Chapter 12
Leveraging AI for Behavioural Analysis of Digital Forensic Artifacts in Cybercrime Investigations

Rituraj Jain
https://orcid.org/0000-0002-5532-1245
Marwadi University, India

Jaishri Gothania
https://orcid.org/0000-0002-2656-642X
Lingaya's Vidyapeeth, India

Priyank Dipakkumar Zaveri
https://orcid.org/0009-0000-0179-8075
B.H. Gardi College of Engineering and Technology, India

Monika Shah
https://orcid.org/0009-0002-2157-8840
B.H. Gardi College of Engineering and Technology, India

Parag Girdharbhai Paija
B.H. Gardi College of Engineering and Technology, India

Yamini Parth Chawda
https://orcid.org/0009-0008-6006-7801
B.H. Gardi College of Engineering and Technology, India

ABSTRACT

In memory execution, OS tools (for example, PowerShell, WMI), and registry manipulation are widely leveraged by fileless malware, which makes it very difficult to detect with the traditional forensic tools. This chapter studies memory forensics as a primary method to trace down attacks such as this one, concentrating on the volatile memory (RAM) analysis. They talk about attack types such as code injection, LOLBins and reflectively loaded DLLs, to name a few, and a few tools such as Cobalt Strike and Empire. Volatility, FTK Imager and YARA rules are leveraged to

DOI: 10.4018/979-8-3373-4898-8.ch012

generate artifacts such as executable injected code, network sockets and command history. In the chapter, find out how we map the findings to the cyber kill chain, and what makes RAM analysis a must for detection, response, and proactive hunting.

1. INTRODUCTION

In the current digital age, the use of technology has revolutionized every facet of life - including communication, business operations and criminal investigations. With the exponential increase in the amount of data generated by digital devices, the amount of cybercrime has escalated and the traditional methods of forensic science have struggled to keep up with the vast amount of data and its complexity. Digital forensics, which is concerned with the identification, collection, and analysis of digital evidence, has become critical to criminal and civil investigations (Breitinger et al., 2024; Dweikat et al., 2021). However, manual analysis of the digital artifacts, like logs, browsing histories, or emails, is a time-consuming and inefficient process, leading to the development of AI-based automation (Dunsin et al., 2024; 2023; Agarwal et al., 2024a; Agarwal et al., 2024b).

AI has changed behaviour analysis in digital forensics by revealing user intent using machine learning and pattern recognition improving accuracy and reducing human bias (Lee & Soh, 2020; Sharma et al., 2019). It is useable for proactive anomaly detection and predictive modeling, which is essential for detecting insider threats and malicious activities (Ghanem et al., 2023; Rexha et al., 2023). Techniques like ML, NLP, and anomaly detection algorithms help in the speedy analysis of a large amount of evidence with improved precision (Sahoo et al., 2023; Preston et al., 2023).

Despite these benefits, the use of AI raises ethical and legal issues such as the violation of privacy rights, bias, and the admissibility of evidence (Dunsin et al., 2024; Lorch et al., 2022; Solanke, 2022). Therefore, the advancement of explainable and trustworthy AI is necessary for trustworthy digital forensic investigations (Beemkumar et al., 2023).

Recent developments in digital forensics need greater alignment between legal-ethical principles and actual investigative practice. Emerging environments - including blockchain, Internet of Things (IoT), mobile platforms and cloud infrastructures - raise complex challenges in data acquisition, attribution and chain-of-custody. These types of distributed systems also require new analytical and automation-based workflows for the timely triage, behavioural correlation and evidence preservation. Interidisciplinary perspectives in law, psychology and cybersecurity also contribute to understanding how human factors, expectations of privacy and social implications can further enrich the understanding of human factors. Integrating the use of forensic tools, automated processing and a structured workflow, in conjunction with

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186