

Capabilities of cellebrite universal forensics extraction device in mobile device forensics

Tole Sutikno¹, Iqbal Busthomi²

¹Master Program of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

²Institute of Advanced Engineering and Science, Yogyakarta, Indonesia

Article Info

Article history:

Received Jul 29, 2024

Revised Oct 2, 2024

Accepted Oct 6, 2024

Keywords:

Cellebrite universal forensics
extraction device
Cybersecurity
Digital forensics
Forensic analysts
Forensic investigation
Mobile device forensics

ABSTRACT

The powerful digital forensics tool cellebrite universal forensics extraction device (UFED) extracts and analyzes mobile device data, helping investigators solve criminal and cybersecurity cases. Advanced methods and algorithms allow Cellebrite UFED to recover data from erased or obscured devices. Cellebrite UFED can pull data from call logs, texts, emails, and social media, providing valuable evidence for investigations. The use of smartphones and tablets in personal and professional settings has spurred the development of mobile device forensics. The intuitive user interface speeds up data extraction and analysis, revealing crucial information. It can decrypt encrypted data, recover deleted files, and extract data from multiple devices. The sector's best data extraction functionality, Cellebrite UFED, helps forensic analysts gather crucial evidence for investigations. Legal and ethical considerations are crucial in mobile device forensics. Legal considerations include allowing access to data, protecting privacy, and adhering to chain of custody protocols. Ethics include transparency, defamation, and information exploitation protection. Using Cellebrite UFED, researchers can navigate complex data on mobile devices more efficiently and precisely. Artificial intelligence (AI) and machine learning (ML) algorithms may automate data extraction in future tools. Examiners must train, maintain, and establish clear protocols for using Cellebrite UFED in forensic investigations.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Tole Sutikno

Master Program of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan
Ahmad Yani Street (South of Ring Road), Tamanan, Yogyakarta 55191, Indonesia

Email: tole@ee.uad.ac.id

1. INTRODUCTION

Cellebrite universal forensics extraction device (UFED) represents a powerful tool for the extraction and analysis of data from mobile devices in the field of digital forensics. This tool equips investigators with essential resources to uncover critical insights that may aid in resolving criminal cases or managing cybersecurity incidents. Cellebrite UFED utilizes advanced methodologies and algorithms to enable forensic practitioners to retrieve data that may have been previously deleted or concealed on the device. The ability to retrieve information such as call logs, text messages, emails, and social media interactions can provide substantial evidence relevant to investigations. Furthermore, the extensive analytical and reporting capabilities of Cellebrite UFED enable investigators to present their findings clearly and concisely, thereby facilitating judicial proceedings. Cellebrite UFED's functionality is essential to digital forensics, enhancing the effectiveness and efficiency of investigative endeavors [1]–[9].

The advancement of mobile device forensics has been significant over time, stemming from the increased reliance on smartphones and tablets in diverse personal and professional settings [9]–[14]. The basis

of mobile device forensics lies in the necessity to extract and analyze data from these devices to aid criminal investigations, cybersecurity incidents, and legal proceedings. As technological advancements continue, the challenges and complexities related to the extraction and interpretation of data from mobile devices also progress. The increasing concerns regarding data privacy and security have significantly heightened the importance of the mobile device forensics field. Researchers have developed sophisticated tools and methodologies-such as Cellebrite UFED-that enable the efficient and effective extraction and analysis of data from mobile devices. These innovations have fundamentally altered the methods used by digital forensics investigators to collect evidence and extract vital insights from mobile devices, thereby enhancing the investigative process [15].

A critical facet of digital forensics in the realm of investigations is the ability to retrieve and scrutinize digital evidence housed within a variety of electronic apparatuses. The increasing reliance on smartphones and other mobile devices for communication and data storage underscores the critical role of digital forensics in investigative settings. Mobile gadgets encompass a considerable reservoir of information that can prove crucial in resolving criminal inquiries or unveiling deceptive actions. Employing instruments such as Cellebrite UFED, investigators possess the means to extract and examine data from these mobile devices, including but not limited to call records, text correspondences, electronic mails, images, videos, and additional forms of data. This extensive form of analysis equips investigators to reconstruct timelines, pinpoint suspects, and discern motives within criminal inquiries. In addition, digital forensics functions as a vital element in the provision of admissible evidence for legal proceedings, assisting in the facilitation of justice. The functionalities present in Cellebrite UFED regarding mobile device forensics extend unmatched support to investigators operating within the continuously changing sphere of digital criminality [1]–[3], [16], [17].

Cellebrite UFED possesses a distinguished reputation for facilitating support across a diverse array of mobile devices, which encompasses smartphones, feature phones, as well as GPS apparatuses, thereby rendering it a tool of high versatility in the realm of forensic inquiries. This extensive compatibility gives investigators the ability to extract data proficiently, regardless of the operating system in use or the device manufacturer. Furthermore, the user interface of Cellebrite UFED, recognized for its intuitiveness, simplifies the intricacies involved in the data extraction and analytical processes, thereby reducing the duration necessary to unearth critical information. Cellebrite UFED helps investigators put together a full picture of what happened on a mobile device by giving them detailed reports and pictures of the data they collect. This makes it easier to piece together what happened and find relevant evidence. In conclusion, the functionalities provided by Cellebrite UFED make it an essential apparatus for professionals in digital forensics who want to extract significant insights from mobile devices during their examinations [18].

Furthermore, in order to achieve the goal of this study, it is critical to emphasize the importance of understanding the functionalities of Cellebrite UFED in the realm of mobile device forensics. Our intention is to provide a thorough assessment of this digital forensic apparatus's efficiency in retrieving and analyzing data from a variety of mobile devices by scrutinizing its attributes and capabilities. This study presents a meaningful evaluation of the functions of Cellebrite UFED, illuminating its advantages and drawbacks within the digital forensics domain. Through this inquiry, we seek to add significant perspectives to the ongoing discussions related to mobile device forensics, allowing forensic specialists and investigators to arrive at educated judgments concerning the deployment of this tool within their investigative operations. The primary goal is to increase understanding of how Cellebrite UFED can facilitate the acquisition and examination of digital evidence, ultimately supporting the effective resolution of criminal investigations and cybersecurity occurrences. Figure 1 displays the mind mapping for this study.



Figure 1. Mind mapping

2. OVERVIEW OF CELLEBRITE UFED

Cellebrite UFED has a user-friendly interface that helps to streamline the extraction and analysis procedures. It makes Cellebrite UFED accessible for both experienced professionals and those who are less familiar with digital forensics. This aspect of usability is particularly essential in the rapidly evolving field of mobile device forensics, wherein time often assumes critical importance in the process of uncovering vital evidence. Cellebrite UFED's sophisticated functionalities, which include decoding encrypted data, recovering deleted materials, and extracting information from a diverse array of devices, complement its "easy-to-use" characteristics. These functionalities contribute to its functionality as a versatile instrument for digital forensics investigators. Furthermore, it empowers them to confront a multitude of cases confidently. Cellebrite UFED distinguishes itself as a leading solution in the domain of mobile device forensics through the integration of these sophisticated capabilities and its intuitive interface [3], [4], [8].

2.1. History and development of Cellebrite UFED

Over several years, Cellebrite UFED has experienced substantial modifications to adapt to the swift progress in mobile technology and the increasing intricacy of digital forensic inquiries. Cellebrite UFED, conceived in the early 2000s, sought to address the challenges posed by the proliferation of mobile devices and the necessity for efficient data extraction and analysis. Cellebrite has expanded the capabilities of UFED through continuous research and development to align with the ever-evolving landscape of digital forensics. The integration of advanced features, such as touchscreen capabilities, intuitive interfaces, and enhanced data parsing algorithms, has solidified Cellebrite UFED as a leading choice in mobile device forensics. Cellebrite UFED has established itself as an essential tool for law enforcement agencies, corporate security divisions, and forensic professionals worldwide, enabling the extraction of critical evidence from mobile devices while maintaining forensic integrity [3], [5].

2.2. Key features of Cellebrite UFED

Cellebrite UFED has numerous key characteristics that make it a vital instrument in mobile device forensics. One noteworthy feature is its ability to bypass security protocols on a wide range of devices, enabling examiners to access encrypted or locked data. This functionality is particularly important in situations where individuals under investigation may attempt to protect their data from government scrutiny. Furthermore, UFED grants extensive data extraction functionalities, thus permitting the retrieval of an assortment of data types, inclusive of text messages, call logs, emails, social media content, and other forms [19]. The software additionally encompasses sophisticated analytical instruments that assist in the systematic organization and interpretation of the extracted information with efficacy. The combination of these attributes makes Cellebrite UFED a formidable and essential tool for conducting digital forensic investigations, empowering investigators to proficiently and effectively compile evidence from mobile devices.

2.3. Compatibility with different mobile devices

In the field of mobile device forensics, compatibility with diverse mobile devices is a critical factor for investigators. The digital crime investigation landscape requires expertise in advanced forensic techniques specific to Android devices, essential for the efficient extraction and analysis of data from smartphones [9], [13], [20]–[23]. Forensic software such as Cellebrite UFED possesses various functionalities that employ both physical and logical techniques. This underscores the necessity for the software to be compatible with a diverse array of devices to facilitate data recovery. Furthermore, as elucidated in [16], the comparison of commercial and open-source mobile forensic tools underscores the significance of assessing compatibility comprehensively, particularly in the context of prevalent cyber threats. Understanding and employing the compatibility of tools such as Cellebrite UFED with diverse mobile devices is essential for improving both efficacy and accuracy in digital crime investigations.

2.4. Comparison with other forensic tools

Furthermore, a comparison of Cellebrite UFED with other forensic tools on the market reveals its distinctiveness, characterized by an intuitive interface, broad device compatibility, and thorough data extraction capabilities. Cellebrite UFED offers a more intuitive interface for extraction and analysis compared to many traditional forensic tools that require specialized training for effective use. Cellebrite UFED provides support for a wide range of mobile devices, including smartphones, feature phones, and GPS units, thus offering investigators the flexibility to interact with various devices. Moreover, its advanced data extraction capabilities facilitate the retrieval of deleted data, application-specific data, cloud backups, and more, thereby providing investigators with a comprehensive overview of the available digital evidence [24]. Compared to other tools, the comprehensive approach of Cellebrite UFED distinguishes it as a superior choice for mobile device forensics.

2.5. Training and certification options for using Cellebrite UFED

For persons aiming to augment their competencies in employing Cellebrite UFED pertaining to mobile device forensics, a plethora of training and certification alternatives exists. Cellebrite proffers an assortment of courses tailored to accommodate varying degrees of proficiency, extending from novices to seasoned practitioners. These pedagogical initiatives encompass subjects including methodologies for data extraction, features pertinent to advanced analytical processes, and the generation of reports. Furthermore, the attainment of certification in Cellebrite UFED serves to authenticate one's adeptness in employing the tool, thereby augmenting one's credibility within the digital forensics' domain. Certification assessments typically evaluate practical capabilities related to data extraction, analysis, and reporting, utilizing the Cellebrite UFED software. Participation in such training and certification schemes can not solely refine an individual's technical acumen but also furnish them with the requisite credentials essential for showcasing their expertise in the realm of mobile device forensics. This methodical learning paradigm can markedly advantage professionals aspiring to excel in the digital forensics field and to effectively exploit the functionalities of Cellebrite UFED to its utmost efficacy [18].

3. DATA EXTRACTION CAPABILITIES

The data extraction capabilities of Cellebrite UFED, in the field of mobile device forensics, are unparalleled in the industry. The software is designed to extract various data types, including call logs, text messages, emails, images, videos, and application-related data from multiple mobile devices. This comprehensive ability to execute data extraction aids forensic analysts in the efficient gathering of essential evidence relevant to investigations. Cellebrite UFED can bypass security measures, including passcodes and encryption techniques. Cellebrite UFED facilitates access to locked devices, enabling forensic specialists to extract information that would otherwise remain inaccessible. The capability to extract data from both iOS and Android platforms further highlights the versatility of Cellebrite UFED in addressing a wide range of cases. An intuitively designed tool combined with robust extraction algorithms, rendering it a dependable and efficient resource for digital forensics professionals seeking significant data extraction capabilities within their investigative endeavors.

3.1. Extraction methods supported by Cellebrite UFED

Furthermore, the extraction techniques facilitated by Cellebrite UFED are essential components of its effectiveness in mobile device forensics. Cellebrite UFED offers multiple extraction methods, including logical, file system, and physical extractions, providing forensic investigators with access to different levels of data based on case requirements. Logical extraction retrieves data from the device's operating system, file system extraction provides access to files and directories, whereas physical extraction captures a comprehensive bit-by-bit image of the device's storage. These methodologies enable investigators to acquire a thorough collection of digital evidence, including call logs, messages, deleted content, and encrypted data. Cellebrite UFED employs various extraction techniques to implement a comprehensive and meticulous approach for obtaining essential information from mobile devices. The ability to choose the most appropriate extraction method based on the unique attributes of the investigation enhances both the efficiency and accuracy of the forensic protocol, reinforcing Cellebrite UFED as a powerful tool in digital forensics [25].

3.2. Recovering deleted data from mobile devices

Within the domain of mobile device forensics, the retrieval of erased data constitutes both a considerable hurdle and a prospect for forensic analysts. Techniques of memory dumping frequently find application for gathering both active and erased data from mobile telephones, aiming ultimately at the discovery of evidence artifacts. The procedure to recover various forms of evidence, for instance, videos, from memory dumps necessitates an amalgamation of specialized apparatus and a profound comprehension of the foundational data structures. The complexities associated with flash memory forensics, which involve issues such as wear leveling and fragmentation, contribute additional layers of intricacy to the data recovery endeavors. Through the utilization of tools and methodologies specifically designed for such purposes, examiners are capable of extracting pertinent information that may no longer exist at the file system tier, illustrating the critical nature of innovative strategies within mobile device forensics [26]. Moreover, as the framework of mobile applications progresses, it becomes essential to analyze artifacts produced by particular applications, such as Pokemon GO, to comprehend their significance within forensic inquiries [17]. By investigating the functionalities of tools like Cellebrite UFED alongside tools tailored to application-specific analysis, forensic investigators can amplify their proficiency in retrieving and scrutinizing vital data from mobile devices, thereby illuminating information that may have previously been beyond reach.

3.3. Handling encrypted data

In the context of mobile device forensics, the handling of encrypted data presents investigators with various challenges notably in terms of accessing and analyzing sensitive information. Common encryption methodologies, such as Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), serve to protect the data and necessitate the use of specialized instruments, for instance, Cellebrite UFED, to effectively decrypt and extract the information. Cellebrite UFED is equipped with advanced functionalities that allow for the circumvention of encryption, retrieval of passwords, and access to secured devices; thereby enabling forensic specialists to securely and efficiently obtain crucial evidence. By employing the sophisticated algorithms and methodologies found in Cellebrite UFED, investigators can navigate encryption impediments and extract essential data for subsequent analysis and evidence gathering. Moreover, this tool adheres to legal standards and necessary protocols pertinent to the management of encrypted information, thus preserving the integrity of the forensic process. In summarization, Cellebrite UFED is instrumental in the extraction, decryption, and analysis of encrypted data within mobile device forensics, thereby enhancing the investigative process and facilitating the identification of critical insights.

3.4. Extracting data from various apps and social media platforms

Within the sphere of digital forensics, the act of retrieving data from a multitude of applications as well as social media sites holds significant importance in the process of revealing essential evidence. Cellebrite UFED stands out for its capability to access not just conventional user-generated materials but also data residing within various applications. Given the escalating frequency of social media utilization, the crucial nature of data extraction from such platforms as Facebook, Twitter, and Instagram is heavily emphasized. These venues frequently harbor pivotal information, which includes communications, geolocation data, and multimedia files, all of which could prove vital to ongoing investigations. Through the application of Cellebrite UFED's functionalities, forensic analysts are equipped to thoroughly investigate these platforms, allowing for the efficient and effective extraction of pertinent data. This diligence ensures that every possible avenue is explored in the pursuit of revealing digital evidence that can bolster investigative endeavors. As digital traces continue to proliferate, the necessity for forensic instruments like Cellebrite UFED, which can extract data from an extensive range of applications and social media platforms, becomes increasingly critical within contemporary digital investigative contexts [27].

3.5. Analyzing extracted data for investigations

The progression of sophisticated Android mobile forensics methodologies, as underscored by Sutikno [9], highlights the essentiality of examining extracted data within the realm of digital crime probes. Instruments such as Cellebrite UFED provide organized methodologies for data retrieval, thus enabling investigators to effectively gather and scrutinize evidence. The intricate nature of mobile-network forensics demands adeptness in diverse methodologies to guarantee the successful acquisition and decryption of data. Furthermore, with the rampant spread of location-driven applications like Pokemon GO, elaborated upon in [17], forensic analysts encounter novel hurdles in comprehending and extracting artifacts that hold forensic significance. By utilizing tools that extend beyond conventional methods, such as the application-specific analysis instrument suggested in the research, investigators can amplify their competencies in revealing crucial information from mobile apparatuses. The evaluation of extracted data emerges as pivotal in deciphering the contexts surrounding occurrences and shedding light on essential insights for investigative endeavors.

4. DATA ANALYSIS CAPABILITIES

Investigations pertaining to digital crime necessitate the existence of strong data analytic competencies. As data analytic competencies are particularly crucial when engaging with mobile apparatuses, such as smartphones and internet of things (IoT) devices. The advancement of mobile forensics (MF) has imposed the requirement for progressive methodologies aimed at the extraction and processing of evidential materials in an efficient manner [28]. In this framework, the implementation of specialized instruments, like Cellebrite UFED, constitutes a vital aspect in the augmentation of forensic inquiries by furnishing methodical strategies for data extraction and analysis [9]. These instruments present a variety of functionalities, which include manual extraction, logical analysis, hex dump processing, chip-off techniques, and micro-read operations, empowering investigators to adeptly compile and decipher evidence. By integrating state-of-the-art technologies, such as mobile-network forensics alongside continuous advancements in tool development, those engaged in digital crime investigations are able to bolster their data analysis proficiencies, thus effectively addressing cyber threats. The intricate interrelationship between data analysis and forensic instruments accentuates the necessity of employing sophisticated techniques to maneuver through the complexities surrounding contemporary criminal activities and digital evidentiary materials.

4.1. Sorting and categorizing extracted data

Within the sphere of mobile device forensics, the procedure of sorting and categorizing the data that has been extracted holds significant importance in the discovery of pertinent evidence. Cellebrite UFED provides sophisticated features that grant investigators the capability to methodically arrange the extensive quantity of data acquired from mobile devices. By organizing the extracted data according to various file types, timestamps, along with additional metadata, analysts are able to promptly detect critical information that may hold substantial relevance to any investigation. Furthermore, the functionality to organize data into distinct folders or tagging systems promotes a more structured methodology for data examination, thereby ensuring that no vital evidence is inadvertently disregarded. Through these sorting and categorization functionalities, Cellebrite UFED improves both the effectiveness and precision of digital forensic evaluations, granting investigators the ability to assemble a thorough narrative of occurrences. This methodology not only optimizes the workflow of investigations but also aids in the delivery of findings in a coherent and orderly fashion.

4.2. Generating reports and timelines

In addition, within the field of digital forensics, the act of generating reports and timelines is of considerable importance for the purpose of documenting the investigative process as well as conveying findings in a manner that is both clear and structured. The Cellebrite UFED system provides advanced functionalities that facilitate investigators in crafting thorough reports that delineate the data extracted, the results of analyses, and the forensic techniques utilized. Such reports are crucial for the presentation of evidence in legal contexts, as they furnish a transparent depiction of the investigative procedures undertaken. Furthermore, timelines produced using Cellebrite UFED can offer a visual representation of the chronological order of events occurring on a mobile device, which assists in the reconstruction of digital behaviors and the establishment of a timeline of occurrences. Such visual aids can prove to be pivotal in discerning underlying patterns, correlations, and possible leads for subsequent inquiry (Initial Publication). In summary, the capability of Cellebrite UFED to produce comprehensive reports and timelines significantly heightens both the efficiency and the efficacy of investigations pertaining to mobile device forensics.

4.3. Keyword searching and filtering options

The functionalities associated with keyword searching and filtering present within the Cellebrite UFED system significantly contribute to the optimization of digital forensics inquiry. Employing these attributes enables investigators to succinctly identify pertinent data amongst large datasets obtained from mobile apparatuses. The capability to enter precise keywords or expressions facilitates targeted inquiries, consequently lessening the duration required to examine non-essential data. Moreover, the filtering mechanisms allow for the further refinement of search returns contingent upon a variety of factors, such as types of files, spans of dates, and methods of communication. This degree of customization amplifies the accuracy of the investigative procedure, culminating in findings and deductions that are more precise. In summation, the formidable keyword searching and filtering features inherent in Cellebrite UFED bolster its standing as an indispensable instrument in the realm of mobile device forensics. Digital forensic analysts are empowered to exploit these functionalities to enhance their operational efficiency and effectively extract vital evidence throughout investigative processes [24].

4.4. Link analysis and data visualization tools

Moreover, the use of link analysis accompanied by data visualization instruments serves an essential function in amplifying the effectiveness and efficiency related to mobile device forensic inquiries. The application of such tools facilitates the revelation of intricate relationships and patterns inherent in the data extracted, thus permitting a more thorough comprehension of the particular case concerned. Link analysis fosters the representation of connections among disparate pieces of data, inclusive of calls, messages, and application interactions, which presents a visual depiction of the interrelations among various entities. Such visual aids can assist investigators in pinpointing significant individuals, chronological sequences, and communication antecedents that might, through conventional examination practices, remain obscure. In addition, the employment of data visualization resources bolsters the presentation of results, thereby simplifying the communication of intricate information to relevant parties or in legal contexts. The integration of link analysis and data visualization tools with the comprehensive functions of Cellebrite UFED propels the investigative process into an advanced domain, facilitating enhanced decision-making and more efficient forensic procedures [29].

4.5. Integrating third-party tools for advanced analysis

In the area of digital forensics, the inclusion of external third-party tools aimed at sophisticated analysis is capable of markedly augmenting the functionalities of pre-existing software such as Cellebrite

UFED. By means of the integration of niche tools specializing in areas such as data visualization, statistical scrutiny, or artificial intelligence methodologies, investigators are afforded the opportunity to enhance their analytical processes and derive more significant insights from data originating from mobile devices. These additional tools provide enhanced functionalities that not only bolster the fundamental attributes of UFED but also present a wider array of analytical methodologies to address the intricacies of forensic challenges that are often encountered. Moreover, the assimilation of external tools can lead to a more streamlined investigative workflow by way of automating particular tasks or broadening the analytical horizon beyond what conventional forensic instruments can achieve. This amalgamation of third-party resources not only extends the analytical prowess of Cellebrite UFED but also accentuates the crucial nature of collaboration and interoperability within the sphere of digital forensics. The collaborative dynamics between these diverse tools ultimately empower investigators to unearth pivotal evidence in a more efficient and effective manner, thereby enhancing the competencies of mobile device forensic investigations.

5. LEGAL AND ETHICAL CONSIDERATIONS

Within the field of mobile device forensics, the interplay of legal and ethical factors is of great significance in guiding the procedures of investigation. It is crucial to adhere to rigorous guidelines and regulations in order to uphold the integrity of the evidence that is both collected and subjected to analysis. Legal factors include securing appropriate permissions to access and scrutinize the data housed within mobile devices, ensuring that the rights to privacy are upheld, and complying with protocols surrounding the chain of custody in order to maintain the evidentiary worth of the information retrieved. Ethical factors necessitate that the investigation is carried out in a manner that is transparent and devoid of bias, honoring the privacy of individuals from whom data is being analyzed, and protecting against any potential exploitation of the information acquired. By maneuvering through the complex framework of legal and ethical matters, digital forensics investigators can strive to maintain the utmost levels of professionalism and integrity in their undertakings. Adopting these tenets not only enhances the credibility of the investigative process but also preserves the rights and dignity of all participants in the case [30].

5.1. Admissibility of evidence obtained using Cellebrite UFED

The exploration into digital forensics has pointed out the growing use of the deep web and dark web for engaging in unlawful activities, making it crucial for there to be advanced methods of investigation. The suggested method, termed D2WFP, provides a sequential methodology that places importance on the order of volatility along with a systematic extraction of artifacts associated with browsing behaviors [31]. Such a strategy boosts the precision and efficacy of inquiries concerning the deep and dark web, exceeding the performance of current industry-standard tools. Furthermore, the critical nature of data from mobile devices, notably concerning location data, has been accentuated in forensic investigations. Instances of case studies conducted under controlled conditions with recorded locations have brought to light the inconsistent dependability of retrieved location data, underlining a significant need for thorough analytical approaches [32]. These revelations are essential when evaluating the acceptability of evidence that has been acquired via instruments like Cellebrite UFED, as they reflect the dynamic nature of the digital forensics landscape and the intricate characteristics of digital evidence.

5.2. Chain of custody and maintaining forensic integrity

Within the field of mobile device forensics, the significance of ensuring a secure chain of custody alongside the preservation of forensic integrity is exceedingly crucial. The introduction of blockchain technology, as indicated by Khubrani [33], presents a potentially advantageous means to augment the reliability and credibility of digital evidence through the secure documentation of the chain of custody. By utilizing the immutable digital ledger characteristic of blockchains and their cryptographic security attributes, one can strengthen both the integrity and authenticity of forensic results, thereby tackling the difficulties posed by the heterogeneous nature of mobile devices. Furthermore, the proposed scientific forensic framework for smartphones by Shahpasand [34] highlights the necessity for structured methodologies to evaluate and exhibit substantive forensic evidence in judicial settings, thereby guaranteeing the authenticity of investigative outcomes. These inputs illuminate the vital importance of maintaining the chain of custody and forensic integrity within mobile device forensics, consequently enhancing the overall effectiveness of investigations and reinforcing the reliability of the findings.

5.3. Compliance with data protection laws and regulations

In addition, as the complexity of digital data increases alongside rising concerns over privacy, ensuring adherence to data protection laws and regulations has emerged as a vital consideration in the realm

of mobile device forensics. It is paramount that the processes of data extraction and analysis from mobile devices are performed in accordance with established legal frameworks so as to sustain the integrity and admissibility of evidence in judicial proceedings. Cellebrite UFED encompasses functionalities that assist forensic investigators in conforming to these legal stipulations, including secure data handling, encryption features, and audit trails that serve to monitor the continuity of custody. By following these protocols, investigators are positioned to guarantee that the acquired evidence is legally robust and capable of enduring judicial examination. Nevertheless, it remains essential for forensic practitioners to remain informed about the shifting landscape of laws and regulations, thereby consistently adapting their practices and methodologies to align with prevailing legal standards.

5.4. Ethical considerations in mobile device forensics

Considering the sensitive characteristics associated with data preserved on mobile apparatuses, ethical dimensions assume a significant function in the realm of mobile device forensics. It is of utmost importance for forensic investigators operating within the digital sphere to comply with established ethical protocols and norms to uphold the integrity associated with the investigative framework. This becomes particularly critical in scenarios where the personal details pertain to individuals who do not have a direct connection to the legal inquiry. Ensuring the protection of privacy and entitlements of those involved emerges as a vital aspect of sustaining ethical benchmarks within mobile device forensics. Furthermore, the appropriate management and preservation of evidence is indispensable, as it serves to avert any potential alterations or interference with data that could jeopardize the legitimacy of the findings. By steadfastly adhering to ethical doctrines in the context of mobile device forensics, investigators are capable of maintaining the reliability and authenticity of their endeavors. The ethical ramifications surrounding the extraction of data from mobile devices warrant meticulous contemplation to preserve the ethical precepts of the field [30].

5.5. Challenges and limitations in using Cellebrite UFED

In spite of the notable capabilities that Cellebrite UFED presents in the realm of mobile device forensics, a variety of challenges and limitations become evident. A primary challenge that arises is the possibility of data corruption amid the extraction process, which inherently may result in evidence that is either incomplete or inaccurate. Furthermore, the landscape pertaining to mobile devices and their respective operating systems is subject to perpetual evolution, thereby constraining the efficacy of the tools, as they may find difficulty in adapting to contemporary updates and encryption methodologies [35]. Moreover, the financial implications associated with procuring and sustaining licenses for Cellebrite UFED can prove to be a significant obstacle for smaller forensic units or organizations that operate under constrained financial circumstances. These challenges underscore the necessity for ongoing training and adaptability to guarantee effective employment of Cellebrite UFED in the domain of mobile device forensics, in conjunction with a comprehensive comprehension of its limitations to alleviate potential risks and inaccuracies that may arise within digital investigations.

6. RESULTS AND DISCUSSION

6.1. Summary of Cellebrite UFED capabilities

Cellebrite UFED presents capabilities that extend beyond mere data extraction and analysis. A notable feature is the ability to circumvent pattern, PIN, and password protections on mobile devices, thereby granting access to locked devices for forensic purposes. Such functionality proves to be particularly beneficial in scenarios where individuals suspected of involvement refuse to provide passcodes or lack the capacity to do so. Furthermore, Cellebrite UFED possesses the ability to retrieve erased data, encompassing text messages, call histories, and images, among other data types, thereby furnishing an all-encompassing perspective of the device's historical usage. This feature is instrumental in reconstructing occurrences and timelines that are critical for investigative purposes. Additionally, UFED extends support to a broad spectrum of mobile devices and operating systems, thus ensuring compatibility across various models and versions. Cellebrite UFED is a very important tool for mobile device forensics because it has all of these features. It gives investigators a complete and powerful way to do digital investigations.

6.2. Implications for the field of mobile device forensics

The unceasing progress witnessed in the realm of technology concerning mobile devices brings forth a duality of challenges and prospects pertinent to the domain of mobile device forensics. As smartphone operating systems and encryption methodologies grow increasingly intricate, forensic professionals encounter the formidable obligation of keeping pace with these swift advancements. Nonetheless, tools such as Cellebrite UFED serve as a noticeable glimmer of optimism within this perpetually shifting digital milieu.

By availing advanced techniques for data extraction and examination, Cellebrite UFED furnishes investigators with essential apparatuses to adeptly maneuver through the convoluted data housed within mobile devices. Such capabilities not only augment the efficiency and precision of forensic inquiries but also unveil novel pathways for the discovery of valuable evidentiary material. The ramifications of the incorporation of Cellebrite UFED within mobile device forensics are profoundly significant, as it empowers investigators to probe more deeply into digital evidence and maintain an advantageous position in the relentless pursuit of truth and justice. Additionally, the application of Cellebrite UFED may play a pivotal role in establishing new benchmarks within the mobile device forensics arena, thereby expanding the limits of what was previously considered achievable in digital investigative efforts [30].

6.3. Future developments and advancements in digital forensics

Furthermore, future trends predict significant changes and advancements in the field of digital forensics due to rapid technological advancements. It is probable that forthcoming forensic instruments will attain higher levels of sophistication, utilizing artificial intelligence and machine learning algorithms to automate and enhance data extraction processes. Such developments stand to facilitate a more rapid and precise examination of digital evidence, thereby diminishing the need for manual input and amplifying the efficacy of forensic inquiries. Furthermore, the increasing prevalence of IoT devices, coupled with the mounting complexity of digital environments, will introduce novel obstacles that the realm of digital forensics must contend with. Investigative pursuits in the field are currently concentrating on tackling these issues by creating innovative methodologies for data acquisition and analysis from a broader spectrum of devices and platforms. As digital technologies persist in their evolution, one can assert that the trajectory of digital forensics will inevitably necessitate ongoing innovation as well as adaptation to satisfy the requirements of an increasingly digital landscape.

6.4. Recommendations for utilizing Cellebrite UFED effectively

Effective use of Cellebrite UFED in mobile device forensics necessitates adherence to a variety of recommended practices. The most important is that all examiners receive comprehensive tool training to maximize its capabilities. Adequate training equips examiners to competently navigate the software interface and fully exploit its extensive suite of functionalities relevant to data extraction and analytical processes. Furthermore, the continuous updating and maintenance of the UFED software is vital for remaining aligned with the advancements in mobile technologies and the shifting landscape of security protocols. In addition to the aforementioned aspects, the formulation and implementation of explicit protocols and guidelines governing the application of UFED within the context of forensic investigations is crucial. This is to ensure that there exists both consistency and accuracy when handling digital evidence. By adhering to these outlined recommendations, forensic examiners can proficiently use the Cellebrite UFED tool for the extraction, analysis, and interpretation of digital evidence from mobile devices, thereby guaranteeing a high level of precision and reliability.

7. CONCLUSION

The use of Cellebrite UFED in mobile device forensics has demonstrated itself to be highly transformative in this specific discipline. Its substantial functionalities have permitted investigators to gain access to and extract data from an extensive assortment of mobile devices, which encompasses smartphones, tablets, and GPS devices. The tool's elaborate features, including both physical and logical extraction options, have equipped forensic specialists with the means to retrieve crucial information that might have remained unattainable otherwise. Cellebrite UFED's ability to decode and analyze data from a wide range of applications and operating systems has also made digital investigations much more effective and efficient. As technology advances at an accelerating pace, the need for advanced forensic instruments like Cellebrite UFED is projected to increase. To summarize, the functionalities afforded by Cellebrite UFED have profoundly transformed the landscape of mobile device forensics, furnishing investigators with essential instruments for unearthing evidence that is pivotal for resolving cases and ensuring accountability for offenders. In conclusion, Cellebrite UFED's functionality in the field of mobile device forensics is noteworthy and significantly impacts the field of digital inquiry. The ability to extract data from a wide range of mobile devices, including sophisticated smartphones, tablets, and even GPS devices, provides investigators with a comprehensive tool for elucidating critical evidence. The software's user interface, which is characterized by its intuitiveness alongside its robust analytical functionalities, empowers forensic analysts to expeditiously scrutinize substantial quantities of data, thereby enhancing efficiency and augmenting productivity. Furthermore, the compatibility of Cellebrite UFED with an array of operating systems and file formats guarantees that investigators are adequately equipped to manage a diverse array of

devices and data categories. As technological advancements persist, Cellebrite UFED sustains its position at the vanguard of mobile device forensics, offering sophisticated capabilities that address the requirements imposed by contemporary investigations. Given these factors, it becomes apparent that Cellebrite UFED constitutes an indispensable resource for professionals engaged in digital forensics who endeavor to navigate the intricate challenges presented by mobile device inquiries.

REFERENCES

- [1] M. S. Al-Faaruuq and D. F. Priambodo, "iOS digital evidence comparison of instant messaging apps," *2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022*, pp. 83–88, 2022, doi: 10.1109/ICSINTESA56431.2022.10041620.
- [2] H. Bowling, K. Seigfried-Spellar, U. Karabiyik, and M. Rogers, "We are meeting on Microsoft teams: forensic analysis in Windows, Android, and iOS operating systems," *Journal of Forensic Sciences*, vol. 68, no. 2, pp. 434–460, 2023, doi: 10.1111/1556-4029.15208.
- [3] P. Jain and A. Mishra, "Extraction of data using cellebrite ufed 4Pc," *International Journal of Medical Toxicology and Legal Medicine*, vol. 26, no. 3–4, pp. 222–232, 2023, doi: 10.5958/0974-4614.2023.00074.8.
- [4] Y. Keim, S. Hutchinson, A. Shrivastava, and U. Karabiyik, "Forensic analysis of tiktok alternatives on android and iOS devices: byte, dubsmash, and triller," *Electronics (Switzerland)*, vol. 11, no. 18, 2022, doi: 10.3390/electronics11182972.
- [5] A. Pal, M. Maheswari, K. B. Jena, and G. K. Singh, "SIM card data extraction in digital investigations: a UFED cellebrite approach," *International Journal of Medical Toxicology and Legal Medicine*, vol. 27, no. 1, pp. 27–37, 2024, doi: 10.52710/ijmtlm.5.
- [6] O. Parhad and V. Naik, "Comparative analysis of data extraction for Qualcomm based Android devices," *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, 2023, doi: 10.1109/ICCCNT56998.2023.10307241.
- [7] H. Tara and A. Mishra, "A comparative study of digital forensic tools for data extraction from electronic devices," *Journal of Punjab Academy of Forensic Medicine and Toxicology*, vol. 21, no. 1, pp. 97–104, 2021, doi: 10.5958/0974-083X.2021.00016.9.
- [8] J. Williams, A. Macdermott, K. Stamp, and F. Iqbal, "Forensic analysis of fitbit versa: Android vs iOS," *Proceedings - 2021 IEEE Symposium on Security and Privacy Workshops, SPW 2021*, pp. 318–326, 2021, doi: 10.1109/SPW53761.2021.00052.
- [9] T. Sutikno, "Mobile forensics tools and techniques for digital crime investigation: a comprehensive review," *International Journal of Informatics and Communication Technology*, vol. 13, no. 2, pp. 321–332, 2024, doi: 10.11591/ijict.v13i2.pp321-332.
- [10] S. Kingra, N. Aggarwal, and R. D. Singh, "Video inter-frame forgery detection approach for surveillance and mobile recorded videos," *International Journal of Electrical and Computer Engineering*, vol. 7, no. 2, pp. 831–841, 2017, doi: 10.11591/ijece.v7i2.pp831-841.
- [11] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Classification and evaluation of digital forensic tools," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, pp. 3096–3106, 2020, doi: 10.12928/TELKOMNIKA.v18i6.15295.
- [12] T. Rasul, R. Latif, and N. S. M. Jamail, "A computational forensic framework for detection of hidden applications on android," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, pp. 353–360, 2020, doi: 10.11591/ijeecs.v20.i1.pp353-360.
- [13] K. S. Vaddi, D. Kamble, R. Vaingankar, T. Khatri, and P. Bhalerao, "Enhancements in the world of digital forensics," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 1, pp. 680–686, 2024, doi: 10.11591/ijai.v13.i1.pp680-686.
- [14] V. Balajichandrasekhar, T. Srinivasa Rao, and G. Srinivas, "An improvised methodology to unbar android mobile phone for forensic examination," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 4, pp. 2239–2246, 2018, doi: 10.11591/ijece.v8i4.pp2239-2246.
- [15] C. Rani Panigrahi, V. H. C. de Albuquerque, A. Kumar Bhoi, and H. K.S., *Big data and edge intelligence for enhanced cyber defense*. CRC Press, 2024.
- [16] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujana, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," *2016 9th International Conference on Contemporary Computing, IC3 2016*, 2017, doi: 10.1109/IC3.2016.7880238.
- [17] J. Sablatura and U. Karabiyik, "Pokémon GO forensics: an android application analysis," *Information (Switzerland)*, vol. 8, no. 3, 2017, doi: 10.3390/info8030071.
- [18] J. Bair, "Seeking the truth from mobile evidence," *Network Security*, vol. 2018, no. 2, pp. 4–4, 2018, doi: 10.1016/s1353-4858(18)30013-8.
- [19] G. Tiepolo, *IOS forensics for investigators*. 2022.
- [20] M. Hassan et al., "Sentiment analysis on Bangla conversation using machine learning approach," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 5, pp. 5562–5572, 2022, doi: 10.11591/ijece.v12i5.pp5562-5572.
- [21] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology," *International Journal of Electrical and Computer Engineering*, vol. 7, no. 5, pp. 2806–2817, 2017, doi: 10.11591/ijece.v7i5.pp2806-2817.
- [22] L. M. Jegaveerapandian, A. J. Rani, P. Periyaswamy, and S. Velusamy, "A survey on passive digital video forgery detection techniques," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 6, pp. 6324–6334, 2023, doi: 10.11591/ijece.v13i6.pp6324-6334.
- [23] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.
- [24] A. Hoog, "Android forensics: investigation, analysis and mobile security for Google Android," *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*, pp. 1–372, 2011, doi: 10.1016/C2010-0-65787-7.
- [25] O. Afonin and V. Katalov, *Mobile forensics - advanced investigative strategies: master powerful strategies to acquire and analyze evidence from real-life scenarios*. Packt Publ. Ltd., 2016.
- [26] K. Mansell and A. Caithness, "Recovering video from memory dumps of mobile phone handsets," pp. 1–7, 2010, [Online]. Available: <http://www.controlf.net/content/uploads/CONTROL-F-Recovering-Video-from-Mobile-Phone-Handsets.pdf>.
- [27] J. Sammons, "Digital forensics," *Elsevier*, 2016.
- [28] G. Anyomi, "Current and future trends in mobile device forensics," *Advances in Multidisciplinary and scientific Research Journal*

Capabilities of cellebrite universal forensics extraction device in mobile device forensics (Tole Sutikno)

- Publication*, vol. 1, no. 1, pp. 215–220, 2022, doi: 10.22624/aims/crp-bk3-p35.
- [29] T. Tryfonas and I. Askoxylakis, “Human aspects of information security, privacy, and trust,” *Springer International Publishing*, 2014.
 - [30] U. Department of Homeland Security, “Test results for mobile device acquisition tool: cellebrite inspector v10.7,” *CreateSpace*, 2023, [Online]. Available: <http://www.cftt.nist.gov/>.
 - [31] M. C. Ghanem, P. Mulvihill, K. Ouazzane, R. Djemai, and D. Dunsin, “D2WFP: a novel protocol for forensically identifying, extracting, and analysing deep and dark web browsing activities,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 808–829, 2023, doi: 10.3390/jcp3040036.
 - [32] C. Bell, “Providing context to the clues: recovery and reliability of location data from android devices,” *Inf. Bull. Var. Stars*, 2015.
 - [33] M. M. Khubrani, “Mobile device forensics, challenges and blockchain-based solution,” *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, pp. 1504–1509, 2023, doi: 10.1109/SmartTechCon57526.2023.10391719.
 - [34] M. Shahpasand, “Scientific forensic framework for smartphones,” *Universiti Putra Malaysia*, 2015, [Online]. Available: [http://psasir.upm.edu.my/id/eprint/65262/1/FSKTM 2015 47IR.pdf](http://psasir.upm.edu.my/id/eprint/65262/1/FSKTM%2015%2047IR.pdf).
 - [35] R. Botwright, “iOS forensics 101: extracting logical and physical data from iPhone, iPad And Mac OS,” *Pastor Publishing Ltd*, 2024.

BIOGRAPHIES OF AUTHORS



Tole Sutikno    is a lecturer and the head of the Master Program of Electrical Engineering at the Faculty of Industrial Technology at Universitas Ahmad Dahlan (UAD) in Yogyakarta, Indonesia. He received his Bachelor of Engineering from Universitas Diponegoro in 1999, Master of Engineering from Universitas Gadjah Mada in 2004, and Doctor of Philosophy in Electrical Engineering from Universiti Teknologi Malaysia in 2016. All three degrees are in electrical engineering. He has been a Professor at UAD in Yogyakarta, Indonesia, since July 2023, following his tenure as an associate professor in June 2008. He is the Editor-in-Chief of TELKOMNIKA and Head of the Embedded Systems and Power Electronics Research Group (ESPERG). He is one of the top 2% of researchers worldwide, according to Stanford University and Elsevier BV's list of the most influential scientists from 2021 to the present. His research interests cover digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded systems, artificial intelligence, intelligent control, digital libraries, and information technology. He can be contacted at email: tole@te.uad.ac.id.



Iqbal Busthomi   received his Master of Computing in Informatics Engineering from Universitas Ahmad Dahlan, Yogyakarta, Indonesia in 2021. After receiving his degree, he became a member of the Institute of Advanced Engineering and Science (IAES) as Information and Communication Technology Team. His research interests include cyber security, web application, and digital forensics. He can be contacted at email: iq.iaes@gmail.com.