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 
/

Forensics: Policy Logging and Auditable Record Keeping as a Life-Long Record. In European 
Conference on Cyber Warfare and Security, pp. 44-52.

https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8 
-steps.

on user data integrity. In Emerging Security Technologies (EST), 2017 Seventh International 
Conference on, pp. 32-37.

framework to ensure the dependable interpretation of digital data for digital forensics. 

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.

OSAC/NIST.

Forensic and Security (ISDFS), 2016 4th International Symposium on, pp. 84-88.

investigation framework for an eGovernment structure for Uganda. In IST-Africa Week 
Conference (IST-Africa) on 1-8.

New Technologies, Mobility and Security (NTMS), IFIP International Conference on, pp. 1-5.

of Social Media, Acquisition and Analysis of Digital Evidence. International Journal of Strategic 
Engineering (IJoSE), 2(1), 52-60.

evidence". In International Conference on Cyber Warfare and Security, p. 491. Academic 
Conferences International Limited.

Forensic Data (pp. 29-47). Springer, Singapore.


Technologies to Defend the Enterprise. CRC Press.

on December 2, 2018 from


Index Terms

Computer Science Information Sciences

Keywords

Linux workflow, E01 image, Digital investigation, Digital Evidence