

BAB I PENDAHULUAN

1.1 Latar Belakang

Forensik komputer adalah bidang forensik digital yang muncul karena kemajuan teknologi yang pesat untuk melacak, mengumpulkan, dan menganalisis data yang diperlukan untuk membuktikan kejahatan di dunia digital dalam bentuk bukti digital atau bukti digital yang menjadikan ini sebagai bukti di pengadilan. Dalam forensik digital, terdapat beberapa tahapan yang harus dilakukan. Tahapan ini dalam beberapa kasus dan menurut beberapa pendapat bisa menjadi tiga tahap atau pun lebih. Namun yang menjadi sangat penting yaitu akuisisi, analisa dan laporan [1]. Model lain dari tahapan dalam forensik digital yaitu *Digital Investigate Framework* dari *Digital Forensics Research Workshop (DFRWS)* [2], [3]. Dalam kerangka tersebut terdapat *Identification, Preservation, Collection, Examination, Analysis dan Presentation*.

Banyak alat-alat pembantu yang dikembangkan untuk keperluan forensik digital. Semuanya jika digolongkan berdasarkan kode sumber yaitu bebas pakai dan sumber terbuka (*open source*) dan sumber tertutup (*close source*). Autopsy merupakan salah satu alat dengan sumber terbuka yang dikembangkan untuk keperluan forensik digital oleh Brian Carrier. Sebelumnya Brian Carrier telah mengembangkan The Sleuth Kit yang berjalan pada mode terminal, kemudian melahirkan Autopsy sebagai antarmuka pengguna dari The Sleuth Kit [4]. Pengembangan awal Autopsy menggunakan teknologi web, kemudian ditahun 2010 Autopsy mulai mengembangkan versi desktopnya. Hingga saat ini Autopsy sudah mencapai versi 5 dan masih tetap dengan sumber terbuka [5].

The Sleuth Kit dan Autopsy dalam halaman resmi masing-masing membuat daftar fiturnya dan tidak menyatakan bahwa terdapat dukungan untuk fitur akuisisi. Keduanya memiliki fokus terhadap analisa dari sistem berkas [6]. Namun sekali lagi dari penjelasan diawal yaitu terdapat tahapan-tahapan yang harus dilakukan dalam forensik digital agar terjamin, diakui dan dinyatakan sah dalam

hukum. Tahapan yang harus dilalui adalah tahapan akuisisi data, dan The Sleuth Kit dan Autopsy belum menyediakan fitur tersebut. Biasanya para investigator mengkalinya dengan menggunakan aplikasi pihak ketiga atau alat-alat akuisisi lain, seperti FTK Imager, EnCase Imager, AFF4 Imager dan DD.

Dari penjelasan tersebut penulis memiliki inisiatif untuk membuat pengembangan agar Autopsy sendiri dapat memenuhi tahapan dalam forensik digital, lebih khusus lagi dalam tahapan akuisisi data. Selain itu penulis juga merasa terpacu untuk mengembangkan penelitian ini karena dalam Autopsy sendiri membuka kesempatan bagi para penggunanya untuk mengembangkan modul sendiri untuk keperluan yang lebih dalam mengenai forensik digital, terutama dalam analisa sistem berkas. Namun tidak banyak yang mengembangkan modul untuk keperluan akuisisi data.

1.2 Rumusan Masalah

Bagaimana cara merancang atau mengembangkan sistem fitur akuisisi pada aplikasi autopsy?

1.3 Batasan Masalah

Berisi teknologi apa yang digunakan dalam skripsi, dan lingkup pembahasan skripsi.

- a. Pengembangan hanya berfokus pada sistem operasi windows.
- b. Bahasa pemrograman yang dipakai adalah java.

1.4 Tujuan Penelitian

Tujuan laporan skripsi ini adalah mengembangkan fitur akuisisi pada aplikasi Autopsy dengan memahami konsep akuisisi data digital, menganalisis fitur akuisisi yang ada, dan mengimplementasikan perubahan yang diperlukan.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini dapat membantu dan menyelesaikan permasalahan-permasalahan yang terjadi pada pengembangan fitur akuisisi pada aplikasi autopsy

1.6 Sistematika Penulisan

Sistematika penulisan dalam menyusun laporan penelitian ini, untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah dan hipotesis, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, berisi: hasil penelitian sejenis yang sudah pernah dilakukan sebelumnya, teori penunjang, dan referensi berupa buku, jurnal, dan laporan skripsi/tesis.

Bab III Metodologi Penelitian, berisi: penjelasan mengenai metode penelitian yang digunakan untuk memahami dan mengeksplorasi obyek penelitian, hasil observasi / pengumpulan data, masalah yang terdapat pada obyek, dan gambaran umum proyek atau obyek penelitian, hingga Rencana Alur Penelitian.

Bab IV Pembahasan, berisi: rancangan proyek, implementasi *coding* dan desain, serta evaluasi rancangan. Selanjutnya alur pengerjaan proyek, metode testing, hingga hasil akhir penelitian dan pembahasan analisis hasil akhir penelitian, termasuk pembahasan hasil-hasil uji coba (*testing*). Data hasil akhir pengujian dapat berupa grafik, table, data monitoring, log system, dan lain-lain, dengan pembahasan.

Bab V Penutup, berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.