backup files.
- **Strengths:** Provides an alternative to physical access when devices are locked.
- **Limitations:** Heavily dependent on backup availability and encryption status.

7. Jailbreaking and Rooting Utilities

- **Jailbreaking (iOS):** Enables bypassing of Apple's restrictions, allowing access to the file system for deeper forensic extraction.
- **Rooting (Android):** Grants privileged access to device storage, enabling full acquisition.
- **Challenges:** Both processes may alter system integrity, and legal admissibility depends on investigative protocols.

8. Memory Forensic Tools

Tools like **Volatility** and **LiME (Linux Memory Extractor)** can be used to acquire volatile memory from mobile devices, though primarily in research contexts. Memory forensics may reveal deleted data fragments or encryption keys.

Summary

The combined use of commercial forensic suites (Cellebrite, Oxygen, Magnet AXIOM) and system-level tools (ADB, iTunes backups, jailbreaking/rooting) provides the best chance of recovering deleted artifacts from Android and iOS. However, effectiveness varies based on device model, operating system version, and security settings.

VII. Environment Setup

To ensure systematic analysis and comparison of deleted data recovery, the research environment was carefully designed to replicate real-world scenarios where forensic practitioners may encounter Android and iOS devices. The setup included test devices, operating systems, applications, and forensic tools, all of which were configured to perform controlled experiments.

1. Test Devices

- **Android Device:**
  - Model: Samsung Galaxy A50
  - OS Version: Android 11 (with EXT4 file system)
  - Root Status: Rooted using Magisk for enabling full forensic extraction.
- **iOS Device:**
  - Model: iPhone 8
  - OS Version: iOS 15.6 (with APFS file system)
  - Jailbreak Status: Jailbroken using Checkra1n for advanced file system access.

2. Applications Installed for Testing

- **WhatsApp Messenger** (for text, images, and call logs).
- **Telegram Messenger** (for encrypted chat and media sharing).
- **Native SMS/Messaging app** (for traditional text message recovery).
- **Phone Dialer and Call Logs** (to test call record deletion and recovery).
- **Gallery App** (for image/video creation and deletion tests).

3. Forensic Tools Used

- **Cellebrite UFED** for logical and physical extractions.
- **Oxygen Forensic Detective** for application and cloud data recovery.
- **Magnet AXIOM** for analysis of deleted artifacts and timeline reconstruction.
- **Autopsy** (with mobile modules) for open-source validation.
- **ADB (Android Debug Bridge)** for Android system-level data extraction.
- **iTunes/iCloud Backups** for iOS data recovery testing.

4. Experiment Scenarios

To simulate realistic forensic investigations, the following scenarios were tested on both devices:

1. **Baseline Activity:** Creation of messages, calls, and media files.
2. **Deletion:** Selected messages, call logs, and media files were deleted manually.
3. **Acquisition:** Devices were acquired using forensic tools (logical, file system, and physical extraction methods).
4. **Recovery Analysis:** Extracted data was examined for deleted artifacts.
5. **Comparison:** Results were compared between Android and iOS platforms.

5. Host System Specifications

- Laptop with Intel Core i5 processor (2.4 GHz), 8 GB RAM, 500 GB SSD.
- Operating System: Windows 10 (64-bit).
- Virtualization tools such as VMware Workstation were also used for testing iTunes backups and forensic software modules.

VIII. Methodology & Experiment

The methodology for this research was designed to replicate real-world forensic investigation practices while maintaining a controlled environment for analysis. The experiment followed a systematic approach consisting of data generation, deletion, acquisition, and recovery on both Android and iOS devices.

Step 1: Data Generation

To create a baseline dataset, various activities were performed on the test devices:

- Sending and receiving **text messages** via native SMS apps.
- Exchanging **WhatsApp and Telegram messages**, including text, emojis, and voice notes.
- Making and receiving **voice and video calls** on WhatsApp and Telegram.
- Creating and storing **images and videos** in the Gallery app.
- Browsing the internet using the default web browser.

This ensured the presence of multiple types of data (structured and unstructured) for later deletion and recovery attempts.

Step 2: Data Deletion

Selected artifacts were manually deleted from both devices to simulate typical user behavior:

- Deletion of specific **SMS conversations**.
- Deletion of **WhatsApp and Telegram chat messages** (individual and group).
- Deletion of **call logs** from the Phone app.
- Removal of **selected images and videos** from the Gallery.

Additionally, cache clearing was performed on some applications to test whether artifacts remained accessible despite user attempts to erase evidence.

Step 3: Acquisition

Data acquisition was carried out using a combination of logical, file system, and physical extraction methods, depending on device compatibility.

- **Android Device:**
    - Logical extraction using **ADB** and Cellebrite UFED.
    - File system extraction via **root access**.
    - Physical extraction attempted through **Magnet AXIOM**.
- **iOS Device:**
    - Logical extraction using **iTunes backup** (unencrypted and encrypted).
    - File system extraction via **Checkra1n jailbreak** and Oxygen Forensic Detective.
    - Cloud data acquisition from **iCloud**, where available.

Step 4: Recovery & Analysis

- Extracted data was analyzed using forensic suites: **Cellebrite UFED Reader**, **Magnet AXIOM**, **Oxygen Forensic Detective**, and **Autopsy**.
- Special focus was placed on recovering:
    - Deleted **messages and chat logs**.
    - Deleted **call records**.
    - Deleted **media files (images/videos)**.
- Tools were cross-validated to ensure consistency of results. For example, a deleted WhatsApp message recovered by Cellebrite was checked in Magnet AXIOM for confirmation.

Step 5: Comparison & Documentation

The results from Android and iOS devices were compared to identify:

- Types of artifacts successfully recovered.
- Recovery success rates across different categories (messages, calls, media).
- Differences in outcomes between logical, file system, and physical acquisitions.
- Limitations encountered in each operating system.

All recovered data was documented, categorized, and tabulated for analysis.

IX. Results & Discussion

The experiments conducted on Android and iOS devices produced varying outcomes in terms of deleted data recovery. The analysis revealed differences in the recoverability of messages, call logs, and multimedia files across both platforms, largely influenced by the operating system architecture, file system, and security mechanisms.

1. Recovery of Deleted SMS and Call Logs

- **Android:**
    - Deleted SMS messages were partially recovered using Cellebrite and Magnet AXIOM.
    - Call logs, including timestamps and contact numbers, were successfully retrieved from unallocated space.
- **iOS:**
    - Recovery of SMS was limited to metadata (timestamps, sender/receiver numbers).
    - Deleted call logs were partially recovered from iTunes backups, but complete recovery required jailbreak-based file system access.

2. Recovery of WhatsApp Data

- **Android:**

- Deleted WhatsApp messages were recoverable from SQLite database remnants (msgstore.db).
- Media files (images/videos) deleted from chats were often retrievable from unallocated storage.
- Magnet AXIOM successfully reconstructed partial chat histories even after deletion.

- **iOS:**
  - WhatsApp deletion left fewer traces due to iOS APFS efficiency.
  - Some deleted records were retrievable via encrypted iTunes backups if credentials were available.
  - File system access via jailbreak yielded limited fragments of deleted chats but not entire conversations.

3. Recovery of Telegram Data

- **Android:**
  - Deleted Telegram messages were harder to recover due to Telegram's cloud-based storage and strong encryption.
  - Metadata (session tokens, login times) was recoverable, but deleted chats were mostly inaccessible.
- **iOS:**
  - Telegram's sandboxing on iOS further reduced recoverability.
  - Only minimal artifacts (timestamps, cached media references) were extracted.

4. Recovery of Media Files (Gallery and Messaging Apps)

- **Android:**
  - Deleted images and videos were recoverable through file carving techniques in Magnet AXIOM and Autopsy.
  - JPEG and MP4 files showed partial recovery success depending on overwrite status.
- **iOS:**
  - Deleted media recovery was significantly limited.

- Partial image thumbnails were found, but complete file recovery was rare without advanced physical acquisition.

5. Comparative Analysis Table

Table 1: Comparison of Deleted Data Recovery between Android and iOS

Artifact Type	Android (Rooted) – Results	iOS (Jailbroken) – Results
SMS Messages	Partially recovered from unallocated storage	Metadata only, limited recovery via backup
Call Logs	Fully recovered (numbers, timestamps)	Partially recovered, metadata available
WhatsApp Messages	Deleted chats recoverable from SQLite remnants	Limited recovery, partial fragments via backup
WhatsApp Media	Recoverable from unallocated storage	Rare recovery, thumbnails only
Telegram Messages	Metadata and limited logs recoverable	Very limited, mostly inaccessible
Telegram Media	Some recoverable, though inconsistent	Rare recovery, mostly inaccessible
Gallery Photos/Videos	Good recovery with carving tools	Limited to thumbnails, few complete files

6. Discussion

The results highlight key differences between Android and iOS forensic recoverability:

- **Android** provides better opportunities for recovering deleted data due to:
  - Open file system architecture (EXT4/F2FS).

    - Greater compatibility with forensic tools.
    - Availability of SQLite database remnants and unallocated storage fragments.
- **iOS**, on the other hand, restricts recovery due to:
    - Stronger sandboxing and APFS structure.
    - Enforced encryption on both backups and device storage.
    - Limited access to application data without jailbreaking.
- **Application-level encryption** significantly reduced recovery success in Telegram across both platforms. WhatsApp showed higher recoverability, especially on Android, as its local databases retained deleted artifacts until overwritten.
- **Multimedia recovery** was more successful on Android than iOS, where only thumbnails and metadata could be retrieved.

These findings confirm that Android devices offer broader forensic opportunities for deleted data recovery, while iOS devices remain more restrictive, requiring advanced techniques and sometimes yielding only limited metadata.

X. Conclusion

This research investigated the recovery of deleted data from Android and iOS devices, focusing on messages, call logs, and multimedia artifacts. By simulating real-world scenarios and applying multiple forensic tools, the study revealed significant differences in the recoverability of deleted artifacts across the two platforms.

The results indicate that:

- **Android devices** provide broader opportunities for deleted data recovery. Due to their relatively open architecture, file system accessibility, and compatibility with forensic tools, Android allows recovery of SMS, WhatsApp chats, and media files even after deletion. SQLite remnants and unallocated storage proved particularly valuable in reconstructing deleted artifacts.
- **iOS devices** pose greater challenges to forensic recovery. Strong security mechanisms such as APFS, sandboxing, and full-disk encryption limit access to deleted data. Recovery of artifacts was mostly restricted to metadata and partial fragments obtained via iTunes backups or jailbreak-based extraction.
- **Application-level encryption** significantly impacts recoverability. Telegram, being highly reliant on cloud-based storage and encryption, revealed minimal deleted data across both platforms, whereas WhatsApp left more recoverable traces, especially on Android devices.

- **Multimedia recovery** demonstrated better results on Android, where complete image and video files could often be carved from unallocated space. On iOS, recovery was largely limited to thumbnails and metadata, highlighting stronger deletion mechanisms.

Overall, this study emphasizes that while deleted data recovery remains feasible, its success depends heavily on the operating system, application architecture, and the tools employed. Forensic practitioners must adapt methodologies based on the device and OS in question, while also being aware of the limitations posed by encryption and secure deletion protocols.

XI. Future Work

While this research has demonstrated the possibilities and limitations of recovering deleted data from Android and iOS devices, several areas remain open for further investigation. The field of mobile forensics is rapidly evolving, and future research can expand on the following aspects:

1. **Integration of AI and Machine Learning**
    - Automated artifact detection using AI can significantly improve the efficiency of forensic investigations.
    - Machine learning algorithms could help in identifying hidden patterns in partially deleted or fragmented data.
2. **Advanced Encryption and Secure Messaging Apps**
    - With the rise of secure apps such as Signal, Wickr, and Threema, future studies should focus on recovery possibilities in these highly encrypted environments.
    - Research can also investigate traffic analysis and memory forensics as alternative approaches to recovering evidence from encrypted apps.
3. **Cloud and Hybrid Forensics**
    - Since many mobile applications synchronize with cloud services (Google Drive, iCloud), forensic recovery should extend to hybrid environments combining device and cloud data.
    - Future work could explore methods of correlating deleted local artifacts with available cloud backups.
4. **Physical Acquisition in Newer Devices**
    - The trend toward stronger hardware-based encryption in modern smartphones limits physical acquisition. Research on novel hardware-level forensic techniques, such as chip-off analysis or JTAG, could improve data recovery.
5. **Cross-Platform Comparative Studies**

- This study focused primarily on Android and iOS. Future research could extend comparisons to other emerging mobile platforms or analyze differences across Android manufacturers (Samsung, OnePlus, Xiaomi).

6. **Legal and Ethical Considerations**
    - As privacy regulations become stricter, studies should also explore the balance between forensic needs and compliance with data protection laws such as GDPR.
    - Ethical frameworks for using intrusive techniques like rooting or jailbreaking should be further developed.
7. **Real-World Case Studies**
    - Practical case studies involving actual investigations (with anonymized data) could provide valuable insights into the effectiveness of current tools and highlight areas needing improvement.

***Research Scholar**
Department of Advance Research
University of Technology
Jaipur (Raj.)

References

1. Al Mutawa, N., Al Awadhi, I., Baggili, I., & Marrington, A. (2011). Forensic artifacts of Facebook's instant messaging service. *International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, pp. 771–776.
2. Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9, S24–S33.
3. Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3), 201–213.
4. Cahyani, N. D. W., Ab Rahman, N. H., Glisson, W. B., & Choo, K. K. R. (2017). The role of mobile forensics in terrorism investigations involving cloud storage and communication apps. *Mobile Networks and Applications*, 22(2), 240–254.
5. Chin, E., Felt, A. P., Greenwood, K., & Wagner, D. (2011). Analyzing inter-application communication in Android. *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, pp. 239–252.
6. Ghafarian, A., & Wood, C. (2018). Forensics data recovery of Skype communication from physical memory. *Science and Information Conference (SAI)*, Springer, Cham, pp. 995–1009.

7. Kitsaki, T. I., Angelogianni, A., Ntantogian, C., & Xenakis, C. (2018). A forensic investigation of Android mobile applications. *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, ACM, pp. 58–63.

8. Majeed, A., & Saleem, S. (2017). Forensic analysis of social media applications in Windows 10. *NUST Journal of Engineering Sciences*, 10(1), 37–45.

9. Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R. (2016). Investigating social networking applications on smartphones: Detecting Facebook, Twitter, LinkedIn, and Google+ artifacts. *Australian Journal of Forensic Sciences*, 48(4), 469–488.

10. Ovens, K. M., & Morison, G. (2016). Forensic analysis of Kik messenger on iOS devices. *Digital Investigation*, 17, 40–52.

11. Sgaras, C., Kechadi, M. T., & Le-Khac, N. A. (2012). Forensics acquisition and analysis of instant messaging and VoIP applications. *Computational Forensics*, Springer, Cham, pp. 188–199.

12. Simon, M., & Slay, J. (2010). Recovery of Skype application activity data from physical memory. *International Conference on Availability, Reliability and Security (ARES)*, IEEE, pp. 283–288.

13. Sudozai, M. A. K., et al. (2018). Forensic analysis of IMO application on Android and iOS. *International Journal of Digital Forensics and Cyber Crime*, 10(2), 45–62.

14. Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of Android social-messaging applications. *Digital Investigation*, 14, S77–S84.

15. Zhang, H., Chen, L., & Liu, Q. (2021). Digital forensic analysis of instant messaging applications on smartphones: Challenges and opportunities. *International Conference on Computing, Networking and Communications (ICNC)*, IEEE, pp. 647–651.

16. Kumar, R., & Meena, S. (2022). Blockchain-assisted mobile forensics for secure evidence handling. *Journal of Digital Forensics, Security and Law*, 17(2), 55–73.

17. Sharma, P., & Patel, R. (2023). Comparative study of deleted data recovery from Android and iOS platforms. *International Journal of Cybersecurity and Digital Forensics*, 12(1), 12–28.

18. Lee, J., & Park, S. (2024). AI-driven approaches for mobile forensic artifact recovery. *Journal of Information Security and Applications*, 78, 103589.