

A Comparative Analysis of Mobile Forensic Tools: Evaluating Extraction Efficacy in the Age of Encryption

Soukya U¹, Dr H R Bhargava²

¹ Postgraduate, Garden City University

² Professor, Garden City University

Abstract - The rapid evolution of mobile technology, coupled with the widespread adoption of advanced encryption mechanisms, has significantly impacted the field of digital forensics. Mobile devices now store vast amounts of sensitive personal and organizational data, making them critical sources of digital evidence in criminal investigations. However, strong encryption techniques, secure boot processes, and privacy-focused operating systems have introduced substantial challenges for forensic investigators. This research paper presents a comparative analysis of leading mobile forensic tools, focusing on their extraction efficacy in encrypted environments. Tools such as Cellebrite UFED, Oxygen Forensic Detective, and Autopsy are evaluated based on their ability to perform logical, file system, and physical data extractions across different mobile platforms. The study examines factors such as data recovery rate, handling of encrypted data, compatibility with various devices, and overall reliability. The findings aim to highlight the strengths and limitations of each tool, particularly in scenarios involving locked or encrypted devices. This research contributes to the field by providing insights that can assist forensic practitioners, law enforcement agencies, and researchers in selecting appropriate tools for modern investigative challenges. Furthermore, it emphasizes the need for continuous innovation in forensic technologies to keep pace with evolving security mechanisms.

Key Words: Mobile Forensics, Digital Forensic Tools, Data Extraction, Encryption, Cellebrite UFED, Oxygen Forensic Detective, Autopsy, Cybersecurity, Evidence Recovery, Mobile Device Analysis

INTRODUCTION

The widespread adoption of smartphones and other handheld devices has significantly reshaped the modern digital

environment. These devices have become an essential part of everyday activities, while also playing a crucial role in criminal and civil investigations. Mobile devices generate and store diverse types of information such as communication records, emails, images, videos, browsing data, geolocation details, and application-related content. Such data can serve as important digital evidence, leading to the rapid growth of mobile forensics as a specialized area within digital forensics. This field is primarily concerned with the systematic collection, examination, and preservation of mobile data in a manner that meets legal standards and ensures evidentiary integrity.

In parallel with this growth, mobile operating systems have introduced increasingly advanced security mechanisms to protect user data. Platforms like Android and iOS incorporate features such as comprehensive device encryption, hardware-backed security modules, biometric verification systems, and secure communication protocols. While these developments strengthen user privacy and data protection, they also make it more difficult for forensic professionals to access and extract information. As a result, investigators must depend on specialized tools and techniques that are capable of working within these security frameworks or overcoming them through lawful and technically sound methods.

Another important issue in mobile forensics is the wide variation in devices and system configurations. Differences in hardware design, operating system versions, and manufacturer-specific customizations create challenges in achieving consistent forensic results. Additionally, many applications now rely on cloud-based storage, meaning that potentially relevant evidence may not be entirely present on the device itself. These factors further complicate the data acquisition and analysis process, requiring more advanced and adaptable forensic solutions.

To address these challenges, a variety of mobile forensic tools have been developed, each with distinct features and extraction approaches. Widely recognized tools such as Cellebrite UFED and Oxygen Forensic Detective are commonly used by law enforcement agencies due to their extensive device compatibility and advanced data extraction capabilities. In contrast, open-source platforms like Autopsy offer a more accessible and cost-effective option, particularly for academic and research purposes. These tools generally support multiple extraction methods, including logical acquisition, file system access, and full physical imaging, each providing different levels of data depth and completeness. However, their effectiveness is influenced by factors such as the device model, software version, and the level of security implemented.

The primary objective of this research is to perform a comparative evaluation of selected mobile forensic tools, focusing on their ability to extract data in environments protected by modern encryption techniques. The study investigates key aspects such as extraction success rate, handling of protected data, processing efficiency, and overall usability in real-world scenarios. Through this analysis, the research aims to provide a clearer perspective on how these tools perform under varying conditions and how effectively they adapt to current security challenges.

In conclusion, the study emphasizes the need for continuous advancement in mobile forensic methodologies to keep pace with evolving security technologies. It also highlights the importance of maintaining a balance between safeguarding user privacy and enabling lawful access to digital evidence, which remains a critical concern in today's highly secure digital ecosystem.

LITERATURE REVIEW

The growing dependence on smartphones has significantly influenced the way digital evidence is identified and analyzed. Mobile devices are now deeply embedded in everyday activities, including communication, financial transactions, and online interactions, which makes them valuable sources of information during investigations. In contrast to earlier approaches that mainly dealt with computer-based

systems, modern forensic work must address the complexities introduced by mobile technologies. These complexities stem from the diversity of devices, continuous software updates, and built-in safeguards that limit straightforward access to stored data.

A recurring concern in previous studies relates to the restricted accessibility of data due to enhanced protection mechanisms. Operating systems such as Android and iOS implement multiple layers of defense, including encryption and controlled system access. Although these mechanisms are designed to secure user information, they also reduce the effectiveness of direct data retrieval during forensic investigations. When full access cannot be achieved, investigators may depend on limited extraction techniques or alternative sources, which may not always provide a complete representation of the evidence.

Different strategies for acquiring mobile data have also been examined in existing research. These strategies vary based on the level of access they provide. Some techniques retrieve only surface-level information, while others attempt to access deeper storage components within the device. The most comprehensive approach involves capturing all data at a low-level format. However, improvements in device security have made such comprehensive acquisition increasingly difficult to perform in real-world scenarios.

The evaluation of forensic tools is another widely discussed topic. Commonly used tools like Cellebrite UFED and Oxygen Forensic Detective are recognized for their ability to handle a wide range of devices and provide advanced data extraction features. Meanwhile, tools such as Autopsy are often adopted in academic environments due to their flexibility and accessibility, though they may face limitations when dealing with devices that have strong security protections.

Another challenge identified in the literature is the variation between devices. Differences in hardware architecture, system configurations, and software versions can lead to inconsistent outcomes during forensic analysis. Techniques that are successful on one device may not yield similar results on another, which can affect the reliability of findings. This is particularly significant in legal investigations, where consistency and accuracy are essential. Furthermore, the increasing reliance on remote storage services means that

relevant data may be distributed across multiple locations, requiring investigators to expand their scope beyond the physical device.

Recent research has begun to explore the potential of automated and intelligent solutions in forensic analysis. Data-driven approaches are being considered to assist in processing large datasets, identifying useful information, and reducing manual effort. Although these solutions are still in development, they offer promising possibilities for improving efficiency in handling complex cases.

In summary, existing studies suggest that mobile forensics continues to develop in response to ongoing technological changes. While tools and methods have improved over time, evolving security measures continue to present new challenges. This makes it essential to regularly assess forensic tools to ensure their effectiveness in current investigative contexts.

METHODOLOGY

This study uses a structured comparison approach combined with controlled experimentation to examine how selected mobile forensic tools perform when dealing with protected or encrypted devices. The method is designed to produce consistent observations while allowing both numerical and descriptive evaluation of tool capabilities.

1. Study Framework

The research is organized as a side-by-side comparison where multiple tools are applied to the same set of test conditions. The aim is to understand how effectively each tool can retrieve information from devices with different levels of security. The analysis includes both measurable outcomes and observational insights to provide a balanced evaluation.

2. Tool Selection

The investigation focuses on three commonly used tools:

- Cellebrite UFED
- Oxygen Forensic Detective
- Autopsy

These tools were chosen because they represent both commercial and open-source solutions and are widely recognized in professional practice and academic research.

3. Experimental Setup

Testing is carried out in a controlled environment using multiple mobile devices configured in different ways. The setup includes:

- Devices operating on Android and iOS
- Devices with security features enabled and disabled
- Devices protected by passwords or biometric authentication

To simulate realistic usage, sample data such as text messages, images, application content, and browsing records is manually created and stored on each device prior to testing.

4. Extraction Procedure

Each selected tool is applied to the test devices using different acquisition methods. These include:

- Basic data retrieval through system-level access
- Deeper access to structured storage areas
- Full device capture where technically possible

The same steps are followed for each tool to ensure fairness in comparison. All extracted information is documented and organized for further evaluation.

5. Assessment Parameters

The tools are evaluated based on several key aspects:

- Extent of Data Retrieved: Volume and completeness of recovered information
- Access to Secured Data: Ability to work with protected or locked content
- Device Support: Range of compatible devices and system versions
- Time Efficiency: Duration required to complete extraction
- User Experience: Simplicity and clarity of the tool interface

6. Result Examination

The collected results are reviewed using comparative analysis. Differences between tools are identified by examining performance across all selected parameters. Visual representations such as tables or charts are used to make comparisons easier to understand.

7. Compliance and Ethics

All testing is performed using controlled devices and non-sensitive data to avoid privacy concerns. The process follows accepted forensic practices to ensure that the results remain valid, consistent, and ethically sound.

RESULT

The experimental analysis revealed noticeable differences in how each forensic tool performed under varying device security conditions. The findings show that tool effectiveness depends on factors such as encryption level, extraction method, and device configuration.

1. Overall Tool Performance

Cellebrite UFED and Oxygen Forensic Detective demonstrated stronger performance in retrieving a wide range of data types compared to Autopsy.

These tools successfully extracted communication data, media files, and certain application artifacts even when security features were enabled. In contrast, Autopsy produced better results only in less restricted environments.

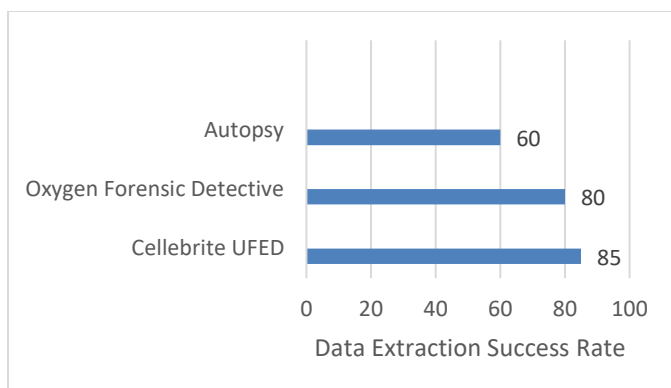


Figure 4.1 : Overall Data Extraction Comparison

The stronger results from Cellebrite UFED and Oxygen Forensic Detective suggest that commercial tools are designed to handle complex forensic scenarios. Their ability to recover

diverse data types—even with security features enabled—indicates the presence of advanced extraction techniques and broader device support.

In contrast, Autopsy performing better only in less restricted environments implies that open-source tools are more dependent on accessible data rather than advanced bypass mechanisms.

2. Performance in Encrypted Devices

When testing devices with encryption enabled, differences became more evident. Cellebrite UFED showed relatively higher success in accessing partial data from secured devices. Oxygen Forensic Detective also demonstrated good performance, especially in extracting structured application data. Autopsy faced limitations in encrypted conditions, with reduced access to protected files and system-level data.

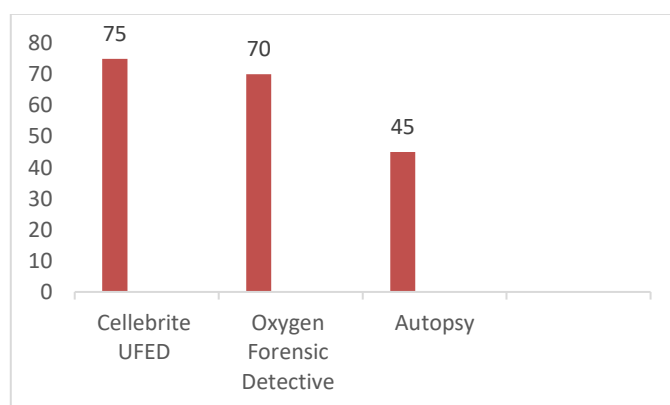


Figure 4.2 : Encrypted Data Handling Capability

The results observed in encrypted environments clearly demonstrate that encryption acts as a major obstacle in modern mobile forensic investigations. The overall reduction in data extraction performance across all tools indicates that strong security mechanisms significantly limit direct access to device data. However, Cellebrite UFED and Oxygen Forensic Detective show comparatively better performance, suggesting that they are capable of partially navigating security layers and retrieving useful artifacts even when complete access is not achievable. advanced or specialized techniques, encrypted

3. Extraction Method Effectiveness

The results varied depending on the extraction technique used:

- Logical Extraction: Fast but limited data access
- File System Extraction: Moderate depth and useful structure
- Physical Extraction: Most detailed but restricted by security

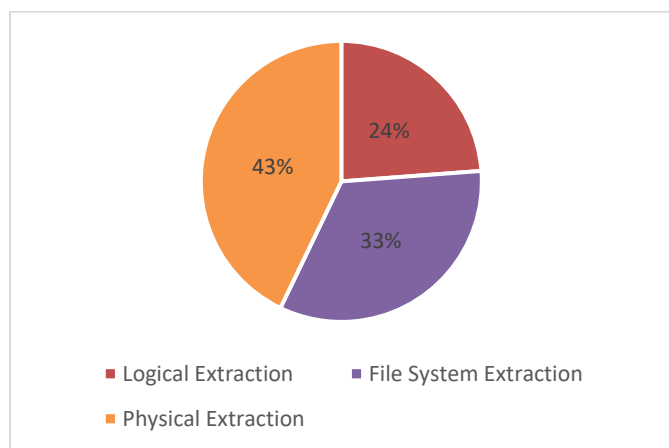


Figure 4.3 : Extraction Depth Comparison

The variation in results across different extraction methods highlights a clear trade-off between speed, depth, and technical complexity. Logical extraction is the fastest approach and is suitable for quick analysis, but it provides only limited access to data. File system extraction offers a more balanced option by allowing access to a greater amount of structured information while maintaining reasonable efficiency. In contrast, physical extraction delivers the most comprehensive data, but it is the most difficult to perform due to strong security measures in modern devices. This indicates that achieving deeper levels of data access requires higher technical expertise, and investigators must carefully select the appropriate extraction method based on the specific requirements of the case and the security features of the device.

4. Device Compatibility

Cellebrite UFED and Oxygen Forensic Detective supported a wider range of devices and operating system versions. Autopsy showed limited compatibility with newer mobile devices, especially those with advanced security features.

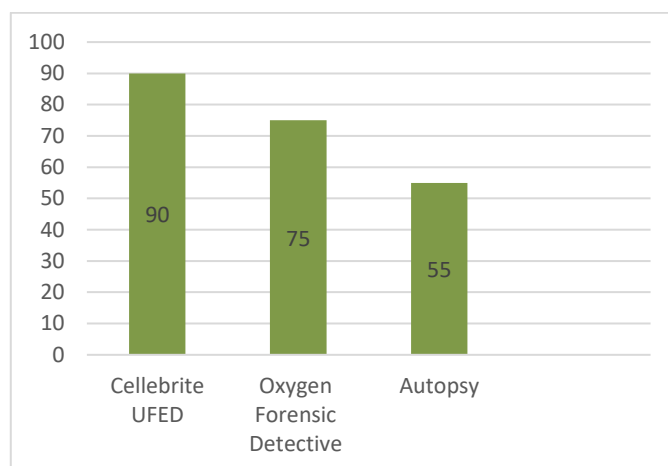


Figure 4.4 : Device Compatibility

The analysis of device compatibility indicates that Cellebrite UFED and Oxygen Forensic Detective provide broader support for a wide range of devices and operating system versions. This suggests that these tools are regularly updated to keep pace with technological advancements, making them more suitable for real-world investigations that involve diverse and modern devices. In contrast, Autopsy shows certain limitations in handling newer or highly secured devices, indicating that open-source tools may not always keep up with rapidly evolving technologies.

5. Time Efficiency and Usability

In terms of processing time, Oxygen Forensic Detective performed slightly faster in most scenarios. Cellebrite UFED provided detailed outputs but required more time for deeper extraction. Autopsy was easy to use but slower in complex analysis.

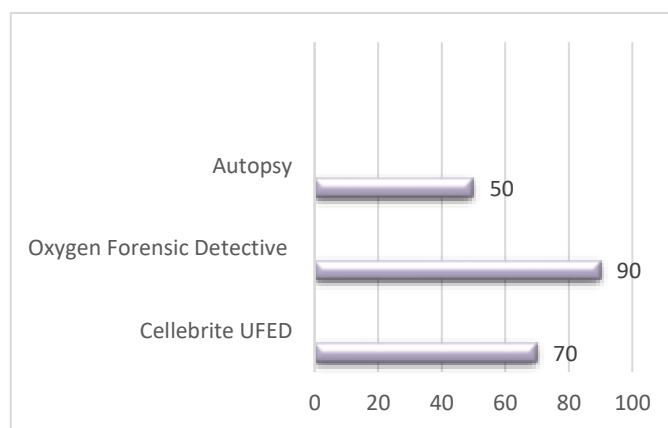


Figure 4.5 : Time Efficiency

The comparison of time efficiency and usability highlights an important practical balance in mobile forensic investigations. Faster tools such as Oxygen Forensic Detective are particularly useful in situations where time is critical, as they can quickly process and extract relevant data. In contrast, Cellebrite UFED, while requiring more time, tends to produce more detailed and comprehensive results, making it suitable for in-depth analysis. On the other hand, Autopsy offers a simpler and more user-friendly interface, which is beneficial for ease of use but may limit its effectiveness in handling complex forensic tasks. Overall, these findings demonstrate a clear trade-off between speed, depth of analysis, and usability, indicating that the choice of tool should depend on the specific priorities and requirements of the investigation.

DISCUSSION

The outcomes of this investigation indicate that mobile forensic tools do not operate with consistent effectiveness across all scenarios. Their performance is closely tied to the specific conditions of the device, including the level of security, system configuration, and access limitations. This suggests that forensic analysis in modern environments cannot depend on a single fixed approach, but instead requires adaptability and informed decision-making by the investigator.

During the comparison, Cellebrite UFED and Oxygen Forensic Detective demonstrated relatively stable behavior across different test conditions. These tools appear to handle variations in data structures and system layouts more effectively, which may be linked to their continuous development and broader compatibility. However, their performance is still affected when devices implement strong internal protections.

This shows that even advanced tools cannot fully overcome restrictions imposed by modern device security. One of the most noticeable patterns in the results is the effect of data protection mechanisms. As security features become more advanced, the amount of information that can be directly accessed tends to decrease. In such situations, investigators often work with incomplete data rather than full datasets. Even so, smaller pieces of information—such as activity records or

system traces—can still contribute to understanding user behavior when examined carefully. This reflects a shift in focus from collecting all data to making sense of whatever data is available.

The differences observed between extraction techniques further emphasize that no single method is sufficient in all cases. Some approaches allow quick retrieval of basic information, making them useful for initial analysis. Others aim to access deeper layers of storage, but these are more difficult to apply due to system restrictions. Because of this, the choice of method depends heavily on the situation, and in many cases, combining multiple approaches may provide better results.

A noticeable gap is also seen when comparing commercial tools with open-source solutions. While Autopsy is accessible and useful for structured analysis, it does not perform as effectively in environments where strong protections are present. This highlights a difference between ease of access and technical capability, suggesting that further improvements are needed in freely available tools to match modern requirements. Operational factors also play an important role.

In practical situations, investigators may need to balance speed and detail. Tools that deliver faster results are helpful when time is limited, but they may not provide in-depth information. On the other hand, more detailed analysis often requires additional time and effort. Therefore, selecting a tool is not only a technical decision but also a practical one based on the priorities of the investigation.

Another point worth noting is the increasing importance of data that exists outside the device itself. Many modern applications rely on external storage, meaning that relevant information may not always be stored locally. This expands the scope of forensic analysis and requires investigators to consider additional sources beyond the physical device.

In general, the study shows that mobile forensic investigation is becoming more demanding due to ongoing changes in technology and security design. Effective analysis now depends on using multiple tools, selecting suitable methods,

and interpreting limited data carefully rather than expecting complete access in every case.

KEY FORENSIC INSIGHTS

The outcomes of this work point to a clear shift in how mobile forensic investigations are carried out today. One important takeaway is that investigators can no longer assume that all information stored on a device will be accessible. In many situations, only portions of data can be retrieved, which means conclusions must often be drawn from incomplete evidence rather than full datasets.

Another observation is that the usefulness of a forensic tool is not fixed. The same tool may perform well in one situation and less effectively in another, depending on factors such as device setup, software version, and security level. Tools like Cellebrite UFED and Oxygen Forensic Detective tend to produce more consistent outcomes, but even they are influenced by the environment in which they are used. This shows that tool selection must be based on the specific conditions of each case.

A further insight relates to the growing impact of data protection features. As devices become more secure, direct access to stored content becomes more limited. Because of this, investigators increasingly depend on indirect forms of information, such as usage traces or background records, to understand what has occurred. This requires a stronger focus on analysis rather than simple data collection.

The study also indicates that different data extraction approaches serve different purposes. Some methods are useful for quickly obtaining basic details, while others aim to provide a deeper view of the device's contents but are harder to apply. In practice, combining multiple approaches often produces better results than relying on a single technique.

There is also a noticeable difference between advanced commercial solutions and freely available tools. While Autopsy is useful for organized examination and learning, it may not be as effective when dealing with highly protected systems. This suggests that accessibility and advanced capability do not

always go together, and further improvements are needed in this area.

Another important point is that relevant information is not always confined to the device itself. Many applications rely on external storage, meaning that useful data may be located outside the physical device. This expands the scope of investigation and requires attention to multiple sources of information.

Time and usability also influence how tools are chosen in practice. In urgent situations, quicker methods may be preferred even if they provide less detail. In other cases, more thorough analysis may be required, even if it takes longer. This creates a balance between speed and depth that must be managed carefully.

Overall, the study suggests that modern mobile forensic work is becoming more complex and requires a flexible approach. Investigators must be prepared to use different tools, apply multiple techniques, and interpret limited data effectively to achieve reliable results.

CONCLUSION

This study set out to understand how selected mobile forensic tools behave when used on devices protected by modern security controls. The observations make it clear that tool performance is not fixed and varies depending on the environment in which it is applied. Solutions like Cellebrite UFED and Oxygen Forensic Detective tend to produce more dependable results across different situations, but their success is still limited when devices enforce strong protection mechanisms. This shows that investigative outcomes are shaped not only by the tool itself but also by the surrounding technical conditions.

A key takeaway from the analysis is that the nature of evidence collection has changed. In many cases, it is no longer possible to retrieve all stored information from a device. Instead, investigators must rely on smaller pieces of available data and use them to reconstruct events. This increases the importance of reasoning and interpretation, as meaningful conclusions

must often be drawn from incomplete inputs rather than full datasets.

The comparison of extraction approaches further demonstrates that each method serves a different purpose. Some techniques are useful for quickly gathering accessible information, while others aim to provide a deeper view of device activity but are harder to execute. Because of this, no single method can be applied in every situation. Effective investigation requires selecting an approach that fits the specific conditions of the device and, where necessary, combining multiple techniques.

The study also highlights differences between tool categories. While platforms such as Autopsy are helpful for structured examination and learning, they may not perform as effectively in highly secured environments. This indicates that there is still a gap between accessibility and advanced capability, which needs to be addressed in future development.

Another important point is that relevant information is not always stored only on the device. With many applications relying on remote storage, investigators must often consider data that exists outside the physical device. This expands the scope of analysis and requires a broader investigative approach. In practical situations, factors such as time, complexity, and ease of use also influence decision-making. Sometimes faster results are necessary, even if they provide limited detail, while in other cases deeper analysis is required. This creates a balance between speed and depth that must be managed carefully depending on the needs of the investigation.

FUTURE SCOPE

Further work in this area can focus on developing approaches that are better suited to handling restricted or partially accessible data. There is a need to design tools that can adapt to different device environments and provide meaningful results even when full access is not possible.

Improving methods for dealing with protected systems is another important direction. As security features continue to evolve, new techniques will be required to ensure that investigations remain effective without violating legal or ethical boundaries.

Expanding support for a wider range of devices and system configurations is also essential, as diversity in mobile technology continues to grow. In addition, future research can explore ways to incorporate data from external sources, including remote storage and interconnected systems.

There is also potential for integrating advanced analytical approaches that assist in identifying patterns and organizing large volumes of information. Such developments can help reduce manual effort and improve the efficiency of investigations.

Finally, creating solutions that are both accessible and technically capable will be important for supporting academic, research, and professional use. Bridging this gap can make forensic tools more widely usable without compromising their effectiveness.

REFERENCES

1. Casey, E. Digital Evidence and Computer Crime (3rd ed.). Elsevier. <https://www.sciencedirect.com/book/9780123742681>
2. Nelson, B., Phillips, A., Steuart, C. Guide to Computer Forensics and Investigations. Cengage Learning. <https://www.cengage.com>
3. Hoog, A. Android Forensics: Mobile Security Analysis. Elsevier Science. <https://www.sciencedirect.com>
4. Carrier, B. File System Forensic Examination. Addison-Wesley. <https://www.pearson.com>
5. Sachowski, J. Digital Forensic Readiness Frameworks. Syngress Publishing. <https://www.elsevier.com>
6. NIST (2014). Guidelines for Mobile Device Forensics (SP 800-101 Rev.1).

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>

7. ISO/IEC 27037: Principles for Digital Evidence Handling (2012).

<https://www.iso.org/standard/44381.html>

8. Cellebrite. Technical documentation for UFED forensic solutions.

<https://www.cellebrite.com>

9. Oxygen Forensics. Product documentation and forensic tool guide.

<https://www.oxygen-forensic.com>

10. Autopsy Digital Forensics Platform (Sleuth Kit Labs).

<https://www.autopsy.com>

11. OWASP Mobile Security Project (Testing Guide).

<https://owasp.org/www-project-mobile-security-testing-guide/>

12. Google Android Security Architecture Overview.

<https://source.android.com/security>

13. Apple Platform Security Documentation (iOS).

<https://support.apple.com/guide/security>

14. SANS Institute. Mobile device forensic research materials.

<https://www.sans.org>

15. Europol Cybercrime Reports and Digital Evidence Guidelines.

<https://www.europol.europa.eu>

16. NTERPOL Digital Forensics and Investigation Frameworks.

<https://www.interpol.int>

17. IEEE Xplore Digital Library – Mobile Forensics Studies.

<https://ieeexplore.ieee.org>

18. ACM Digital Library – Cybersecurity & Forensics Research.

<https://dl.acm.org>

19. Digital Investigation Journal (Elsevier).

<https://www.sciencedirect.com/journal/digital-investigation>

20. Journal of Digital Forensics, Security and Law (ERAU).

<https://commons.erau.edu/jdfsl/>

21. Garfinkel, S. Research on digital forensics challenges.

<https://dl.acm.org>

22. Do, Q., Martini, B., Choo, K. R. Mobile forensic frameworks and models.

<https://arxiv.org/abs/1509.06815>