Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 8, No. 3, June, 2024

Mobile Device Forensics Framework: A Toolbox to Support and Enhance This Process

Bruno M. V. Bernardo [1*], Henrique S. Mamede [2, 3], João M. P. Barroso [1], Vítor M. P. D. dos Santos [4]

[1] *INESC TEC and Universidade de Trás-os-Montes e Alto Douro, Portugal.*

[2] *Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), Porto, Portugal.*

[3] *Department of Science and Technology, Universidade Aberta, Lisbon, Portugal.*

[4] *MagIC and NOVA IMS – Universidade Nova de Lisboa, Portugal.*

Abstract

Cybercrime is growing rapidly, and it is increasingly important to use advanced tools to combat it and support investigations. One of the battlefronts is the forensic investigation of mobile devices to analyze their misuse and recover information. Mobile devices present numerous challenges, including a rapidly changing environment, increasing diversity, and integration with the cloud/IoT. Therefore, it is essential to have a secure and reliable toolbox that allows an investigator to thwart, discover, and solve all problems related to mobile forensics while deciphering investigations, whether criminal, civil, corporate, or other. In this work, we propose an original and innovative instantiation of a structure in a forensic toolbox for mobile devices, corresponding to a set of different applications, methods, and best practice information aimed at improving and perfecting the investigative process of a digital investigator. To ensure scientific support for the construction of the toolbox, the Design Science Research (DSR) methodology was applied, which seeks to create new and unique artifacts, drawing on the strength and knowledge of science and context. The toolbox will help the forensic investigator overcome some of the challenges related to mobile devices, namely the lack of guidance, documentation, knowledge, and the ability to keep up with the fast-paced environment that characterizes the mobile industry and market.

Keywords:
Digital Archaeology;
Digital Evidence;
Digital Forensics;
Mobile Device Forensics;
Data Governance.

Article History:

Received:	29	January	2024
Revised:	19	April	2024
Accepted:	07	May	2024
Published:	01	June	2024

1- Introduction

One of the most used technologies in the world nowadays is the mobile phone device [1]. This technology presents itself as a device that contains numerous distinct characteristics and elements, like brands, accessories/complements, models, and hardware and software features and specifications [2]. Thus, we reside in a digital information era wherein most individuals encounter digital information, which results mainly from technological advancements and its employment in people's daily routines and digital influx [3]. It is expected that the usage of this type of technology, namely mobile devices, explains already the utmost portion of all internet flow [4, 5]. This factual increase in the usage of the internet flow is expected to rise even further due to technological improvements and innovation on mobile devices, where people's capability to process and manipulate digital data is evolving each day [3]. In line, the literature shows that the mobile device industry is highly competitive and is characterized by rapid changes and evolutions, being supported by two strong market players, Android (provided by Google) and iOS (provided by Apple) [6].

* **CONTACT**: al75188@alunos.utad.pt

DOI: http://dx.doi.org/10.28991/ESJ-2024-08-03-011

Consequently, as mobile phones evolve, so do the different types of capabilities, from their actions to the amount of data they create, store, and delete [7]. In line, mobile device forensics science is growing at an incredible pace as it is attempting to sustain the ongoing advances and upgrades in technology that support and change people's daily lives, namely the mobile phone, which has a short cycle for brand new devices [7, 8]. Thus, it is highly relevant to acknowledge the potential impact that data governance in mobile forensics processes can have on its success in ensuring the correct and robust set of responsibilities and management over the procedures performed within an investigation and over the digital evidence gathered [9]. Data governance's ability to ensure data integrity, legality, and ethical standards is critical [10]. In line, although mobile forensics focuses mainly on the extraction, analysis, conservation, and reporting of digital evidence, it should encompass the key pillars of data governance, namely the strategic governance of data assets, by encompassing procedures, policies, guidance, and compliance that measure the investigation success and quality while ensuring the proper and robust management of the data governance [7]. Besides, data governance is expected to foster the accuracy and reliability of the retrieval, analysis, and conservation of digital evidence while ensuring the proper chain of custody, contributing to the credibility of findings [7, 9, 10]. Therefore, literature presents mobile forensics as a science that is likely the most challenging, heterogeneous, and varied, conceivably bringing the ultimate challenge that a digital investigator may encounter [4, 11]. The following section investigates this field's problems and challenges in depth.

1-1- Problem Statement

According to the literature findings, several challenges are rising and categorizing the field of mobile forensics, namely the ones presented and detailed below. Hence, the following statements can be derived:

- There are several distinct models and types of mobile phones that contain numerous different conditions that each user, model, and component can customize [2, 4];
- The boundaries and limitations of forensic tools imposed by the existing numerous types of mobile phones, as well as the growing pace of cybercrime [6–8];
- The absence and unavailability of formal and standardized documentation that describes the techniques and methods that are accessible to be used in a given operation [4];
- The absence of testing procedures and standardized scientific methods [12];
- The limited to no support regarding the process of the integration of data and information from a mobile phone into the IOT ecosystem, such as the cloud, which is more complicated and complex to ensure ownership of the integrated data [4];
- The new peripheral tools, whose purpose is to enhance and innovate the functions of a mobile phone to an even greater extent, enable further, more complex, and more extensive exchanges of data and storage [12–15].

Appropriately, for a digital investigator to become more aware, conscious, and knowledgeable on these topics, there is a recurring need to study and perform continuous, extensive research on the science of mobile forensics. The research problem can be stated as there is a clear gap yet to be fully addressed, namely related to the inexistence of a clear and stable artifact (a toolbox, tools, a model, a formal and standardized documentation and methodology [4, 7, 11].

Considering this, we acknowledge from the literature that even though mobile device forensics tools and methodologies exist, there is a clear research gap within the mobile device forensics field that results from the fact that these tools and methodologies are dispersed, which makes them inaccessible and not readily available for the digital investigator. These tools still need to be studied, compared, put together, and linked to a standardized methodology within the literature. Consequently, this research addresses this gap identified within the literature while presenting a thorough exploration of the field of mobile forensics; this comprehensive study delves into existing methodologies and tools. It introduces a well-structured framework comprising a diverse toolbox of applications, each linked directly to a standardized and formalized methodology. This interconnected approach systematically compares all tools and applications within the toolbox. Nonetheless, it is essential to comprehend the main reasons behind these facts because they are distinct while considering what and why these challenges are urging. Furthermore, within the study of the literature available, we performed a summarization of the previous publications related to studies on mobile device forensics topics. Given this, we identified and analyzed a total of 16 articles related to this topic in the table below, for which we identified the topics that were studied in each of the papers, namely the following.

Table 1 demonstrates that although the majority of literature reviews in the field of mobile device forensics science are theoretical in nature, there is also some concentration on particular areas, such as the examination of the field's state-of-the-art and its difficulties, the evaluation of tools and applications for mobile forensics, and the identification of approaches that aid in the investigative process. Nonetheless, we verified that none of the articles encompassed all the described domains and set a relationship between them, e.g., the analysis of the mobile forensics' environment and its challenges, together with the analysis and characterization of several tools and applications and the mapping between these tools and a defined mobile forensics methodology. Therefore, we propose an approach that is extensive as to allow the digital forensics investigator, organizations, and anyone else who wants to obtain greater knowledge to have a complete perception of the critical aspects of this field.

Table 1. Analysis over papers focused on the review over domains of Mobile Device Forensics and its Tools

References	Date	Mobile Forensics Definition	Mobile Forensics Challenges	Mobile Forensics Methodology	Mobile Forensics Tools/Application Analysis	Mobile Forensics Tools Comparison	Role of Tools/Application in a Mobile Forensics Methodology
Fukami et al. [1]	2021	✓	✓		✓		
Vella & Colombo [2]	2022		✓		✓		
Chernyshev et al. [4]	2017	✓	✓		✓		
Jadhav and Joshi [6]	2016	✓	✓		✓		
Shama et al. [8]	2022	✓	✓				
Barmpats alou et al. [12]	2018	✓	✓	✓	✓		
Faheem et al. [16]	2016	✓		✓	✓	✓	
Sathe & Dongre [17]	2018	✓		✓	✓		✓
Kim et al. [18]	2018	✓			✓		
Omeleze and Venter [19]	2013	✓		✓	✓	✓	
Al-Sabaawi et al. [20]	2019			✓	✓	✓	
Rao & Chakravarthy [21]	2016				✓	✓	
Alhassan et al. [22]	2018				✓	✓	
Gajjar & Shama [23]	2020	✓			✓	✓	
Kapale & Attar [24]	2019	✓		✓	✓		
Mumba & Venter [25]	2014	✓	✓	✓			
Present Study	2024	✓	✓	✓	✓	✓	✓

The following sections will present our framework implementation supporting mobile device forensics science. To do so, in Section 2, we will present the research methodology and how the Design Science Research approach was employed thoroughly. In Section 3, background research, and although there are not yet studies similar to ours, we will present and address critical topics that are important for the mobile device forensics field and for the framework that we propose and that were discussed, analyzed, and unraveled by different authors. Section 4 will introduce the proposed toolbox of applications and tools, exploring its concept and its relationship with mobile device forensics science. This section will be divided into two sub-sections: 4.1. Toolbox Requirements and Architecture, which will explore and describe how the proposed toolbox will be designed, what elements and critical components it will include, and how these topics relate to each other; and 4.2. Toolbox Strategy and the Supporting Stepwise Approach, where we will describe the standardized and formalized methodology that the digital investigator should use to support the toolbox of applications and tools and its data governance. Within Section 5., we will demonstrate the instantiation of the framework and its toolbox of tools and applications, deploying the tools included in the toolbox, its main characteristics, and how they are related to the supporting methodology defined in the previous section. In Section 6. Evaluation, we will present the results of the focus group meeting held within this work, as well as a discussion on the mobile device forensics field and the potential impact of the designed and built framework and its toolbox, as well as address the key outcomes and utility that come from it. In Section 7, Conclusions, we will present the paper's conclusion, our main contribution to the field, define directives and the basis for future work to be performed within the field of mobile device forensics, and appeal to the overall scientific community to foster research in this field.

2- Research Methodology

To attain the study objectives, the research methodology applied within this study is the Design Science Research methodology (DSR), which seeks to bring novel and unique artifacts leveraging the strength and knowledge of science and its community [26]. In general, this methodology can be considered one that can result in products, such as IT artifacts/toolboxes and processes, which consider a set of activities [27]. In line, Ostrowski et al. [28] presented the Design Science Research methodology as one that encompasses six different steps/processes, including: i) Identification of the problem and motivation; ii) definition of the objectives for the solution to be proposed; iii) design and development of the solution prototype; iv) demonstration of the artifact; v) evaluation of the artifact's utility and validity; and, vi) communication of the results. In Figure 1, we projected the methodology into a process flow.

Within the first and second steps, the initial stages of this methodology, we center our discussion on identifying and elucidating the significant problems and motivations that characterize the field of mobile device forensics, as well as the primary objectives of this research [28–30]. To do so, we reviewed the literature surrounding mobile forensics science and presented the main conclusions on this field's problems, challenges, and motivations in sections 1 and 2. Also, within this section, we emphasize the precise definition of our research objectives: to propose and construct a framework encompassing a toolbox of applications and tools to support and enhance mobile forensics investigations and data governance.

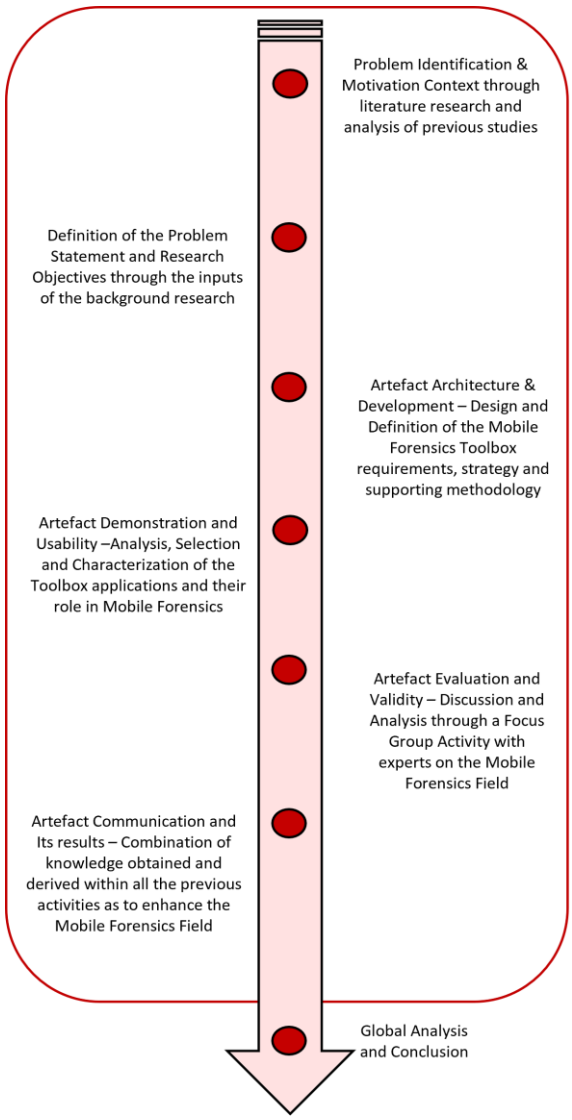

Figure 1. Flowchart of the DSR Model Methodological Approach

In the third and fourth stages, the solution to our main objective involves constructing and designing the artifact, the Toolbox for mobile device forensics. The proposed and drawn artifact was organized into three layers of information and aligned with the inputs obtained from the research in the literature. The toolbox encompasses tools and applications suitable for each phase of the mobile device forensics process, categorized based on features and accessibility. This artifact provides digital investigators with awareness of available applications for mobile forensics investigations, accommodating different budgetary constraints and desired levels of detail and extraction. Likewise, although there is no use case performed over a set of given applications/tools for the mobile device forensics process, our toolbox will be composed of applications/tools that result from a meticulous analysis of the current market and literature aimed at providing the scientific community with a set of applications to support the process of mobile forensics. These selected tools were chosen to answer each of the steps of a designed mobile forensics methodology, contributing to a specific purpose and tasks including evidence acquisition, testing, documentation, and reporting. They were chosen based on the existing literature and market maturity, as well as their reliability, efficiency, and relevance to this field. The fifth stage corresponds to the evaluation phase, where the proposed artifact undergoes assessment to determine its performance [31].

In fact, within this step, we called for users' engagement to be directly and indirectly impacted by the artifact. As such, we conducted a focus group, encompassing different discussion topics for each participant and an overall discussion. This activity will involve participants with different academic and market backgrounds to obtain various inputs to evaluate the proposed artifact.

Additionally, after validating the framework and its toolbox, we proceed with the last phase, the communication phase. We aim to continue our work on mobile device forensics and to reach as much as possible the overall scientific community, providing digital investigators, researchers, and organizations with the most up-to-date knowledge and information in this field.

3- Background Research

3-1- Innovation and Technology Complexity

Throughout the literature, we can denote that digital forensics is surrounded by technology and digital evidence, which it is not yet able to fully encompass and answer due to the large variety and volume of data collected and its sources, which originated from the inexistence of automated analysis methods and knowledge of the tools that currently exist, leading to manual processing of events' digital evidence [7, 32]. Accordingly, these challenges lead to higher dependence on the investigator's job tenure, time and resource consumption activities, and susceptibility to human errors, which severely impact the reconstruction and analysis of the events and the veracity of its digital evidence [32].

Similarly, the literature reveals that the complexity of technology, its innovation, and digital evidence impose challenges that result in the need for advanced and immersed research on new strategies and methodologies that can potentially answer those challenges. However, the root of those challenges is not solely due to the technology complexity, the high volume and variety of data, and the ever-increasing innovation; it is also related to the fact that there is a lack of standardization in the way that digital forensics processes and performed and digital evidence is acquired and preserved, impacting not only the digital forensics field but also its sub-branch, the mobile device forensics one [7]. Besides, these authors denote that there is a concerning lack of knowledge on the latest digital forensics tools and methodologies, which imposes an essential issue that is jeopardizing the efficiency and effectiveness of digital forensics activities, thus reinforcing the need for research such as the one presented within this paper [7]. Likewise, Brunty [33] denotes that given the technological complexity, it is now crucial for the science community to define methods associated with a digital forensics' investigation, ones that refer to the specifications and features of a given technology, software, and methodology. In line, when stablishing a given methodology for digital forensics, it is important to understand what the functionality and capabilities of each of the tools/applications are, as to allow investigators to better determine which of them may be more suitable for a given set of activities and what type of digital forensics dataset can/should be gathered.

3-2- Mobile Phones Main Specifications

Jadhav & Joshi [6] denoted that there are several different types and models of mobile devices, each with an infinite number of specifications and settings. Thus, recognizing that the mobile phone's diversity and complexity are considered among the most compound and difficult challenges that mobile device forensics science must address. Consequently, this results in the need for this field to be adaptable and able to produce and encompass many techniques to support and consider different types of phone devices and their components. Likewise, each mobile contains its own built-in features/characteristics, which is considered a barrier for a digital investigator when accessing and gathering information from these devices [8]. In truth, Jadhav & Joshi [6] strengthened the idea that there are constraints within forensics tools, which may indicate that no universal tool is available for the digital investigator to be capable of accessing and collecting data from a given phone model.

Moreover, as technology and mobile devices evolve, so do the various types of cybercrime, specifically malicious applications and files that can hold corrupt or malicious data due to viruses on mobile phones [6]. Thus, imposing challenges for the digital investigator, who can possibly inspect malicious/corrupted data within a given inquiry. Besides, the data that is stored on a mobile device can be dynamic, i.e., data that may have been changed without the digital investigators' notice, and that can, in turn, direct to misjudgments and incorrect inferences. In line, the digital investigator must consider that data can also be stored on a device that belongs to a different person, and that data can be both professional and personal [6, 11].

Furthermore, data can be considered a critical part within the several aspects of a digital investigation, playing a critical role in the preparation of the investigation, its analysis and testing procedures, and the disclosure of the results obtained [34]. Within the forensics science context, data and its security have a tremendous impact on the success of digital investigations because the data that results from the crime scene and its documentation allow the digital investigator to record the events of the scene and define the foundation for further investigation procedures.

Consequently, the digital investigator should ensure that within a forensics science investigation context, data can be supported by the FAIR principles, highlighted by Hackman et al. [34], which correspond to i) Findable, where data can be easily located for both digital investigators and the supporting tools and applications, as such, unique identifiers, indexed repositories and/or metadata standards can be employed; ii) Accessible, where data must be readily available for the access of the digital investigator, resulting into unrestricted accesses during the course of an investigation and in the removal of process and technological barriers; iii) Interoperable, where data is stored in a structured manner, preserving its integrity and fostering the application of common terminologies, data formats and structures; and iv) Reusable, which corresponds to the principle that states that data should be preserved within a comprehensive manner that ensures the robust documentation and contextualization of data and ready to be use for future research purposes during the course of an investigation. In line, mobile forensics investigators should strive to ensure the adherence of the forensics examination to the FAIR principles over the data collected and throughout the course of the investigation.

3-3- Mobile Forensics Documentation and Methodologies

One of the major issues impacting mobile forensics, according to the literature, is the necessity for greater documentation and guidance on the methods and tools/applications available for usage within a mobile forensics' investigation [4, 8]. The often-used methodologies and applications comprise numerous steps, including the identification of the evidence and the event scene context, the application of different mechanisms (tools, techniques, and applications), as well as the documentation of the activities performed so as to allow for the results of the investigation to be valid and, for example, admissible in court. Sharing the same thoughts, Barmpatsalou et al. [13] denoted that although there are several different techniques and applications that can be employed within a mobile forensics' investigation, there is a clear lack of standardization around this field and these procedures, which in turn can be explained by the lack of awareness and research and by the fast-paced industry of this technology and its rapid changes. Thus, creating strong gaps between the current knowledge and capabilities of mobile forensics and the rapid innovation that is resulting in new and different types and kinds of mobile phones and operating systems.

Moreover, the majority of frameworks and methodologies available for mobile forensics procedures must require a solid scientific foundation of studying, testing, and analyzing them before being fully implemented within a forensics investigation [12]. As such, tools and applications available for this field must contain supporting documentation and allow for the log evidence of the activities that are performed in it. Apart from this, the literature points out that there is an overall lack of instructions and documentation on how to use the available current tools and methodologies, a lack of guidance in what training set should be performed, and which certifications, if applicable, can support an investigator in making the most out of these tools [4, 12].

Considering this, additional documentation is required for those specific tools, namely on what their features are, what their role is within a digital investigation, and how they can be operationalized and produce supporting documentation for the activities performed. This situation is also characterizing the operating systems of each mobile phone, as some of them have minimal documentation and studies available, especially the least used ones, which makes it challenging for the digital investigator to understand where and what to look for in these tools and applications [4, 12].

Additionally, the interface and integration of a person's data on the mobile device with the cloud services allow people to perform real-time interactions and exchanges of information, including uploads, changes, and/or downloads of unlimited data. However, there is little to no support available for retrieving cloud information using mobile forensics tools and applications, and establishing ownership of the data stored in the cloud can be very challenging [4]. Similar to this, people no longer use their mobile devices for just texting or making phone calls; instead, these devices are widely used for a variety of IoT purposes, which makes it much more difficult for a digital investigator to access a mobile's memory and its pertinent data. Thus, with the emergence of peripheral tools that can be utilized together with mobile devices, the digital forensics field needs to evolve and change to handle and address these complex environments [4].

3-4- Mobile Phone Security and Configuration

The digital investigator is currently presented with pertinent challenges with regard namely to the security settings and the antiforensics. For instance, as a security precaution, mobile device manufacturers can allow users to encrypt their mobile phone data, which is thought to be a means of shielding information from outsiders [4, 8]. By doing this, these steps will build and raise a strong resistance barrier that mobile device forensics tools and applications may need to be capable of burrowing through. Accordingly, the literature takes into account antiforensics techniques as a method created to thwart forensics activities and investigators from acquiring evidence and analyzing the data gathered from mobile devices, thus eliminating evidence's traceability and obfuscating the data on the phone [4, 8].

Moreover, Ferreira et al. [35] present a study concentrated on the Android operating system environment, which corresponds to the most used one in the market, offering a comprehensive set of tools, capabilities, and features, including Bluetooth, NFC, and wireless connectivity, GPS, and several security settings, including authentication and access protection controls. However, these authors [35] recognize that despite being popular and a leader in the mobile market, this system is not immune to vulnerabilities. According to the OWASP (Open Web Application Security Project), an international organization focused on software security, the top five mobile phone vulnerabilities include: i) inappropriate platform usage; ii) insecure and doubtful data storage and its management; iii) unprotected communication; iv) insecure validation and authentication; and v) insufficient secure communication and data storage, also recognized as cryptography. Consequently, the digital investigator must be aware of which vulnerabilities exist within the mobile phone environment and what the most common ones are, so that necessary procedures and alerts can be taken into consideration prior to any investigation [35].

Additionally, security and users' privacy concerns related to technological devices have been rising each day, namely due to the fact that these devices do create, manage, and store critical people's personal and professional information. Contrasting with traditional forensics' science, within digital forensics, an investigator must consider the vulnerability that both digital and physical evidence can have, rather than just the physical one. Inline, there is a greater need for the digital investigator to take the appropriate procedures to ensure the safeguard and protection of the evidence [36]. For

instance, digital forensics must be capable of investigating these incidents and coping with them, preventing security concerns from occurring. Nonetheless, Alam & Kabir [36] highlight that there is a need for greater and more in-depth research on the advancement of standardized tools and techniques in the field of digital forensics so as to allow for more efficient and effective procedures, resulting in more accurate and robust conclusions. Moreover, these authors [36] present insights on how to cope with security and users' privacy concerns within a digital forensics' context, namely that the digital forensics investigator must:

- Identify all the devices involved in the scene and gather critical information in a way that assures its integrity and validity (including firmware versions, configurations, device settings, and network flow);
- Perform tests and analysis of the gathered physical and digital evidence using appropriate tools for each of the activities, including software and system settings analysis and data extraction procedures;
- Interpret the data and results obtained while performing testing procedures such as the correlation of data with other historical information sources (including resources such as an inventory of past attacks, a comparable device analysis log, and/or similar evidence);
- Preserve and present the findings obtained within the previous stages while demonstrating that all investigation procedures are robust and clearly documented;

If applicable, physical and digital assets used within an investigation and after its conclusion can be given to their true owner, where criminal evidence was identified and managed appropriately.

3-5- Related Work

Given the challenges described, the authors consider it relevant to unravel and understand the existing literature review on mobile forensics by screening and analyzing the related and relevant work on this science. This section should help the community delve into the existing body of knowledge around this field and the complexity surrounding its environment.

By scrutinizing the literature on mobile device forensics, the authors acknowledged that the mobile phone could be defined as a device that represents a functional and multi-featured computer system that is encompassed within our daily routine and that can embody a "treasure trove of data" allowing for the performance of several and different actions such as those that can englobe i) documents, images, songs, text/video/audio messages and calls log activity, phone numbers, mobile identifiers, emails and their activity, web browser history, location history/log information [4, 11, 16], ii) backups, and applications data [16, 37], while just being able to fit within a pocket. Likewise, given its characteristics, a mobile device can be used together with different additions, such as SIM and Memory Cards, Earphones, and Smartwatches, as well as different and various applications that can be obtained from downloads within the app stores available and/or third-party applications [38]. Given this versatility and complexity, the literature recognizes the importance of a device like a mobile phone to have a specific forensic science. Nonetheless, before defining the concepts and methodologies for a forensics process that focuses solely on mobile devices, it is essential to consider the general foundations of forensics science. Accordingly, the literature perceives this science as the conjunction and application of the law together with science and its methodologies [39, 40]. Thus, having the primary goal of achieving irrefutable answers and conclusions regarding legal problems/investigations by producing relevant interpretations over physical and digital evidence [41, 42]. Also, this science involves various aspects, including temporal and spatial ones, encompassing people, locations, and materials/objects [40].

Given this, as a complex science that is highly volatile due to its different variables and scenarios, researchers recognized that this science demands the existence of "discipline-specific" procedures to sustain conclusions in a robust and documented manner different from every other way of thinking and cognitive reasoning [15]. In light of this, Houck [40] describes the forensics standard process, which can function as a four-step flow, initiated by, namely:

- The detection stage, where the goal is to decode and discover any object that can be considered relevant and/or crucial, especially those that are imperceptible or indistinct, for which the forensic expert should be able to investigate and acknowledge that evidence;
- The direct application of different specialties and methods that belong to accurate knowledge and science;
- The action in which the investigator intends to recreate the storyline of a given event;
- This is the phase where the forensics investigator should evaluate the previously defined performance metrics, namely, the precision, the time, the cost of the examination action that was/is being conducted, and the knowledge that was created from that.

Moreover, related work, but more focused on the digital forensics science itself, recognizes that the traditional forensics science related to physical procedures rather than technological and digital ones has evolved into a science that can be described as an emerging area [4, 43]. This is due to the development of fast-paced, ongoing technology innovation and devices, giving foundation to forensic sciences such as mobile forensics, a subdiscipline of digital forensics [4, 11, 40].

Accordingly, this emergent science, recognized as digital forensics, has received increased research in the last year, mainly due to the rapid increase of the internet, technology, and cyberspace [32]. It can be considered a process flow of actions employed to analyze and display digital evidence obtained from various sources and technologies [7]. Consequently, this science ought to support organizations and individuals in unveiling events arising from a composite technology through three distinct phases, from the acquisition to the examination and conservation [32]. Likewise, literature considers that this process flow resembles the traditional forensics activity by involving the analysis and examination of evidence that is present, but within this field on electronic devices, it is considered digital evidence, i.e., any methodical technique that is accurately applied for the conservation, seizure, assessment, and interpretation of digital evidence collected from a digital device to present digital evidence found and analyzed rather than prove innocence or the result of guilt in a given judicial proceeding [29, 43, 44].

In light of this, the digital forensics process is commonly presented as a process action flow encompassing a specific amount of steps, which, according to Sonmez & Varol [45], begins with the occurrence of a given crime/event, followed by the issuance of a search warrant, yielding the investigator with the right to visit and inspect the crime/event scenario and to secure the evidence, and record in documentation the numbering, type, and descriptive details of the collected evidence. Afterwards, the investigator must be able to pack and transfer the evidence to a protected and accessible location suitable for the digital forensics' activity. To analyze the evidence, the investigator should acknowledge and describe the methodology to be applied and the actions that will be pursued to study and analyze the evidence, namely, a replica of it, recording and documenting each step and the result of the analysis performed. As for the final stage, the digital investigator should focus on producing formal documentation of the investigation, including the techniques and methodologies applied, the outcomes, the steps pursued, and the main conclusions that were produced, which can be turned into a report that is expected to meet the requirements for presentation to the authorities, if necessary [7, 45].

Moreover, the literature denotes that it is essential to acknowledge these concepts and methodologies in digital forensics to set the bridge and basis for mobile device forensics science. In fact, due to this versatility, the literature considers that mobile device forensics science should consider inputs and potential synergies with other emergent sub-branches of digital forensics, which are evolving into different and distinct sciences, such as document forensics, digital evidence, computer and malware forensics, database and email forensics, as well as many other digital forensics sciences that already exist or that are currently being implemented [43]. For instance, to comprehend mobile device forensics science, organizations/individuals need to acknowledge the best practices and methodologies of different sub-areas of the digital forensics' science and the forensics science itself, leveraging on this knowledge and possibly generating synergies and adding value to a given examination [4, 12].

Consequently, the literature presents mobile device forensics as one of the main sub-branches of the digital forensics field, corresponding to the process of obtaining and collecting evidence from a digital resource, namely, the mobile device, by applying a set of methodologies and techniques/tools to retrieve and analyze this type of information [46, 47]. As mentioned, the rising prevalence of handheld devices, such as mobile phones, coupled with the ongoing evolution and advances in the smartphone industry underscores the necessity for digital investigators and organizations to acknowledge and comprehensively explore mobile device forensics methodologies and tools [4, 6]. Thus, there is an urgency in the need for research to present the community with an in-depth understanding and study of this topic [6, 7, 17]. As highlighted by Bjornson & Hunter [48] and Soltani & Hosseini [32], the traditional focus of digital forensics science has been transformed by transitioning from data residing in personal computers to that stored in mobile gadgets. Thus, both exhibit similarities, namely within the process of obtaining an exact copy of the technology (personal computer or mobile phone) and ensuring that this evidence is not tampered with and modified.

Considering this, numerous authors conceptualize mobile device forensics science as an activity supported by a procedural approach. For Barmpatsalou et al. [13], Faheem et al. [46], and Ayers & Jansen [49], this methodology can be designed into four different stages: i) the initial stage, where it involves the preservation process, including actions such as the activation of airplane mode to block network, Wi-Fi, and Bluetooth communications, shutting down the device to halt interactions, and placing the gadget in a shielded box to prevent external network and radio accesses; ii) the acquisition stage, where the objective is to obtain all possible relevant data from the mobile device along with setting up the appropriate tools for the subsequent stages, namely, iii) the examination and analysis stages, and iv) the reporting stage. During these last two phases, the goal is to scrutinize and unravel any digital evidence relevant to a given case, such as deleted or concealed data, call and message logs, images, documents, and any information suitable for the investigation, while preparing the documentation of all the procedures performed and the presentation of the conclusions obtained [12, 46, 49].

Similarly, Sathe & Dongre [17] presented the mobile forensics process as a systematic approach that is initiated by:

- i) identification of the digital evidence, where an investigator examines the device physically to determine if it could potentially be a source of relevant information;
- This step is followed by ii) preservation and iii) acquisition steps, where the investigator is expected to shield the phone from any harmful connection that could compromise its data and to create a replica of the device imagined,

mitigating the risks associated with the device's physical condition and battery, allowing for the investigation to go forward;

- At stages iv) analysis and v) documentation, the investigator is expected to meticulously examine the data obtained from both the device and the replica itself, drawing insights and findings that could prove relevant within an investigation. Simultaneously, the investigator should focus on formally recording any action taken within the investigation to ensure that the procedure can be audited and reviewed, allowing for reproducibility if necessary. The conclusive step vi) is the presentation of the findings drawn within the previous steps [17].

Furthermore, a pivotal distinguishing feature of a mobile phone is its operating system (OS), which is crucial for user-device interactivity. The diversity within OS technology significantly impacts the mobile device forensics process, namely the extraction and replication of digital evidence [4, 17]. The dominant OSs in the smartphone market are Android and iOS, where Android is an open-source Linux-based OS provided by Google and iOS is a universal OS for Apple smartphones. Thus, the literature highlights that Android's unique open-source feature leads to different varieties and applications with the potential to contain lighter authentication, increasing the risks of mobile malware and rogue applications, which mimic trusted ones and contain harmful features [4, 17, 18]. iOS is somewhat less complex as it allows for less customization, and the applications are only distributed within the official store that is associated with the default characteristics of the device; however, by containing built-in data protection mechanisms due to high levels of encryption on the data and its backups, it significantly impacts the success of a digital investigation. Besides these two leading operators, there are more players within this market, namely the Windows Phone OS, Blackberry, and Symbian, which can also be encountered during an investigation. Compared to Android and iOS, these operating systems receive less support and research due to their lower popularity and share on the market, leading to fewer available tools and guidance on how to perform such investigations [4, 11, 17].

Moreover, acknowledging the functioning aspects of mobile phones is also crucial for the success of a mobile digital investigation, namely understanding how and where the data is stored within their components. Mobile phones can include components like SIM cards and memory cards, harboring extensive data [11, 46]. The SIM card, or Subscriber Identity Module, is a crucial piece of physical hardware in mobile devices because it can contain vital information about the device, its usage, and its user. It allows the user to communicate within the identified network to which it belongs, i.e., without this card, a cell phone can only call the emergency numbers in its region. It corresponds to a repository for data such as the user's mobile phone number, call records, SMS texts, and contact list [12]. Also, these authors highlight that SIM cards allow for the transfer of information along with their PIN and PUK Services (a specific set of digits used to access the SIM cards) from one phone to another. In the case of three incorrect attempts to enter the PIN, the digital investigator will be required to use a more complex security authentication method, such as the PUK. If incorrectly entered ten times, the SIM card can become permanently locked. Consequently, literature denotes that company-owned and managed mobile devices are usually configured to override these rules, emphasizing the need for a digital investigator to be aware of these procedures and prevent the permanent lockdown of such a vital source of information [11, 12].

In addition to the SIM card, the literature highlights the importance of critical identifiers that are embedded within a mobile phone, namely the electronic serial number (ESN), the mobile equipment identifier (MEID), and the International Mobile Equipment Identity (IMEI) [11, 12]. IMEI, in particular, can be described as the mobile device's "social security number". As such, Graves [11] denotes that the digital investigator should pursue actions to obtain this information; for example, for retrieving MEID information, the investigator can use the key combination "*#06#" or access settings on an Apple iPhone. The IMEI, which resides within the phone's battery compartment, consists of 15 algorithms indicating the device's model, production origin, serial number, and checksum. Any action to manipulate, tamper with, or remove these labels can obstruct digital investigations [4, 11, 46].

Besides this, the digital investigator needs to acknowledge how to protect and store the mobile device without putting its conditions under any risk of intrusion. As a result, one of the most common techniques corresponds to the usage of Faraday enclosures, including Faraday bags, with the significant objective of isolating the device from any external pings and instructions. If the enclosure is opened, it can allow for exterior connections throughout the study, which can raise risks. For instance, the literature denotes that once the phone is inside a Faraday cage, screen capture devices, such as Paraben's Project-a-phone and the Eclipse screen capture device, can be used to obtain, record, encrypt, and document any action taken for the accurate retrieval and analysis of documentation [11, 12].

Additionally, related work examines how distinct data collection activities and techniques are employed, namely, the three data gathering categories for data collection from mobile phones. In fact, according to Fukami et al. [1] and Zhang et al. [37], the first data-gathering technique is the manual one, which reflects the action of collecting data by interacting with the mobile itself via, e.g., USB. The second regards the logical extraction technique, which can be described as the process of collecting data through access to the mobile phone's file system, which may contain data that has yet to be removed by its user. This section of a mobile file system is used by the operating system while providing the device with the capacity to store data hierarchically within the different repositories [50]. Third, the physical extraction technique

characterizes the collection of data from the mobile phone, where the main goal is to be able to retrieve data that has been deleted or that is possibly missing/hidden. Accordingly, Maras & Miranda [51] defined that after being acquired, evidence can be described and categorized into four distinct groups: physical, pattern, transfer, and trace evidence.

Considering all of the related work troves within the literature, the authors denoted that throughout our review of the related work, there are different studies on explicit tools for specific purposes/phones and/or data extractions, such as the following:

i. Data accessing tools like Project-A-Phone and NFI Memory Toolkit, BitPim, and LiME [4, 11];

ii. Data extraction tools such as the Universal Forensic Extraction Device (UFED), the Chinex device, Device Seizure, and BlackLight [4, 17];

iii. Data analysis tools like Android SDK, Magnet Axiom, qtADB, FTK Imager, and SQLite Forensics [6].

However, research has yet to be performed to identify, characterize, compare, and study the different existing tools and align those with a standard methodology, which is the purpose of this work [7].

4- Proposal - An architecture for Mobile Device Forensics and its Data Governance

This section will introduce the envisioned framework for the mobile device forensics field, encompassing a toolbox of applications and tools directly linked to a standardized forma methodology. In Section 4.1., we will delve into its conceptualization and interconnection with this science, providing researchers with the design principles, inclusive elements, and essential components of the toolbox and exploring their interrelationships. As for Section 4.2, we will define the overview of the standardized and formalized methodology essential for digital investigators to leverage this artifact effectively to perform a robust and precise mobile forensics investigation process.

4-1- Toolbox Requirements and Architecture

There is great concern for the digital investigator to acknowledge the tools and applications that can be used to perform the mobile device forensics investigation. Moreover, the literature review also denotes applications and tools that are free and open-source, i.e., free to use, for which the user is able to make improvements as well as develop on them. Besides, the literature also denotes applications and tools where the user needs to pay in order to be able to have access to them and to apply them during an investigation.

As such, the proposed artifact comprises three different layers of information, which in turn can be considered the requirements for the artifact related to the architecture and process stages/phases studied in the literature available. For instance, to build the toolbox and retrieve and explore the applications and tools most suitable for a digital investigator during a mobile forensics' examination, the current research scrutinized the literature available to find the ones that can answer each phase of the mobile device forensics process.

As previously shown, this branch of forensics, according to Ayers & Jansen [49], can be described as a four-stage process method that is initiated by 1) the preservation phase, followed by 2) acquisition, 3) examination, and 4) reporting. Likewise, Sathe & Dongre [17] described a stepwise approach as the first: 1) identification phase, followed by 2) preservation, 3) acquisition, 4) analysis, 5) documentation, and 6) presentation stages. As such, these methods can be combined to support toolbox creation and the software and hardware that can assist the digital investigator. Therefore, the authors will segment the tools analyzed by the different steps/phases of the mobile forensics process to begin constructing the toolbox. Accordingly, considering the processes described by Ayers & Jansen [49] and Sathe & Dongre [17], the authors considered the following phases:

1) Identification & preservation;

2) Acquisition & extraction;

3) Analysis & examination;

4) Documentation and report.

The reasons and motivations behind this choice were that the literature analyzed highly emphasized the lack of standardization, documentation, and formalization of the techniques available in mobile forensics [12, 13, 19]. As such, the author intends to propose and build a toolbox that will potentially support and improve the mobile forensics investigation and also to acknowledge to the digital investigator what are the methodologies that exist in the literature that support the mobile forensics investigation process, what are the tools available, and how one can leverage them, aiming to build a toolbox that would potentially have installed the best available software to pursue mobile forensics. Given this, it was decided to put together the literature methodology that supports this investigation process to suggest the standardization of this field within the available literature and that there needs to be more acknowledgement. Additionally, recent research has shown that one of the best methods for the digital investigator to face the challenge

that derives from the high pressure to conduct and conclude investigations is to develop a standardized digital forensics methodology and strategy while executing it using appropriate applications, tools, and methods [52]. In fact, the literature acknowledges that although digital forensics tools and applications are a critical part of the forensics process, they should not be applied without having a baseline supporting methodology, i.e., without first understanding what the role of that given tool/application is within the digital forensics' methodology [52].

In a line manner, the selection of the tools that will compose the toolbox will also consider the price characteristics of each tool, regarding whether the application/device chosen is free for an investigator to use or requires the user to pay a given amount or a license. The different types of features of the applications and tools that exist to support the mobile forensics field are presented as a way to allow the digital investigator to acknowledge what are the tools that are available for a mobile device forensics investigation, both free and/or paid, and dependently on the budget and level of detail and extraction that the digital investigator has and wants to reach. There are three choices from which the digital investigator can choose and opt, which will enlarge its awareness of the existing applications available to the mobile forensics science.

4-2- Toolbox Strategy and the Supporting Stepwise Approach

As previously mentioned, to build the artifact, i.e., the toolbox was segmented, and the existing and analyzed applications and tools were linked to different steps/phases of mobile forensics. Accordingly, and considering the methodologies described above, we performed the merge between the best of each of them and derived that the following phases should be considered by a digital investigator, for which the investigator should consider the usage of all of them as to conduct an investigation that is accurately documented and supported, namely the following phases/steps (Figure 2): 1) Identification & Preservation; 2) Acquisition & Extraction; 3) Analysis & Examination; 4) Documentation & Report.

Figure 2. Process Flow developed by the authors for the Toolbox Strategy chosen - Based on the two existing mobile forensics methodologies from Ayers & Jansen [49] and Sathe & Dongre [17]

Likewise, and supported by the literature review on the mobile forensics process, namely the processes defined by both Ayers & Jansen [49] and Sathe & Dongre [17], the authors scrutinized and described each of the steps chosen for the support and strategy of the toolbox.

As such, in the first step, 1st Identification and preservation, it is highly crucial for the digital investigator to keep the physical and digital evidence collected to prevent any modifications that may jeopardize the quality of the investigation and its respective evidence from occurring. According to the literature it analyzed, the first technique to use when retrieving a mobile phone is to turn on the airplane mode, as this mode will prevent and block any communication and connection to the networks available, Wi-Fi and Bluetooth. The second technique is to shut down the device by switching it off, which will, similarly to the first technique, focus on blocking communications into and out of the mobile phone. Last but not least, the third technique is to place the mobile phone into a box that will impede communication, like Faraday's box, which represents a shield box that can block network and radio interactions from the mobile phone to the outside [13, 17, 49]. As such, the tools and applications chosen for this step should be ones that can prevent and protect the evidence, both physically (a mobile phone, memory chip, SIM card, and any other hardware component) and digitally (the contents of the hardware above). This can be done by blocking and impeding any communication from and into the mobile phone and creating an exact copy and replica of the phone and its components. Accordingly, Sathe & Dongre [17] perceive that deciding whether the mobile phone and its data (identification) will be pertinent and vital for a digital investigation is also essential.

The second step, 2nd Acquisition and Extraction, is where the digital investigator intends to start the procedures towards the collection and retrieval of a replica of the device's image, which should be an exact copy of the mobile phone and its content. Thus, the digital investigator is mitigating two different risks, the risk of someone attempting to communicate with the mobile phone after it is retrieved, and the risk of the device's physical conditions and its battery life stamina. As such, the tools and applications chosen for this phase should be ones that are able to replicate the device image and/or perform different levels of extraction and acquisition. As mentioned previously, there are different levels of acquisition, such as the Manual extraction (acquisition of the data and information that is store in the device itself and

that needs no tool), Logical extraction (acquisition of data and information by connecting the device into a computer or a forensics workstation, via USB, Wi-Fi or Bluetooth), Hex dumping extraction (physical acquisition that involves the extraction of data that is residing in a memory card or any type of memory hardware that is a component of the mobile phone), Chip-off extraction (the action of retrieving and extracting the flash memory chip of a mobile phone with a tool that is able to open and deconstruct the mobile phone) and lastly but not least, the micro read extraction (the activity that involves using an electron microscope to conduct physical observations around the logic gates and circuits of a mobile phone) [4, 49].

The third step, 3rd Analysis and Examination, highlights the importance of the digital investigator being aware and having access to tools and applications to further analyze the data and information collected and retrieved from the 1st and 2nd stages. This data can be phonebook numbers, call and message logs, both text and multimedia, photos, document files, videos, location track points, emails, browser history, and many more, and data that may have been hidden or deleted [17, 49].

Lastly, the final step, the 4th Documentation & Report, is where the digital investigator should focus on documenting the process that was pursued in all of the phases/steps of the investigation, as well as the evidence that corroborates the process and its conclusions, so as to be able to have a report that is admissible to a courthouse and that can be potential vital information for a given case [17, 49].

5- Demonstration

Although there is no use case performed over the given applications/tools described below, the toolbox is composed of 33 applications/tools, which resulted from a meticulous analysis of the current market and literature aimed at providing the scientific community with a set of applications to support the forensics process associated with mobile devices. These selected tools were chosen to answer each of the steps of the designed mobile forensics methodology, namely the one presented in Section 4.2. Nonetheless, there are other valuable tools available. The curated selection is an example of the best tools available to design a toolkit that covers and answers the essential aspects of mobile forensics science and each step within the designed mobile forensics methodology process flow. Consequently, these selected applications/tools are intended to serve as an example of market and literature best practices, illustrating the diversity of tools employed in a given mobile forensics activity. By recognizing this dynamic nature that characterizes the field, we can encourage users to adapt, search, and supplement this toolbox with additional applications/tools that are considered relevant to the unique challenges presented in their forensics activities.

Given the afore-mentioned and chosen strategy to support the analysis and choice of the tools and applications that should potentially compose the toolbox, the following applications were analyzed and corresponded to each of the mobile forensics strategies chosen to perform the Toolbox Instantiation and structure, namely the following 33 applications and tools: Project-A-Phone, NFI Memory Toolkit, BitPim Tool, LiME (Linux Memory Extractor), Paladin Forensic Suite and its Autopsy Software, Universal Forensic Extraction Device (UFED) & UFED Chinex Device, UFED Physical Analyzer, UFED Touch, AccessData Forensic Toolkit FTK Imager, Guidance Encase, Micro Systemation XRY, EnCase Neutrino, Paraben Device Seizure, BlackLight, Oxygen Forensic Suite Kit, Android SDK (Software Developer Kit), Magnet Axiom, qtADB, SQLite Forensics Toolkit, Fernico ZRT, EDEC Eclipse, Micro Systemation XAMN, iSesamo Phone Opening Tool, Xytronic 988D Solder Rework Station, FEITA Digital Inspection Station, Circuit Board Holder, FINALMobile Forensics, Susteen Secure View, MOBILedit! Forensic, Andriller, Encase LinEn, Passware Kit Forensic, Elcomsoft iOS Forensic Toolkit.

Through the analysis of the literature available for each of these tools and applications, the authors drew the toolbox architecture, which has the following attributes for each of the 33 applications analyzed: The step that the tools and applications are most likely to fit in the process Flow of the Toolbox Supporting the mobile forensics investigation process (1st Identification & Preservation, 2nd Acquisition & Extraction, 3rd Analysis & Examination, and 4th Documentation & Report), the Free/Paid Feature, and the Motivation/Issue/Usage that characterizes each of them. After doing so, the authors described and analyzed each of the 33 tools and applications, describing their main characteristics, their suitability, some results of tests performed and available in the literature, and more information about them. To do so, the authors started by describing the first application/tool presented in the toolbox, namely the following:

Project-A-Phone tool - The Project-A-Phone tool can be suitable for an investigation, namely those that require manual examinations or that, due to the non-availability of an imaging application or device during an investigation, force the digital investigator to leverage this tool to perform a manual analysis [53]. This tool functions as a peripherical one, including a high-resolution camera that allows the user to integrate this tool with others, thus generating synergies. Likewise, this tool allows the digital investigator to operate within the mobile phone by taking screenshots of every step that is pursued and taken during the investigation, creating instant JPEG, PNG, or BMP image files, and automatically yielding sequenced names to each of the images taken [11, 53]. What is more, this tool allows for the sequenced organization of all the evidence collected during the investigation process, allowing the user to record audio and video frames during the examination process and leverage voice commentary. Due to the size of this device, it allows the user to handle close to any mobile phone on the market, as its equipment allows the tool to adjust to any phone size and

measure. Besides this, the tool can be used to document the work pursued, as it contains a reporting tool in its characteristics. It is essential to notice that this tool requires the mobile phone to be turned on; thus, if not correctly isolated, this tool should not be employed or used as a last option, as it makes the mobile phone more vulnerable to outside connections that can jeopardize the investigation by erasing or hiding the data and its information [53, 54].

The NFI Memory Toolkit tool - The NFI Memory Toolkit device represents a universal tool designated as the combination and articulation of hardware and software while allowing the digital investigator to read memory chips and, by doing so, retrieve essential data, including low-level data extractions and acquisitions. On the one hand, the hardware allows this toolkit to connect physically with the memory chip of the mobile device. On the other hand, the software allows the tool to undergo the required and necessary queries that the digital investigator needs to access the data inside the memory chip. Likewise, it can perform on damaged and/or password-protected mobile phones and retrieve several types of data, including registered phone calls, phone book numbers, pictures, and multimedia, and it may be able to retrieve browser history [55].

The BitPim Tool - The BitPim tool can be regarded as an open-source and free tool that can be used to manage, operate, and view the data from a mobile phone, including data from phones that contain basic features. The tool leverages the proper connection between the forensic workstation (the station where the forensics investigator is pursuing the investigation process) and the mobile phone device. The data included phone calls and message logs, multimedia such as video and images, calendar files, and contacts [53, 56]. Even so, this tool has not been updated since 2010, which, according to Bachler [57], causes many phones not to be recognized by the forensic workstation when connected via a USB Port, and thus, the tool cannot examine the phones.

LiME - Linux Memory Extractor - It is an open-source and free tool that can be perceived as a technique and tool to retrieve and capture volatile memory from an Android phone or any Linux-based one. It works via a debugging bridge via USB between the mobile device and the forensics workstation, where the application is to perform memory retrieval from Android Phones. This tool can thus capture a forensic image of the mobile phone. Accordingly, this tool aims to minimize the interaction between the forensics examiner and the kernel (i.e., the central component of an operating system) space processes during the acquisition phase; hence, by doing so, it yields captures that are more accurate when it comes to forensics analysis [57].

Paladin Forensic Suite and its Autopsy Software - From Sumuri (Paladin's Provider), Paladin represents an open-source toolkit application and suite, which is utilized by the connection of the mobile device to the computer and/or forensics workstation [57, 59]. It encompasses a wide variety of open-source tools, like Autopsy and many others, which focus on imaging the mobile phone, recovering and analyzing information from calls and messages to emails, logs, and multimedia like photos and videos, while giving the digital investigator several tools present in a user-friendly GUI that will potentially guide and aid the investigator process. The Autopsy represents an open-source forensics tool that allows the digital investigator to analyze the image created from the mobile device (the step of imaging must be pursued using a different tool), manage and analyze the digital evidence collected, and document and create a chronological timeline for all the actions that were performed within each phone. This tool can perform manual examinations and access raw files retrieved from an Android mobile phone. Accordingly, this tool must run on the forensics workstation and can retrieve artifacts such as call and text message logs, multimedia, GPS track points, and more [60].

Universal Forensic Extraction Device (UFED) and UFED Chinex - The Universal Forensic Extraction Device (UFED) represents a commercial device, a separate hardware device, from Cellebrite, that aims at performing image extraction on mobile devices due to their physical extraction capabilities [61]. In order to do so, the digital investigator needs to connect the mobile phone to the UFED device, aiming to capture all the available information, from contacts and dial logs to messages, multimedia, and files. This device also supports Bluetooth and infrared transmission [11, 61]. This device can also perform logical acquisitions, represented by the extraction of the data and information present in the logical file allocation memory of a mobile phone [19]. Likewise, the device can physically examine the mobile phone, increasing the success of reaching and retrieving deleted or missing data from the phone [62]. Besides this, the device can also clone SIM cards and extract information from messaging applications like WhatsApp. As such, the UFED can retrieve and gather information from the SIM, even if it is inside the Mobile Phone [61].

Universal Forensic Extraction Device (UFED) Physical Analyzer - The Universal Forensic Extraction Device (UFED) Physical Analyzer represents an analytical platform from Cellebrite that aims at performing analyses of the image extracted from a mobile phone. It encloses the analysis of evidence that was retrieved from a mobile phone while allowing for both logical and physical analysis through the platform that comes with it, namely the query for words and keywords, shaping the data, and creating tailored reports on the data so to reach different conclusions and to support the analysis [60].

Universal Forensic Extraction Device (UFED) Touch - The Universal Forensic Extraction Device (UFED) Touch represents a portable compact version of Cellebrite that can be used in any mobile device investigation, as besides acquiring and performing different levels of extractions, it allows the user to create an exact copy of the memory of the Mobile Device. Likewise, it also supports file system extraction. As such, it can acquire levels of extraction such as the physical, the logical, and the file system. In addition, this tool can also capture screenshots of a mobile phone while providing the digital investigator with a list of activities that can be performed to conduct several different analyses of

the mobile image [57]. This tool contains an easy-to-use and analyze GUI (Graphical User Interface) while capturing mobile phone screenshots. According to Hayes [53], this tool can be used in the field or a forensics laboratory/ workstation.

Access Data Forensic Toolkit FTK Imager - The FTK Imager tool is usually used for physical acquisition, as it can extract the data and information present in the memory chip of a mobile phone through the connection via USB of the phone to the forensics workstation [61]. Besides this, the tool can help the digital investigator pursue the physical examination and analysis of different types of data, namely, contact books, text, multimedia messages, call logs, pictures, and multimedia files [20]. Likewise, according to Rao & Chakravarthy [21], to analyze the different types of data, an investigator can employ the FTK Imager tool, which will allow the analysis of the captured images of the partitions, data, cache, and system, including applications' data and the memory chip data. So, according to the authors, to leverage this application's full potential, the digital investigator should be capable of rooting the device to gain access and privileges as a root user, allowing for deeper and critical access. Accordingly, Jadhav & Joshi [6] perceive the FTK Imager as a tool allowing the investigator to gather information such as the IMEI number and other important ones on the device status and the manufacturer's information. In fact, Shortall & Azhar [62] referred to this tool as one of the most available on the market to perform mobile phone imaging. In addition, Alhassan et al. [22] noticed that this tool could not only able to collect data/evidence that somehow was deleted, such as documents and multimedia files, but also gather different data from the mobile's memory while noticing that the tool was not able to neither spot nor recover any data from the SIM card.

Guidance Encase - The Encase forensic tool focuses on acquiring and capturing digital evidence by imaging the mobile phone through its disk imaging functions. This tool, which runs under the Windows operating system, corresponds to a forensics tool designed for the imaging of mobile phones and provides different and various features to the digital investigator [63]. The Encase tool contains the characteristic, just like the FTK imager, to allow for client-server remote forensics, in which an executable is set on the client workstation. According to the author, this may be a helpful feature for remote forensics, where the workstations may be geographically spread and the digital investigators' team is consolidated in one location [64]. Alhassan et al. [22] noticed that this tool could not collect deleted data from the mobile device.

Micro Systemation XRY – This tool can be perceived as a mobile device forensic tool built and formed by Micro Systemation. This tool guides the digital investigator throughout the process. It is able and available for logical (extracting information by communicating with the mobile operating system) and physical (retrieving the available raw evidence that is residing in the mobile phone) examination and analysis on mobile phone devices [65]. According to the author, one of the most exclusive characteristics that distinguishes this tool is the fact that it embodies a device manual, which comprises a comprehensive list of the support that is presented for each mobile phone, as well as aids the investigator in finding what type and kind of data can be collected and what the application cannot retrieve. Accordingly, the author states that this application can also offer different options report-wise, as the investigator can generate reports in different formats, such as Word, Excel, or PDF, which may include data and evidence regarding the respective analysis. For Gajjar & Sharma [23], this tool, commercial forensics one, provides a fast-paced extraction and acquisition technique that leverages the Windows operating system and can retrieve and analyze information from mobile phones, such as phonebooks, multimedia and document files, messages, and call logs.

Encase Neutrino - According to Hoog [65], the Encase Neutrino tool was developed to answer the needs of one who must forensically retrieve data from a mobile phone and perform analysis to reach a conclusion or corroborate one. This tool focuses on mobile phones with operating systems from iOS to Android and Windows Mobile. Accordingly, the author states that with this tool, the investigator can be able to retrieve, examine, and conserve different types of data, including phone books, text messages, multimedia messages, call and email logs, calendar information, images and videos, and other types of files that may be on the mobile phone. Likewise, the author states that one of the advantages of Encase Neutrino was its capability to integrate with any tool from Encase, like the ones analyzed in this research, allowing for deeper and integrated analysis. Besides this, this tool can also create and generate reports in formats like HTML, allowing the digital investigator to contain all the reports on one page.

Notwithstanding, the author tested this tool and observed that recovering deleted text messages was impossible. It was impossible to retrieve the phones and/or multimedia videos that resided in the phone's memory card, just the ones that were sent as a Multimedia Message. Through research and analysis of the literature available, this tool was discontinued by its manufacturer.

Blacklight - This mobile forensic tool represents a comprehensive one, and it is seen as a multi-platform that helps the digital investigator to pursue the mobile forensics process within iOS devices, such as the iPhone and iPad, on Android devices, and on Windows computers. This tool contains a unique GUI (graphical user interface) designed and built to answer the needs of forensics examiners, containing capabilities and a friendly and insightful user experience on all steps of the mobile forensics' investigation process. Likewise, Blacklight is expected to help the investigator in the acquisition phase of the data on the internal memory of a mobile phone while being able to aid the examiner in the reporting stage with the generation of the reports, namely custom ones. This tool is expected to be able to collect data on the equipment and its user (device type, OS version, IMEI), on book numbers, on calls and messages logs, document

files, application data, GPS location track points, and internet data [66]. Likewise, the tool allows the investigator to use filter options within large data sets, allowing the investigator to apply any filters to quickly seek and retrieve the information that one is looking for, including filters by name, file type, and/or attribute.

Paraben Device Seizure - Perceived as a software kit by Paraben, it aims to allow the digital investigator to extract, collect, examine, and conclude the data retrieved from a mobile phone. Likewise, it is a handheld mobile forensics kit that allows for logical and physical data acquisitions, and it is expected to be able to recover erased data and complete data dumps. Hence, allowing for the analysis and visualization of the data that was acquired and for the bookmarking of the data being analyzed permits the investigator to filter within the data by using text string queries to retrieve and dive into the data the digital investigator is looking for. According to the author Hoog [65], this software kit is regarded as one that does not modify and alter the digital evidence retrieved at any stage, as it acquires data by connecting the device through a USB data cable to the forensics workstation. Moreover, the Device Seizure (DS) allows the digital investigator to retrieve and transfer files to the workstation for further analysis and documentation [56, 65]. Besides this, according to Alhassan et al. [22], this kit is an effective one, which can, with high accuracy and effectiveness, access the phone's memory and retrieve essential and critical data, even those that were somehow deleted.

Oxygen Forensic Suite Kit - According to Cappa et al. [67], the Oxygen Forensic Suite Kit is one of the most noteworthy tools and solutions on the market for the pursuit of digital mobile forensics and establishes a connection to the mobile phone via USB. Accordingly, the authors denote that while there is a significant rise in the need for mobile forensics tools and capabilities, the high initial price plus maintenance costs are usually some of the characteristics of commercial mobile forensics tools. Likewise, Tamma et al. [60] denoted that this tool is an advanced one that allows the digital investigator to recover, retrieve, and analyze data from mobile devices, providing logical guidance for different types and models of mobile phones and allowing for a fully computerized acquisition and examination process. Besides this, the tool allows for integrating images/backups retrieved from a mobile phone using tools like Cellebrite and XRY; henceforth, the digital investigator can pursue analysis on the Oxygen tool. Despite not being able to perform physical and file system extractions, and hence not retrieving a full forensic image, this tool supports logical acquisition and, thus, is expected to be able to recover and retrieve data like book numbers and their photos, calendar details and events, call and message logs, event logs, pictures, video and audio multimedia, passwords, locations, device and user informational data, emails, and its accounts. Even so, it may recover erased data from SQLite databases, thus recovering erased messages, calls, emails, and photos. What is more, the tool contains features like the filtering of the data using keywords and/or regular expressions, report generation in different formats, like Word, Excel, PDF, and HTML, manual analysis of data, a user-friendly and accessible user interface, and a timeline where it is registered the user's actions and movements are organized by date and time [60, 68].

Android SDK (Software Developer Kit) - According to Tamma et al. [60], the Android Software Developer Kit (SDK) corresponds to one tool that aims to allow and guide a user to develop, build, quality test, and debug production applications to be executed and run on Android operating system phones. Although it does not correspond to a forensics tool itself, as it involves software libraries, tools, and documentation material, it provides the investigator with valuable and insightful documentation and support to aid in investigating an Android device. Hence, the authors suggest that the digital investigator obtain a deep and good understanding and knowledge of the Android SDK to understand the particularities of a mobile device and its data [60].

Magnet Axiom - Magnet Axiom corresponds to a tool that allows the loading of the image created based on the user data and analysis of that image, thus analyzing data such as multimedia, browser and activity history, documents, and personal data. This tool can also be applied and employed to document the analysis and the reporting evidence that were under examination and vital for the conclusions taken, as well as the documentation of all log files that illustrate the reperformance of the analysis performed [23].

qtADB - Jadhav & Joshi [6] suggested that the digital investigator should leverage tools like the Android SDK, Magnet Axiom, qtADB, FTK Imager, and SQLite Forensics. The application qtADB will help the digital investigator locate essential data, namely the user data. At this stage, the investigator should look at the block of the mobile phone that contains the user data, representing all the data stored in the device's external and/or internal memory and relating to the user and its activity while using the mobile phone.

SQLite Forensics Toolkit - As previously mentioned, for Jadhav & Joshi [6], a tool that allows the digital investigator to analyze the browser's favorites, history, and activity is SQLite Forensics. Accordingly, the authors Kim et al. [18] perceived that a big part of the data and information stored in a mobile phone and that it creates and transfers may be registered as log files, usually in the SQLite DB format. As such, the SQLite Forensics tool can analyze this data and yield the digital investigator with techniques to quickly filter and search for a given data set, just like in a database. In fact, according to Tamma et al. [60], the SQLite format is a controlled SQL database engine used by almost every mobile phone, including iOS and Android devices. This database format is an open-source one that contains multiple tables and views, being portable and accurate at the same time. It is being heavily used by mobile phones for data storage.

Fernico ZRT - Just like the device Project-a-Phone, it consists of a tool created to photograph the mobile phone's screen while using a digital camera to do so and allow for the documentation of the process by which the digital investigator pursues the analysis [53]. This tool is used to manually acquire data, which consists of the investigator using

the phone screen to get the phone content directly from the mobile phone. As such, this method works with every mobile phone and requires no training. However, it does not preserve the integrity of the digital evidence in analysis and does not perform the extraction and acquisition of missing or erased data [69].

Micro Systemation XAMN - As previously analyzed, the XAMN is from Micro Systemation, which also developed XRY. With XAMN, the company intends to perform link analysis around the mobile phones' forensics investigation, i.e., allowing the digital investigator to leverage multiple images for different smartphones while quickly identifying similarities and differences between the phones, including the phone book [53]. Accordingly, this type of analysis may be relevant when searching for what suspects and victims may have in common. Besides this, the tool contains a calendar and a chronological feature visualization, allowing one to link the time and the place where a supposed suspect and/or victim were at that given time [53, 70].

MOBILedit! Forensic - According to Tamma et al. [60], the MOBILedit mobile forensic tool can be employed by the digital investigator to visualize, search, find, and extract data from a mobile phone, namely, call logs, phone numbers, text and multimedia numbers, document files, calendars and event files, and application data, while also extracting some information on the mobile phone itself, such as the IMEI and details on the SIM card. The authors perceived that the tool could extract deleted data from mobile phones and backup encryptions under some circumstances. This software yields the investigator capabilities that allow for the logical acquisition of data, and by doing so, it allows for examinations and reports on that data. It connects to the mobile phone through infrared, Bluetooth, or cable. This application identifies critical information about the mobile phone, such as the manufacturer, the number of the mobile, and the IMEI. It can retrieve information like SIM card phone call logs and books, last registered numbers dialed, messages, files, and multimedia [22]. Moreover, according to Hayes [53] and Hoog [65], this tool can generate investigation reports in different languages, with preprepared templates developed and designed according to set needs. Moreover, this application allows the digital investigator to clone the SIM card and retrieve the information [23].

Encase LinEN - From the same manufacturer as the Encase analyzed previously, the LinEN software is based on the Linux operating system and aims at disk imaging, i.e., the creation of disk images, which will then be compatible with the Encase software previously analyzed [63].

Andriller - According to Silveira et al. [71], this tool represents one of the forensic tools and suites that allow the digital investigator to acquire and examine data extracted from a mobile device. It is designed and focuses on Android OS mobile phones working through the connection via USB port from the computer/forensics workstation to the mobile phone, and thus, other types of operating systems need to be recognized using this tool [57]. Accordingly, Asim et al. [68] denoted that this forensic tool offers digital investigators tools that allow for the unlocking of smartphones, including phones that are pattern-locked or contain a password or a PIN combination.

Passware Kit Forensic - The Passware Kit Forensic is intended to search the passwords for iOS and Android mobile phones' backups, as well as acquire Android images, extracting the data from them. It can integrate with other software, like the Oxygen Forensic Suite analyzed [72].

Elcomsoft iOS Forensic Toolkit - According to Hoog [65], the Elcomsoft iOS Forensic Toolkit is a commercial application for iOS mobile phones, focusing on being able to perform physical extraction and acquisition on mobile devices running the iOS operating system, namely, the iPhones and the iPads. Accordingly, this tool is also expected to retrieve critical information on the device and its file system, namely, passwords and encryption keys, and it is supported by both Windows OS and Mac OS (iOS).

Other relevant tools for the mobile forensics process - EDEC Eclipse, just like Fernico ZRT and the Project-a-Phone hardware and software kit, represents a tool that allows for the manual extraction of data, where the digital investigator goes through the device's touch screen and/or keypad. The steps and data are documented in photos taken directly with the EDEC Eclipse device [24] for the technique of Chip-off extraction and acquisition, which intends the data to be directly retrieved from the flash memory of the mobile phone, which is removed through the retrieval of the mobile phone’s memory chip directly from the phone. To do so, Kapale & Attar [24] suggest tools like the Xytronic 988D Solder Rework Station, iSesamo Phone Opening Tool, FEITA Digital inspection station and the Circuit Board Holder. In addition, according to Homeland Security – Science and Technology [73], the final mobile forensics tool can be used to capture and/or perform analysis and examinations within a mobile phone via logical and/or physical data acquisitions. This tool can also be applied to identify information and data, like locations, text and multimedia messages, video, audio, social media, and application data [71]. Likewise, Homeland Security – Science and Technology [74] tested the mobile device acquisition tool, Susteen Secure View, which provides the digital investigator with the ability to perform logical and physical acquisitions of data for different mobile devices, including the retrieval and collection of phone books, calls and text messages logs, calendar events, applications, and erased data, yielding the digital investigator with a friendly and accessible graphical interface. To sum up the toolbox generated, as well as the main features and characteristics of each of the applications and tools analyzed, the authors generated a table containing this information for the reader to have an overview of the toolbox and its components, namely, the following (Table 2):

Table 2. Process Flow of the Toolbox Supporting the mobile forensics process

Toolbox Tools and Applications	1st Identification Preservation	2nd Acquisition Extraction	3rd Analysis Examination	4th Report Documentation	Free/ Paid Feature	Summary of the Motivation/Issue/Usage
Project-A-Phone		x		x	Paid	This tool can be suitable for an investigation requiring manual examinations or due to the non-availability of an imaging application or device during an investigation. It functions as a peripherical one, which includes a high-resolution camera that allows the user to integrate this tool with others. This tool also allows the digital investigator to operate within the mobile phone by taking screenshots of every step that is pursued and taken during the investigation, automatically yielding sequenced names to each of the images taken while allowing the user to record audio and video frames during the examination process, as well as letting the user leverage on voice commentary during the process. Due to the size of this device, it allows the user to handle close to any mobile phone in the market.
NFI Memory toolkit		x			Paid	Represents a universal tool designated as the combination and articulation of hardware and software while allowing the digital investigator to read memory chips. The hardware allows this toolkit to connect physically with the memory chip of the mobile device, and the software side allows the tool to undergo the required and necessary queries that the digital investigator needs to access the data inside the memory chip. It can also be performed on damaged and/or password-protected mobile phones.
BitPim Tool		x	x		Free - Open Source	This open-source and free tool can be used to manage, operate, and view data from a mobile phone, including data from phones that contain basic features. The tool leverages the proper connection between the forensic workstation (the station where the forensics investigator is pursuing the investigation process) and the mobile phone device.
LiME - Linux Memory Extractor		x			Free - Open Source	The LiME, an open-source and accessible tool, is a technique and tool to retrieve and capture volatile memory from an Android phone or any Linux-based one. It works via a debugging bridge via USB between the mobile device and the forensics workstation where the application is to perform memory retrieval from Android Phones. This tool can thus capture a forensic image of the mobile phone.
Paladin Forensic Suite and its Autopsy Software		x	x	x	Free - Open Source	Paladin represents an open-source toolkit application and suite which connects the mobile device to the computer and/or forensics workstation. It encompasses a wide variety of open-source tools, like Autopsy and many others, which focus on imaging the mobile phone, recovering and analyzing information from calls and messages to emails, logs and multimedia like photos and videos, while giving the digital investigator several tools present in a user-friendly GUI that will potentially guide and aid the investigator process. The Autopsy, an open-source forensics tool, allows the digital investigator to analyze the image created from the mobile device, manage and analyze the digital evidence collected, and document and create a chronological timeline for all the actions performed within each phone. This tool can perform manual examinations and access raw files retrieved from an Android mobile phone.
Universal Forensic Extraction Device (UFED) & UFED Chinex device	x	x			Paid	It represents a commercial device—a separate hardware one—that aims to perform image extraction for mobile devices due to their physical extraction capabilities. This device also supports Bluetooth and infrared transmission. It can perform logical acquisitions and physical examinations of the mobile phone, increasing the success of reaching and retrieving deleted or missing data from the mobile phone. Besides this, the device can also clone SIM cards and extract information from message applications like WhatsApp.
UFED Physical Analyzer			x	x	Paid	It represents an analytical platform from Cellebrite that aims to perform analyses of images extracted from mobile phones. It encloses the analysis of evidence retrieved from a mobile phone while allowing for logical and physical analysis through the platform that comes with it. Namely, the query for words and keywords shapes the data and creates tailored reports.
UFED Touch	x	x	x		Paid	It represents a portable, compact version of Cellebrite that can be used in any mobile device investigation. Besides acquiring and performing different levels of extraction, it also allows the user to create an exact copy of the mobile device's memory. It also supports file system extraction, physical and logical ones. This tool can also capture screenshots of a mobile phone while providing the digital investigator with a list of activities that can be performed to conduct several different analyses of the mobile image. This tool contains an easy-to-use and analyze GUI while capturing mobile phone screenshots.
AccessData Forensic Toolkit FTK Imager		x	x		Free	It is usually used for physical acquisition and analysis, as it can extract the data and information present in the memory chip of a mobile phone. An investigator can also employ the FTK Imager tool, which will allow the analysis of the captured images of the partitions, data, cache, and system, including applications' data and the memory chip data. It can gather information such as the IMEI number and other on the device status, and the manufacturer's information.
Guidance Encase		x	x	x	Paid	The Encase forensic tool focuses on acquiring and capturing digital evidence by imaging the mobile phone through its disk imaging functions. The tool contains the characteristics, like the FTK imager, to allow for client-server remote forensics, in which an executable is set on the client workstation.

Micro Systemation XRY		x	x	x	Paid	It guides the digital investigator throughout the process and is able and available for logical examination and analysis on mobile phone devices. It embodies a device manual comprising a comprehensive list of the support for each mobile phone. It also aids the investigator in finding what type and kind of data can be collected and what the application cannot retrieve. It can also offer different options report-wise, including data and evidence regarding the respective analysis.
EnCase Neutrino		x	x	x	Paid	This tool focuses on mobile phones with different operating systems, from iOS to Android and Windows Mobile. It can retrieve, examine, and conserve different types of data. It can likely integrate with any tool from Encase, like the ones analyzed in this research. This tool can also create and generate reports in various formats. Throughout the research, and by analyzing the literature available, this tool was discontinued by its manufacturer.
BlackLight		x	x	x	Paid	It is a multi-platform that helps the digital investigator pursue the mobile forensics process within iOS devices, such as the iPhone and iPad, on Android and Windows computers. This tool contains a unique GUI (graphical user interface). It is expected to help the investigator in the acquisition phase of the data on the internal memory of a mobile phone while aiding the examiner in the reporting stage with generating the reports, namely custom ones. This tool is expected to collect data on the equipment and its users (device type, OS version, and IMEI). The tool also allows the investigator to use filter options within large data sets, allowing the investigator to apply filters to quickly seek and retrieve the information one is looking for, including filters by name, file type, and/or attribute.
Paraben Device Seizure	x	x	x		Paid	Perceived as a software kit by Paraben, it aims to allow the digital investigator to extract, collect, examine, and conclude the data retrieved from a mobile phone. Likewise, it is a handheld mobile forensics kit that allows for logical and physical data acquisitions, and it is expected to be able to recover erased data and complete data dumps. Hence, allowing for the analysis and visualization of the data that was acquired and for the bookmarking of the data being analyzed permits the investigator to filter within the data by using text string queries to retrieve and dive into the data the digital investigator is looking for.
Oxygen Forensic Suite Kit		x	x	x	Paid/Free (Lower/Limited Capabilities)	This advanced kit allows the digital investigator to recover, retrieve and analyze data from mobile devices, provide logical guidance for different mobile phone types and models, and allow for a fully computerized acquisition and examination process. Besides this, the tool allows for integrating images/backups retrieved from a mobile phone using tools like Cellebrite and XRY; henceforth, the digital investigator can pursue analysis on the Oxygen tool. Despite being unable to perform physical and file system extractions and hence not retrieving a full forensic image, this tool supports logical acquisition and, thus, is expected to recover and retrieve data. What is more, the tool contains features like the filtering of the data using keywords and/or regular expressions, report generation in different formats, manual analysis of data, a user-friendly and accessible user interface, and a timeline where it is registered the user's actions and movements organized by date and time.
Android SDK (Software Developer Kit)			x		Free	This tool aims to allow and guide a user to develop, build, quality test, and debug into production applications to be executed and run on Android operating system phones. Although it does not correspond to a forensics tool itself, as it involves software libraries, tools and documentation material, it allows the investigator to be provided with valuable and insightful documentation and support that can aid one in an investigation of an Android Device.
Magnet Axiom			x	x	Paid	It is a tool that allows to load the image created based on user data and analyze that image, thus analyzing data. This tool can also be applied and employed to document the analysis and the reporting evidence that were under examination and that are vital for the conclusions taken, and the documentation of all log files that illustrate the reperformance of the analysis.
qtADB	x				Free	The application qtADB will help the digital investigator locate essential data, namely the user data. At this stage, the investigator should look at the block of the mobile phone that contains the user data, representing all the data stored in the device's external and/or internal memory and relating to the user and its activity while using the mobile phone.
SQLite Forensics Toolkit		x	x		Paid	It is a tool that allows the digital investigator to analyze the browser favorites, history, and activity in SQLite Forensics. The tool can analyze this data and yield the digital investigator with techniques to quickly filter and search for a given data set, just like in a database.
Fernico ZRT	x	x			Paid	Fernico ZRT, just like the device Project-a-Phone, consists of a tool created to photograph the mobile phone's screen while using a digital camera to do so and allowing for the documentation of the process that the digital investigator pursues on the analysis. This tool is used to perform the manual acquisition of data.
Micro Systemation XAMN			x		Paid	This tool intends to perform link analysis around the mobile phones' forensics investigation, i.e., allowing the digital investigator to leverage multiple images for different smartphones while quickly identifying similarities and differences between the phones, including the phone book. This type of analysis may be relevant when searching for what suspects and victims may have in common. Besides this, the tool contains a calendar and a chronological feature visualization, allowing one to link the time and the place where a supposed suspect and/or victim were at that given time.

MOBILedit! Forensic		x	x	x	Paid* Free version (MOBILedit Lite)	The digital investigator can use this tool to visualize, search, find, and extract data from a mobile phone while extracting some information on the mobile phone itself, such as the IMEI and details on the SIM card. It can sometimes extract deleted data from mobile phones and backup encryptions. This software yields the investigator capabilities that allow for the logical acquisition of data, and by doing so, it allows for examinations and reports on that data. It connects to the mobile phone through infrared, Bluetooth, or cable. This application identifies critical information about the mobile phone, such as the manufacturer, the number of the mobile, and the IMEI. It can retrieve information like SIM card phone call logs and books, last registered numbers dialed, messages, files, and multimedia. This tool can generate investigation reports in different languages with pre-prepared templates and clone SIM cards.
Encase LinEn		x			Paid	From the same manufacturer of the Encase analyzed previously, the LinEN software is based on the Linux operating system and aims at disk imaging, i.e., the creation of disk images, which will then be compatible with the Encase software previously analyzed.
Andriller	x	x			Free/Paid - Open Source	This tool represents one of the forensic tools and suites that allow the digital investigator to acquire and examine data extracted from a mobile device. It is designed and focuses on Android OS mobile phones working through the connection via USB port from the computer/forensics workstation to the mobile phone, and thus, other types of operating systems are not recognized using this tool. Also, this tool offers digital investigators tools that allow for the unlocking of smartphones, including phones that are pattern-locked or contain a password or a PIN combination.
Passware Kit Forensic	x	x			Paid	The Passware Kit Forensic intends to search mobile phones' backups as well as acquire Android images, extracting the data from them. It can integrate with other software.
Elcomsoft iOS Forensic Toolkit		x	x		Paid	This toolkit is a commercial application for iOS mobile phones, focusing on performing physical extraction and acquisition on mobile devices running the iOS operating system, namely, iPhones and iPads. Accordingly, this tool is also expected to retrieve critical information on the device and its file system, namely, passwords and encryption keys, and it is supported by both Windows OS and Mac OS (iOS).
EDEC Eclipse	x				Paid	EDEC Eclipse, just like Fernico ZRT and the Project-a-Phone hardware and software kit, represents a tool that allows for the manual extraction of data, where the digital investigator goes through the device's touch screen and/or keypad, and the steps and data are documented in photos taken directly with the EDEC Eclipse device.
iSesamo Phone Opening Tool		x			Paid	The technique of ChipThection and acquisition intends for the data to be reared for sieving from the directly retrieved mobile phone, which is then removed through the retrieval of the mobile phone's memory chip directly from the phone. Tools like the XyToolsder Rwork Station, the iSesamo Phone Opening Tool, the FEITA Digital Inspection Station, and the Circuit Board Holder can be employed to do so.
Xytronic 988D Solder Rewor to do sok Station		x			Paid	
FEITA Digital inspection station		x			Paid	
Circuit Board Holder		x			Paid	
FINALMobile Forensics		x	x		Paid	This tool can be used to capture and/or perform analysis and examinations within a mobile phone via logical and/or physical data acquisitions. This tool can also be applied to identify information and data, like locations, text and multimedia messages, video, audio, social media, and application data.
Susteen Secure View		x	x		Paid	This tool provides the digital investigator with the ability to perform logical and physical acquisitions of data for different mobile devices, including the retrieval and collection of a phone book, calls and text message logs, calendar events, applications, and erased data, yielding the digital investigator with a friendly and accessible graphical interface.

6- Evaluation

6-1- Focus Group Activity

In this stage, the proposed artifact undergoes assessment to determine its performance [31]. We aimed to promote users' engagement, directly and indirectly impacted by the artifact, to obtain their overall assessment and feedback on its value and validity. As such, we conducted a focus group, which encompassed different topics of discussion for each participant and an overall discussion.

The topics included in the focus group were the following:

- ***Topic 1*** - Mobile forensics challenges and the eventual ethical questions and issues that may urge and appear from a person's/digital investigator's usage of mobile forensics tools;
- ***Topic 2*** - The utility and contribution of the presented framework for mobile forensics and for the investigators;
- ***Topic 3*** - Reflections and insights on what were studied, as well as the relevance, validity, and viability of what was proposed as a framework;
- ***Topic 4*** - Opinions and feedback containing criticism and suggestions for improvements, as well as what, in the participants' views, are the future and next steps for this field and the research developed on it.

The objective of the first and second topics was to obtain the participants' views on the proposed framework and its toolbox, gauging its utility and relevance in the mobile device forensics field. The third and fourth questions aim to elicit negative and positive feedback, providing valuable insights for refining and enhancing the toolbox and the overall research. The research was strengthened by identifying areas for improvement and acknowledging successful elements of the toolbox. Similarly, input from users not directly involved with the tool was also considered valuable, as their feedback is expected to be objective and less biased than those working directly in the field.

This activity involved three different participants, which included an individual who specialized in computer and network science research, another with expertise in mobile forensics and digital investigations and a leading researcher in this field, and a participant from a leading firm within the market of digital forensics, assurance, cybersecurity, and data analytics domains (Table 3).

Table 3. Process Flow of the Toolbox Supporting the mobile forensics process

Participants	Background/ Expertise
Participant 1	A person whose expertise and field of research is the area of computer and network science and whose work is impacted strongly by digital forensics science and its related fields
Participant 2	A person specialized in the area of mobile forensics and digital forensics investigations, including investigations in both the public and private sectors and leading research in the field of digital forensics and cybersecurity
Participant 3	A person who is responsible for a leading firm in the market of digital forensics, assurance, cybersecurity and data analytics fields, applied to both industries, banking and insurance sectors

Consequently, the focus group participants' inputs resulted in four main vital topics to be addressed by the framework proposed within this paper, namely: i) the mobile forensics challenges and ethical concerns, where the interviewees emphasized that the architecture of newer mobile phone models focuses more on security and privacy, which in turn poses different and complex challenges for a digital investigator. Also, a more significant number of mobile devices nowadays have more than one SIM card, including dual SIM and eSIM cards, which may raise questions about ethical concerns because there may be potential corporate and personal data on a mobile phone, jeopardizing the identification and separation of personal and professional data; ii) the capability of the digital forensics investigator to leverage on other forensics sciences and technology, namely the one employed in traditional computers, where the interviewees emphasized the significant differences and potential synergies between mobile devices and traditional personal computers, namely within the processes of collecting and capturing the device's replica, data and processes; iii) the organization's and/or digital investigator's budget constraints and the integrity of the captured data, as for the interviewees the digital investigator capacity to perform the activities related to an investigator depend highly on the budget available.

As a result, organizations must ensure that the right conditions are in place so that a digital investigator can use the best tools available to ensure efficient and effective results; iv) the acknowledgement of the existing tools and applications for mobile device forensics, as according to the interviewees, the presented framework is of great value and utility for the digital investigator as its answer to one of its most significant challenges, namely the lack of standardized procedures and of a methodological review as to aggregate, formalize, and systematize the knowledge that is dispersed within academia. Also, the interviewee highlighted that the precise characterization of the tools and application and its link to a methodological and formal procedure would enhance the current state-of-the-art in this field, stating that the digital investigator will have the proper toolbox to work with.

6-2- Focus Group Output and Overall Discussion

Given the input and feedback obtained during the previous stages, we can reach a conclusive discussion on several aspects brought to attention during this research and the focus group meeting. Aspects such as the relevance of the work and the toolbox, the validity and viability of the work performed, and the enhancements that could be pursued in future work related to these matters.

Regarding the relevance and utility of this work, the focus group participants agreed on the relevance and criticality of the work being performed within this field. One of the characteristics of the framework that was highlighted was the fact that it is a set of tools and applications that are sprightly available, up-to-date, and convenient for any of the stages that a digital investigator may be in, not only raising knowledge and awareness around the literature available but also bringing to the table a toolbox that contains the practicalities of the different forensics' tasks and stages.

Likewise, it was considered relevant that this work strives to look for quality criteria and perform a methodological systematic review as the basis for any mobile forensics' investigation. However, it is also looking forward to studying the different options that are out there in the market, and digital investigators may need to acknowledge that. Besides this, it also highlighted that the work possesses older and more recent literature that covers both free and paid applications and tools, allowing the reader to have a complete overview of these matters.

Regarding the topic of validity and viability, aspects like the different challenges in this field and the framework were discussed, from the ethical issues that the mobile forensics field is facing, namely, the fact that it is very complex and difficult for a digital investigator to be able to separate what is personal from what is professional information within the mobile phone. Likewise, the architecture of a mobile phone was also discussed, as it is currently imposing several challenges to the digital investigator and to the different applications and tools being utilized, as its architecture and operating systems bring complex and secure security and encryption settings.

Other aspects regarding these topics were the requirements to guarantee the traceability of what is captured in the context of mobile forensics, as the digital investigator has to ensure that the different applications and tools that are used do not alter and manipulate the information that is stored within the device or any of its peripheral components. Likewise, it reflected the impact that the privacy of data could have within an investigation, where it highlighted the possible lack of capability of a digital investigator to guarantee that the data that was captured within the examination was well captured and was not posteriorly manipulated and modified, as to ensure that the hash (encryption key) of the image of the mobile phone when it was received is the same as what was captured.

Besides this, the budget restrictions of the different digital investigators may impose limits on the investigation of a forensics examiner as they can limit the choice within the different applications and tools available. A wealthier budget can reflect in not only the purchase of more expensive licenses and tools, which may be more capable and have more features than the less expensive ones, but also the ability to pay for new developments and customizations around those tools. Regarding the improvements that can be performed to the framework as well as the future work in this science, the authors consider it relevant that research strives to look for the parallelism that may exist between mobile device forensics science and any other digital forensics science, namely computer science, as it may be possible to leverage the best practices and existing literature and tools in the mobile device forensics field itself.

Moreover, it also highlighted the need to overview the possibility of the implementation of given tools and applications on the basis of the operating system of a mobile phone, where the mobile phone would share the hash of its image within a specific time with its operator, which would potentially share this information with a digital investigator under legal requirements. Regarding ethical awareness, it is considered that this science would benefit if some more actions and activities promoted the need to have activities that would potentially increase the awareness and acknowledgement of all the intervenants within an investigation, as well as raise awareness on the topics of resisting to read the information that is being captured, as well as on the temptation of sharing this information with public sources or any other source that is not under the legal flow of that given investigation. Last but not least, other feedback and criteria for improvement included the enclosure of more variables regarding the legal and juridical requirements and, thus, acknowledging if the given applications and tools are compliant with the legal requirements and the RGPD Guidelines.

As such, the framework described above and its methodologically standardized basis were seen by the Focus Group's Participants as very useful and relevant for both the field and its investigators, as they focused on critical aspects. As such, the participants understood and acknowledged that it is very relevant and valid and needs to be communicated to raise awareness and knowledge of this area.

7- Conclusions

Given this, to conclude this research, it is essential to acknowledge and mention that the objectives and sub-objectives defined were achieved within this work. Based on all this information and deliverables, the authors expect that both the science of mobile device forensics and any digital investigator will become more aware, concise, and competent in both the existing knowledge around this field and the different challenges, opportunities, applications, and tools that can boost and aid the digital investigation process.

Considering this and having in mind the gaps identified in the "1-1- Problem Statement Section," we can conclude that our study will provide the mobile device forensics field and its digital investigations with:

- Several distinct tools and applications with a specific role in a mobile device forensics methodology that allow the digital investigator to analyze distinct models and types of mobile phones that contain numerous different conditions that each user, model, and component can customize, gaps identified by Vella Colombo [2] and Chernyshev et al. [4];
- A clear understanding of the boundaries and limitations of several different tools and applications for the activity of mobile forensics, as well as the support regarding the process of integrating the data and information of a mobile phone with those given tools, gaps identified by authors Jadhav & Joshi [6], Balushi et al. [7], and Sharma et al. [8];
- A robust and defined mobile device forensics methodology that allows the digital investigator to have available a formal and standardized documentation that describes the techniques and methods that are accessible to be used in a given operation, gaps identified by authors Chernyshev et al. [4] and Omeleze & Venter [12];
- A set of tools and applications that have capabilities and features to embrace the brand-new peripheral tools whose purpose is to enhance and innovate the functions of a mobile phone to an even greater extent, gaps were identified by Barmpatsalou et al. [12], Casey & Zehnder [14], and Spellman et al. [15].

As previously mentioned, the Design Science Research approach supported the research methodology, which allowed for the acknowledgement and analysis of the different and relevant fields, namely forensics science, digital forensics, mobile device forensics, and the digital archaeology that characterizes its environment. By doing so, a toolbox with a set of applications and tools for supporting and enhancing mobile device forensics was built, and a standard methodology was derived from those existing in the architecture [75, 76]. This supported and helped with the creation and derivation of the framework that was proposed for the field of mobile device forensics. Hence, the Framework has a set of applications and tools to support and enhance mobile device forensics on its composition, as well as a support procedure and standard methodology derived from those existing in the literature analysis. Consequently, by providing the digital investigator with a set of tools, their characterization, and their main role within a defined supporting methodology, we believe that the mobile device investigator will have robust and solid knowledge to ensure the validity, integrity, and authenticity of the data acquired and analyzed.

Moreover, with this framework that contains a baseline supporting methodology, the authors will help digital forensics investigators face one of the biggest challenges regarding the digital forensics field. In fact, as stated by Horsman [52], digital forensics tools and applications are being employed without a baseline supporting methodology and a role in it, thus resulting in weak and inaccurate conclusions.

Furthermore, the toolbox is composed of a wide variety of applications/tools that resulted from a meticulous analysis of the current market and literature, which will provide a solid base to support the digital investigator in performing the activities necessary to conduct a robust investigation. These sets of tools cover and reply entirely to the essential aspects of mobile forensics' science and contain a clear role within the different steps of the designed mobile forensics methodology, answering directly to the concerns around the lack of a standardized methodology and the lack of awareness of mobile forensics tools and techniques, which were highlighted by several authors [4, 7, 52].

Reflecting on the next steps and future work, while considering the limitations mentioned above and in line with the conclusions and discussions from the Focus Group Meeting conducted within the Design Science Research methodology to validate the proposed artifact, this research emphasizes the importance of future research into the legal aspects and requirements, as well as compliance with RGPD guidelines for each of the applications and tools within the scope of our paper. It is crucial to identify which applications and tools meet legal standards and which do not.

Likewise, the authors considered it necessary and exciting for the next steps and further research to sort and choose the applications from those that guarantee more integrity and reliability of the data that was acquired, less prompted to manipulations and alterations, to those that jeopardize the integrity of the data as well as the proof. As such, it is strongly recommended for this field and for the activity of a digital investigator to have access to research that focuses on performing this triage to acknowledge which applications less jeopardize the integrity of the data. In line, it is also considered relevant to this area to acknowledge what law enforcement's most used applications and tools are to create awareness of the applications and tools that are most used by the authorities.

Similarly, it is considered valuable for this field to explore the relationship between the cost of obtaining evidence and capturing data versus its utility in an investigation using different applications, potentially establishing relationships with certain levels of causality.

The focus group also highlighted the need for researchers in this area to consider whether the operating system of a mobile phone itself could include tools or a set of tools to ensure the complete integrity of the captured data. This consideration is particularly important given the more advanced and recent security settings and anti-forensic measures that mobile phone manufacturers implement, which can complicate the analysis and acquisition techniques used by digital investigators. Lastly, it is essential for future research in this field to continuously adapt to the fast-paced nature of the mobile industry and mobile forensics. As new applications and tools emerge, they must be capable of performing more analyses and adjusting to the ever-changing landscape and updates in the industry.

7-1- Contributions of the Research

In this article, we proposed an original and innovative instantiation of a framework for a mobile device forensics toolbox. This toolbox comprises various applications, methods, and information designed to enhance the investigation process for digital investigators, improve the quality and effectiveness of their work, and raise awareness and knowledge in this area. The research approach involves developing an artifact that supports and improves the mobile forensics investigation process and its data governance. This will enable digital investigators to have a stable and up-to-date set of tools to assist them in performing various procedures in mobile forensics. The architecture of the toolbox is expected to include the best available software for conducting mobile device forensics. Our previous work highlighted the urgent need for a framework in the mobile device forensics field that includes a toolbox application to support and improve the investigation process and its data governance. This framework will be supported by a strategic and step-by-step approach, aiming to bring a new perspective to the field while addressing several major challenges currently faced by this science. These challenges include the lack of standardization, research and investigation, and insufficient documentation and knowledge of the available tools. These issues are currently impacting and jeopardizing the accuracy and effectiveness of digital investigations [75–79].

Moreover, such a toolbox will support digital investigators in addressing several challenges, including the lack of guidance, documentation, knowledge, and the ability to keep up with the fast-paced mobile phone industry and market. Considering the necessity for increased study and exploration of forensic topics, as reinforced by the literature, we present a toolbox supported by a methodology based on an in-depth study of academic research. We trust that this toolbox will raise awareness and knowledge in mobile device forensics and its data governance, and will generate more accurate, robust, and comprehensive investigation procedures. This approach addresses the challenges presented in section 1-1, "Problem Statement," such as the existence of various types of mobile devices [2, 4], the limitations of mobile forensics tools [6-8], the emergence of new peripheral tools [14], and the absence of standardized testing procedures and methods [12].

Furthermore, this study aims to raise awareness within the scientific community about the need to study and understand the various opportunities in mobile device forensics. These opportunities include the rapid and continuous innovation in mobile phone technology and its features and capabilities, the potential to develop more robust and accurate methodologies through the efforts of digital researchers and ongoing academic investigations, and the need to create a standardized, universal, and reliable framework for digital investigations. The literature acknowledges that one of the most significant opportunities in this field is the pursuit of deeper research to support and enhance activities related to mobile device forensics. This research is expected to provide digital investigators with greater knowledge and awareness of this science and its practices, potential changes and available methodologies, and adequate training and resources [4, 25, 78].

Accordingly, by addressing the gaps identified in this field, we aim to support digital investigators by providing a universal, standardized, accurate, and consistent framework and toolbox to facilitate their investigations and address any issues or questions that may arise. Chernyshev et al. [4] and Balushi et al. [7] similarly emphasize the urgency of addressing the challenges in mobile forensics science, particularly the lack of knowledge regarding mobile device forensics methodologies, tools, and techniques. Additionally, Sharma et al. [8] point out that the increasing reliance of individuals and organizations on mobile phones and wireless technology underscores the need for methodological guidelines for evaluating these devices. This rising demand for testing is driven by the critical role these devices play in recording essential aspects of our daily lives, including storing information such as call logs, SMS texts, media files, and location data. Moreover, they can establish locations, behaviors, and events stored within these devices.

The authors observed that there is a substantial body of literature on critical topics such as: i) the foundations of mobile device forensics [4, 11, 14], opportunities [4, 7, 17], and challenges [8, 15, 79]; and ii) studies and testing of specific tools [49, 42, 68] and activities in digital forensics and mobile device forensics [6, 11, 12]. However, we recognize that no prior study has conducted an extensive and in-depth examination of mobile forensics science, existing methodologies, and tools, while also presenting a comprehensive framework. This framework includes a toolbox of applications and tools supported by a standardized and formalized methodology, which is directly linked to each of the available tools and applications compared within the toolbox.

8- Declarations

8-1- Author Contributions

Conceptualization, B.B., H.M., J.B., and V.S.; methodology, B.B., H.M., J.B., and V.S.; software, B.B., H.M., J.B., and V.S.; validation, B.B., H.M., J.B., and V.S.; formal analysis, B.B. and H.M.; investigation, B.B., H.M., J.B., and V.S.; resources, H.M., J.B., and V.S.; data curation, J.B. and V.S.; writing—original draft preparation, B.B.; writing—review and editing, B.B., H.M., J.B., and V.S.; visualization, B.B., H.M., J.B., and V.S.; supervision, H.M., J.B., and V.S.; project administration, H.M., J.B., and V.S.; funding acquisition, H.M., J.B. and V.S. All authors have read and agreed to the published version of the manuscript.

8-2- Data Availability Statement

The data presented in this study are available in the article material here.

8-3- Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

8-4- Institutional Review Board Statement

Not applicable.

8-5- Informed Consent Statement

Not applicable.

8-6- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

9- References

[1] Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation, 38, 301169. doi:10.1016/j.fsidi.2021.301169.

[2] Vella, M., & Colombo, C. (2022). D-Cloud-Collector: Admissible Forensic Evidence from Mobile Cloud Storage. ICT Systems Security and Privacy Protection. SEC 2022. IFIP Advances in Information and Communication Technology, Vol 648, Springer, Cham, Switzerland. doi:10.1007/978-3-031-06975-8_10.

[3] Ramazhamba, P. T., & Venter, H. S. (2023). Using distributed ledger technology for digital forensic investigation purposes on tendering projects. International Journal of Information Technology, 15(3), 1255–1274. doi:10.1007/s41870-023-01215-9.

[4] Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Security & Privacy, 15(6), 42–51. doi:10.1109/MSP.2017.4251107.

[5] Klomklin, S., & Lekcharoen, S. (2016). A development of mobile phone forensics procedures for law enforcement agencies in Thailand. 2016 11th International Conference on Computer Science & Education (ICCSE), Nagoya, Japan. doi:10.1109/iccse.2016.7581626.

[6] Jadhav, M., & Joshi, K. K. (2016). Forensic investigation procedure for data acquisition and analysis of Firefox OS based mobile devices. 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India. doi:10.1109/cast.2016.7915012.

[7] Balushi, Y. A., Shaker, H., & Kumar, B. (2023). The Use of Machine Learning in Digital Forensics: Review Paper. Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), 96–113. doi:10.2991/978-94-6463-110-4_9.

[8] Sharma, B. K., Yadav, V., Purba, M. K., Sharma, Y., & Kumar, V. (2022). Challenges, Tools, and Future of Mobile Phone Forensics. Journal of Positive School Psychology, 4463-4474.

[9] Kao, D.-Y., Wu, N.-C., & Tsai, F. (2019). The Governance of Digital Forensic Investigation in Law Enforcement Agencies. 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South). doi:10.23919/icact.2019.8701995.

[10] Rascao, J. P. (2021). Data Governance in the Digital Age. Advances in Information Security, Privacy, and Ethics, 34–62, IGI Global, Pennsylvania, United States. doi:10.4018/978-1-7998-4201-9.ch003.

[11] Graves, M. W. (2013). Digital archaeology: the art and science of digital forensics. Pearson Education, London, United Kingdom.

[12] Omeleze, S., & Venter, H. S. (2019). Digital forensic application requirements specification process. Australian Journal of Forensic Sciences, 51(4), 371–394. doi:10.1080/00450618.2017.1374456.

[13] Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. ACM Computing Surveys, 51(3), 1–31. doi:10.1145/3177847.

[14] Casey, E., & Zehnder, A. (2021). Inter-regional digital forensic knowledge management: needs, challenges, and solutions. Journal of Forensic Sciences, 66(2), 619–629. doi:10.1111/1556-4029.14613.

[15] Spellman, B. A., Eldridge, H., & Bieber, P. (2022). Challenges to reasoning in forensic science decisions. Forensic Science International: Synergy, 4, 100200. doi:10.1016/j.fsisyn.2021.100200.

[16] Tassone, C. F. R., Martini, B., & Choo, K. K. R. (2017). Visualizing Digital Forensic Datasets: A Proof of Concept. Journal of Forensic Sciences, 62(5), 1197–1204. doi:10.1111/1556-4029.13431.

[17] Sathe, S. C., & Dongre, N. M. (2018). Data acquisition techniques in mobile forensics. 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India. doi:10.1109/icisc.2018.8399079.

[18] Kim, D., Lee, Y., & Lee, S. (2018). Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices. Journal of Supercomputing, 74(12), 6618–6632. doi:10.1007/s11227-017-2205-5.

[19] Omeleze, S., & Venter, H. S. (2013). Testing the harmonised digital forensic investigation process model-using an Android mobile phone. In 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 1–8. doi:10.1109/ISSA.2013.6641063.

[20] Al-Sabaawi, A., & Foo, E. (2019). A comparison study of android mobile forensics for retrieving files system. International Journal of Computer Science and Security (IJCSS), 13(4), 148-166.

[21] Rao, V. V., & Chakravarthy, A. S. N. (2016). Forensic analysis of android mobile devices. 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India. doi:10.1109/icraie.2016.7939540.

[22] Alhassan, J.K., Oguntoye, R.T., Misra, S., Adewumi, A., Maskeliūnas, R., Damaševičius, R. (2018). Comparative Evaluation of Mobile Forensic Tools. Proceedings of the International Conference on Information Technology & Systems (ICITS 2018), ICITS 2018, Advances in Intelligent Systems and Computing, Vol 721, Springer, Cham, Switzerland. doi:10.1007/978-3-319-73450-7_11.

[23] Gajjar, K., & Sharma, P. (2020). Android based Mobile Forensic and Comparison using various Tools. International Research Journal of Engineering and Technology (IRJET), 7(4), 1399-1404.

[24] Attar M. I. A &. Kapale M. M. M. (2019). Conceptual Study of Mobile Forensics. International Journal of Trend in Scientific Research and Development, 4(1), 161-163.

[25] Mumba, E. R., & Venter, H. S. (2014). Mobile forensics using the harmonised digital forensic investigation process. Information Security for South Africa, Johannesburg, South Africa. doi:10.1109/issa.2014.6950491.

[26] Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. Journal of the Association for Information Systems, 19(5), 358–376. doi:10.17705/1jais.00495.

[27] Weber, S., Beck, R., & Gregory, R. W. (2012). Combining Design Science and Design Research Perspectives--Findings of Three Prototyping Projects. 2012 45th Hawaii International Conference on System Sciences, Maui, United States. doi:10.1109/hicss.2012.163.

[28] Ostrowski, L., Helfert, M., & Xie, S. (2012). A Conceptual Framework to Construct an Artefact for Meta-Abstract Design Knowledge in Design Science Research. 45th Hawaii International Conference on System Sciences, Maui, United States. doi:10.1109/hicss.2012.51.

[29] Dresch, A., Pacheco Lacerda, D., & Cauchick Miguel, P. A. (2015). A Distinctive Analysis of Case Study, Action Research and Design Science Research. Review of Business Management, 1116–1133. doi:10.7819/rbgn.v17i56.2069.

[30] Schorr, F., & Hvam, L. (2018). The Use of Design-science to Define Information Content Requirements for IT Service Catalogs. 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand. doi:10.1109/ieem.2018.8607318.

[31] Cronholm, S., & Göbel, H. (2016). Evaluation of the information systems research framework: Empirical evidence from a design science research project. Electronic Journal of Information Systems Evaluation, 19(3), 158-168.

[32] Soltani, S., & Hosseini Seno, S. A. (2023). Detecting the software usage on a compromised system: A triage solution for digital forensics. Forensic Science International: Digital Investigation, 44, 301484. doi:10.1016/j.fsidi.2022.301484.

[33] Brunty, J. (2023). Validation of forensic tools and methods: A primer for the digital forensics' examiner. WIREs Forensic Science, 5(2), 1-6. doi:10.1002/wfs2.1474.

[34] Hackman, L., Mack, P., & Ménard, H. (2024). Behind every good research there are data. What are they and their importance to forensic science. Forensic Science International: Synergy, 8, 100456. doi:10.1016/j.fsisyn.2024.100456.

[35] Ferreira, J., Santos, B., Oliveira, W., Antunes, N., Cabral, B., & Fernandes, J. P. (2023). On Security and Energy Efficiency in Android Smartphones. 2023 IEEE/ACM 10th International Conference on Mobile Software Engineering and Systems (MOBILESoft), Melbourne, Australia. doi:10.1109/mobilsoft59058.2023.00018.

[36] Alam, M. N., & Kabir, Md. S. (2023). Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions. 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India. doi:10.1109/incet57972.2023.10170607.

[37] Zhang, X., Liu, C. Z., Choo, K. K. R., & Alvarado, J. A. (2021). A design science approach to developing an integrated mobile app forensic framework. Computers and Security, 105. doi:10.1016/j.cose.2021.102226.

[38] Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. Journal of Supercomputing, 75(8), 4372–4387. doi:10.1007/s11227-019-02779-9.

[39] Årnes, A. (2017). Digital forensics. John Wiley & Sons, Hoboken, United States.

[40] Houck, M. M. (2019). How forensic science works: an architecture for the forensic enterprise. Australian Journal of Forensic Sciences, 51(3), 359–368. doi:10.1080/00450618.2017.1375396.

[41] House of Lords. (2019). Forensic science and the criminal justice system: A blueprint for change science and technology select committee 3rd report of session 2017–19. House of Lords, London, United Kingdom.

[42] Roux, C., Ribaux, O., & Crispino, F. (2018). Forensic science 2020–the end of the crossroads? Australian Journal of Forensic Sciences, 50(6), 607–618. doi:10.1080/00450618.2018.1485738.

[43] Valdez, B. (2018). Spotlight on a Discipline. International Social Science Review, 94(2), 1-6.

[44] Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv: preprint arXiv:1708.01730. doi:10.48550/arXiv.1708.01730.

[45] SONMEZ, Y. U., & VAROL, A. (2017). Review of evidence collection and protection phases in digital forensics process. International Journal of Information Security Science, 6(4), 39-45.

[46] Faheem, M., Le-Khac, N.-A., & Kechadi, T. (2016). Toward a new mobile cloud forensic framework. 2016 Sixth International Conference on Innovative Computing Technology (INTECH). doi:10.1109/intech.2016.7845142.

[47] Mirza, M. M., Ozer, A., & Karabiyik, U. (2022). Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS. Applied Sciences (Switzerland), 12(21). doi:10.3390/app122111180.

[48] Bjornson, J., & Hunter, A. (2016). Mobile forensics for cloud data: Practical and legal considerations. 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand. doi:10.1109/pst.2016.7906927.

[49] Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics. National Institute of Standards and Technology, 1-85. doi:10.6028/nist.sp.800-101r1.

[50] Hummert, C., & Pawlaszczyk, D. (2022). Mobile Forensics – The File Format Handbook. In Mobile Forensics – The File Format Handbook. doi:10.1007/978-3-030-98467-0.

[51] Maras, M. H., & Miranda, M. D. (2014). Forensic Science. Encyclopedia of Law and Economics. Springer, New York, United States. doi:10.1007/978-1-4614-7883-6_11-1.

[52] Horsman, G. (2024). The importance of digital evidence strategies. WIREs Forensic Science, 6(1), 1-10. doi:10.1002/wfs2.1507.

[53] Hayes, D. R. (2015). A practical guide to computer forensics investigations. Pearson Education, London, United Kingdom.

[54] Mullen, G. (2006). Project-a-phone revolutionizes the art of presentation. Telecommunications (Americas Edition), 40(5), 8.

[55] Netherlands Forensic Institute. (2011). The NFI Memory Toolkit II – A universal forensic solution to read memory chips developed by the Netherlands Forensic Institute. Netherlands Forensic Institute, The Hague, Netherlands.

[56] Ayers, R., Jansen, W., Cilleros, N., & Daniellou, R. (2005). Cell phone forensics tools: An overview and analysis. National Institute of Standards and technology (NIST), Gaithersburg, United States.

[57] Bachler, M. (2020). An Analysis of Smartphones Using Open Source Tools versus the Proprietary Tool Cellebrite UFED Touch®. Marshall University Forensic Science Center, Huntington, United States.

[58] Heriyanto, A., Valli, C., & Hannay, P. (2015). Comparison of live response, linux memory extractor (LiME) and Mem tool for acquiring android's volatile memory in the malware incident. Australian Digital Forensics Conference, ADF 2015, l(eld), 5–14. doi:10.4225/75/57b3f143fb884.

[59] Sumuri LLC. (2016). Quick Start Guide - Paladin Forensic Mode Version 7.00.

[60] Bommisetty, S., Tamma, R., & Mahalik, H. (2014). Practical mobile forensics. Packt Publishing Ltd, Birmingham, United Kingdom.

[61] Lessard, J., & Kessler, G.C. (2010). Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal, 4(1), 1-12.

[62] Shortall, A., & Bin Azhar, M. A. H. (2015). Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms. 2015 Sixth International Conference on Emerging Security Technologies (EST). doi:10.1109/est.2015.16.

[63] Byers, D., & Shahmehri, N. (2009). A systematic evaluation of disk imaging in EnCase® 6.8 and LinEn 6.1. Digital Investigation, 6(1–2), 61–70. doi:10.1016/j.diin.2009.05.004.

[64] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, S90–S98. doi:10.1016/j.diin.2012.05.001.

[65] Hoog, A. (2011). Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Syngress, Rockland, United States. doi:10.1016/C2010-0-65787-7.

[66] Homeland Security – Science and Technology. (2016). Test Results for Mobile Device Acquisition Tool – BlackLight v2016.1. DHS Science and Technology Directorate, Washington, United States.

[67] Cappa, F., Del Sette, F., Hayes, D., & Rosso, F. (2016). How to deliver open sustainable innovation: An integrated approach for a sustainable marketable product. Sustainability (Switzerland), 8(12), 1341. doi:10.3390/su8121341.

[68] Asim, M., Amjad, M. F., Iqbal, W., Afzal, H., Abbas, H., & Zhang, Y. (2019). AndroKit: A toolkit for forensics analysis of web browsers on android platform. Future Generation Computer Systems, 94, 781–794. doi:10.1016/j.future.2018.08.020.

[69] Alghafli, K. A., Jones, A., & Martin, T. A. (2012). Forensics data acquisition methods for mobile phones. 2012 International Conference for Internet Technology and Secured Transactions, 10-12 December, London, United Kingdom.

[70] Kim, A. D. (2020). Digital Forensics Tools Integration. The Air Force Institute of Technology (AFIT), Ohio, United States.

[71] da Silveira, C. M., de Sousa, R. T., de Oliveira Albuquerque, R., Nze, G. D. A., de Oliveira Júnior, G. A., Orozco, A. L. S., & Villalba, L. J. G. (2020). Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware. Applied Sciences (Switzerland), 10(12), 4231. doi:10.3390/app10124231.

[72] Passware Inc. (2017). Passware Kit Forensic - The complete encrypted electronic evidence discovery solution. Passware Inc., Mountain View, United States.

[73] Homeland Security – Science and Technology. (2020). Final Mobile Forensics Version 2019.07.05 Test Results for Binary Image Tool. DHS Science and Technology Directorate, Washington, United States.

[74] Homeland Security – Science and Technology. (2016). Test Results for Mobile Device Acquisition Tool - Secure View v4.1.9. 2016. DHS Science and Technology Directorate, Washington, United States.

[75] Bernardo, B. (2021). Toolbox Application to Support and Enhance the Mobile Device Forensics Investigation Process. Forensic Science & Addiction Research, 5(3), 1-105. doi:10.31031/fsar.2021.05.000619.

[76] Bernardo, B., & Santos, V. (2020). Mobile Device Forensics Investigation Process. Handbook of Research on Cyber Crime and Information Privacy, 2021, 256–288. doi:10.4018/978-1-7998-5728-0.ch014.

[77] Bernardo, B. (2022). Artificial Intelligence and Digital Forensics on Data Governance Breaking Through its Importance to Organizations and its Operations. Forensic Science & Addiction Research, 5(4). doi:10.31031/fsar.2022.05.000625.

[78] Li, S., Sun, Q., & Xu, X. (2018). Forensic Analysis of Digital Images over Smart Devices and Online Social Networks. IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, United Kingdom. doi:10.1109/hpcc/smartcity/dss.2018.00168.

[79] Akinbi, A. O. (2023). Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. WIREs Forensic Science, 5(6), 1-21. doi:10.1002/wfs2.1496.