Forensik memori memiliki peran penting dalam keamanan siber, khususnya dalam menganalisis memori volatile selama serangan siber. Paper ini mengkaji analisis forensik memori pada sistem Macintosh berbasis Intel yang ditargetkan oleh serangan penyadapan dalam jaringan. Penelitian ini menggunakan pengaturan terkontrol yang melibatkan Macintosh berbasis Intel yang menjalankan aplikasi web berbasis PHP yang rentan, DVWA (Damn Vulnerable Web Application). Sistem diserang melalui injeksi SQL, injeksi perintah, dan mencerminkan Cross-Site Scripting (XSS) dari perangkat Kali Linux melalui Wi-Fi bersama. Serangan tersebut mengeksploitasi kerentanan aplikasi untuk membahayakan sistem, sehingga memerlukan pemeriksaan forensik. Dump memori dari perangkat Mac dianalisis menggunakan alat seperti Volatility Framework untuk mengekstrak artefak seperti detail proses, aktivitas jaringan, dan kode yang disuntikkan. Artefak memori dikorelasikan dengan analisis paket Wireshark untuk mengungkap bukti tingkat jaringan. Temuan ini menggarisbawahi dampak serangan jarak jauh terhadap integritas sistem dan efektivitas metode forensik memori. Tantangan unik dalam forensik MacOS mencakup persyaratan akses tingkat kernel, Perlindungan Integritas Sistem (SIP), memori pertukaran terkompresi, dan pengacakan tata letak ruang alamat. Perlindungan ini mempersulit analisis forensik dan memerlukan teknik khusus. Studi ini berkontribusi tentang forensik memori macOS dalam skenario serangan penydapan, mengusulkan metodologi untuk mengatasi ancaman yang terus berkembang dan menyoroti pentingnya analisis data yang mudah menguap dalam keamanan sistem.

Kata Kunci—Volatility Framework, RAM, Memory Forensic, DVWA, macOS