Abstrak

Semakin berkembangnya teknik *anti forensic* dan bertambahnya kapasitas media penyimpanan menyebabkan pemakaian teknik *traditional forensic* menjadi kurang efisien. Untuk mengatasi permasalahan tersebut, maka digunakan teknik *live forensic* yang memiliki kecepatan terhadap proses investigasi. *Live forensic* menggunakan data *volatile* sebagai barang bukti sehingga penanganan khusus harus dilakukan. *Network forensic* dilakukan dengan teknik *live forensic* karena informasi yang dihasilkan bersifat *volatile*. Untuk melakukan analisa data pada *network forensic*, penggunaan *tools* yang tepat juga berpengaruh terhadap barang bukti yang akan diproses dan dipertanggungjawabkan di pengadilan. Penggunaan *tools network forensic* akan meninggalkan jejak pada *memory*, sedangkan data *volatile* yang sangat penting berada pada *memory*. Metode antarmuka *network forensic tools* sangat berpengaruh terhadap penggunaan *memory*, sehingga pada tugas akhir ini akan dianalisa metode antarmuka *tools* terhadap parameter akuisisi *memory* dan *file* sistem untuk mengukur dampak metode tersebut terhadap sistem. Selain itu akurasi dan waktu penggunaan(*elapsed time*) *tools* juga menjadi perhatian dalam melakukan proses *live forensic*

Pada tugas akhir ini akan dilakukan pengujian terhadap dua *tools* yang memiliki metode antarmuka yang berbeda, yaitu TCPView dengan antarmuka *Graphical User Interface(GUI)* dan Openports dengan antarmuka *command line.* Pengukuran dampak terhadap memory menggunakan parameter *memory footprint*, penggunaan *file library* sistem(DLL) dan penulisan *registry*, akurasi dan waktu penggunaan(*elapsed time*) *tools* tersebut.

Berdasarkan hasil pengujian yang telah dilakukan, metode antarmuka *command line* merupakan metode antarmuka terbaik untuk melakukan proses *live forensic* karena penggunaan *memory footprint*, penggunaan *file library* sistem dan penulisan *registry* serta *elapsed time* yang lebih rendah daripada metode antarmuka *Graphical User Interface*(GUI). Akurasi yang dihasilkan metode *command line* juga sama baiknya dengan metode antarmuka *Graphical User Interface*(GUI).

Kata kunci: ***traditional forensic, live forensic, network forensic, Graphical User Interface, command line, TCPView, Openports, memory footprint***