ABSTRAK

Semakin berkembangnya teknologi informasi dan komunikasi yang semakin canggih bedampak pada banyaknya celah keamanan yang ditemukan. Oleh karena itu dikembangkan teknik memori forensik untuk melakukan investigasi pada sistem yang telah diserang. Dalam penerapannya teknik memori forensik terdapat dua jenis, forensik tradisional dan *live* forensik. Karena dalam era digital yang sangat pesat penggunaan forensik tradisional dirasa sudah tidak efektif lagi dan digunakan teknik *live* forensik. Investigasi menggunakan teknik *live* forensik membutuhkan penanganan khusus sebab data *volatile* pada RAM dapat hilang jika sistem yang di investigasi mati.

Live forensik sendiri memiliki dua metode untuk mengimplementasikannya, metode internal (*incident response*) dan eksternal (*capture memory*). Metode internal adalah proses investigasi langsung menggunakan sistem yang telah diserang, sedangkan metode eksternal adalah proses investigasi yang dilakukan pada sistem investigator dengan melakukan *dumpmemory/memory imaging/*akuisisi memori terlebih dahulu pada sistem yang diserang untuk dipindahkan file hasil akuisisi memorinya pada sistem investigator.

Proses *dumpmemory* dilakukan dengan bantuan perangkat lunak tambahan untuk melakukan *capture memory.* Proses *dumpmemory* pada sistem operasi windows menggunakan FTK Imager, sedangkan untuk melakukan analisis dari hasil *dumpmemory* digunakan perangkat lunak *volatility, bulk extractor,* dan *wireshark.*

Hasil yang diperoleh adalah metode *dumpmemory* berhasil melakukan akuisisi terhadap *Random Access Memory* dan memberikan banyak informasi dalam *file image*-nya serta hasil analisa dari beberapa skenario serangan yang diujikan telah menghasilkan bukti yang *authentic* dan dapat dipertanggungjawabkan.

Kata Kunci: Forensik digital, live forensic, RAM, dumpmemory, akuisisi memori, memory imaging, analisis memori