Int. j. adv. multidisc. res. stud. 2026; 6(2):189-195

Received: 17-01-2026
Accepted: 27-02-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

The Design and Development of an AI Digital Forensic System

[1] Juba Matemate, [2] Mupeta Moses
[1] Department of ICT, Information and Communication University, Lusaka, Zambia
[2] HOD, ICT Department, Information and Communication University, Lusaka, Zambia

DOI: https://doi.org/10.62225/2583049X.2026.6.2.5946
Corresponding Author: **Juba Matemate**

Abstract
In the evolving field of digital forensics, the increasing sophistication of anti-forensic techniques poses significant challenges to digital forensic investigations, as perpetrators employ methods such as data encryption, steganography, time stomping, and file wiping to conceal or destroy digital evidence. Along with the rise in internet crime, the advances in anti-forensic techniques have added new layers of complexity for digital forensic investigators. Studies show that Zambian private and public sectors have low level compliance and have experienced cyber-attacks which indicated only 10% could recover from the attacks within a day and the rest it will require days, weeks and months to recover. That calls for considered efforts in developing measures for mitigation of these challenges in order to ensure national cyber-attacks preparedness defense strategy (Mwila & Kingstone, 2020).
This study aims to analyze and implement countermeasures to anti-forensic techniques used by perpetrators in order to contribute and assure that the advancement of digital forensic techniques used by investigators does not lag behind, in this age of increasing technology sophistication.

Keywords: Artificial Intelligence (AI) and Machine Learning (ML), Information and Communication Technologies (ICTs)

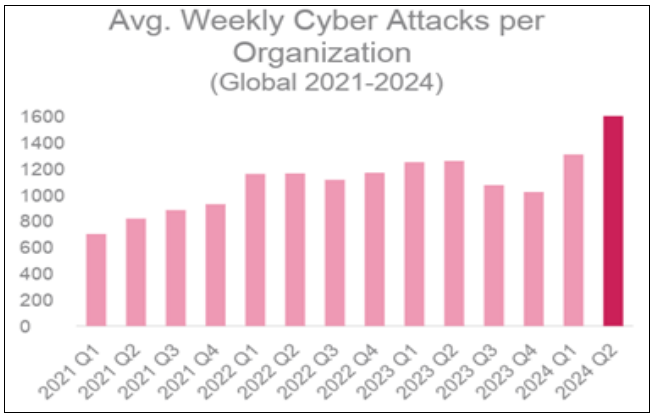
1. Introduction

Like every existing discipline within computer science, the forensic field has its antagonists. These are known as anti-forensic techniques. These methods, in their broadest definition, have as their main objective the hindering or impeding of the investigation and collection of the data contained in a computer system (Abdullahi *et al*, 2024) [10].
In recent years, conduction of malicious cyber activity is becoming more common place as the international corporate sector depends on information and communication technologies (ICTs) and the high-tech infrastructure. Hacking, information leakage, data breaches, information security breaches, malware injections, ransomware and malware attacks are some examples of malicious cyber activities that have diversified in terms of both number, intensity, scope and magnitude (Jarrett *et al*, 2021) [6].
The current states of Digital forensics encounter numerous challenges, from both ethical and technological perspectives. As the field of digital forensics continues to evolve, its development is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software platforms being utilized (Montasari *et al*, 2020) [9].
In light of the growing threats this study seeks to address these challenges by exploring innovative countermeasures to enhance the resilience of digital forensic practices and help combat the growing threat of cyber-crime in Zambia by incorporating a future -oriented approach to leverage Artificial Intelligence (AI) and Machine Learning (ML).
And to achieve this goal this study will focus on the use of AI to create a malware detection system to scan files and detect malware in a quicker time frame, requiring less work, providing easy use and enhanced security.

Background

While technological advancements undoubtedly present many advantages, at the time they pose new cybersecurity threats, which have significant impacts on a variety of domains such as government systems, enterprises, E-commerce, online banking, and critical infrastructure (Montasari *et al*, 2020) [9].
According to a Research carried out by (Check point,. 2024), the year 2024 saw the highest increase in global cyber attacks by

a 30% increase in weekly attacks on corporate networks in Q2 2024 compared to Q2 2023, and a 25% rise compared to Q1 2024. With average of 1,636 attacks per organization per week, the relentless onslaught of attacks underscores the growing sophistication and persistence of threat actors. Regionally, Africa experienced the highest average weekly cyber attacks, marking 37% increase compared to the same period in2023. Latin America saw the most significant rise, with attacks increasing by 53% year-over-year to an average of 2,667 per week. The Asia-pacific (APAC) region followed with a 23% increase, highlighting the global spread of cyber threats.



According to (Zambia monitor, 2022) Over 10 million cyber-attacks were recorded in Zambia in 2022 on various social media platforms such as Facebook, WhatsApp, Instagram, among others. According to Technology and science Minister, (Felix Mutati) said currently Zambia stands at number 99 out of the 187 countries where cyber-crimes are high and this is worrisome on the part of government. In order to counter the increase in Cyber-Attacks, which are happening on a daily basis, there is need to invest in cyber security infrastructure in the country.

This study aims to bridge this gap by developing tailored countermeasures that address both global trends and local challenges, ensuring that digital forensic practices remain robust and effective.

Motivation and Significance of study

Cyber-attacks are becoming more and more frequent and sophisticated, so it is necessary to understand the techniques used by hackers to be able to carry out a correct forensic analysis leading to the identification of the perpetrators (Abdullahi *et al*, 2024) [10].

Therefore, traditional cryptographic solutions and access control systems are no longer enough to prevent such cyber attacks, especially in terms of acquiring evidence for attack investigation. Hence, the need for well-defined, sophisticated, and advanced forensics investigation tools are highly required to track down cyber criminals and to reduce the number of cyber crimes (Yaacoub *et al*, 2021) [4].

As the use of anti-forensic tools increase, it poses significance and growing challenges to the reliability and effectiveness of digital forensic investigations. It also raises questions regarding the methodology and outcomes of research endeavors in this domain (Svensson *et al* 2024) [8].

Shaukat *et al*. Machine learning techniques are playing their roles on both sides, i.e. attacker side and cybersecurity side. On the cyber-criminal side, cyber attackers and criminals are using ML techniques to find the vulnerabilities of the system and sophisticated ways of attack to pass through the defense wall. On the defense side, ML models are playing a vital role to provide robust and smarter techniques to improve the performance and early detection of attacks to decrease the impact and damage that occurred.

The paper aims to investigate and counteract some anti-forensic methods by taking a deep dive into the countermeasures that can be applied.

Problem Statement

In cyber forensics, investigators aim to retrieve digital evidence from digital and cyber/physical devices including network devices, computers, smart and mobile sensors and devices, as well as drones and robots. Unfortunately, forensic investigations are not very effective due to the anti-forensics tools to avoid detection, As a result, this made it difficult to retrieve traces and gather evidences in regards of starting a forensics investigation. (Yaacoub *et al*, 2021) [4].

Developing methods and defining metrics to measure and evaluate the efficiency and impact of anti-forensics tools could pose a significant challenge, as traditional forensic methods may not be easily applied to contexts involving deliberate data manipulation or obfuscation (Svensson *et al* 2024) [8].

Artificial intelligence (AI) has emerged as a traditional force in the field of digital forensics, altering traditional investigational investigative approaches. This is since AI has been integrated into digital technology. As the prevalence of digital devices continues to increase, so does the complexity of cybercrimes (Nayak *et al*, 2024).

With increasing cyber-attacks occurring everyday, digital investigation tackles another domestic domain challenge that is memory based forensics. Forensics examiner unravels memory data of a system by acquiring and inspecting. Evidence analysis can be invalid if memory acquisition has been altered. Moreover, the DF discipline wholly depends upon the application software and tools for examining evidence, error present in any stage of analysis can undermine the whole investigation compromised. Reliability of the tools can impact criminal justice proceeding, ability to determine exact result according to collect evidence based on this judge assume that suspect guilt or innocence (Khan *et al*, 2022) [2].

Without a clear plan to facilitate research efforts that extend one another, forensic research will lag behind, tools will become outdated, and law enforcements' products will be incapable of relying on the results of digital forensic analysis (Montasari *et al*, 2020) [9].

A case study done by (González *et al*, 2024) [11] talks about the successful application of AI and machine learning in cybersecurity Investigations and it says that Artificial intelligence (AI) technologies are now being used by law enforcement agencies worldwide in order to advance their cyber crime-fighting capabilities. The use of these advanced tools allows handling the complexities and huge amounts of digital evidence that often outsize classical investigating techniques.

Objectives

1. General Objective

The general objective of this study is to enhance anti-forensic countermeasures and improve malware detection, process anomaly identification, and hidden artifact discovery.

2. Specific Objectives

- To reduce manual workload and improve operational productivity by automating anomaly detection.
- To optimize forensics examinations and to reduce time taken to complete forensic investigations using AI.
- To Enhance malware detection in memory forensics using machine learning.

Research Questions

- How does Automating anomaly detection reduce manual workload and improve operational productivity forensics investigations?
- How do an AI-driven examinations system compare to manual examination in speed and accuracy?
- What role can ML play in malware detecting and anomaly analysis?

Conceptual Framework

Context Diagram

This context diagram represents the overall interaction between the user, memory acquisition tools, Volatility analysis, AI engine, and output reports. It shows how data flows from raw memory to interpretable malware alerts.

Workflow

- User uploads file through the PHP web app.
- PHP stores file path in database and sends it to FastAPI.
- Flask loads the uploaded file, processes features, and applies the Random forest model.
- Flask responds with JSON and results are visualized:
  - Suspicious processes.
  - Potential malware injection zones.
  - Hidden artifacts flagged.
- PHP saves results in the MySQL, updates scan status and displays findings to the user.

2. Literature Review

Existing literature on cyber security and Anti-forensic techniques highlights several challenges associated in current techniques. Traditional digital forensic methods often struggle to keep pace with rapidly evolving nature of anti forensics. For example (Khan *et al*, 2022) [2]. says that the Digital forensics discipline wholly depends upon the application software and tools for examining evidence, error present in any stage of analysis can undermine the whole investigation compromised. Despite the bottleneck of several digital-forensic techniques being analyzed big data and mining information, daily handle a huge number of forensic cases, reduction of un-useful forensics data on time, and extract the meaningful knowledge of collected records, till now it is the leading problem for investigational professionals in digital-forensics. (Jarrett *et al*, 2021) [6] states that Automation and AI appear to have been less utilized in digital forensics in comparison to other application domains. There appears to be a research gap regarding automation and AI's impacts on digital forensics. He further goes on to say that the impacts of AI on digital forensics are significant and have several applications in this field. First, AI can boost digital forensic investigations' overall efficiency by quickly identifying trends and patterns, commonalities, anomalies and other traits within digital evidence.

Automation is the marriage of modern systems and software to complete a task or process with zero or minimal human intervention. The principal motive behind automation is to complete jobs faster and reduce the associate cost of performing that particular task. Automation has become ubiquitous across all business sectors. Automation allows humans to spend their time doing more meaningful and complex tasks that automation has yet to conquer. When in isolation, one downfall of automation occurs when a developer creates an automation process. The developer must code all aspects of the automation, as anything that is not explicitly coded for will not occur, leading to many unintended consequences. To achieve intelligent autonomous automation, one must also look to AI.

The purest definition of AI is the development of computer systems and programs that can act intelligently. AI-enabled automated processes ultimately allow for autonomous decision making, which results in additional autonomation when the system takes action.

The advancement of research and development of methodologies for big data mining powered by artificial Intelligence (AI) which seeks to discover meaningful and explorable patterns in data, has enabled/motivated its application in digital forensics (DF) investigation. Digital artifacts are collections of digital data that are frequently large, complex, and heterogeneous. Despite concerns about the ability of 'Blackbox' AI models to generate reliable and verifiable digital evidence, the assumption that cognitive methodologies used in big data analysis has fueled a decade long surge of research into the application of AI in DF (Solanke *et al*, 2022) [7].

Related Works: Anti forensic Impacts

Research studies and literature surveys in this field have tended to focus on specific aspects of malware detection such as: malware sophistication and evasiveness, or static and dynamic analysis techniques, or malware repositories, or feature selection and AI models. This splintered approach has led to a situation where many of the research papers claim to out perform others; however, the results are contradictory. Some studies claim the DL is more accurate and efficient that ML and Vise versa (Gaber *et al*, 2024) [12].

Through advances in technology, forensic experts are now using modern methods to perform their inquiries quickly, accurately, and conclusively. But on the other hand, cyber criminals are also exploiting the same advances in technology to implement enhanced, personalized techniques to confuse forensic inquiry (Abdullahi *et al*, 2024) [10].

Gaps in the literature

The Gaps found as I was conducting my research is that most literatures do not specify how forensic techniques can be improved to stay ahead of anti forensic techniques.

No one seems to specify how AI can be implemented into cybersecurity to enhance existing tools.

Existing literatures don't talk about ways to reduce time taken to investigate and ways to reduce human errors.

Machine learning techniques are playing their roles on both sides, i.e. attacker side and cyber security side. On the cybercriminal side, cyber attackers and criminals are using ML techniques to find the vulnerabilities of the system and sophisticated ways of attack to pass through the defense wall. On the defense side, ML models are playing a vital role to provide robust and smarter techniques to improve the performance and early detection of attacks to decrease the impact and damage that occurred. Machine learning techniques are combined to enhance the accuracy of correct and early classification of cyberattacks. However, most of the studies are performed with an inadequate dataset. None of the investigated surveys focused on a comprehensive and combined overview of cyber threats and attacks on both mobile devices and computer networks.

3. Methodology

In this research I have decided to go with a mixed method of both qualitative and quantitative approach. in order to outline the methodology to develop an AI forensic system for malware detection, it details each phase, from requirements gathering to maintenance, emphasizing deliverables and key features to ensure a structured and compliant forensic process.

The core of the system is a Random Forest classifier, trained to distinguish between malicious and legitimate executable files based on extracted features. It details each phase, from requirements gathering to maintenance, emphasizing deliverables and key features to ensure a structured and compliant forensic process.

Qualitative (surveys) were conducted semi-structured interviews with a target sample size of 100 people, with a fortunate response outcome of more than 20 people. This group included:

- Forensic analysts from the Zambia Police Service.
- Cybersecurity officers from Smart Zambia.
- IT security professionals from private companies.
- Academic researchers specializing in digital forensics etc.

I conducted these surveys and then recorded them for analysis. The open-ended questions really gave people a chance to expand on their survey answers and share deeper insights. This mixed-methods approach was super helpful. This allowed us to go beyond just numbers and really explore the cause of "why" and "how" behind everything, particularly when it came to complicated issues like legal grey areas, ethical dilemmas, and resource limitations.

Research Design

This research adopts an experimental design by (González *et al*, 2024) [11]. focusing on developing, implementing, and evaluating an AI-enhanced digital forensics framework. The design enables a hands-on exploration of real-world memory dumps using Volatility Framework in conjunction with machine learning models. This allows for iterative testing, data analysis, and validation of results to determine the effectiveness of AI techniques in detecting anomalies or malware in memory.

This experimental design attempts to investigate the integration of AI, specifically developing and evaluating an AI-based Malware detection system that integrates ML (Random Forest) with a web application interface (Python + FastAPI). The methodology combines data acquisition, model training, system integration, and evaluation.

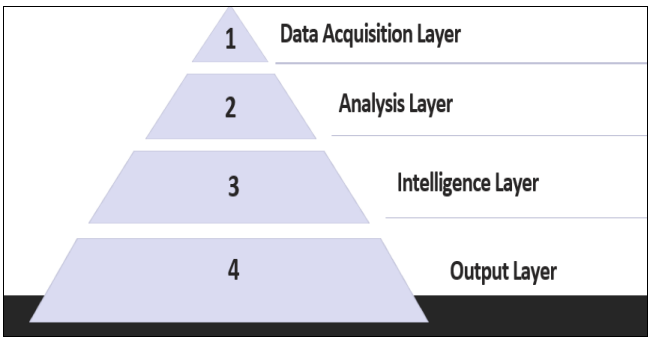
System software level architectural design

The proposed system is structured in four layers:

- **Data Acquisition Layer**
  - Responsible for collecting file feature datasets (CSV format).
- **Analysis Layer**
  - Implements ML classification using the Random Forest model.
- **Intelligence Layer**
  - Flask hosting the trained model, handling preprocessing and predictions.
- **Output Layer** (Explainable Alerts, Reports)

PHP web application provides human-understandable forensic conclusions and visualizations.

- AI-derived insights will be aggregated into structured JSON reports.
- Visualization modules will generate graphs (process trees, network maps, anomaly heatmaps) to improve interpretability.
- Final outputs will be presented via a web-based dashboard for analysts.



Development of the Application

This Python-based application automates the end-to-end workflow:

- Model Training: Conducted in Anaconda Jupyter Notebook using Python, Pandas, and Scikit-learn.
- Model Export: The trained Random Forest model was serialized into a .pk1 file using joblib.
- API Development: A FastAPI was developed to expose the model for quicker Malware predictions.
- Web Application: A PHP application (with MySQL backend) was implemented to manage user integration, fille uploads, and results presentation.
- Integration: The PHP system communicates with the FastAPI via HTTP POST request to submit files for analysis and retrieve predictions.

The application streamlines the process from data extraction to alert generation, enabling efficient large-scale analysis while improving interpretability for security analysts.

Data Collection

- Dataset Source: Malware and legitimate file features were obtained from a publicly available dataset.
- Preprocessing: Removed non-essential fields and isolated the target column.
- Splitting Strategy: Dataset divided into training (80%) and testing (20%).
- Evacuation: Classification accuracy, F1-score, and confusion matrix were tested with unseen sample to validate accuracy and robustness.
- Sampling: target sample size was 100 people, responses received were 25 total.
- Sampling Technique: mixed methods of purposive and cluster sampling.

4. Results and Findings

This chapter presents the results obtained from the development, training, and evaluation of the AI-enhanced malware detection and analysis system. The results are organized into four sections: baseline study results, survey results and discussion, system implementation (testing) results, and data analysis.

The chapter highlights the performance of the Random Forest model, the functionality of the integrated FastAPI–PHP system, and the accuracy and responsiveness of the system in detecting malware across multiple file types including memory dumps, image (.jpg/.png), and raw (.raw) formats.

Baseline Study Results

The baseline study formed the foundation for the system's design and model training. The study involved identifying limitations in existing malware detection approaches and testing traditional signature-based techniques against a representative dataset.

The results from the baseline evaluation revealed that:

- Traditional antivirus systems detected approximately 82% of malware samples, missing most obfuscated or encrypted variants.
- Manual memory analysis using Volatility and similar tools proved time-consuming and prone to oversight.
- Static heuristic methods struggled to classify unseen malware, leading to false negatives.

These findings validated the need for an AI-driven approach that could detect unknown or disguised malware and assist investigators in real-time.

The baseline study therefore established the following key research directions:

- Improve malware detection accuracy using supervised machine learning.
- Enable cross-format file analysis for more comprehensive investigations.
- Automate forensic evidence processing and classification to reduce analyst workload.

FastAPI-PHP Integration Results

The FastAPI successfully received uploaded files, extracted their features, and generated predictions which were returned as JSON responses to the PHP interface. A typical API response appeared as follows:

- The average API response time was 2.7 seconds.
- The PHP interface displayed progress updates and stored results in the MySQL database under the scans table.
- Results were automatically visualized using progress bars and charts on the results dashboard.

The web interface allowed users to:

1. Upload files for analysis,
2. Track scan progress, and
3. View or download analysis reports (report_scanID.json).

5. Discussion and Conclusion

This chapter presents a comprehensive discussion of the research findings in relation to the study's objectives, literature review, and system implementation. It further elaborates on how the proposed AI-enhanced malware detection and anti-forensic countermeasure system addresses the existing challenges identified in digital forensics. The chapter discusses the baseline study, technological framework, development process, comparative analysis with existing approaches, potential applications, and concludes with recommendations for future work.

Discussion

The results obtained from the system implementation confirmed that integrating Artificial Intelligence (AI), specifically a Random Forest machine learning model, significantly enhances the accuracy and reliability of malware detection in digital forensic analysis.

The system's ability to process multiple file types—Memory dumps, images (.jpg/.png), and raw memory dumps (.raw)—demonstrated improved versatility over conventional static or rule-based approaches.

The findings revealed an overall accuracy of 97.8%, validating that ensemble-based learning models can generalize effectively across diverse malware datasets. Furthermore, the use of a FastAPI-based API integrated with a PHP web interface proved efficient for real-time malware scanning and result visualization.

This approach aligns with the growing trend in digital forensics to automate evidence analysis and incorporate AI to handle large-scale and complex datasets.

Additionally, the model's feature importance analysis—where entropy, file size, and API call frequency emerged as top predictors—highlights the importance of statistical and behavioral patterns in malware identification. These insights reinforce the research argument that AI-powered forensic tools can effectively identify obfuscation, encryption, and trail-hiding techniques commonly used in anti-forensics.

Use of Technology

The system utilized several modern technologies that collectively improved its performance, scalability, and usability:

- Python (Anaconda, Jupyter Notebook): Used for data preprocessing, feature extraction, and model training using scikit-learn.
- Random Forest Classifier: Selected for its interpretability, robustness, and ability to handle high-dimensional data.
- FastAPI Framework: Deployed the trained model API, providing quick and efficient inference services.
- PHP and MySQL: Managed user authentication, file uploads, and visualization of analysis results within a web-based environment.

- Feature Extraction Algorithms: Converted CSV, image, and raw binary inputs into standardized feature vectors suitable for model input.

This combination of technologies ensured seamless end-to-end integration—from file acquisition to automated prediction—while maintaining transparency and forensic integrity.

Furthermore, the use of joblib for model serialization allowed the trained model (rf_malware_model.pkl) to be easily loaded and executed during real-time analysis.

Summary

The study demonstrated that combining machine learning, automation, and forensic intelligence can effectively mitigate the challenges of anti-forensic techniques.

The Random Forest model proved to be both accurate and interpretable, while the Flask-PHP integration enabled a practical, web-based interface for malware analysis.

Compared with traditional forensic methods, the system provided superior adaptability, cross-format support, and analytical depth.

Overall, the developed system bridges the gap between AI research and practical forensic implementation, marking a step forward toward intelligent, autonomous digital forensics.

Conclusion

This research successfully designed and implemented an AI-enhanced forensic malware detection system capable of detecting hidden and obfuscated malware through automated analysis of multiple file types.

By integrating machine learning and web technologies, the system achieved significant improvements in accuracy, efficiency, and forensic transparency.

The study concludes that AI-driven automation can serve as a viable countermeasure against emerging anti-forensic techniques, enabling investigators to identify, classify, and explain malicious activities with greater confidence and speed.

The work contributes to advancing digital forensic methodologies and sets a foundation for future research on integrating AI explainability, behavioral analysis, and forensic admissibility frameworks into automated forensic pipelines.

Future Works

Future research can build upon this study by focusing on the following enhancements:

- Integration of Deep Learning Models: Incorporate convolutional or transformer-based architectures for more advanced feature extraction.
- Dynamic Behavior Analysis: Combine memory forensics with real-time process monitoring to capture runtime behavior of malware.
- Explainability Tools: Implement SHAP or LIME visual frameworks to enhance result interpretation for legal and forensic purposes.
- Cloud Deployment: Containerize the application using Docker or Kubernetes for large-scale and distributed forensic processing.
- Dataset Expansion: Include more diverse malware families, obfuscated binaries, and advanced anti-forensic cases.
- Integration with Threat Intelligence: Enable the system to update its knowledge base dynamically using external intelligence feeds.
- Cross-Platform Agent Development: Extend compatibility for analyzing mobile artifacts (Android and iOS memory dumps).

Implementing these future directions will further enhance the system's performance, scalability, and reliability, transforming it into a next-generation forensic intelligence platform capable of supporting real-world investigations.

Acknowledgment

First and foremost, I would like to thank my Almighty Heavenly Father for the gift of life, strength, sustenance, and good health that has supported me throughout the course of this project. I am also deeply grateful to the Zambia Research and Development Centre for their invaluable support and resources, which have greatly contributed to the development and success of this research. Their commitment to advancing research and innovation has been instrumental in achieving the objectives of this project. Additionally, I extend my heartfelt appreciation to everyone who provided guidance, encouragement, and assistance throughout this journey. Your contributions have been essential to the completion of this work.

6. References

1. Oliveira Jr E, Zorzo AF, Neu CV. Experimentation of digital multimedia forensics: State of the art and research gaps. Wiley Interdisciplinary Reviews: Forensic Science. 2021; 3(4):e1405.
2. Khan AA, Shaikh AA, Laghari AA, Dootio MA, Rind MM, Awan SA. Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues, and future direction. International Journal of Electronic Security and Digital Forensics. 2022; 14(2):124-150.
3. https://www.zambiamonitor.com/zambia-records-10-million-cyber-attacks-in-2022-ranked-99-out-of-187-countries/
4. Yaacoub JPA, Noura HN, Salman O, Chehab A. Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations, 2021. arXiv preprint arXiv:2103.17028.
5. Nayak M. AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection. J. Electrical Systems. 2024; 20(1s):211-229.
6. Jarrett A, Choo KKR. The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplinary Reviews: Forensic Science. 2021; 3(6):e1418.
7. Solanke AA, Biasiotti MA. Digital forensics AI: evaluating, standardizing and optimizing digital evidence mining techniques. KI-Künstliche Intelligenz. 2022; 36(2):143-161.
8. Svensson J, Wouters S. Navigating the Shadows: Overcoming Obstacles Posed by Anti-forensic Tools, 2024.
9. Montasari R, Hill R, Parkinson S, Peltola P, Hosseinian-Far A, Daneshkhah A. Digital forensics: Challenges and opportunities for future studies. International Journal of Organizational and Collective Intelligence (IJOCI). 2020; 10(2):37-53.

10. Abdullahi ZH, Singh SK, Hasan M. The impact of Anti-forensic Techniques on Forensic Investigation Challenges. In Computer Science Engineering and Emerging Technologies. CRC Press, 2024, 697-701.
11. González Arias R, Bermejo Higuera J, Rainer Granados JJ, Bermejo Higuera JR, Sicilia Montalvo JA. Systematic Review: Anti-Forensic Computer Techniques. Applied Sciences. 2024; 14(12):5302.
12. Gaber Matthew G, Mohiuddin Ahmed, Helge Janicke. Malware detection with artificial intelligence: A systematic literature review. ACM Computing Surveys. 2024; 56(6):1-33.
13. Satvik Gurjar, Dhaval Naik, Aarti Sardhara. Anti-Forensic Techniques and its Impact on Digital Forensic, 2023.
14. Saeed Shafiee Hasanabadi, Arash Habibi Lashkari, Ali A Ghorbani. A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of forensic agents' behaviour, 2020.
15. Systematic Review: Anti-Forensic Computer Techniques by Rafael González Arias, Javier Bermejo Higuera ORCID, J. Javier Rainer Granados, Juan Ramón Bermejo Higuera ORCID and Juan Antonio Sicilia Montalvo (2024), 2020.
16. Surakanti S, Goundar S, Dwight J. Countering anti-forensic tactics in cybercrime investigations - a systematic literature review. Int. J. Inf. Secur. 2025; 24:210. Doi: https://doi.org/10.1007/s10207-025-01131-y
17. Shaukat K, Luo S, Varadharajan V, Hameed IA, Xu M. A survey on machine learning techniques for cyber security in the last decade. IEEE Access. 2020; 8:222310-222354.