Chapter 10
The Future of Autonomous Forensic Agents and AI-Augmented Investigators

Rebet Keith Jones
https://orcid.org/0009-0008-0487-1301
Capitol Technology University, USA

ABSTRACT

The rapid evolution of artificial intelligence (AI) and autonomous systems is transforming the landscape of digital forensics and cybercrime investigation. This chapter explores the emerging paradigm of autonomous forensic agents and AI-augmented investigators, emphasizing their potential to revolutionize evidence collection, data analysis, and decision-making processes. It delves into the convergence of machine learning, natural language processing, robotics, and cognitive computing to create intelligent agents capable of independently navigating digital environments, identifying anomalies, and assisting human investigators with high precision and efficiency. The chapter also addresses the ethical, legal, and technical challenges that accompany the deployment of such systems, including concerns about bias, accountability, transparency, and interpretability. Drawing from real-world applications, research trends, and interdisciplinary innovations, this forward-looking analysis envisions a future where human expertise is seamlessly integrated with intelligent automation

DOI: 10.4018/979-8-3373-6536-7.ch010

INTRODUCTION

The accelerating integration of artificial intelligence (AI) into digital forensics and cybersecurity is reshaping investigative practices, blurring the boundaries between human expertise and machine autonomy. In a digital era marked by escalating cyber threats, the emergence of autonomous forensic agents and AI-augmented investigators signifies a paradigm shift—transforming the traditionally reactive and manual forensic landscape into a proactive, intelligent, and largely automated domain (Zangana & Omar, 2025).

Historically, digital forensics has been challenged by overwhelming data volumes, complex attack vectors, and limited human resources (Irons & Lallie, 2014; Jarrett & Choo, 2021). However, with the advent of machine learning (ML), large language models (LLMs), and intelligent automation, forensic analysts can now leverage tools that interpret patterns, prioritize evidence, and even simulate adversarial behavior with minimal intervention (Chen et al., 2024; Xu et al., 2024; Motlagh et al., 2024). These AI-driven tools offer unprecedented speed and scalability in analyzing logs, reconstructing timelines, and identifying anomalies, which is particularly crucial in cloud-native, IoT, and blockchain environments (Hamza & Omar, 2013; Omar et al., 2024; Kasri et al., 2025).

The foundational concept of autonomous forensic agents draws on the convergence of robotics, explainable AI, cybersecurity analytics, and NLP-driven decision-making systems (Ganesh, 2017; Dunsin, Ghanem, & Quazzane, 2022; Hall et al., 2022). These agents are designed not merely as tools, but as adaptive entities that can operate independently, intelligently responding to evolving threat landscapes (Costantini et al., 2019; Jeong, 2020). When integrated with LLMs, they gain a cognitive edge—capable of interpreting legal language, predicting attacker behavior, and generating real-time insights during incident response (Ferrag et al., 2024; Gholami & Omar, 2024; Alturkistani & Chuprat, 2024).

Several studies have illustrated the potential of domain-specific LLMs in enhancing forensic workflows. For example, the SecLM model has been tailored for cybersecurity threat mitigation through deep contextual understanding (Asoronye et al., 2024), while lightweight models like GEADD (Jones & Omar, 2024) and privacy-preserving BERT variants (Thandi, 2024) show promise for real-time applications in constrained IoT/IIoT environments (Ferrag et al., 2023, 2024). These models not only accelerate investigations but also ensure explainability and legal defensibility—critical in judicial proceedings (Kelly et al., 2020; Hall et al., 2022).

Concurrently, AI-augmented investigators are becoming integral to security operations centers (SOCs), particularly in enterprise and critical infrastructure settings. These systems augment human investigators by prioritizing high-risk incidents, providing contextual intelligence, and mitigating cognitive overload (Huff et al.,