International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I6P102

Volume 73 Issue 6, 7-15, June 2025

Review Article

Mobile Forensics: Investigation and Tools

P. S. Vinayagam

Department of Computer Science, Pondicherry University Community College, Puducherry, India.

[1]Corresponding Author : psvinayagam@gmail.com

Received: 13 April 2025 Revised: 18 May 2025 Accepted: 03 June 2025 Published: 16 June 2025

Abstract - *Mobile devices, particularly smartphones, have become integral to daily life. The personal and sensitive information stored on these devices has become hot targets for cybercriminals. Crimes such as mobile banking fraud, online scams and payment fraud are taking new forms daily. Mobile phones are also being used for money laundering operations to transfer or exchange illicit funds through mobile payment platforms. Either way, the involvement of mobile phones in committing crimes or mobile devices being targets of attacks has made them a critical source of digital evidence in forensic investigations. To extract evidence from these devices, mobile forensic tools have become essential for law enforcement agencies to preserve, extract and acceptably analyze data from mobile devices in law courts. An in-depth examination of the current state-of-the-art mobile forensic tools is essential to help the investigators make an informed choice while selecting the tools. This paper explores four mobile forensic tools: Cellebrite UFED, XRY, Oxygen Forensics Detective, and Magnet AXIOM. A comprehensive overview of the tools is presented, focusing on their capabilities, technicalities and shortcomings in the ever-evolving mobile ecosystem. Key functionalities such as accessing locked devices, deleted data recovery, app data parsing, cloud storage access, decryption of encrypted data, and timeline generation are discussed to assess the effectiveness of the tools. Even though these tools have become sophisticated over time, they face several technical challenges. No single tool provides a complete solution for mobile forensic investigation. It is recommended that a combination of tools, based on the case-specific requirements, device types and the nature of data extraction, be used. This paper underscores the importance of constant updates, a wide range of device support, and legal compliance to perform mobile forensic tools effectively.*

Keywords - *Cybersecurity, Cyber investigation, Digital forensics, Forensic tools, Mobile forensics.*

1. Introduction

Mobile phones were primarily designed for voice communication. However, over time, they have become multi-functional devices with cameras, internet access, location services, and many other functionalities that use powerful computing capabilities. A big revolution in mobile phones happened in the early 2000s with the introduction of smartphones. These smartphones used mobile platforms such as Symbian, Windows Mobile or BlackBerry OS and allowed the installation of third-party applications. However, another milestone was the release of the Apple iPhone in 2007, which had features like a capacitive touchscreen, internet connectivity and a galaxy of apps. This was followed by the release of Android in 2008, which transformed modern communication.

Today, smartphones have started taking the place of personal computers. They can capture high-resolution images and videos, provide fine location services and provide apps virtually for anything and everything. Because of this, the mobile phones have become an integral part of the people's lives in the modern society. These mobile devices provide convenience and ease of use while being compact and portable.

But these benefits have their downsides. With the rapid developments in mobile technology, criminals also have developed sophistication in exploiting them. These devices are increasingly being used in a variety of illegal activities.

Mobile phones are being targeted by cybercriminals to steal personal details for identity theft, bank account details, login credentials, or to install malware. Phishing attacks and social engineering are usually used by the criminals to deceive the users. Also, owing to the increased userbase of social media platforms and instant messaging apps, the incidents of cyberbullying, cyberstalking and online harassment have increased. The root cause of these incidents is the anonymity inherent in the online interactions. Further, in the case of mobile phone theft, the criminals get easy access to private data stored on the device and the linked cloud services. The unrestricted availability of encrypted messaging apps and phone calls has resulted in the increase of organized crimes such as drug trafficking, human trafficking and prostitution on these messaging apps. Mobile phones are even used for money laundering operations to transfer or exchange illicit funds through mobile payment platforms.

The increased misuse of mobile technology has led to an increased reliance on mobile devices as critical evidence in criminal investigations. Law enforcement agencies often seize mobile phones as part of the investigation. The data stored on mobile devices can provide critical information, including communications, geolocation data, photos, videos and even deleted information. In fraud investigations, data from financial apps and messaging services may provide insight into how the crime was carried out. Mobile phones can also help establish alibis, track criminal movements or identify accomplices involved in illegal activities.

Using location data provided through GPS, investigation agencies can analyze a suspect's location history or real-time tracking to reconstruct the movements of a person leading up to or during a crime. Geolocation data from mobile phones has been used in various cases, including robbery, assault and even terrorism investigations.

However, obtaining data from mobile devices poses numerous challenges. The law enforcement agencies find it difficult to intercept end-to-end encrypted messages. This has often hindered the investigation of criminal activities. Also, remote wiping and locked devices can complicate efforts to access critical information. Hence, law enforcement agencies rely on digital forensic tools to extract, analyze, and preserve data from mobile devices in a forensically sound manner. Though many digital forensic tools are available, they are not well suited to the ecosystem of mobile devices. This has led to the development of mobile forensic tools specifically for handling evidence from mobile devices.

The present paper focuses on this context's widely used mobile forensic tools. The capabilities, technicalities and shortcomings of the tools that are constantly evolving rapidly have been examined. A comparative analysis of the various features has been presented. The rest of the paper is organized as follows. The review of the literature is presented in Section 2. Section 3 briefs the basics of the digital forensic investigation. Mobile forensic investigation is discussed in Section 4. Section 5 details four mobile forensic tools and compares their features. Section 6 summarizes the findings.

2. Literature Review

The field of mobile forensics has evolved significantly in response to the widespread involvement of mobile devices in crimes and their capacity to store Potential Digital Evidence (PDE). Mobile forensics uses established techniques to recover digital evidence from mobile devices such that the evidence is reliable and legally admissible.

A notable contribution to this domain is the study conducted by the authors in [1], which examines the development and structure of Mobile Forensic Investigation Process Models (MFIPMs). This study brings out the various issues in mobile forensics, viz., lack of standardized investigation model, redundancy of processes and concepts, varied mobile device infrastructures and different forensic artifacts. The authors reviewed 100 existing MFIPMs, identifying a lack of uniformity and significant redundancy across models.

The authors propose the Harmonized Mobile Forensic Investigation Process Model (HMFIPM), which aims to unify and structure redundant investigation processes in the mobile forensics field. The state-of-the-art mobile forensic tools, open problems, and future challenges are also discussed.

The authors in [2] explore the growing importance of mobile devices in digital forensic investigations due to their widespread use and the sensitive data they store. The study provides an in-depth review of mobile threats, forensic investigation process models, evidence sources, and available tools. It analyses explicitly and compares tools such as Belkasoft, MOBILedit, and Magnet AXIOM in terms of their data retrieval, analysis, and presentation capabilities. The authors aim to help forensic investigators select appropriate tools based on specific case requirements. The findings highlight the complexity of mobile operating systems and the evolving nature of mobile forensics, emphasizing the need for updated skills and innovative tool development. The paper also discusses key challenges that hinder mobile forensic investigations and suggests ways to improve forensic practices through better understanding and adaptation.

In [3], the authors highlight the critical role of digital forensics in modern criminal investigations, focusing on comparing three widely used tools: FTK, Autopsy, and Cellebrite. Using qualitative and quantitative methods, the authors evaluate these tools based on usability, cost-effectiveness, performance, and functionality.

A case study of the Silk Road investigation illustrates their real-world application. Key findings show that each tool has unique strengths, viz., Autopsy's open-source flexibility, FTK's powerful data processing, and Cellebrite's mobile forensic capabilities. They also face limitations in handling diverse evidence types and ensuring cross-platform compatibility. The study concludes by emphasizing the need for continuous enhancement of forensic tools, particularly in interoperability and data integration, and advises investigators to select tools based on specific case requirements.

The authors in [4] explore the new data types that can serve as potential evidence, the impact of emerging technologies on mobile forensics, and the differences between mobile and traditional computer forensics. It also highlights the limitations of current mobile forensic tools and practices, emphasizing the need for more thorough and advanced approaches to examining mobile phone evidence.

Forensic tools, viz., MOBILedit Forensic Express (MFE), DB Browser for SQLite (DB4S), Oxygen Forensic Detective (OFD) and Final Mobile Forensic (FMF) have been focused upon in [5]. The study reports that FMF has the best extraction capability in obtaining digital evidence. While OFD provides good data acquisition features, MFE performs better in physical evidence preservation and cloning.

The study by the authors in [6] discusses the characteristics of mobile devices and the steps involved in mobile forensic investigation. The performance of Mobiledit Lite and Autopsy tools is compared. It is reported that the Mobiledit Lite comes with a write blocker feature to maintain the integrity of the mobile phone and avoid contamination. It is also observed that Mobiledit Lite and Autopsy alone are not sufficient to recover deleted items. The Timeline Analysis report of the Autopsy proves useful for constructing the sequence of events.

The authors in [7] review open-source and commercial mobile forensic tools and focus on the capability of the tools to locate, track and unlock stolen mobile phones. SOTI, IMEI TRACKER, AirDroid Family Locator, Mobile Tracker Free, mSpy, uMobix, Magnet Forensics and IMEI.INFO are the recommended tools for locating the phone using IMEI. Oxygen Forensics, MOBILedit, Andriller, XRY, SOTI, GrayKey ElcomSoft iOS Forensic Toolkit, Paraben E3: Universal, Mobile Security Framework (MobSF), and Dr. Fone can be used to unlock the phone.

A comparison of free, open-source tools and proprietary tools has been attempted in [8]. The authors have studied four mobile forensic tools: MOBILedit, Oxygen Forensic, Autopsy and Andriller. The study reports that free, open-source tools do not perform as well as proprietary ones. The MOBILedit performs better than the other open-source tools and provides quality reports. The Oxygen forensic tool has proved to be the fastest but has shortcomings in data extraction.

Andriller's digital forensic tool has been focused on in [9]. The tools and methods used to develop effective forensic investigation strategies specifically for Android mobile devices have been elaborated. The study proposes enhancements for the Andriller digital forensic tool to improve its performance in Android forensic investigations. Some improvements include advancements in data extraction techniques, compatibility with new Android versions, support for additional data types, integration with advanced analysis methods, and addressing identified limitations. Special focus is also given to cloud forensics on Android devices to handle data stored in cloud storage services.

The authors in [10] have examined four forensic tools, viz., AccessData FTK Imager, EnCase, MOBILedit Forensic and Oxygen Forensic Suite. The focus is on recovering deleted data from Android phones. The study reports that the AccessData FTK Imager and EnCase performed better than MOBILedit Forensic and Oxygen Forensic Suite in retrieving deleted data. The authors infer that no forensic tool can handle all mobile device platforms.

The performance of the forensic tools in handling Android smartphones in general and WhatsApp in particular has been studied in [11]. For performance evaluation, the authors used parameters from NIST and Whatsapp artefacts. The study reveals that Belkasoft Evidence showcases the highest index number, WhatsApp Key/DB Extractor is better in terms of cost as an open-source tool, and Oxygen Forensic performs better in obtaining WhatsApp artefacts.

The literature review shows that mobile forensics faces numerous challenges owing to the diversity of mobile devices, operating systems, apps, security mechanisms and encryption techniques. Mobile forensics tools are also undergoing rapid changes in their capabilities, technicalities, and shortcomings. In this direction, this paper provides an in-depth examination of the current state-of-the-art mobile forensic tools to help investigators make an informed choice to select the correct tool.

3. Digital Forensic Investigation

Digital forensics is identifying, preserving and analysing digital evidence from electronic devices as part of cybercrime and other criminal investigations. Digital forensic investigation emphasizes following a systematic approach to identify, collect, preserve, analyze, document and present data that maintains its integrity for use in court or other legal proceedings.

Digital forensic investigation requires various digital forensic tools that cater to the investigation needs. The scope of the digital forensic tools during the initial years focused on data access or recovery from hard disk drives. However, as technology evolves, the field has expanded to encompass Operating Systems, Live Memory, Web, Email, Network, Multimedia, Mobile and Database. There is a need for forensic investigators to keep pace with new methods, tools and challenges. No one tool can handle all these varied sources of evidence.

Digital forensics can be classified into the following specialized areas [12, 13]:

a) Operating System Forensics
b) Disk and File System Forensics
c) Live Memory Forensics
d) Web Forensics
e) Email Forensics
f) Network Forensics

g) Multimedia Forensics
h) Mobile Forensics
i) Database Forensics

Digital forensics assist in criminal investigations, civil litigation, corporate security incidents and counterterrorism efforts. The investigators find what happened, where, when, how, who was involved, why, and what digital evidence is available. This is because digital evidence is often one of the most reliable forms of evidence that can provide insight into an individual's activities, communications, and online behavior [14].

Forensic investigations require a meticulous and systematic approach involving documentation, chain of custody, and accepted industry standards and tools. Digital forensic investigators must adhere to a strict set of guidelines to maintain the integrity and admissibility of the evidence. From encrypted files to cloud storage, each platform presents its unique forensic challenges.

The methods employed to detect and investigate crimes require constant improvement owing to the increase in the sophistication of crimes. This has led to the development of advanced forensic tools and techniques that could address the challenges posed by modern technology.

4. Mobile Forensic Investigation

Mobile forensics is a subfield of digital forensics that focuses on extracting, preserving and analysing data stored in mobile devices, such as smartphones and tablets [15]. These devices have become a significant source of digital evidence in both criminal investigations and civil litigation.

The data available on these devices provide critical information, including communications, geolocation data, photos, videos, social media activity and even deleted information [16]. Data from financial apps and messaging services provide insight into the modus operandi of the crime.

Mobile forensics is complex, as mobile devices use various operating systems (iOS, Android, Windows, Blackberry, Symbian, etc.), each with unique security protocols and data structures. Mobile forensic experts must be skilled in handling diverse technicalities while ensuring the data is collected, analyzed and preserved according to established procedures to avoid contamination or legal issues [17].

Early mobile forensics investigations focused primarily on call logs and text messages. However, with advancements in mobile technology, investigators can now extract a much wider range of data, including encrypted information and data stored in cloud backups associated with the device.

Mobile forensics typically involves the following steps – Preservation, Acquisition, Examination and Analysis, and Reporting. Preservation involves the search, recognition, documentation, and collection of electronic-based evidence. Acquisition is the process of imaging or otherwise obtaining information from a mobile device and its associated media [18].

This is followed by the examination process, which is used to uncover digital evidence, even if it is hidden or obscured. The examination results are utilized in the analysis step to look for any significance and value to the case under consideration. The difference between examination and analysis is that a technical process is usually performed by a forensic specialist, whereas analysis may be performed by the investigator or forensic examiner [18].

The next step is reporting, wherein a detailed summary of all the steps performed and the inferences made are documented. It involves recording all the actions performed and the observations made therein. The results of tests and examinations and the inferences drawn should be maintained. The report includes the tool-generated content and other relevant documentation, notes and photographs as applicable and available [18]. This report is a crucial part of the forensic process, as it can be used as evidence in court.

Throughout the mobile forensic investigation, preserving the data's integrity is critical. This includes maintaining a chain of custody, taking detailed notes, and ensuring the data is stored securely and forensically soundly. Any potential evidence must be handled with utmost care to prevent tampering, contamination, or accidental loss of data [19].

Mobile forensic investigations present several unique challenges, such as Encryption, Device locking, App Data and Cloud Storage. Many modern smartphones have built-in encryption features to protect user data. This can pose significant challenges for investigators, as encrypted data is difficult or impossible to access without the proper decryption key [20]. Mobile devices often have password protections or biometric security features (such as fingerprint or facial recognition) that can make gaining access to the device difficult. Many apps store data in proprietary formats, and extracting this data may require specific knowledge of the app's structure and custom tools. Many mobile devices sync their data with cloud services like Google Drive, iCloud, or Dropbox. Investigating this cloud data adds complexity to mobile forensics because data may be located outside the physical device, and different cloud service providers have varying levels of cooperation with law enforcement [14, 18, 20].

5. Mobile Forensic Tools

Numerous forensic tools are available for mobile forensic investigation. They differ in the range of capabilities they offer, operating systems they cater to and the type of analysis they perform. This paper examines four widely used mobile forensic tools: Cellebrite UFED (Universal Forensic Extraction Device), XRY, Oxygen Forensics Detective, and Magnet AXIOM.

5.1. Cellebrite UFED (Universal Forensic Extraction Device)

Cellebrite UFED, developed by Cellebrite Digital Intelligence, is a widely used mobile forensic tool. It is widely adopted by law enforcement agencies, intelligence agencies and investigators. The software provides data extraction facilities for smartphones, drones, SIM cards, SD cards, GPS devices, and legacy phones. The supported extraction methods are logical extraction, physical extraction, file system extraction, and cloud data extraction.

The logical extraction method can extract call logs, messages and contacts using device APIs. To make a bit-for-bit copy of storage, a physical extraction method is used. The physical extraction methods are powerful in that they allow for the recovery of messages, call logs, multimedia files and application data that might otherwise be inaccessible due to encryption or deletion. The cloud extraction method is used to retrieve data from Google Drive, iCloud and WhatsApp backups. The software can decrypt iOS backups, Android File-Based Encryption and app data. Cellebrite Physical Analyzer (PA) tool can perform SQLite parsing, timeline reconstruction and data carving. The latest tool, Inseyets, is the latest addition complementing PA [21].

UFED supports various mobile operating systems such as Android, iOS, Windows Phone, BlackBerry, Bada and Symbian. UFED also provides analysis and reporting capabilities to aid criminal investigations. The software can access and extract data from locked screens or encrypted devices. This makes the software invaluable for law enforcement agencies, military and intelligence agencies. The UFED's core function relies on the hardware and software suite that can bypass device security measures, retrieve deleted data and perform advanced logical and file system-level analysis [21].

The software is continuously updated with the latest versions, targeting the inclusion of features to match the latest developments in mobile technology. The updates also support the latest device models and operating system versions.

Additionally, UFED's ability to analyze app data from various social media and messaging platforms such as WhatsApp, Facebook and Instagram makes it particularly useful for investigating cybercrime and terrorism. This provides forensic investigators with a valuable tool for data retrieval.

The software has a user-friendly interface that simplifies the extraction process for investigators with varying levels of technical expertise. Additionally, the tool integrates with other Cellebrite products, such as the Physical Analyzer, to provide a complete end-to-end solution for mobile forensic investigations. For investigators handling complex cases, the UFED allows customized reports that can be directly utilized in courtrooms [21].

The extracted data are stored in a secure format by the UFED tool. This is essential to meet forensic standards and to preserve the integrity of the evidence throughout the investigative process. The audit trail functionality can document every step of the extraction process and ensure transparency.

However, Cellebrite is not without shortcomings. Cellebrite's ability to bypass security depends on device models, operating system versions and encryption methods. Some newer devices may require Cellebrite Advanced Services or remain partially inaccessible. UFED may be unable to access locked or encrypted devices using newer iOS and Android versions. The ability to parse app data depends on the app version, operating system version, and whether the app data is encrypted or stored in sandboxed storage.

5.2. XRY

XRY is an advanced mobile forensic tool developed by Micro Systemation AB (MSAB). The software enables the extraction and analysis of data from a wide variety of mobile devices. Supported devices include smartphones, tablets, GPS units, and even feature phones. XRY can also retrieve data from devices at various levels of security. Even locked or encrypted devices are accessible using this tool. The XRY tool supports both logical extraction and physical extraction methods. The logical extraction method is used to extract SMS, call logs, and contacts, and the physical extraction method is used for a full file system dump.

There are various tools like XRY Pro, Logical, Physical, Photon, Cloud and Camera for data extraction with varying capabilities to suit the needs of the investigator. The software can recover SIM card data and SD card artefacts. The software supports data extraction from apps such as WhatsApp and Signal [22].

The latest version of the tool is compatible with over 44,200 devices and over 4,360 app versions. This ensures that the professionals and investigators can extract data from almost any mobile device. The tool supports various mobile operating systems such as Android, iOS, Windows Phone and feature phone operating systems, making it an essential tool for investigators working with diverse mobile technologies. The software can extract critical data such as text messages, call logs, contacts, multimedia files, app data, and even deleted files, which is crucial for solving complex criminal cases.

One of the highlights of the software is its ease of use. Even forensic investigators who do not have advanced technical knowledge can use the tool with ease. The user-friendly interface allows users to perform extractions and generate comprehensive reports, which can be presented in the courts of law. Regular updates are provided so that the tool can be used to extract data even from the latest devices and operating system versions [22]. XRY can recover data from cloud services and accounts using XRY Cloud. The investigators can club the cloud and physical device data to get a complete picture of the digital footprint. The software can recover encrypted or deleted data. This makes the software effective for investigations involving cybercrime, terrorism or drug trafficking [22].

With reference to limitations, though XRY can bypass some device locks, it may not be successful in the case of high-security devices running the latest iOS or Android versions, especially with full disk / file-based encryption. Custom solutions may be required for high-security or the latest models. XRY can recover encrypted and deleted data, particularly if decrypted images or encryption keys are accessible. Signal app data extraction is limited due to the app's strong encryption and sandboxing. The ability to extract data depends on the operating system version and extraction method. XRY cloud acquisition tools require user credentials or token-based access to recover data.

5.3. Oxygen Forensics Detective

Oxygen Forensics Detective from Oxygen Forensics is a comprehensive mobile device forensic tool designed for extracting, analysing, and reporting data from mobile devices. This tool is widely used by law enforcement agencies, cybersecurity professionals and forensic experts. Oxygen Forensics Detective supports a wide range of mobile devices, including smartphones, tablets, drones, and IoT devices, and covers various operating systems such as iOS and Android. The software supports both logical extraction and physical extraction methods. This proves to be an effective mechanism for investigators to access and analyze data stored on mobile devices [23].

This tool can recover deleted data or encrypted data. Various security features such as PIN codes, passwords and biometric locks can be bypassed by the software. This enables investigators to access locked devices. The deep analysis capabilities of the tool allow the extraction of application data, call logs, text messages, multimedia files, and GPS data. It also supports data recovery from messaging applications like WhatsApp and Telegram.

This tool also supports the extraction of data from cloud storage platforms. Oxygen can extract data from Google Drive or iCloud. Even deleted cloud data can be recovered using this tool. This is indispensable in cases where mobile data may have been erased from the device but remains available in cloud backups [23].

The built-in visualization feature of Oxygen Forensics Detective helps forensic experts present complex data clearly and understandably. Detailed reports are generated by this tool that can be used in legal proceedings. There is a facility to ensure that the chain of custody is maintained throughout the investigation process. Regular updates are available for the product. Oxygen Forensics Detectives are valuable for modern forensic investigations [23].

This software also has some shortcomings. Without external support or exploits, it cannot bypass full encryption or secure locks on the latest iOS or Android devices. Oxygen can retrieve cloud backups and synced data but does not recover deleted cloud data unless that data is still accessible in the backup or sync cache.

5.4. Magnet AXIOM

Magnet AXIOM of Magnet Forensics is a digital forensics tool that can extract, analyze and report data from a variety of digital devices, including smartphones, computers, and cloud storage. The interface of the tool is user-friendly. This tool supports many devices and operating systems, including iOS, Android, Windows, macOS, and cloud platforms like Google and Apple iCloud. It can perform logical and file system extractions from devices, providing access to deleted data, app data, and cloud-based information [24].

This tool can extract data from messaging platforms, email services, social media accounts and various apps. This makes it an invaluable tool for investigators working on cybercrime, terrorism, and child exploitation cases. Magnet AXIOM also includes advanced data carving techniques to retrieve deleted or partially overwritten files. The tool can recover various types of evidence, such as call logs, text messages, multimedia files, and web browsing history.

The tool also supports the extraction of data from cloud services. This facilitates data extraction from Facebook, Instagram, and iCloud. The software also provides robust data visualization capabilities, making it easier for forensic professionals to analyze and interpret large datasets. Investigators can use the software without extensive training due to its user-friendly interface. The software provides the facility to generate reports that are in court-admissible format [24].

This tool also has a few shortcomings. AXIOM itself does not perform physical extractions directly from locked or encrypted smartphones. It relies on external acquisition tools like Cellebrite UFED or MSAB XRY to perform the extraction. AXIOM then ingests and analyzes that data. AXIOM can analyze the image but not bypass the lock itself. It can analyze encrypted data only if the decryption keys are available or the data has already been decrypted during acquisition. The tool does not recover deleted data from the cloud unless the deleted content is still cached in the backup/sync data. AXIOM can only extract Signal metadata but not end-to-end encrypted content. This tool cannot bypass iOS/Android hardware encryption.

Table 1 compares the various features and capabilities of the four forensic tools discussed, viz., Cellebrite UFED, XRY, Oxygen Forensics Detective, and Magnet AXIOM. It is evident from the table that most of the tools have become competitive in the features that they provide to the investigators. The tools support data extraction from various devices, including the latest drones and IoT devices. Data extraction from varied operating systems' latest versions and multiple extraction methods are also supported. All the tools have developed capabilities to handle data from social media apps and cloud storage. As advancements are made in the encryption standards, the tools are trying to keep pace with the technology, but there are a few challenges in specific types of advanced encryption systems where decryption without keys is still infeasible. Recovery of deleted data, essential in crime investigations, is also being supported largely, though there are a few limitations. With newer security mechanisms being introduced for mobile devices, the tools face challenges in providing updates for overriding such security measures. Court-admissible customized and detailed reports are generated by all the tools under study. There is good support for integration with other apps for a success rate in data extraction. Updates are being released regularly to keep pace with the technology.

Cellebrite UFED supports many devices and provides extensive data extraction capabilities. However, the requirement for proprietary hardware and licensing costs limits procurement by small organizations. XRY provides a user-friendly interface, and its modular design allows integration with other MSAB tools for effective management and analysis. However, XRY may not effectively handle third-party applications and cloud data. Oxygen Forensic Detective’s built-in analytics features make it an effective tool for building timelines and finding hidden communication patterns. On the downside, the performance of the software may be affected by strong app-level encryption methods. Magnet AXIOM integrates mobile forensics with computer and cloud analysis. It provides the capability to correlate data from multiple sources. The raw mobile extraction features of Magnet AXIOM are not as effective as those of Cellebrite or XRY.

6. Conclusion

Mobile forensic tools have become indispensable in crime investigations. There is a constant need for improvement in mobile forensic tools to efficiently extract, analyze and preserve data in a forensically sound and legally admissible manner. This study examined four widely used mobile forensic tools: Cellebrite UFED, XRY, Oxygen Forensic Detective, and Magnet AXIOM. The tools' capabilities, limitations, and effectiveness in handling data extraction from mobile devices have been compared.

In summary, no single tool currently provides a complete solution for all mobile forensic challenges. The best solution would be to use a combination of tools based on the case-specific requirements, device types and the nature of needed data extraction. Mobile forensic tools need to keep pace with the rapid technological advances. Constant updates, a wide range of device support, legal compliance, and investigator training are critical areas to focus on.

Table 1. Comparison of Mobile Forensic Tools

Tool **Feature**	**Cellebrite UFED**	**XRY**	**Oxygen Forensics Detective**	**Magnet AXIOM**
Developer	Cellebrite Digital Intelligence	MSAB (Micro Systemation AB)	Oxygen Forensics	Magnet Forensics
Device Types Supported	Smartphones, legacy phones, GPS, SIM, SD cards, drones	Smartphones, feature phones, GPS, tablets	Smartphones, tablets, drones, IoT devices	Smartphones, computers, cloud services
Operating Systems Supported	Android, iOS, Windows Phone, BlackBerry, Bada, Symbian	Android, iOS, Windows Phone, feature phone OS	Android, iOS	Android, iOS, Windows, macOS
Extraction Methods	Logical, physical, file system, cloud	Logical, physical, cloud	Logical, physical, cloud	Logical file system (uses external tools for physical)
Encrypted Data Recovery	Yes, limited	Yes, limited	Yes, limited	Only if data is already decrypted or keys are available

Locked Device Access	Yes, limited	Yes, limited	Yes, limited	No
Cloud Data Extraction	Google Drive, iCloud, WhatsApp	Google Drive, iCloud	Google Drive, iCloud	iCloud
App Data Support	WhatsApp, Facebook, Instagram, etc.	WhatsApp, Signal	WhatsApp, Telegram	WhatsApp, Instagram
Deleted Data Recovery	Yes, limited	Yes, limited	Yes, limited	Yes, limited
User Interface	User-friendly	User-friendly	User-friendly with visualization tools	User-friendly with visualization tools
Report Generation	Yes, customizable court-ready reports	Yes, comprehensive reports	Yes, detailed reports	Yes, court-admissible reports
Visualization & Timeline Analysis	Yes	Yes	Yes	Yes
Audit Trail / Chain of Custody	Yes	Yes	Yes	Yes
Regular Updates	Yes	Yes	Yes	Yes
Integration with Other Tools	Yes (PA, Inseyets, UFED Cloud)	Yes (XRY Pro, Logical, Physical, Photon, Cloud and Camera)	Yes	Yes (UFED/XRY)

References

[1] Arafat Al-Dhaqm et al., “A Review of Mobile Forensic Investigation Process Models,” *IEEE Access*, vol. 8, pp. 173359-173375, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Bhavini Patel, and Palvinder Singh Mann, “A Survey on Mobile Digital Forensic: Taxonomy, Tools, and Challenges,” *Security and Privacy*, vol. 8, no. 2, pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Victor Agboola, Jude Osamor, and Funminiyi Olajide, “Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools: A Comparative Study in Criminal Investigations,” *International Journal of Intelligent Computing Research*, vol. 15, no. 1, pp. 1279-1291, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Rizwan Ahmed, and Rajiv V. Dharaskar, “Mobile Forensics: An Overview, Tools, Future Trends and Challenges from Law Enforcement Perspective,” *Proceedings of 6th International Conference E-Governance*, pp. 312-323, 2008. [Google Scholar]

[5] Imam Riadi, Anton Yudhana, and Galih Pramuja Inngam Fanani, “Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation,” *International Journal of Safety & Security Engineering*, vol. 13, no. 1, pp. 11-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ritika Lohiya, Priya John, and Pooja Shah, “Survey on Mobile Forensics,” *International Journal of Computer Applications*, vol. 118, no. 16, pp. 6-11, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[7] Sthembile Ntshangase et al., “A Survey of Digital Forensic Tools for Android and iOS Smart Phones,” *IEEE International Conference on Cyber Security and Resilience*, London, United Kingdom, pp. 139-145, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ramy M. Abou-Elzahab, Mohammed F. Al Rahmawy, and Taher T. Hamza, “Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices,” *Mansoura Journal For Computers and Information Sciences*, vol. 16, no. 1, pp. 1-12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Almaha Almuqren et al., “A Systematic Literature Review on Digital Forensic Investigation on Android Devices,” *Procedia Computer Science*, vol. 235, pp. 1332-1352, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Oluwafemi Osho, and Sefiyat Oyiza Ohida, “Comparative Evaluation of Mobile Forensic Tools,” *International Journal of Information Technology and Computer Science*, vol. 8, no. 1, pp. 74-83, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[11] Rusydi Umar, Imam Riadi, and Guntur Maulana Zamroni, “A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 12, pp. 69-75, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Abdul Rehman Javed et al., “A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges and Future Directions,” *IEEE Access*, vol. 10, pp. 11065-11089, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Sakshi Singh, and Suresh Kumar, “Qualitative Assessment of Digital Forensic Tools,” *Asian Journal of Electrical Sciences*, vol. 9, no. 1, pp. 25-32, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., San Diego, CA, USA: Academic Press, 2011. [Google Scholar] [Publisher Link]

[15] EC-Council, Mobile Device Forensics: What it is and how it’s used in Investigations, Cybersecurity Exchange, 2025. [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/mobile-device-forensics/

[16] Marie-Helen Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence*, 2nd ed., Burlington, MA, USA: Jones & Bartlett Learning, 2014. [Google Scholar]

[17] Bruno M. V. Bernardo et al., “Mobile Device Forensics Framework: A Toolbox to Support and Enhance This Process,” *Emerging Science Journal*, vol. 8, no. 3, p. 972, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Rick Ayers, Sam Brothers, and Wayne Jansen, “Guidelines on Mobile Device Forensics,” NIST SP 800-101 Rev. 1. Gaithersburg, MD: NIST, 2014. [Google Scholar] [Publisher Link]

[19] United Nations Office on Drugs and Crime, Handling of Digital Evidence, Cybercrime Module 6 Key Issues, 2015. [Online]. Available: https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[20] Tanita Singano et al., “Digital Forensics Investigations: Major Challenges in Mobile and Cloud Forensics,” *Towards New e-Infrastructure and e-Services for Developing Countries*, vol. 588, pp. 35-53, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Cellebrite UFED, Cellebrite, 2025. [Online]. Available: https://cellebrite.com

[22] XRY - Mobile Device Forensics, Micro Systemation, 2025. [Online]. Available: https://www.msab.com/product/xry-extract/

[23] Oxygen Forensics Detective, Oxygen Forensics, 2025. [Online]. Available: https://www.oxygenforensics.com

[24] Magnet Forensics, Magnet AXIOM, 2025. [Online]. Available: https://www.magnetforensics.com/products/magnet-axiom/