

Design and Development of an Integrated Web-Based System for Managing Digital Evidence in Cybercrime Investigations

Simon Moonga¹

¹Department of Information and Communications Technology, School of Engineering, Information and Communications University, Lusaka, Zambia

ARTICLE INFORMATION	ABSTRACT
Article history: Published: October 2026 Keywords: Digital Evidence Management System Cybercrime Investigation Web-Based System Digital Forensics Web-Based System	The increasing prevalence and sophistication of cybercrime have generated a growing volume of digital evidence from computers, mobile devices, networks, and cloud platforms. Effective management of such evidence is critical for ensuring its integrity, authenticity, confidentiality, and admissibility in legal proceedings. However, many investigative environments, particularly in developing countries, continue to rely on fragmented, manual, or paper-based approaches, resulting in weak chain-of-custody documentation, limited traceability, and elevated risks of evidence tampering or loss. This study designed and developed an Integrated Web-Based Digital Evidence Management System (DEMS) to centralize evidence registration, secure storage, chain-of-custody tracking, role-based access control, audit logging, and reporting. The system was developed using PHP, MySQL, JavaScript, HTML, and CSS, following the Waterfall software development lifecycle. A mixed-methods approach was adopted, comprising a baseline survey of 30 stakeholders (67% response rate) and system evaluation through simulated cybercrime scenarios. The implemented system demonstrated reliable functionality, secure hash-based evidence integrity verification (SHA-256), tamper-evident audit trails, and an intuitive user interface. The study concludes that a locally adaptable, low-cost, open-source DEMS can significantly strengthen investigative efficiency, accountability, and the legal admissibility of digital evidence in resource-constrained jurisdictions. Recommendations for future work include integration with external forensic tools, multi-factor authentication, blockchain-based integrity verification, and mobile application support.

1. Introduction

The rapid growth of digital technologies has increased both digital connectivity and cybercrime, making digital evidence an essential component of modern cybercrime investigations. Digital evidence can be easily altered, deleted, or compromised, requiring secure and systematic management to maintain its integrity, authenticity, and chain of custody (NII, 2018; Casey, 2011). According to the Cybersecurity Ventures Report (2022), global cybercrime costs are projected to reach USD 10.5 trillion annually by 2025, underscoring the urgent need for robust investigative and forensic mechanisms.

In many developing countries, cybercrime investigations are still handled using manual or paper-based evidence management systems. These are prone to evidence loss, manipulation, unauthorized access, and inefficiencies in communication between investigative stakeholders (Karie, Venter & Olivier, 2015). The United Nations Office on Drugs and Crime (UNODC) emphasizes that chain-of-custody records must document who collected, possessed, transferred, and handled evidence throughout its lifecycle. INTERPOL reported that only 29% of surveyed African countries had a digital evidence repository, citing limitations in infrastructure, specialized tools, training, and investigative capacity.

This study addresses this gap by designing and developing an integrated web-based system for managing digital evidence in cybercrime investigations. The system provides centralized mechanisms for evidence registration, secure storage, chain-of-custody tracking, access control, audit logging, and reporting.

1.1 Research Objectives

The general objective was to design and develop an integrated web-based system for secure, efficient, and systematic management of digital evidence throughout the cybercrime investigation lifecycle. The specific objectives were:

- To design a web-based platform that allows secure uploading, classification, and storage of digital evidence in cybercrime investigations.
- To implement features that ensure the integrity and chain of custody of digital evidence through access control, audit logs, and hash verification.
- To evaluate the usability and effectiveness of the developed system using simulated cybercrime scenarios and feedback from potential end-users.

1.2 Research Questions

- How can a web-based system be designed to securely upload and store digital evidence for cybercrime investigations?
- What mechanisms can be incorporated to ensure the integrity and maintain the chain of custody of digital evidence within the system?
- How effective and user-friendly is the developed DEMS in supporting cybercrime investigations?

1.3 Significance of the Study

This study holds significant value in the ongoing fight against cybercrime by addressing one of the most critical aspects of digital investigations: evidence management. The development of a secure and web-based DEMS will provide law enforcement agencies, forensic experts, and judicial officers with a centralized platform to store, access, and manage digital evidence with accountability and integrity. The system ensures that digital evidence is handled in a manner that meets legal and forensic standards, thereby enhancing the credibility and admissibility of evidence in court.

2. Literature Review

Digital forensics involves the identification, acquisition, preservation, examination, analysis, and reporting of digital evidence using appropriate forensic procedures (NIST, 2006). Digital evidence is volatile and can be easily altered if not handled appropriately, necessitating strict procedures to maintain integrity (UNODC, 2024; INTERPOL, 2021).

Chain of custody is fundamental to evidence handling, documenting collection, storage, access, transfer, and handling throughout the evidence lifecycle (UNODC, 2024). The reliability and admissibility of digital evidence depend heavily on the integrity of this chain (US DOJ, 2004; Rogers, 2006). Several DEMS solutions exist globally, including the FBI's Digital Evidence Management System and INTERPOL's ICSE database (FBI, 2021; INTERPOL, 2022). However, these systems are often proprietary, expensive, and not adaptable to local legal and institutional frameworks in resource-limited settings. Web-based platforms in digital forensics offer accessibility, scalability, and centralized control (Garfinkel, 2010). However, cloud-based approaches introduce security and privacy challenges such as data breaches, unauthorized access, and jurisdictional conflicts (Zawoad & Hasan, 2015).

2.1 Gaps in the Literature

The review identified several gaps:

Limited accessibility and localization – Most existing DEMS are developed for well-resourced institutions and do not address infrastructural, legal, or procedural challenges in developing nations (Karie & Venter, 2015).

High implementation and maintenance costs – Proprietary platforms exclude smaller law enforcement units operating under limited budgets (Quick & Choo, 2013).

Lack of integration with other forensic tools – Minimal integration between evidence management systems and forensic tools such as disk imaging or hashing software (Garfinkel, 2010).

Weak support for chain-of-custody automation – Many systems lack real-time logging, audit trails, or automated chain-of-custody tracking (Rogers, 2006; Zawoad & Hasan, 2015).

Security and privacy concerns – Underexplored security controls for safeguarding sensitive digital evidence in transit and at rest (Zhou et al., 2011).

Limited end-user usability – Scarce research addressing usability for non-technical personnel (Casey, 2011).

Scarcity of empirical evaluations – Most studies stop at the conceptual or design phase without real-world pilot testing (Karie et al., 2017).

2.2 Conceptual Framework

The conceptual framework outlines the flow from cybercrime incident through digital evidence identification, acquisition, hashing, and secure upload into the web-based DEMS platform. The platform encompasses chain-of-custody logs, role-based access, an evidence metadata database, and a reporting module, culminating in analysis by the forensic team and presentation in court.

3. Methodology

A mixed-methods approach was adopted, combining qualitative and quantitative data to provide comprehensive insights into user requirements, system functionality, and effectiveness. The Waterfall software development lifecycle (SDLC) model guided the systematic development and implementation of the solution.

3.2 Baseline Study and Data Collection

The baseline study assessed existing methods, tools, and challenges associated with digital evidence management. Interviews and questionnaires were administered to key stakeholders, including law enforcement officers, digital forensic analysts, and IT security professionals. Out of 30 questionnaires administered, 20 were successfully filled and returned, representing a 67% response rate.

3.3 System Development

The system was developed using:

Front-end: HTML5, CSS3, JavaScript, Bootstrap

Back-end: PHP

Database: MySQL

Security: SHA-256 hashing, HTTPS/SSL, input sanitization, session management

The system follows a three-tier architecture:

Presentation layer – User interface for investigators, forensic analysts, and administrators.

Application layer – PHP-based business logic, authentication, access control, and evidence processing.

Data layer – MySQL for structured data and secure file system for evidence storage.

3.4 System Requirements

Table 1: Minimum Hardware Requirements

Hardware	Minimum Requirement
Processor speed	1.6 GHz or 1.3 GHz
Memory	2 GB RAM

RESEARCH ARTICLE

Disk Space (user PC)	5 GB
Bandwidth	1 Mbps
Disk space (server)	50 GB

Source: Research Data, 2025

Table 2: Minimum Software Requirements

SoftwareMinimum	Requirement
Operating System	Windows Mac OS iOS Android
DBMS	MySQL
Browser Chrome	Firefox Edge Opera

Source: Research Data, 2025

3.5 Database Design

The entity-relationship diagram shows the core entities: Users, Cases, Evidence, Chain_of_Custody, Comments, and Logs. Key fields include:

Users: user_id (PK), name, email, password hash, role, created_at

Cases: case_id (PK), title, description, status, created_by, date_opened, date_closed

Evidence: evidence_id (PK), case_id (FK), uploaded_by, file_path, file_name, hash_value, upload_date, description

Chain_of_Custody: custody_id (PK), evidence_id (FK), handled_by, action_type, timestamp, notes

Logs: log_id (PK), user_id (FK), action, target_table, target_id, timestamp

4. Findings

4.1 Baseline Study Results

The survey achieved a 67% response rate. Key demographic findings:

Table 3: Age Distribution of Respondents

Age Range	Percentage (%)
Above 50	26.9
46–50	24.8
41–45	22.5
36–40	16.3
32–35	15.5
Below 30	3

Source: Research Data, 2025

Table 4: Education Level of Respondents

Education Level	Percentage (%)
Diploma	20
Bachelor's Degree	39
Master's Degree	26.4
PhD	14.6

Source: Research Data, 2025

Field data shows that about 80% of respondents were literate at different levels of education from Diploma level to PhD level. This implies that the majority of respondents interviewed have the necessary information on digital evidence management practices.

4.2 System Implementation Results

The system was successfully implemented with the following modules:

- User Account Management – Role-based authentication and authorization distinguishing administrators, investigators, and forensic analysts.
- Case Registration and Assignment – Investigators can create cases with case number, title, description, and assign to personnel.
- Evidence Upload and Tagging – Secure upload with automatic timestamping and metadata tagging (hash values, uploader identity, case association).
- Chain of Custody Tracking – Every interaction with evidence is logged, establishing a tamper-evident chain of custody.
- Search and Retrieval – Efficient search by keywords, case IDs, dates, and evidence types.
- Audit Logs and Reports – System logs capture user activities and evidence handling history; automated reports support case documentation.
- Security and Access Control – HTTPS enforcement, database encryption, input validation, and session management.

4.3 Discussion of Findings

The findings demonstrate that the DEMS effectively addresses the research objectives:

- Improved Evidence Handling and Chain of Custody – End-to-end tracking from acquisition to closure, maintaining verifiable chain of custody.
- Role-Based Access Control (RBAC) – Sensitive data accessible only to authorized personnel, supporting privacy and data segregation.
- Efficient Case Management – Centralized storage and linking of evidence to specific investigations, minimizing fragmentation.
- System Usability – Intuitive interface with dashboard summaries, evidence logs, and responsive design.
- Security and Integrity – SHA-256 hashing verified evidence integrity, essential for legal admissibility.
- Real-Time Collaboration – Web-based architecture enabled remote access and collaboration across jurisdictions.

- Limitations in Integration – Limited integration with external forensic tools (e.g., FTK, EnCase), providing a foundation for future API-based extensions.

4.4 Challenges and Limitations

- Limited integration with external forensic tools – System functions primarily as a repository and management interface.
- Network dependency and latency issues – Web-based access requires stable connectivity.
- Data storage constraints – High-resolution evidence places significant demand on server resources.
- User authentication and security – Advanced features such as MFA and intrusion detection were not fully developed.
- Legal and jurisdictional considerations – Country-specific laws and chain-of-custody documentation formats not yet incorporated.
- Limited user feedback – Small participant group due to time constraints and restricted access to law enforcement personnel.
- Lack of offline capability – Field investigations with poor connectivity cannot use the system until reconnected.

5. Conclusion and Recommendations

5.1 Conclusion

The development of the Web-Based Digital Evidence Management System marks a significant advancement in handling, storing, and coordinating digital evidence in cybercrime investigations. The system successfully addresses the growing challenges faced by law enforcement and forensic analysts in managing increasing volumes of digital evidence with integrity, security, and accountability. Through systems engineering principles and web-based technologies, a functional and user-friendly platform was designed, implemented, and tested. The DEMS platform facilitates streamlined evidence intake, case tracking, chain-of-custody management, and secure access control, demonstrating how digital tools can reinforce investigation reliability, reduce tampering risks, and promote inter-agency collaboration. The study achieves its objectives by presenting a viable solution to the real-world problem of digital evidence mismanagement. It not only contributes to academic knowledge in the field of digital forensics and information systems but also provides a scalable model that can be adopted and further enhanced by law enforcement agencies and cybersecurity institutions.

5.2 Recommendations

Based on the findings and challenges identified, the following recommendations are made for future work:

- Integration with law enforcement databases – Enable real-time evidence sharing and automated background checks across jurisdictions.
- Mobile application support – Allow field officers to upload evidence directly from crime scenes using smartphones or tablets.
- Advanced forensic analytics – Incorporate AI-driven tools for automatic evidence classification, pattern recognition, and anomaly detection.
- Blockchain integration – Enhance integrity and tamper-evidence of the chain of custody through decentralized ledger technology.
- User training and usability testing – Conduct extensive training and usability studies, particularly for non-technical law enforcement personnel.
- Compliance with international standards – Align with ISO/IEC 27037 and 27043 for global applicability and legal admissibility.
- Multi-factor authentication and intrusion detection – Strengthen security against unauthorized access and insider threats.

References

- [1] M. Mupeta, S. Tembo, and L. Phiri, "A transformer-based natural language processing framework for cyber threat detection and intelligence from dark web forums and marketplaces," *African Journal of Artificial Intelligence and Cyber Defence*, Aug. 2026, doi: 10.5281/zenodo.21848806.
- [2] M. Mupeta, S. Tembo, and L. Phiri, "Linguistic patterns of cybercriminal communication in dark web forums using transformer-based natural language processing," *African Journal of Artificial Intelligence and Cyber Defence*, Aug. 2026, doi: 10.5281/zenodo.21818782.
- [3] M. Mupeta, "Assessment of Wilses Darknet Scanner: An AI-powered solution for proactive identity protection," *International Journal of Advances in Engineering and Management*, vol. 6, no. 9, pp. 717–722, Sep. 2024, doi: 10.35629/5252-0609717722
- [4] Casey, D. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.
- [5] Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.
- [6] Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1–12.
- [7] NIST. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (NIST SP 800-86). National Institute of Standards and Technology.
- [8] Kohn, M., Eloff, M., & Eloff, J.H.P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103–115.
- [9] ISO/IEC 27037:2012. (2012). *Information Technology — Guidelines for Digital Evidence*. International Organization for Standardization.
- [10] Sammons, J. (2014). *The Basics of Digital Forensics* (2nd ed.). Syngress.
- [11] Lillis, T. (2020). Digital evidence management systems in law enforcement. *Journal of Law & Technology*, 28(2), 112–125.
- [12] Rogers, M. (2004). The role of criminal profiling in the computer forensics process. *Digital Investigation*, 1(4), 233–237.
- [13] Yen, H., & Chang, F. (2004). A framework for digital evidence management. In *Proceedings of the International Conference on Cyberworlds* (pp. 357–364). Tokyo.
- [14] Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Elsevier.
- [15] Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics* (NIST SP 800-101 Rev. 1). National Institute of Standards and Technology.
- [16] SANS Institute. (2010). *Computer Forensics: Digital Evidence in the Courtroom* (White Paper).
- [17] Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to Computer Forensics and Investigations*. Cengage Learning.
- [18] Agarwal, R., & Dhar, R. (2012). Digital forensics: An overview. *IJCSIT*, 3(1), 242–247.

- [19] Dardick, H. (2007). Forensic data recovery from flash memory. *Small Scale Digital Device Forensics Journal*, 1(1), 1–17.
- [20] Baggili, J., Mislan, R., & Rogers, M. (2006). Mobile phone forensics: What data can be extracted and how? *Journal of Digital Forensics, Security and Law*, 1(1), 35–50.
- [21] Palmer, G. (2001). A Road Map for Digital Forensic Research. *Digital Forensic Research Workshop*.
- [22] Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. *Communications of the ACM*, 49(2), 63–66.
- [23] Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73.
- [24] Zawoad, B., & Hasan, R. (2013). Cloud forensics: A meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv:1302.6312*.
- [25] ENISA. (2012). *Cyber Crisis Cooperation and Management (Tech. Rep.)*. European Network and Information Security Agency.
- [26] Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing (NIST Special Publication 800-145)*.
- [27] Stallings, W. (2017). *Network Security Essentials: Applications and Standards (6th ed.)*. Pearson.
- [28] UNODC. (2024). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.
- [29] INTERPOL. (2021). *Global Guidelines for Digital Forensics*. INTERPOL.
- [30] Cybersecurity Ventures. (2022). *Cybercrime Report*.
- [31] Karie, Venter & Olivier. (2015). Digital forensic readiness in developing countries. *Journal of Digital Forensics*.
- [32] Quick & Choo. (2013). Digital forensic intelligence. *Computers & Security*.
- [33] Zhou et al. (2011). Security and privacy in cloud forensics. *Journal of Information Security*.