Chapter 10
Behavioral Analysis and User Profiling in Forensic Investigations

Angel Justo Jones
https://orcid.org/0009-0007-9740-6611
University of Virginia, USA

Bianca Montes Jones
Capitol Technology University, USA

ABSTRACT

In the rapidly evolving field of digital forensics, the integration of behavioral analysis and user profiling has emerged as a critical component for enhancing investigation accuracy and efficiency. This chapter explores the role of behavioral analysis in forensic investigations, focusing on how user profiling techniques can be utilized to identify behavior patterns, track digital footprints, and detect anomalous activities. We examine various methods for collecting, analyzing, and interpreting user data from diverse digital sources, including social media, browsing history, and mobile devices. Furthermore, we discuss the challenges forensic experts face in handling large volumes of data, maintaining privacy, and ensuring the integrity of evidence. This chapter aims to provide insights into the growing importance of behavioral analysis and user profiling for modern forensic investigations in the digital age through a combination of AI-driven tools and traditional forensic methodologies.

DOI: 10.4018/979-8-3373-0857-9.ch010

1. INTRODUCTION

Digital forensics has become an essential field in investigating cybercrimes, helping to identify, preserve, and analyze digital evidence in a legally sound manner. As technology advances, the role of artificial intelligence (AI) and machine learning (ML) has gained significant prominence in enhancing digital forensic investigations, making them more efficient, accurate, and scalable. Among the key aspects of digital forensics, behavioral analysis, and user profiling play a crucial role in identifying patterns, reconstructing events, and making sense of complex data.

Behavioral analysis in the context of digital forensics involves the study of user actions, system behaviors, and digital footprints left behind during an investigation. This analysis can reveal insights into how individuals interact with systems, how they access sensitive information, and the types of anomalies that can indicate malicious behavior. By applying AI and machine learning, investigators can automate much of the process of identifying suspicious patterns or deviations in user behavior, reducing the workload and increasing the accuracy of investigations.

User profiling is another critical aspect of digital forensics, wherein investigators develop a profile of a user's typical behavior, preferences, and activities based on digital interactions. This profiling helps forensic investigators differentiate between normal and suspicious behavior by using algorithms that analyze large volumes of data. Through the combination of behavioral analysis and user profiling, forensic experts are better equipped to trace a suspect’s actions and intentions, even when those actions are deliberately hidden.

The need for sophisticated tools to analyze digital evidence has never been more pressing as the world becomes increasingly interconnected through the Internet of Things (IoT), cloud computing, and social media. Artificial intelligence has the potential to significantly enhance the capabilities of digital forensic investigators by not only automating routine tasks but also offering advanced techniques for anomaly detection, predictive analysis, and even decision-making in ambiguous situations.

This chapter explores the integration of behavioral analysis and user profiling in the context of digital forensics, with a particular focus on how AI can be leveraged to improve the process. We will highlight recent advancements in AI-based tools' application in analyzing digital evidence, identifying user behavior patterns, and profiling individuals involved in cybercrime. Additionally, the chapter will delve into the challenges and opportunities in this area, exploring how AI can help overcome traditional limitations in digital forensics.

Recent research has provided a solid foundation for the application of AI in digital forensics. For example, Bhawna and Mahajan (2024) discuss how AI perspectives are reshaping the field of digital forensics by enabling more efficient cyber threat detection, while Costantini, De Gasperis, and Olivieri (2019) examine the inter-