IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

An Overview of Mobile Forensic Investigation Process Models

Pawan Madhukar Pawar
Senior Cyber Forensic Analyst
Crypto Forensic Technology, Nagpur, Maharashtra, India

***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.**

Keywords*— 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.

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 digitalization comes the enormity and complexity of digital crimes, a phenomenon that the community of digital forensic professionals (researchers, practitioners, and standardization organizations) 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 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 WORK

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.

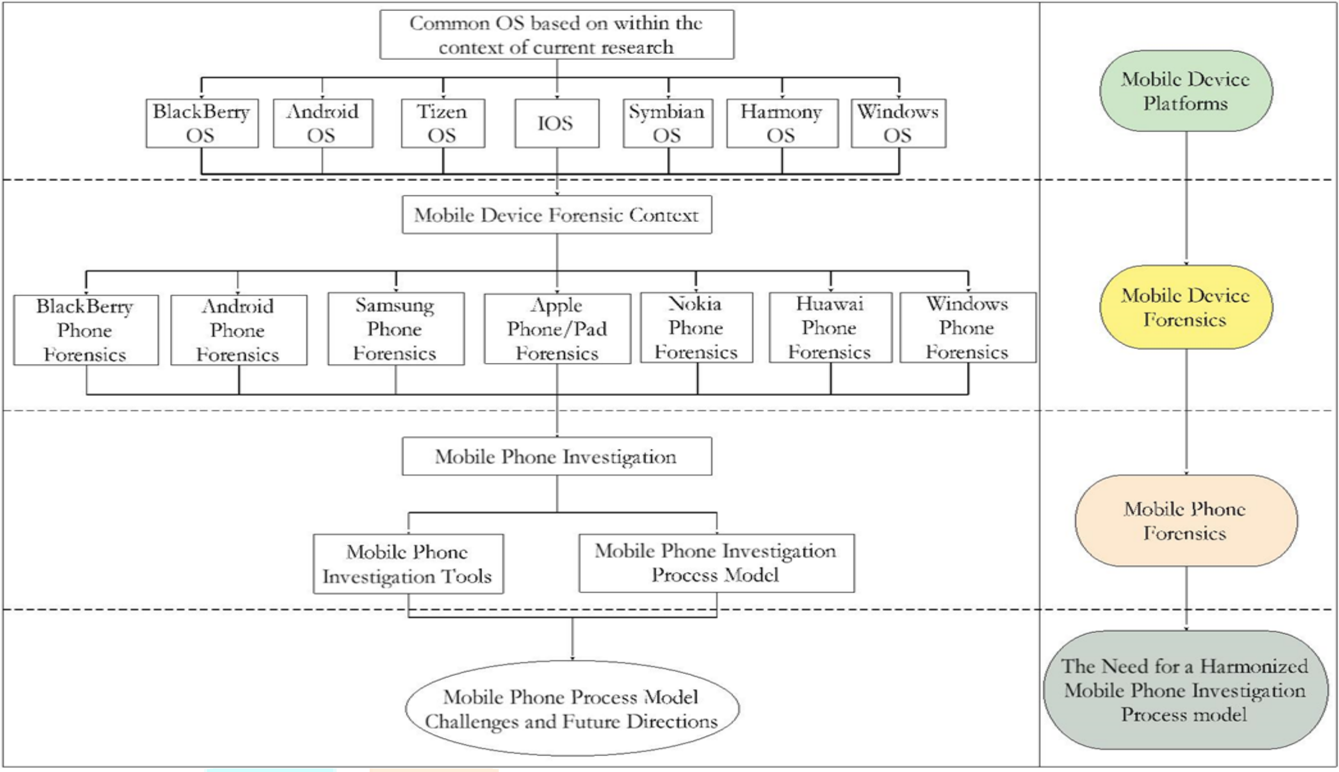
Common OS based on within the context of current research
BlackBerry OS
Android OS
Tizen OS
IOS
Symbian OS
Harmony OS
Windows OS
Mobile Device Forensic Context
BlackBerry Phone Forensics
Android Phone Forensics
Samsung Phone Forensics
Apple Phone/Pad Forensics
Nokia Phone Forensics
Huawai Phone Forensics
Windows Phone Forensics
Mobile Phone Investigation
Mobile Phone Investigation Tools
Mobile Phone Investigation Process Model
Mobile Phone Process Model Challenges and Future Directions
Mobile Device Platforms
Mobile Device Forensics
Mobile Phone Forensics
The Need for a Harmonized Mobile Phone Investigation Process model

Fig.1. Research on Mobile Forensic Investigation Processes that Covered Different Mobile Device

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 _ow 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 customization of existing _le carving tools in a way to recover effectively the thumbnails from the forensic image (Through decreasing the number of irrelevant _les). 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: authorization 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.

III. METHODOLOGY

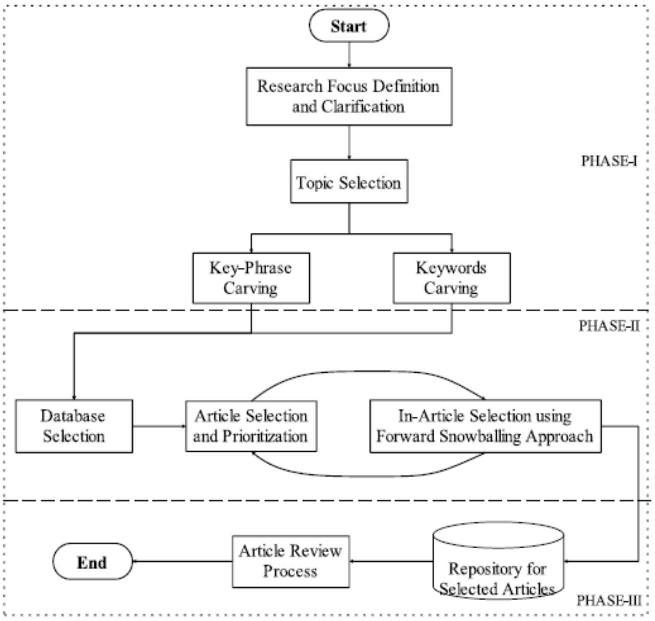
Start
Research Focus Definition and Clarification
PHASE-I
Topic Selection
Key-Phrase Carving
Keywords Carving
PHASE-II
Database Selection
Article Selection and Prioritization
In-Article Selection using Forward Snowballing Approach
End
Article Review Process
Repository for Selected Articles
PHASE-III

Fig.2. Literature Review 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 [13] as further depicted in Figure 2. The method used here consisted of three phases.

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.

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.

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).

IV. 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. 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 _ash 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. 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. 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 enhance 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 discipline. Till date, there is no formal approach to address this feedback process.

V. Conclusion

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.

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 Trust-com/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] 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.