Evaluating Factors Responsible for Inconsistencies in Mobile Devices Digital Forensic Evidence Extraction Process Model

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

Abstract

The proliferation of mobile devices has revolutionized life in the 21st century ranging from the way people socialize to the modes of doing business. Mobile devices contain substantial amounts of private data that in event of crime or security investigations when adduced before any court of law can aid in resolving a number of undetermined causes. However, mobile digital forensics research is still faced with several challenges. Most existing mobile devices digital forensic evidence extraction models are vendor-specific and thus anchored on specific device platforms such as Android, Windows, Apple iOS, and Blackberry. Additionally, these models contain various process inconsistencies and lack specified technical documentation. Further, the growing demand for mobile devices and crime-related occurrences affecting them has strained and exposed the existing models. A number of questions thus remain unanswered into the factors responsible for these inconsistencies and the lack of a unified model that can be applied across these four operating system platforms. A mixed-method approach involving a survey was used in this study where respondents were drawn from ICT practitioners, law enforcement agencies, researchers and the business community. This study highlights several factors that contribute to digital evidence extraction process model inconsistencies which include policy, extraction methods, nature of data, device type, data type, and extraction tools among others. The study proposes systematic documentation of every step followed during evidence extraction from mobile devices so as to avert the inconsistencies.