ABSTRAK

Malware merupakan sebuah perangkat lunak pada komputer yang sifatnya merusak, *malware* senantiasa dikembangkan untuk tujuan khusus atau merugikan pihak lain seperti tindakan kriminal dan sebagainya. Olehnya itu penting untuk mengetahui *file* atau proses dari memori yang ada pada perangkat kita agar tidak menjadi korban serangan *malware*.

Dari permasalahan di atas, maka tugas akhir ini akan merancang sebuah aplikasi yang dapat melakukan analisis dan klasifikasi kategori *malware* pada proses memori volatil. Dalam aplikasi ini digunakan teknik forensik dan pemindaian yara serta virustotal berbasi CLI. Teknik forensik digunakan untuk melakukan analisis proses pada memori volatil sistem dan pemindaian yara digunakan untuk pengklasifikasian *malware* metode I dan pemindaian virustotal berbasis CLI untuk pengklasifikasian *malware* metode II.

Setelah dilakukan analisis proses pada memori maka dilakukan proses klasifikasi *malware* berdasarkan aturan yara atau nilai hash. Proses pada metode I dengan mengecek nilai *string* pada *file* yang diduga *malware* lalu mencocokkan dengan aturan yara yang ada, untuk metode II dilakukan proses *hashing* terlebih dahulu lalu menggunakan nilai hash tadi untuk memulai metode II. Proses ini terbukti tidak membutuhkan waktu lama dengan data hasil pengujian 30 kali percobaan dengan 5 *file* memori masing-masing diuji 6 kali didapatkan hasil 16.053 detik untuk metode I dan 3.516 detik untuk metode II dengan tingkat akurasi dalam memindai proses *ID* pada memori sebesar 50% untuk metode I dan 79%.

Kata Kunci: Forensik Digital, Forensik *Malware*, Forensik Memori, *VirusTotal*, *YaraScan.*