 DOI: 10.5281/zenodo.17795962

Title

DIGITAL FORENSIC TOOLKIT FOR MALAWI LAW ENFORCEMENT - AFRIRESEARCH

Author

FAITH SONKHO

Co-Author

MR. JOEL MULEPA

Issue November 2025

Certificate AR2025IVA60

 DOI: 10.5281/zenodo.17795962

ABSTRACT

With the increasing prevalence of cybercrime in Malawi, law enforcement agencies face significant challenges in effectively investigating digital incidents. Traditional investigative methods are no longer sufficient to address the growing complexity of cybercrimes involving mobile phones, computers, and cloud-based systems. This project aims to develop a comprehensive digital forensics toolkit designed to assist Malawian police and investigative units in the collection, analysis, and reporting of digital evidence. The toolkit will facilitate the extraction and examination of critical data such as deleted messages, browsing histories, multimedia files, and system logs to support the identification and prosecution of offenders.

The research employs a design science methodology, involving requirement analysis with local law enforcement, prototype development, and iterative testing. Key components of the toolkit include modules for computer forensics, mobile device forensics, and cloud data analysis. Each module is tailored to operate within Malawi's legal and technical environment, ensuring compliance with evidence-handling procedures and regional legislation. The system is further designed for usability and accessibility, incorporating user-friendly interfaces, offline functionality, and compatibility with commonly used devices and file formats in Malawi.

Major challenges addressed include limited forensic infrastructure, a shortage of skilled digital investigators, and the rapid evolution of cyber threats. The proposed solution mitigates these issues by providing scalable, adaptable, and resource-efficient tools suitable for both urban and rural contexts. Expected outcomes include enhanced investigative capabilities, improved accuracy in digital evidence management, and strengthened capacity for cybercrime response.

Ultimately, this project contributes to the modernization of digital forensics practices in Malawi, supporting the broader goal of building a resilient and technologically capable law enforcement system. By integrating innovation, practicality, and legal compliance, the toolkit represents a critical step toward improving the nation's digital security landscape.

Keywords: Digital Forensics, Cybercrime Investigation, Law Enforcement, Mobile and Computer Forensics, Evidence Analysis Toolkit, Malawi.

INTRODUCTION

Background

The growth of digital technology has revolutionized how individuals, organizations, and governments communicate and conduct business. The widespread use of computers, smartphones, and the internet has introduced new levels of convenience and efficiency but has also created opportunities for criminal activity in the digital space. Cybercrime has become a serious global concern,

encompassing activities such as online fraud, identity theft, unauthorized access to systems, and the distribution of malicious software. These crimes often leave behind digital traces that can serve as vital evidence for criminal investigations. However, identifying, preserving, and analyzing such evidence requires specialized tools and expertise.

In Malawi, the increasing adoption of digital services and online transactions has led to a corresponding rise in cyber-related offenses. Law enforcement agencies now face the challenge of investigating crimes that involve digital devices and online platforms. Unfortunately, traditional investigation methods are not effective in handling digital evidence, which is fragile, easily alterable, and requires technical skill to recover and interpret correctly. Without modern forensic tools, investigators often struggle to collect and present credible evidence in court.

Context

As Malawi continues its digital transformation journey, the country's dependence on technology for communication, banking, education, and governance has increased significantly. This digital expansion, while beneficial, has also created new vulnerabilities that cybercriminals exploit. Reports of online scams, unauthorized access to systems, data theft, and social media–related crimes are rising. Law enforcement agencies are under growing pressure to respond effectively to these emerging threats. However, their efforts are hindered by several key challenges, including a lack of digital forensic laboratories, limited technical skills among investigators, and insufficient access to appropriate investigative toolMost of the digital forensic tools currently in use are foreign-developed and not tailored to the Malawian context. They often require advanced technical knowledge, continuous internet connectivity, and expensive licensing fees — factors that limit their practical use in many local investigations. Moreover, existing legal frameworks.

To address these challenges, there is a need to develop a localized digital forensics toolkit that is practical, affordable, and aligned with Malawi's law enforcement environment. Such a toolkit should enable investigators to extract, analyze, and report digital evidence from multiple devices, including mobile phones and computers, while ensuring compliance with national laws and international forensic standards. The solution should also consider operational realities such as limited internet access, the need for offline functionality, and support for commonly used devices and platforms in Malawi.

Research Objectives

The main aim of this study is to develop a digital forensics toolkit that enhances the ability of Malawian law enforcement agencies to investigate cybercrime incidents effectively and efficiently.

The specific objectives of the research are to:

- Assess the current challenges,

capabilities, and needs of digital forensics within Malawi's law enforcement sector.

- Design and develop a modular, user-friendly digital forensics toolkit capable of handling evidence from computers, mobile devices, and cloud systems.
- Ensure compliance with Malawi's legal frameworks and international standards on digital evidence collection, analysis, and reporting.
- Support capacity building by introducing tools and documentation that enhance training and knowledge sharing among investigators.

By achieving these objectives, the project aims to strengthen Malawi's digital investigation capacity, promote effective cybercrime management, and contribute to the modernization of the country's justice system. The successful implementation of this toolkit will not only improve law enforcement efficiency but also ensure that digital evidence is collected, analyzed, and preserved in a manner that upholds both technical and legal integrity.

LITERATURE REVIEW

The literature review for the Digital Forensics Toolkit for Malawian Law Enforcement project highlights the growing need for digital forensic capabilities due to the rise in cybercrime and digital evidence in Malawi. It examines existing digital forensics tools both commercial and open-source evaluating their suitability in low-resource settings. The review identifies challenges such as limited technical expertise, lack of infrastructure, and insufficient legal support. It concludes that Malawi's law enforcement agencies need a cost-effective, easy-to-use, and legally compliant digital forensics toolkit, supported by local training and policy development.

In *2021 Suleman, M., Qureshi, M. R. N., & Yamin, M* explored the Challenges of Digital Forensics in Developing Countries that most forensic tools are developed for technologically advanced countries, making them unsuitable for Malawi's infrastructure. Many assume access to high-speed internet, advanced cybersecurity frameworks, and global cyber intelligence databases.

In *2020 Mutemwa W*. explored about the Role of Digital Evidence in Malawian Courts Malawi's legal framework for cybercrime and digital evidence is still evolving. Challenges related to evidence admissibility, proper handling of digital artifacts, and compliance with international standards hinder effective forensic investigations. Without clear cybercrime laws and forensic guidelines, law enforcement officers may face difficulties in securing convictions based on digital evidence.

In *2015 Katos V. & Patel A.* explore the Framework for Cyber Forensics Training that the Role of Digital Evidence in Malawian Courts that digital forensics requires specialized skills in data extraction, evidence handling, and forensic reporting. However, Malawi has a limited number of trained forensic professionals. A study highlights the

global shortage of digital forensics expertise, particularly in developing nations. Without trained personnel, law enforcement agencies struggle to use sophisticated forensic tools effectively.

Prior to Digital Evidence and Computer Crimes, in *2021 Casey E.* Explore that Digital forensics is a branch of forensic science that involves the systematic recovery, analysis, and documentation of digital evidence for use in criminal investigations and legal proceedings. It plays a critical role in solving crimes such as cyber fraud, hacking, online harassment, and terrorism-related activiti1.4.5 Prior to Cyber Security Awareness and Challenges in Africa, in *2009 Dlaminin M.*

T Eloff, J. H. P., & Eloff, M. explore that Malawi is experiencing an increase in cyber-enabled crimes such as online fraud, phishing attacks, and data breaches. However, many existing forensic tools are not designed to handle localized cyber threats, limiting their effectiveness in the Malawian context.

The Design Science Research (DSR) methodology is increasingly used in information systems research to create and evaluate technological artifacts that address identified problems (*Hevner et al., 2004*). In the context of digital forensics, DSR supports the development of tools that are not only technically functional but also practical and aligned with organizational and legal contexts. By engaging end-users—such as law enforcement officers—in iterative design and testing, the resulting systems are more usable and effective. The proposed digital forensics toolkit for Malawi employs DSR to ensure that the solution addresses local technical, legal, and operational constraints.

The proliferation of smartphones and cloud computing introduces new layers of complexity in digital investigations. Mobile forensics involves retrieving data such as call logs, messages, location data, and app activity from mobile devices, which are often encrypted or password- protected (*Alghafli et al., 2019*). Cloud forensics, on the other hand, deals with data stored on remote servers, raising jurisdictional and data access challenges (*Ruan et al., 2018*). Existing tools often struggle with interoperability and lack mechanisms to ensure the privacy and legality of cross-border data collection. For Malawi, where mobile phone usage exceeds 60% of the population (MACRA, 2024), an integrated approach combining mobile and cloud forensics is vital.

Several commercial and open-source tools have been developed to support digital forensics investigations. Popular platforms include EnCase, FTK (Forensic Toolkit), Autopsy, Cellebrite UFED, and XRY (*Al Fahdi et al., 2016*). These tools provide functionalities such as disk imaging, file recovery, metadata extraction, and network traffic analysis. However, most of these systems are resource-intensive, expensive, and tailored for technologically advanced environments. Open- source solutions such as Autopsy and CAINE offer flexibility but often require significant technical expertise to operate effectively (*Quick & Choo, 2018*). For

developing contexts like Malawi, these limitations pose significant barriers to adoption due to budget constraints, low bandwidth, and lack of specialized training.

The rapid advancement of information and communication technologies (ICTs) has revolutionized modern society but has also led to a surge in cybercrime. Globally, cybercrime encompasses offenses such as identity theft, financial fraud, ransomware attacks, data breaches, and online harassment (*Symantec, 2022*). In Africa, increasing internet penetration and mobile money adoption have made digital platforms attractive targets for cybercriminals (*Interpol, 2023*). Malawi, like many developing nations, has witnessed a significant rise in digital crimes, including mobile money fraud, phishing, and unauthorized access to information systems (*Malawi Police Service, 2022*). However, the country's response capacity remains limited due to inadequate infrastructure, lack of expertise, and insufficient policy frameworks.

Digital forensics refers to the systematic process of identifying, preserving, analyzing, and presenting digital evidence in a manner admissible in court (*Casey, 2019*). It plays a crucial role in cybercrime investigations, enabling law enforcement to reconstruct events, identify perpetrators, and substantiate legal claims. The digital forensics process typically involves evidence acquisition, preservation, analysis, and reporting (*NIST, 2020*). Effective forensic investigations require specialized tools capable of handling data from various sources such as computers, mobile devices, and cloud environments. Adherence to principles of data integrity, chain of custody, and legal admissibility is essential to maintain evidential credibility.

METHODOLOGY

Research Design

The study adopted a Design Science Research (DSR) approach, which is well-suited for information systems research focusing on the creation and evaluation of technological artifacts. Design Science emphasizes the design, development, and assessment of innovative solutions that address real-world problems (Hevner et al., 2004). In this research, the artifact is the Digital Forensic Toolkit, designed to meet the operational and legal requirements of Malawian law enforcement.

The DSR approach was chosen because it integrates both theoretical inquiry and practical development, enabling the researcher to iteratively design, test, and refine the toolkit in collaboration with end-users. The research process followed the typical DSR cycle, which includes the following stages:

Problem Identification and Motivation

Understanding the growing challenge of cybercrime in Malawi and the limitations of existing digital forensics infrastructure.

Objectives of the Solution

Establishing clear system objectives to guide the design and ensure alignment with user needs.

Design and Development

Building a prototype of the forensic toolkit with modular components and features.

Demonstration and Evaluation

Testing the prototype in controlled

environments with real or simulated

data. Communication

Documenting results, sharing findings, and providing recommendations for deployment and future improvement.

Research Methodology

The Agile Software Development Methodology was employed during the system development phase. Agile is a flexible and iterative approach that promotes adaptability, user collaboration, and incremental progress (Beck et al., 2001). This methodology was chosen because it allows the system to evolve based on continuous feedback from investigators, forensic analysts, and law enforcement officers.

The development process was divided into sprints, each lasting approximately two to three weeks. Each sprint focused on specific functional modules of the system and concluded with a review session where feedback was gathered and adjustments were made. This iterative cycle ensured continuous improvement and responsiveness to user requirements.

Requirements Gathering and Analysis

The requirements gathering phase was critical to ensuring that the system addressed real operational needs. Data was collected from law enforcement officers, digital forensic analysts, and technical personnel through semi-structured interviews, questionnaires, and document analysis.

a) Interviews

Interviews were conducted with officers from the Malawi Police Service's Cybercrime Unit and representatives fthe Malawi Communications Regulatory Authority (MACRA). The interviews sought to understand existing investigative workflows, challenges in digital evidence handling, and system expectations.

b) Questionnaires

Structured questionnaires were distributed to potential users to gather quantitative data on system needs, usability preferences, and functional priorities.

c) Document Review

Existing policies, cybercrime legislation, and evidence-handling procedures were analyzed to ensure that the system design aligns with Malawian legal frameworks and international forensic standards.

The findings from these data collection activities were used to define both functional requirements (e.g., case management, evidence tracking, report generation) and non-functional requirements (e.g., usability, security, offline functionality).

System Design and Architecture

Based on the analyzed requirements, the system was designed as a modular architecture consisting of several integrated components:

Authentication and Access Control Module: Ensures secure login and role-based access for investigators.

Case Management Module: Enables creation, tracking, and updating of investigation records.

Evidence Management Module: Facilitates evidence registration, categorization, and retrieval. Device Management Module: Tracks devices under investigation and maintains metadata.

Analysis and Reporting Module:

Provides tools for analyzing data and generating reports. Integration Module:

Connects with external digital forensic tools and file systems.

The modular design enhances scalability, maintainability, and the ability to deploy the system in both urban and rural policing environments.

Prototype Development Process

The development of the Digital Forensic Toolkit followed Agile principles, with progress divided into incremental sprints:

Sprint 1: Implementation of user registration and authentication features.

Sprint 2: Database design and case management functionalities.

Sprint 3: Integration of evidence management and storage components.

Sprint 4: Development of analysis, reporting, and dashboard interfaces.

Sprint 5: Integration testing, optimization, and user training.

Each sprint concluded with a review and feedback session, allowing stakeholders to test new functionalities and suggest improvements. The feedback loop played a vital role in refining usability, performance, and reliability.

RESULTS

Prototype Development Outcomes

The project successfully developed a digital forensics toolkit comprising three primary modules:

Computer Forensics Module – Enables extraction and analysis of files, system logs, and browsing histories from desktops and laptops.

Mobile Device Forensics Module – Supports data retrieval from Android and iOS devices, including deleted messages, call logs, and media files.

Cloud Data Analysis Module – Provides access to cloud storage accounts and email services to extract relevant evidence securely.

The toolkit was implemented as a standalone application with an intuitive graphical interface, offline capabilities, and support for commonly used file formats in Malawi (e.g.,

PDF, DOCX, JPEG, MP4).

Usability Testing

The toolkit was evaluated with a small group of Malawian law enforcement officers (N=12) to assess usability and effectiveness. Participants performed typical forensic tasks, and results were measured in terms of task completion rate, time taken, and user satisfaction.

Key Insights

Tasks were completed successfully in most cases.

Cloud data extraction showed slightly lower completion rates due to variations in user credentials and security settings.

Officers highlighted the interface as user-friendly, with minimal technical guidance required.

Forensic Accuracy Evaluation

The toolkit was tested on simulated datasets to validate its ability to extract deleted and hidden data from computers and mobile devices. The evaluation metrics included data recovery rate, accuracy of metadata extraction, and completeness of evidence reporting.

Observations

The toolkit successfully recovered over 90% of deleted files in both mobile and computer devices.

Metadata, such as timestamps and file origins, was accurately captured for all test cases.

Cloud module performance is slightly limited by authentication issues, which can be improved with further integration of cloud APIs.

Resource and Performance Assessment

The toolkit was tested on low- to mid-range devices commonly used in Malawi. Performance metrics included CPU usage, memory consumption, and execution time.

Execution Time Across Modules (on Mid-Range Laptop) Computer Forensics: 5–12 minutes per dataset (average: 8.5 min) Mobile Forensics: 6–15 minutes per device (average: 10.8 min) Cloud Analysis: 8–18 minutes per account (average: 12.3 min) **Observations**
Memory consumption remained below 500 MB during full operations. CPU usage peaked at 60%, allowing for multitasking during investigations. Offline functionality ensures usability in rural areas with limited internet connectivity.

Law Enforcement Feedback

A structured questionnaire was administered to the participating officers after testing. Key findings:
100% agreed the toolkit could improve investigative efficiency. 92% felt it would enhance evidence reliability. 83% suggested adding automated reporting and cloud authentication enhancements.

Officer Feedback on Toolkit Effectiveness (Likert Scale)
Strongly Agree: 58%
Agree: 42%
Neutral: 0%
Disagree: 0%
Strongly Disagree: 0%

Summary of Findings

The results indicate that the digital forensics toolkit:

Provides effective recovery and analysis of computer, mobile, and cloud data. Is user-friendly and suitable for officers with limited technical experience.

Performs efficiently on locally available hardware and supports offline operations. Offers significant potential to improve cybercrime investigations in Malawi.

Next Steps: Incorporate feedback on cloud authentication, integrate automated report generation, and expand mobile OS support.

DISCUSSION

Interpretation of Key Findings

The development and evaluation of the digital forensics toolkit demonstrate its potential to significantly enhance cybercrime investigations in Malawi. The usability testing showed that law enforcement officers could perform critical forensic tasks, such as recovering deleted messages, extracting browsing histories, and generating evidence reports, with high success rates. This aligns with prior research emphasizing the importance of user-friendly forensic tools in regions with limited technical expertise (*Casey, 2011; Nelson et al., 2014*).

The high data recovery and metadata accuracy rates observed across computer and mobile modules indicate that the toolkit can reliably preserve the integrity of digital evidence. This is critical for supporting legal proceedings, as studies have highlighted that improperly handled or incomplete evidence is a major barrier to successful cybercrime prosecution in developing countries (*Choo, 2011; Kizza, 2017*). The toolkit's ability to extract over 90% of deleted files from devices demonstrates its effectiveness, consistent with findings from international forensic tool evaluations (*Rogers, 2018*).

Cloud Module Performance

The cloud data analysis module, while functional, exhibited slightly lower performance metrics due to authentication and account security variations. This is not unexpected, as cloud environments present unique challenges for forensic acquisition, including multi-factor authentication, encryption, and proprietary data formats (*Al Mutawa et al., 2010; Oriwoh & Sant, 2013*). Despite these limitations, the module still retrieved a majority of relevant data and provided accurate reporting, indicating its utility in practical investigations. Future enhancements could incorporate automated authentication methods and API-based data extraction to further improve reliability.

Resource Efficiency and Accessibility

Performance testing revealed that the toolkit is resource-efficient, requiring less than 500 MB of memory and peaking at 60% CPU usage, even during full-scale operations. This is particularly important in the Malawian context, where low- and mid-range devices are more prevalent in both urban and rural police stations. The offline functionality ensures usability in areas with limited internet

connectivity, addressing a common constraint identified in prior studies on forensic practices in developing countries (*Kariuki & Muriuki, 2018*).

The emphasis on usability and interface design also reflects global best practices, as forensic tools are often underutilized when they are overly technical or complex (*Casey, 2011; Rogers, 2018*). Feedback from officers confirmed that minimal training was required to operate the toolkit, which supports scalability and adoption across different police units.

Implications for Cybercrime Investigations in Malawi

The toolkit addresses critical challenges in Malawi's cybercrime response infrastructure, including:

Limited forensic expertise – By simplifying complex processes, it enables officers with minimal technical training to conduct investigations.

Shortage of forensic infrastructure – Its ability to run on locally available hardware reduces dependency on centralized labs.

Rapid evolution of cyber threats – The modular and adaptable design allows updates to address emerging threats without overhauling the entire system.

These improvements have the potential to increase the rate of successful prosecutions, enhance evidence management, and strengthen the overall capacity of law enforcement agencies. This aligns with the broader literature advocating for locally tailored forensic solutions in resource- constrained environments (*Kizza, 2017; Choo, 2011).*

Limitations

While the results are promising, several limitations must be acknowledged:

Sample size for usability testing was relatively small (N=12), which may limit generalizability. Larger studies across multiple districts could provide more robust insights.

Cloud module limitations persist due to authentication challenges and proprietary platform restrictions.

Simulated datasets were used for forensic accuracy testing, which may not capture the full complexity of real-world cybercrime scenarios.

Despite these limitations, the toolkit provides a practical, scalable foundation for further development and adoption.

Recommendations and Future Work

Based on the findings and related

literature, the following

recommendations are proposed: Expand

mobile OS support to cover emerging

platforms and device types.

Integrate automated cloud authentication and API-based extraction for enhanced reliability.

Conduct longitudinal studies with actual case investigations to validate effectiveness in operational settings.

Develop training modules and workshops to

improve adoption and technical proficiency among officers.

Future research could also explore the integration of AI-assisted analysis to detect anomalies and identify cybercrime patterns more efficiently, a strategy increasingly recommended in the field of digital forensics *(Rogers, 2018; Al Mutawa et al., 2010).*

CONCLUSION

This set out to develop a comprehensive digital forensics toolkit tailored for Malawian law enforcement agencies to improve the investigation of cybercrimes. The results demonstrate that the toolkit is effective in extracting, analyzing, and reporting digital evidence from computers, mobile devices, and cloud-based systems. High data recovery rates, accurate metadata extraction, and user-friendly interfaces indicate that the system can enhance investigative capabilities even among officers with limited technical expertise. The usability testing and feedback from participating officers highlighted the toolkit's practical benefits, including offline functionality, compatibility with commonly used devices, and scalability for both urban and rural contexts. While the cloud analysis module exhibited some limitations due to authentication challenges, overall performance confirms the toolkit's suitability for the local operational environment. By addressing constraints such as limited forensic infrastructure, a shortage of skilled investigators, and rapidly evolving cyber threats, this project contributes to modernizing digital forensics practices in Malawi. The toolkit has the potential to improve the accuracy and reliability of digital evidence management, facilitate successful prosecution of cybercriminals, and strengthen the overall capacity of law enforcement agencies to respond to cybercrime. Future work should focus on expanding mobile OS support, enhancing cloud module capabilities, and conducting longitudinal studies to evaluate real-world effectiveness. Ultimately, this project provides a critical step toward building a technologically capable, resilient, and legally compliant cybercrime investigation framework in Malawi.

REFERENCES

Al Mutawa, N., Baggili, I., & Marrington, A. (2010). Cloud computing forensics: Challenges and solutions. Journal of Digital Forensics, Security and Law, 5(3), 7–20.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions.
Computers & Security, *30*(8), 719–731.
https://doi.org/10.1016/j.cose.2011.08.004

Kariuki, J., & Muriuki, P. (2018). Digital forensics in resource-limited environments. African Journal of Information and Communication Technology, 12(2), 45–59.

Kizza, J. M. (2017). *Guide to computer network security* (3rd ed.). Springer.

Oriwoh, E., & Sant, P. (2013). Forensic analysis of cloud storage services. *Digital Investigation, 10*(1), 50–58.
https://doi.org/10.1016/j.diin.2013.02.004

Rogers, M. K. (2018). Digital forensics best

practices and trends. CRC Press.