A Framework for Preserving Data Integrity during Mobile Device Forensic in Open Source Software Environment

Ishola D. Muraina[1], Mustafa Muwafak Alobaedy[2], Huda Haji Ibrahim[3]

***Abstract* - Open Source Software has been helped in selecting the appropriate software in online towards supporting the functionality of hardware infrastructure and enhances the innovation. Forensic analysis of mobile devices can be done in an Open Source Software environment due to the availability of recourses and applications it contains. However, preventing the originality of data contents of the recovered mobile devices in the crime scene from being altered is one of the predicaments baffles the digital forensic domain. Therefore, this study presents framework to preserve integrity of data during mobile device forensic investigation with focus on Open Source Software environment. The presented framework can assist the forensic investigators to proof the reliability and consistency of gathered data from the recovered mobile devices in the crime scene.**

***Index Terms* - Data Integrity, Digital Forensic, Mobile Device Forensic, Open Source Software**

I. INTRODUCTION

Open Source Software (OSS) is the software that is developed by volunteers rather than the traditional approach of software development and freely available in online for the use of software engineers and individuals towards meeting their respective specifications. The OSS has sometimes referred to as Free or Libre as a result of autonomous practices given to the independent volunteer developers in a geographically distributed community-based form.

This OSS has helped in solving some of complex projects due to the availability of software and provided platform which act as problem solving mechanisms. Thus, OSS environment has been helped in selecting the appropriate software online to support the functionality of hardware infrastructure and enhances the innovation brings by the Information Technology [1, 22]. On the other hands, the study of Gallego et al. [2] stressed that OSS may not be freed in terms of cost, but the platform could be used to run program freely, distribute copies and updated version to the users. Besides, Roberts et al. [3] argued that many of the projects that are generally being in use today like Linux Operating Systems, Mozilla browser and the Apache web browser were developed using OSS platform. This shows that many analysis or evaluation of programs can be run using OSS platform, while forensic analysis of the mobile devices is not exempted.

Forensic is the act of investigating the crime scene and the related offences in forms of child exploitation, financial fraud, drug trafficking and homicide [4, 5]. Bringing the forensic analysis into reality has gone beyond the use of manual forms of investigations, thus require the digital approach. Over the years, digital forensic has been involved the use of computer systems, electronic devices, network level-logs and social media to execute investigation that require digital contents and evidences [5, 6] as shown in Figure 1.

[1]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok Kedah Malaysia (phone: +6 017 403 6641; e-mail: ishod@uum.edu.my)

[2]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok Kedah Malaysia

[3]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok Kedah Malaysia

 ISSN: 1813-419X

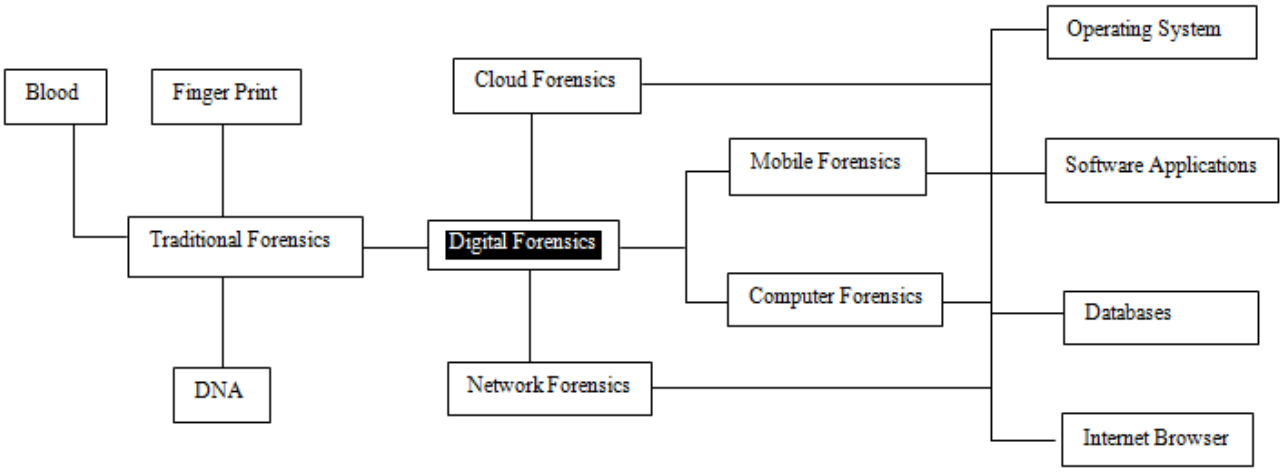

Fig. 1: Fields of Digital Forensics (Source: Lutui, R., 2016)

This shows the effectiveness of digital forensic towards obtaining the truth and avoids bias while carry out investigations in network logs and digital devices, specifically through the use of mobile devices.

Mobile devices have been individual companion in the present emerging technological world for interacting with one another, transacting businesses, transferring and sharing of information with friends and colleagues over social media sites [7]. Studies have shown that some of the smart mobile devices run operating systems that can be sourced free in the open source platform through fast internet streaming called broadband [8]. Besides, the mobile devices are capable of reading both logical and physical locations of the owner, applications in use during conversations, time, type and owner of data in use, which are useful during mobile device forensic activities.

However, studies have shown that paramount issue in mobile device forensic is preventing data alteration from its originality during forensic processes which may sometimes difficult to achieve [5]. Giving protection to the originality of data or data integrity from the mobile devices that operate with the aid of open source applications is necessary towards proofing and acceptability of the forensics' outcomes. Previous studies in the field of digital forensics have focused on the designing of model for the investigation, approach for selecting appropriate tools, threats, challenges, and future trends of mobile device forensic [7, 9, 10]. On the other hands, there has not been study that presents the framework to preserve the originality of the data from alteration during investigation. Therefore, this study presents a framework to preserve the originality of the data content of mobile device during forensic processes in OSS environment.

II. RELATED WORKS

Study has shown that forensics investigation of mobile devices is not limited to data content of mobile devices but also given the opportunity to big data analysis in terms of tracking the bearer's locations through the internet of thing (IoT) infrastructure [11]. Thus, biometric features and face recognition have been suggested to be taken into consideration while carrying out forensic activities in mobile computing platform. On the other hand, Wang [12] argued that face recognition approach in obtaining the information of the carrier of mobile devices is simply dealing with intrinsic mood of the owner of mobile devices. This implies that these metrics are impacted in preserving the data content of mobile devices.

Instant messages in the mobile devices of people under investigation could be extracted to ease forensic activities. The study of Oven and Morison [13] stressed that digital forensic provides platform to ease accessibility of deleted images in the mobile devices from the server of the providers of the application. On the other hands, researchers have emphasized that backup files specifically from the firm ware of mobile devices could be served as the best metric to obtain information needed for mobile device forensic investigators [14]. However, this approach fits recovery of data from the application that is compatible with specific embedded Operating System (OS), such as iOS. Besides, Al Mutawa et al. [15] inspected visibility of recovery data from the mobile devices using social networking applications on the mobile phone running iOS, thus the outcome shows features of social network activities inform of forensic. In a related study by Tso et al. [16] revealed that iOS inbuilt application could be used to extract information transferred between the individuals mobile devices for forensic purposes.

Furthermore, the study of Sgaras et al. [17] suggested that a Universal Forensic Extraction Device (UFED) should be used to address recovery of information being transferred between the perpetrators and the victims from the mobile

device backup server. However, gaining access to the iOS data content in the absence of owners may require backdoor attack [18], which may distort the data from its original form thereby making the outcome of the investigation skeptical. Virtually all the applications or OS used in the mobile devices are sourced freely from open source platform, and need to obtain with carefulness due to their volatility features. Hence, less or no study to the knowledge of researcher has been conducted on preventing the recovered data from the mobile device in an OSS environment from being distorted. Thus, this study presents a framework to preserve and obtain original data from the mobile devices that operate in an OSS environment during forensic investigation.

III. FRAMEWORK DEVELOPMENT

The main objective of this study is to present a framework to prevent alteration of data content of mobile device during the forensic activities in an OSS environment.

Nowadays, individual moves about with mobile phones or devices due to their usefulness in our daily activities. This is why condone-off of the crime site is necessary so as to give protection to the devices found in the scene which may help the analyst in getting the antecedents of the event. Thus, recovery of mobile devices in the crime scenes plays vital roles in gathering useful tools that may help in the forensic investigation. Meanwhile, obtaining data from the recovered mobile devices from the crime scene may be difficult due to their small sizes of memory, processor and storage compared to that of computer systems [19], thus required to be handed over to a qualified mobile device forensic investigators.

Presentation of the recovered mobile devices from the crime scenes or crime's perpetrators to the mobile device forensic investigator is necessary so as to preserve the originality of data contents of the recovered mobile devices, which could be call logs, text messages and contact lists [20]. Moreover, the fact that mobile devices contain micro parts that are difficult to handle, copying and transferring of data can be done in an OSS environment as shown in Figure 2. However, the confidentiality and integrity of data in the recovered mobile devices could be questionable since OSS environment allows independent volunteers at distributed locations to work on the available project at their convenient times.

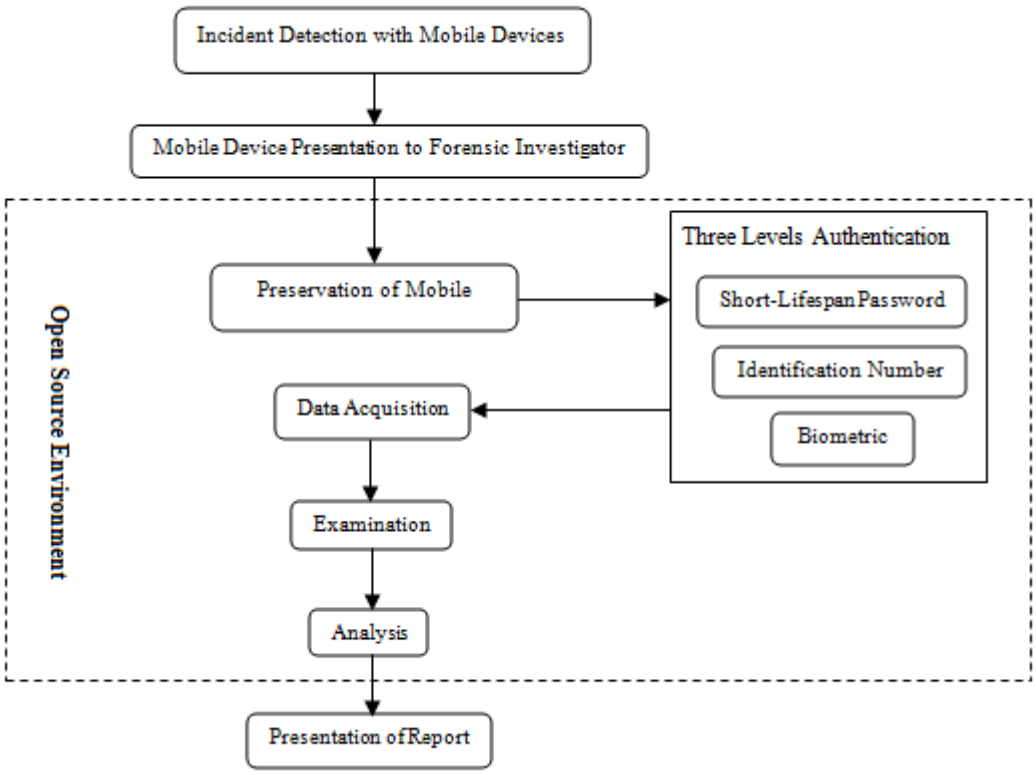

Fig. 2: Framework for Preserving Data Integrity in Open Source Software Environment during Mobile Device Forensic

Lack of adequate security in an OSS environment for forensic investigation in the context of mobile devices can jeopardize the outcome of investigation prior to presentation for the litigation processes. On the other hands, prevention of intrusion in the OSS environment could preserve integrity of data contents in the recovered mobile devices [21]. Thus, three level authentications; short-lifespan password, identification number and biometric [21] are recommended to address the integrity of embedded data contents of recovered mobile devices from the crime scene in the OSS environment. This implies that users of OSS environment for the purpose of forensics analysis of the recovered mobile devices have to obtain permission from the owner of the project prior to their intervention, using "Three Levels Authentication" as shown in Figure 2. This is to ascertain the identity and status of the players to prevent data from intrusion, thus allows data acquisition. Besides, the needed data artefacts are obtained for examination and analysis since the integrity of data of mobile devices under

investigation are guaranteed within the OSS environment with many applications. Hence, the report can be written outside the OSS environment for litigation stage.

IV. FRAMEWORK EVALUATION

The recommended framework for preserving data integrity in an OSS environment during mobile device forensic as presented in Figure 2 would be evaluated by considering the four prominent approaches of evaluation [10], such as observational, analytical, experimental and testing. All these approaches of evaluation would ensure certainty of performance of the recommended framework. Besides, certain metrics like completeness, consistency, accuracy, reliability, efficiency, effectiveness and ethicality of the presented framework as shown in Figure 2 would be measured vis-à-vis observational, analytical, experimental and testing approaches of evaluation. Hence, the result of evaluation of each of the metrics would reveal the status of the recommended framework in terms of low, medium or high.

V. CONCLUSION

Many of the investigations become inconclusive as a result of failure to use the necessary tools and approach to gather information about the event. Therefore, mobile device forensic is recommended to gather the trend of event. The OSS environment has been described as platform that allows processing and running of some programs that may be difficult to obtain their vital information in the real sense. Moreover, preserving the integrity of data content of the recovered mobile devices from the crime scene is necessary towards obtaining the exact flow of discussions or plans of the perpetrators prior to the event, and has been the bottleneck in the domain of mobile device forensic. This study has presented a framework to preserve the integrity or originality of data content of the recovered mobile devices from the crime scene with focus on OSS environment. The use of OSS platform has been claimed to be secure and providing robust applications to obtain volatile data in the electronic devices. Hence, this study would be extended in the future by implementing the presented framework using the four prominent approaches of evaluation; observational, analytical, experimental and testing.

REFERENCES

[1] Zaidan, A.A., Zaidan, B.B., Al-Haiqi, A., Kiah, M.L.M., Hussain, M., & Abdulnabi, M. (2015). Evaluating and Selection of Open-Source EMR Software Packages Based on Integrated AHP and TOPSIS. *Journal of Biomedical informatics*, Vol. 53, pp. 390-404.

[2] Gallego, M.D., Bueno, S., Racero, F.J., & Noyes, J. (2015). Open Source Software: The Effects of Training on Acceptance. *Computers in Human Behaviour*, Vol. 49, pp. 390-399.

[3] Roberts, J., Hann, I.H., & Slaughter, S. (2006). Understanding the Motivations, Participation, and Performance of Open Source Software Developers: A Longitudinal Study of the Apache Projects. *Management Science*, Vol. 52, No. 7, pp. 984-999.

[4] Hitchcock, B., Le-Khac, N.A., & Scanlon, M. (2016). Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. *Digital investigation*, Vol. 16, pp. S75-S85.

[5] Casey, E. (2010). *Hand of Digital Forensics and Investigation*. Elsevier Academic Press, pp. 3-4, Burlington MA, USA.

[6] Gupta, J.N.D., Kalaimannan, E., & Yoo, S.M. (2016). A Heuristic for Maximising Investigation Effectiveness of Digital Forensic Cases Involving Multiple Investigators. *Computer & Operations Research*, Vol. 69, pp. 1-9.

[7] Brunty, J. (2016). Mobile Device Forensics: Threats, Challenges, and Future Trends. *Digital Forensics*, pp. 69-84.

[8] Muraina, I.D., Osman, W.R.S., Ahmad, A., Ibrahim, H., & Yusof, S.A. (2016). Modeling the Behavioural Intention of Broadband Technology Usage among Teenagers: Application of UTAUT Model. *Asian Journal of Information Technology*, Vol. 15, No. 3, pp. 593-601.

[9] Saleem, S., Popov, O., & Baggili, I. (2016). A Method and a Case Study for the Selection of the Best Available Tool for Mobile Device Forensics Using Decision Analysis. *Digital Investigation*, Vol. 16, pp. S55-S64.

[10] Lutui, R. (2016). A Multidisciplinary Digital Forensic Investigation Process Model. *Business Horizons*, Vol. 59, pp. 593-604.

[11] Peoples, C., Parr, G., McClean, S., Scotney, B., & Morrow, V. (2013). Performance Evaluation of Green Data Centre Management Supporting Sustainable Growth of the Internet of Things. *Simul. Model. Pract. Theory*, Vol. 34, pp. 221–242.

[12] Wang, S. (2002). *Bionic (topological) Pattern Recognition: A New Model of Pattern Recognition Theory and Its Applications*. Chin. J. Electron. Vol. 30, No. 10, pp. 1417–1420.

[13] Oven, K.M., & Morison, G. (2016). Forensic Analysis of Kik Messenger on iOS Devices. *Digital Investigation*, Vol. 17, pp. 40-52.

[14] Husain, M., & Sridhar, R. (2010). *iForensics: Forensic Analysis of Instant Messaging on Smart Phones. In: Goel S, editor. Digital Forensics and Cyber Crime*. Vol. 31 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin Heidelberg: Springer; 2010. p. 9-18.

[15] Al Mutawa N, Baggili I, & Marrington A. (2012). Forensic Analysis of Social Networking Applications on Mobile Devices. *Digit Investig*, Vol. 9, pp. 24-33.

[16] Tso, Y.C., Wang, S.J., Huang, C.T., & Wang, W.J. (2012). iPhone Social Networking for Evidence Investigations using iTunes Forensics. *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication*. New York, NY, USA: ACM, pp. 62:1-62:7.

[17] Sgaras, C., Kechadi, M.T., & Le-Khac, N.A. (2015). *Forensics Acquisition and Analysis of Instant Messaging and Voip Applications*. In: Garain U, Shafait F, editors. Computational Forensics. Vol. 8915 of Lecture Notes in Computer Science. Springer International Publishing, pp. 188-99.

[18] Hay, A., Krill, D., Kuhar, B., & Peterson, G. (2011). *Evaluating Digital Forensic Options for the Apple ipad*. Advances in Digital Forensics VII. Vol. 361 of IFIP Advances in Information and Communication Technology. Berlin Heidelberg: Springer, pp. 257-73.

[19] Fang, J., Jiang, Z., Chow, K-P., Yiu, S-M., Hui, L., & Zhou, G., et al. (2012). *Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones*. In G. Peterson & S. Shenoi (Eds.), Advances in Digital Forensics VIII, 8th IFIP

WG 11.9, International Conference on Digital Forensics, Revised Selected Papers: Vol. 383, pp. 129-142, Heidelberg: Springer.

[20] Da-Yu, K., Shiuh-Jeng, W., Sharma, A., & Huang, F.F.Y. (2009). A Case-Oriented Model of Digital Forensics on Infected Zombie Computers. *Proceedings of the 2nd International Conference on Computer Science and Its Applications*, pp. 1-6, Piscataway, NJ: IEEE.

[21] Ahmad, M.K.A., Rosalim, R.V., Beng, L.Y., & Fun, T.S. (2010). Security Issues on Banking Systems. *International Journal of Computer Science and Information Technologies*, Vol. 1, No. 4, pp. 268-272.

[22] Muraina, I.D., & Ibrahim, H. (2016). Student's Perception to Learning of Innovative Skills through Multi-Dimensional Visualization System: Reliability and Validity Tests of Some Measurements. Proceedings of Knowledge Management International Conference (KMICe) 29-30 August, 2016, pp. 162-167.