Digital forensics investigation reduction model (DIFReM) framework for Windows 10 OS

ABSTRACT

The advent of the digital age, globalization and automation has made life easier for people and businesses. However, the ubiquitous use of digital devices and the Internet also heightens the risk and incidents of cybercrimes. Under these circumstances, Digital Forensics has become a critical countermeasure. The ISO/IEC 27001 (Information security standards published jointly by the International Organization for Standardization – ISO and the International Electrotechnical Commission-IEC) provides guidance on identifying, gathering/collecting/acquiring, handling and protecting/preserving Digital Forensic evidence for use in court. The most challenging and important part of Digital Forensic Investigation (DFI) is data examination. Knowing the data created by the Operating System (OS) or user beforehand would ease the process. Unfortunately, most of the time, such details are not available to facilitate investigation. The examination phase is the most challenging for an investigator; in Microsoft Windows OS (Operating System). Investigators have to go through terabytes of system data, most of which are OS and application files irrelevant to the investigation from a suspect's computer. To address the problem highlighted above, this research proposes a data reduction model (DIFReM) and a tool which will not only help the investigator in identifying modified system files but also has the ability to detect files inserted into system directories and also be able to verify integrity using hashing. In the end, this research will provide the investigator with a more effective and efficient digital forensics tools.

Keyword: Digital forensics; Digital forensics investigation; Digital forensics models; Reduction; Windows 10