Memory forensics plays a critical role in cybersecurity, particularly in analyzing volatile memory during cyberattacks. This paper examines memory forensics analysis on Intel-based Macintosh systems targeted by remote attacks within shared networks. The study used a controlled setup involving an Intel-based Macintosh running a vulnerable PHP-based web application, DVWA (Damn Vulnerable Web Application). The system was attacked via SQL injection, command injection, and reflected Cross-Site Scripting (XSS) from a Kali Linux device over shared Wi-Fi. The attacks exploited application vulnerabilities to compromise the system, necessitating forensic examination. Memory dumps from the Mac device were analyzed using tools like the Volatility Framework to extract artifacts such as process details, network activity, and injected code. Memory artifacts were correlated with Wireshark packet analysis to uncover network-level evidence. The findings underscored the impact of remote attacks on system integrity and the effectiveness of memory forensic methods. Unique challenges in MacOS forensics include kernel-level access requirements, System Integrity Protection (SIP), compressed swapped memory, and address space layout randomization. These protections complicate forensic analysis, demanding specialized techniques. This study enhances knowledge of macOS memory forensics under remote attack scenarios, proposing methodologies to address evolving threats and highlighting the importance of volatile data analysis in system security.

Keywords—Volatility Framework, RAM, Memory Forensic, DVWA, macOS