A Novel Framework for Mobile Forensics Investigation Process

Mohammed Moreb
Birzeit University

Saeed Salah
Alquuds University: Al-Quds University

Belal Amro
bilala@hebron.edu

Hebron University https://orcid.org/0000-0003-0421-4404

Research Article

Keywords: Mobile Forensics, Digital Forensics, Forensic tools, Acquisition, iOS, Android, Extraction, Artifacts

Posted Date: March 8th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2611927/v1

License: ☕️ This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Version of Record: A version of this preprint was published at International Journal of Computing and Digital Systems on April 21st, 2024. See the published version at https://doi.org/10.12785/ijcds/160110.
Abstract

Investigating digital evidence by gathering, examining, and maintaining evidence that was stored in smartphones has attracted tremendous attention and become a key part of digital forensics. The mobile forensics process aims to recover digital evidence from a mobile device in a way that will preserve the evidence in a forensically sound condition, this evidence might be used to prove to be a cybercriminal or a cybercrime victim. To do this, the mobile forensics process lifecycle must establish clear guidelines for safely capturing, isolating, transporting, storing, and proving digital evidence originating from mobile devices. There are unique aspects of the mobile forensics procedure that must be taken into account. It is imperative to adhere to proper techniques and norms in order for the testing of mobile devices to produce reliable results. In this paper, we develop a novel methodology for the mobile forensics process model lifecycle named Mobile Forensics Investigation Process Framework (MFIPF) which encompasses all the necessary stages and data sources used to construct the crime case. The developed framework contributes to identifying common concepts of mobile forensics through the development of the mobile forensics model that simplifies the examination process and enables forensics teams to capture and reuse specialized forensic knowledge. Furthermore, the paper provides a list of the most commonly used forensics tools and where can we use them in our proposed mobile forensic process model.

1. Introduction

In the current era of the digital age, it is undoubtedly shown that mobile applications have profoundly transformed every aspect of human lives. Users are now relying on mobile applications to do many online activities such as browsing the internet, shopping, transferring money, doing business, communicating using audio or video calls, texting, entertainment, and education. This massive growth of smartphone usage is still incredibly popular and will continue to be for the foreseeable future. According to Fig. 1, The annual sales of smartphones have tremendously increased to around (1.56) billion devices worldwide, smartphones running the Android operating system hold an (87%) share of the global market in 2019 and this is expected to increase over the forthcoming years, while Apple iOS; the second most popular operating system has a (13%) market share across all devices.

Figure 1: Share of global smartphone shipments by operating system from 2014 to 2023 [1]

With this tremendous use of smartphones worldwide, the wide adoption of these devices to carry out technology-oriented services, and the uncontrolled use of mobile applications have turned the mobile environment into a fertile spot to carry out many unethical and illegal activities. Consequently, smartphones became a famous target for cyber-attacks bearing in mind that these devices contain private data [2]. The portability of these devices and the sensitivity of the data they contain raised great concern about the feasibility of using traditional digital forensic methodologies and to what extent they fit this field [3]. Smartphones are equipped with many capabilities that make forensic steps difficult to be handled and require great attention. These capabilities include the availability of different communication technologies such as SMS, 3G, Wi-Fi, GPS, …, etc., the ability to remotely instruct the
device to switch on or off, and the ability to remotely wipe data using different mobile applications. These issues and others created a big challenge for the investigators when dealing with mobile digital evidence [4].

In this regard, a set of terminologies, definitions, and legal issues have appeared that describe the new criminal situations raised due to this new computing paradigm. One of these terminologies is digital forensics which refers to the process of collecting digital evidence from a digital device and analyzing it to prove the guilt or innocence of persons [5]. Mobile forensics is another terminology derived from digital forensics, it aims to recover digital evidence from a smartphone in a way that will preserve the evidence in a forensically sound condition. To conduct mobile forensics analysis, the mobile forensic process lifecycle needs to set out precise rules that will seize, isolate, transport, store, and proof of digital evidence safely originating from smartphones.

The process of digital forensics has become an important issue and systematic approaches were proposed and adopted by many specialized governmental and private organizations and institutions such as The American Academy of Forensic Sciences (ACFS), the European Network of Forensic Science Institutes (ENFSI), the International Institute of Certified Forensic Investigation Professionals (IICFIP), and many other institutions worldwide. Besides, there are some well-known standards and good practices designed for digital forensics such as the two standards provided by ATSM [6], where issues related to digital forensics education challenges are provided as well as specifying the digital forensics steps with details about the requirements for each step.

As thoroughly explained in the literature, the digital forensics process is divided into the following steps, these steps are common in most references with some slight modifications of the details and functionalities of each step: (i) identification: this step involves finding the evidence and where the required data is located; (ii) preservation: in this step, the evidence is isolated, secured, and data is preserved as well. Access to the evidence and data is allowed only for investigators who are working on the case to prevent people from tampering with the data and hence making the evidence illegal; (iii) analysis: in this step, the reconstruction of evidence fragments is performed and conclusions about the evidence are found; (iv) documentation: a record of all the required data is preserved; this record can be used to recreate the crime scene; (v) presentation: a summary of the case and the conclusion are performed at this step, (vi) case closure: in this step, the case is closed by having a legal decision and the evidence is returned or archived accordingly. These steps may vary in their details from one institution to another; however, all of them will lead to a similar sequence of steps that will finally lead to a successful handling of a digital crime.

The mobile forensics process has its particularities that need to be considered. Thus, following a correct methodology and guidelines are vital preconditions for the examination of smartphones to yield good results. In this paper, we develop a novel methodology for the mobile forensics process lifecycle called Mobile Forensics Investigation Process Framework (MFIPF) encompassing all the necessary stages and data sources used to construct the crime case. The developed methodology will contribute to identifying
common concepts of mobile forensics through the development of the mobile forensics model that simplifies the examination process and enables forensics teams to capture and reuse specialized forensic knowledge. Furthermore, it reduces the difficulty and ambiguity in mobile forensics’ domain. Unlike other models, this proposal divides the evidence lifecycle into several modules and describes each module along with its main components, data sources, tools, intra-module, and inter-module interactions easily and clearly.

The rest of the paper is organized as follows. Section 2 discusses the related work including the most common mobile forensic process models as well as common mobile forensics tools. Section 3 details the proposed mobile forensics process model (MFIPF), describing its various modules and sub-modules and their connectivity and the associated data sources, mechanisms, and tools. In section 4, the common mobile forensic tools are classified and mapped to our proposed model based on their applicability at different stages. In Section 5, we conclude the paper and outline some ongoing and future research lines.

2. Related Work

In this section, a brief review of the related literature will be conducted. First, we introduce the work done in mobile forensics models and stages, and then, we will talk about the common tools used in mobile forensics.

1. Mobile Forensics models and phases:

Due to the previously mentioned reasons and challenges, many researchers have proposed some specific mobile forensics procedures and methods to deal with special mobile investigation cases. The existence of such methods is important for the success probability of an investigation and the avoidance of corrupting the evidence or failing to extract some necessary information. Among these proposed models is a model proposed by Moreb [7], where the author discussed the four process phases used for conducting mobile forensics, they are (i) the identification phase which includes many details such as identifying, acquiring, and protecting the data collected at the crime scene; (ii) the collection phase which starts by processing the collected data or evidence, then extracting the relevant information; (iii) the analysis phase analyzes the extracted information to connect the dots and be able to build a robust and admissible case; and (iv) the reporting phase is the final step that presents the findings of the analysis stage into an admissible and understandable format.

In [8], the authors mentioned that there are five phases in the forensic process (identification, preservation, acquisition, analyzing, and reporting) which are similar to what was proposed by Moreb [7]. The study of [9] concentrated on android forensics and proposed a framework of seven stages namely: Intake, Identification, Preparation, Isolation, Processing, Verication, and Documentation. A comparative analysis of five common process models was provided in [10], these models are SFIPM, WMDFM, NIST, HDFI, and USFIPM & NIST. The authors also proposed a secure model by deploying blockchain using Ethereum or a hyper ledger platform.
In [11] the authors proposed ERFF, which helps the investigator to securely obtain evidence more easily. ERFF is an efficient and reliable forensics framework as compared with other frameworks such as SNIF, LFCCF, and LRFF. It uses edge computing to improve reliability, efficiency, and accuracy. Moreover, it helps identify criminal activities more quickly using low-cost edge devices and involves a detective module and a validation model that detect the interaction between a client terminal and the edge resource. In [12] an analysis of the forensic-by-design framework is proposed which includes investigating the limits of the forensic-by-design and its insufficiencies in a Cloud systems context, and it proposes three new forensic-by-design key factors and associated standards and best practices, it also suggests a new generic systems and software engineering driven forensic-by-design framework.

Reference [13] demonstrates the DFWM that provides a general and updated description of the DF investigation process at the workflow level and can be used as a management tool for unboxing the procedures, tasks, and risks involved in the workflow of the individual DF investigations. Using the investigative strategy for the specific case, DFWM serves as a framework for packaging the digital forensic investigation process, providing a detailed structure and visualization of the physical and investigative chores and decisions. DF workflow which guided by the overall investigative strategy of the particular case as follows: (i) review of client requirements and planning stage, (ii) evaluation of deployed workflow stage, (iii) identify the physical and cognitive tasks, and (iv) make decisions and their associated risks at the respective stage. Based on the existing process and models, the layered framework for mobile forensics is proposed in [14], the results have shown that using only one tool is not sufficient to complete the investigation process, the four layers organize as a framework, the number of layers can be increased or reduced as per the case type, the six layers can be grouped to small categories with tools to use for each one as acquisition process with various tools such as MOBILedit, Bulk extractor; analyze the data with various tools like Autopsy and CellDEK, and reporting the case can be generated using MOBILedit Forensic and CellDEK.

In [15] the authors reviewed about 100 Mobile forensics models with the main conclusion that suggests improving and validating the investigation process model, develop of a meta-modeling language, and develop of a definite mobile forensics source to store and retrieve the knowledge formed in the mobile forensics field.

Many forensics investigation process models are used for the Internet of Things (IoTs) such as CIPM for IoTFs [16], the proposed model assists IoTFs users to facilitate, manage, and organize the investigation tasks, it consists of four common investigation processes, preparation process, collection process, analysis process and report process. The proposed CIPM. The roadmap of DFIP discovery of tools [17] discussed in detail the challenges and opportunities for the digital forensics process concerning different fields such as networks, IoT, cloud computing, database system, big data, mobile and handheld devices, disk and different storage media, and operating system.

As seen from the literature, there is a necessity for adopting a robust model to carry out mobile forensic investigations efficiently, a comparison of well-known proposed models is provided in Table 1, we also
included our proposed model MFIP in this table as proof of its usability.

Table 1: A comparative analysis of five common forensics process models with the proposed one.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Functionality</th>
<th>SFIPM</th>
<th>WMDFM</th>
<th>NIST</th>
<th>HDFI</th>
<th>USFIPM &amp; NIST</th>
<th>MFIPF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phase 1: Data Preparation</strong></td>
<td>Preparation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Handling and securing the evidence scene</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mode selection shielding</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Offset/online storage</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phase 2: Information Analysis</strong></td>
<td>Examination and analysis</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Cell state analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Non-volatile evidence collection</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Volatile evidence collection</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Evidence validation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Phase 3: Case Construction</strong></td>
<td>Presentation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phase 4: Case Closing</strong></td>
<td>Review</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Documentation</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Survey and Recognition</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2) Mobile forensics tools

The definition of mobile phone forensics is the science of extracting digital evidence from a mobile device [18]. It provided a wonderful list of resources for catching online criminals who utilize mobile devices for illegal purposes. With their vast number of applications and current properties, mobile devices' ever-increasing storage and processing power provide new hurdles for digital forensics [19]. In order to
collect digital evidence for use in court trials, mobile forensic tools and applications are essential. They can unearth call metadata, SMS, GPS data, application data, and locally stored files.

A set of mobile forensics tools [20] can be used such as Cellebrite UFED Physical Analyzer and Oxygen Forensic Suite to get details about the mobile device, the results have shown that the device has a name and type, and iOS version Oxygen and UFED forensic tools [21] used to recover app data. In general, digital forensic tools for data extraction are categorized into three types manual, logical, and physical [22].

Many mobile forensics tools [23] such as Belkasoft Evidence Center [24], FINALMobile Forensics [25], 3uTools [26], and Magnet [27] are used to extract artifacts from both Android and iOS devices. The SDCA [28] tool is designed to perform the analysis of the differences automatically between two versions of SQL schema, in addition to its ability to analyze the query. In [29]aid forensic investigation in general, by developing a model and a platform to secure potential digital evidence, the SecureRS model can help to prevent unauthorized access and comply with regulations and privacy policies, the result shows a method of ensuring forensically sound digital evidence for DFR as well as for digital forensics processes in general. In [7] the authors discussed the tools used to acquire the data from iOS or Android devices for both rooted and jailbreak mobile; the results have shown that the XRY software tool can recover deleted materials and can be able to extract all the data from the phone but it cannot retrieve deleted data for not jailbroken iPhone.

The work in [30] found out that the data used in the media directory did not have any change even after jailbreaking the device, which means that the integrity of the data remained unchanged by examining the matching hash value before and after the jailbreak. But by analyzing the source code of the exploit used where voucher swap as jailbreak code. It turned out that there was a change in the system data, where a fake kernel task was created instead of the original kernel task that works inside memory to give the privileges to extract the data. As a result of this study, jailbreaking is considered acceptable to help forensic tools extract more data while preserving user data.

There was a previous study in the use of forensic tools in the process of acquiring data on iOS, Android, and Windows using forensic tools Oxygen and UFED to recover applications’ data, and the tools were able to restore the list of contacts that WhatsApp installed on iOS and Android, and unable to recover anything from the Windows device. In addition to the ability of the tools to restore and decrypt the backups of the Android and iOS devices, and unable to find the encryption key for the Windows device. The result was that it could restore conversations even if the application has been deleted if there are backup copies stored on the device for WhatsApp [21]. In [28] it is noted that the developers of forensic tools have limited knowledge of the changes that have occurred to the SQL Lite schema for iOS backups and need to preserve the tools’ compatibility with recent versions. The SDCASQLite Database Comparison Analyzer (SDCA) tool is designed to perform the analysis of the differences automatically between two versions of SQL schema, in addition to its ability to analyze the query, it also demonstrates
that using the tool is feasible to update the Forensic Targeted Data Extraction Application called FTDEA developed by the authors.

As mentioned in [31] the growth of using smartphones from 2016 until 2021 increased from 2.5 to 3.8 billion smartphones. Also, in the report found in [32], the number of users who use social media is about 4.20 billion active users worldwide. According to the comparison as shown in Table 2 [33–35], the forensic tools deployed for mobile device investigations are considered very different from that available to investigate personal computers in terms of availability. These differences in the operating system and file systems structures create difficult challenges for the whole mobile forensic tools’ developers and investigators. Commercial and open-source forensic tools are available for mobile device investigations.

The availability of many mobile forensics tools might cause some dilemmas in the selection of the best tool, for this reason, for this we will provide a mapping table that helps select the suitable tool for each step of our proposed model MFIP.

3. Proposed Mobile Forensics Framework

In this section, we will deeply describe our MFIPF provided in Figure 2. The stages of the framework (Data Preparation, Information Analysis, Case construction, and Case Closing) will be explained showing the detailed steps at each phase.

Figure 2: The Proposed Forensics Investigation Process Framework (MFIPF)

3.1. Data Preparation

The data preparation phase aims to generate a processed dataset that is technically usable for the analysis phase. In this phase, four steps are carried out to guarantee that the acquainted data is gathered systematically and legally. The four steps shown in Figure 2 are described below:

1. **Resource seizure**: In this step, the mobile device is seized in a way that guarantees that the device will not be modified and there should be no ability to connect with the device. To achieve this step, we have to follow the following process [36]: (i) issuance of research warrant from legal representatives; (ii) turning off all wireless communications and putting the mobile device in Airplane Mode; (iii) shielding the mobile device in a Faraday bag that prohibits any external signals to reach the mobile, and (iv) Document these steps and send the mobile device to the digital forensics lab for investigations.

2. **Resource identification**: Once the mobile device arrives at the digital forensics lab, the resource identification process is carried out. The process aims to identify the mobile device under investigation and choose the suitable tools that can be used for the data extraction phase. A description of the mobile device is provided here, the description includes the model and type, physical status (if the device is broken), and logical status (the device is on or off, the device is
functioning or not). Based on this information, the investigator will be able to determine the suitable tools required for the data extraction process. This process should be formally documented [37].

3. **Data extraction:** This is a very important process where the data is extracted from the mobile device, the extracted data will then be used in further stages to extract evidence. The information gathered in the identification phase is the basis of the data extraction method to be used, these methods include:

- **Manual data extraction:** here the investigator manually navigates the mobile device to search for the required evidence; documentation of this process is essential and might be done by video recording of the screen of the mobile device during the navigation process [37]. It is important here for the investigator to conduct the boundaries of the research warrant and never explore data that is not included in the research warrant. This process requires the ability of the investigator to access the device by having the password or pattern. It is worth mentioning here that manual data extraction will affect the integrity of the files and hence the investigator should precisely document the steps he did and the findings as well.

- **Logical extraction:** When applying this method, the investigator will be able to generate a copy of the file system that can be used later to extract data using some tools designed for this purpose. This copy will enable the investigator to view the same data that can be generated using manual extraction [38]. However, this method does not affect the integrity of the files of the mobile device and the investigator can only work on the copy of the files and the original device will be kept safely in an evidence container.

- **Physical extraction:** in this method, a raw image in a binary format of the mobile device's memory is generated, and the output is a bitwise copy of the memory of the mobile device [39]. This copy includes all system files and can also be used to retrieve some of the deleted files as well. However, to generate this copy usually we need to root the device which will affect the integrity of the evidence, so the investigator has to document the details of this step. The generated copy can then be used to retrieve system files as well as some of the deleted files using dedicated data analysis tools.

It is worth noting that the aforementioned methods can be applied only when the mobile device is functional, *i.e.*, not broken, and does not work for broken or malfunctioning mobile devices. In such a case some other methods might be used such as chip-off by which the memory chip of the mobile device is physically removed and attached to a memory reader or a similar device and the data is then extracted [40]. This method requires high skills in electronic device maintenance and may cause the chip to be destroyed if not removed or attached correctly. Another extremely hard method that might be used in very rare cases such as national security is called Micro-read where an electronic microscope is used to read the contents of the memory on gate level base [41]. This method is very expensive and takes too much time but might be used to extract some data from broken devices.

### 3.1.4 Data preprocessing

In this process, the characteristics of the mobile device operating system are studied, and data is categorized based on applications to pinpoint potential evidence(s). Classification techniques are used here to group data based on file system analysis and system log analysis. The
output of this process is a well-prepared dataset that can be used in the analysis stage to extract evidence. The preprocessing step might also include putting the data in a proper file format that is compatible with mobile forensics tools in the analysis phase [42].

3.2 Information analysis

In the analysis phase, evidence(s) is/are extracted by formally interpreting the information generated by the previous phase – data extraction-. The investigator should follow standards and best practices in the field of forensic analysis so that the evidence will be intact, and results are reproducible and acceptable. For a robust mobile forensic analysis, the following steps are suggested to be followed:

3.2.1 Forensic Tools: The first step in the analysis includes the selection of a forensic tool. The selection of the tool depends on many factors including cost, user interface, the familiarity of the examiner, computing platform and environment, and legislative – whether the tool is legally approved or not [43]. A list of mobile forensics analysis tools and their properties are provided in Table [1].

Typically, the examiner may use different tools to generate different information and events, there is also a possibility to use different tools to generate the same event to make sure that the event is reproducible and to prove its validity [44]. Therefore, an examiner should be familiar with different tools to conduct his analysis successfully.

3.2.2 Information examination: After selecting the appropriate tool(s), the examiner will feed the tool with the data preprocessed data and perform a variety of tests and processing tasks against the data. The processing aims to generate an event from the evidence file. There might be many events generated from the same or multiple tools. These events are then stored and fed to the next step which is evidence validation [45].

Events in a mobile device might be found at different locations according to the information the examiner is trying to find. Some of the events might be found in SMS and call logs, others might be found in saved pictures or emails. Some complex events might require retrieving deleted files using special tools while other events require the use of different tools and gathering information to reconstruct that event. The selection of the tool and the process depends on the examiner and requires skilled persons to successfully perform the task [41].

3.2.3 Evidence validation: According to [46], validation is the process of proving the validity of the evidence to a jury. The process implies proving acceptable error rates as well as using scientifically proven valid data, applications, and results. The validation process is applied to all stages in mobile forensics and covers data collection and storage, system, application, user, and algorithm applicability validation.

A very important issue related to validation is the use and following up of standards and best practices developed for this purpose. Many countries have developed standards for digital and mobile forensics through their dedicated institutions such as NIST in the states. Besides, some well-known digital
forensics developers have also proposed some best practices that are proven to generate valid evidence with an acceptable error rate [47]. The examiner must follow these standards and verify the validity of the evidence during the entire investigation process.

3.2.4 Evidence correlation: Correlation involves the ability to extract the semantics from different sources such as SMS, social media messaging, emails, ..., etc, and to generate a knowledge base that clearly shows the correlation among these generated events. Domain and application ontologies might be used to correlate different events to a knowledge base [48].

Event correlation and reconstruction might be carried out using different techniques and technologies including rule-based, semantic models, tree/graph-based, timestamp-based, finite state machines, and live event construction [49], such techniques aim to construct valid evidence from different sources of events with acceptable error rate. The output of this stage will be used as input for the next phase which is case construction.

3.3. Case Construction

The output of the second stage - information analysis - is fed as an input to the case construction stage, which takes the evidence list to prepare results and move towards closing the case. Four steps are necessary in the process of case construction: results analysis, results examination, results reporting, and results dissemination. In what follows, a detailed explanation is provided for each step.

3.3.1 Results analysis: In this step, examiners must analyze all the technical findings extracted from the information analysis phase consistently and clearly. When analyzing the results, examiners can divide the analysis sequential logical parts divided into multiple headings and comment on results as they are described to ease the decision-making process, the results could be supported by figures, tables, and equations to enrich the findings. In addition, the results’ conclusion must be kept very brief that aggregates the findings with robust paragraphs [50].

During the process of validating the results of a mobile forensic scene, several methods can be used to verify the validity of the results such as calculating the hash value with two different forensics tools, or the various steps might be revisited using the same tool to obtain the digital evidence and recalculated the hash value to validate the results. At some point, the results generated using experimental and validation stages must be repeatable. Any variable that might affect the outcome of the validation should be determined after several test runs. However, some cases require more runs to generate valid results, besides; examiners need to utilize the literature to assess the results' validations [51].

3.3.2 Results reporting: The most fruitful result that should be created following the forensic process is the documentation of the findings. Once completed, investigators can use the report to their advantage in a number of ways, including (i) sharing the results with other investigators and decision-makers for use in making decisions, (ii) communicating the facts that may support the investigation of other cases, (iii)
offering a clear justification for gathering more digital evidence, and (iv) using the report to evaluate the specific case. The final report must be written by digital examiners taking into account all conditions and guidelines established by national law. To ensure that the report complies with the law, they must first independently review it. Any divergent opinions will eventually be examined for flaws to bolster the assertions.

In general, there is no set format or structure for reporting the findings, but any final report must include the bare minimum of the following data: jurisdiction, the nature of the case, the court's document format, and the reason ID, calendar of all depositions (timestamps), deponent's name and ID, and other details like time and date the case created, phone physical situation, the phone status on or off, mobile manufacturer information, pictures for each accessory and the phone itself, which tools used in the investigation, any additional data added during an examination. Many forensics reporting tools provide ways to automatically annotate evidence fragments and generate automatic reports according to the examiner's configuration. These tools enable the examiner to perform sub-functions such as tagging, bookmarking, log reports, or even report generation. The report relies on solid documentation, photos, notes, and tool-generated content. The examiner should then check the report and edit his configuration if necessary [52]

3.3.3 Results dissemination

It describes the procedure the examiner uses to communicate to policymakers the findings from the analysis phase. The major goal of this method is to provide action reports for each detected artifact and its analysis. The investigator's defensive strategy and any potential implementation difficulties can also be included in the presentation phase. In an iterative approach, the results from this phase might be used to conduct additional acquisitions. As a result, each process produces more analytical artifacts, which are then provided as feedback to other processes. For lengthy criminal investigations, this feedback iterative procedure may go through numerous iterations.

This step might help other investigators working on similar cases to proceed with their cases accordingly, or to criticize the case, and hence further steps might be required to be performed for the disseminated case [53].

3.4. Case Closing

Case closing is the last stage in the mobile forensics investigation process framework (MFIPF) which undergoes three main steps to ensure the successful termination of the process model. They are case closing, making the legal decision, and case archiving. Understanding how to close and archive the case is also crucial to perform a targeted analysis of the data for future updates. It is important that the digital examiner must have good knowledge of how to store and collect similar cases which might help in case examination.

3.4.1 Legal decision: The constructed case should be finally put in its legal context, here, the final legal decision should be a judicial determination of all parties rights and obligations reached by a court based on facts and law. A decision can mean either the act of delivering a court's order or the text of the court's
opinion on the case and the accompanying court after you complete a case. Since every user owns his/her data and digital device, forensic examiners face ethical and legal issues in accessing and collecting the required information. [54]

3.4.2 Review: The final step in the lifecycle is to review the case to identify successful decisions and actions and determine how the system performance should be improved in terms of time, and accuracy. Critique the case, self-evaluation and peer review are essential parts of professional growth. Investigators must keep the OS and digital forensics tools current in order for everything to be consistent. This necessitates updating the OS frequently, installing all new system updates and patches, and regularly checking the tools' websites for new updates or patches. [55]

3.4.3 Case archiving: When work on a case is completed and immediate access to it is no longer necessary, that case can be archived. This step aims at closing the case after its resolution. Digital forensics case achieving includes the storage of the electronic copies of evidence as well as the case report and the generated artifacts and the documentation of the whole stages of the case. The aim of case archiving is to enable examiners to review the procedures carried out to use them in similar cases. The case archive should enable the examiner to reconstruct the case from scratch based on the available copies of the case evidence which will help if the case was legally re-opened. [56]. Many tools might be used in case archiving that enable ease of use and retrieval of cases, some of these tools will be provided in Section 4.

4. Common Mobile Forensics Tools Used In Mobile Forensic Investigation:

In this section, we will explain a list of 4 commonly used mobile forensics tools, and map them to our proposed model MFIPF.

1. Common tools:

   In the following, we list the common forensics investigation tools and compare and reflect on their operations with the modules of the proposed MFIPF framework.

   • Belkasoft Evidence Center: It is a comprehensive forensic tool for locating, retrieving, and analyzing digital evidence stored on desktops and mobile devices. This tool makes it simple for investigators to collect, examine, analyze, preserve, and share digital evidence from computers and mobile devices. By analyzing hard disks, drive pictures, memory dumps, iOS, Blackberry, Android backups, UFED, JTAG, and chip-off dumps, the toolkit will efficiently extract digital evidence from many sources. It evaluates the data source automatically and lays out the most forensically significant artifacts for the investigator to study the case or add to the report. [24].

   • FINALMobile: It is a powerful software and mobile solution for legal inspectors that provides the legal community with the most cutting-edge data mining and information extraction capabilities. Thanks to its extensive understanding of system files and information patterns, this software can
transform raw data into executable and ready files in just a few clicks. On mobile devices, data is stored in specialized forms and is frequently left behind after a device is entirely cleaned. The FINALMobile forensics software can easily retrieve deleted (hidden) files by scanning for specific patterns. Additionally, as the majority of mobile devices adhere to the same pattern, data can be gathered for upcoming mobile devices. [25].

- 3uTools: It is a program for flashing and jailbreaking Apple's iPhone, iPad, and iPod touch. It offers three ways to flash Apple mobile devices: easy mode, professional mode, or multiple flash. It automatically selects the proper firmware and supports a fast download speed. 3uTools Free Download for Windows PC Latest Version. It has a complete 3uTools offline setup installer [26].

- Magnet ACQUIRE: This tool combines an easy user interface with dependable and speedy extractions to provide you with the information you need quickly and effortlessly. Furthermore, the data quality will be maximized, and activity logging and documentation will help to understand which procedures were employed [27].

2) Mapping tools to MFIPF:

Table 2 provides a comparative analysis between iOS and Android forensic tools for mobile forensics tools with their functionalities based on MFIPF.

5. Conclusion And Future Work

Cybercrimes are rapidly increasing due to the tremendous reliance on information and telecommunication technologies. This rapid increase is being faced by developing the necessary tools and legislation to fight against these crimes. One of the most challenging investigation issues is mobile device forensics. This challenge is because mobile device is becoming more powerful with tremendous processing and communication capabilities as well as containing sensitive data related to the mobile user. For these reasons, a framework for mobile device forensics must be developed to systematically engineer the investigation process and avoid any issues that might cause to reject the investigation. In this paper, we proposed a mobile forensics lifecycle called Mobile Forensics Investigation Process Framework (MFIPF). MFIPF encompasses all forensics stages and steps that must be followed in each stage. Furthermore, we also proposed a list of the most commonly used mobile forensics tools that might be used in each stage or step. In future work, we will apply this model to different investigation scenarios with different mobile platforms and report the finding and if necessary we will update the model accordingly.

In future work, we will test the utility of using our model MFIPF with different mobile digital forensics scenarios and compare our utility results against other models.

Declarations

Acknowledgements:
Authors’ contributions:
All authors read and approved the manuscript.

Funding:
Not applicable

Availability of data and materials
Not applicable

Ethics approval and consent to participate:
Not applicable

Competing interests:
The authors declare that they have no competing interests.

References


**Table 2**

Table 2 is available in Supplementary Files section.

**Figures**
Figure 1

Share of global smartphone shipments by operating system from 2014 to 2023 [1]

Figure 2

The Proposed Forensics Investigation Process Framework (MFIPF)

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.
• Table2.docx