BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Era digital bisa dikarakteristikkan sebagai penerapan dari teknologi komputer. Penggabungan sistem komputer sebagai alat menjadi privasi, komersial, edukasi, pemerintahan, dan sisi lain dari hidup modern telah meningkatkan produktivitas dan efesiensi dari entitas ini. Dengan cara yang sama, pengenalan komputer sebagai alat kriminal telah meningkatkan kemampuan para kriminal untuk melakukan penyembunyian, atau membantu aktivitas yang melanggar hukum. Secara khusus, peningkatan kemampuan teknis dari populasi umum, ditambah dengan anonimitas, nampaknya mendorong kejahatan menggunakan sistem komputer karena kecil kemungkinan untuk diadili, apalagi ditangkap (Maher, 2000).

Dalam beberapa kasus kriminal seperti korupsi, bukti digital dapat berupa *file* yang sudah dihapus dari *file system* dan pada kenyataannya itu masih bisa dikembalikan. *File* yang sudah dihapus dari *file system* tidak bisa diakses melalui *file manager*. Namun, *file* tersebut masih berada di dalam *hard disk* dan bisa dikembalikan selama ruang alokasi untuk *file* tersebut belum ditimpa dengan data yang lain, melalui penghapusan atau pembersihan *hard disk* (Aburabie dan Alomari, 2006). Saat itulah para ahli ilmu digital forensik menjadi solusi karena mampu membongkar fakta-fakta penting di sidang, mencegah dan melacak pelaku *cybercrime* yang berbahaya dan merugikan (Ramdan, 2017).

Digital forensik adalah satu cabang ilmu forensik yang menggunakan teknik analisis dan investigasi untuk mengidentifikasi/menemukan, mengumpulkan,

memeriksa dan menyimpan bukti/informasi pada sistem komputer atau media penyimpanan digital dengan sebuah standard dan dokumentasi tertentu untuk dapat diajukan sebagai bukti hukum yang sah (Sinambela, 2016).

Pada persidangan kasus Jessica yang lalu turut dihadirkan beberapa ahli digital forensik untuk memaparkan hasil analisisnya terhadap barang bukti yang didapatkan dari penyidik. Barang bukti tersebut berupa *Universal Serial Bus* (USB) Flashdisk yang menyimpan video *Closed-Circuit Television* (CCTV) hasil ekstraksi dari *Digital Video Recorder* (DVR) system monitoring CCTV di Cafe Olivier (Tempat Kejadian Perkara) (Sinambela, 2016). Ahli digital forensik, Christopher Hariman Rianto menyebut *file* barang bukti disalin dengan *forensic imaging* (Muhardi, 2016).

Sebuah *forensic image* mengandung *current file* baik dengan *slack space* dan *unallocated space*. Berhubungan dengan hasil forensik seperti *file* yang dihapus, bagian *file* yang dihapus dan data tersembunyi bisa ditemukan pada *slack space* dan *unallocated space* (Vandeven, 2014). Dalam digital forensik, pencarian teks string digunakan untuk menemukan setiap *byte* dari bukti digital pada level fisik, untuk melokasikan teks string spesifik yang menarik untuk diinvestigasi (Soni, Vyas, dan Sinhal, 2014). Dengan pencarian menggunakan *strings*, seorang analis dapat mengidentifikasi hasil forensik yang berada pada *slack space*, dalam *file* yang terhapus dan *unallocated space*, atau pada *file* yang sudah ada (Schwartz dan Liebrock, 2008).

Untuk melakukan pencarian *file* pada *forensic image*, dapat digunakan algoritma pencarian teks. Salah satu algoritma yang dapat digunakan adalah *Aho-Corasick* yang berguna untuk pencocokan banyak pola dengan *execution time* O

(n+m+z) (Pandiselvam, Marimuthu, dan Lawrance, 2014) dimana n adalah jumlah pola, m adalah panjang teks yang digunakan, dan z adalah jumlah pola yang terjadi (Sitompul, Handoko, dan Rahmat, 2016).

Penelitian mengenai pencarian *file* dengan menggunakan algoritma *Aho-Corasick* telah dilakukan oleh Sitompul, Handoko, dan Rahmat (2016). Pencarian *file* dilakukan berdasarkan keyword yang dipisah dengan spasi sebagai pemisah. Penelitian tersebut menggunakan *disk image* berukuran 4GB dengan ukuran efektif 3,60GB. Terdapat 56 *file* dengan total ukuran 3,45GB, dan berhasil melakukan pencarian dan extraksi *file* sebanyak 55 *file* (98,21%), kemudian dihitung *elapsed times* untuk setiap pencarian yang dilakukan dan mendapatkan total waktu 3,198 detik dengan rata-rata waktu 0,320 detik dari 10 kali pencarian yang dilakukan. Terdapat juga pencarian *file* dengan menggunakan algoritma *Boyer-Moore* yang telah dilakukan oleh Povar dan Bhadran (2010) dengan rata-rata jumlah *file* yang ditemukan secara utuh adalah 87%. Berdasarkan latar belakang tersebut, dilakukan implementasi algoritma pencocokan string *Aho-Corasick* untuk melakukan pencarian teks string pada aplikasi pencari *file* dalam *forensic image* untuk digital forensik.

1.2 Rumusan Masalah

Berdasarkan kebutuhan yang dijabarkan sebelumnya, masalah yang dirumuskan antara lain sebagai berikut.

a. Bagaimana mengimplementasikan algoritma *Aho-Corasick* pada aplikasi pencari *file* dalam *forensic image* untuk *digital forensic*?

b. Berapa tingkat *precision, recall,* dan *f-measure* dari aplikasi pencari *file* dalam *forensic image*?

c. Berapa kecepatan dari aplikasi pencari *file* dalam *forensic image*?

1.3 Batasan Masalah

Batasan masalah dibagi menjadi dua, yaitu batasan konsep dan teknis. Batasan dari sisi konsep antara lain sebagai berikut.

a. Kamus data yang digunakan berupa *file extension* (gif, jpg, jpeg, exe, zip, jar, doc, docx, xls, xlsx, ppt, pptx, rar, png, pdf, wma, wmv, wav, avi, mp3, bmp, iso, tar, 7z, mkv, xml, rtf, mpg, mpeg, dat).

b. *File System* yang digunakan *New Technology File System* (NTFS).

c. Batasan dari sisi teknis adalah aplikasi dijalankan pada *desktop*.

1.4 Tujuan Penelitian

Sesuai dengan rumusan masalah, tujuan dari penelitian ini antara lain sebagai berikut.

a. Mengimplementasikan algoritma *Aho-Corasick* pada aplikasi pencari *file* dalam *forensic image* untuk *digital forensic*.

b. Mengukur tingkat *precision, recall,* dan *f-measure* dalam aplikasi pencari *file* dalam *forensic image*.

c. Mengukur kecepatan dari aplikasi pencari *file* dalam *forensic image*.

1.5 Manfaat penelitian

Manfaat yang diharapkan dari implementasi algoritma *Aho-Corasick* pada aplikasi pencari *file* dalam *forensic image* untuk *digital forensic* yaitu dapat

membantu mendapatkan *file* yang dibutuhkan dalam *forensic image* tanpa harus melakukan ekstraksi *forensic image* secara keseluruhan sehingga menghemat banyak waktu dalam melakukan kegiatan *digital forensic*.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyajian laporan skripsi ini adalah sebagai berikut.

1. BAB I PENDAHULUAN

Bab ini berisi latar belakang pemilihan judul "Implementasi Algoritma *Aho-Corasick* pada Aplikasi Pencari *File* dalam *Forensic Image* untuk *Digital Forensic*", rumusan masalah, batasan masalah dalam penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan skripsi.

2. BAB II LANDASAN TEORI

Bab ini berisi dasar-dasar teori yang digunakan dalam penelitian terkait permasalahan yang dibahas. Teori-teori yang digunakan dalam penelitian ini antara lain *Digital Forensic*, *New Technology File System* (NTFS), *Master File* Table (MFT), *Forensic Image, File Signature,* algoritma *Aho-Corasick*, FTK Imager, HashMyFiles, *Architecture of File Undelete with Aho-Corasick algorithm* dan *F-measure*.

3. BAB III METODOLOGI DAN PERANCANGAN APLIKASI

Bab ini berisi metodologi penelitian yang terdiri dari studi literatur, perancangan, pembangunan aplikasi, *testing* dan *debugging* aplikasi, dan analisis hasil uji coba aplikasi. Perancangan aplikasi terdiri atas *flowchart diagram* dan

mock-up tampilan antarmuka dari aplikasi yang dirancang dan dibangun dengan implementasi algoritma *Aho*-Corasick.

4. BAB IV IMPLEMENTASI DAN HASIL UJI COBA

Bab ini berisi hasil implementasi algoritma, diikuti oleh data hasil uji coba penelitian yang dilakukan beserta hasil analisis data berdasarkan hasil uji coba penelitian yang dilakukan.

5. BAB V SIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil uji coba dan analisis yang telah dilakukan dalam penelitian, beserta saran untuk pengembangan penelitian lebih lanjut.