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.


Index Terms

Computer Science
Information Sciences

Keywords

Linux workflow, E01 image, Digital investigation, Digital Evidence