IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, December 2025

Impact Factor: 7.67

Autonomous AI Agent for Digital Forensics Investigation (Self-Investigating System)

Lohokare Hardik Bhikaji, Ghongane Suyog Somnath, Aher Chinmay Sunil

Department of Commerce and Research Center BBA(CA)
Shri Shiv Chhatrapati College, Junnar, Maharashtra, India

Abstract: *Digital forensics involves the systematic examination of digital evidence to understand cyber incidents and support investigations. However, the increasing volume of data and complexity of cyberattacks often results in delays when investigations rely only on manual processes. This paper presents the concept of an Autonomous AI Agent that performs digital forensic tasks independently. The approach integrates machine learning, log analysis and natural language processing to automate evidence collection, anomaly detection, event reconstruction and report preparation. The objective is to demonstrate how an autonomous model can reduce investigation time, enhance accuracy and support investigators in rapidly evolving cyber environments.*

Keywords*:* Digital Forensics, Artificial Intelligence, Autonomous Agents, Anomaly Detection, Cybercrime Analysis

I. INTRODUCTION

Digital forensics plays an essential role in identifying, preserving and analyzing digital evidence. As cyberattacks grow more sophisticated, investigators are expected to process large datasets, interpret complex patterns and prepare detailed reports within limited timeframes. Traditional methods rely heavily on human expertise, making the process slow and prone to oversight.

Artificial Intelligence has the potential to support forensic investigations, but existing tools are primarily assistive. They help with specific tasks but cannot conduct a full investigation independently. This research proposes an advanced concept—an **Autonomous AI Agent** capable of performing the complete forensic cycle without direct human control. The agent can monitor systems, collect relevant evidence, identify suspicious activities and prepare structured forensic summaries. This model represents a step toward future investigative systems that combine automation with intelligent analysis.

II. METHOD

This research uses a structured methodology to adapt AI for autonomous forensic operations. The study begins with a review of digital forensics methods, intrusion detection techniques and behavioural analysis models, leading to the development of a modular framework. The system automatically collects evidence such as logs, memory artifacts and file changes using predefined rules, and then uses machine learning to classify data and detect abnormal activities like unauthorized access or hidden malware.

Extracted timestamps help the AI reconstruct the attack timeline, while Natural Language Processing generates clear and concise forensic reports. Both qualitative and quantitative evaluations were conducted to measure the system’s accuracy, efficiency and reliability.

III. RESULTS

The evaluation of the proposed Autonomous AI Agent shows that the system performs digital forensic tasks with high accuracy and efficiency across multiple investigation stages. The AI demonstrated strong capability in identifying unusual activities, classifying evidence and reconstructing the sequence of events. It was able to detect suspicious behaviours in logs, recognize hidden malware patterns and analyse system changes more rapidly than manual methods. The overall

DOI: 10.48175/568

performance indicates that the autonomous model reduces investigation time and improves the clarity of forensic findings. Some of the key outcomes are described below:

Timeline Reconstruction

The AI generated a clear chronological flow of events using timestamp correlation, making the attack sequence easy to understand. It linked system activities with network logs to highlight cause-and-effect relationships within the incident, helping investigators trace how the attack progressed. The reconstructed timeline reduced manual verification effort and improved overall investigation accuracy.

Anomaly Identification

The system detected irregular system behaviour such as unexpected logins, unusual file executions and modifications in system configuration. These observations enabled early recognition of suspicious patterns that are often difficult to detect manually.

Evidence Classification

The AI classified collected files, logs and memory artifacts based on behaviour and relevance to the case. It separated normal activities from suspicious ones, allowing investigators to focus only on meaningful evidence.

Report Generation

The model produced structured and readable forensic summaries, presenting key findings in clear language. The reports maintained consistency across different test scenarios and provided investigators with a reliable overview of the incident. reports within limited timeframes. Traditional methods rely heavily on human expertise, making the process slow and prone to oversight.

Artificial Intelligence has the potential to support forensic investigations, but existing tools are primarily assistive. They help with specific tasks but cannot conduct a full investigation independently. This research proposes an advanced concept—an **Autonomous AI Agent** capable of performing the complete forensic cycle without direct human control. The agent can monitor systems, collect relevant evidence, identify suspicious activities and prepare structured forensic summaries. This model represents a step toward future investigative systems that combine automation with intelligent analysis.

IV. CONCLUSION

This research introduces the design and working of an Autonomous AI Agent for digital forensics. The proposed model demonstrates how automation can accelerate evidence analysis and reduce the burden on investigators. Although AI cannot fully replace human intelligence, it can support large-scale investigations through rapid data processing and accurate pattern detection. As cyber threats continue to evolve, integrating autonomous AI systems into forensic environments may become an essential part of modern cybersecurity strategies.

V. ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who contributed to the successful completion of this research. Our heartfelt thanks to the faculty and staff of Shri Shiv Chhatrapati College, Junnar, for their continuous guidance and support throughout this study.We also acknowledge the valuable insights from previous research in the fields of digital forensics and artificial intelligence, which provided a strong foundation for this work.

Finally, we extend our appreciation to our peers and family members for their encouragement and motivation during the preparation of this paper.

REFERENCES

[1]. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2023). *The role of AI and Machine Learning in digital forensics.* Forensic Science International: Digital Investigation, 48, 301675.

[2]. Nayerifard, T., Amintoosi, H., Ghaemi Bafghi, A., & Dehghantanha, A. (2023). *Machine Learning in Digital Forensics: A Systematic Review.* arXiv:2306.04965.

DOI: 10.48175/568

[3]. Al-Zubi, S., & Alrawashdeh, M. (2022). *Autonomous forensic investigation using AI agents.* Journal of Digital Forensics, Security and Law, 17(4), 1–15.

[4]. Authors. (2025). *AI-driven DFIR: Automation of evidence collection and cyberattack analysis.* Journal of Cybersecurity Research, 3(2), 10–25.

[5]. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* 3rd Edition, Academic Press.

DOI: 10.48175/568