Towards Adapting Metamodeling approach for the Mobile Forensics Investigation Domain

Abdulalem Ali[1*], Shukor Abd Razak[1], Siti Hajar Othman[1], Arafat Mohammed[1]
[1] Faculty of Computing, Universiti Teknologi Malaysia

* corresponding author: almaldolah2012@gmail.com

Abstract
Mobile phones have become quite important tools in the modern world. The forensics field heavily relies on knowledge as an important resource. Due to the ongoing changes in digital technology, the power of knowledge enables innovation and assists in establishing proper standards and procedures. As such, it is necessary to establish a relationship between the information derived from knowledge to form new concepts and ideas. Knowledge in mobile forensics is scattered and huge. Hence, this leads to lack of knowledge management in mobile forensics. In addition, lead to complexity of investigation for new investigators, ambiguity in concepts and terminologies of mobile forensics domain and waste time to understand mobile forensics domain. Therefore, mobile forensics investigators are quite suffering with forensics investigation processes in their domain. This paper will develop a new approach for mobile forensics domain which is based on metamodeling. This approach contributes to unify common concepts of mobile forensics. It also provides many benefits which include simplifying the investigation process and guide investigations team, capture and reuse specialized forensic knowledge and support training and knowledge management activities. Furthermore, it reduces complexity and ambiguity in mobile forensic domain.

Keywords: Digital forensics; Metamodeling; Mobile forensics

Introduction

Mobile phone forensics is considered a new field comparing to the other digital forensics such as computer forensics, and database forensics. According to [1], Mobile Forensics (MF) is a branch of digital forensics relating to recovery of digital evidence from a mobile device under forensically sound conditions. MF has many interacting elements such as people, authority, investigators team, resources, procedures, policy etc. The sophistication of the crimes and the variety of mobile phone devices used in these offenses are becoming major challenges to the investigators [2]. In addition, volume data and complexity of investigation are one of the major issues in MF[3].

Besides, modeling coordination of MF activities is hard task and complex. Moreover, as the investigator may not have a clear view of which potential evidence to start the investigation with. However, previous researches mostly discussed mobile forensics only in data acquisition terms and only in a problem solving scenario as a subset to computer forensics. They did not take mobile forensics to go beyond the paradigm that is known as computer forensics. Additionally, previous researches in MF domain did not focus on modeling case domain information involved in investigations. This paper develops a new approach for MF domain which is based on metamodeling. This approach contributes to unify common concepts of MF. It also provides many benefits which include simplifying the investigation process and guide forensic investigators, capture and reuse specialized forensic knowledge and support training and knowledge management activities. Moreover, it reduces complexity and ambiguity in MF domain. The rest of this paper is structured as follows. Section 2 presents the MF issues and challenges. Methods and Metamodeling approach is discussed in section 3. Finally, the conclusion of the paper is presented in Section 4.

Mobile Forensics Issues and Challenges

Many research conducted in the MF domain. Certain studies discussed MF in general devices, while the majority of previous studies discussed the smartphone forensics. Digital evidence in mobile phones is easily to tampering through overwritten or remote commands received from the wireless network [4]. Rapid proliferation of phones on the market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques. In addition, [5] mentioned that mobile phones contain many digital evidence for digital

investigation processes. The extracted evidence from mobile phones play significant role for forensics investigation in recent years. For instance, mobile phone evidence was used in the prosecution of Ian Huntley who killed two girls, and also used to locate and arrested suspects in the failed London car bomb attacks in 2007[5]. However, validated frameworks and methods to extract mobile phone data are practically non-existent [6]. The rapid development in the mobile phone devices cause difficulties to design a single forensic tool or standards specific to one platform [5]. In addition, [7] stated that the lack of hardware, software and standardization in mobile phone devices are one of the significant difficulties in the MF domain. This fact makes investigation process a hard task. Furthermore, the lack of standardization is a major issue in the field of MF. Advanced development in technology as well as variety of mobile of mobile devices and OSs are making the procedure of developing a common framework or standardization model a hard task. [8], [7, 9]. Besides, [10] stated that the major issue in mobile phone is that there is no standard forensic model as well as no standard process for the forensic examination of smart phones.

Research by Hoog mentioned that digital forensic investigators and security engineers have face difficulties dealing with mobile phone crimes due to the lack of knowledge [11]. Furthermore, [12] stated that the members of the legal profession need to increase their level of understanding and knowledge of mobile phone forensics terminology, techniques and procedures. In [13] mentioned that the major issues in law enforcement agencies in many countries is the lack of knowledge management. Therefore, forensic investigators are facing difficult challenges to conduct the forensic investigation processes in digital crimes particularly for mobile phones. The recent NIST Mobile Forensics Workshop (2014) [14] conducted by researchers in the MF domain. They discussed all issues related to MF domain. In addition, they mentioned that investigators are suffering with MF domain because they do not have sufficient knowledge, training and education related to proper seizure procedures for mobile devices, proper transport procedures and proper forensic examinations and analysis [14]. Furthermore, There are a number of digital forensic process models developed by various organizations worldwide, but yet, there is no agreement among forensic investigations and legislative delegation which procedures to adhere to; specially in the case of facing mobile devices with latest technologies [15].

Method

The metamodeling approach is the main method used in this paper. This approach is a foundational for many modeling frameworks. According to [16] metamodeling is activity and processes which generating a metamodel. The metamodel contributes to analysis, construct and develop the frames, rules, constraints, models and theories applicable[17]. In addition, it supports facilities to identifying primitive concepts for instance entity, activity and goal within the metamodel. Figure 1 illustrates the process of developing the Mobile Forensics Metamodel. However, mobile forensics investigation has four common phases which are preservation, acquisition, examination and analysis and report. The Mobile Forensic Metamodel (MFM) will present in four different diagrams to clearly group the classes into four areas of concern: the Preservation-phase, the Acquisition-phase, the Examination and analysis-phase and the Report-phase. Figure 2 illustrates activities and processes of preservation- phase as well as demonstrates relationship between them.

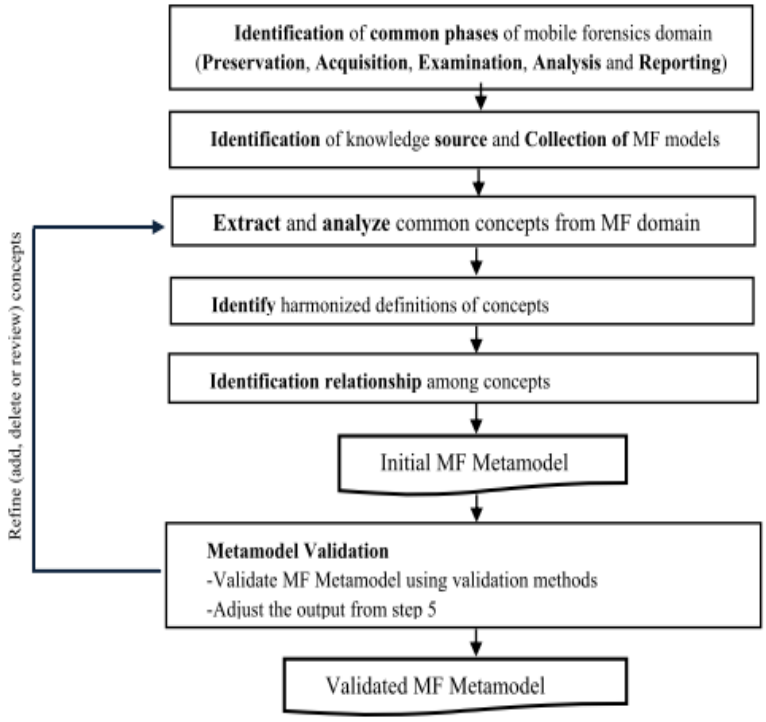

Figure 1 The process of developing the Mobile Forensics Metamodel

Conclusion

Mobile forensics investigation issues and challenges have presented in this paper. Lack of knowledge management in mobile forensics lead to complexity of investigation for new investigators, ambiguity in concepts and terminologies of mobile forensics and waste time to understand this domain. In addition, the proposed Mobile Forensics Metamodel has discussed briefly in this paper. This approach will contribute to increase and build blocks of knowledge for both members and non-members of the digital forensic community towards the mobile forensic investigation in the forensic agencies.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education Malaysia (MoHE) and Universiti Teknologi Malaysia (UTM) for funding this study under the Fundamental Research Grant Scheme (FRGS) of Grant No. PY/2014/03139 (R.J130000.7828.4F498).

References

1. Jansen, W. and R. Ayers. Guidelines on cell phone forensics. *NIST Special Publication*. 2007. 800: 101.
2. Sophos, Security Threat Report 2014. 2014.
3. Alzaabi, M. Ontology-based forensic analysis of mobile devices. *Electronics, Circuits, and Systems (ICECS), 2013 IEEE 20th International Conference on*: IEEE. 2013. 64-65.
4. Eoghan, C. Digital evidence and computer crime. *Forensic Science, Computers and the Internet*. 2000: 1-2.
5. Casey, E. *Digital evidence and computer crime: forensic science, computers and the internet*: Academic press. 2011
6. Ahmed, R. and R. V. Dharaskar. Mobile forensics: an introduction from Indian law enforcement perspective. *Information Systems, Technology and Management*. Springer. 173-184; 2009

7. Lessard, J. and G. Kessler. Android Forensics: Simplifying Cell Phone Examinations. 2010.
8. Jansen, W. A. and A. Delaitre. *Mobile forensic reference materials: A methodology and reification*: US Department of Commerce, National Institute of Standards and Technology. 2009
9. Barmpatsalou, K., D. Damopoulos, G. Kambourakis and V. Katos. A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*. 2013. 10(4): 323-349.
10. Khelalfa, H. M. Forensics Challenges for Mobile Phone Security. *Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances*. 2011: 72.
11. Hoog, A. *Android forensics: investigation, analysis and mobile security for Google Android*: Elsevier. 2011
12. McMillan, J. E. R., W. B. Glisson and M. Bromby. Investigating the increase in mobile phone evidence in criminal activities. *System Sciences (HICSS), 2013 46th Hawaii International Conference on*: IEEE. 2013. 4900-4909.
13. Chang, W. and P. Chung. Knowledge Management in Cybercrime Investigation–A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. *Intelligence and Security Informatics*. Springer. 8-17; 2014
14. Gary Kessler, R. A., Sam Brothers, Rick Mislan, NIST Mobile Forensics Workshop and Webcast. 2014, National Institute of Standards and Technology (NIST): Gaithersburg.
15. Anahita Farjamfar, M. T. A., Ramlan Mahmod and Nur Izura Udzir. A Review on Mobile Device's Digital Forensic Process Models. *Research Journal of Applied Sciences, Engineering and Technology 8(3): 358-366,*. 2014.
16. OMG. Unified Modelling Language Specification, version 1.4. version 1.4 ed.: Object Management Group. 2001.
17. Othman, S. H., G. Beydoun and V. Sugumaran. Development and validation of a Disaster Management Metamodel (DMM). *Information Processing & Management*. 2014. 50(2): 235-271.