FORENSIC IMAGING APPLICATION USING RASPBERRY PI

APLIKASI FORENSIC IMAGING MENGGUNAKAN RASPBERRY PI

Razan Maulida Komaryan
Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Jalan Kaliurang Km. 14,5 Yogyakarta 55501-Indonesia
Telp. (0274) 895287 ext. 122, Faks. (0274) 895007 ext 148
e-mail:13523228@students.uii.ac.id

Fietyata Yudha S.Kom., M.Kom
Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Jalan Kaliurang Km. 14,5 Yogyakarta 55501-Indonesia
Telp. (0274) 895287 ext. 122, Faks. (0274) 895007 ext 148

***Abstract* - Cybercrime atau kejahatan siber adalah sebuah tindak pidana kejahatan yang merugikan orang lain dengan memanfaatkan komputer sebagai media kejahatannya. Tren kejahatan siber terus mengalami kenaikan, menurut data kepolisian Republik Indonesia jumlah kejahatan siber yang ditangani Polri pada tahun 2017 mengalami kenaikan sebesar 3% jika dibandingkan dengan kejahatan siber yang ditangani Polri pada tahun 2016. Untuk membuktikan sebuah kejahatan siber maka diperlukan barang bukti sebagai pembuktian di mata hukum. Untuk mendapatkan barang bukti kejahatan siber yang tertinggal di media penyimpanan dibutuhkan aplikasi forensic imaging yang mampu melakukan akusisi terhadap media penyimpanan. Berdasarkan uraian masalah diatas, penenliti mengangkat judul "Forensic Imaging Application Using Raspberry Pi".**

Keywords – Cybercrime, Forensic Imaging

I. PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komputer sangat terasa di tengah kehidupan masyarakat. Karena dengan berkembangnya teknologi informasi dan komputer dapat mempermudah pekerjaan manusia, mulai dari anak – anak yang masih duduk di bangku sekolah hingga orang dewasa memanfaatkannya guna membantu menyelesaikan pekerjaan mereka. Namun ada saja pihak - pihak yang memanfaatkan kemajuan teknologi informasi dan komputer ini untuk berbuat hal – hal negatif yang sifatnya mengarah kepada modus kejahatan. Selanjutnya istilah kejahatan yang memanfaatkan komputer disebut cybercrime. Dilansir dari situs kominfo.go.id Wakil Kepala Kepolisian Republik Indonesia Komisaris Jendral Syafruddin mengatakan bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahaan siber tertinggi. Kejahatan siber di Indonesia tertinggi ke dua di dunia setelah Jepang. Total serangan kejahatan siber di Indonesia mencapai 90 juta [1].

Cybercrime adalah kejahatan yang dilakukan oleh pihak yang tidak bertanggung jawab dengan tujuan untuk merusak, memodifikasi dan mengeliminasi data [2]. Menurut Muhammad Nur Al-Azhar dalam bukunya yang berjudul Digital Forensic, cybercrime merupakan kejahatan yang menggunakan komputer sebagai alat utama untuk melakukan aksi kejahatannya, misalnya defacement (pengubahan halaman – halaman suatu situs secara ilegal), denial distributed of service (membuat suatu sistem tidak berjalan atau berfungsi sebagaimana mestinya setelah dibanjiri data oleh sekian banyak komputer yang telah terinfeksi dan menjadi robot network), intrusion (masuk secara ilegal ke dalam suatu sistem), dan lain–lain [3]. Guna menangkal cybercrime maka harus ada perangkat hukum yang jelas, dalam hal ini perangkat hukum dibuat dalam bentuk aturan dan perundang - undangan. Disisi lain dari aspek ilmiah dan teknis juga diperlukan mekanisme pembuktian. Dalam hal ini komputer forensik adalah salah satu bidang yang dapat membantu dalam upaya pembuktian cybercrime.

Menurut Muhammad Nur Al-Azhar dalam bukunya yang berjudul Digital Forensic, komputer forensik adalah ilmu forensik yang berkaitan dengan pemeriksaan dan analisis barang bukti elektronik berupa komputer pribadi (personal computer-PC), laptop/notebook, netbook, dan tablet. Pemeriksaan terhadap jenis barang bukti ini biasanya berkaitan dengan file recovery, yaitu suatu metode untuk mengambil file logical atau memunculkan kembali file yang sudah dihapus (deleted) maupun hilang (lost) dikarenakan tidak tercatat lagi di file system. File–file tersebut diperlukan untuk membuktikan kejahatan yang terjadi dan menghubungkannya dengan pelaku [3]. Peran komputer forensik menjadi vital guna mengungkap

setiap kehajatan siber, dilansir dari berita elektronik pada situs nasional.kompas.com, Kapolri Jendral Pol Tito Karnavian mengatakan, ada peningkatan jumlah perkara yang menyangkut kejahatan dunia maya atau cybercrime. Jika dibandingkan dengan tahun 2016, pada tahun 2017 mengalami kenaikan sebanyak tiga persen. Pada 2016 kejahatan siber yang ditangani Polri sebanyak 4.931 kasus, dan yang berhasil diselesaikan sebanyak 1.119 kasus, sedangkan pada tahun 2017 kejahatan siber yang ditangani Polri sebanyak 5.061 kasus, dan yang berhasil diselesaikan sebanyak 1.368 kasus [4].

Salah satu cara agar mengamankan barang bukti digital dengan menyalin data dari media penyimpanan secara Bitstream Image dan menempatkannya pada tempat yang aman. Teknik mengambil bit demi bit data dari media penyimpanan fisik disebut Cloning Disk, dan hasil dari cloning tersebut disebut imaging. Bitstream adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk file yang tersembunyi (hidden file), file temporer (temp file), file yang terdefragmen (fragmen file), dan file yang belum ter-overwrite [5].

Penelitian ini dilakukan untuk membuat perangkat *forensic imaging* dengan memanfaatkan *single board computer* Raspberry Pi sebagai papan sirkuitnya. Kemudian untuk mengoperasikan perangkat *forensic imaging* tersebut, maka dibuatkan aplikasi berbasis *Graphical User Interface* (GUI). Dengan dilakukannya penelitian ini diharapkan peneliti mampu membuat perangkat *forensic imaging* yang dapat melakukan akusisi media penyimpanan dengan menggunakan Raspberry Pi sebagai *single board computer* nya.

II. LANDASAN TEORI

A. *Cybercrime*

Cybercrime atau kejahatan siber adalah sebuah tindak pidana kejahatan yang lahir karena kemajuan teknologi informasi yang merugikan orang lain dengan memanfaatkan komputer sebagai media kejahatannya. Pelaku kejahatan siber dapat dituntut dengan undang-undang nomor 11 tahun 2008 tentang transaksi dan elektronik (UU ITE). Cybercrime adalah kejahatan yang dilakukan oleh pihak yang tidak bertanggung jawab dengan tujuan untuk merusak, memodifikasi dan mengeliminasi data [2]. Sedangkan menurut Muhammad Nur Al-Azhar dalam bukunya yang berjudul Digital Forensic, cybercrime merupakan kejahatan yang menggunakan komputer sebagai alat utama untuk melakukan aksi kejahatannya, misalnya defacement (pengubahan halaman – halaman suatu situs secara ilegal), denial distributed of service (membuat suatu sistem tidak berjalan atau berfungsi sebagaimana mestinya setelah dibanjiri data oleh sekian banyak komputer yang telah terinfeksi dan menjadi robot network), intrusion (masuk secara ilegal ke dalam suatu sistem), dan lain–lain [3].

Dilansir dari media online tekno.kompas.com, menurut perusahaan keamanan Symantec dalam Internet Security Threat Report volume 17, Indonesia menempati peringkat 10 sebagai negara dengan aktivitas kejahatan siber terbanyak sepanjang tahun 2011. Indonesia menyumbang 2,4% kejahatan siber di dunia, angka ini naik 1,7% jika dibandingkan pada tahun 2010 lalu dimana Indonesia menempati peringkat 28 [6].

B. *Komputer Forensik*

Komputer berdasarkan Kamus Besar Bahasa Indonesia (KBBI) adalah alat elektronik otomatis yang dapat menghitung atau mengelolah data secara cermat menurut yang diinstruksikan, dan memberikan hasil pengolahan, serta dapat menjalankan sistem multimedia(film, music, televise, faksimile, dan sebagainya), biasanya terdiri atas unit pemasukan, unit pengeluaran, unit penyimpanan, serta unit pengontrolan. Sedangkan forensik menurut Kamus Besar Bahasa Indonesia (KBBI) adalah cabang ilmu kedokteran yang berhubungan dengan penerapan fakta-fakta medis pada masalah-masalah hukum. Komputer forensik adalah cabang ilmu forensik yang berkaitan dengan analisis dan pembuktian barang bukti kejahatan siber untuk pembuktian hukum sebagai barang bukti yang sah di mata hukum.

Menurut Muhammad Nur Al-Azhar dalam bukunya yang berjudul Digital Forensic, komputer forensik adalah ilmu forensik yang berkaitan dengan pemeriksaan dan analisis barang bukti elektronik berupa komputer pribadi (personal computer-PC), laptop/notebook, netbook, dan tablet. Pemeriksaan terhadap jenis barang bukti ini biasanya berkaitan dengan file recovery, yaitu suatu metode untuk mengambil file logical atau memunculkan kembali file yang sudah dihapus (deleted) maupun hilang (lost) dikarenakan tidak tercatat lagi di file system [3]. Sedangkan menurut Ruby Alamsyah, komputer forensik adalah suatu ilmu yang menganalisis barang bukti secara digital hingga dapat dipertanggungjawabkan di pengadilan. Yang termasuk barang bukti digital tersebut antara lain: laptop, handphone, notebook, dan alat teknologi lain yang memiliki tempat penyimpanan dan dapat dianalisa [7].

Saat ini kejahatan siber terus mengalami tren kenaikan, dikutip dari berita elektronik pada situs nasional.kompas.com, jumlah kejahatan siber pada tahun 2017 mengalami kenaikan sebesar tiga persen jika dibandingkan pada tahun 2016. Dengan adanya tren kenaikan kejahatan siber maka ilmu komputer forensik menjadi sangat dibutuhkan, karena barang bukti kejahatan siber adalah barang bukti yang rentan dan mudah rusak, sehingga dibutuhkan seseorang dengan keahlian khusus untuk mengungkap dan menganalisa bukti yang terdapat di komputer atau media penyimpanan digital. Didalam UU ITE pasal 43 ayat 5 huruj (J) dikatakan bawah “Meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik”.

C. *Forensic Imaging*

Forensic imaging adalah salah satu elemen dari ilmu komputer forensik yang berfungsi untuk melakukan akusisi terhadap media penyimpanan yang berstatus sebagai barang bukti dalam kejahatan siber. Barang bukti berupa media penyimpanan harus diduplikasikan guna penyidikan, agar barang bukti aslinya tidak mengalami perubahan sehingga integritas barang bukti tetap terjaga. Sesuai teori Locard Exchange Principle yang dikemukakan oleh Dr. Edmond Locard yang menyebutkan bahwa “*every contact leaves a trace*” artinya “setiap kontak meninggalkan jejak” [8]. Maksudnya adalah setiap kali seseorang melakukan tindak pidana kejahatan maka seseorang itu pasti akan meninggalkan jejak dalam bentuk apapun, maka tugas penyidik adalah

menelusuri jejak itu sampai mendapatkan barang buktinya. Maka teori Locard Exchange Principle pun berlaku di dalam kasus kejahatan siber, karena di dalam kasus kejahatan siber pun pasti akan meninggalkan barang bukti yang mungkin saja tertinggal di dalam media penyimpanan, selanjutnya media penyimpanan tersebut harus di akusisi guna menjaga mengamankan barang bukti yang asli.

Forensic imaging bekerja dengan menyalin secara langsung dari perangkat penyimpanan fisik secara bit demi bit, sektor demi sektor termasuk semua file, folder, unallocated, free dan slack space. Forensic imaging tidak hanya menyalin file–file yang terlihat saja, tetapi juga menyalin file–file yang telah terhapus yang tertinggal di slack dan free space dari media penyimpanan fisik. Dengan di aksusisinya barang bukti maka seorang investigator mendapatkan keseluruhan file yang terdapat di dalam media penyimpanan, baik file yang memang ada di dalam media penyimpanan tersebut ataupun file yang sudah dihapus sebelumnya.

D. File Ekstensi Hasil Akusisi

File format dengan ekstensi dd adalah *file* format ekstensi tertua karena ekstensi dd lahir sebelum ekstensi E01 maupun AFF dan ekstensi dd adalah *file* format yang termasuk ke dalam *file* tipe RAW. *File* dengan ekstensi dd bekerja dengan cara menyalin data media penyimpanan secara keseluruhan dengan cara menyalin setiap sektor dari media sumber penyimpanannya tanpa ada satu pun sektor yang terlewatkan. Namun *file* format dengan ekstensi dd memiliki kekurangan yaitu *file* hasil akusisi tidak mengandung *file* metadata, melainkan hanya berisi data orisinil saja yang didapatkan dari sumber penyimpanan yang diakusisi. Untuk informasi terkait metadata biasanya ditempatkan di dalam *file* yang berbeda. Menurut Simson L. Garfinkel dalam jurnalnya yang berjudul A*dvanced Forensic Format: An Open, Extensible Format For Disk Imaging* mengatakan bahwa mengakusisi media penyimpanan dengan cara menyalin sektor demi sektor dari penyimpanan orisinil dan menyimpannya di dalam satu *file* kemudian menaruh hasil *file* akusisi di media penyimpanan lainnya dan *file* hasil akusisi tersebut memiliki ukuran yang sama persis dengan penyimpanan orisinilnya itu disebut raw atau dd. *File* dengan ektensi dd adalah *file* yang tidak di kompresi sebelumnya, sehingga berimbas pada hasil *file* akusisinya yang memiliki ukuran yang sangat besar walaupun sebenarnya data yang diakusisi sangat kecil [9].

Sedangkan *file* format dengan ekstensi E01 adalah format ekstensi yang dimiliki oleh Guidance Software dan ekstensi E01 masuk ke dalam *file* dengan tipe Expert Witness Format (EWF). Cara kerja *file* dengan ekstensi E01 hampir sama dengan *file* ber ekstensi dd, *file* dengan ekstensi E01 bekerja dengan cara menyalin bit demi bit data dari media penyimpanan yang dijadikan sebagai sumber akusisi tanpa ada satu pun bit data yang terlewatkan. Yang membedakan antara ektensi dd dan E01 adalah, *file* format E01 akan membagi *file* hasil akusisi ke dalam beberapa segmen dan menyisipkan metadata berupa informasi penting baik terkait sumber penyimpanan yang diakusisi, maupun informasi tentang *file* hasil akusisi seperti *hash* MD5 maupun penguji yang melakukan akusisi. File dengan ekstensi E01 akan memiliki *header* pada file nya yang berisi tanggal dan waktu akusisi, nama penguji dan catata untuk file akusisi kemudian diikuti oleh *footer* yang berisikan informasi tentang *hashing* MD5 [9].

Selanjutnya *file* dengan format ekstensi Advanced Forensic Format (AFF) adalah format ekstensi yang dikenalkan dan dikembangkan oleh Simson L. Garfinkel. Advanced Forensic Format (AFF) diciptakan untuk memberikan pilihan alternatif bagi seorang investigator forensik di dalam memilih format ekstensi *file* hasil akusisinya. Simson L. Garfinkel dalam jurnalnya yang berjudul A*dvanced Forensic Format: An Open, Extensible Format For Disk Imaging* mengatakan bahwa *file* format dengan ekstensi AFF menawarkan dua keuntungan yang dapat diperoleh, pertama *file* hasil akusisi dengan ekstensi AFF lebih fleksibel karena dapat menyimpan metadata yang lebih besar dan kedua ekstensi AFF memiliki ukuran *file* yang lebih kecil jika dibandingkan dengan *file image* lainnya karena *file* dengan ekstensi AFF akan di kompres sehingga memiliki ukuran yang lebih kecil karena *file* format ekstensi lainnya tidak mengalami proses kompresi [9].

III. METODOLOGI

A. Metodologi Penelitian

Metodologi penelitian adalah prinsip dasar analisis proses ilmiah untuk mendapatkan data yang akan digunakan dalam kepentingan penelitian. Di dalam memecahkan masalahnya peneliti dapat menggunakan berbagai metode penelitian yang ada guna membantu peneliti untuk memecahkan masalah. Proses pengumpulan data menjadi sesuatu yang sangat penting di dalam proses penelitian, karena data yang terkumpul akan menjadi landasan teori suatu penelitian dan juga mampu meperkuat argumentasi proses penelitian itu sendiri. Di dalam pembuatan aplikasi Forensic Imaging Application Using Raspberry Pi peneliti menggunakan teknik studi literatur atau biasa disebut dengan studi pustaka sebagai metode pengumpulan datanya.

Studi pustaka adalah mengumpulkan informasi dan data dengan bantuan berbagai macam material yang ada di perpustakaan seperti dokumen, buku, catatan, majalah, kisah-kisah sejarah dsb [10]. Definisi lainnya, studi pustaka adalah mempelajari berbagai buku referensi serta hasil penelitian sebelumnya yang sejenis yang berguna untuk mendapatkan landasan terori mengenai masalah yang akan diteliti [11]. Dalam proses pembuatan aplikasi Forensic Imaging Application Using Raspberry Pi peneliti melakukan studi literatur atau studi pustaka dengan cara mencari jurnal ilmiah, artikel ilmiah, makalah ilmiah, dan tugas akhir baik di perpustakaan maupun di internet.

B. Analisis Kebutuhan Sistem

Untuk membangun aplikasi Forensic Imaging Application Using Raspberry Pi ini dibutuhkan proses analisis kebutuhan sistem agar mengetahui secara detail apa-apa saja kebutuhan yang dibutuhkan guna membangun sistem ini. Analisis yang dilakukan peneliti diantaranya analisis kebutuhan perangkat

keras, analisis kebutuhan perangkat lunak,, dan analisis kebutuhan keluaran.

1) Analisis Kebutuhan Perangkat Keras

Berikut kebutuhan perangkat keras yang diperlukan:

- Single Board Computer
- Power Adapter
- Keyboard dan Mouse
- LCD Monitor
- Microd SD dan Flashdrive

2) Analisis Kebutuhan Perangkat Lunak

Berikut kebutuhan perangkat lunak yang diperlukan:

- Sistem Operasi
- Text Editor
- Python
- QT Designer

3) Analisis Kebutuhan Keluaran

Analisis kebutuhan keluaran adalah analisis yang dilakukan untuk mengidentifikasi keluaran apa saja yang harus dihasilkan oleh aplikasi Forensic Imaging Application Using Raspberry Pi.

a) File Format .dd

Setelah aplikasi menyelesaikan proses akusisinya, maka aplikasi akan menghasilkan sebuah file hasil akusisi terhadap media penyimpanan dengan format .dd. File dengan format .dd adalah salah satu format yang sering digunakan di dalam lingkungan pengakusisian forensic imaging, dan file format .dd termasuk ke dalam jenis file tipe RAW.

b) File logging

Selain menghasilkan file akusisi dengan format .dd, aplikasi Forensic Imaging Application Using Raspberry Pi juga menghasilkan keluaran berupa file logging yang berisikan informasi detail mengenai data-data terkait media penyimpanan yang diakusisi oleh aplikasi. Keberadaan file logging menjadi sangat penting, karena file logging juga berguna sebagai dokumentasi dari hasil proses akusisi media penyimpanan.

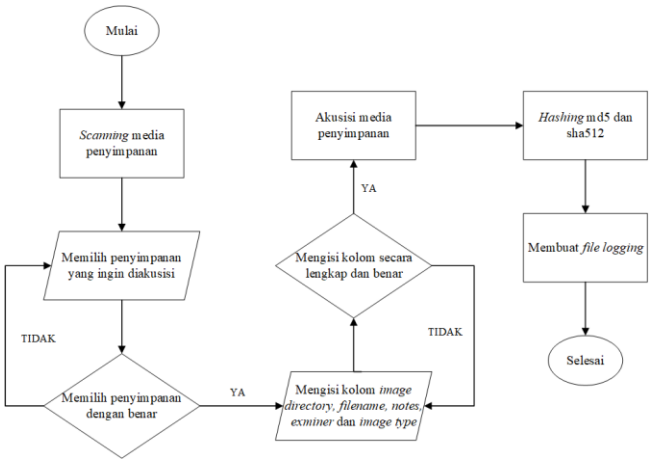
c) Hash MD5 dan SHA512

Didalam dunia forensik integritas adalah segalanya, maka ketika proses akusisi berjalan peneliti harus memastikan bahwa aplikasi Forensic Imaging Application Using Raspberry Pi tidak merubah nilai-nilai bit yang terdapat di media penyimpanan yang diakusisi. Untuk memastikan bahwa tidak ada bit-bit yang berubah, peneliti menggunakan MD5 dan SHA512 sebagai acuan integritas file hasil akusisi.

C. Perancangan Aplikasi

Perancangan menurut kamus besar Bahasa Indonesia (KBBI) adalah proses, cara, perbuatan merancang. Maka perancangan aplikasi adalah suatu proses yang dilakukan untuk mebuat konsep dan mendesain alur kerja sistem guna memenuhi kebutuhan aplikasi Forensic Imaging Application Using Raspberry Pi sehingg aplikasi dapat bekerja dengan baik sesuai dengan apa yang diharapkan oleh peneliti. Perancangan aplikasi meliputi tiga aspek berikut:

- Flowchart
- Pseudocode
- Desain Antarmuka



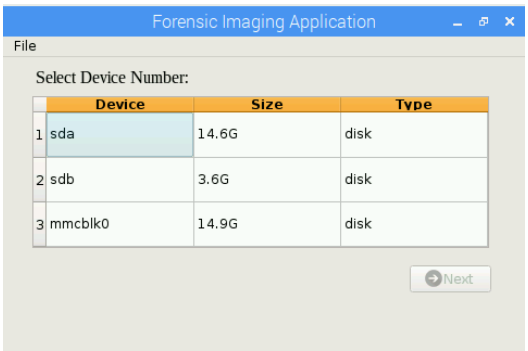
Gambar C.1 Flowchart Aplikasi

IV. IMPLEMENTASI

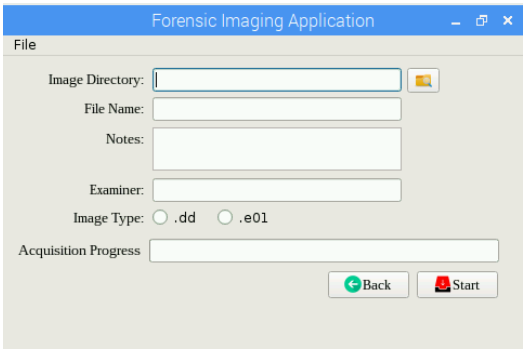
Implementasi menurut kamus besar Bahasa Indonesia (KBBI) adalah pelaksanaan atau penerapan. Maka tahap implementasi adalah tahap dimana peneliti menerapkan serta menuangakan ide dan konsep, rancangan, serta analisis yang telah dibuat pada pembahasan bab sebelumnya ke dalam aplikasi Forensic Imaging Application Using Raspberry Pi.

A. Implementasi Antarmuka Aplikasi

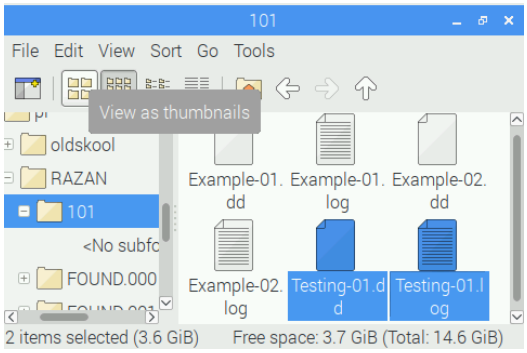
Untuk memulai tahap implementasi aplikasi langkah awal yang dilakukan adalah dengan mengimplementasikan antarmuka yang telah didesain pada tahap sebelumnya. Antarmuka aplikasi dapat dilihat pada gambar Gambar A.1 dan Gambar A.2.



Gambar A.1 Interface 1



Gambar A.2 Interface 2

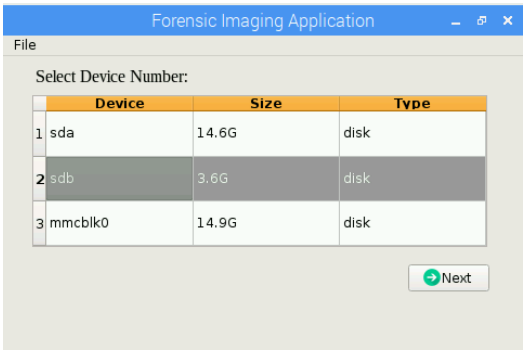


Gambar B.3 File Keluaran Apikasi

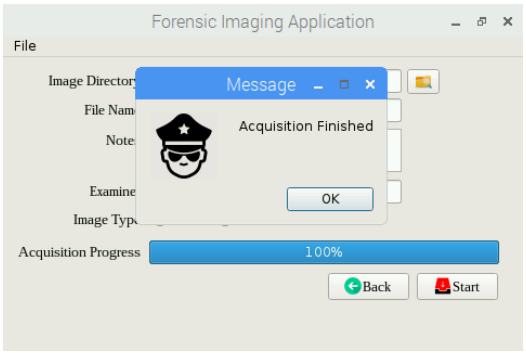
B. *Implementasi Proses Akusisi*

Selanjutnya untuk mengetahui apakah aplikasi dapat berjalan dengan baik, maka dilakukan implementasi proses akusisi. Proses akusisi aplikasi dilakukan dengan cara mengakusisi sebuah flashdrive berukuran 3,6GB kemudian menyimpan file hasil kloningannya di flashdrive yang lain yang memiliki ukuran kapasitas penyimpanan sebesar 14.6GB seperti yang terlihat pada Gambar B.1. Setelah proses akusisi dijalankan ternyata aplikasi dapat berjalan dengan baik, karena aplikasi dapat menyelesaikan proses akusisi dengan lancar seperti yang terlihat pada gambar Gambar B.2.

Setelah proses akusisi yang dijalankan selesai, maka seharusya aplikasi mengeluarkan 2 file, file pertama adalah file hasil akusisi, kemudian file kedua adalah file logging yang berisikan rincian detail informasi terkait proses akusisi yang dijalankan aplikasi Forensic Imaging Application Using Raspberry Pi seperti yang terlihat pada Gambar B.3.



Gambar B.1 Proses Akusisi



Gambar B.2 Proses Akusisi Selesai

C. *Pengujian Performa Aplikasi*

Tahap pengujian performa aplikasi adalah sebuah tahap yang dilakukan peneliti untuk mengetahui sejauh mana performa aplikasi yang peneliti buat dapat bekerja. Selain itu tahap pengujian performa aplikasi juga berguna untuk mengetahui apakah dengan menggunakan flash drive dengan merek yang berbeda tetapi ukurannya sama mempengaruhi kecepatan proses akusisi. Untuk menguji serta mengetahui sejauh mana performa aplikasi Forensic Imaging Application Using Raspberry Pi dapat bekerja, peneliti menguji aplikasi forensic imaging ini dengan cara melakukan enam kali percobaan proses akusisi, yang kemudian nantinya dari setiap proses akusisi yang telah dilakukan akan terlihat sejauh mana performa aplikasi dapat bekerja, baik dari sisi waktu proses akusisi maupun dari sisi kecepatan transfer datanya.

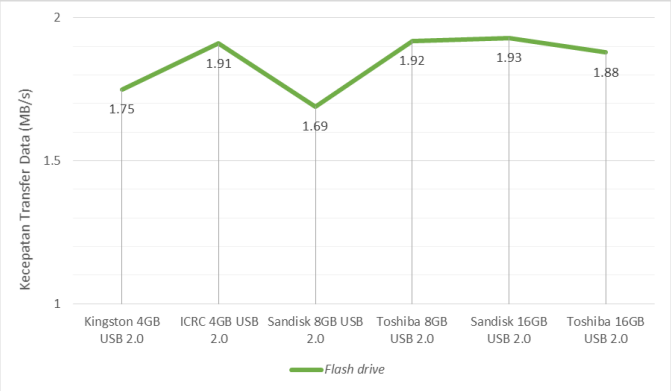
Proses akusisi sendiri menggunakan enam buah flash drive yang memiliki kapasitas penyimpanan dan merek yang berbeda, yakni Kingston 4GB, ICRC 4GB, Sandisk 8GB, Toshiba 8GB, Sandisk 16GB, dan Toshiba 16GB. Keenam flash drive tersebut nantinya akan diakusisi menggunakan aplikasi Forensic Imaging Application Using Raspberry Pi dan file hasil akusisi akan disimpan di flash drive Sandisk 64GB. Setelah keseluruhan proses percobaan akusisi selesai dilakukan, langkah selanjutnya adalah peneliti mencari tahu tentang kecepatan transfer data dari setiap proses akusisi yang telah dijalankan, untuk kemudian nantinya akan dicari nilai rata-rata kecepatan transfer datanya. Untuk detail rincian pengujian performa aplikasi Forensic Imaging Application Using Raspberry Pi dapat dilihat pada Tabel C.1

Tabel C.1 Pengujain Performa Aplikasi

No	Input	Output	Durasi Proses Akusisi	Kecepatan Trasnfer Data
1	Kingston 4GB USB 2.0	Sandisk 64GB USB 2.0	35 Menit	1,75 MB/s
2	ICRC 4GB USB 2.0	Sandisk 64GB USB 2.0	34 Menit	1,91 MB/s
3	Sandisk 8GB USB 2.0	Sandisk 64GB USB 2.0	73 Menit	1,69 MB/s
4	Toshiba 8GB USB 2.0	Sandisk 64GB USB 2.0	64 Menit	1,92 MB/s
5	Sandisk 16GB USB 2.0	Sandisk 64GB USB 2.0	129 Menit	1,93 MB/s

6	Toshiba 16GB USB 2.0	Sandisk 64GB USB 2.0	131 Menit	1,88 MB/s
Kecepatan Rata-rata Trasnfer Data				1,85 MB/s

Pada proses pengujian performa aplikasi Forensic Imaging Application Using Raspberry Pi yang dilakukan, peneliti mengakusisi tiga buah flash drive yang memiliki kapasitas penyimpanan dan merek yang berbeda, diantaranya Kingston 4GB, Sandisk 8GB, dan Sandisk 16GB. Kemudian setelah mendapatkan data waktu proses akusisi dan kecepatan transfer data akusisi, selanjutnya peneliti akan membandingkan proses waktu akusisi dan kecepatan transfer data akusisi dengan menggunakan flash drive yang memiliki ukuran yang sama tetapi dengan merek yang berbeda, flash drive yang peneliti gunakan adalah ICRC 4GB, Toshiba 8GB, dan Toshiba 16GB. Dengan proses uji coba tersebut diharapkan peneliti dapat mengetahui adakah pengaruh proses waktu akusisi dan kecepatan transfer data akusisi dengan flash drive yang memiliki merek berbeda tetapi ukuran kapasitas penyimpanan sama. Dari hasil uji coba yang dilakukan didapatkan bahwa menggunakan flash drive dengan ukuran kapasitas penyimpanan yang sama tetapi merek berbeda tidak mempengaruhi kecepatan transfer data akusisi dan nilai kecepatan rata-rata transfer data akusisi dari enam kali percobaan adalah sebesar 1,85 MB/s. Untuk melihat bagaimana grafik kecepatan transfer data dari enam percobaan yang telah dilakukan dapat dilihat pada Gambar C.1



Gambar C.1 Grafik Pengujian Aplikasi

REFERENCES

[1] D. Hutabarat, "Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia," 2018. [Online]. Available: https://kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media.

[2] I. Taufiqurrohman, N. Widiyasono, and H. Mubarok, "Pemanfaatan Raspberry Pi untuk Hacking dan Forensic dengan metode NIST (National Institute of Standards and Technology)," vol. 3, pp. 231–244, 2017.

[3] M. N. Al-Azhar, *Digital Forensic: panduan praktis investigasi komputer*. Jakarta: Salemba Empat, 2012.

[4] A. N. K. Movanita, "Ini Hasil Kerja Polri Perangi Kejahatan Siber Sepanjang 2017," 2017. [Online]. Available: https://nasional.kompas.com/read/2017/12/29/17233911/ini-hasil-kerja-polri-perangi-kejahatan-siber-sepanjang-2017.

[5] Y. Prayudi and D. S. Afrianto, "Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik," *Snati*, vol. 2007, no. Snati, pp. 1–4, 2007.

[6] Kompas, "Indonesia Masuk 10 Besar Penyumbang 'Cyber Crime' Terbanyak," 2012. [Online]. Available: https://tekno.kompas.com/read/2012/05/16/09403718/Indonesia.Masuk.10.Besar.Penyumbang.Cyber.Crime.Terbanyak.

[7] Bobsusanto, "Komputer Forensik: Pengertian Dan Tujuan Lengkap," 2014. [Online]. Available: http://www.sepengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan.html.

[8] A. Baharuddin, A. Ruskam, and A. Yacob, "Prinsip Asas Sains Forensik dari Perspektif Islam: Suatu Sorotan Literatur," *Sains Humanika*, vol. 2, no. 2008, pp. 7–15, 2015.

[9] S. L. Garfinkel, D. J. Malan, K.-A. Dubec, C. C. Stevens, and C. Pham, "Advanced Forensic Format: An Open, Extensible Format for Disk Imaging," *Adv. Digit. Forensics II FIP Int. Conf. Digit. Forensics*, vol. 222, pp. 17–31, 2006.

[10] Mardalis, *Metode penelitian : suatu pendekatan proposal*. Jakarta: PT. Bumi Aksara, 2002.

[11] J. Sarwono, *Metode penelitian kuantitatif & kualitatif*. Yogyakarta: Graha Ilmu, 2006.