ELECTRONIC EVIDENCE MANAGEMENT: ADOPTION OF STANDARD OPERATING PROCEDURES FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE IN THE UGANDAN COURTS OF LAW

A Thesis

Presented to the

Directorate of Higher Degrees and Research

Kampala International University

Kansanga, Uganda

In Partial Fulfillment of the Requirements for the

Master's Degree in Information Systems

By:

SSEMUDDU JONATHAN KALINDA

MIS/43936/143/DU

MAY, 2017
ABSTRACT

The study intended to establish the level of awareness of electronic evidence (e-evidence) management of the people entrusted with the duty of electronic crime investigations so that question of how to adopt standard operating procedures (SOPs) can be answered. The study was guided by three specific objectives; (i) to determine the operational knowledge level and awareness of SOPs in regard to electronic evidence management among e-crime investigators in Uganda (ii) to examine the current level of admissibility of e-evidence in Ugandan courts of law presented by e-crime investigators and (iii) to establish how internationally accepted e-evidence management SOPs may be adopted as standard operating procedures in Uganda for admissibility of e-evidence in Ugandan courts of law? The study comprised of a target population of 55 respondents from which the sample size of 48 was arrived at using Solven’s formula of Sampling. The study was based on sampling techniques; Multistage sampling in which the researcher started with organizations in Uganda that are majoring in electronic evidence management; Cyber crime unit, Directorate of forensic services, Directorate of investigations of the Uganda Police Force, NITA-Uganda, URA, GAL, UCC and Private forensics labs. The data collection instruments were basically self-administered questionnaires, which comprised of open and closed-ended questions, interview guide and analysis of journals. The following respondents were approached; Scenes of Crime Officers (SOCOs), Technical staff, Electronic evidence analysts, Investigators, Common police officers and private investigators with e-evidence exposure. 48.6 of the respondents were less exposed to e-evidence management for a period of 0 to 3 years where as 12 years and above of exposure to e-evidence management were the minority with 2.7 percent of the total respondents. 54.1 percent of the respondents confirmed that non qualified staff always responds to crime scenes which is detrimental to electronic evidence management. However, it was evident that the respondents in the organizations visited by the researcher were theoretically exposed to foreign SOPs without adopting their own. Research described measures to be undertaken if adoption is to of SOPs is to take place, equip forensic labs with routine upgrades, train their staff and the field response teams like SOCOs among others, and to have a memorandum of understanding among different organizations involved, and with other foreign countries so that there is partnership in recovering e-evidence from those countries where perpetrators could hide or commit cyber crimes.