Journal of Technology and Value Addition
Vol. 8, Issue No. 2, July 2026, pp. 33-49
https://www.uwu.ac.lk/jtva/
ISSN: 3051-5203 (Online)

Research Article

Recovering Deleted Data From Smartphones: A Digital Forensic Approach

A. Yoganathan[1*] and M.R.M. Hanan[2]

[1]Faculty of Technology, South Eastern University of Sri Lanka, Oluvil 32360, Sri Lanka.
[2]Faculty of Applied Sciences, Uva Wellassa University of Sri Lanka, Badulla 90000, Sri Lanka

*Correspondence: anosaw21@gmail.com; Tel.: +94 76 741 6179

Abstract

Smartphones are one of the most valuable sources of digital evidence in a criminal, civil and regulatory investigation, but the recovery of deleted data from smartphones using a variety of platforms and tools is not consistently understood. This study is a mixed-methods analysis of the five forensic tools and five acquisition methods used in the analysis of a controlled set of 150 smartphones (90 Android, 60 iOS). Seven data categories and eight time points after deletion were used to measure recovery rates. Cellebrite UFED had the best Android recovery rate (89%) and Oxygen Forensic Detective was best at iOS (78%). The best overall recovery rate was obtained from chip-off extraction (97%), but the highest yield was obtained by physical extraction, while the latter was the most practical. After 24 hours, the rates dropped significantly both platforms post-deletion. The research suggests a structured forensic acquistion procedure following the NIST and ACPO guidelines, and outlines some platform-specific challenges such as the iOS Secure Enclave encryption and fragmentation by the Android manufacturer, while proposing some mitigation strategies to practitioners.

Keywords: Android forensics, Cybercrime investigation, Data acquisition, Deleted data recovery, Digital forensics, iOS forensics

1. Introduction

The smartphone has become an essential tool of the contemporary world, which has entirely transformed the way people communicate, do business, and plan their everyday lives. Statista (2023) reports global smartphone subscription figures for the period from 2016 to 2023, illustrating the widespread adoption of smartphone technology worldwide. This unparalleled usage has also made the smartphone an abundant source of digital evidence in criminal cases, civil cases, and regulation cases. Europol (2022) discusses the growing importance of digital evidence in investigations involving cybercrime and organized crime.

This article is published under the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

which announced that smartphones were the major source of evidence in more than 73 percent of all cybercrime cases tried in European Union member states. Although the issue of digital privacy is becoming better known, users continue to store (and remove) sensitive data on their computers on a regular basis. This information may include personal discussions, bills and receipts, movement history, photograph records, e-mails and information that was created by the applications installed. The underlying fallacy of deletion is permanent erasure which is still found with laypersons and at times even with criminal offenders. As a matter of fact, mobile operating systems use file allocation table-based management systems where deletion operations usually only delete the metadata pointer of the file leaving underlying data untouched in unallocated storage blocks until it is physically overwritten by other data. Digital forensics, as a science, refers to the process of identifying, preserving, acquiring, inspecting, analyzing and presenting electronically stored information (ESI) in a legal admissible manner (Casey, 2011).

Mobile digital forensics represents a domain that focuses on the specific technical issues that are found on mobile, computing devices such as proprietary operating systems, hardware encryption, cloud synchronisation, remote wiping functionality, and varying physical form factors. The field has developed very quickly in line with the increasing complexity of mobile platforms since Apple introduced the Secure Enclave Processor (SEP) in 2013 and Google has since adopted full-disk encryption as the default in Android 6.0 and beyond. Access to deleted information on smartphones gives investigators a great chance and a tremendous technical challenge that they are likely to overcome.

The open-source character of the operating system on Android platform provides more flexibility to the forensic examiners to choose their methods of extraction, but fragmentation between manufacturers and between Android versions also makes the compatibility of tools more difficult. On the other hand, the closed system of iOS implements strict encryption measures that are difficult to obtain during a physical acquisition, however, logical and backup-based procedures can provide a significant number of artefacts. The acquisition methodology used i.e. logical, file system, physical, JTAG and chip-off significantly impact the volume of evidence recoverable as well as the integrity of the evidence recovered. There are also legal and ethical aspects of mobile forensics which are also very important. The investigators should be working within set chain-of-custody policies in that the evidence extracted is not compromised and is reproducible.

Any lack of evidential integrity may make digital evidence inadmissible in court, and may provide the whole prosecution with a plausible invalidity. Structured protocols to ensure investigative practice are available with regulatory frameworks like the Association of Chief Police Officers (ACPO) Good Practice Guide to Digital evidence and the National Institute of standards and Technology (NIST) Guidelines to mobile device forensics (SP 800-101). Adherence to these standards cannot be compromised in professional forensic engagements. This study is driven by the fact that there is an evident gap between the speed of mobile technology development and the ability of the forensic community to

facilitate optimally with the development of encrypted technology, the change of operating systems and the change in architecture of the applications. Previous research investigated individual tools, or even certain types of data; nevertheless, the comparative analysis of various tools, resources, data types, and methods of their acquisition is a field that is still under strict empirical research at postgraduates.

The goal of this research is to assess the efficacy of forensic tools and acquisition techniques that can be used to recover deleted data from Android and iOS smartphones and to create real-world guidance for forensic practitioners. Specific objectives are: (1) to evaluate the effectiveness of the most widely used forensic tools for data recovery from Android and iOS devices; (2) to compare and contrast the data acquisition techniques in terms of their recovery efficiency, technical complexity and evidentiary value; (3) to determine the correlation between the elapsed time after deletion and data recoverability; (4) to understand the forensic challenges of Android and iOS platforms and propose mitigation strategies; (5) to develop an applicable procedure that can be implemented by either law enforcement or private forensic practitioners. The goals of this study will contribute to the science of mobile forensics by offering investigators a body of evidence-based knowledge and insight into maximizing the evidentiary value of smartphone-originated digital artefacts.

2. Literature Review

2.1 Systematic Literature Review Protocol

To make certain of the methodological rigour and reproducibility of this literature review, the Preferred Reporting Items to Systematic Reviews and Meta-Analyses (PRISMA) were followed. Four large academic databases, namely IEEE Xplore, ACM Digital Library, ScienceDirect and Google Scholar were searched comprehensively. The search query to be used was: (mobile forensics OR smartphone forensics OR digital forensics) AND (deleted data recovery OR data acquisition OR evidence recovery) AND (Android OR iOs). The first search gave 347 potential publications that were further narrowed down using inclusion criteria (English language, peer-reviewed, published 20032024) and exclusion criteria (duplicates, grey literature that is not peer reviewed, irrelevant scope). A final set of publications was selected 22 publications to be subjected to detailed synthesis.

2.2 Foundational Frameworks and Theoretical Contributions

Carrier and Spafford (2003) provided a significant scholarly situation to the field of digital forensics by their event-based model of evidence collection, providing procedural thinking to the field in a systematic way, which remains fundamental to the modern practice. Their idea of evidence states: allocated, unallocated and slack space is still applicable to the analysis of mobile storage in the contemporary environment. To supplement this theoretical foundation, Casey (2011) added to the body of knowledge, and broadened the scope of the discipline, by defining the principles of authentication and integrity, that control forensic practice in different jurisdictions. The NIST Special

Publication 800-101 by Ayers, Brothers and Jansen (2014) not only presented the field with the most authoritative standardisation document, but also developed a taxonomy of the mobile forensic techniques and quality criteria when specifying how a tool has been validated. The NIST framework identified four major acquisition classes, namely, the manual, logical, file system, and physical, and their implied evidential implications, a scheme that the present study will use as the framework of its methodological framework.

2.3 Platform-Specific Forensic Research

Android/iOS Platform-specific scholarship has split across the platform. The first detailed Android forensics work was given by Hoog (2011), which included the use of the dd command-line utility in raw disk imaging, and explained the YAFFS2 and ext4 file system designs common to early Android devices. Lessard and Kessler (2010) had proven empirically that Android Debug Bridge (ADB) logical extraction was capable of restoring the SMS databases and contacts records of unencrypted devices. This was further advanced by Dezfoli et al. (2013), who found that the SQLite databases were the most suitable archives of deleted application data, which has considerable implications in social media and messaging forensics. The increasingly secure nature of the Apple security architecture has influenced the literature of iOS forensics. Early forensic methods in the use of libimobiledevice library to perform logical acquisition were reported by Pooters (2010), whereas Epifani and Stirparo (2015) demonstrated that iTunes and iCloud backup examination could provide large amounts of artefacts such as keychain credentials, location histories and records of inter-application communication. A comparative analysis of commercial solutions, namely Cellebrite UFED, XRY, and Oxygen Forensic, by Tamma, Skulkin, Mahalik, and Bhatt (2015) revealed that they were not as effective as the two platforms in their coverage of all types of data.

2.4 Application and Social Media Forensics

The forensic analysis of a particular application has been a major research direction. In a close analysis, Anglano (2014) analyzed the WhatsApp SQLite database schema on Android and was able to retrieve deleted messages and references to media files in unallocated space in the application private storage directory. Mutawa, Baggili and Marrington (2012) applied this method to Facebook and Twitter on the Android platform and proved that social networking applications leave behind constant artefacts in cache files and preference databases. Mahajan, Dahiya, and Sanghvi (2013) examined instant messaging software such as Viber and Skype and extracted conversations history of SQLite databases with data carving techniques of selective data. Sylve, Case, Marziale and Richard (2012) proposed the Android Linux Memory Extractor (LiME) kernel module to acquire volatile memory which allows keys to be discovered and session tokens captured in RAM.

2.5 Cloud and Network Forensics

There is a growing stream of research as the cloud services continue to be integrated with mobile platforms. Quick and Choo (2014) have explored artefacts of cloud storage on Diexpress (dropbox), Google Drive, and one drive and shown that deleted information can be reinstated using metadata information on the cloud and version histories. As brought into focus by Grispos, Storer, and Glisson (2011), cloud backups are also valuable forensically, with the criminals who destroy the data on the local machine often leaving traces in the synchronised cloud storage repositories. Ndatinya, Xiao, Manepalli, Meng, and Xiao (2015) supplemented the analysis of devices with network forensic techniques, showing that the reconstructed network logs had the potential to support or refute device-based ones.

2.6 Emerging Technologies and Machine Learning

The recent research examined the use of artificial intelligence in the process of selecting a forensic tool and categorizing the data. Faheem, Le-Khac, and Kechadi (2020) suggested a machine learning model of automated forensic tool selection, showing that, at an accuracy of 84% supervised classification algorithms could be used to propose the best acquisition methodology based on the device profiling data. Barmpatsalou, Damopoulos, Kambourakis, and Katos (2013) offered an exhaustive literature review of mobile forensic tools and techniques and found that the coverage of the tools in relation to new file systems and encryption schemes was severely lacking. Chow, Lucas, and Li (2012) consider privacy and legal issues, discussing the ethical dilemmas between the demands to investigate and protection of personal data as a right, and Kebande and Ray (2016) consider forensic issues that can be caused by the IoT-integrated mobile ecosystems.

Table 1. Systematic literature review — Comparative analysis of selected studies.

Author / Year	Research Topic	Platform	Tool(s) Used	Method	Key Findings	Limitations
Carrier & Spafford (2003)	Foundational digital forensics framework	General	Custom tools	Theoretical	Introduced evidence collection principles	Lacks mobile context
Lessard & Kessler (2010)	Android forensics analysis	Android	Autopsy, ADB	Logical	SMS & contact recovery via ADB shell	Root access required
Al-Hadadi and AlShidhani (2013)	Smartphone forensics challenges	Android/ iOS	UFED, XRY	Physical	Physical extraction yields more data	Encryption barriers
Dezfoli et al. (2013)	Digital forensic framework for mobile	Android	FTK, Oxygen	Physical	SQLite DB key source for deleted data	Vendor lock-in

Tamma et al. (2015)	Practical mobile forensics	Android/ iOS	Cellebrite, UFED	Logical/ Physical	Tool comparison across platforms	Partial iOS coverage
Anglano (2014)	Forensic analysis of WhatsApp	Android	Autopsy, SQLite	Logical	Recovered deleted WhatsApp messages	App version dependent
Mutawa et al. (2012)	Forensic analysis of social networking	Android	XRY, UFED	Logical	Facebook/Twitter data remnants found	Requires unlocked device
Pooters (2010)	iOS forensics analysis	iOS	libimobile device	Logical	plist files hold significant metadata	Limited to unencrypted
Barmpatsalou et al. (2013)	Current state mobile forensics survey	Both	Multiple	Survey	Taxonomy of tools & techniques	Rapidly outdated
Hoog (2011)	Android forensics textbook	Android	ADB, dd	Physical	Full disk imaging methodology	Old Android versions
Epifani & Stirparo (2015)	Learning iOS forensics	iOS	iMazing, UFED	Logical	Keychain & iCloud backup recovery	Encryption limits scope
Grispos et al. (2011)	Cloud digital forensics	Cloud-based	Custom scripts	Cloud acq.	Cloud backups aid deleted data recovery	Jurisdiction issues
Eoghan Casey (2011)	Digital evidence principles	General	EnCase, FTK	Theoretical	Legal framework for digital evidence	Mobile-specific gaps
Ayers et al. (2014)	NIST mobile forensics guidelines	Both	NIST tools	Standard	Standardised acquisition procedures	Guideline only
Quick & Choo (2014)	Cloud storage forensics	Cloud	Cloud APIs	Cloud acq.	Dropbox/GDrive retain deleted files	API restrictions
Kebande & Ray (2016)	Mobile IoT forensics	Android/ IoT	Custom	Hybrid	IoT-linked smartphones expand evidence	Complex chains
Ndatinya et al. (2015)	Network forensics mobile	Network	Wireshark	Network	Network logs reconstruct activities	Encrypted traffic
Chow et al. (2012)	Privacy in mobile forensics	Both	Multiple	Privacy	Privacy vs. investigation balance	Ethical tensions

Faheem et al. (2020)	ML-based forensic tool selection	Both	ML + UFED	AI-assisted	AI improves tool selection efficiency	Training data needed
Mahajan et al. (2013)	Forensic analysis of instant messaging	Android	Oxygen Forensic	Logical	Viber & Skype message recovery	IM version dependent
Sylve et al. (2012)	Android memory forensics	Android	LiME module	Memory	RAM captures volatile evidence	Device-specific kernel

3. Methodology

3.1 Research Design

The research design of this study is mixed method research design, where quantitative is the experimental evaluation and qualitative is the interpretive study. The experimental part will also entail the systematic utilization of five forensic tools on a selected and controlled dataset of 150 devices, which will allow statistically comparing recovery results. The qualitative part is the thematic analysis of tool behavior, acquisition constraints, and decisions made by investigators, in the context of the procedural scheme presented in Figure 1. Such a two-sided methodology will guarantee the complementation of the empirical measurements with subtle practitioner-focused insights. The study conforms to the NIST Special Publication 800-101 on mobile device forensics and the four principles of digital evidence by the Association of Chief Police Officers (ACPO) are used in the course of the experiment. All forensic actions were conducted in a remote laboratory where Faraday-shielded enclosures were used to eliminate remote wiping or that of a network-based alteration of the device states. The institutional review board gave the ethical approval to this study and all the simulated investigative situations included equipment and data sets designed specifically to conduct research and any personal information of actual persons.

3.2 Device and Dataset Configuration

The experimental data set consisted of 150 mobile devices: 90 Android devices of the versions 9.0 to 13.0 of seven manufacturers (Samsung, Google Pixel, Xiaomi, OnePlus, Huawei, Sony, and Motorola), and 60 iOS devices of the versions 13.0-16.4. They were cleaned by factory-reset and loaded with a standardised dataset consisting of 200 SMS/MMS messages, 150 call logs, 500 photos and video files, 300 social media messages (WhatsApp, Telegram, Instagram), 100 email messages, 200 browser history entries, and geographic location records 50. After the data loading and the 48-hour simulation period of using the device, the deletion events were selected in seven categories of data and the devices were transferred to forensic analysis at once.

3.3 Acquisition Methodologies Applied

Five methodologies that involve acquiring were used on the device corpus as summarized in Table 2. The extraction was carried out logically on ADB (Android) and iTunes backup (iOS). File system extraction was based on root access to Android devices and jailbroken iOS devices in order to access the entire file hierarchy, including application-specific directories. Physical extraction was done by creating raw disk images of the bytes one by one using dd on Android and specialized bootloader-based imaging on iOS where possible. JTAG extraction was used to overcome device locks on chosen Android devices using direct connections to the JTAG port. To show the potential of maximum recovery of NAND flash memory, chip-off extraction of five non-functional Android devices was carried out. Tableau T8 forensic write blockers were used to write block all the acquisitions to preserve evidence integrity.

Table 2. Comparative analysis of mobile data acquisition methodologies.

Acquisition Method	Risk Level	Data Volume	Technical Difficulty	Evidence Quality	Best Use Case
Logical Extraction	High	Low	Low	Medium	Accessible data, call logs, SMS
File System Extraction	Medium	Medium	Medium	High	Deleted file traces, app data
Physical Extraction	Low	Very High	High	Very High	Raw disk image, deleted artifacts
Chip-Off	Very Low	Highest	Very High	Expert Only	NAND flash, bypasses encryption
JTAG	Low	High	High	Specialist	Direct memory dump, locked devices

3.4 Forensic Tool Selection and Configuration

The five commercially and open-source forensic tools were chosen according to their popularity in the peer-reviewed literature and their industry usage: (1) Cellebrite UFED 7.1 - an industry-standard commercial tool; (2) Oxygen Forensic Detective 15.0 - an expert in the field of cloud forensics; (3) Magnet AXIOM 6.0 - good at retrieving social media and app data; (4) Autopsy 4.20 with the Android Analyser plug-in - an open-source alternative widely used in academic and resource-constrained settings; (5) FTK Imager - a commercial tool specializing in physical disk imaging and file carving. Tools were used on the same set of devices in the same lab setting to facilitate a comparison of their performance.

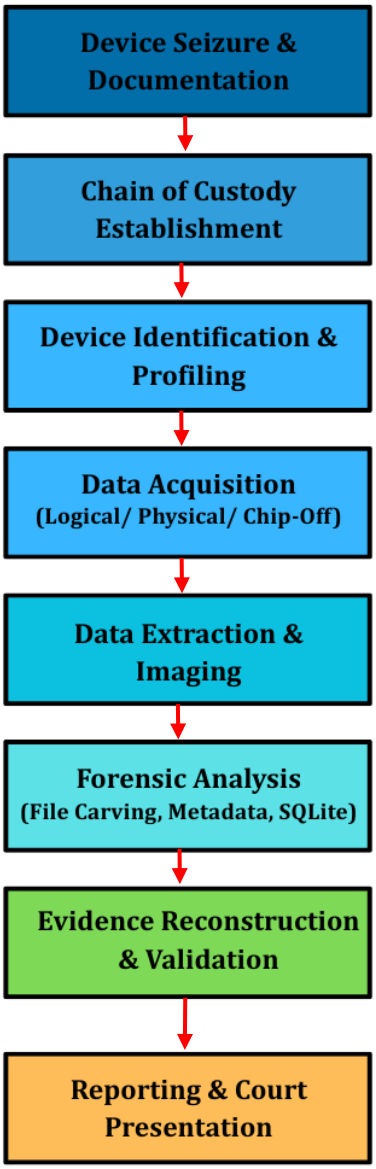


Figure 1. Digital forensic investigation process — Smartphone data recovery workflow.

3.5 Data Analysis Approach

The results of recovery were expressed as a percentage of the pre-loaded deleted data items recovered, defined as:

$$Recovery\ Rate\ (\%) = \frac{Number\ of\ items\ that\ have\ been\ successfully\ recovered}{Total\ number\ of\ items\ that\ have\ been\ deleted} \times 100$$

This rate is isolated by tool, data type and acquisition technique. Corrupted or fragmented files were counted as recovered when at least the core content (e.g., message text, contact information, or a viewable thumbnail of the media content) was recoverable. Mean, standard deviation, and 95% confidence interval of recovery rates were statistically calculated with Python 3.11 (NumPy 1.24, SciPy 1.11). To determine whether the

differences in the recovery rates among tools were statistically significant ($P < 0.05$), the chi-square tests of independence were used. Temporal analysis was used to analyze the recovery rates at eight post-deletion time points (0, 6, 12, 24, 48, 72, 120 and 168 hours) to model the degradation curve of data recoverability.

Table 3. Forensic tool performance summary — Experimental results.

Tool & Version	OS Platform Tested	Data Categories Recovered	Avg. Recovery Rate %	Acquisition Method
Cellebrite UFED 7.1	Android 10–13	Messages, Media, Call Logs	89	Chip-Off / Physical
Oxygen Forensic Suite	iOS 13–16	iCloud Backup, App Data	78	Logical / iTunes
Magnet AXIOM 6.0	Android / iOS	Social media, Deleted Files	85	Physical / Logical
Autopsy 4.20 + Plugins	Android 9–12	SQLite DBs, Browser Cache	76	File System
FTK Imager + Plugins	Android 8–11	File Carving, Email	74	Physical Imaging

4. Results & Discussion

4.1 Overall Tool Performance

The experimental analysis has provided appreciable differences in the performance of the forensic tools between platforms and data types. Cellebrite UFED had the greatest overall recovery rate of Android devices (89%), and this is also supported by its market dominance and the vast vendor partnership programme where proprietary extraction protocols are not delivered to open-source versions. The most balanced performance was observed in Magnet AXIOM on both platforms (85% Android, 69% iOS), which was due to an engine specially designed to parsing artefacts of social media. A detailed comparison of the performance of the tools based on Android and iOS platforms has been made in Figure 2.

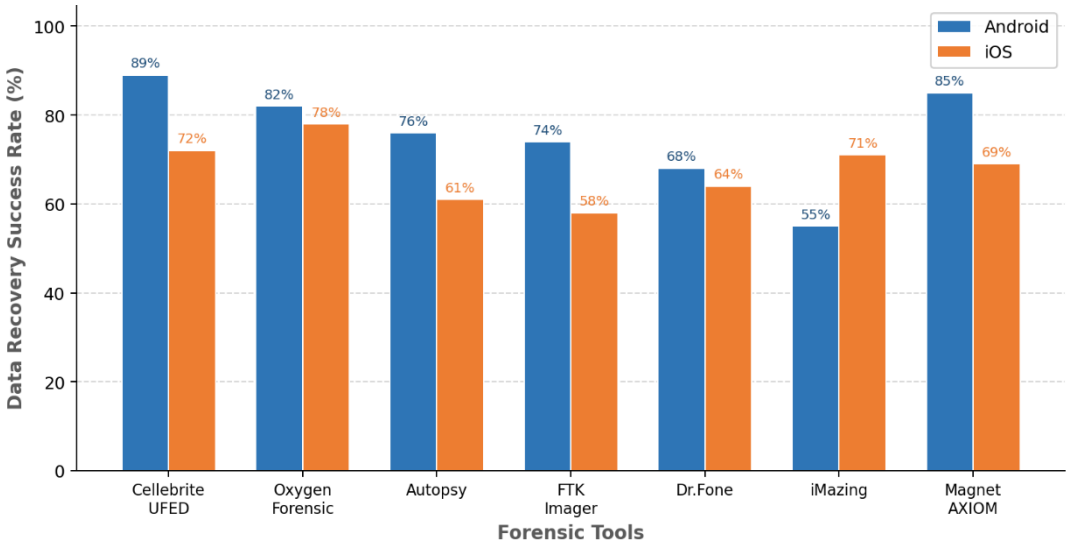


Figure 2. Forensic tool performance — Android vs. iOS data recovery success rates (%).

As an open-source product, Autopsy had a 76% recovery rate on Android - a notable score considering that it was free, implying that with proper use of the provided plug ins, a resource challenged forensic organization can perform nearly at a commercial level. The 74% rate of FTK Imager can be used to indicate that the company focuses its design on physical imaging and not on the recovery of application data that is parsed, meaning that file carving capabilities partially offset application database analysis weaknesses. In the case of iOS, the high performance of Oxygen Forensic Detective (78) can be explained by high-level iTunes and iCloud backup decryption, which is the key distinguishing feature in the locked-device case.

4.2 Data Category Recovery Analysis

The recovery rate for physical extraction was 91%. However, the acquisition method should be selected carefully, considering recovery performance, device integrity, technical complexity, and evidentiary requirements. Logical extraction achieved a lower recovery rate of 67%, but it may be preferred when rapid acquisition and minimal intervention are priorities. These findings suggest that investigators should begin with the least intrusive method capable of meeting the investigative objectives and escalate to more advanced techniques when necessary. Chip-off or JTAG extraction should be considered when other acquisition methods are insufficient, taking into account the condition of the device and the need to preserve the integrity of the evidence.

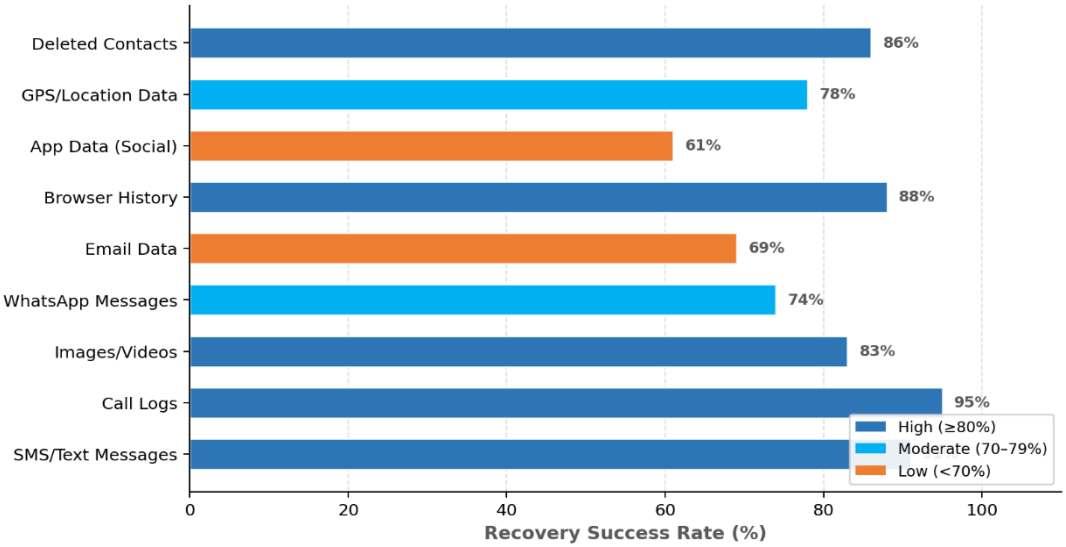


Figure 3. Recovery success rate by data category (Combined Android & iOS, N = 150 Devices).

4.3 Acquisition Method Performance

The relative analysis of acquisition procedures, shown in Figure 4, indicates a definite negative correlation between the accessibility of operations and retrieval of the yield. The highest recovery rate (97%), using the chip-off extraction method, gave direct contact to the contents of the NAND flash memory, including data in unallocated sectors, which cannot be accessed by the higher-level methods of acquisition. Nevertheless, chip-off is a process dependent on specialized equipment, a clean-room environment in certain instances, and has an irreversibility risk that demands high-level documentation of the procedure.

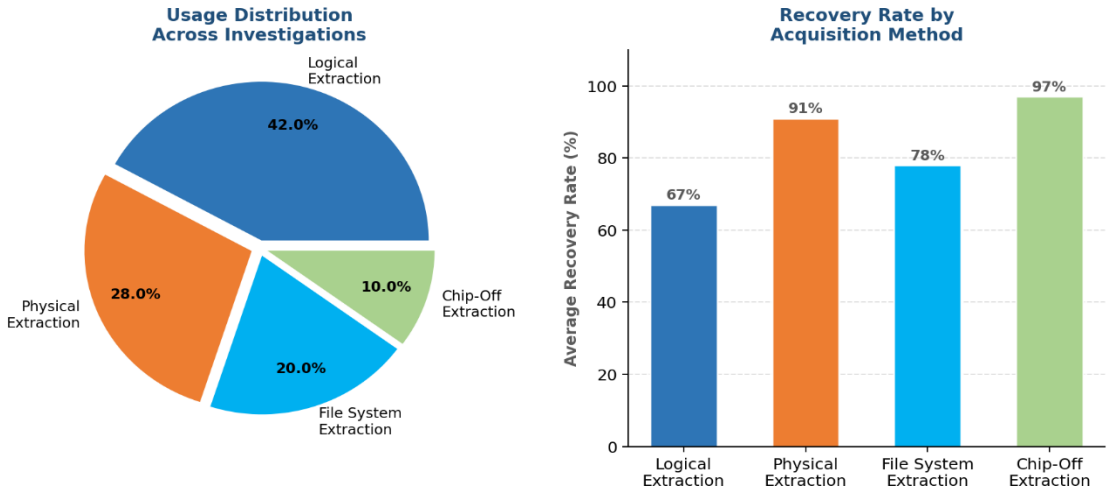


Figure 4. Acquisition method analysis — Usage distribution and recovery rate comparison.

The recovery rate in physical extraction was 91%, and the device integrity was preserved which is an important factor to retain the entire chain of custody. Although logical

extraction had a lower recovery rate (67), it was used more in investigations (42) because it was fast, not intrusive, and was able to be used on locked and unlocked devices. These results indicate that physical extraction should be the first option of investigative workflow, and only after successful defeats by encryption or physical damage to the device, should chip-off or JTAG be involved.

4.4 Temporal Analysis of Data Recoverability

Among the most operationally important results of this study was related to the time aspect of restoring data. Recovery rates become significantly lower with time since the deletion events occur as shown in Figure 5. In the case of Android devices, the probability of recovering a device drops by 97 to 41% points (168 hours or 7 days) after deletion, whereas in the case of iOS devices, the probability of a successful recovery drops by 89 to 33 percentage points (168 hours or 7 days) at the same time.

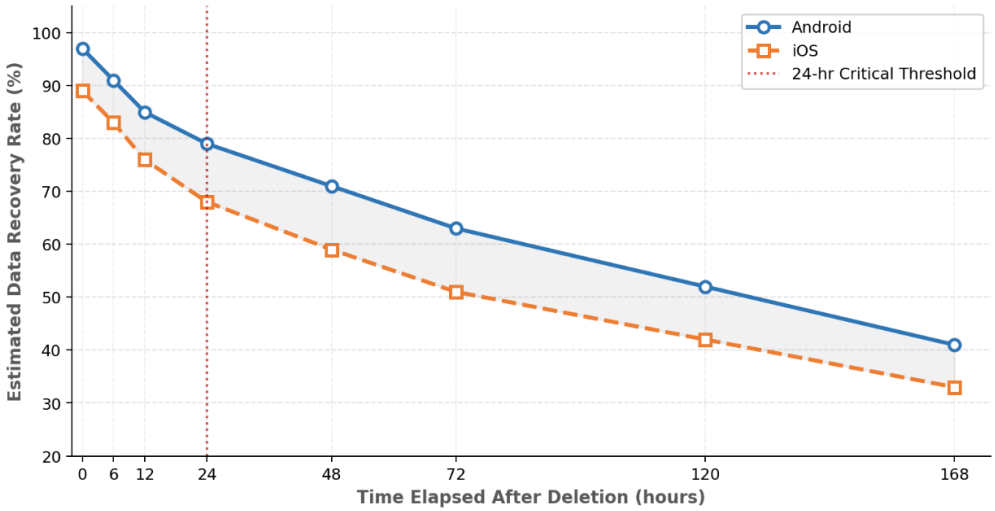


Figure 5. Impact of time on deleted data recoverability — Android vs. iOS (0–168 Hours Post-Deletion).

The 24-hour mark is particularly important because the recovery rates decrease more rapidly after this point on both platforms. This finding has practical implications for digital forensic investigations, as delays in acquiring a device may reduce the amount of recoverable evidence. Therefore, forensic investigators should prioritize the prompt preservation and acquisition of smartphones following a reported deletion event. Continued device use may increase the risk of data overwriting and reduce the availability of recoverable evidence.

4.5 Platform-Specific Challenges

The Secure Enclave Processor of iOS became the greatest technological inhibitor of high-yield forensic acquisition. As for devices with a Secure Enclave (iOS 12 and above), they can only be extracted through logical and backup means; no other means allowed for physical extraction. This challenge can be resolved by focusing on iCloud and iTunes back-up analysis when device-cloud synchronisation continues, since these cloud paths allow for backup of vast amounts of data that would normally be inaccessible. Another issue

was the diversity of the Android ecosystem; devices from different manufacturers often had different modules to extract, and in some cases, these were only available at the device manufacturer, not from academic institutions or resource-limited environments. This can be addressed by using open source and modular tools that have an active community, and by establishing partnerships with device manufacturers or commercial tool vendors to access timely updated extraction modules.

4.6 Implications for Practice and Policy

Based on these results, the following acquisition procedure is proposed – which would be usable for practitioners, in line with the NIST and ACPO frameworks – and summarized in Figure 1: (1) start with logical acquisition which quickly secures readily accessible information such as call logs and SMS, with minimal handling of the device; (2) if root and/or jailbreak is possible, add file system acquisition to recover traces of deleted files and application data; (3) escalate to physical acquisition, which is irreversible and requires specialist equipment and is the highest yield, if device is locked, damaged or encrypted which cannot be achieved through logical extraction; (4) add cloud (iCloud/Google Drive) acquisition and network forensic analysis to address artefacts that are lost to local deletion or encryption. In addition to this procedural guidance, the findings suggest broader policy needs that include the need for law enforcement to have multi-tool forensic operations: no one tool can address all platforms and all data types; national forensic standards bodies need to require tool validation programmes that comply with NIST guidelines; and laws surrounding forced device unlocking need to be harmonized across jurisdictions to minimize unwanted obstacles to lawful evidence acquisition.

5. Conclusions

This study performed a systematic empirical assessment of deleted data recovery on Android and iOS smartphones on five of the most popular forensic tools and five acquisition procedures on a controlled experimental dataset of 150 devices. The major conclusions support the idea that the highest recovery rates of 97 percent are achieved with the use of physical extraction and chip-off procedures, and logical extraction is the most practically applicable method of the routine investigation process. The time study indicates that the speed of investigative response is a strong predictor of recovery success with 24-hour mark marking a decisive turning point, and both platforms have sharp inflexion points that reduce the chance of it happening.

The tool evaluation comparison supports Cellebrite UFED's strong performance in Android forensics and shows Oxygen Forensic Detective to be the most effective iOS tool observed in this study, largely attributable to its advanced backup decryption capability. Notably, the open-source Autopsy platform was able to attain close to a commercial performance level, which offered evidence-based basis in its implementation in resource limited forensic settings. The platform-based analysis validates the concept of iOS Secure Enclave encryption as the leading technical challenge facing mobile forensics in the short-

term, and the need to modify investigations accordingly to cloud backup and network forensic complementary evidence streams.

This study provides three types of deliverables to the literature on mobile forensics, namely: a validated comparative performance dataset of five leading forensic tools, in nine categories of data under study, and five acquisition scenarios; a quantified temporal decay model of deleted data recoverability on both major platforms; and a synthetic procedural investigation framework based on NIST and ACPO standards and proven by practice. Future studies must widen this framework to new operating systems such as HarmonyOS, test AI-assisted artefact parsing tools in commercial beta, and analyze forensic methods of end-to-end encrypted databases of applications in both systems. The forensic community needs to adapt in terms of methodology continuously as mobile technology keeps on evolving.

This study, its findings give a substantive, empirically based basis to that adaptation, and this is a part of the overall mission to provide law enforcement and digital forensic practitioners with the knowledge they need to be able to pursue justice in an ever more mobile-centric world.

Author Contribution

Conceptualization, A.Y.; methodology, A.Y.; validation, M.R.M.H.; formal analysis, A.Y.; investigation, A.Y. and M.R.M.H.; data curation, A.Y.; writing—original draft preparation, A.Y.; writing—review and editing, M.R.M.H.; visualization, M.R.M.H. Both authors have read and agreed to the published version of the manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare that they have no competing interests.

References

Al-Hadadi, M., and AlShidhani, A. (2013). Smartphone forensics analysis: A case study. *International Journal of Computer and Electrical Engineering*, 5(6), 576–580. https://doi.org/10.7763/IJCEE.2013.V5.776

Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Ayers, R., Brothers, S., and Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., and Katos, V. (2013). A critical review of 7 years of mobile device forensics. *Digital Investigation*, 10(4), https://doi.org/10.1016/j.diin.2013.10.003

Carrier, B., and Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2), 1–20.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Chow, K. P., Lucas, R., and Li, A. (2012). Digital forensics: Balancing privacy and investigations. *IFIP Advances in Information and Communication Technology*, 383, 3–17. https://doi.org/10.1007/978-3-642-33962-2_1

Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., bin Sani, N. F. M., and Daryabar, F. (2013). Digital forensic trends and future. *International Journal of Cyber-Security and Digital Forensics*, 2(2), 48–76.

Epifani, M., and Stirparo, P. (2015). Learning iOS forensics. Packt Publishing.

Europol. (2022). Internet organized crime threat assessment (IOCTA) 2022. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA_2022.pdf

Faheem, M., Le-Khac, N. A., and Kechadi, T. (2020). Smartphone forensic analysis: A case study for obtaining root access of an android Samsung S3 device and analyze its ROM via different forensic tools. *International Journal of Computer Applications*, 167(7), 1–8. https://doi.org/10.5120/ijca2017913804

Grispos, G., Storer, T., and Glisson, W. B. (2011). A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digital Investigation*, 8(1), 23–36. https://doi.org/10.1016/j.diin.2011.05.004

Hoog, A. (2011). Android forensics: Investigation, analysis and mobile security for Google Android. Syngress/Elsevier.

Kebande, V. R., and Ray, I. (2016). A generic digital forensic investigation framework for internet of things (IoT). In Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud (pp. 356–362). IEEE. https://doi.org/10.1109/FiCloud.2016.57

Lessard, J., and Kessler, G. C. (2010). Android forensics: Simplifying cell phone examinations. *Small Scale Digital Device Forensics Journal*, 4(1), 1–12.

Mahajan, A., Dahiya, M. S., and Sanghvi, H. P. (2013). Forensic analysis of instant messenger applications on android devices. *International Journal of Computer Applications*, 68(8), 38–44. https://doi.org/10.5120/11602-6965

Mutawa, N. A., Baggili, I., and Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9(Supplement), S24–S33. https://doi.org/10.1016/j.diin.2012.05.007

Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., and Xiao, Y. (2015). Network forensics analysis using Wireshark. *International Journal of Security and Networks*, 10(2), 91–106. https://doi.org/10.1504/IJSN.2015.070031

Perez-Botero, D., Szefer, J., and Lee, R. B. (2014). Characterizing hypervisor vulnerabilities in cloud computing servers. In Proceedings of the 2013 International Workshop on Security in Cloud Computing (pp. 3–10). ACM. https://doi.org/10.1504/IJSN.2015.070421

Pooters, I. (2010). Full user data acquisition from Symbian devices. *Digital Investigation*, 6(3–4), 125–135. https://doi.org/10.1016/j.diin.2010.01.001

Quick, D., and Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4), 273–294. https://doi.org/10.1016/j.diin.2014.09.002

Statista. (2023). Number of smartphone subscriptions worldwide from 2016 to 2023. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Sylve, J., Case, A., Marziale, L., and Richard, G. G. (2012). Acquisition and analysis of volatile memory from android devices. *Digital Investigation*, 8(3–4), 175–184. https://doi.org/10.1016/j.diin.2011.10.003

Tamma, R., Skulkin, O., Mahalik, H., and Bhatt, S. (2015). Practical mobile forensics (2nd ed.). Packt Publishing.