Chapter 1
Volatile Evidence:
Memory Forensics in Digital Investigations

Roshni Pandey
https://orcid.org/0009-0006-4379-4906
Gujarat University, India

Kiranbhai R. Dodiya
https://orcid.org/0009-0001-9409-7303
Gujarat University, India

Parvesh Sharma
https://orcid.org/0000-0002-0245-5186
Gujarat University, India

Kapil Kumar
Gujarat University, India

ABSTRACT

Volatile evidence in system memory (RAM) has become vital in digital forensics, capturing live data such as active processes, network sessions, cryptographic keys, and malware fragments often absent from disk analysis. Its transient nature makes memory forensics essential for reconstructing attacks, uncovering sophisticated intrusions, and exposing anti-forensic

DOI: 10.4018/979-8-3373-5992-2.ch001

tactics. This chapter examines key acquisition and analysis techniques, emphasizing challenges of volatility, scalability, and data integrity. It also explores advanced applications—like AI-driven anomaly detection, blockchain-based chain-of-custody, and quantum-safe approaches—positioning memory forensics as a cornerstone of next-generation digital investigations.

1. INTRODUCTION

To examine digital forensics today is to examine real-time, memory-centric investigations, probing for ephemeral digital traces. Of all media of digital evidence, random access memory (RAM) is the most elusive, most fragile, yet most vivid in capturing real-time events. The very notion of volatile data exists as long as the plummeting systems are powered, harbouring vital intel of the executed processes, the in-situ network sessions, the ephemeral encryption keys, and the overt actions of the users, which otherwise cease to exist post system shutdown. The Omnipresence of capturing evidence during a critical security incident is rare, yet in abundance. Fatefully, while capturing sensitive data in a decisive moment of time, evidence is the most volatile. For as long as cyber Investigation Forensics has existed, more focus has been based on pieces of non-volatile data (log files, a complex digital filing system, a copy of a hard drive, and other myriad digital Integration sheets). More Forensic Fileless Malware struggled far more than APTs(Mehmood, 2023a). However, as technology advanced, cyber forensics started focusing more and more on real-time evidence. Bridging the most critical gap in modern cyber investigations is memory forensics. The chapter analyses volatile memory from legal, technical, and forensic angles. It examines fundamental aspects, types of volatility, acquisition methods, analytical paradigms, and the evidential integrity paradox. The chapter advocates the need for greater standardisation of policy and practice, coupled with the deployment of technology like artificial intelligence, to process the vast quantities of digital data characteristic of contemporary technologies. They argue that forensics of the volatile memory is crucial for investigators, cybersecurity professionals, and law enforcement who need to gather and understand the ephemeral