ABSTRAK

Citadel malware merupakan suatu *malware* yang dikenal sebagai versi lanjutan dari *zeus malware* yang memiliki dampak yang begitu besar atas kerugian yang ditimbulkan dari transaksi perbankan illegal. Aktifitasnya sangat bersangkutan dengan jaringan dan memori komputer karena proses terjadi ketika sistem saling terhubung dengan keadaan komputer yang sedang menyala. Oleh karena itu, dibutuhkan penanganan khusus untuk melakukan kegiatan investigasi kejahatan yang terkait aktivitas *malware*, yaitu dengan mengimplementasikan teknik *live forensics* pada digital forensik. Prinsip kerja dari *live forensics* adalah menyelamatkan bukti digital berupa proses dan segala aktivitas komputer ketika dalam keadaan menyala dan terhubung pada sebuah jaringan komputer, hal ini disebabkan karena barang bukti digital pada komputer akan menghilang apabila komputer telah dimatikan sehingga teknik *live forensics* menjadi pilihan tepat dalam menangani kasus *malware.* Penelitian ini dilakukan dengan membandingkan dua kerangka investigasi yang nantinya dilakukan proses evaluasi untuk mendapatkan kerangka investigasi yang lebih baik, analisis yang dilakukan diantaranya adalah penanganan bukti digital, *capture image*, analisis *process*, analisis *apihooks*, analisis *registry*, analisis *dump process*, dan analisis *file dump.* Proses analisis ini dilakukan menggunakan *tools volatility* yang berjalan pada sistem operasi perangkat Linux. Hasil analisis memperlihatkan bahwa kerangka investigasi Aan lebih baik dibandingkan dengan kerangka investigasi Philip dalam penanganan kasus *malware forensics.*

Kata kunci : *Malware, Citadel*, *live forensics*, bukti digital, *malware forensics.*