Chapter 5
Evolution of Digital Evidence in Uganda: A Records Management Perspective

David Luyombya
https://orcid.org/0000-0002-2156-7386
Makerere University, Kampala, Uganda

Sylvia Namujuzi
https://orcid.org/0000-0003-3806-407X
Makerere University, Kampala, Uganda

Francis Ssekitto
https://orcid.org/0000-0001-8027-3794
Makerere University, Kampala, Uganda

ABSTRACT

This chapter explores the evolution of digital evidence in Uganda's judicial system, highlighting the shift from traditional paper-based to digital records. It reviews key literature that informed legal reforms establishing the framework for admitting and managing digital evidence, marking a digital evidence revolution in Uganda. The chapter examines how courts interpret laws to tackle challenges unique to digital data, noting benefits like greater efficiency and accuracy in judicial processes. It also discusses ongoing challenges and gaps in digital evidence management. Emerging trends emphasize sustainable digital records management practices to ensure long-term reliability and authenticity in court proceedings. The study stresses embedding digital records management within legal frameworks to secure evidence

DOI: 10.4018/979-8-3373-3023-5.ch005

integrity and admissibility. Ultimately, proactive integration of digital features helps organizations address security, legal, and regulatory concerns, safeguarding the credibility of digital evidence in Uganda's judicial system.

1.0 INTRODUCTION AND CONTEXTUAL BACKGROUND

The term digital evidence describes digitally stored or transmitted transaction that can be used as proof in court, during an investigation or to guide business choices (Law Dictionary, 2021). Strong legal positions, improved operational performance and reputation of the organization and compliance with stringent legal rules are only a few benefit of effective digital evidence management (Illési, 2025). On the other hand, poor evidence management can have detrimental effects on operations, reputation, legal penalties, and defense in court (Lee & Oh, 2021). Computer data, such as emails, electronic documents, computer traceability logs, and data from mobile devices, such as GPS and text messages, cloud storage, social media posts, network devices, and even Internet of Things (IoT) devices, are all considered forms of digital evidence (Munyika & Schellnack-Kelly, 2024). Digital evidence also includes digital audio and video recordings (Youn, 2019).

Unlike physical evidence, digital evidence is highly unstable, easily altered, deleted, and corrupted if not handled with extreme care (McLeod & Lomas, 2023). As a result, preserving its validity and integrity is decisive to its dependability and admissibility in legal proceedings as legitimate when it is used as evidence (Mukiibi, 2023). For digital records to be considered authentic and intact, the evidence must match the original record and not have been tampered with or altered (ISO15489, 2016). Though the international standard (ISO15489, 2016) does not specifically define "digital evidence", it establishes the principles and requirements for managing digital evidence, so that it can be considered a reliable and authentic record and thus serve as valid evidence.

The management of digital evidence is a key focus in contemporary records management, primarily because of the rapid development of digital technologies and its growing significance in the legal landscape. An unprecedented challenge is presented by the sheer volume of records created every day by businesses at all levels, both public and private, from emails and social media to Internet of Things devices and cloud apps, and whether the evidence or information will be accepted by a court (Ngoepe, Mukwevho, & Mosweu, 2022). Mahlangu and Ruhode (2020) explain that because digital records come in a variety of formats, including text, audio, video, pictures, and databases, each type has distinct qualities and presents particular challenges for its production, accessibility, and preservation in order to meet legal requirements and be recognised as legitimate. The premise that digital