1. PENDAHULUAN

1.1 Latar Belakang

Network forensic merupakan cabang ilmu dari *computer forensic* yang berhubungan dengan analisis dan pengawasan *traffic* pada jaringan komputer yang bertujuan untuk pengumpulan informasi dan bukti, atau deteksi gangguan. Tidak seperti area lain dari *computer forensic*, *network forensic* sangat berhubungan dengan *volatile* dan *dynamic information***[11].** *Traffic* jaringan di transmisikan kemudian *traffic* tersebut hilang, jadi *network forensic* adalah investigasi yang dilakukan secara proaktif.

Computer forensic pada awalnya dilakukan dengan cara menghidupkan perangkat yang diduga menjadi penyerang dan melakukan proses pemeriksaan pada media penyimpanan yang bersifat *non-volatile*. Cara ini disebut dengan *traditional forensic*. Namun dengan berkembangnya teknologi dan *tools* serta teknik *anti-forensic* yang makin canggih, maka teknik tersebut dapat menyembunyikan bukti penting yang bisa digunakan untuk proses investigasi. Selain itu, kelemahan *traditional forensic* yang lain adalah media penyimpanan atau perangkat saat ini yang memiliki kapasitas yang sangat besar sehingga membutuhkan waktu yang lama untuk proses analisis dan duplikasi barang bukti. Pemutusan hubungan listrik juga bisa mengakibatkan rusaknya bukti penting dan potensial untuk proses investigasi**[9]**.

Dengan kelemahan dari *traditional forensic* tersebut, maka dibutuhkan suatu teknik yang dapat mengumpulkan barang bukti secara cepat dan akurat. Teknik *live forensic* adalah pengembangan dari *traditional forensic*. Teknik analisis *live forensic* dilakukan dengan menggunakan data *volatile* yang ada pada RAM*(Random Access Memory)* sehingga analisis dan pengumpulan *data volatile* dapat dilakukan dalam waktu lebih cepat dibandingkan dengan *traditional forensic*. Karena *network forensic* dilakukan secara proaktif dan berhubungan dengan informasi yang bersifat *volatile*, maka pada penelitian kali ini akan digunakan teknik *live forensic.*

Data *volatile* merupakan data yang sangat penting karena dapat memberikan informasi yang lebih baik tentang jalannya sistem pada saat, atau setelah terjadi serangan**[5][7].** Karena mengandung informasi yang sangat penting, maka penanganan terhadap data *volatile* pada RAM harus hati-hati. Selain data akan hilang jika komputer dimatikan, juga penggunaan *network forensic tools* dapat meninggalkan jejak pada RAM sehingga akan menimpa bukti penting yang ada pada RAM**[6]**. Oleh karena itu dibutuhkan *network forensic tools* yang memiliki dampak paling kecil pada *memory* RAM tersebut.

Pada penelitian sebelumnya, dilakukan pengujian terhadap beberapa *network forensic tools*. Dari penelitian tersebut didapat TCPView dan Openports merupakan *tools* yang memiliki jejak paling sedikit terhadap *memory***[9].** Kedua *tools* tersebut memiliki metode antarmuka yang berbeda, dimana TCPView berbasis GUI(*Graphical User Interface*) dan Openports berbasis *command line*. Metode antarmuka tersebut tentu menghasilkan jejak yang berbeda pula pada *memory* maupun di sistem. Dengan menggunakan teknik *live forensic* dan data *volatile* pada *memory* RAM, tentu akuisisi *network forensic tools* terhadap *memory* menjadi hal yang sangat penting untuk diuji dan diukur sesuai dengan

metode antarmuka *tools* yang digunakan. Alasan pengujian kedua metode antarmuka *tools* tersebut adalah karena sampai sekarang belum ada standarisasi mengenai metode antarmuka yang paling tepat untuk digunakan untuk semua kasus forensik. Masing-masing metode memiliki kelebihan dan kekurangan masing-masing sehingga perlu dilakukan pengujian dengan skenario kasus tertentu dan selanjutnya dapat dilihat pengaruhnya terhadap sistem menggunakan parameter akuisisi memori dan file sistem.

Oleh karena itu, dalam tugas akhir ini akan dilakukan pengujian metode antarmuka *Graphical User Interface*(GUI) dengan *tools* TCPView dan *command line* dengan *tools* Openports untuk mengukur dampak kedua metode tersebut pada *memory* dengan menggunakan parameter akuisisi *memory*, seperti *memory footprint*, penggunaan *file registry* dan *library* sistem, waktu yang digunakan, serta akurasi untuk mengukur performansinya sesuai dengan metode antarmuka yang digunakan. Pengujian *tools* dilakukan dengan beberapa simulasi kasus sehingga diharapkan akan didapat kinerja *tools* sesuai dengan metode masing-masing dan kasus yang dihadapi.

1.2 Perumusan masalah

Dengan latar belakang yang telah disebutkan sebelumnya, maka masalah yang dapat diangkat adalah sebagai berikut:

1. Bagaimana mengukur dampak metode antarmuka *Graphical User Interface*(GUI) dan *command line* terhadap *memory* berdasarkan parameter akuisisi *memory* dan *file* sistem yaitu *memory footprint*, penggunaan *file library* sistem dan *registry* sistem, waktu yang digunakan, serta akurasi dari dua *tools* tersebut sesuai dengan kasus yang dihadapi.
2. Bagaimana membandingkan dan menganalisis performa metode antarmuka *Graphical User Interface*(GUI) dan *command line* sesuai dengan kasus yang dihadapi.

Dari perumusan masalah di atas, maka disusun juga batasan masalah yang akan ditangani yaitu:

1. Proses pengambilan data dilakukan pada saat komputer dalam keadaan menyala untuk semua kasus
2. Sistem operasi yang digunakan adalah Windows 7 Ultimate Edition.
3. Jaringan yang digunakan berbasis IPv4 dan arsitektur jaringan pengujian kasus menggunakan *link point-to-point* antara komputer penyerang dan korban.
4. Tidak membahas analisis lanjutan dari proses *network forensic* untuk skenario kasus yang telah dibuat.

1.3 Tujuan

Berdasarkan perumusan masalah, diharapkan tercapai beberapa tujuan sebagai berikut:

1. Mengukur dan membandingkan dampak penggunaan metode antarmuka *Graphical User Interface*(GUI) dan *command line* terhadap *memory* berdasarkan parameter akuisisi memory dan file sistem yaitu *memory footprint*, penggunaan *file library* sistem dan *registry* sistem, waktu yang digunakan serta akurasi dari dua *tools* tersebut.

2. Menentukan metode antarmuka terbaik dalam proses *live forensic* sesuai dengan skenario kasus yang dihadapi

1.4 Hipotesa

TCPView dan Openports memiliki implikasi yang berbeda terhadap sistem *memory* karena memiliki metode antarmuka yang berbeda, yaitu TCPView menggunakan *Graphical User Interface*(GUI) dan Openports menggunakan *command line*. Pada parameter *memory footprint*, TCPView memiliki *working set* dan *virtual bytes* lebih besar daripada Openports. Untuk parameter *time and file system impact*, Openports unggul dalam hal akuisisi file sistem karena paling sedikit dampaknya terhadap *registry* maupun pengelolaan *file library*. Pada tugas akhir ini diharapkan dapat diuji kedua aplikasi tersebut agar diperoleh data dan dampaknya terhadap sistem sesuai dengan skenario kasus yang dihadapi.

1.5 Metodologi Penyelesaian Masalah

Metode penelitian yang akan digunakan dalam menyelesaikan permasalahan yang ada adalah sebagai berikut :

1. Tahap studi literatur
   Pada tahap ini akan pendalaman pemahaman tentang konsep dan teori dari *forensic networking*, baik melalui literatur maupun pustaka *online*. Untuk dasar teori tentang *network forensic*, sumber berasal dari jurnal *online* internasional seperti *direct science, google scholar*,dan *elsevier*. Untuk referensi *tools* dan pengujiannya didapat dari jurnal internasional berjudul "*Acquiring Volatile Operating System Data Tools and Technique*" karya Ian Sutherland, Jon Evans, Theodore Tryfonas, dan Andrew Blyth.
2. Tahap perancangan sistem
   Pada tahap ini akan dilakukan perancangan aplikasi dan pengumpulan data *volatile* dengan beberapa *tools* dan dilanjutkan dengan proses uji performansi TCPView dan Openports. Uji performansi dilakukan dengan mempersiapkan beberapa *profiling tools* dan skenario kasus kejahatan jaringan komputer.
3. Tahap pengujian dan analisis
   Pada tahap ini akan dilakukan pengumpulan data *volatile* menggunakan aplikasi perantara yang terintegrasi dengan beberapa *forensic tools* termasuk TCPView dan Openports, kemudian mengukur dampak metode antarmuka TCPView dan Openports menggunakan *profiling tools* sesuai dengan kasus yang dibuat. Kemudian membandingkan dan menganalisis hasil pengujian berdasarkan parameter akusisi memori dan metode antarmuka dari *tools* tersebut.
4. Penulisan laporan
   Tahap penulisan laporan dilakukan dengan mengumpulkan seluruh dokumentasi perancangan, pengujian, dan penyimpulan hasil akhir dari penelitian