International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1, 125-135 (Jul-24)

http://dx.doi.org/10.12785/ijcds/160110

A Novel Framework for Mobile Forensics Investigation Process

Mohammed Moreb[1], **Saeed Salah**[2] **and Belal Amro** [3]

[1] *Smart University College for Modern Education, Hebron, Palestine, P.O. Box 777*
[2]*Department of Computer Science, Al-Quds University, Jerusalem, Palestine, P.O. Box 20002*
[3]*College of Information Technology, Hebron University, Hebron, Palestine, P.O. Box 40*

Received 7 Nov. 2023, Revised 31 Mar. 2024, Accepted 15 Apr. 2024, Published 1 Jul. 2024

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 being 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 considered. It is imperative to adhere to proper techniques and norms 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 we can use them in our proposed mobile forensic process model.

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

1. Introduction and Overview

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 Figure 1, the annual sales of smartphones have tremendously increased to around (1.56) billion devices worldwide, smartphones running the Android operating system held 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. 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 [1]. 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 [2]. Smartphones are equipped with many capabilities that make forensic steps difficult to handle and require great attention. These capabilities include the availability of different communication technologies such as Short Message Service (SMS), 3G, Wi-Fi, Global Positioning System (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 [3]. 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 [4]. 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

E-mail address: m.moreb@scme.edu.ps, sasalah@staff.alquds.edu, bilala@hebron.edu

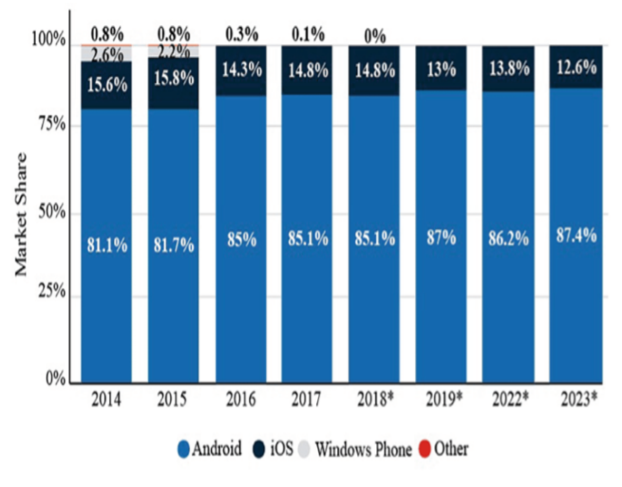

Figure 1. Share of global smartphone shipments by operating system from 2014 to 2023 [5]

smartphones. Mobile forensics investigation frameworks are essential for gathering, examining, and preserving digital evidence from mobile devices in a forensically sound manner, the research [6] discussed the challenges faced by forensic investigators in extracting data from mobile devices and suggested a new model for mobile forensic acquisition, but it does not provide a detailed explanation of a mobile forensics investigation framework. [7] helped in simplifying the examination process and enabled the capture and reuse of specialized forensic knowledge, the result compared the forensics investigation framework for the association of Chief Police Officers (ACPO) and Digital Forensic Research Workshop (DFRWS) frameworks and DFRWS, which has the most complete stages to support the investigation process, DFRWS includes five substations of digital forensics in general [7]. DFRWS framework is considered one of the best frameworks, as it encompasses all the necessary stages and data sources used to construct a crime case, the results show that the Belkasoft Evidence Center forensic tool has the highest accuracy rate of 78.69%, while Magnet AXIOM has an accuracy rate of 26.23% and MOBILedit Forensic Express has an accuracy rate of 9.84%. [8] supports the investigation process by providing a comprehensive set of stages. The use of mobile forensics tools, such as Belkasoft Evidence Center, Magnet AXIOM, and MOBILedit Forensic Express, can aid in the extraction of digital evidence from mobile applications like Signal Messenger. These tools have varying levels of accuracy and capabilities in recovering different types of data. Overall, the development and use of mobile forensics investigation frameworks and tools are crucial for effectively investigating and analyzing digital evidence from mobile devices. This research introduced the frameworks that provide guidelines for capturing, isolating, transporting, storing, and proving digital evidence including all details as a novel framework used by mobile forensics to extract and present results. The process of digital forensics has become an important analysis 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 [9], 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 the following steps:

(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 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 life cycle 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 the mobile forensics domain. Unlike other models, this proposal divides the evidence life cycle 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.

A. Related work

In this section, a brief review of the related literature will be conducted. First, we will 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 [10], where the author discussed the four process phases used for conducting mobile forensics, 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 [11], the authors mentioned that there are five phases in the forensic process (identification, preservation, acquisition, analysis, and reporting) which are similar to what was proposed by Moreb [10]. The study [12] concentrated on android forensics and proposed a framework of seven stages namely: Intake, Identification, Preparation, Isolation, Processing, Verification, and Documentation. A comparative analysis of five common process models was provided by [13], these models are the Smartphone Forensic Investigation Process Model (SFIPM), Windows Mobile Device Forensic Model (WMDFM), National Institute of Standards and Technology (NIST), Harmonized Digital Forensic Investigation (HDFI), and USFIPM. The authors also proposed a secure model by deploying blockchain using Ethereum or a hyperledger platform. In [14], the authors proposed an Efficient and Reliable Forensics Framework (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 detects the interaction between a client terminal and the edge resource. In [15] an analysis of the forensic-by-design framework is proposed which includes investigating the limits of the forensic-by-design and its Insufficiency that could be rewritten as ”deficiencies” or ”shortcomings”. Please let me know if you need any further help with this. 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. In [16], the Goel authors demonstrate 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 [17], the results have shown that using only one tool is not sufficient to complete the investigation process, the four layers are organized 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; data analysis is carried out with various tools like Autopsy and CellDEK, and reporting the case can be generated using MOBILedit Forensic and CellDEK. In [18], the authors reviewed about 100 Mobile forensics models with the main conclusion that suggests improving and validating the investigation process model, developing a meta-modeling language, and developing 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 [19], the proposed model assists

IoTF users in facilitating, managing, and organizing the investigation tasks, it consists of four common investigation processes, preparation process, collection process, analysis process, Patiland report process. The roadmap of DFIP discovery of tools [20] discussed in detail the challenges and opportunities of the digital forensics process concerning different fields such as networks, IoT, cloud computing, database systems, 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.

2) *Mobile forensics tools*

The definition of mobile phone forensics is the science of extracting digital evidence from a mobile device [21]. 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 [22]. 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 [23] can be used such as Cellebrite UFED Physical Analyzer and Oxygen Forensic Suite to get details about the mobile device, Oxygen and UFED forensic tools [24] are used to recover app data. In general, digital forensic tools for data extraction are categorized into three types: manual, logical, and physical [25]. Many mobile forensics tools [26] such as Belkasoft Evidence Center [27], FINALMobile Forensics [28], 3uTools [29], and Magnet [30] are used to extract artifacts from both Android and iOS devices. The SDCA [31] tool is designed to perform the analysis of the differences between two versions of SQL schema, in addition to its ability to analyze the query. According to [32], SecureRS aided 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, and the result shows a method of ensuring forensically sound digital evidence for DFR as well as for digital forensics processes in general. In [10] the authors discussed the tools used to acquire the data from iOS or Android devices for both rooted and jailbroken mobile. The work of [33]found that the data used in the media directory will not change even after jailbreaking the device, which means that the integrity of the data is maintained. 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 were 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 were 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 [24]. In [31] 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 [34] the growth of using smartphones from 2016 until 2021 increased from 2.5 to 3.8 billion smartphones. As reported by [35], the number of users who use social media is about 4.20 billion active users worldwide. According to the comparison as shown in. 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, details about these tools will be provided in Section 4.

B. *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.

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:

a) *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.

b) *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,

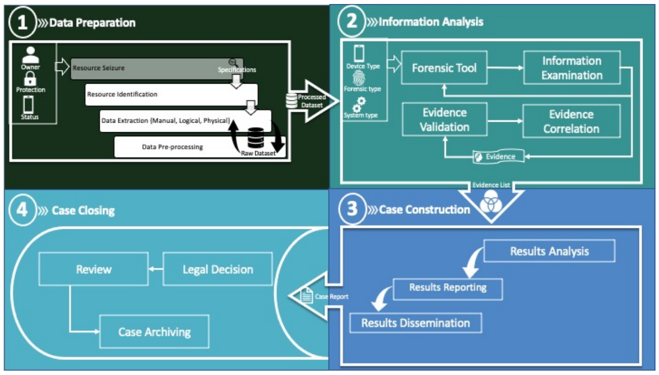

Figure 2. The proposed Mobile Forensics Investigation Process Framework (MFIPF)

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].

c) 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, this method includes:

1) 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 took and the findings as well.

2) 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.

3) 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.

d) 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 [42].

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:

a) Selection of the 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, 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 Section 4. 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 ensure the use and follow up of reproducibility of the event and to prove its validity [44] Therefore, an examiner should be familiar with different tools to conduct his analysis successfully.

b) Information examination

After selecting the appropriate tool(s), the examiner will feed the tool with the preprocessed data and perform a variety of tests and processing tasks against the data. The process 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].

c) 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.

d) 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 ontology's 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) 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.

a) 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 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 and 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 recalculate 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, and; examiners need to utilize the literature to assess the results' validations [51].

b) 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 several ways:

- Sharing the results with other investigators and decision-makers.
- Communicating the facts that may support the investigation of other cases.
- Offering a clear justification for gathering more digital evidence.
- Using the report to evaluate the specific case.

The final report must be written by digital examiners considering 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

TABLE I. Mapping iOS and Android forensic tools with the MFIPF framework.

Phases	Capability	Magnet AXIOM		FINALMobile		BelkaSoft		MOBILedit	
		IOS	Andriod	IOS	Andriod	IOS	Andriod	IOS	Andriod
Phase 1: Data Preparation	Logical Imaging	✔	✔	✔	✔	✔	✔	✔	✔
	Physical Image	✖	✖	✖	✖	✔	✔	✔	✔
	Manual	✔	✔	✔	✔	✔	✔	✔	✔
Phase 2: Information Analysis	SQLite	✔	✔	✔	✔	✔	✔	✔	✔
	Hash-Comparison	✔	✔	✔	✔	✔	✔	✔	✔
	Retrieves Deleted Files	✔	✔	✔	✔	✔	✔	✔	✔
	Information examination	✔	✖	✔	✖	✔	✔	✔	✔
	Evidence validation	✔	✔	✔	✔	✔	✔	✔	✔
Phase 3: Case Construction	Results examination	✖	✖	✖	✔	✔	✔	✔	✔
	Results analysis	✔	✔	✔	✔	✔	✔	✔	✔
	Results reporting	✔	✔	✔	✔	✔	✔	✔	✔
	Results dissemination	✖	✖	✖	✖	✖	✖	✔	✔
Phase 4: Case Closing	Case Archiving	✖	✖	✖	✖	✖	✖	✖	✖
	Legal Decision	✔	✔	✔	✔	✖	✖	✔	✔
	Categorization	✔	✔	✔	✔	✖	✖	✖	✖
	Advance Search	✔	✔	✔	✔	✔	✔	✖	✖

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].

c) 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].

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 performing a targeted analysis of the data for future updates. The digital examiner must have good knowledge of how to store and collect similar cases which might help in case examination.

a) 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].

b) 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 up-to-date 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].

c) 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 cases include the storage of electronic copies of evidence as well as the case report and the generated artifacts and the documentation of the whole stages of the case. Case archiving aims 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 is 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.

C. *Common mobile forensic investigation tools*

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 [27].

- 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 [28].

- 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 can be freely downloaded for Windows PC Latest Version. It has a complete 3uTools offline setup installer [29].

- 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 [30].

For comparative analysis between our approach and existing frameworks, we have utilized the comparison done by [13] who compared five forensic frameworks, they are SFIPM, WMDFM, NIST, HDFI, and USFIPM and NIST. Table 1 shows an updated version of this comparison including our approach as proof of its usability. Furthermore, Table 2 provides a comparative analysis between iOS and Android forensic tools for mobile forensics tools and their reflection on our proposed MFIPF based on a set of capabilities.

2) *Practical Example of Using MFIPF Over a Digital Crime Case*

It is worth mentioning here that MFIPF is a comprehensive model to be used during the mobile investigation process. As an example, we will assume that we are supposed to work on child pornography conducted using the suspect's WhatsApp account. Below practical example which summarizes the steps to be followed based on the proposed MFPIF model.

1) Data Preparation, a search warrant is issued. The device is seizure and a report of the device status is done: iPhone 8, 128G, iOS version 13.1.1 WhatsApp version 14.0.1. Assuming the device was on and we had access to it, we chose logical extraction using Mobile Edit Forensics Express

2) Information Analysis, we use Mobile Edit Forensics Express to analyze our image. A set of images and videos as well as conversations was found to contain child pornography. We may use another tool such as Belkasoft to perform the analysis and verify the results. Correlation among evidence might be done to find all victims and criminals from the contact list

TABLE II. A comparative analysis of five common forensics process models with the proposed one.

Phases	Capability	SFIPM	WMDFM	NIST	HDFI	USFIPM, NIST	MFIPF
Phase 1: Data Preparation	Preparation	✓	✓	✗	✓	✓	✓
	Handling and securing the evidence scene	✓	✓	✗	✗	✗	✗
	Mode selection shielding	✓	✗	✗	✗	✗	✓
	Offset/online storage	✓	✗	✗	✗	✗	✗
Phase 2: Information Analysis	Examination and analysis	✓	✓	✓	✓	✓	✓
	Cell state analysis	✓	✗	✗	✗	✗	✓
	Non-volatile evidence collection	✓	✓	✗	✗	✗	✓
	Volatile evidence collection	✓	✓	✗	✗	✗	✓
	Evidence validation	✓	✓	✓	✓	✓	✓
Phase 3: Case Construction	Presentation	✓	✓	✓	✓	✓	✗
	Communication Scheduling	✗	✓	✗	✗	✗	✗
Phase 4: Case Closing	Review	✓	✓	✓	✗	✓	✗
	Documentation	✗	✗	✓	✗	✓	✗
	Survey and Recognition	✓	✓	✗	✗	✗	✗

3) Case Construction, each evidence is analyzed and related to a victim and a list of contacts who were shared with each evidence is listed as well. This might lead to the identification of some suspects who might be colluding together. Results reporting is to be done, it might be done automatically using a specialized tool such as Mobile Edit Forensics express. Detectors will then conduct their interviews and interrogations with witnesses and suspects and come up with a final report to the corresponding agencies.

4) Case Closing, a legal decision is carried out; a Case Review is done for any new updates about the considered crime case. finally, case Archiving is the last step that saves the complete case for future reference.

2. 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 devices are 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 the rejection of 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 findings and if necessary, we will update the model accordingly, we will also test the utility of using our model MFIPF with different mobile digital forensics scenarios and compare our utility results against other models.

References

[1] S. N. Zakaria and M. F. Zolkipli, “Review on mobile attacks: Operating system, threats and solution,” *Borneo International Journal eISSN 2636-9826*, vol. 4, no. 2, Jun. 2021. [Online]. Available: https://majmuah.com/journal/index.php/bij/article/view/81

[2] A. M. Alashjaee, N. Almolhis, and M. Haney, “Mobile malware forensic review: Issues and challenges,” p. 367–375, 2021.

[3] M. Kumar, “Mobile phone forensics – a systematic approach, tools, techniques and challenges,” *International Journal of Electronic Security and Digital Forensics*, vol. 13, no. 1, p. 53–63, 2021.

[4] O. Ameerbakhsh, F. M. Ghabban, I. M. Alfadli, A. N. Abuali, A. Al-Dhaqm, and M. A. Al-Khasawneh, “Digital forensics domain and metamodeling development approaches,” *2021 2nd International Conference on Smart Computing and Electronic Enterprise: Ubiquitous, Adaptive, and Sustainable Computing Solutions for New Normal, ICSCEE 2021*, p. 67–71, Jun. 2021.

[5] Www.statista.com, “Share of global smartphone shipments by operating system from 2014 to 2023,” 2021. [Online]. Available: https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/

[6] A. J. Karjagi and S. A. Quadri, “Design of a framework for data extraction and analysis from android-embedded smartphones,” *Russian Law Journal*, vol. 11, no. 3, p. 3, Apr. 2023. [Online]. Available: https://typeset.io/papers/design-of-a-framework-for-data-extraction-and-analysis-from-162hm86l

[7] I. Riadi, A. Yudhana, G. Pramuja, and I. Fanani, “Comparative analysis of forensic software on android-based michat using acpo and dfrws framework,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, p.

286–292, Mar. 2023. [Online]. Available: https://typeset.io/papers/comparative-analysis-of-forensic-software-on-android-based-25qqa6xn

[8] J. R. Hildebrandt, E. M. Schomakers, M. Ziefle, and A. Calero Valdez, "Understanding indirect users' privacy concerns in mobile forensics — a mixed method conjoint approach," *Frontiers in Computer Science*, vol. 5, Jul. 2023. [Online]. Available: https://typeset.io/papers/understanding-indirect-users-privacy-concerns-in-mobile-2l1zkdkm

[9] J. Howe, M. Baylor, and R. H. Liu, "Advancing the practice of forensic science in the united states–practitioners' efforts." *Forensic Science Review*, vol. 34, no. 1, p. 7–15, Jan. 2022.

[10] M. Moreb, "Introduction to android forensics," *Practical Forensic Analysis of Artifacts on iOS and Android Devices*, p. 71–108, 2022.

[11] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative analysis of android mobile forensics tools," *2020 IEEE Conference on Computer Applications, ICCA 2020*, p. 1–6, 2020.

[12] A. Al-Sabaawi and E. Foo, "A comparison study of android mobile forensics for retrieving files system," *Ernest Foo International Journal of Computer Science and Security (IJCSS)*, no. 13, p. 2019–148, 2019.

[13] W. Asghari, A. Suresh Kumar, A. S. Singh, and K. Thirunavukkarasu, "A comparison analysis of mobile forensic investigation framework," p. 595–602, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-6707-0_58

[14] A. Razaque, M. Aloqaily, M. Almiani, Y. Jararweh, and G. Srivastava, "Efficient and reliable forensics using intelligent edge computing," *Future Generation Computer Systems*, vol. 118, p. 230–239, May 2021.

[15] A. Akilal and M. T. Kechadi, "An improved forensic-by-design framework for cloud computing with systems engineering standard compliance," *Forensic Science International: Digital Investigation*, vol. 40, Mar. 2022.

[16] G. Horsman and N. Sunde, "Unboxing the digital forensic investigation process," *Science and Justice*, vol. 62, no. 2, p. 171–180, Mar. 2022.

[17] M. Goel and V. Kumar, *Layered Framework for Mobile Forensics Analysis*.

[18] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A review of mobile forensic investigation process models," *IEEE Access*, vol. 8, p. 173359–173375, 2020.

[19] M. A. Saleh, S. Hajar Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common investigation process model for internet of things forensics," *2021 2nd International Conference on Smart Computing and Electronic Enterprise: Ubiquitous, Adaptive, and Sustainable Computing Solutions for New Normal, ICSCEE 2021*, p. 84–89, Jun. 2021.

[20] A. Patil, S. Banerjee, D. Jadhav, and G. Borkar, "Roadmap of digital forensics investigation process with discovery of tools," *Cyber Security and Digital Forensics*, p. 241–269, Jan. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/9781119795667.ch11

[21] K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile phone forensic analysis," *International Journal of Digital Crime and Forensics*, vol. 2, no. 3, p. 15–27, 2010.

[22] D. Hamdi, F. Iqbal, T. Baker, and B. Shah, "Multimedia file signature analysis for smartphone forensics," *Proceedings - 2016 9th International Conference on Developments in eSystems Engineering, DeSE 2016*, p. 130–137, 2017.

[23] M. Al-Hadadi and A. AlShidhani, "Smartphone forensics analysis: A case study," *International Journal of Computer and Electrical Engineering*, vol. 5, no. 6, p. 576–580, 2013.

[24] A. Shortall and M. A. B. Azhar, "Forensic acquisitions of whatsapp data on popular mobile platforms," *Proceedings - 2015 6th International Conference on Emerging Security Technologies, EST 2015*, p. 13–17, 2016.

[25] M. Moreb, "Introduction to ios forensics," *Practical Forensic Analysis of Artifacts on iOS and Android Devices*, p. 37–70, 2022.

[26] H. Azhar, . Cox, R., and A. Chamberlain, "Forensic investigations of popular ephemeral messaging applications on android and ios platforms," *International Journal on Advances Security*, vol. 13, no. 1 & 2, p. 41–53, 2020.

[27] Belkasoft.com, "Belkasoft evidence center," 2021. [Online]. Available: https://belkasoft.com/ru/bec/en/Evidence_Center.asp

[28] Finaldata, "Finalmobile forensics," 2021. [Online]. Available: https://finaldata.com/mobile/

[29] 3uTools, "http://www.3u.com/," 2021. [Online]. Available: http://www.3u.com/

[30] Magnet, "Magnet acquire," 2021. [Online]. Available: https://www.magnetforensics.com/resources/magnet-acquire/

[31] S. S. Shimmi, G. Dorai, U. Karabiyik, and S. Aggarwal, "Analysis of ios sqlite schema evolution for updating forensic data extraction tools," *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, 2020.

[32] A. Singh, R. A. Ikuesan, and H. Venter, "Secure storage model for digital forensic readiness," *IEEE Access*, vol. 10, p. 19469–19480, 2022.

[33] A. Aenurahman Ali, N. Dwi Wahyu Cahyani, and E. Musthofa Jadied, "Digital forensic analysis on idevice: Jailbreak ios 12.1.1 as a case study," *Indonesia Journal of Computing*, vol. 4, no. 2, p. 205–218, 2019.

[34] A. Turner, "How many people have smartphones worldwide (april 2021)," Jan. 2021. [Online]. Available: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[35] S. Kemp, "Digital 2021: Global overview report — datareportal – global digital insights," Jan. 2021. [Online]. Available: https://datareportal.com/reports/digital-2021-global-overview-report

[36] A. Hrenak, "Mobile device forensics: An introduction," *Cyber Forensics*, p. 291–322, Sep. 2021. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003057888-8/mobile-device-forensics-andrew-hrenak

[37] C. Arumugam and S. Shunmuganathan, "Digital forensics: Essential competencies of cyber-forensics practitioners," p.

843–851, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-5243-4_81

[38] A. e. Majdoub, C. Saadi, and H. Chaoui, "Mobile forensics data acquisition," *ITM Web of Conferences*, vol. 46, p. 02006, 2022. [Online]. Available: https://www.itm-conferences.org/articles/itmconf/abs/2022/06/itmconf_iceas2022_02006/itmconf_iceas2022_02006.html

[39] L. A. Herrera, "Challenges of acquiring mobile devices while minimizing the loss of usable forensics data," *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, Jun. 2020.

[40] A. M. da Costa, A. O. de Sa, and R. C. Machado, "Data acquisition and extraction on mobile devices-a review," *2022 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2022 - Proceedings*, p. 294–299, 2022.

[41] M. Kumar, "Mobile forensics: Tools, techniques and approach," *Crime Science and Digital Forensics*, p. 102–116, Sep. 2021.

[42] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective android forensics," *Forensic Science International: Digital Investigation*, vol. 33, p. 200897, Jun. 2020. [Online]. Available: https://koreauniv.pure.elsevier.com/en/publications/study-of-identifying-and-managing-the-potential-evidence-for-effe

[43] M. Lovanshi and P. Bansal, "Comparative study of digital forensic tools," *Data, Engineering and Applications*, p. 195–204, 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-13-6351-1_15

[44] J. E. Oliveira, T. Silva, A. Zorzo, and C. Neu, "Digital forensics experimentation: Analysis and recommendations." *Forensic Science Review*, vol. 34, no. 1, p. 21–42, Jan. 2022.

[45] S. Dogan and E. Akbal, "Analysis of mobile phones in digital forensics," *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, p. 1241–1244, Jul. 2017.

[46] R. F. Erbacher, "Validation for digital forensics," *ITNG2010 - 7th International Conference on Information Technology: New Generations*, p. 756–761, 2010.

[47] H. Arshad, A. b. Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *Journal of Information Processing Systems*, vol. 14, no. 2, p. 346–376, 2018.

[48] H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, "Formal knowledge model for online social network forensics," *Computers and Security*, vol. 89, Feb. 2020. [Online]. Available: https://dl.acm.org/doi/10.1016/j.cose.2019.101675

[49] L. F. Sikos, "Ai in digital forensics: Ontology engineering for cybercrime investigations," *Wiley Interdisciplinary Reviews: Forensic Science*, vol. 3, no. 3, p. e1394, May 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/wfs2.1394

[50] M. R. Al-Mousa, "Analyzing cyber-attack intention for digital forensics using case-based reasoning," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, p. 3243–3248, Jan. 2021. [Online]. Available: http://arxiv.org/abs/2101.01395

[51] H. Page, G. Horsman, A. Sarna, and J. Foster, "A review of quality procedures in the uk forensic sciences: What can the field of digital forensics learn?" *Science & justice: journal of the Forensic Science Society*, vol. 59, no. 1, p. 83–92, Jan. 2019. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/30654972/

[52] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, p. 11065–11089, 2022.

[53] G. Horsman, "Tool testing and reliability issues in the field of digital forensics," *Digital Investigation*, vol. 28, p. 163–175, Mar. 2019.

[54] G. Horsman and N. Sunde, "Part 1: The need for peer review in digital forensics," *Forensic Science International: Digital Investigation*, vol. 35, p. 301062, Dec. 2020.

[55] G. Horsman, "Tool testing and reliability issues in the field of digital forensics," *Digital Investigation*, vol. 28, p. 163–175, Mar. 2019.

[56] Z. Bartliff, Y. Kim, F. Hopfgartner, and G. Baxter, "Leveraging digital forensics and data exploration to understand the creative work of a filmmaker: A case study of stephen dwoskin's digital archive," *Information Processing and Management*, vol. 57, no. 6, Nov. 2020.

Dr. Mohammed Moreb is a Vice President of Academic Affairs at Smart University College for Modern Education. He obtained his Ph.D. iIn Electrical and Computer Engineering Dr. Moreb has Expertise in Cybercrimes and Digital Evidence Analysis, specifically focusing on Information and Network Security, with a strong publication track record, many books published by Dr. Moreb specialize in mobile forensics such as Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices 1st ed. published by Apress.

Dr. Saeed Salah is an Assistant Professor and researcher at the Department of Computer Science at Al-Quds University in Jerusalem. He received his BSc. in Electrical/Computer Engineering from Al-Najah National University in 2003, his MSc. degree in Computer Science from Al-Quds University in 2009, and his Ph.D. from the Department of Signal Theory, Telematics and Communications of the University of Granada in 2015. His research interests are focused on network management, information and network security machine learning, data mining, MANETs, routing protocols, and blockchain. Dr. Salah published many peer-reviewed research papers in recognized international journals and conferences. Moreover, he acts as a reviewer for several journals in his field.

Dr. Belal M. Amro is an assistant professor at the College of IT at Hebron University – Palestine. Dr. Belal received his PhD in Computer Science and Engineering from Sabanci University- Istanbul, Turkey in 2012. In 2004 he received his MSc in complexity and its interdisciplinary applications from IUSS, Pavia, Italy. His BSc degree was awarded from Palestine Polytechnic University in computer systems engineering in 2003. Dr. Amro has served as a technical program committee member for different international conferences and journals and reviewed more than 50 papers in the field of information technology including privacy and security. Currently, Mr. Amro is conducting research in network security, wireless security, and privacy preserving data mining techniques and has published more than 22 papers in international journals and conferences in the field of computer security and privacy.