Abstrak

Berkembangnya teknik enkripsi serta bertambahnya kapasitas media penyimpanan menyebabkan penggunaan teknik foreksik tradisional tidak memadai lagi. Oleh karena itu sebagai penggantinya digunakan teknik *live forensics* untuk melakukan investigasi. Investigasi menggunakan teknik *live forensics* memerlukan perhatian khusus sebab data *volatile* pada RAM yang dapat hilang jika sistem mati, serta kemungkinan tertimpanya data berharga yang ada pada RAM oleh aplikasi yang lainnya. Karena itu diperlukan metode *live forensics* yang dapat menjamin integritas data *volatile* tanpa menghilangkan data yang berpotensial menjadi barang bukti.

Pada tugas akhir ini dilakukan perbandingan metode *live forensics* yang memiliki kemampuan paling baik dalam melakukan *live forensics*. Kemampuan yang dimaksud adalah penggunaan *memory* yang kecil untuk menghindari tertimpanya data yang ada pada RAM, tidak melakukan perubahan pada *file* sistem, akurasi yang tinggi, waktu yang cepat serta jumlah langkah yang dilakukan dalam menganalisis.

Hasil yang diperoleh adalah metode *live forensics* yang memiliki performa terbaik adalah metode eksternal dengan ManTech sebagai *tools* akuisisi *memory* serta Volatility sebagai *tools* analisis dengan penggunaan *virtual memory* sebesar 24,492 KB, *working sets* 1,388 KB, melakukan penulisan pada registry sebanyak 8 key dengan akurasi 75% lalu waktu total yang digunakan 311 dan total langkah yang digunakan 22.

Kata kunci: **live forensic, *tools*, metode, windows xp, RAM, investigasi**