Chapter 1
Introduction to Digital Forensics and Artificial Intelligence

Hewa Majeed Zangana
https://orcid.org/0000-0001-7909-254X
Duhok Polytechnic University, Iraq

Marwan Omar
Illinois Institute of Technology, USA

ABSTRACT

This chapter explores the intersection of digital forensics and artificial intelligence (AI), emphasizing the transformative impact AI is having on digital investigative techniques. Digital forensics, traditionally focused on the collection, preservation, and analysis of electronic evidence, is facing new challenges and opportunities in the era of AI. The rapid proliferation of digital devices and the sophistication of cyber threats demand enhanced methods for accurate and timely evidence gathering. AI technologies, including machine learning, natural language processing, and deep learning, are empowering forensic professionals to detect, analyze, and interpret vast volumes of data with unprecedented efficiency. This chapter discusses the fundamentals of digital forensics, examines the integration of AI tools within forensic processes, and addresses the ethical and privacy concerns that arise. The insights provided will help readers understand how AI can bolster digital forensics, enabling more proactive and precise responses to cybercrime.

DOI: 10.4018/979-8-3373-0857-9.ch001

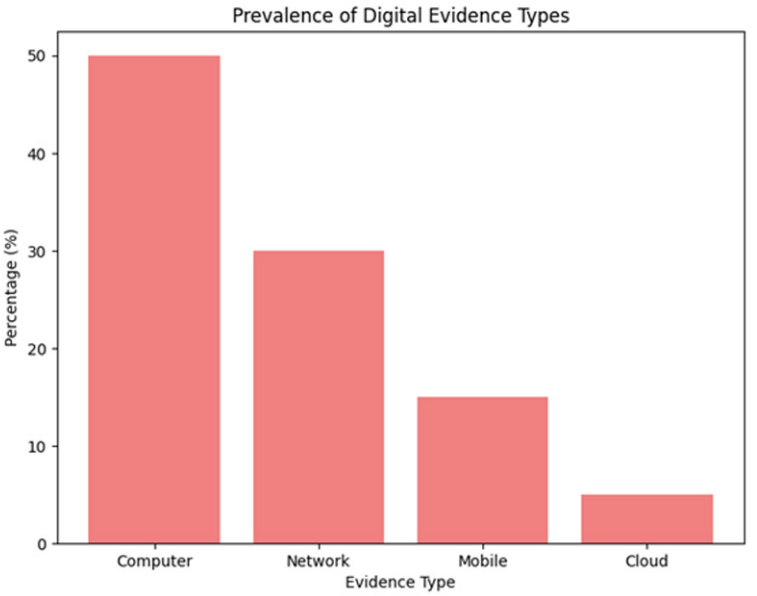
1. OVERVIEW OF DIGITAL FORENSICS

Digital forensics involves the identification, acquisition, analysis, and reporting of electronic evidence from digital devices to investigate cyber incidents, criminal activities, and security breaches. With the widespread adoption of digital devices and networks, digital forensics has evolved into a critical discipline that plays an essential role in supporting law enforcement, cybersecurity, and regulatory compliance. This overview provides insights into the foundational aspects of digital forensics, including key processes, challenges, and the discipline's growing interconnection with artificial intelligence (AI).

Digital forensics traditionally covers various domains, including computer forensics, network forensics, mobile device forensics, and cloud forensics (Adam & Varol, 2020). Each of these domains focuses on extracting, preserving, and analyzing digital evidence from different environments. For example, computer forensics involves recovering data from computers and storage devices, while network forensics emphasizes monitoring and analysis of network traffic to detect and reconstruct cyber events (Jeong, 2020; Wright, Dawson Jr, & Omar, 2012).

Forensic analysis spans various evidence types, each necessitating specialized handling techniques. This bar chart illustrates common digital evidence types and their relative prevalence in investigations.

Figure 1. Forensic Evidence Types



Generating a Mental Health Curve for Monitoring Depression in Real Time by Incorporating Multimodal Feature Analysis Through Social Media Interactions

Moumita Chatterjee, Piyush Kumarand Dhrubasish Sarkar (2023). *International Journal of Intelligent Information Technologies (pp. 1-25).*
www.irma-international.org/article/generating-a-mental-health-curve-for-monitoring-depression-in-real-time-by-incorporating-multimodal-feature-analysis-through-social-media-interactions/324600