IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 4, 2020, accepted July 20, 2020, date of publication August 6, 2020, date of current version October 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3014615

A Review of Mobile Forensic Investigation Process Models

ARAFAT AL-DHAQM[1,2], (Member, IEEE), SHUKOR ABD RAZAK[1], (Member, IEEE), RICHARD ADEYEMI IKUESAN[3], (Member, IEEE), VICTOR R. KEBANDE[4], AND KAMRAN SIDDIQUE[5], (Member, IEEE)

[1]Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia (UTM), Skudai 81310, Malaysia
[2]Department of Computer Science, Aden Community College, Aden, Yemen
[3]Science and Technology Division, Department of Cyber and Networking Security, School of Information Technology, Community College of Qatar, Doha, Qatar
[4]Computer Science and Media Technology Department, Malmö Universitet, 1, 211 18 Malmö, Sweden
[5]School of Electrical and Computer Engineering, Information and Communication Technology Department, Xiamen University Malaysia, Kuala Lumpur 43900, Malaysia

Corresponding authors: Arafat Al-Dhaqm (mrarafat@utm.my) and Richard Adeyemi Ikuesan (richard.ikuesan@ccq.edu.qa)

This work was supported in part by the Research Management Center, Universiti Technologi Malaysia, through the Modeling Information Security Policy Field under Grant R.J130000.7113.04E96, and in part by the Open Access Funding provided by the Qatar National Library.

ABSTRACT Mobile Forensics (MF) field uses prescribed scientific approaches with a focus on recovering Potential Digital Evidence (PDE) from mobile devices leveraging forensic techniques. Consequently, increased proliferation, mobile-based services, and the need for new requirements have led to the development of the MF field, which has in the recent past become an area of importance. In this article, the authors take a step to conduct a review on Mobile Forensics Investigation Process Models (MFIPMs) as a step towards uncovering the MF transitions as well as identifying open and future challenges. Based on the study conducted in this article, a review of the literature revealed that there are a few MFIPMs that are designed for solving certain mobile scenarios, with a variety of concepts, investigation processes, activities, and tasks. A total of 100 MFIPMs were reviewed, to present an inclusive and up-to-date background of MFIPMs. Also, this study proposes a Harmonized Mobile Forensic Investigation Process Model (HMFIPM) for the MF field to unify and structure whole redundant investigation processes of the MF field. The paper also goes the extra mile to discuss the state of the art of mobile forensic tools, open and future challenges from a generic standpoint. The results of this study find direct relevance to forensic practitioners and researchers who could leverage the comprehensiveness of the developed processes for investigation.

INDEX TERMS Mobile forensics, investigation process model, digital forensics.

I. INTRODUCTION

Mobile Forensics (MF) as a branch of science is concerned with the recovery of digital evidence from mobile devices using prescribed and appropriate scientific forensic conditions [1]. Furthermore, this branch has become essential, owing to the increased demand for mobile-based services, increased users, and the sporadic changes that have been witnessed in mobile technologies like ubiquity, pervasiveness, and the fast-growing Internet of Things (IoT) technology that demands device connectivity. As a result, there is a growth in the popularity of mobile computing and the transactions tend to be scaling in an upward trajectory.

The associate editor coordinating the review of this manuscript and approving it for publication was Longxiang Gao.

Current research trends are mainly focused on exploring the MF professionals' perception regarding the lack of digital investigation processes that can be used to prepare forensic reports applicable to court cases. Digital forensics is gradually becoming a complex discipline, especially with the proliferation of mobile devices in society. This is further complicated with the trend towards a digital interconnected society and industry 4.0 era. With this digitalisation comes the enormity and complexity of digital crimes, a phenomenon that the community of digital forensic professionals (researchers, practitioners, and standardisation organisations) is required to address. However, the complexity of investigating mobile devices is considerably different from investigating the other types of digital devices; as a result, the present study selected 24 MFIPMs proposed in the literature to offer

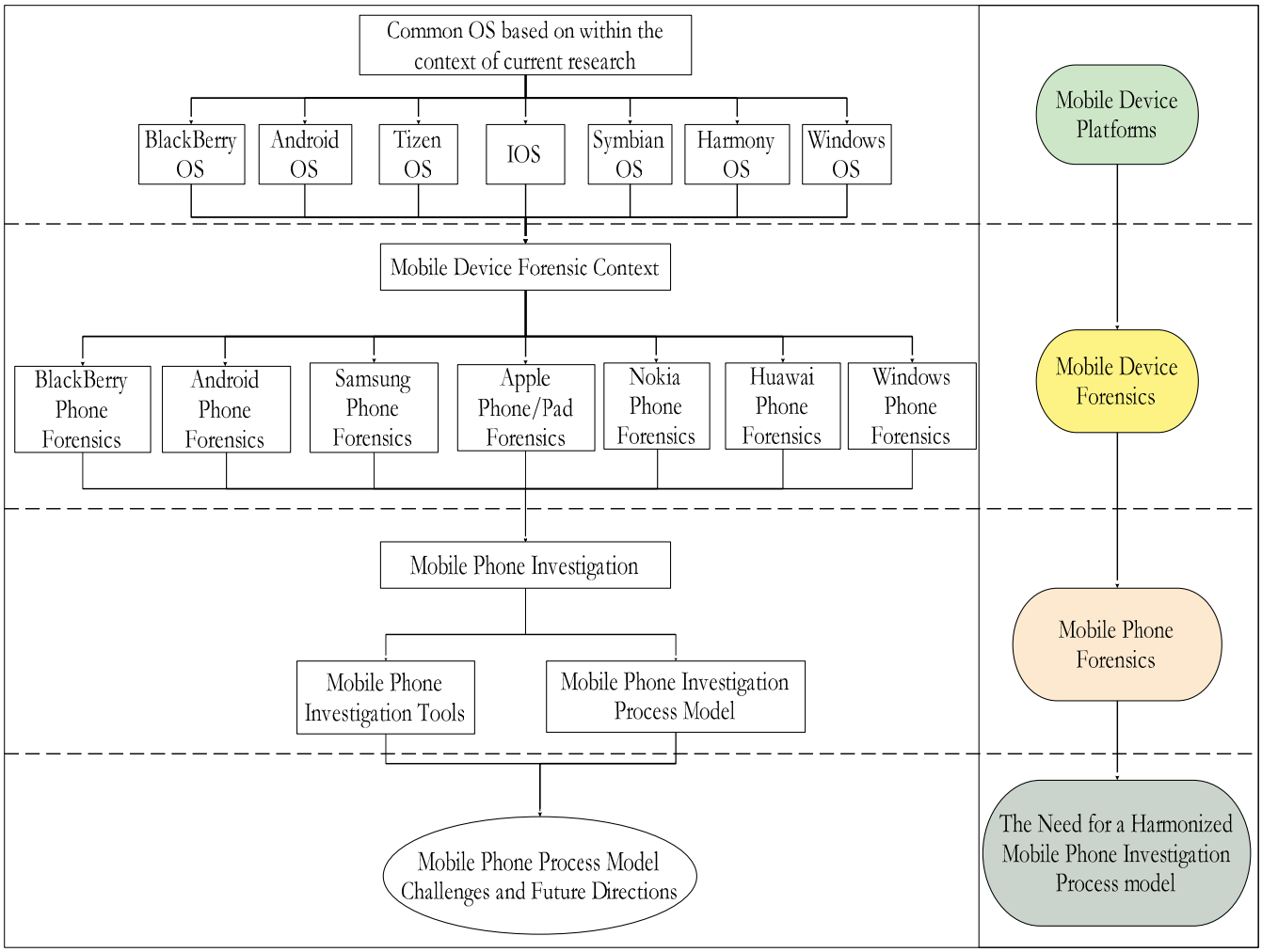

FIGURE 1. Research on mobile forensic investigation processes that covered different mobile device.

an up-to-date and comprehensive background of existing research on the MF process models and the related challenges that may arise for newcomers and also discuss possible methods that can be used to solve these issues effectively. From this study, a review of literature has revealed the need for standardized models unifying the related concepts and terminologies in a way that can allow to decrease confusion and organize existing knowledge that is pertinent to the field of MF. This article has three main objectives:

1) present a broad literature review of the MF domain that will assist field researchers to comprehend MF from different perspectives;
2) discuss the issues and drawbacks of the MF domain; and,
3) suggest some solutions for the discovered limitations.

The rest of the paper is structured as follows: Section 2 provides the study background and related works. Section 3 presents the research methodology. Section 4 presents the results and discussions. Section 5 discusses open problems and future challenges, while Section 6 concludes this article.

II. BACKGROUND AND RELATED WORKS

In literature, several models proposed by different scholars on forensic investigation processes have been observed, which deal with various mobile devices (e.g., BlackBerry, Personal Digital Assistants (PDAs), Cellular mobile, GSM, Mobile phone Linux and Windows platforms, Huawei, Korea CDMA, Symbian, iPhone, etc.). However, these models can be only applied to certain specific mobile devices with varied investigation processes. Figure 1 provides a synopsis of the mobile phone forensic perspective, and the composition of this study. Although, this synopsis could be construed to include the general notion of mobile device forensics which encompasses diverse variance of mobile smart devices. However, this study limits the scope to mobile phone forensics which is hereinafter referred to as mobile forensics (MF). In [2], the authors proposed an adaptive forensic process model for smartphones of the Symbian type based on various versions of Symbian smartphones. Their model comprised of five forensic processes, namely the preparing and identifying the version, acquiring remote evidence, acquiring internal

evidence, analyzing, presenting, and reviewing. Nevertheless, their model was entirely centered on Symbian smartphone's forensic investigation and the set of activities provided in the model is rather incomplete. The authors in [3] introduced an innovative forensic process model that its focus was on the issues related to the Windows mobile device forensic investigations and approaching standardized. This model comprised 12 investigation processes as follows: preparing, securing the scene, survey, and recognition, documentation of the scene, communication shielding, collecting volatile evidence, collecting non-volatile evidence, preserving, examining, analyzing, presenting, and reviewing. It can be said that this model initiated a step toward filling the existing gap between digital investigation and models law enforcement ones. Although very pertinent, the set of activities provided in this model still stands as incomplete. In [4], a model of the Windows mobile device forensic process was designed. The model consisted of 12 investigation processes: preparing, securing the scene, documenting the scene, collecting volatile evidence, collecting non-volatile evidence, off-set, analyzing cell site, preserving, examination, analyzing, presenting, and reviewing. It showed two main advantages: 1) serving as a benchmark and a reliable reference for those who investigate Smartphones regarding criminal cases, and 2) providing a generalized solution and addressing the challenging issue of digital technological scenarios that are highly vulnerable and change quickly. In [5], an investigation process model was introduced for Smartphone DEFSOP in a way to give necessary help to investigators and provide a way for preventing the destruction of digital evidence. In this model, four investigation phases are taken into account: conception phase, the preparation phase, operation phase, and reporting phase. Its operation phase, in turn, comprises three processes: collection, analysis, and forensics. In their model, law and principles are taken into consideration as the first phase, aiming at the provision of help for the other phases and authentic digital evidence. Unlike the NIST model, this one involves training and preparation processes before the forensics process. According to the designers of the above-mentioned model, issues such as Acquisition and Examination/Analysis are completely technical; as a result, they are better to be placed in a single phase, which is the operation phase in this model. Due to taking into account the digital evidence legitimacy, they maintain that their proposed model is of higher reliability compared to NIST. Researchers in [6] proposed a simple and low-cost framework to analyze iPhone forensic. It can extract digital evidence from an iPhone. Three processes are involved in this model: acquiring data, analyzing the data, and reporting the data. In [7], the researchers introduced a new synthesized process model referred to as the Integrated Digital Forensic Process Model (IDFPM), which included a physical investigation component, and Harmonized Digital Forensic Investigation (HDFI) process model. Nevertheless, their model needs to be tested extensively and verified technologically in a way to confirm that the high-level process flow offered by the scholars is a practical, forensically comprehensive, and generally applicable characteristic. The model is composed of five investigation processes: identifying the device, acquisitions, triage, analyzing, and reporting. In another study [8], a methodology was introduced applicable to collecting evidential data from Android devices. Their method contained five investigation processes as follows: identifying the device and preserving the evidence, collecting the evidence, examining and analyzing, and reporting and presentation. To make sure that there is forensic soundness, this methodology makes minimum possible changes to the evidence source device. After this change is realized it gets discrete. This way, it can be simply taken into account by investigating forensic practitioners. After identifying the device in hand and doing the preservation techniques (for instance, making sure the device is radio suppressed, which aims at preventing the remote wiping), the initial technique setting up the device in a way to boot a live collection OS from volatile memory (RAM) of the device.

In [9], the authors introduced an adversary model applicable to social App forensics of Android OS. The model was capable of examining five prevalent Android social apps (i.e., Twitter, Snapchat, POF Dating, Pinterest, and Fling). In their model, App security was offered in addition to an overall understanding of capacities of an adversary model regarding forensic communities and the best practices for informing mobile app design. The model involved four investigation processes as follows: collecting, examining, analyzing, and reporting. In another project [10], the researchers introduced a method with the capacity of collecting and analyzing thumbnails from Android devices. The proposed model contained four 4 investigation processes: identifying, preserving, analyzing, and presenting. They evaluated their methodology with the use of a case study. In that case study, they attempted to identify the thumbnail characteristics aiming for the customisation of existing file carving tools in a way to recover effectively the thumbnails from the forensic image (Through decreasing the number of irrelevant files). In [11], an investigation framework was constructed with a sole aim of applying it to the Samsung Star 3G. It comprised six processes as follow: authorisation process, first response process, device transportation process, live acquisition process, maintenance process, and analysis of evidence. Their proposed framework is practical, and some processes offered are also applicable to other phones and portable devices, particularly the transportation process wherein aluminum foil is suggested to be used. An experiment was carried out by the researcher to verify this statement. The obtained experimental results showed that the material was completely efficient in the protection of signals; for this reason, it was suggested as an alternate solution for the cases where signal insulation bags are not accessible. The authors in [12] introduced a common process model to guide the forensic examiners when conducting a required investigation upon an Android smartphone notwithstanding its manufacturer. Their model contained four processes: pre-incidence readiness, collecting the evidence, examining and analyzing, and

information diffusion. It should be noted that their model lacked real application to an actual scenario. The UML use-case diagram was utilized for demonstrating the proposed model efficiency. In another research [13] focused on Firefox OS, a methodology of mobile forensic procedures was proposed for forensic investigations. It was composed of three processes of preparing, preserving, and acquiring. They made use of a basic approach and configured the model specifically for Firefox OS. Among the wide variety of files and analyses, it was constructed to hold only some certain targeted data checklist in a way to determine pertinent data align with specific analyses. It is possible to update the above-noted checklist occasionally. Authors in [14] proposed a method of investigating in a way to effectively acquire data and analyze Android smartphones. Their method considered the techniques currently used to examine the computers and cellphones in a forensic way. They also considered issues such as an adaptation of the method to certain characteristics of Android, the structure provided for data storage purposes, applications of high popularity, and also the question of under what conditions the device is sent to forensic examiners. Without mentioning the tools or techniques explicitly, the method was broadly defined. It involved only two investigation processes: acquisition and examination. In another project conducted in [15], the researchers introduced a commonly-used investigation process of digital evidence forensic on smartphones. It comprised four investigation phases as follows: principle concept, preparation, operation, and reporting. In [16], a new methodology was suggested for the examination of mobile electronic devices. It involved the techniques, tools, and procedures that are necessary for collecting data from various commonly-utilized devices. Four investigation processes were included in this method: seizure, acquiring, analyzing, and reporting. A common process for gathering data of Android devices was introduced by the authors in [17]. The process they suggested was useful in recovering the partition and accompanying recovery mode of an Android device for data gathering purposes. In [18], a novel approach was introduced to acquire live data in addition to data stored within the external or internal memory of Android mobile devices. It comprised only one process, i.e., live data collection. The authors in [19] proposed a proactive smartphone investigation scheme centering upon ad hoc acquisition of evidence from a smartphone. Their scheme includes six processes as follows: engagement in the investigation, selecting the evidence type, collecting the evidence, transmitting the evidence, storing the evidence, and completing the investigation. This scheme was applicable to the examination of the technological aspects of proactive smartphone digital forensics. In another study [20], the authors introduced a well-organized generalized forensics framework in order to extract and document the evidence from Android devices. With the use of hashing algorithms, the attempt was to achieve a comprehensive and reliable snapshot of Android devices with high integrity verification. It contained two processes: extracting the evidence and documenting it. In [21], a forensic adversary model was introduced to be applied to forensic contexts. In this model, two processes were involved: collecting the evidence and analyzing the evidence. The study carried out by [22] proposed a layered architecture applicable to mobile forensic analyses in such a way to make the investigation process as easy as possible. It comprised seven layers as follows: preparing and strategizing, detecting the crime scene, seizure and preservation, extracting and acquiring the data, examining and analyzing, and reporting and documenting. To acquire data, it makes use of different forensic tools such as Bulk extractor and MOBILedit. In another research [23], a new framework was introduced by authors in order to validate the digital forensics software data particularly to apply to smartphones. The framework is mainly centered upon iOS apps; the process of gathering data is performed on iOS devices, then the collected data is transferred onto a laptop to do the validation processes.

III. METHODOLOGY

A systematic review research design was conceptualized for this study. However, given the diversity of the field of mobile forensics, a mixture of database-driven and forward snowballing approach was considered. The methodology for this study was adapted from that of [24], [152], as further depicted in Figure 2. The method used here consisted of three phases:

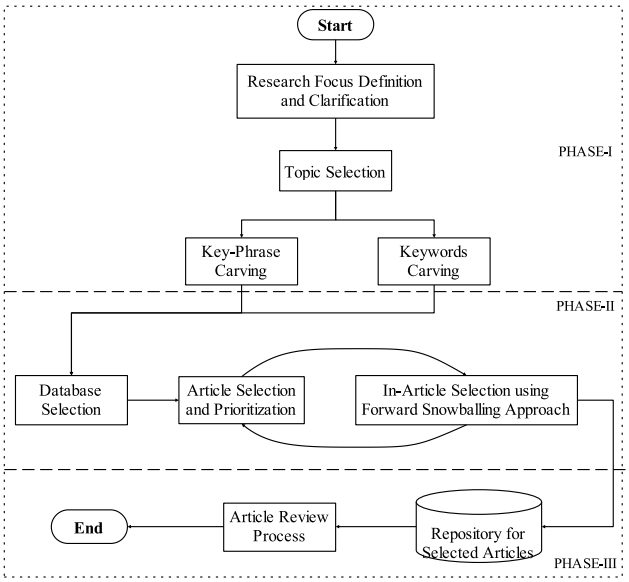

FIGURE 2. Literature review methodology.

i) The selection of a topic and development of keywords/phrases;
ii) The selection of online databases using specific institutional database and further literature extraction based on in-article citation, and compilation of related literature;
iii) Reviewing the current literature on the selected topic.

In this article, the currently-used MFIPMs are studied in detail in such a way to find out the common challenges and problems that arise in this field.

PHASE I: SELECTION OF A TOPIC

The topic for the present study was selected using questions in relation to the main subject of the research and considering the background of the topic of focus. Three fundamental questions outline the whole research, which are:

1. What MFIPMs exist currently in literature?
2. Does literature consist of any common process model/framework for the MF field?
3. What are the limitations of the currently-used MFIPMs?

Based on these questions, appropriate keywords and key-phrases were developed. One core component of this process is the use of conjunction to join multiple keywords. Sample of the keywords and the conjunctions used to combine multiple keywords is further presented in Table 1.

TABLE 1. Sample of key-Phrase and conjunction.

Sample keywords	List of Joining conjunction
Mobile forensic investigation model	& (and)
Mobile forensic tools	""
Mobile investigation frameworks	+ (plus)
Digital forensics on mobile phone	Or
Portable Device forensics	&&
Portable Device investigation model	

This was carried out on the selected databases. The process of selecting the databases and the selected databases are further discussed in the next section.

PHASE II: SELECTION OF ONLINE DATABASES AND FINDING RELATED LITERATURE

To perform this phase, a definite scope was defined for reviewing the literature. The term ''Mobile Forensics'' was searched in such a way to collect the models proposed in the MF field. In this phase, the knowledge sources were gathered to be used. The Web of Science, IEEE Explore, Scopus, Springer Link, ACM, and Google Scholar were the popular digital libraries that were searched through in order to find the papers related to the MF field. To this end, we made use of the term 'Mobile Forensics' as the searching keywords. In regard to the time duration, the search was confined to the period of time between 2000 and 2020. For the purpose of the present paper, documents like the research articles, conference papers, dissertations, books, and book chapters were taken into account, whereas the other types of documents were left out. In addition, the duplicate, the articles related to public health and medicine, and screening the topic and abstracts were removed, and also the articles discussing Deoxyribonucleic Acid (DNA) were removed. Table 2 summarizes the details of the search protocols employed in this study. Finally, 100 out of 2229 articles were identified to be completely focused upon the topic of MF processes and technology perspectives in this field.

PHASE III: REVIEWING THE CURRENT LITERATURE

A review of the literature revealed that scholars and developers generally approach to the MF field through various perspectives like the Investigation process, Operating Systems, Mobile devices, and mobile forensic tools. The present paper is focused on the investigation process. Using the forward snowballing approach, the study observed that most in-paper referenced articles have been identified in the respective databases which are considered. This was however not a surprise as the database selection process considered both specific institution (subscribed) and context-free database (Google Scholar in this case) as shown in Table 2. In the following, the MF field is discussed in detail.

TABLE 2. Systematic review protocols.

Database Search Engines	"Mobile Forensics"
Web of Science	123
Scopus	247
IEEE Explore	68
Springer Links	114
Google Scholar	1,670
ACM	7
Total	2229

A. MOBILE FORENSICS INVESTIGATION PROCESS MODELS

Totally, 100 documents were found in the process of literature review, which were centered completely upon the MF topic from various perspectives as noted before (see Table 3).

For instance, the authors in the [25] carried out examined the wireless devices for BlackBerry from a forensic perspective. On the other hand, in [26], the researchers introduced an innovative instrument called PDD for forensic analysis and memory imaging purposes of devices that run the Palm OSs for PDAs. In [27]–[29], several procedures, tools, and guidelines were proposed to be applied to GSM, PDAs, and Cellular mobile phones. In another study [30], a novel method was developed to extract the evidence from SIM card and internal memory of Mobile phones, GPSs, as well as PDAs. The authors in [31] designed a SIMbrush tool for the extraction of the full files system for Mobile phones, Linux, and Windows platforms. On the other hand, in [32], and the on-phone forensic tool was presented that was shown capable of extracting evidence from active files on mobile. The researchers in [33] introduced a tool for the extraction of evidence from the internal flash memory of CDMA mobile phones manufactured in Korea. In [34], a detailed discussion is presented regarding the flasher devices of mobile phones. The authors in [35] attempted to develop a database-driven

TABLE 3. Mobile forensic models.

Year	Mobile Forensic Models	Mobile device
2002	A forensic examination of a RIM (BlackBerry) wireless device [25]	BlackBerry
2002	memory imaging and forensic analysis of palm OS devices[26]	PDAs
2003	Forensics and the GSM mobile telephone system. International Journal of Digital Evidence [27]	GSM
2004	Guidelines on PDA forensics [28]	PDA.
2004	A forensic examination of mobile phones [29]	Cellular mobile phone
2005	Forensic analysis of mobile phone internal memory, in Advances in Digital Forensics [30]	Mobile phones, PDAs, and GPSs).
2006	Forensics and SIM cards: an Overview [31]	Mobile phone Linux and Windows platforms.
2007	Acquisition of a Symbian smartphone's content with an on-phone forensic tool[32]	Symbian.
2007	Data acquisition from cell phone using a logical approach [33]	Korea CDMA mobile phones.
2007	Introduction to mobile phone flasher devices and considerations for their use in mobile phone forensics [34]	Mobile phone.
2007	Mobile phone forensics tool testing: A database-driven approach [35]	Mobile phone.
2007	Guidelines on cell phone forensics. NIST Special Publication [36]	Mobile phone.
2007	Forensic data recovery from flash memory [37]	Mobile phones.
2008	An integrated approach to recovering deleted files from NAND flash data [38]	Mobile phones.
2008	Overcoming impediments to cell phone forensics [39]	Mobile phones.
2008	iPhone forensics: recovering evidence, personal data, and corporate assets[40]	iPhone.
2008	An overall assessment of mobile internal acquisition tool[41]	Symbian.
2009	Hashing Techniques for Mobile Device Forensics.[42]	Smartphones.
2009	Issues in Symbian S60 platform forensics [43]	Symbian.
2009	A comparison between windows mobile and Symbian S60 embedded forensics [44]	Symbian and Windows Mobile devices.
2009	A process model for forensic analysis of Symbian smartphones, in Advances in Software Engineering [45]	Symbian.
2009	iPhone forensics [46]	iPhone.
2009	Data reverse engineering on a smartphone [47]	Symbian.
2009	Research of Mobile Forensic Software System Based on Windows Mobile [48]	Windows Mobile.
2009	Forensic information acquisition in mobile networks. in Communications, Computers and Signal Processing [49]	Windows mobile.
2009	BlackBerry IPD parsing for open source forensics [50]	Blackberry.
2009	Fast smartphones forensic analysis results through mobile internal acquisition tool and forensic farm [51]	Symbian and Windows Mobile.
2010	Windows Mobile advanced forensics [52]	Windows Mobile.
2010	Android Forensics: Simplifying Cell Phone Examinations [53]	Android phones.
2010	Introduction to windows mobile forensics. digital investigation [54]	Windows Mobile.
2010	iPhone 3GS forensics: a logical analysis using apple iTunes backup utility [55]	iPhone.
2010	Campbell, iOS forensic analysis for iPhone, iPad, and iPod touch [56]	iPhone.
2010	Full user data acquisition from Symbian smartphones [57]	Symbian.
2010	Windows mobile advanced forensics: An alternative to existing tools [58]	Windows Mobile.
2010	Chang, Live memory forensics of mobile phones [59]	Symbian.
2010	Android anti-forensics through a local paradigm [60]	Android.
2010	iForensics: forensic analysis of instant messaging on smartphones, in Digital forensics and cyber crime [61]	Apple iPhone.
2011	Digital Trails Discovering of a GPS Embedded Smart Phone-Take Nokia N78 [62]	Symbian.
2011	iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices [63]	iPhone.
2011	A simple cost-effective framework for iPhone forensic analysis, in Digital Forensics and Cyber Crime [64]	iPhone.
2011	Android forensics: investigation, analysis, and mobile security for Google Android [65]	Android.
2011	Forensic analysis of the Android file system YAFFS2 [66]	Android phones.
2011	A comparison of forensic evidence recovery techniques for a windows mobile smartphone [67]	Windows Mobile.
2011	Acquisition and analysis of digital evidence in android smartphones [14]	Android.
2011	Toward a general collection methodology for Android devices [17]	Android.
2011	Sensitive privacy data acquisition in the iPhone for digital forensic analysis [68]	iPhone.
2011	Forensic Analysis of Geodata in Android Smartphones [69]	Android.
2011	Blackberry forensics: An agent-based approach for database acquisition, in Advances in Computing and Communications [70]	Blackberry
2011	Design and implementation of a mobile forensic tool for android smartphone through cloud computing, in Convergence and Hybrid Information Technology [71]	Android
2011	A novel anti-forensics technique for the android OS [72]	Android
2011	Third-party application forensics on apple mobile devices [73]	iPhone. Appel
2012	A study on the forensic data extraction method for SMS, photo and mobile image of google android and windows mobile smartphone, in Convergence and Hybrid Information Technology [74]	Android & windows mobile
2012	Symbian smartphone forensics: Linear bitwise data acquisition and fragmentation analysis, in Computer Applications for Security, Control and System Engineering [75]	Symbian
2012	Symbian smartphone forensics and security: Recovery of privacy-protected deleted data, in Information and Communications Security [76]	Symbian
2012	Volatile memory acquisition using backup for forensic investigation [77]	General
2012	Analysis of Smartphone-Based Location Information, in Computer Science and Convergence [78]	Android & iPhone
2012	Forensic analysis of social networking applications on mobile devices [79]	BlackBerrys, iPhones, and Android
2012	Forensic analysis techniques for fragmented flash memory pages in smartphones [80]	Android and iPhone phones.
2012	Acquisition and analysis of volatile memory from	Android

TABLE 3. *(Continued.)* **Mobile forensic models.**

	android devices [81]	
2012	Forensic analysis of wireless networking evidence of Android smartphones [82]	Android
2012	Versatile iPad forensic acquisition using the Apple Camera Connection Kit [83]	iPhone
2012	A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking [84]	iPhone
2012	An agent-based tool for windows mobile forensics, in Digital Forensics and Cyber Crime [85]	Windows Mobile
2012	A Case Study of the "HTC Incredible" Phone, in Proceedings of Student-Faculty Research Day [86]	Android
2012	Results of Field Testing Mobile Phone Shielding Devices, in Digital Forensics and Cyber Crime [87]	Mobile phones
2013	Forensic Analysis of Instant Messenger Applications on Android Devices [88]	Android
2013	Forensic Analysis of WhatsApp on Android Smartphones [89]	Android
2013	A study of user data integrity during the acquisition of Android devices [90]	Android
2013	iOS Forensics: How can we recover deleted image files with a timestamp in a forensically sound manner? in Availability, Reliability, and Security (ARES) [91]	iPhone
2013	Blackberry playbook backup forensic analysis, in Digital Forensics and Cyber Crime [92]	Blackberry
2013	Forensic research on data recovery of android smartphone [93]	Android
2013	Windows Mobile LiveSD Forensics [94]	Windows Mobile.
2013	Analysis of the forensic traces left by AirPrint in Apple iOS devices [95]	iPhone and iPad devices
2013	Automated identification of installed malicious Android applications [96]	Android
2013	Applied Cryptography and Network Security [97]	Android
2013	. Design and Implementation of Digital Forensic Software for iPhone [98]	iPhone
2013	Smartphone sensor data as digital evidence [99]	Android
2013	Forensic Data Recovery from Android OS Devices: An Open Source Toolkit [100]	Android
2013	Droid Analytics: A Signature-Based Analytic System to Collect, Extract, Analyze and Associate Android Malware [101]	Android
2013	General Collection Methodology for Android Devices [102]	Android
2013	Forensic analysis of social networking application on iOS devices [103]	iPhone and iPad devices
2013	Development and Evaluation of Guideline Total Support System for Evidence Preservation by Using an Android Phone [104]	Android
2013	Physical Forensic Acquisition and Pattern Unlock on Android Smart Phones [105]	Android
2013	Fast data acquisition with a mobile device in digital crime [106]	iPhone and Android
2014	A Comparison of Forensic Acquisition Techniques for Android Devices: A Case Study Investigation of Orweb Browsing Sessions [107]	Android
2014	Android forensics: Interpretation of timestamps [108]	Android
2014	A visual approach to interpreting NAND flash memory [109]	Android
2014	Forensic analysis of WhatsApp Messenger on Android smartphones [110]	Android
2014	Historical Data Recovery from Android Devices, in Future Information Technology [111]	Android
2015	A forensically sound adversary model for mobile devices [21]	Android
2015	The Forensic Process Analysis of Mobile Device [16]	Android
2017	Extraction of common concepts for the mobile forensics domain [112]	Android
2017	A metamodel for mobile forensics investigation domain [113]	Android
2018	A framework for validating aimed at mobile digital forensics evidence [23]	Android
2019	Layered Framework for Mobile Forensics Analysis [22]	Android
2019	Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases [114]	
2019	Forensic Analysis of Water Damaged Mobile Devices [115]	Android
2019	Smartphone Security and Forensic Analysis [116]	
2020	Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications [124]	Android
2020	Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications [159]	Android

approach for the evaluation of the tools proposed for mobile phone acquisition. In [36], some guidelines are offered for cell phones, which discuss all of the acquisition types that are present in literature. In another research [37], an innovative recovery approach is introduced for the extraction of videos and/or images from the mobile phones flash memories. In [38], a recovery method was proposed to extract evidence (of both file and video types) deleted already from the NAND flash memories. The researchers in [39] proposed two new approaches: (1) Phone manager protocol filtering, and (2) Identity module programming for SIM card. In [40], a physical acquisition method is introduced that applies to the iPhone. In another project [41], and inclusive discussion is presented regarding assessing the mobile internal acquisition tools and logical acquisition. In [42], hashing techniques are suggested to be used for MF purposes. The authors in [43] addressed the Symbian forensics and all acquisition approaches. In another study [44], Windows Mobile and Symbian forensic processes were compared to each other. In [45], a process model is introduced for forensic analyses of Symbian smartphones in five phases. The researchers in [46] presented a detailed discussion concerning all of the acquisition techniques that have been presented in literature in case of iPhone. Reference [47], an innovative methodology is presented, which makes use of data reverse-engineering in the case of Symbian devices. In another study [48], a new model was suggested by the researchers to extract phone contacts, call recordings, SMS, documents, scheduling, as well as all of the acquisition methods available in literature in the case of Windows Mobile. The authors in [49] attempted to develop a model for the extraction of evidence from wireless connections in the case of Windows mobile phones. On the other hand, in [50], logical acquisition for Blackberry devices was argued. In [51], a novel technique, as well as a tool, were

introduced to acquire data from a memory card (SD, mini SD, MMC) in the case of the Windows Mobile and Symbian devices. The researchers in [52] examined the physical acquisition mechanisms upon smartphones with the use of pseudo-physical acquisition proposed for Windows Mobile devices. In [53], the authors suggested the first research into the Android from a forensics point of view and provided a comprehensive discussion about all methods available in the literature for acquiring data from the Android devices. In [54], the authors discuss physical methods for acquiring data, which are implemented only in devices without password protection with the use of pseudo-physical acquisition for the Windows mobile phones. The study conducted by authors in [62] has attempted to present the methods generally applied to the extraction of evidence from GPS of mobile phones. In another research [66], the authors carried out a number of experiments through the use of physical and logical techniques of acquisition on the Sony Xperia 10i. The researchers in [14] attempted to design a framework for forensic acquisition and analysis, which can be applicable effectively to Android devices. In [74], four methods of extracting data were presented and discussed, which were SMS, mobile image, photo, and logical acquisition. The authors in [80] presented a discussion on all acquisition methods with a certain focus upon recovering the data that have been already removed from smartphones. Besides, they introduced innovative methods applicable to analyzing the fragmented flash memory. In [81], a novel method is introduced together with a toolset for physically acquiring and extracting evidence from volatile Android memory. In another study [89], the researchers attempted to analyze the popular application of WhatsApp upon Android Smartphones from a forensics perspective. On the other hand, in [92], the logical acquisition method was introduced in the case of a Blackberry device. In [97], several techniques were proposed for the extraction of evidence from Android smartphones that have been encrypted. The researchers' aim in [104] was the development of support systems to efficiently preserve evidence from an Android phone. In [107], the forensic acquisition methods proposed in literature for Android devices were compared to each other. In [109], the focus of the researchers was on developing techniques for the interpretation of the contents of raw NAND flash memory images. In another research [110], a discussion is provided about how to analyze the WhatsApp chat performed with Android smartphones in such a way to effectively identify the messages that have been already removed from the phone. The authors in [21], on the other hand, introduced an adversary model that can be used in facilitating the forensic investigations on mobile devices with systems such as iOS, Android, and Windows. They attempted to design their model in a way to be simply adapted to the latest technologies offered for mobile devices. In [117], a model was proposed integrating the criminal profiling and suspicious pattern detection method to be applied to two criminal activities with a moderate-to-heavy involvement of mobile devices, cyberbullying, and low-level drug dealing. In another project [23], the researchers attempted to develop a new approach to the validation of the data stored in a device and also the tools employed in MF field of study. Reference [124] introduced an improved mobile cloud forensic investigation process model for social network applications for enhancing the cloud action traceability. The improved forensic investigation process includes the time synchronization process and inter and intra-application analysis in addition to the traditional forensic investigation processes. Time synchronization allowed forensic analysis of the mobile device enhances the evidence traceability in the cloud and therefore, achieves the investigation performance rapidly. However, a common forensic investigation model for the mobile cloud traceability that supports all kinds of mobile cloud applications is still missing. Reference [159] proposed a mobile cloud forensic readiness process model to recognize the elements and organize the data that efficiently encourages forensic examinations. The proposed process model includes requirements for the mobile cloud forensics from various views with the purpose of creating the forensic-ready approach.

As a result, the mainstream of research carried out between 2000 and 2020 into smartphone forensics have been particularly centered on iPhone and Android. Moreover, these studies have been focused upon acquiring and analyzing required evidence from these devices and also the practical implementations. On the other hand, the above-mentioned studies have overlooked the fundamental concept of MF investigations. Additionally, it should be noted that in these studies, other MF investigation processes like preserving, examining, and reporting have not received adequate attention. Furthermore, issues such as management of knowledge and activities of each phase in the MF field were overlooked.

Apart from various MF knowledge, there are also quite a several forensic techniques have previously addressed on how mobile forensics tools can be used to prove facts in the wake of potential security incidents. We explore the state of the art of mobile forensic tools, which has helped the authors to coin a discussion.

Research by [123] has conducted an experiment using the available Belkasoft Evidence tool by utilizing NIST forensic techniques. The focus of this research is to extract WhatsApp artifacts using a mobile forensic tool. By adopting the four Investigation processes from NIST, the technique was evaluated and the extraction of the artifacts has been able to meet the validation test with ease. Next, an enhances forensic process that is more focused on improving mobile cloud traceability for cloud-based mobile applications can maintain a timeline of chronological evidence, which allows potential digital evidence correlation for mobile cloud [124]. Another pertinent research by [125], [126], has focused on the following aspects: Proposing a mobile forensic readiness model that utilizes agent solutions to conduct forensic readiness through a collection of evidence from mobile devices, which counters cyber-bullying. This is applied in conditions when the mobile device is used as an instrument of crime. Based on

this model, the extraction of potential digital evidence from the mobile has been used as a way of achieving incidental preparation. Notably, a study on mobile forensic tools by the Law Enforcement Agencies (LEAs) during forensic investigations has revealed that many mobile applications are not supported by current forensic tools, which tend to extract artifacts manually in the long run [127]. Next, an analysis of SQLite schema evaluation that is aimed to assist digital forensic tool developers has been used to map different ways of keeping mobile tools compatible with the iOS version. In this study, an SQLite Database Comparison Analyzer tool has been developed that has the capability of locating the existing differences on two distinct SQLite schemas in an automated way. Eventually, this tool has been able to be executed forensically based on the knowledge that is gathered by the SQLDCA [128]. This has been followed by a comparative analysis study on Andriod mobile forensic tools on opensource and commercial tools using two popular tools (Autopsy and Belkasoft Evidence) that have been utilized in the acquisition of data given there are currently exist quite a several huge numbers of models from a different manufacturer. Most of these tools have different approaches when it comes to conducting digital forensic investigations. Based on that, it is worth to point that, artifacts, digital data, and the structure of different devices are different and they may pose a challenge during investigations [129], [130]. Consequently, the changes that have occurred on Android and iOS over the last decade has meant that more research is needed to stay up to date with the changing forensic techniques of these Operating Systems (OS), given that they currently are widely used [131]. Additionally, most of the current tools use the available widely used logical techniques, however, this does not also give direct access to mobile phone file systems during forensic investigations [132]. More so, current tools and investigation processes emphasize analysing the plurality that comes with devices and investigation processes. This allows tools to conduct an extensive scan of the digital artifacts in memory, processes of devices, changes, and reconstructing current data-which is an important aspect of the mobile forensic technique [133], [134]. Additionally, a software tool named AnForA that can automate a different set of activities that need to undergo forensic activities has different properties (evidence precision, effectiveness, and repeatability) and this tool shows that it is possible to monitor the changes in file systems [135]. A synopsis of some common MF tools is presented in table 4.

Having explored the state of the art on mobile forensic tools (as distilled in Table 4), in the next section, the authors give a discussion that emanates from the aforementioned works.

TABLE 4. Summary of mobile forensic tools.

Tools	Source	Features
MOBILedit	Mixed	Can extract deleted data and perform a deep analysis of the features of a phone.
Oxygen Forensics	Commercial	Practitioner toolset capable of extracting forensic data, and generating reports.
SIMBrush	Open	Imager, Wrapper, and reporting
MSAB (XRY,AMN,XEC)	Mixed	Can extract forensic data from a diverse mobile device. Automation.
Belkasoft	Open	Can extract, search and analyse forensic artifact from mobile phones
AnForA	Open	Can automate a different set of activities that need to undergo investigation
Cellebrite UFED (Universal Forensic Extraction Device)	Open	It can perform logical, physical, file system and password acquisition on a wide range on mobile devices such as Android, and smartphones
Magnet AXIOM	Open	Magnet AXIOM is a complete digital investigation platform that allows examiners to seamlessly acquire and analyze forensic data, as well as share their findings
Autopsy	Open	Autopsy is an open source digital forensic tool that can be used for investigating cyber-crime. The purpose of the tool is to identify all possible pieces of information which could be useful for further forensic examination.
FTK AccessData	Commercial	Make a forensic copy of the digital evidence, then created a searchable index for the investigation, that allowed a search and a record of the frequency of words and other groups of letters and numbers.
R-Studio	Open	STUDIO is the most comprehensive data recovery solution for recovery files from NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS+ and APFS (Macintosh), Little and Big Endian variants of UFS1/UFS2.
TSK (The Sleuth Kit)		
BitPim	Open	It designed for managing content on CDMA devices.
Manifest Explorer		It can be used on any device using the Google Android operating system (OS).

IV. RESULTS AND DISCUSSION

Through this review, MF field has suffered from several issues as shown previously in Figure 3:

1. Lack of standardized investigation model: Several specific investigation process models have been proposed in the literature. Each MF has a specific investigation process model, which are largely at variance with other models.
2. Redundancy of processes and concepts: Several investigation processes and concepts have been proposed which make MF field ambiguous amongst forensic practitioners. The choice of what specific process or concept to select for a given investigation is laced with diverging perspective, which could result to inappropriate process selection. An investigator might simply resort to select at random, or even choose a process by order of occurence.
3. Different mobile devices infrastructures: One of the main drawbacks facing MF developers and researchers is the varying structure of mobile device infrastructure.

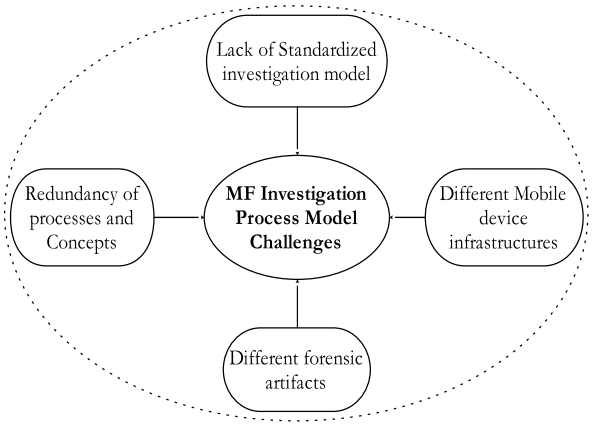

FIGURE 3. Mobile forensic issues.

Each mobile device has a different physical and logical infrastructure.

4. Different forensic artifacts: Due to the variety of the mobile device infrastructures, different forensic artifacts which have similar meanings and activities have been offered with different names, which produced confusion among MF forensic practitioners. Consequently, a lack of standardized format for forensic artifacts extracted for MF.

Therefore, this study proposes a Harmonized Mobile Forensic Investigation Process Model (HMFIPM) for MF field. To develop the HMFIPM, the Design Science Research (DSR) has been adapted from [149]–[152]. The DSR is useful in solving a problem that has been unsolved before or solving a known problem in a more effective or efficient manner. According to [153], DSR is a methodology which is suitable for developing a model that contributes to the growth of knowledge in the domain. Thus, four steps have been adapted to develop the HMFIPM as shown in Fig 4:

1. *Identify and Select MF models*: Several MF models have been discussed in the Section III, Phase III. Models selection for development the HMFIPM is based on the coverage perspectives that were identified in previous research [153], [154]. A coverage of investigation processes are required to fulfill the aim of developing a HMFIPM. Using coverage metric quickly provides an indication of sourced models' applicability. The models which have covered investigation processes of the MF field were selected as a development process models, whereas the models which have not covered investigation process were neglected. Thus, 24 MF models identified and selected for development process, and 76 models were neglected. Table 5 displays twenty-four (24) MFIPM that were identified and selected from existing MF models.
2. *Recognize and Extract Investigation Processes*: in this step MF processes from the 24 MFIPM were extracted based on criteria adapted from [153], [155]:

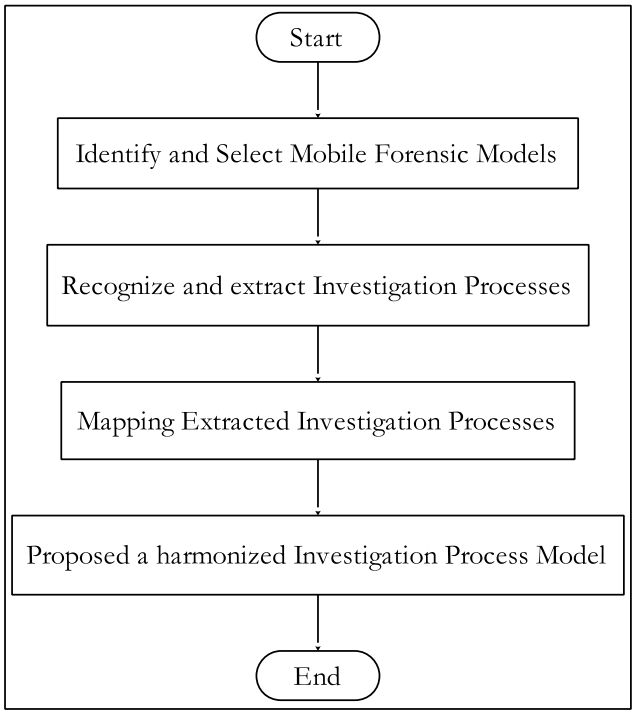

FIGURE 4. Development process adapted from [148]–[151].

i. Titles, abstracts, related works, and conclusions were excluded: the investigation process was either extracted from the diagram or from the main textual model.
ii. The investigation process must have a definition, activity, or task; to recognize the purpose and meaning of the process.
iii. Irrelevant investigation processes not related to conducting MF were excluded.
iv. Include explicit and implicit investigation processes from models.

As shown in Table 6 it was discovered there are 108 investigation processes from the 24 MF models. Most of these 108 investigation processes are redundant and need to be merged in order to produce common/harmonized investigation processes for MF field. Next section discusses the merging process

3. *Mapping Extracted Investigation Process*: Since some of these processes overlap, it is necessary to consider the activities and tasks performed in each of the investigative processes and not to rely solely on naming conventions [156]–[158]. The mapping process is adapted to select the more frequent investigation process for every investigation process. Table 6 shows the mapping process of extracted forensic investigation processes.
4. *Propose harmonized Investigation Process*: Obviously, 7 investigation processes have a high frequency than other investigation processes which are: *preparation, data acquisition, preservation, examination, analysis,*

TABLE 5. Development and validation models.

No	Mobile Forensics Models	Investigation Processes	Processes
1.	Windows Mobile Forensic Process Model [3]	preparation, securing the scene, survey and recognition, documenting the scene, communication shielding, volatile evidence collection, non-volatile evidence collection, preservation, examination, analysis, presentation, review	12
2.	Smartphone Forensic Investigation Process Model [4]	preparation, securing the scene, documenting the scene, volatile evidence collection, non-volatile evidence collection, off-set, cell site analysis, preservation, examination, analysis, presentation, and review	12
3.	Mobile Forensics Model [121]	preparation, handling evidence & secure the evidence, data acquisition, documentation, examination and analysis, presentation, and review	7
4.	Framework of Digital Forensics for the Samsung Star Series Phone [11]	authorisation procedures, first response procedures, device transportation procedures, live acquisition procedures, maintenance procedures and evidence analysis	6
5.	Smartphone Forensics: A Proactive Investigation Scheme [19]	investigation engagement, evidence type selection, evidence collection, evidence transmission, evidence storage and investigation completion	6
6.	A quantitative approach to Triaging in Mobile Forensics [118]	device identification, acquisitions, triage, analysis, and reporting	5
7.	A Theoretical Process Model for Smartphones [119]	transportation, classification, analysis, interpretation, and retention	5
8.	Conceptual Evidence Collection and Analysis Methodology for Android Devices [8]	identify device and preserve evidence, collect evidence, examination and analysis, and reporting and presentation	5
9.	Symbian smartphones forensic process model [2]	preparation and version identification, remote evidence acquisition, internal evidence acquisition, analysis, and presentation and review	4
10.	Smart-Phone DEFSOP [5]	conception phase, the preparation phase, operation phase, and reporting phase	4
11.	An Android Social App Forensics Adversary Model [9]	collection, examination, analysis, and reporting	4
12.	Thumbnail forensic recovery process for Android devices [10]	identify, preserve, analyze, and present	4
13.	Generic Process Model for Smartphones Live Memory Forensics [12]	pre-incidence readiness, evidence collection, examination and analysis and information diffusion	4
14.	Smart Handheld Device Digital Evidence Forensic Procedures [15]	principle concept phase, preparation phase, operation phase, and report phase	4
15.	The Forensic Process Analysis of Mobile Device [16]	seizure, acquisition, analysis, and reporting	4
16.	Framework for iPhone Forensic [6]	data acquisition, data analysis, and data reporting	3
17.	Mobile Forensics using the Harmonized Digital Forensic Investigation Process [7]	initialisation process, acquisition process, and investigative process	3
18.	Mobile Forensic Investigation Life Cycle Process [120]	data gathering, preserve all original data sources, report generation	3
19.	Advances of Mobile Forensic Procedures in Firefox OS [13]	preparation, preservation, and acquisition	3
20.	Acquisition and Analysis of Digital Evidence in Android Smartphones [14]	acquisition and examination	2
21.	Digital evidence extraction and documentation from mobile devices [20]	extraction and documentation	2
22.	Mobile Forensic Adversary Model [21]	evidence collection and analysis	2
23.	A General Collection Methodology for Android Devices [17]	data collection	1
24.	Logical acquisition and analysis of data from android mobile devices [18]	collection of live data	1

reporting, and presentation. Figure 5 displays the HMFIPM.

The preparation process is the first MF investigation process that is used to prepare a clean forensic investigation environment and a verifiable forensic techniques, as well as allowing the investigation team to isolate the mobile device enough from the network to prevent users from tampering and capturing volatile and non-volatile data. The preservation process is used to protect the integrity of the mobile device and data. The data acquisition process is a process that utilized to gather/ acquire volatile and non-volatile data from a suspected mobile device. It consists of two sub-processes: live acquisition, and dead acquisition. A live acquisition is a kind of data acquisition that occur when the OS being analyzed is still running while the analysis is being performed. A dead acquisition process involves copying data from the non-volatile memory of the moile system under investigation, while the system is shut down. The examination process is used to ensure that the data acquired is authentic

TABLE 6. Mapping of extracted investigation process models.

Models\ Process	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8	Model 9	Model 10	Model 11	Model 12	Model 13	Model 14	Model 15	Model 16	Model 17	Model 18	Model 19	Model 20	Model 21	Model 22	Model 23	Model 24
Preparation	√	√	√					√	√	√		√	√	√					√					
Securing the Scene	√	√																						
Survey and Recognition	√																							
Documenting the Scene	√	√	√																					
Communication Shielding																								
Volatile Evidence Collection	√	√																						√
Non-volatile Evidence Collection	√	√																						
Preservation	√	√						√				√						√	√					
Examination	√	√	√					√			√		√							√				
Analysis	√	√	√			√	√	√	√		√	√	√		√	√						√		
Presentation	√	√	√					√	√			√												
Review	√	√	√						√															
Off-Set		√																						
cell site analysis		√																						
Handling Evidence & Secure the Evidence			√																					
Data Acquisition			√			√									√	√	√		√	√				
Authorisation Procedures				√																				
First Response Procedures				√																				
Device Transportation Procedures				√																				
Live Acquisition Procedures				√																				
Maintenance Procedures				√																				
evidence analysis				√																				
Investigation Engagement					√																			
Evidence Type Selection					√																			
Evidence Collection					√		√						√									√		
Evidence Transmission					√																			
Evidence Storage					√																			
Investigation Completion					√																			
Device Identification						√																		
Reporting						√		√		√	√			√	√	√		√						
Transportation							√																	
Classification							√																	
Interpretation							√																	
Retention							√		√															
Remote evidence acquisition									√															
internal evidence acquisition									√															
Conception Phase										√														
Operation Phase										√				√										
Collection											√												√	
Information diffusion													√											
Principle concept phase														√										
Seizure															√									
Initialisation process																	√							
Investigative process																	√							
Data Gathering																		√						
Extraction																					√			
Documentation																					√			

and has not been tampered with. Output from this process is fed into the analysis process. The analysis process is used to analyze examined data, activity reconstruction and data recovery using special forensic techniques to reveal who is tampering, when and where the tampering happened and how the tampering happened. The reporting process is used to document the whole investigation stages. Two feedback processes are further considered in the proposed HMFIPM -examination and analysis feedback. The examination feedback provide a means for knowledge re-intregation and re-evalaution. In some cases, the initial outcome of the examination might be revised to accommodate perceived discrepancies, or the need to update the examination process. Given that the examination process feeds into the analysis, the output of the analysis process could require further re-evalaution. Changes in this regard will, however, be required to follow the standardized chain of evidence and custody process. In instances where 'new-found knowledge' scenario is observed, the entire investigation process might be required. Therefore, knowledge from these feedback loops could be a cache of useful knowledge for post-investigation processes, as well as investigation repeatability enhancement. Finally, the presentation process is used to present the investigation stages and submit the results to the court.

The authors next explore some of the open and future challenges as a result of conducting this research study.

V. OPEN PROBLEMS AND FUTURE CHALLENGES

A concise description of the observed lingering challenges and the potential future research direction for MF discipline is presented in this section. Most of the mobile forensic tools do not support or do not have capabilities that can enable integration of application artifacts with known encodings like PDF or MS-Word. It would be important if machine learning approaches would be used in this context so that it would assist to classify and apply known encoding in forensic tools accordingly. While different artifacts are extracted using different forensic processes, the behavior analysis of these artifacts and how specifically the user-information is normalized continues to be an area that is least explored. Also, the perspective on how data analysis is conducted and the relationship that exist between artifact analysis and location analysis is a potential area that could be explored to explore anti-forensic problems [136]. Nevertheless, many

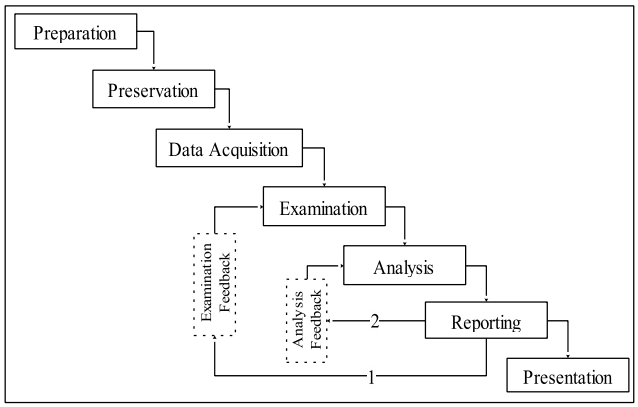

FIGURE 5. **Proposed HMFIPM.**

mobile forensic approaches have not incorporated incidental planning and preparation (Readiness) as is highlighted by [137], [138]. Mainly, it defeats the purpose of mobile devices given that in the recent past, their proliferations [139] have been one of the enablers of the rise of Internet of Things (IoT). Realistically, IoT environment connectivity is as a result of mobile devices, hence, forensic readiness is a key concern for mobile devices. Also, the techniques that can be used for data acquisition for mobile devices presents a challenge because they are not able to synchronize the metadata and the flash storage memory type, if addressed this could give investigators a forensic breakthrough. The variety of operating systems have also introduced diversity in the investigation process. This, however, implies that there is a need for an integrated investigation model which is context independent. Addressing this challenge could provide a baseline for the development of a standardized process model for conducting mobile forensics. Additionally, the lack of a standardized approach which can scale beyond OS-specific requirement presents a major limitation in developing an MF investigation process model that can scale legal scrutiny. Furthermore, this inefficiency implies the lack of well-structured and unified model that can facilitate, manage, share, and reuse the knowledge created in the MF field among all practitioners. Studies have established the propensity of human behavioral consistencies with the use of technology [140]–[143]. An exploration of these qualities as a component of investigation framework could present a novel platform in user attribution. Attribution as a forensic component is major research challenge which has led to the adoption of some scientific evidence (or the lack of it) in litigation. However, till date, the scientific committee continue to grabble with the development of a reliable process model for user and device attribution in digital forensics [144]–[147]. That notwithstanding, with the changing nature of how data keeps changing with changing technologies, a more resilient cognitive model is projected to be a future challenge given that the forensic investigation of mobile architecture still remains complicated [148]. Attempts to develop an investigative process model applicable for mobile forensics remains a research gap that requires special attention. Approach to develop a formal feedback collection and format is also a potential open challenge. Whilst investigators would need such knowledge to enahnce the investigation process, a formal approach and format would be required to define modalities to do so. One logic would be to leave the process to the context of the investigation. However, this could also implies that the investigator can provide such feedback based on their biases. Arguably, this will remain an open challenge which has the potential to escalate to other forensic disciplie. Till date, there is no formal approach to address this feedback process.

VI. CONCLUSION

This article reviewed totally 100 MF models. Using different terminologies, the scholars in this field have made use of various approaches regarding the number of phases in the investigation process. As confirmed by a review of the literature, the majority of MF process models are centered upon particular mobile events, which makes available low-level details. In addition, since models had a variety of perspectives, it was not possible to mark out a single model as a 'standardized' one. A significant contribution of the present study to the MF field is conducting a comprehensive review of MF-related literature, which can help effectively the field researchers to further comprehend MF. This article started with reviewing all existing MF studies; then, it discussed the challenges, limitations, and drawbacks of the field, and suggested a number of solutions to the limitations identified. In the following, some ideas are recommended for future research in the MF field: 1) improving and validating the proposed investigation process model (HMFIPM); 2) Development of a meta-modeling language that can be applied to structuring, managing, organizing, sharing, and reusing the created MF knowledge; and 3) Development of a definite MF source for the purpose of storing and retrieving the knowledge formed in the MF field.

REFERENCES

[1] I. Riadi, R. Umar, and A. Firdonsyah, "Identification of digital evidence on Android's blackberry messenger using NIST mobile forensic method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 155–160, 2017.

[2] X. Yu, L.-H. Jiang, H. Shu, Q. Yin, and T.-M. Liu, "A process model for forensic analysis of Symbian smart phones," in *Proc. Int. Conf. Adv. Softw. Eng. Appl.* Berlin, Germany: Springer, 2009, pp. 86–93.

[3] A. Ramabhadran, "Forensic investigation process model for windows mobile devices," Tata Elxsi Secur. Group, Tech. Rep., May 2009, vol. 11, pp. 1–16.

[4] A. Goel, A. Tyagi, and A. Agarwal, "Smartphone forensic investigation process model," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 5, pp. 322–341, 2012.

[5] I.-L. Lin, H.-C. Chao, and S.-H. Peng, "Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Oct. 2011, pp. 386–391.

[6] M. I. Husain, I. Baggili, and R. Sridhar, "A simple cost-effective framework for iPhone forensic analysis," in *Proc. Int. Conf. Digit. Forensics Cyber Crime*. Berlin, Germany: Springer, 2010, pp. 27–37.

[7] E. R. Mumba and H. S. Venter, "Mobile forensics using the harmonised digital forensic investigation process," in *Proc. Inf. Secur. South Africa*, 2014, pp. 1–10.

[8] B. Martini, Q. Do, and K.-K. R. Choo, "Conceptual evidence collection and analysis methodology for Android devices," 2015, *arXiv:1506.05527*. [Online]. Available: http://arxiv.org/abs/1506.05527

[9] A. Azfar, K.-K.-R. Choo, and L. Liu, "An Android social app forensics adversary model," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 5597–5606.
[10] D. L. Ming, C. J. D'Orazio, G. Deegan, and K.-K.-R. Choo, "Forensic collection and analysis of thumbnails in Android," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 1059–1066.
[11] S. Parvez, A. Dehghantanha, and H. G. Broujerdi, "Framework of digital forensics for the Samsung star series phone," in *Proc. 3rd Int. Conf. Electron. Comput. Technol.*, 2011, pp. 264–267.
[12] K. Paul, "Generic process model for Android smartphones live memory forensics," Fac. Comput. Inf. Manage., KCA Univ., Nairobi, Kenya, Tech. Rep., 2014, pp. 1–87.
[13] M. N. Yusoff, R. Mahmod, A. Dehghantanha, and M. T. Abdullah, "Advances of mobile forensic procedures in Firefox OS," *Int. J. Cyber-Secur. Digit. Forensics*, vol. 3, no. 4, pp. 183–199, 2014.
[14] A. M. de Lima Simão, F. C. Sícoli, L. P. de Melo, F. E. G. de Deus, and R. T. de Sousa Júnior "Acquisition and analysis of digital evidencein Android smartphones," Brazilian Assoc. High Technol. Experts (ABEAT), Brazil, Tech. Rep., 2011, pp. 28–43.
[15] C.-P. Chang, C.-T. Chen, T.-H. Lu, I.-L. Lin, P. Huang, and H.-S. Lu, "Study on constructing forensic procedure of digital evidence on smart handheld device," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, 2013, pp. 223–228.
[16] D. M. Sai, N. Prasad, and S. Dekka, "The forensic process analysis of mobile device," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 5, pp. 4847–4850, 2015.
[17] T. Vidas, C. Zhang, and N. Christin, "Toward a general collection methodology for Android devices," *Digit. Invest.*, vol. 8, pp. S14–S24, Aug. 2011.
[18] H. Srivastava and S. Tapaswi, "Logical acquisition and analysis of data from Android mobile devices," *Inf. Comput. Secur.*, vol. 23, no. 5, pp. 450–475, Nov. 2015.
[19] A. Mylonas, V. Meletiadis, B. Tsoumas, L. Mitrou, and D. Gritzalis, "Smartphone forensics: A proactive investigation scheme for evidence acquisition," in *Proc. IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2012.
[20] R. Ahmed, R. Dharaskar, and V. Thakare, "Digital evidence extraction and documentation from mobile devices," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 1, pp. 1019–1024, 2013.
[21] Q. Do, B. Martini, and K.-K.-R. Choo, "A forensically sound adversary model for mobile devices," *PLoS ONE*, vol. 10, no. 9, Sep. 2015, Art. no. e0138449.
[22] M. Goel and V. Kumar, "Layered framework for mobile forensics analysis," KNIT, Sultanpur, Sultanpur, India, Tech. Rep., Mar. 2019.
[23] R. Wilson and H. Chi, "A framework for validating aimed mobile digital forensics evidences," in *Proc. ACMSE Conf.*, 2018, pp. 1–8.
[24] A. Al-Dhaqm, S. Razak, and S. H. Othman, "Model derivation system to manage database forensic investigation domain knowledge," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2018, pp. 75–80.
[25] M. W. Burnette, "Forensic examination of a RIM (BlackBerry) wireless device," Tech. Rep., 2002.
[26] J. Grand, "pdd: Memory imaging and forensic analysis of palm OS devices," in *Proc. 14th Annu. 1st Conf. Comput. Secur. Incident Handling Response*, 2002, pp. 1–13.
[27] S. Willassen, "Forensics and the GSM mobile telephone system," *Int. J. Digit. Evidence*, vol. 2, no. 1, pp. 1–17, 2003.
[28] W. Jansen and R. Ayers, "Guidelines on PDA forensics," NIST Special Publication, Tech. Rep. 80072, Nov. 2004, vol. 800, p. 72.
[29] B. Mellars, "Forensic examination of mobile phones," *Digit. Invest.*, vol. 1, no. 4, pp. 266–272, Dec. 2004.
[30] S. Willassen, "Forensic analysis of mobile phone internal memory," in *Advances in Digital Forensics*. Boston, MA, USA: Springer, 2005, pp. 191–204.
[31] F. Casadei, A. Savoldi, and P. Gubian, "Forensics and SIM cards: An overview," *Int. J. Digit. Evidence*, vol. 5, no. 1, pp. 1–21, 2006. [Online]. Available: https://github.com/PicciMario/SimBrush
[32] P. M. Mokhonoana and M. S. Olivier, "Acquisition of a Symbian smart phone's content with an on-phone forensic tool," Dept. Comput. Sci., Univ. Pretoria, Pretoria, South Africa, Tech. Rep., 2007, pp. 1–7.
[33] K. Kim, D. Hong, K. Chung, and J.-C. Ryou, "Data acquisition from cell phone using logical approach," *World Acad. Sci., Eng. Technol.*, vol. 26, pp. 1–4, Dec. 2007.
[34] M. Al-Zarouni, "Introduction to mobile phone flasher devices and considerations for their use in mobile phone forensics," Cowan Univ., Joondalup, WA, Australia, Tech. Rep., 2007, pp. 1–6.
[35] I. M. Baggili, R. Mislan, and M. Rogers, "Mobile phone forensics tool testing: A database driven approach," *Int. J. Digit. Evidence*, vol. 6, no. 2, pp. 168–178, 2007.
[36] W. Jansen and R. Ayers, "Guidelines on cell phone forensics," NIST Special Publication, Gaithersburg, MD, USA, Tech. Rep. 2007.800, 2007, vol. 800, p. 101.
[37] M. Breeuwsma, M. De Jongh, C. Klaver, R. Van Der Knijff, and M. Roeloffs, "Forensic data recovery from flash memory," *Small Scale Digit. Device Forensics J.*, vol. 1, no. 1, pp. 1–17, 2007.
[38] J. Luck and M. Stokes, "An integrated approach to recovering deleted files from NAND flash data," *Small Scale Digit. Device Forensics J.*, vol. 2, no. 1, pp. 1941–6164, 2008.
[39] W. Jansen, A. Delaitre, and L. Moenner, "Overcoming impediments to cell phone forensics," in *Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2008, p. 483.
[40] J. Zdziarski, *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets*. Sebastopol, CA, USA: O'Reilly Media, 2008.
[41] A. Distefano and G. Me, "An overall assessment of mobile internal acquisition tool," *Digit. Invest.*, vol. 5, pp. S121–S127, Sep. 2008.
[42] S. Danker, R. Ayers, and R. P. Mislan, "Hashing techniques for mobile device forensics," *Stress*, vol. 1, no. 3, 2009
[43] A. Savoldi and P. Gubian, "Issues in Symbian S60 platform forensics," *J. Commun. Comput.*, vol. 6, no. 3, pp. 16–22, 2009.
[44] A. Savoldi, P. Gubian, and I. Echizen, "A comparison between windows mobile and Symbian S60 embedded forensics," in *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Sep. 2009, pp. 546–550.
[45] X. Yu, L.-H. Jiang, H. Shu, Q. Yin, and T.-M. Liu, "A process model for forensic analysis of Symbian smart phones," in *Advances in Software Engineering*. Berlin, Germany: Springer, 2009, pp. 86–93.
[46] A. Hoog and K. Gaffaney, "iPhone forensics," Via Forensics White Paper, 2009.
[47] F. Dellutri, V. Ottaviani, D. Bocci, G. F. Italiano, and G. Me, "Data reverse engineering on a smartphone," in *Proc. Int. Conf. Ultra Mod. Telecommun. Workshops (ICUMT)*, Oct. 2009, pp. 1–8.
[48] C. Shaoyan, H. Xianwei, and L. Ming, "Research of mobile forensic software system based on windows mobile," in *Proc. Int. Conf. Wireless Netw. Inf. Syst. (WNIS)*, Dec. 2009, pp. 366–369.
[49] D. Irwin and R. Hunt, "Forensic information acquisition in mobile networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PacRim)*, Aug. 2009, pp. 163–168.
[50] K. Fairbanks, K. Atreya, and H. Owen, "BlackBerry IPD parsing for open source forensics," in *Proc. IEEE SOUTHEASTCON*, Mar. 2009, pp. 195–199.
[51] R. Berte, F. Dellutri, A. Grillo, A. Lentini, G. Me, and V. Ottaviani, "Fast smartphones forensic analysis results through mobile internal acquisition tool and forensic farm," *Int. J. Electron. Secur. Digit. Forensics*, vol. 2, no. 1, pp. 18–28, 2009.
[52] C. Klaver, "Windows mobile advanced forensics," *Digit. Invest.*, vol. 6, nos. 3–4, pp. 147–167, May 2010.
[53] J. Lessard and G. Kessler, "Android forensics: Simplifying cell phone examinations," Cowan Univ., Joondalup, WA, Australia, Tech. Rep., 2010, pp. 1–12.
[54] E. Casey, M. Bann, and J. Doyle, "Introduction to windows mobile forensics," *Digit. Invest.*, vol. 6, nos. 3–4, pp. 136–146, May 2010.
[55] M. Bader and I. Baggili, "iPhone 3GS forensics: Logical analysis using apple iTunes backup utility," *Small Scale Digit. Device Forensics J.*, vol. 4, no. 1, pp. 1–15, 2010.
[56] S. Morrissey and T. Campbell, *IOS Forensic Analysis: For iPhone, iPad, and iPod Touch*, vol. 23. New York, NY, USA: Springer, 2010.
[57] I. Pooters, "Full user data acquisition from Symbian smart phones," *Digit. Invest.*, vol. 6, nos. 3–4, pp. 125–135, May 2010.
[58] F. Rehault, "Windows mobile advanced forensics: An alternative to existing tools," *Digit. Invest.*, vol. 7, nos. 1–2, pp. 38–47, Oct. 2010.
[59] V. L. L. Thing, K.-Y. Ng, and E.-C. Chang, "Live memory forensics of mobile phones," *Digit. Invest.*, vol. 7, pp. S74–S82, Aug. 2010.
[60] A. Distefano, G. Me, and F. Pace, "Android anti-forensics through a local paradigm," *Digit. Invest.*, vol. 7, pp. S83–S94, Aug. 2010.
[61] M. I. Husain and R. Sridhar, "iForensics: Forensic analysis of instant messaging on smart phones," in *Digital Forensics and Cyber Crime*. Berlin, Germany: Springer, 2010, pp. 9–18.
[62] H.-C. Chu, "Digital trails discovering of a GPS embedded smart phone—Take Nokia N78 running Symbian S60 Ver 3.2 for example," in *Secure and Trust Computing, Data Management, and Applications*. Berlin, Germany: Springer, 2011, pp. 41–49.

[63] A. Hoog and K. Strzempka, *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*. Amsterdam, The Netherlands: Elsevier, 2011.
[64] M. I. Husain, I. Baggili, and R. Sridhar, "A simple cost-effective framework for iPhone forensic analysis," in *Digital Forensics and Cyber Crime*. Berlin, Germany: Springer, 2011, pp. 27–37.
[65] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Amsterdam, The Netherlands: Elsevier, 2011.
[66] D. Quick and M. Alzaabi, "Forensic analysis of the Android file system YAFFS2," Cowan Univ., Joondalup, WA, Australia, Tech. Rep., 2011, pp. 100–109.
[67] G. Grispos, T. Storer, and W. B. Glisson, "A comparison of forensic evidence recovery techniques for a windows mobile smart phone," *Digit. Invest.*, vol. 8, no. 1, pp. 23–36, 2011.
[68] J. Jung, C. Jeong, K. Byun, and S. Lee, "Sensitive privacy data acquisition in the iPhone for digital forensic analysis," in *Secure and Trust Computing, Data Management and Applications*. Berlin, Germany: Springer, 2011, pp. 172–186.
[69] S. Maus, H. Höfken, and M. Schuba, "Forensic analysis of Geodata in Android smartphones," Univ. Appl. Sci., Glasgow, U.K., Tech. Rep., 2010, pp. 1–12.
[70] S. K. Sasidharan and K. Thomas, "Blackberry forensics: An agent based approach for database acquisition," in *Advances in Computing and Communications*. Berlin, Germany: Springer, 2011, pp. 552–561.
[71] Y. Lai, C. Yang, C. Lin, and T. Ahn, "Design and implementation of mobile forensic tool for Android smart phone through cloud computing," in *Convergence and Hybrid Information Technology*. Berlin, Germany: Springer, 2011, pp. 196–203.
[72] P. Albano, A. Castiglione, G. Cattaneo, and A. De Santis, "A novel anti-forensics technique for the Android OS," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Oct. 2011, pp. 380–385.
[73] A. Levinson, B. Stackpole, and D. Johnson, "Third party application forensics on apple mobile devices," in *Proc. 44th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2011, pp. 1–9.
[74] W.-S. Chun and D.-W. Park, "A study on the forensic data extraction method for SMS, photo and mobile image of Google Android and windows mobile smart phone," in *Convergence and Hybrid Information Technology*. Berlin, Germany: Springer, 2012, pp. 654–663.
[75] V. L. Thing and T.-W. Chua, "Symbian smartphone forensics: Linear bitwise data acquisition and fragmentation analysis," in *Computer Applications for Security, Control and System Engineering*. Berlin, Germany: Springer, 2012, pp. 62–69.
[76] V. L. L. Thing and D. J. J. Tan, "Symbian smartphone forensics and security: Recovery of privacy-protected deleted data," in *Information and Communications Security*. Berlin, Germany: Springer, 2012, pp. 240–251.
[77] F. N. Dezfouli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and S. B. Shamsuddin, "Volatile memory acquisition using backup for forensic investigation," in *Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec)*, Jun. 2012, pp. 186–189.
[78] D. Kim, J. Bang, and S. Lee, "Analysis of smartphone-based location information," in *Computer Science and Convergence*. Dordrecht, The Netherlands: Springer, 2012, pp. 43–53.
[79] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digit. Invest.*, vol. 9, pp. S24–S33, Aug. 2012.
[80] J. Park, H. Chung, and S. Lee, "Forensic analysis techniques for fragmented flash memory pages in smartphones," *Digit. Invest.*, vol. 9, no. 2, pp. 109–118, Nov. 2012.
[81] J. Sylve, A. Case, L. Marziale, and G. G. Richard, "Acquisition and analysis of volatile memory from Android devices," *Digit. Invest.*, vol. 8, nos. 3–4, pp. 175–184, Feb. 2012.
[82] P. Andriotis, G. Oikonomou, and T. Tryfonas, "Forensic analysis of wireless networking evidence of Android smartphones," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2012, pp. 109–114.
[83] L. Gómez-Miralles and J. Arnedo-Moreno, "Versatile iPad forensic acquisition using the apple camera connection kit," *Comput. Math. Appl.*, vol. 63, no. 2, pp. 544–553, Jan. 2012.
[84] B. Iqbal, A. Iqbal, and H. Al Obaidli, "A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Mar. 2012, pp. 238–243.
[85] S. S. Kumar, B. Thomas, and K. Thomas, "An agent based tool for windows mobile forensics," in *Digital Forensics and Cyber Crime*. Berlin, Germany: Springer, 2012, pp. 77–88.
[86] C. Racioppo and N. Murthy, "Android forensics: A case study of the," HTC Incredible Phone, Student-Fac. Res. Day, CSIS, Pace Univ., Seidenberg School CSIS, Pace Univ., New York, NY, USA, Tech. Rep., 2012, pp. B6.1–B6.8.
[87] E. Katz, R. Mislan, M. Rogers, and A. Smith, "Results of field testing mobile phone shielding devices," in *Digital Forensics and Cyber Crime*. Berlin, Germany: Springer, 2012, pp. 47–61.
[88] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "Forensic analysis of instant messenger applications on Android devices," 2013, *arXiv:1304.4915*. [Online]. Available: http://arxiv.org/abs/1304.4915
[89] N. S. Thakur, "Forensic analysis of WhatsApp on Android amartphones," Univ. New Orleans, New Orleans, LA, USA, Tech. Rep., 2013, pp. 38–44.
[90] N. Son, Y. Lee, D. Kim, J. I. James, S. Lee, and K. Lee, "A study of user data integrity during acquisition of Android devices," *Digit. Invest.*, vol. 10, pp. S3–S11, Aug. 2013.
[91] A. Ariffin, C. Doorazio, K.-K. R. Choo, and J. Slay, "iOS Forensics: How can we recover deleted image files with timestamp in a forensically sound manner?" in *Proc. 8th Int. Conf. Availability, Rel. Secur. (ARES)*, 2013, pp. 375–382.
[92] M. Al Marzougy, I. Baggili, and A. Marrington, "Blackberry playbook backup forensic analysis," in *Digital Forensics and Cyber Crime*. Berlin, Germany: Springer, 2013, pp. 239–252.
[93] X. Chang, X.-H. Tang, and J. Wu, "Forensic research on data recovery of Android smartphone," in *Proc. 2nd Int. Conf. Comput. Sci. Electron. Eng.*, 2013, pp. 1–4.
[94] E. S. Canlar, M. Conti, B. Crispo, and R. Di Pietro, "Windows mobile LiveSD forensics," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 677–684, Mar. 2013.
[95] L. Gomez-Miralles and J. Arnedo-Moreno, "Analysis of the forensic traces left by AirPrint in apple iOS devices," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2013, pp. 703–708.
[96] M. Guido, J. Ondricek, J. Grover, D. Wilburn, T. Nguyen, and A. Hunt, "Automated identification of installed malicious Android applications," *Digit. Invest.*, vol. 10, pp. S96–S104, Aug. 2013.
[97] T. Müller and M. Spreitzenbarth, "FROST," in *Applied Cryptography and Network Security*. Berlin, Germany: Springer, 2013.
[98] C.-N. Chen, R. Tso, and C.-H. Yang, "Design and implementation of digital forensic software for iPhone," in *Proc. 8th Asia Joint Conf. Inf. Secur. (Asia JCIS)*, Jul. 2013, pp. 90–95.
[99] A. Mylonas, V. Meletiadis, L. Mitrou, and D. Gritzalis, "Smartphone sensor data as digital evidence," *Comput. Secur.*, vol. 38, pp. 51–75, Oct. 2013.
[100] P. Dibb and M. Hammoudeh, "Forensic data recovery from Android OS devices: An open source toolkit," in *Proc. Eur. Intell. Secur. Informat. Conf. (EISIC)*, Aug. 2013, p. 226.
[101] M. Zheng, M. Sun, and J. C. S. Lui, "Droid analytics: A signature based analytic system to collect, extract, analyze and associate Android malware," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Jul. 2013, pp. 163–171.
[102] D. Votipka, T. Vidas, and N. Christin, "Passe-partout: A general collection methodology for Android devices," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1937–1946, Dec. 2013.
[103] S. Zhang and L. Wang, "Forensic analysis of social networking application on iOS devices," *Proc. SPIE*, vol. 9067, Dec. 2013, Art. no. 906715.
[104] W. Takahashi, R. Sasaki, and T. Uehara, "Development and evaluation of guideline total support system for evidence preservation by using an Android phone," in *Proc. IEEE 37th Annu. Comput. Softw. Appl. Conf. Workshops (COMPSACW)*, Jul. 2013, pp. 21–26.
[105] Y.-C. Tsai and C.-H. Yang, "Physical forensic acquisition and pattern unlock on Android smart phones," in *Future Information Communication Technology and Applications*. Dordrecht, The Netherlands: Springer, 2013, pp. 871–881.
[106] C.-W. Song, J.-H. Lim, K.-Y. Chung, K.-W. Rim, and J.-H. Lee, "Fast data acquisition with mobile device in digital crime," in *IT Convergence and Security 2012*. Dordrecht, The Netherlands: Springer, 2013, pp. 711–717.
[107] N. Al Barghouthy and A. Marrington, "A comparison of forensic acquisition techniques for Android devices: A case study investigation of orweb browsing sessions," in *Proc. 6th Int. Conf. New Technol., Mobility Secur. (NTMS)*, Mar. 2014, pp. 1–4.
[108] M. Kaart and S. Laraghy, "Android forensics: Interpretation of timestamps," *Digit. Invest.*, vol. 11, no. 3, pp. 234–248, 2014.
[109] D. B. L. Schatz, "A visual approach to interpreting NAND flash memory," *Digit. Invest.*, vol. 11, no. 3, pp. 214–223, Sep. 2014.

[110] C. Anglano, "Forensic analysis of WhatsApp messenger on Android smartphones," *Digit. Invest.*, vol. 11, no. 3, pp. 201–213, Sep. 2014.
[111] Y. Yang, Z. Zu, and G. Sun, "Historical data recovery from Android devices," in *Future Information Technology*. Berlin, Germany: Springer, 2014, pp. 251–257.
[112] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Extraction of common concepts for the mobile forensics domain," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.* Cham, Switzerland: Springer, 2017, pp. 141–154.
[113] A. Ali, S. A. Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," *PLoS ONE*, vol. 12, no. 4, Apr. 2017, Art. no. e0176223.
[114] F. G. Hikmatyar and B. Sugiantoro, "Digital forensic analysis on Android smartphones for handling cybercrime cases," *Int. J. Inform. Develop.*, vol. 7, no. 2, pp. 19–22, 2019.
[115] A. Fukami and K. Nishimura, "Forensic analysis of water damaged mobile devices," *Digit. Invest.*, vol. 29, pp. S71–S79, Jul. 2019.
[116] D. K. Sharma, K. Kwatra, and M. Manwani, "Smartphone security and forensic analysis," in *Forensic Investigations and Risk Management in Mobile and Wireless Communications*. Hershey, PA, USA: IGI Global, 2020, pp. 26–50.
[117] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, "Mobile forensic data analysis: Suspicious pattern detection in mobile evidence," *IEEE Access*, vol. 6, pp. 59705–59727, 2018.
[118] F. Marturana, G. Me, R. Berte, and S. Tacconi, "A quantitative approach to triaging in mobile forensics," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 582–588.
[119] F. C. Dancer, D. A. Dampier, J. M. Jackson, and N. Meghanathan, "A theoretical process model for smartphones," in *Advances in Computing and Information Technology*. Berlin, Germany: Springer, 2013, pp. 279–290.
[120] S. Rajendran and N. P. Gopalan, "Mobile forensic investigation (MFI) life cycle process for digital data discovery (DDD)," in *Proc. Int. Conf. Soft Comput. Syst.* New Delhi, India: Springer, 2016.
[121] M. Sadiq, M. S. Iqbal, M. Sajad, K. Naveed, and A. Malip, "Mobile devices forensics investigation: Process models and comparison," *Theor. Appl. Sci.*, vol. 33, no. 1, pp. 164–168, Jan. 2016.
[122] B. McTurk, "Forensic professionals' views on the lack of standards in the digital forensic field: A generic qualitative inquiry," Capella Univ., Minneapolis, MN, USA, Tech. Rep., 2019, Art. no. 13811364.
[123] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, p. 949, 2018.
[124] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced forensic process for improving mobile cloud traceability in cloud-based mobile applications," *Procedia Comput. Sci.*, vol. 167, pp. 907–917, Jan. 2020.
[125] V. R. Kebande, N. M. Karie, and S. Omeleze, "A mobile forensic readiness model aimed at minimizing cyber bullying," *Int. J. Comput. Appl.*, vol. 140, no. 1, pp. 28–33, Apr. 2016.
[126] A. Chamberlain and M. H. B. Azhar, "Comparisons of forensic tools to recover ephemeral data from iOS apps used for cyberbullying," in *Proc. IARIA*, 2019, pp. 1–6.
[127] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," *Austral. J. Forensic Sci.*, vol. 50, no. 5, pp. 552–591, Sep. 2018.
[128] K. Billups, "New and emerging mobile apps among teens-are forensic tools keeping up?" Ph.D. dissertation, Graduate School, Purdue Univ., West Lafayette, IN, USA, 2020.
[129] S. S. Shimmi, G. Dorai, U. Karabiyik, and S. Aggarwal, "Analysis of iOS SQLite schema evolution for updating forensic data extraction tools," in *Proc. 8th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2020, pp. 1–7.
[130] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative analysis of Android mobile forensics tools," in *Proc. IEEE Conf. Comput. Appl. (ICCA)*, Feb. 2020, pp. 1–6.
[131] J.-U. Lee and W.-Y. Soh, "Comparative analysis on integrated digital forensic tools for digital forensic investigation," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 834, Jun. 2020, Art. no. 012034.
[132] C. Troutman and V. Mancha, "Mobile forensics," in *Digital Forensic Education*. Cham, Switzerland: Springer, 2020, pp. 175–201.
[133] A. U. Mentsiev and M. T. Alams, "Mobile forensic tools and techniques: Android data security," *Don's Eng. Gazette*, vol. 2, p. 53, Feb. 2019.
[134] M. D. Guido, "Attributing users based on Web browser history," U.S. Patent 10 194 321, Nov. 10, 2017.
[135] C. Anglano, M. Canonico, and M. Guazzone, "The Android forensics automator (AnForA): A tool for the automated forensic analysis of Android applications," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101650.
[136] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Sci. Int., Digit. Invest.*, vol. 33, Jun. 2020, Art. no. 200897.
[137] V. R. Kebande and H. S. Venter, "A comparative analysis of digital forensic readiness models using CFRaaS as a baseline," *Wiley Interdiscipl. Rev., Forensic Sci.*, vol. 1, no. 6, p. e1350, Nov. 2019.
[138] V. R. Kebande and H. S. Venter, "Adding event reconstruction to a cloud forensic readiness model," in *Proc. Inf. Secur. South Afr. (ISSA)*, Aug. 2015, pp. 1–9.
[139] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, p. 356.
[140] I. R. Adeyemi, S. A. Razak, M. Salleh, and H. S. Venter, "Observing consistency in online communication patterns for user re-identification," *PLoS ONE*, vol. 11, no. 12, pp. 1–27, 2016.
[141] A. R. Ikuesan, S. A. Razak, H. S. Venter, and M. Salleh, "Polychronicity tendency-based online behavioral signature," *Int. J. Mach. Learn. Cybern.*, vol. 10, no. 8, pp. 2103–2118, Aug. 2019.
[142] M. Mohlala, A. R. Ikuesan, and H. S. Venter, "User attribution based on keystroke dynamics in digital forensic readiness process," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2017, pp. 1–6.
[143] S. Pretorius, A. R. Ikuesan, and H. S. Venter, "Attributing users based on Web browser history," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2017, pp. 1–6.
[144] D. Ernsberger, A. R. Ikuesan, H. S. Venter, and A. Zugenmaier, "A Web-based mouse dynamics visualization tool for user attribution in digital forensic readiness," in *Proc. 9th EAI Int. Conf. Digit. Forensics Cyber Crime*. Berlin, Germany: Springer, 2017, pp. 1–13.
[145] I. R. Adeyemi, S. A. Razak, and M. Salleh, "A psychographic framework for online user identification," in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Aug. 2014, pp. 198–203.
[146] D. Ellison, H. Venter, and A. Ikuesan, "An improved ontology for knowledge management in security and digital forensics," in *Proc. Eur. Conf. Cyber Warfare Secur.*, 2017, pp. 725–733.
[147] A. R. Ikuesan and H. S. Venter, "Digital forensic readiness framework based on behavioral-biometrics for user attribution," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2017, pp. 54–59.
[148] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," *Forensic Sci. Int., Synergy*, vol. 1, pp. 61–67, Jan. 2019.
[149] A. Al-Dhaqm, S. Razak, S. H. Othman, K.-K.-R. Choo, W. B. Glisson, A. Ali, and M. Abrar, "CDBFIP: Common database forensic investigation processes for Internet of Things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017.
[150] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a database forensic metamodel (DBFM)," *PLoS ONE*, vol. 12, no. 2, Feb. 2017, Art. no. e0170793.
[151] A. Al-Dhaqm, S. A. Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," *J. Teknologi*, vol. 78, nos. 6–11, Jun. 2016.
[152] A. Al-Dhaqm, S. A. Razak, D. A. Dampier, K.-K.-R. Choo, K. Siddique, R. A. Ikuesan, A. Alqarni, and V. R. Kebande, "Categorization and organization of database forensic investigation processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020.
[153] M. F. Caro, D. P. Josyula, M. T. Cox, and J. A. Jiménez, "Design and validation of a metamodel for metacognition support in artificial intelligent systems," *Biologically Inspired Cognit. Archit.*, vol. 9, pp. 82–104, Jul. 2014.
[154] S. Kelly and R. Pohjonen, "Worst practices for domain-specific modeling," *IEEE Softw.*, vol. 26, no. 4, pp. 22–29, Jul. 2009.
[155] A. C. Bogen, "Selecting keyword search terms in computer forensics examinations using domain analysis and modeling," Ph.D. dissertation, Mississippi State Univ., Starkville, MA, USA, 2006, Art. no. aAI3241379.
[156] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping process of digital forensic investigation framework," *Int. J. Comput. Sci. Netw. Secur.*, vol. 8, no. 10, pp. 163–169, 2008.
[157] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," *Wiley Interdiscipl. Rev., Forensic Sci.*, vol. 2, no. 5, p. e1372, Sep. 2020.

[158] V. R. Kebande and H. S. Venter, "On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges," *Austral. J. Forensic Sci.*, vol. 50, no. 2, pp. 209–238, Mar. 2018.
[159] P. Sharma, D. Arora, and T. Sakthivel, "Mobile cloud forensic readiness process model for cloud-based mobile applications," *Int. J. Digit. Crime Forensics*, vol. 12, no. 3, pp. 58–76, Jul. 2020.

ARAFAT AL-DHAQM (Member, IEEE) received the B.Sc. degree in information system from the University of Technology, Iraq, and the M.Sc. degree (Hons.) in information security and the Ph.D. degree in computer science from University Technology Malaysia (UTM). His Ph.D. research focused on solving the heterogeneity and ambiguity of the database forensic investigation field using a meta-modeling approach. He is currently working as a Senior Lecturer at UTM. His current research interests include digital forensics and cybersecurity. He serves as an Editorial Board Member of *Forensic Genetics* Journal and the *Canadian Journal of Biomedical Research and Technology (CJBRT)*.

SHUKOR ABD RAZAK (Member, IEEE) is currently an Associate Professor with Universiti Teknologi Malaysia. His research interests include the security issues for mobile ad hoc networks, mobile IPv6, vehicular ad hoc networks, and network security. He also actively conducts several types of research in digital forensic investigation, wireless sensor networks, and cloud computing. He is the author or coauthor of many journals and conference proceedings at national and international levels.

RICHARD ADEYEMI IKUESAN (Member, IEEE) received the M.Sc. and Ph.D. degrees (Hons.) in computer science from Universiti Teknologi Malaysia. He is an Active Researcher currently pioneering a digital policing and forensic project for developing nations, using Nigeria and South Africa as a hub for West Africa and Southern Africa. He is an Assistant Professor with the IT Department, Cyber Security Section, Community College of Qatar.

VICTOR R. KEBANDE received the Ph.D. degree in computer science in the area of information and computer security architectures and digital forensics from the University of Pretoria, Hatfield, South Africa. He previously belonged to ICSA and DIgiFORS Research Groups, University of Pretoria. He is currently a Cyber and Information Security Postdoctoral Researcher with the Internet of Things and People (IoTaP) Center, Department of Computer Science and Media Technology, Malmö University, Sweden. His main research interests include cyber, information security, and digital forensics in the area of the IoT, (mainly IoT security), digital forensics-incident response, cyber-physical system protection, critical infrastructure protection, adversarial motives and detecting in the IoT infrastructures, cloud security, computer systems, distributed system security, threat hunting and modeling and cyber-security risk assessment, blockchain technologies, and privacy preserving techniques. He also serves as an Editorial Board Member of *Forensic Science International: Reports* Journal. He serves as a reviewer and an editor for number of well reputed journals.

KAMRAN SIDDIQUE (Member, IEEE) received the Ph.D. degree in computer engineering from Dongguk University, South Korea. He is currently an Associate Professor with Xiamen University Malaysia. His research interests include cybersecurity, machine learning, and big data processing.