Abstract

Window based digital forensic workflow has been the traditional investigation model for digital evidence. Investigating using Linux based platform tends challenging since there is no specific investigation workflow for Linux platform. This study designed and implemented a Linux forensic based-workflow for digital investigation. The workflow was divided into different investigation phases. The digital investigations processes in all the phases were performed using Linux riggings. The work-flow was tested and evidence such as (E01) Image was accurately acquired. This paper is presented in the following sections. Section one and two provided introduction and literature on existing forensic workflow using windows-based workflow respectively. Section three provided the approach to window workflow. The experimental design and tools used were presented in section four. The rest of the sections considered the research analysis, discussion and conclusion respectively. The implication of the test conducted, tools used with their corresponding weakness and strengths were highlighted in the appendix.

References
1. M, Ashawa, and Innocent, O. 2017. Forensic Data Extraction and Analysis of Left Artifacts on emulated Android Phones: A Case Study of Instant Messaging Applications," Seizure 19, 16.

2. Andreafortuna.org. Retrieved on October 22, 2018 from https://www.andreafortuna.org/dfir/forensic-disk-images-of-a-windows-system-my-own-workflow

3. Bird, B. Diana, H., and Mandeep, P. 2017. Professionalising the Science of Digital Forensics: Policy Logging and Auditble Record Keeping as a Life-Long Record. In European Conference on Cyber Warfare and Security, pp. 44-52.

4. countuponsecurity.com. 2018. Retrieved on September 2, 2018 from https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps.

5. Hassan, M., and Lutta, P. 2017. An investigation into the impact of rooting android device on user data integrity. In Emerging Security Technologies (EST), 2017 Seventh International Conference on, pp. 32-37.

6. Horsman, G. 2018. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. International Journal of Computers & Security, 73(5), 294-306.

7. Hintea, D., Robert, B., and James, M. 2017. An Investigation into Identifying Password Recovery and Data Retrieval in the Android Operating System", In ECCWS 2017 16th European Conference on Cyber Warfare and Security, p. 165. Academic Conferences and publishing limited.

8. Jaquet, C., David, O, Eoghan, C., Mark, P., and Pavel, G. 2018. A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence. No. 0002. OSAC/NIST.

9. Karabiyik, U., and Sudhir, A. 2016. Model of hierarchical disk investigation. In Digital Forensic and Security (ISDFS), 2016 4th International Symposium on, pp. 84-88.

10. Kigwana, I., Vícctor, R. Kebande, and Venter H. S. 2018. A proposed digital forensic investigation framework for an eGovernment structure for Uganda. In IST-Africa Week Conference (IST-Africa) on 1-8.

11. MacDermott, A. Thar, B., and Qi, S. 2018. IoT Forensics: Challenges for The IoT Era. In New Technologies, Mobility and Security (NTMS), IFIP International Conference on, pp. 1-5.

12. Montasari, R., Hill, R., Carpenter, V., & Montaseri, F. 2019. Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence. International Journal of Strategic Engineering (IJoSE), 2(1), 52-60.

13. Omeleze, S., and Hein, V. 2015. A model for access management of potential digital evidence". In International Conference on Cyber Warfare and Security, p. 491. Academic Conferences International Limited.

14. Quick, D., & Choo, K. K. R. 2018. Digital Forensic Data and Intelligence. In Big Digital Forensic Data (pp. 29-47). Springer, Singapore.

15. Roussev, V. 2016. Digital forensic science. 1st ed. pp.29-70.

16. Sachowski, J. 2018. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise. CRC Press.

17. SAN. 2018. Using Image Excerpts to Jumpstart Windows Forensic Analysis. Retrieved on December 2, 2018 from
18. Soltani, S., & Seno, S. A. H. 2017. A survey on digital evidence collection and analysis. In Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on 247-253. IEEE.

19. Sumalatha, M. R., and Pranab, B. 2016. Data collection and audit logs of digital forensics in cloud. In Recent Trends in Information Technology (ICRTIT), 2016 International Conference on, pp. 1-8.

20. Wahyudi, E., Imam, R., and Yudi, P. 2018. Virtual Machine Forensic Analysis and Recovery Method for Recovery and Analysis Digital Evidence". International Journal of Computer Science and Information Security (IJCSIS), 16(2), 1-7.

21. Wilson, R., and Hongmei, C. 2018. A framework for validating aimed mobile digital forensics evidences. In Proceedings of the ACMSE 2018 Conference, p. 17.

22. Winehq.org. 2018. Retrieved on July 03, 2018 from https://www.winehq.org.

Index Terms

Computer Science

Information Sciences

Keywords

Linux workflow, E01 image, Digital investigation, Digital Evidence