An Algorithm and Process Flow Model for The Extraction of Digital Forensic Evidence in Android Devices

Gilbert Gilibrays Ocen, Makau Stephen Mutua, Gilbert Barasa Mugeni, Simon Karume, Davis Matovu

Abstract

Abstract: The advancement in technology especially the use of mobile devices has revolutionized the way of life in the 21st century. This ranges from the way people socialize to the modes of business that take place today. Consequently, mobile devices have become very vital part of life and thus contain substantial amounts of private data. Accordingly, in event of crime and/or security investigations, these gadgets carry with them crucial evidence that when adduced before any court of law can aid in resolving a number of undetermined cases and appeals. However, mobile digital forensics research is still faced with a number of challenges. One popular challenge is seeking a standard process model to make the digital forensic evidence extraction process accurate and consistent. Earlier process models proposed, present basic steps that can be categorized as: collection, Examination, Analysis and Reporting. This has sparked significant research and proposition of numerous process models to try and explain these steps further sophisticating the problem and creating more complexity and inconsistencies, for this reason, sporadic increase in the use of mobile devices and huge volumes of data they carry that can be adduced as potential evidence in the event of dispute or court proceedings has raised the need to develop standardized extraction process models and procedures for mobile devices running android operating system, in this paper we propose an algorithm and process flow model for the extraction of digital evidence in android devices that can be adapted to the latest release of android operating system especially given the ongoing rapid changing nature of mobile device. Using this algorithm and process flow model, a procedural experiment was done on the extraction of digital evidence from an android device. The results of this experiment highlights key steps that must be followed and carefully documented during evidence extraction from mobile devices in order to ensure consistency and reduction of the complexities in early proposed models

Fulltext: ISJ Theoretical & Applied Science, 04 (72), 1-10

Link: http://t-science.org/arxivDOI/2019/04-72/PDF/04-72-1.pdf