Crimson Publishers
Wings to the Research

Opinion

Toolbox Application to Support and Enhance the Mobile Device Forensics Investigation Process

Bruno Bernardo* and Vitor Santos

NOVA Information Management School, New University of Lisbon, Lisbon, Portugal

ISSN: 2578-0042

***Corresponding author:** Bruno Bernardo, NOVA Information Management School, New University of Lisbon, Lisbon, Portugal

Submission: February 11, 2021

Published: March 04, 2021

Volume 5 - Issue 3

How to cite this article: Bruno Bernardo, Vitor Santos. Toolbox Application to Support and Enhance the Mobile Device Forensics Investigation Process. Forensic Sci Add Res. 5(3). FSAR. 000619. 2021.
DOI: 10.31031/FSAR.2021.05.000619

Opinion

Throughout the study on the topic regarding Mobile Device Forensics, the authors noticed the different challenges that arise from the digital investigation associated with this science. Moreover, to address these different challenges, namely, the ones regarding the lack of documentation, standardization and research on this science Chernyshev et al. [1]; Barmpatsalou et al. [2]; Omeleze and Venter [3], the authors studied not only the Forensics field but also the Digital and Mobile Forensics ones, in other to understand the different and critical challenges that are jeopardizing and affecting the accuracy and integrity of these types of sciences and its investigations. As such, the authors proposed to study this field by firstly performing a systematic literature review using the PRISMA Methodology (presented in the chapter from the authors, Bernardo B and Santos V [4] and secondly building a toolbox application to support and enhance the Mobile Device Forensics investigation process, by analyzing, describing, and constructing an architecture and its contents.

To do so, the authors had to first acknowledge the context and background around this science, the different challenges and opportunities, the tools, and applications available while understanding how a digital investigator can leverage on it. The main objective is to achieve a toolbox that would potentially have in its architecture the most up-to-date available software to pursue Mobile Forensics. Throughout the study performed by the authors in the chapter Bernardo B and Santos V [4], the authors acknowledged the increasing concern on this field and on digital examiners, around what are the tools and applications available and on can these be put into practice to perform a given analysis. As such, the toolbox architecture aims to describe what are the tools and applications that are open source, i.e., free to be used and those that the user needs to pay a specific license to be able to access and utilize it within a forensics process.

Likewise, the authors noticed the lack of standardization around the Mobile Forensics science regarding a given digital investigation. As such, the authors studied and scrutinized within the previously described systematic literature review, the methodologies that exists in the literature available on this science. The objective for the authors, was to compile and standardize the investigation process methodology, as such, the authors aim to purpose a methodology that will be the result of the conjunction and alignment of the best and key phases of different existing methodologies. For instance, and according to some of the literature studied, namely, Ayers et al. [5], the Mobile Device Forensics Science can be defined as a process-wise that contains four stages, being the first, the preservation phase, followed by the second, acquisition, the third, examination, and fourth, report. Likewise, other authors, such as Sathe and Dongre [6], describe this branch of Forensics science as, a stepwise methodology, that encompasses 6 stages, being the first the identification followed by the preservation, acquisition, analysis, documentation, and presentation. As such, these methodologies and others that are presented within the literature, can be put together and support the toolbox creation as well as well as to choose which tools and applications can address each of the derived stages.

While achieving a standardized methodology, the authors aim to fit and align the different existing tools and applications within the process stages/phases archived by putting together the literature methodology that supports the Mobile Investigation Forensics analysis, as to suggest the standardization of this field within the literature that is available and to address the existing lack of research and knowledge databases.

Given this and in lines manner, the selection of the tools that will compose the toolbox, will also have in consideration the price characteristic of each tool, regarding if the application/device chosen is free for an investigator to use or requires the user to pay a given amount or a license.

After acknowledging and studying extensively the literature regarding the topics of Forensics, Digital Forensics and Mobile Device Forensics and, in a deeper and more conclusive detail, the architecture and archeology of mobile phones, its features and main components, the several and various types of information and storage that it can contain, the different information extraction layers that one can perform during a mobile forensics analysis, and the existing and available paid and open-source applications to perform a mobile forensics analysis, it was possible to have a crystal clear acknowledgement and prototype on how a Mobile Forensics Toolbox must look like in order to support and enhance the Mobile Forensics Investigation Process.

As such, the authors pretend to propose a toolbox of tools and applications that are presented as a way to allow the digital investigator to acknowledge what are the tools that are available for a Mobile Devices Forensics investigation, both free and/or paid, and dependently on the budget and level of detail and extraction that the digital investigator has and wants to reach, which will enlarge its awareness on the existing applications available to the Mobile Forensics science. Likewise, the authors aim to communicate the results of the research that is being performed on the construction and application of the toolbox for the Mobile Device Forensics process.

References

1. Chernyshev M, Zeadally S, Baig Z, Woodward A (2017) Mobile forensics: Advances, challenges, and research opportunities. IEEE Security & Privacy 15(6): 42.
2. Barmpatsalou K, Cruz T, Monteiro E, Simoes P (2018) Current and future trends in mobile device forensics: A survey. ACM Computing Surveys 51(3): 1-31.
3. Omeleze S, Venter HS (2013) Testing the harmonised digital forensic investigation process model-using an android mobile phone. 2013 information security for South Africa, information security for South Africa 1.
4. Bernardo B, Santos V (2021) Mobile device forensics investigation process: A systematic review. In: Cruz-Cunha M, Mateus-Coelho NR (eds.), Handbook Of Research On Cyber Crime And Information Privacy IGI Global, pp. 256-288.
5. Ayers R, Brothers S, Jansen W (2014) Guidelines on mobile device forensics. National Institute of Standards and Technology Special Publication, pp. 800-101.
6. Sathe SC, Dongre NM (2018) Data acquisition techniques in mobile forensics. Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC, pp. 280-286.