Abstract

Nothing epitomizes modern life better than the computer. For better or worse, computers have infiltrated every aspect of our society and for millions of people worldwide, the use of computers has become a central part of life. These advances has led to new opportunities, risks and challenges for technical and legal structures. The increase of digital crimes puts a lot of pressure on law enforcement agencies and or organizations across the globe to produce credible digital forensic evidence. This has seen a paradigm shift in the world where there is an increasing need for Digital Forensics (DF). This growth of technology has therefore produced a completely new source of evidence referred to as 'electronic evidence'. Electronic evidence is fragile and volatile by nature and therefore requires the investigator always to exercise reasonable care during its collection, preservation and analysis to protect its identity and integrity. The purpose of this research was two-fold, to investigate factors that influence digital forensic reliability, admissibility and secondly, to develop a novel digital forensic model for the next generation that will produce authentic and hence admissible e-evidence for legal proceedings. Thorough review of existing literature on digital forensics and forensic models was done and from gaps identified, a novel conceptual model towards sound forensics processes is proposed here. The findings is critical in developing as a guide in providing Digital Forensics services whether internal investigation, disciplinary hearing or court case. Recommendation is that the forensics investigators need to ensure that their evidence meets legal requirements and that their legal professionals are trained in digital forensic procedures. Establish a well-defined forensic policy that will mandate and provides guidelines for forensic investigations, establishment of a digital forensic laboratory and organizations should ensure more effort is given to digital forensics training and awareness.