Abstract

The internet and advanced technologies have been used as tools by criminals these days to perpetrate all forms of crime and the digital world is exploited to facilitate crimes which are mostly technology driven. The evidence of such crimes which are technologically driven are in digital form hence the need to employ techniques, procedures, and methodologies that are technology inclined to reconstruct events and uncover evidence that are admissible in court. Digital forensics therefore provides the investigative techniques, scientifically derived and proven methods for preserving, collecting, validating, identifying, analyzing, interpreting and presenting admissible digital evidence derived from digital source(s). Methods used to undertake forensic investigation are paramount since inappropriate model choice may result in incomplete or missing evidence. In this paper, we look at some commonly used models, their strength and weakness to inform investigators where to appropriately use those forensic investigation model(s) as well as a proposed scheme to aid the selection of the appropriate investigative model.
References


Index Terms
Computer Science Information Sciences

Keywords
Digital Forensic Models